On Proving Equivalence Class Signatures Secure from Non-interactive Assumptions

Balthazar Bauer[1(✉)], Georg Fuchsbauer[2], and Fabian Regen[2]

[1] UVSQ, Versailles, France
balthazar.bauer@ens.fr
[2] TU Wien, Vienna, Austria
{georg.fuchsbauer,fabian.regen}@tuwien.ac.at

Abstract. Equivalence class signatures (EQS), introduced by Hanser and Slamanig (AC'14, J. Crypto'19), sign vectors of elements from a bilinear group. Their main feature is "adaptivity": given a signature on a vector, anyone can transform it to a (uniformly random) signature on any multiple of the vector. A signature thus authenticates equivalence classes and unforgeability is defined accordingly. EQS have been used to improve the efficiency of many cryptographic applications, notably (delegatable) anonymous credentials, (round-optimal) blind signatures, group signatures and anonymous tokens. EQS security implies strong anonymity (or blindness) guarantees for these schemes which holds against malicious signers without trust assumptions.

Unforgeability of the original EQS construction is proven directly in the generic group model. While there are constructions from standard assumptions, these either achieve prohibitively weak security notions (PKC'18) or they require a common reference string (AC'19, PKC'22), which reintroduces trust assumptions avoided by EQS.

In this work we ask whether EQS schemes that satisfy the original security model can be proved secure under standard (or even non-interactive) assumptions with standard techniques. Our answer is negative: assuming a reduction that, after running once an adversary breaking unforgeability, breaks a non-interactive computational assumption, we construct efficient meta-reductions that either break the assumption or break class-hiding, another security requirement for EQS.

1 Introduction

Structure-preserving signatures (SPS) [AFG+10] are defined over groups of prime order p equipped with a bilinear map (pairing), and their messages are group elements. *SPS on equivalence classes*, or equivalence class signatures (EQS) for short, introduced by Hanser and Slamanig [HS14] and later refined [FHS19], sign vectors of (non-zero) group elements, that is, messages are from $M = (\mathbb{G}^*)^\ell$ for a group $\mathbb{G}$ (where $\ell = 2$ suffices for most applications). Compared to standard signature schemes, EQS provide an additional functionality Adapt: given the public key, a signature σ on $m \in M$ and $\mu \in \mathbb{Z}_p^*$, Adapt returns, without requiring the signing key, a signature on the message $\mu \cdot m$. Signing $m \in M$ thus

Q. Tang and V. Teague (Eds.): PKC 2024, LNCS 14601, pp. 3–36, 2024.
https://doi.org/10.1007/978-3-031-57718-5_1

authenticates the equivalence class $[m]_\sim$, where $m \sim m' :\Leftrightarrow \exists\, \mu \in \mathbb{Z}_p^* : m' = \mu \cdot m$. Unforgeability means that after querying signatures on (polynomially many) messages $m_1, m_2, \ldots$, no adversary can compute a signature for any m^* with $m^* \notin [m_1] \cup [m_2] \cup \ldots$

A second security notion is *class-hiding*, meaning that it is hard to distinguish a random message pair (m, m') from the same class (i.e., $m \sim m'$) from a random pair $(m, m') \leftarrow\!\$\, M \times M$. Note that this is equivalent to the hardness of the decisional Diffie-Hellman (DDH) problem in $\mathbb{G}$. The third property is *signature adaptation* (under malicious keys): it states that, even if a public key pk was set up maliciously, when running $\sigma' \leftarrow \mathsf{Adapt}(pk, m, \sigma, \mu)$ for a σ valid on m, then σ' is uniformly random in the set of all valid signatures on $\mu \cdot m$.

Together with class-hiding, this yields the following guarantee against malicious signers, which lies at the core of applications of EQS: after issuing a signature σ on a message m, when later given $\mu \cdot m$ and $\sigma' \leftarrow \mathsf{Adapt}(pk, m, \sigma, \mu)$ for $\mu \leftarrow\!\$\, \mathbb{Z}_p^*$, the signer cannot distinguish $(\sigma', \mu \cdot m)$ from a *random* signature on a *random* message $m' \leftarrow\!\$\, M$ valid under pk.

The original work [FHS19] gives a very efficient construction of EQS with signatures consisting of 2 elements from $\mathbb{G}$ and 1 from $\hat{\mathbb{G}}$ (the other source group of the asymmetric pairing). Unforgeability is proved directly in the generic group model [Nec94, Sho97, Mau05].

Applications of EQS. Since their introduction, equivalence class signatures have been used to instantiate numerous cryptographic concepts.

Anonymous Credentials. The first application of EQS were attribute-based credentials (ABC) [CL03]. In an ABC scheme, users are issued credentials for a set of attributes they possess. Users can then selectively disclose attributes, that is, *show* that they possess any subset of their attributes. Anonymity requires that no one can tell whether two showings were done by the same user and that they reveal nothing about the non-disclosed attributes.

To showcase the power of EQS, the authors [FHS19] use it to construct the first ABC scheme for which the communication complexity of showing a credential is independent of the number of (possessed or showed) attributes. In their scheme, a credential is an EQS signature σ on a (randomizable) commitment $c \in M$ to the user's attributes; when a user wants to prove she owns certain attributes, she adapts σ for $\mu \cdot c$ for $\mu \leftarrow\!\$\, \mathbb{Z}_p^*$ and opens the commitment $\mu \cdot c$ to the disclosed attributes. Anonymity (even against malicious credential issuers) follows from the adaptivity properties of EQS. Note that this construction avoids using zero-knowledge proofs to hide signatures, which are a source of inefficiency in many prior constructions. (Interactive proofs could still be required to prevent replay attacks.[1]) Slamanig and others added the possibility of revoking users to

[1] Note that the following simple pseudonym system from EQS would not use any ZK proofs during showing. A user creates $pk = sk \cdot g$, with party i she establishes pseudonym $(r_i \cdot g, r_i \cdot pk)$ for random r_i, and she transforms (via Adapt) signatures (credentials) on one pseudonym to another. ZK proofs (of DL-knowledge) would only be needed when establishing a new pseudonym.

the credential scheme [DHS15] and construct credentials that allow outsourcing of sensitive computation to a restricted device [HS21].

EQS were generalized by considering adaptivity within equivalence classes not only for messages but also for keys, termed "signatures with flexible public key" [BHKS18] or "mercurial signatures" [CL19, CL21, CLPK22]. Mercurial signatures were used to construct *delegatable* anonymous credentials [BCC+09] with non-interactive delegation [Fuc11]. New credentials constructions from EQS are still being proposed [MSBM23, MBG+23].

Group Signatures. EQS were used to construct efficient group signatures [DS16, CS20], in particular supporting dynamic adding of members [DS18]. Group signatures, as well as ring signatures, have also been constructed from the generalization of EQS to adaptable public keys [BHKS18].

Blind Signatures. Another line of research uses EQS to construct blind signatures, which let a user obtain a signature on a message that remains hidden from the signer. This builds on earlier work [BFPV13], which use randomizable zero-knowledge proofs [FP09] and thus require a trusted common reference string (CRS). In contrast, the EQS-based schemes [FHS15, FHKS16] do not assume common reference strings or random oracles and achieve blindness against malicious signers, leveraging the adaptivity property of EQS. Moreover, the schemes are round-optimal [Fis06], meaning the signing protocol consists of one message from the user to the signer and one message back; such schemes are thus *concurrently secure* [HKKL07] by default. Hanzlik [Han23] went further and uses the FHS EQS scheme to construct *non-interactive* blind signatures on random messages.

Other Cryptographic Primitives. EQS also yield [HRS15] verifiably encrypted signatures. *Access-control encryption* [DHO16] was efficiently instantiated using EQS [FGKO17], as well as [BLL+19] *sanitizable signatures* [ACdMT05] and privacy-preserving incentive systems from EQS [BEK+20]. The FHS scheme [FHS19] was used [HPP20] to instantiate highly scalable mix nets and [ST21] the anonymous authentication protocol *EPID*. It was also used for the most efficient instantiation of *anonymous counting tokens* [BRS23].

Constructions from Standard Assumptions. Despite applications of EQS requiring neither CRS nor random oracles, the first instantiation of EQS [FHS19] only has a proof in the generic group model (GGM). Therefore, calling constructions using that scheme "standard-model" has attracted some criticism [KM19]. This motivated the search for constructions from *falsifiable* [Nao03] assumptions, that is, assumptions where the challenger that sets up the problem instance can efficiently decide whether an adversary has broken the assumption. The assumption that a given EQS satisfies unforgeability is for example *not* falsifiable, since, by the class-hiding property, deciding whether the adversary's message lies in one of the queried classes is hard.

The first EQS from falsifiable assumptions was proposed by Fuchsbauer and Gay [FG18], based on Matrix-Diffie-Hellman assumptions [EHK+13]. However, its signatures can only be adapted once (after which they change format) and

the scheme only satisfies a weakened security notion: when querying a signature, the unforgeability adversary must provide the discrete logarithms of the queried messages. Note that this unforgeability notion *is* efficiently decidable.[2]

Unfortunately, the notion of *signature adaption* that the scheme achieves assumes honest keys and honest signatures, which excludes all applications except to access control encryption, as later argued [KSD19].

Motivated by this, Khalili, Slamanig and Dakhilalian [KSD19] propose an EQS construction from the SXDH assumption (i.e., DDH is hard in $\mathbb{G}$ and $\hat{\mathbb{G}}$) with signatures in $\mathbb{G}^8 \times \hat{\mathbb{G}}^9$. Building on this work, Connolly, Lafourcade and Perez-Kempner [CLPK22] propose a more efficient scheme (with signatures in $\mathbb{G}^9 \times \hat{\mathbb{G}}^4$), which requires an additional assumption (extKerMDH). A drawback of both schemes is that they assume a trusted CRS to achieve signature adaption under malicious keys. Sadly, this foils the main security benefit of EQS-based constructions: anonymity guarantees (against blind signers or credential issuers, etc.) without any trust assumptions in the standard model. We note that for schemes with a uniform CRS (of group elements) the CRS could be generated "transparently" by hashing (into the group). Formally, one would then need to prove adaptation security in the ROM.

A recent work [BFR24] points out a flaw in the security proofs of the CRS-based schemes [KSD19, CLPK22] and thus their security is currently unclear. (A game hop in the unforgeability proofs modifies the adversary's view and the change in its advantage is then bounded by the advantage of a reduction in solving a computational problem. But since EQS-unforgeability is not efficiently decidable, the reduction would not be efficient.[3])

The current state of affairs remains thus that the only scheme enabling trustless applications is FHS [FHS19], and it is only proven secure in the GGM. This poses two independent questions: can we prove stronger security guarantees for FHS; and do there exist more efficient schemes? Since any EQS scheme can be transformed into a structure-preserving signature (SPS) scheme without changing the signature format [FHS15], known impossibility results for SPS imply the following: First, the signature size of FHS is optimal, since 3 group elements per signature are necessary [AGHO11]. Second, FHS cannot be proven secure from a non-interactive assumption via an *algebraic* reduction, since this is the case for all 3-element schemes [AGO11].

[2] Consider $\ell = 2$. For all i, let $(x_{i,1}, x_{i,2}) \in (\mathbb{Z}_p^*)^2$ be the logarithms of the components of the queried message m_i (i.e., $m_{i,j} = x_{i,j} \cdot g$, where $\mathbb{G} = \langle g \rangle$). When the adversary returns a signature on $m^* = (m_1^*, m_2^*)$, it wins if $x_{i,2} \cdot m_1^* \neq x_{i,1} \cdot m_2^*$ for all i.

[3] In the hop from Game 2 to Game 3 [KSD19, Theorem 2], the distribution of the signatures output by the signing oracle is modified and thus $\mathcal{A}$'s advantage of breaking unforgeability could also change, without being efficiently detectable. However, the constructed reduction $\mathcal{B}_1$ (to the "core lemma", which relies on the computational hardness of Matrix-DDH [EHK+17]) only checks an (efficiently testable) property of $\mathcal{A}$'s forgery but not whether $\mathcal{A}$ was successful. The implication $\mathbf{Adv}_2 - \mathbf{Adv}_3 \leq \mathbf{Adv}^{\text{core}}_{\mathcal{B}_1}$ derived by the authors is thus not justified. As the proof of the second work [CLPK22, eprint, Appendix D] is virtually identical, the above applies as well.

Since the second result only applies to 3-element schemes, the question that has been open for a decade remains: do there exist (less efficient) instantiations of EQS with a security proof from a non-interactive assumption at all? We answer this in the negative for black-box reductions that run the unforgeability adversary once.

Impossibility Results. To prove our result, we use the meta-reduction technique: one assumes that a reduction $\mathcal{R}$ (with certain properties, such as being algebraic or being tight) exists; that is, when given access to an adversary that breaks the scheme, $\mathcal{R}$ can efficiently solve a (conjectured-to-be-hard) computational problem. One then derives a contradiction by showing how to use $\mathcal{R}$ to break a computational assumption. Building on earlier work [BV98], Coron [Cor02] first used this technique to show that there is no tight security proof for the RSA full-domain hash signature scheme. (A reduction has tightness ϕ if it can use an adversary breaking the scheme with probability ϵ to break the underlying assumption with probability at least $\phi \cdot \epsilon$). His result was later revisited by Kakvi and Kiltz [KK12].

Hofheinz, Jager and Knapp [HJK12] extended Coron's ideas to Waters signatures [Wat05] and, more generally, any *re-randomizable* signature scheme. These schemes let anyone transform a signature on a message into a random signature on that message. They show that a reduction can have tightness at most $\phi = 1/\Omega(q)$, where q is the number of signing queries, as follows. Assume there exists a reduction $\mathcal{R}$, which must thus break the computational assumption using the following (inefficient) adversary: $\mathcal{A}$ makes queries on random messages and then returns a random signature on a random message m^*. The authors construct a(n efficient) meta-reduction $\mathcal{M}$ that simulates $\mathcal{A}$: to obtain the signature on m^*, $\mathcal{M}$ *rewinds* $\mathcal{R}$, that is, it runs $\mathcal{R}$ again on the same randomness; $\mathcal{M}$ then queries a signature on m^*, randomizes it and returns it as the forgery in the first run (re-randomizability is thus crucial for the simulation of the adversary).

