


Towards post-quantum secure PAKE - A tight security proof for OCAKE in the BPR model

Nouri Alnahawi¹ * , Kathrin Hövelmanns² , Andreas Hülsing² ** , and Silvia Ritsch² *** 

¹ Darmstadt University of Applied Sciences, Germany

² Eindhoven University of Technology, The Netherlands

Abstract. We revisit OCAKE (ACNS 23), a generic recipe that constructs password-based authenticated key exchange (PAKE) from key encapsulation mechanisms (KEMs), to allow instantiations with post-quantum KEM like KYBER.

The ACNS23 paper left as an open problem to argue security against quantum attackers, with its security proof being in the universal composability (UC) framework. This is common for PAKE, however, at the time of this submission’s writing, it was not known how to prove (computational) UC security against quantum adversaries. Doing this becomes even more involved if the proof uses idealizations like random oracles or ideal ciphers.

To pave the way towards post-quantum security proofs, we therefore resort to a (still classical) game-based security proof in the BPR model (EUROCRYPT 2000). We consider this a crucial stepping stone towards a fully satisfying post-quantum security proof. We also hope that a game-based proof is easier to (potentially formally) verify.

We prove security of (a minor variation of) OCAKE, assuming the underlying KEM satisfies notions of ciphertext indistinguishability, anonymity, and (computational) public-key uniformity. Using multi-user variants of these properties, we achieve tight security bounds.

We provide a full detailed proof – something often omitted in publications on game-based security of PAKE. As a side-contribution, we demonstrate in detail how to handle password guesses, which is something we were unable to find in the existing literature at the time of writing.

Finally, we discuss which current PQC KEMs can be plugged into the proposed protocol and provide a concrete instantiation, accompanied by a proof-of-concept implementation and respective run-time benchmarks.

Keywords: Public-key cryptography, password-based authenticated key exchange, PAKE, CAKE, OCAKE, post-quantum cryptography, ROM, game-based security.

1 Introduction

A central problem of secure communication is how to securely agree on a shared secret key via public communication. The generic solution is called an authenticated key exchange (AKE) protocol, which usually uses public-key cryptography to agree on the shared secret. This is the basis of most modern secure communication protocols, including TLS, SSH, or WireGuard. The drawback of this solution is that it requires users to maintain a cryptographic key pair for authentication. As cryptographic keys are hard to memorize, they require secure storage with all the related challenges for usability. Hence, in many scenarios only the server is authenticated during the AKE protocol.

* N.A. was supported by National Research Center for Applied Cyber-Security ATHENE.

** A.H. was supported by an NWO VIDI grant (Project No. VI.Vidi.193.066).

*** S.R. is part of the Quantum-Safe Internet (QSI) ITN which received funding from the European Union’s Horizon-Europe programme as Marie Skłodowska-Curie Action (PROJECT 101072637 - HORIZON - MSCA-2021-DN-01)

Users are often authenticated via the use of human-memorable passwords within the already established communication that is secured via the shared secret. This is the case as passwords are far easier to handle for humans. However, this means that additional measures have to be taken to link the authentication to the session secured via the shared secret. A way out of this is to use a user password for the purpose of authentication in an AKE. This is called password-authenticated key exchange (PAKE). In general, PAKE allow the use of any low-entropy shared secret (like a password or a PIN) to provide the agreement with authentication. Hao and van Oorschot classify in their SoK on PAKE[HvO22] real-world use-cases of PAKE protocols and the currently used PAKEs related to them. These include credential recovery using the SRP-6a protocol in iCloud; device pairing (mostly IoT or embedded devices), using the PACE³ protocol in eIDs or eMRTDs to prevent skimming, as well as Dragonfly in WPA3 (standard for WiFi connection establishment); and E2E secure channel establishment using the J-PAKE⁴ protocol in Thread. A few years ago, interest in the design and theory surrounding PAKE was increased further when the Crypto Forum Research Group (CFRG) - advisory body to the Internet Engineering Task Force (IETF) - performed a selection process for new PAKE standards. The defined requirements⁵ emphasized high efficiency and simultaneously high security, supported by a formal security proof.

The quantum threat. While the CFRG announced two winners in 2020, all proposals (including the winners OPAQUE [JKX18] and CPace [AHH23]) have in common that they rely on the computational hardness of the Diffie-Hellman (DH) problem – something they share with most currently deployed public-key cryptography. Since Shor famously showed how to solve this problem on a quantum computer, public-key cryptography based on DH – including the proposed PAKE protocols – do not offer resilience against quantum attacks. As a first step towards dealing with the quantum threat, the National Institute of Standards and Technology (NIST) posed a call for proposals in 2017 with the goal to develop quantum-resistant standards for public-key encryption (PKE) and digital signature schemes, which are the most fundamental building blocks underpinning public-key cryptography. More accurately, rather than aiming at PKE schemes, NIST aimed at key encapsulation mechanisms (KEMs). A KEM is similar to a PKE, but focused on the use-case of establishing a shared secret by sending a symmetric key in encrypted form. This allows the encapsulation algorithm to internally chose the key, instead of taking it as an input, and then return it together with a ciphertext that “encapsulates” it. This change in functionality allows for more efficient constructions as the key cannot be adversarially chosen during attacks. The NIST process recently selected Kyber [BDK⁺18] as KEM and Dilithium [DKL⁺18], Falcon [PFH⁺22], and SPHINCS⁺ [BHK⁺19] as signatures for standardization. In the context of this work we are only interested in KEMs. It should be noted that KEMs are fundamentally different from the Diffie-Hellman key exchange (DHXX), although they serve the same purpose. The DHXX is a non-interactive key exchange (NIKE) with a lot of additional algebraic structure. In comparison, when KEMs are used for key exchange, the resulting protocol is interactive, and they do not provide additional structure generically (although specific proposals do). While NIST is continuing the selection process for further KEM and signature schemes, there is no process for NIKE. The reason is the lack of an efficient candidate with reliable security at this time (first proposals exist though [CLM⁺18, DKS18, RS06, Cou06]).

Designing post-quantum PAKE. A major challenge regarding the transition to post-quantum secure systems, is to transform existing protocols into post-quantum secure ones, replacing quantum-vulnerable building blocks by the available KEM and signatures. A general challenge – which also concerns PAKE – is that the NIST proposals cannot replace the Diffie-Hellman key exchange in a

³ <https://www.rfc-editor.org/rfc/rfc6631.html>

⁴ <https://www.rfc-editor.org/rfc/rfc8236>

⁵ Specified in datatracker.ietf.org/doc/html/rfc8125, and expanded upon in ietf.org/proceedings/104/slides/slides-104-cfrg-pake-selection-01.pdf

‘plug-n-play’ way: most PAKE protocols rely on the additional algebraic properties of the group operation in DHXX which are not known to be offered by KEMs. This gave rise to the requirement to design new PAKE protocols, preferably in a way that

- is versatile, i.e., designed in a way that works for various PQC proposals or even pre- and post-quantum hybrids (instead of being tied to a specific proposal’s internal workings);
- works with already proposed algorithms (to avoid having to introduce new primitives);
- avoids complex mapping operations used, e.g., by elliptic-curve-based protocols; and
- satisfies state-of-the-art security notions (supported by a formal security proof).

The first property is motivated by the idea of crypto agility, i.e., the option to easily replace a building block in case of successful cryptanalysis. Additionally, this also allows for the possibility to select different candidates depending on specific performance requirements like, e.g., fast computations or low memory consumption. A candidate proposal that aims at fulfilling the above requirements is OCAKE, recently proposed by Beguinet, Chevalier, Pointcheval, Ricosset, and Rossi [BCP⁺23]. OCAKE is based on the EKE paradigm [BM92], but replaces the need for Diffie-Hellman by building generically on suitable KEMs, thereby setting a foundation to build quantum-resistant PAKE.

Towards post-quantum security of PAKEs. Modern security notions and proofs for PAKE are usually given in the universal composability (UC) framework introduced in [Can01] (see full version of this paper for a list of examples). This is also the case for OCAKE. While security proofs in the UC framework are desirable in the sense that UC-proven building blocks can always be composed securely, they come with a limitation when addressing post-quantum security: so far, we are not aware of works that consider computational security against quantum attackers in the UC framework. Hence, it is not known how these proofs can be translated into a setting that considers quantum attacks. At the same time, there is continuous progress in lifting game-based security results to a setting with quantum adversaries. Up to minor complications, such lifts are straight-forward as long as no idealized models are used [Son14]. However, when proofs are given in idealized models like the random oracle model (ROM) and/or the ideal cipher (IC) model, lifting becomes less straight-forward. This is also the case for PAKEs. Both the ROM and the IC model do not account for quantum attacks and therefore make it necessary to adapt both the models and the proofs. By now, we have a somewhat well-understood quantum counterpart to the ROM, called quantum-accessible ROM (QROM) [BDF⁺11]. Ongoing efforts to develop the necessary techniques for lifting proofs to the QROM are well under way (see, e.g., [Zha19, DFMS21, CFHL21, GHHM21, HHM22, DFMS22]). Similar results for the quantum-accessible ideal cipher model are still extremely limited, but a model exists and first proofs have been done [HY18]. This suggests that game-based security notions and proofs may be a good target for proving security against quantum attacks. There are several game-based security models for PAKE [BPR00, AFP05, Lan16]. What is still missing are detailed formal proofs for PAKE protocols that could be lifted.

Our contribution. In this work, we progress towards a PAKE protocol with proven security against quantum adversaries. Towards this end, we analyse the security of a minor variation of OCAKE. We present a rigorous game-based security proof of the protocol in the BPR model for PAKE proposed by Bellare, Pointcheval, and Rogaway [BPR00]. We give a concrete security bound rather than an asymptotic relation, thereby allowing to reason about concrete parameter instantiations. To achieve a tight bound, we make use of multi-user security notions. As a side contribution, we show how to formally treat password guesses in a detailed game-based proof. So far, we are only aware of detailed proofs in which this step is hidden within a proof in the generic group model [BFK09]. Interestingly, in UC, this step is easy to formalize, but verifying the security reasoning can be challenging. Our proposal differs from OCAKE in two minor points. First, we omit session identifiers which are included in OCAKE (to enable a proof in the UC framework), but are not necessary for a game-based proof. Second, we consciously add a final key confirmation message that achieves explicit

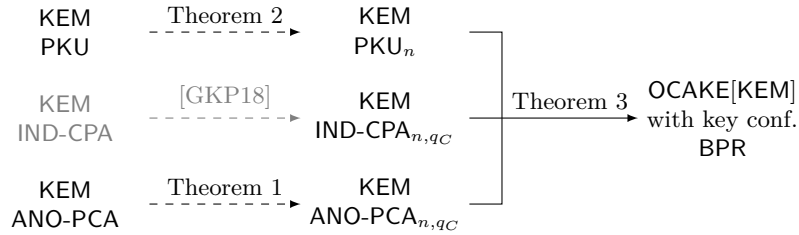


Fig. 1: Our results. Solid (dashed) arrows indicate tight (non-tight) reductions.

mutual authentication. This is not necessary to prove security in the BPR model, but we consider explicit authentication a relevant feature of a protocol. (BPR already discussed that it can be added by adding key confirmation.)

A limitation. Although we ultimately aim for security against quantum adversaries, our proof is still in the (classical) ideal cipher and random oracle model. While it would have likely been possible to replace the ROM by the QROM for this proof, handling the ideal cipher seems more challenging due to the limited known proof techniques. This work presents a solid foundation for future work in which either new techniques to lift results with ideal ciphers are developed, or the use of ideal ciphers is omitted.

Organization of this paper. After recalling basic notions (including the relevant security notions for KEMs) in Section 2 and introducing multi-user notions for KEMs in Section 2.1, we describe the OCAKE protocol extended with a key confirmation in Section 3. We recall the BPR security model for PAKE in Section 4, and then prove OCAKE secure in Section 5.

1.1 Concurrent and related work

A recent publication [PZ23] gave a game-based proof for CAKE, another protocol from the [BCP⁺23] PAKE family. Having proofs for different PAKEs from the same family surely is to be welcomed since it establishes trust in the family’s overall design approach, we however wanted to also point out a few advantages of this work:

Protocol advantages. Comparing to CAKE, our protocol avoids the usage of ideal ciphers (ICs) for its second message and thus reduces overhead in terms of both necessary computations and dealing with the IC during the proof. So far, IC handling still poses a major barrier when proving security against quantum attackers, we thus followed the maxim ‘the less IC, the better’. (Although it cannot be ruled out that any IC involvement at all already hinders a proof against quantum attacks.) As stated in [PZ23], CAKE was chosen over OCAKE because OCAKE only was known to achieve weak forward secrecy. This limitation seems to stem from the comparably weak anonymity requirement made in [BCP⁺23], and is overcome by strengthening the requirement in a way such that it still is achieved by – amongst others – the post-quantum KEMs Kyber [MX23], McEliece, NTRU, BIKE and SIKE (all [Xag22]), as well as FrodoKEM [GMP22].

KEM requirement advantages. Both works require anonymity and indistinguishability notions. In [PZ23], both notions deviate from their standard variant by providing the attacker with an additional oracle (called PCO). We offer two independent improvements: 1.) Our indistinguishability notion does without the additional PCO attack surface and thus leads to an easier-to-analyze (more standard) requirement with potential for more efficient instantiations. 2.) We attenuate the anonymity requirement (again creating space for efficiency improvements):

- In [PZ23], the number of PCO queries may be high – it’s bounded by how many random oracle queries an attacker could reasonably perform. In comparison, we only need to allow a single query, which may allow simpler and more efficient designs (see, e.g., [HV22]).
- To adapt [PZ23] to the QROM, PCO needs to be made quantum-accessible, and it is likely that quantum access to PCO limits with which parameters KEM can still be instantiated securely. In comparison, our proof technique would allow to still work with a classically-accessible PCO, even in the QROM, which simplifies both the analysis and the KEM design.

Since multi-instance security of lattice-based cryptosystems (such as Kyber) has recently been subject to debate [Ber22], we also included (generic, non-tight) single-to-multi-user results that enable a proof based on single-user security.

Proof advantages. Both proofs deal with attackers that correctly guess a password by defining a respective ‘bad’ event in the security game and proving its probability to be small. Our probability term compares favorably to the one in [PZ23]: the term in [PZ23] involves the number of *all* established sessions, including observed honest protocol runs (which will be very large in practice), whereas ours only involves the number of sessions with which an attacker can actively interfere (which in practice will be limited). We stress, however, that the term in [PZ23] can easily be shrunk down to our term with a more fine-grained analysis.

Additionally, we believe it might be easier to (formally) verify our treatment of ‘bad’ event – in [PZ23], the event is treated by raising an internal flag and performing flag-dependent changes to the game. We early on change the game such that correct guesses are ‘punished’ by aborting and analyse how this probability is affected by subsequent game modifications. Second, the recognition of the ‘bad’ event differs due to protocol differences. CAKE encrypts both protocol messages via the ideal cipher, [PZ23] can thus identify password guesses by connecting the protocol message to a previous ideal cipher query. In our modification of OCAKE, the second message is not IC-encrypted. We can, however, identify password guesses via the included authentication tag since it is computed using a hash function (modelled as a random oracle). The protocol differences also affects how the simulation deals with server impersonation. Since an attacker may corrupt a server password during a protocol run, the simulated client must be able to respond to ciphertexts generated by an attacker in possession of the public key. [PZ23] cover this case by simulating the involved random oracle in a certain way (‘oracle patching’). In particular, the random oracle internally calls the plaintext checking oracle upon each query. Our authentication tag is the reason why we do not need a random oracle patching technique- we can directly identify a password guess by connecting the tag to a previous random oracle query. This allows us to a) limit the number of PCO queries to 1, and b) work with a non-quantum version of PCO even when adapting the proof to the QROM.

