FIDO2, CTAP 2.1, and WebAuthn 2: Provable Security and Post-Quantum Instantiation

(Full version v1.1 with supplementary materials, including full proofs)

Nina Bindel
SandboxAQ
Palo Alto, USA
nina.bindel@sandboxaq.com

Cas Cremers
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany
cremers@cispa.de

Mang Zhao
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany
mang.zhao@cispa.de

***Abstract*—The FIDO2 protocol is a globally used standard for passwordless authentication, building on an alliance between major players in the online authentication space. While already widely deployed, the standard is still under active development. Since version 2.1 of its CTAP sub-protocol, FIDO2 can potentially be instantiated with post-quantum secure primitives.**

We provide the first formal security analysis of FIDO2 with the CTAP 2.1 and WebAuthn 2 sub-protocols. Our security models build on work by Barbosa et al. for their analysis of FIDO2 with CTAP 2.0 and WebAuthn 1, which we extend in several ways. First, we provide a more fine-grained security model that allows us to prove more relevant protocol properties, such as guarantees about token binding agreement, the `None` attestation mode, and user verification. Second, we can prove post-quantum security for FIDO2 under certain conditions and minor protocol extensions. Finally, we show that for some threat models, the downgrade resilience of FIDO2 can be improved, and show how to achieve this with a simple modification.

I. Introduction

One of the largest projects globally to mitigate the problems of weak passwords is the FIDO protocol by the Fast Identity Online (FIDO) Alliance. The alliance has brought together over forty key companies in the online authentication space, including Amazon, Apple, Google, Intel, Microsoft, RSA, VISA, and Yubico, and has brought security devices to the wider public to improve the security of important logins.

The FIDO2 standard – the latest of the protocols – is built around two sub-protocols that are critical for enabling security-device supported logins. The first one is *WebAuthn*, which is a protocol between web applications, web browsers, and authenticator hardware tokens. At its core, WebAuthn allows a website (a Relying Party) to perform a *passwordless* challenge-response protocol with a token (an Authenticator) – where the browser acts as an intermediary – and challenges are signed by credential keys generated and stored in the token. The protocol supports multiple optional modes and features, such as attestation and user involvement.

This research was supported by the Microsoft Identity Project Research Grant "Developing Post-Quantum Secure Identity Services" from Microsoft Security Response Center (MSRC).

The second relevant protocol is *CTAP* (Client To Authenticator Protocol), which is a protocol between an authenticator (e.g., a hardware security token) and a client (e.g., a browser). The goal of the protocol is to bind (and thus to restrict) which clients can use the authenticator's API (Application Programming Interface). To enable API access, the client asks the user to enter the authenticator's PIN; this PIN is checked by the token, and a shared secret is established that represents the binding and is used to authenticate all subsequent client accesses to the authenticator.

The FIDO2 standard, while already widely deployed, is subject to ongoing development. Previous versions of these standards have been studied. However, as we will see later, the main study has made strong assumptions that do no hold for the majority of deployed systems, such as relying on the attestation[1] mode to prove core properties. Moreover, the recently proposed CTAP 2.1 [6] includes a completely new base protocol that has not yet been analyzed in any framework.

Notably, the most recent version of the FIDO2 standard with CTAP 2.1 and WebAuthn 2 [12] appears to be "post-quantum ready", because it enables a mode of operation that only uses on symmetric cryptographic primitives, digital signatures, and KEMs (Key Encapsulation Mechanisms). However, no post-quantum instantiations have been proposed, nor has the CTAP 2.1 protocol received any analysis. In this work we set out to fill this gap: analyse the newest version and assess its post-quantum security.

Contributions

1) We prove that FIDO2 with WebAuthn 2 and CTAP 2.1 is provably secure against classical adversaries in a fine-grained security and protocol model. Our security models are more fine-grained or cover other aspects than previous versions such as [3, 11]. For example, we add important aspects such as algorithm negotiation, required user actions, and

[1]In the context of WebAuthn, "attestation" means identification of device type/manufacturer, and notably does not imply any check of the software that is being executed.

token binding. For CTAP 2.1, our security proofs confirm the stronger containment properties (reduced "blast radius") offered by the protocol compared to CTAP 2.0. Our analysis of WebAuthn 2 also has new implications for WebAuthn 1: we provide the first guarantees of the most widely used `None` attestation mode, user verification, user presence, and token binding.

2) We prove that if FIDO2 with WebAuthn 2 and CTAP 2.1 is instantiated with post-quantum (PQ) secure KEMs and signatures, then it is secure against quantum adversaries in the same model. We give concrete suggestions for PQ secure algorithm and negotiation design choices, including classical-PQ hybrids as suggested by standardization agencies, such as NIST (National Institute for Standards and Technology) [8].
3) We propose a simple improvement to WebAuthn 2 that improves its resilience to certain types of downgrade attack. While these can only occur for strong threat models, these improvements yield stronger classical security against broken cryptographic primitives, and are even more relevant for their PQ instantiations.

Overview

We provide a high-level background on FIDO2's CTAP and WebAuthn protocols, and previous analysis models, in Section II. Next, we define notational preliminaries in Section III. Afterwards, we first present the analysis of WebAuthn 2 in Section IV, and then that of CTAP 2.1 in Section V. We prove the security of their composition in FIDO2 in Section VI. We then return to related work in Section VII, and describe limitations and future work in Section VIII.

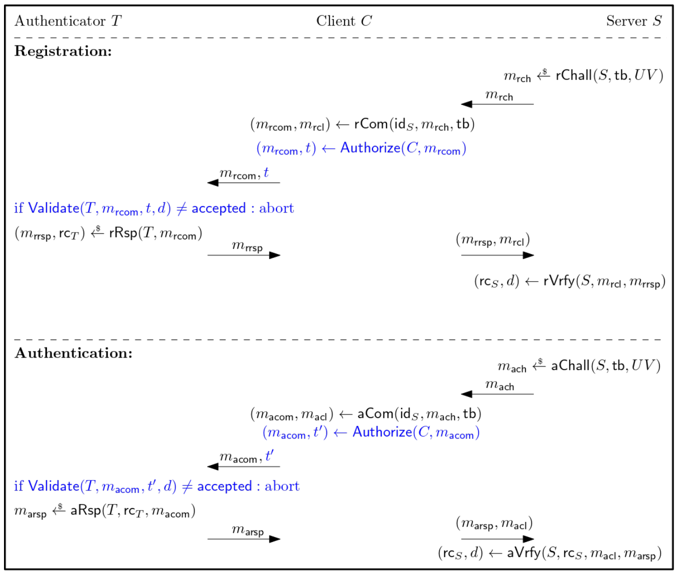
In the appendix, we give more detailed descriptions of the algorithms modeled, full proofs, and further details.

II. Background

A. High-level overview of FIDO2

The FIDO2 protocol incorporates the two sub-protocols WebAuthn and CTAP, and involves four main types of parties: relying parties (e.g., a server, online service, or an operating system feature), authenticators (e.g., token or security key), clients (e.g., web browsers or other applications), and users. WebAuthn typically leaves the users implicit in the description of the authenticator.

Initially, the client and authenticator run the setup and binding phase of the CTAP 2.1 protocol. Once this is completed, relying parties can register and authenticate authenticators by running WebAuthn 2 through CTAP 2.1, which we depict in Figure 1. WebAuthn 2 is used in two phases: in the registration phase, an authenticator produces a fresh credential key pair whose public key is sent to the relying party and stored. Afterwards, each time the relying party wants to authenticate a user, it performs a challenge-response protocol with the authenticator who signs the challenge using the credential private key, which is then verified by the relying party. We next expand the two protocols in more detail.



Authenticator T
Client C
Server S
Registration:
$m_{\mathsf{rch}} \xleftarrow{\$} \mathsf{rChall}(S, \mathsf{tb}, UV)$
m_{rch}
$(m_{\mathsf{rcom}}, m_{\mathsf{rcl}}) \leftarrow \mathsf{rCom}(\mathsf{id}_S, m_{\mathsf{rch}}, \mathsf{tb})$
$(m_{\mathsf{rcom}}, t) \leftarrow \mathsf{Authorize}(C, m_{\mathsf{rcom}})$
m_{rcom}, t
if $\mathsf{Validate}(T, m_{\mathsf{rcom}}, t, d) \neq \mathsf{accepted}$: abort
$(m_{\mathsf{rrsp}}, \mathsf{rc}_T) \xleftarrow{\$} \mathsf{rRsp}(T, m_{\mathsf{rcom}})$
m_{rrsp}
$(m_{\mathsf{rrsp}}, m_{\mathsf{rcl}})$
$(\mathsf{rc}_S, d) \leftarrow \mathsf{rVrfy}(S, m_{\mathsf{rcl}}, m_{\mathsf{rrsp}})$
Authentication:
$m_{\mathsf{ach}} \xleftarrow{\$} \mathsf{aChall}(S, \mathsf{tb}, UV)$
m_{ach}
$(m_{\mathsf{acom}}, m_{\mathsf{acl}}) \leftarrow \mathsf{aCom}(\mathsf{id}_S, m_{\mathsf{ach}}, \mathsf{tb})$
$(m_{\mathsf{acom}}, t') \leftarrow \mathsf{Authorize}(C, m_{\mathsf{acom}})$
m_{acom}, t'
if $\mathsf{Validate}(T, m_{\mathsf{acom}}, t', d) \neq \mathsf{accepted}$: abort
$m_{\mathsf{arsp}} \xleftarrow{\$} \mathsf{aRsp}(T, \mathsf{rc}_T, m_{\mathsf{acom}})$
m_{arsp}
$(m_{\mathsf{arsp}}, m_{\mathsf{acl}})$
$(\mathsf{rc}_S, d) \leftarrow \mathsf{aVrfy}(S, \mathsf{rc}_S, m_{\mathsf{acl}}, m_{\mathsf{arsp}})$

Fig. 1. The main message flow of FIDO2 with WebAuthn 2 with attestation type `None` is shown in black. The blue flows indicate interaction with the third CTAP 2.1 phase (i.e. after CTAP 2.1's setup and binding phases.) The user is left implicit in the flow of the authenticator token. For registration, the server generates a challenge. This is forwarded through the client to the token (possibly authorized through CTAP 2.1), which returns a public credential key and additional data, which is stored by the server. Afterwards, for each authentication, a similar process occurs, but the token now signs challenge and data with the with the signing key corresponding to the public credential key that was registered previously.

1) WebAuthn: The goal of WebAuthn is to enable relying parties to authenticate users through authenticator tokens using a challenge-response protocol. WebAuthn is specified as an API rather than as a protocol; in practice, a common scenario is that the relying party is an online service with server backend code and Javascript running in the browser, and the server's Javascript then uses the WebAuthn API supported by the browser to communicate with the token. The first interaction, when the server communicates with the token, is called registration phase. In this phase, the server S sends a challenge message (m_{rch}) to the token through the client C. This challenge contains a random nonce, parameters such as whether user verification (UV) is required, and optionally a value tb that uniquely identifies the underlying channel (in practice typically identifying a unique Transport Layer Security (TLS) connection, which can provide channel binding to prevent some types of man-in-the-middle attacks).

The client C parses the challenge message and turns it into a command message (m_{rcom}) and a client message (m_{rcl}), and forwards the command message to the token T. The token T produces a credential public-private key pair, which is bound to the server S and enables S to perform verification during the following authentication phase, and outputs a response message (m_{rrsp}). The client then returns this together with the client message to the server S. The response message specifies the type of "attestation statement" selected by the token, which enables the server S to perform verification during the registration phase, and includes the credential public key. WebAuthn 2 supports five attestation types; these include `Basic` and `None` [2]. Tokens that support type `Basic` are equipped with an attestation key pair, which is specific to the token model, but not unique: by design, the attestation key pair is shared by a batch of tokens[3]. The `None` mode provides no token-specific information and is supported by all tokens.

The authentication phase is executed after the completion of the registration in a slightly different way. When the client parses the challenge message (m_{ach}) from the server S and turns it into a command message (m_{acom}) and a client message (m_{acl}), followed by sending the command message to the token T. The token T produces a response message (m_{arsp}) signed using the credential private key, and bound to the server S. The server S finally accepts a response message and a client message only when they pass verification using the corresponding credential public key.

2) CTAP: (Client To Authenticator Protocol) The CTAP protocol allows the client (e.g., a browser) to communicate with the authenticator. Using only WebAuthn, any application might try to access a token to request credential keys or responses to challenges. In practice, we would like to limit the client applications that are allowed to use the token's API. One of the goals of the CTAP protocol is to limit this access.

CTAP proceeds in three phases. In the setup phase, a client C' initializes a PIN, which is collected from the user, into the token T. In the binding phase, the client C (not necessarily same as C') and the token T exchange a shared binding state, if the client C is able to provide information about the PIN stored on the token T. The binding state is expected to uniquely bind the client C to the token T. If the client C fails 3 times consecutively, the token T is rebooted and all previously established binding states are reset. If the client C fails 8 times in total, the token T is blocked. When the above preparation is done, the client C authorizes any command message by outputting a tag t, which is forward to the token T along with the command message itself. The token T only proceeds upon the positive decision d from the user, e.g., by pressing a button, and then validates the command message and the tag. In particular, a token only produces a response message in WebAuthn when its validation process in CTAP succeeds. Note that the binding state is repeatedly used during a period, the length of which depends on the concrete CTAP version and the type of token devices, and will be blocked afterwards.

B. Previous analysis by Barbosa et al. [2, 3]

Barbosa et al. [2, 3] gave the first formal analysis of FIDO2, and in particular the version with CTAP 2.0 and WebAuthn 1. We recall some important conclusions.

1) **WebAutnn**: Barbosa et al. formalize WebAuthn 1 as a *passwordless authentication* (PlA) protocol. Assuming the uniqueness of each attestation key pair, they then prove that WebAuthn 1 with attestation type `Basic` provides *secure passwordless authentication*. However, since each attestation key pair is in fact necessarily shared by a large batch of tokens (often called *batch attestation*), their main theorem establishes uniqueness properties of partnering for each batch of tokens that share the same attestation key pair instead of each single token. Moreover, their analysis has no clear implications for the `None` mode.
2) **CTAP**: Barbosa et al. formalize CTAP 2.0 as a *PIN-based access control for authenticators* (PACA) protocol. Then, they prove the *Unforgeability with trusted binding* ($\mathsf{UF\text{-}t}$) of CTAP 2.0. In Section VII-A we show that the difference between CTAP 2.0 and CTAP 2.1 is substantial, which means the previous results cannot simply be translated.

Thus, Barbosa et al. [2] provided the first formal analysis of FIDO2 with CTAP 2.0 and WebAuthn 1, which was ground-breaking in many ways, but as a first attempt also left open many questions and subtle proof issues. We provide a detailed comparison between [2] and our work in Section VII-B.

III. Preliminaries

Notation. In this paper, we write PQ in place of "post-quantum". We write λ for the security parameter of each protocol. We assume that λ is the implicit input of each algorithm if it is unambiguous. Let PPT and QPT respectively denote the probabilistic and quantum turning machines (e.g., adversaries) that are executed in polynomial time. For a finite set S, we use $x \overset{\$}{\leftarrow} S$ to represent sampling x uniformly at random from set S. For a value y, we write $x \leftarrow y$ for assigning y to x. For a probabilistic algorithm Y (resp. a deterministic algorithm Y'), we use $x \overset{\$}{\leftarrow} Y(z)$ (resp. $x \leftarrow Y'(z)$) to denote assigning the output of the execution Y (resp. Y') on input z. For an integer n, we denote by $[n] := \{1, ...n\}$ the set of integers from 1 to n. By $\{0,1\}^\star$ we denote the set of all strings with finite length. For each string x, let $|x|$ denote the bit-length of x. All undefined variables are initialized with a specific symbol $\perp$. In this paper, we use $\epsilon_{\Pi}^{\mathsf{sec}}$ to denote the advantage of any Compl adversary that breaks sec security of Π protocol, if the complexity $\mathsf{Compl} \in \{\mathsf{PPT}, \mathsf{QPT}\}$ is unambiguous from the context. We introduce two novel security notions in Section A and the cryptographic building blocks and all other security notions in Section E in the appendix. We omit the analysis of protocol correctness for page limitations.

IV. WebAuthn 2 and Extended Passwordless Authentication Protocols

For our analysis of WebAuthn 2 and its PQ instantiation, we follow the high-level approach from [2, 3], which proposed the class of PlA protocols that generalizes WebAuthn 1, and proposed a corresponding security notion. We provide a more fine-grained model of WebAuthn 2, notably including the default mode `None` in which no attestation is performed, as well as the user presence and user verification checks, and a stronger threat model. We compare the details in our work and [2] in Section VII-B These aspects and their security

[2]The remaining three modes are: `Self`, `AttCA`, and `AnonCA`, which are less common and out of scope of this work.

[3]The number of tokens in each batch is at least 100,000, cf. [12, Section 14.4.1].

cannot be captured in the PIA class without modification. In this section, we therefore first extend [2]'s formalisation and propose the *extended* PIA (ePIA) protocol class, and instantiate WebAuthn 2 as an ePIA protocol. We then introduce our new model to define *secure passwordless authentication* (auth) for ePIA protocols and prove that WebAuthn 2 satisfies it. We then show how to instantiate PQ-WebAuthn 2. Our proof of auth implies PQ security against a PPT if the schemes used in a session are PQ secure. We return to downgrade attacks in Section IV-E.

A. *Extended Passwordless Authentication Protocols (*ePIA*)*

Similar to the PIA model from [2], we define our *extended passwordless authentication protocol* ePIA by two phases, Register and Authenticate:

Register**:** a two-pass challenge-response protocol run between a token T, a client C, and a server S, which is run at most once per tuple (T, S) (i.e., not for additional clients). At the end, both T and S hold registration contexts, which are relevant for subsequent authentications. Register can be decomposed into the following algorithms:

rChall**:** inputs a server S, a token binding state tb, and a user verification condition $UV \in \{\mathsf{true}, \mathsf{false}\}$, and outputs a challenge message m_{rch}, i.e., $m_{\mathsf{rch}} \xleftarrow{\$} \mathsf{rChall}(S, \mathsf{tb}, UV)$.

rCom**:** inputs the intended server identity id_S, a challenge message m_{rch}, and a token binding state tb, and outputs a client message m_{rcl} and a command message m_{rcom}, i.e., $(m_{\mathsf{rcom}}, m_{\mathsf{rcl}}) \leftarrow \mathsf{rCom}(\mathsf{id}_S, m_{\mathsf{rch}}, \mathsf{tb})$.

rRsp**:** inputs a token T and a command message m_{rcom} and outputs a response message m_{rrsp} and an token-associated registration context rc_T, i.e., $(m_{\mathsf{rrsp}}, \mathsf{rc}_T) \xleftarrow{\$} \mathsf{rRsp}(T, m_{\mathsf{rcom}})$.

rVrfy**:** inputs a server S, a client message m_{rcl}, and a response message m_{rrsp}, and outputs a server-associated registration context rc_S and a decision bit $d \in \{0, 1\}$ to indicate whether the registration request was accepted ($d = 1$) or not ($d = 0$), i.e., $(\mathsf{rc}_S, d) \leftarrow \mathsf{rVrfy}(S, m_{\mathsf{rcl}}, m_{\mathsf{rrsp}})$.

Authenticate**:** a two-pass challenge-response protocol run between a token T, a client C, and a server S after a successful run of Register, in which both T and S generated their registration contexts. At the end, S either accepts or rejects the authentication attempt. Similarly to Register, Authenticate can be decomposed into four algorithms:

aChall**:** inputs a server S, a token binding state tb, and a user verification condition $UV \in \{\mathsf{true}, \mathsf{false}\}$, and outputs a challenge message m_{ach}, i.e., $m_{\mathsf{ach}} \xleftarrow{\$} \mathsf{aChall}(S, \mathsf{tb}, UV)$.

aCom**:** inputs the intended server identity id_S, a challenge message m_{ach}, and a token binding state tb, and outputs a client message m_{acl} and a command message m_{acom}, i.e., $(m_{\mathsf{acl}}, m_{\mathsf{acom}}) \leftarrow \mathsf{aCom}(\mathsf{id}_S, m_{\mathsf{ach}}, \mathsf{tb})$.

aRsp**:** inputs a token T along with its associated registration context rc_T, and a command message m_{acom}, and outputs a response message m_{arsp} and the updated registration context rc_T, i.e., $(m_{\mathsf{arsp}}, \mathsf{rc}_T) \xleftarrow{\$} \mathsf{aRsp}(T, \mathsf{rc}_T, m_{\mathsf{acom}})$.

aVrfy**:** inputs a server S along with its associated registration context rc_S, a client message m_{acl}, and a response message m_{arsp}, and outputs the updated registration context rc_S and a decision bit $d \in \{0, 1\}$ indicating whether the authentication request was accepted by the user (output 1) or not (output 0), i.e., $(\mathsf{rc}_S, d) \leftarrow \mathsf{aVrfy}(S, \mathsf{rc}_S, m_{\mathsf{acl}}, m_{\mathsf{arsp}})$.

To model concurrent or sequential sessions of a server S (associated with ID id_S) and sequential sessions of a token T, we use π^i_S and π^j_T to denote their i-th and j-th instances respectively, i.e., $S = \{\pi^i_S\}_i$ and $T = \{\pi^j_T\}_j$. Our new abstraction retains the black message flow from Figure 1.

B. *WebAuthn 2 is an ePIA Protocol*

We use the following session variables for WebAuthn 2.

$\pi^i_S.\mathsf{ch}$: challenge nonce sampled in this session

$\pi^i_S.\mathsf{uid}$: user identifier sampled in this session

$\pi^i_S.\mathsf{tb}$: token binding state used in this session

$\pi^i_S.UV$: user verification condition, indicating whether the user should be verified, e.g., via PIN or Biometrics

$\pi^i_S.UP$: user presence condition, indicating whether the presence of the user is sufficient; constant true value

$\pi^i_S.\mathsf{pkCP}$: list of digital signature schemes accepted by S

$\pi^j_T.\mathsf{suppUV}$: indicates whether T supports user verification

$\pi^i_S.\mathsf{st}_{\mathsf{exe}}, \pi^j_T.\mathsf{st}_{\mathsf{exe}} \in \{\bot, \mathsf{running}, \mathsf{accepted}\}$: execution state of each session

$\pi^i_S.\mathsf{agCon}, \pi^j_T.\mathsf{agCon}$: the content that is expected to be agreed with other parties. These variables are protocol-specific. In WebAuthn 2, both variables include the server identifier, the hash of the client messages, the UP and UV conditions, and other session-specific data.

$\pi^i_S.\mathsf{sid}, \pi^j_T.\mathsf{sid}$: session identifiers. Two distinct sessions that have communicated with each other are expected to own the identical session identifiers. These variables are protocol-specific. In WebAuthn 2, both variables include the hash of the server identifier and other session-specific data.

Intuitively, the registration phase starts with the execution of rChall algorithm, where the server S samples random challenge nonce $\pi^i_S.\mathsf{ch}$ and user identifier $\pi^i_S.\mathsf{uid}$, initializes the user verification condition $\pi^i_S.UV$, and outputs the challenge message m_{rch}, which includes the above data as well as the server domain id_S and accepted list $\pi^i_S.\mathsf{pkCP}$. Additionally, the server also stores the token binding states $\pi^i_S.\mathsf{tb}$, which is shared with a client. Receiving m_{rch}, the client is supposed to verify the server domain followed by computing the hash value h of the client message $m_{\mathsf{rcl}} := (\mathsf{ch}, \mathsf{tb})$. Compared with m_{rch}, the output command message m_{rcom} replaces ch with h and add a constant user presence condition $UP := \mathsf{true}$. Receiving m_{rcom}, the token T picks a suitable signature scheme Σ in the list pkCP (if available) and checks whether the user verification mechanism is supported (if required). After that, T samples a public-private key pair (pk, sk) of Σ and a credential identifier cid, followed by initializing the associated registration context $\mathsf{rc}_T[\mathsf{id}_S]$ and the agreed content $\pi^j_T.\mathsf{agCon}$. The session identifier $\pi^j_T.\mathsf{sid}$ is set to the hash of the server domain, the credential identifier, and the initial counter $n := 0$. The output response message m_{rrsp} includes the session identifier $\pi_T^j.\text{sid}$ as well as pk, Σ, UP and UV. The server S finally inputs both m_{rcl} and m_{rrsp} and executes a number of checks. If all checks pass, S also initializes its associated registration context $\text{rc}_S[\text{cid}]$ and the agreed content $\pi_S^i.\text{agCon}$. The session identifier $\pi_S^i.\text{sid}$ is identical to $\pi_T^j.\text{sid}$.

The authentication phase is very similar. The crucial difference is that the token outputs a signature, which signs the $\pi_S^i.\text{agCon}$-relevant data using the private key sk of Σ. Moreover, the session identifiers of token and servers additionally include the hash of the client message m_{acl}.

We give the concrete definition of algorithms of WebAuthn 2 with the default attestation type `None` in Section C.

C. Security Experiment for ePIA

The desired security property is that a server accepts an authentication response if and only if it was generated by a unique honest partnered token session. We capture it by our auth security experiment in Figure 2.

a) Threat Model: To closely capture the official security statement[4], we assume that all communication channels in the registration phase are authenticated. In contrast, there are no security assumptions on the communication channels between token, client, and server in the authentication phase. We assume that the users always provide the user presence or user verification confirmation when it is required and leave the users implicit in the security model. We assume the identifier id_S of each server S is unique. Unlike [2], we do *not* assume tokens to be “tamper-proof”, i.e., the adversary is allowed to corrupt locally stored registration contexts.

b) Oracles: During the game execution the adversary $\mathcal{A}$ can create new servers and tokens through the oracles NEWS and NEWTPLA. In particular, the adversary can customize the concrete setting of the created parties, i.e., the supported signature list of the server and whether the token supports user verification. By invoking the REGISTER oracle, $\mathcal{A}$ is able to eavesdrop on honest registrations between servers and tokens of its choice. Moreover, via the oracles CHALLENGE, RESPONSE and COMPLETE, $\mathcal{A}$ can actively interfere during authentication. Note that sessions which have accepted or rejected can no longer be queried. Furthermore, the adversary $\mathcal{A}$ can also query the CORRUPT oracle to reveal a token's registration context related to a server.

c) Session Partnering: Partnering identifies token and server sessions that are successfully communicating with each other as expected, and is encoded through matching session identifiers. More precisely, we say a server session π_S^i *partners with a token session* π_T^j if and only if $\pi_S^i.\text{sid} = \pi_T^j.\text{sid} \neq \perp$. We say a server session π_S^i *partners with a token* T if it partners with one of T's sessions. We say a token T is the *registration partner* of a server S, if the registration context of T at S has been set, i.e., $\text{rc}_T[\text{id}_S] \neq \perp$.

[4]“Under the assumption that a registration ceremony is completed securely, and that the authenticator maintains confidentiality of the credential private key, subsequent authentication ceremonies using that public key credential are resistant to man-in-the-middle attacks” [12, Section 13.4.4]

d) Winning Conditions: We call a server session a *test session* if it accepts a response message. We say that the secure passwordless authentication for an ePIA holds if there exists a test session π_S^i such that none of the following winning conditions holds:

1) the non-$\perp$ session identifiers of two token sessions collide.
2) the non-$\perp$ session identifiers of two server sessions collide.
3) π_S^i does not partner with T and CORRUPT(S, T) was not queried (i.e., the registration context of T at S has not been revealed), where T is any registration partner of S.
4) the agreed contents of a pair of partnered server session $\pi_{S'}^{i'}$ and token sessions $\pi_{T'}^{j'}$ are distinct and CORRUPT(S', T') has not been queried.

```
$\text{Expt}^{\text{auth}}_{\text{ePIA},\text{Compl}}(\mathcal{A})$:
    $\mathcal{L}_{\text{frsh}} \leftarrow \emptyset$
    $\text{win-auth} \leftarrow 0$
    $() \xleftarrow{\$} \mathcal{A}^{\mathcal{O}}(1^\lambda)$
    return win-auth

$\text{regPartner}(S)$:
    if $\exists T$ such that $\text{rc}_T[\text{id}_S] \neq \perp$
        return $T$
    return $\perp$

$\text{Win-auth}(S, i)$:
    if $\exists (T_1, j_1), (T_2, j_2)$ such that $(T_1, j_1) \neq (T_2, j_2)$ and $\pi_{T_1}^{j_1}.\text{sid} = \pi_{T_2}^{j_2}.\text{sid} \neq \perp$ : return 1
    if $\exists (S_1, i_1), (S_2, i_2)$ such that $(S_1, i_1) \neq (S_2, i_2)$ and $\pi_{S_1}^{i_1}.\text{sid} = \pi_{S_2}^{i_2}.\text{sid} \neq \perp$ : return 1
    $T \leftarrow \text{regPartner}(S)$
    if $(S, T) \in \mathcal{L}_{\text{frsh}}$ and $\neg\exists j$ such that $\pi_S^i.\text{sid} = \pi_T^j.\text{sid}$: return 1
    if $\exists (S', i'), (T', j')$ such that $\pi_{S'}^{i'}.\text{sid} = \pi_{T'}^{j'}.\text{sid} \neq \perp$ and $(S', T') \in \mathcal{L}_{\text{frsh}}$ and $\pi_{S'}^{i'}.\text{agCon} \neq \pi_{T'}^{j'}.\text{agCon}$: return 1
    return 0

REGISTER$((S, i), (T, j), \text{tb}, UV)$:
    if $\text{pkCP}_S = \perp$ or $\text{suppUV}_T = \perp$ or $\pi_S^i \neq \perp$ or $\pi_T^j \neq \perp$ or $\text{rc}_T[S] \neq \perp$
        return $\perp$
    $\pi_S^i.\text{pkCP} \leftarrow \text{pkCP}_S$
    $\pi_T^j.\text{suppUV} \leftarrow \text{suppUV}_T$
    $m_{\text{rch}} \xleftarrow{\$} \text{rChall}(\pi_S^i, \text{tb}, UV)$
    $(m_{\text{rcom}}, m_{\text{rcl}}) \leftarrow \text{rCom}(\text{id}_S, m_{\text{rch}}, \text{tb})$
    $(m_{\text{rrsp}}, \text{rc}_T) \xleftarrow{\$} \text{rRsp}(\pi_T^j, m_{\text{rcom}})$
    $(\text{rc}_S, d) \xleftarrow{\$} \text{rVrfy}(\pi_S^i, m_{\text{rcl}}, m_{\text{rrsp}})$
    $\mathcal{L}_{\text{frsh}} \leftarrow \mathcal{L}_{\text{frsh}} \cup \{(S, T)\}$
    return $(m_{\text{rch}}, m_{\text{rcl}}, m_{\text{rcom}}, m_{\text{rrsp}}, d)$

NEWS$(S, \text{pkCP})$:
    if $\text{pkCP}_S \neq \perp$
        return
    $\text{pkCP}_S \leftarrow \text{pkCP}$
    return

NEWTPLA$(T, \text{suppUV})$:
    if $\text{suppUV}_T \neq \perp$
        return
    $\text{suppUV}_T \leftarrow \text{suppUV}$
    return

CHALLENGE$((S, i), \text{tb}, UV)$:
    if $\text{pkCP}_S = \perp$ or $\pi_S^i \neq \perp$
        return $\perp$
    $\pi_S^i.\text{pkCP} \leftarrow \text{pkCP}_S$
    $m_{\text{ach}} \leftarrow \text{aChall}(\pi_S^i, \text{tb}, UV)$
    return $m_{\text{ach}}$

RESPONSE$((T, j), m_{\text{acom}})$:
    if $\text{suppUV}_T = \perp$ or $\pi_T^j \neq \perp$
        return $\perp$
    $\pi_T^j.\text{suppUV} \leftarrow \text{suppUV}_T$
    $(m_{\text{arsp}}, \text{rc}_T) \xleftarrow{\$} \text{aRsp}(\pi_T^j, \text{rc}_T, m_{\text{acom}})$
    return $m_{\text{arsp}}$

COMPLETE$((S, i), m_{\text{acl}}, m_{\text{arsp}})$:
    if $\pi_S^i = \perp$ or $\pi_S^i.\text{st}_{\text{exe}} \neq \text{running}$
        return $\perp$
    $(\text{rc}_S, d) \xleftarrow{\$} \text{aVrfy}(\pi_S^i, \text{rc}_S, m_{\text{acl}}, m_{\text{arsp}})$
    if $d = 1$
        $\text{win-auth} \leftarrow \text{Win-auth}(S, i)$
    return $d$

CORRUPT$(S, T)$:
    if $\text{rc}_T[S] = \perp$
        return $\perp$
    $\mathcal{L}_{\text{frsh}} \leftarrow \mathcal{L}_{\text{frsh}} \setminus \{(S, T)\}$
    return $\text{rc}_T[S]$
```

Fig. 2. Security experiment for extended Passwordless Authentication Protocols ePIA $=$ (Register, Authenticate), where $\mathcal{O} = \{$NEWS, NEWTPLA, CORRUPT, REGISTER, CHALLENGE, RESPONSE, COMPLETE$\}$ and Compl $\in \{$PPT, QPT$\}$. We highlight the difference to PIA from [2] in blue. The variables agCon and sid are instance-specific, see Section IV-B.

Definition 1 (Secure passwordless authentication (auth) for ePIA)**.** *Let* Compl $\in \{$PPT, QPT$\}$. *Let* ePIA $=$ (Register, Authenticate) *be an extended passwordless authenti-*

cation protocol. We say that ePIA *provides* secure passwordless authentication*, or* auth *for short, if for all* Compl *adversaries* $\mathcal{A}$ *the advantage*

$$\mathsf{Adv}^{\mathsf{auth}}_{\mathsf{ePIA},\mathsf{Compl}}(\mathcal{A}) := \Pr\left[\mathsf{Expt}^{\mathsf{auth}}_{\mathsf{ePIA},\mathsf{Compl}}(\mathcal{A}) = 1\right]$$

in winning the game $\mathsf{Expt}^{\mathsf{auth}}_{\mathsf{ePIA},\mathsf{Compl}}$ *defined in Figure 2 is negligible in the security parameter* λ.

Conversely, we say a Compl *adversary* $\mathcal{A}$ *breaks the secure passwordless authentication of* ePIA *for some test session* π*, if* $\mathcal{A}$ *wins* $\mathsf{Expt}^{\mathsf{auth}}_{\mathsf{ePIA},\mathsf{Compl}}$ *game via* π.

In the following theorem, we show that WebAuthn 2 satisfies the defined security property auth. We sketch the proof here and give the full proof in Section H in the appendix.

Theorem 1 (PPT/QPT security of WebAuthn 2)**.** *Let* $\mathsf{Compl} \in \{\mathsf{PPT}, \mathsf{QPT}\}$*. Let* $\mathsf{ePIA} = (\mathsf{Register}, \mathsf{Authenticate})$ *denote the WebAuthn 2 protocol depicted in Figure 11. Assume that the underlying function* H *is* $\epsilon^{\mathsf{coll\text{-}res}}_{\mathsf{H}}$*-collision resistant. If there exists a* Compl *adversary* $\mathcal{A}$ *that breaks the secure passwordless authentication of* ePIA *for a test session* π *and the digital signature scheme* Σ *used in* π *is* $\epsilon^{\mathsf{euf\text{-}cma}}_{\Sigma}$*-*$\mathsf{euf\text{-}cma}$ *secure against* Compl *adversaries, then it holds that*

$$\mathsf{Adv}^{\mathsf{auth}}_{\mathsf{ePIA},\mathsf{Compl}}(\mathcal{A}) \leq \binom{q_{\textsc{Register}}}{2} 2^{-\lambda} + \binom{q_{\textsc{Challenge}}}{2} 2^{-\lambda} + \epsilon^{\mathsf{coll\text{-}res}}_{\mathsf{H}} + 2 q_{\textsc{Register}} \epsilon^{\mathsf{euf\text{-}cma}}_{\Sigma}$$

where $q_{\mathcal{O}}$ *denotes the number of* $\mathcal{A}$*'s queries to* $\mathcal{O} \in \{\textsc{Register}, \textsc{Challenge}\}$.

Proof Sketch. Notice that the token session identifiers include credential identifiers, which are sampled of length $\geq \lambda$ for different tokens only in the $\textsc{Register}$ queries, and a counter n, which is incremented in each sessions of the same token. The adversary $\mathcal{A}$ cannot win via winning condition in Line 8 except probability $\binom{q_{\textsc{Register}}}{2} 2^{-\lambda}$. Note that the server session identifiers include the hash of server id, which is assumed to be unique for each server. Note also that the server session identifiers in the authentication phases additionally includes the hash of the token binding state tb and challenge nonces ch, which are of length $\geq \lambda$ and sampled only in the $\textsc{Challenge}$ queries. The adversary $\mathcal{A}$ cannot win via winning condition in Line 9 except with probability $\binom{q_{\textsc{Challenge}}}{2} 2^{-\lambda} + \epsilon^{\mathsf{coll\text{-}res}}_{\mathsf{H}}$. Finally, observe that the registration phases are authenticated and that the identifier of each server session in the authentication phases is set only when the corresponding server session accepts a signature, which signs the hash of the unique server id, the counter n, the hash of the client message m_{acl}, UP, and UV. Moreover, there are at most $q_{\textsc{Register}}$ private signing keys in the experiment. The winning conditions in Line 11 and Line 12 indicate that the adversary $\mathcal{A}$ can forge any signature of Σ without corrupting the private signing key of any token, which happens with probability at most $2\epsilon^{\mathsf{euf\text{-}cma}}_{\Sigma}$ for each token and thus in total $2 q_{\textsc{Register}} \epsilon^{\mathsf{euf\text{-}cma}}_{\Sigma}$. □

Theorem 1 shows that no polynomial-time attackers against WebAuthn 2 in the auth experiment can trigger any winning condition, through which the following aspects are captured. Conditions 1 and 2 capture the uniqueness of each session identifiers. i.e., if two sessions are partnered with each other, they are each other's unique partners. Condition 3 encodes the official security statement (see footnote 4). Condition 4 ensures that under the same assumption, the token and server sessions in the subsequent authentication ceremonies using that public key credential must agree on the server identifier id_S, the hash value $\mathsf{H}(\mathsf{ch}, \mathsf{tb})$, the local counter n, and the user presence UP and verification UV conditions. As a corollary, if the underlying hash function H is collision resistant, then the token and server sessions also implicitly agree on the token binding state tb.

D. Post-Quantum Instantiation of WebAuthn 2

To add the ability to authenticate using PQ or hybrid signature schemes with minimal changes to the WebAuthn 2 protocol, we propose to only extend the supported digital signature list pkCP (encoding an "or" choice) and explicitly allowing hybrid schemes (to encode "and", e.g., for classical and PQ schemes).

Following the WebAuthn 2 specification, the server has the option to include RSASSA–PKCS1–v1_5, RSASSA–PSS [13], or/and ECDSA–P256 [14] in pkCP, see Section II for an explanation of pkCP. Recall that the auth security of the WebAuthn 2 is proven in the standard model in Theorem 1. Therefore, the auth security for WebAuthn 2 also holds against quantum adversaries, assuming that $\epsilon^{\mathsf{coll\text{-}res}}_{\mathsf{H}}$ and $\epsilon^{\mathsf{euf\text{-}cma}}_{\Sigma}$ are sufficiently small against quantum adversaries, i.e., are instantiated with PQ secure algorithms. Instead of accepting only plain PQ signatures schemes, the server could also select hybrid signature schemes for pkCP as below.

Let Σ_1 and Σ_2 be signature schemes. We write $\mathcal{C}[\Sigma_1, \Sigma_2] = (\mathsf{KG}_{\mathcal{C}}, \mathsf{Sign}_{\mathcal{C}}, \mathsf{Vfy}_{\mathcal{C}})$ for the hybrid signature schemes constructed from Σ_1 and Σ_2[5]. $\mathsf{KG}_{\mathcal{C}}$ simply returns the concatenation of the two ingredient public and secret keys. Similarly, the signature returned by $\mathsf{Sign}_{\mathcal{C}}$ is the concatenation of the ingredient signatures over the same message. $\mathsf{Vfy}_{\mathcal{C}}$ returns 1 if and only if both ingredient signatures are valid. Otherwise it returns 0. The ingredient schemes could either be instantiated with different PQ (PQ-PQ hybrid), or with one classical and one PQ signature scheme (classical-PQ hybrid). Note that many other combiners exists, such as nested approaches that have been formalized in [5], which are particularly well suited to achieve backwards compatibility in, e.g., X.509 certificates.

In case of WebAuthn 2, backwards compatibility is important as not all authenticators, e.g., USB tokens, can be updated to support new algorithms via software updates. To offer backwards compatibility, the server includes classical algorithms in pkCP as less preferred algorithms and PQ/hybrid schemes with higher preference, e.g., $\mathsf{pkCP} = \{\Sigma_1 = \mathcal{C}[\Sigma_2, \Sigma_3], \Sigma_2, \Sigma_3\}$ with $\Sigma_3 \in \{$RSASSA–PKCS1–v1_5, RSASSA–PSS, ECDSA–P256$\}$. Then, the (honest) token would always choose the more

[5]This description can easily be extended to more than two ingredient schemes.

preferred hybrid or PQ algorithms for the PQ security, unless they are not supported.

E. Stronger Downgrade Protection

Our WebAuthn 2 results in the previous sections assume that the registration phase is authenticated (as in the standard), which means that the supported schemes list cannot be modified, and thus basic scheme downgrade attacks are impossible. On the other end of the spectrum, if an active attacker interferes continuously with *all* phases, we cannot detect or prevent downgrades.

However, there is an intermediate threat model, for which WebAuthn 2 could, but does not, provide downgrade protection. Note that the (ordered) list of the relying party's accepted signature algorithms $\pi_S^i.\mathsf{pkCP}$ is sent in plain from the relying party to the authenticator via the client (see Figure 11). The credential keys are then generated using the first algorithm in the *received* pkCP that is supported by the authenticator, see [12, Section 6.3.2.7.1]. During rVrfy, the relying party checks that the used signature scheme Σ is in $\pi_S^i.\mathsf{pkCP}$. Hence, if the communication in the registration phase is not authenticated, an adversary can easily change the list pkCP during transmission to the authenticator. For example, during the PQ transition, ideally security is based on classical and PQ algorithms in a backwards compatible way. While we explain how to achieve backwards compatibility with authenticators that only support classical algorithms in Section IV-D, a quantum adversary is able to break RSA or ECDSA might change pkCP such that the authenticator only has the choice between classical algorithms.