If the hardness assumption holds, then it must be the case that either $\mathcal{R}$ cannot provide a signature on m^*, or $\mathcal{R}$ cannot use the randomized signature to break the assumption. Intuitively, every message m is thus "signable" (i.e., the reduction can provide a signature), or "exploitable" (i.e., the reduction can use a forgery on m to break the assumption). The probability that all messages queried by $\mathcal{A}$ are signable and $\mathcal{A}$'s forgery is exploitable is thus bounded by the inverse of the number of signing queries, which yields the upper-bound on tightness. Since EQS are randomizable (by running Adapt with $\mu = 1$), this readily implies that EQS cannot be proven tightly secure.[4]

Meta-reductions have also been used to prove impossibility or optimality results about Schnorr signatures [PV05, Seu12, GBL08, FJS14], and more general statements [FF13]. Bader et al. [BJLS16] consider the multi-user setting and extend Coron's technique to other cryptographic primitives.

[4] Note that this does not extend to CRS-based EQS, since these are only guaranteed to be randomizable under a trusted CRS [KSD19]. As in the proof of impossibility of tightness [HJK12] the CRS is set up by the reduction, it might detect the meta-reduction's simulation.

Fischlin and Schröder [FS10] show that no three-move blind signature scheme can be proved secure from non-interactive assumptions if it satisfies certain conditions. One might wonder whether, together with the fact that EQS were used by FHS [FHS15] to construct round-optimal (i.e., two-move) blind signatures, this already implies the impossibility of EQS from non-interactive assumptions.

This is not the case. The blind-signature construction [FHS15] only satisfies computational blindness, a case Fischlin and Schröder deal with in their full version.[5] For their impossibility to hold, they must assume that blindness of the scheme holds relative to two oracles (Definition A.3 in the full version), of which "$\Sigma.\mathsf{sk}^{\mathrm{c}}$", given a public key, returns a matching secret key. For FHS this means solving discrete logarithms, which can be used to break blindness.[6]

Our Result

Statement. Our result can be (simplified and) summarized as follows (as done in Corollary 1):

> *Let Σ be an EQS scheme with signature-adaptivity under malicious keys. Let Π be a (non-interactive) computational problem and $\mathcal{R}$ be a reduction from Π that runs an adversary $\mathcal{A}$ against unforgeability of Σ once, so that if $\mathcal{A}$ wins with probability ϵ, then $\mathcal{R}$ breaks Π with probability at least $\phi \cdot \epsilon$. Then there exist an adversary $\mathcal{B}$ against unforgeability of Σ running in constant time, as well as the following, which run in time linear in that of $\mathcal{R}$: meta-reductions $\mathcal{M}$, attacking Π, and $\mathcal{D}$, attacking class-hiding (CH) of Σ, such that*
>
> $$\mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}} + \mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}} + \mathsf{Adv}^{\mathrm{CH}}_{\Sigma,\mathcal{D}^{\mathcal{R}}} \geq \phi^5/384 \ . \tag{1}$$
>
> *(By $\mathsf{Adv}^{\mathrm{X}}_{[\Sigma,]\mathcal{Y}}$ we denote $\mathcal{Y}$'s advantage in breaking the notion X [for scheme Σ] and $\mathcal{Y}^{\mathcal{Z}}$ denotes that $\mathcal{Y}$ has oracle access to $\mathcal{Z}$.)*

This implies that if the reduction for unforgeability is successful (i.e., ϕ is not "small") then either Σ does not satisfy CH, or the problem Π is not hard. Considering asymptotic security would yield that if the three advantages in Eq. (1) are negligible then so will be the success probability of the reduction.

Implications for Extensions of EQS. Since mercurial signatures and "signatures with flexible public key" are EQS with additional functionality, one would expect our result to carry over. However, all existing constructions [CL19, BHKS18, CL21, CLPK22] only consider adaptation under honest keys (arguably, because

[5] https://www.cryptoplexity.informatik.tu-darmstadt.de/media/crypt/publications_1/fischlinthree-moves2010.pdf.

[6] Using their notation [FHS15], after receiving the user's protocol message $M = (sC, sP)$ the signer can use $\Sigma.\mathsf{sk}^{\mathrm{c}}$ to compute s and thus C, and when later given a challenge message/blind-signature pair $(m, (\sigma, R, T))$, it checks if $C = mP + T$.

anonymity of the resulting delegatable credential schemes is only weak anyway), whereas our result requires adaptation under malicious keys.

Proof Ideas. The central idea for our impossibility result is to leverage the following discrepancy: for falsifiable assumptions the challenger can efficiently determine whether the adversary has won, whereas this cannot be efficiently done for unforgeability of an EQS scheme Σ. In particular, consider an unforgeability adversary $\mathcal{A}$ that queries a signature on a single message m and then returns a signature on some m^*. According to the definition of EQS-unforgeability, if $m \sim m^*$, that is, they are from the same class, then the adversary has not won; if $m \not\sim m^*$ then it has won. Now consider a reduction $\mathcal{R}$ to a falsifiable assumption Π, which runs such an adversary. In case $(\not\sim)$ the reduction must break Π with good probability. However, whereas in case $(\sim)$ it cannot: this is because a case-$(\sim)$ adversary $\mathcal{A}_\sim$ can be efficiently implemented using signature adaptation: it queries a signature on m and adapts it to one on m^*. The reduction combined with the adversary ($\mathcal{R}^{\mathcal{A}_\sim}$) would thus be an efficient algorithm for solving Π.

Distinguishing case $(\sim)$ from $(\not\sim)$ corresponds to breaking class-hiding (CH), where CH is equivalent to DDH being hard in the underlying group. It seems thus that we can use reduction $\mathcal{R}$ to break CH, i.e., DDH: Construct the following meta-reduction $\mathcal{M}_1$ that is given (m, m^*) and has to decide if $m \sim m^*$: $\mathcal{M}_1$ queries a signature σ^* on m^*, rewinds the reduction, queries m and returns (m^*, σ^*). The meta-reduction concludes that $m \sim m^*$ iff $\mathcal{R}$ fails to solve Π.

A problem ignored so far is that a reduction will typically not be able to exploit a signature σ^* it created itself; otherwise, it could just solve Π on its own.[7] We thus define the adversaries $\mathcal{A}_\sim$ and $\mathcal{A}_{\not\sim}$ simulated to $\mathcal{R}$ as follows: given the public key, they sample $m \leftarrow\!\!\$\, M$ (where M is the message space) and query a signature on m; next they sample m^*: $\mathcal{A}_\sim$ samples $m^* \leftarrow\!\!\$\, [m]$ and $\mathcal{A}_{\not\sim}$ samples $m^* \leftarrow\!\!\$\, M$; they then *sample a random signature* σ^* *from the set of all valid signatures on* m^* and return σ^*. (This is analogous to the proof of the impossibility of tight reductions for re-randomizable signatures [HJK12].)

Define meta-reduction $\mathcal{M}_2$ as follows: given a class-hiding instance (m, m^*), it simulates $\mathcal{A}_\sim$ or $\mathcal{A}_{\not\sim}$ (not knowing which) by obtaining a signature σ' on m^* via rewinding and using Adapt (with $\mu = 1$) to transform σ' to a uniform σ^*; decide according to whether $\mathcal{R}$ breaks Π.

This proof strategy only works for *perfect* reductions, which break Π whenever an adversary returns a forgery. Using the ideas for re-randomizable signatures [HJK12], this could be used to show that there are no tight reductions. However, we have not yet excluded the existence of non-tight reductions, such as *partitioning* reductions [Cor00, BLS01, Wat05]: given the problem instance, such

[7] The problem is that the definition of the adversary $\mathcal{A}$ simulated by $\mathcal{M}_1$ *depends* on $\mathcal{R}$ (as it uses a signature produced by $\mathcal{R}$). But a reduction only guarantees that when given any efficient adversary (defined independently of the reduction), it can use it to solve the problem. We must therefore start with defining $\mathcal{A}$ (who is not necessarily efficient, but whose behavior is precisely defined). Really we specify two adversaries, one simulated in the DDH case (not breaking the scheme) and one breaking the scheme.

reductions set up the public key (or program the random oracle in a way) so that they can answer signing queries for a subset S of messages, whereas for messages from another subset E, they can "exploit" forgeries to solve the problem.

Reductions that Partition Along Classes. To see how $\mathcal{M}_2$, defined above, fails for a non-tight reduction, assume $\mathcal{R}^p$ partitions the message space M "along classes", that is, if some m is in S (the set of "signable" messages) then all the messages of its class $[m]$ are, and if $m \in E$ (the set of "exploitable" messages) then $[m] \subseteq E$. We first observe that S and E must be (almost) disjoint, as otherwise $\mathcal{R}^p$ can solve the problem Π on its own (by producing a signature and then exploiting it). This case is reflected in the first term in Eq. (1) via an adversary $\mathcal{B}$ that simply aborts if it receives an invalid signature.

Applying $\mathcal{M}_2$ to $\mathcal{R}^p$ yields the following: if the signatures on m and m^* returned by $\mathcal{R}^p$ are valid, they both come from S, either in the same class or not; in both cases, since S and E are (almost) disjoint, σ^* will (almost certainly) not be exploitable by $\mathcal{R}^p$. Thus, $\mathcal{M}_2$ cannot exploit $\mathcal{R}^p$: either one of the signatures is invalid, or $\mathcal{R}^p$ will not solve the problem (no matter whether $m \sim m^*$ or not).

While this shows that the strategy $\mathcal{M}_2$ does not work for a reduction $\mathcal{R}^p$ that partitions along classes, a different meta-reduction $\mathcal{D}$ (which is the one used in our proof and appearing in Eq. (1)) can actually exploit $\mathcal{R}^p$ to distinguish classes: given an instance (m, m^*), $\mathcal{D}$ queries a signature on m, and (after rewinding) it queries a signature on m^*; if (a) one of them is valid and the other one isn't, it deduces that $m \not\sim m^*$, whereas if (b) they are both valid or both invalid, it guesses $m \sim m^*$. Since $\mathcal{R}^p$ partitions along classes, if ($\sim$) then (b) must occur, whereas if ($\not\sim$) then (a) occurs with good probability. For the last argument, we show, again via $\mathcal{B}$, that the sets S and E must both be "big" for a "good" reduction.

Other Reductions. So far, we have discussed that no reduction that partitions entire *classes* (into "simulatable" and "exploitable") can exist. The first question this raises is what to do about *non*-partitioning reductions. It turns out that we can view any reduction $\mathcal{R}$ as partitioning: let r be $\mathcal{R}$'s randomness given to it as explicit input and let st be $\mathcal{R}$'s internal state (which incorporates r) after returning the public key pk. For a fixed st, $\mathcal{R}$'s next step, $\mathcal{R}.\mathsf{sign}$ which takes input st and a query m and returns σ, is then a deterministic function.

For any (st, pk) we now define $S_{st,pk}$ as the set of messages m for which $\mathcal{R}.\mathsf{sign}(st, m)$ returns a signature valid under pk. Similarly, $\mathcal{R}.\mathsf{fin}$ taking a state and a forgery (m, σ) and returning a solution for Π is deterministic. We define $E_{st,pk}$ as the set of messages m^* for which, if $\mathcal{R}$ is given st and a *uniform* valid signature on m^*, it solves the Π-instance with a probability greater than a threshold we set.

It remains to show that a reduction $\mathcal{R}'$ that does *not* partition along classes cannot exist either. For such $\mathcal{R}'$, there are (many) classes which contain (many) messages in S as well as (many) messages in E. Now we can use *signature-adaptation* to directly attack the underlying problem Π (and thus, if the problem is hard to begin with, then no such reduction can exist). We construct a meta-reduction $\mathcal{M}$ (appearing in Eq. (1)) against Π, analogous to $\mathcal{R}^{\mathcal{A}_\sim}$ from the

beginning of the proof intuition. Given an instance of Π, $\mathcal{M}$ runs $\mathcal{R}'$ to receive pk and queries a signature σ on a message $m \leftarrow\!\!\$\, M$; it then runs $\sigma^* \leftarrow \mathsf{Adapt}(pk, m, \sigma, \mu)$ for $\mu \leftarrow\!\!\$\, \mathbb{Z}_p^*$ and returns $(\mu \cdot m, \sigma^*)$.[8] The forgery returned by $\mathcal{M}$ is thus a uniform signature on a random message m^* in $[m]$. Thus, since there are many classes with many elements in S and many elements in E, there is a "good" probability that $m \in S$ and $m^* \in E$, meaning $\mathcal{R}'$ solves the problem instance.

Challenges. Turning the above intuition (with all its "many", "big", "almost certainly", etc.) into a rigorous proof turns out quite tricky. We need to argue that our meta-reductions really cover all possible reduction strategies. That is, show that if both $\mathcal{B}$ (the trivial adversary) and $\mathcal{M}$ (the meta-reduction that returns a forgery on a multiple of the queried message) fail then the correlation between classes and the partitioning by S and E must be high enough so $\mathcal{D}$ can decide whether two messages m and m^* are from the same class. What complicates the computation of probabilities are dependencies of random variables. Moreover, the above sets S and E depend on the intermediate values generated by the reduction (and these sets are of the form $S_{st,pk}$ and $E_{st,pk}$), whereas the success of the reduction is guaranteed for random st and pk.

Proof Overview. The first meta-reduction $\mathcal{M}_1$ (simulating $\mathcal{A}_\sim$ or $\mathcal{A}_\not\sim$) with which we started discussing proof ideas is not used in our proof. $\mathcal{M}_1$ only works for reductions that have both signable and exploitable signature in many classes, but for these, $\mathcal{M}$ (from two paragraphs above) can directly break Π: it runs the reduction on a problem instance, queries a signature on a random message m, adapts it to a random multiple $\mu \cdot m$, and returns it to the reduction. The latter solves the instance if m is signable ($m \in S$) and $\mu \cdot m$ is exploitable ($\mu \cdot m \in E$).

