Tightly-Secure Signatures from Five-Move Identification Protocols

Eike Kiltz[1⋆], Julian Loss[1⋆⋆], and Jiaxin Pan[2⋆⋆⋆]

[1] Ruhr-Universität Bochum, Germany
{eike.kiltz,julian.loss}@rub.de
[2] Karlsruher Institut für Technologie, Germany
jiaxin.pan@kit.edu

Abstract. We carry out a concrete security analysis of signature schemes obtained from five-move identification protocols via the Fiat-Shamir transform. Concretely, we obtain tightly-secure signatures based on the computational Diffie-Hellman (CDH), the short-exponent CDH, and the Factoring (FAC) assumptions. All our signature schemes have tight reductions to search problems, which is in stark contrast to all known signature schemes obtained from the classical Fiat-Shamir transform (based on three-move identification protocols), which either have a non-tight reduction to a search problem, or a tight reduction to a (potentially) stronger decisional problem. Surprisingly, our CDH-based scheme turns out to be (a slight simplification of) the Chevallier-Mames signature scheme (CRYPTO 05), thereby providing a theoretical explanation of its tight security proof via five-move identification protocols.
Keywords: Signatures, Five-Move Identification Protocols, Fiat-Shamir, Tightness.

1 Introduction

The security of public-key cryptographic primitives is commonly analyzed via a security reduction to a suitable cryptographic assumption (such as the factoring assumption). Concretely, a security reduction converts a successful adversary A against the cryptographic scheme's security into a successful solver B against the hardness of the underlying assumption. If the reduction provides the bound $\varepsilon_{\mathsf{A}} \leq L \cdot \varepsilon_{\mathsf{B}}$ (where ε_{A} is A's success probability and ε_{B} is B's success probability) then L is called the (multiplicative) security loss of the reduction.[1] Clearly, it is desirable to have the security loss L as small as a constant so that $\varepsilon_{\mathsf{A}} \approx \varepsilon_{\mathsf{B}}$. If furthermore the running times of A and B are approximately the same, then the reduction is said to be *tight*. Cryptographic schemes with tight reductions recently drew a large amount of attention (e.g., [31, 18, 12, 13, 29, 30, 4]) due to

⋆ Eike Kiltz was partially supported by ERC Project ERCC (FP7/615074) and by DFG SPP 1736 Big Data.
⋆⋆ Julian Loss was supported by ERC Project ERCC (FP7/615074).
⋆⋆⋆ Jiaxin Pan was supported by the DFG grant HO 4534/4-1.
[1] We ignore the additive negligible terms to simplify our discussion.

the fact that tightly-secure schemes do not need to compensate for the security loss with increased parameters.

Digital signature schemes are one of the most important public-key cryptographic primitives. They have numerous applications and often serve as a building block for advanced cryptographic protocols. Ideally, we desire to have signature schemes with short signature sizes, efficient signing and verification algorithms, and tight security based on weak, well studied assumptions.

Tightness, Efficiency, and Decisional Assumptions. We will focus on signature schemes in the random oracle model [8] which usually have better efficiency than the ones in the standard model. Even in the random oracle model, there seems to be a prevalence of efficient, yet tightly-secure signature schemes based on decisional rather than search assumptions [34, 3, 33, 2]. Notable exceptions are the Rabin-Williams (RW) scheme from factoring (FAC) [9, 10], the BLS and RSA-PSS variants with the "selector bit" technique [9, 14, 26, 34], the Chevallier-Mames scheme (and its variants) (CM) from CDH [20, 26], and the Micali-Reyzin scheme (MR) from FAC [39, 7].

The Fiat-Shamir Transform and its Tightness. The Fiat-Shamir (FS) method [21] transforms a (canonical) three-move identification scheme ID into a digital signature scheme SIG[ID] using a hash function. A canonical identification scheme ID as formalized by [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., [21, 28, 11, 40, 49, 15, 23, 42, 41, 34, 26], the most popular among them being the scheme by Schnorr [49].

As discussed above, obtaining tightly secure signatures with short parameters has been proven to be notoriously hard. In particular, schemes obtained via the classical FS transform are usually proven via the Forking Lemma [46] and therefore are not tightly secure. For example, the Schnorr signature is obtained from the Fiat-Shamir transform and has an *inherently* loose security reduction [50, 22, 35] to the discrete logarithm problem. This issue was addressed by [34, 3] who showed how to improve the tightness of signature schemes obtained from the FS transform by basing their security on decisional assumptions such as DDH (and a short exponent variant thereof), quadratic residuosity, and (Ring)-LWE. However, to the best of our knowledge, there is currently no FS-derived signature scheme known which can be tightly proven secure under a *search assumption*. Moreover, there seems to be some evidence to support that this is impossible: the results of [22] show that the Schnorr scheme cannot be proven tightly secure under any non-interactive assumption. However, tight variants of the FS transform for three-move schemes may still exist if the scheme meets some additional requirements.

1.1 Our Contributions

In this work, we consider the Fiat-Shamir transform applied to a five-move identification scheme (rather than a three-move scheme). More precisely, we first formalize syntax and security of a five-move identification scheme and, following [35], provide a concrete and modular security analysis of the Fiat-Shamir transformed signature scheme. Next, we instantiate our framework to obtain schemes with security from search assumptions, such as the classical CDH and FAC assumptions. All our security reductions are tight.

Five-move Identification Schemes. A five-move identification scheme ID is an extension of the three-move identification scheme, where there are two "commitment-challenge" rounds (compared to one), followed by a final response output by the prover. (Each round has two moves, so five moves in total.) Intuitively, the additional rounds give us the handle to tightly embed the challenge of a search assumption. Following [35], we consider PIMP-KOA security (parallel impersonation against key-only attacks) of identification schemes where the adversary, given the public-key, tries to impersonate a prover in one of many parallel "commitment-challenge" sessions.

Fiat-Shamir for Five-Move Identification Schemes. We consider two variants FS[ID] and OF[ID] of the five-move Fiat-Shamir transformation. Both have tight security reductions given that the identification scheme has honest-verifier zero-knowledge (HVZK) and is secure against parallel impersonation attacks. [2] The two variants come with different trade-offs. OF[ID] requires *special soundness* but results in an online/offline signature scheme [52], which allows to pre-compute most of the signature in an offline phase to have a computationally cheap online signing phase (that requires knowledge of the message to be signed). FS[ID] does not require special soundness but does not come with the online/offline property. Interestingly, we are able to explain the Chevallier-Mames signature scheme [20] in our framework and show that it can be obtained from a five-move identification scheme by applying OF[ID]. We now give some details of our obtained signature schemes. A detailed comparison of their properties is given in Table 1.

A New Online/Offline Scheme With a Tight Security Reduction. Using our OF[ID] transform, we present a modified version of the Girault-Poupard-Stern (GPS) signature scheme [24]. The main interest of this scheme lies within its online signing step which can be made extremely efficient, given that most of the work can be precomputed in the *offline-step*, i.e., before seeing the message m. Concretely, the scheme only performs arithmetics over the integers in its online step, thereby even getting rid of modular reductions. [24] provide a loose security reduction to the Short-Exponent Discrete Logarithm (SEDL) assumption [36] which states that the discrete logarithm problem remains hard even if

[2] We also consider identification schemes with correctness error and statistical HVZK and define the notion of non-aborting HVZK. In this section, we ignore these for simplicity.

the discrete logarithm is known to lie in some fixed interval. Subsequently, [3] proved a tight reduction for the GPS scheme to the decisional variant of the SEDL [36]. However, so far, there has been no known tight reduction of the GPS scheme to a *search assumption*. Our scheme resolves this issue by offering a tight reduction to the Short Exponent CDH (SCDH) assumption. The relation between these aforementioned problems is explained in [36] as follows. First, the SEDL assumption is (non-tightly) equivalent to its decisional version. Second, the SCDH assumption is (non-tightly) equivalent to the assumption that both the full length CDH problem *and* the SEDL problem are hard.

A Tightly Secure Factoring-Based Scheme With Efficient Signing. As an application of our second transform, FS[ID], we present a new signature scheme with a tight security reduction to factoring. While our signature generation step and size are not quite as efficient than the ones of the factoring-based schemes of [39, 9, 10], our scheme highlights the usefulness of our (generic) FS[ID] transform.

A Tightly Secure Scheme from CDH. Our instantiation from CDH results in a slight simplification of the Chevallier-Mames signature scheme [20]. (Slight simplification in the sense that some inputs to the hash function can be left out in our scheme.) We believe that our framework provides interesting insights to the original scheme and underlines the usefulness of our (generic) OF[ID] transform.

Scheme	Origin	Approx. Size	Off-line Comp.	On-line Comp.	Ass.	Search Ass.?
KW	[26]	$k + \|p\|$	(2,0,0)	(0,1,1)	DDH	–
GJKW	[26]	$G + k + \|p\|$	(1,0,0)	(2,1,2)	CDH	✓
$\mathsf{FS}_{\mathsf{CDH}}$	new	$G + k + \|p\|$	(1,0,0)	(2,1,2)	CDH	✓
$\mathsf{OF}_{\mathsf{CDH}}$	[20]	$G + k + \|p\|$	(3,0,1)	(0,1,1)	CDH	✓
AFLT	[3]	$2k + c$	(1,0,0)	$(0, 1^*, 1)$	DSDL	–
$\mathsf{FS}_{\mathsf{SCDH}}$	new	$G + 2k + c$	(1,0,0)	$(2, 1^*, 2)$	SCDH	✓
$\mathsf{OF}_{\mathsf{SCDH}}$	new	$G + 2k + c$	(3,0,1)	$(0, 1^*, 1)$	SCDH	✓
MR	[39, §4.3]	$k + \|N\|$	$(1, 0, 0)$	$(1, \mathsf{const}, 1)$	FAC	✓
BR	[9]	$k + \|N\|$	$(0, 0, 0)$	$(0, \mathsf{const}, 1)$	FAC	✓
$\mathsf{FDH}_{\mathsf{RSA}}$	[33]	$\|N\|$	(0,0,0)	(1,0,1)	ΦH	–
$\mathsf{FS}_{\mathsf{FAC}}$	new	$G + k + \|N\|$	(1,0,0)	$(2, 1, 2)$	FAC	✓

Table 1: Comparison between some known tightly-secure signature schemes in the random oracle model. Top: schemes in a cyclic group $\mathbb{G}$ of prime order p. Bottom: schemes over $\mathbb{Z}_N$ for composite N. Elements of $\mathbb{G}$ have bit length G and k denotes the security parameter. $c < |p|$ is a parameter for the short Diffie-Hellman assumptions. Computational cost (x, y, z) denotes x modular exponentiations, y modular multiplications, and z hash operations, * indicates multiplication over integers, and const is a small constant.

1.2 Related Work

There exists a large body of literature on variants and improvements for the Fiat-Shamir transform. [35] give a concrete and modularized security treatment for signatures obtained from identification schemes via the Fiat-Shamir transform in both the multi- and single user settings which yields optimal security parameters for a wide array of important signatures in the ROM, in particular for Schnorr signatures. Our work is based on their modular framework. More recently, [7] put forth a new framework which includes multiple transforms that allow to tightly convert an ID scheme satisfying certain requirements into a signature. Their framework captures some existing transformations that have so far not received any theoretical treatment. Most notably, they give a characterization of the 'swap' method used in [38] to obtain a signature based tightly on the factoring assumption. [26, 2, 3] propose methods to obtain tight security for FS-derived signature schemes, with two of the schemes in [3] satisfying (conjectured) *post-quantum security*.

Deriving signature schemes from five-move ID schemes (or more generally from schemes with $2n + 1$ rounds) in an FS-like manner is a natural idea and thus has already been in the literature [51, 55, 54, 44, 45, 16, 17, 48, 53, 5, 19]. Surprisingly, many of them in the context of post-quantum security. However, none of these works proposes generic transforms for five-move ID schemes which makes the resulting proofs rather complex. Furthermore, none of the presented signature schemes admits a tight security reduction.

2 Preliminaries

2.1 Notations

We define $[N] := \{1, \ldots, N\}$ and $\mathbb{Z}_N := \mathbb{Z}/N\mathbb{Z}$ as the residual ring for an integer N. Let S be a finite set. $a \xleftarrow{\$} S$ denotes choosing an element a from S uniformly at random. Our algorithms are considered to be probabilistic polynomial time unless stated otherwise. If A is an algorithm, then $a \xleftarrow{\$} \mathsf{A}(b)$ denotes the random variable which is defined as the output of A on input b. With $a \in \mathsf{A}(b)$ we denote a possible output a of the execution of A on input b. When we want to make the randomness explicit, we use the notation $a := \mathsf{A}(b; \rho)$ meaning that the algorithm is executed on input b and randomness ρ. Note that A's execution is now deterministic.

2.2 Digital Signatures

We begin by defining syntax and security of a (digital) signature scheme. Let par denote some common system parameters shared among all participants.

