Optimal Security Proofs for Signatures from Identification Schemes

Eike Kiltz[1], Daniel Masny[1], and Jiaxin Pan[1,2](✉)

[1] Ruhr-Universität Bochum, Bochum, Germany
{eike.kiltz,daniel.masny,jiaxin.pan}@rub.de
[2] Karlsruher Institut Für Technologie, Karlsruhe, Germany

Abstract. We perform a concrete security treatment of digital signature schemes obtained from canonical identification schemes via the Fiat-Shamir transform. If the identification scheme is random self-reducible and satisfies the weakest possible security notion (hardness of key-recoverability), then the signature scheme obtained via Fiat-Shamir is unforgeable against chosen-message attacks in the multi-user setting. Our security reduction is in the random oracle model and loses a factor of roughly Q_h, the number of hash queries. Previous reductions incorporated an additional multiplicative loss of N, the number of users in the system. Our analysis is done in small steps via intermediate security notions, and all our implications have relatively simple proofs. Furthermore, for each step, we show the optimality of the given reduction in terms of model assumptions and tightness.

As an important application of our framework, we obtain a concrete security treatment for Schnorr signatures in the multi-user setting.

Keywords: Signatures · Identification · Schnorr · Tightness

1 Introduction

Canonical Identification Schemes and the Fiat-Shamir Transform. A canonical identification scheme ID as formalized by Abdalla et al. [1] is a three-move public-key authentication protocol of a specific form. The prover (holding the secret-key) sends a commitment R to the verifier. The verifier (holding the public-key) returns a random challenge h, uniformly chosen from a set ChSet (of exponential size). The prover sends a response s. Finally, using the verification algorithm, the verifier publicly checks correctness of the transcript (R, h, s). There is a large number of canonical identification schemes known (e.g. [13,15,20,28,29,31,34,36,38,39,42], the most popular among them being the scheme by Schnorr [42]. The Fiat-Shamir method [20] transforms any such

E. Kiltz—Supported in part by ERC Project ERCC (FP7/615074). D. Masny—Supported by the DFG Research Training Group GRK 1817/1. J. Pan—Supported by the DFG Research Training Group GRK 1817/1 and by the DFG grant HO 4534/4-1.

M. Robshaw and J. Katz (Eds.): CRYPTO 2016, Part II, LNCS 9815, pp. 33–61, 2016.
DOI: 10.1007/978-3-662-53008-5_2

canonical identification scheme into a digital signature scheme $\mathsf{SIG}[\mathsf{ID}]$ using a hash function.

Digital Signatures in the Multi-User Setting. When it comes to security of digital signature schemes, in the literature almost exclusively the standard security notion of unforgeability against chosen message attacks ($\mathsf{UF\text{-}CMA}$) [30] is considered. This is a *single-user setting*, where an adversary obtains one single public-key and it is said to break the scheme's security if he can produce (after obtaining Q_s many signatures on messages of his choice) a valid forgery, i.e. a message-signature pair that verifies on the given public-key. However, in the real world the attacker is usually confronted with many public-keys and presumably he is happy if he can produce a valid forgery under any of the given public-keys. This scenario is captured in the *multi-user setting* for signatures schemes. Concretely, in multi-user unforgeability against chosen message attacks ($\mathsf{MU\text{-}UF\text{-}CMA}$) the attacker obtains N independent public-keys and is said to break the scheme's security if he can produce (after obtaining Q_s many signatures on public-keys of his choice) a valid forgery that verifies under any of the public-keys.

There are essentially two reasons why one typically only analyzes signatures in the single-user setting. First, the single-user security notion and consequently their analysis are simpler. Second, there exists a simple generic security reduction [25] between multi-user security and standard single-user security. Namely, for any signature system, attacking the scheme in the multi-user setting with N public-keys cannot increase the attacker's success ratio (i.e., the quotient of its success probability and its running time) by a factor more than N compared to attacking the scheme in the single-user setting. As the number of public-keys N is bounded by a polynomial, asymptotically, the single-user and the multi-user setting are equivalent. However, the security reduction is not tight: it has a loss of a non-constant factor N. This is clearly not satisfactory as in complex environments one can easily assume the existence of at least $N = 2^{30}$ ($\approx$ 1 billion) public-keys, thereby increasing the upper bound on the attacker's success ratio by a factor of 2^{30}. For example, if we assume the best algorithm breaking the single-user security having success ratio $\rho = 2^{-80}$, then it can only be argued that the best algorithm breaking the multi-user security has success ratio $\rho' = 2^{-80} \cdot 2^{30} = 2^{-50}$, which is not a safe security margin that defends against today's attackers.

Tightness. Generally, we call a security implication between two problems *tight* [9], if the success ratio ρ of any adversary attacking the first problem cannot decease by more than a small constant factor compared to the success ratio ρ' of any adversary attacking the second problem [7,26]. Here the success ratio ρ is defined as the quotient between the adversary's success probability and its running time. We note that this notion of tightness is slightly weaker than requiring that both, success probability and running time, cannot decrease by more than a small constant factor (called strong tightness in [26]). However, the main goal of a concrete security analysis is to derive parameters provably guaranteeing *k-bit security*. As the term *k-bit security* is commonly defined as the non-existence of any adversary that breaks the scheme with a success ratio better than 2^{-k} (see, e.g., [7,18]), our definition of tightness is sufficient for this purpose.

1.1 Our Contributions

This work contains a concrete and modular security analysis of signatures $\mathsf{SIG}[\mathsf{ID}]$ obtained via the Fiat-Shamir transform. Throughout this paper we assume that our identification schemes ID are Σ-protocols, i.e. they are honest-verifier zero-knowledge (HVZK), have special soundness (SS), and commitments R are sampled at random from a sufficiently large set. For some of our tight implications we furthermore require ID to be random self-reducible (RSR), a property we formally define in Definition 5. Most known canonical identification schemes satisfy the above properties.

Security Notions. For identification schemes we consider XXX-YYY security, where $\mathsf{XXX} \in \{\mathsf{KR}, \mathsf{IMP}, \mathsf{PIMP}\}$ denotes the attacker's goal and $\mathsf{YYY} \in \{\mathsf{KOA}, \mathsf{PA}\}$ the attacker's capabilities. If the attacker's goals defined as follows: in key-recovery (KR), it tries to compute a valid secret-key; in impersonation (IMP), it tries to impersonate a prover by convincing an honest verifier; parallel impersonation (PIMP) is a parallel version of IMP, where the adversary tries to convince a verifier in one of Q_{CH} many parallel sessions. The attacker's capabilities are defined as follows: in a key-only attack (KOA), the adversary is only given the public-key; in a passive attack (PA), the adversary is provided with valid transcripts between an honest prover and verifier. In total, we obtain $3 \times 2 = 6$ different security notions that were all previously considered in the literature [1,37,41], except PIMP-YYY security.

Overview. We show via a chain of implications that KR-KOA-security (the weakest possible security notion for ID where the adversary has to compute a secret-key from a given public-key without any further oracle access) implies multi-user unforgeability against chosen message attacks (MU-UF-CMA) of $\mathsf{SIG}[\mathsf{ID}]$. The diagram in Fig. 1 summarizes our results. All implications are optimal in terms of tightness and model requirements in the following sense. If one implication makes use of a special model requirement, we prove its impossibility without this requirement. For example, our implication PIMP-$\mathsf{KOA} \rightarrow \mathsf{UF}$-$\mathsf{KOA}$ requires the random oracle model [8] (with its well-known deficiencies [17]) and we show that the non-programmable random oracle model [22] is not sufficient to prove the same implication. Exactly one of our implications, namely IMP-$\mathsf{KOA} \rightarrow \mathsf{PIMP}$-$\mathsf{KOA}$ is non-tight, and we prove the impossibility of such a tight implication. We now discuss the implications from Fig. 1 in more detail.

From Identification to Single User Security for Signatures. Our first main theorem can be informally stated as follows.

Theorem 1. *If the identification scheme is* KR-KOA*-secure against any adversary having success ratio* ρ*, then* $\mathsf{SIG}[\mathsf{ID}]$ *is* UF-CMA*-secure in the random oracle model against any adversary having success ratio* $\rho' \approx \rho/Q_h$*, where* Q_h *is the maximal number of the adversary's random oracle queries.*

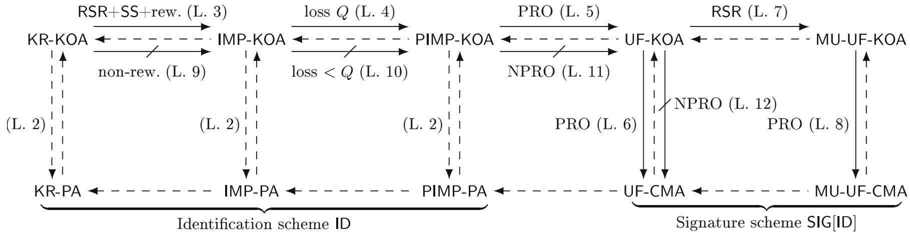


Fig. 1. Overview of our notions and results for canonical identification schemes ID and their implied signature schemes SIG[ID]. $\mathsf{X} \xrightarrow{\mathrm{Z}} \mathsf{Y}$ means that X-security implies Y-security under condition Z. Trivial implications are denoted with dashed arrows. All implications are tight except the one marked with "loss Q". The conditions are: rew. (reduction rewinds), loss Q (reduction loses a factor of Q), PRO (reduction is in the programmable random oracle model), SS (reduction uses special soundness), and RSR (reduction uses random self-reducibility for tightness). All implications from top to bottom require HVZK. $\mathsf{X} \overset{\mathrm{Z}}{\not\to} \mathsf{Y}$ means that X-security does not imply Y-security if only condition Z is fulfilled. The conditions are: non-rew. (reduction does not rewind), loss < Q (reduction loses a factor smaller than Q), and NPRO (reduction is in the non-programmable random oracle model).

The proof of this theorem is obtained by combining four independent Lemmas 3, 4, 5, and 6 via intermediate security notions IMP-KOA, PIMP-KOA, and UF-KOA[1] security, see Fig. 1. We certainly do not claim any novelty of the above lemmas, nor a new proof technique. For example, the implication IMP-KOA → UF-CMA is already explicitly contained in [37] (and implicitly in the seminal paper by Pointcheval and Stern [41]). However, by our specific choice of the intermediate security notions, all four proofs are simple and intuitive. In particular, unlike previous proofs, none of our proofs requires the full power of the Forking Lemma [5,41]. At the core of Lemma 3 (KR-KOA → IMP-KOA) we use a new Multi-Instance Reset Lemma (Lemma 1) which is a generalization of Bellare and Palacio's (Single-Instance) Reset Lemma [6] and may be of independent interest. The key to simplicity is the fact that IMP-KOA security only deals with one single impersonation session, which greatly simplifies the probability analysis. Even though the reduction uses rewinding, the RSR property makes the implication KR-KOA → IMP-KOA tight. We view identifying the intermediate security notions that allow for simple proofs as a conceptual contribution. Our result show that IMP-KOA and PIMP-KOA security can be seen as the *tightness barrier* for identification schemes in the sense that PIMP-KOA is the weakest of our notions for ID that is tightly equivalent to (multi-user) UF-CMA security of SIG[ID] in the random oracle model, whereas IMP-KOA is tightly equivalent to KR-KOA.

One particular advantage of our modular approach is that we are able to prove optimality of all four implications via meta-reductions (Lemmas 9, 10, 11, and 12). Lemma 10 proving the impossibility of a tight reduction between

[1] Unforgeability against key-only attack (UF-KOA security) is the same as standard UF-CMA security, but the adversary is not allowed to ask any signing query.

PIMP-KOA and IMP-KOA security is a generalization of Seurin's impossibility result to canonical identification schemes [43]; Lemmas 11 and 12 proving the impossibility of a reduction in the non-programmable random oracle model between PIMP-KOA, UF-KOA, and UF-CMA can be considered as a fine-grained version of a general impossibility result by Fukumitsu and Hasegawa [24] who only consider the implication IMP-PA → UF-CMA; All our impossibility results assume the reductions to be key-preserving [40] and are conditional in the sense that the existence of a reduction would imply that ID does not satisfy some other natural security property (that is believed to hold).

From Single-User to Multi-User Security for Signatures. Our second main theorem can be informally stated as follows.

Theorem 2. *If* ID *is* UF-KOA*-secure against any adversary having success ratio ρ, then it is* MU-UF-CMA*-secure in the random oracle model against any adversary having success ratio $\rho' \approx \rho/4$, independent of the number of users N in the multi-user scenario.*

This theorem improves the bound implied by previous generic reductions [25] by a factor of N. Following our modular approach, the theorem is proved in two steps via Lemmas 7 and 8. Lemma 7 proves that UF-KOA tightly implies MU-UF-KOA. Tightness stems from the RSR property, meaning that from a given public key pk we can derive properly distributed $pk_1, \ldots, pk_N$ such that any signature σ which is valid under pk can be transformed into a signature σ_i which is valid under pk_i and vice-versa.