Consider an adversary that can forge signatures of one of the accepted and supported algorithms. Moreover, assume this adversary is able to compromise the browser or control the network used during registration but not the ones used for authentication, e.g., in an internet cafe a compromised machine is used for registration but others for authentication. Then tricking the authenticator to choose the vulnerable algorithm (and create a corresponding credential key pair) is beneficial because it allows the adversary to forge authentications later on even if they do not control the network anymore.

If the adversary has permanent control of the machine used for registration and authentication, and can forge signatures of an algorithm that is accepted and supported by the relying party and the authenticator, respectively, this attack cannot be prevented. Moreover, it is impossible to prevent the authenticator being tricked into using a less preferred algorithm without substantial changes to the WebAuthn 2 protocol and the public-key infrastructure within. However, we suggest changes that enable *detecting* such an event with high probability, calling the resulting protocol WebAuthn 2^+, if at least one message without interference of the adversary is sent. We depict the changes as boxed operations in Figure 11. Essentially, the idea is to include the hash $\mathsf{h_{CP}}$ of the *received* list of accepted algorithms pkCP' during registration, in the authentication response. The relying party compares $\mathsf{H}(\mathsf{pkCP})$ with $\mathsf{h_{CP}}$ to detect whether authenticator and relying party agree on the list of algorithms. To enable the above changes, both the relying party and the authenticator must store respective lists; we suggest to include them in the registration context.

```
$\underline{\mathsf{Expt}^{\mathsf{AlgAgree}}_{\text{WebAuthn } 2^+,\mathsf{Compl}}(\mathcal{A})}$:
$(S, i, T, j, \mathsf{tb}, UV) \xleftarrow{\$} \mathcal{A}^{\mathcal{O}}(1^\lambda)$
$m^\star_{\mathsf{ach}} \xleftarrow{\$} \textsc{Challenge}((S,i), \mathsf{tb}, UV)$
$(m^\star_{\mathsf{acom}}, m^\star_{\mathsf{acl}}) \leftarrow \mathsf{aCom}(\mathsf{id}_S, m^\star_{\mathsf{ach}}, \mathsf{tb})$
$m^\star_{\mathsf{arsp}} \xleftarrow{\$} \textsc{Response}((T,j), m^\star_{\mathsf{acom}})$
$d^\star_a \xleftarrow{\$} \textsc{Complete}((S,i), m^\star_{\mathsf{acl}}, m^\star_{\mathsf{arsp}})$
$\mathsf{Supp} \leftarrow$ list of supported algorithms by $T$
$d^\star_{T,S} \leftarrow [\![(\mathsf{pkCP}_S \cap \mathsf{Supp})[1] \neq \mathsf{rc}_T[S].\Sigma]\!]$
$\mathbf{return}\ [d^\star_{(T,S)} = 1 \wedge d^\star_a = 1]$

$\underline{\textsc{rChallenge}((S,i), \mathsf{tb}, UV)}$:
$\mathbf{if}\ \mathsf{pkCP}_S = \bot\ \mathbf{or}\ \pi_S^i \neq \bot$
    $\mathbf{return}\ \bot$
$\pi_S^i.\mathsf{pkCP} \leftarrow \mathsf{pkCP}_S$ /ordered list of accepted algorithms
$m_{\mathsf{rrsp}} \leftarrow \mathsf{rChall}(\pi_S^i, \mathsf{tb}, UV)$
$\mathbf{return}\ m_{\mathsf{rrsp}}$

$\underline{\textsc{rResponse}((T,j), m_{\mathsf{rcom}})}$:
$\mathbf{if}\ \mathsf{suppUV}_T = \bot\ \mathbf{or}\ \pi_T^j \neq \bot$
    $\mathbf{return}\ \bot$
$\pi_T^j.\mathsf{suppUV} \leftarrow \mathsf{suppUV}_T$
$(m_{\mathsf{rrsp}}, \mathsf{rc}_T) \xleftarrow{\$} \mathsf{rRsp}(\pi_T^j, m_{\mathsf{rcom}})$
$\mathbf{return}\ m_{\mathsf{rrsp}}$

$\underline{\textsc{rComplete}((S,i), m_{\mathsf{rcl}}, m_{\mathsf{rrsp}})}$:
$\mathbf{if}\ \mathsf{pkCP}_S = \bot\ \mathbf{or}\ \pi_S^i = \bot$
$\mathbf{or}\ \pi_S^i.\mathsf{st_{exe}} \neq \mathsf{running} : \mathbf{return}\ \bot$
$(\mathsf{rc}_S, d) \xleftarrow{\$} \mathsf{rVrfy}(\pi_S^i, m_{\mathsf{rcl}}, m_{\mathsf{rrsp}})$
$\mathbf{return}\ d$
```

Fig. 3. Game $\mathsf{Expt}^{\mathsf{AlgAgree}}_{\text{WebAuthn } 2^+,\mathsf{Compl}}$ and oracles rChallenge, rResponse, rComplete; note that NewS, NewTPlA, Challenge, Response, and Complete are given in Figure 2.

If an adversary changed the list pkCP during registration in WebAuthn 2^+, the adversary would need to change the value $\mathsf{h_{CP}}$ during every authentication response to avoid detection of the attack. We stress that it would not be sufficient to only reject authentications when such an attack is detected, since the honest authenticator would then be unable to communicate with the relying party due to the disagreement on the list pkCP. Even worse, only those authentication responses in which the adversary successfully switched the value $\mathsf{h_{CP}}$ would be accepted. Thus, the detection of this downgrade attack should trigger deregistering the authenticator by the relying party and notifying the user (ideally out-of-band).

More formally, we say that WebAuthn 2^+ satisfies our property *Algorithm Agreement* (AlgAgree) against $\mathsf{Compl} \in \{\mathsf{PPT}, \mathsf{QPT}\}$ adversaries if the advantage

$$\mathsf{Adv}^{\mathsf{AlgAgree}}_{\text{WebAuthn } 2^+,\mathsf{Compl}}(\mathcal{A}) := \Pr\left[\mathsf{Expt}^{\mathsf{AlgAgree}}_{\text{WebAuthn } 2^+,\mathsf{Compl}}(\mathcal{A}) = 1\right]$$

in winning the game $\mathsf{Expt}^{\mathsf{AlgAgree}}_{\text{WebAuthn } 2^+,\mathsf{Compl}}$ (defined in Figure 3) is negligible in the security parameter λ. We view WebAuthn 2^+ as an instantiation of an ePlA and give the adversary access to the following oracles: rChallenge, rResponse, and rComplete given in Figure 3, and NewS, NewTPlA, Challenge, Response, and Complete given in Figure 2.

The adversary wins the game $\mathsf{Expt}^{\mathsf{AlgAgree}}_{\text{WebAuthn } 2^+,\mathsf{Compl}}$ if the generated key pair is not of the most preferred server's algorithm that is supported by the token (i.e., it is not the first element in the intersection of the supported and the preferred algorithms, see line 7 in Figure 3), and honestly generated authentications are always accepted by the server (see line 5 in Figure 3). It is important to emphasize that our threat model here is different than the one for Section IV-C. Namely, we assume that the communication channels in the registration and authentication phase are unauthenticated with one exception. We assume that there is at least one honest authentication, i.e., during this one authentication the adversary does not actively interfere with the communication between the three parties.

We can show that WebAuthn 2^+ satisfies the above property if H is a collision resistant hash function. The proof sketch is as follows. Assume the adversary $\mathcal{A}$ wins $\mathsf{Expt}^{\mathsf{AlgAgree}}_{\mathsf{WebAuthn}\ 2^+,\mathsf{Compl}}$ (i.e., $d^\star_{(T,S)} = 1$ and $d^\star_a = 1$). This implies that the adversary is able to successfully register the token T at server S such that the chosen signature algorithm is supported by the token, accepted by the server, and not the most preferred algorithm in the intersection of supported and accepted algorithms. Furthermore, it means that line 57 in Figure 11 holds, i.e., that the hash value $\mathsf{h_{CP}}$ over the received list pkCP' (computed and sent by the token) is the same as the hash value $\mathsf{rc}_S[\mathsf{cid}].\mathsf{h_{CP}}$ over the original pkCP. This contradicts the collision-resistance of H, as $\mathsf{pkCP} \neq \mathsf{pkCP}'$.

V. CTAP 2.1 and Extended Pin-based Access Control for Authenticator Protocols

In this section, we first define the *extended PIN-based Access Control for Authenticators* (ePACA) protocol following [2] and describe CTAP 2.1 as an ePACA instance. Next, we present a variant of the strong unforgeability with trust-binding ($\mathsf{SUF\text{-}t}'$) experiment. Finally, we extend CTAP 2.1 for PQ compatibility and formally prove the $\mathsf{SUF\text{-}t}'$ security of the extension.

A. Extended Pin-based Access Control for Authenticator Protocols

An *extended PIN-based Access Control for Authenticators* protocol $\mathsf{ePACA} = (\mathsf{Reboot}, \mathsf{Setup}, \mathsf{Bind}, \mathsf{Auth}, \mathsf{Validate})$ is an interactive protocol between a client C, an authenticator token T, and a user U, specified by the following algorithms:

$\mathsf{Reboot}(T)$**:** runs at each power-up of the token T and initializes the inherent state with a mandatory user interaction. This algorithm is expected to be invoked to power up T and initialize the local state before the execution of any other algorithms on T.

$\mathsf{Setup}(T, C, U)$**:** inputs a token T, a client C, and a user U and outputs the transcript trans. During this interactive sub-protocol, U securely transfers the PIN to T via C. Note that this algorithm is invoked on each token T at most once. We write $\mathsf{trans} \xleftarrow{\$} \mathsf{Setup}(T, C, U)$.

$\mathsf{Bind}(T, C, U)$**:** During this interactive sub-protocol, the client C is bound to the token T under the confirmation of the user U. This sub-protocol is further divided into two algorithms:

- $\mathsf{Bind\text{-}C}(C, U, m)$**:** inputs a client C, a user U, and an incoming message m and outputs an outgoing message m'. During this algorithm, C processes m under the confirmation from U. We write $m' \xleftarrow{\$} \mathsf{Bind\text{-}C}(C, U, m)$.
- $\mathsf{Bind\text{-}T}(T, m)$**:** inputs a token T and an incoming message m, and outputs an outgoing message m'. We write $m' \xleftarrow{\$} \mathsf{Bind\text{-}T}(T, m)$.

$\mathsf{Auth}(C, M)$**:** inputs a client C and a command M, and outputs both the command M and its authorization tag t. We write $(M, t) \xleftarrow{\$} \mathsf{Auth}(C, M)$.

$\mathsf{Validate}(T, M, t, d)$**:** inputs a token T, a command M, an authorization tag t, and a user decision $d \in \{\mathsf{accepted}, \mathsf{rejected}\}$, and outputs status $\in \{\mathsf{accepted}, \mathsf{rejected}\}$ indicating whether the authorization can be verified or not. We write status $\xleftarrow{\$} \mathsf{Validate}(T, M, t, d)$.

B. CTAP 2.1 is an ePACA protocol

CTAP 2.1 [6] is a substantial change from CTAP 2.0 [7] in terms of generalization and modularity. More concretely, CTAP 2.1 makes use of a generic stateful so-called *Pin/Uv Auth Protocol* $\mathsf{puvProtocol} = (\mathsf{initialize}, \mathsf{regenerate}, \mathsf{resetpuvToken}, \mathsf{getPublicKey}, \mathsf{encapsulate}, \mathsf{decapsulate}, \mathsf{encrypt}, \mathsf{decrypt}, \mathsf{authenticate}, \mathsf{verify})$, which can be instantiated using $\mathsf{puvProtocol}_1$ and $\mathsf{puvProtocol}_2$ from the standard that we depict in Section D. Additionally, we here propose a third instantiation $\mathsf{puvProtocol}_3$ that allows for PQ security in Section V-C. Each $\mathsf{puvProtocol}$ has its internal state including a public-private key pair (pk, sk) and a string pt.

Similar to the treatment in Section IV, we use π^i_T and π^j_C to denote token T's i-th and client C's j-th instance respectively. In addition, each T has a token-associated state st_T that is shared by all of T's instances. Namely, we have $T = \{\mathsf{st}_T\} \cup \{\pi^i_T\}_i$ and $C = \{\pi^j_C\}_j$. We use pin_U to denote U's unique PIN. In addition, we define the following variables for tokens T or clients C:

$\mathsf{st}_T.\mathsf{version} \in \{2.0, 2.1\}$**:** denotes the CTAP version.

$\mathsf{st}_T.\mathsf{puvProtocol}$**:** denotes a stateful Pin/Uv Auth Protocol.

$\mathsf{st}_T.\mathsf{puvProtocolList}$**:** denotes the list of Pin/Uv Auth Protocol instantiations that T supports.

$\mathsf{st}_T.\mathsf{pinHash} \in \{0,1\}^\star \cup \{\perp\}$**:** denotes the hash of a user PIN. This variable is expected to be set during Setup.

$\mathsf{st}_T.\mathsf{pinRetries} \in \{0, ..., \mathsf{pinRetriesMax}\}$**:** denotes the number of remaining tries for clients to deliver a pinHash, where pinRetriesMax denotes the maximal number of tries.

$\mathsf{st}_T.m \in \{0, ..., 3\}$**:** denotes the remaining consecutive tries for clients to deliver pinHash.

$\pi^i_T.\mathsf{st_{exe}}, \pi^j_C.\mathsf{st_{exe}} \in \{\mathsf{waiting}, \mathsf{bindStart}, \mathsf{bindDone}, \perp\}$**:** denotes the execution state of a token/client session.

$\pi^i_T.\mathsf{bs}, \pi^j_C.\mathsf{bs} \in \{0,1\}^\star \cup \{\perp\}$**:** denotes the binding state. This variable is expected to be set during Bind.

$\pi^i_T.\mathsf{sid}, \pi^j_C.\mathsf{sid} \in \{0,1\}^\star \cup \{\perp\}$**:** denotes the session identifiers; defined as the full transcript of the Bind execution.

$\pi^j_C.\mathsf{selectedpuvProtocol}$**:** denotes the puvProtocol instantiation chosen by the client.

$\pi^j_C.\mathsf{K} \in \{0,1\}^\star \cup \{\perp\}$**:** denotes the shared key with a token.

Next, we formalize CTAP 2.1 as an ePACA protocol.

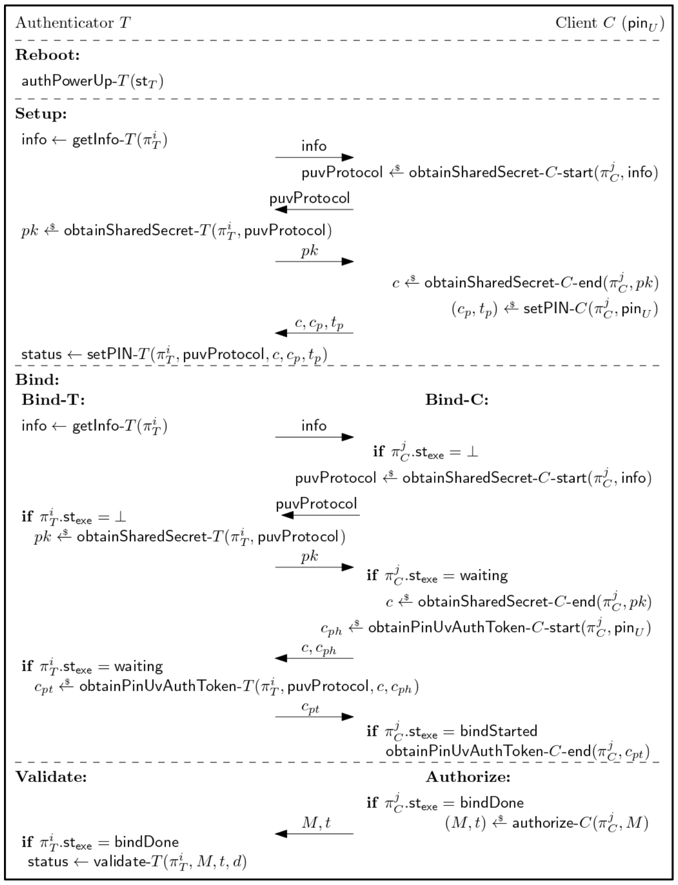

Authenticator T
Client C (pin_U)
Reboot:
$\mathsf{authPowerUp}\text{-}T(\mathsf{st}_T)$
Setup:
$\mathsf{info} \leftarrow \mathsf{getInfo}\text{-}T(\pi_T^i)$
info
$\mathsf{puvProtocol} \xleftarrow{\$} \mathsf{obtainSharedSecret}\text{-}C\text{-}\mathsf{start}(\pi_C^j, \mathsf{info})$
$\mathsf{puvProtocol}$
$pk \xleftarrow{\$} \mathsf{obtainSharedSecret}\text{-}T(\pi_T^i, \mathsf{puvProtocol})$
pk
$c \xleftarrow{\$} \mathsf{obtainSharedSecret}\text{-}C\text{-}\mathsf{end}(\pi_C^j, pk)$
$(c_p, t_p) \xleftarrow{\$} \mathsf{setPIN}\text{-}C(\pi_C^j, \mathsf{pin}_U)$
c, c_p, t_p
$\mathsf{status} \leftarrow \mathsf{setPIN}\text{-}T(\pi_T^i, \mathsf{puvProtocol}, c, c_p, t_p)$
Bind:
Bind-T:
Bind-C:
$\mathsf{info} \leftarrow \mathsf{getInfo}\text{-}T(\pi_T^i)$
info
if $\pi_C^j.\mathsf{st_{exe}} = \perp$
$\mathsf{puvProtocol} \xleftarrow{\$} \mathsf{obtainSharedSecret}\text{-}C\text{-}\mathsf{start}(\pi_C^j, \mathsf{info})$
$\mathsf{puvProtocol}$
if $\pi_T^i.\mathsf{st_{exe}} = \perp$
$pk \xleftarrow{\$} \mathsf{obtainSharedSecret}\text{-}T(\pi_T^i, \mathsf{puvProtocol})$
pk
if $\pi_C^j.\mathsf{st_{exe}} = \mathsf{waiting}$
$c \xleftarrow{\$} \mathsf{obtainSharedSecret}\text{-}C\text{-}\mathsf{end}(\pi_C^j, pk)$
$c_{ph} \xleftarrow{\$} \mathsf{obtainPinUvAuthToken}\text{-}C\text{-}\mathsf{start}(\pi_C^j, \mathsf{pin}_U)$
c, c_{ph}
if $\pi_T^i.\mathsf{st_{exe}} = \mathsf{waiting}$
$c_{pt} \xleftarrow{\$} \mathsf{obtainPinUvAuthToken}\text{-}T(\pi_T^i, \mathsf{puvProtocol}, c, c_{ph})$
c_{pt}
if $\pi_C^j.\mathsf{st_{exe}} = \mathsf{bindStarted}$
$\mathsf{obtainPinUvAuthToken}\text{-}C\text{-}\mathsf{end}(\pi_C^j, c_{pt})$
Validate:
Authorize:
if $\pi_C^j.\mathsf{st_{exe}} = \mathsf{bindDone}$
$(M, t) \xleftarrow{\$} \mathsf{authorize}\text{-}C(\pi_C^j, M)$
M, t
if $\pi_T^i.\mathsf{st_{exe}} = \mathsf{bindDone}$
$\mathsf{status} \leftarrow \mathsf{validate}\text{-}T(\pi_T^i, M, t, d)$

Fig. 4. CTAP 2.1 is an $\mathsf{ePACA} = (\mathsf{Reboot}, \mathsf{Setup}, \mathsf{Bind}, \mathsf{Auth}, \mathsf{Validate})$ protocol. All algorithms are defined in Section D.

Overall CTAP 2.1 includes 12 algorithms[6]. We depict the communication flow of CTAP 2.1 in Figure 4. Intuitively, the Reboot algorithm initializes the underlying puvProtocols and resets the remaining consecutive tries $\mathsf{st}_T.m$ to 3.

In the Setup interaction, the token T first outputs its information info, which includes the supported list $\mathsf{st}_T.\mathsf{puvProtocolList}$. Next, the client selects and initializes one $\pi_C^j.\mathsf{selectedpuvProtocol}$ from the received list followed by sending its choice back to T. Then, the token T returns the public key pk of the chosen $\mathsf{st}_T.\mathsf{puvProtocol}$. Afterwards, the client runs the encapsulation of its $\pi_C^j.\mathsf{selectedpuvProtocol}$ upon pk for a key $\pi_C^j.\mathsf{K}$, which is then used to encrypt and authenticate the PIN pin_U collected from user U, and forwards all derived ciphertexts and tags to T. The token T finally decapsulates the key, followed by verifying the ciphertext, and recovers pin_U. The local $\mathsf{st}_T.\mathsf{pinHash}$ stores the hash of pin_U and the remaining retries $\mathsf{st}_T.\mathsf{pinRetries}$ is set to pinRetriesMax.

[6]Similar to the treatment in [2], we omit the algorithms for PIN reset and leave it for future work. The suffix -T and -C in the names of algorithms indicates the algorithm executor to be either a token or a client. The suffix -start and -end indicates that this algorithm is the first or the final step in an interactive execution.

The Bind interaction is identical to Setup until the client derives the key $\pi_C^j.\mathsf{K}$. Then, the client uses $\pi_C^j.\mathsf{K}$ to encrypt the hash of the user pin pin_U and sends the ciphertext to T. If $\mathsf{st}_T.\mathsf{pinRetries}$ does not reach 0, the token decapsulates the key and recovers a pinHash. If the pinHash does not match the hash of the local $\mathsf{st}_T.\mathsf{pinHash}$, the underlying $\mathsf{st}_T.\mathsf{puvProtocol}$ re-generates the public key pk. If the remaining consecutive retries meanwhile arrive at 0, the token is forced to reboot. If the pinHash matches the hash of the local $\mathsf{st}_T.\mathsf{pinHash}$, the remaining retries $\mathsf{st}_T.m$ and $\mathsf{st}_T.\mathsf{pinRetries}$ are reset to their maximal values. The pts of all underlying $\mathsf{st}_T.\mathsf{puvProtocol}$ are re-sampled. The token finally sets the binding state $\pi_T^i.\mathsf{bs}$ to the pt of the current $\mathsf{st}_T.\mathsf{puvProtocol}$, which is then encrypted using the decapsulated key. The client eventually recovers the pt and sets it to $\pi_C^j.\mathsf{bs}$.

After the negotiation for the binding states, the client can invoke Auth algorithm to authorize command M using its binding state $\pi_T^i.\mathsf{bs}$. Similarly, the token can invoke the Validate algorithm to verify the authorized command using $\pi_C^j.\mathsf{bs}$.

We delay the description of the 12 algorithms to Section D.

C. *Post-Quantum Instantiation of CTAP 2.1*

We propose a third instantiation of the Pin/Uv Auth Protocol in Figure 5 that provides PQ compatibility in a hybrid manner. Compared to $\mathsf{puvProtocol}_2$, the most important changes made to achieve PQ security are as follows. First, in addition to an ECDH (over curve NIST P-256) key pair, a key pair of a PQ secure KEM is sampled during $\mathsf{regenerate}_3$. Second, the algorithm $\mathsf{encapsulate}_3$ executes both the ECDH key exchange and the encapsulation of the PQ KEM to derive a hybrid ciphertext c and key $K = (K_1, K_2)$. Finally, the algorithm $\mathsf{decapsulate}_3$ correspondingly recovers the hybrid key $K = (K_1, K_2)$ from the ciphertext c.

Instantiation: We suggest to instantiate the underlying KEM with any Round 3 Finalist nominated by NIST and the SKE_3 with AES-512-CBC with randomized initial vector. The underlying functions $\mathsf{H}_i : \{0,1\}^\star \to \{0,1\}^{l_i}$ for $i \in \{5,6,7\}$ can be instantiated with HMAC-SHA-512. Moreover, we suggest $\mu' \geq 2$ to against Grover's attack and to achieve 256-bits security.

D. *Security Model of* ePACA *Protocols*

Moving forward, we model the security of ePACA protocols as security experiment $\mathsf{Expt}^{\mathsf{SUF\text{-}t'}}_{\mathsf{ePACA},\mathsf{Compl}}$. The security goal is to ensure that a token can only accept a command that has been authorized by a trusted client under user permission.

a) Trust Model: Similarly to [2], we assume "trust-on-first-use", which means that the interactive execution of Setup is authenticated without any active interference of an eavesdropping adversary. Moreover, we assume no active attacks against clients during the interactive execution of Bind, while active attacks against tokens are allowed. More concretely, active attacks against clients are allowed only when the execution state of the clients turns from waiting to bindStart. However, active attacks against tokens are allowed

```
$\underline{\mathsf{initialize}_3():}$
    $\mathsf{regenerate}_3()$
    $\mathsf{resetpuvToken}_3()$
$\underline{\mathsf{regenerate}_3():}$
    $(pk_1, sk_1) \xleftarrow{\$} \mathsf{ECDH.KG}()$
    $(pk_2, sk_2) \xleftarrow{\$} \mathsf{KEM.KG}()$
    $pk \leftarrow (pk_1, pk_2)$
    $sk \leftarrow (sk_1, sk_2)$
$\underline{\mathsf{encrypt}_3(K, m):}$
    $(K_1, K_2) \leftarrow K$
        s.t. $|K_1| = \mu'\lambda$
    $c \leftarrow \mathsf{SKE}_3.\mathsf{Enc}(K_2, m)$
    return $c$
$\underline{\mathsf{decrypt}_3(K, c):}$
    $(K_1, K_2) \leftarrow K$
        s.t. $|K_1| = \mu'\lambda$
    $m \leftarrow \mathsf{SKE}_3.\mathsf{Dec}(K_2, c)$
    return $m$
$\underline{\mathsf{authenticate}_3(K', m):}$
    $(K'_1, K'_2) \leftarrow K'$
        s.t. $|K'_1| = \mu'\lambda$
    $t \leftarrow \mathsf{H}_7(K'_1, m)$
    return $t$
$\underline{\mathsf{verify}_3(K', m, t):}$
    $(K'_1, K'_2) \leftarrow K'$
        s.t. $|K'_1| = \mu'\lambda$
    $t' \leftarrow \mathsf{H}_7(K', m)$
    return $[\![t = t']\!]$

$\underline{\mathsf{getPublicKey}_3():}$
    return $pk$
$\underline{\mathsf{resetpuvToken}_3():}$
    $pt \xleftarrow{\$} \{0,1\}^{\mu'\lambda}$
$\underline{\mathsf{encapsulate}_3(pk'):}$
    $(pk'_1, pk'_2) \leftarrow pk'$
    $(sk_1, sk_2) \leftarrow sk$
    $Z_1 \leftarrow \mathsf{XCoordinateOf}(sk_1 \cdot pk'_1)$
    $(c_2, Z_2) \leftarrow \mathsf{KEM.Encaps}(pk'_2)$
    $Z \leftarrow \mathsf{H}_5(Z_1, Z_2)$
    $K_1 \leftarrow \mathsf{H}_6(Z, \text{“CTAP2 HMAC key”})$
    $K_2 \leftarrow \mathsf{H}_6(Z, \text{“CTAP2 AES key”})$
    $K \leftarrow (K_1, K_2)$
    $c \leftarrow (pk, c_2)$
    return $(c, K)$
$\underline{\mathsf{decapsulate}_3(c):}$
    Parse $(c_1, c_2) \leftarrow c$
    Parse $(sk_1, sk_2) \leftarrow sk$
    $Z_1 \leftarrow \mathsf{XCoordinateOf}(sk_1 \cdot c_1)$
    $Z_2 \leftarrow \mathsf{KEM.Decaps}(sk_2, c_2)$
    $Z \leftarrow \mathsf{H}_5(Z_1, Z_2)$
    $K_1 \leftarrow \mathsf{H}_6(Z, \text{“CTAP2 HMAC key”})$
    $K_2 \leftarrow \mathsf{H}_6(Z, \text{“CTAP2 AES key”})$
    $K \leftarrow (K_1, K_2)$
    return $K$
```

Fig. 5. The third instantiation of PIN/UV Auth Protocol $\mathsf{puvProtocol}_3$. The operation $\cdot$ denotes the scalar-multiplication.

even if the execution state of tokens is still waiting. We further assume that each user holds a unique PIN pin_U that is independently sampled from the domain $\mathcal{PIN}$[7] following some distribution $\mathfrak{D}$ with min-entropy $\alpha_{\mathfrak{D}}$. All tokens are assumed to share a common pinRetriesMax. We assume that each ECDH point is bijective to its x-coordinate.

b) Experiment-specific Variables: Each session π is associated with a variable $\mathsf{isValid} \in \{\mathsf{true}, \mathsf{false}, \perp\}$ that denotes whether the session is still accessible (by users or attackers) or not. Each token session π_T^i is associated with a variable $\mathsf{pinCorr} \in \{\mathsf{true}, \mathsf{false}\}$ that indicates whether the setup user PIN of T has been corrupted.

c) Oracles: The oracles in our security experiment (see Figure 6) are defined similarly to the ones in [2]. More concretely, the oracles NEWT and NEWU create new tokens and users, respectively. In particular, the adversary can customize the token with specific initial data when querying NEWT. The REBOOT(T) oracle invokes Reboot and marks all previously established sessions of T as invalid. The oracle SETUP runs the authenticated interaction of Setup. The oracle EXECUTE captures that the Bind interaction is partially authenticated until the client's execution state is set to bindStart and the remaining interaction of Bind is not authenticated, as the adversary can deliver messages to token and client by SEND-BIND-T and SEND-BIND-C oracles respectively. The AUTH and VALIDATE oracles simulate the Auth and Validate execution of clients and tokens, respectively. Furthermore, querying CORRUPTUSER and COMPROMISE reveals a user's PIN and a client's binding state, respectively. Notably, whenever Reboot or Bind are completed on a token T, we mark all of T's previously established sessions as invalid.

d) Session Partnering: Partnering identifies the sessions of a token T and a client C that successfully completed $\mathsf{Bind}(T, C, U)$ for some user U. We call a token session π_T^i *partnered* with a client session π_C^j if and only if $\pi_T^i.\mathsf{sid} = \pi_C^j.\mathsf{sid} \neq \perp$.

e) Winning Conditions: We call a token session *test session* if it accepts an authorized command-tag pair under some user decision. An adversary $\mathcal{A}$ wins $\mathsf{Expt}^{\mathsf{SUF\text{-}t'}}_{\mathsf{ePACA},\mathsf{Compl}}$ (with $\mathsf{Compl} \in \{\mathsf{PPT}, \mathsf{QPT}\}$) if there exists a test session π_T^i that accepts an authorized command (M, t) with user decision d and any of the following conditions holds:

1) the user decision $d \neq \mathsf{accepted}$.
2) two distinct client sessions that completed Bind have the same session identifiers.
3) two distinct token sessions that completed Bind have the same session identifiers.
4) (M, t) was not output by any of π_T^i's uncompromised valid partners π_C^j before the corruption of the user PIN that was setup on the token T.

Definition 2 (SUF-t$'$ security of ePACA)**.** *Let* $\mathsf{Compl} \in \{\mathsf{PPT}, \mathsf{QPT}\}$. *Let* $\mathsf{ePACA} = (\mathsf{Reboot}, \mathsf{Setup}, \mathsf{Bind}, \mathsf{Auth}, \mathsf{Validate})$ *be an extended PIN-based Access Control for Authenticators protocol. We say that* ePACA *is* strongly unforgeable with trusted binding, *or is* SUF-t$'$*-secure for short, if for all* Compl *adversaries* $\mathcal{A}$

$$\mathsf{Adv}^{\mathsf{SUF\text{-}t'}}_{\mathsf{PACA},\mathsf{Compl}}(\mathcal{A}) := \Pr[\mathsf{Expt}^{\mathsf{SUF\text{-}t'}}_{\mathsf{ePACA},\mathsf{Compl}}(\mathcal{A}) = 1]$$

in winning the game $\mathsf{Expt}^{\mathsf{SUF\text{-}t'}}_{\mathsf{ePACA},\mathsf{Compl}}$ *as described in Figure 6 is negligible in the security parameter* λ.

E. Security Conclusions for CTAP 2.1

After having defined security for ePACA protocols above, we now present the security statements for CTAP 2.1. We give the full proofs of our two theorems (against PPT and QPT adversaries) in Section I and J in the appendix. Our first theorem shows the SUF-t$'$ security of CTAP 2.1 against PPT adversaries.

Theorem 2 (PPT security of CTAP 2.1)**.** *Let* $\mathsf{ePACA} = (\mathsf{Reboot}, \mathsf{Setup}, \mathsf{Bind}, \mathsf{Auth}, \mathsf{Validate})$ *denote the CTAP 2.1 protocol described in Section V-B. Assume that* ePACA *supports* $\mathsf{puvProtocol}_i$ *for* $i \in \{1, 2, 3\}$. *If the hash function* H *is* $\epsilon_{\mathsf{H}}^{\mathsf{coll\text{-}res}}$ *collision resistant,* $\mathsf{H}_i : \{0,1\}^\star \to \{0,1\}^{l_i}$ *is modeled as independent random oracle for* $i \in \{1, ..., 7\}$, SKE_1 *is* $\epsilon_{\mathsf{SKE}_1}^{\mathsf{ind\text{-}1cpa\text{-}H_2}}$-IND-1CPA-H$_2$ *and* $\epsilon_{\mathsf{SKE}_1}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}$-IND-1\$PA-LPC *secure,* SKE_i *is* $\epsilon_{\mathsf{SKE}_i}^{\mathsf{ind\text{-}1cpa}}$-IND-1CPA *and* $\epsilon_{\mathsf{SKE}_i}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}$-IND-1\$PA-LPC *secure for* $i \in \{2, 3\}$, *and the* sCDH *problem over* ECDH *with prime order*

[7]In practice, each PIN must have a maximal length of 63 bytes and a minimal length of four code points (on tokens) or four unicode characters (on client).

```
$\mathsf{Expt}^{\mathsf{SUF\text{-}t'}}_{\mathsf{ePACA},\mathsf{Compl}}(\mathcal{A})$:
1   $\mathcal{L}_{\text{AUTH}} \leftarrow \emptyset$
2   $\mathsf{win\text{-}SUF\text{-}t'} \leftarrow 0$
3   $() \xleftarrow{\$} \mathcal{A}^{\mathcal{O}}(1^\lambda)$
4   return $\mathsf{win\text{-}SUF\text{-}t'}$

$\mathsf{bindPartner}(T, i)$:
5   if $\exists(C, j)$ s.th. $\pi_T^i.\mathsf{sid} = \pi_C^j.\mathsf{sid}$
6     return $(C, j)$
7   return $(\bot, \bot)$

$\mathsf{Win\text{-}SUF\text{-}t'}(T, i, M, t, d)$:
8   if $d \neq \mathsf{accepted}$: return 1
9   if $\exists(C_1, j_1), (C_2, j_2)$ s.t. $(C_1, j_1) \neq (C_2, j_2)$ and $\pi_{C_1}^{j_1}.\mathsf{st}_{\mathsf{exe}} = \pi_{C_2}^{j_2}.\mathsf{st}_{\mathsf{exe}} =$
    $\mathsf{bindDone}$ and $\pi_{C_1}^{j_1}.\mathsf{sid} = \pi_{C_2}^{j_2}.\mathsf{sid}$: return 1
10  if $\exists(T_1, i_1), (T_2, i_2)$ s.t. $(T_1, i_1) \neq (T_2, i_2)$ and $\pi_{T_1}^{i_1}.\mathsf{st}_{\mathsf{exe}} = \pi_{T_2}^{i_2}.\mathsf{st}_{\mathsf{exe}} =$
    $\mathsf{bindDone}$ and $\pi_{T_1}^{i_1}.\mathsf{sid} = \pi_{T_2}^{i_2}.\mathsf{sid}$: return 1
11  $(C, j) \leftarrow \mathsf{bindPartner}(T, i)$
12  if $(C, j, M, t) \notin \mathcal{L}_{\text{AUTH}}$
13    if $(C, j) = (\bot, \bot)$ or $\pi_C^j.\mathsf{compromised} = \mathsf{false}$
14      if $\pi_T^i.\mathsf{pinCorr} = \mathsf{false}$: return 1
15  return 0

$\text{NEWT}(T, \mathsf{initialData})$:
16  if $\mathsf{st}_T \neq \bot$: return $\bot$
17  $(\mathsf{version}, \mathsf{puvProtocolList}) \leftarrow \mathsf{initialData}$
18  $\mathsf{st}_T.\mathsf{version} \leftarrow \mathsf{version}$
19  $\mathsf{st}_T.\mathsf{puvProtocolList} \leftarrow \mathsf{puvProtocolList}$
20  $\mathsf{Reboot}(\mathsf{st}_T)$
21  return

$\text{NEWU}(U)$:
22  if $\mathsf{pin}_U = \bot$
23    $\mathsf{pin}_U \xleftarrow{\$} \mathcal{PIN}$
24  return

$\text{CORRUPTUSER}(U)$:
25  $\mathsf{corr}_U \leftarrow \mathsf{true}$
26  return $\mathsf{pin}_U$

$\text{SEND-BIND-T}(T, i, m)$:
27  if $\mathsf{st}_T = \bot$ or $\pi_T^i = \bot$ or
    $\pi_T^i.\mathsf{st}_{\mathsf{exe}} \neq \mathsf{waiting}$ or $\pi_T^i.\mathsf{isValid} = \mathsf{false}$
28    return $\bot$
29  $\pi_T^i.\mathsf{pinCorr} \leftarrow \mathsf{corr}_{\mathsf{st}_T.\mathsf{user}}$
30  $m' \xleftarrow{\$} \mathsf{Bind\text{-}T}(\pi_T^i, m)$
31  $c_{pt} \parallel \mathsf{calledReboot} \leftarrow m'$
32  if $\mathsf{calledReboot} = \mathsf{true}$
33    foreach $i'$ s.t. $\pi_T^{i'} \neq \bot$
34      $\pi_T^{i'}.\mathsf{isValid} \leftarrow \mathsf{false}$
35  elseif $\pi_T^i.\mathsf{st}_{\mathsf{exe}} = \mathsf{bindDone}$
36    foreach $i' \neq i$ and $\pi_T^i \neq \bot$
37      $\pi_T^{i'}.\mathsf{isValid} \leftarrow \mathsf{false}$
38  return $m'$

$\text{REBOOT}(T)$:
39  if $\mathsf{st}_T = \bot$: return
40  foreach $i$ s.t. $\pi_T^i \neq \bot$
41    $\pi_T^i.\mathsf{isValid} \leftarrow \mathsf{false}$
42  $\mathsf{Reboot}(\mathsf{st}_T)$
43  return

$\text{SEND-BIND-C}(C, j, m)$:
44  if $\pi_C^j = \bot$ or $\pi_C^j.\mathsf{st}_{\mathsf{exe}} \neq$
    $\mathsf{bindStart}$ or $\pi_C^j.\mathsf{isValid} =$
    $\mathsf{false}$
45    return $\bot$
46  return $\mathsf{Bind\text{-}C}(\pi_C^j, m)$

$\text{SETUP}(T, i, C, j, U)$:
47  if $\mathsf{st}_T = \bot$ or $\pi_T^i \neq \bot$ or $\pi_C^j \neq \bot$
    or $\mathsf{pin}_U = \bot$
48    return $\bot$
49  $\pi_T^i \leftarrow \mathsf{st}_T$
50  $\mathsf{trans} \xleftarrow{\$} \mathsf{Setup}(\pi_T^i, \pi_C^j, \mathsf{pin}_U)$
51  $\pi_T^i.\mathsf{isValid}, \pi_C^j.\mathsf{isValid} \leftarrow \mathsf{false}$
52  $\mathsf{st}_T.\mathsf{user} \leftarrow U$
53  return $\mathsf{trans}$

$\text{EXECUTE}(T, i, C, j, U)$:
54  if $\mathsf{st}_T = \bot$ or $\pi_T^i \neq \bot$ or $\pi_C^j \neq$
    $\bot$ or $\mathsf{pin}_U = \bot$
55    return $\bot$
56  $\pi_T^i \leftarrow \mathsf{st}_T$
57  $\mathsf{trans}, m_C \leftarrow \bot$
58  while $\pi_C^j.\mathsf{st}_{\mathsf{exe}} \neq \mathsf{bindStart}$
59    $m_T \xleftarrow{\$} \mathsf{Bind\text{-}T}(\pi_T^i, m_C)$
60    $m_C \xleftarrow{\$} \mathsf{Bind\text{-}C}(\pi_C^j, U, m_T)$
61    $\mathsf{trans} \leftarrow \mathsf{trans} \parallel m_T \parallel m_C$
62  return $\mathsf{trans}$

$\text{AUTH}(C, j, M)$:
63  if $\pi_C^j = \bot$ or $\pi_C^j.\mathsf{st}_{\mathsf{exe}} \neq \mathsf{bindDone}$
64    return $\bot$
65  $(M, t) \xleftarrow{\$} \mathsf{auth\text{-}}C(\pi_C^j, M)$
66  $\mathcal{L}_{\text{AUTH}} \leftarrow \mathcal{L}_{\text{AUTH}} \cup \{(C, j, M, t)\}$
67  return $(M, t)$

$\text{COMPROMISE}(C, j)$:
68  if $\pi_C^j = \bot$ or $\pi_C^j.\mathsf{st}_{\mathsf{exe}} \neq$
    $\mathsf{bindDone}$: return $\bot$
69  $\pi_C^j.\mathsf{compromised} \leftarrow \mathsf{true}$
70  return $\pi_C^j.\mathsf{bs}$

$\text{VALIDATE}(T, i, M, t, d)$:
71  if $\pi_T^i = \bot$ or $\pi_T^i.\mathsf{st}_{\mathsf{exe}} \neq \mathsf{bindDone}$ or $\pi_T^i.\mathsf{isValid} = \mathsf{false}$
72    return $\bot$
73  $\mathsf{status} \leftarrow \mathsf{validate\text{-}}T(\pi_T^i, M, t, d)$
74  if $\mathsf{status} = \mathsf{accepted}$: $\mathsf{win\text{-}SUF\text{-}t'} \leftarrow \mathsf{Win\text{-}SUF\text{-}t'}(T, i, M, t, d)$
75  return $\mathsf{status}$
```

Fig. 6. Security Game for extended PIN-based Access Control Authenticators Protocol for $\mathsf{ePACA} = (\mathsf{Reboot}, \mathsf{Setup}, \mathsf{Bind}, \mathsf{Auth}, \mathsf{Validate})$, where $\mathcal{O} = \{\text{NEWT}, \text{NEWU}, \text{COMPROMISE}, \text{CORRUPTUSER}, \text{REBOOT}, \text{SETUP}, \text{EXECUTE}, \text{SEND-BIND-T}, \text{SEND-BIND-C}, \text{AUTH}, \text{VALIDATE}\}$ and $\mathsf{Compl} \in \{\mathsf{PPT}, \mathsf{QPT}\}$. We highlight differences to the SUF-t security game from [2] in blue.

q is $\epsilon^{\mathsf{sCDH}}_{\mathsf{ECDH}}$ hard, then the advantage of any PPT *adversary $\mathcal{A}$ that breaks* SUF-t′ *security of* ePACA *is bounded by*

$$\begin{aligned}
&\mathsf{Adv}^{\mathsf{SUF\text{-}t'}}_{\mathsf{PACA},\mathcal{A}}(1^\lambda)\\
&\leq (q_{\text{SETUP}} + q_{\text{EXECUTE}})\epsilon^{\mathsf{sCDH}}_{\mathsf{ECDH}} + \epsilon^{\mathsf{coll\text{-}res}}_{\mathsf{H}}\\
&+\binom{q_{\text{SETUP}} + q_{\text{EXECUTE}}}{2}(2^{2-\min\{l_1,l_3,l_5,l_6\}} + 2^{1-q})\\
&+q_{\text{NEWU}}2^{-\alpha_{\mathfrak{D}}} + \binom{q_{\text{SEND-BIND-T}}}{2}2^{-\min\{\mu,2,\mu'\}\lambda}\\
&+q_{\text{SETUP}}\max\{\epsilon^{\mathsf{ind\text{-}1cpa\text{-}H_2}}_{\mathsf{SKE}_1}, \epsilon^{\mathsf{ind\text{-}1cpa}}_{\mathsf{SKE}_2}, \epsilon^{\mathsf{ind\text{-}1cpa}}_{\mathsf{SKE}_3}\}\\
&+q_{\text{EXECUTE}}\max\{\epsilon^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}_{\mathsf{SKE}_1}, \epsilon^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}_{\mathsf{SKE}_2}, \epsilon^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}_{\mathsf{SKE}_3}\}\\
&+q_{\text{SETUP}}\mathsf{pinRetriesMax}2^{-\alpha_{\mathfrak{D}}}\\
&+q_{\text{VALIDATE}}2^{-\min\{\mu\lambda,2\lambda,\mu'\lambda,l_2,l_4,l_7\}}
\end{aligned}$$

*where $q_{\mathcal{O}}$ denotes the number of queries to $\mathcal{O} = \{$*SETUP, EXECUTE, VALIDATE*$\}$ and q_i denotes the number of queries to random oracle H_i for $i \in \{1, ..., 7\}$.*

Proof Sketch. The proof is divided into the following steps: (1) By the random oracle H_i for $i \in \{1, 3, 5, 6\}$ and the sCDH assumption on the underlying ECDH, all keys K derived from the encapsulation of the underlying puvProtocol in the obtainSharedSecret-C-end algorithm, which is only invoked in the SETUP and EXECUTE oracles, are distinct except probability $(q_{\text{SETUP}} + q_{\text{EXECUTE}})\epsilon^{\mathsf{sCDH}}_{\mathsf{ECDH}} + \binom{q_{\text{SETUP}}+q_{\text{EXECUTE}}}{2}2^{2-\min\{l_1,l_3,l_5,l_6\}}$. (2) By the entropy of the user PIN $\alpha_{\mathfrak{D}}$, none of the user PIN sampled in NEWU oracle is predicable except with probability $q_{\text{NEWU}}2^{-\alpha_{\mathfrak{D}}}$. (3) By the collision-resistance of H and the entropy of the Diffie-Hellman public keys 2^q and of pt values $2^{\max\{\mu,2,\mu'\}\lambda}$, we have the all H(pin), Diffie-Hellman public keys, pt values, are respectively distinct except probability in total $\epsilon^{\mathsf{coll\text{-}res}}_{\mathsf{H}} + \binom{q_{\text{SETUP}+\text{EXECUTE}}}{2}2^{1-q} + \binom{q_{\text{SEND-BIND-T}}}{2}2^{-\min\{\mu,2,\mu'\}\lambda}$. (4) By the IND-1CPA-H$_2$ security of SKE$_1$ and the IND-1CPA security of SKE$_2$ and SKE$_3$, the pins encrypted by the underlying puvProtocol in the setPIN-C algorithm, which is only invoked in the SETUP oracle, are indistinguishable from random except probability $q_{\text{SETUP}}\max\{\epsilon^{\mathsf{ind\text{-}1cpa\text{-}H_2}}_{\mathsf{SKE}_1}, \epsilon^{\mathsf{ind\text{-}1cpa}}_{\mathsf{SKE}_2}, \epsilon^{\mathsf{ind\text{-}1cpa}}_{\mathsf{SKE}_3}\}$. (5) By the IND-1\$PA-LPC security of SKE$_i$ for $i \in \{1, 2, 3\}$, the pinHashs encrypted by the underlying puvProtocol in the obtainPinUvAuthToken-C-start algorithm, which is invoked only in the EXECUTE oracle, are indistinguishable from random except probability $q_{\text{EXECUTE}}\max\{\epsilon^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}_{\mathsf{SKE}_1}, \epsilon^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}_{\mathsf{SKE}_2}, \epsilon^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}_{\mathsf{SKE}_3}\}$.