Definition 1 (Signature Scheme). *A digital signature scheme* $\mathsf{SIG} := (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ *is defined as follow.*

- *The key generation algorithm* Gen *takes system parameters* par *as inputs and returns the public and secret keys* (pk, sk)*. We assume that* pk *implicitly defines a message space* $\mathcal{M}$ *and a signature space* Σ*.*
- *The signing algorithm* Sign *takes a secret key* sk *and a message* $m \in \mathcal{M}$ *as inputs and returns a signature* $\sigma \in \Sigma$*.*
- *The deterministic verification algorithm* Ver *takes a public key* pk*, a message* m *and a signature* σ *as inputs and returns 1 (accept) or 0 (reject).*

SIG *has correctness error* ρ *if for all* $(pk, sk) \in \mathsf{Gen}(\mathsf{par})$ *and all messages* $m \in \mathcal{M}$*, with probability at least* $1 - \rho$ $\mathsf{Sign}(sk, m)$ *outputs a valid signature* σ *such that* $\mathsf{Ver}(pk, m, \sigma) = 1$*.*

Definition 2 (UF-CMA Security). *A signature scheme* SIG *is said to satisfy* (t, ε, Q_s)-$\mathsf{UF\text{-}CMA}$ *security (unforgeability against chosen message attacks) if for all adversaries* A *running in time at most* t *and making at most* Q_s *queries to the signing oracle,*

$$\Pr\left[\begin{array}{l|l} \mathsf{Ver}(pk, m^*, \sigma^*) = 1 & (pk, sk) \xleftarrow{\$} \mathsf{Gen}(\mathsf{par}) \\ \wedge\ m^* \notin \mathcal{M} & (m^*, \sigma^*) \xleftarrow{\$} \mathsf{A}^{\textsc{Sign}(\cdot)}(pk) \end{array}\right] \leq \varepsilon,$$

where on query m *the signing oracle* $\textsc{Sign}$ *adds* m *to list* $\mathcal{M}$ *and returns* $\sigma \xleftarrow{\$} \mathsf{Sign}(sk, m)$ *to* A*, i.e., a signature on message* m *under public-key* pk*.*

As a special case of $\mathsf{UF\text{-}CMA}$ security, we define (t, ε)-$\mathsf{UF\text{-}KOA}$ security (unforgeability against key-only attacks) as $(t, \varepsilon, 0)$-$\mathsf{UF\text{-}CMA}$ security, i.e. $Q_s = 0$. In other words, the adversary is not allowed to make any signing query in the $\mathsf{UF\text{-}KOA}$ security experiment.

Security in the random oracle model. A common approach to analyze the security of signature schemes that involve a hash function is to use the random oracle model [8] in which hash queries are answered by an oracle H. H is defined as follows. On input x, it first checks whether $H(x)$ has previously been defined. If so, it returns $H(x)$. Otherwise, it sets $H(x)$ to a uniformly random value in the codomain of H and then returns $H(x)$. This allows us to parametrize the maximal number of hash queries in our security notions. As an example, we define $(t, \varepsilon, Q_s, Q_h)$-$\mathsf{UF\text{-}CMA}$ as security against any adversary that makes at most Q_h queries to H in the $\mathsf{UF\text{-}CMA}$ game. Furthermore, we make the standard convention that any random oracle query that is asked as a result of a query to the signing oracle in the $\mathsf{UF\text{-}CMA}$ game is also counted as a query to the random oracle. This implies that $Q_s \leq Q_h$.

2.3 Identification Schemes

A five-move identification protocol of the form depicted in Figure 1 is defined as follows.

Definition 3 (Five-move Identification Scheme). *A five-move identification scheme* $\mathsf{ID} := (\mathsf{IGen}, \mathsf{P}, \mathsf{ChSet}_1, \mathsf{ChSet}_2, \mathsf{V})$ *is defined as follow.*

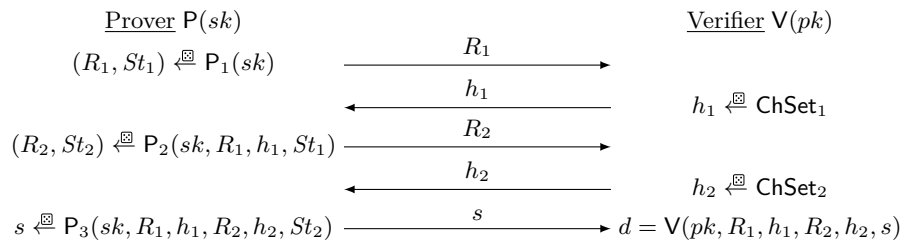

Fig. 1: A 5-move identification scheme and its transcript (R_1, h_1, R_2, h_2, s).

- *The key generation algorithm* IGen *takes system parameters* par *as input and returns a public key and a secret key* (pk, sk)*. We assume that* pk *defines two challenge sets* ChSet_1 *and* ChSet_2*.*
- *The prover algorithm* $\mathsf{P} = (\mathsf{P}_1, \mathsf{P}_2, \mathsf{P}_3)$ *is split into three algorithms.* P_1 *takes as input the secret key* sk *and returns a first-move commitment* R_1 *and a state* St_1*;* P_2 *takes as input the secret key* sk*, a first-move commitment* R_1*, a challenge* h_1*, and a state* St_1 *and returns a second-move commitment* R_2*;* P_3 *takes as input the secret key* sk*, a transcript* (R_1, h_1, R_2, h_2)*, and a state* St_2 *and returns a response* s*.*
- *The deterministic verifier algorithm* V *takes the public key* pk *and the conversation transcript as input and outputs a* decision*, 1 (acceptance) or 0 (rejection).*

We define some useful terms. A *transcript* for a canonical five-move identification scheme is of the form (R_1, h_1, R_2, h_2, s). A transcript (R_1, h_1, R_2, h_2, s) is *valid* (with respect to pk) if $\mathsf{V}(pk, R_1, h_1, R_2, h_2, s) = 1$ and it is *real* if it is output by the following algorithm $\mathsf{SKTran}(sk)$. We elaborate further on the purpose of SKTran below when defining the notion of naHVZK (non-aborting honest-verifier zero-knowledge).

$\underline{\mathsf{SKTran}(sk)}$:
$(R_1, St_1) \xleftarrow{\$} \mathsf{P}_1(sk)$
$h_1 \xleftarrow{\$} \mathsf{ChSet}_1$
$(R_2, St_2) \xleftarrow{\$} \mathsf{P}_2(sk, R_1, h_1, St_1)$
$h_2 \xleftarrow{\$} \mathsf{ChSet}_2$
$s \xleftarrow{\$} \mathsf{P}_3(sk, R_1, h_1, R_2, h_2, St_2)$
If $s = \perp$ then $T := (\perp, \perp, \perp, \perp, \perp)$
Else $T := (R_1, h_1, R_2, h_2, s)$
Return T

Definition 4 (Correctness error ρ). *We call an* ID *has correctness error* ρ *if, for all* $(pk, sk) \in \mathsf{IGen}(\mathsf{par})$*, the following holds:*

- *For all* $(R_1, h_1, R_2, h_2, s) \xleftarrow{\$} \mathsf{SKTran}(sk)$ *with* $s \neq \perp$*, we have* $\mathsf{V}(pk, R_1, h_1, R_2, h_2, s) = 1$*.*
- *A real transcript* (R_1, h_1, R_2, h_2, s) *contains* $s = \perp$ *with probability at most* ρ*, i.e.,* $\Pr[s = \perp \mid (R_1, h_1, R_2, h_2, s) \xleftarrow{\$} \mathsf{SKTran}(sk)] \leq \rho$*.*

Generalizing [35] we now define parallel impersonation against key-only attacks (KOA) for five-move identification schemes.

Definition 5 (Non-aborting (Parallel) Impersonation). *A five-move identification scheme* ID *is* $(t, \varepsilon, Q_{\mathrm{CH}_1}, Q_{\mathrm{CH}_2}, Q_{\mathrm{O}})$-$\mathsf{naPIMP\text{-}ATK}$ *secure (non-aborting parallel impersonation against* ATK *attacks,* $\mathsf{ATK} \in \{\mathsf{KOA}, \mathsf{PA}\}$*) if for all adversaries* A *running in time at most* t *and making at most* Q_{CH_1} *queries to the challenge oracle* CH_1 *and* Q_{CH_2} *queries to oracle* CH_2*, we have*

$$\Pr\left[\begin{array}{l}\mathsf{V}(pk, R_1, h_1, R_2, h_2, s^*) = 1 \\ \wedge\ (R_1, h_1) \in \mathcal{L}_1 \wedge\ (R_2, h_2) \in \mathcal{L}_2\end{array}\ \middle|\ \begin{array}{l}(pk, sk) \xleftarrow{\$} \mathsf{IGen}(\mathsf{par}) \\ s^* \xleftarrow{\$} \mathsf{A}^{\mathrm{CH}_1(\cdot), \mathrm{CH}_2(\cdot)}(pk, St)\end{array}\right] \leq \varepsilon,$$

where the challenge oracles $\mathrm{CH}_i(R_i)$ *(*$i \in \{1, 2\}$*) return* $h_i \xleftarrow{\$} \mathsf{ChSet}_i$ *to* A *and store* (R_i, h_i) *in set* $\mathcal{L}_i$*.*[3] *For different kinds of attacks, oracle* O *is defined as follows.*

- *If* $\mathsf{ATK} = \mathsf{KOA}$ *(key-only attack), then* O *always returns* $\perp$*.*
- *If* $\mathsf{ATK} = \mathsf{PA}$ *(passive attack), then* $\mathrm{O} := \textsc{Tran}$*, and the transcript oracle* $\textsc{Tran}()$ *returns a real transcript* $(R_1', h_1', R_2', h_2', s')$ *to* A*, i.e.,* $(R_1', h_1', R_2', h_2', s') \xleftarrow{\$} \mathsf{SKTran}(sk)$*.*

We do not use the parameter Q_{O} *for* $\mathsf{ATK} = \mathsf{KOA}$ *and simply speak of* $(t, \varepsilon, Q_{\mathrm{CH}_1}, Q_{\mathrm{CH}_2})$-$\mathsf{naPIMP\text{-}KOA}$*. Moreover,* $(t, \varepsilon, Q_{\mathrm{O}})$-$\mathsf{naIMP\text{-}ATK}$ *(*impersonation against ATK attack*) security is defined as* $(t, \varepsilon, 1, 1, Q_{\mathrm{O}})$-$\mathsf{naPIMP\text{-}ATK}$ *security, i.e., the adversary is only allowed* $Q_{\mathrm{CH}_1} = 1$ *query to the* CH_1 *oracle and* $Q_{\mathrm{CH}_2} = 1$ *to* CH_2*.*

Definition 6 (Special Soundness). *A five-move identification scheme* ID *is* SS *(special sound) if there exists an extractor* Ext *such that, for all* $(pk, sk) \in \mathsf{IGen}(\mathsf{par})$*, given any two valid transcripts* (R_1, h_1, R_2, h_2, s) *and* $(R_1, h_1', R_2', h_2', s')$ *with* $h_2 \neq h_2'$*, it outputs a valid secret key* sk^* *such that* $(pk, sk^*) \in \mathsf{IGen}(\mathsf{par})$*, i.e., we have* $\Pr[(sk^*, pk) \in \mathsf{IGen}(\mathsf{par}) \mid sk^* \xleftarrow{\$} \mathsf{Ext}(pk, R_1, h_1, R_2, h_2, s, h_1', R_2', h_2', s')] = 1$*. The winning condition* $(pk, sk^*) \in \mathsf{IGen}(\mathsf{par})$ *means that the tuple* (pk, sk^*) *is in the support of* $\mathsf{IGen}(\mathsf{par})$*, i.e., that* A *outputs a valid secret-key* sk^* *with respect to* pk*.*

We now introduce the notion of (statistical) *non-aborting honest-verifier zero-knowledge* [37], abbreviated as naHVZK. This notion generalizes the standard definition of honest-verifier zero-knowledge by including also identification schemes

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

ID with correctness error ρ. Note that a real run of ID might produce a transcript of the form $(R_1, h_1, R_2, h_2, \perp)$ with probability ρ. Unfortunately, it might not be efficiently possible to simulate a correctly distributed transcript in this case. Therefore, we again make use of the algorithm SKTran which on input a secret key sk internally generates a valid transcript of ID (with respect to the matching public key pk), but outputs $\perp$ if the transcript matches an execution of ID in which $s = \perp$. We now require an efficient simulator Sim that produces transcripts which are statistically close in distribution to the ones output by SKTran.

Definition 7 (Δ-Statistical Non-Aborting Honest-Verifier Zero-Knowledge with α Bits Min-Entropy). *A five-move identification scheme* ID *is said to be* Δ-statistically naHVZK (non-aborting honest-verifier zero-knowledge) with α bits min-entropy *if there exists an algorithm* Sim *that, given a valid public key* pk*, outputs* (R_1, h_1, R_2, h_2, s) *such that the distribution of* (R_1, h_1, R_2, h_2, s) *has statistical distance at most* Δ *from the distribution of a transcript output by* SKTran *on input* sk *and if for all* $(pk, sk) \in \mathsf{IGen}(\mathsf{par})$ *and strings* R_1', R_2' *we have*

$$\Pr\left[\, R_1 = R_1' \text{ or } R_2 = R_2' \;\middle|\; (R_1, h_1, R_2, h_2, s) \xleftarrow{\$} \mathsf{Sim}(pk) \,\right] \leq 2^{-\alpha}.$$

If $\Delta = 0$*, we say that* ID *is* perfectly naHVZK.

