Extended Security Arguments for Signature Schemes

Sidi Mohamed El Yousfi Alaoui, Özgür Dagdelen, Pascal Véron, David Galindo, Pierre-Louis Cayrel

Extended Security Arguments for Signature Schemes

Sidi Mohamed El Yousfi Alaoui[1], Özgür Dagdelen[1], Pascal Véron[2], David Galindo[3], and Pierre-Louis Cayrel[4]

[1] Darmstadt University of Technology, Germany
[2] IML/IMATH Université du Sud Toulon-Var, France
[3] University of Luxembourg, Luxembourg
[4] Laboratoire Hubert Curien Université de Saint-Etienne, France

Abstract. The well-known forking lemma by Pointcheval and Stern has been used to prove the security of the so-called generic signature schemes. These signature schemes are obtained via the Fiat-Shamir transform from three-pass identification schemes. A number of five-pass identification protocols have been proposed in the last few years. Extending the forking lemma and the Fiat-Shamir transform would allow to obtain new signature schemes since, unfortunately, these newly proposed schemes fall outside the original framework. In this paper, we provide an extension of the forking lemma in order to assess the security of what we call n-generic signature schemes. These include signature schemes that are derived from certain $(2n + 1)$-pass identification schemes. We thus obtain a generic methodology for proving the security of a number of signature schemes derived from recently published five-pass identification protocols, and potentially for $(2n + 1)$-pass identification schemes to come.

Keywords: signature schemes, forking lemma, identification schemes.

1 Introduction

The focus of this work is on methodologies to prove the security of digital signature schemes. Thus, instead of providing security reductions from scratch, the goal is to provide security arguments for a class of signature schemes, as previously done in [12,13,9,1,19]. In particular, we aim at extending a pioneering work by Pointcheval and Stern [12] where a reduction technique was introduced to obtain security arguments for the so-called generic signature schemes. These security arguments allow for simple proofs and for efficient signature schemes. Moreover, this type of signature schemes can be derived from identification schemes if the latter satisfy certain requirements.

Generic Signature Schemes. Pointcheval and Stern call generic signature schemes those whose signatures are of the form $\sigma = (\sigma_0, h_1, \sigma_1)$, where σ_0 is uniformly

A. Mitrokotsa and S. Vaudenay (Eds.): AFRICACRYPT 2012, LNCS 7374, pp. 19–34, 2012.

distributed over a large set, $h_1 = H(m, \sigma_0)$ with H being a hash function modeled as a random oracle, m is the message to be signed and σ_1 depends just on σ_0 and h_1.

The works [12,13] provide security arguments for generic signature schemes thanks to the use of the forking lemma. This lemma states that a successful forger can be restarted with a different random oracle in order to get two distinct but related forgeries. If the generic signature schemes additionally enjoy the existence of a polynomial-time algorithm, called extractor, that recovers the signing key from two signatures $\sigma = (\sigma_0, h_1, \sigma_1)$ and $\sigma' = (\sigma_0, h_1', \sigma_1')$ with $h_1 \neq h_1'$, then unforgeability is guaranteed under a supposedly intractable problem.

Unfortunately, the forking lemma is restricted to 3-tupled signatures. One would like to obtain an unbounded version of this lemma for signatures of the form $(\sigma_0, h_1, \sigma_1, \ldots, h_n, \sigma_n)$ where $h_i = H_i(m, \sigma_0, h_1, \sigma_1, \ldots, h_{i-1}, \sigma_{i-1})$ for $n \in \mathbb{N}$. This would allow to address a greater class of signatures. In this work, we provide such an extension and apply it to assess the security of n-generic signature schemes. Roughly speaking, n-generic signature schemes are built as generic signature schemes but are not restricted in the number of tuple entries as mentioned above.

From Identification Schemes to Signature Schemes. One of the ways to build a signature scheme is to depart from an existing identification protocol and convert it into a signature scheme using the well-known Fiat-Shamir (FS) paradigm [5]. In an identification protocol a series of messages are exchanged between two parties, called prover and verifier, in order to enable a prover to convince a verifier that it knows a given secret. Zero-knowledge identification protocols [7] convince a verifier without revealing any other information whatsoever about the secret itself. Informally, the FS paradigm builds a signature scheme as the transcript of one execution of the identification scheme, where the challenges sent by the verifier are replaced by the output of a secure hash function having as input the message and the current transcript.

In [12] the signatures obtained by applying the FS transform to canonical identification schemes were generalized to the concept of generic signatures schemes. Schematically, in a canonical identification scheme a prover sends first a commitment Com, then receives a challenge Ch drawn from a uniform distribution, and finishes the interaction with a message, called response Rsp. Finally, the verifier applies a verifying algorithm to the prover's public key, determining acceptance or rejection. In addition, the identification protocol needs to satisfy special-soundness. Roughly, special-soundness means there exists a polynomial-time algorithm which is able to extract the witness of the prover, given two correlated transcripts $(\mathsf{Com}, \mathsf{Ch}, \mathsf{Rsp}), (\mathsf{Com}', \mathsf{Ch}', \mathsf{Rsp}')$ with $\mathsf{Com} = \mathsf{Com}'$ and $\mathsf{Ch} \neq \mathsf{Ch}'$.

Many zero-knowledge identification schemes have been proposed whose conversion to signature schemes lead to generic signature schemes like [5,6,17]. However, several signature schemes which are derived from 5-pass identification protocols are not covered by the abstraction above. Thus, we are obliged to prove their security from scratch. Examples of schemes falling outside the

Pointcheval-Stern framework can be found in [3,16,17,4,10,11,15,8,18]. The authors must provide direct proofs for the signature schemes in these works deriving from 5-pass identification. These proofs often appear quite complex. Moreover, the authors of [14] recently left open to find a security reduction for signatures derived from a 5-pass identification protocol. We show that all aforementioned 5-pass identification schemes give raise to 2-generic signature schemes. We isolate a property, called n-soundness, that implies unforgeability of all the schemes satisfying it. Informally, n-soundness means that the signing key can be extracted from two correlated valid signatures $\sigma = (\sigma_0, h_1, \ldots, \sigma_{n-1}, h_n, \sigma_n)$ and $\sigma' = (\sigma_0, h_1, \ldots, \sigma_{n-1}, h'_n, \sigma'_n)$ with $h_n \neq h'_n$. In particular, we prove in Section 4 the security of the resulting signature scheme from [14], which was missing in the original paper.