Lemma 8 is our main technical contribution and proves MU-UF-KOA → MU-UF-CMA in the programmable random oracle model, again with a tight reduction. One is tempted to believe that it can be proved the same way as in the single user setting (i.e., the same way as UF-KOA → UF-CMA). In the single user setting, the reduction simulates signatures on m_j using the HVZK property to obtain a valid transcript (R_j, h_j, s_j) and programs the random oracle as $H(R_j, m_j) := h_j$. However, in the MU-UF-KOA experiment an adversary can ask for a signature under pk_1 on message m which makes the reduction program the random oracle $H(R_1, m) := h_1$. Now, if the adversary submits a forgery (R_1, s_2) under pk_2 on the same message m, the reduction cannot use this forgery to break the MU-UF-KOA experiment because the random oracle $H(R_1, m)$ was externally defined by the reduction. Hence, for the MU-UF-KOA experiment, $m, (R_1, s_2)$ does not constitute a valid forgery. In order to circumvent the above problem we make a simple probabilistic argument. In our reduction, about one half of the multi-user public-keys are coming from the MU-UF-KOA experiment, for the other half the reduction knows the corresponding secret-keys. Which secret-keys are known is hidden from the adversary's view. Now, if the multi-user adversary first obtains a signature on message m under pk_1 and then submits a forgery on the same message m under pk_2, the reduction hopes for the good case that one of the public-keys comes from the MU-UF-KOA experiment and the other one is known. This happens with probability $1/4$ which is precisely the loss of our new reduction.

1.2 Example Instantiations

Schnorr Signatures. One of the most important and signature schemes in the discrete logarithm setting is the Schnorr signature scheme [42]. It is obtained via the Fiat-Shamir transform applied to the Schnorr identification protocol. The recent expiry of the patent in 2008 has triggered a number of initiatives to obtain standardized versions of it.

Theorems 1 and 2 can be used to derive a concrete security bound for strong multi-user MU-UF-CMA-security of Schnorr signatures in the random oracle model from the DLOG problem.[2] Our reduction loses a factor of roughly Q_h, the number of random oracle queries. This improves previous bounds by a factor of N, the number of users in the system. We derive concrete example parameters for a provably secure instantiation. Figure 1 shows that DLOG is tightly equivalent to IMP-KOA-security and PIMP-KOA-security is tightly equivalent to MU-UF-CMA-security, meaning the tightness barrier for Schnorr lies precisely between IMP-KOA and PIMP-KOA security.

Katz-Wang Signatures. The Chaum-Pedersen identification scheme [19] is a double-generator version of Schnorr. It is at least as secure as Schnorr which means one cannot hope for a tight proof under the DLOG assumption. However, we can use a simple argument from [29,34] for a tight security proof of its PIMP-KOA security under the (stronger) Decision Diffie-Hellman Assumption. The resulting signature scheme is known as the Katz-Wang signature scheme [34] and our framework yields a tight proof of its strong MU-UF-CMA-security. Again, this improves previous bounds by a factor of N, the number of users in the system.

Guillou-Quisquater Signatures. Another canonical identification scheme of interest with the required properties is the one by Guillou-Quisquater [31]. Similar to Katz-Wang, for the Guillou-Quisquater scheme, we can use an argument from [2] for a tight proof of PIMP-KOA security under the Phi-hiding assumption. Alternatively, we can give a proof with loss Q_h under the Factoring assumption. Our framework also shows that this loss is unavoidable. Details are shown in the full version [35].

1.3 Related Work

Single-User Security. There have been many different works addressing the single-user security of Fiat-Shamir based signature schemes SIG[ID]. In pioneering work, Pointcheval and Stern [41] introduced the Forking Lemma as a tool to prove UF-CMA security of SIG[ID] from HVZK, SS and KR-KOA-security. Ohta and Okamoto [37] gave an alternative proof from IMP-KOA security and HVZK. Abdalla et al. [1] prove the equivalence of IMP-PA-security of ID and UF-CMA security of SIG[ID] in the random oracle model. All above results incorporate a

[2] We can even prove *strong* MU-UF-CMA security of Schnorr signatures in the sense that a new signature on a previously signed message already counts as a valid forgery.

security loss of at least Q_h and can be seen as a special case of our framework. Furthermore, [6] consider stronger security notions (e.g., IMP-AA and man-in-the middle security) for the Schnorr and GQ identification schemes. Abdalla et al. [3] show that lossy identification schemes tightly imply UF-CMA-secure signatures in the random oracle model from decisional assumptions. Our Multi-Instance Reset Lemma (Lemma 1) is a generalization to the Reset Lemma of Bellare and Palacio [6].

Multi-user security. To mitigate the generic security loss problem in the multi-user setting for the special case of Schnorr's signature scheme, Galbraith, Malone-Lee, and Smart (GMLS) proved [25] a tight reduction, namely that attacking the Schnorr signatures in the multi-user setting with N public-keys provably cannot decrease (by more than a small constant factor) the attacker's success ratio compared to attacking the scheme in the single-user setting. Unfortunately, Bernstein [11] recently pointed out an error in the GMLS proof leaving a tight security reduction for Schnorr signatures as an open problem. Even worse, Bernstein identifies an "apparently insurmountable obstacle to the claimed [GMLS] theorem". Section 4.3 of [11] further expands on the insurmountable obstacle. Our Theorem 2 shows there is such a tight security reduction for Schnorr signatures if one is willing to rely on the random oracle model. Additionally, in [35] we also prove an alternative tight reduction in the standard model which assumes *strong* UF-CMA security. (Schnorr is generally believed to be strongly UF-CMA secure and this is provably equivalent to UF-CMA security in the random oracle model.) Proving the original GMLS theorem (i.e., without random oracles and from standard UF-CMA security) remains an open problem.

Impossibility Results. In terms of impossibility results, Seurin [43], building on earlier work of [27,40], proves that there is no tight reduction from the (one-more) discrete logarithm assumption to UF-KOA-security of Schnorr signatures. A more recent result by [23] even excludes a reduction from any non-interactive assumption.[3] Fukumitsu and Hasegawa [24], generalizing earlier work on Schnorr signatures [21,40], prove that SIG[ID] cannot be proved secure in the non-programmable random oracle model only assuming IMP-PA security of ID.

Schnorr signatures vs. Key-Prefixed Schnorr signatures. After identifying the error in the GMLS proof, Bernstein [11] uses the lack of a tight security reduction for Schnorr's signature scheme as a motivation to promote a "key-prefixed" modification to Schnorr's signature scheme which includes the verifier's public-key in the hash function. The EdDSA signature scheme by Bernstein et al. [12] is essentially a key-prefixing variant of Schnorr's signature scheme. (In the context of security in a multi-user setting, key-prefixing was considered before, e.g., in [14].) In [12] key-prefixing is advertized as "an inexpensive way to alleviate concerns that several public keys could be attacked simultaneously." Indeed, Bernstein [11] proves that single-user security of the original

[3] The main result of the published paper [23] even excludes reduction from any *interactive* assumption (with special algebraic properties), but the proof turned out to be flawed.

Schnorr signatures scheme tightly implies multi-user security of the key-prefixed variant of the scheme. That is, the key-prefixed variant has the advantage of a standard model proof of its tight multi-user security, whereas for standard Schnorr signatures one has to assume strong security or rely on the random oracle model.

The TLS standard used to secure HTTPS connections is maintained by the Internet Engineering Task Force (IETF) which delegates research questions to the Internet Research Task Force (IRTF). Cryptographic research questions are usually discussed in the Crypto Forum Research Group (CFRG) mailing list. In the last months the CFRG discussed the issue of key-prefixing.

Key-prefixing comes with the disadvantage that the entire public-key has to be available at the time of signing. Specifically, in a CFRG message from September 2015 Hamburg [32] argues "having to hold the public key along with the private key can be annoying" and "can matter for constrained devices". Independent of efficiency, we believe that a cryptographic protocol should be as light as possible and prefixing (just as any other component) should only be included if its presence is justified. Naturally, in light of the GMLS proof, Hamburg [32] and Struik [44] (among others) recommended against key prefixing for Schnorr. Shortly after, Bernstein [10] identifies the error in the GMLS theorem and posts a tight security proof for the key-prefixed variant of Schnorr signatures. In what happens next, the participant of the CFRG mailing list switched their minds and mutually agree that key-prefixing should be preferred, despite of its previously discussed disadvantages. Specifically, Brown writes about Schnorr signatures that "this justifies a MUST for inclusion of the public key in the message of the classic signature" [16]. As a consequence, key-prefixing is contained in the current draft for EdDSA [33]. In the light of our new results, we recommend to reconsider this decision.

2 Definitions

2.1 Preliminaries

For an integer p, define $[p] := \{1, \ldots, p\}$ and $\mathbb{Z}_p$ as the residual ring $\mathbb{Z}/p\mathbb{Z}$. If A is a set, then $a \overset{\boxdot}{\leftarrow} A$ denotes picking a from A according to the uniform distribution. All our algorithms are probabilistic polynomial time unless stated otherwise. If A is an algorithm, then $a \overset{\boxdot}{\leftarrow} \mathsf{A}$ denotes the random variable which is defined as the output of $\mathcal{A}$ on input b. To make the randomness explicit, we use the notation $a := (A)(b; \rho)$ meaning that the algorithm is executed on input b and randomness ρ. Note that A's execution is now deterministic.

2.2 Canonical Identification Schemes

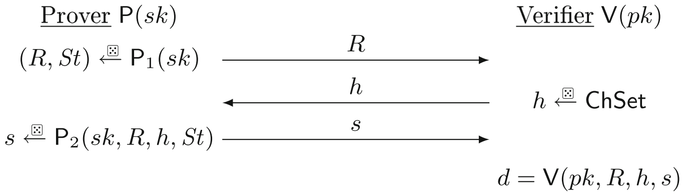
A canonical identification scheme ID is a three-move protocol of the form depicted in Fig. 2. The prover's first message R is called *commitment*, the verifier selects a uniform *challenge* h from set ChSet, and, upon receiving a *response* s from the prover, makes a deterministic decision.

Definition 1 (Canonical Identification Scheme). *A canonical identification scheme* ID *is defined as a tuple of algorithms* $\mathsf{ID} := (\mathsf{IGen}, \mathsf{P}, \mathsf{ChSet}, \mathsf{V})$.

- *The key generation algorithm* IGen *takes system parameters* par *as input and returns public and secret key* (pk, sk). *We assume that* pk *defines* ChSet, *the set of challenges.*
- *The prover algorithm* $\mathsf{P} = (\mathsf{P}_1, \mathsf{P}_2)$ *is split into two algorithms.* P_1 *takes as input the secret key* sk *and returns a commitment* R *and a state* St; P_2 *takes as input the secret key* sk, *a commitment* R, *a challenge* h, *and a state* St *and returns a response* s.
- *The verifier algorithm* V *takes the public key* pk *and the conversation transcript as input and outputs a* deterministic decision, *1 (acceptance) or 0 (rejection).*

We require that for all $(pk, sk) \in \mathsf{IGen}(\mathsf{par})$, *all* $(R, St) \in \mathsf{P}_1(sk)$, *all* $h \in \mathsf{ChSet}$ *and all* $s \in \mathsf{P}_2(sk, R, h, St)$, *we have* $\mathsf{V}(pk, R, h, s) = 1$.

We make a couple of useful definitions. An identification scheme ID is called *unique* if for all $(pk, sk) \in \mathsf{IGen}(\mathsf{par})$, $(R, St) \in \mathsf{P}_1(sk)$, $h \in \mathsf{ChSet}$, there exists at most one response $s \in \{0,1\}^*$ such that $\mathsf{V}(pk, R, h, s) = 1$. A *transcript* is a three-tuple (R, h, s). It is called *valid* (with respect to public-key pk) if $\mathsf{V}(pk, R, h, s) = 1$. Furthermore, it is called *real*, if it is the output of a real interaction between prover and verifier as depicted in Fig. 2. A canonical identification schemes ID has α *bits of min-entropy*, if for all $(pk, sk) \in \mathsf{IGen}(\mathsf{par})$, the commitment generated by the prover algorithm is chosen from a distribution with at least α bits of min-entropy. That is, for all strings R' we have $\Pr[R = R'] \le 2^{-\alpha}$, if $(R, St) \overset{\$}{\leftarrow} \mathsf{P}_1(sk)$ was honestly generated by the prover.



Prover $\mathsf{P}(sk)$
Verifier $\mathsf{V}(pk)$
$(R, St) \overset{\$}{\leftarrow} \mathsf{P}_1(sk)$
R
h
$h \overset{\$}{\leftarrow} \mathsf{ChSet}$
$s \overset{\$}{\leftarrow} \mathsf{P}_2(sk, R, h, St)$
s
$d = \mathsf{V}(pk, R, h, s)$

Fig. 2. A canonical identification scheme and its transcript (R, h, s).

We now define (parallel) impersonation against key-only attack (KOA), passive attack (PA), and active attack (AA).