3 Signatures from Five-move Identification Schemes

We extend the generalized Fiat-Shamir transform [6] to construct signatures for 5-move identification schemes. We also present an online/offline variant of our transformation, where parts of the computation can be performed off-line which leads to a better performance in the signing step, but requires special soundness for the underlying identification schemes. Furthermore, we give an alternative Fiat-Shamir transform, which outputs shorter signatures, but retains the same security.

3.1 The Fiat-Shamir transform and its Online/Offline variant

Fix some system parameters par. Let $\mathsf{ID} := (\mathsf{IGen}, \mathsf{P}, \mathsf{ChSet}_1, \mathsf{ChSet}_2, \mathsf{V})$ be a five-move identification scheme and $H_1 : \{0,1\}^* \to \mathsf{ChSet}_1$ and $H_2 : \{0,1\}^* \to \mathsf{ChSet}_2$ be two hash functions. We also fix $\ell \in \mathbb{N}$ which controls the scheme's correctness. The signature scheme $\mathsf{FS}[\mathsf{ID}, H_1, H_2, \ell] := (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ from ID is defined as follows. Its online/offline variant $\mathsf{OF}[\mathsf{ID}, H_1, H_2, \ell] := (\mathsf{Gen}, \mathsf{Sign}_\mathsf{o}, \mathsf{Ver}_\mathsf{o})$ is defined with the boxed differences.

$\underline{\mathsf{Gen}(\mathsf{par})}$:	$\underline{\mathsf{Sign}(sk,m)}$, $\boxed{\mathsf{Sign}_{\mathsf{o}}(sk,m)}$:
$(pk,sk) \xleftarrow{\$} \mathsf{IGen}(\mathsf{par})$	$i := 0$
Return (pk,sk)	While $i \le \ell$ and $s = \bot$:
	$i := i+1$
$\underline{\mathsf{Ver}(pk,m,\sigma)}$, $\boxed{\mathsf{Ver}_{\mathsf{o}}(pk,m,\sigma)}$:	$(R_1, St_1) \xleftarrow{\$} \mathsf{P}_1(sk)$
Parse $\sigma = (R_1, R_2, s)$	$h_1 = H_1(R_1, m)$
$h_1 = H_1(R_1, m)$	$\boxed{h_1 = H_1(R_1)}$
$\boxed{h_1 = H_1(R_1)}$	$(R_2, St_2) \xleftarrow{\$} \mathsf{P}_2(sk, R_1, h_1, St_1)$
$h_2 = H_2(R_2, m)$	$h_2 = H_2(R_2, m)$
Return $\mathsf{V}(pk, R_1, h_1, R_2, h_2, s)$	$s \xleftarrow{\$} \mathsf{P}_2(sk, R_1, h_1, R_2, h_2, St_2)$
	If $s = \bot$ then $\sigma := \bot$
	Else $\sigma := (R_1, R_2, s)$
	Return σ

If ID has correctness error ρ, then both $\mathsf{FS}[\mathsf{ID}, H_1, H_2, \ell]$ and $\mathsf{OF}[\mathsf{ID}, H_1, H_2, \ell]$ are signature schemes with correctness error ρ^ℓ.

The following theorem states the security of $\mathsf{FS}[\mathsf{ID}, H_1, H_2, \ell]$ and $\mathsf{OF}[\mathsf{ID}, H_1, H_2, \ell]$.

Theorem 1 (Security of FS and OF). *Suppose that* ID *has* Δ*-statistical* naHVZK *with* α *bits min-entropy and is* $(t, \varepsilon, Q_{\mathrm{CH}_1}, Q_{\mathrm{CH}_2})$-naPIMP-KOA *secure. Then the signature scheme* $\mathsf{FS}[\mathsf{ID}, H_1, H_2, \ell]$ *is* $(t', \varepsilon', Q_s, Q_1, Q_2)$-UF-CMA*-secure in the random oracle model, where*

$$\varepsilon' \le \varepsilon + \tfrac{(Q_1+Q_2)Q_s}{2^\alpha} + Q_s \cdot \ell\Delta, \quad t \approx t', \quad Q_1 = Q_{\mathrm{CH}_1} - 1, \quad Q_2 = Q_{\mathrm{CH}_2} - 1,$$

and Q_{CH_1} *and* Q_{CH_2} *are upper bounds on the number of* CH_1 *and* CH_2 *queries in the* PIMP-KOA *experiment, respectively, and* Q_s, Q_1, *and* Q_2 *are upper bounds on the number of signing and random oracles* H_1 *and* H_2 *queries in the* UF-CMA *experiment, respectively. Moreover, if* ID *has special soundness (*SS*), then* $\mathsf{OF}[\mathsf{ID}, H_1, H_2, \ell]$ *is* $(t', \varepsilon', Q_s, Q_1, Q_2)$-UF-CMA*-secure in the random oracle model, where*

$$\varepsilon' \le \varepsilon + \tfrac{(Q_1+Q_2)Q_s}{2^\alpha} + Q_s \cdot \ell\Delta + \tfrac{1}{|\mathsf{ChSet}_2|}, \quad t \approx t',$$
$$Q_1 = Q_{\mathrm{CH}_1} - 2, \qquad Q_2 = Q_{\mathrm{CH}_2} - 2.$$

The proof of Theorem 1 is obtained by combining Lemmas 1 to 3.

Alternative Fiat-Shamir Transform. We call ID *partially commitment-recoverable* if the second-move commitment R_2 can be partitioned into $R_2 = (R_L, R_R)$, a left part R_L and a right part R_R, and $\mathsf{V}(pk, R_1, h_1, R_2, h_2, s)$ is such that it first recomputes $R_1' = \mathsf{V}_1(pk, h_2, s)$ and $R_R' = \mathsf{V}_2(pk, R_L, h_1, h_2, s)$ and then outputs 1 iff $(R_1', R_R') = (R_1, R_R)$. It is *fully commitment-recoverable* if $R_2 = R_R$ and R_L is the empty string. For commitment-recoverable ID, we can define an alternative Fiat-Shamir transformation $\mathsf{FS}'[\mathsf{ID}, H_1, H_2, \ell] := (\mathsf{Gen}, \mathsf{Sign}', \mathsf{Ver}')$, where Gen is as in $\mathsf{FS}[\mathsf{ID}, H_1, H_2, \ell]$. Algorithm $\mathsf{Sign}'(sk, m)$ is defined as $\mathsf{Sign}(sk, m)$ with the modified output $\sigma' = (R_L, h_2, s)$. Algorithm $\mathsf{Ver}'(pk, m, \sigma')$ first parses $\sigma' = (R_L, h_2, s)$, then recomputes $R_1' = \mathsf{V}_1(pk, h_2, s)$ and $R_R' := \mathsf{V}_2(pk, R_L, h_1, h_2, s)$,

where $h_1 = H_1(R_1')$, and finally returns 1 iff $H_2((R_L, R_R'), m) = h_2$. Its online/offline variant $\mathsf{OF}'[\mathsf{ID}, H_1, H_2, \ell] := (\mathsf{Gen}, \mathsf{Sign_o}', \mathsf{Ver_o}')$ is defined in the similar manner with the boxed differences.

$\underline{\mathsf{Gen}(\mathsf{par})}$:	$\underline{\mathsf{Sign}'(sk, m), \boxed{\mathsf{Sign_o}'(sk, m)}}$:
$(pk, sk) \xleftarrow{\$} \mathsf{IGen}(\mathsf{par})$	$i := 0$
Return (pk, sk)	While $i \leq \ell$ and $s = \bot$:
	$(R_1, St_1) \xleftarrow{\$} \mathsf{P}_1(sk)$
$\underline{\mathsf{Ver}'(pk, m, \sigma'), \boxed{\mathsf{Ver_o}'(pk, m, \sigma')}}$:	$h_1 = H_1(R_1, m)$
Parse $\sigma' = (R_L, h_2, s)$	$\boxed{h_1 = H_1(R_1)}$
$R_1 = \mathsf{V}_1(pk, h_2, s)$	$(R_2, St_2) \xleftarrow{\$} \mathsf{P}_2(sk, R_1, h_1, St_1)$
$h_1 = H_1(R_1, m)$	$h_2 = H_2(R_2, m)$
$\boxed{h_1 = H_1(R_1)}$	$s \xleftarrow{\$} \mathsf{P}_2(sk, R_1, h_1, R_2, h_2, St_2)$
$R_R = \mathsf{V}_2(pk, R_L, h_1, h_2, s)$	If $s = \bot$ then $\sigma' := \bot$
$R_2 = (R_L, R_R)$	Else $\sigma' = (R_L, h_2, s)$
If $h_2 = H_2(R_2, m)$	Return σ'
then return 1	
Else return 0	

Since $\sigma = (R_1, R_2, s)$ can be publicly transformed into $\sigma' = (R_L, h_2, s)$ and vice versa, $\mathsf{FS}[\mathsf{ID}, H_1, H_2, \ell]$ and $\mathsf{FS}'[\mathsf{ID}, H_1, H_2, \ell]$ are equivalent in terms of security. The same argument holds for $\mathsf{OF}[\mathsf{ID}, H_1, H_2, \ell]$ and $\mathsf{OF}'[\mathsf{ID}, H_1, H_2, \ell]$. On the one hand, the alternative Fiat-Shamir transform yields shorter signatures if $h_2 \in \mathsf{ChSet}_2$ has a smaller representation size than (R_1, R_R). 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.

Lemma 1 (UF-KOA security of FS and OF). *Suppose that* ID *is* $(t, \varepsilon, Q_{\mathrm{CH}_1}, Q_{\mathrm{CH}_2})$-naPIMP-KOA*-secure. Then the signature schemes* $\mathsf{FS}[\mathsf{ID}, H_1, H_2, \ell]$ *and* $\mathsf{OF}[\mathsf{ID}, H_1, H_2, \ell]$ *are* $(t', \varepsilon', Q_1, Q_2)$-UF-KOA*-secure in the random oracle model, where*

$$\varepsilon = \varepsilon', t \approx t', Q_1 = Q_{\mathrm{CH}_1} - 1, Q_2 = Q_{\mathrm{CH}_2} - 1,$$

and Q_1, Q_2 are upper bounds on the numbers of hash queries to H_1 and H_2, respectively.

Proof. We prove the statement for $\mathsf{OF}[\mathsf{ID}, H_1, H_2, \ell]$; the proof for $\mathsf{FS}[\mathsf{ID}, H_1, H_2, \ell]$ is identical. Assume that an adversary A breaks the $(t', \varepsilon', Q_1, Q_2)$-UF-KOA-security of $\mathsf{OF}[\mathsf{ID}, H_1, H_2, \ell]$. We construct an adversary B that breaks the $(t, \varepsilon, Q_{\mathrm{CH}_1}, Q_{\mathrm{CH}_2})$-PIMP-KOA security of ID, with $(t, \varepsilon, Q_{\mathrm{CH}_1}, Q_{\mathrm{CH}_2})$ as claimed.

At the beginning, after obtaining pk from the PIMP-KOA experiment, B forwards it to A. If A makes a query R_1 to the random oracle H_1, B returns $H_1(R_1)$ if it is already defined, otherwise B makes a query $h_1 \xleftarrow{\$} \mathrm{CH}_1(R_1)$ and programs $H_1(R_1) := h_1$. If A makes a query (R_2, m) to the random oracle H_2, B returns $H_2(R_2, m)$ if it is already defined, otherwise B makes a query $h_2 \xleftarrow{\$} \mathrm{CH}(R_2)$ and programs the random oracle $H_2(R_2, m) := h_2$.

Eventually, A submits a forgery $(m, \sigma = (R_1, R_2, s))$, and terminates. We assume that $h_1 := H_1(R_1)$ and $h_2 := H_2(R_2, m)$ were already queried by A.

(Otherwise, B queries $H_1(R_1)$ and $H_2(R_2, m)$ which are simulated as described above.) Hence, in total, there are $Q_{\text{CH}_1} = Q_1 + 1$ and $Q_{\text{CH}_2} = Q_2 + 1$ queries to H_1 and H_2, respectively. Adversary B outputs s and terminates. According to the simulations of H_1 and H_2, we have $(R_1, h_1) \in \mathcal{L}_1$ and $(R_2, h_2) \in \mathcal{L}_2$, and (R_1, h_1, R_2, h_2, s) is a valid transcript and hence breaks the PIMP-KOA security if A's forgery is valid. This establishes $\varepsilon = \varepsilon'$. The running time of B is roughly that of A, and thus $t' \approx t$.