Related Work. Pointcheval and Stern [12,13] provided security arguments for generic signature schemes. However, these generic signature schemes are restrictive in the sense that (a) they allow transformations only based on canonical identification schemes, and (b) there exists an extractor for these schemes. The work of Abdalla *et al.* [1] introduced a new transformation from identification schemes (IS) to signature schemes (SS) without insisting on the existence of such an extractor. Nonetheless, they require again canonical IS. Ohta and Okamoto [9] assume that the IS is honest-verifier (perfect) zero-knowledge and that it is computationally infeasible for a cheating prover to convince the verifier to accept. Again, this result is valid only for three-pass IS.

Very recently, Yao and Zhao [19] presented what they call challenge-divided Fiat-Shamir paradigm. Here, security results are set for three-pass IS with divided random challenges. Even though they consider more challenges, still identification schemes with more than three interactions are not captured by their paradigm. In this work, we consider an unlimited number of challenges as long as they are randomly chosen from large enough sets. To the best of our knowledge this is the first transformation which gives generic security statements for SS derived from $(2n + 1)$-pass IS.

Organization. We introduce in Section 2 the necessary background to understand the paper. In Section 3 we present the notion of n-generic signature schemes and provide an extended forking lemma that applies to this new signature type. We exemplify in Section 4 our paradigm and derive a provably secure 2-generic signature scheme based on multivariate polynomials.

2 Preliminaries

We begin by introducing some notations and briefly reviewing some definitions. A function $\mu(\cdot)$ is *negligible in* n, or just *negligible*, if for every positive polynomial $p(\cdot)$ and all sufficiently large n it holds that $\mu(n) < 1/p(n)$. Otherwise, we call $\mu(\cdot)$ *non-negligible*. Note that the sum of two negligible functions (resp. non-negligible) is again negligible (resp. non-negligible) whereas the sum of one

non-negligible function $\pi(\cdot)$ and one negligible function $\mu(\cdot)$ is non-negligible, i.e. there exists a positive polynomial $p(\cdot)$ such that for infinitely many n's it holds that $\pi(n) + \mu(n) > 1/p(n)$.

Two distributions ensembles $\{X_n\}_{n\in\mathbb{N}}$ and $\{Y_n\}_{n\in\mathbb{N}}$ are said to be *(computationally) indistinguishable*, if for every non-uniform polynomial-time algorithm D, there exists a negligible function $\mu(\cdot)$ such that

$$|\Pr[\,D(X_n) = 1] - \Pr[\,D(Y_n) = 1]\,| \leq \mu(n).$$

We write $s \xleftarrow{\$} \mathcal{A}^{\mathcal{O}}(x)$ to denote the output s by a probabilistic algorithm $\mathcal{A}$ with input x having black-box access to an oracle $\mathcal{O}$. In particular, this means, that $\mathcal{A}$ may query oracle $\mathcal{O}$ in order to derive s from its answers.

Digital Signatures. In the following we give the definition of a signature scheme together with the corresponding standard security level.

Definition 1 (Signature scheme). *A signature scheme is a collection of the following algorithms* $\mathrm{S} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vf})$ *defined as follows.*

$\mathsf{KGen}(1^\kappa)$ *is a probabilistic algorithm which, on input a security parameter* 1^κ*, outputs a secret and a public key* $(\mathsf{sk}, \mathsf{pk})$.

$\mathsf{Sign}(\mathsf{sk}, m)$ *is a probabilistic algorithm which, on input a secret key* sk *and a message* m*, outputs a signature* σ.

$\mathsf{Vf}(\mathsf{pk}, m, \sigma)$ *is a deterministic algorithm which, on input a public key* pk*, a message* m *and a signature* σ*, outputs either* 1 (= *valid*) *or* 0 (= *invalid*).

We require correctness of the verification, i.e., the verifier will always accept genuine signatures. More formally, for all $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\kappa)$, any message m, any $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m)$, we always have $\mathsf{Vf}(\mathsf{pk}, m, \sigma) = 1$.

From signature schemes we require that no outsider should be able to forge a signer's signature. The following definition captures this property formally.

Definition 2 (Unforgeability of a Signature Scheme). *A signature scheme* $\mathrm{S} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vf})$ *is existentially unforgeable under (adaptively) chosen-message attacks if for any efficient algorithm* $\mathcal{A}$ *making at most* q_s *oracle queries, the probability that the following experiment returns* 1 *is negligible:*

Experiment $\mathsf{Unforgeability}^{\mathrm{S}}_{\mathcal{A}}(\kappa)$

$(\mathsf{sk}, \mathsf{pk}) \xleftarrow{\$} \mathsf{KGen}(1^\kappa)$

$(\sigma^*, m^*) \xleftarrow{\$} \mathcal{A}^{\mathsf{Sign}'(\cdot)}(\mathsf{pk})$

$\mathsf{Sign}'(\cdot)$ *on input* m *outputs* $\sigma \xleftarrow{\$} \mathsf{Sign}(\mathsf{sk}, m)$

Return 1 *iff*

$\mathsf{Vf}(\mathsf{pk}, m^*, \sigma^*) = 1$ *and* m^* *was not queried to* $\mathsf{Sign}'(\cdot)$ *by* $\mathcal{A}$

The probability is taken over all coin tosses of KGen*,* Sign*, and* $\mathcal{A}$.

Note that q_s is bounded by a polynomial in the security parameter κ. Definition 2 captures unforgeability against adaptively chosen-message attacks for signature schemes. Unforgeability against no-message attacks is defined analogously but q_s must be 0.

Splitting Lemma. The following lemma is extensively used in the forking lemma proofs. It states that one can split a given set X into two subsets, (a) a non-negligible subset Ω consisting of "good" x's which provides a non-negligible probability of success over y, and (b) its complement, consisting of "bad" x's.

Lemma 1 (Splitting Lemma [12, Lemma 3]). *Let A be a subset of $X \times Y$ such that $Pr[A(x,y)] \geq \epsilon$, then there exist $\Omega \subset X$ such that*

1. *$Pr[x \in \Omega] \geq \epsilon/2$*
2. *If $a \in \Omega$, then $Pr[A(a,y)] \geq \epsilon/2$.*

See [12, Lemma 3] for the proof.

3 Extended Security Arguments for Digital Signatures

In this section we give the formal definition of an n-generic signature scheme and extend the forking lemma accordingly. This allows us to prove that any n-generic signature scheme satisfying what we call n-soundness is existentially unforgeable in the random oracle model.