Definition 2 ((Parallel) Impersonation). *Let* $\mathsf{YYY} \in \{\mathsf{KOA}, \mathsf{PA}, \mathsf{AA}\}$. *A canonical identification* ID *is said to be* $(t, \varepsilon, Q_{\mathrm{CH}}, Q_{\mathrm{O}})$-$\mathsf{PIMP}$-$\mathsf{YYY}$ *secure (parallel impersonation against* YYY *attacks) if for all adversaries* $\mathcal{A}$ *running in time at most* t *and making at most* Q_{CH} *queries to the challenge oracle* CH *and* Q_{O} *queries to oracle* O,

$$\Pr\left[\mathsf{V}(pk, R_{i^*}, h_{i^*}, s_{i^*}) = 1 \wedge\ i^* \in [Q_{\mathrm{CH}}] \;\middle|\; \begin{array}{l} (pk, sk) \xleftarrow{\$} \mathsf{IGen}(\mathsf{par}) \\ St \xleftarrow{\$} \mathcal{A}^{\mathrm{O}(\cdot)}(pk) \\ (i^*, s_{i^*}) \xleftarrow{\$} \mathcal{A}^{\mathrm{CH}(\cdot)}(pk) \end{array}\right] \le \varepsilon,$$

where on the i-th query $\mathrm{CH}(R_i)$ *(*$i \in [Q_{\mathrm{CH}}]$*), the challenge oracle returns* $h_i \xleftarrow{\$} \mathsf{ChSet}$ *to* $\mathcal{A}$*.*[4] *Depending on* YYY*, oracle* O *is defined as follows.*

- *If* $\mathsf{YYY} = \mathsf{KOA}$ *(key-only attack), then* O *always returns* $\perp$*.*
- *If* $\mathsf{YYY} = \mathsf{PA}$ *(passive attack), then* $\mathrm{O} := \mathrm{TRAN}$*, where on the j-th empty query* $\mathrm{TRAN}(\epsilon)$ *(*$j \in Q_{\mathrm{O}}$*), the transcript oracle returns a real transcript* (R'_j, h'_j, s'_j) *to* $\mathcal{A}$*, where* $(R'_j, St'_j) \xleftarrow{\$} \mathsf{P}_1(sk)$*,* $h'_j \xleftarrow{\$} \mathsf{ChSet}$*;* $s'_j \xleftarrow{\$} \mathsf{P}_2(sk, R'_j, h'_j, St'_j)$*.*
- *If* $\mathsf{YYY} = \mathsf{AA}$ *(active attack), then* $\mathrm{O} := \mathrm{PROVER} = (\mathrm{PROVER}_1, \mathrm{PROVER}_2)$*, where on the j-th query* $\mathrm{PROVER}_1(\epsilon)$ *(*$j \in Q_{\mathrm{O}}$*), the prover oracle returns* R'_j *for* $(R'_j, St'_j) \xleftarrow{\$} \mathsf{P}_1(sk)$ *to* $\mathcal{A}$*; on query* $\mathrm{PROVER}_2(j, h'_j)$*, the oracle returns* $s'_j \xleftarrow{\$} \mathsf{P}_2(sk, R'_j, h'_j, St'_j)$*, if* R'_j *is already defined (and* $\perp$ *otherwise).*

If $\mathsf{YYY} = \mathsf{KOA}$*, then the parameter* Q_{O} *is not used and we simply speak of* $(t, \varepsilon, Q_{\mathrm{CH}})$-$\mathsf{PIMP}$-$\mathsf{KOA}$*. Moreover,* $(t, \varepsilon, Q_{\mathrm{O}})$-$\mathsf{IMP}$-$\mathsf{YYY}$ *(*impersonation against YYY attack*) security is defined as* $(t, \varepsilon, 1, Q_{\mathrm{O}})$-$\mathsf{PIMP}$-$\mathsf{YYY}$ *security, i.e., the adversary is only allowed* $Q_{\mathrm{CH}} = 1$ *query to the* CH *oracle.*

Definition 3 (Key-recovery). *Let* $\mathsf{YYY} \in \{\mathsf{KOA}, \mathsf{PA}, \mathsf{AA}\}$*. A canonical identification* ID *is said to be* (t, ε)-KR-YYY *secure (key recovery under* YYY *attack) if for all adversaries* $\mathcal{A}$ *running in time at most* t*,*

$$\Pr\left[(sk^*, pk) \in \mathsf{IGen}(\mathsf{par}) \;\middle|\; \begin{array}{l} (pk, sk) \xleftarrow{\$} \mathsf{IGen}(\mathsf{par}) \\ sk^* \xleftarrow{\$} \mathcal{A}^{\mathrm{O}(\cdot)}(pk) \end{array}\right] \le \varepsilon,$$

where depending on YYY *oracle* O *is defined as in Definition 2. The winning condition* $(sk^*, pk) \in \mathsf{IGen}(\mathsf{par})$ *means that the tuple* (sk^*, pk) *is in the support of* $\mathsf{IGen}(\mathsf{par})$*, i.e., that* $\mathcal{A}$ *outputs a valid secret-key* sk^* *with respect to* pk*.*

Definition 4 (Special Soundness). *A canonical identification* ID *is said to be* SS *(special sound) if there exists an extractor algorithm* Ext *such that, for all* $(pk, sk) \in \mathsf{IGen}(\mathsf{par})$*, given any two accepting transcripts* (R, h, s) *and* (R, h', s') *(where* $h \neq h'$*), we have* $\Pr[(sk^*, pk) \in \mathsf{IGen}(\mathsf{par}) \mid sk^* \xleftarrow{\$} \mathsf{Ext}(pk, R, h, s, h', s')] = 1$*.*

Definition 5 (Random Self-reducibility). *A canonical identification* ID *is said to be* RSR *(random self-reducible) if there is an algorithm* Rerand *and two deterministic algorithms* Tran *and* Derand *such that, for all* $(pk, sk) \in \mathsf{IGen}(\mathsf{par})$*:*

- pk' *and* pk'' *have the same distribution, where* $(pk', \tau') \xleftarrow{\$} \mathsf{Rerand}(pk)$ *is the rerandomized key-pair and* $(pk'', sk'') \xleftarrow{\$} \mathsf{IGen}(\mathsf{par})$ *is a freshly generated key-pair.*

[4] On two queries $\mathrm{CH}(R_i)$ and $\mathrm{CH}(R_{i'})$ with the same input $R_i = R_{i'}$ the oracle returns two independent random challenges $h_i \xleftarrow{\$} \mathsf{ChSet}$ and $h_{i'} \xleftarrow{\$} \mathsf{ChSet}$.

- *For all* $(pk', \tau') \in \mathsf{Rerand}(pk)$*, all* $(pk', sk') \in \mathsf{IGen}(\mathsf{par})$*, and* $sk^* = \mathsf{Derand}(pk, pk', sk', \tau')$*, we have* $(pk, sk^*) \in \mathsf{IGen}(\mathsf{par})$*, i.e.,* Derand *returns a valid secret-key* sk^* *with respect to* pk*, given any valid* sk' *for* pk'*.*
- *For all* $(pk', \tau') \in \mathsf{Rerand}(pk)$*, all transcripts* (R', h', s') *that are valid with respect to* pk'*, the transcript* $(R', h', s := \mathsf{Tran}(pk, pk', \tau', (R', h', s')))$ *is valid with respect to* pk*.*

Definition 6 (Honest-verifier Zero-knowledge). *A canonical identification* ID *is said to be (perfect)* HVZK *(honest-verifier zero-knowledge) if there exists an algorithm* Sim *that, given public key* pk*, outputs* (R, h, s) *such that* (R, h, s) *is a real (i.e., properly distributed) transcript with respect to* pk*.*

2.3 Digital Signatures

We now define syntax and security of a digital signature scheme. Let par be common system parameters shared among all participants.

Definition 7 (Digital Signature). *A digital signature scheme* SIG *is defined as a triple of algorithms* $\mathsf{SIG} = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$*.*

- *The key generation algorithm* $\mathsf{Gen}(\mathsf{par})$ *returns the public and secret keys* (pk, sk)*.*
- *The signing algorithm* $\mathsf{Sign}(sk, m)$ *returns a signature* σ*.*
- *The deterministic verification algorithm* $\mathsf{Ver}(pk, m, \sigma)$ *returns 1 (accept) or 0 (reject).*

We require that for all $(pk, sk) \in \mathsf{Gen}(\mathsf{par})$*, all messages* $m \in \{0,1\}^*$*, we have* $\mathsf{Ver}(pk, m, \mathsf{Sign}(sk, m)) = 1$*.*

Definition 8 (Multi-user Security). *A signature scheme* SIG *is said to be* (t, ε, N, Q_s)*-*$\mathsf{MU\text{-}SUF\text{-}CMA}$ *secure (multi-user strongly unforgeable against chosen message attacks) if for all adversaries* $\mathcal{A}$ *running in time at most* t *and making at most* Q_s *queries to the signing oracle,*

$$\Pr\left[\begin{array}{l|l} \mathsf{Ver}(pk_{i^*}, m^*, \sigma^*) = 1 & \textit{For } i = 1, \ldots, N : (pk_i, sk_i) \stackrel{\$}{\leftarrow} \mathsf{Gen}(\mathsf{par}) \\ \wedge\ (i^*, m^*, \sigma^*) \notin \{(i_j, m_j, \sigma_j) \mid j \in [Q_s]\} & (i^*, m^*, \sigma^*) \stackrel{\$}{\leftarrow} \mathcal{A}^{\textsc{Sign}(\cdot,\cdot)}(pk_1, \ldots, pk_N) \end{array}\right] \leq \varepsilon,$$

where on the j*-th query* $(i_j, m_j) \in [N] \times \{0,1\}^*$ *(*$j \in [Q_s]$*) the signing oracle* $\textsc{Sign}$ *returns* $\sigma_j \stackrel{\$}{\leftarrow} \mathsf{Sign}(sk_{i_j}, m_j)$ *to* $\mathcal{A}$*, i.e., a signature on message* m_j *under public-key* pk_{i_j}*.*

We stress that an adversary in particular breaks multi-user security if he asks for a signature on message m under pk_1 and submits a valid forgery on the same message m under pk_2.

The first condition in the probability statement of Definition 8 is called the correctness condition, the second condition is called the freshness condition. Definition 8 covers *strong* security in the sense that a new signature on a previously queried message is considered as a fresh forgery. For standard (non-strong) MU-UF-CMA security (multi-user unforgeablility against chosen message attack) we modify the freshness condition in the experiment to $(i^*, m^*) \notin \{(i_j, m_j,) \mid j \in [Q_s]\}$, i.e., to break the scheme the adversary has to come up with a signature on a message-key pair which has not been queried to the signing oracle. We also define (t, ε, N)-MU-UF-KOA security (multi-user unforgeability against key only attack) as $(t, \varepsilon, N, 0)$-MU-UF-CMA security, i.e. $Q_s = 0$, the adversary is not allowed to make any signing query.

Definition 9 (Single-user Security). *In the single-user setting, i.e. $N = 1$ users, (t, ε, Q_s)-*SUF-CMA *security (strong unforgeablility against chosen message attacks) is defined as $(t, \varepsilon, 1, Q_s)$-*MU-SUF-CMA *security. Similarly, standard (non-strong) (t, ε, Q_s)-*UF-CMA *security (unforgeablility against chosen message attack) is defined as $(t, \varepsilon, 1, Q_s)$-*MU-UF-CMA *security. Further, (t, ε)-*UF-KOA *security (unforgeablility against key-only attack) is defined as $(t, \varepsilon, 1, 0)$-*MU-SUF-CMA *security, i.e., $N = 1$ users and $Q_s = 0$ signing queries.*

Security in the random oracle model. The security of identification and signature schemes containing a hash function can be analyzed in the random oracle model [8]. In this model hash values can only be accessed by an adversary through queries to an oracle H. On input x this oracle returns a uniformly random output $H(x)$ which is consistent with previous queries for input x. Using the random oracle model, the maximal number of queries to H becomes a parameter in the concrete security notions. For example, for $(t, \varepsilon, N, Q_s, Q_h)$-MU-SUF-CMA security we consider all adversaries making at most Q_h queries to the random oracle. We make the convention that each query to the random oracle made during a signing query is counted as the adversary's random oracle query, meaning $Q_h \geq Q_s$.

2.4 Signatures from Identification Schemes

Let $\mathsf{ID} := (\mathsf{IGen}, \mathsf{P}, \mathsf{ChSet}, \mathsf{V})$ be a canonical identification scheme. By the generalized Fiat-Shamir transformation [6], the signature scheme $\mathsf{SIG}[\mathsf{ID}] := (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ from ID is defined as follows. par contains the system parameters of ID and a hash function $H : \{0,1\}^* \to \mathsf{ChSet}$.

```
Gen(par):
  $(pk, sk) \stackrel{\$}{\leftarrow} \mathsf{IGen}(\mathsf{par})$
  Return $(pk, sk)$

Sign$(sk, m)$:
  $(R, St) \stackrel{\$}{\leftarrow} \mathsf{P}_1(sk)$
  $h = H(R, m)$
  $s \stackrel{\$}{\leftarrow} \mathsf{P}_2(sk, R, h, St)$
  Return $\sigma = (R, s)$

Ver$(sk, m, \sigma)$:
  Parse $\sigma = (R, s)$
  $h = H(R, m)$
  Return $\mathsf{V}(pk, R, h, s)$
```

In some variants of the Fiat-Shamir transform, the hash additionally inputs some public parameters, for example $h = H(pk, R, m)$.

We call ID *commitment-recoverable*, if $\mathsf{V}(pk, R, h, s)$ first recomputes $R' = \mathsf{V}'(pk, h, s)$ and then outputs 1 iff $R' = R$. For commitment-recoverable

ID, we can define an alternative Fiat-Shamir transformation $\mathsf{SIG}'[\mathsf{ID}] := (\mathsf{Gen}, \mathsf{Sign}', \mathsf{Ver}')$, where Gen is as in $\mathsf{SIG}[\mathsf{ID}]$. Algorithm $\mathsf{Sign}'(sk, m)$ is defined as $\mathsf{Sign}(sk, m)$ with the modified output $\sigma' = (h, s)$. Algorithm $\mathsf{Ver}'(pk, m, \sigma')$ first parses $\sigma' = (h, s)$, then recomputes the commitment as $R' := \mathsf{V}'(pk, h, s)$, and finally returns 1 iff $H(R', m) = h$.