Lemma 2 (UF-CMA security of FS). *If* ID *is Δ-statistically* naHVZK *with α-bits min-entropy and* $\mathsf{FS}[\mathsf{ID}, H_1, H_2, \ell]$ *is $(t, \varepsilon, Q_1, Q_2)$-*UF-KOA *secure, then* $\mathsf{FS}[\mathsf{ID}, H_1, H_2, \ell]$ *is $(t', \varepsilon', Q_s, Q'_1, Q'_2)$-*UF-CMA *secure in the random oracle model, where*

$$\varepsilon' \leq \varepsilon + \frac{(Q'_1 + Q'_2)Q_s}{2^\alpha} + Q_s \cdot \ell\Delta, \quad t' \approx t, \quad Q'_1 = Q_1 \quad Q'_2 = Q_2$$

and Q_1 and Q_2 are upper bounds on the numbers of hash queries to H_1 and H_2, respectively, and Q_s, Q'_1 and Q'_2 are upper bounds on the number of signing and hash queries to H'_1 and H'_2 in the UF-CMA *experiment, respectively.*

Proof. Assume that an adversary A breaks $(t', \varepsilon', Q_s, Q'_1, Q'_2)$-UF-CMA security of $\mathsf{FS}[\mathsf{ID}, H_1, H_2, \ell]$. We construct an adversary B invokes A and breaks $(t, \varepsilon, Q_1, Q_2)$-UF-KOA security of $\mathsf{FS}[\mathsf{ID}, H_1, H_2, \ell]$ with (t, ε) as stated in the lemma. Adversary B is executed in the UF-KOA experiment. It obtains public key pk and has access to random oracles H_1 and H_2.

Adversary B runs A on input pk answering hash queries to random oracles H'_1 and H'_2 and signing queries as follows.

Simulation of hash queries. A hash query $H'_1(R, m)$ is answered by B by querying its own hash oracle $H_1(R, m)$ and storing its answer and returning it. H'_2 is simulated in the same way by using B's own oracle H_2.

Simulation of signing queries. On A's signature query m, B uses the naHVZK property of ID to generate a signature σ on message m. Concretely, B defines $i := 0$ and simulates the signing query as follows.

- While $i \leq \ell$ and $s = \perp$:
  - $(R_1, h_1, R_2, h_2, s) \xleftarrow{\boxtimes} \mathsf{Sim}(pk)$ and $i := i + 1$;
- If $s = \perp$, then return $\perp$;
- Else
  - If $H'_1(R_1, m) \neq \perp$ or $H'_2(R_2, m) \neq \perp$, then define Incon $:= 1$ and return $\perp$
  - Else define
$$H'_1(R_1, m) := h_1, \; H'_2(R_2, m) := h_2 \tag{1}$$
and return $\sigma := (R_1, R_2, s)$.

We note that, by Equation (1), B makes the hash functions inconsistent, since $H_1(R_1, m) \neq h_1 =: H'_1(R_1, m)$ and $H_2(R_2, m) \neq h_2 =: H'_2(R_2, m)$ with high probability. Adversary A can detect this inconsistence if Incon $= 1$, namely, A queries the exact $H'_1(R_1, m)$ or $H'_2(R_2, m)$ before asking the signing query on

m. For each signing query, this can be bounded (namely, B aborts because of $\textsc{Incon} = 1$) by probability at most $(Q'_1+Q'_2)/2^\alpha$, since ID has α-bits min-entropy. Moreover, for each signing query, B runs Sim at most ℓ times and produces a real transcript from $\mathsf{SKTran}(sk)$ oracle with statistical distance at most Δ in each of these runs. Since the number of signing queries is bounded by Q_s, the statistical distance between the real $\mathsf{UF\text{-}CMA}$ experiment and the simulated one is at most $Q_s \cdot ((Q'_1 + Q'_2)/2^\alpha + \ell\Delta)$.

Forgery. Eventually, A submits its forgery $(m, \sigma := (R_1, R_2, s))$. We assume that it is a valid forgery in the $\mathsf{UF\text{-}CMA}$ experiment, namely, for $h_1 = H'_1(R_1, m)$ and $h_2 = H'_2(R_2, m)$ we have $\mathsf{V}(pk, R_1, h_1, R_2, h_2, s) = 1$. Furthermore, it satisfies the freshness condition, i.e., $m \notin \mathcal{M}$. Note that by the freshness condition, we have $H_1(R_1, m) = H'_1(R_1, m) = h_1$ and $H_2(R_2, m) = H'_2(R_2, m) = h_2$ since $H'_1(R_1, m)$ and $H'_2(R_2, m)$ were not programmed via (1). After receiving A's forgery, B computes a forgery for the $\mathsf{UF\text{-}KOA}$ experiment as $\sigma = (R_1, R_2, s)$.

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

$$\varepsilon \geq \varepsilon' - \frac{(Q'_1 + Q'_2)Q_s}{2^\alpha} - Q_s \cdot \ell\Delta.$$

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

Lemma 3 ($\mathsf{UF\text{-}CMA}$-security of OF). *If ID is Δ-statistically naHVZK with α-bits min-entropy, has SS, and $\mathsf{OF}[\mathsf{ID}, H_1, H_2, \ell]$ is $(t, \varepsilon, Q_1, Q_2)$-$\mathsf{UF\text{-}KOA}$ secure, then $\mathsf{OF}[\mathsf{ID}, H_1, H_2, \ell]$ is $(t', \varepsilon', Q_s, Q'_1, Q'_2)$-$\mathsf{UF\text{-}CMA}$ secure in the random oracle model, where*

$$\varepsilon' \leq \varepsilon + \frac{(Q'_1 + Q'_2)Q_s}{2^\alpha} + Q_s \cdot \ell\Delta + \frac{1}{|\mathsf{ChSet}_2|}, \quad t' \approx t, \quad Q'_1 = Q_1 - 1 \quad Q'_2 = Q_2 - 1$$

and Q_1 and Q_2 are upper bounds on the numbers of hash queries to H_1 and H_2, respectively, and Q_s, Q'_1 and Q'_2 are upper bounds on the number of signing and hash queries to H'_1 and H'_2 in the $\mathsf{UF\text{-}CMA}$ experiment, respectively.

Proof. Let A be an algorithm that breaks $(t', \varepsilon', Q_s, Q'_1, Q'_2)$-$\mathsf{UF\text{-}CMA}$ security of $\mathsf{OF}[\mathsf{ID}, H_1, H_2, \ell]$. We will describe an adversary B invoking A that breaks $(t, \varepsilon, Q_1, Q_2)$-$\mathsf{UF\text{-}KOA}$ security of $\mathsf{OF}[\mathsf{ID}, H_1, H_2, \ell]$ with (t, ε) as stated in the lemma. Adversary B is executed in the $\mathsf{UF\text{-}KOA}$ experiment and obtains public-key pk, and has access to random oracles H_1 and H_2.

Adversary B runs A on input pk answering hash queries to random oracles H'_1 and H'_2 and signing queries as follows.

Simulation of hash queries. A hash query $H'_1(R)$ is answered by B by querying its own hash oracle $H_1(R)$ and storing its answer and returning it. H'_2 is simulated in the same way by using B's own oracle H_2.

Simulation of signing queries. The simulation here is similar to that in Lemma 2 except for the simulation of H'_1. For completeness, we present the details as follows.

On A's signature query m, B uses the naHVZK property of ID to generate a signature σ on message m. Concretely, B defines $i := 0$ and simulates the signing query as follows.

- While $i \leq \ell$ and $s = \perp$:
  - $(R_1, h_1, R_2, h_2, s) \xleftarrow{\boxtimes} \mathsf{Sim}(pk)$ and $i := i + 1$;
- If $s = \perp$, then return $\perp$;
- Else
  - If $H'_1(R_1) \neq \perp$ or $H'_2(R_2, m) \neq \perp$, then define $\textsc{Incon} := 1$ and return $\perp$
  - Else define
$$H'_1(R_1) := h_1,\ H'_2(R_2, m) := h_2 \tag{2}$$
    and return $\sigma := (R_1, R_2, s)$.

We note that, by Equation (2), B makes the hash functions inconsistent, since $H_1(R_1) \neq h_1 =: H'_1(R_1)$ and $H_2(R_2, m) \neq h_2 =: H'_2(R_2, m)$ with high probability. Adversary A can detect this inconsistence if $\textsc{Incon} = 1$, namely, A queries the exact $H'_1(R_1)$ or $H'_2(R_2, m)$ before asking the signing query on m. For each signing query, this can be bounded (namely, B aborts because of $\textsc{Incon} = 1$) by probability at most $(Q'_1 + Q'_2)/2^\alpha$, since ID has α-bits min-entropy. Moreover, for each signing query, B runs Sim at most ℓ times and produces a real transcript from $\mathsf{SKTran}(sk)$ oracle with statistical distance at most Δ in each of these runs. Since the number of signing queries is bounded by Q_s, the statistical distance between the real UF-CMA experiment and the simulated one is at most $Q_s \cdot ((Q'_1 + Q'_2)/2^\alpha + \ell\Delta)$.

Forgery. Eventually, A will submit its forgery $(m, \sigma := (R_1, R_2, s))$. We assume that it is a valid forgery in the UF-CMA experiment, namely, for $h_1 = H'_1(R_1)$ and $h_2 = H'_2(R_2, m)$ we have $\mathsf{V}(pk, R_1, h_1, R_2, h_2, s) = 1$. Furthermore, it satisfies the freshness condition, i.e., $m \notin \mathcal{M}$. After receiving A's forgery, B computes a forgery for the UF-KOA experiment according to the following case distinction.

- Case 1: R_1 was defined in a signing query on some message m' via (2), i.e., $(R_1, h'_1, R'_2, h'_2, s')$ was generated by using $\mathsf{Sim}(pk)$. The freshness condition implies $m' \neq m$ and hence $h_2 = H'_2(R_2, m) \neq H'_2(R'_2, m') = h'_2$, except with probability $1/|\mathsf{ChSet}_2|$. In that case we have two valid transcripts (R_1, h_1, R_2, h_2, s) and $(R_1, h'_1, R'_2, h'_2, s')$ with $h_2 \neq h'_2$. By the special soundness of ID, B extracts a valid sk^* by running Ext such that $(pk, sk^*) \in \mathsf{IGen}(\mathsf{par})$, and then B use sk^* to generate a fresh and valid UF-CMA forgery. In this case, $Q'_1 = Q_1 + 1$ and $Q'_2 = Q_2 + 1$.
- Case 2: R_1 was queried to the H'_1 oracle, i.e., $H_1(R_1) = H'_1(R_1) = h_1$. By the freshness condition, $h_2 = H'_2(R_2, m)$ was defined in a hash query, but not in a signing query, i.e., $h_2 = H'_2(R_2, m) = H_2(R_2, m)$. B returns $\sigma = (R_1, R_2, s)$ as a valid forgery to its UF-CMA experiment.

Overall, B returns a valid forgery of UF-KOA experiment with probability

$$\varepsilon \geq \varepsilon' - \frac{(Q'_1 + Q'_2)Q_s}{2^\alpha} - Q_s \cdot \ell\Delta - \frac{1}{|\mathsf{ChSet}_2|}.$$

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

4 Instantiations

In the following, 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.

4.1 Instantiation from CDH

We briefly recall the CDH problem.

Definition 8 (Computation Diffie-Hellman Assumption). *The computational Diffie-Hellman problem* CDH *is* (t, ε)*-hard in* par *if for all adversaries* A *running in time at most* t*,*

$$\Pr\left[Z = g^{xy} \mid x, y \xleftarrow{\$} \mathbb{Z}_p; Z \xleftarrow{\$} \mathsf{A}(g^x, g^y)\right] \leq \varepsilon.$$

Identification Scheme. The identification scheme $\mathsf{ID}_{\mathsf{CDH}} := (\mathsf{IGen}, \mathsf{P}, \mathsf{ChSet}_1, \mathsf{ChSet}_2, \mathsf{V})$ is defined as follows.

$\underline{\mathsf{IGen}(\mathsf{par})}$:	$\underline{\mathsf{P}_1(sk)}$:
$sk := x \xleftarrow{\$} \mathbb{Z}_p$	$St_1 := r \xleftarrow{\$} \mathbb{Z}_p$; $R_1 = g^r$
$pk := X = g^x$	Return (R_1, St_1)
$\mathsf{ChSet}_1 := \mathbb{G}$; $\mathsf{ChSet}_2 := \{0, ..., 2^k - 1\}$	
Return (pk, sk)	$\underline{\mathsf{P}_2(sk, R_1, h_1, St_1)}$:
	Parse $St_1 := r$
$\underline{\mathsf{V}(pk, R_1, h_1, R_2, h_2, s)}$:	$R_L := h_1^x$; $R_R := h_1^r$
Parse $R_2 := (R_L, R_R)$	Return $(R_2 := (R_L, R_R), St_2 := r)$
If $R_1 = g^s \cdot X^{-h_2}$ and $R_R = h_1^s \cdot R_L^{-h_2}$	
then return 1	$\underline{\mathsf{P}_3(sk, R_1, h_1, R_2, h_2, St_2)}$:
Else return 0	Parse $St_2 = r$
	Return $s = x \cdot h_2 + r \bmod p$

Lemma 4. $\mathsf{ID}_{\mathsf{CDH}}$ *is a perfectly correct five-move identification scheme and has perfect non-aborting honest-verifier zero-knowledge (*naHVZK*) with* $\alpha = \log p$ *bits min-entropy and special soundness (*SS*). Moreover, if* CDH *is* (t, ε)*-hard in* $\mathsf{par} = (p, g, \mathbb{G})$ *then* $\mathsf{ID}_{\mathsf{CDH}}$ *is* $(t', \varepsilon', Q_{\mathrm{CH}_1}, Q_{\mathrm{CH}_2})$-$\mathsf{PIMP\text{-}KOA}$ *secure, where* $t \approx t'$ *and* $\varepsilon \geq \varepsilon' - \frac{Q_{\mathrm{CH}_2}}{2^k}$.

