On Security Proofs of Existing Equivalence Class Signature Schemes

Balthazar Bauer[1] and Georg Fuchsbauer[2]

[1] UVSQ, France
[2] TU Wien, Austria
first.last@{ens.fr, tuwien.ac.at}

Abstract. Equivalence class signatures (EQS), introduced by Hanser and Slamanig (AC '14), sign vectors of elements from a bilinear group. Signatures can be "adapted", meaning that anyone can transform a signature on a vector to a (random) signature on any multiple of that vector. (Signatures thus authenticate equivalence classes.) A transformed signature/message pair is then indistinguishable from a random signature on a random message. EQS have been used to efficiently instantiate (delegatable) anonymous credentials, (round-optimal) blind signatures, ring and group signatures and anonymous tokens.
The original EQS construction (J. Crypto '19) is only proven in the generic group model, while the first construction from standard assumptions (PKC '18) only yields security guarantees insufficient for most applications. Two works (AC '19, PKC '22) propose applicable schemes which assume the existence of a common reference string for the anonymity notion. Their unforgeability is argued via a security proof from standard (or non-interactive) assumptions.
In this work we show that their security proof is flawed and explain the subtle issue.

1 Introduction

Structure-preserving signatures (SPS) [AFG+10] are defined over a *bilinear group*, which consists of three groups $(\mathbb{G}_t, +)$, for $t \in \{1, 2, T\}$, of prime order p and a (non-degenerate) bilinear map $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In SPS, messages, as well as verification keys and signatures, consist of elements from $\mathbb{G}_1$ and $\mathbb{G}_2$.

The concept of *SPS on equivalence classes*, or equivalence class signatures (EQS) for short, was introduced by Hanser and Slamanig [HS14] and later securely instantiated [Fuc14, FHS19]. EQS are SPS with message space $\mathcal{M} = (\mathbb{G}_t^*)^\ell$, for some $t \in \{1, 2\}$, $\ell > 1$ and $\mathbb{G}_t^* := \mathbb{G}_t \setminus \{0_t\}$, on which one defines the following equivalence relation:

$$\boldsymbol{M} \sim \boldsymbol{M'} :\Leftrightarrow \exists\, \mu \in \mathbb{Z}_p^* : \boldsymbol{M'} = \mu \cdot \boldsymbol{M}. \tag{1}$$

EQS provide an additional functionality ChgRep: given a verification key pk, a signature σ on $\boldsymbol{M} \in \mathcal{M}$ under pk, and a value $\mu \in \mathbb{Z}_p^*$, ChgRep returns a signature on the message $\mu \cdot \boldsymbol{M}$, without requiring the secret key. A signature on

$\boldsymbol{M}$ thus authenticates the entire equivalence class $[\boldsymbol{M}]_\sim$ of $\boldsymbol{M}$ w.r.t. the relation in (1), and ChgRep lets one change the *representative* of that class.

Accordingly, *unforgeability* is defined w.r.t. classes, that is, for any adversary, given pk and an oracle for signatures on messages $\boldsymbol{M}_1, \boldsymbol{M}_2, \dots$ of its choice, it is infeasible to compute a signature on any $\boldsymbol{M}^*$ with $\boldsymbol{M}^* \notin [\boldsymbol{M}_1]_\sim \cup [\boldsymbol{M}_2]_\sim \cup \dots$ EQS must also be *class-hiding*, which means it is hard to distinguish random message pairs $(\boldsymbol{M}, \boldsymbol{M}')$ with $\boldsymbol{M} \sim \boldsymbol{M}'$ from random pairs $(\boldsymbol{M}, \boldsymbol{M}') \leftarrow\!\!\$\ \mathcal{M} \times \mathcal{M}$ (this is equivalent to the decisional Diffie-Hellman (DDH) problem being hard in $\mathbb{G}_t$).

Signature adaptation is another EQS security notion, requiring that for any (possibly maliciously generated) public key pk, any $\boldsymbol{M} \in \mathcal{M}$, any valid σ on $\boldsymbol{M}$ under pk and any $\mu \in \mathbb{Z}_p^*$, running $\mathsf{ChgRep}(pk, \boldsymbol{M}, \sigma, \mu)$ returns a uniform element in the set of all valid signatures on $\mu \cdot \boldsymbol{M}$. This notion, together with class-hiding, implies that a malicious signer that is given some $\boldsymbol{M}$ and generates a signature σ on $\boldsymbol{M}$ cannot distinguish the following: either $\sigma' \leftarrow \mathsf{ChgRep}(pk, \boldsymbol{M}, \sigma, \mu)$ and $\mu \cdot \boldsymbol{M}$ for $\mu \leftarrow\!\!\$\ \mathbb{Z}_p^*$; or a uniformly random signature on a message $\boldsymbol{M}' \leftarrow \mathcal{M}$ under pk.

The first EQS scheme [FHS19] remains the most efficient to date, with signatures in $\mathbb{G}_1^2 \times \mathbb{G}_2$. However, unforgeability of the scheme is proved directly in the generic group model [Nec94, Sho97, Mau05].

Applications of EQS. Equivalence class signatures have found numerous applications in concepts related to anonymous authentication. The resulting instantiations are particularly efficient, since both messages and signatures can be *re-randomized*, after which they can be given "in the clear", where in other constructions they need to be hidden using zero-knowledge proofs.

Anonymous credentials. The first application of EQS was the construction of *attribute-based credentials* [CL03], which let users obtain credentials for a set of attributes, of which they can later selectively disclose any subset. Such *showings* of attributes should be unlinkable and reveal only the disclosed attributes. The EQS-based credential construction [FHS19] is the first for which the communication complexity of showing a credential is independent of the number of disclosed attributes. Moreover, it achieves strong anonymity guarantees even against malicious credential issuers. Slamanig and others added revocation of users [DHS15] and give a scheme that enables outsourcing of sensitive computation to a restricted device [HS21].