Other related work. There already exists some work on PAKE protocols based on PQC primitives in the literature. However, these designs are not generic and most of them rely directly on the hardness assumptions of the LWE (Learning with Errors) lattice problem, its variants MLWE and RLWE, and a smaller number based on isogenies (i.e., CSIDH). In addition to the choice of underlying hardness assumption, PAKEs can be divided into two classes: augmented (asymmetric) and balanced (symmetric). Most proposed PAKEs are of the augmented PAKE class, which aim to provide protection against server compromise by not storing the (full) password on the server. However, these proposals commonly require a trusted setup (e.g., using a CRS (Common Reference String) or identity based signatures) that takes place prior to the actual authenticated key agreement. Works following this trusted-setup design are based on lattices [XHCC17, CAK18, LZJY19, DBK20, WCL⁺22, GSG⁺23, CKS23], or isogenies [ZHS14, AEK⁺22]. Others make use of Smooth Projective Hash Functions (SPHF) based on PQC assumptions and lattice primitives such as [KV09, ZY17, LW18, KAA19, JGH⁺20, YGS⁺20, LWM20, TLZ⁺21, LW22]. The works utilizing SPHF incorporate Non-Interactive Zero-Knowledge Proof System (NIZKs) in most cases. Other

proposals follow a Diffie-Hellman (DH)-like approach, where the password (or a password-derived value) is used to generate a common generator for commutative key agreement. Works following this design are mainly based on isogenies [TSJL18, ZG17], since the primitive from this mathematical structure can be utilized in a manner similar to the classical DH or ECDH key agreement with a common generator. The protocols (O)CAKE [BCP⁺23] are in the class of balanced PAKEs, and use the long-lived secret (i.e., the password) to directly authenticate a public key of the underlying PKE for the following key agreement. This can be done by using the password (or a password derived symmetric key) as the encryption key of a block-cipher to encrypt the public key (EKE-style in the IC model) as in [TY19], or by using its hash value to alter or "mask" the public key (PAK-style in ROM) as in [DAL⁺17, YGWX19, RG21, RGW23, SA23]. All of the works mentioned here directly use a PQC PKE rather than a PQC KEM, most of them provide a game-based (BPR) security proof in either the standard model or the Random Oracle model (ROM), with a few exceptions that provide a UC proof. Nevertheless, one cannot consider a comparison between our contribution and the previous constructions, due to major design differences.

Acknowledgements. We would like to thank Thomas Pöppelmann for valuable discussions about the design of PAKE protocols, and Afonso Arriaga, Manuel Barbosa, Paul Crowley, Stanislaw Jarecki, and Marjan Skrobot for valuable discussions.

2 Preliminaries

In the following we recall the ideal cipher model and provide definitions for key encapsulation mechanisms (KEM). We assume the reader is familiar with the random oracle model (ROM) [BR93].

The Ideal Cipher Model. We prove security of the OCAKE protocol in the ideal cipher model [Bla06]. Analogously to the ROM for hash functions, the ideal cipher (IC) is an idealized description of a block cipher.

Definition 1 (Block Cipher (BC)). *A block cipher of block length n and key length k consists of two algorithms $BC.\text{enc} : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ and $BC.\text{dec} : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ such that for every plaintext $m \in \{0, 1\}^n$ and key $k \in \{0, 1\}^k$, decryption undoes encryption: $IC.\text{dec}(k, IC.\text{enc}(k, m)) = m$.*

Definition 2 (Ideal Cipher (IC)). *An ideal cipher is a collection of random permutations indexed by a key, to which all parties (including the adversary) are given oracle access. I.e., it is a pair of random functions $IC.\text{enc}, IC.\text{dec} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{M}$, such that $IC.\text{dec}(k, IC.\text{enc}(k, m)) = m$ and $IC.\text{enc}(k, IC.\text{dec}(k, m)) = m$ for all k, m in $\mathcal{K} \times \mathcal{M}$.*

We start with the functional definition of KEMs, then discuss their security.

Definition 3 (Key Encapsulation Mechanisms (KEMs)). *A KEM is a triple of algorithms $KEM = (\text{KGen}, \text{Encap}, \text{Decap})$, together with a public key space \mathcal{PK} and secret key space \mathcal{SK} .*

- $\text{KGen} \rightarrow (pk, sk)$: *On empty input probabilistically **return** key pair (pk, sk) , where pk also defines a finite key space \mathcal{K} and a ciphertext space \mathcal{C} .*
- $\text{Encap}(pk) \rightarrow (c, K)$: *On input pk probabilistically **return** a pair $(K, c) \in \mathcal{K} \times \mathcal{C}$. We call c the encapsulation of the key K .*
- $\text{Decap}(sk, c) \rightarrow K$: *On input sk and ciphertext c deterministically **return** a key $K \in \mathcal{K}$.*

Definition 4 (δ -Correctness (average-case)). *We say that KEM is average-case $(1 - \delta)$ -correct if*

$$\Pr[\text{Decap}(sk, c) = K \mid (c, K) \leftarrow \text{Encap}(pk)] \geq 1 - \delta,$$

where the probability is taken over $(pk, sk) \leftarrow \text{KGen}()$ and the random coins of Encap .

We use three security notions for KEMs: ANonymity under Plaintext- Checking Attacks (ANO-PCA), an extension of the anonymity notion given in [BBDP01, GMP22], INDistinguishability under Chosen- Plaintext- Attacks (IND-CPA), and Public Key Uniformity. We begin with the first two as they share the plaintext checking oracle (PCO). The presence of a PCO may look artificial at a first glance. Looking ahead, we will need it in our PAKE proof to simulate a proper reaction to a particular corruption-impersonation pattern. In our proof we require that attackers could mistake any element of the public-key space for an honestly generated public key. Concretely, we formalise this below as a public-key uniformity game that asks the attacker to distinguish honestly generated public keys from uniformly random ones. This property was introduced as *fuzziness* in [BCP⁺23], where it was also proven for the post-quantum KEM Kyber. There also exist stronger (statistical) definitions – e.g., [BCJ⁺19] proved statistical public-key uniformity of discrete-log-based PKE schemes, due to public keys being uniformly chosen group elements.

Definition 5 (Public-key Uniformity (PKU)). *Let $\text{KEM} = (\text{KGen}, \text{Encap}, \text{Decap})$ be a key encapsulation mechanism with public-key space \mathcal{PK} . We define the PKU game as in Fig. 2, relative to challenge bit b , and the respective advantage function of an adversary \mathcal{A} against KEM as*

$$\text{Adv}_{\text{KEM}}^{\text{PKU}}(\mathcal{A}) := |\Pr[\text{PKU}^0(\mathcal{A}) \Rightarrow 0] - \Pr[\text{PKU}^1(\mathcal{A}) \Rightarrow 0]| .$$

2.1 Multi-user notions for KEMs

Multi-user security notions were first introduced for public-key encryption in [BBM00] and then extended to IND-CPA security of KEMs in [GKP18]. To obtain a tight security proof for our PAKE protocol, we now define multi-user (and multi-challenge) counterparts for the previously introduced security notions. For IND-CPA and ANO-PCA, the respective notion ($\text{IND-CPA}_{n,q_C}$ and $\text{ANO-PCA}_{n,q_C}$) models the setting where an adversary can ask for up to q_C many challenges for each of n many different key pairs. The adversary wins if it successfully attacks *any* of the up to nq_C challenges. We will also use a multi-user notion of public-key uniformity (PKU_n), where the adversary is tasked with distinguishing a vector of n many honestly generated public keys from a vector that consists of elements picked uniformly from the public key space. We include generic reductions between single- and multi-user security in the full version of this paper.. The loss that occurs in these reductions reflects how session guessing would introduce reduction losses in our PAKE proof, where the multi-user notions replaced by single-user notions.

Definition 6 (Multi-user security notions for KEM). *Let KEM be a key encapsulation mechanism with public-key space \mathcal{PK} and key space \mathcal{K} . For integers n and q_C , we define the PKU_n game, the $\text{IND-CPA}_{n,q_C}$ game and the $\text{ANO-PCA}_{n,q_C}$ game as in Figures 2, Fig. 3 and 4, each relative to challenge bit b , and the respective advantage function of an adversary \mathcal{A} against KEM as*

$$\begin{aligned} \text{Adv}_{\text{KEM}}^{\text{IND-CPA}_{n,q_C}}(\mathcal{A}) &:= |\Pr[\text{IND-CPA}_{n,q_C}^0(\mathcal{A}) \Rightarrow 0] - \Pr[\text{IND-CPA}_{n,q_C}^1(\mathcal{A}) \Rightarrow 0]| , \\ \text{Adv}_{\text{KEM}}^{\text{ANO-PCA}_{n,q_C}}(\mathcal{A}) &:= |\Pr[\text{ANO-PCA}_{n,q_C}^0(\mathcal{A}) \Rightarrow 0] - \Pr[\text{ANO-PCA}_{n,q_C}^1(\mathcal{A}) \Rightarrow 0]| \text{ and} \\ \text{Adv}_{\text{KEM}}^{\text{PKU}_n^{(n)}}(\mathcal{A}) &:= |\Pr[\text{PKU}_n^0(\mathcal{A}) \Rightarrow 0] - \Pr[\text{PKU}_n^1(\mathcal{A}) \Rightarrow 0]| . \end{aligned}$$

It is known [GKP18, Lemma 3.2] that ‘plain’ IND-CPA security lifts generically to its multi-user counterpart with a loss of $n \cdot q_C$, where n is the number of users (the number of public keys) and q_C is the maximal number of challenge queries per public key. We now show that this also holds for anonymity for adversaries that also have access to a plaintext checking oracle (ANO-PCA) and public-key uniformity (PKU) (with a loss of n). The obtained generic bounds may be overly pessimistic for specific KEMs, considering that a KEM’s underlying structure may allow for tighter reasoning. However, since multi-instance security of lattice-based cryptosystems (such as Kyber) has recently

$\text{PKU}^b(\mathcal{A})$	$\text{PKU}_n^b(\mathcal{A})$
01 $(pk_0, sk_0) \leftarrow \$ \text{KGen}$	05 for $j \in [n]$
02 $pk_1 \leftarrow \$ \mathcal{PK}$	06 $(pk_{j,0}, sk_{j,0}) \leftarrow \$ \text{KGen}$
03 $b' \leftarrow \mathcal{A}(pk_b)$	07 $pk_{j,1} \xleftarrow{\text{unif}} \mathcal{PK}$
04 return b'	08 $\mathbf{pk}.\text{append}(pk_{j,b})$
	09 $b' \leftarrow \mathcal{A}(\mathbf{pk})$
	10 return b'

Fig. 2: Public-key uniformity game PKU for KEM, and its multi-user counterpart PKU_n for n many users. Public-key uniformity is also known as fuzziness.

Game $\text{IND-CPA}_{n,q_C}^b$	Chall _{q_C} ^{b} (j)
11 for $i \in [n]$	16 $(c, K_0) \leftarrow \$ \text{Encap}(pk_j)$
12 $(pk_i, sk_i) \leftarrow \$ \text{KGen}$	17 $K_1 \xleftarrow{\text{unif}} \mathcal{K}$
13 $\mathbf{pk}.\text{append}(pk_i)$	18 return (c, K_b)
14 $b' \leftarrow \mathcal{A}^{\text{Chall}}(\mathbf{pk})$	
15 return b'	

Fig. 3: Multi-user indistinguishability game $\text{IND-CPA}_{n,q_C}$ for KEM, for n many users. Challenge oracle **Chall** can be queried at most q_C many times per user.

been subject to debate [Ber22], we also included (generic, non-tight) single-to-multi-user results that enable a proof based on single-user security in the full version.

Theorem 1. *Let KEM be a key encapsulation mechanism. For any $\text{ANO-PCA}_{n,q_C}$ adversary \mathcal{A} against KEM, there exists an ANO-PCA adversary \mathcal{B} against KEM such that*

$$\text{Adv}_{\text{KEM}}^{\text{ANO-PCA}_{n,q_C}}(\mathcal{A}) \leq n \cdot q_C \cdot \text{Adv}_{\text{KEM}}^{\text{ANO-PCA}}(\mathcal{B}).$$

and the running time of \mathcal{B} is about that of \mathcal{A} .

Proof. We reduce single-user ANO-PCA anonymity of KEM to multi-user anonymity $\text{ANO-PCA}_{n,q_C}$, using a very similar hybrid argument. Let \mathcal{A} be an adversary in the $\text{ANO-PCA}_{n,q_C}$ game defined in Fig. 4. Consider the sequence of hybrid games $\mathbf{G}_{j,i}$ that successively changes the game for \mathcal{A} from $b = 1$ (all challenges built using \mathbf{pk}_1) to $b = 0$ (all challenges built using \mathbf{pk}_0). We will iterate over j/i , the number of public keys/queries per public key for which we will implement the change: In game $\mathbf{G}_{j,i}$, oracle **Chall**(j') upon the i' -th query uses

- the respective public key $pk_{0,j'}$ from \mathbf{pk}_0 if $(j' < j)$ or if (both $j' = j$ and $i' < i$),
- the respective public key $pk_{1,j'}$ from \mathbf{pk}_1 if $j' > j$ or if (both $j' = j$ and $i' \geq i$).

Using the triangle inequality yields

$$\begin{aligned} \text{Adv}_{\text{KEM}}^{\text{ANO-PCA}_{n,q_C}}(\mathcal{A}) &= \left| \sum_{j=0}^{n-1} \sum_{i=0}^{q_C-1} \Pr[\mathbf{G}_{j,i}^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathbf{G}_{j,i+1}^{\mathcal{A}} \Rightarrow 1] \right| \\ &\leq \sum_{j=0}^{n-1} \sum_{i=0}^{q_C-1} |\Pr[\mathbf{G}_{j,i}^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathbf{G}_{j,i+1}^{\mathcal{A}} \Rightarrow 1]| . \end{aligned}$$

Game ANO-PCA $_{n,q_C}^b(\mathcal{A})$	Chall $_{q_C}^b(j)$	1-PCO(j, c, K)	//once per j
01 for $j \in [n]$	08 $(c_0, K_0) \leftarrow \text{\$ Encap}(pk_{0,j})$	12 if $c \notin \mathcal{L}_j^*$	
02 $(pk_{0,j}, sk_{0,j}) \leftarrow \text{\$ KGen}$	09 $(c_1, K_1) \leftarrow \text{\$ Encap}(pk_{1,j})$	13 $K' \leftarrow \text{Decap}(sk_{0,j}, c)$	
03 $(pk_{1,j}, sk_{1,j}) \leftarrow \text{\$ KGen}$	10 $\mathcal{L}_j^* \leftarrow \mathcal{L}_j^* \cup \{c_b\}$	14 return $[K = K']$	
04 $\mathbf{pk}_0.\text{append}(pk_{0,j})$	11 return (c_b, K_b)	15 else return \perp	
05 $\mathbf{pk}_1.\text{append}(pk_{1,j})$			
06 $b' \leftarrow \mathcal{A}^\mathcal{O}(\mathbf{pk}_0, \mathbf{pk}_1)$			
07 return b'			

Fig. 4: Multi-user anonymity game ANO-PCA $_{n,q_C}$ for KEM, for n many users. The collection \mathcal{O} of \mathcal{A} 's oracles is $\mathcal{O} = \{1\text{-PCO}, \text{Chall}_{q_C}^b\}$. We make the same query restrictions and initialisation conventions as in Fig. 3.

where we made the convention that $\mathbf{G}_{j,q_C} := \mathbf{G}_{j+1,q_0}$ to handle index wrap-arounds.

We now give single-user ANO-PCA adversaries \mathcal{B}_{ji} to upper bound the summands $|\Pr[\mathbf{G}_{j,i}^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathbf{G}_{j,i+1}^{\mathcal{A}} \Rightarrow 1]|$: \mathcal{B}_{ji} receives a single set of two challenge public keys, a ciphertext, and an encapsulated key, so (pk_0, pk_1, c^*, K^*) , from its ANO-PCA challenger. \mathcal{B}_{ji} will use its challenge input to simulate either $\mathbf{G}_{j,i}$ or $\mathbf{G}_{j,i+1}$: \mathcal{B}_{ji} generates 2 vectors of $n - 1$ many public keys $\mathbf{pk}_0, \mathbf{pk}_1$ using KGen and turns them into vectors of length n by inserting its own challenge public keys at the j -th position. \mathcal{B}_{ji} then runs \mathcal{A} on input $\mathbf{pk}_0, \mathbf{pk}_1$ and answers \mathcal{A} 's challenge queries as follows: upon the i' -th query to $\text{Chall}(j')$, \mathcal{B}_{ji} responds with

- a challenge constructed using the respective public key $pk_{0,j'}$ from \mathbf{pk}_0 if $j' < j$, or if both $j' = j$ and $i' < i$
- a challenge constructed using the respective public key $pk_{1,j'}$ from \mathbf{pk}_1 if $j' > j$, or if both $j' = j$ and $i' > i$
- its own challenge (c^*, K^*) if $j' = j$ and $i' = i$

For all vector positions except for j , \mathcal{B}_{ji} possesses the secret key belonging to pk_j , thereby being able to respond to all of \mathcal{A} 's respective 1-PCO queries. If \mathcal{A} queries the 1-PCO with index j , \mathcal{B} forwards the query to its own 1-PCO oracle. When \mathcal{A} outputs a guess to \mathcal{B}_{ji} , \mathcal{A} forwards the guess to its own challenger. Since \mathcal{B}_{ji} perfectly simulates $\mathbf{G}_{j,i}$ if its own challenge bit is 1, and $\mathbf{G}_{j,i+1}$ if its own challenge bit is 0, we have

$$|\Pr[\mathbf{G}_{j,i}^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathbf{G}_{j,i+1}^{\mathcal{A}} \Rightarrow 1]| \leq \text{Adv}_{\text{KEM}}^{\text{ANO-PCA}}(\mathcal{B}_{ji}) .$$

The running time of \mathcal{B}_{ji} is about that of \mathcal{A} . Upper bounding $|\Pr[\mathbf{G}_{j,i}^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathbf{G}_{j,i+1}^{\mathcal{A}} \Rightarrow 1]|$ accordingly yields

$$\begin{aligned} \sum_{j=0}^{n-1} \sum_{i=0}^{q_C-1} |\Pr[\mathbf{G}_{j,i}^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathbf{G}_{j,i+1}^{\mathcal{A}} \Rightarrow 1]| &\leq \sum_{j=0}^{n-1} \sum_{i=0}^{q_C-1} |\text{Adv}_{\text{KEM}}^{\text{ANO-PCA}}(\mathcal{B}_{ji})| \\ &= n \cdot q_C \cdot \text{Adv}_{\text{KEM}}^{\text{ANO-PCA}}(\mathcal{B}) , \end{aligned}$$

where \mathcal{B} stems from folding the adversaries \mathcal{B}_{ji} into a single one. The running time of \mathcal{B} is about that of \mathcal{A} . □

Theorem 2 (Multi-User Public-Key Uniformity from Single-User Public-Key Uniformity). *Let KEM be a key encapsulation mechanism. For any PKU $_{(n)}$ adversary \mathcal{A} against KEM,*

there exists an PKU adversary \mathcal{B} against KEM such that

$$\mathbf{Adv}_{\text{KEM}}^{\text{PKU}_{n,qC}}(\mathcal{A}) \leq n \cdot \mathbf{Adv}_{\text{KEM}}^{\text{PKU}}(\mathcal{B}).$$

and the running time of \mathcal{B} is about that of \mathcal{A} .