Proof. The perfect correctness of $\mathsf{ID}_{\mathsf{CDH}}$ is straightforward to verify. We show the other properties as follows:

Perfect Non-Aborting Honest-Verifier Zero-Knowledge (naHVZK). Given public key $pk = X$, Sim first samples $s, w, h_2 \xleftarrow{\$} \mathbb{Z}_p$. It then computes $h_1 := g^w$, $R_1 := g^s X^{-h_2}$, $R_L := X^w$, and $R_R := R_1^w$, defines $R_2 := (R_L, R_R)$ and outputs the transcript (R_1, h_1, R_2, h_2, s). Clearly, (R_1, h_1, R_2, h_2, s) is distributed the same as the one from $\mathsf{SKTran}(sk)$, since s is uniformly random over $\mathbb{Z}_p$ and R_1, R_L and R_R satisfy $R_1 = g^s \cdot X^{-h_2}$ and $R_R = h_1^s \cdot R_L^{-h_2}$. Moreover, we note that the entropy of $(R_1, St_1 := r) \xleftarrow{\$} \mathsf{P}_1(sk)$ and $(R_2, St_2) \xleftarrow{\$} \mathsf{P}_2(sk, R_1, h_1)$

comes only from R_1, which is uniformly random over $\mathbb{G}$. Hence, since the outputs of $\mathsf{Sim}(pk)$ are identically distributed to the outputs of $\mathsf{SKTran}(sk)$, $\mathsf{ID}_{\mathsf{CDH}}$ has $\log|\mathbb{G}| = \log p$ bits min-entropy as claimed.

Special Soundness. Given two accepting transcripts (R_1, h_1, R_2, h_2, s) and $(R_1, h_1', R_2', h_2', s')$ with $h_2 \neq h_2'$, we define an extractor Ext with the property that $\mathsf{Ext}(pk, R_1, h_1, R_2, h_2, s, h_1', R_2', h_2', s')$ outputs $x^* := (s - s_i')/(h_2 - h_2') \bmod p$. We have $\Pr[g^{x^*} = X] = 1$ for all $(X := g^x, x) \in \mathsf{IGen}(\mathsf{par})$, since $R_1 = g^s \cdot X^{-h_2} = g^{s'} \cdot X^{-h_2'}$ and $X = g^{(s-s')/(h_2-h_2')}$.

PIMP-KOA-Security. Let A be an attacker against the $(t', \varepsilon', Q_{\mathrm{CH}_1}, Q_{\mathrm{CH}_2})$-$\mathsf{PIMP\text{-}KOA}$ security of $\mathsf{ID}_{\mathsf{CDH}}$. We construct an attacker B that (t, ε)-breaks CDH.

Construction of B. Let $(X := g^x, Y := g^y)$ denote the CDH instance. B runs A with input $pk := X$ and answers A's challenge queries as follows.

For A's CH_1 query on $R_1 \in \mathbb{G}$, B chooses $a \xleftarrow{\boxdot} \mathbb{Z}_p$ and computes $h_1 = Y \cdot g^a$. For A's CH_2 query on $R_2 \in \mathbb{G} \times \mathbb{G}$, B chooses $h_2 \xleftarrow{\boxdot} \mathbb{Z}_p$ and returns it to A. Clearly, B's simulation of the $\mathsf{PIMP\text{-}KOA}$ game is perfect, since both h_1 and h_2 are uniformly random over $\mathbb{G}$ and $\mathbb{Z}_p$, respectively.

Eventually, A returns its response s^* for the $\mathsf{PIMP\text{-}KOA}$ experiment. We assume that A's response is valid, i.e., there exist $(R_1, h_1) \in \mathcal{L}_1$ and $(R_2 := (R_L, R_R), h_2) \in \mathcal{L}_2$ such that $R_1 = g^{s^*} \cdot X^{-h_2}$ and $R_R = h_1^{s^*} \cdot R_L^{-h_2}$. We denote the discrete logarithm of R_L based on h_1 by $x' = \mathsf{DL}_{h_1}(R_L)$ and do the following cases distinction:

- Case 1: $x = x'$. By the simulation of CH_1, we have $R_L = h_1^x = (Yg^{a_i})^x = Y^x X^{a_i}$ for some $i \in [Q_{\mathrm{CH}_1}]$. Thus, B returns $Z := R_L \cdot X^{-a_i} = Y^x$ to break the CDH problem.
- Case 2: $x \neq x'$. We show in this case even an unbounded adversary A can only win with probability $Q_{\mathrm{CH}_2}/2^k$. For each index $i \in [Q_{\mathrm{CH}_2}]$, before receiving $h_{2,i}$, A first commits to some $R_1 = g^{r_1}$, $R_L = h_1^{x'}$ and $R_R = h_1^{r_2}$ (for arbitrary $r_1, r_2, x' \in \mathbb{Z}_p$ and $x' \neq x$) and there exists $(R_1, h_1) \in \mathcal{L}_1$. A can only win if there exists an $s_i \in \mathbb{Z}_p$ such that

$$r_1 + h_{2,i}x = s_i = r_2 + h_{2,i}x' \Leftrightarrow h_{2,i} = \tfrac{r_2 - r_1}{x - x'}.$$

  where $h_{2,i} \xleftarrow{\boxdot} \mathsf{ChSet}_2 := \{0, ..., 2^k - 1\}$ is chosen independently of r_1, r_2 and x'. This happens with probability at most $1/|\mathsf{ChSet}_2| = 2^{-k}$. By the union bound we obtain the bound $Q_{\mathrm{CH}_2}/2^k$ as claimed.

Overall, B returns a valid solution of the CDH challenge with probability $\varepsilon \geq \varepsilon' - \frac{Q_{\mathrm{CH}_2}}{2^k}$. This completes the proof.

(Online/offline) Signature. Let $H_1 : \{0,1\}^* \to \mathbb{G}$ and $H_2 : \{0,1\}^* \to \{0, ..., 2^k - 1\}$ be two hash functions. As $\mathsf{ID}_{\mathsf{CDH}}$ is perfectly correct and partially commitment-recoverable, we can use the alternative Fiat-Shamir transformation from Section 3.1 with $\ell := 1$ to obtain the signature scheme $\mathsf{FS}_{\mathsf{CDH}} := (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ and its online/offline variant $\mathsf{OF}_{\mathsf{CDH}} := (\mathsf{Gen}, \mathsf{Sign}_{\mathsf{o}}, \mathsf{Ver}_{\mathsf{o}})$. Here, $\mathsf{FS}_{\mathsf{CDH}}$ does not include X, R_1 and (g, h_1) in the hash H_2, which is slightly simpler than the Chevallier-Mames scheme in [20].

$\mathsf{Gen}(\mathsf{par})$:	$\mathsf{Sign}(sk, m)$, $\boxed{\mathsf{Sign}_\circ(sk, m)}$:	$\mathsf{Ver}(pk, m, \sigma)$, $\boxed{\mathsf{Ver}_\circ(pk, m, \sigma)}$:
$sk := x \xleftarrow{\$} \mathbb{Z}_p$	$r \xleftarrow{\$} \mathbb{Z}_p$; $R_1 = g^r$	Parse $\sigma := (R_L, h_2, s)$
$pk := X = g^x$	$h_1 = H_1(R_1, m)$; $\boxed{h_1 = H_1(R_1)}$	$R_1 = g^s \cdot X^{-h_2}$
Return (pk, sk)	$R_L = h_1^x \in \mathbb{G}$; $R_R = h_1^r$	$h_1 = H_1(R_1, m)$; $\boxed{h_1 = H_1(R_1)}$
	$R_2 := (R_L, R_R)$	$R_R = h_1^s \cdot R_L^{-h_2}$
	$h_2 = H_2(R_2, m) \in \{0, ..., 2^k - 1\}$	$R_2 := (R_L, R_R)$
	$s = x \cdot h_2 + r \in \mathbb{Z}_p$	If $h_2 = H_2(R_2, m)$
	$\sigma = (R_L, h_2, s)$	then return 1
	Return σ	Else return 0.

By Lemma 4 and Theorem 1, we have

Theorem 2 (Security of $\mathsf{FS}_{\mathsf{CDH}}$ and $\mathsf{OF}_{\mathsf{CDH}}$). *If* CDH *is* (t, ε)*-hard in* $\mathsf{par} := (p, g, \mathbb{G})$ *then scheme* $\mathsf{FS}_{\mathsf{CDH}}$ *is* $(t', \varepsilon', Q_s, Q_1, Q_2)$-UF-CMA *secure and scheme* $\mathsf{OF}_{\mathsf{CDH}}$ *is* $(t'', \varepsilon'', Q_s, Q_1, Q_2)$-UF-CMA *secure in the programmable random oracle model, where*

$$\varepsilon' \leq \varepsilon + \frac{Q_2 + 1}{2^n} + \frac{(Q_1 + Q_2)Q_s}{2^n}, \qquad t' \approx t,$$

$$\varepsilon'' \leq \varepsilon + \frac{Q_2 + 2}{2^n} + \frac{(Q_1 + Q_2)Q_s}{2^n} + \frac{1}{2^n}, \qquad t'' \approx t.$$

4.2 Instantiation from Short CDH

We recall the short exponent CDH assumption from [36].

Definition 9 (c-SCDH Assumption). *The c-short exponent computational Diffie-Hellman problem c-*SCDH *is* (t, ε)*-hard in* par *if for all adversaries* A *running in time at most t,*

$$\Pr\left[Z = g^{xy} \mid x, y \xleftarrow{\$} \{0, ..., 2^c - 1\}; Z \xleftarrow{\$} \mathsf{A}(g^x, g^y)\right] \leq \varepsilon.$$

Identification Scheme. Let $\mathsf{par} := (p, g, \mathbb{G}, k, k', c)$ be a set of system parameters, where $\mathbb{G} = \langle g \rangle$ is a cyclic group of prime order p with a hard c-SCDH problem and $k = \omega(\log p)$. The identification scheme $\mathsf{ID}_{\mathsf{SCDH}} := (\mathsf{IGen}, \mathsf{P}, \mathsf{ChSet}_1, \mathsf{ChSet}_2, \mathsf{V})$ is defined as follows. Here the response s is computed over the integers (rather than over $\mathbb{Z}_p$).

$\underline{\mathsf{IGen}(\mathsf{par})}$:	$\underline{\mathsf{P}_1(sk)}$:
$sk := x \xleftarrow{\boxdot} \{0,...,2^c-1\}$	$St_1 := r \xleftarrow{\boxdot} \{0,...,2^{k+k'+c}-1\}$;
$pk := X = g^x$	$R_1 = g^r$
$\mathsf{ChSet}_1 := \mathbb{G}$; $\mathsf{ChSet}_2 := \{0,...,2^k-1\}$	Return (R_1, St_1)
Return (pk, sk)	
	$\underline{\mathsf{P}_2(sk, R_1, h_1, St_1)}$:
$\underline{\mathsf{V}(pk, R_1, h_1, R_2, h_2, s)}$:	Parse $St_1 := r$
Parse $R_2 := (R_L, R_R)$	$R_L = h_1^x$; $R_R = h_1^r$
If $s \notin \{2^{k+c},...,2^{k+k'+c}-1\}$	$R_2 := (R_L, R_R)$; $St_2 := St_1$
then return 0	Return (R_2, St_2)
If $R_1 = g^s X^{-h_2}$ and $R_R = h_1^s R_L^{-h_2}$	
then return 1	$\underline{\mathsf{P}_3(sk, R_1, h_1, R_2, h_2, St_2)}$:
Else return 0	Parse $St_2 := r$
	$s = x \cdot h_2 + r$
	If $s \notin \{2^{k+c},...,2^{k+k'+c}-1\}$
	then return $\perp$
	Else return s

Lemma 5 ([3]). *Let $x \xleftarrow{\boxdot} \{0,...2^c-1\}, h_2 \xleftarrow{\boxdot} \{0,...,2^k-1\}, r \xleftarrow{\boxdot} \{0,...,2^{k'+k+c}-1\}$. Then, $s := xh_2 + r \in \{2^{k+c},...,2^{k'+k+c}-1\}$ with probability $1-2^{-k'}$. Moreover, if $s \in \{2^{k+c},...,2^{k'+k+c}-1\}$, then it is uniformly distributed in this interval.*

Lemma 6. $\mathsf{ID}_{\mathsf{SCDH}}$ *is a five-move identification scheme with correctness error $2^{-k'}$ and has perfect non-aborting honest-verifier zero-knowledge (*naHVZK*) with $\alpha = c$ bits min-entropy and special soundness. Moreover, if c-*SCDH *is (t,ε)-hard in* $\mathsf{par} = (p, g, \mathbb{G})$ *then* $\mathsf{ID}_{\mathsf{SCDH}}$ *is $(t', \varepsilon', Q_{\mathrm{CH}_1}, Q_{\mathrm{CH}_2})$-*PIMP-KOA*-secure, where $\varepsilon' \le \varepsilon + Q_{\mathrm{CH}_2}/2^k$ and $t' \approx t$.*

Proof. By Lemma 5, $\mathsf{ID}_{\mathsf{SCDH}}$ has correctness error $2^{-k'}$. We note that the entropy of $R_1 = g^r$ and $R_2 := (h_1^x, h_1^r)$ comes only from r, which is chosen uniformly from $\{0,...,2^c-1\}$. Hence $\mathsf{ID}_{\mathsf{SCDH}}$ has c bits min-entropy. We show the other properties as follows.