Finally, the adversary $\mathcal{A}$ cannot trigger the flip of the win-SUF-t′ predicate in Figure 6 via condition (i) in Line 8, due to the design of CTAP 2.1, see validate-T algorithm in CTAP 2.1. (ii) in Line 9, due to the distinction of Diffie-Hellman public keys, (iii) in Line 10, due to the distinction of Diffie-Hellman public keys and pts, (iv) in Line 11-14, since $\mathcal{A}$ obtains no information about pins or pts and can only win by randomly guessing the pin in the SETUP oracle maximal pinRetriesMax times for each token session, or the pt values or the tags t in the Validate algorithm in the VALIDATE oracle, which happens with probability except

$q_{\textsc{Setup}}\mathsf{pinRetriesMax}2^{-\alpha_{\mathfrak{D}}} + q_{\textsc{Validate}}2^{-\min\{\mu\lambda,2\lambda,\mu'\lambda,l_2,l_4,l_7\}}$ in total, modeling H_7 as a random oracle. □

The above theorem proves that CTAP 2.1 only accepts messages under the user's approval, which is captured by winning condition 1. Winning conditions 2 and 3 capture the uniqueness of each session identifiers: if two sessions are partnered with each other, then they are each other's unique partners. Condition 4 ensures the token only accepts the authorization from a client that it binds to if (1) the binding phase is trusted, (2) the binding state (on the client side) is not compromised if available, and (3) the user PIN that sets up the token is not corrupted.

As is to be expected, the above theorem only holds when the token's user PINs have large enough entropy. If a user PIN is predictable, the attacker can perform active attacks and authorize malicious commands towards the token.

Moving to the security guarantees against quantum adversaries, we note that the asymmetric cryptographic primitives in $\mathsf{puvProtocol}_1$ and $\mathsf{puvProtocol}_2$ are simply ECDH, which is quantum-vulnerable. Therefore, $\mathcal{A}$ can trivially win SUF-t′ experiment by selecting the Pin/Uv Auth Protocol in a test session to be $\mathsf{puvProtocol}_1$ or $\mathsf{puvProtocol}_2$. The theorem below suggests the security of the test session if $\mathsf{puvProtocol}_3$ is selected as instantiation.

Theorem 3 (QPT security of CTAP 2.1)**.** *Let* $\mathsf{ePACA} = (\mathsf{Reboot}, \mathsf{Setup}, \mathsf{Bind}, \mathsf{Auth}, \mathsf{Validate})$ *denote the CTAP 2.1 protocol described in Section V-B. Assume that the underlying* H *is* $\epsilon_{\mathsf{H}}^{\mathsf{coll\text{-}res}}$*-collision resistant,* H_5 *is* $\epsilon_{\mathsf{H}_5}^{\mathsf{swap}}$*-*$\mathsf{swap}$ *secure,* H_i *is* $\epsilon_{\mathsf{H}_i}^{\mathsf{prf}}$*-*$\mathsf{prf}$ *secure for* $i \in \{6,7\}$*,* SKE_3 *is* $\epsilon_{\mathsf{SKE}_3}^{\mathsf{ind\text{-}1cpa}}$*-IND-1CPA and* $\epsilon_{\mathsf{SKE}_3}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}$*-IND-1\$PA-LPC secure, and that the KEM in* $\mathsf{puvProtocol}_3$ *with public-key entropy* α_{pk} *and ciphertext entropy* α_c *is* $\epsilon_{\mathsf{KEM}}^{\mathsf{ind\text{-}cca}}$*-IND-CCA secure. If there exists a QPT adversary* $\mathcal{A}$ *that breaks the SUF-t′ security of ePACA for a test session* π *that uses* $\mathsf{puvProtocol}_3$*, then we have that*

$$\begin{aligned}
&\mathsf{Adv}_{\mathsf{ePACA},\mathsf{QPT}}^{\mathsf{SUF\text{-}t'}}(\mathcal{A})\\
\leq&(q_{\textsc{Setup}} + q_{\textsc{Execute}})(\epsilon_{\mathsf{KEM}}^{\mathsf{ind\text{-}cca}} + \epsilon_{\mathsf{H}_5}^{\mathsf{swap}} + \epsilon_{\mathsf{H}_6}^{\mathsf{prf}})\\
&+\binom{q_{\textsc{Setup}} + q_{\textsc{Execute}}}{2}2^{1-l_6} + \epsilon_{\mathsf{H}}^{\mathsf{coll\text{-}res}} + q_{\textsc{NewU}}2^{-\alpha_{\mathfrak{D}}}\\
&+\binom{q_{\textsc{Send-Bind-T}}}{2}2^{-\mu'\lambda} + \binom{q_{\textsc{Execute}}}{2}(2^{-\alpha_{pk}} + 2^{-\alpha_c})\\
&+q_{\textsc{Setup}}\epsilon_{\mathsf{SKE}_3}^{\mathsf{ind\text{-}1cpa}} + q_{\textsc{Execute}}\epsilon_{\mathsf{SKE}_3}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}\\
&+q_{\textsc{Setup}}\mathsf{pinRetriesMax}2^{-\alpha_{\mathfrak{D}}} + \binom{q_{\textsc{Execute}}}{2}(2^{-\alpha_{pk}} + 2^{-\alpha_c})\\
&+q_{\textsc{Validate}}(2^{-\mu'\lambda} + \epsilon_{\mathsf{H}_7}^{\mathsf{prf}} + 2^{-l_7})
\end{aligned}$$

where $q_{\mathcal{O}}$ *denotes the number of queries to* $\mathcal{O} = \{\textsc{Setup}, \textsc{Execute}, \textsc{Validate}\}$.

Proof Sketch. The proof is similar to the one for Theorem 2 and consists of following steps: (1) By the IND-CCA security of KEM, the swap security of H_5, and the prf security of H_6, all keys K derived in from the encapsulation of the underlying puvProtocol in the obtainSharedSecret-C-end algorithm, which is only invoked in the SETUP and EXECUTE oracles, are distinct except probability $(q_{\textsc{Setup}}+q_{\textsc{Execute}})\epsilon_{\mathsf{ECDH}}^{\mathsf{sCDH}} + (q_{\textsc{Setup}} + q_{\textsc{Execute}})(\epsilon_{\mathsf{KEM}}^{\mathsf{ind\text{-}cca}} + \epsilon_{\mathsf{H}_5}^{\mathsf{swap}} + \epsilon_{\mathsf{H}_6}^{\mathsf{prf}}) + \binom{q_{\textsc{Setup}}+q_{\textsc{Execute}}}{2}2^{1-l_6}$. (2) By the entropy of the user PIN $\alpha_{\mathfrak{D}}$, none of the user PIN sampled in NEWU oracle is predicable except with probability $q_{\textsc{NewU}}2^{-\alpha_{\mathfrak{D}}}$. (3) By the collision-resistance of H and the entropy $2^{-\mu'\lambda}$ of pt values sampled in the SEND-BIND-T oracle, we have all $\mathsf{H}(\mathsf{pin})$ and pt values respectively distinct except probability in total $\epsilon_{\mathsf{H}}^{\mathsf{coll\text{-}res}} + \binom{q_{\textsc{Send-Bind-T}}}{2}2^{-\mu'\lambda}$. (4) By the IND-1CPA security of SKE_3, the pins encrypted by the underlying $\mathsf{puvProtocol}_3$ in the setPIN-C algorithm, which is only invoked in the SETUP oracle, are indistinguishable from random except probability $q_{\textsc{Setup}}\epsilon_{\mathsf{SKE}_3}^{\mathsf{ind\text{-}1cpa}}$. (5) By the IND-1\$PA-LPC security of SKE_3, the pinHashs encrypted by the underlying $\mathsf{puvProtocol}_3$ in the obtainPinUvAuthToken-C-start algorithm, which is invoked only in the EXECUTE oracle, are indistinguishable from random except probability $q_{\textsc{Execute}}\epsilon_{\mathsf{SKE}_3}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}$.

Finally, the adversary $\mathcal{A}$ cannot trigger the flip of the win-SUF-t′ predicate in Figure 6 via condition (i) in Line 8, due to the design of CTAP 2.1, see validate-T algorithm in CTAP 2.1, (ii) in Line 9, since the collision of KEM public keys or ciphertexts with entropy α_{pk} or α_c happens at most $\binom{q_{\textsc{Execute}}}{2}(2^{-\alpha_{pk}} + 2^{-\alpha_c})$, (iii) in Line 10, due to the pairwise distinct KEM public keys and pts in the tokens' session identifiers, (iv) in Line 11-14, since $\mathcal{A}$ obtains no information about pins or pts and can only win by randomly guessing the pin in the SETUP oracle maximal pinRetriesMax times for each token session, or the pt values or the tags t in the Validate algorithm in the VALIDATE oracle, which happens with probability except $q_{\textsc{Setup}}\mathsf{pinRetriesMax}2^{-\alpha_{\mathfrak{D}}} + q_{\textsc{Validate}}2^{-\mu'\lambda} + \epsilon_{\mathsf{H}_7}^{\mathsf{prf}} + 2^{-l_7}$ in total, assuming the prf security of the underlying H_7. □

As such, we suggest to add our PQ instantiation $\mathsf{puvProtocol}_3$ of CTAP 2.1 to the specifications. As mentioned in Section V-C, we also suggest to increase the security parameter from 256 to 512, in order to preserve the current 256-bits level security.

VI. FIDO2 COMPOSITION

In this section, we analyze the security of the composition of WebAuthn 2 and CTAP 2.1. To provide a more generalized result, we first define the *user authentication* (ua) security model for the composition of any ePIA and ePACA protocols, which we refer to as ePIA+ePACA. Then, we formally reduce the ua security of ePIA+ePACA to the auth security of the underlying ePIA (see Section IV-C) and the SUF-t′ security of the underlying ePACA protocols (see Section V-D). In this section, we respectively use $\bar{\pi}$ and π to denote the ePIA and ePACA session, respectively, to distinguish them clearly.

A. Security Model of ePIA+ePACA

As before, to define the ua security property, we start with describing the trust model, oracles, and winning conditions.

a) Trust Model: The trust model for ua covers both the ones for auth and for SUF-t$'$. Additionally, we assume a server-to-client authenticated channel, which is in practice guaranteed by a TLS connection. As before, we assume "trust-on-first-use", which means, the Setup phase and the initialization of the Bind phase in ePACA and the Register phase in ePIA are authenticated.

b) Oracles: During the execution of the ua experiment, the adversary $\mathcal{A}$ has access to all oracles defined in the SUF-t$'$ experiment except AUTH and VALIDATE. Furthermore, $\mathcal{A}$ is allowed to query NEWS, NEWTPLA, and CORRUPT from the auth experiment, in addition to the following oracles:

REGISTER$((S,i),(T,j,j'),(C,k),\mathsf{tb},UV,d)$**:** This oracle simulates the honest registration between server S and token T via client C. This oracle is the same as the one in the auth experiment except that after the invocation of $(m_{\mathsf{rcom}}, m_{\mathsf{rcl}}) \leftarrow \mathsf{rCom}(\mathsf{id}_S, m_{\mathsf{rch}}, \mathsf{tb})$, additionally $(m_{\mathsf{rcom}}, t) \leftarrow \textsc{Auth}(C,k,m_{\mathsf{rcom}})$ and $\mathsf{status} \leftarrow \textsc{Validate}(T, j', m_{\mathsf{rcom}}, t, d)$ are queried. Moreover, the game aborts if $\mathsf{status} \neq \mathsf{accepted}$. Here, AUTH and VALIDATE are defined in the SUF-t$'$ experiment.

CHALLENGE$((S,i),(C,k),\mathsf{tb},UV)$**:** This oracle simulates the process of the server S generating a challenge nonce and sending it to the client C in an authenticated channel. This oracle is the same as in the auth experiment except that after the invocation of $(m_{\mathsf{rcom}}, m_{\mathsf{rcl}}) \leftarrow \mathsf{rCom}(\mathsf{id}_S, m_{\mathsf{rch}}, \mathsf{tb})$ we additionally query $(m_{\mathsf{rcom}}, t) \leftarrow \textsc{Auth}(C,k,m_{\mathsf{rcom}})$ and $\mathsf{status} \leftarrow \textsc{Validate}(T, j', m_{\mathsf{rcom}}, t, d)$, and append tag t to the output.

RESPONSE$((T,j,j'),m_{\mathsf{acom}},t,d)$**:** This oracle simulates the token receiving messages from a client and producing its response. This oracle is the same as the one defined in the auth experiment except that we additionally query $\mathsf{status} \leftarrow \textsc{Validate}(T, j', m_{\mathsf{rcom}}, t, d)$, and abort if $\mathsf{status} \neq \mathsf{accepted}$.

COMPLETE$((S,i),m_{\mathsf{acl}},m_{\mathsf{arsp}})$**:** This oracle simulates the server verifying the response message and the client message. This oracle is the same as in the auth experiment except that the winning predicate is Win-ua defined in Figure 8.

It is important to note that AUTH and VALIDATE (from the SUF-t$'$ experiment) are embedded in the REGISTER, CHALLENGE, and RESPONSE oracles in Figure 7.

c) Winning Conditions: We say *user authentication* (ua) holds, if all of the following conditions hold when an ePIA server session $\bar{\pi}_S^i$ accepts a client message m_{acl} and a response message m_{arsp}:

1) The non-$\perp$ session identifiers of the ePIA token (resp., server) sessions do not collide with each other, see Line 37 - 40 in Figure 8.
2) The partnered token and server sessions must have the identical agreed content unless the registration context on the token is corrupted, see Line 42 in Figure 8.
3) The non-$\perp$ session identifiers of the ePACA token (resp., client) sessions that completed Bind, do not collide with each other, see Line 44 - 45 in Figure 8.
4) During registration, the ePIA token and server sessions must partner with each other and the authorized command message and tag must have been output by one of the non-compromised partners of the ePACA token session without corrupting its setup user, see Line 47 - 50 in Figure 8.
5) The token T that has been registered with S, must own an ePIA session $\bar{\pi}_T^i$ that is partnered with $\bar{\pi}_S^i$ and produce a response message unless T's registration context of S is corrupted, see Line 52 - 56 in Figure 8.
6) The above response message must be produced after an ePACA session $\pi_T^{j'}$ validates some authorized command m_{acom} and tag t with the approval from the user, see Line 58 - 58 in Figure 8.
7) The above command m_{acom} and tag t must be authorized by a client ePACA session π_C^k that is partnered with $\pi_T^{j'}$ for some challenge message m_{rch} that has been produced by the ePIA session $\bar{\pi}_S^i$, unless π_C^k is compromised or the PIN that sets up token T has been corrupted, see Line 61 - 66 in Figure 8.

```
$\mathsf{Expt}^{\mathsf{ua}}_{\mathsf{ePIA+ePACA},\mathsf{Compl}}(\mathcal{A})$:
    $\mathcal{L}_{\mathsf{frsh}}, \mathcal{L}_{\textsc{Auth}} \leftarrow \emptyset$ //as in auth and SUF-t$'$ experiments
    $\mathcal{L}_{\textsc{Register}}, \mathcal{L}_{\textsc{Challenge}}, \mathcal{L}_{\textsc{Response}} \leftarrow \emptyset$
    $\mathsf{win\text{-}ua} \leftarrow \mathsf{false}$
    $() \xleftarrow{\$} \mathcal{A}^{\mathcal{O}}(1^\lambda)$
    $\mathbf{return}\ \mathsf{win\text{-}ua}$

$\textsc{Register}((S,i),(T,j,j'),(C,k),\mathsf{tb},UV,d)$:
    $\mathbf{if}\ \mathsf{pkCP}_S = \perp\ \mathbf{or}\ \mathsf{suppUV}_T = \perp\ \mathbf{or}\ \bar{\pi}_S^i \neq \perp\ \mathbf{or}\ \bar{\pi}_T^j \neq \perp\ \mathbf{or}\ \mathsf{rc}_T[S] \neq \perp$:
        $\mathbf{return}\ \perp$
    $\bar{\pi}_S^i.\mathsf{pkCP} \leftarrow \mathsf{pkCP}_S$, $\bar{\pi}_T^j.\mathsf{suppUV} \leftarrow \mathsf{suppUV}_T$
    $m_{\mathsf{rch}} \xleftarrow{\$} \mathsf{rChall}(\bar{\pi}_S^i, \mathsf{tb}, UV)$
    $(m_{\mathsf{rcom}}, m_{\mathsf{rcl}}) \xleftarrow{\$} \mathsf{rCom}(\mathsf{id}_S, m_{\mathsf{rch}}, \mathsf{tb})$
    $(m_{\mathsf{rcom}}, t) \leftarrow \textsc{Auth}(C, k, m_{\mathsf{rcom}})$
    $\mathsf{status} \leftarrow \textsc{Validate}(T, j', m_{\mathsf{rcom}}, t, d)$
    $\mathbf{if}\ \mathsf{status} \neq \mathsf{accepted}$: $\mathbf{return}\ (m_{\mathsf{rch}}, m_{\mathsf{rcl}}, m_{\mathsf{rcom}}, t, \perp, \perp)$
    $(m_{\mathsf{rrsp}}, \mathsf{rc}_T) \xleftarrow{\$} \mathsf{rRsp}(\bar{\pi}_T^j, m_{\mathsf{rcom}})$
    $(\mathsf{rc}_S, d') \leftarrow \mathsf{rVrfy}(\bar{\pi}_S^i, m_{\mathsf{rcl}}, m_{\mathsf{rrsp}})$
    $\mathcal{L}_{\mathsf{frsh}} \leftarrow \mathcal{L}_{\mathsf{frsh}} \cup (S, T)$
    $\mathcal{L}_{\textsc{Register}} \leftarrow \mathcal{L}_{\textsc{Register}} \cup \{(S, i, T, j, j', C, k, m_{\mathsf{rch}}, m_{\mathsf{rcl}}, m_{\mathsf{rcom}}, t, m_{\mathsf{rrsp}})\}$
    $\mathbf{return}\ (m_{\mathsf{rch}}, m_{\mathsf{rcl}}, m_{\mathsf{rcom}}, t, m_{\mathsf{rrsp}}, d')$
$\textsc{Challenge}((S,i),(C,k),\mathsf{tb},UV)$:
    $\mathbf{if}\ \mathsf{pkCP}_S = \perp\ \mathbf{or}\ \bar{\pi}_S^i \neq \perp$: $\mathbf{return}\ \perp$
    $\bar{\pi}_S^i.\mathsf{pkCP} \leftarrow \mathsf{pkCP}_S$
    $m_{\mathsf{ach}} \xleftarrow{\$} \mathsf{aChall}(\bar{\pi}_S^i, \mathsf{tb}, UV)$
    $(m_{\mathsf{acom}}, m_{\mathsf{acl}}) \leftarrow \mathsf{aCom}(\mathsf{id}_S, m_{\mathsf{ach}}, \mathsf{tb})$
    $(m_{\mathsf{acom}}, t) \leftarrow \textsc{Auth}(C, k, m_{\mathsf{acom}})$
    $\mathcal{L}_{\textsc{Challenge}} \leftarrow \mathcal{L}_{\textsc{Challenge}} \cup \{(S, i, C, k, m_{\mathsf{ach}}, m_{\mathsf{acl}}, m_{\mathsf{acom}}, t)\}$
    $\mathbf{return}\ (m_{\mathsf{ach}}, m_{\mathsf{acl}}, m_{\mathsf{acom}}, t)$
$\textsc{Response}((T,j,j'),m_{\mathsf{acom}},t,d)$:
    $\mathsf{status} \leftarrow \textsc{Validate}(T, j', m_{\mathsf{acom}}, t, d)$
    $\mathbf{if}\ \mathsf{status} \neq \mathsf{accepted}$: $\mathbf{return}\ \perp$
    $\mathbf{if}\ \mathsf{suppUV}_T = \perp\ \mathbf{or}\ \bar{\pi}_T^j \neq \perp$: $\mathbf{return}\ \perp$
    $\bar{\pi}_T^j.\mathsf{suppUV} \leftarrow \mathsf{suppUV}_T$
    $(m_{\mathsf{arsp}}, \mathsf{rc}_T) \xleftarrow{\$} \mathsf{aRsp}(\bar{\pi}_T^j, \mathsf{rc}_T, m_{\mathsf{acom}})$
    $\mathcal{L}_{\textsc{Response}} \leftarrow \mathcal{L}_{\textsc{Response}} \cup \{(T, j, j', m_{\mathsf{acom}}, t, d, m_{\mathsf{arsp}})\}$
    $\mathbf{return}\ m_{\mathsf{arsp}}$
$\textsc{Complete}((S,i),m_{\mathsf{acl}},m_{\mathsf{arsp}})$:
    $\mathbf{if}\ \bar{\pi}_S^i = \perp\ \mathbf{or}\ \bar{\pi}_S^i.\mathsf{st}_{\mathsf{exe}} \neq \mathsf{running}$: $\mathbf{return}\ \perp$
    $(\mathsf{rc}_S, d) \xleftarrow{\$} \mathsf{aVrfy}(\bar{\pi}_S^i, \mathsf{rc}_S, m_{\mathsf{acl}}, m_{\mathsf{arsp}})$
    $\mathbf{if}\ d = 1$: $\mathsf{win\text{-}ua} \leftarrow \mathsf{Win\text{-}ua}(S, i)$
    $\mathbf{return}\ d$
```

Fig. 7. The ua security experiment for ePIA+ePACA. The winning condition Win-ua is defined in Figure 8. The AUTH and VALIDATE oracles are defined in $\mathsf{Expt}^{\mathsf{SUF\text{-}t'}}_{\mathsf{ePACA},\mathsf{Compl}}$ experiment in Figure 6.

```
Win-ua$(S, i)$:
  //The non-$\perp$ session identifiers of ePIA token (resp. server) sessions do not collide with each other
  if $\exists (T_1, j_1), (T_2, j_2)$ s.t. $(T_1, j_1) \neq (T_2, j_2)$ and $\pi_{T_1}^{j_1}.\mathsf{sid} = \pi_{T_2}^{j_2}.\mathsf{sid} \neq \perp$
    return 1
  if $\exists (S_1, i_1), (S_2, i_2)$ s.t. $(S_1, i_1) \neq (S_2, i_2)$ and $\pi_{S_1}^{i_1}.\mathsf{sid} = \pi_{S_2}^{i_2}.\mathsf{sid} \neq \perp$
    return 1
  //In ePIA, the partnered session have the identical agreed content unless the registration context on the token is corrupted
  if $\exists (S', i'), (T', j')$ s.t. $\bar{\pi}_{S'}^{i'}.\mathsf{sid} = \bar{\pi}_{T'}^{j'}.\mathsf{sid} \neq \perp$ and $(S', T') \in \mathcal{L}_{\mathsf{frsh}}$
      and $\bar{\pi}_{S'}^{i'}.\mathsf{agCon} \neq \bar{\pi}_{T'}^{j'}.\mathsf{agCon}$: return 1
  //The non-$\perp$ session identifiers of ePACA token (resp. client) sessions that completed Bind algorithm don't collide with each other
  if $\exists (C_1, k_1), (C_2, k_2)$ s.t. $(C_1, k_1) \neq (C_2, k_2)$ and $\pi_{C_1}^{k_1}.\mathsf{st}_{\mathsf{exe}} =$
      $= \pi_{C_2}^{k_2}.\mathsf{st}_{\mathsf{exe}} = \mathsf{bindDone}$ and $\pi_{C_1}^{j_1}.\mathsf{sid} = \pi_{C_2}^{j_2}.\mathsf{sid}$: return 1
  if $\exists (T_1, j_1'), (T_2, j_2')$ s.t. $(T_1, j_1') \neq (T_2, j_2')$ and $\pi_{T_1}^{j_1'}.\mathsf{st}_{\mathsf{exe}} =$
      $= \pi_{T_2}^{j_2'}.\mathsf{st}_{\mathsf{exe}} = \mathsf{bindDone}$ and $\pi_{T_1}^{j_1'}.\mathsf{sid} = \pi_{T_2}^{j_2'}.\mathsf{sid}$: return 1
  //The ePIA or ePACA sessions used in the registration phase must partner with each other.
  foreach $(S', x, T', y, y', C', z, m_{\mathsf{rch}}, m_{\mathsf{rcl}}, m_{\mathsf{rcom}}, t_{\mathsf{rcom}}, m_{\mathsf{rrsp}}) \in \mathcal{L}_{\textsc{Register}}$
    if $\bar{\pi}_{T'}^{y}.\mathsf{sid} \neq \bar{\pi}_{S'}^{x}.\mathsf{sid}$: return 1
    $(C'', z') \leftarrow \mathsf{bindPartner}(T', y')$
    if $(C'', z', m_{\mathsf{rcom}}, t_{\mathsf{rcom}}) \notin \mathcal{L}_{\textsc{Auth}}$ and $\Big((C'', z') = (\perp, \perp)$
        or $\pi_{C''}^{z'}.\mathsf{compromised} = \mathsf{false}\Big)$ and $\pi_{T'}^{y'}.\mathsf{pinCorr} = \mathsf{false}$: return 1
  //A response message $m_{\mathsf{arsp}}$ must be output by $T$ that registered with $S$, unless $T$'s registration context of $S$ is corrupted
  $T \leftarrow \mathsf{regPartner}(S, i)$
  if $\nexists j$ s.t. $\bar{\pi}_S^i.\mathsf{sid} = \bar{\pi}_T^j.\mathsf{sid}$
    if $(S, T) \in \mathcal{L}_{\mathsf{frsh}}$: return 1
  elseif $\nexists (j', m_{\mathsf{acom}}, t, d, m_{\mathsf{arsp}})$ s.t. $(T, j, j', m_{\mathsf{acom}}, t, d, m_{\mathsf{arsp}}) \in \mathcal{L}_{\textsc{Response}}$
    return 1
  //Above $m_{\mathsf{arsp}}$ must be output under user approval
  elseif $d \neq \mathsf{accepted}$: return 1
  else
  //Above $m_{\mathsf{arsp}}$ must be output after above $T$ validates above message-tag pair $(m_{\mathsf{acom}}, t)$, which encodes $m_{\mathsf{ach}}$ output by session $\bar{\pi}_S^i$
    $(C, k) \leftarrow \mathsf{bindPartner}(T, j')$
    if $(C, k, m_{\mathsf{acom}}, t) \notin \mathcal{L}_{\textsc{Auth}}$
      if $(C, k) = (\perp, \perp)$ or $\pi_C^k.\mathsf{compromised} = \mathsf{false}$
        if $\pi_T^{j'}.\mathsf{pinCorr} = \mathsf{false}$: return 1
    elseif $\nexists (m_{\mathsf{ach}}, m_{\mathsf{acl}})$ s.t. $(S, i, C, k, m_{\mathsf{ach}}, m_{\mathsf{acl}}, m_{\mathsf{acom}}, t) \in \mathcal{L}_{\textsc{Challenge}}$
      return 1
  return 0
```

Fig. 8. The Win-ua in ua security experiment for ePIA+ePACA. The regPartner and bindPartner predicates are defined in Figure 2 and Figure 6, respectively.

Definition 3 (ua security for ePIA+ePACA)**.** *Let* Compl $\in \{\mathsf{PPT}, \mathsf{QPT}\}$*,* ePACA *be an extended PIN-based access control for authenticators protocol, and* ePIA *be an extended passwordless authentication protocol. We say that the composition* ePIA+ePACA *has* user authentication*, or is* ua*-secure for short, if for all* Compl *adversaries* $\mathcal{A}$ *the advantage*

$$\mathsf{Adv}^{\mathsf{ua}}_{\mathsf{ePIA+ePACA,Compl}}(\mathcal{A}) := \Pr[\mathsf{Expt}^{\mathsf{ua}}_{\mathsf{ePIA+ePACA,Compl}}(\mathcal{A}) = 1]$$

in winning the game $\mathsf{Expt}^{\mathsf{ua}}_{\mathsf{ePIA+ePACA,Compl}}$ *as described in Figure 7 is negligible in the security parameter* λ*.*

We can reduce the security of the ePIA+ePACA protocol to the security of the ePIA and the ePACA protocol as stated in the next theorem. We give the full proof in Section K in the appendix.

Theorem 4 (PPT/QPT security of the composition)**.** *Let* Compl $\in \{\mathsf{PPT}, \mathsf{QPT}\}$*. Let* Σ *denote an* ePIA *protocol and* Π *denote an* ePACA *protocol. If there exists a* Compl *adversary* $\mathcal{A}$ *that breaks the* ua *security of the composition* $\Sigma + \Pi$*, then there must exist* Compl *adversaries* $\mathcal{A}_1$ *and* $\mathcal{A}_2$ *that respectively break the* auth *security of* Σ *and the* SUF-t$'$ *security of* Π *such that*

$$\mathsf{Adv}^{\mathsf{ua}}_{\Sigma+\Pi,\mathsf{Compl}}(\mathcal{A}) \leq \mathsf{Adv}^{\mathsf{auth}}_{\Sigma,\mathsf{Compl}}(\mathcal{A}_1) + \mathsf{Adv}^{\mathsf{SUF\text{-}t'}}_{\Pi,\mathsf{Compl}}(\mathcal{A}_2).$$

In particular, the winning condition 1 and 3 capture the uniqueness of each WebAuthn 2 and CTAP 2.1 session identifiers. If two sessions are partnered with each other, then they are each other's unique partners. The winning condition 2 ensures that if the credential private key between the partnered token and server sessions is not corrupted, then both sessions must agree on the server identifier id_S, the $\mathsf{H}(\mathsf{ch}, \mathsf{tb})$ hash of the challenge nonce and the token binding states, the local counter n, and the user presence UP and verification UV conditions. Furthermore, if the underlying hash function H is collision resistant, the token and server sessions also implicitly agree on the token binding state tb. Our theorem proves partnership of WebAuthn 2 sessions in the authenticated registration phase and the resilience of man-in-the-middle attacks against WebAuthn 2 in the authentication phase unless the corruption of the registration context on the token, which are captured by winning conditions 4 and 5. The messages between every partnered token and server session in WebAuthn 2 must be authorized by the client, which is connected to the server over an authenticated channel in WebAuthn 2 and bound to the token in CTAP 2.1 unless the adversary make certain corruptions, which is captured by wining conditions 4,6,7.

VII. Related work

The only published in-depth formal analysis of FIDO2 is Barbosa et al. [2], which we address in-depth. We note that a recently released manuscript [11] also analyzes aspects of FIDO2, but their work focuses on WebAuthn's privacy aspects, and introducing the possibility of revocation, notably in the context of cryptocurrency wallets. Our work is essentially orthogonal to [11] in terms of focus, and we consider the newer versions of both sub-protocols.

To provide context for our comparison to [2], we first revisit the largest changes in CTAP 2.1 compared to CTAP 2.0.

A. Comparison between CTAP 2.0 and CTAP 2.1

Compared to the expired proposed standard of CTAP 2.0 [7], the latest draft review of CTAP 2.1 [6] has a number of differences, mainly from the following four aspects:

1) The definition of CTAP 2.0 is directly based on the concrete primitives such as the Diffie-Hellman key exchange and hash functions, while CTAP 2.1 is based on a so-called "PIN/UV Auth Protocol" abstract scheme, denoted by puvProtocol for short, which leads CTAP 2.1 to be PQ ready. Up to date, two instantiations of puvProtocol are officially announced, where CTAP 2.1 instantiated by the $\mathsf{puvProtocol}_1$ is close to CTAP 2.0. In particular, CTAP 2.1 instantiated with our hybrid construction $\mathsf{puvProtocol}_3$ proposed in Section V-C is provably PQ secure, as proven in Theorem 3.
2) In CTAP 2.0, the binding state that is used for the client's authorization and the token's validation is defined as so-called *pinToken*, which has the length of multiple of 128 bits and can be of unlimited length. In CTAP 2.1, the binding state is defined as so-called *pinUvAuthToken*, the length of which is however fixed: either 128 or 256 bits.

3) In CTAP 2.0, the pinToken is sampled during the reboot phase and then repeatedly re-used until the next invocation of the reboot algorithm. In contrast, the pinUvAuthToken in CTAP 2.1 is one-time – it is re-sampled after every usage. This difference exerts a great influence on the security: While CTAP 2.0 only satisfies $\mathsf{UF\text{-}t}$ security as proven by Barbosa et al. [2], CTAP 2.1 provably satisfies $\mathsf{SUF\text{-}t'}$ security, see Theorem 2.
4) CTAP 2.0 allows tokens and clients to share a pinUvAuthToken only when the users provide their correct pin, which is called *clientPIN method*. Instead, CTAP 2.1 additionally enables users to input their biometric information such as fingerprint if the built-in on-device user verification is physically supported by the token, which is called *built-in user verification method*. Notably, the built-in user verification method is always the preferred option when it is supported by the token. The biometric information is assumed to be unique and unpredictable for each user and is input to the token without any intermediary (therefore, the transmission can be considered to be authenticated). In our model, built-in user verification can be viewed as the simplified CTAP 2.1 using clientPIN method without the transmission of the encryption of pinHash.

B. Comparison with Barbosa et al. [2]

As mentioned before, our work builds on the first formal FIDO2 analysis in [2], and we compare several aspects.

WebAuthn comparison:

1) **Different analysis target**: The analysis of [2] assumes attestation type `Basic` such that "the server is assumed to know the attestation public key that uniquely identifies the authenticator" [2]. However, the token's attestation key pair is generated in the factory and at least 100,000 tokens should share same attestation key pair to ensure privacy ([1, Section 14.4], [12, Section 14.4.1]). Thus, Barbosa et al.'s analysis indeed proves the security of a batch of tokens that share the same attestation key pair instead of a single token. In contrast, we investigate WebAuthn with the default attestation type `None`, and our Theorem 1 also applies to WebAuthn with attestation type `Basic`. In particular, our analysis focuses on the security of each single token rather than a batch of tokens.
2) **Fine-grained abstraction**: Our WebAuthn abstraction is more detailed than [2]. For example, we include the supported signature list pkCP of the server, the optional UV-support of the token, and the token binding state tb. Our theorem implies that the server and token ultimately agree on these values, which is crucial for the desired security. Furthermore, the supported schemes list enables us to to exhibit a downgrade attack against WebAuthn and specify a security notion "Algorithm Agreement" for the corresponding protection.
3) **Active interference**: The security model of WebAuthn in [2] seems to allow active interference during the registration. This is true in [2]'s model because it assumes that each token has a unique attestation key pair and the server knows in advance which public key to use for signature verification; yet this is not true in practice by design, as mentioned previously. The official specification [12, Section 13.4.4] clearly acknowledges the MitM attack on registration, contradicting the implication of [2].
4) **Stronger adversary capability**: Barbosa et al. assume the tokens to be tamper-proof, i.e., the adversary is prevented from corrupting the internal state of any token. Our model, instead, includes a corruption oracle that enables an adversary to reveal the private signing key, capturing the real world scenario in which some tokens might be stolen and the private keys compromised.

CTAP comparison:

1) **Different analysis target**: Barbosa et al. analyzed CTAP 2.0 [7], while we investigate CTAP 2.1 [6]. As explained in Section VII-A, these two versions have numerous differences. Our paper carefully explores the abstraction gaps between CTAP 2.0 and CTAP 2.1.
2) **Improved security model**: We refine Barbosa et al.'s PACA security model. For example, the token binding states may be reset in REBOOT or SEND oracle. However, Barbosa et al. only mark the token sessions invalid in the REBOOT oracle but forgot the ones in the SEND oracle[8]. Furthermore, the PACA definition of invalidity is not suitable for CTAP 2.1, as the previous binding states of a token are reset after not only reboot but also the establishment of a new session. In this work, we define a code-based $\mathsf{SUF\text{-}t'}$ security, which refines and generalizes $\mathsf{SUF\text{-}t}$ security in [2].
3) **Proof gaps**: Although Barbosa et al. proved the security of CTAP 2.0, their proof has several technical gaps. To address this, we base the $\mathsf{SUF\text{-}t'}$ security of CTAP 2.1 on novel assumptions and provide a detailed proof. We summarize the gaps and shortcomings of the proofs from [2] in Section L in the appendix, and show how we solve each for our work.

The Composition of WebAuthn and CTAP:

1) **Different security model**: The security of the composition of WebAuthn 2 and CTAP 2.1 relies on the respective security guarantees. The differences between the syntax and the security models of both WebAuthn and CTAP compared to [2] propagate into a different security model for the composition, and we provide a fully detailed proof.

VIII. Limitations and Future Work

While our work covers many core aspects of CTAP and WebAuthn beyond the state-of-the-art, it remains an abstraction. Some of our main current limitations include that we do not yet model some of the new CTAP 2.1 features for enterprise customers, and do not make formal statements about the unlinkability of credentials or other detailed privacy statements. We leave the proof methodology for tighter upper bounds in all theorems in our paper as an open question.

[8]Recall that [2] defines the invalidity of a session such that "*if a token is rebooted, its binding states got reset and hence become invalid*" [2]

Acknowledgments

We are very grateful to Jacqueline Brendel for initiating the project, initial analysis of the standards, and valuable support throughout.

References

[1] Dirk Balfanz, Alexei Czeskis, Jeff Hodges, J.C. Jones, Michael B. Jones, Akshay Kumar, Angelo Liao, Rolf Lindemann, Emil Lundberg, Vijay Bharadwaj, Arnar Birgisson, Hubert Le Van Gong, Christiaan Brand, Langley Adam, Giridhar Mandyam, Mike West, and Jeffrey Yasskin. *Web authentication: An API for accessing public key credentials level 1 – W3C recommendation*. https://www.w3.org/TR/2019/REC-webauthn-1-20190304/. March 2019.

[2] Manuel Barbosa, Alexandra Boldyreva, Shan Chen, and Bogdan Warinschi. *Provable Security Analysis of FIDO2*. Cryptology ePrint Archive, Paper 2020/756. https://eprint.iacr.org/2020/756, accessed on 18.08.2022. 2020.