"Signatures with flexible public key" [BHKS18] adapt the concept of adaptation within equivalence classes from messages to public keys, and "mercurial signatures" [CL19, CL21, CLP22] let one adapt signatures to equivalent keys and equivalent messages. The main motivation of mercurial signatures was the construction of (non-interactively) *delegatable* anonymous credentials [BCC+09, Fuc11], which were later improved [MSBM23]. Multi-authority anonymous credentials have also been constructed from mercurial signatures [MBG+23] .

Blind signatures. Building on earlier work [BFPV13] that uses randomizable zero-knowledge proofs [FP09], another line of research [FHS15, FHKS16] constructs *blind signatures* from EQS. These allow a user to obtain a signature from a signer, who learns neither the message nor the signature. These EQS-based schemes do not assume a common reference string, achieve blindness against malicious signers and are round-optimal and thus concurrently secure. Hanzlik [Han23] recently used the original EQS scheme [FHS19] to construct *non-interactive* blind signatures on random messages.

Group signatures. Derler and Slamanig [DS16] and Clarisse and Sanders [CS20] use EQS to construct very efficient group signatures schemes. The former also added dynamic adding of members [DS18].

Other cryptographic primitives. Further applications of EQS include *verifiably encrypted signatures* [HRS15], *access-control encryption* [FGKO17], *sanitizable signatures* [BLL+19] and privacy-preserving *incentive systems* [BEK+20]. The original EQS scheme [FHS19] was used to build highly scalable *mix nets* [HPP20] and the most efficient instantiation of *anonymous counting tokens* [BRS23].

Constructions from falsifiable assumptions. A computational hardness assumption is *falsifiable* [Nao03] if the challenger that runs the security game with an adversary can efficiently decide whether the adversary has broken the assumption. The first instantiation of EQS [FHS19] can be considered based on an (interactive and) *non-falsifiable* assumption: namely its unforgeability, justified via a proof in the generic group model (GGM). Recall that to determine whether the adversary broke unforgeability, one needs to check whether the message $\boldsymbol{M}^*$ returned by the adversary is in the same equivalence class as one of the queried messages (in which case the adversary could efficiently compute a signature on $\boldsymbol{M}^*$ via ChgRep). Now, by the *class-hiding* property, this is hard to decide.

The first EQS scheme from standard assumptions, namely Matrix-Diffie-Hellman assumptions [EHK+13], was proposed by Fuchsbauer and Gay [FG18], but the scheme has some drawbacks: its signatures can only be adapted once and it only satisfies a weaker notion called *existential unforgeability under chosen open message attack* (EUF-CoMA): when the adversary makes a signing query, it must provide the discrete logarithms of the components of the queried message. Note that EUF-CoMA *is* efficiently decidable: For simplicity, consider $\ell = 2$ and for all i, let $(m_{i,1}, m_{i,2}) \in (\mathbb{Z}_p^*)^2$ be the adversary's queries (i.e., the logarithms of the components of the queried message $\boldsymbol{M}_i$). Then the message $\boldsymbol{M}^* = (M_1^*, M_2^*)$ returned by the adversary is not in any of the queried classes if and only if $m_{i,2} \cdot M_1^* \neq m_{i,1} \cdot M_2^*$ for all i.

Khalili, Slamanig and Dakhilalian [KSD19] show that the notion of *signature adaption* achieved by the scheme [FG18] must assume honest keys and honest signatures, which makes it inadequate for most applications. To construct a scheme appropriate for applications with standard-model security, they first propose more syntax modifications: in addition to a signature, the signing algorithm also creates a *tag*, which is required by ChgRep (but not needed for signature verification). As with the previous scheme [FG18], signatures can only be adapted once (which does not impact the considered applications).

Moreover, they consider a trusted setup, which generates a *common reference string* (CRS) in addition to setting up the groups. *Signature adaptation* is then defined w.r.t. honestly generated parameters. This change weakens the anonymity guarantees in applications such as anonymous credentials, which did not require trust assumptions in the original model [FHS19].

Building on an existing SPS scheme [GHKP18], Khalili, Slamanig and Dakhilalian [KSD19] propose an EQS construction in their new model with signatures in $\mathbb{G}_1^8 \times \mathbb{G}_2^9$. Their construction is (claimed to be) proved secure under the *SXDH* assumption, which states that DDH is hard in $\mathbb{G}_1$ and $\mathbb{G}_2$. Building on this work, Connolly, Lafourcade and Perez-Kempner [CLP22] propose a more efficient scheme (with signatures in $\mathbb{G}_1^9 \times \mathbb{G}_2^4$), which uses as additional assumption *extKerMDH* [CH20].

A flaw in the security proof of the CRS-based schemes. We describe a flaw in the security proofs of the two CRS-based schemes [KSD19, CLP22]. In particular, a game hop in the unforgeability proof changes the distribution of the signatures given to the adversary. The change in the adversary's winning probability is then bounded by the advantage of a reduction in solving a computational problem. However, since EQS-unforgeability is not efficiently decidable, the resulting reduction would not be efficient, and the security bound of the underlying problem can thus not be applied. In fact, the authors do specify an efficient reduction, but its winning probability is not the difference of the adversary's winning probabilities.