Since $\sigma = (R, s)$ can be publicly transformed into $\sigma' = (h, s)$ and vice-cersa, $\mathsf{SIG}[\mathsf{ID}]$ and $\mathsf{SIG}'[\mathsf{ID}]$ are equivalent in terms of security. On the one hand, the alternative Fiat-Shamir transform yields shorter signatures if $h \in \mathsf{ChSet}$ has a smaller representation size than response s. On the other hand, signatures of the Fiat-Shamir transform maintain their algebraic structure which in some cases enables useful properties such as batch verification.

3 Security Implications

In this section we will prove the following two main results.

Theorem 3 (Main Theorem 1). *Suppose* ID *is* SS, HVZK, RSR *and has* α *bit min-entropy. If* ID *is* (t, ε)-$\mathsf{KR\text{-}KOA}$ *secure then* $\mathsf{SIG}[\mathsf{ID}]$ *is* $(t', \varepsilon', Q_s, Q_h)$-$\mathsf{UF\text{-}CMA}$-*secure and* $(t'', \varepsilon'', N, Q_s, Q_h)$-$\mathsf{MU\text{-}UF\text{-}CMA}$-*secure in the programmable random oracle model, where*

$$\frac{\varepsilon'}{t'} \leq 6(Q_h + 1) \cdot \frac{\varepsilon}{t} + \frac{Q_s}{2^\alpha} + \frac{1}{|\mathsf{ChSet}|},$$
$$\frac{\varepsilon''}{t''} \leq 24(Q_h + 1) \cdot \frac{\varepsilon}{t} + \frac{Q_s}{2^\alpha} + \frac{1}{|\mathsf{ChSet}|}.$$

The proof of Theorem 3 is obtained by combining Lemmas 3–8 below and using $Q_h \leq t' - 1$.

Theorem 4 (Main Theorem 2). *Suppose* $\mathsf{SIG}[\mathsf{ID}]$ *is* HVZK, RSR *and has* α *bit min-entropy. If* $\mathsf{SIG}[\mathsf{ID}]$ *is* $(t, \varepsilon, Q_h + Q_s)$-$\mathsf{UF\text{-}KOA}$ *secure then* $\mathsf{SIG}[\mathsf{ID}]$ *is* $(t', \varepsilon', N, Q_s, Q_h)$-$\mathsf{MU\text{-}UF\text{-}CMA}$ *secure in the programmable random oracle model, where*

$$\varepsilon' \leq 4\varepsilon + \frac{Q_h Q_s}{2^\alpha}, \qquad t' \approx t$$

and Q_s, Q_h *are upper bounds on the number of signing and hash queries in the* $\mathsf{MU\text{-}UF\text{-}CMA}$ *experiment, respectively.*

The proof of Theorem 4 is obtained by combining Lemmas 7 and 8 below.

Here we present the proofs of Lemmas 1 and 3 (a new Multi-Instance Reset Lemma and an application of it), Lemmas 7 and 8 (the implication of "UF-KOA → MU-UF-CMA"), which are the main contributions of this paper. All remaining proofs are deferred to [35].

3.1 Multi-Instance Reset Lemma

We first state a new reset lemma that we will later use in the proof of Theorem 3. It is presented in the style of Bellare and Neven's General Forking Lemma [5] and does not talk about signatures or identification protocols. It is a generalization to many parallel instances of the Reset Lemma [6], which is obtained by setting $N = 1$.

Lemma 1 (Multi-Instance Reset Lemma). *Fix an integer $N \geq 1$ and a non-empty set H. Let $\mathcal{C}$ be a randomized algorithm that on input (I, h) returns a pair (b, σ), where b is a bit and σ is called the side output. Let IG be a randomized algorithm that we call the input generator. The accepting probability of $\mathcal{C}$ is defined as*

$$\mathsf{acc} := \Pr[b = 1 \mid I \xleftarrow{\$} \mathsf{IG}; h \xleftarrow{\$} H; (b, \sigma) \xleftarrow{\$} \mathcal{C}(I, h)]$$

The (multi-instance) reset algorithm $\mathcal{R}_{\mathcal{C}}$ associated to $\mathcal{C}$ is the randomized algorithm that takes input $I_1, \ldots, I_N$ and proceeds as follows.

```
Algorithm $\mathcal{R}_{\mathcal{C}}(I_1, \ldots, I_N)$:
For $i \in [N]$:
    Pick random coins $\rho_i$
    $h_i \xleftarrow{\$} H$
    $(b_i, \sigma_i) \xleftarrow{\$} \mathcal{C}(I_i, h_i; \rho_i)$
If $b_1 = \ldots = b_N = 0$ then return $(0, \epsilon, \epsilon)$        // Abort in Phase 1
Fix $i^* \in [N]$ such that $b_{i^*} = 1$
For $j \in [N]$:
    $h'_j \xleftarrow{\$} H$
    $(b'_j, \sigma'_j) \xleftarrow{\$} \mathcal{C}(I_{i^*}, h'_j; \rho_{i^*})$
If $\exists j^* \in [N] : (h_{i^*} \neq h'_{j^*}$ and $b'_{j^*} = 1)$ then return $(i^*, \sigma_{i^*}, \sigma'_{j^*})$
Else return $(0, \epsilon, \epsilon)$                                   // Abort in Phase 2
```

Let $\mathsf{res} := \Pr[i^* \geq 1 \mid I_1, \ldots, I_N \xleftarrow{\$} \mathsf{IG}; (i^*, \sigma, \sigma') \xleftarrow{\$} \mathcal{R}_{\mathcal{C}}(I_1, \ldots, I_N)]$. *Then*

$$\mathsf{res} \geq \left(1 - \left(1 - \mathsf{acc} + \frac{1}{|H|}\right)^N\right)^2 .$$

Proof. For fixed instance I and coins ρ, we define the probabilities

$$\mathsf{acc}(I, \rho) := \Pr_{h \xleftarrow{\$} H}[b = 1 \mid (b, \sigma) \xleftarrow{\$} \mathcal{A}(I, h; \rho)],$$

$$\mathsf{res}(I, \rho) := \Pr_{h, h' \xleftarrow{\$} H}\left[b = 1 \wedge b' = 1 \wedge h \neq h' \,\middle|\, \begin{array}{l}(b, \sigma) \xleftarrow{\$} \mathcal{A}(I, h; \rho); \\ (b', \sigma') \xleftarrow{\$} \mathcal{A}(I, h'; \rho)\end{array}\right].$$

As for fixed I, ρ, the two events $b = 1$ and $b' = 1$ are independent and we obtain

$$\mathsf{res}(I, \rho) \geq \mathsf{acc}(I, \rho) \cdot \left(\mathsf{acc}(I, \rho) - \frac{1}{|H|}\right), \tag{1}$$

where the additive factor $\frac{1}{|H|}$ accounts for the fact that $\Pr[h' = h] = 1/|H|$. With the expectation taken over $I \overset{⚄}{\leftarrow} \mathsf{IG}$ and random coins ρ, we bound

$$\begin{aligned}\mathsf{E}_{I,\rho}\left[\mathsf{res}(I, \rho)\right] &\geq \mathsf{E}_{I,\rho}\left[\mathsf{acc}(I, \rho) \cdot \left(\mathsf{acc}(I, \rho) - \frac{1}{|H|}\right)\right] \\ &\geq \mathsf{E}_{I,\rho}[\mathsf{acc}(I, \rho)] \cdot \left(\mathsf{E}_{I,\rho}[\mathsf{acc}(I, \rho)] - \frac{1}{|H|}\right) \\ &= \mathsf{acc}\left(\mathsf{acc} - \frac{1}{|H|}\right).\end{aligned}$$

Above, we used (1), Jensen's inequality[5] applied to the convex function $\varphi(X) := X \cdot (X - 1/|H|)$, and the fact that $\mathsf{acc} = \mathsf{E}_{I,\rho}[\mathsf{acc}(I, \rho)]$.

Next, consider the random variables b_{i^*} and b'_j ($j \in [N]$) as defined during in the execution of $\mathcal{R}_{\mathcal{A}}(I_1, \ldots, I_N)$. Using $\mathsf{acc} = \Pr[b_{i^*} = 1]$ and $\Pr[b'_j = 1 \wedge b_{i^*} = 1] = \mathsf{E}_{I_{i^*}, \rho_{i^*}}\left[\mathsf{res}(I_{i^*}, \rho_{i^*})\right]$, we obtain

$$\Pr[b'_j = 1 \mid b_{i^*} = 1] = \frac{\Pr[b'_j = 1 \wedge b_{i^*} = 1]}{\Pr[b_{i^*} = 1]} \geq \mathsf{acc} - \frac{1}{|H|}.$$

Finally, we bound

$$\begin{aligned}\Pr[\text{no abort in phase 2} \mid \text{no abort in phase 1}] &= 1 - \prod_{j=1}^{N}(1 - \Pr[b'_j = 1 \mid b_{i^*} = 1]) \\ &\geq 1 - \left(1 - \mathsf{acc} + \frac{1}{|H|}\right)^N,\end{aligned}$$

and

$$\Pr[\text{no abort in phase 1}] = 1 - \prod_{i=1}^{N}(1 - \Pr[b_i = 1]) = 1 - (1 - \mathsf{acc})^N$$

to establish

$$\mathsf{res} = \Pr[\text{no abort in phase 1} \wedge \text{no abort in phase 2}] \geq (1 - (1 - \mathsf{acc} + \frac{1}{|H|})^N)^2.$$

This completes the proof. □

[5] Jensen's inequality states that if φ is a convex function and X is a random variable, then $\mathsf{E}[\varphi(X)] \geq \varphi(\mathsf{E}[X])$.

3.2 Proof of the Main Theorems

Lemma 2 ($\mathsf{XXX\text{-}KOA} \to \mathsf{XXX\text{-}PA}$)**.** *Let* $\mathsf{XXX} \in \{\mathsf{KR}, \mathsf{IMP}, \mathsf{PIMP}\}$. *If* ID *is* $(t, \varepsilon, Q_{\mathrm{CH}})$-$\mathsf{XXX\text{-}KOA}$ *secure and* HVZK*, then* ID *is* $(\approx t, \varepsilon, Q_{\mathrm{CH}}, Q_{\mathrm{O}})$-$\mathsf{XXX\text{-}PA}$ *secure.*

The proof is given in the full version [35].

Lemma 3 below proving that $\mathsf{KR\text{-}KOA}$ tightly implies $\mathsf{IMP\text{-}KOA}$ uses the Multi-Instance Reset Lemma and that takes advantage of ID's random self-reducibility (RSR).

Lemma 3 ($\mathsf{KR\text{-}KOA} \xrightarrow{\textbf{rewinding}} \mathsf{IMP\text{-}KOA}$)**.** *If* ID *is* (t, ε)-$\mathsf{KR\text{-}KOA}$ *secure,* SS *and* RSR*, then* ID *is* (t', ε')-$\mathsf{IMP\text{-}KOA}$ *secure, where for any* $N \geq 1$*,*

$$\varepsilon \geq (1 - (1 - \varepsilon' + \frac{1}{|\mathsf{ChSet}|})^N)^2, \quad t \approx 2Nt'. \tag{2}$$

In particular, the two success ratios are related as

$$\frac{\varepsilon'}{t'} - \frac{1}{t'|\mathsf{ChSet}|} \leq 6 \cdot \frac{\varepsilon}{t}. \tag{3}$$

We remark that without RSR, we can still obtain the weaker bounds $\varepsilon \geq \varepsilon'(\varepsilon' - \frac{1}{|\mathsf{ChSet}|})$, $t \approx 2t'$.

Proof. We first show how to derive (3) from (2). If $\varepsilon' \leq 1/|\mathsf{ChSet}|$, then (3) holds trivially. Assuming $\varepsilon' > 1/|\mathsf{ChSet}|$, we set $N := (\varepsilon' - 1/|\mathsf{ChSet}|)^{-1}$ to obtain $t \approx 2t'/(\varepsilon' - 1/|\mathsf{ChSet}|)$ and $\varepsilon \geq (1 - \frac{1}{e})^2 \geq \frac{1}{3}$. Dividing ε by t yields (3).

To prove (2), let $\mathcal{A}$ be an adversary against the (t', ε')-$\mathsf{IMP\text{-}KOA}$-security of ID. We now build an adversary $\mathcal{B}$ against the (t, ε)-$\mathsf{KR\text{-}KOA}$ security of ID, with (t, ε) as claimed in (2).

We use the Multi-Instance Reset Lemma (Lemma 1), where $H := \mathsf{ChSet}$ and IG runs $(pk, sk) \overset{\$}{\leftarrow} \mathsf{IGen}$ and returns pk as instance I. We first define adversary $\mathcal{C}(pk, h; \rho)$ that executes $\mathcal{A}(pk; \rho)$, answers $\mathcal{A}$'s single query R with h, and finally receives s from $\mathcal{A}$. If transcript (R, h, s) is valid with respect to pk (i.e., $\mathsf{V}(pk, R, h, s) = 1$)), $\mathcal{C}$ returns $(b = 1, \sigma = (R, h, s))$; otherwise, it returns $(b = 0, \epsilon)$. By construction, $\mathcal{C}$ returns $b = 1$ iff $\mathcal{A}$ is successful: $\mathsf{acc} = \varepsilon'$.