PERFECT naHVZK. Given public key $pk = X$, simulator Sim first samples $s \xleftarrow{\boxdot} \{2^{k+c},...,2^{k'+k+c}-1\}, w \xleftarrow{\boxdot} \mathbb{Z}_p$ and $h_2 \leftarrow \{0,...,2^k-1\}$. It then computes $h_1 = g^w, R_1 = g^s X^{-h_2}, R_L = X^w$, and $R_R = R_1^w$, defines $R_2 := (R_L, R_R)$ and outputs the transcript (R_1, h_1, R_2, h_2, s) with probability $1-2^{-k'}$, or $(\perp,\perp,\perp,\perp,\perp)$ with probability $2^{-k'}$. Clearly, the output of $\mathsf{Sim}(pk)$ is identical to that of $\mathsf{SKTran}(sk)$. According to the simulation, with probability $1-2^{-k'}$, $\mathsf{Sim}(pk)$ will output a transcript (R_1, h_1, R_2, h_2, s), where s is uniformly random over the interval $\{2^{k+c},...,2^{k'+k+c}-1\}$ and R_1, R_L and R_R are values satisfying $R_1 = g^s \cdot X^{-h_2}$ and $R_R = h_1^s \cdot R_L^{-h_2}$. Due to Lemma 5, the probability that such a transcript is output by Sim is the same as that for SKTran, and, moreover, the probability that Sim outputs $(\perp,\perp,\perp,\perp,\perp)$ is also the same as that for SKTran. We note that the entropy of $R_1 = g^r$ and $R_2 := (h_1^x, h_1^r)$ comes only from r, which is chosen uniformly from $\{0,...,2^c-1\}$. Since $\mathsf{Sim}(pk)$ outputs transcripts identically distributed to the ones output by $\mathsf{SKTran}(sk)$, $\mathsf{ID}_{\mathsf{SCDH}}$ has c bits min-entropy. Thus, $\mathsf{ID}_{\mathsf{SCDH}}$ is perfectly naHVZK.

Special Soundness. Given two accepting transcripts (R_1, h_1, R_2, h_2, s) and $(R_1, h_1', R_2', h_2', s')$ with $h_2 \neq h_2'$, we define an extractor Ext with the property that $\mathsf{Ext}(pk, R_1, h_1, R_2, h_2, s, h_1', R_2', h_2', s')$ outputs $x^* := (s - s_i')/(h_2 - h_2')$. We note that $x^* \in \{0, ..., 2^c - 1\}$, since $s, s_i' \in \{2^{k+c}, ..., 2^{k+k'+c} - 1\}$ and $h_2, h_2' \in \{0, ..., 2^k\}$. Moreover, for all $(X := g^x, x) \in \mathsf{IGen}(\mathsf{par})$, we have $\Pr[X = g^{x^*}] = 1$, since $R_1 = g^s X^{-h_2} = g^{s'} X^{-h_2'}$ and then $X = g^{(s-s')/(h_2 - h_2')}$.

$\mathsf{PIMP\text{-}KOA}$-security. Let A be an attacker against the $(t', \varepsilon', Q_{\mathrm{CH}_1}, Q_{\mathrm{CH}_2})$-$\mathsf{PIMP\text{-}KOA}$ security of $\mathsf{ID}_{\mathsf{SCDH}}$. We construct an attacker B that (t, ε)-breaks c-SCDH.

Construction of B. Let $(X := g^x, Y := g^y)$ denote the c-SCDH instance. B runs A with input $pk := X$ and answers A's challenge queries as follows.

For A's CH_1 query on $R_1 \in \mathbb{G}$, B chooses $a \xleftarrow{\boxtimes} \mathbb{Z}_p$ and computes $h_1 = Y \cdot g^a$. For A's CH_2 query on $R_2 \in \mathbb{G} \times \mathbb{G}$, B chooses $h_2 \xleftarrow{\boxtimes} \{0, ...2^k - 1\}$ and returns it to A. Clearly, B's simulation of the $\mathsf{PIMP\text{-}KOA}$ game is perfect, since both h_1 and h_2 are uniformly random over $\mathbb{G}$ and $\{0, ..., 2^k\}$, respectively.

Eventually, A returns its response s^* for the $\mathsf{PIMP\text{-}KOA}$ experiment. We assume that A's response is valid, i.e., $s^* \in \{2^{k+c}, ..., 2^{k+k'+c} - 1\}$ and there exist $(R_1, h_1) \in \mathcal{L}_1$ and $(R_2 := (R_L, R_R), h_2) \in \mathcal{L}_2$ such that $R_1 = g^{s^*} \cdot X^{-h_2}$ and $R_R = h_1^{s^*} \cdot R_L^{-h_2}$. We denote the discrete logarithm of R_L based on h_1 by $x' = \mathsf{DL}_{h_1}(R_L)$ and do the following cases distinction:

- Case 1: $x = x'$. By the simulation of CH_1, we have $R_L = h_1^x = (Y g^{a_i})^x = Y^x X^{a_i}$ for some $i \in [Q_{\mathrm{CH}_1}]$. Thus, B returns $Z := R_L \cdot X^{-a_i} = Y^x$ to break the c-SCDH problem.
- Case 2: $x \neq x'$. We show in this case even an unbounded adversary A can only win with probability $Q_{\mathrm{CH}_2}/2^k$. For each index $i \in [Q_{\mathrm{CH}_2}]$, before receiving $h_{2,i}$, A first commits to some $R_1 = g^{r_1}$, $R_L = h_1^{x'}$ and $R_R = h_1^{r_2}$ (for arbitrary $r_1, r_2, x' \in \mathbb{Z}_p$ and $x' \neq x$) and there exists $(R_1, h_1) \in \mathcal{L}_1$. A can only win if there exists an $s_i \in \{2^{k+c}, ..., 2^{k+k'+c} - 1\}$ such that

$$r_1 + h_{2,i} x = s_i = r_2 + h_{2,i} x' \Leftrightarrow h_{2,i} = \tfrac{r_2 - r_1}{x - x'},$$

  where $h_{2,i} \xleftarrow{\boxtimes} \mathsf{ChSet}_2 := \{0, ..., 2^k\}$ is chosen independently of r_1, r_2 and x'. This happens with probability at most $1/2^k$. By the union bound we obtain the bound $Q_{\mathrm{CH}_2}/2^k$ as claimed.

Overall, B returns a valid solution of the c-SCDH challenge with probability $\varepsilon \geq \varepsilon' - \frac{Q_{\mathrm{CH}_2}}{2^k}$. This completes the proof.

(Online/Offline) Signature. Let $H_1 : \{0,1\}^* \to \mathbb{G}$ and $H_2 : \{0,1\}^* \to \{0, ..., 2^k - 1\}$ be two hash functions. Since $\mathsf{ID}_{\mathsf{SCDH}}$ has $2^{-k'}$ correctness error, given the required correctness of the signature, we fix a $\ell \in \mathbb{N}$, and as the scheme $\mathsf{ID}_{\mathsf{SCDH}}$ is partially commitment recoverable, we can use the alternative Fiat-Shamir transform to obtain the signature scheme $\mathsf{FS}_{\mathsf{SCDH}} := (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ and its online/offline variant $\mathsf{OF}_{\mathsf{SCDH}} := (\mathsf{Gen}, \mathsf{Sign}_{\mathsf{o}}, \mathsf{Ver}_{\mathsf{o}})$. For simplicity of notation, let $\mathcal{I} := \{2^{k+c}, ..., 2^{k+k'+c} - 1\}$.

$\underline{\mathsf{Gen}(\mathsf{par})}$:	$\underline{\mathsf{Sign}(sk,m)}$, $\boxed{\mathsf{Sign}_{\mathsf{o}}(sk,m)}$:	$\underline{\mathsf{Ver}(pk,m,\sigma)}$, $\boxed{\mathsf{Ver}_{\mathsf{o}}(pk,m,\sigma)}$:
$x \xleftarrow{\boxtimes} \{0,...,2^c-1\}$	$i := 0$	Parse $\sigma = (R_L, h_2, s)$
$pk := X = g^x$	While $i \le \ell$ and $s = \perp$:	$R_1 = g^s \cdot X^{-h_2}$
$sk := x$	$i := i + 1$	$h_1 = H_1(R_1, m)$
Return (pk, sk)	$r \xleftarrow{\boxtimes} \{0,...,2^{k+k'+c}-1\}$	$\boxed{h_1 = H_1(R_1)}$
	$R_1 = g^r$	$R_R = h_1^s \cdot R_L^{-h_2}$
	$h_1 = H_1(R_1, m) \in \mathbb{G}$	$R_2 := (R_L, R_R)$
	$\boxed{h_1 = H_1(R_1) \in \mathbb{G}}$	If $s \in \mathcal{I} \wedge h_2 = H_2(R_2, m)$
	$R_2 := (R_L, R_R) := (h_1^x, h_1^r)$	then return 1
	$h_2 = H_2(R_2, m) \in \{0,...,2^k-1\}$	Else return 0.
	$s = x \cdot h_2 + r$	
	If $s \notin \mathcal{I}$ then $s := \perp$	
	If $s = \perp$ then $\sigma := \perp$	
	Else $\sigma := (R_L, h_2, s)$	
	Return σ	

By Lemma 6 and Theorem 1, we have

Theorem 3 (Security of $\mathsf{FS}_{\mathsf{SCDH}}$ and $\mathsf{OF}_{\mathsf{SCDH}}$). *If c-SCDH is (t,ε)-hard in $\mathsf{par} := (p, g, \mathbb{G})$ then $\mathsf{FS}_{\mathsf{SCDH}}$ is $(t', \varepsilon', Q_s, Q_1, Q_2)$-UF-CMA secure and $\mathsf{OF}_{\mathsf{SCDH}}$ is $(t'', \varepsilon'', Q_s, Q_1, Q_2)$-UF-CMA secure in the programmable random oracle model, where*

$$\varepsilon' \le \varepsilon + \frac{Q_2+1}{2^k} + \frac{(Q_1+Q_2)Q_s}{2^c}, \qquad t' \approx t,$$

$$\varepsilon'' \le \varepsilon + \frac{Q_2+2}{2^k} + \frac{(Q_1+Q_2)Q_s}{2^c} + \frac{1}{2^k}, \qquad t'' \approx t.$$

Size of Parameters. We follow the analyses provided in [25, 20, 35]. We set $t' = t = Q_s = Q_h := Q_1 + Q_2$. Let A be and adversary that runs in time t', makes at most Q_s signature queries, at most Q_h has queries and breaks the UF-CMA-security of $\mathsf{FS}_{\mathsf{SCDH}}$ with probability at least ε' (the analysis applies also to $\mathsf{OF}_{\mathsf{SCDH}}$). If A is run multiple times, the expected time to produce a forgery is t'/ε', so we are looking for a security parameter κ with $\varepsilon'/t' \le 2^{-\kappa}$. Setting $\varepsilon'/t' \approx (\varepsilon + \frac{Q_2+1}{2^k} + \frac{(Q_1+Q_2)Q_s}{2^c})/t$, we can bound each of the additive terms separately by $2^{-\kappa}$ by choosing k and c accordingly. Concretely, we choose $c = 2\kappa$ and $k = \kappa$. Given that the Pollard lambda algorithm [47] running in time $O(\sqrt{2^c})$ is the best algorithm for solving the c-SCDH problem over $\mathbb{G}$, $\frac{\varepsilon}{t} \le \frac{t}{2^c} \le \frac{2^{c/2}}{2^c} = 2^{-\kappa}$. Also, by assumption, $\frac{Q_2+1}{t2^k} \le \frac{t}{2^k t} = 2^{-\kappa}$ and $\frac{(Q_1+Q_2)Q_s}{t2^c} = \frac{t^2}{t2^c} = \frac{t}{2^c}$ which we have already shown to be bounded by $2^{-\kappa}$. Setting $k' = 8$, this gives a signature of size of about $\ell' + 4 \cdot \kappa + 8$, where ℓ' denotes the size of a group element.

4.3 Instantiation from Factoring

Signed Quadratic Residues and the Factoring Assumption. We begin by recalling the useful group of signed quadratic residues from [27, 32]. For $n \in \mathbb{N}$ we denote the set of all $n/2$-bit primes by $\mathbb{P}_{n/2}$ and $\mathsf{Blum}_n := \{N \mid N = (2p +$

$1)(2q+1) \wedge (2p+1), (2q+1), p, q \in \mathbb{P}_{n/2} \wedge p \neq q\}$. Let $\varphi(N) = 4pq$ be Euler's totient function for $N \in \mathsf{Blum}_n$.

We define the factoring assumption as follows.