[3] Manuel Barbosa, Alexandra Boldyreva, Shan Chen, and Bogdan Warinschi. "Provable Security Analysis of FIDO2". In: *CRYPTO 2021, Part III*. Vol. 12827. LNCS. Virtual Event: Springer, Heidelberg, Aug. 2021.

[4] Mihir Bellare, Anand Desai, Eric Jokipii, and Phillip Rogaway. "A Concrete Security Treatment of Symmetric Encryption". In: *38th FOCS*. IEEE Computer Society Press, Oct. 1997.

[5] Nina Bindel, Udyani Herath, Matthew McKague, and Douglas Stebila. "Transitioning to a Quantum-Resistant Public Key Infrastructure". In: *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017*. Springer, Heidelberg, 2017.

[6] John Bradley, Jeff Hodges, Michael B. Jones, Akshay Kumar, Rolf Lindemann, Johan Verrept, Chad Armstrong, Konstantinos Georgantas, Fabian Kaczmarczyck, Nina Satragno, and Nuno Sung. *Client to Authenticator Protocol (CTAP) – Proposed Standard, June 15, 2021*. https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html. 2021.

[7] Christiaan Brand, Alexei Czeskis, Ehrensvärd Jakob, Michael B. Jones, Akshay Kumar, Rolf Lindemann, Adam Powers, and Johan Verrept. *Client to Authenticator Protocol (CTAP) – Proposed Standard, January 30, 2019*. https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html. 2019.

[8] Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. *NISTIR 8105 Report on Post-Quantum Cryptography*. Tech. rep. National Institute for Standards and Technology (NIST), 2016.

[9] Ronald Cramer and Victor Shoup. "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack". In: *SIAM Journal on Computing* 33.1 (2003). eprint: https://doi.org/10.1137/S0097539702403773.

[10] William F Ehrsam, Carl HW Meyer, John L Smith, and Walter L Tuchman. *Message verification and transmission error detection by block chaining*. US Patent 4,074,066. 1978.

[11] Lucjan Hanzlik, Julian Loss, and Benedikt Wagner. *Token meets Wallet: Formalizing Privacy and Revocation for FIDO2*. Cryptology ePrint Archive, Report 2022/084. https://ia.cr/2022/084. 2022.

[12] Jeff Hodges, J.C. Jones, Michael B. Jones, Akshay Kumar, Emil Lundberg, John Bradley, Christiaan Brand, Langley Adam, Giridhar Mandyam, Nina Satragno, Nick Steele, Jiewen Tan, Shane Weeden, Mike West, and Jeffrey Yasskin. *Web authentication: An API for accessing public key credentials level 2 – W3C recommendation*. https://www.w3.org/TR/2021/REC-webauthn-2-20210408/. April 2021.

[13] B. Kaliski, J. Jonsson, and A. Rusch. *PKCS #1: RSA Cryptography Specifications Version 2.2*. RFC 8017 (Informational). Internet Engineering Task Force, Nov. 2016.

[14] Jim Schaad. *CBOR Object Signing and Encryption (COSE)*. RFC 8152. July 2017.

Appendix A
Preliminaries

Definition 4. *We say* $\mathsf{F} : \mathcal{K} \times \mathcal{M} \to \mathcal{O}$ *is* ϵ-prf *secure, if for any efficient adversaries* $\mathcal{A}$*, any* $k \xleftarrow{\$} \mathcal{K}$*, and any truly random function* $\mathsf{R} : \mathcal{M} \to \mathcal{O}$*, it holds that,*

$$\mathsf{Adv}^{\mathsf{prf}}_{\mathsf{F},\mathcal{A}} := \left| \Pr[\mathcal{A}^{\mathsf{F}(k,\cdot)} = 1] - \Pr[\mathcal{A}^{\mathsf{R}(\cdot)} = 1] \right| \leq \epsilon$$

We say F *is* ϵ-swap *secure, if the function* $\bar{\mathsf{F}}$ *defined below is* ϵ-prf *secure.*

$$\bar{\mathsf{F}} : \mathcal{M} \times \mathcal{K} \to \mathcal{O}, \bar{\mathsf{F}}(m, k) := \mathsf{F}(k, m)$$

Definition 5. *Let* $\mathsf{SKE} = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ *be a symmetric key encryption scheme with symmetric key space* $\mathcal{K}$*. We say* SKE *is* ϵ*-one time* $\mathsf{IND\text{-}CPA}$ *secure with respect to function* H *(denoted by* $\mathsf{IND\text{-}1CPA\text{-}H}$*) secure, if the blow defined advantage of every (potential quantum) adversary* $\mathcal{A}$ *against* $\mathsf{Expt}^{\mathsf{IND\text{-}1CPA\text{-}H}}_{\mathsf{SKE}}$ *experiment in Figure 9 is bounded by,*

$$\mathsf{Adv}^{\mathsf{IND\text{-}1CPA\text{-}H}}_{\mathsf{SKE}}(\mathcal{A}) := \left| \Pr[\mathsf{Expt}^{\mathsf{IND\text{-}1CPA\text{-}H}}_{\mathsf{SKE}}(\mathcal{A}) = 1] - \frac{1}{2} \right| \leq \epsilon.$$

Definition 6. *Let* $\mathsf{SKE} = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ *be a symmetric key encryption scheme with symmetric key space* $\mathcal{K}$*. We say* SKE *is* ϵ-$\mathsf{IND\text{-}1\$PA\text{-}LPC}$ *secure, if the blow defined advantage of every (potential quantum) adversary* $\mathcal{A}$ *against* $\mathsf{Expt}^{\mathsf{IND\text{-}1\$PA\text{-}LPC}}_{\mathsf{SKE}}$ *experiment in Figure 9 is bounded by,*

$$\mathsf{Adv}^{\mathsf{IND\text{-}1\$PA\text{-}LPC}}_{\mathsf{SKE}}(\mathcal{A}) := \left| \Pr[\mathsf{Expt}^{\mathsf{IND\text{-}1\$PA\text{-}LPC}}_{\mathsf{SKE}}(\mathcal{A}) = 1] - \frac{1}{2} \right| \leq \epsilon.$$

```
$\mathsf{Expt}^{\mathsf{IND\text{-}1CPA\text{-}H}}_{\mathsf{SKE}}(\mathcal{A})$:
  $\mathsf{b} \xleftarrow{\$} \{0,1\}$
  $K \xleftarrow{\$} \mathsf{KG}()$
  $(m_0^\star, m_1^\star) \xleftarrow{\$} \mathcal{A}()$
  $\mathbf{if}\ |m_0^\star| \neq |m_1^\star|$
    $\mathbf{return}\ 0$
  $c^\star \xleftarrow{\$} \mathsf{Enc}(K, m_{\mathsf{b}}^\star)$
  $t^\star \leftarrow \mathsf{H}(K, c^\star)$
  $\mathsf{b}' \xleftarrow{\$} \mathcal{A}(c^\star, t^\star)$
  $\mathbf{return}\ [\![\mathsf{b} = \mathsf{b}']\!]$

$\mathsf{Expt}^{\mathsf{IND\text{-}1\$PA\text{-}LPC}}_{\mathsf{SKE}}(\mathcal{A})$:
  $\mathsf{b} \xleftarrow{\$} \{0,1\}$
  $K \xleftarrow{\$} \mathsf{KG}()$
  $(m_0^\star, m_1^\star) \xleftarrow{\$} \mathcal{A}()$
  $\mathbf{if}\ |m_0^\star| \neq |m_1^\star|$
    $\mathbf{return}\ 0$
  $c^\star \xleftarrow{\$} \mathsf{Enc}(K, m_{\mathsf{b}}^\star)$
  $\mathsf{b}' \xleftarrow{\$} \mathcal{A}^{\textsc{Rand},\textsc{Lpc}}(c^\star)$
  $\mathbf{return}\ [\![\mathsf{b} = \mathsf{b}']\!]$

$\textsc{Rand}(l)$:
  $m_0' \xleftarrow{\$} \{0,1\}^l$
  $m_1' \xleftarrow{\$} \{0,1\}^l$
  $c' \xleftarrow{\$} \mathsf{Enc}(K, m_{\mathsf{b}}')$
  $\mathbf{return}\ (m_0', m_1', c')$
$\textsc{Lpc}(c)$:
  $\mathbf{if}\ c = c^\star$
    $\mathbf{return}\ 0$
  $\mathbf{return}\ [\![m_0^\star = \mathsf{Dec}(K, c)]\!]$
```

Fig. 9. $\mathsf{IND\text{-}1CPA\text{-}H}$ and $\mathsf{IND\text{-}1\$PA\text{-}LPC}$ experiments for $\mathsf{SKE} = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$.

Appendix B
CBC Mode and IND-1$PA-LPC Security

The Cipher Block Chaining (CBC) mode is a block cipher mode of operation invented by Ehrsam et al. in 1976 [10]. The CBC can be divided into two categories: CBC_0, whose initial vector is a string of zero bits, and CBC_R, whose initial vector is a random bit string. We first recall CBC as an instance of symmetric key encryption. Let $\mathcal{K} := \{0,1\}^{f_1(\lambda)}$, $\mathcal{M} := \{0,1\}^{f_2(\lambda)}$, and $\mathcal{O} := \{0,1\}^{f_2(\lambda)}$ respectively denote the symmetric key space, message space, and output space of an invertible function $\mathsf{F} : \mathcal{K} \times \mathcal{M} \to \mathcal{O}$, where f_1 and f_2 denote arbitrary polynomial functions. Then, both CBC_0 and CBC_R are defined in Figure 10. Here, we simply assume that the input message m of the encryption algorithm always has the length of a multiple of $f_2(\lambda)$. It is straightforward that CBC_0 is a deterministic encryption scheme.

The $\mathsf{IND\text{-}1\$PA}$ security of the deterministic CBC_0 was proven by Barbosa et al. [2]. Moreover, the $\mathsf{IND\text{-}CPA}$ security of the randomized CBC_R was proven by Bellare et al. [4].

```
$\mathsf{KG}(1^\lambda)$:
    $K \xleftarrow{\$} \mathcal{K}$
    return $K$
$\mathsf{Enc}(K, m)$:
    $x_1 \| \ldots \| x_n \leftarrow m$ s.t. $|x_i| = f_2(\lambda)\ \forall i \in \{1, \cdots, n\}$
    $y_0 \xleftarrow{\$} \mathsf{SetIV}()$
    for $i = 1, \ldots, n$
        $y_i \leftarrow \mathsf{F}(K, y_{i-1} \oplus x_i)$
    $y \leftarrow y_0 \| \cdots \| y_n$
    return $y$

$\mathsf{Dec}(K, c)$:
    $y_0 \| \ldots \| y_n \leftarrow c$ s.t. $|y_i| = f_2(\lambda)\ \forall i \in \{0, \cdots, n\}$
    for $i = 1, \ldots, n$
        $x_i \leftarrow y_{i-1} \oplus \mathsf{F}^{-1}(K, y_i)$
    $m \leftarrow x_1 \| \cdots \| x_n$
    return $m$
```

Fig. 10. CBC mode $\mathsf{SKE} = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ with symmetric key space $\mathcal{K} := \{0,1\}^{f_1(\lambda)}$ for arbitrary polynomial function f_1. If $\mathsf{SKE} = \mathsf{CBC}_0$, then $\mathsf{SetIV}()$ outputs a string of zero bits of length $f_2(\lambda)$. If $\mathsf{SKE} = \mathsf{CBC}_R$, then $\mathsf{SetIV}()$ outputs a random string of length $f_2(\lambda)$.

Below, we prove the IND-1\$PA-LPC security of both CBC_0 and CBC_R based on above two security conclusions.

Theorem 5 (IND-CPA $\implies$ IND-1\$PA)**.** *Let* $\mathsf{SKE} = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ *denote a symmetric encryption scheme. If* SKE *is* $\epsilon_{\mathsf{SKE}}^{\mathsf{ind\text{-}cpa}}$-IND-CPA *secure, then* SKE *is* $\epsilon_{\mathsf{SKE}}^{\mathsf{ind\text{-}1\$pa}}$-IND-1\$PA *secure such that* $\epsilon_{\mathsf{SKE}}^{\mathsf{ind\text{-}1\$pa}} \leq \epsilon_{\mathsf{SKE}}^{\mathsf{ind\text{-}cpa}}$.

Theorem 6 (IND-1\$PA $\implies$ IND-1\$PA-LPC)**.** *Let* $\mathsf{SKE} = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ *denote* CBC_0 *or* CBC_R*. If* SKE *is* $\epsilon_{\mathsf{SKE}}^{\mathsf{ind\text{-}1\$pa}}$-IND-1\$PA *secure and the underlying function* $\mathsf{F} : \{0,1\}^{f_1(\lambda)} \times \{0,1\}^{f_2(\lambda)} \to \{0,1\}^{f_2(\lambda)}$ *is* $\epsilon_{\mathsf{F}}^{\mathsf{prp}}$-prp *secure, then* SKE *is* $\epsilon_{\mathsf{SKE}}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}$-IND-1\$PA-LPC *secure such that*

$$\epsilon_{\mathsf{SKE}}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}} \leq 2\epsilon_{\mathsf{F}}^{\mathsf{prp}} + q_{\text{LPC}} 2^{-f_2(\lambda)} + q_{\text{RAND}} \lceil \frac{l_{\mathsf{max}}}{f_2(\lambda)} \rceil 2^{-f_2(\lambda)} + \epsilon_{\mathsf{SKE}}^{\mathsf{ind\text{-}1\$pa}}$$

where $q_{\mathcal{O}}$ *denotes the maximal number of queries to* $\mathcal{O} \in \{\text{RAND}, \text{LPC}\}$ *oracles and* $l_{\max}$ *denotes the maximal input to the* RAND *oracle.*

Appendix C
Detailed Description of WebAuthn 2

In Figure 11, the security parameter $\lambda = 128$. For each server S, the associated identifier id_S is its effective domain. The official supported signature algorithms are RSASSA–PKCS1–v1_5 and RSASSA–PSS. As discussed in Section IV-D, the list of signature schemes can be extended by PQ compatible hybrid signature scheme. The underlying hash function H is SHA-256. We assume that each token has a unique user and can be registered at most once per server. The $\mathsf{Register} = (\mathsf{rChall}, \mathsf{rCom}, \mathsf{rRsp}, \mathsf{rVrfy})$ sub-protocol is executed as follows.

- $\mathsf{rChall}(\pi_S^i, \mathsf{tb}, UV)$: The server S samples a random challenge nonce $\pi_S^i.\mathsf{ch}$ and a user identifier $\pi_S^i.\mathsf{uid}$ and initializes the token biding state $\pi_S^i.\mathsf{tb}$ and user verification condition $\pi_S^i.UV$. Finally, S sets $\pi_S^i.\mathsf{st}_{\mathsf{exe}}$ to running and outputs a challenge message, see Line 3.
- $\mathsf{rCom}(\mathsf{id}_S, m_{\mathsf{rch}}, \mathsf{tb})$: The client parses m_{rch} into a server identifier id, a challenge nonce ch, a user identifier uid, a supported signature list pkCP and a user verification condition UV. Next, the client aborts if $\mathsf{id} \neq \mathsf{id}_S$. Otherwise, the client sets the user presence condition UP to true and computes the hash h of client message m_{rcl}, which is defined in Line 8. Finally, the client outputs the client and command messages m_{rcl} and m_{rcom}, respectively, see Line 10.
- $\mathsf{rRsp}(\pi_T^j, m_{\mathsf{rcom}})$: The token T first parses m_{rcom} into a server identifier id, a user identifier uid, a hash value h, a signature list pkCP, and the user presence and user verification conditions UP and UV, respectively. Next, T picks one supported signature scheme Σ in pkCP with the highest preference, i.e., with the smallest index possible. Afterwards, T checks whether it can support the required user verification condition UV. If either step fails, the token aborts. Otherwise, T generates a public-private key pair using the key generation algorithm of Σ, initializes the counter n to 0, samples a random credential identifier cid, and sets its execution state to accepted. Finally, T extends the registration context as in Line 20, and outputs it together with a response message m_{rrsp}, as defined in Line 18. The agreed content includes the server identifier id, the hash value h, the credential identifier cid, the counter n, the list pkCP, the public key pk, the signature scheme Σ, and the user presence UP and verification UV conditions. The session identifier is the tuple of the hash of server identifier id, the credential identifier cid, and the counter n.
- $\mathsf{rVrfy}(\pi_S^i, m_{\mathsf{rcl}}, m_{\mathsf{rrsp}})$: The server S parses the client message m_{rcl} and the response message m_{rrsp} and executes a few checks as in Line 26. It outputs abort and decision $d = 0$ if any check fails. Otherwise, S sets the execution state to accepted. Finally, S extends the registration context as in Line 28 and outputs it together with decision $d = 1$. The agreed content and the session identifier are defined as the ones in the rRsp algorithm.

$\mathsf{Authenticate} = (\mathsf{aChall}, \mathsf{aCom}, \mathsf{aRsp}, \mathsf{aVrfy})$ is defined next.

- $\mathsf{aChall}(\pi_S^i, \mathsf{tb}, UV)$: The server S samples a random challenge nonce $\pi_S^i.\mathsf{ch}$ and initializes its token binding state $\pi_S^i.\mathsf{tb}$ and user condition $\pi_S^i.UV$. Finally, S sets π_S^i to running and outputs a challenge message, see Line 34.
- $\mathsf{aCom}(\mathsf{id}_S, m_{\mathsf{ach}}, \mathsf{tb})$: The client parses m_{ach} into an identifier id, a challenge nonce ch, and user verification condition UV. Next, the client aborts if $\mathsf{id} \neq \mathsf{id}_S$. Otherwise, the client sets the user presence condition UP to true and compute the hash h of the client message m_{acl}, which is defined in Line 39. Finally, the client outputs the client message m_{acl} and command message m_{acom}, see Line 41.
- $\mathsf{aRsp}(\pi_T^j, \mathsf{rc}_T, m_{\mathsf{acom}})$: The token T first parses the command message m_{acom} into a server identifier id, a hash value h, and user presence and user verification conditions UP and UV. Next, T checks whether the corresponding registration context exists and whether it can satisfy the user verification requirement. T aborts if either of the above steps fails. Then, T increments the counter $\mathsf{rc}_T[\mathsf{id}].n$ by 1 and defines the associated data ad that includes the hash of id, the counter $\mathsf{rc}_T[\mathsf{id}].n$, and the conditions UP and UV, followed by computing a signature σ on ad and h using the signing key $\mathsf{rc}_T[\mathsf{id}].sk$. Finally, T sets its execution state to accepted and outputs the response message m_{arsp} defined in Line 49

```
Register
$\underline{\mathsf{rChall}(\pi_S^i, \mathsf{tb}, UV)}$: // 1. Server
1   $\pi_S^i.\mathsf{ch} \xleftarrow{\$} \{0,1\}^{\geq\lambda}$, $\pi_S^i.\mathsf{tb} \leftarrow \mathsf{tb}$, $\pi_S^i.UV \leftarrow UV$
2   $\pi_S^i.\mathsf{uid} \xleftarrow{\$} \{0,1\}^{\leq 4\lambda}$
3   $m_{\mathsf{rch}} \leftarrow (\mathsf{id}_S, \pi_S^i.\mathsf{ch}, \pi_S^i.\mathsf{uid}, \pi_S^i.\mathsf{pkCP}, \pi_S^i.UV)$
4   $\pi_S^i.\mathsf{st}_{\mathsf{exe}} \leftarrow \mathsf{running}$
5   $\textbf{return } m_{\mathsf{rch}}$
$\underline{\mathsf{rCom}(\mathsf{id}_S, m_{\mathsf{rch}}, \mathsf{tb})}$: // 2. Client
6   $(\mathsf{id}, \mathsf{ch}, \mathsf{uid}, \mathsf{pkCP}, UV) \leftarrow m_{\mathsf{rch}}$
7   $\textbf{if } \mathsf{id} \neq \mathsf{id}_S\textbf{: return } \perp$
8   $m_{\mathsf{rcl}} \leftarrow (\mathsf{ch}, \mathsf{tb})$
9   $UP \leftarrow \mathsf{true}$, $h \leftarrow \mathsf{H}(m_{\mathsf{rcl}})$
10  $m_{\mathsf{rcom}} \leftarrow (\mathsf{id}, \mathsf{uid}, h, \mathsf{pkCP}, UP, UV)$
11  $\textbf{return } (m_{\mathsf{rcom}}, m_{\mathsf{rcl}})$
$\underline{\mathsf{rRsp}(\pi_T^j, m_{\mathsf{rcom}})}$: // 3. Token
12  $(\mathsf{id}, \mathsf{uid}, h, \mathsf{pkCP}, UP, UV) \leftarrow m_{\mathsf{rcom}}$
13  $\textbf{if}$ at least one algorithm in $\mathsf{pkCP}$ is supported
14      $\Sigma \leftarrow \mathsf{pkCP}[i]$ with smallest $i$ possible
15  $\textbf{else return } (\perp, \perp)$
16  $\textbf{if } \pi_T^j.\mathsf{suppUV} = \mathsf{false} \textbf{ and } UV = \mathsf{true}\textbf{: return } (\perp, \perp)$
17  $(pk, sk) \xleftarrow{\$} \Sigma.\mathsf{KG}(1^\lambda)$, $\mathsf{cid} \xleftarrow{\$} \{0,1\}^{\geq\lambda}$, $n \leftarrow 0$
18  $m_{\mathsf{rrsp}} \leftarrow (\mathsf{H}(\mathsf{id}), n, \mathsf{cid}, pk, \Sigma, UP, UV)$
19  $\boxed{\mathsf{h}_{\mathsf{CP}} \leftarrow \mathsf{H}(\mathsf{pkCP})}$
20  $\mathsf{rc}_T[\mathsf{id}] \leftarrow (\mathsf{uid}, \mathsf{cid}, sk, n, \Sigma, \boxed{\mathsf{h}_{\mathsf{CP}}})$
21  $\pi_T^j.\mathsf{agCon} \leftarrow (\mathsf{id}, h, \mathsf{cid}, n, \mathsf{pkCP}, pk, \Sigma, UV, UP)$
22  $\pi_T^j.\mathsf{sid} \leftarrow (\mathsf{H}(\mathsf{id}), \mathsf{cid}, n)$
23  $\pi_T^j.\mathsf{st}_{\mathsf{exe}} \leftarrow \mathsf{accepted}$
24  $\textbf{return } (m_{\mathsf{rrsp}}, \mathsf{rc}_T)$
$\underline{\mathsf{rVrfy}(\pi_S^i, m_{\mathsf{rcl}}, m_{\mathsf{rrsp}})}$: // 4. Server
25  $(\mathsf{ch}, \mathsf{tb}) \leftarrow m_{\mathsf{rcl}}$, $(h, n, \mathsf{cid}, pk, \Sigma, UP, UV) \leftarrow m_{\mathsf{rrsp}}$
26  $\textbf{if } h \neq \mathsf{H}(\mathsf{id}_S) \textbf{ or } n \neq 0 \textbf{ or } \mathsf{ch} \neq \pi_S^i.\mathsf{ch} \textbf{ or } \mathsf{tb} \neq \pi_S^i.\mathsf{tb} \textbf{ or } \Sigma \notin \pi_S^i.\mathsf{pkCP}$
    $\textbf{or } UP \neq \mathsf{true} \textbf{ or } UV \neq \pi_S^i.UV\textbf{: return } (\perp, 0)$
27  $\boxed{\mathsf{h}_{\mathsf{CP}} \leftarrow \mathsf{H}(\pi_S^i.\mathsf{pkCP})}$
28  $\mathsf{rc}_S[\mathsf{cid}] \leftarrow (\pi_S^i.\mathsf{uid}, pk, n, \Sigma, \boxed{\mathsf{h}_{\mathsf{CP}}})$
29  $\pi_S^i.\mathsf{agCon} \leftarrow (\mathsf{id}_S, \mathsf{H}(m_{\mathsf{rcl}}), \mathsf{cid}, n, \pi_S^i.\mathsf{pkCP}, pk, \Sigma, UV, UP)$
30  $\pi_S^i.\mathsf{sid} \leftarrow (\mathsf{H}(\mathsf{id}), \mathsf{cid}, n)$
31  $\pi_S^i.\mathsf{st}_{\mathsf{exe}} \leftarrow \mathsf{accepted}$
32  $\textbf{return } (\mathsf{rc}_S, 1)$
```

```
Authenticate
$\underline{\mathsf{aChall}(\pi_S^i, \mathsf{tb}, UV)}$: // 1. Server
33  $\pi_S^i.\mathsf{ch} \xleftarrow{\$} \{0,1\}^{\geq\lambda}$, $\pi_S^i.\mathsf{tb} \leftarrow \mathsf{tb}$, $\pi_S^i.UV \leftarrow UV$
34  $m_{\mathsf{ach}} \leftarrow (\mathsf{id}_S, \pi_S^i.\mathsf{ch}, \pi_S^i.UP, \pi_S^i.UV)$
35  $\pi_S^i.\mathsf{st}_{\mathsf{exe}} \leftarrow \mathsf{running}$
36  $\textbf{return } m_{\mathsf{ach}}$
$\underline{\mathsf{aCom}(\mathsf{id}_S, m_{\mathsf{ach}}, \mathsf{tb})}$: // 2. Client
37  $(\mathsf{id}, \mathsf{ch}, UV) \leftarrow m_{\mathsf{ach}}$
38  $\textbf{if } \mathsf{id} \neq \mathsf{id}_S\textbf{: return } \perp$
39  $m_{\mathsf{acl}} \leftarrow (\mathsf{ch}, \mathsf{tb})$
40  $UP \leftarrow \mathsf{true}$, $h \leftarrow \mathsf{H}(m_{\mathsf{acl}})$
41  $m_{\mathsf{acom}} \leftarrow (\mathsf{id}, h, UP, UV)$
42  $\textbf{return } (m_{\mathsf{acom}}, m_{\mathsf{acl}})$
$\underline{\mathsf{aRsp}(\pi_T^j, \mathsf{rc}_T, m_{\mathsf{acom}})}$: // 3. Token
43  $(\mathsf{id}, h, UP, UV) \leftarrow m_{\mathsf{acom}}$
44  $\textbf{if } \mathsf{rc}_T[\mathsf{id}] = \perp\textbf{: return } (\perp, \mathsf{rc}_T)$
45  $\textbf{if } \pi_T^j.\mathsf{suppUV} = \mathsf{false} \textbf{ and } UV = \mathsf{true}\textbf{: return } (\perp, \mathsf{rc}_T)$
46  $\mathsf{rc}_T[\mathsf{id}].n \leftarrow \mathsf{rc}_T[\mathsf{id}].n + 1$
47  $ad \leftarrow (\mathsf{H}(\mathsf{id}), \mathsf{rc}_T[\mathsf{id}].n, UP, UV)$
48  $\sigma \xleftarrow{\$} \mathsf{rc}_T[\mathsf{id}].\Sigma.\mathsf{Sign}(\mathsf{rc}_T[\mathsf{id}].sk, (ad, h))$
49  $m_{\mathsf{arsp}} \leftarrow (\mathsf{rc}_T[\mathsf{id}].\mathsf{cid}, ad, \boxed{\mathsf{rc}_T[\mathsf{id}].\mathsf{h}_{\mathsf{CP}},}\ \sigma, \mathsf{rc}_T[\mathsf{id}].\mathsf{uid})$
50  $\pi_T^j.\mathsf{agCon} \leftarrow (\mathsf{id}, h, \mathsf{rc}_T[\mathsf{id}].n, \boxed{\mathsf{rc}_T[\mathsf{id}].\mathsf{h}_{\mathsf{CP}},}\ UV, UP)$
51  $\pi_T^j.\mathsf{sid} \leftarrow (\mathsf{H}(\mathsf{id}), \mathsf{rc}_T[\mathsf{id}].\mathsf{cid}, h, n)$
52  $\pi_T^j.\mathsf{st}_{\mathsf{exe}} \leftarrow \mathsf{accepted}$
53  $\textbf{return } (m_{\mathsf{arsp}}, \mathsf{rc}_T)$
$\underline{\mathsf{aVrfy}(\pi_S^i, \mathsf{rc}_S, m_{\mathsf{acl}}, m_{\mathsf{arsp}})}$: // 4. Server
54  $(\mathsf{ch}, \mathsf{tb}) \leftarrow m_{\mathsf{acl}}$, $(\mathsf{cid}, ad, \boxed{\mathsf{h}_{\mathsf{CP}},}\ \sigma, \mathsf{uid}) \leftarrow m_{\mathsf{arsp}}$
55  $(h, n, UP, UV) \leftarrow ad$
56  $\textbf{if } \mathsf{rc}_S[\mathsf{cid}] = \perp\textbf{: return } (\mathsf{rc}_S, 0)$
57  $\boxed{\textbf{if } \mathsf{h}_{\mathsf{CP}} \neq \mathsf{rc}_S[\mathsf{cid}].\mathsf{h}_{\mathsf{CP}}\text{: } \mathsf{rc}_S[\mathsf{cid}] \leftarrow \perp \textbf{ and return } (\mathsf{rc}_S, 0)}$
58  $\textbf{if } \pi_S^i.\mathsf{ch} \neq \mathsf{ch} \textbf{ or } \pi_S^i.\mathsf{tb} \neq \mathsf{tb} \textbf{ or } h \neq \mathsf{H}(\mathsf{id}_S) \textbf{ or } UP \neq \mathsf{true} \textbf{ or } UV \neq \pi_S^i.UV$
    $\textbf{or } \mathsf{rc}_S[\mathsf{cid}].\Sigma.\mathsf{Vfy}(\mathsf{rc}_S[\mathsf{cid}].pk, (ad, \mathsf{H}(m_{\mathsf{acl}})), \sigma) = 0 \textbf{ or } n \leq \mathsf{rc}_S[\mathsf{cid}].n$:
    $\textbf{return } (\mathsf{rc}_S, 0)$
59  $\mathsf{rc}_S[\mathsf{cid}].n \leftarrow n$
60  $\pi_S^i.\mathsf{agCon} \leftarrow (\mathsf{id}_S, \mathsf{H}(m_{\mathsf{acl}}), n, \boxed{\mathsf{h}_{\mathsf{CP}},}\ UV, UP)$
61  $\pi_S^i.\mathsf{sid} \leftarrow (h, \mathsf{cid}, \mathsf{H}(m_{\mathsf{acl}}), n)$
62  $\pi_S^i.\mathsf{st}_{\mathsf{exe}} \leftarrow \mathsf{accepted}$
63  $\textbf{return } (\mathsf{rc}_S, 1)$
```

Fig. 11. Instantiation of $\mathsf{ePIA} = (\mathsf{Register}, \mathsf{Authenticate})$ with WebAuthn 2 (and WebAuthn 2^+ that includes boxed operations) with attestation type `None`, where $\mathsf{Register} = (\mathsf{rChall}, \mathsf{rCom}, \mathsf{rRsp}, \mathsf{rVrfy})$ and $\mathsf{Authenticate} = (\mathsf{aChall}, \mathsf{aCom}, \mathsf{aRsp}, \mathsf{aVrfy})$.

along with rc_T. The agreed context is defined as the tuple of the server identifier id, the value h, the counter $\mathsf{rc}_T[\mathsf{id}].n$, and the user conditions UV and UP. The session identifier is defined as the tuple of the hash of the server identifier id, the credential identifier $\mathsf{rc}_T[\mathsf{id}].\mathsf{cid}$, the hash value h, and the counter n.

- $\mathsf{aVrfy}(\pi_S^i, \mathsf{rc}_S, m_{\mathsf{acl}}, m_{\mathsf{arsp}})$: The server S parses the client message m_{acl} and the response message m_{arsp} and executes checks as in Line 58 if the corresponding registration context exists. It aborts and produces decision $d = 0$ if any check fails. Otherwise, S updates the counter in the registration context and sets the execution state to accepted and outputs rc_S together with decision $d = 1$. The agreed context and the session identifier are the same as in aRsp.

Appendix D
Detailed Description of CTAP 2.1

A. Description of CTAP 2.1 Algorithms

authPowerUp-T: inputs a token state st_T and resets each underlying Pin/Uv Auth Protocol puvProtocol. The counter m for the consecutive tries for binding phase is set to its maximum of 3.

getInfo-T: inputs a token session π_T^i and outputs its version and the list of the supported Pin/Uv Auth Protocol. We write $\mathsf{info} \leftarrow \mathsf{getInfo}\text{-}T(\pi_T^i)$.

obtainSharedSecret-C-start: inputs a client session π_C^j and token information $\mathsf{info} = (\mathsf{version}, \mathsf{puvProtocolList})$ and aborts if version $= 2.0$. Otherwise, the client session π_C^j selects a Pin/Uv Auth Protocol puvProtocol from the list puvProtocolList and initializes it locally. The execution state of π_C^j is set to waiting. Finally, this algorithm outputs the selected Pin/Uv Auth Protocol puvProtocol. We write $\mathsf{puvProtocol} \xleftarrow{\$} \mathsf{obtainSharedSecret}\text{-}C\text{-}\mathsf{start}(\pi_C^j, \mathsf{info})$.

obtainSharedSecret-T: inputs a token session π_T^i and a Pin/Uv Auth Protocol puvProtocol aborts if puvProtocol is not supported by the token T. Otherwise, this algorithm simply outputs the public key of the local instance of puvProtocol. During the execution, the status of the token session is set to waiting. We write $pk \leftarrow \mathsf{obtainSharedSecret}\text{-}T(\pi_T^i, \mathsf{puvProtocol})$.

```
authPowerUp-$T(\mathsf{st}_T)$:
  foreach puvProtocol $\in \mathsf{st}_T$.puvProtocolList
    $\mathsf{st}_T$.puvProtocol.initialize()
  $\mathsf{st}_T.m \leftarrow 3$
obtainSharedSecret-$C$-start$(\pi_C^j, \mathsf{info})$:
  Parse (version, puvProtocolList) $\leftarrow$ info
  if version $= 2.0$: return $\perp$
  select puvProtocol $\leftarrow$ puvProtocolList
  $\pi_C^j$.selectedpuvProtocol $\leftarrow$ puvProtocol
  $\pi_C^j$.selectedpuvProtocol.initialize()
  $\pi_C^j.\mathsf{st}_{\mathsf{exe}} \leftarrow$ waiting
  $\pi_C^j.\mathsf{sid} \leftarrow \pi_C^j.\mathsf{sid} \parallel \mathsf{info} \parallel \mathsf{puvProtocol}$
  return puvProtocol
obtainSharedSecret-$T(\pi_T^i, \mathsf{puvProtocol})$ :
  if puvProtocol $\notin \mathsf{st}_T$.puvProtocolList: return $\perp$
  $pk_T \leftarrow \mathsf{st}_T$.puvProtocol.getPublicKey()
  $\pi_T^i.\mathsf{st}_{\mathsf{exe}} \leftarrow$ waiting
  $\pi_T^i.\mathsf{sid} \leftarrow \pi_T^i.\mathsf{sid} \parallel \mathsf{puvProtocol} \parallel pk_T$
  return $pk_T$
obtainSharedSecret-$C$-end$(\pi_C^j, pk)$ :
  $(c, K) \xleftarrow{\$} \pi_C^j$.selectedpuvProtocol.encapsulate$(pk)$
  $\pi_C^j.\mathsf{K} \leftarrow K$
  $\pi_C^j.\mathsf{sid} \leftarrow \pi_C^j.\mathsf{sid} \parallel pk \parallel c$
  return $c$
setPIN-$C(\pi_C^j, \mathsf{pin})$ :
  if pin $\notin \mathcal{PIN}$: return $\perp$
  $c_p \xleftarrow{\$} \pi_C^j$.selectedpuvProtocol.encrypt$(\pi_C^j.\mathsf{K}, \mathsf{pin})$
  $t_p \xleftarrow{\$} \pi_C^j$.selectedpuvProtocol.authenticate$(\pi_C^j.\mathsf{K}, c_p)$
  return $(c_p, t_p)$
setPIN-$T(\pi_T^i, \mathsf{puvProtocol}, c, c_p, t_p)$:
  if puvProtocol $\notin \mathsf{st}_T$.puvProtocolList $\vee$ $\mathsf{st}_T$.pinHash $\neq \perp$: return $\perp$
  $K \leftarrow \mathsf{st}_T$.puvProtocol.decapsulate$(c)$
  if $K = \perp \vee \mathsf{st}_T$.puvProtocol.verify$(K, c_p, t_p)$ = false: return $\perp$
  pin $\leftarrow \mathsf{st}_T$.puvProtocol.decrypt$(K, c_p)$
  if pin $\notin \mathcal{PIN}$: return $\perp$
  $\mathsf{st}_T$.pinHash $\leftarrow$ H(pin)
  $\mathsf{st}_T$.pinRetries $\leftarrow$ pinRetriesMax
  return accepted
getInfo-$T(\pi_T^i)$:
  info $\leftarrow$ ($\mathsf{st}_T$.version, $\mathsf{st}_T$.puvProtocolList)
  $\pi_T^i.\mathsf{sid} \leftarrow \pi_T^i.\mathsf{sid} \parallel \mathsf{info}$
  return info
obtainPinUvAuthToken-$C$-start$(\pi_C^j, \mathsf{pin})$:
  pinHash $\leftarrow$ H(pin)
  $c_{ph} \xleftarrow{\$} \pi_C^j$.selectedpuvProtocol.encrypt$(\pi_C^j.\mathsf{K}, \mathsf{pinHash})$
  $\pi_C^j.\mathsf{st}_{\mathsf{exe}} \leftarrow$ bindStart
  $\pi_C^j.\mathsf{sid} \leftarrow \pi_C^j.\mathsf{sid} \parallel c_{ph}$
  return $c_{ph}$
obtainPinUvAuthToken-$T(\pi_T^i, \mathsf{puvProtocol}, c, c_{ph})$:
  if puvProtocol $\notin \mathsf{st}_T$.puvProtocolList $\vee$ $\mathsf{st}_T$.pinRetries $= 0$
    return $(\perp, \mathsf{false})$
  $K \leftarrow \mathsf{st}_T$.puvProtocol.decapsulate$(c)$
  if $K = \perp$: return $(\perp, \mathsf{false})$
  $\mathsf{st}_T$.pinRetries $\leftarrow \mathsf{st}_T$.pinRetries $- 1$
  pinHash $\leftarrow \mathsf{st}_T$.puvProtocol.decrypt$(K, c_{ph})$
  if pinHash $\neq \mathsf{st}_T$.pinHash
    $\mathsf{st}_T$.puvProtocol.regenerate()
    if $\mathsf{st}_T.m = 0$: authPowerUp-$T(\mathsf{st}_T)$: return $(\perp, \mathsf{true})$
  $\mathsf{st}_T.m \leftarrow 3$, $\mathsf{st}_T$.pinRetries $\leftarrow$ pinRetriesMax
  foreach puvProtocol$'$ $\in \mathsf{st}_T$.puvProtocolList
    $\mathsf{st}_T$.puvProtocol$'$.resetpuvToken()
  $\pi_T^i.\mathsf{bs} \leftarrow \pi_T^i$.puvProtocol.$pt$
  $c_{pt} \xleftarrow{\$} \mathsf{st}_T$.puvProtocol.encrypt$(K, \pi_T^i.\mathsf{bs})$
  $\pi_T^i.\mathsf{st}_{\mathsf{exe}} \leftarrow$ bindDone
  $\pi_T^i.\mathsf{sid} \leftarrow \pi_T^i.\mathsf{sid} \parallel \mathsf{puvProtocol} \parallel c \parallel c_{ph} \parallel c_{pt} \parallel \mathsf{false}$
  return $(c_{pt}, \mathsf{false})$
obtainPinUvAuthToken-$C$-end$(\pi_C^j, c_{pt})$:
  $\pi_C^j.\mathsf{bs} \leftarrow \pi_C^j$.selectedpuvProtocol.decrypt$(\pi_C^j.\mathsf{K}, c_{pt})$
  $\pi_C^j.\mathsf{st}_{\mathsf{exe}} \leftarrow$ bindDone
  $\pi_C^j.\mathsf{sid} \leftarrow \pi_C^j.\mathsf{sid} \parallel c$
  return
auth-$C(\pi_C^j, M)$:
  $t \xleftarrow{\$} \pi_C^j$.selectedpuvProtocol.authenticate$(\pi_C^j.\mathsf{bs}, M)$
  return $(M, t)$
validate-$T(\pi_T^i, M, t, d)$:
  if $\mathsf{st}_T$.puvProtocol.verify$(\pi_T^i.\mathsf{bs}, M, t)$ = true: return $d$
  return rejected
```

Fig. 12. CTAP 2.1 is an ePACA = (Reboot, Setup, Bind, Auth, Validate) protocol. The flow of ePACA protocol is given in Figure 4.

obtainSharedSecret-C-end: inputs a client session π_C^j and a public key pk. During the execution, the client session produces a shared secret K and a ciphertext c, followed by storing the secret K locally in π_C^j.K. This algorithm outputs the ciphertext c. We write $c \xleftarrow{\$}$ obtainSharedSecret-C-end(π_C^j, pk).

setPIN-C: inputs a client session π_C^j and a PIN pin and aborts if pin is not in the PIN domain $\mathcal{PIN}$. Otherwise, π_C^j encrypts this pin and authenticates the encryption using the selected Pin/Uv Auth Protocol and the locally stored shared secret π_C^j.K. This algorithm outputs the ciphertext c and the authentication tag t. We write $(c, t) \xleftarrow{\$}$ setPIN-$C(\pi_C^j, \mathsf{pin})$.

setPIN-T: inputs a token session π_T^i, a Pin/Uv Auth Protocol puvProtocol, two ciphertexts c and c_p, and an authentication tag t_p. It aborts if puvProtocol is not supported or the local pinHash has been set. Then, the token decapsulates c for a shared secret K and verifies the ciphertext c_p and tag t using K. If K cannot be correctly decapsulated or the verification falls, then this algorithm aborts. If a PIN pin can be correctly decrypted, then the local pinHash π_T^i.pinHash is set to hash of pin and the local counter pinRetries is set to the maximum. Otherwise, this algorithm aborts. In the end, this algorithm outputs a status status $\in$ {accepted, rejected} indicating success or failure. [9] We write status $\leftarrow$ setPIN-$T(\pi_T^i, \mathsf{puvProtocol}, c, c_p, t_p)$.

obtainPinUvAuthToken-C-start: inputs a client session π_C^j and a PIN pin. The client session π_C^j computes the hash of pin and encrypts it using the selected Pin/Uv Auth Protocol and the locally stored share secret π_C^j.K. This algorithm outputs the encryption c. During the execution, the status of the client session is set to bindStart. We write $c \xleftarrow{\$}$ obtainPinUvAuthToken-C-start(π_C^j, pin).

obtainPinUvAuthToken-T: inputs a token session π_T^i, a Pin/Uv Auth Protocol puvProtocol, and two ciphertexts c and c_{ph}. It aborts if puvProtocol is not supported by T or if the local counter pinRetries is 0. Otherwise, session π_T^i decapsulates c for a key K and aborts if a failure happens during the decapsulation. Then, π_T^i decrements the counter pinRetries by 1 and decrypts c_ph using K for a hash value pinHash. If pinHash matches the locally stored st_T.pinHash, then the counter m and pinRetries is set to their maximum. Otherwise, the local instance puvProtocol

[9]In practice, the user confirmation is required in this step. Here, we simply assume the user confirmation and omit it in the algorithm.

regenerates its key pair. If the counter for the consecutive retries reaches 0, then the token is rebooted. In all cases, the token resets the pts in all Pin/Uv Auth Protocol instances. Then, the session π_T^i sets the pt underlying puvProtocol as the binding state π_T^i.bs and encrypts it using K for a ciphertext c_{pt}. This algorithm outputs c_{pt} and a boolean value calledReboot indicating whether authPowerUp-T is invoked or not. After the successful completion, the status of the token session is set to bindDone. We write $(c_{pt}, \mathsf{calledReboot}) \xleftarrow{\$} \mathsf{obtainPinUvAuthToken}\text{-}T(\pi_T^i, \mathsf{puvProtocol}, c, c_{ph})$.

obtainPinUvAuthToken-C-end: inputs a client session π_C^j and a ciphertext c_{pt}. During the execution, the client decrypts the binding state π_C^j.bs from c_{pt} and the status of the client session is set to bindDone.

auth-C: inputs a client session π_C^j and a command M. The client session authenticates M using the selected Pin/Uv Auth Protocol and the local binding state for a tag t. This algorithm then outputs M and an authorized tag t[10]. We write $(M, t) \xleftarrow{\$} \mathsf{auth}\text{-}C(\pi_C^j, M)$.

validate-T: inputs a token session π_T^i, a command M, an authorized tag t, and a user decision $d \in \{\mathsf{accepted}, \mathsf{rejected}\}$, and outputs status status $=$ accepted if $d =$ accepted and M and t can be verified using the binding state π_T^i.bs and the Pin/Uv Auth Protocol, which is specified by the tag t (Cf. footnote 10); and rejected otherwise.