3.1 n-Generic Signature Schemes

Let H_i denote a hash function with output of cardinality 2^{κ_i} (derived from the security parameter κ).

Definition 3 (n-Generic Signature Scheme). *An n-generic signature scheme is a digital signature scheme $\mathrm{S} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vf})$ with the following properties:*

Structure *A signature σ for a message m is of the form $(\sigma_0, h_1, \ldots, \sigma_{n-1}, h_n, \sigma_n)$ where $h_1 = H_1(m, \sigma_0)$ and $h_i = H_i(m, \sigma_0, \ldots, h_{i-1}, \sigma_{i-1})$ for $i = 2, \ldots, n$ with H_i being modeled as a random oracle. σ_i depends on previous $\sigma_0, \ldots, \sigma_{i-1}$ and hash values $h_1, \ldots, h_i$ for $i = 1, \ldots, n$.*

Honest-Verifier Zero-Knowledge (HVZK) *Assume the hash functions H_i are modeled by publicly accessible random oracles. There exists a PPT algorithm Z, the zero-knowledge simulator, controlling the random oracles, such that for any pair of PPT algorithms $D = (D_0, D_1)$ the following distributions are computationally indistinguishable:*

- *Let $(\mathsf{pk}, \mathsf{sk}, m, state) \leftarrow D_0(1^\kappa)$. If pk belongs to sk, then set $\sigma = (\sigma_0, h_1, \ldots, \sigma_{n-1}, h_n, \sigma_n) \leftarrow \mathsf{Sign}(\mathsf{sk}, m)$, else $\sigma \leftarrow \perp$. Output $D_1(\sigma, state)$.*
- *Let $(\mathsf{pk}, \mathsf{sk}, m, state) \leftarrow D_0(1^\kappa)$. If pk belongs to sk, then set $\sigma = (\sigma_0, h_1, \ldots, \sigma_{n-1}, h_n, \sigma_n) \leftarrow Z(\mathsf{pk}, m, 1)$, else $\sigma \leftarrow Z(\mathsf{pk}, m, 0)$. Output $D_1(\sigma, state)$.*

Notice that the structure of a generic signature as originally proposed in [12] matches that of a 1-generic signature. For the sake of simplicity we occasionally write $\sigma = (\sigma_0, \ldots, \sigma_n, h_1 \ldots, h_n)$ instead of $(\sigma_0, h_1, \ldots, \sigma_{n-1}, h_n, \sigma_n)$.

3.2 An Extended Forking Lemma

Pointcheval and Stern introduced in [12] the forking lemma as a technique to prove the security of some families of signature schemes, namely generic signature schemes with special-soundness. This well-known lemma is applied to get two forgeries for the same message using a replay attack, after that, one can use the two obtained forgeries to recover the secret key. They also show that a successful forger in the adaptive chosen-message attack model implies a successful forger in the no-message attack model, as long as the honest-verifier zero-knowledge property holds. In the following we propose an extension of the original forking lemma that applies to n-generic signature schemes. We first provide the Extended Forking Lemma in the no-message attack model.

No-Message Attack Model

Lemma 2. *Let* S *be an n-generic signature scheme with security parameter κ. Let $\mathcal{A}$ be a PPT Turing machine given only the public data as input. If $\mathcal{A}$ can find a valid signature $(\sigma_0, \ldots, \sigma_n, h_1, \ldots, h_n)$ for a message m with a non-negligible probability, after asking the n random oracles $\mathcal{O}_1, \ldots, \mathcal{O}_n$ polynomially often (in κ), then, a replay of this machine with the same random tape, the same first oracles $\mathcal{O}_1, \ldots, \mathcal{O}_{n-1}$ and a different last oracle $\mathcal{O}_n$, outputs two valid signatures $(\sigma_0, \ldots, \sigma_n, h_1, \ldots, h_n)$ and $(\sigma_0, \ldots, \sigma'_n, h_1, \ldots, h'_n)$ for the same message m with a non-negligible probability such that $h_n \neq h'_n$.*

Proof. We are given a no-message adversary $\mathcal{A}$, which is a PPT Turing machine with a random tape ω taken from a set R_ω. During the attack, $\mathcal{A}$ may ask $q_1, \ldots, q_n$ (polynomially bounded in κ) queries to random oracles $\mathcal{O}_1, \ldots, \mathcal{O}_n$ with $q_j^{(i)}$ denoting the j-query to oracle $\mathcal{O}_i$. We denote by $q_1^{(i)}, \ldots, q_{q_i}^{(i)}$ the q_i distinct queries to the random oracles $\mathcal{O}_i$ and let $r^{(i)} = (r_1^{(i)}, \ldots, r_{q_i}^{(i)})$ be the answers of $\mathcal{O}_i$, for $1 \leq i \leq n$. Let $S_i^{q_i}$ denote the set of all possible answers from $\mathcal{O}_i$, i.e., $\{r_1^{(i)}, \ldots, r_{q_i}^{(i)}\} \in S_i^{q_i}$. Furthermore, we denote by

- $\mathcal{E}$ the event that $\mathcal{A}$ can produce a valid signature $(\sigma_0, \ldots, \sigma_n, h_1, \ldots, h_n)$ for message m by using random tape ω and the answers $r_1^{(i)}, \ldots, r_{q_i}^{(i)}$ for $i \leq n$. Note that a valid signature implies $h_i = \mathcal{O}_i(m, \sigma_0, h_1, \ldots, h_{i-1}, \sigma_{i-1})$.
- $\mathcal{F}$ the event that $\mathcal{A}$ has queried the oracle $\mathcal{O}_n$ with input $(m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1})$, i.e.,

$$\exists j \leq q_n : \; q_j^{(n)} = (m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1}).$$

  Accordingly, its complement $\neg\mathcal{F}$ denotes

$$\forall j \leq q_n : \; q_j^{(n)} \neq (m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1}).$$

By hypothesis of the lemma, the probability that event $\mathcal{E}$ occurs ($\Pr[\mathcal{E}]$), is non-negligible, i.e., there exists a polynomial function $T(\cdot)$ such that $\Pr[\mathcal{E}] \geq \frac{1}{T(\kappa)}$. We know that

$$\Pr[\mathcal{E}] = \Pr[\mathcal{E} \wedge \mathcal{F}] + \Pr[\mathcal{E} \wedge \neg\mathcal{F}]. \tag{1}$$