Proof. We reduce PKU security of KEM to multi-user security anonymity PKU_n via a hybrid argument. Let \mathcal{A} be an adversary in the PKU_n experiment as defined in Fig. 2. Consider the sequence of hybrid games \mathbf{G}_i that successively changes the game for \mathcal{A} from $b = 1$ (all public keys generated using KGen) to $b = 0$ (all public keys sampled uniformly): In game \mathbf{G}_i , the first i many public keys in \mathbf{pk} are sampled using KGen , and the last $n - i$ many are sampled uniformly at random from \mathcal{PK} . Using the triangle inequality yields

$$\begin{aligned} \mathbf{Adv}_{\text{KEM}}^{\text{PKU}_n}(\mathcal{A}) &= \left| \sum_{i=0}^{n-1} \Pr[\mathbf{G}_i^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathbf{G}_{i+1}^{\mathcal{A}} \Rightarrow 1] \right| \\ &\leq \sum_{i=0}^{n-1} \left| \Pr[\mathbf{G}_i^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathbf{G}_{i+1}^{\mathcal{A}} \Rightarrow 1] \right|. \end{aligned}$$

We now give single-user PKU adversaries \mathcal{B}_i to upper bound the summands $|\Pr[\mathbf{G}_i^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathbf{G}_{i+1}^{\mathcal{A}} \Rightarrow 1]|$: \mathcal{B}_i receives a single public key pk^* from its PKU challenger. \mathcal{B}_i will use its challenge input to simulate either \mathbf{G}_i or \mathbf{G}_{i+1} : \mathcal{B}_i generates a vector of n many public keys \mathbf{pk} by using random sampling from \mathcal{PK} for the first $i - 1$ many, inserting its own challenge public key pk^* at the i -th position, and using KGen for the positions $i + 1$ to n . When \mathcal{A} outputs its guess to \mathcal{B}_i , \mathcal{B}_i forwards the guess to its own challenger. Since \mathcal{B}_i perfectly simulates \mathbf{G}_i if its own challenge bit is 1, and \mathbf{G}_{i+1} if its own challenge bit is 0, we have

$$\left| \Pr[\mathbf{G}_i^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathbf{G}_{i+1}^{\mathcal{A}} \Rightarrow 1] \right| \leq \mathbf{Adv}_{\text{KEM}}^{\text{PKU}}(\mathcal{B}_i).$$

Upper bounding $|\Pr[\mathbf{G}_i^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathbf{G}_{i+1}^{\mathcal{A}} \Rightarrow 1]|$ accordingly yields

$$\sum_{i=0}^{n-1} \left| \Pr[\mathbf{G}_i^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathbf{G}_{i+1}^{\mathcal{A}} \Rightarrow 1] \right| \leq \sum_{i=0}^{n-1} \left| \mathbf{Adv}_{\text{KEM}}^{\text{PKU}}(\mathcal{B}_i) \right| = n \cdot \mathbf{Adv}_{\text{KEM}}^{\text{PKU}}(\mathcal{B}),$$

where \mathcal{B} stems from folding the adversaries \mathcal{B}_{j_i} into a single one. The running time of \mathcal{B} is about that of \mathcal{A} . □

3 The Protocol OCAKE

We describe a 3-message password-authenticated key exchange (PAKE) protocol based on an ideal cipher IC and an implicitly-rejecting key encapsulation mechanism KEM in Figure 5. The protocol achieves mutual authentication and AKE security according to the BPR model, which we prove in Section 5. Two parties, the initiator (\mathcal{I}) and the responder (\mathcal{R}), share a common password pw and proceed in three phases. First, \mathcal{I} will generate a KEM key pair, encrypt the public key using the password, and send the encrypted public key apk to \mathcal{R} . After receipt, \mathcal{R} uses the password to recover the public key, then computes an encapsulation c and pre-key K . As response, \mathcal{R} sends the encapsulation c and a responder tag tag_1 to \mathcal{I} . On receipt, \mathcal{I} decapsulates the ciphertext to obtain a pre-key K' and compares the received tag to the one it derives from its own state. If the tags

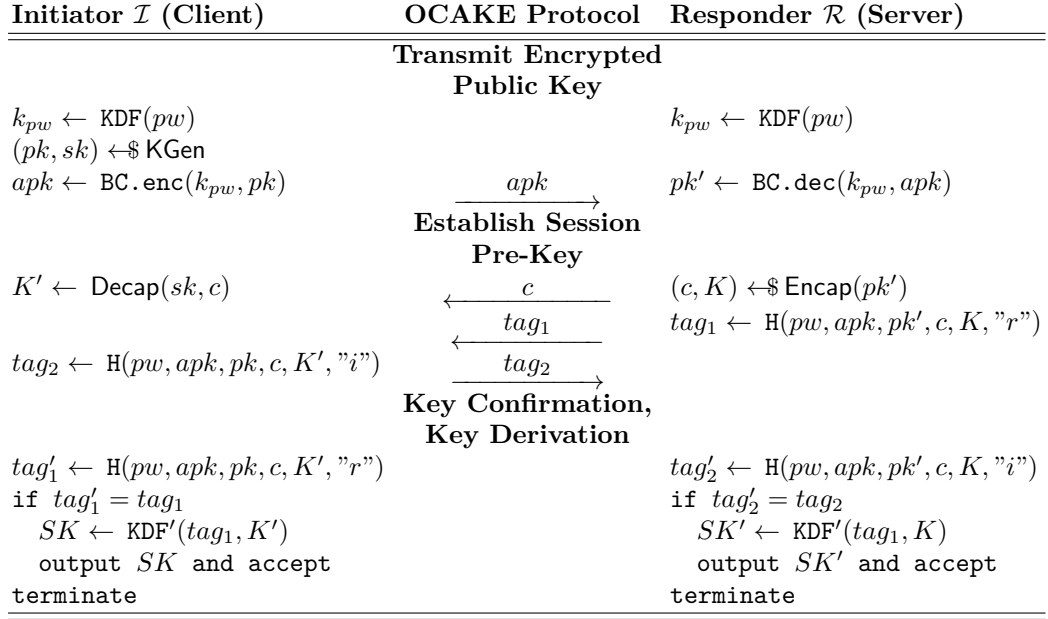


Fig. 5: The OCAKE protocol, using a key encapsulation mechanism $\text{KEM} = (\text{KGen}, \text{Encap}, \text{Decap})$ and a block cipher $\text{BC} = (\text{BC. enc}, \text{BC. dec})$ that is modeled as an ideal cipher in the proof. Messages c and tag_1 are part of the same round, making this a three-round protocol. The second tag is used to extend the protocol to achieve mutual authentication and is not needed for our security definition.

match, \mathcal{I} outputs a session key SK derived from the pre-key. For key confirmation, \mathcal{I} also computes an initiator tag and sends it to \mathcal{R} . The received tag is checked by \mathcal{R} against its own state and if it matches, \mathcal{R} outputs a session key SK' derived from its pre-key. Under the correctness of KEM, both parties only output a session key if and only if both parties used the same password, in which case the two session keys SK and SK' are identical.

Instantiating KEM and IC. To instantiate the protocol, it is necessary select a KEM that fulfills the security requirements in section Section 2. Several post-quantum secure KEMs have recently been standardized by government standardization agencies such as NIST, BSI and ANSSI. Table Table 1 shows an overview of KEMs and references to the relevant security proofs. This list is non-exhaustive, but includes schemes currently considered in these standardization efforts. Since PKU is less of a standard notion, we give a more detailed description.

CRYSTALS-Kyber Beguinet et al [BCP⁺23] point out that PKU reduces directly to the Decisional (D)-MLWE assumption.

Frodo-KEM in analogous argument as for CRYSTALS-Kyber, PKU reduces directly to the Decisional Learning with Errors (D-LWE) assumption.

Classic McEliece Key generation returns a public key ($ek = T$) where T is a Goppa code chosen uniformly at random from the set, provided that the choice of polynomial α is uniform.

BIKE PKU is equivalent to the hardness of QC-MDPC-McEliece ([ABB⁺22] Table 2).

HQC PKU reduces tightly to the decisional 2-WCSD Problem. Distinguishing $(h, s = x_1 + h \cdot x_2)$ from random is equivalent to distinguishing $(H, H \cdot [x_1, x_2]^\top)$ from random since h and H uniquely and efficiently identify each other and $\text{rot}(h) \times x_2^\top = h \cdot x_2$.

Table 1: An overview of PQ KEMs and their relevant properties. Note that ATK-CCA security implies ATK-PCA security directly. A more detailed overview is given by K. Xagawa [Xag21].

KEM	IND-CPA	ANO-PCA	PKU
CRYSTALS-Kyber	[BDK ⁺ 17]	[MX23]	[BCP ⁺ 23] as <i>fuzziness</i>
Frodo-KEM	[NAB ⁺ 20]	[GMP21]	[BCP ⁺ 23] argument applies
Classic McEliece	[ABC ⁺ 20]	[Xag21] ⁶	this work
BIKE	[ABB ⁺ 20]	[Xag21]	[ABB ⁺ 22]
HQC	[AAB ⁺ 20]	[Xag21]	this work

Instantiating the Ideal cipher As discussed by Beguinet et al [BCP⁺23], instantiation of the ideal cipher requires an appropriate choice of encoding of public keys. Where the ideal cipher operates on the set \mathcal{PK} , the block cipher will in general operate on bitstrings of fixed length. Critically, the proof relies on the assumption that decryption outputs are indistinguishable from honestly generated public keys. Public-key encodings that include checksums or other structure will not fulfill this property directly. However, as discussed by Beguinet et al., it is possible to create an encoding from the public key space to the block cipher domain, provided that the sizes of domains are appropriately chosen, with negligible distinguishing advantage.

Implementation and performance analysis. To assess the practicality of OCAKE, we provide a generic implementation framework ⁷ written in C that compatible with all mentioned KEM, providing crypto-agility. We present benchmarking for the execution time in a linux-based environment and an embedded one. On the other hand, we present benchmarking values for the execution time of the protocol in two settings: a linux-based environment and an embedded one. For the linux-based environment, the benchmarks were obtained on an Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz running Ubuntu 22.04.3 LTS Jammy. Speed is measured in the form of cpu clock cycles. The number of clock cycles was acquired using the `clock()` function in `time.h`, and are then converted to milliseconds. All binaries for the linux-based speed benchmark are compiled using `gcc` version 11.4.0 (Arm GNU Toolchain 10.3.1) at optimization level 0. For the embedded environment, all benchmarks were obtained on the STM32 NUCLEO-L4R5ZI development board. Speed is also measured in the form of cpu clock cycles, and all acquired values are averaged over 100 executions of the protocol. Execution times in seconds are calculated from the number of cpu cycles and the board’s default cpu frequency. All binaries for speed benchmarks running on the board are compiled using `arm-none-eabi-gcc` (Arm GNU Toolchain 10.3.1) at optimization level 2. Currently, we provide benchmarks with various parameter choices for Kyber, SABER, FrodoKEM, BIKE, and Classic McEliece (only linux-based) using KEM implementations from the PQClean and the pqm4 projects, and using AES and SHAKE to instantiate BC and KDF respectively, as shown in Tab. 2 and Tab. 3. As the concurrent works do not provide any implementations, a comparison to similar constructions is currently not possible.

4 Security Model

Our security analysis is based on the BPR model for authenticated key exchange [BPR00]: security of a protocol Π is modeled using a security experiment in which the attacker interacts with oracles that represent honest parties (**Execute** and **Send**) as well as oracles that represent leakage of secret material (**Reveal** and **Corrupt**), and wins if it can distinguish an established session key from random. The involved oracles are described in more detail in Fig. 7. To exclude trivial attacks from

⁷ Link blinded for review

consideration, [BPR00] define a freshness condition (Definition 8 below) that permits revealing a key on one side, and then testing the other (partnered) side, where partnered is defined as follows:

Definition 7 (Partnering). *Two instances $(P, i), (P', j)$ are partnered iff both have reached an **accept** instruction with the same transcript and session key.*

Intuitively, ‘unfreshness’ expresses that the adversary may have learned the to-be-tested session’s key SK in a trivial way, i.e., by having interacted with the oracles revealing secret information in a way such that SK becomes trivially derivable regardless of the protocol’s nature. Concretely, the cases we cover in our freshness definition below are a), simply requesting the key from the **Reveal** oracle, and b), learning a password pw via **Corrupt** and then actively interfering with the test session, e.g., using pw to manipulate the peer into using a session key of the adversary’s choosing.

Definition 8 (Freshness with Forward Secrecy). *Suppose that the adversary made exactly one **Test** query, and it was to party P and instance i . We say session i of party P is **unfresh** if there was a **Reveal** query to instance (P, i) or the instance (P', j) that it is partnered with. We also say the session is **unfresh** if both the following conditions hold:*

- Before the **Test** query, there was a **Corrupt** query on the test session’s holder P or its partnered peer P' .
- One of the messages sent to P concerning the test session was manipulated by the adversary, i.e., there was a **Send** (P, i) query.

The session (P, i) is only considered **fresh** if neither of these conditions are met.

Experiment $\text{Exp}_\Pi^{\text{BPR}}(\mathcal{A})$

```

16  $b \xleftarrow{\text{unif}} \{0, 1\}$ 
17  $b' \leftarrow \mathcal{A}^{\mathcal{O}^b}(\mathcal{P})$ 
18 return  $\llbracket b = b' \rrbracket$ 

```

Fig. 6: The BPR security game for active adversaries. $\mathcal{O}^b =$ indicates the collection of oracles $\{\text{Execute}, \text{KDF}, \text{H}, \text{KDF}', \text{IC. enc}, \text{IC. dec}, \text{Send}, \text{Reveal}, \text{Corrupt}, \text{Test}^b\}$. Here, \mathcal{P} is the party set.

Definition 9 (Key indistinguishability of PAKE). *Let Π be a PAKE protocol. We say that an adversary \mathcal{A} , run in experiment $\text{Exp}_\Pi^{\text{BPR}}$, wins if it correctly guesses the bit according to which the test query was defined and if the **Test** query was issued for a party (P, i) that has terminated and is fresh (see Definition 8). We define the advantage of \mathcal{A} against a PAKE protocol Π as*

$$\text{Adv}_\Pi^{\text{BPR}}(\mathcal{A}) := |\Pr[\text{Exp}_\Pi^{\text{BPR}}(\mathcal{A}) \Rightarrow 1] - 1/2| .$$

Our modification of OCAKE uses key confirmation tags in both directions. While only the responder tag actually is needed for our security proof, we additionally include an initiator tag – following the ‘add client-to-server authentication’ (AddCSA) paradigm [BPR00] – to achieve explicit mutual authentication.

Definition 10 (Explicit Mutual Authentication). *A protocol achieves explicit mutual authentication if parties accept if and only if there exists a partnered party that accepts with the same output.*

5 Security of OCAKE

Our main result is Theorem 3 below which relates forward security of OCAKE to security of the used KEM, in the combined Random Oracle (RO) and Ideal Cipher (IC) model. During its proof, we consider an adversary playing the BPR security game for our protocol OCAKE.