In more detail, the hop from Game 0 to Game 1 [KSD19, Theorem 2] modifies the way the purported forgery, i.e, the signature on $\boldsymbol{M}^*$ output by the adversary $\mathcal{A}$ is verified. The authors then argue that from a forgery that verifies in Game 0 but not Game 1 (which is a property that can be checked efficiently), a reduction $\mathcal{B}$ can extract a solution to a computational problem (*KerMDH* [MRV16]). From this, the authors deduce that $\mathbf{Adv}_0 - \mathbf{Adv}_1 \leq \mathbf{Adv}_{\mathcal{B}}^{\mathsf{KerMDH}}$. This reasoning is *correct*, because (though not stated by the authors) $\mathcal{A}$'s view is equally distributed in both games and thus the probability that $\boldsymbol{M}^*$ does not fall in a class of a queried message (which is not efficiently verifiable) is the same.

In contrast, a similar argument cannot be made for the hop from Game 2 to Game 3. Here the distribution of the signatures output by the signing oracle changes and thus the probability that $\boldsymbol{M}^*$ falls in a queried class can change in arbitrary ways, but this is not efficiently detectable. In fact, the constructed reduction $\mathcal{B}_1$ (to their "core lemma", which relies on the computational hardness of *MDDH* [EHK+17]) only checks an (efficiently testable) property of $\mathcal{A}$'s forgery (but not whether $\mathcal{A}$ was successful). Since whether $\boldsymbol{M}^*$ falls in a queried class determines whether the adversary wins, one can therefore not deduce that $\mathbf{Adv}_2 - \mathbf{Adv}_3 \leq \mathbf{Adv}_{\mathcal{B}_1}^{\mathrm{core}}$, as the authors do. We detail our argument in Sect. 3.

The proof of the other CRS-based scheme [CLP22, eprint, Appendix D] is virtually identical and has thus the same issue. The security of both schemes is thus currently unclear.

2 Preliminaries

Notation. Assigning a value x to a variable var is denoted by $var := x$. All algorithms are randomized unless otherwise indicated. By $y \leftarrow \mathcal{A}(x_1, \ldots, x_n)$ we denote the operation of running algorithm $\mathcal{A}$ on inputs $x_1, \ldots, x_n$ and letting y denote the output; by $[\mathcal{A}(x_1, \ldots, x_n)]$ we denote the set of values that have positive probability of being output. If S is a finite set then $x \leftarrow\!\!\$\, S$ denotes picking an element uniformly from S and assigning it to x.

Bilinear groups. EQS schemes are defined over an (asymmetric) bilinear group $gr = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, G_1, G_2, e)$, where $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ are (additively denoted) groups of prime order p, G_1 and G_2 are generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, resp., and $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a bilinear map so that $G_T := e(G_1, G_2)$ generates $\mathbb{G}_T$. For $t \in \{1, 2, T\}$, we let $\mathbb{G}_t^* := \mathbb{G}_t \setminus \{0_t\}$. We assume that there exists a probabilistic polynomial-time (p.p.t.) algorithm BGGen, which on input 1^λ, the security parameter in unary, returns the description of a bilinear group gr so that the bit length of p is λ.

Following the examined work [KSD19], we use "implicit" representation of group elements: for $\mathbf{A} = (a_{i,j})_{i,j} \in \mathbb{Z}_p^{m\times n}$ and $t \in \{1, 2, T\}$, we let $[\mathbf{A}]_t$ denote the matrix $(a_{i,j}G_b)_{i,j} \in \mathbb{G}_t^{m\times n}$ and define $e([\mathbf{A}]_1, [\mathbf{B}]_2)$ as $[\mathbf{AB}]_T$, which can be computed efficiently. We use upper-case slanted font $G, \boldsymbol{G}$ to denote group elements and vectors of group elements and use $a, \mathbf{a}, \mathbf{A}$ to denote scalars, vectors and matrices of elements from $\mathbb{Z}_p$.

EQS. An *equivalence class signature (EQS) scheme* Σ specifies an algorithm $\mathsf{ParGen}(1^\lambda)$, which on input the security parameter returns general parameters par, which specify a bilinear group $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, G_1, G_2, e)$. $\mathsf{KeyGen}(par, 1^\ell)$, on input the parameters and the message length $\ell > 1$, returns a key pair (sk, pk), which defines the message space $\mathcal{M} := (\mathbb{G}_t^*)^\ell$ for a fixed $t \in \{1, 2\}$. The message space is partitioned into equivalence classes by the following relation for $\boldsymbol{M}, \boldsymbol{M}' \in \mathcal{M}$:

$$\boldsymbol{M} \sim \boldsymbol{M}' :\Leftrightarrow \exists\, \mu \in \mathbb{Z}_p^* : \boldsymbol{M}' = \mu \cdot \boldsymbol{M}. \tag{1}$$

A *tag-based* EQS scheme [KSD19] moreover consists of the following algorithms:

– $\mathsf{Sign}(sk, \boldsymbol{M})$, on input a secret key and a message $\boldsymbol{M} \in \mathcal{M}$, returns a signature σ and (possibly) a tag τ.
– $\mathsf{ChgRep}(pk, \boldsymbol{M}, (\sigma, \tau), \mu)$, on input a public key, a message $\boldsymbol{M} \in \mathcal{M}$, a signature σ (and possibly a tag τ) on $\boldsymbol{M}$, as well as a scalar $\mu \in \mathbb{Z}_p^*$, returns a signature σ' on the message $\mu \cdot \boldsymbol{M}$.
– $\mathsf{Verify}(pk, \boldsymbol{M}, (\sigma, \tau))$ is deterministic and, on input a public key, a message $\boldsymbol{M} \in \mathcal{M}$, a signature σ (and possibly a tag τ), returns a bit indicated acceptance.