B. *Official Instances of Pin/Uv Auth Protocol*

CTAP 2.1 officially introduces two instantiations of Pin/Uv Auth Protocol puvProtocol, as in Fig. 13 and 14. The first, $\mathsf{puvProtocol}_1$, runs $\mathsf{initialize}_1$ by simply invoking $\mathsf{regenerate}_1$ and $\mathsf{resetpuvToken}_1$, which further samples a public-private key pair from ECDH over curve NIST P-256 and samples a random pt with length $\mu\lambda$ for $\mu \in \{1, 2\}$ and $\lambda = 128$ bits. $\mathsf{getPublicKey}_1$ outputs the internal public key pk. $\mathsf{encapsulate}_1$ computes the key exchange using as input ECDH public key and its internal private key and applies $\mathsf{H}_1 = $ SHA-256 to the x-coordinate of the key exchange result for a shared K, followed by outputting its internal public key and K. $\mathsf{decapsulate}_1$ recovers the shared secret K from ciphertext c using its internal private key sk. $\mathsf{encrypt}_1$ encrypts a message m using SKE_1 and a symmetric key K, where SKE_1 denotes AES-256-CBC encryption using an all-zero initial vector IV. $\mathsf{decrypt}_1$ recovers the message from ciphertext c by using SKE_1 and key K. $\mathsf{authenticate}_1$ authenticates a message m using K' by applying H_2 to both, where H_2 runs HMAC-SHA-256 and truncates the result to the first 128 bits. verify_1 outputs true if $t = \mathsf{H}_2(K', m)$, and false otherwise[11].

The second instantiation $\mathsf{puvProtocol}_2$ runs $\mathsf{initialize}_2$, $\mathsf{regenerate}_2$, and $\mathsf{getPublicKey}_2$ identical to the ones in $\mathsf{puvProtocol}_1$. The $\mathsf{resetpuvToken}_2$ algorithm outputs a pt with fixed 256 bits length. The algorithm $\mathsf{encapsulate}_2$ first

```
initialize_1():
    regenerate_1()
    resetpuvToken_1()
regenerate_1():
    $(pk, sk) \xleftarrow{\$}$ ECDH.KG()
resetpuvToken_1():
    $pt \xleftarrow{\$} \{0,1\}^{\mu\lambda}$
encapsulate_1(pk'):
    $Z \leftarrow$ XCoordinateOf$(sk \cdot pk')$
    $K \leftarrow \mathsf{H}_1(Z)$ , $c \leftarrow pk$
    return $(c, K)$
decapsulate_1(c):
    $Z \leftarrow$ XCoordinateOf$(sk \cdot c)$
    $K \leftarrow \mathsf{H}_1(Z)$
    return $K$
getPublicKey_1():
    return $pk$
encrypt_1(K, m):
    $c \leftarrow \mathsf{SKE}_1.\mathsf{Enc}(K, m)$
    return $c$
decrypt_1(K, c):
    $m \leftarrow \mathsf{SKE}_1.\mathsf{Dec}(K, c)$
    return $m$
authenticate_1(K', m):
    $t \leftarrow \mathsf{H}_2(K', m)$
    return $t$
verify_1(K', m, t):
    $t' \leftarrow \mathsf{H}_2(K', m)$
    return $[\![t = t']\!]$
```

Fig. 13. The first instantiation of PIN/UV Auth Protocol $\mathsf{puvProtocol}_1$. The operation $\cdot$ denotes scalar multiplication.

```
initialize_2():
    regenerate_2()
    resetpuvToken_2()
regenerate_2():
    $(pk, sk) \xleftarrow{\$}$ ECDH.KG()
resetpuvToken_2():
    $pt \xleftarrow{\$} \{0,1\}^{2\lambda}$
encapsulate_2(pk'):
    $Z \leftarrow$ XCoordinateOf$(sk \cdot pk')$
    $K_1 \leftarrow \mathsf{H}_3(Z,$ "CTAP2 HMAC key"$)$
    $K_2 \leftarrow \mathsf{H}_3(Z,$ "CTAP2 AES key"$)$
    $K \leftarrow (K_1, K_2)$
    $c \leftarrow pk$
    return $(c, K)$
decapsulate_2(c):
    $Z \leftarrow$ XCoordinateOf$(sk \cdot c)$
    $K_1 \leftarrow \mathsf{H}_3(Z,$ "CTAP2 HMAC key"$)$
    $K_2 \leftarrow \mathsf{H}_3(Z,$ "CTAP2 AES key"$)$
    $K \leftarrow (K_1, K_2)$
    return $K$
getPublicKey_2():
    return $pk$
encrypt_2(K, m):
    Parse $(K_1, K_2) \leftarrow K$
        s.t. $|K_1| = 2\lambda$
    $c \leftarrow \mathsf{SKE}_2.\mathsf{Enc}(K_2, m)$
    return $c$
decrypt_2(K, c):
    Parse $(K_1, K_2) \leftarrow K$
        s.t. $|K_1| = 2\lambda$
    $m \leftarrow \mathsf{SKE}_2.\mathsf{Dec}(K_2, c)$
    return $m$
authenticate_2(K', m):
    Parse $(K_1', K_2') \leftarrow K'$
        s.t. $|K_1'| = 2\lambda$
    $t \leftarrow \mathsf{H}_4(K_1', m)$
    return $t$
verify_2(K', m, t):
    Parse $(K_1', K_2') \leftarrow K'$
        s.t. $|K_1'| = 2\lambda$
    $t' \leftarrow \mathsf{H}_4(K_1', m)$
    return $[\![t = t']\!]$
```

Fig. 14. The 2nd instantiation of PIN/UV Auth Protocol $\mathsf{puvProtocol}_2$.

computes the x coordinate of the ECDH exchange of input public key and internal private key, denoted by Z, followed by applying H_3 to Z and "CTAP2 HMAC key" for a HMAC key K_1 and to Z and "CTAP2 AES key" for a AES key K_2. Finally, $\mathsf{encapsulate}_2$ outputs its internal public key as ciphertext as well as K_1 and K_2. $\mathsf{decapsulate}_2$ recovers HMAC key K_1 and AES key K_2 from the input ciphertext c using its internal private key. $\mathsf{encrypt}_2$ splits the input K into two sub-keys K_1 and K_2 where K_1 has length of 256 bits. Then, it encrypts a message m using SKE_2 on key K_2, where SKE_2 denotes AES-256-CBC encryption using a randomized initial vector IV. $\mathsf{decrypt}_2$ recovers the message m from ciphertext c using the key K_2, where K_2 discards the first 256 bits of K. $\mathsf{authenticate}_2$ applies H_4 to key K_1' and a message m to produce a tag t, where H_4 denotes HMAC-SHA-256 and K_1' is the first 256 bits of the input K'. verify_2 on a key K', a message m, and a tag t, verifies whether the tag t matches $\mathsf{H}_4(K_1', m)$, where K_1' is the first 256 bits of K'.

[10]In practice, this authorized tag t also includes information that specifies the index of Pin/Uv Auth Protocol. Here, we omit this.

[11]In practice, if $K' = pt$, then verify_1 also outputs fails if pt is not in-use. Note that the usage time of the pt is out of the scope of this paper. We omit this here and in the following verify_2 in $\mathsf{puvProtocol}_2$.

Supplementary Materials

APPENDIX E
FULL PRELIMINARIES

Definition 7. *Let $\mathbb{G} = \langle g \rangle$ denotes a cyclic group of prime order q with generator g. We say the* computational Diffie-Hellman (CDH) *problem is $\epsilon^{\mathsf{CDH}}_{\mathbb{G},g}$ hard if for all* PPT *adversaries $\mathcal{A}$ it holds that*

$$\Pr[g^{ab} \leftarrow \mathcal{A}(\mathbb{G}, g, g^a, g^b) : a, b \xleftarrow{\$} \mathbb{Z}_q] \le \epsilon^{\mathsf{CDH}}_{\mathbb{G},g}$$

We say the strong CDH (sCDH) *problem is $\epsilon^{\mathsf{sCDH}}_{\mathbb{G},g}$ hard if for all* PPT *adversaries $\mathcal{A}$ the CDH problem is $\epsilon^{\mathsf{CDH}}_{\mathbb{G},g} = \epsilon^{\mathsf{sCDH}}_{\mathbb{G},g}$ hard even when $\mathcal{A}$ has access to an oracle $\mathcal{O}_a(\cdot,\cdot)$ that inputs $Y, Z \in \mathbb{G}$ and outputs whether $Y^a = Z$.*

Definition 8. *Let $\mathsf{H} : \mathcal{M} \to \mathcal{O}$ denote a function that maps from message space $\mathcal{M}$ to output space $\mathcal{O}$. We say H is ϵ-*collision resistant*, if for any efficiency adversaries $\mathcal{A}$ it holds that,*

$$\mathsf{Adv}^{\mathsf{coll\text{-}res}}_{\mathsf{H},\mathcal{A}} := \Pr[(m_1, m_2) \xleftarrow{\$} \mathcal{A}(1^\lambda) \text{ such that } m_1, m_2 \in \mathcal{M}, \\ m_1 \ne m_2, \mathsf{H}(m_1) = \mathsf{H}(m_2)] \le \epsilon$$

Definition 9. *Let $\mathsf{F} : \mathcal{K} \times \mathcal{M} \to \mathcal{O}$ be a function that maps a key $k \in \mathcal{K}$ and a message $m \in \mathcal{M}$ to an output $y \in \mathcal{O}$. We say F is ϵ-*prf *secure, if for any efficiency adversaries $\mathcal{A}$, any $k \xleftarrow{\$} \mathcal{K}$, and any truly random function $\mathsf{R} : \mathcal{M} \to \mathcal{O}$, it holds that,*

$$\mathsf{Adv}^{\mathsf{prf}}_{\mathsf{F},\mathcal{A}} := \left| \Pr[\mathcal{A}^{\mathsf{F}(k,\cdot)} = 1] - \Pr[\mathcal{A}^{\mathsf{R}(\cdot)} = 1] \right| \le \epsilon$$

Definition 10. *Let $\mathsf{F} : \mathcal{K} \times \mathcal{M} \to \mathcal{O}$ be a function that maps a key $k \in \mathcal{K}$ and a message $m \in \mathcal{M}$ to an output $y \in \mathcal{O}$. We say F is ϵ-*swap *secure, if the function $\bar{\mathsf{F}}$ defined below is ϵ-*prf *secure.*

$$\bar{\mathsf{F}} : \mathcal{M} \times \mathcal{K} \to \mathcal{O}, \bar{\mathsf{F}}(m, k) := \mathsf{F}(k, m)$$

Definition 11. *Let $\mathsf{F} : \mathcal{K} \times \mathcal{M} \to \mathcal{O}$ be a function that maps a key $k \in \mathcal{K}$ and a message $m \in \mathcal{M}$ to an output $y \in \mathcal{O}$. We say F is ϵ-*dual *secure, if F is both ϵ-*prf *and ϵ-*swap *secure.*

Definition 12. *Let $\mathsf{F} : \mathcal{K} \times \mathcal{M} \to \mathcal{O}$ be a function that maps a key $k \in \mathcal{K}$ and a message $m \in \mathcal{M}$ to an output $y \in \mathcal{O}$. We say F is ϵ-*prp *secure, if*

1) *for any $k \in \mathcal{K}$, F is bijective from $\mathcal{M}$ to $\mathcal{O}$, this indicates that $\mathcal{O} = \mathcal{M}$*
2) *for any $k \in \mathcal{K}$, $\mathsf{F}(k, m)$ can be evaluated in polynomial time for any $m \in \mathcal{M}$*
3) *for any $k \in \mathcal{K}$, the inversion $\mathsf{F}^{-1}(k, y)$ can be evaluated in polynomial time for any $y \in \mathcal{O}$*
4) *for any efficiency adversaries $\mathcal{A}$, any $k \xleftarrow{\$} \mathcal{K}$, and any truly random invertible permutation $f : \mathcal{M} \to \mathcal{O}$, it holds that*

$$\mathsf{Adv}^{\mathsf{prp}}_{\mathsf{F},\mathcal{A}} := \left| \Pr[\mathcal{A}^{\mathsf{F}(k,\cdot), \mathsf{F}^{-1}(k,\cdot)} = 1] - \Pr[\mathcal{A}^{f(\cdot), f^{-1}(\cdot)} = 1] \right| \le \epsilon$$

Definition 13. *A digital signature scheme over secret key space $\mathcal{SK}$, public key space $\mathcal{PK}$, and message space $\mathcal{M}$, is a tuple of algorithms $\mathsf{DS} = (\mathsf{KG}, \mathsf{Sign}, \mathsf{Vfy})$ as defined below.*

- ***Key Generation*** $(pk, sk) \xleftarrow{\$} \mathsf{KG}(1^\lambda)$*: takes as input the public parameter 1^λ and outputs a public-secret key pair $(pk, sk) \in \mathcal{PK} \times \mathcal{SK}$.*
- ***Signing*** $\sigma \xleftarrow{\$} \mathsf{Sign}(sk, m)$*: takes as input a secret key $sk \in \mathcal{SK}$ and a message $m \in \mathcal{M}$ and outputs a signature σ.*
- ***Verification*** $\mathsf{b} \leftarrow \mathsf{Vfy}(pk, m, \sigma)$*: takes as input a public key $pk \in \mathcal{PK}$, a message $m \in \mathcal{M}$, and a signature σ and outputs a bit $\{0, 1\} \in \{0, 1\}$.*

We say a DS is δ-correct if for every $(pk, sk) \xleftarrow{\$} \mathsf{KG}()$ and every message $m \in \mathcal{M}$, we have $\Pr[1 \ne \mathsf{Vfy}(pk, m, \mathsf{Sign}(sk, m))] \le \delta$. In particular, we call a DS *(perfectly) correct* if $\delta = 0$.

Definition 14. *Let $\mathsf{DS} = (\mathsf{KG}, \mathsf{Sign}, \mathsf{Vfy})$ be a digital signature scheme with message space $\mathcal{M}$. We say DS is ϵ-EUF-CMA secure, if the below defined advantage of every (potential quantum) adversary $\mathcal{A}$ against $\mathsf{Expt}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{DS}}$ experiment in Figure 15 is bounded by,*

$$\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{DS}}(\mathcal{A}) := \Pr[\mathsf{Expt}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{DS}}(\mathcal{A}) = 1] \le \epsilon$$

```
$\mathsf{Expt}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{DS}}(\mathcal{A})$:
    $\mathcal{L}_{\text{SIGN}} \leftarrow \emptyset$
    $(pk, sk) \xleftarrow{\$} \mathsf{KG}()$
    $(m^\star, \sigma^\star) \xleftarrow{\$} \mathcal{A}^{\text{SIGN}}(pk)$
    return $[\![\mathsf{Vfy}(pk, m^\star, \sigma^\star) \wedge m^\star \notin \mathcal{L}_{\text{SIGN}}]\!]$

$\text{SIGN}(m)$:
    if $m \notin \mathcal{M}$: return $\perp$
    $\sigma \xleftarrow{\$} \mathsf{Sign}(sk, m)$
    $\mathcal{L}_{\text{SIGN}} \leftarrow \mathcal{L}_{\text{SIGN}} \cup \{m\}$
    return $\sigma$
```

Fig. 15. EUF-CMA experiment for $\mathsf{DS} = (\mathsf{KG}, \mathsf{Sign}, \mathsf{Vfy})$ with message space $\mathcal{M}$.

Definition 15. *A key encapsulation mechanism scheme over secret key space $\mathcal{SK}$, public key space $\mathcal{PK}$, symmetric key space $\mathcal{K}$, and ciphertext space $\mathcal{CT}$, is a tuple of algorithms $\mathsf{KEM} = (\mathsf{KG}, \mathsf{Encaps}, \mathsf{Decaps})$ as defined below.*

- ***Key Generation*** $(pk, sk) \xleftarrow{\$} \mathsf{KG}(1^\lambda)$*: takes as input the public parameter 1^λ and outputs a public-secret key pair $(pk, sk) \in \mathcal{PK} \times \mathcal{SK}$.*
- ***Encapsulation*** $(c, k) \xleftarrow{\$} \mathsf{Encaps}(pk)$*: takes as input a public key $pk \in \mathcal{PK}$ and outputs a ciphertext $c \in \mathcal{CT}$ and a symmetric key $k \in \mathcal{K}$.*
- ***Decapsulation*** $k \leftarrow \mathsf{Decaps}(sk, c)$*: takes as input a secret key $sk \in \mathcal{SK}$ and a ciphertext $c \in \mathcal{CT}$ and outputs either a symmetric key $k \in \mathcal{K}$ or an error symbol $\perp$.*

We say a KEM is δ-correct if for every $(pk, sk) \xleftarrow{\$} \mathsf{KG}()$, we have $\Pr[k \ne \mathsf{Decaps}(sk, c) : (c, k) \xleftarrow{\$} \mathsf{Encaps}(pk)] \le \delta$. In particular, we call a KEM *(perfectly) correct* if $\delta = 0$.

We define the min-entropy α_{pk} of public keys pk and α_c of the ciphertext c by

$$\alpha_{pk} := -\log \max_{pk' \in \mathcal{PK}} \Pr[pk' = pk : (pk, sk) \xleftarrow{\$} \mathsf{KG}()]$$

$$\alpha_c := -\log \max_{c' \in \mathcal{CT}} \Pr_{(pk,sk) \xleftarrow{\$} \mathsf{KG}()}[c = c' : (c, \mathsf{K}) \xleftarrow{\$} \mathsf{Encaps}(pk)]$$

In terms of the security notions, we recall the standard *indistinguishability under chosen plaintext* (IND-CPA). The IND-CPA security prevents an adversary from distinguishing the encapsulated symmetric key of a challenge ciphertext from a random one.

Definition 16. *Let* $\mathsf{KEM} = (\mathsf{KG}, \mathsf{Encaps}, \mathsf{Decaps})$ *be a key encapsulation mechanism scheme with symmetric key space* $\mathcal{K}$. *We say* KEM *is* ϵ-$\mathsf{IND\text{-}CCA}$ *secure, if the below defined advantage of every (potential quantum) adversary* $\mathcal{A}$ *against* $\mathsf{Expt}_{\mathsf{KEM}}^{\mathsf{IND\text{-}CCA}}$ *experiment in Figure 16 is bounded by,*

$$\mathsf{Adv}_{\mathsf{KEM}}^{\mathsf{IND\text{-}CCA}}(\mathcal{A}) := \left| \Pr[\mathsf{Expt}_{\mathsf{KEM}}^{\mathsf{IND\text{-}CCA}}(\mathcal{A}) = 1] - \frac{1}{2} \right| \leq \epsilon$$

```
$\mathsf{Expt}_{\mathsf{KEM}}^{\mathsf{IND\text{-}CCA}}(\mathcal{A})$:
  $\mathsf{b} \xleftarrow{\$} \{0,1\}$
  $(pk, sk) \xleftarrow{\$} \mathsf{KG}()$
  $(c^\star, k_0^\star) \xleftarrow{\$} \mathsf{Encaps}(pk)$
  $k_1^\star \xleftarrow{\$} \mathcal{K}$
  $\mathsf{b}' \xleftarrow{\$} \mathcal{A}^{\textsc{Decaps}}(pk, c^\star, k_{\mathsf{b}}^\star)$
  return $[\![\mathsf{b} = \mathsf{b}']\!]$

$\textsc{Decaps}(c)$:
  if $c = c^\star$: return $\perp$
  $\mathsf{K}' \leftarrow \mathsf{Decaps}(sk, c)$
  return $\mathsf{K}'$
```

Fig. 16. IND-CCA experiment for $\mathsf{KEM} = (\mathsf{KG}, \mathsf{Encaps}, \mathsf{Decaps})$ with symmetric key space $\mathcal{K}$.

Definition 17. *A symmetric key encryption scheme over key space* $\mathcal{K}$ *and ciphertext space* $\mathcal{CT}$, *is a tuple of algorithms* $\mathsf{KEM} = (\mathsf{KG}, \mathsf{Encaps}, \mathsf{Decaps})$ *as defined below.*

- ***Key Generation*** $K \xleftarrow{\$} \mathsf{KG}(1^\lambda)$: *takes as input the public parameter* 1^λ *and outputs a symmetric key* $K \in \mathcal{K}$.
- ***Encryption*** $c \xleftarrow{\$} \mathsf{Enc}(K, m)$: *takes as input a key* $K \in \mathcal{K}$ *and a message* m *and outputs a ciphertext* $c \in \mathcal{CT}$.
- ***Decryption*** $m \leftarrow \mathsf{Decaps}(K, c)$: *takes as input a symmetric key* $K \in \mathcal{K}$ *and a ciphertext* $c \in \mathcal{CT}$ *and outputs either a message* m *or an error symbol* $\perp$.

We say a SKE is δ-correct if for every $K \xleftarrow{\$} \mathsf{KG}()$, we have

$$\Pr[m \neq \mathsf{Dec}(K, \mathsf{Enc}(K, m))] \leq \delta$$

In particular, we call a SKE *(perfectly) correct* if $\delta = 0$.

In terms of the security, we first recall the standard *indistinguishability under chosen plaintext attacks (*$\mathsf{IND\text{-}CPA}$*)*.

Definition 18. *Let* $\mathsf{SKE} = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ *be a symmetric key encryption scheme with symmetric key space* $\mathcal{K}$. *We say* SKE *is* ϵ-$\mathsf{IND\text{-}CPA}$ *secure, if the blow defined advantage of every (potential quantum) adversary* $\mathcal{A}$ *against* $\mathsf{Expt}_{\mathsf{SKE}}^{\mathsf{IND\text{-}CPA}}$ *experiment in Figure 17 is bounded by,*

$$\mathsf{Adv}_{\mathsf{SKE}}^{\mathsf{IND\text{-}CPA}}(\mathcal{A}) := \left| \Pr[\mathsf{Expt}_{\mathsf{SKE}}^{\mathsf{IND\text{-}CPA}}(\mathcal{A}) = 1] - \frac{1}{2} \right| \leq \epsilon$$

```
$\mathsf{Expt}_{\mathsf{SKE}}^{\mathsf{IND\text{-}CPA}}(\mathcal{A})$:
  $\mathsf{b} \xleftarrow{\$} \{0,1\}$
  $K \xleftarrow{\$} \mathsf{KG}()$
  $\mathsf{b}' \xleftarrow{\$} \mathcal{A}^{\textsc{Enc}}()$
  return $[\![\mathsf{b} = \mathsf{b}']\!]$

$\textsc{Enc}(m_0, m_1)$:
  $c \xleftarrow{\$} \mathsf{Encaps}(K, m_{\mathsf{b}})$
  return $c$
```

Fig. 17. IND-CPA experiment for $\mathsf{SKE} = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$.

Then, we recall two notions, the *one time* $\mathsf{IND\text{-}CPA}$ *(*$\mathsf{IND\text{-}1CPA}$*)* security [9] and *indistinguishability under one-time chosen and then random plaintext attack (*$\mathsf{IND\text{-}1\$PA}$*)* security [2].

Definition 19. *Let* $\mathsf{SKE} = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ *be a symmetric key encryption scheme with symmetric key space* $\mathcal{K}$. *We say* SKE *is* ϵ-$\mathsf{IND\text{-}1CPA}$ *secure, if the blow defined advantage of every (potential quantum) adversary* $\mathcal{A}$ *against* $\mathsf{Expt}_{\mathsf{SKE}}^{\mathsf{IND\text{-}1CPA}}$ *experiment in Figure 18 is bounded by,*

$$\mathsf{Adv}_{\mathsf{SKE}}^{\mathsf{IND\text{-}1CPA}}(\mathcal{A}) := \left| \Pr[\mathsf{Expt}_{\mathsf{SKE}}^{\mathsf{IND\text{-}1CPA}}(\mathcal{A}) = 1] - \frac{1}{2} \right| \leq \epsilon$$

Definition 20. *Let* $\mathsf{SKE} = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ *be a symmetric key encryption scheme with symmetric key space* $\mathcal{K}$. *We say* SKE *is* ϵ-$\mathsf{IND\text{-}1\$PA}$ *secure, if the blow defined advantage of every (potential quantum) adversary* $\mathcal{A}$ *against* $\mathsf{Expt}_{\mathsf{SKE}}^{\mathsf{IND\text{-}1\$PA}}$ *experiment in Figure 18 is bounded by,*

$$\mathsf{Adv}_{\mathsf{SKE}}^{\mathsf{IND\text{-}1\$PA}}(\mathcal{A}) := \left| \Pr[\mathsf{Expt}_{\mathsf{SKE}}^{\mathsf{IND\text{-}1\$PA}}(\mathcal{A}) = 1] - \frac{1}{2} \right| \leq \epsilon$$

Then, we define a new customized notion for SKE: the IND-CPA security with respect to function H (IND-1CPA-H). Compared to IND-1CPA security, the attacker additionally obtains a challenge tag that is produced by applying H to both a symmetric key, which is same as the one used by the SKE, and the challenge ciphertext.

Definition 21. *Let* $\mathsf{SKE} = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ *be a symmetric key encryption scheme with symmetric key space* $\mathcal{K}$. *We say* SKE *is* ϵ*-one time* $\mathsf{IND\text{-}CPA}$ *secure with respect to function* H *(denoted by* $\mathsf{IND\text{-}1CPA\text{-}H}$*) secure, if the blow defined advantage of every (potential quantum) adversary* $\mathcal{A}$ *against* $\mathsf{Expt}_{\mathsf{SKE}}^{\mathsf{IND\text{-}1CPA\text{-}H}}$ *experiment in Figure 18 is bounded by,*

$$\mathsf{Adv}_{\mathsf{SKE}}^{\mathsf{IND\text{-}1CPA\text{-}H}}(\mathcal{A}) := \left| \Pr[\mathsf{Expt}_{\mathsf{SKE}}^{\mathsf{IND\text{-}1CPA\text{-}H}}(\mathcal{A}) = 1] - \frac{1}{2} \right| \leq \epsilon$$

We further extend IND-1\$PA security to a new notion IND-1\$PA-LPC that additionally gives the adversary the access to a challenge plaintext checking oracle, which returns whether the input ciphertext can be decrypted to the challenge plaintext.

Definition 22. *Let* $\mathsf{SKE} = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ *be a symmetric key encryption scheme with symmetric key space* $\mathcal{K}$. *We say* SKE *is* ϵ-$\mathsf{IND\text{-}1\$PA\text{-}LPC}$ *secure, if the blow defined advantage of every (potential quantum) adversary* $\mathcal{A}$ *against* $\mathsf{Expt}_{\mathsf{SKE}}^{\mathsf{IND\text{-}1\$PA\text{-}LPC}}$ *experiment in Figure 18 is bounded by,*

$$\mathsf{Adv}_{\mathsf{SKE}}^{\mathsf{IND\text{-}1\$PA\text{-}LPC}}(\mathcal{A}) := \left| \Pr[\mathsf{Expt}_{\mathsf{SKE}}^{\mathsf{IND\text{-}1\$PA\text{-}LPC}}(\mathcal{A}) = 1] - \frac{1}{2} \right| \leq \epsilon$$

Appendix F
Proof of Theorem 5

Proof. The proof is given by a simple reduction. If there exists an adversary $\mathcal{A}$ that breaks $\mathsf{IND\text{-}1\$PA}$ security of SKE, then we can construct another adversary $\mathcal{B}$ that breaks $\mathsf{IND\text{-}CPA}$ security of SKE as follows:

1) $\mathcal{B}$ invokes $\mathcal{A}$.

```
$\mathsf{Expt}^{\mathsf{IND\text{-}1CPA}}_{\mathsf{SKE}}(\mathcal{A})$:
    $\mathsf{b} \xleftarrow{\$} \{0,1\}$
    $K \xleftarrow{\$} \mathsf{KG}()$
    $(m_0^\star, m_1^\star) \xleftarrow{\$} \mathcal{A}()$
    if $|m_0^\star| \neq |m_1^\star|$
        return 0
    $c^\star \xleftarrow{\$} \mathsf{Enc}(K, m_{\mathsf{b}}^\star)$
    $\mathsf{b}' \xleftarrow{\$} \mathcal{A}(c^\star)$
    return $[\![\mathsf{b} = \mathsf{b}']\!]$

$\mathsf{Expt}^{\mathsf{IND\text{-}1CPA\text{-}H}}_{\mathsf{SKE}}(\mathcal{A})$:
    $\mathsf{b} \xleftarrow{\$} \{0,1\}$
    $K \xleftarrow{\$} \mathsf{KG}()$
    $(m_0^\star, m_1^\star) \xleftarrow{\$} \mathcal{A}()$
    if $|m_0^\star| \neq |m_1^\star|$
        return 0
    $c^\star \xleftarrow{\$} \mathsf{Enc}(K, m_{\mathsf{b}}^\star)$
    $t^\star \leftarrow \mathsf{H}(K, c^\star)$
    $\mathsf{b}' \xleftarrow{\$} \mathcal{A}(c^\star, t^\star)$
    return $[\![\mathsf{b} = \mathsf{b}']\!]$

$\mathsf{Expt}^{\mathsf{IND\text{-}1\$PA}}_{\mathsf{SKE}}(\mathcal{A})$:
    $\mathsf{b} \xleftarrow{\$} \{0,1\}$
    $K \xleftarrow{\$} \mathsf{KG}()$
    $(m_0^\star, m_1^\star) \xleftarrow{\$} \mathcal{A}()$
    if $|m_0^\star| \neq |m_1^\star|$
        return 0
    $c^\star \xleftarrow{\$} \mathsf{Enc}(K, m_{\mathsf{b}}^\star)$
    $\mathsf{b}' \xleftarrow{\$} \mathcal{A}^{\textsc{Rand}}(c^\star)$
    return $[\![\mathsf{b} = \mathsf{b}']\!]$

$\mathsf{Expt}^{\mathsf{IND\text{-}1\$PA\text{-}LPC}}_{\mathsf{SKE}}(\mathcal{A})$:
    $\mathsf{b} \xleftarrow{\$} \{0,1\}$
    $K \xleftarrow{\$} \mathsf{KG}()$
    $(m_0^\star, m_1^\star) \xleftarrow{\$} \mathcal{A}()$
    if $|m_0^\star| \neq |m_1^\star|$
        return 0
    $c^\star \xleftarrow{\$} \mathsf{Enc}(K, m_{\mathsf{b}}^\star)$
    $\mathsf{b}' \xleftarrow{\$} \mathcal{A}^{\textsc{Rand},\textsc{Lpc}}(c^\star)$
    return $[\![\mathsf{b} = \mathsf{b}']\!]$

$\textsc{Rand}(l)$:
    $m_0', m_1' \xleftarrow{\$} \{0,1\}^l$
    $c' \xleftarrow{\$} \mathsf{Enc}(K, m_{\mathsf{b}}')$
    return $(m_0', m_1', c')$

$\textsc{Lpc}(c)$:
    return $[\![m_0^\star = \mathsf{Dec}(K, c)]\!]$
```

Fig. 18. IND-1CPA, IND-1CPA-H, IND-1\$PA, and IND-1\$PA-LPC experiments for SKE = (KG, Enc, Dec).

2) When $\mathcal{A}$ outputs $(m_0^\star, m_1^\star)$, $\mathcal{B}$ returns 0 if $m_0^\star$ and $m_1^\star$ do not have the same length. Otherwise, $\mathcal{B}$ forwards $(m_0^\star, m_1^\star)$ to its Enc oracles, and returns the response to $\mathcal{A}$.
3) Whenever $\mathcal{A}$ queries Rand oracle with input l, $\mathcal{B}$ first samples $m_0', m_1' \xleftarrow{\$} \{0,1\}^l$. Then, $\mathcal{B}$ sends (m_0', m_1') to its Enc oracle and receives response c'. Finally, $\mathcal{B}$ returns (m_0', m_1', c') to $\mathcal{A}$.
4) When $\mathcal{A}$ outputs b', $\mathcal{B}$ also outputs b'.

It is straightforward that $\mathcal{B}$ perfectly simulates IND-1\$PA experiment to $\mathcal{A}$ and $\mathcal{B}$ wins if and only if $\mathcal{A}$ wins. Thus, we have that

$$\epsilon^{\mathsf{ind\text{-}1\$pa}}_{\mathsf{SKE}} \leq \epsilon^{\mathsf{ind\text{-}cpa}}_{\mathsf{SKE}}$$

□

Appendix G
Proof of Theorem 6

Proof. The proof is given by a sequence of games. Let Adv_i denote the adversary $\mathcal{A}$'s advantage in winning Game i. It is straightforward that the adversary $\mathcal{A}$ can win only by random guessing if it outputs $m_0^\star = m_1^\star$, which yields the advantage 0. So, in the proof below, we assume $m_0^\star \neq m_1^\star$. Let $i^\star$ denote the smallest index such that the $i^\star$-th block of $m_0^\star$ does not equal the one of $m_1^\star$.

Game 0. This game is identical to the original IND-1\$PA-LPC experiment defined in Definition 22. Thus, we have that

$$\mathsf{Adv}_0 = \epsilon^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}_{\mathsf{SKE}}$$

Game 1. This game is identical to **Game 0** except the following modification:

1) The challenger $\mathcal{C}$ samples a random invertible permutation $f : \{0,1\}^{f_2(\lambda)} \to \{0,1\}^{f_2(\lambda)}$ in advance,
2) Whenever $\mathcal{C}$ needs to execute the encryption $\mathsf{Enc}(K, \cdot)$ on some messages, $\mathcal{C}$ replaces the underlying computation of $\mathsf{F}(K, \cdot)$ by $f(\cdot)$, and $\mathsf{F}^{-1}(K, \cdot)$ by $f^{-1}(\cdot)$.

It is straightforward that if $\mathcal{A}$ can distinguish **Game 0** and **Game 1**, then there exists an adversary $\mathcal{B}_1$ that can break the prp security of F. Thus, we have that

$$\mathsf{Adv}_0 - \mathsf{Adv}_1 \leq \epsilon^{\mathsf{prp}}_{\mathsf{F}}$$

Game 2. In this game, the challenger aborts and let $\mathcal{A}$ immediately win if $\mathcal{A}$ can query Lpc with input c such that $m_0^\star = \mathsf{Dec}(K, c)$ but $c \neq c^\star$. Let $n \cdot f_2(\lambda)$ denote the length of $m_0^\star$ for $n \geq 1$. We parse $m_0^\star$ into n blocks such that $m_0^\star = x_1^\star \parallel \cdots \parallel x_n^\star$. Similarly, we parse $c^\star = y_0^\star \parallel \cdots \parallel y_n^\star$ and $c = y_0 \parallel \cdots \parallel y_n$. Note that the condition $c \neq c^\star$. We use $j^\star$ to denote the smallest index such that $y_{j^\star} \neq y_{j^\star}^\star$.

We separate the analysis into the following two cases.

a) If $\mathsf{b} = 0$*:* In this case, $m_0^\star = \mathsf{Dec}(K, c) = \mathsf{Dec}(K, c^\star)$ but $c \neq c^\star$. We first claim that $j^\star = 0$. Suppose that $j^\star > 0$, which means $y_0 = y_0^\star$. Note that $m_0^\star = \mathsf{Dec}(K, c) = \mathsf{Dec}(K, c^\star)$, which implies that

$$x_i^\star = y_{i-1} \oplus f^{-1}(y_i) = y_{i-1}^\star \oplus f^{-1}(y_i^\star), \forall i \in \{1, \cdots, n\}$$

In particular,

$$x_1^\star = y_0 \oplus f^{-1}(y_1) = y_0^\star \oplus f^{-1}(y_1^\star)$$

By $y_0 = y_0^\star$, we can observe that $y_1 = f(x_1^\star \oplus y_0) = f(x_1^\star \oplus y_0^\star) = y_1^\star$. Repeating the steps above, we can further observe that $y_i = y_i^\star$ for $i = 1, 2, ..., n$ step by step. This contradicts to our condition $c \neq c^\star$.

Now, we focus on the first two blocks of the ciphertext c and $c^\star$. By the equation above, $m_0^\star = \mathsf{Dec}(K, c) = \mathsf{Dec}(K, c^\star)$ in particular implies that $y_1 = f(x_1^\star \oplus y_0) = f(f^{-1}(y_1^\star) \oplus y_0^\star \oplus y_0)$. Recall that f is a random permutation as defined in **Game 1** and that $\mathcal{A}$ has no access to f or f^{-1}. Unless the permutation f has applied to $f^{-1}(y_1^\star) \oplus y_0^\star \oplus y_0$ in the Rand oracle, which happens with probability at most $q_{\textsc{Rand}} \lceil \frac{l_{\mathsf{max}}}{f_2(\lambda)} \rceil 2^{-f_2(\lambda)}$, where l_{max} denotes the maximal input of the queries to Rand oracle, the adversary has no information about y_1 and can guess y_1 only by random guessing, which happens at most $2^{-f_2(\lambda)}$ per query. Note that $\mathcal{A}$ can query Lpc at most $q_{\textsc{Lpc}}$ times, by union bound theorem, we know that the adversary can win by query Lpc oracle with probability at most $q_{\textsc{Lpc}} 2^{-f_2(\lambda)} + q_{\textsc{Rand}} \lceil \frac{l_{\mathsf{max}}}{f_2(\lambda)} \rceil 2^{-f_2(\lambda)}$.

b) If $\mathsf{b} = 1$*:* In this case, the adversary needs to forge the ciphertext c that can be decrypted to $m_0^\star$ by himself. In particular, the adversary $\mathcal{A}$ needs to forge the ($i^\star$-1)-th and $i^\star$-th blocks of the ciphertext such that $y_{i^\star} = f(y_{i^\star\text{-}1} \oplus x_{i^\star}^\star)$. Unless the permutation has applied to $y_{i^\star\text{-}1} \oplus x_{i^\star}^\star$, which happens with probability at most $q_{\textsc{Rand}} \lceil \frac{l_{\mathsf{max}}}{f_2(\lambda)} \rceil 2^{-f_2(\lambda)}$, the adversary receives no information about $y_{i^\star}$ and can only randomly guess, which happens with probability $2^{-f_2(\lambda)}$ per query. Note that $\mathcal{A}$ can query Lpc at most $q_{\textsc{Lpc}}$ times, by union bound theorem, we know that the adversary can win by query Lpc oracle with probability at most $q_{\textsc{Lpc}} 2^{-f_2(\lambda)} + q_{\textsc{Rand}} \lceil \frac{l_{\mathsf{max}}}{f_2(\lambda)} \rceil 2^{-f_2(\lambda)}$.

To sum up, we have that

$$\mathsf{Adv}_1 - \mathsf{Adv}_2 \leq q_{\text{LPC}} 2^{-f_2(\lambda)} + q_{\text{RAND}} \lceil \frac{l_{\mathsf{max}}}{f_2(\lambda)} \rceil 2^{-f_2(\lambda)}$$

Game 3. This game is identical to **Game 2** except the following modification:

1) Whenever the adversary $\mathcal{A}$ queries LPC with some input c, the challenger $\mathcal{C}$ simply returns 1 if $c = c^\star$, and 0 otherwise.

Recall that we ensure that the adversary $\mathcal{A}$ cannot query LPC with any input c such that $m_0^\star = \mathsf{Dec}(K, c)$ but $c \neq c^\star$. So, **Game 2** and **Game 3** look identical from the adversary's view and we have that

$$\mathsf{Adv}_2 = \mathsf{Adv}_3$$

Game 4. This game is identical to **Game 3** except the following modification:

1) Whenever $\mathcal{C}$ needs to execute the encryption $\mathsf{Enc}(K, \cdot)$ on some messages, $\mathcal{C}$ replaces the underlying computation of $f(\cdot)$ by $\mathsf{F}(K, \cdot)$, and $f^{-1}(\cdot)$ by $\mathsf{F}^{-1}(K, \cdot)$.