Theorem 3 (Tight security of OCAKE in the combined RO and IC model from multi-user security of KEM). *Let KEM be a key encapsulation mechanism that is $(1 - \delta)$ -correct, let KDF, KDF', and H be modeled as random oracles with domains \mathcal{K}_{pw} and \mathcal{T} , BC be modeled as an ideal cipher, and let \mathcal{A} be a BPR adversary against OCAKE[KEM, KDF, KDF', H, BC], issuing at most n_a many **Send** queries (i.e. active attacks), n_p many **Execute** queries (number of transcripts the adversary can see), $q_{IC.dec}$ many decryption queries to the ideal cipher, q_{IC} many queries to the ideal cipher in total (encryption or decryption), and q_{RO} many queries to its respective random oracles. Let $n_s := n_a + n_p$ be the total number of sessions. We denote the cardinality of a set \mathcal{S} as $|\mathcal{S}|$. Then there exist a multi-user-IND-CPA adversary \mathcal{B}^{IND} , a multi-user-ANO-PCA adversary \mathcal{B}^{ANO} and a multi-user-PKU adversary \mathcal{B}^{PKU} against KEM such that*

$$\begin{aligned} \text{Adv}_{\text{OCAKE}}^{\text{BPR}}(\mathcal{A}) &\leq \frac{n_a}{|\mathcal{D}|} + \text{Adv}_{\text{KEM}}^{\text{PKU}(q_{IC.dec} + n_s)}(\mathcal{B}^{\text{PKU}}) + 2 \cdot \text{Adv}_{\text{KEM}}^{\text{ANO-PCA}(q_{IC.dec} + n_s, n_a + 1)}(\mathcal{B}^{\text{ANO}}) \\ &\quad + 2 \cdot \text{Adv}_{\text{KEM}}^{\text{IND-CPA}(n_s, n_a + 1)}(\mathcal{B}^{\text{IND}}) + \frac{3 \cdot q_{IC}^2}{2 \cdot |\mathcal{PK}|} + 2 \cdot n_s \cdot \delta \\ &\quad + q_{RO} \cdot n_s \cdot \left(\frac{2}{|\mathcal{SK}|} + \frac{2}{|\mathcal{K}|} \right) + q_{RO}^2 \cdot \left(\frac{1}{2 \cdot |\mathcal{T}|} + \frac{1}{2 \cdot |\mathcal{K}_{pw}|} \right) \end{aligned}$$

and the running time of \mathcal{B}^{IND} , \mathcal{B}^{ANO} , and \mathcal{B}^{PKU} is about that of \mathcal{A} .

Intuitively, the proof of Theorem 3 reflects three security goals. We show that (SG1) the adversary can test at most one password per session with which it actively interferes, (SG2) honest protocol runs do not leak a significant amount of information on the password, and (SG3) the session key looks independent of both session transcript and password to the adversary unless it manages to attack the underlying KEM. Since we achieve forward secrecy, goal (SG3) is also achieved for sessions where the adversary knows the password, as long as the session is not actively attacked.⁸ Pseudocode for the BPR oracles is shown in Figure 8. Amongst the other oracles, Fig. 8 sketches the **Sendⁱ** oracles, where i indicates the flow number to separate the different stages of the protocol. We make the convention that oracle **Send** will only proceed if it is in the correct state for the received message: for example, if an instance receives a ciphertext c without having received a flow-0 message that caused it to generate a key pair, it will not respond. As shown in Figure 8, we at first will also model the **Execute** oracle using the **Send** oracle. \mathcal{A} can query the **Test** oracle exactly once, for a party and instance fulfilling the freshness definition.

High-level overview of proof. In the security proof, we argue that for every actively manipulated session, we can uniquely determine which password was tested. During that argument, we need to exclude the bad-case that protocol messages could stem from multiple passwords due to collisions. Game hops \mathbf{G}_0 to \mathbf{G}_5 aim at eliminating this bad-case. These game hops follow standard PAKE techniques and have been omitted due to page constraints. They are shown in full detail in the full version of the paper and in the appendix.

Then, we address security goals SG2 and SG3 by eliminating leakage on the password and the session key with game hops \mathbf{G}_9 to \mathbf{G}_{11} . Game hops \mathbf{G}_6 to \mathbf{G}_8 are preparation for these changes.

⁸ We use these intuitive security goals to structure the proof, however the only formal security goal is indistinguishability of session keys.

Query	Return Value	Description
$\text{Execute}(P, i, P', j)$	(apk, c, tag_1, tag_2)	Passive attack: Return transcript of an honest protocol execution between parties P and P' , using the i th/ j th session of P/P' .
$\text{Send}(P, i, msg, flow)$	msg'	Active attack: Send message msg to the oracle representing honest party P , causing it to proceed depending on its state. Flow indicator enumerates the messages in a run of the protocol and improves readability of the oracle.
$\text{Reveal}(P, i)$	$SK[P, i]/\perp$	Session key leakage: Return session key SK of (P, i) iff (P, i) terminated, else \perp ; marks this instance and its matching instance "un-fresh".
$\text{Corrupt}(P, PWD')$	$PWD[P, :]$	Password leakage or overwrite: Either return dictionary of passwords $PWD[P, :]$ held by party P , or allow adversary to overwrite password dictionary with $PWD'[P, :]$.
$\text{Test}^b(P, i)$	$SK[P, i]/SK^{\$}$	Session key challenge: Attack i th session of party P . Only for fresh, accepting instances. Returns either real or random session key depending on challenge bit b .
$\text{KDF}(pw)$	k_{pw}	Random oracle, input password $pw \in PWD$, output Ideal Cipher key k_{pw} .
$\text{H}(msg)$	tag	Random oracle, input message msg , output $tag \in \mathcal{T}$.
$\text{KDF}'(msg)$	SK	Random oracle, input message msg , output session key $SK \in \mathcal{SK}$.
$\text{IC.enc}(k, m)$	c	Ideal cipher encryption on input (key, message).
$\text{IC.dec}(k, c)$	m	Ideal cipher decryption on input (key, ciphertext).

Fig. 7: Overview of the PAKE adversary's oracles provided by the security game. Top part (above double midrule): oracles present in the BPR model. Bottom part: Random oracles and ideal cipher oracles to which the attacker additionally has access to when attacking the OCAKE protocol.

	Change	Reasoning	Loss
\mathbf{G}_1	Prevent KGen collisions	KGen entropy	$n_s^2 \cdot \eta_{\text{KGen}}$
\mathbf{G}_2	Prevent KDF collisions	Search Bound	$\frac{q_{\text{KDF}}^2}{2 \cdot \mathcal{K}_{pw} }$
\mathbf{G}_3	IC lazy sampling w/ abort	Search Bound	$\frac{q_{\text{IC}}^2}{2 \cdot \mathcal{PK} }$
\mathbf{G}_4	Prevent IC collisions	Search Bound	$\frac{q_{\text{IC}}^2}{ \mathcal{PK} }$
\mathbf{G}_5	Prevent resp. tag collision	Search Bound	$\frac{q_{\text{H}}^2}{2 \cdot \mathcal{T} }$
\mathbf{G}_6	Sample IC using KGen	pk uniformity	$(q_{\text{IC.dec}} + n_s)$ -PKU
\mathbf{G}_7	Abort on corr pw	Password Guessing	$\frac{n_a}{ \mathcal{D} } + \Delta \text{Pr}[\text{corrPW}]$
\mathbf{G}_8	Honest c : Replace Decap by responder's pre-key	Correctness	$n_s \cdot \delta$
\mathbf{G}_9	Randomize public-key pk	Anonymity	$(q_{\text{IC.dec}} + n_s, n_a + 1)$ -ANO-PCA
\mathbf{G}_{10}	Randomize pre-key K	Indistinguishability	$(n_s, n_a + 1)$ -IND-CPA
\mathbf{G}_{11}	Randomize tags tag_1, tag_2	Random Oracle	$\frac{q_{\text{H}} \cdot n_s}{ \mathcal{K} }$
\mathbf{G}_{12}	Randomize session key SK	Random Oracle	$\frac{q_{\text{KDF}'} \cdot n_s}{ \mathcal{SK} }$

Fig. 9: Overview of all game changes and their associated loss. $\Delta \text{Pr}[\text{corrPW}]$ is equal to the sum of all following game hops.

<u>Initialisation</u>	<u>Test^b(P, i)</u>	<u>Send²(P, i, msg)</u>
01 for (P, P') ∈ P × P	16 SK ₀ ← K[(P, i)]	34 MANIP[(P, i)] ← true
02 pw ← \$PW()	17 SK ₁ ← ^{unif} SK	35 c, tag ₁ ← ^{parse} msg
03 PWD[{P, P'}] ← ^{set} pw	18 if (CRPT[{P, P'}])	36 K' ← Decap(sk, c)
	MANIP[(P, i)]	37 if tag ₁ = H(pw, apk, pk, c, K', "r"):
<u>Execute(P, i, P', j)</u>	19 or if (RVL[(P, i)] or RVL[(P', j)])	38 tag ₂ ← H(pw, apk, pk, c, K', "i")
04 apk ← Send ⁰ (P, i, ⊥)	20 or if (K[(P, i)] = ⊥): return ⊥	39 SK ← KDF'(tag ₁ , K')
05 c, tag ₁ ← Send ¹ (P', j, apk)	21 else: return SK _b	40 K[(P, i)] ← ^{set} SK
06 tag ₂ ← Send ² (P, i, (c, tag ₁))	<u>Send⁰(P, i, msg)</u>	41 return tag ₂
07 Send ³ (P', j, tag ₂)	22 MANIP[(P, i)] ← true	42 else: return ⊥
08 MANIP[{P, :}] ← false	23 k _{pw} ← KDF(pw)	<u>Send³(P, i, msg)</u>
09 return (apk, c, tag ₂ , tag ₁)	24 (pk, sk) ← \$KGen	43 MANIP[(P, i)] ← true
<u>Corrupt(P, PWD')</u>	25 apk ← IC.enc(k _{pw} , pk)	44 tag ₂ ← ^{parse} msg
10 PWD _P ← PWD[{P, :}]	26 return apk	45 if tag ₂ = H(pw, apk, pk', c, K, "i"):
11 CRPT[{P, :}] ← true	<u>Send¹(P, i, msg)</u>	46 SK ← KDF'(tag ₁ , K)
12 PWD[{P, :}] ← PWD'[{P, :}]	27 MANIP[(P, i)] ← true	47 K[(P, i)] ← ^{set} SK
13 return PWD _P	28 apk ← ^{parse} msg	
<u>Reveal(P, i)</u>	29 k _{pw} ← KDF(pw)	
14 RVL[(P, i)] ← true	30 pk' ← IC.dec(k _{pw} , apk)	
15 return SK[(P, i)]	31 (c, K) ← \$Encap(pk')	
	32 tag ₁ ← H(pw, apk, pk', c, K, "r")	
	33 return (c, tag ₁)	

Fig. 8: The oracles in the security game for OCAKE. PWD is the dictionary of the parties' passwords and CRPT, MANIP and RVL indicate the corruption status of a session. Password generation in the initialization phase (**Initialization**) is modeled using the long-lived key generator PW .

5.1 Original Security Game

Original game G₀. The first game is the original BPR security game, with oracles Send and Execute answering queries according to the protocol (see Fig. 8).

$$\text{Adv}_{\text{OCAKE}}^{\text{BPR}}(\mathcal{A}) = |\Pr[\mathbf{G}_0(\mathcal{A}) \Rightarrow 1]| - 1/2 .$$

In the following game hops, we will use the notational convention $\text{Adv}_i := |\Pr[\mathbf{G}_i(\mathcal{A}) \Rightarrow 1]|$.

5.2 Eliminating Collisions (SG1)

In a first step, we address collision events that would allow distinct passwords to result in the same transcript.

Game G₁: Abort on Collision in Key Generation. In this game, we abort whenever there are at least two sessions where the same ephemeral key pair (pk, sk) is sampled by the KEM key generation. Let η_{KGen} be the collision probability of KGen. Since games \mathbf{G}_0 and \mathbf{G}_1 are identical unless a collision occurs, we have that:

$$|\text{Adv}_0 - \text{Adv}_1| = \Pr[\text{KDFColl}] \leq n_s^2 \cdot \eta_{\text{KGen}}$$

Game G₂: Abort on Key Derivation Function Collisions. First we address collisions in the key derivation function that would allow an adversary to use an ideal cipher key that corresponds to multiple passwords. Intuitively, this could mean that an adversary could use this derived key and succeed in an attack on a session even if a password that is not the correct one for this session is

used. We now keep a list of all previous queries to the KDF oracle by recording all input-output pairs (pw, k_{pw}) . Let KDFCo11 be the event there were two queries to the KDF oracle s.t. for two distinct passwords $pw \neq pw'$, the derived keys are the same:

$$\text{KDFCo11} : k_{pw} = k_{pw'} \text{ for queries } k_{pw} \leftarrow \text{KDF}(pw), k_{pw'} \leftarrow \text{KDF}(pw').$$

In game \mathbf{G}_1 , we abort whenever this event occurs. Let q_{KDF} be the number of queries to KDF. Since KDF is modeled as a random oracle, we can bound the probability of this event using a standard collision bound over the number of queries and the size of the output space of KDF: $\Pr[\text{KDFCo11}] \leq \frac{q_{\text{KDF}}^2}{2 \cdot |\mathcal{K}_{pw}|}$. Since games \mathbf{G}_1 and \mathbf{G}_2 are identical unless KDFCo11 occurs, the distance of the adversary's success probability is bounded:

$$|\text{Adv}_1 - \text{Adv}_2| = \Pr[\text{KDFCo11}] \leq \frac{q_{\text{KDF}}^2}{2 \cdot |\mathcal{K}_{pw}|}$$

From now on, we can argue that any password-derived key k_{pw} used in some protocol execution or oracle query corresponds to at most one password.

Game \mathbf{G}_3 : Simulate Ideal Cipher with abort. We now simulate a "modified" ideal cipher by lazy sampling where instead of choosing an output from the set of remaining outputs, we sample one from the entire domain and abort in case we sample a value that would violate the permutation property. For every record, we also record the direction of the query that first created the record, with a label "enc" for encryption and "dec" for decryption. We give a pseudocode description in Figure Fig. 10. Sampling this way is done in preparation for games \mathbf{G}_6 and \mathbf{G}_9 , where we replace ideal cipher outputs with public keys generated using KGen . Game \mathbf{G}_3 is identical to \mathbf{G}_2 unless it

$\text{IC. enc}(k_{pw}, pk)$ 01 if $\exists \text{ record } (k_{pw}, pk, apk, \star)$: 02 return apk 03 else 04 $apk' \xleftarrow{\text{unif}} \mathcal{PK}$ 05 if $\exists \text{ record } (k_{pw}, \star, apk', \star)$: abort 06 create record $(k_{pw}, pk, apk', \text{"enc"})$ 07 return apk'	$\text{IC. dec}(k_{pw}, apk)$ 08 if $\exists \text{ record } (k_{pw}, pk, apk)$: 09 return pk 10 else 11 $pk' \xleftarrow{\text{unif}} \mathcal{PK}$ 12 if $\exists \text{ record } (k_{pw}, pk', \star, \star)$: abort 13 create record $(k_{pw}, pk', apk, \text{"dec"})$ 14 return pk'
---	---

Fig. 10: The simulated ideal cipher sampling with abort. The star (\star) matches any value in that field.

aborts in line 5 of Figure Fig. 10. The probability of this occurring can be bounded using a standard collision bound in the total number of ideal cipher queries q_{IC} and the size of the public-key space $|\mathcal{PK}|$ and therefore:

$$|\text{Adv}_2 - \text{Adv}_3| \leq \frac{q_{\text{IC}}^2}{2 \cdot |\mathcal{PK}|}$$

Game \mathbf{G}_4 : Abort on Ideal Cipher Collisions. Next we eliminate collisions in the ideal cipher. Collisions can allow the adversary to test multiple passwords in a single session, violating security goal (SG1). The probability of such collisions occurring is therefore directly relevant to the security of the scheme. There are two types of collision for which this is the case. The *first* type of collision

occurs if the adversary finds that some public key and authenticated public key are mapped to each other under two distinct passwords. Formally, this would imply that there were two queries to the ideal cipher such that for $k_{pw} \neq k'_{pw}$

$$\begin{aligned} \text{ICCo111} : (pk, apk) = (pk', apk') \text{ for two queries:} \\ (\text{either } apk \leftarrow \text{IC.enc}(k_{pw}, pk) \text{ or } pk \leftarrow \text{IC.dec}(k_{pw}, apk)) \\ \text{and } (\text{either } (apk' \leftarrow \text{IC.enc}(k'_{pw}, pk') \text{ or } pk' \leftarrow \text{IC.dec}(k'_{pw}, apk')) \end{aligned}$$

To give an example, an adversary sending an apk with this property to the **Send** oracle could test the passwords corresponding to k_{pw} and k'_{pw} in one query. The *second* type of collision occurs if there were at least two ideal cipher *encryption* queries for distinct passwords and public keys that returned the same authenticated public key. Knowledge of apk with this property allows the adversary to test both passwords in one query.⁹ Formally, this would imply that there were two queries to the ideal cipher such that for $k_{pw} \neq k'_{pw}$:

$$\text{ICCo112} : apk = apk' \text{ for queries: } apk \leftarrow \text{IC.enc}(k_{pw}, pk), apk' \leftarrow \text{IC.enc}(k'_{pw}, pk')$$

In game \mathbf{G}_4 , we abort whenever ICCo111 or ICCo112 occur. We define the event ICCo11 where

$\text{IC.enc}_{\mathbf{G}_3}(k_{pw}, pk)$ $\text{IC.enc}_{\mathbf{G}_4}(k_{pw}, pk)$	$\text{IC.dec}_{\mathbf{G}_3}(k_{pw}, apk)$ $\text{IC.dec}_{\mathbf{G}_4}(k_{pw}, apk)$
01 if \exists record (k_{pw}, pk, apk, \star) :	10 if \exists record (k_{pw}, pk, apk, \star) :
02 return apk	11 return pk
03 else	12 else
04 $apk' \xleftarrow{\text{unif}} \mathcal{PK}$	13 $pk' \xleftarrow{\text{unif}} \mathcal{PK}$
05 if \exists record $(k_{pw}, \star, apk', \star)$: abort	14 if \exists record $(k_{pw}, pk', \star, \star)$: abort
06 if \exists record (\star, pk, apk', \star) : ICCo111	15 if \exists record (\star, pk', apk, \star) : ICCo111
07 if \exists record $(\star, \star, apk', \text{"enc"})$: ICCo112	16 create record $(k_{pw}, pk', apk, \text{"dec"})$
08 create record $(k_{pw}, pk, apk', \text{"enc"})$	17 return pk'
09 return apk'	

Fig. 11: The simulated ideal cipher. In game \mathbf{G}_4 , the game aborts whenever there is a collision in the ideal cipher that would allow the adversary to test two passwords.