Furthermore, we get

$$\begin{aligned}
&\Pr\left[h_n = \mathcal{O}_n(m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1}) \wedge \neg\mathcal{F}\right] \\
&\quad = \Pr\left[h_n = \mathcal{O}_n(m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1}) \mid \neg\mathcal{F}\right] \cdot \Pr[\neg\mathcal{F}] \\
&\quad \leq \Pr\left[h_n = \mathcal{O}_n(m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1}) \mid \neg\mathcal{F}\right] \\
&\quad \leq \frac{1}{2^{k_n}},
\end{aligned}$$

because the output of $\mathcal{O}_n$ is unpredictable. The event $\mathcal{E}$ implies that $h_n = \mathcal{O}_n(m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1})$, and thus we get

$$\Pr[\mathcal{E} \wedge \neg\mathcal{F}] \leq \Pr\left[h_n = \mathcal{O}_n(m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1}) \wedge \neg\mathcal{F}\right] \leq \frac{1}{2^{k_n}} \tag{2}$$

Relations (1) and (2) lead to

$$\Pr[\mathcal{E} \wedge \ \mathcal{F}] \geq \frac{1}{T(\kappa)} - \frac{1}{2^{k_n}} \geq \frac{1}{T'(\kappa)} \tag{3}$$

Note that a polynomial $T'(\cdot)$ must exist since the difference between a non-negligible and negligible term is non-negligible. Therefore, $\exists l \leq q_n$ so that

$$\Pr\left[\mathcal{E} \wedge q_l^{(n)} = (m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1})\right] \geq \frac{1}{q_n T'(\kappa)}.$$

Indeed, if we suppose that, $\forall l \in \{1, \ldots, q_n\}$,

$$\Pr\left[\mathcal{E} \wedge q_l^{(n)} = (m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1})\right] < \frac{1}{q_n T'(\kappa)}$$

then,

$$\begin{aligned}
\Pr[\mathcal{E} \wedge \ \mathcal{F}] &= \Pr\left[\mathcal{E} \wedge (\exists j \leq q_n, q_j^{(n)} = (m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1}))\right] \\
&\leq \sum_{j=1}^{q_n} \Pr\left[\mathcal{E} \wedge q_j^{(n)} = (m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1})\right] \\
&< \frac{q_n}{q_n T'(\kappa)} = \frac{1}{T'(\kappa)}
\end{aligned}$$

This leads to a contradiction with (3). Further, we define

$$B = \{(\omega, r^{(1)}, \ldots, r^{(n)}) \text{ s.t. } \mathcal{E} \wedge q_l^{(n)} = (m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1})\}.$$

Since, $B \subset R_\omega \times S_1^{q_1} \times \ldots \times S_n^{q_n}$ and $\Pr[B] \geq \frac{1}{q_n T'(\kappa)}$, by using the splitting lemma we have:

- $\exists \Omega \subset R_\omega$ such that $\Pr[\omega \in \Omega] \geq \frac{1}{2q_n T'(\kappa)}$.
- $\forall \omega \in \Omega$, $\Pr\left[(\omega, r^{(1)}, \ldots, r^{(n)}) \in B\right] \geq \frac{1}{2q_n T'(\kappa)}$, where the probability is taken over $S_1^{q_1} \times \ldots \times S_n^{q_n}$.

We define

$$B' = \{(\omega, r^{(1)}, \ldots, r^{(n)}) \text{ s.t. } (\omega, r^{(1)}, \ldots, r^{(n)}) \in B \wedge \omega \in \Omega\}.$$

Recall that $r^{(i)} = (r_1^{(i)}, \ldots, r_{q_i}^{(i)})$ where $r_j^{(i)} \in S_i$ for $1 \leq j \leq q_i$. Since,

$$B' \subset (R_\omega \times S_1^{q_1} \times \ldots \times S_n^{l-1}) \times S_n^{q_n - l + 1},$$

by using the splitting lemma again we get

- $\exists \Omega' \subset R_\omega \times S_1^{q_1} \times \ldots \times S_n^{l-1}$ such that
  $\Pr\left[(\omega, r^{(1)}, \ldots, r^{(n-1)}, (r_1^{(n)}, \ldots, r_{l-1}^{(n)})) \in \Omega'\right] \geq \frac{1}{4q_n T'(\kappa)}$.
- $\forall (\omega, r^{(1)}, \ldots, r^{(n-1)}, (r_1^{(n)}, \ldots, r_{l-1}^{(n)})) \in \Omega'$,
  $\Pr\left[(\omega, r^{(1)}, \ldots, r^{(n-1)}, (r_1^{(n)}, \ldots, r_{l-1}^{(n)}, r_l^{(n)}, \ldots, r_{q_n}^{(n)})) \in B'\right] \geq \frac{1}{4q_n T'(\kappa)}$,
  where the probability is taken over $S_n^{q_n - l + 1}$.

As a result, if we choose l, ω, $(r^{(1)}, \ldots, r^{(n-1)}, (r_1^{(n)}, \ldots, r_{l-1}^{(n)}), (r_l^{(n)}, \ldots, r_{q_n}^{(n)})$, and $(r'^{(n)}_l, \ldots, r'^{(n)}_{q_n})$ randomly, then we obtain two valid signatures $(\sigma_0, \ldots, \sigma_n, h_1, \ldots, h_n)$ and $(\sigma_0, \ldots, \sigma'_n, h_1, \ldots, h'_n)$ for message m with a non-negligible probability such that $h_n \neq h'_n$.[1]

□

Chosen-Message Attack Model

We now provide the Extended Forking Lemma in the adaptively chosen-message attack model. In this model, an adversary may adaptively invoke a signing oracle and is successful if it manages to compute a signature on a new message. If the signing oracle outputs signatures which are indistinguishable from a genuine signer without knowing the signing key, then using the simulator one can obtain two distinct signatures with a suitable relation from a single signature, similarly to the no-message scenario.