Adversary $\mathcal{B}$ is defined as follows. For each $i \in [N]$, it uses the RSR property of ID to generate a fresh public key/trapdoor pair $(pk_i, \tau_i) \overset{\$}{\leftarrow} \mathsf{Rerand}(pk)$. Next, it runs $(i^*, \sigma, \sigma') \overset{\$}{\leftarrow} \mathcal{R}_{\mathcal{C}}(pk_1, \ldots, pk_N)$, with $\mathcal{C}$ defined above. If $i^* \geq 1$, then both transcripts $\sigma = (R, h, s)$ and $\sigma' = (R, h', s')$ are valid with respect to pk_{i^*} and $h \neq h'$. $\mathcal{B}$ uses the SS property of ID and computes $sk_{i^*} \leftarrow \mathsf{Ext}(pk_{i^*}, R, h, s, h', s')$. Finally, using the RSR property of ID, it returns $sk = \mathsf{Derand}(pk_{i^*}, sk_{i^*}, \tau_{i^*})$ and terminates. By construction, $\mathcal{B}$ is successful iff $\mathcal{R}_{\mathcal{C}}$ is. By Lemma 1 we can bound $\mathcal{B}$'s success probability as

$$\varepsilon = \mathsf{res} \geq (1 - (1 - \varepsilon' + \frac{1}{|\mathsf{ChSet}|})^N)^2.$$

The running time t of $\mathcal{B}$ is that of $\mathcal{R}_{\mathcal{C}}$, meaning $2Nt'$ plus the N times the time to run the Rerand and Derand algorithms of RSR plus the time to run the Ext algorithm of SS. We write $t \approx 2Nt'$ to indicate that this is the dominating running time of $\mathcal{B}$. □

Lemma 4 (IMP-KOA $\xrightarrow{\textbf{loss } Q}$ PIMP-KOA)**.** *If* ID *is* (t, ε)-IMP-KOA *secure, then* ID *is* $(t', \varepsilon', Q_{\text{CH}})$-PIMP-KOA *secure, where*

$$\varepsilon' \leq Q_{\text{CH}} \cdot \varepsilon, \quad t' \approx t.$$

The proof is given in the full version [35].

Lemma 5 (PIMP-KOA $\xrightarrow{\textbf{PRO}}$ UF-KOA)**.** *If* ID *is* $(t, \varepsilon, Q_{\text{CH}})$-PIMP-KOA *secure, then* SIG[ID] *is* (t', ε', Q_h)-UF-KOA *secure in the programmable random oracle model, where*

$$\varepsilon' = \varepsilon, \quad t' \approx t, \quad Q_h = Q_{\text{CH}} - 1.$$

The proof is given in the full version [35].

The following lemma is a special case of Lemma 8 (with a slightly improved bound).

Lemma 6 (UF-KOA $\xrightarrow{\textbf{PRO}}$ UF-CMA)**.** *Suppose* ID *is* HVZK *and has α bit min-entropy. If* SIG[ID] *is* (t, ε, Q_h)-UF-KOA *secure, then* SIG[ID] *is* $(t', \varepsilon', Q_s, Q_h)$-UF-CMA *secure in the programmable random oracle model, where*

$$\varepsilon' \leq \varepsilon + \frac{Q_h Q_s}{2^\alpha}, \quad t' \approx t,$$

and Q_s, Q_h are upper bounds on the number of signing and hash queries in the UF-CMA *experiment, respectively.*

Lemma 7 (UF-KOA $\xrightarrow{\textbf{RSR}}$ MU-UF-KOA)**.** *Suppose* ID *is* RSR. *If* SIG[ID] *is* (t, ε)-UF-KOA *secure, then* SIG[ID] *is* (t', ε', N)-MU-UF-KOA *secure, where*

$$\varepsilon' = \varepsilon, \qquad t' \approx t.$$

Note that without the RSR property one can use the generic bounds from [25] to obtain a non-tight bound with a loss of N.

Proof. Let $\mathcal{A}$ be an algorithm that breaks (t', ε', N)-MU-UF-KOA security of SIG[ID]. We will describe an adversary $\mathcal{B}$ invoking $\mathcal{A}$ that breaks (t, ε)-UF-KOA security of SIG[ID] with (t, ε) as stated in the lemma. Adversary $\mathcal{B}$ is executed in the UF-KOA experiment and obtains a public-key pk.

Simulation of public-keys input to $\mathcal{A}$. For each $i \in [N]$, $\mathcal{B}$ generates $(pk_i, \tau_i) \overset{\$}{\leftarrow}$ Rerand(pk) by using the RSR property of ID. Then $\mathcal{B}$ runs $\mathcal{A}$ on input $(pk_1, \ldots, pk_N)$.

Forgery. Eventually, $\mathcal{A}$ will submit its forgery $(i^*, m^*, \sigma^* := (R^*, s^*))$ in the MU-UF-KOA experiment. $\mathcal{B}$ computes $h^* = H(m^*, R^*)$ and runs

$s \xleftarrow{\$} \mathsf{Tran}(pk, pk_{i^*}, \tau_{i^*}, (R^*, h^*, s^*))$. By the RSR property of ID, the random variables (pk, R^*, h^*, s) and $(pk_{i^*}, R^*, h^*, s^*)$ are identically distributed. If σ^* is a valid signature on message m^* under pk_{i^*}, then (R^*, s) is also a valid signature on m^* under pk. Thus, we have $\varepsilon = \varepsilon'$. The running time t of $\mathcal{B}$ is t' plus the N times the time to run the Rerand and Tran algorithms of RSR. We again write $t \approx t'$. □

Lemma 8 ($\mathsf{MU\text{-}UF\text{-}KOA} \xrightarrow{\textbf{PRO}} \mathsf{MU\text{-}UF\text{-}CMA}$)**.** *Suppose* ID *is* HVZK *and has* α *bit min-entropy. If* $\mathsf{SIG[ID]}$ *is* (t, ε, N, Q_h)-$\mathsf{MU\text{-}UF\text{-}KOA}$ *secure, then* $\mathsf{SIG[ID]}$ *is* $(t', \varepsilon', N, Q_s, Q_h)$-$\mathsf{MU\text{-}UF\text{-}CMA}$ *secure in the programmable random oracle model, where*

$$\varepsilon' \leq 4\varepsilon + \frac{Q_h Q_s}{2^\alpha}, \quad t' \approx t,$$

and N *is the number of users and* Q_s *and* Q_h *are upper bounds on the number of signing and hash queries in the* $\mathsf{MU\text{-}UF\text{-}CMA}$ *experiment, respectively.*

Proof. Let $\mathcal{A}$ be an algorithm that breaks $(t', \varepsilon', N, Q_s, Q_h)$-$\mathsf{MU\text{-}UF\text{-}CMA}$ security of $\mathsf{SIG[ID]}$. We will describe an adversary $\mathcal{B}$ invoking $\mathcal{A}$ that breaks (t, ε, N, Q_h)-$\mathsf{MU\text{-}UF\text{-}KOA}$ security of $\mathsf{SIG[ID]}$ with (t, ε) as stated in the lemma. Adversary $\mathcal{B}$ is executed in the $\mathsf{MU\text{-}UF\text{-}KOA}$ experiment and obtains public-keys $(pk_1, \ldots, pk_N)$, and has access to a random oracle H.

Preparation of public-keys. For each $i \in [N]$, adversary $\mathcal{B}$ picks a secret bit $b_i \xleftarrow{\$} \{0, 1\}$. If $b_i = 1$ then $\mathcal{B}$ defines $pk'_i := pk_i$, else $\mathcal{B}$ generates the key-pair $(pk'_i, sk'_i) \xleftarrow{\$} \mathsf{Gen}(\mathsf{par})$ itself. We note that all simulated public-keys are correctly distributed.

Adversary $\mathcal{B}$ runs $\mathcal{A}$ on input $(pk'_1, \ldots, pk'_N)$ answering hash queries to random oracle H' and signing queries as follows.

Simulation of hash queries. A hash query $H'(R, m)$ is answered by $\mathcal{B}$ by querying its own hash oracle $H(R, m)$ and returning its answer.

Simulation of signing queries. On $\mathcal{A}$'s j-th signature query (i_j, m_j), $\mathcal{B}$ returns a signature σ_j on message m_j under pk_{i_j} according to the following case distinction.

- Case A: $b_{i_j} = 0$. In that case sk'_{i_j} is known to $\mathcal{B}$ and the signature is computed as $\sigma_j := (R_j, s_j) \xleftarrow{\$} \mathsf{Sign}(sk'_{i_j}, m_j)$. Note that this involves $\mathcal{B}$ making a hash query and defining $H'(R_j, m_j) := H(R_j, m_j)$.
- Case B: $b_{i_j} = 1$. In that case sk'_{i_j} is unknown to $\mathcal{B}$ and the signature is computed using the HVZK property of ID. Concretely, $\mathcal{B}$ runs $(R_j, h_j, s_j) \xleftarrow{\$} \mathsf{Sim}(pk'_{i_j})$. If hash value $H'(R_j, m_j)$ was already defined (via one of $\mathcal{A}$'s hash/signing queries) and $H'(R_j, m_j) \neq h_j$, $\mathcal{B}$ aborts. Otherwise, it defines the random oracle
$$H'(R_j, m_j) := h_j \tag{4}$$
and returns $\sigma_j := (R_j, s_j)$, which is a correctly distributed valid signatures on m_j under pk_{i_j}. Note that by (4), $\mathcal{B}$ makes H and H' inconsistent, i.e., we

have $H(R_j, m_j) \neq H'(R_j, m_j)$ with high probability. Also note that for each signing query, $\mathcal{B}$ aborts with probability at most $Q_h/2^\alpha$ because R_j has min-entropy α. Since the number of signing queries is bounded by Q_s, $\mathcal{B}$ aborts overall with probability at most $Q_h Q_s/2^\alpha$.

Forgery. Eventually, $\mathcal{A}$ will submit its forgery $(i^*, m^*, \sigma^* := (R^*, s^*))$. We assume that it is a valid forgery in the $\mathsf{MU\text{-}UF\text{-}CMA}$ experiment, i.e., for $h^* = H'(R^*, m^*)$ we have $\mathsf{V}(pk'_{i^*}, R^*, h^*, s^*) = 1$. Furthermore, it satisfies the freshness condition, i.e.,

$$(i^*, m^*) \notin \{(i_j, m_j) : j \in [Q_s]\}. \tag{5}$$

After receiving $\mathcal{A}$'s forgery, $\mathcal{B}$ computes a forgery for the $\mathsf{MU\text{-}UF\text{-}KOA}$ experiment according to the following case distinction.

- Case 1: There exists a $j \in [Q_s]$ such that $(m^*, R^*) = (m_j, R_j)$. (If there is more than one j, fix any of them.) In that case we have and $h^* = h_j$ and furthermore $i^* \neq i_j$ by the freshness condition (5).
  - Case 1a: $(b_{i^*} = 1)$ and $(b_{i_j} = 0)$. Then the hash value $h^* = H'(R^*, m^*)$ was not programmed by $\mathcal{B}$ in (4). That means $h^* = H'(R^*, m^*) = H(R^*, m^*)$ and $\mathcal{B}$ returns $(i^*, m^*, (R^*, s^*))$ as a valid forgery to its $\mathsf{MU\text{-}UF\text{-}KOA}$ experiment.
  - Case 1b: $(b_{i^*} = b_{i_j})$ or $(b_{i^*} = 0 \wedge b_{i_j} = 1)$. Then $\mathcal{B}$ aborts.

  Note that in case 1 we always have $i^* \neq i_j$ and therefore $\mathcal{B}$ does not abort with probability $1/4$ in which case it outputs a valid forgery.
- Case 2: For all $j \in [Q_s]$ we have: $(m^*, R^*) \neq (m_j, R_j)$.
  - Case 2a: $b_{i^*} = 1$. Then the hash value $h^* = H'(R^*, m^*)$ was not programmed by $\mathcal{B}$ in (4). That means $h^* = H'(R^*, m^*) = H(R^*, m^*)$ and $\mathcal{B}$ returns $(i^*, m^*, (R^*, s^*))$ as a valid forgery to its $\mathsf{MU\text{-}UF\text{-}KOA}$ experiment.
  - Case 2b: $b_{i^*} = 0$. Then $\mathcal{B}$ aborts.

  Note that in case 2, $\mathcal{B}$ does not abort with probability $1/2$ in which case it outputs a valid forgery.

Overall, $\mathcal{B}$ returns a valid forgery of $\mathsf{MU\text{-}UF\text{-}KOA}$ experiment with probability

$$\varepsilon \geq \min\left\{\frac{1}{4}, \frac{1}{2}\right\} \cdot \left(\varepsilon' - \frac{Q_h Q_s}{2^\alpha}\right) = \frac{1}{4}\left(\varepsilon' - \frac{Q_h Q_s}{2^\alpha}\right).$$

The running time of $\mathcal{B}$ is that of $\mathcal{A}$ plus the Q_s executions of Sim. We write $t' \approx t$. This completes the proof. □

If s in ID is uniquely defined by (pk, R, h) (e.g., as in the Schnorr identification scheme), then one can show the above proof even implies $\mathsf{MU\text{-}SUF\text{-}CMA}$ security of $\mathsf{SIG}[\mathsf{ID}]$. The simulation of hash and signing queries is the same as in the above proof. Let (i^*, m^*, R^*, s^*) be $\mathcal{A}$'s forgery. The freshness condition of the $\mathsf{MU\text{-}SUF\text{-}CMA}$ experiment says that $(i^*, m^*, R^*, s^*) \notin \{(i_j, m_j, R_j, s_j) : j \in [Q_s]\}$. Together with the uniqueness of ID, this implies $(i^*, m^*, R^*) \notin \{(i_j, m_j, R_j) : j \in [Q_s]\}$. If $(i^*, m^*) \notin \{(i_j, m_j) : j \in [Q_s]\}$, then $\mathcal{B}$ can break $\mathsf{MU\text{-}UF\text{-}KOA}$ security by the same case distinction as in the proof above. Otherwise, we have $R^* \notin \{R_j : j \in [Q_s]\}$, in which case we can argue as in case 2.