$\Pr[\text{ICCo11}] := \Pr[\text{ICCo111} \vee \text{ICCo112}]$. We argue that the probability of this event is upper-bounded by a standard collision bound in the total number of ideal cipher queries (encryption and decryption) q_{IC} and the size of the ideal cipher domain $|\mathcal{PK}|$, since it requires sampling. In game \mathbf{G}_4 , we abort whenever ICCo11 occurs. Since games \mathbf{G}_3 and \mathbf{G}_4 are identical unless ICCo11 occurs, it holds that

$$|\text{Adv}_3 - \text{Adv}_4| = \Pr[\text{ICCo11}] \leq \frac{q_{\text{IC}}^2}{2 \cdot |\mathcal{PK}|} + \frac{q_{\text{IC}, \text{enc}}^2}{2 \cdot |\mathcal{PK}|} \leq \frac{q_{\text{IC}}^2}{|\mathcal{PK}|}.$$

⁹ To further elaborate, this would imply that for this apk , there are two keys $k_{pw} \neq k_{pw'}$ and therefore two passwords $pw \neq pw'$ for which the adversary could know the secret keys associated with the public keys $pk \neq pk'$. This would then allow the adversary to decrypt ciphertexts for both these public keys, to derive two candidate session keys. Either one of them could then be compared to the session key output by the **Test** query.

$\text{IC.dec}_{\mathbf{G}_5}(k_{pw}, apk)$	$\text{IC.dec}_{\mathbf{G}_6}(k_{pw}, apk)$
01 if \exists record (k_{pw}, pk, apk)	
02 return pk	
03 else	
04 $pk' \xleftarrow{\text{unif}} \mathcal{PK}$	$pk' \xleftarrow{\$} \text{KGen}$
05 if \exists record (k_{pw}, pk', \star) : abort	
06 if \exists record (\star, pk', apk) : abort	
07 create record (k_{pw}, pk', apk)	
08 return pk'	

Fig. 12: The simulated ideal cipher now samples using the KEM’s key generation algorithm KGen instead of uniformly at random from the domain \mathcal{PK} .

Game \mathbf{G}_5 : Abort on Responder Tag Collision. We now create a record for all queries to \mathbb{H} by the adversary and let ROCo11 be the event that the random oracle outputs the same value twice, for different inputs, in which case game \mathbf{G}_5 aborts. The probability of ROCo11 occurring is bounded using a standard collision bound given by the number of queries $q_{\mathbb{H}}$ to \mathbb{H} and the size of the tag space T : $\Pr[\text{ROCo11}] \leq \frac{q_{\mathbb{H}}^2}{2 \cdot |T|}$. Since games \mathbf{G}_4 and \mathbf{G}_5 are identical unless ROCo11 or occurs, it holds that:

$$|\text{Adv}_4 - \text{Adv}_5| = \Pr[\text{ROCo11}] \leq \frac{q_{\mathbb{H}}^2}{2 \cdot |T|}.$$

For every responder tag output by the \mathbb{H} , there is now exactly one password that was used to create it. Therefore, whenever a *malicious responder* adversary submits such a tag, this tag corresponds to at most one password. At this point, we have proven that it is unlikely for an adversary to be able to test multiple passwords in a single query, in accordance with security goal 1 (SG1).

Game \mathbf{G}_6 : Sample Ideal Cipher Outputs Using KEM Key Generation. In game \mathbf{G}_6 , we replace the way the simulated ideal cipher samples outputs. On decryption queries, instead of sampling from the output domain uniformly at random, we use the key generation algorithm of KEM. This is an auxiliary step we do in preparation for the separation of ciphertexts c and the password, which we will do using the anonymity property of KEM in game \mathbf{G}_9 . The change is depicted in Fig. 12. We will now argue that an adversary that can distinguish game \mathbf{G}_5 from \mathbf{G}_6 can be used to attack the n -public-key-uniformity (PKU_n) property of the underlying KEM for $n = q_{\text{IC.dec}} + n_s$, by means of a reduction \mathcal{B}^{PKU} . Let \mathcal{A} be the adversary running either in game \mathbf{G}_5 or \mathbf{G}_6 , issuing at most $q_{\text{IC.dec}}$ many queries to the ideal cipher decryption oracle. We define adversary \mathcal{B}^{PKU} against the PKU_n experiment (defined in Fig. 2) as follows (for the sake of formality, we give the pseudo-code of \mathcal{B}^{PKU} in Fig. 13):

\mathcal{B}^{PKU} receives a vector of challenge public keys \mathbf{pk} of dimension n from its PKU_n challenger, where $n := q_{\text{IC.dec}} + n_s$. (Depending on the challenger’s bit b_{PKU} , \mathbf{pk} is generated using KGen or drawn uniformly at random from \mathcal{PK} .) \mathcal{B}^{PKU} samples an own challenge bit b' , runs \mathcal{A} and answers \mathcal{A} ’s queries to the Oracles \mathbb{H} , IC.enc , KDF , KDF' , Reveal , Send , Execute , and $\text{Test}^{b'}$ according to the oracles in \mathbf{G}_5 . When simulating ideal cipher decryption queries, \mathcal{B}^{PKU} embeds the challenge public keys from its input vector \mathbf{pk} : Upon a query to oracle IC.dec , instead of sampling an output like game \mathbf{G}_5 , \mathcal{B}^{PKU} uses the next value in \mathbf{pk} . In case a query is repeated, it repeats the respective public key. \mathcal{B}^{PKU} needs to produce at most $q_{\text{IC.dec}} + n_s$ many outputs for IC.dec , one for each

Adversary $\mathcal{B}^{\text{PKU}}(\mathbf{pk})$	IC.dec(k_{pw}, apk)
01 $\text{pkIndex} = 0$	05 if \exists record (k_{pw}, pk, apk):
02 $b \xleftarrow{\text{unif}} \{0, 1\}$	06 return pk
03 $b' \leftarrow \mathcal{A}^{\mathcal{O}^b}(\mathbf{pk})$	07 else
04 output $b'_{\text{PKU}} := [b = b']$	08 $pk^* \leftarrow \mathbf{pk}[\text{pkIndex}]$ // pk^* is real or random
	09 $\text{pkIndex} += 1$
	10 if \exists record (k_{pw}, pk^*, \star): abort
	11 if \exists record (\star, pk^*, apk): abort
	12 create record (k_{pw}, pk^*, apk)
	13 return pk'

Fig. 13: PKU adversary \mathcal{B}^{PKU} , used to reason about the hop from game \mathbf{G}_5 to \mathbf{G}_6 . Adversary \mathcal{A} has access to oracles $\mathcal{O} = \{\text{KDF}, \text{KDF}', \text{IC.enc}, \text{IC.dec}, \text{Execute}, \text{Send}, \text{Reveal}, \text{Corrupt}\}$.

direct query ($q_{\text{IC.dec}}$), and one per protocol session (n_s). When \mathcal{A} outputs a guess b , \mathcal{B}^{PKU} checks if $b = b'$ and in that case returns $b'_{\text{PKU}} := 1$ as its own output bit, otherwise, \mathcal{B}^{PKU} returns $b'_{\text{PKU}} := 0$.

\mathcal{B}^{PKU} perfectly simulates \mathbf{G}_6 when run with KGen-generated public keys, and \mathbf{G}_5 when run with uniform public keys. Since \mathcal{B}^{PKU} uses at most $n = q_{\text{IC.dec}} + n_s$ many public keys in total, the difference between \mathcal{A} 's winning probabilities in games \mathbf{G}_5 and \mathbf{G}_6 is upper bounded by the n -uniformity advantage of \mathcal{B}^{PKU} against KEM:

$$|\text{Adv}_5 - \text{Adv}_6| \leq \text{Adv}_{\text{KEM}}^{\text{PKU}(q_{\text{IC.dec}} + n_s)}$$

5.3 Preparing to handle messages involving the correct password

To quantify the protocol's leakage of the password, we randomize protocol messages in Section 5.4. For these randomizations to go unnoticed, we need to rule out the case that the adversary sent messages constructed using the correct password. Therefore, when the adversary makes a **Send** query, we check if the correct password was used. If such a query occurs, there are three possible reasons:

1. **trivGuess** \mathcal{A} obtained the password by *corrupting* one of the parties involved in the session. We raise the flag **trivGuess** for that session and continue the protocol without applying the changes of the following games, i.e., without randomization. In cases where **trivGuess** is raised during a session, in between subsequent **Send** queries to the same session, it is relevant for which message this flag is first raised. We denote the event that **trivGuess** is raised for the flow- i message as **trivGuess_i**.
2. **forward** \mathcal{A} *forwards* a message generated honestly by a previous query to the **Send** oracle. Clearly, this event does not imply that the adversary has guessed the password or knows any of the secret information associated with the message. Therefore, we do not count this as a correct guess and continue by randomizing the outputs according to Section 5.4. The game detects the event by keeping a record of all honestly generated transcripts.
3. **corrPW** \mathcal{A} *guessed* the password. We call this event **corrPW** and abort the game whenever it occurs. This way, no **Test** query can be issued to such a session, and we do not have to randomize the protocol messages. Throughout the games, we will bound how the probability of event **corrPW** changes, until we end up with a game in which we can bound the probability of event **corrPW** in terms of the dictionary size.

In conclusion, we will show that we can make the protocol messages independent of the password for all sessions where neither 1. nor 3. occurred.¹⁰

Game G_7 : Abort on Correct Password. We consider two cases of correct password guesses:

Authenticated Public Key (apk) Consider the event where the adversary sends apk built from the correct password *and* the respective message was indeed generated by the adversary, i.e., not honestly generated by a previous call to **Send**. We'll call this event **apkCorrPw**. The game detects this event using a record of honestly generated messages and the ideal cipher encryption records. The changes in the previous games guarantee that the record is unique.

Responder Tag (tag_1) Consider the event where the adversary sends a valid tag_1 built from the correct password *and* the message was indeed generated by the adversary. We'll call this event **tagCorrPw**. The game detects this as follows: When the adversary submits a responder tag to the **Send** oracle, we look for records in \mathbb{H} linking this tag to the input used to create it which contains a password. By the changes made in previous games, there is at most one record for this tag, uniquely determining the *password* that was used / tested in this query.

Combining the two cases and ruling out corruptions, we let **corrPW** be the event that either **apkCorrPw** or **tagCorrPw** occur *and* that neither party in the session was corrupted. In case the adversary submits a tag_2 (i.e. flow 3 message) formed using the correct password, one of two things has happened: either the tag matches the responder's transcript, and we are in the forwarding case, or it does not, in which case the responder rejects. Therefore, we do not have to consider this event a correct guess. We let game G_7 abort whenever **corrPW** occurs. Since both games proceed identically unless **corrPW** occurs, we have

$$|\mathbf{Adv}_6 - \mathbf{Adv}_7| = \Pr[\mathbf{corrPW}_{G_7}]$$

We track how the probability of event **corrPW** changes throughout the sequence of games, and finish by bounding its probability in game G_{12} .

5.4 Randomizing Protocol Messages (SG2)

Next we make the protocol messages independent of password and session key. We then argue that the modified game is indistinguishable to the adversary, using anonymity and indistinguishability of KEM. Using these computational assumptions, we can bound the amount of information leaked by the protocol messages concerning the password. As stated above, the adversary could notice this if they used the correct password to create a session but this case does not matter anymore since the game then aborts, anyways. We only need to keep track of how the probability of **corrPW** changes, which we can also bound in terms of the computational assumptions on KEM since **corrPW** is an event that can be checked by a respective reduction.

Game G_8 : Do Not Decapsulate Honest Ciphertexts. In game G_8 , whenever there is a flow 2 query where the message was honestly generated by a matching session, we do not decapsulate to obtain the pre-key. Instead, if the message was generated by a matching session, we use the pre-key generated by that instance. Adversarially generated messages as well as ones that are forwarded from a non-matching session are decapsulated as before. This step is done in preparation for the reductions in the following two game hops. Games G_7 and G_8 are indistinguishable unless a correctness error occurred in game G_7 and therefore $|\Pr[\mathbf{corrPW}_{G_7}] - \Pr[\mathbf{corrPW}_{G_8}]| = |\mathbf{Adv}_7 - \mathbf{Adv}_8| = n_s \cdot \delta$.

Game G_9 : Randomize Encapsulation Public Key. In the first randomization step, we make the following change for all queries to the **Send** oracles where flag **trivGuess** is not raised: The public

¹⁰ There is a small subtlety here: in an edge-case discussed later, we make the change also when **trivGuess** is raised in the middle of a session.

$\text{Send}_{\mathbf{G}_7}^2(P, i, \text{msg})$	$\text{Send}_{\mathbf{G}_8}^2(P, i, \text{msg})$
01 $c, \text{tag}_1 \xleftarrow{\text{parse}} \text{msg}$ 02 $K' \leftarrow \text{Decap}(sk, c)$ 03 04 if $\text{tag}_1 = \text{H}(pw, apk, pk, c, K', "r")$: 05 $\text{tag}_2 \leftarrow \text{H}(pw, apk, pk, c, K', "i")$ 06 $SK \leftarrow \text{KDF}'(\text{tag}_1, K')$ 07 $\text{K}[(P, i)] \xleftarrow{\text{set}} SK$ 08 return tag_2 09 else: return \perp	if forward: $K' \leftarrow$ responder's key K else: $K' \leftarrow \text{Decap}(sk, c)$

Fig. 14: In game \mathbf{G}_8 , whenever **forward** occurs (i.e., c is a matching responder's honest ciphertext) we use the responder's pre-key K instead of decapsulating c .