Theorem 1 (The Chosen-Message Extended Forking Lemma). *Let* S *be an n-generic signature scheme with security parameter κ. Let $\mathcal{A}$ be a PPT algorithm given only the public data as input. We assume that $\mathcal{A}$ can find a valid signature $(\sigma_0, \ldots, \sigma_n, h_1, \ldots, h_n)$ for message m with a non-negligible probability, after asking the n random oracles $\mathcal{O}_1, \ldots, \mathcal{O}_n$, and the signer polynomially often (in κ). Then, there exists another PPT algorithm $\mathcal{B}$ which has control over $\mathcal{A}$ by replacing interactions with the real signer by a simulation, and which provides with a non-negligible probability two valid signatures $(\sigma_0, \ldots, \sigma_n, h_1, \ldots, h_n)$ and $(\sigma_0, \ldots, \sigma'_n, h_1, \ldots, h'_n)$ for the same message m such that $h_n \neq h'_n$.*

[1] Since l is the index of $\mathcal{A}$'s query and there are only polynomially number of queries made by $\mathcal{A}$, our success probability remains non-negligible when picking l randomly.

Proof. We consider a PPT algorithm $\mathcal{B}$ that executes $\mathcal{A}$ in such a way that $\mathcal{B}$ simulates the environment of $\mathcal{A}$. Therefore, $\mathcal{B}$ must simulate the interactions of $\mathcal{A}$ with random oracles $\mathcal{O}_1, \ldots, \mathcal{O}_n$ and with the real signer. Then, we could see $\mathcal{B}$ as an algorithm performing a no-message attack against the signature scheme S.

Let Sim denote the zero-knowledge simulator of S that can simulate the answers of the real signer without knowledge of the secret key and has access to the random oracles $\mathcal{O}_i$ $(1 \leq i \leq n)$. Let $\mathcal{A}$ be an adaptively chosen-message adversary, which is a probabilistic polynomial time Turing machine with a random tape ω taken from a set R_ω. During the attack, $\mathcal{A}$ may ask $q_1, \ldots, q_n$ queries to random oracles $\mathcal{O}_1, \ldots, \mathcal{O}_n$, and q_s queries (possibly repeated) to Sim. The values $q_1, \ldots, q_n$ and q_s are polynomially bounded in κ. We denote by $q_1^{(i)}, \ldots, q_{q_i}^{(i)}$ the q_i distinct queries to the random oracles $\mathcal{O}_i$, and by $m^{(1)}, \ldots, m^{(q_s)}$ the q_s queries to the simulator Sim.

The simulator Sim answers a tuple $(\sigma_0^{(j)}, \ldots, \sigma_n^{(j)}, h_1^{(j)}, \ldots, h_n^{(j)})$ as a signature for a message $m^{(j)}$, for each integer j with $1 \leq j \leq q_s$. Then, the adversary $\mathcal{A}$ assumes that $h_i^{(j)} = \mathcal{O}_i(m^{(j)}, \sigma_0^{(j)}, h_1^{(j)}, \ldots, h_{i-1}^{(j)}, \sigma_{i-1}^{(j)})$ holds for all $1 \leq i \leq n$ and $1 \leq j \leq q_s$, and stores all these relations.

Now we need to consider potential "collisions" of queries in the random oracles. There are two kind of collisions that can appear. That is, (a) the simulator Sim queries the random oracle with the same input the adversary has asked before (let us denote this event by $\mathcal{E}_1$), and (b) Sim asks the same question repeatedly (let us denote this event by $\mathcal{E}_2$).

We show that the probabilities of such events are negligible.

$$\Pr[\mathcal{E}_1] = \Pr[\exists i \in \{1, \ldots, n\}; \exists j \in \{1, \ldots, q_s\}; \exists t \in \{1, \ldots, q_n\} | (m^{(j)}, \sigma_0^{(j)}, h_1^{(j)}, \ldots, h_{i-1}^{(j)}, \sigma_{i-1}^{(j)}) = q_t^{(i)}]$$

$$\leq \sum_{i=1}^{n} \sum_{j=1}^{q_s} \sum_{t=1}^{q_n} \Pr[(m^{(j)}, \sigma_0^{(j)}, h_1^{(j)}, \ldots, h_{i-1}^{(j)}, \sigma_{i-1}^{(j)}) = q_t^{(i)}] \leq \frac{n q_s q_n}{2^\kappa},$$

which is negligible, assuming that the σ_i's are random values drawn from a large set with cardinality greater than 2^κ.
Moreover, we have

$$\Pr[\mathcal{E}_2] = \Pr[\exists i \in \{1, \ldots, n\}; \exists j, j' \in \{1, \ldots, q_s\} : j \neq j' | (m^{(j)}, \sigma_0^{(j)}, h_1^{(j)}, \ldots, h_{i-1}^{(j)}, \sigma_{i-1}^{(j)}) = (m^{(j')}, \sigma_0^{(j')}, h_1^{(j')}, \ldots, h_{i-1}^{(j')}, \sigma_{i-1}^{(j')})]$$

$$\leq \sum_{i=1}^{n} \sum_{j=1}^{q_s} \sum_{j'=1}^{j} \Pr[(m^{(j)}, \sigma_0^{(j)}, h_1^{(j)}, \ldots, h_{i-1}^{(j)}, \sigma_{i-1}^{(j)}) = (m^{(j')}, \sigma_0^{(j')}, h_1^{(j')}, \ldots, h_{i-1}^{(j')}, \sigma_{i-1}^{(j')})] \leq \frac{n q_s^2}{2^\kappa},$$

which is also negligible.

Algorithm $\mathcal{B}$ succeeds whenever the machine $\mathcal{A}$ produces a valid signature without any collisions. Hence, we have

$$\Pr[\mathcal{B} \text{ succeeds }] = \Pr[\mathcal{A} \text{ succeeds }] - \Pr[\mathcal{E}_1] - \Pr[\mathcal{E}_2] \geq \frac{1}{T(\kappa)} - \frac{nq_sq_n}{2^\kappa} - \frac{nq_s^2}{2^\kappa},$$

which is non-negligible.

Summing up, we have an algorithm $\mathcal{B}$ that performs a no-message attack against the signature scheme S in polynomial time with non-negligible probability of success. So we can use Lemma 2 applied to algorithm $\mathcal{B}$, and we will obtain two valid signatures for the same message, such that $h_n \neq h'_n$ again in polynomial time.

□

3.3 Security of n-Generic Signature Schemes

Similar to generic signature schemes defined by Pointcheval and Stern [12], for security under chosen-message attacks we require from n-generic signature schemes a property which we call n-soundness. Informally, n-soundness means that the secret key can be extracted from two correlated valid signatures $\sigma = (\sigma_0, h_1, \ldots, \sigma_{n-1}, h_n, \sigma_n)$ and $\sigma' = (\sigma_0, h_1, \ldots, \sigma_{n-1}, h'_n, \sigma'_n)$ with $h_n \neq h'_n$ in polynomial-time and with a non-negligible probability. The notion of special-soundness[2] and n-soundness coincide if $n = 1$.