4 Impossibility Results

In this section, we show that Theorems 3 and 4 from the previous section are optimal in the sense that the security reduction requires: rewinding (Lemma 9), security loss of at least $O(Q)$ (Lemma 10) and programmability of random oracles (Lemmas 11 and 12).

Let X and Y be some hard cryptographic problems, defined through a (possibly) interactive experiment. A black-box reduction $\mathcal{R}$ from X to Y is an algorithm that, given black-box access to an adversary $\mathcal{A}$ breaking problem Y, breaks problem X. If X and Y are security notions for identification or signatures schemes, then a reduction $\mathcal{R}$ is called key-preserving, if $\mathcal{R}$ only makes calls to $\mathcal{A}$ with the same pk that it obtained by its own problem X. All our reductions considered in this section are key-preserving. All proofs from this section are given in the full version [35].

Lemma 9 ($\mathsf{KR\text{-}KOA} \overset{\textbf{non-rewind.}}{\not\longrightarrow} \mathsf{IMP\text{-}KOA}$). *If there is a key-preserving reduction $\mathcal{R}$ that $(t_{\mathcal{R}}, \varepsilon_{\mathcal{R}})$-breaks* $\mathsf{KR\text{-}KOA}$ *security of* ID *with* one-time black-box *access to an adversary $\mathcal{A}$ that $(t_{\mathcal{A}}, \varepsilon_{\mathcal{A}})$-breaks* $\mathsf{IMP\text{-}KOA}$ *security of* ID*, then there exists an algorithm $\mathcal{M}$ that $(t_{\mathcal{M}}, \varepsilon_{\mathcal{M}}, Q_{\mathrm{O}})$-breaks* $\mathsf{IMP\text{-}AA}$ *security of* ID*, where*

$$\varepsilon_{\mathcal{M}} \geq \varepsilon_{\mathcal{R}} - \frac{1}{|\mathsf{ChSet}|}, \quad t_{\mathcal{M}} \approx t_{\mathcal{R}}, \quad Q_{\mathrm{O}} = 1.$$

For our next impossibility result, we will require the following definition for identification schemes.

Definition 10 (Concurrent (Weak) Impersonation against Man-in-the-Middle Attacks). *A canonical identification* ID *is said to be $(t, \varepsilon, Q_{\mathrm{CH}}, Q_{\mathrm{O}})$-*$\mathsf{IMP\text{-}MIM}$ *secure (impersonation against man-in-the-middle attacks) if for all adversaries $\mathcal{A}$ running in time at most t and adaptively making at most Q_{O} queries to the prover oracle* Prover *and Q_{CH} queries to the challenge oracle* Ch*,*

$$\Pr\left[\begin{matrix} \mathsf{V}(pk, R_{i^*}, h_{i^*}, s_{i^*}) = 1 \wedge (i^* \in [Q_{\mathrm{CH}}]) \\ \wedge (R_{i^*}, h_{i^*}, s_{i^*}) \notin \{(R'_j, h'_j, s'_j) \mid j \in [Q_{\mathrm{O}}]\} \end{matrix} \;\middle|\; \begin{matrix} (pk, sk) \overset{\$}{\leftarrow} \mathsf{IGen}(\mathsf{par}) \\ (i^*, s_{i^*}) \overset{\$}{\leftarrow} \mathcal{A}^{\textsc{Prover}(\cdot), \textsc{Ch}(\cdot)}(pk) \end{matrix}\right] \leq \varepsilon,$$

where oracles Prover *and* Ch *are defined as in Definition 2. We define weak impersonation against man-in-the-middle attack (*$\mathsf{wIMP\text{-}MIM}$*) by restricting $R_{i^*} \in \{R'_1, \ldots, R'_{Q_{\mathrm{O}}}\}$.*

We remark that $\mathsf{wIMP\text{-}MIM}$ is a non-standard definition without any practical relevance, but it will only be used for showing negative results. The following generalizes a result by Seurin [43] to canonical identification schemes.

Lemma 10 ($\mathsf{IMP\text{-}KOA} \overset{\textbf{loss<Q}}{\not\longrightarrow} \mathsf{PIMP\text{-}KOA}$). *Suppose that* ID *has α bit min-entropy and there is a key-preserving reduction $\mathcal{R}$ that $(t_{\mathcal{R}}, \varepsilon_{\mathcal{R}})$-breaks* $\mathsf{IMP\text{-}KOA}$

security of ID *with* n-time black-box *access to an adversary* $\mathcal{A}$ *that* $(t_{\mathcal{A}}, \varepsilon_{\mathcal{A}}, Q_{\mathrm{CH}})$-*breaks* PIMP-KOA *security of* ID*. Then there exists an algorithm* $\mathcal{M}$ *that* $(t_{\mathcal{M}}, \varepsilon_{\mathcal{M}}, 1, Q_{\mathrm{O}} = nQ_{\mathrm{CH}})$-*breaks* IMP-MIM *security of* ID*, where*

$$\varepsilon_{\mathcal{M}} \geq \varepsilon_{\mathcal{R}} - \frac{n \ln\left((1-\varepsilon_{\mathcal{A}})^{-1}\right)}{Q_{\mathrm{CH}}} - \frac{n}{|\mathsf{ChSet}|} - \frac{n}{2^{\alpha}}, \quad t_{\mathcal{M}} \approx t_{\mathcal{R}}.$$

For a precise analysis of the function $\ln\left((1-\varepsilon_{\mathcal{A}})^{-1}\right)$, we refer to [43]. For our purpose, it is sufficient that for a concrete choice of $\varepsilon_{\mathcal{A}}$, there is a constant c such that $c \cdot \varepsilon_{\mathcal{A}} = \ln\left((1-\varepsilon_{\mathcal{A}})^{-1}\right)$. Hence Lemma 10 gives roughly $\varepsilon_{\mathcal{M}} \geq \varepsilon_{\mathcal{R}} - (c \cdot n/Q_{\mathrm{CH}}) \cdot \varepsilon_{\mathcal{A}}$ for a suitable choice of $\varepsilon_{\mathcal{A}}$. Therefore $\varepsilon_{\mathcal{R}}$ can be at most $(c \cdot n/Q_{\mathrm{CH}}) \cdot \varepsilon_{\mathcal{A}}$. Otherwise $\mathcal{M}$ would break IMP-MIM security of ID with $\varepsilon_{\mathcal{M}} > 0$.

In the proof of Lemma 10 (cf. [35]), the meta-reduction just forwards all $R_{j,i}$ received during the Man-in-the-Middle attack and R sent by $\mathcal{R}$. So if $\mathcal{R}$ is furthermore randomness-preserving, i.e., it chooses $R \in \{R_{1,1}, \ldots, R_{n,Q_{\mathrm{CH}}}\}$, then $\mathcal{M}$ attacks wIMP-MIM-security of ID. This observation (formalized in the following corollary) is important since the Schnorr identification scheme is wIMP-MIM but not IMP-MIM-secure.

Corollary 1. *If* ID *has* α *bit min-entropy and there exists a key- and randomness-preserving reduction* $\mathcal{R}$ *that* $(t_{\mathcal{R}}, \varepsilon_{\mathcal{R}})$-*breaks* IMP-KOA *security of* ID *with* n-time black-box *access to an adversary* $\mathcal{A}$ *that* $(t_{\mathcal{A}}, \varepsilon_{\mathcal{A}}, Q_{\mathrm{CH}})$-*breaks* PIMP-KOA *security of* ID*, then there exists an algorithm* $\mathcal{M}$ *that* $(t_{\mathcal{M}}, \varepsilon_{\mathcal{M}}, 1, Q_{\mathrm{O}} = nQ_{\mathrm{CH}})$-*breaks* wIMP-MIM *security of* ID*, where*

$$\varepsilon_{\mathcal{M}} \geq \varepsilon_{\mathcal{R}} - \frac{n \ln\left((1-\varepsilon_{\mathcal{A}})^{-1}\right)}{Q_{\mathrm{CH}}} - \frac{n}{|\mathsf{ChSet}|} - \frac{n}{2^{\alpha}}, \quad t_{\mathcal{M}} \approx t_{\mathcal{R}}.$$

Lemma 11 (IMP-KOA $\overset{\textbf{NPRO}}{\not\longrightarrow}$ UF-KOA). *If there exists a key-preserving reduction* $\mathcal{R}$ *in the non-programmable random oracle (NPRO) model that* $(t_{\mathcal{R}}, \varepsilon_{\mathcal{R}})$-*breaks* IMP-KOA *security of* ID *with* n*-time black-box access to an adversary* $\mathcal{A}$ *that* $(t_{\mathcal{A}}, \varepsilon_{\mathcal{A}}, Q_h)$-*breaks* UF-KOA *security of* SIG[ID]*, then there exists an algorithm* $\mathcal{M}$ *that* $(t_{\mathcal{M}}, \varepsilon_{\mathcal{M}}, 1)$-*breaks* IMP-AA-*security of* ID*, where*

$$\varepsilon_{\mathcal{M}} \geq \varepsilon_{\mathcal{R}} - \frac{1}{|\mathsf{ChSet}|}, \quad t_{\mathcal{M}} \approx t_{\mathcal{R}}.$$

By Lemmas 4 and 11 implies that there is no reduction from PIMP-KOA to UF-KOA in the non-programmable random oracle model.

The following simple lemma actually holds for any signature scheme SIG.

Lemma 12 (UF-KOA $\overset{\textbf{NPRO}}{\not\longrightarrow}$ UF-CMA). *Suppose that there is a key-preserving reduction* $\mathcal{R}$ *in the non-programmable random oracle (NPRO) model that* $(t_{\mathcal{R}}, \varepsilon_{\mathcal{R}}, Q_h)$-*breaks* UF-KOA *security of* SIG *with* n*-time black-box access to an adversary* $\mathcal{A}$ *that* $(t_{\mathcal{A}}, \varepsilon_{\mathcal{A}}, Q_s, Q_h)$-*breaks* UF-CMA *security of* SIG*. Then there exists an algorithm* $\mathcal{M}$ *that* $(t_{\mathcal{M}}, \varepsilon_{\mathcal{M}})$-*breaks* UF-KOA *security of* SIG*, where*

$$\varepsilon_{\mathcal{M}} \geq \varepsilon_{\mathcal{R}}, \quad t_{\mathcal{M}} \approx t_{\mathcal{R}}.$$

Remark 1. All the reductions considered in this section are key-preserving which is the main restriction of our results. If pk and R are elements from some multiplicative group $\mathbb{G}$ of prime order p, then we can extend our previous techniques to exclude the larger class of algebraic reductions. A reduction is algebraic, if for all group elements h output by the reduction, their respective representation is known. That is, if at some point of its execution the reduction holds group elements $g_1, \ldots, g_n \in \mathbb{G}$ and outputs a new group element h, then it also knows it representation meaning it also outputs $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_p^n$ satisfying $h = \prod g_i^{\alpha_i}$. Note that key-preserving and randomness-preserving reductions are a special case of algebraic reductions.

5 Instantiations

In this section we consider two important identification schemes, namely the ones by Schnorr [42] and by Katz-Wang [19,34]. We use our framework to derive tight security bounds and concrete parameters for the corresponding Schnorr/Katz-Wang signature schemes. In the full version [35] we discuss one more identification scheme, namely the one by Guillou-Quisquater [31].

5.1 Schnorr Identification/Signature Scheme

Schnorr's Identification Scheme. The well-known Schnorr's identification scheme is one of the most important instantiations of our framework. For completeness we show that Schnorr's identification has large min-entropy, special soundness (SS), honest-verifier zero-knowledge (HVZK), random-self reducibility (RSR) and key-recovery security (KR-KOA) based on the discrete logarithm problem (DLOG). Moreover, based on the one-more discrete logarithm problem (OMDL), Schnorr's identification is actively secure (IMP-AA) and weakly secure against man-in-the-middle attack (wIMP-MIM).

Let $\mathsf{par} := (p, g, \mathbb{G})$ be a set of system parameters, where $\mathbb{G} = \langle g \rangle$ is a cyclic group of prime order p with a hard discrete logarithm problem. Examples of groups $\mathbb{G}$ include appropriate subgroups of certain elliptic curve groups, or subgroups of $\mathbb{Z}_q^*$. The Schnorr identification scheme $\mathsf{ID_S} := (\mathsf{IGen}, \mathsf{P}, \mathsf{ChSet}, \mathsf{V})$ is defined as follows.

```
IGen(par):
$sk := x \xleftarrow{\$} \mathbb{Z}_p$
$pk := X = g^x$
ChSet $:= \{0,1\}^n$
Return $(pk, sk)$

V$(pk, R, h, s)$:
If $R = g^s \cdot X^{-h}$ then return 1
Else return 0
```

```
P$_1(sk)$:
$r \xleftarrow{\$} \mathbb{Z}_p$; $R = g^r$
$St := r$
Return $(R, St)$

P$_2(sk, R, h, St)$:
Parse $St = r$
Return $s = x \cdot h + r \bmod p$
```

We recall the DLOG assumption.