$\text{Send}_{\mathbf{G}_8}^1(P, i, \text{msg})$	$\text{Send}_{\mathbf{G}_9}^1(P, i, \text{msg})$
01 $apk \xleftarrow{\text{parse}} \text{msg}$ 02 $k_{pw} \leftarrow \text{KDF}(pw)$ 03 $pk' \leftarrow \text{IC.dec}(k_{pw}, apk)$ 04 if $\text{PK}[(k_{pw}, apk)] \neq \perp$: $pk'_s \leftarrow \text{PK}[(k_{pw}, apk)]$ else: $(pk'_s, sk'_s) \leftarrow \KGen $\text{PK}[(k_{pw}, apk)] \xleftarrow{\text{set}} pk'_s$ 05 $(c, K) \leftarrow \$\text{Encap}(pk')$ 06 $\text{tag}_1 \leftarrow \text{H}(pw, apk, pk', c, K, "r")$ 07 return c, tag_1	$(c, K) \leftarrow \$\text{Encap}(pk'_s)$

Fig. 15: Game \mathbf{G}_9 : Randomizing public key in Send^1 queries. The dictionary PK is a book-keeping tool introduced in game \mathbf{G}_9 to ensure consistency of replays.

key used for the encapsulation is now generated independently of the password and the previously sent session messages (see the pseudo-code in Figure 15). We will now argue that an adversary noticing this change can be used to attack the multi-user anonymity property $\text{ANO-PCA}_{n, q_C}$ where $n := q_{\text{IC.dec}} + n_s$ and $q_C := n_a + 1$. Intuitively, parameter n represents the number of public-keys in the reduction and is equal to the total number of potential public keys for any ciphertext c output by the Send oracles. Since the Send and Execute oracles query IC.dec , the number of sessions has to be added to the number of IC.dec queries the adversary is allowed to make. Parameter q_C represents the maximal number of challenges issued for a given key pair, and is equal to the number of times an adversary could replay an authenticated public key. We define adversary $\mathcal{B}_0^{\text{ANO}}$ against the $\text{ANO-PCA}_{n, q_C}$ experiment (defined in Fig. 4) as follows (for the sake of formality, we give the pseudo-code of $\mathcal{B}_0^{\text{ANO}}$ in Fig. 16):

$\mathcal{B}_0^{\text{ANO}}$ receives two vectors of challenge public keys (pk_0, pk_1) of dimension $n = q_{\text{IC.dec}} + n_s$, and can query its challenge oracle Chall , provided by its $\text{ANO-PCA}_{n, q_C}$ challenger, at most $q_C = n_a + 1$ many times. (Depending on the challenger's bit, the challenges are generated using either pk_0 or

pk_1 .) $\mathcal{B}_0^{\text{ANO}}$ samples an own challenge bit b' , runs \mathcal{A} and answers \mathcal{A} 's queries to the Oracles H , $\mathsf{IC. enc}$, KDF , KDF' , Send^3 , Reveal , and $\mathsf{Test}^{b'}$ according to the oracles in \mathbf{G}_8 . **Execute** queries are answered using Send as before. On ideal cipher decryption queries, $\mathcal{B}_0^{\text{ANO}}$ embeds the challenge public keys contained in pk_0 (see Fig. 16). When \mathcal{A} queries Send^0 , $\mathcal{B}_0^{\text{ANO}}$ uses one of the challenge public keys in pk_0 . Whenever \mathcal{A} queries the Send^1 oracle and $\mathsf{trivGuess}$ has not been raised, the ideal cipher decryption oracle is evaluated on the apk value sent by the initiator and the password-derived key of that session. Due to the abort conditions in game \mathbf{G}_3 , there must exist $j \in [n]$ s.t. $pk' = pk_{0,j}$. Then, to answer the query, $\mathcal{B}_0^{\text{ANO}}$ queries $\mathsf{Chall}(j)$ to receive a challenge (c^*, K^*) , outputs c^* to \mathcal{A} and uses K^* as K (see Fig. 16). Ciphertexts returned by the Send^1 oracle are then either encapsulations under the public key $pk_{0,j}$ or under $pk_{1,j}$, depending on the challenge bit in the $\text{ANO-PCA}_{n,q_C}$ game. Note that since \mathcal{A} can replay an apk value in each of the n_a many sessions, the same public key will sometimes be used to obtain multiple challenges and $q_C = n_a + 1$. Whenever \mathcal{A} queries Send^2 , there is an edge-case to consider: In case the adversary causes the $\mathsf{trivGuess}$ flag to be raised *before* Send^2 is queried but *after* Send^0 is, the adversary is able to forge a tag for an arbitrary ciphertext under the challenge public key chosen in Send^0 . To learn the pre-key needed to complete the simulation of the initiator, $\mathcal{B}_0^{\text{ANO}}$ queries the 1-PCO oracle using the pre-key K' matching the record of tag_1 . If that query returns true, the instance accepts and with $SK \leftarrow \mathsf{KDF}'(tag_1, K')$, and rejects if not. When \mathcal{A} outputs a guess b , $\mathcal{B}_0^{\text{ANO}}$ checks if $b = b'$. In the case that corrPW did not occur and that $b = b'$, it returns 1 as its own output bit, otherwise, it returns 0.

$\mathcal{B}_0^{\text{ANO}}$ perfectly simulates \mathbf{G}_8 when run in the $\text{ANO-PCA}_{n,q_C}$ -game with challenge bit 0, \mathbf{G}_9 when run with with challenge bit 1, and returns 1 if the adversary wins. Therefore, the difference between \mathcal{A} 's winning probabilities in games \mathbf{G}_8 and \mathbf{G}_9 is upper bounded by the respective $\text{ANO-PCA}_{n,q_C}$ advantage of $\mathcal{B}_0^{\text{ANO}}$ against KEM:

$$|\mathbf{Adv}_8 - \mathbf{Adv}_9| \leq \mathbf{Adv}_{\text{KEM}}^{\text{ANO-PCA}_{(q_{\text{IC.dec}} + n_s, n_a + 1)}}(\mathcal{B}_0^{\text{ANO}})$$

To keep track of the change in the probability of $\Pr[\mathsf{corrPW}]$, we can slightly adapt the reduction $\mathcal{B}_0^{\text{ANO}}$: our new reduction $\mathcal{B}_1^{\text{ANO}}$ behaves exactly like $\mathcal{B}_0^{\text{ANO}}$ except for its output: $\mathcal{B}_1^{\text{ANO}}$ returns 1 if corrPW occurred, and otherwise 0.

$$|\Pr[\mathsf{corrPW}_{\mathbf{G}_8}] - \Pr[\mathsf{corrPW}_{\mathbf{G}_9}]| \leq \mathbf{Adv}_{\text{KEM}}^{\text{ANO-PCA}_{(q_{\text{IC.dec}} + n_s, n_a + 1)}}(\mathcal{B}_1^{\text{ANO}})$$

Game \mathbf{G}_{10} : Randomize Session Pre-Key. For all queries to the Send or $\mathsf{Execute}$ oracles where flag $\mathsf{trivGuess}$ is not raised before the query, we now randomize the pre-key K that is used to derive the final session key and the responder tag. For more details, see the pseudo-code in Figure 17. This change makes the pre-key independent of the ciphertext and the password for all fresh sessions. We now argue that an adversary noticing this change can be used to attack the indistinguishability property of the KEM. We define adversary $\mathcal{B}_0^{\text{IND}}$ against the $\text{IND-CPA}_{n,q_C}$ experiment (defined in Fig. 3) as follows (for the sake of formality, we give the pseudo-code of $\mathcal{B}_0^{\text{IND}}$ in Fig. 18):

$\mathcal{B}_0^{\text{IND}}$ receives a vector of challenge public keys pk , of dimension $n = n_s$ and can query its challenge oracle Chall , provided by its $\text{IND-CPA}_{n,q_C}$ challenger, at most $q_C = n_a + 1$ many times. $\mathcal{B}_0^{\text{IND}}$ samples a challenge bit b' , runs \mathcal{A} and answers \mathcal{A} 's queries to the Oracles H , $\mathsf{IC. enc}$, KDF , Reveal , Send^0 , Send^2 , and $\mathsf{Test}^{b'}$ according to the oracles in \mathbf{G}_9 .

On Send^1 queries, $\mathcal{B}_0^{\text{IND}}$ issues a $\mathsf{Chall}(j)$ query to its own challenger receive (c^*, K^*) , where j is the index of the public key which it uses to answer the query. If $\mathsf{trivGuess}$ has been raised, $\mathcal{B}_0^{\text{IND}}$ generates a key pair and continues the protocol honestly without inserting any challenges in this

Adversary $\mathcal{B}_0^{\text{ANO}}(\mathbf{pk}_0, \mathbf{pk}_1)$	IC.dec(k_{pw}, apk)
01 $\text{pkIndex} = 0$	06 if \exists record (k_{pw}, pk, apk) return pk :
02 $b \xleftarrow{\text{unif}} \{0, 1\}$	07 else
03 $b' \leftarrow \mathcal{A}^{\mathcal{O}^b}()$	08 $pk' \leftarrow \mathbf{pk}_0[\text{pkIndex}] // pk' \leftarrow \$ \text{KGen}$
04 $b'_{\text{ANO}} := [b = b']$	09 $\text{pkIndex} += 1$
05 output b'_{ANO}	10 if \exists record (k_{pw}, pk', \star): abort
	11 if \exists record (\star, pk', apk): abort
	12 create record (k_{pw}, pk', apk)
	13 return pk'
<u>Send⁰(P, i, msg)</u>	
14 if trivGuess_0 : return Send ⁰ (P, i, msg) $_{\mathbf{G}_7}$	
15 $k_{pw} \leftarrow \text{KDF}(pw)$	
16 $pk \leftarrow \mathbf{pk}_0[\text{pkIndex}] // pk' \leftarrow \$ \text{KGen}$	
17 $\text{pkIndex} += 1$	
18 $apk \leftarrow \text{IC.enc}_{k_{pw}}(pk) // \text{get challenge } pk$	
19 return apk	
<u>Send¹(P, i, msg)</u>	
20 if trivGuess_0 or trivGuess_1 : return Send ¹ (P, i, msg) $_{\mathbf{G}_7}$	
21 $apk \xleftarrow{\text{parse}} msg$	
22 $k_{pw} \leftarrow \text{KDF}(pw)$	
23 $pk' \leftarrow \text{IC.dec}(k_{pw}, apk)$	
24 find j s.t. $pk' = \mathbf{pk}_0[j] // \text{IC returned challenge } pk \text{ from } \mathbf{pk}_0$	
25 $(c, K) \leftarrow \text{Chall}(j) // (c, K) \leftarrow \text{Encap}(pk')$	
26 $tag_1 \leftarrow \text{H}(pw, apk, pk', c, K, "r")$	
27 return c, tag_1	
<u>Send²(P, i, msg)</u>	
28 if trivGuess_0 or trivGuess_1 : return Send ² (P, i, msg) $_{\mathbf{G}_7}$	
29 $c, tag_1 \xleftarrow{\text{parse}} msg$	
30 if forward : $K' \leftarrow$ responder's key K	
31 else if \exists record $tag_1 = \text{H}(pw, apk, pk, c, K_{\mathcal{A}}, "r")$: //event trivGuess_2	
32 find j s.t. $pk = \mathbf{pk}_0[j] // \text{see flow 0 to see this exists}$	
33 if $[1\text{-PCO}(j, c, K_{\mathcal{A}}) \Rightarrow \text{true}]$: $K' \leftarrow K_{\mathcal{A}}$	
34 else: return \perp	
35 else: return \perp	
36 if $tag_1 = \text{H}(pw, apk, pk, c, K', "r")$:	
37 $tag_2 \leftarrow \text{H}(pw, apk, pk, c, K', "i")$	
38 $SK \leftarrow \text{KDF}'(tag_1, K)$	
39 $\text{K}[(P, i)] \xleftarrow{\text{set}} SK$	
40 return tag_2	
41 else: return \perp	

Fig. 16: ANO-PCA $_{n, qc}$ adversary $\mathcal{B}_0^{\text{ANO}}$, used to reason about the hop from game \mathbf{G}_8 to \mathbf{G}_9 . The collection \mathcal{O} of \mathcal{A} 's oracles is $\mathcal{O} = \{\text{KDF}, \text{KDF}', \text{IC.enc}, \text{IC.dec}, \text{Execute}, \text{Send}, \text{Reveal}, \text{Corrupt}\}$. In case of corruption prior to each query, $\mathcal{B}_0^{\text{ANO}}$ follows the protocol according to the oracles in game \mathbf{G}_7 , with the exception of the edge case shown in lines 31 to 35.

$\text{Send}_{\mathbf{G}_9}^1(P, i, \text{msg})$	$\text{Send}_{\mathbf{G}_{10}}^1(P, i, \text{msg})$
01 $apk \xleftarrow{\text{parse}} \text{msg}$	
02 $k_{pw} \leftarrow \text{KDF}(pw)$	
03 $pk' \leftarrow \text{IC.dec}(k_{pw}, apk)$	
04 if $\text{PK}[(k_{pw}, apk)] \neq \perp$:	
05 $pk'_s \leftarrow \text{PK}[(k_{pw}, apk)]$	
06 else:	
07 $(pk'_s, sk_s) \leftarrow \text{\$KGen}$	
08 $\text{PK}[(k_{pw}, apk)] \xleftarrow{\text{set}} pk'_s$	
09 $(c, K) \leftarrow \text{\$Encap}(pk'_s)$	
10	$K_s \xleftarrow{\text{unif}} \mathcal{K}$
11 $tag_1 \leftarrow \text{H}(pw, apk, pk', c, K, "r")$	$tag_1 \leftarrow \text{H}(pw, apk, pk', c, K_s, "r")$
12 return c, tag_1	

Fig. 17: In game \mathbf{G}_{10} , the pre-key set after querying **Send** or **Execute** is sampled independently of the password and the previous messages. Due to the change in game \mathbf{G}_8 , this also randomizes the initiator side and we also write $K'_s \leftarrow K_s$.

session. If the same apk is submitted multiple times for sessions using the same password, the game is kept consistent by re-using the respective public key. When \mathcal{A} outputs a guess b , $\mathcal{B}_0^{\text{IND}}$ checks if $b = b'$. In the case that $b = b'$, it returns 1 as its own output bit, otherwise, it returns 0.

$\mathcal{B}_0^{\text{IND}}$ perfectly simulates \mathbf{G}_9 when run in the $\text{IND-CPA}_{n_s, n_a+1}$ -game with challenge bit 0, \mathbf{G}_{10} when run with challenge bit 1, and returns 1 if the adversary wins. Therefore, the difference between \mathcal{A} 's winning probabilities in games \mathbf{G}_9 and \mathbf{G}_{10} is upper bounded by the respective $\text{IND-CPA}_{n_s, n_a+1}$ advantage of $\mathcal{B}_0^{\text{IND}}$ against KEM:

$$|\text{Adv}_9 - \text{Adv}_{10}| \leq \text{Adv}_{\text{KEM}}^{\text{IND-CPA}_{(n_s, n_a+1)}}(\mathcal{B}_0^{\text{IND}})$$

To keep track of the change in the probability of $\text{Pr}[\text{corrPW}]$, we can adapt the reduction $\mathcal{B}_0^{\text{IND}}$ exactly like in the game-hop before by redefining the output bit to be 1 iff corrPW occurred and $|\text{Pr}[\text{corrPW}_{\mathbf{G}_9}] - \text{Pr}[\text{corrPW}_{\mathbf{G}_{10}}]| \leq \text{Adv}_{\text{KEM}}^{\text{IND-CPA}_{(n_s, n_a+1)}}(\mathcal{B}_1^{\text{IND}})$. At this point, pre-key K (for sessions between non-corrupted parties) is independent of the password and the protocol messages.