Definition 4 (n-Soundness). *Let* S $= (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vf})$ *be an n-generic signature scheme. We call* S *n-sound if there exists a PPT algorithm K, the knowledge extractor, such that for any κ and m, any* $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\kappa)$*, any* $\sigma = (\sigma_0, h_1, \ldots, \sigma_{n-1}, h_n, \sigma_n)$ *and* $\sigma' = (\sigma_0, h_1, \ldots, \sigma_{n-1}, h'_n, \sigma'_n)$ *with* $\mathsf{Vf}(\mathsf{pk}, m, \sigma) = \mathsf{Vf}(\mathsf{pk}, m, \sigma') = 1$ *and $h'_n \neq h_n$, we have* $\mathsf{sk} \leftarrow K(\mathsf{pk}, \sigma, \sigma')$ *with non-negligible probability.*

The following theorem states that all n-generic signature schemes satisfying n-soundness are existentially unforgeable under adaptively chosen-message attacks in the random oracle model.

Theorem 2 (Security of n-Generic Signature Schemes). *Let* S *be an n-generic signature scheme satisfying n-soundness with underlying hard problem* **P***. Let κ be the security parameter. Then,* S *is existentially unforgeable under adaptively chosen-message attacks.*

Proof. We assume that the underlying hardness **P** of the n-generic signature scheme is hard, i.e., for all PPT algorithms $\mathcal{A}$ the probability to solve a hard instance of **P** is negligible. The key generation algorithm KGen of S outputs a secret and public key pair $(\mathsf{sk}, \mathsf{pk})$ derived by a hard instance and its corresponding solution of the problem **P**.

[2] Actually, special-soundness is a notion belonging to identification schemes. However, since this property is quite similar to the required property of generic signature schemes, this concept is used for both cases in the literature.

Now, assume by contradiction, that S is *not* existentially unforgeable under chosen-message attacks. That is, there exists a PPT algorithm $\mathcal{B}_1$ such that $\mathcal{B}_1$ is able to output a signature $\sigma^* = (\sigma_0, h_1, \ldots, \sigma_{n-1}, h_n, \sigma_n)$ for a fresh message m^* with non-negligible probability. Then, due to the Extended Forking Lemma, one can construct a PPT algorithm $\mathcal{B}_2$ which outputs two correlated signatures $\sigma^* = (\sigma_0, h_1, \ldots, \sigma_{n-1}, h_n, \sigma_n)$ and $\sigma^{**} = (\sigma_0, h_1, \ldots, \sigma_{n-1}, h'_n, \sigma'_n)$ with non-negligible probability such that $h_n \neq h'_n$.

Due to the n-soundness of S, we know that there exists an "extractor" which extracts the secret key given the two signatures above. This contradicts with the assumption that the underlying problem **P** is hard, and by implication, we learn that there cannot exist such a successful forger $\mathcal{B}_1$.

4 Applications

In this section we first discuss a transformation from $(2n + 1)$-pass identification protocols with a special structure to signature schemes that in many cases yields n-generic signature schemes. This is essentially an extended Fiat-Shamir transform. Then we go on with a specific instance of the aforementioned transformation. We obtain a new signature scheme based on multivariate polynomials by applying our method to a five-pass identification scheme recently introduced in [14].

4.1 n-Generic Signature Schemes Derived from Identification Schemes

Our goal is to enlarge the class of identification protocols to which the Fiat-Shamir transformation can be applied. We identify a potential set of candidates that we name *n-canonical identification schemes*. By n-canonical identification we mean schemes secure with respect to impersonation against passive attacks, where the challenges are drawn from an uniform distribution and have $2n + 1$ moves.

Definition 5 (n-canonical Identification Protocol). *An n-canonical identification scheme* $\mathrm{IS} = (\mathcal{K}, \mathcal{P}, \mathcal{V})$ *is a $(2n + 1)$-pass interactive protocol. $\mathcal{K}$ and $\mathcal{P} = (\mathsf{P}_1, \ldots, \mathsf{P}_{n+1})$ are PPT algorithms whereas $\mathcal{V} = (\mathsf{ChSet}, \mathsf{Vf})$ with ChSet being a PPT algorithm and Vf a deterministic boolean algorithm. These algorithms are defined as follows:*

$\mathcal{K}(1^\kappa)$ *upon input a security parameter 1^κ, outputs a secret and public key $(\mathsf{sk}, \mathsf{pk})$ and challenge spaces $G_1, \ldots, G_n$ with $1/|G_i|$ negligible in 1^κ.*

$\mathsf{P}_1(\mathsf{sk})$ *upon input a secret key sk outputs the commitment R_1.*

$\mathsf{P}_i(\mathsf{sk}, R_1, C_1, \ldots, R_{i-1}, C_{i-1})$ *for $i = 2, \ldots, n$, upon input a secret key sk and the current transcript $R_1, C_1, \ldots, R_{i-1}, C_{i-1}$, outputs the i-th commitment R_i.*

$\mathsf{P}_{n+1}(\mathsf{sk}, R_1, C_1, \ldots, R_n, C_n)$ *upon input a secret key sk and the current transcript $R_1, C_1, \ldots, R_n, C_n$, outputs a response Rsp.*

$\mathsf{ChSet}(\mathsf{pk}, i)$ *upon input a public key* pk *and round number* i*, outputs a challenge* $C_i \in G_i$.

$\mathsf{Vf}(\mathsf{pk}, R_1, C_1, \ldots, R_n, C_n, Rsp)$ *upon input a public key* pk*, and the current transcript* $R_1, C_1, \ldots, R_n, C_n, Rsp$*, outputs either* 1 (= *valid*) *or* 0 (= *invalid*).

An n*-canonical identification scheme* IS *has the following properties.*

Public-Coin. *For any index* $i \in \{1, \ldots, n\}$ *and any* $(\mathsf{sk}, \mathsf{pk}, G_1, \ldots, G_n) \leftarrow \mathcal{K}(1^\kappa)$ *the challenge* $C_i \leftarrow \mathsf{ChSet}(\mathsf{pk}, i)$ *is uniform in* G_i.