Definition 11 (Discrete Logarithm Assumption). *The discrete logarithm problem* DLOG *is* (t, ε)*-hard in* $\mathsf{par} = (p, g, \mathbb{G})$ *if for all adversaries* $\mathcal{A}$ *running in time at most* t*,* $\Pr\left[g^x = X \,\middle|\, X \stackrel{\$}{\leftarrow} \mathbb{G}; x \stackrel{\$}{\leftarrow} \mathcal{A}(X)\right] \leq \varepsilon$*.*

Lemma 13. $\mathsf{ID_S}$ *is a canonical identification with* $\alpha = \log p$ *bit min-entropy and it is unique, has special soundness (*SS*), honest-verifier zero-knowledge (*HVZK*) and is random-self reducible (*RSR*). Moreover, if* DLOG *is* (t, ε)*-hard in* $\mathsf{par} = (p, g, \mathbb{G})$ *then* $\mathsf{ID_S}$ *is* (t, ε)*-*$\mathsf{KR\text{-}KOA}$ *secure.*

Proof. The correctness of $\mathsf{ID_S}$ is straightforward to verify. We note that R in $(R, St) \stackrel{\$}{\leftarrow} \mathsf{P}_1(sk)$ is uniformly random over $\mathbb{G}$. Hence, $\mathsf{ID_S}$ has $\log|\mathbb{G}| = \log p$ bit min-entropy. We show the other properties as follows.

Uniqueness. For all $(X, x) \in \mathsf{IGen}(\mathsf{par})$, $(R := g^r, St := r) \in \mathsf{P}_1(sk)$ and $h \in \{0,1\}^n$, the value $s \in \mathbb{Z}_p$ satisfying $g^s = X^h R \Leftrightarrow s = xh + r$ is uniquely defined.

Special Soundness (SS). Given two accepting transcripts (R, h, s) and (R, h', s') with $h \neq h'$, we define an extractor algorithm $\mathsf{Ext}(X, R, h, s, h', s') := x^* := (s - s')/(h - h')$ such that, for all $(X := g^x, x) \in \mathsf{IGen}(\mathsf{par})$, we have $\Pr[g^{x^*} = X] = 1$, since we have $R = g^s X^{-h} = g^{s'} X^{-h'}$ and then $X = g^{(s-s')/(h-h')}$.

Honest-verifier Zero-knowledge (HVZK). Given public key X, we let $\mathsf{Sim}(X)$ first sample $h \stackrel{\$}{\leftarrow} \{0,1\}^n$ and $s \stackrel{\$}{\leftarrow} \mathbb{Z}_p$ and then output $(R := g^s X^{-h}, h, s)$. Clearly, (R, h, s) is a real transcript, since s is uniformly random over $\mathbb{Z}_p$ and R is the unique value satisfying $R = g^s X^{-h}$.

Random-self Reducibility (RSR). Algorithm Rerand and two deterministic algorithm Derand and Tran are defined as follows:

- $\mathsf{Rerand}(X)$ chooses $\tau' \stackrel{\$}{\leftarrow} \mathbb{Z}_p$ and outputs $(X' := X \cdot g^{\tau'}, \tau')$. We have that, for all $(X, x) \in \mathsf{IGen}(\mathsf{par})$, X' is uniform and has the same distribution as X'', where $(X'', x'') \stackrel{\$}{\leftarrow} \mathsf{IGen}(\mathsf{par})$.
- $\mathsf{Derand}(X, X', x', \tau')$ outputs $x^* = x' - \tau'$. We have, for all $(X', \tau') \stackrel{\$}{\leftarrow} \mathsf{Rerand}(X := g^x)$ and $(X', x') \in \mathsf{IGen}(\mathsf{par})$, $X' = g^{x'}$ and $x' = x + \tau'$ and thus $x^* = x$.
- $\mathsf{Tran}(X, X', \tau', (R', h', s'))$ outputs $s = s' - \tau' \cdot h'$. We have, for all $(X', \tau') \in \mathsf{Rerand}(X := g^x)$, if (R', h', s') is valid with respect to $X' := g^{x+\tau'}$ then $s = s' - \tau' \cdot h' = (x + \tau')h' + r - \tau' \cdot h' = xh' + r$ and (R', h', s) is valid with respect to X.

Key-recovery against Key-only Attack ($\mathsf{KR\text{-}KOA}$). $\mathsf{KR\text{-}KOA}$-security for ID is exactly the DLOG assumption. □

Under the one-more discrete logarithm assumption [4], $\mathsf{ID_S}$ is $\mathsf{IMP\text{-}AA}$ secure [6] and in the full version [35] we show that $\mathsf{ID_S}$ is weakly $\mathsf{IMP\text{-}MIM}$ secure.

We now define the Q-interactive discrete-logarithm problem which precisely models $\mathsf{PIMP\text{-}KOA}$-security for $\mathsf{ID_S}$, where $Q = Q_{\mathrm{O}}$ is the number of parallel impersonation rounds.

Definition 12 (Q-IDLOG). *The interactive discrete-logarithm assumption Q-IDLOG is said to be (t, ε)-hard in $\mathsf{par} = (p, g, \mathbb{G})$ if for all adversaries $\mathcal{A}$ running in time at most t and making at most Q queries to the challenge oracle* $\mathrm{C}\textsc{h}$,

$$\Pr\left[s \in \{xh_i + r_i \mid i \in [Q]\} \;\middle|\; \begin{array}{l} x \xleftarrow{\$} \mathbb{Z}_p; X = g^x \\ s \xleftarrow{\$} \mathcal{A}^{\mathrm{C}\textsc{h}(\cdot)}(X) \end{array} \right] \leq \varepsilon,$$

where on the i-th query $\mathrm{C}\textsc{h}(g^{r_i})$ $(i \in [Q])$, the challenge oracle returns $h_i \xleftarrow{\$} \mathbb{Z}_p$ to $\mathcal{A}$.

In [35] we prove that in the generic group model, the Q-IDLOG problem in groups of prime-order p is at least $(t, 2t^2/p)$-hard. Note that the bound is independent of Q.

Schnorr's Signature Scheme. Let $H : \{0,1\}^* \to \{0,1\}^n$ be a hash function with $n < \log_2(p)$. As $\mathsf{ID_S}$ is commitment-recoverable we can use the alternative Fiat-Shamir transformation to obtain the Schnorr signature scheme $\mathsf{Schnorr} := (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$.

$\mathsf{Gen}(\mathsf{par})$:	$\mathsf{Sign}(sk, m)$:	$\mathsf{Ver}(sk, m, \sigma)$:
$sk := x \xleftarrow{\$} \mathbb{Z}_p$ $pk := X = g^x$ Return (pk, sk)	$r \xleftarrow{\$} \mathbb{Z}_p$; $R = g^r$ $h = H(R, m)$ $s = x \cdot h + r \bmod p$ $\sigma = (h, s) \in \{0,1\}^n \times \mathbb{Z}_p$ Return σ	Parse $\sigma = (h, s) \in \{0,1\}^n \times \mathbb{Z}_p$ $R = g^s X^{-h}$ If $h = H(R, m)$ then return 1 Else return 0.

The DLOG problem is tightly equivalent to the 1-IDLOG problem by Lemma 3. Assuming the OMDL problem is hard, $\mathsf{Schnorr}$ is wIMP-MIM-secure and by Corollary 1 there cannot exist a tight implication 1-IDLOG → Q-IDLOG meaning the bound from Lemma 4 is optimal. By Lemmas 5 and 6, the Q-IDLOG problem is tightly equivalent to SUF-CMA-security of $\mathsf{Schnorr}$ in the programmable ROM. The latter is only tightly equivalent to MU-SUF-CMA-security in the programmable ROM (via Lemmas 7 and 8). In the full version [35] we improve this by proving that SUF-CMA security is tightly equivalent to MU-SUF-CMA-security in the standard model. Figure 3 summarizes the modular security implications for $\mathsf{Schnorr}$.

We derive the following concrete security implications.

Lemma 14. *If* DLOG *is (t, ε)-hard in* $\mathsf{par} = (p, g, \mathbb{G})$ *then* $\mathsf{Schnorr}$ *is* $(t', \varepsilon', Q_s, Q_h)$-$\mathsf{SUF}$-$\mathsf{CMA}$ *secure and* $(t'', \varepsilon'', N, Q_s, Q_h)$-$\mathsf{MU}$-$\mathsf{SUF}$-$\mathsf{CMA}$ *secure in the programmable random oracle model, where*

$$\frac{\varepsilon'}{t'} \leq 6(Q_h + 1) \cdot \frac{\varepsilon}{t} + \frac{Q_s}{p} + \frac{1}{2^n},$$
$$\frac{\varepsilon''}{t''} \leq 12(Q_h + 1) \cdot \frac{\varepsilon}{t} + \frac{Q_s}{p} + \frac{1}{2^n}.$$

Lemma 15. *If* Q_h-IDLOG *is* (t, ε)*-hard in* par *then* Schnorr *is* $(t', \varepsilon', N, Q_s, Q_h)$-MU-SUF-CMA *secure in the programmable random oracle model, where*

$$\varepsilon' \leq 2\varepsilon + \frac{Q_h Q_s}{p}, \qquad t' \approx t.$$

We leave it an open problem to come up with a more natural hard problem over par that tightly implies Q-IDLOG (and hence MU-SUF-CMA-security of Schnorr). Note that according to [23], the hard problem has to have at least one round of interaction.

$$\begin{tikzcd}
\mathsf{DLOG} \arrow[r, shift left=2, "\text{rew. (L. 3)}"] \arrow[r, leftarrow, dashed] \arrow[r, shift right=2, "/" marking, "\text{non-rew. (L. 9)}"'] & \mathsf{1\text{-}IDLOG} \arrow[r, shift left=2, "\text{loss } Q \text{ (L. 4)}"] \arrow[r, leftarrow, dashed] \arrow[r, shift right=2, "/" marking, "\text{loss} < Q \text{ (L. 10)}"'] & Q\text{-}\mathsf{IDLOG} \arrow[r, shift left=2, "\text{PRO (L. 5, L. 6)}"] \arrow[r, leftarrow, dashed] \arrow[r, shift right=2, "/" marking, "\text{NPRO (L. 11, L. 12)}"'] & \mathsf{SUF\text{-}CMA} \arrow[r, shift left=2, "\text{(L. B.1 [35])}"] \arrow[r, leftarrow, dashed] & \mathsf{MU\text{-}SUF\text{-}CMA}
\end{tikzcd}$$

Fig. 3. Security relations for the Schnorr signature scheme. All implications except "1-IDLOG → Q-IDLOG" are tight.

The interpretation for the multi-user security of Schnorr over elliptic-curve groups is as follows. It is well-known that a group of order p providing k-bits security against the DLOG problem requires $\log p \geq 2k$. If one requires provable security guarantees for Schnorr under DLOG, then one has to increase the group size by $\approx \log(Q_h)$ bits. Reasonable upper bounds for $\log Q_h$ are between 40 and 80. However, the generic lower bound for the Q-IDLOG problem indicates that the only way to attack Schnorr in the sense of UF-KOA (and hence to attack Q-IDLOG) is to break the DLOG problem. In that case using groups with $\log p \approx 2k$ already gives provable security guarantees for Schnorr.

5.2 Chaum-Pedersen Identification/Katz-Wang Signature Scheme

Chaum-Pedersen Identification Scheme. Let par $:= (p, g_1, g_2, \mathbb{G})$ be a set of system parameters, where $\mathbb{G} = \langle g_1 \rangle = \langle g_2 \rangle$ is a cyclic group of prime order p. The Chaum-Pedersen identification scheme $\mathsf{ID_{CP}} := (\mathsf{IGen}, \mathsf{P}, \mathsf{ChSet}, \mathsf{V})$ is defined as follows.

```
IGen(par):
    $sk := x \xleftarrow{\$} \mathbb{Z}_p$
    $pk := (X_1, X_2) = (g_1^x, g_2^x)$
    $\mathsf{ChSet} := \{0,1\}^n$
    Return $(pk, sk)$

V($pk, R = (R_1, R_2), h, s$):
    If $R_1 = g^s \cdot X_1^{-h}$ and $R_2 = g^s \cdot X_2^{-h}$
    then return 1
    Else return 0

P_1($sk$):
    $r \xleftarrow{\$} \mathbb{Z}_p$; $R = (R_1, R_2) = (g_1^r, g_2^r)$
    $St := r$
    Return $(R, St)$

P_2($sk, R, h, St$):
    Parse $St = r$
    Return $s = x \cdot h + r \bmod p$
```

We recall the DDH assumption.

Definition 13 (Decision Diffie-Hellman Assumption). *The Decision Diffie-Hellman problem* DDH *is* (t,ε)*-hard in* $\mathsf{par} = (p, g_1, g_2, \mathbb{G})$ *if for all adversaries* $\mathcal{A}$ *running in time at most* t*,*

$$|\Pr\left[1 \overset{\$}{\leftarrow} \mathcal{A}(g_1^x, g_2^x) \mid x \overset{\$}{\leftarrow} \mathbb{Z}_p\right] - \Pr\left[1 \overset{\$}{\leftarrow} \mathcal{A}(g_1^{x_1}, g_2^{x_2}) \mid x_1 \overset{\$}{\leftarrow} \mathbb{Z}_p; x_2 \overset{\$}{\leftarrow} \mathbb{Z}_p \setminus \{x_1\}\right] | \le \varepsilon.$$

Clearly, all security results of Schnorr carry over to the Chaum-Pedersen identification scheme, i.e., $\mathsf{ID}_{\mathsf{CP}}$ is at least as secure as ID_{S}. That also means that we cannot hope for tight PIMP-KOA security from the DLOG assumption. Instead, for the Chaum-Pedersen identification scheme, we give a direct tight proof of PIMP-KOA security under the DDH assumption which we extracted from [34].