Game \mathbf{G}_{11} : Randomize Tags. To argue that the responder tag does not leak significant information on the password or the session key, we replace it with a random value. The change for **Send** queries is shown in Figure 19. Let **TagQueried** be the event that the adversary has queried the random oracle H on input $(pw, apk, pk', c, K_s, "r")$ or $(pw, apk, pk, c, K'_s, "i")$. We argue that due to H being a random oracle, games \mathbf{G}_{10} and \mathbf{G}_{11} are indistinguishable to the adversary unless **TagQueried** occurs. Therefore, if \mathcal{A} can issue at most q_{H} queries to the random oracle H , we have

$$\text{Pr}[\text{corrPW}_{\mathbf{G}_{10}}] - \text{Pr}[\text{corrPW}_{\mathbf{G}_{11}}] = |\text{Adv}_{10} - \text{Adv}_{11}| \leq \text{Pr}[\text{TagQueried}] \leq \frac{q_{\text{H}} \cdot n_s}{|\mathcal{K}|}.$$

5.5 Randomizing Session Key (SG3)

Game \mathbf{G}_{12} : Randomize Session Key. Finally, we replace the final session key for all **Send** and **Execute** queries where flag **trivGuess** did not occur with one chosen independently at random from the session key space \mathcal{SK} , making them independent of previous messages and the password. Let **SKQueried** be the event that the adversary has queried $\text{KDF}'(tag_1, K_s)$. In game \mathbf{G}_{12} , we abort

Adversary $\mathcal{B}_0^{\text{IND}}$	$\text{Send}^1(P, i, msg)$
01 input \mathbf{pk}	07 $k_{pw} \leftarrow \text{KDF}(pw)$
02 $\text{pkIndex} = 0$	08 if \exists record $\text{PK}[(k_{pw}, apk)]:$ //handle replays
03 $b \xleftarrow{\text{unif}} \{0, 1\}$	09 $pk'_s \leftarrow \text{PK}[(k_{pw}, apk)]$
04 $b' \leftarrow \mathcal{A}^{\mathcal{O}^b}(\mathbf{pk})$	10 else:
05 $b'_{\text{IND}} := [b = b']$	11 $pk'_s \leftarrow \mathbf{pk}[\text{pkIndex}]$
06 output b'_{IND}	12 $\text{pkIndex} += 1$
	13 $\text{PK}[(k_{pw}, apk)] \xleftarrow{\text{set}} pk'_s$
	14 find j s.t. $pk'_s = \mathbf{pk}_j$
	15 $(c, K) \leftarrow \text{Chall}(j)$
	16 $tag_1 \leftarrow \text{H}(pw, apk, pk', c, K, "r")$
	17 return c, tag_1

Fig. 18: IND-CPA $_{n,q_C}$ adversary $\mathcal{B}_0^{\text{IND}}$, used to reason about the hop from game \mathbf{G}_9 to \mathbf{G}_{10} . The set of oracles is $\mathcal{O} = \{\text{KDF}, \text{KDF}', \text{IC. enc}, \text{IC. dec}, \text{Execute}, \text{Send}, \text{Reveal}, \text{Corrupt}\}$.

whenever this occurs. We argue that due to KDF' being a random oracle, games \mathbf{G}_{11} and \mathbf{G}_{12} are indistinguishable to the adversary unless SKQueried occurs. Therefore, for an adversary that can issue at most q'_{KDF} queries to the random oracle KDF' and n_s potential session keys, we have that

$$\Pr[\text{corrPW}_{\mathbf{G}_{11}}] - \Pr[\text{corrPW}_{\mathbf{G}_{12}}] = |\mathbf{Adv}_{11} - \mathbf{Adv}_{12}| \leq \Pr[\text{SKQueried}] \leq \frac{q_{\text{KDF}'} \cdot n_s}{|\mathcal{SK}|}$$

After this change, the adversary's **Test** query always responds with a uniformly random value independent of the challenge bit. The winning probability of \mathcal{A} in game \mathbf{G}_{12} is therefore reduced to that of random guessing:

$$\mathbf{Adv}_{12} = \frac{1}{2}.$$

Bounding Correct Password Event. All protocol messages are now independent of the respective password for all fresh sessions, meaning they do not give the adversary any information about those passwords. However, the adversary can still attempt a password guess by picking a password from the password space, using it in a **Send** query, and observing if the game aborts. We can bound the probability of a correct guess using the number of send queries and the password distribution. Assuming a uniform distribution on a password dictionary of size $|\mathcal{D}|$, and \mathcal{A} issues n_a many send queries, we get the bound: $\Pr[\text{corrPW}_{\mathbf{G}_{12}}] \leq \frac{n_a}{|\mathcal{D}|}$. Collecting the probabilities, we can now bound the probability of event **corrPW** occurring in game 7:

$$\begin{aligned} \Pr[\text{corrPW}_{\mathbf{G}_7}] &\leq \sum_{i=7}^{11} |\Pr[\text{corrPW}_{\mathbf{G}_i}] - \Pr[\text{corrPW}_{\mathbf{G}_{i+1}}]| + \Pr[\text{corrPW}_{\mathbf{G}_{12}}] \\ &\leq \frac{n_a}{|\mathcal{D}|} + \mathbf{Adv}_{\text{KEM}}^{\text{ANO-PCA}(q_{\text{IC.dec}} + n_s, n_a + 1)}(\mathcal{B}_1^{\text{ANO}}) + \mathbf{Adv}_{\text{KEM}}^{\text{IND-CPA}(n_s, n_a + 1)}(\mathcal{B}_1^{\text{IND}}) \\ &\quad + \frac{q_{\text{H}} \cdot n_s}{|\mathcal{K}|} + \frac{q_{\text{KDF}'} \cdot n_s}{|\mathcal{SK}|} \end{aligned}$$

To wrap up the proof, we now bound the BPR advantage of an adversary against OCAKE using the triangle inequality. We also fold the two anonymity adversaries $\mathcal{B}_0^{\text{ANO}}$ and $\mathcal{B}_1^{\text{ANO}}$ into one (\mathcal{B}^{ANO}) and

$\text{Send}_{\mathbf{G}_{10}}^1(P, i, msg)$	$\text{Send}_{\mathbf{G}_{11}}^1(P, i, msg)$	$\text{Send}_{\mathbf{G}_{10}}^2(P, i, msg)$	$\text{Send}_{\mathbf{G}_{11}}^2(P, i, msg)$
01 $apk \xleftarrow{\text{parse}} msg$	01 $apk \xleftarrow{\text{parse}} msg$	14 $c, tag_1 \xleftarrow{\text{parse}} msg$	14 $c, tag_1 \xleftarrow{\text{parse}} msg$
02 $k_{pw} \leftarrow \text{KDF}(pw)$	02 $k_{pw} \leftarrow \text{KDF}(pw)$	15 if forward :	15 if forward :
03 $pk' \leftarrow \text{IC.dec}(k_{pw}, apk)$	03 $pk' \leftarrow \text{IC.dec}(k_{pw}, apk)$	16 $K'_s \leftarrow \text{responder's key } K_s$	16 $K'_s \leftarrow \text{responder's key } K_s$
04 if $\text{PK}[(k_{pw}, apk)] \neq \perp$:	04 if $\text{PK}[(k_{pw}, apk)] \neq \perp$:	17 $tag'_{1s} \leftarrow \text{responder's tag } tag_{1s}$	17 $tag'_{1s} \leftarrow \text{responder's tag } tag_{1s}$
05 $pk'_s \leftarrow \text{PK}[(k_{pw}, apk)]$	05 $pk'_s \leftarrow \text{PK}[(k_{pw}, apk)]$	18 else:	18 else:
06 else:	06 else:	19 $K'_s \leftarrow \text{Decap}(sk', c)$	19 $K'_s \leftarrow \text{Decap}(sk', c)$
07 $(pk'_s, sk_s) \leftarrow \$ \text{KGen}$	07 $(pk'_s, sk_s) \leftarrow \$ \text{KGen}$	20 $tag_{1s} \leftarrow \text{H}(pw, apk, pk, c, K'_s, "r")$	20 $tag_{1s} \leftarrow \text{H}(pw, apk, pk, c, K'_s, "r")$
08 $\text{PK}[(k_{pw}, apk)] \xleftarrow{\text{set}} pk'_s$	08 $\text{PK}[(k_{pw}, apk)] \xleftarrow{\text{set}} pk'_s$	21 if $tag_1 = \text{H}(pw, apk, pk, c, K'_s, "r")$:	21 if $tag_1 = \text{H}(pw, apk, pk, c, K'_s, "r")$:
09 $(c, K) \leftarrow \$ \text{Encap}(pk'_s)$	09 $(c, K) \leftarrow \$ \text{Encap}(pk'_s)$	22 if $tag_1 = tag'_{1s}$:	22 if $tag_1 = tag'_{1s}$:
10 $K_s \xleftarrow{\text{unif}} \mathcal{K}$	10 $K_s \xleftarrow{\text{unif}} \mathcal{K}$	23 $tag_2 \leftarrow \text{H}(pw, apk, pk, c, K'_s, "i")$	23 $tag_2 \leftarrow \text{H}(pw, apk, pk, c, K'_s, "i")$
11 $tag_1 \leftarrow \text{H}(pw, apk, pk', c, K_s, "r")$	11 $tag_1 \leftarrow \text{H}(pw, apk, pk', c, K_s, "r")$	24 $tag_{2s} \xleftarrow{\text{unif}} \mathcal{T}$	24 $tag_{2s} \xleftarrow{\text{unif}} \mathcal{T}$
12 $tag_{1s} \xleftarrow{\text{unif}} \mathcal{T}$	12 $tag_{1s} \xleftarrow{\text{unif}} \mathcal{T}$	25 $SK \leftarrow \text{KDF}'(tag_1, K'_s)$	25 $SK \leftarrow \text{KDF}'(tag_1, K'_s)$
13 return c, tag_1	return c, tag_{1s}	26 $SK \leftarrow \text{KDF}'(tag_{1s}, K'_s)$	26 $SK \leftarrow \text{KDF}'(tag_{1s}, K'_s)$
		27 $K[(P, i)] \xleftarrow{\text{set}} SK$	27 $K[(P, i)] \xleftarrow{\text{set}} SK$
		28 return tag_2	return tag_{2s}

Fig. 19: Randomizing tags. The domain of the random oracle H is \mathcal{T} . The tag check for the initiator tag is modified in an equivalent fashion.

the two indistinguishability adversaries $\mathcal{B}_0^{\text{IND}}$ and $\mathcal{B}_1^{\text{IND}}$ into \mathcal{B}^{IND} . We consolidate the random oracles into RO.

$$\begin{aligned}
\text{Adv}_{\text{OCAKE}}^{\text{BPR}}(\mathcal{A}) &= \underbrace{|\Pr[\mathbf{G}_0 \Rightarrow 1]|}_{=\text{Adv}_0} - \frac{1}{2} = |\text{Adv}_0 - \text{Adv}_1 + \text{Adv}_1 - \dots + \text{Adv}_{12} - \frac{1}{2}| \\
&= \frac{n_a}{|\mathcal{D}|} + n_s^2 \cdot \eta_{\text{KGen}} + \frac{q_{\text{KDF}}^2}{2 \cdot |\mathcal{K}_{pw}|} + \frac{q_{\text{IC}}^2}{2 \cdot |\mathcal{PK}|} + \frac{q_{\text{IC}}^2}{|\mathcal{PK}|} \\
&\quad + \frac{q_{\text{H}}^2}{2 \cdot |\mathcal{T}|} + 2 \cdot \frac{q_{\text{H}} \cdot n_s}{|\mathcal{K}|} + \text{Adv}_{\text{KEM}}^{\text{PKU}(q_{\text{IC.dec}} + n_s)}(\mathcal{B}^{\text{PKU}}) \\
&\quad + \text{Adv}_{\text{KEM}}^{\text{ANO-PCA}(q_{\text{IC.dec}} + n_s, n_a + 1)}(\mathcal{B}_0^{\text{ANO}}) + \text{Adv}_{\text{KEM}}^{\text{ANO-PCA}(q_{\text{IC.dec}} + n_s, n_a + 1)}(\mathcal{B}_1^{\text{ANO}}) \\
&\quad + \text{Adv}_{\text{KEM}}^{\text{IND-CPA}(n_s, n_a + 1)}(\mathcal{B}_0^{\text{IND}}) + \text{Adv}_{\text{KEM}}^{\text{IND-CPA}(n_s, n_a + 1)}(\mathcal{B}_1^{\text{IND}}) \\
&\quad + 2 \cdot n_s \cdot \delta + 2 \cdot \frac{q_{\text{KDF}' \cdot n_s}}{|\mathcal{SK}|} \\
&\leq \frac{n_a}{|\mathcal{D}|} + \text{Adv}_{\text{KEM}}^{\text{PKU}(q_{\text{IC.dec}} + n_s)}(\mathcal{B}^{\text{PKU}}) + 2 \cdot \text{Adv}_{\text{KEM}}^{\text{ANO-PCA}(q_{\text{IC.dec}} + n_s, n_a + 1)}(\mathcal{B}^{\text{ANO}}) \\
&\quad + 2 \cdot \text{Adv}_{\text{KEM}}^{\text{IND-CPA}(n_s, n_a + 1)}(\mathcal{B}^{\text{IND}}) + \frac{3 \cdot q_{\text{IC}}^2}{2 \cdot |\mathcal{PK}|} + 2 \cdot n_s \cdot \delta + n_s^2 \cdot \eta_{\text{KGen}} \\
&\quad + q_{\text{RO}} \cdot n_s \cdot \left(\frac{2}{|\mathcal{SK}|} + \frac{2}{|\mathcal{K}|} \right) + q_{\text{RO}}^2 \cdot \left(\frac{1}{2 \cdot |\mathcal{T}|} + \frac{1}{2 \cdot |\mathcal{K}_{pw}|} \right)
\end{aligned}$$

$\text{Send}_{\mathbf{G}_{11}}^2(P, i, msg)$	$\text{Send}_{\mathbf{G}_{12}}^2(P, i, msg)$	$\text{Send}_{\mathbf{G}_{11}}^3(P, i, msg)$	$\text{Send}_{\mathbf{G}_{12}}^3(P, i, msg)$
01 $c, tag_1 \xleftarrow{\text{parse}} msg$		14 $tag_2 \xleftarrow{\text{parse}} msg$	
02 if forward :		15 if forward :	
03 $K'_s \leftarrow$ responder's key K_s		16 $tag'_{2s} \leftarrow$ responder's tag tag_{2s}	
04 $tag'_{1s} \leftarrow$ responder's tag tag_{1s}		17 else:	
05 else:		18 $tag_{2s} \leftarrow H(pw, apk, pk, c, K'_s, "i")$	
06 $K'_s \leftarrow \text{Decap}(sk', c)$		19 if $tag_2 = tag'_{2s}$	
07 $tag_{1s} \leftarrow H(pw, apk, pk, c, K'_s, "r")$		20 $SK \leftarrow \text{KDF}'(tag_{1s}, K_s)$	
08 ...		21 $K[(P,i)] \xleftarrow{\text{set}} SK$	$K[(P,i)] \xleftarrow{\text{set}} SK_s$
09 if $tag_1 = tag'_{1s}$:			
10 $tag_{2s} \xleftarrow{\text{unif}} \mathcal{T}$			
11 $SK \leftarrow \text{KDF}'(tag_1, K'_s)$	$SK_s \xleftarrow{\text{unif}} SK$		
12 $K[(P,i)] \xleftarrow{\text{set}} SK$	$K[(P,i)] \xleftarrow{\text{set}} SK_s$		
13 return tag_{2s}			

Fig. 20: In game \mathbf{G}_{12} , the final session key is randomized. To remain consistent, the initiator uses the responder's session key.

References

- AAB⁺20. Carlos Aguilar-Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor, and Jurjen Bos. HQC. Technical report, National Institute of Standards and Technology, 2020. available at <https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions>.
- ABB⁺20. Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Phillippe Gaborit, Shay Gueron, Tim Guneyasu, Carlos Aguilar-Melchor, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, Gilles Zémor, Valentin Vasseur, and Santosh Ghosh. BIKE. Technical report, National Institute of Standards and Technology, 2020. available at <https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions>.
- ABB⁺22. Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Phillippe Gaborit, Shay Gueron, Tim Guneyasu, Carlos Aguilar-Melchor, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, Gilles Zémor, Valentin Vasseur, Santosh Ghosh, and Jan Richter-Brokmann. BIKE. Technical report, National Institute of Standards and Technology, 2022. available at <https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions>.
- ABC⁺20. Martin R. Albrecht, Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, Tanja Lange, Varun Maram, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Kenneth G. Paterson, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Cen Jung Tjhai, Martin Tomlinson, and Wen Wang. Classic McEliece. Technical report, National Institute of Standards and Technology, 2020. available at <https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions>.
- AEK⁺22. Michel Abdalla, Thorsten Eisenhofer, Eike Kiltz, Sabrina Kunzweiler, and Doreen Riepel. Password-authenticated key exchange from group actions. In *Annual International Cryptology Conference*, pages 699–728. Springer, 2022.
- AFP05. Michel Abdalla, Pierre-Alain Fouque, and David Pointcheval. Password-based authenticated key exchange in the three-party setting. In Serge Vaudenay, editor, *PKC 2005*, volume 3386 of *LNCS*, pages 65–84. Springer, Heidelberg, January 2005.