Using $\mathcal{M}$, our proof first establishes that for an exploitable message there cannot be many signable messages in the same class (Lemmas 1 and 2). This shows that (roughly) classes contain either signable or exploitable messages but not both. We also show that there must be many signable messages, as otherwise the reduction does not correctly simulate the game to the adversary (Lemma 3, which constructs a "trivial" adversary $\mathcal{B}$); moreover, there cannot be too few exploitable messages either, as otherwise the reduction is not successful (Lemmas 5 and 6).

Together, this yields that while overall there are many signable messages, there are also many classes that contain (almost) none (since the exploitable messages must also be somewhere). This can be leveraged by the meta-reduction $\mathcal{D}$ (also previously discussed) against class-hiding: given an instance (m, m^*), $\mathcal{D}$ asks the reduction for signatures on both. If exactly one of the messages is signable, then they are likely to be in different classes. This suffices to obtain an advantage solving class-hiding. (Note that $\mathcal{D}$ need not "fully" simulate an adversary outputting a forgery.)

[8] Really, $\mathcal{M}$ first rewinds $\mathcal{R}'$ and returns $(\mu \cdot m, \sigma^*)$ in an execution in which it did not query a signature ($\mathcal{M}$ thus differs from $\mathcal{A}_\sim$ defined earlier). The reason is that the signing query could modify the set E, which could foil our analysis. (This is also why $\mathcal{D}$, defined above, rewinds the reduction).

To make this argument formal, we port the above properties to the level of state/public-key pairs (st, pk), which corresponds to the point when the reduction starts running the adversary on pk. This is done to then leverage the conditional independence of uniformly sampled messages falling into S or E respectively in the proof. Let $I^{(S)}$ be the set of pairs (st, pk) for which there are "sufficiently many" signable messages and let $I^{(\cap)}$ be the set of pairs (st, pk) which have very few classes that have many signable and exploitable messages. We show that $I^{(S)}$ is large (Lemma 4), that $I^{(\cap)}$ is large (Lemmas 7 and 8) and their intersection is large (Lemma 9).

These lemmas yield that (for many state/public-key pairs) there is a correlation between whether two messages are in the same class and whether these two messages are signable, which is what the success of the meta-reduction $\mathcal{D}$ against class-hiding relies on. This is made formal in Theorem 1.

2 Preliminaries

2.1 Notation

For a prime p, by $\mathbb{Z}_p^*$ we denote the non-zero elements of the finite field $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$. In this paper we will consider a fixed group $(\mathbb{G}, +)$ of prime order p. Define its non-zero elements $\mathbb{G}^* := \mathbb{G} \setminus \{0_\mathbb{G}\}$. We will denote by $k \cdot g := \sum_1^k g$. Note that $\mathbb{G}$ having prime order implies that for $g \neq 0_\mathbb{G}$ and $k \neq 0$ we have $k \cdot g \neq 0_\mathbb{G}$. We will naturally extend this operation to vectors by applying the operation "$\cdot$" defined above component-wise: for $m = (g_1, g_2) \in (\mathbb{G}^*)^2$ and $k \in \mathbb{Z}_p^*$ define $k \cdot m := (k \cdot g_1, k \cdot g_2)$. Let g denote a fixed generator of $\mathbb{G}$, which exists due to p being prime. For a set A denote by $\bar{A}$ the complement of A.

Assigning a value b to a variable a is denoted by $a := b$. When a denotes the output of a probabilistic algorithm B write $a \leftarrow B$, while drawing a value a uniformly from a finite set A is denoted by $a \leftarrow\!\$\, A$.

2.2 DDH

In this work we consider concrete security treatment, that is, we do not consider "negligible" advantages, but concretely relate the security of a scheme to the hardness of an underlying computational problem. The decisional Diffie-Hellamn (DDH) problem will be of central importance.

Definition 1. *Define for a group $\mathbb{G}$ of prime order p with g generating $\mathbb{G}$ the* DDH*-Game, played by an adversary $\mathcal{A}$ for $b \in \{0, 1\}$ as:*

$\mathrm{DDH}^b_{\mathbb{G},\mathcal{A}}$

1 : $x, y, t \leftarrow\!\$\, \mathbb{Z}_p^*$
2 : $b' \leftarrow \mathcal{A}(\mathbb{G}, x \cdot g, y \cdot g, (bxy + (1-b)t) \cdot g)$
3 : **return** b'

Define the advantage of an adversary $\mathcal{A}$ as

$$\mathsf{Adv}^{\mathrm{DDH}}_{\mathbb{G},\mathcal{A}} := \left|\Pr\left[\mathrm{DDH}^1_{\mathbb{G},\mathcal{A}} = 1\right] - \Pr\left[\mathrm{DDH}^0_{\mathbb{G},\mathcal{A}} = 1\right]\right|.$$

2.3 EQS Signature Schemes

For concreteness, we consider Equivalence Class Signature schemes for the message space $M := (\mathbb{G}^*)^2$. (All our results easily generalize to $(\mathbb{G}^*)^\ell$ for $\ell > 2$). This message space is partitioned into equivalence classes by the following relation for $m, m' \in M$:

$$m \sim m' \;:\Leftrightarrow\; \exists\, \mu \in \mathbb{Z}_p^* : m' = \mu \cdot m.$$

Define the set of classes of M as $\mathcal{C} := M/_\sim$. An EQS Scheme for message space M consists of the following algorithms:

- $\mathsf{Keygen}()$: a probabilistic algorithm that outputs a key pair (sk, pk) with $pk \in PK$, the public key space.
- $\mathsf{Sign}(sk, m)$: a probabilistic algorithm that takes a secret key sk and a message $m \in M$ and outputs a signature $\sigma \in \mathbb{S}$, where $\mathbb{S}$ is the (finite) signature space.
- $\mathsf{Verify}(pk, m, \sigma)$: a deterministic algorithm taking a public key pk, a message $m \in M$ and a signature σ and outputting 1 if the triple is valid and 0 otherwise.
- $\mathsf{Adapt}(pk, m, \sigma, \mu)$: a probabilistic algorithm taking a public key pk, a message $m \in M$, a signature σ on m and a scalar $\mu \in \mathbb{Z}_p^*$ as inputs and outputting a signature $\sigma' \in \mathbb{S}$ on the message $\mu \cdot m$.

By $[\mathsf{Keygen}]$ we will denote the set of pairs (sk, pk) that have non-zero probability of being output by Keygen. The next definition ensures that Sign and Adapt generate valid signatures.

Definition 2. *An EQS scheme is* correct *if for all $m \in M$ and for all $(sk, pk) \in [\mathsf{Keygen}]$ and for all $\mu \in \mathbb{Z}_p^*$ it holds that*

$$\Pr[\mathsf{Verify}(pk, m, \mathsf{Sign}(sk, m)) = 1] = 1 \qquad \textit{and}$$
$$\Pr[\mathsf{Verify}(pk, \mu \cdot m, \mathsf{Adapt}(pk, m, \mathsf{Sign}(sk, m), \mu)) = 1] = 1.$$

The following definition [FHS19, Definition 20] guarantees that signatures returned by Adapt are distributed uniformly.

Definition 3. *An EQS scheme perfectly adapts signatures under malicious keys if for all tuples $(pk, m, \sigma, \mu) \in PK \times M \times \mathbb{S} \times \mathbb{Z}_p^*$ for which*

$$\mathsf{Verify}(pk, m, \sigma) = 1$$

the output of $\sigma' \leftarrow \mathsf{Adapt}(pk, m, \sigma, \mu)$ is a uniformly random element of $\mathbb{S}$ conditioned on $\mathsf{Verify}(pk, \mu \cdot m, \sigma') = 1$.

Unforgeability is defined via a game. It starts by generating a key pair and initializing the set Q of messages for whose class a query has been issued. It then hands over the public key to $\mathcal{A}$, giving it access to an oracle $\mathcal{O}$. The oracle, when queried with a message m, adds the class of m to Q. In the end $\mathcal{A}$ outputs a message/signature pair (m^*, σ^*), which is considered a forgery if it is valid and no oracle query has been asked on the equivalence class of m^*.

Definition 4. *For an EQS scheme Σ and for a forger $\mathcal{A}$ that has access to a signing oracle $\mathcal{O}$, which can modify the set Q and has access to sk, we define the* UNF *game as follows:*

$\mathrm{UNF}_{\Sigma,\mathcal{A}}$

1: $(sk, pk) \leftarrow \mathsf{Keygen}()$
2: $Q := \emptyset$
3: $(m^*, \sigma^*) \leftarrow \mathcal{A}^{\mathcal{O}(\cdot)}(pk)$
4: **return** $(\mathsf{Verify}(pk, m^*, \sigma^*) \wedge m^* \notin Q)$

$\mathcal{O}(m)$

1: $Q := Q \cup [m]$
2: **return** $\mathsf{Sign}(sk, m)$

where $[m] := \{m' \in M \mid m \sim m'\}$ is the equivalence class of m. Define the advantage of an adversary $\mathcal{A}$ as

$$\mathsf{Adv}^{\mathrm{UNF}}_{\Sigma,\mathcal{A}} := \Pr[\mathrm{UNF}_{\Sigma,\mathcal{A}} = 1].$$

The next definition requires it to be hard to distinguish message pairs from the same class from random pairs.

Definition 5. *Let Σ be an EQS scheme with message space M. Define the Class-hiding game played by an adversary $\mathcal{D}$ for $b \in \{0, 1\}$:*

$\mathrm{CH}^b_{\Sigma,\mathcal{D}}$

1: $m \leftarrow\!\$\, M$
2: $m_0 \leftarrow\!\$\, M$
3: $m_1 \leftarrow\!\$\, [m]$
4: $b' \leftarrow \mathcal{D}(m, m_b)$
5: **return** b'

The advantage of $\mathcal{D}$ is defined as

$$\mathsf{Adv}^{\mathrm{CH}}_{\Sigma,\mathcal{D}} := \left|\Pr\left[\mathrm{CH}^1_{\Sigma,\mathcal{D}} = 1\right] - \Pr\left[\mathrm{CH}^0_{\Sigma,\mathcal{D}} = 1\right]\right|.$$

The proof of the following is straightforward and given in [FHS19].

Proposition 1 ([FHS19, **Proposition 1**])**.** *Let $\mathbb{G}$ be a group of prime order p and Σ an EQS scheme with $M = (\mathbb{G}^*)^2$. Then Σ is class-hiding if and only if* DDH *is hard in $\mathbb{G}$, in particular, we have $\mathsf{Adv}^{\mathrm{CH}}_{\Sigma,\mathcal{A}} = \mathsf{Adv}^{\mathrm{DDH}}_{\mathbb{G},\mathcal{A}}$ for all $\mathcal{A}$.*

2.4 Computational Problems

The following definition is due to [HJK12].

Definition 6. *A computational problem $\Pi := (C_\Pi, S_\Pi)$ consists of a set of challenges C_Π and a family of sets of solutions S_Π for each challenge c, i.e. $S_\Pi := (S_c)_{c \in C_\Pi}$. Additionally, we require the existence of two deterministic (polynomial-time) algorithms.*

– $\mathsf{Sample}(\rho)$ *takes randomness* ρ *and outputs* $c \in C_{\Pi}$.
– $\mathsf{Check}(\rho, s)$ *takes randomness* ρ *and an element* s *and checks whether* $s \in S_c$ *for* $c := \mathsf{Sample}(\rho)$.

We will denote the randomness space of Sample *by* P. *For an algorithm* $\mathcal{A}$ *define the game* Π *played by* $\mathcal{A}$ *below.*

$\Pi_{\mathcal{A}}$

1 : $\rho \leftarrow\!\!\$\, \mathrm{P}$
2 : $c := \mathsf{Sample}(\rho)$
3 : $s \leftarrow \mathcal{A}(c)$
4 : **return** $\mathsf{Check}(\rho, s)$

3 Our Impossibility Result

We strengthen our impossibility result in that we only consider adversaries that make one single signing query. That is, we show that even reductions that *only* work for single-query adversaries do not exist.

We will first establish some definitions and notations used throughout this section. Let R denote the randomness space of $\mathcal{R}$, then fixing its randomness $r \leftarrow\!\!\$\, \mathrm{R}$ lets us think of $\mathcal{R}$ as deterministic. When talking about a reduction $\mathcal{R}$ from Π to UNF that is being run by a meta-reduction $\mathcal{D}$, which simulates an adversary $\mathcal{A}$ for UNF that uses at most one signing query, we can think of $\mathcal{R}$ as split into three deterministic algorithms:

– $\mathcal{R}.\mathsf{init}(c, r)$: is the initialization routine of $\mathcal{R}$, which takes a challenge c of Π and some randomness $r \leftarrow\!\!\$\, \mathrm{R}$ and returns the state st of $\mathcal{R}$ and the public key pk of the UNF game;
– $\mathcal{R}.\mathsf{sign}(st, m)$: implements the signing oracle of $\mathcal{R}$. Given a state st which is output by $\mathcal{R}.\mathsf{init}$ and a message m it outputs a new state st' and a signature σ;
– $\mathcal{R}.\mathsf{fin}(st, m^*, \sigma^*)$: takes a state st returned by either $\mathcal{R}.\mathsf{init}$ or $\mathcal{R}.\mathsf{sign}$ (in the former case the adversary made no signing queries); it also takes a message m^* and a purported forgery σ^* for m^*. The algorithm then outputs its solution s to the problem c received in $\mathcal{R}.\mathsf{init}$.

Definition 7. *We say* $\mathcal{R}$ *reducing* Π *to* UNF *communicating with an adversary* $\mathcal{A}$ *for* UNF *has a (multiplicative) reduction tightness* $\phi \in (0, 1]$ *if the following holds:*

$$\phi \cdot \mathsf{Adv}^{\mathrm{UNF}}_{\mathcal{A}} \leq \mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{A}}}.$$

To condense notation and make calculations more readable, we introduce the following shorthand.