Definition 10 (Factoring Assumption). *The factoring problem* FAC *is* (t, ε)*-hard for* Blum_n *if for all adversaries* A *running in time at most* t*,*

$$\Pr\left[N = PQ \wedge P, Q \in \mathbb{P}_{n/2} \;\middle|\; N \xleftarrow{\$} \mathsf{Blum}_n; (P, Q) \xleftarrow{\$} \mathsf{A}(N) \right] \leq \varepsilon.$$

For an element $a \in \mathbb{Z}_N$, we define the absolute value

$$|x| := \begin{cases} x & \text{if } x \leq (N-1)/2 \\ -x & \text{otherwise} \end{cases}.$$

We define the group of signed quadratic residues as $\mathbb{QR}_N^+ := \{|x| : x \in \mathbb{QR}_N\}$. We have that $(\mathbb{QR}_N^+, \circ)$ is a cyclic group with order $|\mathbb{QR}_N^+| = \varphi(N)/4$, where, for all $a, b \in \mathbb{QR}_N^+$ and $x \in \mathbb{Z}_N$, group operations are defined as follows:

$$a \circ b := |a \cdot b \bmod N|, \quad a^x := \underbrace{a \circ a \circ ... \circ a}_{x \text{ times}} = |a^x \bmod N|, \quad a^{-1} := |a^{-1} \bmod N|.$$

By Theorem 2 of [32], we note that the factoring assumption tightly implies the CDH assumption over $\mathbb{QR}_N^+$ (henceforth denoted as CDH_N). Let $\mathsf{par}_1 := \mathsf{Blum}_n$ and $\mathsf{par}_2 := (N, g, \mathbb{QR}_N^+)$, where $N \xleftarrow{\$} \mathsf{Blum}_n$ and g is a random generator of $\mathbb{QR}_N^+$.

Corollary 1 ($\mathsf{FAC} \rightarrow \mathsf{CDH}_N$). *If* FAC *is* (t, ε)*-hard in* par_1*, then* CDH_N *is* (t', ε')*-hard in* par_2*, where* $t' \approx t$ *and* $\varepsilon' \leq \varepsilon + 2^{-n/2}$.

Identification Scheme. Let $\mathsf{par} := \mathbb{P}_{n/2}$. The identification scheme $\mathsf{ID}_{\mathsf{FAC}} := (\mathsf{IGen}, \mathsf{P}, \mathsf{ChSet}_1, \mathsf{ChSet}_2, \mathsf{V})$ is defined as follows.

$\underline{\mathsf{IGen}(\mathsf{par}):}$	$\underline{\mathsf{P}_1(sk):}$
$p, q \xleftarrow{\$} \mathbb{P}_{n/2}$ s.t. $P = 2p+1 \in \mathbb{P}_{n/2}$	$r \xleftarrow{\$} \mathbb{Z}_{N/4}$; $R_1 = g^r$; $St_1 := r$
and $Q = 2q+1 \in \mathbb{P}_{n/2}$	Return (R_1, St_1)
$N = PQ$	
$x \xleftarrow{\$} \mathbb{Z}_{N/4}$; $X := g^x$	$\underline{\mathsf{P}_2(sk, R_1, h_1, St_1):}$
$sk := (x, p, q)$	Parse $St_1 := r$
$pk := (X, N)$	$R_L = h_1^x$; $R_R = h_1^r$
$\mathsf{ChSet}_1 := \mathbb{QR}_N^+$	$R_2 := (R_L, R_R)$; $St_2 := St_1$
$\mathsf{ChSet}_2 := \{0, ..., 2^k - 1\}$	Return (R_2, St_2)
Return (pk, sk)	
	$\underline{\mathsf{P}_3(sk, R_1, h_1, R_2, h_2, St_2):}$
$\underline{\mathsf{V}(pk, R_1, h_1, R_2, h_2, s):}$	Parse $St_2 := r$
Parse $R_2 := (R_L, R_R)$	$s = xh_2 + r \bmod (\varphi(N)/4)$
If $R_1 = g^s \circ X^{-h_2}$ and $R_R = h_1^s \circ R_L^{-h_2}$	Return s
then return 1	
Else return 0	

Lemma 7. *Let* $N' := \lceil N/4 \rceil$, $\mathbb{G} := \mathbb{QR}_N^+$, *and* $X \xleftarrow{\boxtimes} \mathbb{Z}_{N'}, Y \xleftarrow{\boxtimes} \mathbb{Z}_{|\mathbb{G}|}$. *Then the statistical distance* $D(X,Y)$ *satisfies* $D(X,Y) \leq \frac{2(P+Q)}{PQ}$.

Proof. We split the term $D(X,Y)$ as

$$D(X,Y) = \sum_{x \in \mathbb{Z}_{N'}} \Big| \Pr[X=x] - \Pr[Y=x] \Big|$$
$$= \sum_{x \in \mathbb{Z}_{|\mathbb{G}|}} \Big| \Pr[X=x] - \Pr[Y=x] \Big| + \sum_{x \in [N' - |\mathbb{G}|]} \Big| \Pr[X=x] - \Pr[Y=x] \Big| .$$

In the first term, $\Pr[X=x] = \frac{1}{N'} \leq \frac{4}{PQ}, \Pr[Y=x] = \frac{1}{|\mathbb{G}|} = \frac{4}{(P-1)(Q-1)}$. Therefore, the first summand is equal to $\left| \frac{1-P-Q}{PQ} \right| \leq \frac{P+Q}{PQ}$. Similarly, the second term can be bounded by $\frac{P+Q}{PQ}$ and thus, $D(X,Y) \leq \frac{2(P+Q)}{PQ}$.

Lemma 8. $\mathsf{ID}_{\mathsf{FAC}}$ *is a perfectly correct five-move identification scheme and has* $\frac{2(P+Q)}{PQ}$*-statistical non-aborting honest-verifier zero-knowledge (*naHVZK*) with* $\alpha = \log(\varphi(N)/4) - \frac{2(P+Q)}{PQ}$ *bits min-entropy. Moreover, if* FAC *is* (t,ε)*-hard then* $\mathsf{ID}_{\mathsf{FAC}}$ *is* $(t', \varepsilon', Q_{\mathrm{CH}_1}, Q_{\mathrm{CH}_2})$*-*PIMP-KOA*-secure, where* $\varepsilon' \leq \varepsilon + \frac{1}{2^k}$ *and* $t' \approx t$.

Proof. The perfect correctness of $\mathsf{ID}_{\mathsf{FAC}}$ is straightforward to verify, since $R_1 = g^s \circ X^{-h_2}$ and $R_R = h_1^s \circ R_L^{-h_2}$ hold if and only if $s = xh_2 + r \bmod \varphi(N)/4$ holds.

$\frac{2(P+Q)}{PQ}$-Statistical naHVZK. Given public key $pk = X$, Sim first samples $s, w, h_2 \xleftarrow{\boxtimes} \mathbb{Z}_{N/4}$. It then computes $h_1 := g^w, R_1 := g^s \circ X^{-h_2}, R_L := R_1^w$, and $R_R := X^w$ and outputs the transcript $(R_1, h_1, R_L, R_R, h_2, s)$.

The simulated transcript (R_1, h_1, R_2, h_2, s) is close to the transcript output by $\mathsf{SKTran}(sk)$ with statistical distance $2(P+Q)/(PQ)$, since s has statistical distance at most $\frac{2(P+Q)}{PQ}$ from a uniformly random variable over $\mathbb{Z}_{|\mathbb{QR}_N^+|}$, according to Lemma 7 and R_1, R_L and R_R are values $R_1 = g^s \circ X^{-h_2}$ and $R_R = h_1^s \circ R_L^{-h_2}$. The entropy of $(R_1, St_1) \xleftarrow{\boxtimes} \mathsf{P}_1(sk)$ and $(R_2, St_2) \xleftarrow{\boxtimes} \mathsf{P}_2$ comes only from R_1, which is uniformly random from $\mathbb{QR}_N^+$. Since the transcripts output by $\mathsf{Sim}(pk)$ are statistically $\frac{2(P+Q)}{PQ}$ close to the ones produced by $\mathsf{SKTran}(sk)$, $\mathsf{ID}_{\mathsf{FAC}}$ has $\log|\mathbb{QR}_N^+| = \log(\varphi(N)/4) - \frac{2(P+Q)}{PQ}$ bits min-entropy.

PIMP-KOA-security. Let A be an attacker against the $(t', \varepsilon', Q_{\mathrm{CH}_1}, Q_{\mathrm{CH}_2})$-PIMP-KOA security of $\mathsf{ID}_{\mathsf{FAC}}$. We construct an attacker B that (t,ε)-breaks CDH over $\mathbb{QR}_N^+$.

Construction of B. Let $(X := g^x, Y := g^y)$ denote the CDH instance. B runs A with input $pk := X$ and answers A's challenge queries as follows.

For A's CH_1 query on $R_1 \in \mathbb{QR}_N^+$, B chooses $a \xleftarrow{\boxtimes} \mathbb{Z}_{N/4}$ and computes $h_1 = Y \circ g^a$. For A's CH_2 query on $R_2 \in \mathbb{QR}_N^+ \times \mathbb{QR}_N^+$, B chooses $h_2 \xleftarrow{\boxtimes} \mathbb{Z}_{N/4}$ and returns it to A. Clearly, B's simulation of the PIMP-KOA game is perfect, since both h_1 and h_2 are uniformly random over $\mathbb{QR}_N^+$ and $\mathbb{Z}_{N/4}$, respectively.

Eventually, A returns its response s^* for the $\mathsf{PIMP\text{-}KOA}$ experiment. We assume that A's response is valid, i.e., there exist $(R_1, h_1) \in \mathcal{L}_1$ and $(R_2 := (R_L, R_R), h_2) \in \mathcal{L}_2$ such that $R_1 = g^{s^*} \circ X^{-h_2}$ and $R_R = h_1^{s^*} \circ R_L^{-h_2}$. We denote the discrete logarithm of R_L based on h_1 by $x' = \mathsf{DL}_{h_1}(R_L) \bmod (\varphi(N)/4)$ and do the following cases distinction:

- Case 1: $x = x' \bmod (\varphi(N)/4)$. By the simulation of CH_1, we have $R_L = h_1^x = (Y \circ g^{a_i})^x = Y^x \circ X^{a_i}$ for some $i \in [Q_{\mathrm{CH}_1}]$. Thus, B returns $Z := R_L \circ X^{-a_i} = Y^x$ to break the CDH problem over $\mathbb{QR}_N^+$.
- Case 2: $x \neq x' \bmod (\varphi(N)/4)$. We show in this case even an unbounded adversary A can only win with probability $Q_{\mathrm{CH}_2}/2^k$. For each index $i \in [Q_{\mathrm{CH}_2}]$, before receiving $h_{2,i}$, A first commits to some $R_1 = g^{r_1}$, $R_L = h_1^{x'}$ and $R_R = h_1^{r_2}$ (for arbitrary $r_1, r_2, x' \in \mathbb{Z}_{N/4}$ and $x' \neq x \bmod (\varphi(N)/4)$) and there exists $(R_1, h_1) \in \mathcal{L}_1$. A can only win if there exists an $s_i \in \mathbb{Z}_{N/4}$ such that

$$\begin{aligned} & r_1 + h_{2,i}x = s_i = r_2 + h_{2,i}x' \bmod (\varphi(N)/4) \\ \Leftrightarrow\ & h_{2,i} = \frac{r_2 - r_1}{x - x'} \bmod (\varphi(N)/4) \end{aligned}$$

  where $h_{2,i}$ is distributed uniformly over $\{0, ..., 2^k - 1\}$ and independently of r_1, r_2 and x'. The equation $h_{2,i} = \frac{r_2 - r_1}{x - x'} \bmod (\varphi(N)/4)$ holds with probability at most $1/2^k$. By the union bound we obtain the bound $Q_{\mathrm{CH}_2}/2^k$ as claimed.

Overall, B returns a valid solution of the CDH challenge with probability $\varepsilon \geq \varepsilon' - \frac{Q_{\mathrm{CH}_2}}{2^k}$. This completes the proof.

Signature Scheme. Let $H_1 : \{0,1\}^* \to \mathbb{QR}_N^+$ and $H_2 : \{0,1\}^* \to \{0, ..., 2^k - 1\}$ be two hash functions. We note that H_1 has been used in [32, 43]. As $\mathsf{ID}_{\mathsf{FAC}}$ is perfectly correct and partial commitment-recoverable, we can use the alternative Fiat-Shamir transformation from Section 3.1 with $\ell := 1$ to obtain the signature scheme $\mathsf{FS}_{\mathsf{FAC}} := (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$.

$\underline{\mathsf{Gen}(\mathsf{par})}$:	$\underline{\mathsf{Sign}(sk, m)}$:	$\underline{\mathsf{Ver}(pk, m, \sigma)}$:
$p, q \xleftarrow{\$} \mathbb{P}_{n/2}$ s.t.	$r \xleftarrow{\$} \mathbb{Z}_{N/4}$; $R_1 = g^r$	Parse $\sigma = (R_L, h_2, s)$
$P = 2p + 1 \in \mathbb{P}_{n/2}$	$h_1 = H_1(R_1, m) \in \mathbb{QR}_N^+$;	$R_1 = g^s \circ X^{-h_2}$
$Q = 2q + 1 \in \mathbb{P}_{n/2}$	$R_L = h_1^x$; $R_R = h_1^r$	$h_1 = H_1(R_1, m)$;
$N = PQ$	$R_2 := (R_L, R_R)$	$R_R = h_1^s \circ R_L^{-h_2}$
$x \xleftarrow{\$} \mathbb{Z}_{N/4}$; $X := g^x$	$h_2 = H_2(R_2, m) \in \{0, ...2^k - 1\}$	$R_2 := (R_L, R_R)$
$sk := (x, p, q)$	$s = xh_2 + r \bmod (\varphi(N)/4)$	If $h_2 = H_2(R_2, m)$
$pk := (X, N)$	$\sigma = (R_L, h_2, s)$	then return 1
Return (pk, sk)	Return σ	Else return 0.