- AHH23. Michel Abdalla, Björn Haase, and Julia Hesse. CPace, a balanced composable PAKE. Internet-Draft draft-irtf-cfrg-cpace-08, Internet Engineering Task Force, July 2023. Work in Progress.
- BBDP01. Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. Key-privacy in public-key encryption. In Colin Boyd, editor, *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 566–582. Springer, Heidelberg, December 2001.
- BBM00. Mihir Bellare, Alexandra Boldyreva, and Silvio Micali. Public-key encryption in a multi-user setting: Security proofs and improvements. In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 259–274. Springer, Heidelberg, May 2000.
- BCJ⁺19. Tatiana Bradley, Jan Camenisch, Stanislaw Jarecki, Anja Lehmann, Gregory Neven, and Jiayu Xu. Password-authenticated public-key encryption. In Robert H. Deng, Valérie Gauthier-Umaña, Martín Ochoa, and Moti Yung, editors, *ACNS 19*, volume 11464 of *LNCS*, pages 442–462. Springer, Heidelberg, June 2019.
- BCP⁺23. Hugo Beguinet, Céline Chevalier, David Pointcheval, Thomas Ricosset, and Mélissa Rossi. Get a cake: Generic transformations from key encapsulation mechanisms to password authenticated key exchanges. *Cryptology ePrint Archive*, 2023.
- BDF⁺11. Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 41–69. Springer, Heidelberg, December 2011.
- BDK⁺17. Joppe Bos, Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, and Damien Stehlé. CRYSTALS – Kyber: a CCA-secure module-lattice-based KEM. *Cryptology ePrint Archive*, Report 2017/634, 2017. <https://eprint.iacr.org/2017/634>.
- BDK⁺18. Joppe Bos, Leo Ducas, Eike Kiltz, T Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehle. CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM. In *IEEE (EuroS&P) 2018*, pages 353–367, 2018.
- Ber22. Daniel J. Bernstein. Multi-ciphertext security degradation for lattices. *Cryptology ePrint Archive*, Report 2022/1580, 2022. <https://eprint.iacr.org/2022/1580>.
- BFK09. Jens Bender, Marc Fischlin, and Dennis Kügler. Security analysis of the PACE key-agreement protocol. In Pierangela Samarati, Moti Yung, Fabio Martinelli, and Claudio Agostino Ardagna, editors, *ISC 2009*, volume 5735 of *LNCS*, pages 33–48. Springer, Heidelberg, September 2009.
- BHK⁺19. Daniel J. Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe. The SPHINCS⁺ signature framework. In Lorenzo Cavallaro, Johannes Kinder, XiaoFeng Wang, and Jonathan Katz, editors, *ACM CCS 2019*, pages 2129–2146. ACM Press, November 2019.
- Bla06. John Black. The ideal-cipher model, revisited: An uninstantiable blockcipher-based hash function. In Matthew J. B. Robshaw, editor, *FSE 2006*, volume 4047 of *LNCS*, pages 328–340. Springer, Heidelberg, March 2006.
- BM92. Steven Bellovin and Michael Merritt. Encrypted key exchange: Password-based protocols secure against dictionary attacks. *Security and Privacy, IEEE Symposium on*, 0:72, 04 1992.
- BPR00. Mihir Bellare, David Pointcheval, and Phillip Rogaway. Authenticated key exchange secure against dictionary attacks. In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 139–155. Springer, Heidelberg, May 2000.
- BR93. Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM CCS 93*, pages 62–73. ACM Press, November 1993.
- CAK18. Rakyong Choi, Hyeongcheol An, and Kwangjo Kim. Atlast: Another three-party lattice-based pake scheme. 2018.
- Can01. Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *42nd FOCS*, pages 136–145. IEEE Computer Society Press, October 2001.
- CFHL21. Kai-Min Chung, Serge Fehr, Yu-Hsuan Huang, and Tai-Ning Liao. On the compressed-oracle technique, and post-quantum security of proofs of sequential work. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 598–629. Springer, Heidelberg, October 2021.
- CKS23. Dharminder Chaudhary, Uddeshaya Kumar, and Kashif Saleem. A construction of three party post quantum secure authenticated key exchange using ring learning with errors and ecc cryptography. *IEEE Access*, 2023.

- CLM⁺18. Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part III*, volume 11274 of *LNCS*, pages 395–427. Springer, Heidelberg, December 2018.
- Cou06. Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006. <https://eprint.iacr.org/2006/291>.
- DAL⁺17. Jintai Ding, Saed Alsayigh, Jean Lancrenon, Saraswathy Rv, and Michael Snook. Provably secure password authenticated key exchange based on rlwe for the post-quantum world. In *Cryptographers Track at the RSA conference*, pages 183–204. Springer, 2017.
- DBK20. Vivek Dabra, Anju Bala, and Saru Kumari. Lba-pake: Lattice-based anonymous password authenticated key exchange for mobile devices. *IEEE Systems Journal*, 15(4):5067–5077, 2020.
- DFMS21. Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Online-extractability in the quantum random-oracle model. Cryptology ePrint Archive, Report 2021/280, 2021. <https://eprint.iacr.org/2021/280>, accepted for publication at Eurocrypt 2022.
- DFMS22. Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Online-extractability in the quantum random-oracle model. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part III*, volume 13277 of *LNCS*, pages 677–706. Springer, Heidelberg, May / June 2022.
- DKL⁺18. Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Dilithium: A lattice-based digital signature scheme. *IACR TCHES*, 2018(1):238–268, 2018. <https://tches.iacr.org/index.php/TCHES/article/view/839>.
- DKS18. Luca De Feo, Jean Kieffer, and Benjamin Smith. Towards practical key exchange from ordinary isogeny graphs. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part III*, volume 11274 of *LNCS*, pages 365–394. Springer, Heidelberg, December 2018.
- GHHM21. Alex B. Grilo, Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz. Tight adaptive reprogramming in the QROM. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part I*, volume 13090 of *LNCS*, pages 637–667. Springer, Heidelberg, December 2021.
- GKP18. Federico Giacon, Eike Kiltz, and Bertram Poettering. Hybrid encryption in a multi-user setting, revisited. In Michel Abdalla and Ricardo Dahab, editors, *PKC 2018, Part I*, volume 10769 of *LNCS*, pages 159–189. Springer, Heidelberg, March 2018.
- GMP21. Paul Grubbs, Varun Maram, and Kenneth G. Paterson. Anonymous, robust post-quantum public key encryption. Cryptology ePrint Archive, Report 2021/708, 2021. <https://eprint.iacr.org/2021/708>.
- GMP22. Paul Grubbs, Varun Maram, and Kenneth G. Paterson. Anonymous, robust post-quantum public key encryption. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part III*, volume 13277 of *LNCS*, pages 402–432. Springer, Heidelberg, May / June 2022.
- GSG⁺23. Songhui Guo, Yunfan Song, Song Guo, Yeming Yang, and Shuaichao Song. Three-party password authentication and key exchange protocol based on mlwe. *Symmetry*, 15(9):1750, 2023.
- HHM22. Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz. Failing gracefully: Decryption failures and the Fujisaki-Okamoto transform. In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part IV*, volume 13794 of *LNCS*, pages 414–443. Springer, Heidelberg, December 2022.
- HV22. Loïs Huguenin-Dumittan and Serge Vaudenay. On IND-qCCA security in the ROM and its applications - CPA security is sufficient for TLS 1.3. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part III*, volume 13277 of *LNCS*, pages 613–642. Springer, Heidelberg, May / June 2022.
- HvO22. Feng Hao and Paul C. van Oorschot. Sok: Password-authenticated key exchange – theory, practice, standardization and real-world lessons. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, ASIA CCS ’22, page 697711, New York, NY, USA, 2022. Association for Computing Machinery.
- HY18. Akinori Hosoyamada and Kan Yasuda. Building quantum-one-way functions from block ciphers: Davies-Meyer and Merkle-Damgård constructions. In Thomas Peyrin and Steven Galbraith,

- editors, *ASIACRYPT 2018, Part I*, volume 11272 of *LNCS*, pages 275–304. Springer, Heidelberg, December 2018.
- JGH⁺20. Shaoquan Jiang, Guang Gong, Jingnan He, Khoa Nguyen, and Huaxiong Wang. Pakes: new framework, new techniques and more efficient lattice-based constructions in the standard model. In *IACR International Conference on Public-Key Cryptography*, pages 396–427. Springer, 2020.
- JKX18. Stanislaw Jarecki, Hugo Krawczyk, and Jiayu Xu. OPAQUE: An asymmetric PAKE protocol secure against pre-computation attacks. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 456–486. Springer, Heidelberg, April / May 2018.
- KAA19. Amir Hassani Karbasi, Reza Ebrahimi Atani, and Shahabaddin Ebrahimi Atani. A new ring-based sphf and pake protocol on ideal lattices. *ISecure*, 11(1), 2019.
- KV09. Jonathan Katz and Vinod Vaikuntanathan. Smooth projective hashing and password-based authenticated key exchange from lattices. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 636–652. Springer, 2009.
- Lan16. Jean Lancrenon. On password-authenticated key exchange security modeling. In Frank Stajano, Stig F. Mjølsnes, Graeme Jenkinson, and Per Thorsheim, editors, *Technology and Practice of Passwords*, pages 120–143, Cham, 2016. Springer International Publishing.
- LW18. Zengpeng Li and Ding Wang. Two-round pake protocol over lattices without nizk. In *International Conference on Information Security and Cryptology*, pages 138–159. Springer, 2018.
- LW22. Zengpeng Li and Ding Wang. Achieving one-round password-based authenticated key exchange over lattices. *IEEE Transactions on Services Computing*, 15(1):308–321, 2022.
- LWM20. Zengpeng Li, Ding Wang, and Eduardo Morais. Quantum-safe round-optimal password authentication for mobile devices. *IEEE transactions on dependable and secure computing*, 19(3):1885–1899, 2020.
- LZJY19. Chao Liu, Zhongxiang Zheng, Keting Jia, and Qidi You. Provably secure three-party password-based authenticated key exchange from rlwe. In *Information Security Practice and Experience: 15th International Conference, ISPEC 2019, Kuala Lumpur, Malaysia, November 26–28, 2019, Proceedings 15*, pages 56–72. Springer, 2019.
- MX23. Varun Maram and Keita Xagawa. Post-quantum anonymity of Kyber. In Alexandra Boldyreva and Vladimir Kolesnikov, editors, *PKC 2023, Part I*, volume 13940 of *LNCS*, pages 3–35. Springer, Heidelberg, May 2023.
- NAB⁺20. Michael Naehrig, Erdem Alkim, Joppe Bos, Léo Ducas, Karen Easterbrook, Brian LaMacchia, Patrick Longa, Ilya Mironov, Valeria Nikolaenko, Christopher Peikert, Ananth Raghunathan, and Douglas Stebila. FrodoKEM. Technical report, National Institute of Standards and Technology, 2020. available at <https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions>.
- PFH⁺22. Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. FALCON. Technical report, National Institute of Standards and Technology, 2022. available at <https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022>.
- PZ23. Jiaxin Pan and Runzhi Zeng. A generic construction of tightly secure password-based authenticated key exchange. Cryptology ePrint Archive, Paper 2023/1334, 2023. <https://eprint.iacr.org/2023/1334>.
- RG21. Peixin Ren and Xiaozhuo Gu. Practical post-quantum password-authenticated key exchange based-on module-lattice. In *International Conference on Information Security and Cryptology*, pages 137–156. Springer, 2021.
- RGW23. Peixin Ren, Xiaozhuo Gu, and Ziliang Wang. Efficient module learning with errors-based post-quantum password-authenticated key exchange. *IET Information Security*, 17(1):3–17, 2023.
- RS06. Alexander Rostovtsev and Anton Stolbunov. Public-Key Cryptosystem Based On Isogenies. Cryptology ePrint Archive, Report 2006/145, 2006. <https://eprint.iacr.org/2006/145>.
- SA23. Kübra Seyhan and Sedat Akleylek. A new password-authenticated module learning with rounding-based key exchange protocol: Saber. pake. *The Journal of Supercomputing*, pages 1–38, 2023.

- Son14. Fang Song. A note on quantum security for post-quantum cryptography. In Michele Mosca, editor, *Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014*, pages 246–265. Springer, Heidelberg, October 2014.
- TLZ⁺21. Yongli Tang, Ying Li, Zongqu Zhao, Jing Zhang, Lina Ren, and Yuanhong Li. Improved verifier-based three-party password-authenticated key exchange protocol from ideal lattices. *Security and Communication Networks*, 2021:1–13, 2021.
- TSJL18. Oleg Taraskin, Vladimir Soukharev, David Jao, and Jason T LeGrow. An isogeny-based password-authenticated key establishment protocol. *IACR Cryptol. ePrint Arch.*, 2018:886, 2018.
- TY19. Shintaro Terada and Kazuki Yoneyama. Password-based authenticated key exchange from standard isogeny assumptions. In *Provable Security: 13th International Conference, ProvSec 2019, Cairns, QLD, Australia, October 1–4, 2019, Proceedings 13*, pages 41–56. Springer, 2019.
- WCL⁺22. Jinhua Wang, Ting Chen, Yanyan Liu, Yu Zhou, and XinFeng Dong. Efficient two-party authentication key agreement protocol using reconciliation mechanism from lattice. In *International Conference on Security and Privacy in New Computing Environments*, pages 32–47. Springer, 2022.
- Xag21. Keita Xagawa. Anonymity of NIST PQC round-3 KEMs. Cryptology ePrint Archive, Report 2021/1323, 2021. <https://eprint.iacr.org/2021/1323>.
- Xag22. Keita Xagawa. Anonymity of NIST PQC round 3 KEMs. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part III*, volume 13277 of *LNCS*, pages 551–581. Springer, Heidelberg, May / June 2022.
- XHCC17. Dongqing Xu, Debiao He, Kim-Kwang Raymond Choo, and Jianhua Chen. Provably secure three-party password authenticated key exchange protocol based on ring learning with error. *Cryptology ePrint Archive*, 2017.
- YGS⁺20. Anqi Yin, Yuanbo Guo, Yuanming Song, Tongzhou Qu, and Chen Fang. Two-round password-based authenticated key exchange from lattices. *Wireless Communications and Mobile Computing*, 2020:1–13, 2020.
- YGWX19. Yingshan Yang, Xiaozhuo Gu, Bin Wang, and Taizhong Xu. Efficient password-authenticated key exchange from rlwe based on asymmetric key consensus. In *International Conference on Information Security and Cryptology*, pages 31–49. Springer, 2019.
- ZG17. Hongfeng Zhu and Shuai Geng. Simple and universal construction for round-optimal password authenticated key exchange towards quantum-resistant. *J. Inf. Hiding Multim. Signal Process.*, 8(4):798–807, 2017.
- Zha19. Mark Zhandry. How to record quantum queries, and applications to quantum indistinguishability. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 239–268. Springer, Heidelberg, August 2019.
- ZHS14. Hongfeng Zhu, Xin Hao, and Yang Sun. Elliptic curve isogenies-based three-party password authenticated key agreement scheme towards quantum-resistant. *J. Inf. Hiding Multim. Signal Process.*, 5(4):672–689, 2014.
- ZY17. Jiang Zhang and Yu Yu. Two-round pake from approximate sph and instantiations from lattices. In *Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3–7, 2017, Proceedings, Part III 23*, pages 37–67. Springer, 2017.

Table 2: Execution times in ms on Intel(R) Core(TM) i7-8565U @1.80GHz

KEM	KGen	Decap	Encap	Hashing	Full Protocol
kyber512	0.106	0.181	0.231	0.044	0.570
kyber768	0.181	0.276	0.280	0.060	0.798
kyber1024	0.273	0.370	0.323	0.075	1.048
lightsaber	0.266	0.369	0.321	0.078	1.041
saber	0.373	0.573	0.246	0.006	1.255
firesaber	0.636	0.901	0.293	0.068	1.899
bikel1	10.202	18.247	0.307	0.076	28.849
frodokem640shake	13.658	15.954	1.286	0.407	31.332
frodokem976shake	29.279	32.791	2.011	0.659	64.773
frodokem1344shake	53.376	62.659	2.776	0.920	119.768
mceliece348864f	1125.563	70.416	36.463	8.057	1240.570
mceliece460896f	4411.609	143.784	74.199	16.065	4645.813
mceliece6688128f	4406.359	143.925	74.011	15.941	4640.402
mceliece6960119f	8269.310	263.632	148.240	32.938	8714.488
mceliece8192128f	11216.323	334.980	191.893	41.960	11785.619

Table 3: Execution times in clock cycles on STM32-NUCLEO-L4R5ZI - *Last column in seconds

KEM	Impl	KGen	Decap	Encap	Hashing	Full Protocol	Full Protocol*
kyber512	m4fspeed	745668.8	801732.8	611474.6	791643.0	3979406.0	0.9949
	m4fstack	745289.5	803584.3	611474.5	791625.0	3979289.0	0.9948
kyber768	m4fspeed	1206150.1	1316398.2	832517.0	1131008.0	5778158.9	1.4445
	m4fstack	1202797.1	1317317.0	832512.2	1131007.0	5770321.9	1.4426
kyber1024	m4fspeed	1914393.3	2035966.4	1053568.2	1536296.0	8155277.7	2.0388
	m4fstack	1919265.7	2046946.9	1053567.4	1536296.0	8164499.4	2.0411
lightsaber	m4fspeed	600635.0	724859.0	537659.8	701149.0	3546177.6	0.8865
	m4fstack	672138.0	855452.0	537645.9	701125.0	3750526.8	0.9376
saber	m4fspeed	1076086.0	1230242.0	721860.4	1017093.0	5257675.2	1.3144
	m4fstack	1253891.0	1497496.0	721841.8	1017047.0	5712326.0	1.4281
firesaber	m4fspeed	1646591.0	1829134.0	906052.8	1334116.0	7208626.4	1.8022
	m4fstack	1978657.1	2283628.0	906052.0	1334064.0	7982843.9	1.9957
frodokem640shake	clean	135141547.0	134830464.0	5686100.0	9133260.0	292227256.8	73.0568
bikel1	m4f	32084596.0	69879800.0	1035143.6	1514263.0	106074175.2	26.5185