It is straightforward that if $\mathcal{A}$ can distinguish **Game 3** and **Game 4**, then there exists an adversary $\mathcal{B}_2$ that can break the prp security of F. Thus, we have that

$$\mathsf{Adv}_3 - \mathsf{Adv}_4 \leq \epsilon_{\mathsf{F}}^{\mathsf{prp}}$$

Final Analysis. In the end, we analyze the adversary $\mathcal{A}$'s advantage in winning **Game 4** by reduction. Namely, if $\mathcal{A}$ can break **Game 4**, then we can construct an adversary $\mathcal{B}_3$ that breaks $\mathsf{IND\text{-}1\$PA}$ security of $\mathsf{SKE} = \mathsf{CBC}_0$ as follows:

1) $\mathcal{B}_3$ invokes $\mathcal{A}$.
2) When $\mathcal{A}$ outputs $(m_0^\star, m_1^\star)$, $\mathcal{B}_3$ forwards it to its challenger. Later, when $\mathcal{B}_3$ receives $c^\star$ from its challenger, $\mathcal{B}_3$ forwards $c^\star$ to $\mathcal{A}$.
3) When $\mathcal{A}$ queries RAND(l), $\mathcal{B}_3$ forwards this query to its challenger and the response back to $\mathcal{A}$.
4) When $\mathcal{A}$ queries LPC(c), $\mathcal{B}_3$ returns 1 if $c = c^\star$ and 0 otherwise.
5) When $\mathcal{A}$ outputs a bit b', $\mathcal{B}_3$ forwards b' to its challenger.

It is straightforward that $\mathcal{B}_3$ perfectly simulates **Game 4** to $\mathcal{A}$ and $\mathcal{B}_3$ wins if and only if $\mathcal{A}$ wins. Thus, we have that

$$\mathsf{Adv}_4 \leq \epsilon_{\mathsf{SKE}}^{\mathsf{ind\text{-}1\$pa}}$$

Combing the statements above, the proof is concluded by

$$\begin{aligned} &\epsilon_{\mathsf{SKE}}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}} \\ \leq & 2\epsilon_{\mathsf{F}}^{\mathsf{prp}} + q_{\text{LPC}} 2^{-f_2(\lambda)} + q_{\text{RAND}} \lceil \frac{l_{\mathsf{max}}}{f_2(\lambda)} \rceil 2^{-f_2(\lambda)} + \epsilon_{\mathsf{SKE}}^{\mathsf{ind\text{-}1\$pa}} \end{aligned}$$

□

APPENDIX H
PROOF OF THEOREM 1

Proof. The proof is given by a sequence of games. Let Adv_i denotes the advantage of the Compl adversary $\mathcal{A}$ in winning Game i.

Game 0. This game is identical to the original experiment depicted in Figure 2. It holds that

$$\mathsf{Adv}_0 = \mathsf{Adv}_{\mathsf{PIA,Compl}}^{\mathsf{auth}}(\mathcal{A})$$

Game 1. This game is identical to **Game 0** except that the game aborts let $\mathcal{A}$ immediately win if there exist two credential identifiers that collide with each other. By this, we ensure that all credential identifiers are distinct. Note that cids are only sampled in the token's registration response rRsp algorithm and that the rRsp algorithm is invoked only when the adversary $\mathcal{A}$ queries REGISTER oracle, which happens at most q_{REGISTER} times, there are maximal $\binom{q_{\text{REGISTER}}}{2}$ pairs of cids. Note also that each cid is independently sampled from the set $\{0,1\}^{\geq\lambda}$. The collision of cids happens with probability $\binom{q_{\text{REGISTER}}}{2} 2^{-\lambda}$. Hence, it holds that

$$\mathsf{Adv}_0 - \mathsf{Adv}_1 \leq \binom{q_{\text{REGISTER}}}{2} 2^{-\lambda}$$

Game 2. This game is identical to **Game 1** except that the challenger aborts the game and let $\mathcal{A}$ immediately win if there are two challenge nonces ch during the authentication phases that collide. By this, we ensure that all challenges nonce ch sampled in the authentication phases are distinct. Note that chs in the authentication phase are only sampled in the server's authentication challenge aChall algorithm and that the aChall algorithm is invoked only when the adversary $\mathcal{A}$ queries CHALLENGE oracle, which happens at most $q_{\text{CHALLENGE}}$ times. There are maximal $\binom{q_{\text{CHALLENGE}}}{2} = \frac{q_{\text{CHALLENGE}}(q_{\text{CHALLENGE}}-1)}{2}$ pairs of chs in the authentication phases. Note also that each ch is independently sampled in the set $\{0,1\}^{\geq\lambda}$. The collision of such chs happens with probability at most $\binom{q_{\text{CHALLENGE}}}{2} 2^{-\lambda}$. Hence, it holds that

$$\mathsf{Adv}_1 - \mathsf{Adv}_2 \leq \binom{q_{\text{CHALLENGE}}}{2} 2^{-\lambda}$$

Game 3. This game is identical to **Game 2** except that the game aborts and the adversary $\mathcal{A}$ immediately wins if there exist two hash values $\mathsf{H}(x_1) = \mathsf{H}(x_2)$ that collide on different inputs $x_1 \neq x_2$. Note that this is in fact captured by the collision resistance of the underlying H by definition. Thus, we have that

$$\mathsf{Adv}_2 - \mathsf{Adv}_3 \leq \epsilon_{\mathsf{H}}^{\mathsf{coll\text{-}res}}$$

Final Analysis. Now, we analyze the probability that $\mathcal{A}$ wins **Game 3**. Note that $\mathcal{A}$ can win only when if one of the following conditions holds when a server π_S^i accepts a response message in the COMPLETE oracle,

1) if $\exists (T_1, j_1), (T_2, j_2)$ such that $(T_1, j_1) \neq (T_2, j_2)$ and $\pi_{T_1}^{j_1}.\mathsf{sid} = \pi_{T_2}^{j_2}.\mathsf{sid} \neq \perp$

2) if $\exists(S_1, i_1), (S_2, i_2)$ s.t. $(S_1, i_1) \neq (S_2, i_2)$ and $\pi_{S_1}^{i_1}.\mathsf{sid} = \pi_{S_2}^{i_2}.\mathsf{sid} \neq \bot$
3) if $(S, T) \in \mathcal{L}_{\mathsf{frsh}}$ and $\nexists j$ such that $\pi_S^i.\mathsf{sid} = \pi_T^j.\mathsf{sid}$ for $T \leftarrow \mathsf{regPartner}(S)$
4) if $\exists(S', i'), (T', j')$ such that $\pi_{S'}^{i'}.\mathsf{sid} = \pi_{T'}^{j'}.\mathsf{sid} \neq \bot$ and $(S', T') \in \mathcal{L}_{\mathsf{frsh}}$ and $\pi_{S'}^{i'}.\mathsf{agCon} \neq \pi_{T'}^{j'}.\mathsf{agCon}$

Let $\mathsf{Adv}_{3.1}$, $\mathsf{Adv}_{3.2}$, $\mathsf{Adv}_{3.3}$, and $\mathsf{Adv}_{3.4}$ respectively denote the advantage of $\mathcal{A}$ in winning **Game 3** via condition (1), (2), (3), or (4). Thus, we have that

$$\mathsf{Adv}_3 \leq \max(\{\mathsf{Adv}_{3.1}, \mathsf{Adv}_{3.2}, \mathsf{Adv}_{3.3}, \mathsf{Adv}_{3.4}\})$$

Case (1): Note that the session identifier of the token sessions $\pi_T^j.\mathsf{sid}$ for any (T, j) includes the credential identifier cid, which is sampled by the token at the registration phase and then stored in the registration context. Note also that we have ensured that all cids sampled by tokens are distinct in **Game 1**. So, no session identifiers can be identical across the token sessions that uses different registration contexts.

Note that the identifier of a token sessions at the registration phase include the counter $n = 0$. Note also that the identifier of a token session at the authentication phase includes the counter n, which is stored in the registration context and incremented by 1 before the session identifiers are set. This means, no session identifiers of different token sessions that makes use of the same registration context collide due to the increment of counter n.

To sum up, we have that

$$\mathsf{Adv}_{3.1} = 0$$

Case (2): First, we can observe that the session identifiers of each server session π_S^i includes $\mathsf{H}(\mathsf{id}_S)$. Note that we assume the identifier id_S of each server S is unique and that we have ensured no collision of the hash output on different inputs. So, no session identifiers can be identical across different servers.

Note that the session identifier of a server session at the registration phase does not include the $\mathsf{H}(m_{\mathsf{rcl}})$, while the one of a server session at the authentication includes $\mathsf{H}(m_{\mathsf{acl}})$. The session identifiers of server sessions at the registration phase and the authentication phases can be easily distinguished. Note also that we have ensured that all chs are distinct in **Game 2** and that no collision of the hash output on different inputs exists in **Game 3**. This means, no session identifiers of different sessions of the same server can be identical.

To sum up, we have that

$$\mathsf{Adv}_{3.2} = 0$$

Case (3): Note that server session π_S^i accepts the response message only when $\mathsf{rc}_S[\mathsf{cid}] \neq \bot$ for some cid. Note also that $\mathsf{rc}_S[\mathsf{cid}] \neq \bot$ is set only in the registration phase and that all cids are sampled by the tokens followed by sending to the server session over an authenticated channel. There must be a token T that registers with the server S, which further implies that there must exist a token T such that $\mathsf{rc}_T[S] \neq \bot$. Thus, we have $T = \mathsf{regPartner}(S, i) \neq \bot$.

Then, we compute the probability of the occurrence of Case (3) by reduction. We construct an adversary $\mathcal{B}$ that breaks the euf-cma security of Σ, which is invoked in the COMPLETE oracle, by invoking $\mathcal{A}$. Note that $\mathcal{A}$ can query REGISTER oracle at most q_{REGISTER} times. $\mathcal{B}$ first guesses an index y such that the y-th REGISTER query inputs $((S, \pi_S^i.\mathsf{regIndex}), (T, j), \mathsf{tb}, UV)$ and that the adversary $\mathcal{A}$ can finally wins condition (3) due to $\mathsf{Win\text{-}auth}(S, i)$. Note that each session can be constructed at most once. So, the existence of such y-th query is well-defined and unique. It's obvious that $\mathcal{B}$ guesses correctly with probability at least $\frac{1}{q_{\text{REGISTER}}}$.

Next, $\mathcal{B}$ receives a public verification key pk from his challenger and honestly simulates **Game 3** to $\mathcal{A}$ except when answering the following queries:

- The y-th query $\text{REGISTER}((S, i), (T, j), \mathsf{tb}, UV)$: $\mathcal{B}_3$ honestly simulates this oracle except that he directly uses pk, the public verification key from his challenger, in the rRsp algorithm instead of sampling it by himself. Moreover, $\mathcal{B}$ records $\tilde{S} := S$ and $\tilde{T} := T$.
- $\text{RESPONSE}((T, j), m_{\mathsf{acom}})$, where $m_{\mathsf{acom}} = (\mathsf{id}, h, UV, UP)$ for $\mathsf{id} = \mathsf{id}_{\tilde{S}}$, $T = \tilde{T}$, and some h, UV, UP: $\mathcal{B}$ honestly simulates this oracle except that he queries his signing oracle on (ad, h) for the signature σ instead of computing it by himself.
- $\text{CORRUPT}(S, T)$: If $(S, T) \neq (\tilde{S}, \tilde{T})$, $\mathcal{B}$ simply returns the $\mathsf{rc}_T[S].sk$. Otherwise, $\mathcal{B}$ aborts the simulation.

Recall that the server's session at the authentication phase is set to accepted only in the COMPLETE oracle. If $\mathcal{B}$ guesses the index y correctly, in order to trigger the winning condition, then $\mathcal{A}$ must query $\text{COMPLETE}((\tilde{S}, i), m_{\mathsf{acl}}, m_{\mathsf{arsp}})$ at some point for some $m_{\mathsf{acl}} = (\mathsf{ch}, \mathsf{tb})$ and $m_{\mathsf{arsp}} = (\mathsf{cid}, ad, \sigma, \mathsf{uid})$. Moreover $(\tilde{S}, \tilde{T}) \in \mathcal{L}_{\mathsf{frsh}}$ indicates that the adversary $\mathcal{A}$ has never queried $\text{CORRUPT}(\tilde{S}, \tilde{T})$, which further means that the abortion never happens.

Then, assume that $\mathcal{A}$ can win via the $\text{COMPLETE}((\tilde{S}, i), m_{\mathsf{acl}}, m_{\mathsf{arsp}})$ query for some i, m_{acl}, and m_{arsp}. $\mathcal{B}$ outputs (m', σ') where $m' = (ad, \mathsf{H}(m_{\mathsf{acl}}))$ and $\sigma' = \sigma$. It is straightforward that $\mathcal{B}$ perfectly simulates **Game 3** to $\mathcal{A}$ if $\mathcal{B}$ guesses the index y correctly.

Note that the session identifier of each token at the authentication phase is part of the m_{arsp} that it produced. The condition $\nexists j$ such that $\pi_{\tilde{S}}^i.\mathsf{sid} = \pi_{\tilde{T}}^j.\mathsf{sid}$ indicates that such m_{arsp} must not be produced by any token sessions. Further, this also implies that the message $m' = (ad, h)$ has never been sent to the signing oracle. Moreover, $\pi_S^i.\mathsf{st}_{\mathsf{exe}} = \mathsf{accepted}$ implies that $\Sigma.\mathsf{Vfy}(pk, m', \sigma') = 1$. To sum up, $\mathcal{B}$ will always win the euf-cma experiment. Thus, we have that

$$\mathsf{Adv}_{3.3} \leq q_{\text{REGISTER}} \epsilon_{\Sigma}^{\mathsf{euf\text{-}cma}}$$

Case (4): First, by Case (1) and (2) we know that there are no two distinct token (resp. server) sessions that have the identical non-$\bot$ session identifiers. Thus, if there exist $(S', i'), (T', j')$ such that $\pi_{S'}^{i'}$ partner with $\pi_{T'}^{j'}$, then they are each other's unique partner.

Second, we first consider the registration phase. Note that the registration phase is over an authenticated channel. In each registration query $\textsc{Register}((S', i'), (T', j'), \mathsf{tb}, UV)$ for some tb and UV, $\pi_{S'}^{i'}$ will partner with $\pi_{T'}^{j'}$ if no abortion happens. Moreover, each message sent by the server session $\pi_{S'}^{i'}$ will then arrive at the token session $\pi_{T'}^{j'}$, which trivially indicates that $\pi_{S'}^{i'}.\mathsf{agCon} = \pi_{T'}^{j'}.\mathsf{agCon}$.

Finally, we consider the authentication phase. If $\pi_{S'}^{i'}.\mathsf{sid} \neq \perp$ is set during the authentication phase, then the session $\pi_{S'}^{i'}$ must accepts a response message via the $\textsc{Complete}$ oracle. By Case (3), we know that $\pi_{S'}^{i'}$ partner with π_{T}^{j}, where T is the registration partner of S', except probability at most $\mathsf{Adv}_{3.3}$. Recall that $\pi_{S'}^{i'}$ and $\pi_{T'}^{j'}$ are each other's unique partner. We have that $(T, j) = (T', j')$ except probability at most $\mathsf{Adv}_{3.3}$.

Note that $\pi_{S'}^{i'}.\mathsf{sid} = \pi_{T'}^{j'}.\mathsf{sid} \neq \perp$ indicates that $\pi_{S'}^{i'}$ and $\pi_{T'}^{j'}$ agree on the hash of the server identifier $\mathsf{H}(\mathsf{id}_S)$, the credential identifier cid, the hash of the client message $\mathsf{H}(m_{\mathsf{acl}})$, and the counter n. Recall that the we ensure that the hash values will not collie on different input. So, the agreement on the hash of the server identifier $\mathsf{H}(\mathsf{id}_S)$ indicates the agreement on the server identifier id_S. The adversary $\mathcal{A}$ can wins via Case (4) only when $\pi_{S'}^{i'}$ and $\pi_{T'}^{j'}$ do not have agreement on the UP and UV conditions. However, note that UP and UV are included in the associated data, which is an input of the digital signature verification algorithm in the aVrfy algorithm. By applying a reduction similar to the one in Case (3), we know that the adversary can win with probability at most $\mathsf{Adv}_{3.3} \leq q_{\textsc{Register}} \epsilon_{\Sigma}^{\mathsf{euf\text{-}cma}}$.

To sum up, the adversary $\mathcal{A}$ can wins Case (4) with advantage:

$$\mathsf{Adv}_{3.4} \leq \mathsf{Adv}_{3.3} + \mathsf{Adv}_{3.3} \leq 2q_{\textsc{Register}} \epsilon_{\Sigma}^{\mathsf{euf\text{-}cma}}$$

Merging the statements above, we have that

$$\begin{aligned}\mathsf{Adv}_3 &\leq \max\{\mathsf{Adv}_{3.1}, \mathsf{Adv}_{3.2}, \mathsf{Adv}_{3.3}, \mathsf{Adv}_{3.4}\} \\ &\leq 2q_{\textsc{Register}} \epsilon_{\Sigma}^{\mathsf{euf\text{-}cma}}\end{aligned}$$

The proof is concluded by

$$\begin{aligned}\mathsf{Adv}_{\mathsf{PIA,Compl}}^{\mathsf{auth}}(1^\lambda) \leq &\binom{q_{\textsc{Register}}}{2} 2^{-\lambda} + \binom{q_{\textsc{Challenge}}}{2} 2^{-\lambda} \\ &+ \epsilon_{\mathsf{H}}^{\mathsf{coll\text{-}res}} + 2q_{\textsc{Register}} \epsilon_{\Sigma}^{\mathsf{euf\text{-}cma}}\end{aligned}$$

□

Appendix I
Proof of Theorem 2

Proof. We give the proof by a sequence of games. Each game is simulated between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$. Let Adv_i denote the adversary $\mathcal{A}$'s advantage in winning game i. Let $(pk_{T,i}, sk_{T,i})$ denote the ECDH public key pair owned and used by π_T^i. Let $(pk_{C,j}, sk_{C,j})$ denote the ECDH public key pair owned and used by π_C^j.

Game 0. This game is identical to the $\mathsf{Expt}_{\mathsf{PACA}}^{\mathsf{SUF\text{-}t'}}$ experiment. Hence, it holds that

$$\mathsf{Adv}_0 = \mathsf{Adv}_{\mathsf{PACA},\mathcal{A}}^{\mathsf{SUF\text{-}t'}}(1^\lambda)$$

Game 1. This game is identical to **Game 0** except the following modifications:

1) At the beginning of this game, the challenger $\mathcal{C}$ sets up two lists $\mathcal{L}_{\mathsf{sCDH}}^1$ and $\mathcal{L}_{\mathsf{H}_1}$, which are initialized to $\emptyset$.
2) When the adversary $\mathcal{A}$ queries $\textsc{Setup}$ and $\textsc{Execute}$ oracles such that the challenger $\mathcal{C}$ needs to run $\mathsf{encapsulate}_1(pk')$ of a stateful Pin/Uv Auth Protocol $\mathsf{puvProtocol}_1$, $\mathcal{C}$ first looks up whether there exists a value $\tilde{K}$ such that $(pk', \mathsf{puvProtocol}_1.pk, \tilde{K}) \in \mathcal{L}_{\mathsf{sCDH}}^1$.
   If such value does not exist, $\mathcal{C}$ then checks for all $(u, v) \in \mathcal{L}_{\mathsf{H}_1}$ such that u is the x-coordinate of any ECDH point P whether $(pk')^{\mathsf{puvProtocol}_1.sk} = P$. If any such check succeeds, the challenger sets $\tilde{K} \leftarrow v$ and adds $(pk', \mathsf{puvProtocol}_1.pk, \tilde{K})$ into list $\mathcal{L}_{\mathsf{sCDH}}^1$.
   Otherwise, $\mathcal{C}$ simply samples $\tilde{K} \xleftarrow{\$} \{0,1\}^{l_1}$ uniformly at random and adds $(pk', \mathsf{puvProtocol}_1.pk, \tilde{K})$ into list $\mathcal{L}_{\mathsf{sCDH}}^1$.
   Finally, the challenger replaces the computation of Line 133 and Line 134 in Figure 13 by
   $$K \leftarrow \tilde{K}$$
3) When the adversary $\mathcal{A}$ queries $\textsc{Setup}$ and $\textsc{Send-Bind-T}$ oracles such that the challenger $\mathcal{C}$ needs to run $\mathsf{decapsulate}_1(c)$ of a stateful Pin/Uv Auth Protocol $\mathsf{puvProtocol}_1$, $\mathcal{C}$ first looks up whether there exists a value $\tilde{K}$ such that $(\mathsf{puvProtocol}_1.pk, c, \tilde{K}) \in \mathcal{L}_{\mathsf{sCDH}}^1$.
   If such value does not exist, $\mathcal{C}$ then checks for all $(u, v) \in \mathcal{L}_{\mathsf{H}_1}$ such that u is the x-coordinate of any ECDH point P whether $c^{\mathsf{puvProtocol}_1.sk} = P$. If any such check succeeds, the challenger sets $\tilde{K} \leftarrow v$ and adds $(\mathsf{puvProtocol}_1.pk, c, \tilde{K})$ into list $\mathcal{L}_{\mathsf{sCDH}}^1$.
   Otherwise, $\mathcal{C}$ simply samples $\tilde{K} \xleftarrow{\$} \{0,1\}^{l_1}$ uniformly at random and adds $(\mathsf{puvProtocol}_1.pk, c, \tilde{K})$ into list $\mathcal{L}_{\mathsf{sCDH}}^1$.
   Finally, the challenger replaces the computation of Line 136 and Line 137 in Figure 13 by
   $$K \leftarrow \tilde{K}$$
4) Whenever the adversary $\mathcal{A}$ queries random oracle H_1 with input u and the random oracle outputs v, the challenger adds (u, v) into $\mathcal{L}_{\mathsf{H}_1}$.

We compute the probability that the adversary $\mathcal{A}$ can distinguish **Game 0** and **Game 1** by $n_{1,1}$ hybrid games, where $n_{1,1}$ denotes the number of ECDH public keys that underlie the stateful Pin/Uv Auth Protocol $\mathsf{puvProtocol}_1$ of any token and are sent to the adversary $\mathcal{A}$. Let $(pk_{\mathsf{token}}^y, sk_{\mathsf{token}}^y)$ denote the y-th ECDH key pair that are sampled by the underlying stateful Pin/Uv Auth Protocol $\mathsf{puvProtocol}_1$ of any token and are sent to the adversary $\mathcal{A}$ for $y \in [n_{1,1}]$. Recall that the same ECDH key pairs of tokens might be repeatedly used by different sessions and the adversary knows the public keys of each token's or client's session only by querying $\textsc{Setup}$ and $\textsc{Execute}$ oracles. Each hybrid game $\mathsf{hy}.y$ for $y \in [n_{1,1}]$ is simulated as following:

Game $\mathsf{hy}.0$**.** This game is identical to **Game 0** except that at the beginning of this game the challenger $\mathcal{C}$ sets up two lists $\mathcal{L}_{\mathsf{sCDH}}^1$ and $\mathcal{L}_{\mathsf{H}_1}$, which are initialized to $\emptyset$. Whenever the adversary $\mathcal{A}$ queries random oracle H_1 with input u and the random oracle outputs v, the challenger adds (u, v) into $\mathcal{L}_{\mathsf{H}_1}$.

The list $\mathcal{L}^1_{\mathsf{sCDH}}$ is never used. This is indeed the modification 1 and 4 in **Game 1**. Obviously, **Game 0** and **Game** hy.0 are identical from the adversary's view, and we have:

$$\mathsf{Adv}_0 = \mathsf{Adv}_{\mathsf{hy}.0}$$

Game hy.y**.** This game is identical to **Game** hy.(y-1) except the following modifications:

1) When $\mathcal{A}$ sends any query SETUP or EXECUTE on input (T, i, C, j, U) such that the underlying Pin/Uv Auth Protocol protocol of session π^i_T is a $\mathsf{puvProtocol}_1$ with $(pk_{T,i}, sk_{T,i}) = (pk^y_{\mathsf{token}}, sk^y_{\mathsf{token}})$, the challenger has to execute $\mathsf{encapsulate}_1(pk_{T,i})$. Instead of invoking $\mathsf{encapsulate}_1(pk_{T,i})$ directly, $\mathcal{C}$ first looks up whether there exists a value $\tilde{K}$ such that $(pk_{T,i}, pk_{C,j}, \tilde{K}) \in \mathcal{L}^1_{\mathsf{sCDH}}$.
If such value does not exist, $\mathcal{C}$ then checks for all $(u, v) \in \mathcal{L}_{\mathsf{H}_1}$ such that u is the x-coordinate of any ECDH point P whether $pk_{C,j}^{sk^y_{\mathsf{token}}} = P$. If any such check succeeds, the challenger sets $\tilde{K} \leftarrow v$ and adds $(pk_{T,i}, pk_{C,j}, \tilde{K})$ into list $\mathcal{L}^1_{\mathsf{sCDH}}$.
Otherwise, $\mathcal{C}$ simply samples $\tilde{K} \xleftarrow{\$} \{0,1\}^{l_1}$ uniformly at random and adds $(pk_{T,i}, pk_{C,j}, \tilde{K})$ into list $\mathcal{L}^1_{\mathsf{sCDH}}$.
Finally, the challenger replaces the computation of Line 133 and Line 134 in Figure 13 by
$$K \leftarrow \tilde{K}$$

2) When $\mathcal{A}$ sends the query SEND-BIND-T on input (T, i, m) such that $(pk_{T,i}, sk_{T,i}) = (pk^y_{\mathsf{token}}, sk^y_{\mathsf{token}})$ and that $m = c \parallel c_{ph}$, the challenger first checks whether there exists a value $\tilde{K}$ such that $(pk_{T,i}, c, \tilde{K}) \in \mathcal{L}^1_{\mathsf{sCDH}}$.
If such value does not exist, $\mathcal{C}$ then checks for all $(u, v) \in \mathcal{L}_{\mathsf{H}_1}$ such that u is the x-coordinate of any ECDH point P whether $c = P$. If any such check succeeds, the challenger sets $\tilde{K} \leftarrow v$ and adds $(pk_{T,i}, c, \tilde{K})$ into list $\mathcal{L}^1_{\mathsf{sCDH}}$.
Otherwise, $\mathcal{C}$ simply samples $\tilde{K} \xleftarrow{\$} \{0,1\}^{l_1}$ uniformly at random and adds $(pk_{T,i}, c, \tilde{K})$ into list $\mathcal{L}^1_{\mathsf{sCDH}}$.
Finally, the challenger $\mathcal{C}$ is supposed to execute $\mathsf{decapsulate}_1(c)$. Instead of invoking $\mathsf{decapsulate}_1(c)$ directly, $\mathcal{C}$ replaces the computation of Line 136 and Line 137 in Figure 13 by
$$K \leftarrow \tilde{K}$$

Let event E_1 denote the probability that the adversary $\mathcal{A}$ can distinguish **Game** hy.(y-1) and **Game** hy.y. Note that the modifications between every two adjacent hybrid games are independent. It holds that

$$\mathsf{Adv}_{\mathsf{hy}.(y\text{-}1)} - \mathsf{Adv}_{\mathsf{hy}.y} \leq \Pr[E_1], \forall y \in [n_{1,1}]$$

Then, we analyze the probability of the occurrence of E_1 by reduction. Namely, if E_1 occurs, then we can construct an adversary $\mathcal{B}_1$ that breaks sCDH assumption over ECDH by invoking $\mathcal{A}$. On inputs $(\mathsf{ECDH}, A = g^a, B = g^b)$, $\mathcal{B}_1$ sets the y-th ECDH public key pk^y_{token} among all ECDH public key underlying any $\mathsf{puvProtocol}_1$ of all tokens to be $A = g^a$. Then, $\mathcal{B}_1$ simulates **Game** hy.(y-1) honestly, except the following modifications:

1) When $\mathcal{A}$ sends $\mathcal{B}_1$ the w-th query SETUP or EXECUTE on input (T, i, C, j, U) for $w \geq 1$ such that $pk_{T,i}$ is supposed to be pk^y_{token}, $\mathcal{B}_1$ first samples $r_w \leftarrow \mathbb{Z}_q$, where q is the prime order of the the underlying cyclic group of ECDH and sets $pk_{C,j} \leftarrow B \cdot g^{r_w} = g^{b+r_w}$ in the $\mathsf{obtainSharedSecret}$-$C$-end algorithms. Next, when $\mathcal{B}_1$ needs to run $\mathsf{encapsulate}_1(pk_{T,i})$ algorithm in $\mathsf{obtainSharedSecret}$-$C$-end algorithm, $\mathcal{B}_1$ first looks up whether there exists a value $\tilde{K}$ such that $(pk_{T,i}, pk_{C,j}, \tilde{K}) \in \mathcal{L}^1_{\mathsf{sCDH}}$.
If such value does not exist, for all $(u, v) \in \mathcal{L}_{\mathsf{H}_1}$ such that u is the x-coordinate of any ECDH point P, $\mathcal{B}_1$ queries its $\mathcal{O}_a$ oracle on $(pk_{C,j}, P)$. If any response is true, the challenger sets $\tilde{K} \leftarrow v$ and adds $(pk_{T,i}, pk_{C,j}, \tilde{K})$ into list $\mathcal{L}^1_{\mathsf{sCDH}}$.
Otherwise, $\mathcal{B}_1$ simply samples $\tilde{K} \xleftarrow{\$} \{0,1\}^{l_1}$ uniformly at random and adds $(pk_{T,i}, pk_{C,j}, \tilde{K})$ into list $\mathcal{L}^1_{\mathsf{sCDH}}$.
Finally, $\mathcal{B}_1$ honestly performs the remaining execution except replacing the computation of Line 133 and Line 134 in Figure 13 by
$$K \leftarrow \tilde{K}$$

2) When $\mathcal{A}$ sends the query SEND-BIND-T on input (T, i, m) such that $pk_{T,i} = A = g^a$ and $m = c \parallel c_{ph}$, $\mathcal{B}_1$ first checks whether there exists a value $\tilde{K}$ such that $(pk_{T',i'}, c, \tilde{K}) \in \mathcal{L}^1_{\mathsf{sCDH}}$.
If such value does not exist, for each tuple $(u, v) \in \mathcal{L}_{\mathsf{H}_1}$ such that u is the x-coordinate of any point P on ECDH, $\mathcal{B}_1$ queries $\mathcal{O}_a$ to its challenger on input (c, P). If any response from the challenger is true, $\mathcal{B}_1$ uses the corresponding value v as the hash H_1 of x-coordinate of the Diffie-Hellman exchange of $pk_{T,i}$ and c for the subsequent computation.
If no response from the challenger is true, this means, c_{ph} is a random ciphertext that is produced by $\mathcal{A}$ without knowing the correct symmetric key K. $\mathcal{B}_1$ simply samples $\tilde{K} \xleftarrow{\$} \{0,1\}^{l_1}$ uniformly at random and adds $(pk_{T,i}, c, \tilde{K})$ into list $\mathcal{L}^1_{\mathsf{sCDH}}$.
Finally, $\mathcal{B}_1$ simply uses $\tilde{K}$ as the hash H_1 of x-coordinate of the Diffie-Hellman exchange of $pk_{T,i}$ and c for the subsequent computation.

3) Finally, $\mathcal{A}$ terminates at some point and is expected to distinguish **Game** hy.(y-1) from **Game** hy.y. For all $(u, v) \in \mathcal{L}_{\mathsf{H}_1}$ such that u is the x-coordinate of some ECDH point P and all r_w sampled above, $\mathcal{B}_1$ queries $\mathcal{O}_a(B \cdot g^{r_w}, P)$ to its challenger. If any response is true, $\mathcal{B}_1$ returns $P \cdot A^{-r_w}$ to its challenger. Otherwise, $\mathcal{B}_1$ outputs a random cyclic group element on ECDH.

Obviously, $\mathcal{B}_1$ simulates **Game** hy.(y-1) and **Game** hy.y to $\mathcal{A}$ perfectly. From the adversary $\mathcal{A}$'s view, the only difference between **Game** hy.(y-1) and **Game** hy.y is whether the key $\tilde{K}$ is computed from the hash H_1 of the x-coordinate of the real Diffie-Hellman exchange or sampled uniformly at random. If $\mathcal{A}$ can distinguish **Game** hy.(y-1) from **Game** hy.y effectively, $\mathcal{A}$ must have queried the x-coordinate of the real Diffie-Hellman exchange of A and $B \cdot g^{r_w}$ to the random oracle H_1 for some w. This means, $\mathcal{B}_1$ can always return $P \cdot A^{-r_w} = (B \cdot g^{r_w})^a \cdot A^{-r_w} = g^{ab+ar_w-ar_w} = g^{ab}$ to its challenger. Thus, it holds that

$$\Pr[E_1] \leq \epsilon^{\mathsf{sCDH}}_{\mathsf{ECDH}}$$

Furthermore, **Game** $\mathsf{hy}.n_{1,1}$ have replaced all shared symmetric key K produced by honest clients in $\mathsf{encapsulate}_1$ algorithm with a random key $\tilde{K}$. Thus, **Game** $\mathsf{hy}.n_{1,1}$ is identical to **Game 1** and we have:

$$\mathsf{Adv}_1 = \mathsf{Adv}_{\mathsf{hy}.n_{1,1}}$$

Combing the statements above, we have that

$$\mathsf{Adv}_0 - \mathsf{Adv}_1 \leq n_{1,1}\epsilon^{\mathsf{sCDH}}_{\mathsf{ECDH}}$$

For now, we continue to use the term $n_{1,1}$ and will reduce it in the subsequent games.

Game 2. This game is identical **Game 1** except that the challenger $\mathcal{C}$ aborts the simulation and let $\mathcal{A}$ immediately win if there exists collision between $\tilde{K}$ sampled in **Game 1**. Recall that $\tilde{K}$s are sampled at most $n_{1,1}$ times. Note that the collision happens between every two keys with probability at most 2^{-l_1} and that there exists at most $\binom{n_{1,1}}{2}$ pairs. We have that

$$\mathsf{Adv}_1 - \mathsf{Adv}_2 \leq \binom{n_{1,1}}{2} 2^{-l_1}$$

Game 3. This game is identical to **Game 2** except the following modifications:

1) At the beginning of this game, the challenger $\mathcal{C}$ sets up two lists $\mathcal{L}^2_{\mathsf{sCDH}}$ and $\mathcal{L}_{\mathsf{H}_3}$, which are initialized to $\emptyset$.
2) When the adversary $\mathcal{A}$ queries SETUP and EXECUTE oracles such that the challenger $\mathcal{C}$ needs to run $\mathsf{encapsulate}_2(pk')$ of a stateful Pin/Uv Auth Protocol $\mathsf{puvProtocol}_2$, $\mathcal{C}$ first looks up whether there exists values $\tilde{K}_1$ and $\tilde{K}_2$ such that $(pk', \mathsf{puvProtocol}_2.pk, \tilde{K}_1, \tilde{K}_2) \in \mathcal{L}^2_{\mathsf{sCDH}}$.
   If such value does not exist, $\mathcal{C}$ then checks for all $((u,u'),v) \in \mathcal{L}_{\mathsf{H}_3}$ such that u is the x-coordinate of any ECDH point P and $u' \in$ {"CTAP2 HMAC key", "CTAP2 AES key"} whether $(pk')^{\mathsf{puvProtocol}_2.sk} = P$. If any such check succeeds, the challenger queries random oracle H_3 and sets $\tilde{K}_1 \leftarrow \mathsf{H}_3(u,$"CTAP2 HMAC key"$)$ and $\tilde{K}_2 \leftarrow \mathsf{H}_3(u,$"CTAP2 AES key"$)$ and adds $(pk', \mathsf{puvProtocol}_2.pk, \tilde{K}_1, \tilde{K}_2)$ into list $\mathcal{L}^2_{\mathsf{sCDH}}$.
   Otherwise, $\mathcal{C}$ simply samples $\tilde{K}_1, \tilde{K}_2 \xleftarrow{\$} \{0,1\}^{l_3}$ uniformly at random and adds $(pk', \mathsf{puvProtocol}_2.pk, \tilde{K}_1, \tilde{K}_2)$ into list $\mathcal{L}^2_{\mathsf{sCDH}}$.
   Finally, the challenger replaces the computation of Line 152-154 in Figure 14 by
   $$K_1 \leftarrow \tilde{K}_1, K_2 \leftarrow \tilde{K}_2$$
3) When the adversary $\mathcal{A}$ queries SETUP and SEND-BIND-T oracles such that the challenger $\mathcal{C}$ needs to run $\mathsf{decapsulate}_2(c)$ of a stateful Pin/Uv Auth Protocol $\mathsf{puvProtocol}_2$, $\mathcal{C}$ first looks up whether there exists values $\tilde{K}_1$ and $\tilde{K}_2$ such that $(\mathsf{puvProtocol}_2.pk, c, \tilde{K}_1, \tilde{K}_2) \in \mathcal{L}^2_{\mathsf{sCDH}}$.
   If such value does not exist, $\mathcal{C}$ then checks for all $((u,u'),v) \in \mathcal{L}_{\mathsf{H}_3}$ such that u is the x-coordinate of any ECDH point P and $u' \in$ {"CTAP2 HMAC key", "CTAP2 AES key"} whether $c^{\mathsf{puvProtocol}_2.sk} = P$. If any such check succeeds, the challenger queries random oracle H_3 and sets $\tilde{K}_1 \leftarrow \mathsf{H}_3(u,$"CTAP2 HMAC key"$)$ and $\tilde{K}_2 \leftarrow \mathsf{H}_3(u,$"CTAP2 AES key"$)$ and adds $(pk', \mathsf{puvProtocol}_2.pk, \tilde{K}_1, \tilde{K}_2)$ into list $\mathcal{L}^2_{\mathsf{sCDH}}$.
   Otherwise, $\mathcal{C}$ simply samples $\tilde{K}_1, \tilde{K}_2 \xleftarrow{\$} \{0,1\}^{l_3}$ uniformly at random and adds $(\mathsf{puvProtocol}_2.pk, c, \tilde{K}_1, \tilde{K}_2) \in \mathcal{L}^2_{\mathsf{sCDH}}$ into list $\mathcal{L}^2_{\mathsf{sCDH}}$.
   Finally, the challenger replaces the computation of Line 158-160 in Figure 14 by
   $$K_1 \leftarrow \tilde{K}_1, K_2 \leftarrow \tilde{K}_2$$
4) Whenever the adversary $\mathcal{A}$ queries random oracle H_3 with input u and the random oracle outputs v, the challenger adds (u, v) into $\mathcal{L}_{\mathsf{H}_3}$.

Similar to **Game 1**, we can compute the probability that the adversary $\mathcal{A}$ can distinguish **Game 2** and **Game 3** by $n_{1,2}$ hybrid games, where $n_{1,2}$ denotes the number of ECDH public keys that underlie the stateful Pin/Uv Auth Protocol $\mathsf{puvProtocol}_2$ of any token and are sent to the adversary $\mathcal{A}$. Thus, we can easily have that

$$\mathsf{Adv}_2 - \mathsf{Adv}_3 \leq n_{1,2}\epsilon^{\mathsf{sCDH}}_{\mathsf{ECDH}}$$

Game 4. This game is identical **Game 3** except that the challenger $\mathcal{C}$ aborts the simulation and let $\mathcal{A}$ immediately win if there exists collision between $\tilde{K}_1$ or collision between $\tilde{K}_2$ sampled in **Game 3**. Recall that $\tilde{K}_1$s and $\tilde{K}_2$ both are sampled at most $n_{1,2}$ times. Note that the collision happens between every two keys with probability at most 2^{-l_3} and that there exists at most $\binom{n_{1,2}}{2}$ pairs. We have that

$$\mathsf{Adv}_3 - \mathsf{Adv}_4 \leq 2\binom{n_{1,2}}{2}2^{-l_3} = \binom{n_{1,2}}{2}2^{-l_3+1}$$

Game 5. This game is identical to **Game 4** except the following modifications:

1) At the beginning of this game, the challenger $\mathcal{C}$ sets up two lists $\mathcal{L}^3_{\mathsf{sCDH}}$ and $\mathcal{L}_{\mathsf{H}_5}$, which are initialized to $\emptyset$.
2) When the adversary $\mathcal{A}$ queries SETUP and EXECUTE oracles such that the challenger $\mathcal{C}$ needs to run $\mathsf{encapsulate}_3(pk')$ of a stateful Pin/Uv Auth Protocol $\mathsf{puvProtocol}_3$, where $pk' = (pk'_1, pk'_2)$, $\mathcal{C}$ first executes $(c_2, Z_2) \leftarrow \mathsf{KEM.Encaps}(pk'_2)$ and looks up whether there exists a value $\tilde{Z}$ such that $(pk'_1, \mathsf{puvProtocol}_3.pk_1, Z_2, \tilde{Z}) \in \mathcal{L}^3_{\mathsf{sCDH}}$.
   If such value does not exist, $\mathcal{C}$ then checks for all $((u,u'),v) \in \mathcal{L}_{\mathsf{H}_5}$ such that u is the x-coordinate of any ECDH point P and $u' = Z_2$ whether $(pk'_1)^{\mathsf{puvProtocol}_3.sk_1} = P$. If any such check succeeds, the challenger sets $\tilde{Z} \leftarrow v$ and adds $(pk'_1, \mathsf{puvProtocol}_3.pk_1, Z_2, \tilde{Z})$ into list $\mathcal{L}^3_{\mathsf{sCDH}}$.
   Otherwise, $\mathcal{C}$ simply samples $\tilde{Z} \xleftarrow{\$} \{0,1\}^{l_5}$ uniformly at random and adds $(pk'_1, \mathsf{puvProtocol}_3.pk_1, Z_2, \tilde{Z})$ into list $\mathcal{L}^3_{\mathsf{sCDH}}$.

Finally, the challenger replaces the computation of Line 44-46 in Figure 5 by

$$Z \leftarrow \tilde{Z}$$

3) When the adversary $\mathcal{A}$ queries SETUP and SEND-BIND-T oracles such that the challenger $\mathcal{C}$ needs to run $\mathsf{decapsulate}_3(c)$ of a stateful Pin/Uv Auth Protocol $\mathsf{puvProtocol}_3$, where $c = (c_1, c_2)$, $\mathcal{C}$ first executes $Z_2 \leftarrow \mathsf{KEM.Decaps}(\mathsf{puvProtocol}_3.sk_2, c_2)$ and looks up whether there exists a value $\tilde{Z}$ such that $(\mathsf{puvProtocol}_3.pk_1, c_1, Z_2, \tilde{Z}) \in \mathcal{L}^3_{\mathsf{sCDH}}$.
If such value does not exist, $\mathcal{C}$ then checks for all $((u, u'), v) \in \mathcal{L}_{\mathsf{H}_5}$ such that u is the x-coordinate of any ECDH point P and $u' = Z_2$ whether $(c_1)^{\mathsf{puvProtocol}_3.sk_1} = P$.
If any such check succeeds, the challenger sets $\tilde{Z} \leftarrow v$ and adds $(\mathsf{puvProtocol}_3.pk_1, c_1, Z_2, \tilde{Z})$ into list $\mathcal{L}^3_{\mathsf{sCDH}}$.
Otherwise, $\mathcal{C}$ simply samples $\tilde{Z} \xleftarrow{\$} \{0,1\}^{l_5}$ uniformly at random and adds $(\mathsf{puvProtocol}_3.pk_1, c_1, Z_2, \tilde{Z})$ into list $\mathcal{L}^3_{\mathsf{sCDH}}$.
Finally, the challenger replaces the computation of Line 54-56 in Figure 5 by

$$Z \leftarrow \tilde{Z}$$

4) Whenever the adversary $\mathcal{A}$ queries random oracle H_5 with input u and the random oracle outputs v, the challenger adds (u, v) into $\mathcal{L}_{\mathsf{H}_5}$.