Sign and ChgRep must generate valid signatures, as defined next.

Definition 1. *An EQS scheme is* correct *if for all* $\lambda \in \mathbb{N}$, $\ell > 1$, *any* $par \in [\mathsf{ParGen}(1^\lambda)]$, $(sk, pk) \in [\mathsf{KeyGen}(par, 1^\ell)]$, $\boldsymbol{M} \in \mathcal{M}$ *and* $\mu \in \mathbb{Z}_p^*$*:*

$$\Pr\left[\mathsf{Verify}\big(pk, \boldsymbol{M}, \mathsf{Sign}(sk, \boldsymbol{M})\big) = 1\right] = 1 \qquad \textit{and}$$
$$\Pr\left[\mathsf{Verify}\big(pk, \mu \cdot \boldsymbol{M}, \mathsf{ChgRep}(pk, \boldsymbol{M}, \mathsf{Sign}(sk, \boldsymbol{M}), \mu)\big) = 1\right] = 1.$$

Unforgeability requires that after receiving the public key and signatures (and tags) on messages of its choice, the adversary cannot produce a valid signature on a message that is not contained in any of the classes of the queried signatures.

Definition 2. *An EQS scheme* Σ *is* existentially unforgeable under chosen-message attack *if* $\mathsf{Adv}^{\mathrm{UNF}}_{\Sigma,\mathcal{A}}(\lambda) := \Pr[\mathrm{UNF}_{\Sigma,\mathcal{A}}(\lambda) = 1]$ *is negligible for all p.p.t. adversaries* $\mathcal{A}$*, where game* UNF *is defined as follows:*

$\mathrm{UNF}_{\Sigma,\mathcal{A}}(\lambda)$

```
par ← ParGen(1^λ)
(sk, pk) ← KeyGen()
Q := ∅
(M*, σ*) ← A^{O(·)}(pk)
return (M* ∉ Q ∧ Verify(pk, M*, σ*))
```

$\mathcal{O}(\boldsymbol{M})$

```
Q := Q ∪ [M]~
return Sign(sk, M)
```

where $[\boldsymbol{M}]_\sim := \{\boldsymbol{M'} \in \mathcal{M} \mid \boldsymbol{M} \sim \boldsymbol{M'}\}$ *is the equivalence class of* $\boldsymbol{M}$ *for* $\sim$ *defined in* (1)*.*

A further security requirement is that signatures generated by ChgRep should either be indistinguishable from signatures output by Sign or uniformly random in the space of all valid signatures. As these notions are not relevant for our result, we refrain from stating them and refer to the original work [FHS19].

3 A Flaw in the Security Proofs of KSD19 and CLP22

The proof of unforgeability [KSD19] defines Game 0 as the game UNF from Definition 2 instantiated with their construction as Σ, and, in a series of "hops", the games are gradually modified until Game 6 can only be won with probability $1/p$, even by an unbounded adversary. The difference between the adversary's advantage $\mathbf{Adv}_i$ in winning Game i and its advantage $\mathbf{Adv}_{i+1}$ in winning Game $(i+1)$ is then bounded. Of these bounds, two depend on the hardness of a computational problem.

Define event N_i as $\boldsymbol{M}^* \notin Q$ when running Game i (where $\boldsymbol{M}^*$ is from $\mathcal{A}$'s output and Q is the union of all classes of queried messages). Moreover, let V_i be the event that when running Game i, we have $\mathsf{Verify}_i(pk, \boldsymbol{M}^*, \sigma^*)$, where Verify_i is how verification of $\mathcal{A}$'s signature is defined in Game i. (The details of Verify_i are not relevant here.) We thus have $\mathbf{Adv}_i = \Pr[\mathrm{N}_i \wedge \mathrm{V}_i]$.

The first hop. In Game 0 and Game 1 the adversary's view remains the same, and we therefore have $\mathrm{N}_0 = \mathrm{N}_1$. The only thing that changes is that when verifying $\mathcal{A}$'s forgery, which contains group-element vectors $[\mathbf{u}_1^*]_1$ and $[\mathbf{t}^*]_1$, against $pk = ([\mathbf{A}]_2, [\mathbf{K}_0\mathbf{A}]_2, [\mathbf{K}\mathbf{A}]_2)$, instead of checking

$$e([\mathbf{u}_1^*]_1^\top, [\mathbf{A}]_2) - e([\mathbf{t}^*]_1^\top, [\mathbf{K}_0\mathbf{A}]_2) - e([\mathbf{m}^*]_1^\top, [\mathbf{K}\mathbf{A}]_2) = 0,$$

one checks if $\boldsymbol{S} := [\mathbf{u}_1^*]_1 - \mathbf{K}_0^\top[\mathbf{t}^*]_1 - \mathbf{K}^\top[\mathbf{m}^*]_1 = 0$.