By Corollary 1, Lemma 8 and Theorem 1, we have

Theorem 4 (Security of $\mathsf{FS}_{\mathsf{FAC}}$). *If* FAC *is* (t, ε)*-hard in* $\mathsf{par} := \mathsf{Blum}_n$ *then* $\mathsf{FS}_{\mathsf{FAC}}$ *is* $(t', \varepsilon', Q_s, Q_1, Q_2)$-$\mathsf{UF\text{-}CMA}$ *secure in the programmable random oracle*

model, where

$$\varepsilon' \leq \varepsilon + \frac{1}{2^{n/2}} + \frac{Q_2+1}{2^k} + \frac{(Q_1+Q_2)Q_s}{2^{n-3}} + \frac{Q_s(P+Q)}{2^{n-1}}, \qquad t' \approx t.$$

Size of Parameters. We argue along the lines of our analysis provided above. We again set $Q_s = Q_h = t' = t$. Here, we only need to bound the term $\frac{Q_2+1}{t2^k} \leq \frac{1}{2^k}$, as all terms in the above theorem vanish. Thus, we set again $k = \kappa$ to achieve a security of κ bits. This yields a signature of size $2 \cdot \ell' + \kappa$ bits where again ℓ' denotes the size of a group element of $\mathbb{G}$.

References

1. M. Abdalla, J. H. An, M. Bellare, and C. Namprempre. From identification to signatures via the Fiat-Shamir transform: Minimizing assumptions for security and forward-security. In L. R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 418–433. Springer, Heidelberg, Apr. / May 2002.
2. M. Abdalla, F. Ben Hamouda, and D. Pointcheval. Tighter reductions for forward-secure signature schemes. In K. Kurosawa and G. Hanaoka, editors, *PKC 2013*, volume 7778 of *LNCS*, pages 292–311. Springer, Heidelberg, Feb. / Mar. 2013.
3. M. Abdalla, P.-A. Fouque, V. Lyubashevsky, and M. Tibouchi. Tightly-secure signatures from lossy identification schemes. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 572–590. Springer, Heidelberg, Apr. 2012.
4. M. Abe, D. Hofheinz, R. Nishimaki, M. Ohkubo, and J. Pan. Compact Structure-preserving Signatures with Almost Tight Security. In *CRYPTO 2017*, LNCS. Springer, Heidelberg, 2017. To appear.
5. S. M. E. Y. Alaoui, Ö. Dagdelen, P. Véron, D. Galindo, and P.-L. Cayrel. Extended security arguments for signature schemes. In A. Mitrokotsa and S. Vaudenay, editors, *AFRICACRYPT 12*, volume 7374 of *LNCS*, pages 19–34. Springer, Heidelberg, July 2012.
6. M. Bellare and A. Palacio. GQ and Schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks. In M. Yung, editor, *CRYPTO 2002*, volume 2442 of *LNCS*, pages 162–177. Springer, Heidelberg, Aug. 2002.
7. M. Bellare, B. Poettering, and D. Stebila. From identification to signatures, tightly: A framework and generic transforms. In J. H. Cheon and T. Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 435–464. Springer, Heidelberg, Dec. 2016.
8. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In V. Ashby, editor, *ACM CCS 93*, pages 62–73. ACM Press, Nov. 1993.
9. M. Bellare and P. Rogaway. The exact security of digital signatures: How to sign with RSA and Rabin. In U. M. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 399–416. Springer, Heidelberg, May 1996.
10. D. J. Bernstein. Proving tight security for Rabin-Williams signatures. In N. P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 70–87. Springer, Heidelberg, Apr. 2008.

11. T. Beth. Efficient zero-knowledge identification scheme for smart cards. In C. G. Günther, editor, *EUROCRYPT'88*, volume 330 of *LNCS*, pages 77–84. Springer, Heidelberg, May 1988.
12. O. Blazy, S. A. Kakvi, E. Kiltz, and J. Pan. Tightly-secure signatures from chameleon hash functions. In J. Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 256–279. Springer, Heidelberg, Mar. / Apr. 2015.
13. O. Blazy, E. Kiltz, and J. Pan. (Hierarchical) identity-based encryption from affine message authentication. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 408–425. Springer, Heidelberg, Aug. 2014.
14. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In C. Boyd, editor, *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 514–532. Springer, Heidelberg, Dec. 2001.
15. E. F. Brickell and K. S. McCurley. An interactive identification scheme based on discrete logarithms and factoring. In I. Damgård, editor, *EUROCRYPT'90*, volume 473 of *LNCS*, pages 63–71. Springer, Heidelberg, May 1991.
16. P.-L. Cayrel, R. Lindner, M. Rückert, and R. Silva. Improved zero-knowledge identification with lattices. In S.-H. Heng and K. Kurosawa, editors, *ProvSec 2010*, volume 6402 of *LNCS*, pages 1–17. Springer, Heidelberg, Oct. 2010.
17. P.-L. Cayrel, P. Véron, and S. M. E. Y. Alaoui. A zero-knowledge identification scheme based on the q-ary syndrome decoding problem. In A. Biryukov, G. Gong, and D. R. Stinson, editors, *SAC 2010*, volume 6544 of *LNCS*, pages 171–186. Springer, Heidelberg, Aug. 2011.
18. J. Chen and H. Wee. Fully, (almost) tightly secure IBE and dual system groups. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 435–460. Springer, Heidelberg, Aug. 2013.
19. M.-S. Chen, A. Hülsing, J. Rijneveld, S. Samardjiska, and P. Schwabe. From 5-pass MQ-based identification to MQ-based signatures. In J. H. Cheon and T. Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 135–165. Springer, Heidelberg, Dec. 2016.
20. B. Chevallier-Mames. An efficient CDH-based signature scheme with a tight security reduction. In V. Shoup, editor, *CRYPTO 2005*, volume 3621 of *LNCS*, pages 511–526. Springer, Heidelberg, Aug. 2005.
21. A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A. M. Odlyzko, editor, *CRYPTO'86*, volume 263 of *LNCS*, pages 186–194. Springer, Heidelberg, Aug. 1987.
22. N. Fleischhacker, T. Jager, and D. Schröder. On tight security proofs for Schnorr signatures. In P. Sarkar and T. Iwata, editors, *ASIACRYPT 2014, Part I*, volume 8873 of *LNCS*, pages 512–531. Springer, Heidelberg, Dec. 2014.
23. M. Girault. An identity-based identification scheme based on discrete logarithms modulo a composite number (rump session). In I. Damgård, editor, *EUROCRYPT'90*, volume 473 of *LNCS*, pages 481–486. Springer, Heidelberg, May 1991.
24. M. Girault, G. Poupard, and J. Stern. On the fly authentication and signature schemes based on groups of unknown order. *Journal of Cryptology*, 19(4):463–487, Oct. 2006.
25. E.-J. Goh and S. Jarecki. A signature scheme as secure as the Diffie-Hellman problem. In E. Biham, editor, *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 401–415. Springer, Heidelberg, May 2003.
26. E.-J. Goh, S. Jarecki, J. Katz, and N. Wang. Efficient signature schemes with tight reductions to the Diffie-Hellman problems. *Journal of Cryptology*, 20(4):493–514, Oct. 2007.

27. S. Goldwasser, S. Micali, and R. L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2):281–308, Apr. 1988.
28. L. C. Guillou and J.-J. Quisquater. A "paradoxical" indentity-based signature scheme resulting from zero-knowledge. In S. Goldwasser, editor, *CRYPTO'88*, volume 403 of *LNCS*, pages 216–231. Springer, Heidelberg, Aug. 1990.
29. D. Hofheinz. Algebraic partitioning: Fully compact and (almost) tightly secure cryptography. In E. Kushilevitz and T. Malkin, editors, *TCC 2016-A, Part I*, volume 9562 of *LNCS*, pages 251–281. Springer, Heidelberg, Jan. 2016.
30. D. Hofheinz. Adaptive partitioning. In *Eurocrypt 2017*, mylncs, pages 489–518. Springer, Heidelberg, 2017.
31. D. Hofheinz and T. Jager. Tightly secure signatures and public-key encryption. In R. Safavi-Naini and R. Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 590–607. Springer, Heidelberg, Aug. 2012.
32. D. Hofheinz and E. Kiltz. The group of signed quadratic residues and applications. In S. Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 637–653. Springer, Heidelberg, Aug. 2009.
33. S. A. Kakvi and E. Kiltz. Optimal security proofs for full domain hash, revisited. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 537–553. Springer, Heidelberg, Apr. 2012.
34. J. Katz and N. Wang. Efficiency improvements for signature schemes with tight security reductions. In S. Jajodia, V. Atluri, and T. Jaeger, editors, *ACM CCS 03*, pages 155–164. ACM Press, Oct. 2003.
35. E. Kiltz, D. Masny, and J. Pan. Optimal security proofs for signatures from identification schemes. In M. Robshaw and J. Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 33–61. Springer, Heidelberg, Aug. 2016.
36. T. Koshiba and K. Kurosawa. Short exponent Diffie-Hellman problems. In F. Bao, R. Deng, and J. Zhou, editors, *PKC 2004*, volume 2947 of *LNCS*, pages 173–186. Springer, Heidelberg, Mar. 2004.
37. V. Lyubashevsky. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In M. Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 598–616. Springer, Heidelberg, Dec. 2009.
38. S. Micali and L. Reyzin. Improving the exact security of digital signature schemes. Cryptology ePrint Archive, Report 1999/020, 1999. http://eprint.iacr.org/1999/020.
39. S. Micali and L. Reyzin. Improving the exact security of digital signature schemes. *Journal of Cryptology*, 15(1):1–18, 2002.
40. S. Micali and A. Shamir. An improvement of the Fiat-Shamir identification and signature scheme. In S. Goldwasser, editor, *CRYPTO'88*, volume 403 of *LNCS*, pages 244–247. Springer, Heidelberg, Aug. 1990.
41. T. Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In E. F. Brickell, editor, *CRYPTO'92*, volume 740 of *LNCS*, pages 31–53. Springer, Heidelberg, Aug. 1993.
42. H. Ong and C.-P. Schnorr. Fast signature generation with a Fiat-Shamir-like scheme. In I. Damgård, editor, *EUROCRYPT'90*, volume 473 of *LNCS*, pages 432–440. Springer, Heidelberg, May 1991.
43. B. Poettering and D. Stebila. Double-authentication-preventing signatures. In M. Kutylowski and J. Vaidya, editors, *ESORICS 2014, Part I*, volume 8712 of *LNCS*, pages 436–453. Springer, Heidelberg, Sept. 2014.

44. D. Pointcheval. A new identification scheme based on the perceptrons problem. In L. C. Guillou and J.-J. Quisquater, editors, *EUROCRYPT'95*, volume 921 of *LNCS*, pages 319–328. Springer, Heidelberg, May 1995.
45. D. Pointcheval and G. Poupard. A new np-complete problem and public-key identification. 28(1):5–31, 2003.
46. D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, 2000.
47. J. M. Pollard. Monte Carlo methods for index computation mod p. *Mathematics of Computation*, 32:918–924, 1978.
48. K. Sakumoto, T. Shirai, and H. Hiwatari. Public-key identification schemes based on multivariate quadratic polynomials. In P. Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 706–723. Springer, Heidelberg, Aug. 2011.
49. C.-P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3):161–174, 1991.
50. Y. Seurin. On the exact security of Schnorr-type signatures in the random oracle model. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 554–571. Springer, Heidelberg, Apr. 2012.
51. A. Shamir. An efficient identification scheme based on permuted kernels (extended abstract) (rump session). In G. Brassard, editor, *CRYPTO'89*, volume 435 of *LNCS*, pages 606–609. Springer, Heidelberg, Aug. 1990.
52. A. Shamir and Y. Tauman. Improved online/offline signature schemes. In J. Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 355–367. Springer, Heidelberg, Aug. 2001.
53. R. Silva, P.-L. Cayrel, and R. Lindner. Zero-knowledge identification based on lattices with low communication costs. In *XI Simposio Brasileiro de Seguranca da Informacao e de Sistemas Computacionais 8*, pages 95–107, 2011.
54. J. Stern. Designing identification schemes with keys of short size. In Y. Desmedt, editor, *CRYPTO'94*, volume 839 of *LNCS*, pages 164–173. Springer, Heidelberg, Aug. 1994.
55. J. Stern. A new identification scheme based on syndrome decoding. In D. R. Stinson, editor, *CRYPTO'93*, volume 773 of *LNCS*, pages 13–21. Springer, Heidelberg, Aug. 1994.