Definition 8. *Define* Init *as the code fragment given below.*

$\underline{\mathsf{Init}}$

$r \leftarrow\!\$\, \mathrm{R}$
$\rho \leftarrow\!\$\, \mathrm{P}$
$c := \mathsf{Sample}(\rho)$
$(st, pk) := \mathcal{R}.\mathsf{init}(c, r)$
return (st, pk)

Definition 9. *Let Π be a computational problem. Let $\mathcal{R}$ be a reduction from Π to* UNF *with tightness ϕ. Given $(st, pk) \in [\mathsf{Init}]$ we define for a message m the set of valid signatures $V_{m,pk} := \{\sigma \in \mathbb{S} \mid \mathsf{Verify}(pk, m, \sigma) = 1\}$. We then define subsets of M:*

$$S_{st,pk} := \{m \in M \mid \mathcal{R}.\mathsf{sign}(st, m) \in V_{m,pk}\},$$
$$E_{st,pk} := \left\{ m \in M \mid \Pr_{\sigma \leftarrow\!\$\, V_{m,pk}} [\mathsf{Check}(\rho, \mathcal{R}.\mathsf{fin}(st, (m, \sigma))) = 1] > \frac{\phi}{2} \right\},$$

where $S_{st,pk}$ (signable messages) corresponds to the set of messages for which $\mathcal{R}$ is able to provide a valid signature, and $E_{st,pk}$ (exploitable messages) corresponds to the set of messages for which $\mathcal{R}$ is "likely" to win game Π when given a uniform forgery on that message. Note that ρ is implicitly defined in the execution of Init.

The following result will show that whenever there is a message m that is "exploitable", then the probability of finding a multiple of m to be "signable" is bounded by the advantage of an efficient adversary winning Π. Intuitively this means that whenever we can find a message that $\mathcal{R}$ can sign, which can then be adapted into a message which $\mathcal{R}$ can exploit, then Π can be solved efficiently.

Lemma 1. *Let Σ be an EQS scheme that adapts perfectly under malicious keys (Definition 3). Let $\mathcal{R}$ be a reduction from Π to* UNF *running in time τ with reduction tightness ϕ. Then there exists a meta-reduction $\mathcal{M}$ running in time $\approx\tau$ such that*

$$\Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ m \leftarrow\!\$\, M, \mu \leftarrow\!\$\, \mathbb{Z}_p^* : \mu \cdot m \in S_{st,pk} \wedge m \in E_{st,pk}\end{matrix}\right] \leq \frac{2}{\phi} \mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}}.$$

Proof. Consider the meta-reduction $\mathcal{M}^{\mathcal{R}}$ playing Π that rewinds $\mathcal{R}$ given in Fig. 1. Then it holds that

$$\begin{aligned}\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}} &= \Pr[\Pi_{\mathcal{M}^{\mathcal{R}}} = 1] \\ &\geq \Pr\left[\Pi_{\mathcal{M}^{\mathcal{R}}} = 1 \mid m \in S_{st,pk} \wedge \zeta \cdot m \in E_{st,pk}\right] \\ &\qquad \cdot \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ m \leftarrow\!\$\, M, \zeta \leftarrow\!\$\, \mathbb{Z}_p^* : m \in S_{st,pk} \wedge \zeta \cdot m \in E_{st,pk}\end{matrix}\right]\end{aligned}$$

by the definition of $E_{st,pk}$ we have that $\mathcal{R}$ wins with probability $\geq \frac{\phi}{2}$ when $\zeta \cdot m \in E_{st,pk}$. Therefore

$\mathcal{M}^{\mathcal{R}}(c)$

1 $r \leftarrow\$ \mathrm{R}$
2 $(st, pk) := \mathcal{R}.\mathsf{init}(c, r)$
3 $m \leftarrow\$ M$
4 $(st', \sigma) \leftarrow \mathcal{R}.\mathsf{sign}(st, m)$
5 **if** $\mathsf{Verify}(pk, m, \sigma) = 0$
6 **abort**
7 $\mu \leftarrow \mathbb{Z}_p^*$
8 $\sigma' := \mathsf{Adapt}(pk, m, \sigma, \mu)$
9 **return** $\mathcal{R}.\mathsf{fin}(st, \mu \cdot m, \sigma')$

Recall:

$\Pi_{\mathcal{M}^{\mathcal{R}}}$

1 $\rho \leftarrow\$ \mathrm{P}$
2 $c := \mathsf{Sample}(\rho)$
3 $s \leftarrow \mathcal{M}^{\mathcal{R}}(c)$
4 **return** $\mathsf{Check}(\rho, s)$

Fig. 1. The meta-reduction $\mathcal{M}$

$$\begin{aligned}\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}} &\geq \frac{\phi}{2} \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init},\\ m \leftarrow\$ M, \zeta \leftarrow\$ \mathbb{Z}_p^*\end{matrix} : m \in S_{st,pk} \wedge \zeta \cdot m \in E_{st,pk}\right] \\ &= \frac{\phi}{2} \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init},\\ m \leftarrow\$ M, \mu \leftarrow\$ \mathbb{Z}_p^*\end{matrix} : \mu \cdot m \in S_{st,pk} \wedge m \in E_{st,pk}\right].\end{aligned}$$

□

The following result will be analogous to Lemma 1. It intuitively shows that if the problem Π is computationally hard then when sampling two random messages from an equivalence class, it is unlikely that the reduction can sign one of them while exploiting the other one to solve Π. In particular, we bound the probability that a random message is "signable" and there are many "exploitable" messages in its class, where "signable" and "exploitable" are as described in Definition 9. This is the case because when $\mathcal{R}$ is able to provide signatures on messages which can be adapted to exploitable ones, it could solve Π on its own.

Lemma 2. *Let Σ be an EQS scheme that adapts perfectly under malicious keys (Definition 3). Let $\mathcal{R}$ be a reduction from Π to* UNF *running in time τ with reduction tightness ϕ. Let $\delta \in [0, 1]$. Then there exists a meta-reduction $\mathcal{M}$ aiming to solve Π and running in time $\approx\tau$ such that*

$$\Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init},\\ m \leftarrow\$ M\end{matrix} : m \in S_{st,pk} \wedge \frac{|E_{st,pk} \cap [m]|}{|[m]|} \geq \delta\right] \leq \frac{2}{\delta\phi}\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}}.$$

Proof. Consider the meta-reduction $\mathcal{M}^{\mathcal{R}}$ playing Π that *rewinds* $\mathcal{R}$ which is given in Fig. 1 (note that $\mathcal{M}$ runs $\mathcal{R}.\mathsf{fin}$ on st and not st'). The reason for $\mathcal{M}$'s need to rewind $\mathcal{R}$ is that this allows us to view the sets $S_{st,pk}$ and $E_{st,pk}$ as fixed for each execution, as opposed to them changing after each call of the signing

oracle. Then we can show the following.

$$
\begin{aligned}
&\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}} = \Pr[\Pi_{\mathcal{M}^{\mathcal{R}}} = 1] \\
&\geq \Pr\left[\Pi_{\mathcal{M}^{\mathcal{R}}} = 1 \;\middle|\; m \in S_{st,pk} \wedge \frac{|E_{st,pk} \cap [m]|}{|[m]|} \geq \delta\right] \\
&\quad \cdot \Pr\left[\Pi_{\mathcal{M}^{\mathcal{R}}} : m \in S_{st,pk} \wedge \frac{|E_{st,pk} \cap [m]|}{|[m]|} \geq \delta\right] \\
&\geq \Pr\left[\Pi_{\mathcal{M}^{\mathcal{R}}} = 1 \;\middle|\; m \in S_{st,pk} \wedge \frac{|E_{st,pk} \cap [m]|}{|[m]|} \geq \delta \wedge \mu \cdot m \in E_{st,pk}\right] \qquad \text{(a)} \\
&\quad \cdot \Pr\left[\Pi_{\mathcal{M}^{\mathcal{R}}} : \mu \cdot m \in E_{st,pk} \;\middle|\; m \in S_{st,pk} \wedge \frac{|E_{st,pk} \cap [m]|}{|[m]|} \geq \delta\right] \qquad \text{(b)} \\
&\quad \cdot \Pr\left[\Pi_{\mathcal{M}^{\mathcal{R}}} : m \in S_{st,pk} \wedge \frac{|E_{st,pk} \cap [m]|}{|[m]|} \geq \delta\right]
\end{aligned}
$$

where $(b) \geq \delta$, while $(a) \geq \frac{\phi}{2}$ since $\mathcal{R}$ wins with probability $\frac{\phi}{2}$ if $\mu \cdot m \in E_{st,pk}$ and a uniformly random valid signature is given to $\mathcal{R}$, which is the case due to Σ fulfilling Definition 3. Therefore

$$
\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}} \geq \frac{\phi}{2}\delta \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ m \leftarrow\!\!\$\, M\end{matrix} : m \in S_{st,pk} \wedge \frac{|E_{st,pk} \cap [m]|}{|[m]|} \geq \delta\right],
$$

which concludes the lemma. □

Having established how $E_{st,pk}$ is distributed with respect to $S_{st,pk}$, we will now shift our attention to $S_{st,pk}$, the set of all messages which $\mathcal{R}$ can sign. The first result will establish a lower bound on the expected size of $S_{st,pk}$. Intuitively, this bound exists since in order to simulate UNF $\mathcal{R}$ has to provide signatures on "many" messages.

Lemma 3. *Let Σ be an EQS scheme. Let $\mathcal{R}$ have a reduction tightness ϕ. Then there exists an adversary $\mathcal{B}$ running in constant time such that the probability of a uniformly sampled m falling into $S_{st,pk}$, as defined in Definition 9, is lower-bounded as follows:*

$$
\Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ m \leftarrow\!\!\$\, M\end{matrix} : m \in S_{st,pk}\right] \geq \phi - \mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}}
$$

Proof. Consider the unbounded adversary $\mathcal{U}_S$ (showing a bound on "S") playing UNF which is defined in Fig. 2. $\mathcal{U}_S$ wins with probability 1, since in the game UNF the signature returned by the oracle is always valid, and therefore $\mathcal{U}_S$ never aborts. Now define the efficient adversary $\mathcal{B}$ (Fig. 3), which queries a signature σ and then aborts. Conditioned on σ being invalid, $\mathcal{B}$ perfectly simulates $\mathcal{U}_S$. We obtain

$$
\begin{aligned}
\phi &\leq \phi \cdot \mathsf{Adv}^{\mathrm{UNF}}_{\Sigma,\mathcal{U}_S} \\
&\leq \mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{U}_S}} \\
&= \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ (m', \sigma') \leftarrow \mathcal{U}_S^{\mathcal{R}.\mathsf{sign}(st,\cdot)}(pk)\end{matrix} : \mathsf{Check}(\rho, \mathcal{R}.\mathsf{fin}(m', \sigma')) = 1\right],
\end{aligned}
$$

$\mathcal{U}_S^{\mathsf{sign}(\cdot)}(pk)$

1 $m \leftarrow\!\!\$\ M$
2 $\sigma \leftarrow \mathsf{sign}(m)$
3 **if** $\mathsf{Verify}(pk, m, \sigma) = 0$
4 **abort**
5 $m' \leftarrow\!\!\$\ M \setminus [m]$
6 $\sigma' \leftarrow\!\!\$\ V_{m',pk}$
7 **return** (m', σ')

Fig. 2. The unbounded adversary $\mathcal{U}_S$

$\mathcal{B}^{\mathsf{sign}(\cdot)}(pk)$

1 $m \leftarrow\!\!\$\ M$
2 $\sigma \leftarrow \mathsf{sign}(m)$
3 **abort**

Fig. 3. The a$\mathcal{B}$orting adversary $\mathcal{B}$

where ρ is implicitly defined in Init,

$$= \Pr[\Pi_{\mathcal{R}^{\mathcal{U}_S}} = 1 \mid m \in \bar{S}_{st,pk}] \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ m \leftarrow\!\!\$\ M\end{matrix} : m \in \bar{S}_{st,pk}\right]$$
$$+ \Pr[\Pi_{\mathcal{R}^{\mathcal{U}_S}} = 1 \mid m \in S_{st,pk}] \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ m \leftarrow\!\!\$\ M\end{matrix} : m \in S_{st,pk}\right]$$

where the m in the two left-handed factors refers to the one chosen in line 1 of $\mathcal{U}_S$, and due to $\mathcal{B}$ simulating $\mathcal{U}_S$ in the case where σ is invalid we get

$$= \Pr[\Pi_{\mathcal{R}^{\mathcal{B}}} = 1 \mid m \in \bar{S}_{st,pk}] \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ m \leftarrow\!\!\$\ M\end{matrix} : m \in \bar{S}_{st,pk}\right]$$
$$+ \Pr[\Pi_{\mathcal{R}^{\mathcal{U}_S}} = 1 \mid m \in S_{st,pk}] \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ m \leftarrow\!\!\$\ M\end{matrix} : m \in S_{st,pk}\right]$$
$$\leq \mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}} + \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ m \leftarrow\!\!\$\ M\end{matrix} : m \in S_{st,pk}\right],$$

where the last inequality is due to

$$\Pr[\Pi_{\mathcal{R}^{\mathcal{B}}} = 1 \mid m \in \bar{S}_{st,pk}] \leq \frac{\mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}}}{\Pr[m \in \bar{S}_{st,pk}]}.$$

□

The next statement will translate the previous lemma to a setting where we will fix (st, pk). Fixing (st, pk) will enable us to remove dependencies of events at the expense of an additional condition, namely that of the fixed state/public-key pair. This tradeoff is well worth it due to the following lemma allowing us to reason with a similar bound about a reduced but still "large" set of state/public-key pairs. The intuition is that if for a random state/public-key pair generated by the experiment there is a bound, then the set of state/public-key pairs for which a similar bound holds must be large. Since $S_{st,pk}$ is "big", there must also be "many" state/public-key pairs for which a slightly worse bound holds. We will

denote subsets of $[\mathsf{Init}]$ with $I^{(x)}$, where x will identify the subset in question. For example the next lemma will define the subset for which the set $S_{st,pk}$ is "big".