Honest-Verifier Zero-Knowledge. *There exists a PPT algorithm* Z*, the zero-knowledge simulator, such that for any pair of PPT algorithms* $D = (D_0, D_1)$ *the following distributions are computationally indistinguishable:*

- *Let* $(\mathsf{pk}, \mathsf{sk}, state) \leftarrow D_0(1^\kappa)$*, and* $trans = (R_1, C_1, \ldots, R_n, C_n, Rsp) \leftarrow \langle \mathcal{P}(\mathsf{sk}, \mathsf{pk}), \mathcal{V}(\mathsf{pk}) \rangle$ *if* pk *belongs to* sk*, and otherwise* $trans \leftarrow \perp$*. Output* $D_1(trans, state)$.
- *Let* $(\mathsf{pk}, \mathsf{sk}, state) \leftarrow D_0(1^\kappa)$*, and* $trans = (R_1, C_1, \ldots, R_n, C_n, Rsp) \leftarrow Z(\mathsf{pk}, 1)$ *if* pk *belongs to* sk*, and otherwise* $trans \leftarrow Z(\mathsf{pk}, 0)$*. Output* $D_1(trans, state)$.

Note that the definition of 1-canonical identification schemes is identical to that of canonical identification schemes [1]. An extended Fiat-Shamir transform is applied to an n-canonical identification scheme and yields an n-generic signature scheme, just as the original Fiat-Shamir transform yields a generic signature scheme in [12]. The idea of this transformation consists on replacing the uniformly random challenges of the verifier as set by ChSet in the identification scheme by the outputs of some secure hash functions $\mathrm{H}_i : \{0,1\}^* \to G_i$ modeled as random oracles. More precisely, let $\mathrm{IS} = (\mathcal{K}, \mathcal{P}, \mathcal{V})$ be an n-canonical identification scheme. The joint execution of $\mathcal{P}(\mathsf{sk}, \mathsf{pk})$ and $\mathcal{V}(\mathsf{pk})$ then defines an interactive protocol between the prover $\mathcal{P}$ and the verifier $\mathcal{V}$. At the end of the protocol $\mathcal{V}$ outputs a decision bit $b \in \{0,1\}$. An n-generic signature scheme $\mathrm{S} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vf})$ is derived as follows:

$\mathsf{KGen}(1^\kappa)$ takes as input security parameter 1^κ and returns $\mathcal{K}(1^\kappa)$.

$\mathsf{Sign}(\mathsf{sk}, m)$ takes as input a secret key sk and a message m and returns the transcript $\langle \mathcal{P}(\mathsf{sk}, \mathsf{pk}), \mathcal{V}(\mathsf{pk}) \rangle$ as the signature σ, i.e.,

$$\sigma = (\sigma_0, h_1, \ldots, h_n, \sigma_n) = (R_1, C_1, \ldots, R_n, C_n, Rsp)$$

or simply $\sigma = (\sigma_0, \ldots, \sigma_n, h_1 \ldots, h_n) = (R_1, \ldots, R_n, Rsp, C_1, \ldots, C_n)$. Here, C_i is defined by the equation $C_i := \mathrm{H}_i(m, R_1, \ldots, R_i, C_1, \ldots, C_{i-1})$.

$\mathsf{Vf}(\mathsf{pk}, m, \sigma)$ takes as input a public key pk, a message m and a signature σ and returns $\mathcal{V}.\mathsf{Vf}(\mathsf{pk}, m, \sigma)$[3] as the decision bit.

[3] By $\mathcal{V}.\mathsf{Vf}(\mathsf{pk}, m, \sigma)$ we mean the verification algorithm performed by the verifier from the underlying identification scheme IS.

The resulting scheme S is an n-generic signature scheme. Indeed, the obtained scheme S has the right structure and the honest-verifier zero-knowledge property is guaranteed by (the similar property of) the identification scheme.

However, it is still not guaranteed that S is existentially unforgeable. It lacks then to check/prove that the resulting scheme S is n-sound. If this is the case then one can apply Theorem 2 and S is guaranteed to have security against adaptive chosen-message attacks.

Let us point out that the plain version of most identification protocols does not directly satisfy the required security level by their choice of challenges spaces $G_1, \ldots, G_n$. In particular, it might be the case that $1/|G_i|$ is not negligible in the security parameter 1^κ. For that reason, one should typically repeat the ID protocol several (say δ) times until the desired security level is reached. In that case the concatenation of δ transcripts $\langle \mathcal{P}(\mathsf{sk}, \mathsf{pk}), \mathcal{V}(\mathsf{pk}) \rangle$ builds the signature (instead of a single execution of the ID scheme). Moreover, for our security analysis, we consider that the commitments R_i in all contain more entropy than k_n, the output size of the last hash function. This condition can be achieved by choosing their domain as large as necessary. Note that in [12] it is assumed that R_1 is uniformly distributed over its corresponding set.

4.2 Examples

Many zero-knowledge identification schemes have been proposed, whose conversion to signature schemes does not lead to generic signature schemes according to the definition of Pointcheval and Stern [12]. Examples of such schemes are those based on the Permuted Kernel Problem [15,8], the Permuted Perceptron Problem [10,11], the Constrained Linear Equations [18], the five-pass variant of SD problem [17,2], the q-SD problem [4], the SIS problem [3,16] and the MQ-problem [14]. Fortunately, their conversion to signature schemes belong to the class of n-generic signature schemes. Unlike [10,11], they even satisfy n-soundness. Consequently, our result for security of n-generic signature schemes satisfying n-soundness carries over to the resulting signature schemes derived from all these aforementioned identification schemes in the random oracle model.

We provide next the security argument for the resulting signature scheme derived from the MQ-based identification scheme [14]. The conversion of all aforementioned identification schemes to n-generic signature schemes and its security can be formulated in a very similar fashion. For this reason, we omit these proofs here.

The (Five-Pass) MQ Identification Scheme [14] and Its Signature. Recently at Crypto 2011, Sakumoto et al. presented a five-pass public-key identification scheme based on multivariate quadratic polynomials [14]. Assuming the existence of a non-interactive commitment scheme Com which should be statistically hiding and computationally binding, the authors of [14] showed that their scheme is an honest-verifier zero-knowledge identification scheme whereas the n-soundness property is also verified as we will later see in the security analysis.

We first briefly describe the identification scheme [14], following the procedure to convert it into a signature scheme using Section 4.1. Finally, we analyze the security of the obtained signature scheme using the Extended Forking Lemma discussed in Section 3.2.