Similar to **Game 1**, we can compute the probability that the adversary $\mathcal{A}$ can distinguish **Game 4** and **Game 5** by $n_{1,3}$ hybrid games, where $n_{1,3}$ denotes the number of ECDH public keys that underlie the stateful Pin/Uv Auth Protocol $\mathsf{puvProtocol}_3$ of any token and are sent to the adversary $\mathcal{A}$. Thus, we can easily have that

$$\mathsf{Adv}_4 - \mathsf{Adv}_5 \le n_{1,3}\epsilon^{\mathsf{sCDH}}_{\mathsf{ECDH}}$$

Game 6. This game is identical **Game 5** except that the challenger $\mathcal{C}$ aborts the simulation and let $\mathcal{A}$ immediately win if there exists collision between $\tilde{Z}$ sampled in **Game 5**. Recall that $\tilde{Z}$s are sampled (either uniformly at random or from the random oracle) at most $n_{1,3}$ times. Note that the collision happens between every two keys with probability at most 2^{-l_5} and that there exist at most $\binom{n_{1,3}}{2}$ pairs. We have that

$$\mathsf{Adv}_5 - \mathsf{Adv}_6 \le \binom{n_{1,3}}{2} 2^{-l_5}$$

Game 7. This game is identical **Game 6** except that the challenger $\mathcal{C}$ aborts the simulation and let $\mathcal{A}$ immediately win if there exists collision between K_1s or collision between K_2s derived in $\mathsf{encapsulate}_3$. Recall that K_1s and K_2s both are produced by $\mathsf{H}_6(\tilde{Z}, \text{“CTAP2 HMAC key”})$ in $\mathsf{encapsulate}_3$ at most $n_{1,3}$ times and that $\tilde{Z}$s are assumed to be distinct from each other in **Game 6**. Note that the collision happens between every two keys with probability at most 2^{-l_6} and that there exists at most $\binom{n_{1,3}}{2}$ pairs. We have that

$$\mathsf{Adv}_6 - \mathsf{Adv}_7 \le 2\binom{n_{1,3}}{2} 2^{-l_6} = \binom{n_{1,3}}{2} 2^{-l_6+1}$$

Recall that the honest public keys of tokens (resp. the ones of clients) used in the $\mathsf{encapsulate}_i$ and $\mathsf{decapsulate}_i$ for $i \in \{1,2,3\}$ are sent to adversary $\mathcal{A}$ in $\mathsf{obtainSharedSecret}\text{-}T$ (resp. $\mathsf{obtainSharedSecret}\text{-}C\text{-end}$) algorithm only when answering the SETUP and EXECUTE oracles. So, we have that $n_{1,1} + n_{1,2} + n_{1,3} \le q_{\text{SETUP}} + q_{\text{EXECUTE}}$.

Merging the statements above, we can state the upper bound as:

$$\begin{aligned}
&\mathsf{Adv}_0 - \mathsf{Adv}_7 \\
\le& (n_{1,1} + n_{1,2} + n_{1,3})\epsilon^{\mathsf{sCDH}}_{\mathsf{ECDH}} + \binom{n_{1,1}}{2} 2^{-l_1} + \binom{n_{1,2}}{2} 2^{-l_3+1} \\
&+ \binom{n_{1,3}}{2}(2^{-l_5} + 2^{-l_6+1}) \\
\le& (q_{\text{SETUP}} + q_{\text{EXECUTE}})\epsilon^{\mathsf{sCDH}}_{\mathsf{ECDH}} \\
&\quad + \binom{q_{\text{SETUP}} + q_{\text{EXECUTE}}}{2} 2^{2-\min\{l_1,l_3,l_5,l_6\}}
\end{aligned}$$

Game 8. In this game, the challenger $\mathcal{C}$ aborts the game and lets the adversary $\mathcal{A}$ immediately win if there exist two inputs pin and pin' during $\mathcal{C}$'s execution such that $\mathsf{H}(\mathsf{pin}) = \mathsf{H}(\mathsf{pin}')$. This violates the collision resistance of H by definition. Since H is assumed to be $\epsilon^{\mathsf{coll\text{-}res}}_{\mathsf{H}}$-collision resistant, we have that

$$\mathsf{Adv}_7 - \mathsf{Adv}_8 \le \epsilon^{\mathsf{coll\text{-}res}}_{\mathsf{H}}$$

Game 9. In this game, the challenger $\mathcal{C}$ aborts the game and lets the adversary $\mathcal{A}$ immediately win if the challenger honestly samples two identical ECDH public keys of tokens or of clients and sends them to the adversary. Recall that each sampled ECDH public keys are sent to the adversary only in SETUP or EXECUTE oracles. And one newly sampled ECDH keys of tokens and one of clients are sent to the adversary in both SETUP and EXECUTE queries. In total, there are at most $(q_{\text{SETUP}} + q_{\text{EXECUTE}})$ ECDH public keys of tokens and $(q_{\text{SETUP}} + q_{\text{EXECUTE}})$ ECDH public keys of clients. Note that the collision happens between every two public keys with probability at most 2^{-q}, where q denote the prime order of the underlying ECDH group, and that there exist at most $\binom{q_{\text{SETUP}}+q_{\text{EXECUTE}}}{2}$ pairs of tokens (resp. of clients). We have that

$$\begin{aligned}
\mathsf{Adv}_8 - \mathsf{Adv}_9 &\le 2\binom{(q_{\text{SETUP}} + q_{\text{EXECUTE}})}{2} 2^{-q} \\
&\le \binom{(q_{\text{SETUP}} + q_{\text{EXECUTE}})}{2} 2^{1-q}
\end{aligned}$$

Game 10. This game is identical to **Game 9** except that the following modifications:

1) The challenger $\mathcal{C}$ samples a random $\tilde{\mathsf{pin}} \xleftarrow{\$} \mathfrak{D}$ at the beginning of the game but never uses it. The challenger aborts and lets $\mathcal{A}$ immediately win if $\tilde{\mathsf{pin}}$ collides with any user pin pin_U for any user U.
2) Whenever the adversary $\mathcal{A}$ queries oracle SETUP inputting any (T, i, C, j, U), the challenger replaces $\mathsf{pin} \leftarrow \mathsf{st}_T.\mathsf{puvProtocol.decrypt}(K, c_p)$ in the $\mathsf{setPIN}\text{-}T$ algorithm by

$$\mathsf{pin} \leftarrow \mathsf{pin}_U$$

3) The challenger aborts the game and lets $\mathcal{A}$ immediately win if there exits a collision between pts used in SEND-BIND-T oracles.

Note that the Setup phase is assumed to be authenticated. The user U's pin pin_U, which was encrypted by the client, can always be decrypted by the token.

Moreover, note that the adversary can query NEWU at most q_{NEWU} times and each user pin is sampled from distribution $\mathfrak{D}$ with min-entropy $\alpha_{\mathfrak{D}}$. The probability that $\tilde{\mathsf{pin}}$ collides with any other user pin pin_U is bounded by $q_{\mathrm{NEWU}} 2^{-\alpha_{\mathfrak{D}}}$.

Furthermore, note that the pts are random strings of length $\mu\lambda, 2\lambda, \mu'\lambda$ respectively in $\mathsf{puvProtocol}_1$, $\mathsf{puvProtocol}_2$, and $\mathsf{puvProtocol}_3$. Note also that pts are used only in SEND-BIND-T oracles. The collision between pts happens with probability at most $\binom{q_{\text{SEND-BIND-T}}}{2} 2^{-\min\{\mu,2,\mu'\}\lambda}$.

So, we have that

$$\mathsf{Adv}_9 - \mathsf{Adv}_{10} \le q_{\mathrm{NEWU}} 2^{-\alpha_{\mathfrak{D}}} + \binom{q_{\text{SEND-BIND-T}}}{2} 2^{-\min\{\mu,2,\mu'\}\lambda}$$

Game 11. This games is identical to **Game 10** except the following modification:

1) Whenever $\mathcal{A}$ queries SETUP(T, i, C, j, U) and the challenger sets the selected Pin/Uv Auth Protocol of the client session π_C^j to be $\pi_C^j.\mathsf{selectedpuvProtocol} = \mathsf{puvProtocol}_1$ during the execution, the challenger replaces $c_p = \mathsf{SKE}_1.\mathsf{Enc}(\tilde{K}, \mathsf{pin}_U)$ in the $\mathsf{setPIN}\text{-}C(\pi_C^j, \mathsf{pin}_U)$ by $\tilde{c}_p \leftarrow \mathsf{SKE}_1.\mathsf{Enc}(\tilde{K}, \tilde{\mathsf{pin}})$, where $\tilde{\mathsf{pin}}$ was sampled in **Game 10**.

We prove that **Game 10** and **Game 11** are indistinguishable from $\mathcal{A}$'s view by $n_{2,1}$ hybrid games, where $n_{2,1}$ denotes the number of $\tilde{K}$ sampled in SETUP oracle when the underlying Pin/Uv Auth Protocol is $\mathsf{puvProtocol}_1$. Let $\tilde{K}^y$ denotes the y-th $\tilde{K}$ sampled by the challenger $\mathcal{C}$ in SETUP oracle when the underlying Pin/Uv Auth Protocol is $\mathsf{puvProtocol}_1$. The hybrid game $\mathsf{hy}.y$ for $y \in [n_{2,1}]$ is defined below.

Game $\mathsf{hy}.0$**.** This game is identical to **Game 10** and we have that:

$$\mathsf{Adv}_{10} = \mathsf{Adv}_{\mathsf{hy}.0}$$

Game $\mathsf{hy}.y$**.** This game is identical to **Game** $\mathsf{hy}.(y\text{-}1)$ except the following modifications:

1) When $\mathcal{A}$ queries SETUP(T, i, C, j, U) and that will produce the y-th $\tilde{K}^y$ during the game, the challenger replaces $c_p = \mathsf{SKE}_1.\mathsf{Enc}(\tilde{K}^y, \mathsf{pin}_U)$ in the $\mathsf{setPIN}\text{-}C(\pi_C^j, \mathsf{pin}_U)$ by $\tilde{c}_p \leftarrow \mathsf{SKE}_1.\mathsf{Enc}(\tilde{K}^y, \tilde{\mathsf{pin}})$.

Let event E_2 denote the probability that the adversary $\mathcal{A}$ can distinguish **Game** $\mathsf{hy}.(y\text{-}1)$ and **Game** $\mathsf{hy}.y$. Note that the modifications between every two adjacent hybrid games are independent. It holds that

$$\mathsf{Adv}_{\mathsf{hy}.(y\text{-}1)} - \mathsf{Adv}_{\mathsf{hy}.y} \le \Pr[E_2], \forall y \in [n_{2,1}]$$

Then, we analyze the probability of the occurrence of E_2 by reduction. Namely, if E_2 occurs, then we can construct an adversary $\mathcal{B}_2$ that breaks IND-1CPA-H_2 security of SKE_1 by invoking $\mathcal{A}$. $\mathcal{B}_2$ simulates **Game** $\mathsf{hy}.(y\text{-}1)$ honestly, except for the query to the SETUP(T, i, C, j, U) that will produce the y-th $\tilde{K}^y$ during the game. To handle this query, $\mathcal{B}_2$ executes following step:

1) $\mathcal{B}_2$ sends $(\mathsf{pin}_U, \tilde{\mathsf{pin}})$ to its challenger and obtains (c, t). Then, $\mathcal{B}_2$ sets (c, t) as the output of $\mathsf{setPIN}\text{-}C(\pi_C^j, \mathsf{pin}_U)$ algorithm.

Note that we have ensured that all sampled ECDH public keys are distinct in **Game 9** and that all sampled $\tilde{K}$s in $\mathcal{L}^1_{\mathsf{sCDH}}$ are distinct in **Game 2**. It's easy to observe that $\mathcal{B}_2$ perfectly simulates **Game** $\mathsf{hy}.(y\text{-}1)$ or **Game** $\mathsf{hy}.y$. Moreover, $\mathcal{B}_2$ simulates **Game** $\mathsf{hy}.(y\text{-}1)$ if $(c, t) = (\mathsf{SKE}_1.\mathsf{Enc}(\tilde{K}^y, \mathsf{pin}_U), \mathsf{H}_2(\tilde{K}^y, c))$ and **Game** $\mathsf{hy}.y$ if $(c, t) = (\mathsf{SKE}_1.\mathsf{Enc}(\tilde{K}^y, \tilde{\mathsf{pin}}), \mathsf{H}_2(\tilde{K}^y, c))$. Thus, $\mathcal{B}_2$ can win IND-1CPA-H_2 experiment whenever $\mathcal{A}$ can distinguish **Game** $\mathsf{hy}.(y\text{-}1)$ and **Game** $\mathsf{hy}.y$. Thus, we have that

$$\Pr[E_2] \le \epsilon^{\mathsf{ind\text{-}1cpa\text{-}H_2}}_{\mathsf{SKE}_1}$$

Moreover, **Game** $\mathsf{hy}.n_{2,1}$ have replaced all c_p in the SETUP oracles whenever the client chooses $\mathsf{puvProtocol}_1$. Thus, **Game** $\mathsf{hy}.n_{2,1}$ is identical to **Game 11** and we have

$$\mathsf{Adv}_{11} = \mathsf{Adv}_{\mathsf{hy}.n_{2,1}}$$

Note that all hybrid games are independent. Combing the statements above, we have that

$$\mathsf{Adv}_{10} - \mathsf{Adv}_{11} \le n_{2,1} \epsilon^{\mathsf{ind\text{-}1cpa\text{-}H_2}}_{\mathsf{SKE}_1}$$

Here, we simply keep using the number $n_{2,1}$, which would be helpful for us to tighten our security upper bound in the following games.

Game 12. This games is identical to **Game 11** except the following modification:

1) When $\mathcal{A}$ queries SETUP(T, i, C, j, U), where pin_U is not corrupted, and the challenger sets the selected Pin/Uv Auth Protocol of the client session π_C^j to be $\pi_C^j.\mathsf{selectedpuvProtocol} = \mathsf{puvProtocol}_2$ during the execution, the challenger replaces $c_p = \mathsf{SKE}_2.\mathsf{Enc}(\tilde{K}_2, \mathsf{pin}_U)$ in the $\mathsf{setPIN}\text{-}C(\pi_C^j, \mathsf{pin}_U)$ by $\tilde{c}_p \leftarrow \mathsf{SKE}_2.\mathsf{Enc}(\tilde{K}_2, \tilde{\mathsf{pin}})$, where $\tilde{\mathsf{pin}}$ was sampled in **Game 10**.

We prove that **Game 11** and **Game 12** are indistinguishable from $\mathcal{A}$'s view by $n_{2,2}$ hybrid games, where $n_{2,2}$ denotes the number of $\tilde{K}_2$ sampled in SETUP oracle when the underlying Pin/Uv Auth Protocol is $\mathsf{puvProtocol}_2$. Let $\tilde{K}_2^y$ denote the y-th $\tilde{K}_2$ sampled in SETUP oracle when the underlying Pin/Uv Auth Protocol is $\mathsf{puvProtocol}_2$. The hybrid game $\mathsf{hy}.y$ for $y \in [n_{2,2}]$ is defined below.

Game $\mathsf{hy}.0$**.** This game is identical to **Game 11** and we have:

$$\mathsf{Adv}_{11} = \mathsf{Adv}_{\mathsf{hy}.0}$$

Game $\mathsf{hy}.y$**.** This game is identical to **Game** $\mathsf{hy}.(y\text{-}1)$ except the following modifications:

1) When $\mathcal{A}$ queries SETUP(T, i, C, j, U) that will make use of the y-th $\tilde{K}_2^y$ for $\mathsf{puvProtocol}_2$ during the game, the challenger replaces $c_p = \mathsf{SKE}_2.\mathsf{Enc}(\tilde{K}_2^y, \mathsf{pin}_U)$ in the $\mathsf{setPIN}\text{-}C(\pi_C^j, \mathsf{pin}_U)$ by $\tilde{c}_p \leftarrow \mathsf{SKE}_2.\mathsf{Enc}(\tilde{K}_2^y, \tilde{\mathsf{pin}})$.

Let event E_3 denote the probability that the adversary $\mathcal{A}$ can distinguish **Game** $\mathsf{hy}.(y\text{-}1)$ and **Game** $\mathsf{hy}.y$. Note that the modifications between every two adjacent games are independent. It holds that

$$\mathsf{Adv}_{\mathsf{hy}.(y\text{-}1)} - \mathsf{Adv}_{\mathsf{hy}.y} \le \Pr[E_3], \forall y \in [n_{2,2}]$$

Then, we analyze the probability of the occurrence of E_3 by reduction. Namely, if E_3 occurs, then we can construct an adversary $\mathcal{B}_3$ that breaks IND-1CPA security of SKE_2 by invoking $\mathcal{A}$. $\mathcal{B}_3$ simulates **Game** hy.(y-1) honestly, except for the query to the SETUP(T, i, C, j, U) and that will produce the y-th $\tilde{K}_2^y$ for $\mathsf{puvProtocol}_2$ during the game. To handle this query, $\mathcal{B}_3$ executes the following steps:

1) $\mathcal{B}_3$ sends query($\mathsf{pin}_U, \tilde{\mathsf{pin}}$) to its challenger and obtains c. Then, $\mathcal{B}_3$ sets c as the first output of setPIN-$C(\pi_C^j, \mathsf{pin}_U)$ algorithm.

Note that we have already ensured that all ECDH public keys are distinct in **Game 9** and that all used $\tilde{K}_2$ are distinct in **Game 4**. It's easy to observe that $\mathcal{B}_3$ perfectly simulates **Game** hy.(y-1) or **Game** hy.y. Moreover, $\mathcal{B}_3$ simulates **Game** hy.(y-1) if $c = \mathsf{SKE}_2.\mathsf{Enc}(\tilde{K}_2^y, \mathsf{pin}_U)$ and **Game** hy.y if $c = \mathsf{SKE}_2.\mathsf{Enc}(\tilde{K}^y, \tilde{\mathsf{pin}})$. Thus, $\mathcal{B}_3$ can win IND-1CPA experiment whenever $\mathcal{A}$ can distinguish **Game** hy.(y-1) and **Game** hy.y. Thus, we have that

$$\Pr[E_3] \le \epsilon_{\mathsf{SKE}_2}^{\text{ind-1cpa}}$$

Moreover, **Game** hy.$n_{2,2}$ have replaced all c_p in the SETUP oracles whenever the client chooses $\mathsf{puvProtocol}_2$. Thus, **Game** hy.$n_{2,2}$ is identical to **Game 12** and we have

$$\mathsf{Adv}_{12} = \mathsf{Adv}_{\mathsf{hy}.n_{2,2}}$$

Combing the statements above, we have that

$$\mathsf{Adv}_{11} - \mathsf{Adv}_{12} \le n_{2,2}\epsilon_{\mathsf{SKE}_2}^{\text{ind-1cpa}}$$

Here, we simply keep using the number $n_{2,2}$, which would be helpful for us to tighten our security upper bound in the following games.

Game 13. This games is identical to **Game 12** except the following modification:

1) When $\mathcal{A}$ queries SETUP(T, i, C, j, U) and the challenger sets the selected Pin/Uv Auth Protocol of the client session π_C^j to be $\pi_C^j.\mathsf{selectedpuvProtocol} = \mathsf{puvProtocol}_3$ during the execution, the challenger replaces $c_p = \mathsf{SKE}_3.\mathsf{Enc}(K_2, \mathsf{pin}_U)$ in setPIN-$C(\pi_C^j, \mathsf{pin}_U)$ by $\tilde{c}_p \leftarrow \mathsf{SKE}_3.\mathsf{Enc}(K_2, \tilde{\mathsf{pin}})$, where $\tilde{\mathsf{pin}}$ was sampled in **Game 10**.

Let $n_{2,3}$ denote the number of K_2 sampled in SETUP oracle when the underlying Pin/Uv Auth Protocol is $\mathsf{puvProtocol}_3$. Similar to the analysis in **Game 12**, we can easily have that

$$\mathsf{Adv}_{12} - \mathsf{Adv}_{13} \le n_{2,3}\epsilon_{\mathsf{SKE}_3}^{\text{ind-1cpa}}$$

Note that $n_{2,1}$, $n_{2,2}$, and $n_{2,3}$ respectively denote the number of symmetric encryption keys produced by $\mathsf{puvProtocol}_1$, $\mathsf{puvProtocol}_2$, and $\mathsf{puvProtocol}_3$ in the SETUP oracle. Moreover, our CTAP 2.1 only supports these three versions. This implies that $n_{2,1} + n_{2,2} + n_{2,3} \le q_{\text{SETUP}}$. Further, we have that

$$\begin{aligned}\mathsf{Adv}_{10} - \mathsf{Adv}_{13} &\le n_{2,1}\epsilon_{\mathsf{SKE}_1}^{\text{ind-1cpa-H}_2} + n_{2,2}\epsilon_{\mathsf{SKE}_2}^{\text{ind-1cpa}} + n_{2,3}\epsilon_{\mathsf{SKE}_3}^{\text{ind-1cpa}} \\ &\le q_{\text{SETUP}} \max\{\epsilon_{\mathsf{SKE}_1}^{\text{ind-1cpa-H}_2}, \epsilon_{\mathsf{SKE}_2}^{\text{ind-1cpa}}, \epsilon_{\mathsf{SKE}_3}^{\text{ind-1cpa}}\}\end{aligned}$$

Game 14. This game is identical to **Game 13** except the following modification:

1) Whenever the adversary $\mathcal{A}$ queries SEND-BIND-T(T, i, m) oracle, instead of checking the decrypted $\mathsf{pinHash} \neq \mathsf{st}_T.\mathsf{pinHash}$ in the obtainPinUvAuthToken-T algorithm, the challenger checks whether $\mathsf{pinHash} \neq \mathsf{H}(\mathsf{pin}_{\mathsf{st}_T.\mathsf{user}})$

Note that $\mathsf{st}_T.\mathsf{pinHash} = \mathsf{H}(\mathsf{pin}_{\mathsf{st}_T.\mathsf{user}})$. **Game 13** and **Game 14** are indeed identical and we have that:

$$\mathsf{Adv}_{13} = \mathsf{Adv}_{14}$$

Game 15. This games is identical to **Game 14** except the following modification:

1) When $\mathcal{A}$ queries EXECUTE(T, i, C, j, U) and the challenger sets the selected Pin/Uv Auth Protocol of the client sessions π_C^j to be $\pi_C^j.\mathsf{selectedpuvProtocol} = \mathsf{puvProtocol}_1$, the challenger replaces $c_{ph} = \mathsf{SKE}_1.\mathsf{Enc}(\tilde{K}, \mathsf{H}(\mathsf{pin}_U))$ in the obtainPinUvAuthToken-C-start$(\pi_C^j, \mathsf{pin}_U)$ by $\tilde{c}_{ph} \leftarrow \mathsf{SKE}_1.\mathsf{Enc}(\tilde{K}, \mathsf{H}(\tilde{\mathsf{pin}}))$, where $\tilde{K}$ is the underlying symmetric key produced by $\mathsf{puvProtocol}_1$ and that $\tilde{\mathsf{pin}}$ was sampled in **Game 10**.

We prove that **Game 14** and **Game 15** are indistinguishable by $n_{3,1}$ hybrid games, where $n_{3,1}$ denotes the number of $\tilde{K}$ sampled in EXECUTE oracle when the underlying Pin/Uv Auth Protocol is $\mathsf{puvProtocol}_1$. Let $\tilde{K}^y$ denotes the y-th $\tilde{K}$ sampled in EXECUTE oracle when the underlying Pin/Uv Auth Protocol is $\mathsf{puvProtocol}_1$. The hybrid game hy.y for $y \in [n_{3,1}]$ is defined below.

Game hy.0**.** This game is identical to **Game 14** and we have:

$$\mathsf{Adv}_{14} = \mathsf{Adv}_{\mathsf{hy}.0}$$

Game hy.y**.** This game is identical to **Game** hy.(y-1) except the following modifications:

1) When $\mathcal{A}$ queries EXECUTE(T, i, C, j, U) that will produce the y-th $\tilde{K}^y$ for $\mathsf{puvProtocol}_1$, the challenger replaces $c_{ph} = \mathsf{SKE}_1.\mathsf{Enc}(\tilde{K}^y, \mathsf{H}(\mathsf{pin}_U))$ in obtainPinUvAuthToken-C-start$(\pi_C^j, \mathsf{pin}_U)$ by $\tilde{c}_{ph} \leftarrow \mathsf{SKE}_1.\mathsf{Enc}(\tilde{K}^y, \tilde{\mathsf{pin}})$.

Let event E_4 denote the probability that the adversary $\mathcal{A}$ can distinguish **Game** hy.(y-1) and **Game** hy.y. It holds that

$$\mathsf{Adv}_{\mathsf{hy}.(y\text{-}1)} - \mathsf{Adv}_{\mathsf{hy}.y} \le \Pr[E_4]$$

Then, we analyze the probability of the occurrence of E_4 by reduction. Namely, if E_4 occurs, then we can construct an adversary $\mathcal{B}_4$ that breaks IND-1\$PA-LPC security of SKE_1 by invoking $\mathcal{A}$. $\mathcal{B}_4$ simulates **Game** hy.(y-1) honestly, except for the following queries:

1) When $\mathcal{A}$ sends EXECUTE(T, i, C, j, U) that will produce the y-th $\tilde{K}^y$ for $\mathsf{puvProtocol}_1$ in this phase. To handle this query, $\mathcal{B}_4$ sends $(\mathsf{H}(\mathsf{pin}_{\tilde{U}}), \mathsf{H}(\tilde{\mathsf{pin}}))$ to its challenger and obtains $\tilde{c}$. Then, $\mathcal{B}_4$ sets $\tilde{c}$ as the output of obtainPinUvAuthToken-C-start$(\pi_C^j, \mathsf{pin}_{\tilde{U}})$ algorithm. The reaming of this query is answered honestly.

2) When $\mathcal{A}$ queries SEND-BIND-T(T, i, m) following the above EXECUTE(T, i, C, j, U) query, $\mathcal{B}_4$ separate the cases depending on whether $m = pk_{C,j} \parallel \tilde{c}_{ph}$.
   a) If $\mathsf{st}_T.\mathsf{user} \neq U$, then $\mathcal{B}_4$ simply performs as if the decrypted pinHash is unequal to $\mathsf{H}(\mathsf{pin}_{\mathsf{st}_T.\mathsf{user}})$.
   b) If $\mathsf{st}_T.\mathsf{user} = U$ and $m = pk_{C,j} \parallel \tilde{c}_{ph}$, then $\mathcal{B}_4$ queries RAND with input $\mu\lambda$ to its challenger and obtains $(pt_0, pt_1, \tilde{c}')$. Then, $\mathcal{B}_4$ sets $(\tilde{c}', \mathsf{false})$ as the output of $\mathsf{obtainPinUvAuthToken}\text{-}T(\pi_T^i, \mathsf{puvProtocol}_1, c, c_{ph})$. Meanwhile, $\mathcal{B}_4$ sets $\pi_T^i.\mathsf{bs} = pt_0$.
   c) If $\mathsf{st}_T.\mathsf{user} = U$ but $m = pk_{C,j} \parallel c_{ph}$ for $c_{ph} \neq \tilde{c}_{ph}$, then $\mathcal{B}_4$ queries LPC(c_{ph}) to its challenger. If the response is false, then $\mathcal{B}_4$ performs as if the decrypted pinHash does not match $\mathsf{H}(\mathsf{pin}_{\mathsf{st}_T.\mathsf{user}})$. Otherwise, $\mathcal{B}_4$ queries RAND with input $\mu\lambda$ to its challenger and obtains $(pt_0, pt_1, \tilde{c}')$. Then, $\mathcal{B}_4$ sets $(\tilde{c}', \mathsf{false})$ as the output of $\mathsf{obtainPinUvAuthToken}\text{-}T(\pi_T^i, \mathsf{puvProtocol}_1, c, c_{ph})$. Meanwhile, $\mathcal{B}_4$ sets $\pi_T^i.\mathsf{bs} = pt_0$.

3) When $\mathcal{A}$ afterwards sends SEND-BIND-C(C, j, m) following the above EXECUTE(T, i, C, j, U) and SEND-BIND-T(T, i, m) queries without abortion, $\mathcal{B}$ sets $\pi_C^j.\mathsf{bs} = pt_0$ if $m = \tilde{c}'$, and $\pi_C^j.\mathsf{bs} = pt_1$ otherwise.

It's easy to observe that $\mathcal{B}_4$ perfectly simulates **Game** hy.(y-1) if $c_{ph} = \mathsf{SKE}_1.\mathsf{Enc}(\tilde{K}^y, \mathsf{H}(\mathsf{pin}_U))$ and **Game** hy.y if $c_{ph} = \mathsf{SKE}_1.\mathsf{Enc}(\tilde{K}^y, \mathsf{H}(\tilde{\mathsf{pin}}))$. Thus, $\mathcal{B}_4$ can win IND-1\$PA experiment whenever $\mathcal{A}$ can distinguish **Game** hy.(y-1) and **Game** hy.y. Thus, we have

$$\Pr[E_4] \leq \epsilon_{\mathsf{SKE}_1}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}$$

Moreover, **Game** hy.$n_{3,1}$ have replaced all c_{ph} in the EXECUTE oracles whenever the client chooses $\mathsf{puvProtocol}_1$. Thus, **Game** hy.$n_{3,1}$ is identical to **Game 15** and we have

$$\mathsf{Adv}_{15} = \mathsf{Adv}_{\mathsf{hy}.n_{3,1}}$$

Note that we have assumed all $\tilde{K}$ of $\mathsf{puvProtocol}_1$ are distinct in **Game 2** and all above hybrid games are independent. Combing the statements above, we have that

$$\mathsf{Adv}_{14} - \mathsf{Adv}_{15} \leq n_{3,1}\epsilon_{\mathsf{SKE}_1}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}$$

Similar as before, we simply keep using the number $n_{3,1}$, which would be helpful for us to tighten our security upper bound in the following games.

Game 16. This game is identical to **Game 15** except the following modification:

1) When $\mathcal{A}$ queries EXECUTE(T, i, C, j, U) and the challenger sets the Pin/Uv Auth Protocol of the client session π_C^j to be $\pi_C^j.\mathsf{selectedpuvProtocol} = \mathsf{puvProtocol}_2$, the challenger replaces $c_{ph} \xleftarrow{\$} \mathsf{SKE}_2.\mathsf{Enc}(\tilde{K}_2, \mathsf{H}(\mathsf{pin}_U))$ in the $\mathsf{obtainPinUvAuthToken}\text{-}C\text{-}\mathsf{start}(\pi_C^j, \mathsf{pin}_U)$ by $\tilde{c}_{ph} \xleftarrow{\$} \mathsf{SKE}_2.\mathsf{Enc}(\tilde{K}_2, \mathsf{H}(\tilde{\mathsf{pin}}))$, where $\tilde{K}_2$ is the underlying symmetric key produced by $\mathsf{puvProtocol}_2$ and that $\tilde{\mathsf{pin}}$ was sampled in **Game 10**.

Similar to the analysis in **Game 15**, let $n_{3,2}$ denotes the number of $\tilde{K}_2$ of $\mathsf{authenticate}_2$ that are generated in EXECUTE(T, i, C, j, U) oracles. We can easily have the equation below by a sequence of hybrid games.

$$\mathsf{Adv}_{15} - \mathsf{Adv}_{16} \leq n_{3,2}\epsilon_{\mathsf{SKE}_2}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}$$

Game 17. This games is identical to **Game 16** except the following modification:

1) When $\mathcal{A}$ queries EXECUTE(T, i, C, j, U) and the challenger sets the Pin/Uv Auth Protocol of the client session π_C^j to be $\pi_C^j.\mathsf{selectedpuvProtocol} = \mathsf{puvProtocol}_3$, the challenger replaces $c_{ph} \xleftarrow{\$} \mathsf{SKE}_3.\mathsf{Enc}(K_2, \mathsf{H}(\mathsf{pin}_U))$ in the $\mathsf{obtainPinUvAuthToken}\text{-}C\text{-}\mathsf{start}(\pi_C^j, \mathsf{pin}_U)$ by $\tilde{c}_{ph} \xleftarrow{\$} \mathsf{SKE}_3.\mathsf{Enc}(K_2, \mathsf{H}(\tilde{\mathsf{pin}}))$, where K_2 is the underlying symmetric key produced by $\mathsf{puvProtocol}_3$ and that $\tilde{\mathsf{pin}}$ was sampled in **Game 10**.

Similar to the analysis in **Game 16**, let $n_{3,3}$ denotes the number of K_2 of $\mathsf{authenticate}_3$ that are generated in EXECUTE(T, i, C, j, U) oracles. We can easily have the equation below by a sequence of hybrid games.

$$\mathsf{Adv}_{16} - \mathsf{Adv}_{17} \leq n_{3,3}\epsilon_{\mathsf{SKE}_3}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}$$

Note that there are only 3 kinds of puvProtocols. We have $n_{3,1} + n_{3,2} + n_{3,3} \leq q_{\text{EXECUTE}}$. It holds that

$$\begin{aligned}&\mathsf{Adv}_{14} - \mathsf{Adv}_{17}\\ \leq& n_{3,1}\epsilon_{\mathsf{SKE}_1}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}} + n_{3,2}\epsilon_{\mathsf{SKE}_2}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}} + n_{3,3}\epsilon_{\mathsf{SKE}_3}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}\\ \leq& q_{\text{EXECUTE}} \max\{\epsilon_{\mathsf{SKE}_1}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}, \epsilon_{\mathsf{SKE}_2}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}, \epsilon_{\mathsf{SKE}_3}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}\}\end{aligned}$$

Game 18. In this game, the challenger $\mathcal{C}$ aborts the game and let $\mathcal{A}$ immediately win if there exists a token session π_T^i that accepts a malicious c_{ph} sent by $\mathcal{A}$ via SEND-BIND-T query without corrupting the pin of the user $\mathsf{st}_T.\mathsf{user}$. More formally and concretely, the challenger $\mathcal{C}$ aborts the game and let $\mathcal{A}$ immediately win if there exists a token session π_T^i such that

1) the adversary has queried SEND-BIND-T(T, i, m) such that $m = pk \parallel c_{ph}$ is not included in the output of any query EXECUTE(T, i, C, j, U) for any C, j, U.
2) $\pi_T^i.\mathsf{pinCorr} = \mathsf{false}$
3) $\pi_T^i.\mathsf{st}_{\mathsf{exe}} = \mathsf{bindDone}$ and $\pi_T^i.\mathsf{bs} \neq \perp$

In this case, the input message m of SEND-BIND-T is forged by $\mathcal{A}$. Note that all the transcripts of a token T that $\mathcal{A}$ eavesdrops are independent of pin_U with $\mathsf{pin}_U \neq \tilde{\mathsf{pin}}$ and that $\mathcal{A}$ is not allowed to corrupt the user pin $\mathsf{pin}_{\mathsf{st}_T.\mathsf{user}}$ that setups token T. The condition "$\pi_T^i.\mathsf{st}_{\mathsf{exe}} = \mathsf{bindDone}$ and $\pi_T^i.\mathsf{bs} \neq \perp$" indicates that the adversary $\mathcal{A}$ must encrypt $\mathsf{H}(\mathsf{pin}_{\mathsf{st}_T.\mathsf{user}})$. Recall that the pin_U of any honest users U are sampled randomly following distribution $\mathfrak{D}$ with min-entropy $\alpha_{\mathfrak{D}}$ and that $\mathcal{A}$ can try at most pinRetriesMax times for each token session π_T^i. $\mathcal{A}$ can guess the $\mathsf{pin}_{\mathsf{st}_T.\mathsf{user}}$ for each token session π_T^i correctly with probability at most $\mathsf{pinRetriesMax}2^{-\alpha_{\mathfrak{D}}}$. Note also that tokens can be set pin only in SETUP oracles, which happens at most q_{SETUP} times. By union bound, we have that

$$\mathsf{Adv}_{17} - \mathsf{Adv}_{18} \leq q_{\text{SETUP}}\mathsf{pinRetriesMax}2^{-\alpha_{\mathfrak{D}}}$$

Final Analysis. Now, let's finally check $\mathcal{A}$ can satisfy the winning conditions.

Note that the win-SUF-t$'$ is set to true in the VALIDATE(T, i, M, t, d) query only when at least one of the following four winning conditions

1) the user decision $d \neq$ accepted, or
2) two distinct client sessions that completed Bind have the same session identifiers, or
3) two distinct token sessions that completed Bind have the same session identifiers, or
4) (M, t) was not output by any of π_T^i's uncompromised valid partners π_C^j before the setup user of token T is corrupted

However, we can observe that

1) $d \neq$ accepted: This is always false by definition, see validate-T algorithm in Figure D-A.
2) $\exists (C_1, j_1), (C_2, j_2)$ such that $(C_1, j_1) \neq (C_2, j_2)$ **and** $\pi_{C_1}^{j_1}.\mathsf{st}_{\mathsf{exe}} = \pi_{C_2}^{j_2}.\mathsf{st}_{\mathsf{exe}} = \mathsf{bindDone}$ **and** $\pi_{C_1}^{j_1}.\mathsf{sid} = \pi_{C_2}^{j_2}.\mathsf{sid}$: Recall that the client sends the randomly sampled $\mathsf{puvProtocol}_i.pk$, which includes ECDH public key, to the tokens in the EXECUTE oracles. Recall also that we have ensured that all honestly sampled ECDH public keys are distinct and that the session identifier is defined as the full transcript during the execution of Bind algorithm. This means, two client sessions can never have the same identifier (not matter whether they are valid or not). Thus, this condition is always false.
3) $\exists (T_1, i_1), (T_2, i_2)$ such that $(T_1, i_1) \neq (T_2, i_2)$ **and** $\pi_{T_1}^{i_1}.\mathsf{st}_{\mathsf{exe}} = \pi_{T_2}^{i_2}.\mathsf{st}_{\mathsf{exe}} = \mathsf{bindDone}$ **and** $\pi_{T_1}^{i_1}.\mathsf{sid} = \pi_{T_2}^{i_2}.\mathsf{sid}$: Note that session identifiers of token sessions includes the token's public key pk, the client's encapsulation c, the encryption of pinHash c_{ph}, and the encryption of pt c_{pt}. Then, $\pi_{T_1}^{i_1}.\mathsf{sid} = \pi_{T_2}^{i_2}.\mathsf{sid}$ holds only when $(pk^1, c^1, c_{ph}^1, c_{pt}^1) = (pk^2, c^2, c_{ph}^2, c_{pt}^2)$, where $(pk^1, c^1, c_{ph}^1, c_{pt}^1)$ is included in the $\pi_{T_1}^{i_1}.\mathsf{sid}$ and $(pk^2, c^2, c_{ph}^2, c_{pt}^2)$ is included in the $\pi_{T_2}^{i_2}.\mathsf{sid}$. In particular, $(pk^1, c^1) = (pk^2, c^2)$ indicates that c_{pt}^1 and c_{ph}^2 are encrypted under the same symmetric key. Moreover, in **Game 10** we ensured that there exists no collision between pts, which further implies that $c_{pt}^1 \neq c_{pt}^2$ if the underlying symmetric encryption is correct. Thus, this condition is always false.
4) for $(C', j') \leftarrow \mathsf{bindPartner}(T, i)$, all of the following conditions must hold: a) $(C', j', M, t) \notin \mathcal{L}_{\text{AUTH}}$, b) $\pi_{C'}^{j'} = (\perp, \perp)$ **or** $\pi_{C'}^{j'}.\mathsf{compromised} = \mathsf{false}$, c) $\pi_T^i.\mathsf{pinCorr} = \mathsf{false}$: According to the condition (2), we know that the adversary $\mathcal{A}$ is not allowed to compromise the binding state of any client (C', j') such that $\pi_{C'}^{j'}.\mathsf{bs} = \pi_T^i.\mathsf{bs}$ According to the condition (3)$\pi_T^i.\mathsf{pinCorr} = \mathsf{false}$ and **Game 18**, we know that the adversary $\mathcal{A}$ cannot execute active attack against token to obtain the token biding state $\pi_T^i.\mathsf{bs}$. Thus, the adversary $\mathcal{A}$ has no idea about the $\pi_T^i.\mathsf{bs}$.

According to the condition (1) $(C', j', M, t) \notin \mathcal{L}_{\text{AUTH}}$, we know that (M, t) was never output by any of the session π_T^i's partner. The adversary therefore has to forge the message-tag pair (M, t). Recall that the tag t is computed by applying random oracles H_2, H_4, and H_7 to the corresponding binding state $\pi_T^i.\mathsf{bs}$ and message M, respectively in $\mathsf{puvProtocol}_1$, $\mathsf{puvProtocol}_2$, and $\mathsf{puvProtocol}_3$. The adversary can only guess the either the tag directly or the toke binding state $\pi_T^i.\mathsf{bs}$. Moreover, recall that:

a) If the underlying authProtocol is $\mathsf{puvProtocol}_1$, then the adversary $\mathcal{A}$ can guess $\pi_T^i.\mathsf{bs}$ with probability $2^{-\mu\lambda}$ and tag t with probability 2^{-l_2}
b) If the underlying authProtocol is $\mathsf{puvProtocol}_2$, then the adversary $\mathcal{A}$ can guess $\pi_T^i.\mathsf{bs}$ with probability $2^{-2\lambda}$ and tag t with probability 2^{-l_4}.
c) If the underlying authProtocol is $\mathsf{puvProtocol}_3$, then the adversary $\mathcal{A}$ can guess $\pi_T^i.\mathsf{bs}$ with probability $2^{-\mu'\lambda}$ and the tag with probability 2^{-l_7}.