Lemma 4. *Let Σ be an EQS scheme that adapts perfectly under malicious keys. Let $\mathcal{R}$ have a reduction tightness ϕ. Let $\mathcal{B}$ be as defined in Fig. 3. Define a subset of $[\mathsf{Init}]$ for which it is "likely" to sample a message in $S_{st,pk}$ conditioned on the given state and public key:*

$$I^{(S)} := \left\{ (st, pk) \,\middle|\, \Pr\left[m \leftarrow M : m \in S_{st,pk}\right] \geq \frac{\phi - \mathsf{Adv}^{\Pi}_{\mathcal{R},\mathcal{B}}}{2} \right\}.$$

Then $\Pr[(st, pk) \leftarrow \mathsf{Init} : (st, pk) \in I^{(S)}] \geq \frac{\phi - \mathsf{Adv}^{\Pi}_{\mathcal{R},\mathcal{B}}}{2}$.

Proof. From Lemma 3 we have

$$\begin{aligned}
\phi - \mathsf{Adv}^{\Pi}_{\mathcal{R},\mathcal{B}} &\leq \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init},\\ m \leftarrow\$\, M\end{matrix} : m \in S_{st,pk}\right] \\
&= \sum_{(st,pk)} \Pr[(st, pk)] \Pr\left[m \leftarrow\$\, M : m \in S_{st,pk}\right] \\
&= \sum_{(st,pk)\in I^{(S)}} \Pr[(st, pk)] \Pr\left[m \leftarrow\$\, M : m \in S_{st,pk}\right] \\
&\qquad + \sum_{(st,pk)\notin I^{(S)}} \Pr[(st, pk)] \Pr\left[m \leftarrow\$\, M : m \in S_{st,pk}\right] \\
&\leq \Pr[(st, pk) \leftarrow \mathsf{Init} : (st, pk) \in I^{(S)}] \\
&\quad + \frac{\phi - \mathsf{Adv}^{\Pi}_{\mathcal{R},\mathcal{B}}}{2}(1 - \Pr[(st, pk) \leftarrow \mathsf{Init} : (st, pk) \in I^{(S)}]).
\end{aligned}$$

And therefore

$$\Pr[(st, pk) \leftarrow \mathsf{Init} : (st, pk) \in I^{(S)}] \geq \frac{\phi - \mathsf{Adv}^{\Pi}_{\mathcal{R},\mathcal{B}}}{2}.$$

□

Similar to Lemma 3 we can obtain a bound on the size of $E_{st,pk}$. An obvious observation is that in order for $\mathcal{R}$ to be successful, there must be many messages such that when given a forgery on said message it wins Π. This follows because $\mathcal{R}$ must keep its tightness guarantees even for very successful UNF-adversaries. This idea, captured rigorously, yields the next lemma.

Lemma 5. *Let Σ be an EQS scheme that adapts perfectly under malicious keys. Let $\mathcal{R}$ have a reduction tightness ϕ. Then the probability of sampling $m \in M$ and it falling into $E_{st,pk}$, as defined in Definition 9, is lower-bounded as follows:*

$$\Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init},\\ m \leftarrow\$\, M\end{matrix} : m \in E_{st,pk}\right] \geq \frac{\phi}{2}$$

Proof. Consider the unbounded adversary $\mathcal{U}_E$ (showing a bound on "E") playing the UNF game and not making any signing queries defined as follows:

$\mathcal{U}_E(pk)$

1 : $m \leftarrow\!\$\, M$
2 : $\sigma \leftarrow\!\$\, V_{m,pk}$
3 : **return** (m, σ)

Then $\mathcal{U}_E$ wins with probability 1. Note that $\mathcal{U}_E$ is inefficient because (for a secure scheme) one cannot efficiently sample from $V_{m,pk}$. We get

$$\begin{aligned}
\phi = \phi \cdot \mathsf{Adv}^{\mathrm{UNF}}_{\Sigma,\mathcal{U}_E} &\leq \mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{U}_E}} \\
&= \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ (m, \sigma) \leftarrow \mathcal{U}_E(pk)\end{matrix} : \mathsf{Check}(\rho, \mathcal{R}.\mathsf{fin}(m, \sigma)) = 1\right] \\
&\leq \Pr\left[\Pi_{\mathcal{R}^{\mathcal{U}_E}} = 1 \,\middle|\, m \in E_{st,pk}\right] \cdot \Pr\left[\Pi_{\mathcal{R}^{\mathcal{U}_E}} : m \in E_{st,pk}\right] \\
&\quad + \Pr\left[\Pi_{\mathcal{R}^{\mathcal{U}_E}} = 1 \,\middle|\, m \in \bar{E}_{st,pk}\right] \cdot \Pr\left[\Pi_{\mathcal{R}^{\mathcal{U}_E}} : m \in \bar{E}_{st,pk}\right]. \qquad (2)
\end{aligned}$$

Now by the definition of $E_{st,pk}$, if $\mathcal{R}$ is given a uniform forgery on a message m which is not in $E_{st,pk}$, then its winning probability is less than $\frac{\phi}{2}$, therefore

$$(2) \leq \Pr\left[\Pi_{\mathcal{R}^{\mathcal{U}_E}} : m \in E_{st,pk}\right] + \frac{\phi}{2}.$$

Rearranging yields the result. □

We just showed that if $\mathcal{R}$ is "tight" then $E_{st,pk}$ is "big". We will lift this result onto a level of classes by showing that there also must be "many" classes C, which we will call "heavy", for which the proportion of $E_{st,pk}$-elements is "big". This partioning of the message space will be denoted by the superscript (C), indicating that we are operating on the level of classes. This will essentially be done by a variation of a technical lemma known as either the *Splitting Lemma* or *Heavy Row Lemma*, for which a version can be found in [PS00, Lemma 7]. Note that our "rows" much rather resemble the classes into which M is partitioned as opposed to "rows" in a two dimensional representation of $(\mathbb{G}^*)^2$ with a basis (g, g), which would correspond to the setting common in the literature.

Additionally we will show, in the spirit of Lemma 2, that finding messages in a "heavy" class for which $\mathcal{R}$ can provide a signature can be used to solve Π.

Lemma 6. *Let Σ be an EQS scheme that adapts perfectly under malicious keys. Let $\mathcal{R}$ have a reduction tightness ϕ. Define for $(st, pk) \in [\mathsf{Init}]$ the set of $E_{st,pk}$-"heavy" classes*

$$E^{(C)}_{st,pk} := \left\{ m \in M \,\middle|\, \frac{|E_{st,pk} \cap [m]|}{|[m]|} \geq \frac{\phi}{4} \right\}.$$

Then

1. $\Pr[(st, pk) \leftarrow \mathsf{Init}, m \leftarrow\!\$\, M : m \in E^{(C)}_{st,pk}] \geq \frac{\phi}{4}$, *and*
2. $\Pr\left[(st, pk) \leftarrow \mathsf{Init}, m \leftarrow\!\$\, E^{(C)}_{st,pk} : m \in S_{st,pk}\right] \leq \frac{32}{\phi^3}\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}}$.

Proof. To show that $E^{(C)}_{st,pk}$ is "big" assume towards a contradiction that $\Pr[(st, pk) \leftarrow \mathsf{Init}, m \leftarrow\!\$\, M : m \in E^{(C)}_{st,pk}] < \frac{\phi}{4}$. From Lemma 5 we get $\Pr[(st, pk) \leftarrow \mathsf{Init}, m \leftarrow\!\$\, M : m \in E_{st,pk}] \geq \phi/2$. Then since for m and μ uniformly chosen, $\mu \cdot m \in E_{st,pk}$ has the same probability as $m \in E_{st,pk}$ we get

$$\begin{aligned}
\frac{\phi}{2} &\leq \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init},\\ m \leftarrow\!\$\, M, \mu \leftarrow\!\$\, \mathbb{Z}^*_p\end{matrix} : \mu \cdot m \in E_{st,pk}\right] \\
&= \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init},\\ m \leftarrow\!\$\, M, \mu \leftarrow\!\$\, \mathbb{Z}^*_p\end{matrix} : \mu \cdot m \in E_{st,pk} \,\middle|\, m \in E^{(C)}_{st,pk}\right] \\
&\quad \cdot \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init},\\ m \leftarrow\!\$\, M, \mu \leftarrow\!\$\, \mathbb{Z}^*_p\end{matrix} : m \in E^{(C)}_{st,pk}\right] \\
&\quad + \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init},\\ m \leftarrow\!\$\, M, \mu \leftarrow\!\$\, \mathbb{Z}^*_p\end{matrix} : \mu \cdot m \in E_{st,pk} \,\middle|\, m \notin E^{(C)}_{st,pk}\right] \\
&\quad \cdot \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init},\\ m \leftarrow\!\$\, M, \mu \leftarrow\!\$\, \mathbb{Z}^*_p\end{matrix} : m \notin E^{(C)}_{st,pk}\right]. \qquad (3)
\end{aligned}$$

By the premise and since $m \notin E^{(C)}_{st,pk}$ implies that $\Pr_{\mu \in \mathbb{Z}^*_p}[\mu \cdot m \in E_{st,pk}] < \phi/4$ we get

$$(3) < \frac{\phi}{4} + \frac{\phi}{4} = \frac{\phi}{2},$$

a contradiction. This proves the first part.

To prove the second part, we apply Lemma 2 for $\delta := \frac{\phi}{4}$ to get

$$\begin{aligned}
\frac{8}{\phi^2}\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}} &\geq \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init},\\ m \leftarrow\!\$\, M\end{matrix} : m \in S_{st,pk} \wedge \frac{|E_{st,pk} \cap [m]|}{|[m]|} \geq \frac{\phi}{4}\right] \\
&= \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init},\\ m \leftarrow\!\$\, M\end{matrix} : m \in S_{st,pk} \wedge m \in E^{(C)}_{st,pk}\right] \\
&= \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init},\\ m \leftarrow\!\$\, M\end{matrix} : m \in S_{st,pk} \,\middle|\, m \in E^{(C)}_{st,pk}\right] \\
&\quad \cdot \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init},\\ m \leftarrow\!\$\, M\end{matrix} : m \in E^{(C)}_{st,pk}\right] \\
&= \Pr\left[(st, pk) \leftarrow \mathsf{Init}, m \leftarrow\!\$\, E^{(C)}_{st,pk} : m \in S_{st,pk}\right] \\
&\quad \cdot \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init},\\ m \leftarrow\!\$\, M\end{matrix} : m \in E^{(C)}_{st,pk}\right]. \qquad (4)
\end{aligned}$$

Using the first part of this lemma,

$$(4) \geq \Pr\left[(st, pk) \leftarrow \mathsf{Init}, m \leftarrow\!\$\, E^{(C)}_{st,pk} : m \in S_{st,pk}\right] \cdot \frac{\phi}{4}.$$

Rearranging yields

$$\Pr\left[(st, pk) \leftarrow \mathsf{Init}, m \leftarrow\!\$\, E^{(C)}_{st,pk} : m \in S_{st,pk}\right] \leq \frac{32}{\phi^3}\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}},$$

which concludes the proof of the lemma. □

Similar to Lemma 4 we will transform the statement we just obtained into a setting where we fix the state and public-key, and then show that many such pairs exist for which a weaker bound holds. Since we are concerned with the state/public-key pairs for which the intersection of $E_{st,pk}$-heavy classes and $S_{st,pk}$ is "small", we will denote this subset of $[\mathsf{Init}]$ with "$\cap$".

Lemma 7. *Let Σ be an EQS scheme that adapts perfectly under malicious keys. Let $\mathcal{R}$ have a reduction tightness ϕ. Let $\mathcal{M}$ be the meta-reduction defined in Fig. 1. For $\delta \in [0,1]$ define a subset of $[\mathsf{Init}]$ for which the size of the intersection of $E^{(C)}_{st,pk}$ and $S_{st,pk}$ obeys a weaker bound than the one in Lemma 6 once we condition the probability on that fixed state/public-key pair:*

$$I^{(\cap)}_{\delta} := \left\{(st, pk) \,\middle|\, \Pr\left[m \leftarrow\!\$\, E^{(C)}_{st,pk} : m \in S_{st,pk}\right] \leq \frac{32}{\delta\phi^3}\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}}\right\}.$$

Then the probability of $(st, pk) \leftarrow \mathsf{Init}$ falling into $I^{(\cap)}_{\delta}$ has the following lower bound

$$\Pr[(st, pk) \leftarrow \mathsf{Init} : (st, pk) \in I^{(\cap)}_{\delta}] \geq 1 - \delta.$$

Proof. From Lemma 6 we get

$$\begin{aligned}
\frac{32}{\phi^3}\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}} &\geq \Pr\left[(st, pk) \leftarrow \mathsf{Init}, m \leftarrow\!\$\, E^{(C)}_{st,pk} : m \in S_{st,pk}\right] \\
&= \sum_{(st,pk)} \Pr[(st, pk)] \Pr\left[m \leftarrow\!\$\, E^{(C)}_{st,pk} : m \in S_{st,pk}\right] \\
&\geq \sum_{(st,pk)\notin I^{(\cap)}_{\delta}} \Pr[(st, pk)] \Pr\left[m \leftarrow\!\$\, E^{(C)}_{st,pk} : m \in S_{st,pk}\right] \\
&\geq \sum_{(st,pk)\notin I^{(\cap)}_{\delta}} \Pr[(st, pk)] \cdot \frac{32}{\delta\phi^3}\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}} \\
&= (1 - \Pr[(st, pk) \leftarrow \mathsf{Init} : (st, pk) \in I^{(\cap)}_{\delta}]) \cdot \frac{32}{\delta\phi^3}\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}}.
\end{aligned}$$

Rearranging yields $\Pr[(st, pk) \leftarrow \mathsf{Init} : (st, pk) \in I^{(\cap)}_{\delta}] \geq 1 - \delta$. □

In the same manner we can reason that if the bound from Lemma 7 holds for a random class, then a similar bound will hold for a "large" subset of classes when we fix the class.