We thus have $\mathrm{V}_1 \subseteq \mathrm{V}_0$ and if V_0 occurs but V_1 does not, then $\mathcal{A}$ has found a non-zero vector $\boldsymbol{S}$ in the kernel of $\mathbf{A}$. The authors construct a reduction $\mathcal{B}$ which uses this to break KerMDH [MRV16] in $\mathbb{G}_2$. We have

$$\begin{aligned}
\mathbf{Adv}_0 - \mathbf{Adv}_1 &= \Pr[\mathrm{N}_0 \wedge \mathrm{V}_0] - \Pr[\mathrm{N}_1 \wedge \mathrm{V}_1] \\
&= \Pr[\mathrm{N}_0 \wedge \mathrm{V}_0 \wedge \mathrm{V}_1] + \Pr[\mathrm{N}_0 \wedge \mathrm{V}_0 \wedge \neg\mathrm{V}_1] \\
&\qquad\qquad - \Pr[\mathrm{N}_1 \wedge \mathrm{V}_1 \wedge \mathrm{V}_0] - \Pr[\mathrm{N}_1 \wedge \mathrm{V}_1 \wedge \neg\mathrm{V}_0] \\
&= \Pr[\mathrm{N}_0 \wedge \mathrm{V}_0 \wedge \neg\mathrm{V}_1] \quad (\text{since } \mathrm{N}_0 = \mathrm{N}_1 \text{ and } \mathrm{V}_1 \subseteq \mathrm{V}_0) \\
&\leq \Pr[\mathrm{V}_0 \wedge \neg\mathrm{V}_1] \leq \mathbf{Adv}_{\mathcal{B}}^{\mathsf{KerMDH}}.
\end{aligned}$$

Note that for this argument it was essential that N_0, N_1, V_0 and V_1 are all events in the same probability space (which will not be the case in the hop from Game 2 to Game 3).

The bad hop. In the hop from Game 2 to Game 3, the distribution of the game changes and thus we do not have $\mathrm{N}_2 = \mathrm{N}_3$ (which is also syntactically meaningless). The authors construct a reduction $\mathcal{B}_1$ which bounds $\Pr[\mathrm{V}_2] - \Pr[\mathrm{V}_3] \leq \mathbf{Adv}_{\mathcal{B}_1}^{\mathrm{core}}$, where the latter is $\mathcal{B}_1$'s probability in winning the game from their "core lemma" [KSD19, Sect. 4.1], which is bounded by breaking another computational problem (Matrix-DDH [EHK+17]). However, it is not clear how to use this to bound the change in advantage from Game 2 to Game 3. We have

$$\begin{aligned}
\mathbf{Adv}_2 - \mathbf{Adv}_3 &= \Pr[\mathrm{N}_2 \wedge \mathrm{V}_2] - \Pr[\mathrm{N}_3 \wedge \mathrm{V}_3] \\
&= \Pr[\mathrm{N}_2 \mid \mathrm{V}_2] \cdot \big(\underbrace{\Pr[\mathrm{V}_2] - \Pr[\mathrm{V}_3]}_{(1)}\big) + \big(\underbrace{\Pr[\mathrm{N}_2 \mid \mathrm{V}_2] - \Pr[\mathrm{N}_3 \mid \mathrm{V}_3]}_{(2)}\big) \cdot \Pr[\mathrm{V}_3].
\end{aligned}$$

So while we can bound (1) by $\mathcal{B}_1$'s advantage of breaking the "core lemma", it is unclear how to bound (2). In particular, N_i is an event that cannot be efficiently checked, and moreover, in contrast to N_0 and N_1, the events N_2 and N_3 are not equivalent, since the adversary's view is different on Game 2 and Game 3.

To show this, we spell out Game i for $i = 2, 3$ in Figure 1, where Verify_i denotes how verification is defined in Game i (both Verify_2 and Verify_3 are efficient, but their details not relevant here). Moreover, $\mathcal{D}_1$ is a distribution of matrices from $\mathbb{Z}_p^{2\times 1}$ for which the MDDH assumption must hold; PGen and PPro belong to a proof system for statements $([\mathbf{t}]_1, [\mathbf{w}]_1)$ which are true if $[\mathbf{t}]_1 = [\mathbf{A}_b]_1 r_1$ and $[\mathbf{w}]_1 = [\mathbf{A}_b]_1 r_2$ for some $b \in \{0, 1\}$ and $r_1, r_2 \in \mathbb{Z}_p$ (again, the details are not relevant here); and $\mathbf{F}\colon \mathbb{Z}_p \to \mathbb{Z}_p^2$ is a random function.

Game $(2+\beta)$

$gr \leftarrow \mathsf{BGGen}(1^\lambda)$; $\color{blue}{ctr := 0}$

$\mathbf{A}_0 \leftarrow\!\!\$\ \mathcal{D}_1$; $\mathbf{A}_1 \leftarrow\!\!\$\ \mathcal{D}_1$

$crs \leftarrow \mathsf{PGen}(gr, [\mathbf{A}_0]_1, [\mathbf{A}_1]_1)$

$par := (gr, [\mathbf{A}_0]_1, [\mathbf{A}_1]_1, crs)$

$\mathbf{A} \leftarrow\!\!\$\ \mathcal{D}_1$

$\mathbf{K}_0 \leftarrow\!\!\$\ \mathbb{Z}_p^{2\times 2}$; $\mathbf{K} \leftarrow\!\!\$\ \mathbb{Z}_p^{\ell\times 2}$

$\color{red}{\mathbf{a}^\perp \leftarrow\!\!\$\ \{\mathbf{a}^\perp \in \mathbb{Z}_p^2 \mid (\mathbf{a}^\perp)^\top \mathbf{A} = 0\}}$

$\mathbf{k}_0 \leftarrow\!\!\$\ \mathbb{Z}_p^2$; $\color{blue}{\mathbf{k}_1 \leftarrow\!\!\$\ \mathbb{Z}_p^2}$

$\color{gray}{\mathbf{K}_0 := \mathbf{K}_0 + \mathbf{k}_0(\mathbf{a}^\perp)^\top}$

$pk := ([\mathbf{A}]_2, [\mathbf{K}_0\mathbf{A}]_2, [\mathbf{K}\mathbf{A}]_2)$

$Q := \emptyset$

$([\mathbf{m}^*]_1, \sigma^*) \leftarrow \mathcal{A}^{\mathcal{O}(\cdot)}(par, pk)$