Thus, the probability that $\mathcal{A}$ finds can forge tag t for any message M in each VALIDATE query is bounded by

$$\begin{aligned}&\max\{2^{-\mu\lambda}, 2^{-l_2}, 2^{-2\lambda}, 2^{-l_4}, 2^{-\mu'\lambda}, 2^{-l_7}\}\\ =&2^{-\min\{\mu\lambda, 2\lambda, \mu'\lambda, l_2, l_4, l_7\}}\end{aligned}$$

Note that the adversary $\mathcal{A}$ can attempts only in VALIDATE oracle, which can be invoked at most q_{VALIDATE} times. By union bound, we have that

$$\mathsf{Adv}_{18} \leq q_{\text{VALIDATE}}2^{-\min\{\mu\lambda, 2\lambda, \mu'\lambda, l_2, l_4, l_7\}}$$

Combing all statements above, the proof is concluded by:

$$\begin{aligned}&\mathsf{Adv}_{\mathsf{PACA},\mathcal{A}}^{\mathsf{SUF\text{-}t'}}(1^\lambda)\\ \leq&(q_{\text{SETUP}} + q_{\text{EXECUTE}})\epsilon_{\mathsf{ECDH}}^{\mathsf{sCDH}} + \epsilon_{\mathsf{H}}^{\mathsf{coll\text{-}res}}\\ &+\binom{q_{\text{SETUP}} + q_{\text{EXECUTE}}}{2}(2^{2-\min\{l_1, l_3, l_5, l_6\}} + 2^{1-q})\\ &+q_{\text{NEWU}}2^{-\alpha_{\mathfrak{D}}} + \binom{q_{\text{SEND-BIND-T}}}{2}2^{-\min\{\mu, 2, \mu'\}\lambda}\\ &+q_{\text{SETUP}}\max\{\epsilon_{\mathsf{SKE}_1}^{\mathsf{ind\text{-}1cpa\text{-}H_2}}, \epsilon_{\mathsf{SKE}_2}^{\mathsf{ind\text{-}1cpa}}, \epsilon_{\mathsf{SKE}_3}^{\mathsf{ind\text{-}1cpa}}\}\\ &+q_{\text{EXECUTE}}\max\{\epsilon_{\mathsf{SKE}_1}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}, \epsilon_{\mathsf{SKE}_2}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}, \epsilon_{\mathsf{SKE}_3}^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}\}\\ &+q_{\text{SETUP}}\mathsf{pinRetriesMax}2^{-\alpha_{\mathfrak{D}}}\\ &+q_{\text{VALIDATE}}2^{-\min\{\mu\lambda, 2\lambda, \mu'\lambda, l_2, l_4, l_7\}}\end{aligned}$$

□

APPENDIX J
PROOF OF THEOREM 3

Proof. We give the proof by a sequence of games. Each game is simulated between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$. Let Adv_i denote the adversary $\mathcal{A}$'s advantage in winning game i.

Game 0. This game is identical to the $\mathsf{Expt}_{\mathsf{PACA}}^{\mathsf{SUF\text{-}t'}}$ experiment. Hence, it holds that

$$\mathsf{Adv}_0 = \mathsf{Adv}_{\mathsf{PACA},\mathcal{A}}^{\mathsf{SUF\text{-}t'}}(1^\lambda)$$

Game 1. This game is identical to **Game 0** except that the following modifications:

1) Whenever a client executes $\mathsf{puvProtocol}_3.\mathsf{encapsulate}_3$ on a token's public key pk', the challenger $\mathcal{C}$ executes the following steps:
   a) Parse $(pk'_1, pk'_2) \leftarrow pk'$
   b) Run $(c_2, Z_2) \xleftarrow{\$} \mathsf{KEM.Encaps}(pk'_2)$
   c) Sample a random $\tilde{Z}_2$ in the key space of KEM
   d) Replace Z_2 by $\tilde{Z}_2$ for the subsequent execution.
   e) Finally, output a ciphertext $c = (c_1, c_2)$ for some c_1.
2) Whenever a token holding $pk'' = (pk''_1, pk''_2)$ such that $pk'_2 = pk''_2$ and needs to execute $\mathsf{decapsulate}_3$ on $c'' = (c''_1, c''_2)$ such that $c''_2 = c_2$, the challenger executes $\mathsf{decapsulate}_3$ honestly except that $\mathcal{C}$ directly sets $Z_2 \leftarrow \tilde{Z}_2$.

We prove that $\mathcal{A}$ cannot distinguishable **Game 0** and **Game 1** by n hybrid games, where n denotes the number of encapsulations that was output by all tokens in the SETUP and EXECUTE oracles. Then, we have that $n \leq q_{\text{SETUP}} + q_{\text{EXECUTE}}$. Let (sk_T^y, pk_T^y) denote the y-th KEM public-private key pair among all tokens. The **Game** $\mathsf{hy}.y$ for $y \in [n]$ is defined as follows:

Game $\mathsf{hy}.0$. This game is identical to **Game 0** and we have that

$$\mathsf{Adv}_0 = \mathsf{Adv}_{\mathsf{hy}.0}$$

Game $\mathsf{hy}.y$. This game is identical to **Game** $\mathsf{hy}.(y\text{-}1)$ except that the following modifications:

1) Whenever $\mathcal{A}$ queries SETUP and EXECUTE oracles where $\mathcal{C}$ needs to returns y-th KEM public key pk_T^y among all tokens and executes $\mathsf{KEM.Encaps}(pk_T^y)$, the challenger executes $(c_2, Z_2) \xleftarrow{\$} \mathsf{KEM.Encaps}(pk_T^y)$ and samples $\tilde{Z}_2$ in the key space of KEM. Next, $\mathcal{C}$ replaces Z_2 by $\tilde{Z}_2$ for the subsequent execution.
2) Whenever $\mathcal{C}$ needs to execute $\mathsf{KEM.Decaps}(sk_T^y, c_2)$, it directly uses $Z_2 \leftarrow \tilde{Z}_2$ for the subsequent execution instead of computing Z_2 using KEM.

If $\mathcal{A}$ can distinguish **Game** $\mathsf{hy}.y$ from **Game** $\mathsf{hy}.(y\text{-}1)$, then we can construct an adversary $\mathcal{B}_1$ that breaks $\mathsf{IND\text{-}CCA}$ security of KEM. The $\mathsf{IND\text{-}CCA}$ experiment executes $(pk, sk) \xleftarrow{\$} \mathsf{KG}()$ and $(c^\star, k_0^\star) \xleftarrow{\$} \mathsf{Encaps}(pk)$ honestly and samples $\mathsf{b} \xleftarrow{\$} \{0,1\}$ and $k_1^\star$ from the key space $\mathcal{K}$ randomly. On input $(pk, c^\star, k_\mathsf{b}^\star)$, $\mathcal{B}_1$ runs **Game** $\mathsf{hy}.(y\text{-}1)$ honestly except the following modification:

1) When the algorithm $\mathsf{obtainSharedSecret}\text{-}T$ needs to output y-th KEM public key pk_T^y, $\mathcal{B}_1$ uses $pk_T^y \leftarrow pk$ instead of sampling it using $\mathsf{KG}()$
2) When $\mathcal{B}_1$ needs to execute $\mathsf{KEM.Encaps}(pk_T^y)$ in $\mathsf{encapsulate}_3$, $\mathcal{B}_1$ simply uses $(c_2, Z_2) \leftarrow (c^\star, k_\mathsf{b}^\star)$ for the subsequent execution.
3) When $\mathcal{B}_1$ needs to execute $Z_2 \leftarrow \mathsf{KEM.Decaps}(sk_T^y, c)$ in $\mathsf{decapsulate}_3$ algorithm, $\mathcal{B}_1$ does not know sk_T^y and performs as follows instead:
   - If $c = c^\star$, then $\mathcal{B}_1$ simply uses $Z_2 \leftarrow k_\mathsf{b}^\star$.
   - If $c \neq c^\star$, then $\mathcal{B}_1$ queries its decapsulation oracle DECAPS on c. When receiving an answer k, $\mathcal{B}_1$ sets $Z_2 \leftarrow k$ for the remaining computation.

It is straightforward that $\mathcal{B}_1$ perfectly simulates **Game** $\mathsf{hy}.(y\text{-}1)$ if $\mathsf{b} = 0$ and **Game** $\mathsf{hy}.y$ if $\mathsf{b} = 1$. So, $\mathcal{B}_1$ can win $\mathsf{IND\text{-}CCA}$ experiment whenever $\mathcal{A}$ can distinguish **Game** $\mathsf{hy}.(y\text{-}1)$ and **Game** $\mathsf{hy}.y$. Thus, it holds that

$$\mathsf{Adv}_{\mathsf{hy}.(y\text{-}1)} - \mathsf{Adv}_{\mathsf{hy}.y} \leq \epsilon_{\mathsf{KEM}}^{\mathsf{ind\text{-}cca}}$$

Moreover, when all the encapsulated keys of KEM are replaced by random keys, **Game** $\mathsf{hy}.n$ is identical to **Game 1**. Then, we have that

$$\mathsf{Adv}_{\mathsf{hy}.n} = \mathsf{Adv}_1$$

Note that all hybrid games above are independent, by union bound, we have that

$$\mathsf{Adv}_0 - \mathsf{Adv}_1 \leq n\epsilon_{\mathsf{KEM}}^{\mathsf{ind\text{-}cca}} \leq (q_{\text{SETUP}} + q_{\text{EXECUTE}})\epsilon_{\mathsf{KEM}}^{\mathsf{ind\text{-}cca}}$$

Game 2. This game is identical to **Game 1** except the following modification:

1) The challenger replaces each function $\mathsf{H}_5(\cdot, \tilde{Z}_2)$ by a truly random function $f_{\tilde{Z}_2}$, where $\tilde{Z}_2$s are sampled in **Game 1**.

We can easily reduce the indistinguishability between **Game 1** and **Game 2** to the $\epsilon_{\mathsf{H}_5}^{\mathsf{swap}}$-swap security of H_5 in n hybrid games, where n denotes the number of $\tilde{Z}_2$ in **Game 1**. Obviously, it holds that $n \leq q_{\text{SETUP}} + q_{\text{EXECUTE}}$. Thus, we have that

$$\mathsf{Adv}_1 - \mathsf{Adv}_2 \leq (q_{\text{SETUP}} + q_{\text{EXECUTE}})\epsilon_{\mathsf{H}_5}^{\mathsf{swap}}$$

In particular, for any $\tilde{Z} \leftarrow f_{\tilde{Z}_2}(Z_1)$, we know that $\tilde{Z}$ is uniformly at random, since $f_{\tilde{Z}_2}$ is a truly random function for any $\tilde{Z}_2$ that is sampled by the challenger in **Game 1** and not leaked to the adversary $\mathcal{A}$.

Game 3. This game is identical to **Game 2** except the following modification:

1) The challenger replaces each function $\mathsf{H}_6(\tilde{Z}, \cdot)$ by a truly random function $f'_{\tilde{Z}}$, where $\tilde{Z}$s are derived in **Game 2**.

Similarly to **Game 2**, we can easily reduce the indistinguishability between **Game 2** and **Game 3** to the $\epsilon_{\mathsf{H}_6}^{\mathsf{prf}}$-prf security of H_6 in n hybrid games, where n denotes the number of $\tilde{Z}$ produced in **Game 2**. Obviously, we have that $n \leq q_{\text{SETUP}} + q_{\text{EXECUTE}}$. Thus, we have that

$$\mathsf{Adv}_2 - \mathsf{Adv}_3 \leq (q_{\text{SETUP}} + q_{\text{EXECUTE}})\epsilon_{\mathsf{H}_6}^{\mathsf{prf}}$$

In particular, for any $K_1 \leftarrow f'_{\tilde{Z}}(\text{“CTAP2 HMAC key”})$ and $K_2 \leftarrow f'_{\tilde{Z}}(\text{“CTAP2 AES key”})$, we know that K_1s and K_2s are uniformly at random, since $f'_{\tilde{Z}}$ is a truly random function in **Game 2** and $\tilde{Z}$s are not leaked to the adversary $\mathcal{A}$.

Game 4. In this game, the challenger $\mathcal{C}$ aborts and lets $\mathcal{A}$ immediately win if there exists collision between $\tilde{K}_1$s or $\tilde{K}_2$s in **Game 3**. Note that $\tilde{K}_1$ as well as $\tilde{K}_2$ is derived only in the SETUP and EXECUTE oracles. So, there are at most $q_{\text{SETUP}} + q_{\text{EXECUTE}}$ keys and $\binom{q_{\text{SETUP}}+q_{\text{EXECUTE}}}{2}$ pairs. The collision of every two keys happens $\tilde{K}_1$ with probability 2^{-l_6}. The same holds for $\tilde{K}_2$.

Thus, we have that

$$\mathsf{Adv}_3 - \mathsf{Adv}_4 \leq \binom{q_{\text{SETUP}} + q_{\text{EXECUTE}}}{2} 2^{1-l_6}$$

Game 5. In this game, the challenger $\mathcal{C}$ aborts and lets $\mathcal{A}$ immediately win if there exists two distinct inputs $\mathsf{pin}, \mathsf{pin}'$ during $\mathcal{C}$'s execution such that $\mathsf{H}(\mathsf{pin}) = \mathsf{H}(\mathsf{pin}')$. Note that this abortion indicates the violation of collision resistance of H by definition. Since H is $\epsilon_{\mathsf{H}}^{\text{coll-res}}$-collision resistant, we have that

$$\mathsf{Adv}_4 - \mathsf{Adv}_5 \leq \epsilon_{\mathsf{H}}^{\text{coll-res}}$$

Game 6. This game is identical to **Game 5** except that the following modifications:

1) The challenger $\mathcal{C}$ samples a random $\tilde{\mathsf{pin}} \xleftarrow{\$} \mathfrak{D}$ at the beginning of the game but never uses it. The challenger aborts and lets $\mathcal{A}$ immediately win if $\tilde{\mathsf{pin}}$ collides with any user pin pin_U for any user U.
2) Whenever the adversary $\mathcal{A}$ queries oracle SETUP inputting any (T, i, C, j, U), the challenger replaces $\mathsf{pin} \leftarrow \mathsf{st}_T.\mathsf{puvProtocol.decrypt}(K, c_p)$ in the setPIN-T algorithm by
$$\mathsf{pin} \leftarrow \mathsf{pin}_U$$
3) The challenger aborts the game and lets $\mathcal{A}$ immediately win if there exits a collision between pts used in SEND-BIND-T oracles.

The analysis for this game is also identical to the **Game 10** in the proof of Theorem 2. The only difference is that each pt is sampled only in $\{0,1\}^{\mu'\lambda}$ and there are at most $\binom{q_{\text{SEND-BIND-T}}}{2}$ pairs of used pts.

So, we have that

$$\mathsf{Adv}_5 - \mathsf{Adv}_6 \leq q_{\text{NEWU}} 2^{-\alpha_{\mathfrak{D}}} + \binom{q_{\text{SEND-BIND-T}}}{2} 2^{-\mu'\lambda}$$

Game 7. This game is identical to **Game 6** except the following modification:

1) When $\mathcal{A}$ queries SETUP(T, i, C, j, U) and the challenger $\mathcal{C}$ replaces $c_p \leftarrow \mathsf{SKE}_3.\mathsf{Enc}(K_2, \mathsf{pin}_U)$ in setPIN-$C(\pi_C^j, \mathsf{pin}_U)$ by $\tilde{c}_p \leftarrow \mathsf{SKE}_3.\mathsf{Enc}(K_2, \tilde{\mathsf{pin}})$, where K_2 is the corresponding random key derived in **Game 3** and $\tilde{\mathsf{pin}}$ is sampled in **Game 6**.

Similar to the discussion in **Game 13** in the proof of Theorem 2, we have that

$$\mathsf{Adv}_6 - \mathsf{Adv}_7 \leq q_{\text{SETUP}} \epsilon_{\mathsf{SKE}_3}^{\text{ind-1cpa}}$$

Game 8. This game is identical to **Game 7** except the following modification:

1) When $\mathcal{A}$ queries EXECUTE(T, i, C, j, U), the challenger replaces $c_{ph} \leftarrow \mathsf{SKE}_3.\mathsf{Enc}(K_2, \mathsf{H}(\mathsf{pin}_{\tilde{U}}))$ in obtainPinUvAuthToken-C-start by $\tilde{c}_{ph} \leftarrow \mathsf{SKE}_3.\mathsf{Enc}(K_2, \mathsf{H}(\tilde{\mathsf{pin}}))$, where K_2 is the corresponding key computed in **Game 3** and $\tilde{\mathsf{pin}}$ is the one sampled in **Game 6**.

Similar to the discussion in **Game 17** in the proof of Theorem 2, we have that

$$\mathsf{Adv}_7 - \mathsf{Adv}_8 \leq q_{\text{EXECUTE}} \epsilon_{\mathsf{SKE}_3}^{\text{ind-1\$pa-lpc}}$$

Game 9. In this game, the challenger $\mathcal{C}$ aborts the game and let $\mathcal{A}$ immediately win if there exists a token session π_T^i that accepts a malicious c_{ph} sent by $\mathcal{A}$ via SEND-BIND-T query without corrupting the pin of the user $\mathsf{st}_T.\mathsf{user}$. More formally and concretely, the challenger $\mathcal{C}$ aborts the game and let $\mathcal{A}$ immediately win if there exists a token session π_T^i such that

1) the adversary has queried SEND-BIND-T(T, i, m) such that $m = pk \parallel c_{ph}$ is not included in the output of any query EXECUTE(T, i, C, j, U) for any C, j, U.
2) $\pi_T^i.\mathsf{pinCorr} = \mathsf{false}$
3) $\pi_T^i.\mathsf{st_{exe}} = \mathsf{bindDone}$ and $\pi_T^i.\mathsf{bs} \neq \perp$

The analysis for this game is identical to the one in **Game 18** in the proof of Theorem 2. Thus, we can easily have that

$$\mathsf{Adv}_8 - \mathsf{Adv}_9 \leq q_{\text{SETUP}} \mathsf{pinRetriesMax} 2^{-\alpha_{\mathfrak{D}}}$$

Final Analysis. Now, let's finally check $\mathcal{A}$ can satisfy the winning conditions.

Note that the win-SUF-t$'$ is set to true in the VALIDATE(T, i, M, t, d) query only when at least one of the following four winning conditions

1) the user decision $d \neq$ accepted, or
2) two distinct client sessions that completed Bind have the same session identifiers, or
3) two distinct token sessions that completed Bind have the same session identifiers, or
4) (M, t) was not output by any of π_T^i's uncompromised valid partners π_C^j before the setup user of token T is corrupted

However, we can observe that

1) $d \neq$ accepted: This is always false by definition, see validate-T algorithm in Figure D-A.
2) $\exists (C_1, j_1), (C_2, j_2)$ such that $(C_1, j_1) \neq (C_2, j_2)$ **and** $\pi_{C_1}^{j_1}.\mathsf{st_{exe}} = \pi_{C_2}^{j_2}.\mathsf{st_{exe}} = \mathsf{bindDone}$ **and** $\pi_{C_1}^{j_1}.\mathsf{sid} = \pi_{C_2}^{j_2}.\mathsf{sid}$: Recall that the client receives the honest token's public key and sends the encapsulation to the tokens in the EXECUTE oracles. Note that the KEM has public key entropy α_{pk} and ciphertext entropy α_c. Note also that EXECUTE can be invoked at most q_{EXECUTE} times, which means there are at most $\binom{q_{\text{EXECUTE}}}{2}$ public key and encapsulation pair. The adversary can win via this condition with probability at most $\binom{q_{\text{EXECUTE}}}{2}(2^{-\alpha_{pk}} + 2^{-\alpha_c})$.
3) $\exists (T_1, i_1), (T_2, i_2)$ such that $(T_1, i_1) \neq (T_2, i_2)$ **and** $\pi_{T_1}^{i_1}.\mathsf{st_{exe}} = \pi_{T_2}^{i_2}.\mathsf{st_{exe}} = \mathsf{bindDone}$ **and** $\pi_{T_1}^{i_1}.\mathsf{sid} = \pi_{T_2}^{i_2}.\mathsf{sid}$: Recall that the session identifier of token sessions includes the token's public key and the client's encapsulation. $\pi_{T_1}^{i_1}.\mathsf{sid} = \pi_{T_2}^{i_2}.\mathsf{sid}$ indicates that $\pi_{T_1}^{i_1}$ and $\pi_{T_2}^{i_2}$ agree on the token's public key and the client's encapsulation, which further implies the agreement on the symmetric encryption key of pt. For the correct symmetric key, this further indicates that the $\pi_{T_1}^{i_1}$ and $\pi_{T_2}^{i_2}$ produces the same pt, which violates the assumption that there are no collision between the used pts in **Game 6**. Thus, this condition is always false.
4) for $(C', j') \leftarrow \mathsf{bindPartner}(T, i)$, all of the following conditions must hold: a) $(C', j', M, t) \notin \mathcal{L}_{\text{AUTH}}$, b) $\pi_{C'}^{j'} = (\perp, \perp)$ **or** $\pi_{C'}^{j'}.\mathsf{compromised} = \mathsf{false}$, c) $\pi_T^i.\mathsf{pinCorr} = \mathsf{false}$: According to the condition (2), we know that the adversary $\mathcal{A}$ is not allowed to compromise the binding state of any

client (C', j') such that $\pi^{j'}_{C'}.\mathsf{bs} = \pi^{i}_{T}.\mathsf{bs}$ According to the condition (3)$\pi^i_T.\mathsf{pinCorr} = \mathsf{false}$ and **Game 9**, we know that the adversary $\mathcal{A}$ cannot execute active attack against token to obtain the token biding state $\pi^i_T.\mathsf{bs}$. Thus, the adversary $\mathcal{A}$ has no idea about the $\pi^i_T.\mathsf{bs}$.

According to the condition (1) $(C', j', M, t) \notin \mathcal{L}_{\text{AUTH}}$, we know that (M, t) was never output by any of the session π^i_T's partner. The adversary therefore has to forge the message-tag pair (M, t). Recall that the tag t is computed by applying a function H_7 to the corresponding binding state $\pi^i_T.\mathsf{bs}$ and message M. The adversary can only guess the either the tag directly or the toke binding state $\pi^i_T.\mathsf{bs}$. Moreover, recall that:

a) The binding state $\pi^i_T.\mathsf{bs}$ is sampled from $\{0,1\}^{\mu'\lambda}$. The adversary $\mathcal{A}$ can guess $\pi^i_T.\mathsf{bs}$ with probability $2^{-\mu'\lambda}$.
b) The tag is computed by $t \leftarrow \mathsf{H}_7(\pi^i_T.\mathsf{bs}, M)$ for some message M chosen by the adversary $\mathcal{A}$. Unless the adversary $\mathcal{A}$ can guess the token binding state $\pi^i_T.\mathsf{bs}$ correctly, it is random from the adversary's view, which further implies that t indistinguishable from a random string due to the $\epsilon^{\mathsf{prf}}_{\mathsf{H}_7}$-prf security of H_7. Thus, the adversary can guess tag t correctly with probability at most 2^{-l_7}.

Thus, the probability that $\mathcal{A}$ finds can forge tag t for any message M in each VALIDATE query is bounded by

$$2^{-\mu'\lambda} + \epsilon^{\mathsf{prf}}_{\mathsf{H}_7} + 2^{-l_7}$$

Note that the adversary $\mathcal{A}$ can attempts only in VALIDATE oracle, which can be invoked at most q_{VALIDATE} times. By union bound, the advantage that the adversary $\mathcal{A}$ wins via condition 4) is bounded by

$$q_{\text{VALIDATE}}(2^{-\mu'\lambda} + \epsilon^{\mathsf{prf}}_{\mathsf{H}_7} + 2^{-l_7})$$

To sum up, we have that

$$\mathsf{Adv}_9 \leq \binom{q_{\text{EXECUTE}}}{2}(2^{-\alpha_{pk}} + 2^{-\alpha_c}) + q_{\text{VALIDATE}}(2^{-\mu'\lambda} + \epsilon^{\mathsf{prf}}_{\mathsf{H}_7} + 2^{-l_7})$$

Combing all statements above, the proof is concluded by:

$$\begin{aligned}
&\mathsf{Adv}^{\mathsf{SUF\text{-}t'}}_{\mathsf{PACA},\mathcal{A}}(1^\lambda) \\
\leq &(q_{\text{SETUP}} + q_{\text{EXECUTE}})(\epsilon^{\mathsf{ind\text{-}cca}}_{\mathsf{KEM}} + \epsilon^{\mathsf{swap}}_{\mathsf{H}_5} + \epsilon^{\mathsf{prf}}_{\mathsf{H}_6}) \\
&+ \binom{q_{\text{SETUP}} + q_{\text{EXECUTE}}}{2} 2^{1-l_6} + \epsilon^{\mathsf{coll\text{-}res}}_{\mathsf{H}} + q_{\text{NEWU}} 2^{-\alpha_{\mathfrak{D}}} \\
&+ \binom{q_{\text{SEND-BIND-T}}}{2} 2^{-\mu'\lambda} + \binom{q_{\text{EXECUTE}}}{2}(2^{-\alpha_{pk}} + 2^{-\alpha_c}) \\
&+ q_{\text{SETUP}}\epsilon^{\mathsf{ind\text{-}1cpa}}_{\mathsf{SKE}_3} + q_{\text{EXECUTE}}\epsilon^{\mathsf{ind\text{-}1\$pa\text{-}lpc}}_{\mathsf{SKE}_3} \\
&+ q_{\text{SETUP}}\mathsf{pinRetriesMax}2^{-\alpha_{\mathfrak{D}}} + \binom{q_{\text{EXECUTE}}}{2}(2^{-\alpha_{pk}} + 2^{-\alpha_c}) \\
&+ q_{\text{VALIDATE}}(2^{-\mu'\lambda} + \epsilon^{\mathsf{prf}}_{\mathsf{H}_7} + 2^{-l_7})
\end{aligned}$$

□

APPENDIX K
PROOF OF THEOREM 4

Proof. The proof is given by reduction. If $\mathcal{A}$ can break the ua security of $\Sigma + \Pi$, then there must exist adversaries $\mathcal{A}_1$ against auth security of Σ and $\mathcal{A}_2$ against $\mathsf{SUF\text{-}t'}$ security of Π such that either or both can win. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively denote the challengers in auth and $\mathsf{SUF\text{-}t'}$ experiments. The adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$ simulate the ua experiment to $\mathcal{A}$ as follows:

1) $\mathcal{A}_1$ and $\mathcal{A}_2$ initialize lists $\mathcal{L}_{\mathsf{frsh}}$, $\mathcal{L}_{\text{AUTH}}$, $\mathcal{L}_{\text{REGISTER}}$, $\mathcal{L}_{\text{CHALLENGE}}$, and $\mathcal{L}_{\text{RESPONSE}}$ to $\emptyset$.
2) When $\mathcal{A}$ queries $\text{REGISTER}((S,i),(T,j,j'),(C,k),\mathsf{tb}, UV, d)$, $\mathcal{A}_1$ first queries $\text{REGISTER}((S,i),(T,j),\mathsf{tb}, UV)$ to $\mathcal{C}_1$ and receives $(m_{\mathsf{rch}}, m_{\mathsf{rcl}}, m_{\mathsf{rcom}}, m_{\mathsf{rrsp}}, d')$. Then, $\mathcal{A}_2$ sends its challenger $\mathcal{C}_2$ the queries $(m_{\mathsf{rcom}}, t) \leftarrow \text{AUTH}(C, k, m_{\mathsf{rcom}})$ and status $\leftarrow \text{VALIDATE}(T, j', m_{\mathsf{rcom}}, t, d)$. Finally, $\mathcal{A}_1$ and $\mathcal{A}_2$ add $(S, i, T, j, j', C, k, m_{\mathsf{rch}}, m_{\mathsf{rcl}}, m_{\mathsf{rcom}}, t, m_{\mathsf{rrsp}})$ into $\mathcal{L}_{\text{REGISTER}}$ and return $(m_{\mathsf{rch}}, m_{\mathsf{rcl}}, m_{\mathsf{rcom}}, t, m_{\mathsf{rrsp}}, d')$.
3) When $\mathcal{A}$ queries $\text{CHALLENGE}((S,i),(C,k),\mathsf{tb}, UV)$, the adversary $\mathcal{A}_1$ first queries $m_{\mathsf{acom}} \xleftarrow{\$} \text{CHALLENGE}((S,i),\mathsf{tb}, UV)$ to $\mathcal{C}_1$ followed by executing $(m_{\mathsf{acom}}, t) \leftarrow \mathsf{aCom}(\mathsf{id}_S, m_{\mathsf{ach}}, \mathsf{tb})$. Then, $\mathcal{A}_2$ sends its challenger $\mathcal{C}_2$ the query $(m_{\mathsf{acom}}, t) \leftarrow \text{AUTH}(C, k, m_{\mathsf{acom}})$. Finally, $\mathcal{A}_1$ and $\mathcal{A}_2$ add $(S, i, C, k, m_{\mathsf{ach}}, m_{\mathsf{acl}}, m_{\mathsf{acom}}, t)$ into $\mathcal{L}_{\text{CHALLENGE}}$ and return $(m_{\mathsf{ach}}, m_{\mathsf{acl}}, m_{\mathsf{acom}}, t)$.
4) When $\mathcal{A}$ queries $\text{RESPONSE}((T,j,j'), m_{\mathsf{acom}}, t, d)$, the adversary $\mathcal{A}_2$ first queries status $\leftarrow \text{VALIDATE}(T, j', m_{\mathsf{acom}}, t, d)$ to its challenger $\mathcal{C}_2$ and directly returns $\perp$ if status $\neq$ accepted. Then, $\mathcal{A}_1$ queries $m_{\mathsf{arsp}} \xleftarrow{\$} \text{RESPONSE}((T,j), m_{\mathsf{acom}})$ to its challenger $\mathcal{C}_1$. Finally, $\mathcal{A}_1$ and $\mathcal{A}_2$ add $(T, j, j', m_{\mathsf{acom}}, t, m_{\mathsf{arsp}})$ into $\mathcal{L}_{\text{RESPONSE}}$ and return m_{arsp}.
5) When $\mathcal{A}$ queries $\text{COMPLETE}((S,i), m_{\mathsf{acl}}, m_{\mathsf{arsp}})$, the adversary $\mathcal{A}_1$ forwards this query to its challenger $\mathcal{C}_1$ and receives a boolean value d. If $d = 1$, then $\mathcal{A}_1$ additionally sets the winning predicate win-ua to be $\mathsf{Win\text{-}ua}(S, i)$ and returns d.
6) For all other queries from $\mathcal{A}$, $\mathcal{A}_1$ and $\mathcal{A}_2$ simply forward them to $\mathcal{C}_1$ or $\mathcal{C}_2$ depending whether they are defined in auth or $\mathsf{SUF\text{-}t'}$ experiment and return the results back to $\mathcal{A}$.
7) When $\mathcal{A}$ terminates at some point, $\mathcal{A}_1$ and $\mathcal{A}_2$ both terminate.

Now, we analyze the winning probability of $\mathcal{A}_1$ and $\mathcal{A}_2$ when $\mathcal{A}$ wins. Note that $\mathcal{A}$ can win by violating one of the following cases:

1) The non-$\perp$ session identifiers of ePIA token (resp. server) sessions do not collide with each other, see Line 37 - 40 in Figure 8.
In this case, $\mathcal{A}_1$ also wins by Line 8 - 9 in Figure 2.
2) The partnered token and server sessions must have the identical agreed content unless the registration context on the token is corrupted, see Line 42 in Figure 8.
In this case, $\mathcal{A}_1$ also wins by Line 12 in Figure 2.
3) The non-$\perp$ session identifiers of ePACA token (resp. client) sessions that completed Bind algorithm do not collide with each other, see Line 44 - 45 in Figure 8.
In this case, $\mathcal{A}_2$ also wins by Line 9 - 10 in Figure 6.

4) During the registration interaction, The ePIA token and server sessions must partner with each other and the authorized command message and tag must have been output by one of the non-compromised partners of the ePACA token session without corrupting its setup user, see Line 47 - 50 in Figure 8.
In this case, we separately consider the case whether the condition regarding PIA or PACA sessions is violated. For each $(S', x, T', y, y', C', z, m_{\mathsf{rch}}, m_{\mathsf{rcom}}, t_{\mathsf{rcom}}, m_{\mathsf{rrsp}}) \in \mathcal{L}_{\textsc{Register}}$
   a) If $\bar{\pi}^x_S.\mathsf{sid} \neq \bar{\pi}^y_{T'}.\mathsf{sid}$, this is impossible since it is orthogonal to the definition of session partner (and session identifiers). Recall that partnering identifies token and server sessions that are successfully communicate with each other and is achieved via the coincidence of the session identifiers, as described in Section IV-C.
   b) Otherwise, $\mathcal{A}_2$ can trivially win by the Line 11 - 14 in Figure 6.
5) The token T that was registered with S, must own an ePIA session $\bar{\pi}^i_T$ that is partnered with $\bar{\pi}^i_S$ and produce a response message unless T's registration context of S is corrupted,see Line 52 - 56 in Figure 8.
In this case, we separately consider whether there exists j such that $\bar{\pi}^i_T$ is partnered with $\bar{\pi}^i_S$.
   a) If such j does not exist, then $\mathcal{A}$ can win only when $(S, T) \in \mathcal{L}_{\mathsf{frsh}}$. This means, $\mathcal{A}_1$ can also win auth experiment by Line 8 - 8 in Figure 6.
   b) Otherwise, such j exists. This means, the adversary $\mathcal{A}_1$ must have queried the oracle $\textsc{Response}(T, j, m_{\mathsf{acom}})$ to its challenger $\mathcal{C}_1$ for some command message m_{acom}. Recall that such query can only be made when $\mathcal{A}$ queries $\textsc{Response}((T, j, j'), m_{\mathsf{acom}}, t, d)$ for some $(j', m_{\mathsf{acom}}, t, d)$. So, the adversary $\mathcal{A}$ wins by the condition $\not\exists (j', m_{\mathsf{acom}}, t, d, m_{\mathsf{arsp}})$ such that $(T, j, j', m_{\mathsf{acom}}, t, d, m_{\mathsf{arsp}}) \in \mathcal{L}_{\textsc{Response}}$ with probability 0.
6) The above response message must be produced after an ePACA session $\pi^{j'}_T$ validates some authorized command m_{acom} and tag t with the approval from user, see Line 58 - 58 in Figure 8.
In this case, the adversary $\mathcal{A}_2$ can trivially win SUF-t$'$ experiment by Line 8 - 8 in Figure 6.
7) The above command m_{acom} and tag t must be authorized by a client ePACA session π^k_C that is partnered with $\pi^{j'}_T$ for some challenge message m_{rch} that was produced by the ePIA session $\bar{\pi}^i_S$, unless π^k_C is compromised or the PIN that sets up token T has been corrupted, see Line 61 - 66 in Figure 8.
We separately consider the cases whether m_{acom} and tag t are authorized by a client ePACA session π^k_C that is partnered with $\pi^{j'}_T$:
   a) If $(C, k, m_{\mathsf{acom}}, t) \notin \mathcal{L}_{\textsc{Auth}}$ for $(C, k) \leftarrow \mathsf{bindPartner}(T, j')$, then $\mathcal{A}_2$ can trivially win the SUF-t$'$ experiment by the Line 11 - 14 in Figure 6.
   b) Otherwise $(C, k, m_{\mathsf{acom}}, t) \in \mathcal{L}_{\textsc{Auth}}$. Note that $\textsc{Auth}$ oracle is only queried by $\mathcal{A}_2$ when $\mathcal{A}$ queries $\textsc{Challenge}$ or $\textsc{Register}$ oracles and that m_{acom} is the command message at authentication phase. This means, $\mathcal{A}$ must have queried $\textsc{Challenge}((S', i'), (C, k), \mathsf{tb}, UV)$ for some $(S', i', \mathsf{tb}, UV)$ that outputs m_{acom} and t. Moreover, recall that $\mathcal{A}$ has queried $\textsc{Response}((T, j, j'), m_{\mathsf{acom}}, t, d)$. By the definition of PIA session identifiers, we have that $\bar{\pi}^j_T.\mathsf{sid} = \bar{\pi}^{i'}_{S'}.\mathsf{sid}$. Furthermore, recall that $\bar{\pi}^j_T.\mathsf{sid} = \bar{\pi}^i_S.\mathsf{sid}$. It then holds that

$$\bar{\pi}^i_S.\mathsf{sid} = \bar{\pi}^j_T.\mathsf{sid} = \bar{\pi}^{i'}_{S'}.\mathsf{sid}$$

Recall that we have ensured that the non-$\perp$ session identifiers of PIA token (resp. server) sessions do not collide with each other in the Condition 1. So, it holds that $(S', i') = (S, i)$.
This means, $\mathcal{A}$ has queried $\textsc{Challenge}((S, i), (C, k), \mathsf{tb}, UV)$ for some tb and UV. Consequently, there must exist $(S, i, C, k, m_{\mathsf{ach}}, m_{\mathsf{acl}}, m_{\mathsf{acom}}, t) \in \mathcal{L}_{\textsc{Challenge}}$ for some m_{ach} and m_{acl}. The adversary $\mathcal{A}$ wins via this case with probability 0.

To sum up, when every Compl adversary $\mathcal{A}$ wins ua experiment against the composition of the ePIA scheme Σ and the ePACA scheme Π, then the Compl adversaries $\mathcal{A}_1$ or $\mathcal{A}_2$ must be able to win in the auth experiment against the underlying ePIA scheme Σ or in the SUF-t$'$ experiment against the underlying ePACA scheme Π, which implies the following inequality and concludes the proof.

$$\mathsf{Adv}^{\mathsf{ua}}_{\Sigma+\Pi,\mathsf{Compl}}(\mathcal{A}) \leq \mathsf{Adv}^{\mathsf{auth}}_{\Sigma,\mathsf{Compl}}(\mathcal{A}_1) + \mathsf{Adv}^{\mathsf{SUF\text{-}t'}}_{\Pi,\mathsf{Compl}}(\mathcal{A}_2)$$

□

Appendix L
Flaws in Barbosa et al. [2]

In this section, we collect the flaws in the Proof for CTAP 2.0 (See Section D.3 in [2]) and clarify their impact on the security.

1) In Game 3 in [2], Barbosa et al. "replace all authenticated tags $t_p \leftarrow \mathsf{H}_2(\tilde{K}, c_p)$ computed in Setup queries with independent random values $\tilde{t}_p$" without any assumption on the underlying symmetric encryption scheme SKE in the same Setup queries. Here, c_p encrypts the pin pin_U for some user U.
We claim that this is wrong. Recall that the key of the underlying SKE is also used in the derivation of t_p in Setup queries. Let's see the following trivial construction of SKE: The encryption algorithm inputs a symmetric key K and a message m simply outputs $c = (K, m)$. Under the usage of this SKE, the adversary in Game 2 receives $(c_p, t_p) = \Big((\tilde{K}, \mathsf{pin}_U), \mathsf{H}_2(\tilde{K}, \tilde{K}, \mathsf{pin}_U)\Big)$ but in Game 3 receives $(c_p, t_p) = \Big((\tilde{K}, \mathsf{pin}_U), \tilde{t}_p\Big)$ for a random $\tilde{t}_p$. The adversary can easily distinguish Game 2 and Game 3 by checking whether checking whether $t_p = \mathsf{H}_2(c_p[1], c_p)$, where $c_p[1]$ denotes the first component of c_p. This counterexample shows that the gap of the adversary's advantage in winning Game 2 and 3 in [2] is not necessarily negligible. In other words, the security of the composition of H_2 and SKE using the shared key cannot be simply reduced to the one of either component using a different key (even assuming that H' is modeled as random oracle).

In our proof, we instead rely the reduction on the conjectured $\mathsf{IND\text{-}1CPA\text{-}H_2}$ security of the underlying CBC mode SKE_1. This yields an additional upper bound $\epsilon^{\text{ind-1cpa-H}_2}_{\mathsf{SKE}_1}$. However, we stress that it is unknown how to formally reduce the hardness of $\mathsf{IND\text{-}1CPA\text{-}H_2}$ of CBC mode to other standard assumption. Similar to the argument given by Barbosa et al, we strongly suggest to block the usage of $\mathsf{puvProtocol}_1$, since using the same key across different primitives is very dangerous.

2) In Game 4 in [2], Barbosa et al. "replace all encrypted PINs c_p computed in SETUP queries with independent random values $\tilde{c}_p$" and reduce the security to the IND-1CPA security of the underlying CBC mode.
We claim that this is not absolutely true. Note that the symmetric keys $\tilde{K}$s are sampled randomly in their Game 1 and that the challenge ciphertext on each symmetric key $\tilde{K}$ can be queried at most once in the IND-1CPA experiment. Once two random symmetric keys collide, the reduction cannot simulate Game 4 correctly, since it cannot query two challenge ciphertexts on the same symmetric key.
In our proof, before the reduction to IND-1CPA as well as IND-1\$PA-LPC and IND-1CPA-H security, we ensure that all symmetric keys are distinct in respective puvProtocol, which yields an additional upper bound $\binom{q_{\text{SETUP}}+q_{\text{EXECUTE}}}{2}2^{2-\min\{l_1,l_3,l_5,l_6\}}$.

3) In Game 5 in [2], Barbosa et al. "replace all encrypted PIN hashes c_{ph} and encrypted pinTokens c_{pt} computed in EXECUTE queries with respectively $\tilde{c}_{ph}$ and $\tilde{c}_{pt}$ for an independent random values $\tilde{c}_p$" and reduce the security to the IND-1\$PA security of the underlying CBC mode.
We claim that this is wrong. Note that the Bind phase is not fully authenticated and that the adversary is able to send arbitrary message to tokens via the send oracle. When a token T receives some $(c'_{ph}, c'_{pt}) \neq (\tilde{c}_{ph}, \tilde{c}_{pt})$, in order to simulate Game 4 or 5 perfectly, the reduction is expected to check whether c'_{ph} can be decrypted to the PIN hash, which is the hash of the pin that sets up T, or not. However, this is impossible since the reduction does not know the symmetric key.
In our proof, we rely the corresponding steps to a new IND-1\$PA-LPC security of the underlying CBC mode with zero or randomized initial vector SKE_i for all $i \in \{1,2,3\}$, which yields an additional upper bound $q_{\text{EXECUTE}} \max\{\epsilon^{\text{ind-1\$pa-lpc}}_{\mathsf{SKE}_1}, \epsilon^{\text{ind-1\$pa-lpc}}_{\mathsf{SKE}_2}, \epsilon^{\text{ind-1\$pa-lpc}}_{\mathsf{SKE}_3}\}$. Of course, we also formally prove that such security is indeed achieved by SKE_i for all $i \in \{1,2,3\}$ in Section B.

APPENDIX M
CHANGELOG

We provide a summary of the main changes between versions here.

- v1.0, Aug 9: Initial release.
- v1.1, Aug 18: Our initial comparison to [3] did not take into account that some issues had been fixed in their eprint version [11]. Updated comments to reflect this, notably about comments about trust in registration phase.