Lemma 8. *Let Σ be an EQS scheme that adapts perfectly under malicious keys. Let $\mathcal{R}$ have a reduction tightness ϕ. Let $\mathcal{M}$ be the meta-reduction defined in Fig. 1. For $\delta \in [0,1]$, $(st, pk) \in I_\delta^{(\cap)}$ define the following subset of $\mathcal{C}$: all classes for which the intersection of $E_{st,pk}^{(C)}$ and $S_{st,pk}$ is bounded by a multiple of $\mathcal{M}$'s advantage*

$$\mathcal{C}_{st,pk,\delta}^{(\cap)} := \left\{ C \in \mathcal{C} \;\middle|\; \Pr\left[m \leftarrow\!\$\, E_{st,pk}^{(C)} : m \in S_{st,pk} \middle| m \in C \right] \leq \frac{64}{\delta\phi^3} \mathsf{Adv}_{\mathcal{M}^{\mathcal{R}}}^{\Pi} \right\}.$$

Then $\Pr\left[(st, pk) \leftarrow \mathsf{Init}, m \leftarrow\!\$\, M : [m] \in \mathcal{C}_{st,pk,\delta}^{(\cap)}\right] \geq \frac{\phi}{8}$.

Proof. Let $(st, pk) \in I_\delta^{(\cap)}$ then by definition of $I_\delta^{(\cap)}$ in Lemma 7 we have

$$\begin{aligned}
\frac{32}{\delta\phi^3}\mathsf{Adv}_{\mathcal{M}^{\mathcal{R}}}^{\Pi} &\geq \Pr\left[m \leftarrow\!\$\, E_{st,pk}^{(C)} : m \in S_{st,pk} \right] \\
&\geq \sum_{C \notin \mathcal{C}_{st,pk,\delta}^{(\cap)}} \Pr[m \leftarrow\!\$\, E_{st,pk}^{(C)} : m \in C] \\
&\qquad \cdot \Pr\left[m \leftarrow\!\$\, E_{st,pk}^{(C)} : m \in S_{st,pk} \,|\, m \in C \right] \\
&\geq \sum_{C \notin \mathcal{C}_{st,pk,\delta}^{(\cap)}} \Pr[m \leftarrow\!\$\, E_{st,pk}^{(C)} : m \in C] \frac{64}{\delta\phi^3}\mathsf{Adv}_{\mathcal{M}^{\mathcal{R}}}^{\Pi} \\
&= (1 - \Pr[m \leftarrow\!\$\, E_{st,pk}^{(C)} : [m] \in \mathcal{C}_{st,pk,\delta}^{(\cap)}]) \frac{64}{\delta\phi^3}\mathsf{Adv}_{\mathcal{M}^{\mathcal{R}}}^{\Pi}
\end{aligned}$$

And therefore

$$\Pr[(st, pk) \leftarrow \mathsf{Init}, m \leftarrow\!\$\, E_{st,pk}^{(C)} : [m] \in \mathcal{C}_{st,pk,\delta}^{(\cap)}] \geq \frac{1}{2}$$

Now using this and Lemma 6 we get

$$\begin{aligned}
&\Pr\left[(st, pk) \leftarrow \mathsf{Init}, m \leftarrow\!\$\, M : [m] \in \mathcal{C}_{st,pk,\delta}^{(\cap)}\right] \\
&\quad \geq \Pr\left[\begin{matrix} (st, pk) \leftarrow \mathsf{Init}, \\ m \leftarrow\!\$\, E_{st,pk}^{(C)} \end{matrix} : [m] \in \mathcal{C}_{st,pk,\delta}^{(\cap)} \right] \Pr\left[\begin{matrix} (st, pk) \leftarrow \mathsf{Init}, \\ m \leftarrow\!\$\, M \end{matrix} : m \in E_{st,pk}^{(C)} \right] \\
&\quad \geq \frac{1}{2} \cdot \frac{\phi}{4} = \frac{\phi}{8}
\end{aligned}$$

concluding the proof. □

Having established lower bounds on the sizes of both $I^{(S)}$ and $I_\delta^{(\cap)}$, we will reason that for an appropriate value for δ their intersection must be "large" as well. This intersection contains state/public-key pairs for which both $S_{st,pk}$ is big and $S_{st,pk}$ and $E_{st,pk}$ have a small intersection. This is of interest because the separation along classes will enable us to construct a reduction which leverages $\mathcal{R}$'s implicit separation of classes to break DDH.

Lemma 9. *Let Σ be an EQS scheme that adapts perfectly under malicious keys. Let $\mathcal{R}$ have a reduction tightness ϕ. Let $I^{(S)}$ be as defined in Lemma 4, $I_\delta^{(\cap)}$ be as defined in Lemma 7 and $\mathcal{B}$ be the aborting adversary defined in Fig. 3. Then for $\delta := \phi - \mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}}$ we get that $I^{(S)} \cap I^{(\cap)}_{\phi-\mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}}}$ is "big", namely*

$$|I^{(S)} \cap I^{(\cap)}_{\phi-\mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}}}| \geq \frac{\phi - \mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}}}{2}.$$

Proof. Fix $\delta := \phi - \mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}}$; then Lemma 7 and Lemma 4 yield

$$\begin{aligned}|\overline{I^{(S)} \cap I_\delta^{(\cap)}}| &= |\overline{I^{(S)}} \cup \overline{I_\delta^{(\cap)}}| \leq |\overline{I^{(S)}}| + |\overline{I_\delta^{(\cap)}}| \\ &\leq \frac{\phi - \mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}}}{2} + 1 - \phi + \mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}} = 1 - \frac{\phi - \mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}}}{2}.\end{aligned}$$

And therefore $|I^{(S)} \cap I^{(\cap)}_{\phi-\mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}}}| \geq (\phi - \mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}})/2$. □

With many lemmas in the bag we can now tackle the main result of this work. The intuitive statement is that if $\mathcal{R}$ is "tight" then we can construct meta-reductions such that either one such meta-reduction will use $\mathcal{R}$ to win DDH, or a different meta-reduction will use $\mathcal{R}$ to win Π, or $\mathcal{R}$ is able to win Π itself (formally, with the help of an efficient but trivial adversary).

Theorem 1. *For all groups $\mathbb{G}$ and all EQS schemes Σ over $\mathbb{G}$ that adapt perfectly under malicious keys (as defined in Sect. 2.3), for all computational problems Π and all reductions $\mathcal{R}$ that reduce Π to* UNF*, running the adversary once, with a reduction tightness of ϕ and running in time τ, there exist meta-reductions $\mathcal{D}$ attacking* DDH *running in time $\approx 2\tau$ and $\mathcal{M}$ attacking Π running in time $\approx \tau$ as well as an adversary $\mathcal{B}$ attacking* UNF *of Σ running in constant time such that*

$$\mathsf{Adv}^{\mathrm{DDH}}_{\mathbb{G},\mathcal{D}^{\mathcal{R}}} + \frac{3\phi^3}{32}\mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}} + \frac{12}{\phi}\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}} \geq \frac{\phi^4}{32}.$$

Proof Idea. Let's start by first giving an idea of the proof. For a reduction $\mathcal{R}$ having defined the sets $S_{st,pk}$ and $E_{st,pk}$ we have established that both these sets must be reasonably "large" if $\mathcal{R}$ is to be "successful". Now if it is the case that both of these sets are spread evenly across the message space, then there exist (many) classes with both elements of $S_{st,pk}$ and $E_{st,pk}$. This can be used to solve Π, as can be seen in the analysis of $\mathcal{M}$ defined in Fig. 1. On the other hand, if the sets are separated into different classes, then we can construct a meta-reduction $\mathcal{D}$ which extracts this information from $\mathcal{R}$ in order to reason about DDH. The main effort will be in establishing an appropriate lower bound on this latter process being successful.

The proof will use the following technical lemma.

Lemma 10. *Let I be a finite set of indices. Let $\lambda_i \geq 0$ for $i \in I$ with $\sum_i \lambda_i = 1$, $x_i \in [0,1]$ for $i \in I$, and $y := \sum_i \lambda_i x_i$. Then*

$$\sum_{i \in I} \lambda_i x_i^2 - y^2 = \sum_{i \in I} \lambda_i (x_i - y)^2.$$

Proof.

$$\sum_i \lambda_i (x_i - y)^2 = \sum_i \lambda_i (x_i^2 - 2x_i y + y^2) = \sum_i \lambda_i x_i^2 - 2y \sum_i \lambda_i x_i + y^2$$
$$= \sum_i \lambda_i x_i^2 - 2y^2 + y^2 = \sum_i \lambda_i x_i^2 - y^2.$$

□

$\mathcal{D}^{\mathcal{R}}(g, x \cdot g, y \cdot g, z \cdot g)$

1 $r \leftarrow\$ \mathrm{R}$ // where z = bxy + (1-b)t
2 $\rho \leftarrow\$ \mathrm{P}$
3 $c := \mathsf{Sample}(\rho)$
4 $(st, pk) := \mathcal{R}.\mathsf{init}(c, r)$
5 $\zeta \leftarrow\$ \mathbb{Z}_p^*$
6 $m := \zeta \cdot (g, x \cdot g)$
7 $m' := (y \cdot g, z \cdot g)$
8 $\sigma \leftarrow \mathcal{R}.\mathsf{sign}(st, m)$
9 $\sigma' \leftarrow \mathcal{R}.\mathsf{sign}(st, m')$
10 **if** $\mathsf{Verify}(pk, m, \sigma) = \mathsf{Verify}(pk, m', \sigma')$:
11 **return** 1
12 **return** 0

Fig. 4. The DDH distinguisher $\mathcal{D}$

Proof of Theorem 1. Consider the efficient meta-reduction $\mathcal{D}$ which rewinds the reduction $\mathcal{R}$ and uses it in order to win the DDH-Game defined in Fig. 4. (Note that $\mathcal{D}$ runs $\mathcal{R}.\mathsf{sign}$ twice on the *same* value *st*.) The first four lines correspond to the Init experiment, in which $\mathcal{D}$ obtains the problem instance c for $\mathcal{R}$. It then groups its inputs into two messages m and m' and obtains a signature from $\mathcal{R}$ on both messages. If the validity of both signatures matches, then $\mathcal{D}$ outputs "DDH-pair". For a fixed $(st, pk) \in [\mathsf{Init}]$ we will write $\Pr[(st, pk)]$instead

of $\Pr[(st', pk') \leftarrow \mathsf{Init} : (st', pk') = (st, pk)]$ to enhance readability. Then when $\mathcal{D}$ plays the DDH game on a "random" instance, it will be right with the following probability:

$$\begin{aligned}\Pr[\mathrm{DDH}^0_{\mathcal{D}} = 0] &= \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ m, m' \leftarrow\$ M\end{matrix} : \begin{matrix}\left(m \in S_{st,pk} \wedge m' \in \bar{S}_{st,pk}\right) \\ \vee \left(m \in \bar{S}_{st,pk} \wedge m' \in S_{st,pk}\right)\end{matrix}\right] \\ &= 2\Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ m, m' \leftarrow\$ M\end{matrix} : m \in S_{st,pk} \wedge m' \in \bar{S}_{st,pk}\right] \qquad (5)\end{aligned}$$

Fixing (st, pk) will remove the dependency between the events $m \in S_{st,pk}$ and $m' \in \bar{S}_{st,pk}$, since m and m' are independent

$$\begin{aligned}(5) &= 2\sum_{(st,pk)} \Pr[(st, pk)] \cdot \Pr\left[m, m' \leftarrow\$ M : m \in S_{st,pk} \wedge m' \in \bar{S}_{st,pk}\right] \\ &= 2\sum_{(st,pk)} \Pr[(st, pk)] \cdot \Pr\left[m \leftarrow\$ M : m \in S_{st,pk}\right] \\ &\qquad \cdot \Pr\left[m' \leftarrow\$ M : m' \in \bar{S}_{st,pk}\right] \\ &= 2\sum_{(st,pk)} \Pr[(st, pk)] \cdot \Pr\left[m \leftarrow\$ M : m \in S_{st,pk}\right] \\ &\qquad \cdot \left(1 - \Pr\left[m \leftarrow\$ M : m \in S_{st,pk}\right]\right) \\ &= 2\Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ m \leftarrow\$ M\end{matrix} : m \in S_{st,pk}\right] \\ &\quad - 2\sum_{(st,pk)} \Pr[(st, pk)] \cdot \Pr\left[m \leftarrow\$ M : m \in S_{st,pk}\right]^2 \qquad (6)\end{aligned}$$

On the other hand, when $\mathcal{D}$ plays the DDH game on a "DDH" instance, its guess will be wrong with the following probability:

$$\begin{aligned}&\Pr[\mathrm{DDH}^1_{\mathcal{D}} = 0] = \\ &= \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ m \leftarrow\$ M, \mu \leftarrow\$ \mathbb{Z}_p^*\end{matrix} : \begin{matrix}\left(m \in S_{st,pk} \wedge \mu \cdot m \in \bar{S}_{st,pk}\right) \\ \vee \left(m \in \bar{S}_{st,pk} \wedge \mu \cdot m \in S_{st,pk}\right)\end{matrix}\right] \\ &= 2\Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ m \leftarrow\$ M, \mu \leftarrow\$ \mathbb{Z}_p^*\end{matrix} : m \in \bar{S}_{st,pk} \wedge \mu \cdot m \in S_{st,pk}\right] \\ &= 2\left(\Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ m \leftarrow\$ M, \mu \leftarrow\$ \mathbb{Z}_p^*\end{matrix} : m \in \bar{S}_{st,pk} \wedge \mu \cdot m \in S_{st,pk} \wedge m \in E_{st,pk}\right]\right. \\ &\quad \left. + \Pr\left[\begin{matrix}(st, pk) \leftarrow \mathsf{Init}, \\ m \leftarrow\$ M, \mu \leftarrow\$ \mathbb{Z}_p^*\end{matrix} : m \in \bar{S}_{st,pk} \wedge \mu \cdot m \in S_{st,pk} \wedge m \in \bar{E}_{st,pk}\right]\right) \qquad (7)\end{aligned}$$

For the second term in parenthesis we obtain the following upper bound.