$\texttt{return } \big([\mathbf{m}^*]_1 \notin Q$

$\quad \wedge \color{gray}{\mathsf{Verify}_i}(pk, [\mathbf{m}^*]_1, \sigma^*)\big)$

$\mathcal{O}([\mathbf{m}]_1)$

$Q := Q \cup [[\mathbf{m}]_1]_\sim$

$r_1, r_2 \leftarrow\!\!\$\ \mathbb{Z}_p$

$[\mathbf{t}]_1 := [\mathbf{A}_0]_1 r_1$; $[\mathbf{w}]_1 := [\mathbf{A}_0]_1 r_2$

$\Omega \leftarrow \mathsf{PPro}(crs, [\mathbf{t}]_1, r_1, [\mathbf{w}]_1, r_2)$

$(\Omega_1, \Omega_2, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi) := \Omega$

$\color{blue}{ctr := ctr + 1}$

$[\mathbf{u}_1]_1 := \mathbf{K}_0^\top [\mathbf{t}]_1 + \mathbf{K}^\top [\mathbf{m}]_1$
$\quad \color{gray}{+ \mathbf{a}^\perp \big(\mathbf{k}_0} \color{blue}{+ \beta \cdot \mathbf{F}(ctr)}\color{gray}{\big)^\top [\mathbf{t}]_1}$

$[\mathbf{u}_2]_1 := \mathbf{K}_0^\top [\mathbf{w}]_1$
$\quad \color{gray}{+ \mathbf{a}^\perp \big(\mathbf{k}_0} \color{blue}{+ \beta \cdot \mathbf{k}_1}\color{gray}{\big)^\top [\mathbf{w}]_1}$

$\sigma := ([\mathbf{u}_1]_1, \Omega_1, [\mathbf{z}_0]_2, [\mathbf{z}_1]_2, \pi, [\mathbf{t}]_1)$

$\tau := ([\mathbf{u}_2]_1, \Omega_2, [\mathbf{w}]_1)$

$\texttt{return } (\sigma, \tau)$

Fig. 1. Games 2 and 3 in the unforgeability proof of [KSD19]. Changes w.r.t. game UNF are denoted in gray, the differences between Games 2 and 3 are highlighted in blue. The line in red is our interpretation, since the distribution of $\mathbf{a}^\perp$ is not specified.

To argue that $\mathcal{A}$'s view changes from Game 2 to Game 3, an easy way is to have $\mathcal{A}$ query the signing oracle $\mathcal{O}$ twice on the same (arbitrary) message. For the i-th query, let $r_1^{(i)}$ and $r_2^{(i)}$ be the randomness sampled by $\mathcal{O}$ and let $\mathbf{u}_1^{(i)}, \mathbf{t}^{(i)}, \mathbf{u}_2^{(i)}, \mathbf{w}^{(i)} \in \mathbb{Z}_p^2$ be the logarithms of the respective components returned by $\mathcal{O}$.

Since $\mathbf{A}_0 \in \mathbb{Z}_p^{2\times 1}$ is from a "matrix distribution" [KSD19, Definition 1], it has full rank and is thus non-zero. The value $\mathbf{t}^{(i)} = \mathbf{A}_0 r_1^{(i)}$ thus uniquely determines $r_1^{(i)}$ and $\mathbf{w}^{(i)} = \mathbf{A}_0 r_2^{(i)}$ uniquely determines $r_2^{(i)}$. Let $r_1' := r_1^{(1)} - r_1^{(2)}$ and $r_2' := r_2^{(1)} - r_2^{(2)}$, and thus $\mathbf{t}^{(1)} - \mathbf{t}^{(2)} = \mathbf{A}_0 r_1'$ and $\mathbf{w}^{(1)} - \mathbf{w}^{(2)} = \mathbf{A}_0 r_2'$, and consider these further differences:

$$\mathbf{u}_1' := \mathbf{u}_1^{(1)} - \mathbf{u}_1^{(2)} = \mathbf{K}_0^\top \mathbf{A}_0 r_1' + \mathbf{a}^\perp \mathbf{k}_0^\top \mathbf{A}_0 r_1' + \beta \cdot \mathbf{a}^\perp \big(\mathbf{F}(1)^\top \mathbf{A}_0 r_1^{(1)} - \mathbf{F}(2)^\top \mathbf{A}_0 r_1^{(2)}\big)$$
$$\mathbf{u}_2' := \mathbf{u}_2^{(1)} - \mathbf{u}_2^{(2)} = \mathbf{K}_0^\top \mathbf{A}_0 r_2' + \mathbf{a}^\perp \mathbf{k}_0^\top \mathbf{A}_0 r_2' + \beta \cdot \mathbf{a}^\perp \mathbf{k}_1^\top \mathbf{A}_0 r_2'$$

In Game 2, where $\beta = 0$, we thus have

$$\mathbf{u}_1' r_2' = \mathbf{u}_2' r_1'. \tag{2}$$

On the other hand, for (2) to hold in Game 3, we would have to have

$$\mathbf{a}^\perp \big(\mathbf{F}(1)^\top \mathbf{A}_0 r_1^{(1)} - \mathbf{F}(2)^\top \mathbf{A}_0 r_1^{(2)}\big) r_2' = \mathbf{a}^\perp \mathbf{k}_1^\top \mathbf{A}_0 r_2' (r_1^{(1)} - r_1^{(2)}),$$

or equivalently

$$\mathbf{a}^{\perp}\big(\underbrace{\mathbf{F}(1)^{\top}r_1^{(1)} - \mathbf{F}(2)^{\top}r_1^{(2)} - \mathbf{k}_1^{\top}(r_1^{(1)} - r_1^{(2)})}_{=:\mathbf{U}^{\top}}\big)\mathbf{A}_0 r_2' = \mathbf{0}. \tag{3}$$