Lemma 16. $\mathsf{ID}_{\mathsf{CP}}$ *is a canonical identification scheme with* $\alpha = \log p$ *bit min-entropy and it is unique, has special soundness (*SS*), honest-verifier zero-knowledge (*HVZK*) and is random-self reducible (*RSR*). Moreover, if* DDH *is* (t,ε)*-hard in* $\mathsf{par} = (p, g_1, g_2, \mathbb{G})$ *then* $\mathsf{ID}_{\mathsf{CP}}$ *is* $(t', \varepsilon', Q_{\text{CH}})$-PIMP-KOA *secure, where* $t \approx t'$ *and* $\varepsilon \ge \varepsilon' - Q_{\text{CH}}/2^n$*.*

Proof. The proof of SS, HVZK, uniqueness, and RSR is the same as in ID_{S}.

To prove PIMP-KOA-security under DDH, let $\mathcal{A}$ be an adversary that $(t', \varepsilon', Q_{\text{CH}})$-breaks PIMP-KOA security. We build an adversary $\mathcal{B}$ against the (t,ε)-hardness of DDH as follows. Adversary $\mathcal{B}$ inputs (X_1, X_2) and defines $pk := (X_1, X_2)$. On the i-th challenge query $\text{CH}(R_{i,1}, R_{i,2})$, it returns $h_i \overset{\$}{\leftarrow} \mathbb{Z}_p$. Eventually, $\mathcal{A}$ returns $i^* \in [Q_{\text{CH}}]$ and s_{i^*} and terminates. Finally, $\mathcal{B}$ outputs $d := \mathsf{V}(pk, R_{i^*}, h_{i^*}, s_{i^*})$.

Analysis of $\mathcal{B}$. If $(X_1, X_2) = (g_1^x, g_2^x)$, then $\mathcal{B}$ perfectly simulates the PIMP-KOA game and hence $\Pr[d = 1 \mid (X_1, X_2) = (g_1^x, g_2^x)] = \varepsilon'$. If $(X_1, X_2) = (g_1^{x_1}, g_2^{x_2})$ with $x_1 \ne x_2$, then we claim that even a computationally unbounded $\mathcal{A}$ can only win with probability $Q_{\text{CH}}/2^n$, i.e., $\Pr[d = 1 \mid (X_1, X_2) = (g_1^{x_1}, g_2^{x_2})] \le Q_{\text{CH}}/2^n$.

It remains to prove the claim. For each index $i \in [Q_{\text{CH}}]$, $\mathcal{A}$ first commits to $R_{i,1} = g_1^{r_{i,1}}$ and $R_{i,2} = g_2^{r_{i,2}}$ (for arbitrary $r_{i,1}, r_{i,2} \in \mathbb{Z}_p$) and can only win if there exists an $s_i \in \mathbb{Z}_p$ such that

$$\begin{aligned} r_{i,1} + h_i x_1 = s_i &= r_{i,2} + h_i x_2 \\ \Leftrightarrow h_i &= \frac{r_{i,2} - r_{i,1}}{x_1 - x_2} \end{aligned}$$

where $h_i \overset{\$}{\leftarrow} \{0,1\}^n$ is chosen independently of $r_{i,1}, r_{i,2}$. This happens with probability at most $1/2^n$, so by the union bound we obtain the bound $Q_{\text{CH}}/2^n$, as claimed. □

Katz-Wang Signature Scheme. Let $H : \{0,1\}^* \to \{0,1\}^n$ be a hash function with $n < \log_2(p)$. As $\mathsf{ID}_{\mathsf{CP}}$ is commitment-recoverable we can use the alternative Fiat-Shamir transformation to obtain a signature scheme which is known as the Katz-Wang signature scheme $\mathsf{KW} := (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$.

```
$\underline{\mathsf{Gen}(\mathsf{par})\text{:}}$
$sk := x \xleftarrow{\$} \mathbb{Z}_p$
$(X_1, X_2) = (g_1^x, g_2^x)$
$pk := (X_1, X_2)$
Return $(pk, sk)$
```

```
$\underline{\mathsf{Sign}(sk, m)\text{:}}$
$r \xleftarrow{\$} \mathbb{Z}_p$
$R = (R_1, R_2) = (g_1^r, g_2^r)$
$h = H(R, m)$
$s = x \cdot h + r \bmod p$
$\sigma = (h, s) \in \{0,1\}^n \times \mathbb{Z}_p$
Return $\sigma$
```

```
$\underline{\mathsf{Ver}(sk, m, \sigma)\text{:}}$
Parse $\sigma = (h, s) \in \{0,1\}^n \times \mathbb{Z}_p$
$R = g^s X^{-h}$
If $h = H(R, m)$ then return 1
Else return 0.
```

By our results we obtain the following concrete security statements, where the first bound matches [34, Theorem1].

Lemma 17. *If* DDH *is* (t, ε)*-hard in* par $= (p, g_1, g_2, \mathbb{G})$ *then* KW *is* $(t', \varepsilon', Q_s, Q_h)$-SUF-CMA *secure and* $(t'', \varepsilon'', N, Q_s, Q_h)$-MU-SUF-CMA *secure in the programmable random oracle model, where*

$$\frac{\varepsilon'}{t'} \leq \frac{\varepsilon}{t} + \frac{Q_s}{p} + \frac{1}{2^n},$$

$$\frac{\varepsilon''}{t''} \leq 4 \cdot \frac{\varepsilon}{t} + \frac{Q_s}{p} + \frac{1}{2^n}.$$

References

1. Abdalla, M., An, J.H., Bellare, M., Namprempre, C.: From identification to signatures via the Fiat-Shamir transform: minimizing assumptions for security and forward-security. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 418–433. Springer, Heidelberg (2002)
2. Abdalla, M., Ben Hamouda, F., Pointcheval, D.: Tighter reductions for forward-secure signature schemes. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 292–311. Springer, Heidelberg (2013)
3. Abdalla, M., Fouque, P.-A., Lyubashevsky, V., Tibouchi, M.: Tightly-secure signatures from lossy identification schemes. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 572–590. Springer, Heidelberg (2012)
4. Bellare, M., Namprempre, C., Pointcheval, D., Semanko, M.: The one-more-RSA-inversion problems and the security of Chaum's blind signature scheme. J. Cryptology **16**(3), 185–215 (2003)
5. Bellare, M., Neven, G.: Multi-signatures in the plain public-key model and a general forking lemma. In: Juels, A., Wright, R.N., Vimercati, S. (eds.) ACM CCS 2006, pp. 390–399. ACM Press, October/November 2006
6. Bellare, M., Palacio, A.: GQ and schnorr identification schemes: proofs of security against impersonation under active and concurrent attacks. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 162–177. Springer, Heidelberg (2002)
7. Bellare, M., Ristenpart, T.: Simulation without the artificial abort: simplified proof and improved concrete security for Waters' IBE scheme. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 407–424. Springer, Heidelberg (2009)
8. Bellare, M., Rogaway, P.: Random oracles are practical: a paradigm for designing efficient protocols. In: Ashby, V. (ed.) ACM CCS 1993, pp. 62–73. ACM Press, November 1993
9. Bellare, M., Rogaway, P.: The exact security of digital signatures - how to sign with RSA and Rabin. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 399–416. Springer, Heidelberg (1996)

10. Bernstein, D.: [Cfrg] key as message prefix => multi-key security. https://mailarchive.ietf.org/arch/msg/cfrg/44gJyZlZ7-myJqWkChhpEF1KE9M, 2015
11. Bernstein, D.J.: Multi-user Schnorr security, revisited. Cryptology ePrint Archive, Report 2015/996, 2015. http://eprint.iacr.org/
12. Bernstein, D.J., Duif, N., Lange, T., Schwabe, P., Yang, B.-Y.: High-speed high-security signatures. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 124–142. Springer, Heidelberg (2011)
13. Beth, T.: Efficient zero-knowledged identification scheme for smart cards. In: Günther, C.G. (ed.) EUROCRYPT 1988. LNCS, vol. 330, pp. 77–84. Springer, Heidelberg (1988)
14. Boneh, D., Gentry, C., Lynn, B., Shacham, H.: Aggregate and verifiably encrypted signatures from bilinear maps. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 416–432. Springer, Heidelberg (2003)
15. Brickell, E.F., McCurley, K.S.: An interactive identification scheme based on discrete logarithms and factoring. In: Damgård, I.B. (ed.) EUROCRYPT 1990. LNCS, vol. 473, pp. 63–71. Springer, Heidelberg (1991)
16. Brown, D.: [Cfrg] key as message prefix => multi-key security. http://www.ietf.org/mail-archive/web/cfrg/current/msg07336.html, 2015
17. Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology, revisited (preliminary version). In: 30th ACM STOC, pp. 209–218. ACM Press, May 1998
18. Chatterjee, S., Koblitz, N., Menezes, A., Sarkar, P.: Another look at tightness II: practical issues in cryptography. Cryptology ePrint Archive, Report 2016/360 (2016). http://eprint.iacr.org/
19. Chaum, D., Pedersen, T.P.: Wallet databases with observers. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 89–105. Springer, Heidelberg (1993)
20. Fiat, A., Shamir, A.: How to prove yourself: practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987)
21. 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)
22. Fischlin, M., Lehmann, A., Ristenpart, T., Shrimpton, T., Stam, M., Tessaro, S.: Random oracles with(out) programmability. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 303–320. Springer, Heidelberg (2010)
23. Fleischhacker, N., Jager, T., Schröder, D.: On tight security proofs for schnorr signatures. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 512–531. Springer, Heidelberg (2014)
24. Fukumitsu, M., Hasegawa, S.: Black-box separations on Fiat-shamir-type signatures in the non-programmable random oracle model. In: López, J., Mitchell, C.J. (eds.) ISC 2015. LNCS, vol. 9290, pp. 3–20. Springer, Heidelberg (2015)
25. Galbraith, S.D., Malone-Lee, J., Smart, N.P.: Public key signatures in the multi-user setting. Inf. Process. Lett. **83**(5), 263–266 (2002)
26. Galindo, D.: The exact security of pairing based encryption and signature schemes. Based on a talk at Workshop on Provable Security, INRIA, Paris (2004). http://www.dgalindo.es/galindoEcrypt.pdf
27. 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)
28. Girault, M.: An identity-based identification scheme based on discrete logarithms modulo a composite number. In: Damgård, I.B. (ed.) EUROCRYPT 1990. LNCS, vol. 473, pp. 481–486. Springer, Heidelberg (1991)

29. Goh, E.-J., Jarecki, S., Katz, J., Wang, N.: Efficient signature schemes with tight reductions to the Diffie-Hellman problems. J. Cryptology **20**(4), 493–514 (2007)
30. Goldwasser, S., Micali, S., Rivest, R.L.: A digital signature scheme secure against adaptive chosen-message attacks. SIAM J. Comput. **17**(2), 281–308 (1988)
31. Guillou, L.C., Quisquater, J.-J.: A "Paradoxical" identity-based signature scheme resulting from zero-knowledge. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 216–231. Springer, Heidelberg (1990)
32. Hamburg, M.: Re: [Cfrg] EC signature: next steps (2015). https://mailarchive.ietf.org/arch/msg/cfrg/af170b6OrLyNZUHBMOPWxcDrVRI
33. Josefsson, S., Liusvaara, I.: Edwards-curve digital signature algorithm (EdDSA), 7 October 2015. https://tools.ietf.org/html/draft-irtf-cfrg-eddsa-00
34. Katz, J., Wang, N.: Efficiency improvements for signature schemes with tight security reductions. In: Jajodia, S., Atluri, V., Jaeger, T. (eds.) ACM CCS 2003, pp. 155–164. ACM Press, October 2003
35. Kiltz, E., Masny, D., Pan, J.: Optimal security proofs for signatures from identification schemes. Cryptology ePrint Archive, Report 2016/191 (2016). http://eprint.iacr.org/
36. Micali, S., Shamir, A.: An improvement of the Fiat-Shamir identification and signature scheme. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 244–247. Springer, Heidelberg (1990)
37. Ohta, K., Okamoto, T.: On concrete security treatment of signatures derived from identification. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 354–369. Springer, Heidelberg (1998)
38. Okamoto, T.: Provably secure and practical identification schemes and corresponding signature schemes. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 31–53. Springer, Heidelberg (1993)
39. Ong, H., Schnorr, C.-P.: Fast signature generation with a Fiat-Shamir-like scheme. In: Damgård, I.B. (ed.) EUROCRYPT 1990. LNCS, vol. 473, pp. 432–440. Springer, Heidelberg (1991)
40. 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)
41. Pointcheval, D., Stern, J.: Security arguments for digital signatures and blind signatures. J. Cryptology **13**(3), 361–396 (2000)
42. Schnorr, C.-P.: Efficient signature generation by smart cards. J. Cryptology **4**(3), 161–174 (1991)
43. 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)
44. Struik, R.: Re: [Cfrg] EC signature: next steps (2015). https://mailarchive.ietf.org/arch/msg/cfrg/TOWH1DSzB-PfDGK8qEXtF3iC6Vc