$$
\begin{aligned}
&\Pr\left[\begin{matrix}(st,pk)\leftarrow \mathsf{Init},\\ m\leftarrow\$\, M, \mu\leftarrow\$\, \mathbb{Z}_p^*\end{matrix} : m\in \bar{S}_{st,pk}\wedge \mu\cdot m\in S_{st,pk}\wedge m\in \bar{E}_{st,pk}\right]\\
&=\sum_{C\in\mathcal{C}}\frac{1}{|\mathcal{C}|}\Pr\left[\begin{matrix}(st,pk)\leftarrow \mathsf{Init},\\ m\leftarrow\$\, M,\\ \mu\leftarrow\$\, \mathbb{Z}_p^*\end{matrix} : m\in \bar{S}_{st,pk}\wedge m\in \bar{E}_{st,pk}\wedge \mu\cdot m\in S_{st,pk}\middle| m\in C\right]\\
&=\sum_{C\in\mathcal{C}}\frac{1}{|\mathcal{C}|}\sum_{(st,pk)}\Pr[(st,pk)]\Pr[m\leftarrow\$\, M,\mu\leftarrow\$\,\mathbb{Z}_p^* : m\in\bar{S}_{st,pk}\\
&\qquad\qquad\wedge m\in\bar{E}_{st,pk}\wedge\mu\cdot m\in S_{st,pk}\mid m\in C]\\
&=\sum_{C\in\mathcal{C}}\frac{1}{|\mathcal{C}|}\sum_{(st,pk)}\Pr[(st,pk)]\Pr[m\leftarrow\$\, M : m\in\bar{S}_{st,pk}\\
&\qquad\qquad\wedge m\in\bar{E}_{st,pk}\mid m\in C]\\
&\qquad\qquad\cdot\Pr\left[m\leftarrow\$\, M,\mu\leftarrow\$\,\mathbb{Z}_p^* : \mu\cdot m\in S_{st,pk}\,|m\in C\right]
\end{aligned}
$$

From $\bar{S}_{st,pk}\cap\bar{E}_{st,pk}\subseteq\bar{S}_{st,pk}$ and both m and $\mu\cdot m$ being a uniform element of a class C, we get

$$
\begin{aligned}
&\leq\sum_{C\in\mathcal{C}}\frac{1}{|\mathcal{C}|}\sum_{(st,pk)}\Pr[(st,pk)]\cdot\Pr\left[m\leftarrow\$\, M : m\in\bar{S}_{st,pk}\,|m\in C\right]\\
&\qquad\qquad\cdot\Pr\left[m\leftarrow\$\, M : m\in S_{st,pk}\,|m\in C\right]\\
&=\sum_{C\in\mathcal{C}}\frac{1}{|\mathcal{C}|}\sum_{(st,pk)}\Pr[(st,pk)]\cdot\left(1-\Pr\left[m\leftarrow\$\, M : m\in S_{st,pk}\,|m\in C\right]\right)\\
&\qquad\qquad\cdot\Pr\left[m\leftarrow\$\, M : m\in S_{st,pk}\,|m\in C\right]\\
&=\sum_{(st,pk)}\Pr[(st,pk)]\sum_{C\in\mathcal{C}}\frac{1}{|\mathcal{C}|}\left(1-\Pr\left[m\leftarrow\$\, M : m\in S_{st,pk}\,|m\in C\right]\right)\\
&\qquad\qquad\cdot\Pr\left[m\leftarrow\$\, M : m\in S_{st,pk}\,|m\in C\right]\\
&=\sum_{(st,pk)}\Pr[(st,pk)]\sum_{C\in\mathcal{C}}\frac{1}{|\mathcal{C}|}\Big(\Pr\left[m\leftarrow\$\, M : m\in S_{st,pk}\,|m\in C\right]\\
&\qquad\qquad-\Pr\left[m\leftarrow\$\, M : m\in S_{st,pk}\,|m\in C\right]^2\Big)\\
&=\Pr\left[(st,pk)\leftarrow\mathsf{Init}, m\leftarrow\$\, M : m\in S_{st,pk}\right]\\
&\quad-\sum_{(st,pk)}\Pr[(st,pk)]\sum_{C\in\mathcal{C}}\frac{1}{|\mathcal{C}|}\Pr\left[m\leftarrow\$\, M : m\in S_{st,pk}\,|m\in C\right]^2.
\end{aligned}
$$

Plugging this result together with

$$\Pr\left[\begin{matrix}(st,pk)\leftarrow\mathsf{Init},\\ m\leftarrow\!\$\, M,\mu\leftarrow\!\$\,\mathbb{Z}_p^*\end{matrix} : m\in\bar{S}_{st,pk}\wedge\mu\cdot m\in S_{st,pk}\wedge m\in E_{st,pk}\right]$$
$$\leq\Pr\left[\begin{matrix}(st,pk)\leftarrow\mathsf{Init},\\ m\leftarrow\!\$\, M,\mu\leftarrow\!\$\,\mathbb{Z}_p^*\end{matrix} : \mu\cdot m\in S_{st,pk}\wedge m\in E_{st,pk}\right]$$

into Eq. (7), we obtain

$$\begin{aligned}&\Pr[\mathrm{DDH}^1_{\mathcal{D}}=0]\\ &\quad\leq 2\Pr\left[\begin{matrix}(st,pk)\leftarrow\mathsf{Init},\\ m\leftarrow\!\$\, M,\mu\leftarrow\!\$\,\mathbb{Z}_p^*\end{matrix} : \mu\cdot m\in S_{st,pk}\wedge m\in E_{st,pk}\right]\\ &\qquad+2\Pr\left[(st,pk)\leftarrow\mathsf{Init},m\leftarrow\!\$\, M : m\in S_{st,pk}\right]\\ &\qquad-2\sum_{(st,pk)}\Pr[(st,pk)]\sum_{C\in\mathcal{C}}\frac{1}{|\mathcal{C}|}\Pr\left[m\leftarrow\!\$\, M : m\in S_{st,pk}\,|m\in C\right]^2. \qquad (8)\end{aligned}$$

Putting Eqs. (6) and (8) together yields

$$\begin{aligned}\mathsf{Adv}^{\mathrm{DDH}}_{\mathbb{G},\mathcal{D}^{\mathcal{R}}}&=\Pr[\mathrm{DDH}^1_{\mathcal{D}}=1]-\Pr[\mathrm{DDH}^0_{\mathcal{D}}=1]\\ &=\Pr[\mathrm{DDH}^0_{\mathcal{D}}=0]-\Pr[\mathrm{DDH}^1_{\mathcal{D}}=0]\\ &\geq 2\Pr\left[\begin{matrix}(st,pk)\leftarrow\mathsf{Init},\\ m\leftarrow\!\$\, M\end{matrix} : m\in S_{st,pk}\right]\\ &\quad-2\sum_{(st,pk)}\Pr[(st,pk)]\cdot\Pr\left[m\leftarrow\!\$\, M : m\in S_{st,pk}\right]^2\\ &\quad-2\Pr\left[\begin{matrix}(st,pk)\leftarrow\mathsf{Init},\\ m\leftarrow\!\$\, M,\mu\leftarrow\!\$\,\mathbb{Z}_p^*\end{matrix} : \mu\cdot m\in S_{st,pk}\wedge m\in E_{st,pk}\right]\\ &\quad-2\Pr\left[\begin{matrix}(st,pk)\leftarrow\mathsf{Init},\\ m\leftarrow\!\$\, M\end{matrix} : m\in S_{st,pk}\right]\\ &\quad+2\sum_{(st,pk)}\Pr[(st,pk)]\sum_{C\in\mathcal{C}}\frac{1}{|\mathcal{C}|}\Pr\left[m\leftarrow\!\$\, M : m\in S_{st,pk}\,|m\in C\right]^2 \qquad (9)\end{aligned}$$

Lemma 1 yields $\Pr\left[\begin{matrix}(st,pk)\leftarrow\mathsf{Init},\\ m\leftarrow\!\$\, M,\mu\leftarrow\!\$\,\mathbb{Z}_p^*\end{matrix} : \mu\cdot m\in S_{st,pk}\wedge m\in E_{st,pk}\right]\leq\frac{2}{\phi}\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}}$ with $\mathcal{M}$ as defined in Fig. 1, and therefore

$$\begin{aligned}(9)\geq 2\sum_{(st,pk)}\Pr[(st,pk)]\Bigg(&\sum_{C\in\mathcal{C}}\frac{1}{|\mathcal{C}|}\Pr\left[m\leftarrow\!\$\, M : m\in S_{st,pk}\,|m\in C\right]^2\\ &-\Pr\left[m\leftarrow\!\$\, M : m\in S_{st,pk}\right]^2\Bigg)-\frac{4}{\phi}\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}}. \qquad (10)\end{aligned}$$

Applying Lemma 10 for $I := \mathcal{C}$, $x_C := \Pr\left[m \leftarrow\!\$\, M : m \in S_{st,pk} \,|\, m \in C\right]$, and $\lambda_C := \frac{1}{|\mathcal{C}|}$ yields

$$\begin{aligned}(10) &= 2 \sum_{(st,pk)} \Pr[(st,pk)] \sum_{C \in \mathcal{C}} \frac{1}{|\mathcal{C}|} \Big(\Pr\left[m \leftarrow\!\$\, M : m \in S_{st,pk} \,|\, m \in C\right] \\ &\qquad - \Pr\left[m \leftarrow\!\$\, M : m \in S_{st,pk}\right] \Big)^2 - \frac{4}{\phi} \mathsf{Adv}^{\Pi}_{\mathcal{M}\mathcal{R}} \\ &= 2 \sum_{(st,pk)} \Pr[(st,pk)] \sum_{C \in \mathcal{C}} \frac{1}{|\mathcal{C}|} \Big(\Pr\left[m \leftarrow\!\$\, M : m \in S_{st,pk}\right] \\ &\qquad - \Pr\left[m \leftarrow\!\$\, M : m \in S_{st,pk} \,|\, m \in C\right] \Big)^2 - \frac{4}{\phi} \mathsf{Adv}^{\Pi}_{\mathcal{M}\mathcal{R}}.\end{aligned}$$

Let $\mathcal{B}$ be the aborting adversary defined in Fig. 3. Let $\delta := \phi - \mathsf{Adv}^{\Pi}_{\mathcal{R}\mathcal{B}}$. Then since $I := I^{(S)} \cap I^{(\cap)}_{\phi - \mathsf{Adv}^{\Pi}_{\mathcal{R}\mathcal{B}}} \subseteq [\mathsf{Init}]$ and $\mathcal{C}^{(\cap)}_{st,pk} := \mathcal{C}^{(\cap)}_{st,pk,\phi - \mathsf{Adv}^{\Pi}_{\mathcal{R}\mathcal{A}}} \subseteq \mathcal{C}$ we get

$$\begin{aligned}&\geq 2 \sum_{(st,pk) \in I} \Pr[(st,pk)] \sum_{C \in \mathcal{C}^{(\cap)}_{st,pk}} \frac{1}{|\mathcal{C}|} \Big(\Pr\left[m \leftarrow\!\$\, M : m \in S_{st,pk}\right] \\ &\qquad - \Pr\left[m \leftarrow\!\$\, M : m \in S_{st,pk} \,|\, m \in C\right] \Big)^2 - \frac{4}{\phi} \mathsf{Adv}^{\Pi}_{\mathcal{M}\mathcal{R}}\end{aligned}$$

by the definition of $I^{(S)}$ in Lemma 4 and by the definition of $\mathcal{C}^{(\cap)}_{st,pk}$ in Lemma 8 we get

$$\begin{aligned}&\geq 2 \sum_{(st,pk) \in I} \Pr[(st,pk)] \sum_{C \in \mathcal{C}^{(\cap)}_{st,pk}} \frac{1}{|\mathcal{C}|} \\ &\qquad \underbrace{\left(\frac{\phi - \mathsf{Adv}^{\Pi}_{\mathcal{R}\mathcal{B}}}{2} - \frac{64}{(\phi - \mathsf{Adv}^{\Pi}_{\mathcal{R}\mathcal{B}})\phi^3} \mathsf{Adv}^{\Pi}_{\mathcal{M}\mathcal{R}} \right)^2}_{(*)} - \frac{4}{\phi} \mathsf{Adv}^{\Pi}_{\mathcal{M}\mathcal{R}}. \qquad (11)\end{aligned}$$

For the term $(*)$ we obtain the following bound by expanding the square and ignoring the squared terms:

$$\begin{aligned}(*) &= \frac{\phi^2}{4} - \frac{\phi \mathsf{Adv}^{\Pi}_{\mathcal{R}\mathcal{B}}}{2} + \left(\frac{\mathsf{Adv}^{\Pi}_{\mathcal{R}\mathcal{B}}}{2} \right)^2 - \frac{64 \mathsf{Adv}^{\Pi}_{\mathcal{M}\mathcal{R}}}{\phi^3} + \left(\frac{64 \mathsf{Adv}^{\Pi}_{\mathcal{M}\mathcal{R}}}{(\phi - \mathsf{Adv}^{\Pi}_{\mathcal{R}\mathcal{B}})\phi^3} \right)^2 \\ &\geq \frac{\phi^2}{4} - \frac{\phi \mathsf{Adv}^{\Pi}_{\mathcal{R}\mathcal{B}}}{2} - \frac{64 \mathsf{Adv}^{\Pi}_{\mathcal{M}\mathcal{R}}}{\phi^3}\end{aligned}$$

and therefore

$$\begin{aligned}(11) \geq 2 \sum_{(st,pk) \in I} \Pr[(st,pk)] \sum_{C \in \mathcal{C}^{(\cap)}_{st,pk}} \frac{1}{|\mathcal{C}|} \left(\frac{\phi^2}{4} - \frac{\phi}{2} \mathsf{Adv}^{\Pi}_{\mathcal{R}\mathcal{B}} - \frac{64}{\phi^3} \mathsf{Adv}^{\Pi}_{\mathcal{M}\mathcal{R}} \right) \\ - \frac{4}{\phi} \mathsf{Adv}^{\Pi}_{\mathcal{M}\mathcal{R}}\end{aligned}$$

Lemma 9 yields a bound on the size of $I = I^{(S)} \cap I^{(\cap)}_{\phi-\mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}}}$ while Lemma 8 gives a bound on the size of $\mathcal{C}^{(\cap)}_{st,pk}$. These facts combine to

$$\geq 2 \cdot \frac{\phi - \mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}}}{2} \cdot \frac{\phi}{8} \cdot \left(\frac{\phi^2}{4} - \frac{\phi}{2}\mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}} - \frac{64}{\phi^3}\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}} \right) - \frac{4}{\phi}\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}}$$
$$\geq \frac{\phi^4}{32} - \left(\frac{3\phi^3}{32}\mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}} + \frac{12}{\phi}\mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}} \right),$$

where the last inequality comes from discarding terms that contain products of advantages. Rearranging yields the result. □

Expanding denominators, upper-bounding $\phi \leq 1$, and using Proposition 1 stating equivalence of class-hiding and DDH, Theorem 1 implies the following:

Corollary 1. *For all EQS schemes Σ as defined in Sect. 2.3, for all computational problems Π and all reductions $\mathcal{R}$ that reduce Π to* UNF*, running the adversary once, with a reduction tightness of ϕ and running in time τ, there exist meta-reductions $\mathcal{D}$ attacking class-hiding of Σ running in time $\approx 2\tau$ and $\mathcal{M}$ attacking Π running in time $\approx \tau$ as well as an adversary $\mathcal{B}$ attacking* UNF *of Σ running in constant time such that*

$$\mathsf{Adv}^{CH}_{\Sigma,\mathcal{D}^{\mathcal{R}}} + \mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{B}}} + \mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}} \geq \frac{\phi^5}{384}.$$

Therefore in an asymptotic setting where Σ is class-hiding (CH) and adapts perfectly under malicious keys, and $\mathcal{R}$ is an efficient reduction reducing a "hard" problem Π to UNF, Corollary 1 states that $\mathcal{R}$'s tightness ϕ is bound by the sum of the advantages of efficient reductions. Because of the hardness of CH and Π, we get that these advantages are negligible. Therefore also ϕ must be negligible, which yields that $\mathcal{R}$ is not a "useful" reduction.