Since $\mathbf{F}(1)$ is independent and uniformly distributed in $\mathbb{Z}_p^2$, the term $\mathbf{U}$ is uniform in $\mathbb{Z}_p^2$, except with negligible probability (when $r_1^{(1)} = 0$). As argued above, $\mathbf{A}_0$ is non-zero and thus $\mathbf{U}^{\top}\mathbf{A}_0$ is uniform in $\mathbb{Z}_p$ (except with negligible probability). The authors [GHKP18, KSD19] do not specify how $\mathbf{a}^{\perp}$ is distributed, but for their last argument in the proof to work, namely that Game 6 can only be won with probability $1/p$ (or with negligible probability), we must have $\mathbf{a}^{\perp} \neq \mathbf{0}$ (with overwhelming probability). Thus for (3) (and thus (2)) to hold, we must either have $\mathbf{a}^{\perp} = \mathbf{0}$ or $\mathbf{U}^{\top}\mathbf{A}_0 = 0$ or $r_2' = 0$, which happens with negligible probability only.

Thus, the view of the adversary changes between Games 2 and 3, and therefore so can its probability of returning a messages that is in the class of a queried message, i.e., we can have that $\Pr[\mathrm{N}_2]$ and $\Pr[\mathrm{N}_3]$ differ by a non-negligible amount. The argument which worked for bounding $\mathbf{Adv}_0 - \mathbf{Adv}_1$ (a reduction that only considers the events V_0 and V_1), and which the authors also apply to bound $\mathbf{Adv}_2 - \mathbf{Adv}_3$, can thus not be made again.

Acknowledgments. This work was funded by the Vienna Science and Technology Fund (WWTF) [10.47379/VRG18002] and by the Austrian Science Fund (FWF) [10.55776/F8515-N].

References

[AFG+10] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 209–236. Springer, 2010.

[BCC+09] Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Hovav Shacham. Randomizable proofs and delegatable anonymous credentials. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 108–125. Springer, 2009.

[BEK+20] Jan Bobolz, Fabian Eidens, Stephan Krenn, Daniel Slamanig, and Christoph Striecks. Privacy-preserving incentive systems with highly efficient point-collection. In Hung-Min Sun, Shiuh-Pyng Shieh, Guofei Gu, and Giuseppe Ateniese, editors, *ASIACCS 20*, pages 319–333. ACM Press, 2020.

[BFPV13] Olivier Blazy, Georg Fuchsbauer, David Pointcheval, and Damien Vergnaud. Short blind signatures. *J. Comput. Secur.*, 21(5):627–661, 2013.

[BHKS18] Michael Backes, Lucjan Hanzlik, Kamil Kluczniak, and Jonas Schneider. Signatures with flexible public key: Introducing equivalence classes for public keys. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 405–434. Springer, 2018.

[BLL$^+$19] Xavier Bultel, Pascal Lafourcade, Russell W. F. Lai, Giulio Malavolta, Dominique Schröder, and Sri Aravinda Krishnan Thyagarajan. Efficient invisible and unlinkable sanitizable signatures. In Dongdai Lin and Kazue Sako, editors, *PKC 2019, Part I*, volume 11442 of *LNCS*, pages 159–189. Springer, 2019.

[BRS23] Fabrice Benhamouda, Mariana Raykova, and Karn Seth. Anonymous counting tokens. Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part II*, volume 14439 of *LNCS*, pages 245–278. Springer, 2023.

[CH20] Geoffroy Couteau and Dominik Hartmann. Shorter non-interactive zero-knowledge arguments and ZAPs for algebraic languages. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part III*, volume 12172 of *LNCS*, pages 768–798. Springer, 2020.

[CL03] Jan Camenisch and Anna Lysyanskaya. A signature scheme with efficient protocols. In Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, editors, *SCN 02*, volume 2576 of *LNCS*, pages 268–289. Springer, 2003.

[CL19] Elizabeth C. Crites and Anna Lysyanskaya. Delegatable anonymous credentials from mercurial signatures. In Mitsuru Matsui, editor, *CT-RSA 2019*, volume 11405 of *LNCS*, pages 535–555. Springer, 2019.

[CL21] Elizabeth C. Crites and Anna Lysyanskaya. Mercurial signatures for variable-length messages. *PoPETs*, 2021(4):441–463, 2021.

[CLP22] Aisling Connolly, Pascal Lafourcade, and Octavio Perez-Kempner. Improved constructions of anonymous credentials from structure-preserving signatures on equivalence classes. In Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe, editors, *PKC 2022, Part I*, volume 13177 of *LNCS*, pages 409–438. Springer, 2022.

[CS20] Remi Clarisse and Olivier Sanders. Group signature without random oracles from randomizable signatures. In Khoa Nguyen, Wenling Wu, Kwok-Yan Lam, and Huaxiong Wang, editors, *ProvSec 2020*, volume 12505 of *LNCS*, pages 3–23. Springer, 2020.

[DHS15] David Derler, Christian Hanser, and Daniel Slamanig. A new approach to efficient revocable attribute-based anonymous credentials. In Jens Groth, editor, *15th IMA International Conference on Cryptography and Coding*, volume 9496 of *LNCS*, pages 57–74. Springer, 2015.

[DS16] David Derler and Daniel Slamanig. Fully-anonymous short dynamic group signatures without encryption. Cryptology ePrint Archive, Report 2016/154, 2016. https://eprint.iacr.org/2016/154.