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]. The authors would like to thank the anonymous reviewers for their valuable comments and suggestions.

References

[ACdMT05] Ateniese, G., Chou, D.H., de Medeiros, B., Tsudik, G.: Sanitizable signatures. In: di Vimercati, S.C., Syverson, P., Gollmann, D. (eds.) ESORICS 2005. LNCS, vol. 3679, pp. 159–177. Springer, Heidelberg (2005). https://doi.org/10.1007/11555827_10

[AFG+10] Abe, M., Fuchsbauer, G., Groth, J., Haralambiev, K., Ohkubo, M.: Structure-preserving signatures and commitments to group elements. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 209–236. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_12

[AGHO11] Abe, M., Groth, J., Haralambiev, K., Ohkubo, M.: Optimal structure-preserving signatures in asymmetric bilinear groups. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 649–666. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22792-9_37

[AGO11] Abe, M., Groth, J., Ohkubo, M.: Separating short structure-preserving signatures from non-interactive assumptions. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 628–646. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_34

[BCC+09] Belenkiy, M., Camenisch, J., Chase, M., Kohlweiss, M., Lysyanskaya, A., Shacham, H.: Randomizable proofs and delegatable anonymous credentials. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 108–125. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03356-8_7

[BEK+20] Bobolz, J., Eidens, F., Krenn, S., Slamanig, D., Striecks, C.: Privacy-preserving incentive systems with highly efficient point-collection. In: Sun, H.-M., Shieh, S.-P., Gu, G., Ateniese, G. (eds.) ASIACCS 2020, October 2020, pp. 319–333. ACM Press (2020)

[BFPV13] Blazy, O., Fuchsbauer, G., Pointcheval, D., Vergnaud, D.: Short blind signatures. J. Comput. Secur. **21**(5), 627–661 (2013)

[BFR24] Bauer, B., Fuchsbauer, G., Regen, F.: On security proofs of existing equivalence class signature schemes. Cryptology ePrint Archive, Paper 2024/183 (2024). https://eprint.iacr.org/2024/183

[BHKS18] Backes, M., Hanzlik, L., Kluczniak, K., Schneider, J.: Signatures with flexible public key: introducing equivalence classes for public keys. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part II. LNCS, vol. 11273, pp. 405–434. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03329-3_14

[BJLS16] Bader, C., Jager, T., Li, Y., Schäge, S.: On the impossibility of tight cryptographic reductions. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016, Part II. LNCS, vol. 9666, pp. 273–304. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49896-5_10

[BLL+19] Bultel, X., Lafourcade, P., Lai, R.W.F., Malavolta, G., Schröder, D., Thyagarajan, S.A.K.: Efficient invisible and unlinkable sanitizable signatures. In: Lin, D., Sako, K. (eds.) PKC 2019, Part I. LNCS, vol. 11442, pp. 159–189. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17253-4_6

[BLS01] Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 514–532. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45682-1_30

[BRS23] Benhamouda, F., Raykova, M., Seth, K.: Anonymous counting tokens. IACR Cryptology ePrint Archive, p. 320 (2023, to appear at Asiacrypt 2023)

[BV98] Boneh, D., Venkatesan, R.: Breaking RSA may not be equivalent to factoring. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 59–71. Springer, Heidelberg (1998). https://doi.org/10.1007/BFb0054117

[CL03] Camenisch, J., Lysyanskaya, A.: A signature scheme with efficient protocols. In: Cimato, S., Persiano, G., Galdi, C. (eds.) SCN 2002. LNCS, vol. 2576, pp. 268–289. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-36413-7_20

[CL19] Crites, E.C., Lysyanskaya, A.: Delegatable anonymous credentials from mercurial signatures. In: Matsui, M. (ed.) CT-RSA 2019. LNCS, vol. 11405, pp. 535–555. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-12612-4_27

[CL21] Crites, E.C., Lysyanskaya, A.: Mercurial signatures for variable-length messages. In: PoPETs, vol. 2021, no. 4, pp. 441–463 (2021)

[CLPK22] Connolly, A., Lafourcade, P., Perez-Kempner, O.: Improved constructions of anonymous credentials from structure-preserving signatures on equivalence classes. In: Hanaoka, G., Shikata, J., Watanabe, Y. (eds.) Public-Key Cryptography, PKC 2022, Part I. LNCS vol. 13177, pp. 409–438. Springer, Heidelberg (2022). https://doi.org/10.1007/978-3-030-97121-2_15

[Cor00] Coron, J.-S.: On the exact security of full domain hash. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 229–235. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-44598-6_14

[Cor02] Coron, J.-S.: Optimal security proofs for PSS and other signature schemes. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 272–287. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-46035-7_18

[CS20] Clarisse, R., Sanders, O.: Group signature without random oracles from randomizable signatures. In: Nguyen, K., Wu, W., Lam, K.Y., Wang, H. (eds.) ProvSec 2020. LNCS, vol. 12505, pp. 3–23. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-62576-4_1

[DHO16] Damgård, I., Haagh, H., Orlandi, C.: Access control encryption: enforcing information flow with cryptography. In: Hirt, M., Smith, A. (eds.) TCC 2016. LNCS, vol. 9986, pp. 547–576. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53644-5_21

[DHS15] Derler, D., Hanser, C., Slamanig, D.: A new approach to efficient revocable attribute-based anonymous credentials. In: Groth, J. (ed.) IMACC 2015. LNCS, vol. 9496, pp. 57–74. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-27239-9_4

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

[DS18] Derler, D., Slamanig, D.: Highly-efficient fully-anonymous dynamic group signatures. In: Kim, J., Ahn, G.-J., Kim, S., Kim, Y., López, J., Kim, T. (eds.) ASIACCS 18, April 2018, pp. 551–565. ACM Press (2018)

[EHK+13] Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.: An algebraic framework for Diffie-Hellman assumptions. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 129–147. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40084-1_8

[EHK+17] Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.L.: An algebraic framework for Diffie-Hellman assumptions. J. Cryptol. **30**(1), 242–288 (2017)

[FF13] Fischlin, M., Fleischhacker, N.: Limitations of the meta-reduction technique: the case of Schnorr signatures. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 444–460. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38348-9_27

[FG18] Fuchsbauer, G., Gay, R.: Weakly secure equivalence-class signatures from standard assumptions. In: Abdalla, M., Dahab, R. (eds.) PKC 2018, Part II. LNCS, vol. 10770, pp. 153–183. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76581-5_6

[FGKO17] Fuchsbauer, G., Gay, R., Kowalczyk, L., Orlandi, C.: Access control encryption for equality, comparison, and more. In: Fehr, S. (ed.) PKC 2017, Part II. LNCS, vol. 10175, pp. 88–118. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-662-54388-7_4

[FHKS16] Fuchsbauer, G., Hanser, C., Kamath, C., Slamanig, D.: Practical round-optimal blind signatures in the standard model from weaker assumptions. In: Zikas, V., De Prisco, R. (eds.) SCN 2016. LNCS, vol. 9841, pp. 391–408. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-44618-9_21

[FHS15] Fuchsbauer, G., Hanser, C., Kamath, C., Slamanig, D.: Practical round-optimal blind signatures in the standard model from weaker assumptions. In: Zikas, V., De Prisco, R. (eds.) SCN 2016, Part II. LNCS, vol. 9841, pp. 391–408. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-44618-9_21

[FHS19] Fuchsbauer, G., Hanser, C., Slamanig, D.: Structure-preserving signatures on equivalence classes and constant-size anonymous credentials. J. Cryptol. **32**(2), 498–546 (2019)

[Fis06] Fischlin, M.: Round-optimal composable blind signatures in the common reference string model. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 60–77. Springer, Heidelberg (2006). https://doi.org/10.1007/11818175_4

[FJS14] Fleischhacker, N., Jager, T., Schröder, D.: On tight security proofs for Schnorr signatures. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014, Part I. LNCS, vol. 8873, pp. 512–531. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45611-8_27

[FP09] Fuchsbauer, G., Pointcheval, D.: Proofs on encrypted values in bilinear groups and an application to anonymity of signatures. In: Shacham, H., Waters, B. (eds.) Pairing 2009. LNCS, vol. 5671, pp. 132–149. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03298-1_10

[FS10] Fischlin, M., Schröder, D.: On the impossibility of three-move blind signature schemes. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 197–215. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_10

[Fuc11] Fuchsbauer, G.: Commuting signatures and verifiable encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 224–245. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20465-4_14

[GBL08] Garg, S., Bhaskar, R., Lokam, S.V.: Improved bounds on security reductions for discrete log based signatures. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 93–107. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85174-5_6

[Han23] Hanzlik, L.: Non-interactive blind signatures for random messages. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 722–752. Springer, Heidelberg (2023). https://doi.org/10.1007/978-3-031-30589-4_25

[HJK12] Hofheinz, D., Jager, T., Knapp, E.: Waters signatures with optimal security reduction. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 66–83. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30057-8_5

[HKKL07] Hazay, C., Katz, J., Koo, C.-Y., Lindell, Y.: Concurrently-secure blind signatures without random oracles or setup assumptions. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 323–341. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-70936-7_18

[HPP20] Hébant, C., Phan, D.H., Pointcheval, D.: Linearly-homomorphic signatures and scalable mix-nets. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020, Part II. LNCS, vol. 12111, pp. 597–627. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45388-6_21

[HRS15] Hanser, C., Rabkin, M., Schröder, D.: Verifiably encrypted signatures: security revisited and a new construction. In: Pernul, G., Ryan, P.Y.A., Weippl, E. (eds.) ESORICS 2015, Part I. LNCS, vol. 9326, pp. 146–164. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-24174-6_8

[HS14] Hanser, C., Slamanig, D.: Structure-preserving signatures on equivalence classes and their application to anonymous credentials. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014, Part I. LNCS, vol. 8873, pp. 491–511. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45611-8_26

[HS21] Hanzlik, L., Slamanig, D.: With a little help from my friends: constructing practical anonymous credentials. In: Vigna, G., Shi, E. (eds.) ACM CCS 2021, November 2021, pp. 2004–2023. ACM Press (2021)

[KK12] Kakvi, S.A., Kiltz, E.: Optimal security proofs for full domain hash, revisited. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 537–553. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_32

[KM19] Koblitz, N., Menezes, A.: Critical perspectives on provable security: fifteen years of "another look" papers. Cryptology ePrint Archive, Report 2019/1336 (2019). https://eprint.iacr.org/2019/1336

[KSD19] Khalili, M., Slamanig, D., Dakhilalian, M.: Structure-preserving signatures on equivalence classes from standard assumptions. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part III. LNCS, vol. 11923, pp. 63–93. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-34618-8_3

[Mau05] Maurer, U.: Abstract models of computation in cryptography. In: Smart, N.P. (ed.) Cryptography and Coding 2005. LNCS, vol. 3796, pp. 1–12. Springer, Heidelberg (2005). https://doi.org/10.1007/11586821_1

[MBG+23] Mir, O., Bauer, B., Griffy, S., Lysyanskaya, A., Slamanig, D.: Aggregate signatures with versatile randomization and issuer-hiding multi-authority anonymous credentials. In: Meng, W., Jensen, C.D., Cremers, C., Kirda, E. (eds.) ACM CCS 2023, pp. 30–44. ACM (2023)

[MSBM23] Mir, O., Slamanig, D., Bauer, B., Mayrhofer, R.: Practical delegatable anonymous credentials from equivalence class signatures. Proc. Priv. Enhancing Technol. **2023**(3), 488–513 (2023)

[Nao03] Naor, M.: On cryptographic assumptions and challenges. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 96–109. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-45146-4_6

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

[PS00] Pointcheval, D., Stern, J.: Security arguments for digital signatures and blind signatures. J. Cryptol. **13**(3), 361–396 (2000)

[PV05] Paillier, P., Vergnaud, D.: Discrete-log-based signatures may not be equivalent to discrete log. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 1–20. Springer, Heidelberg (2005). https://doi.org/10.1007/11593447_1

[Seu12] Seurin, Y.: On the exact security of Schnorr-type signatures in the Random Oracle Model. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 554–571. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_33

[Sho97] Shoup, V.: Lower bounds for discrete logarithms and related problems. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 256–266. Springer, Heidelberg (1997). https://doi.org/10.1007/3-540-69053-0_18

[ST21] Sanders, O., Traoré, J.: EPID with malicious revocation. In: Paterson, K.G. (ed.) CT-RSA 2021. LNCS, vol. 12704, pp. 177–200. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-75539-3_8

[Wat05] Waters, B.: Efficient identity-based encryption without Random Oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_7