[DS18] David Derler and Daniel Slamanig. Highly-efficient fully-anonymous dynamic group signatures. In Jong Kim, Gail-Joon Ahn, Seungjoo Kim, Yongdae Kim, Javier López, and Taesoo Kim, editors, *ASIACCS 18*, pages 551–565. ACM Press, April 2018.

[EHK$^+$13] Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Villar. An algebraic framework for Diffie-Hellman assumptions. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147. Springer, 2013.

[EHK$^+$17] Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Luis Villar. An algebraic framework for Diffie-Hellman assumptions. *Journal of Cryptology*, 30(1):242–288, January 2017.

[FG18] Georg Fuchsbauer and Romain Gay. Weakly secure equivalence-class signatures from standard assumptions. In Michel Abdalla and Ricardo Dahab, editors, *PKC 2018, Part II*, volume 10770 of *LNCS*, pages 153–183. Springer, 2018.

[FGKO17] Georg Fuchsbauer, Romain Gay, Lucas Kowalczyk, and Claudio Orlandi. Access control encryption for equality, comparison, and more. In Serge Fehr, editor, *PKC 2017, Part II*, volume 10175 of *LNCS*, pages 88–118. Springer, 2017.

[FHKS16] Georg Fuchsbauer, Christian Hanser, Chethan Kamath, and Daniel Slamanig. Practical round-optimal blind signatures in the standard model from weaker assumptions. In Vassilis Zikas and Roberto De Prisco, editors, *SCN 16*, volume 9841 of *LNCS*, pages 391–408. Springer, 2016.

[FHS15] Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig. Practical round-optimal blind signatures in the standard model. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 233–253. Springer, 2015.

[FHS19] Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig. Structure-preserving signatures on equivalence classes and constant-size anonymous credentials. *Journal of Cryptology*, 32(2):498–546, April 2019.

[FP09] Georg Fuchsbauer and David Pointcheval. Proofs on encrypted values in bilinear groups and an application to anonymity of signatures. In Hovav Shacham and Brent Waters, editors, *PAIRING 2009*, volume 5671 of *LNCS*, pages 132–149. Springer, 2009.

[Fuc11] Georg Fuchsbauer. Commuting signatures and verifiable encryption. In Kenneth G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 224–245. Springer, 2011.

[Fuc14] Georg Fuchsbauer. Breaking existential unforgeability of a signature scheme from asiacrypt 2014. Cryptology ePrint Archive, Report 2014/892, 2014. https://eprint.iacr.org/2014/892.

[GHKP18] Romain Gay, Dennis Hofheinz, Lisa Kohl, and Jiaxin Pan. More efficient (almost) tightly secure structure-preserving signatures. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part II*, volume 10821 of *LNCS*, pages 230–258. Springer, 2018.

[Han23] Lucjan Hanzlik. Non-interactive blind signatures for random messages. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part V*, volume 14008 of *LNCS*, pages 722–752. Springer, 2023.

[HPP20] Chloé Hébant, Duong Hieu Phan, and David Pointcheval. Linearly-homomorphic signatures and scalable mix-nets. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020, Part II*, volume 12111 of *LNCS*, pages 597–627. Springer, 2020.

[HRS15] Christian Hanser, Max Rabkin, and Dominique Schröder. Verifiably encrypted signatures: Security revisited and a new construction. In Günther Pernul, Peter Y. A. Ryan, and Edgar R. Weippl, editors, *ESORICS 2015, Part I*, volume 9326 of *LNCS*, pages 146–164. Springer, 2015.

[HS14] Christian Hanser and Daniel Slamanig. Structure-preserving signatures on equivalence classes and their application to anonymous credentials. In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Part I*, volume 8873 of *LNCS*, pages 491–511. Springer, 2014.

[HS21] Lucjan Hanzlik and Daniel Slamanig. With a little help from my friends: Constructing practical anonymous credentials. In Giovanni Vigna and Elaine Shi, editors, *ACM CCS 2021*, pages 2004–2023. ACM Press, November 2021.

[KSD19] Mojtaba Khalili, Daniel Slamanig, and Mohammad Dakhilalian. Structure-preserving signatures on equivalence classes from standard assumptions. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 63–93. Springer, 2019.

[Mau05] Ueli M. Maurer. Abstract models of computation in cryptography (invited paper). In Nigel P. Smart, editor, *10th IMA International Conference on Cryptography and Coding*, volume 3796 of *LNCS*, pages 1–12. Springer, 2005.

[MBG+23] Omid Mir, Balthazar Bauer, Scott Griffy, Anna Lysyanskaya, and Daniel Slamanig. Aggregate signatures with versatile randomization and issuer-hiding multi-authority anonymous credentials. In Weizhi Meng, Christian Damsgaard Jensen, Cas Cremers, and Engin Kirda, editors, *ACM CCS 2023*, pages 30–44. ACM, 2023.

[MRV16] Paz Morillo, Carla Ràfols, and Jorge Luis Villar. The kernel matrix Diffie-Hellman assumption. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 729–758. Springer, 2016.

[MSBM23] Omid Mir, Daniel Slamanig, Balthazar Bauer, and René Mayrhofer. Practical delegatable anonymous credentials from equivalence class signatures. *Proc. Priv. Enhancing Technol.*, 2023(3):488–513, 2023.

[Nao03] Moni Naor. On cryptographic assumptions and challenges (invited talk). In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 96–109. Springer, 2003.

[Nec94] V. I. Nechaev. Complexity of a determinate algorithm for the discrete logarithm. *Mathematical Notes*, 55(2):165–172, 1994.

[Sho97] Victor Shoup. Lower bounds for discrete logarithms and related problems. In Walter Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 256–266. Springer, 1997.