Let n, m and q be positive integers. We denote by $\mathcal{MQ}(n, m, \mathbb{F}_q)$ a family of functions

$$\{F(x) = (f_1(x), \cdots, f_m(x)) \mid f_l(x) = \sum_{i,j} a_{l,i,j} x_i x_j + \sum_i b_{l,i} x_i, \quad a_{l,i,j}, b_{l,i} \in \mathbb{F}_q \text{ for } l = 1, \cdots, m\},$$

where $x = (x_1, \cdots, x_n)$. An element F of $\mathcal{MQ}(n, m, \mathbb{F}_q)$ is called an MQ function and a function $G(x, y) = F(x + y) - F(x) - F(y)$ is called the polar form of F.

Let κ be a security parameter. Let $n = n(\kappa), m = m(\kappa)$ and $q = q(\kappa)$ be polynomially bounded functions. The key-generation algorithm $\mathcal{K}$ of this identification scheme can be described as follows. It takes 1^κ as input and creates a system parameter $F \in \mathcal{MQ}(n, m, \mathbb{F}_q)$ which consists of an m-tuple of random multivariate quadratic polynomials. Then, it randomly chooses a vector $s \in \mathbb{F}_q^n$ (secret key), and computes the corresponding public key $v := F(s)$. Finally, it returns the key pair $(\mathsf{pk}, \mathsf{sk}) = (v, s)$. Figure 1 illustrates the interaction protocol between the prover and the verifier.

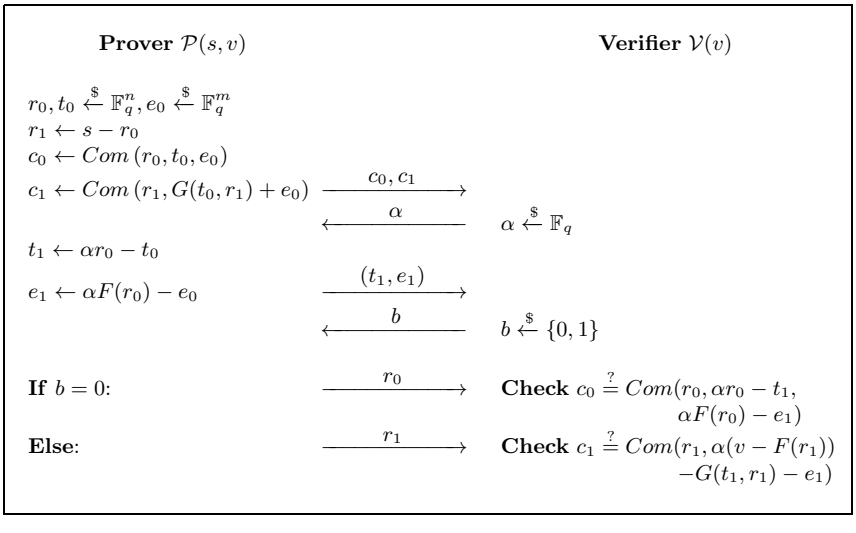

Fig. 1. The five-pass MQ identification scheme

The resulting Signature Scheme and its Security. According to Section 4.1, the MQ-based identification scheme described above can be turned to an n-generic signature scheme $\mathrm{S} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vf})$ as follows. Let δ be the number of rounds needed to achieve the required impersonation resistance.

$\mathsf{KGen}(1^\kappa)$ takes as input a security parameter 1^κ and outputs $\mathcal{K}(1^\kappa)$. The random oracles $\mathcal{O}_1$ and $\mathcal{O}_2$ output elements of $\mathbb{F}_q$ and $\{0,1\}$, respectively.

$\mathsf{Sign}(\mathsf{sk}, m)$ takes as input sk and a message m, and computes for all $1 \leq i \leq \delta$,

- $r_{1,i} = s - r_{0,i}$ where $r_{0,i} \xleftarrow{\$} \mathbb{F}_q^n$,
- $c_{0,i} = Com\left(r_{0,i}, t_{0,i}, e_{0,i}\right), c_{1,i} = Com\left(r_{1,i}, G(t_{0,i}, r_{1,i}) + e_{0,i}\right)$, and sets $\sigma_{0,i} = (c_{0,i}, c_{1,i})$, where $t_{0,i} \xleftarrow{\$} \mathbb{F}_q^n$ and $e_{0,i} \xleftarrow{\$} \mathbb{F}_q^m$,
- $h_{1,i} \in \mathbb{F}_q$ such that $h_{1,i} = \mathcal{O}_1(m, \sigma_{0,i})$,
- $(t_{1,i}, e_{1,i}) = (h_{1,i} r_{0,i} - t_{0,i}, h_{1,i} F(r_{0,i}) - e_{0,i})$ and sets $\sigma_{1,i} = (t_{1,i}, e_{1,i})$,
- $h_{2,i}$ such that $h_{2,i} = \mathcal{O}_2(m, \sigma_{0,i}, h_{1,i}, \sigma_{1,i})$,
- $(\sigma_{0,i}, h_{1,i}, \sigma_{1,i}, h_{2,i}, \sigma_{2,i})$, where $\sigma_{2,i} := r_{0,i}$ if $h_{2,i} = 0$ and, otherwise, $\sigma_{2,i} := r_{1,i}$,
- and finally, returns the signature σ for the message m as $(\sigma_0, h_1, \sigma_1, h_2, \sigma_2)$, where $\sigma_j = (\sigma_{j,1}, \ldots, \sigma_{j,\delta})$ and $h_k = (h_{k,1}, \ldots, h_{k,\delta})$ with $0 \leq j \leq 2$ and $1 \leq k \leq 2$.

$\mathsf{Vf}(\mathsf{pk}, m, \sigma)$ takes as input a public key pk, a message m and a signature σ, outputs 1 iff $(\sigma_{0,1}, \ldots, \sigma_{0,\delta})$ is well calculated as in the identification protocol, i.e., the following respective equation is valid for all $1 \leq i \leq \delta$:

$$\text{If } h_{2,i} = 0: \; c_{0,i} = Com\left(r_{0,i}, h_{1,i} r_{0,i} - t_{1,i}, h_{1,i} F(r_{0,i}) - e_{1,i}\right)$$
$$\text{If } h_{2,i} = 1: \; c_{1,i} = Com\left(r_{1,i}, h_{1,i}(v - F(r_{1,i})) - G(t_{1,i}, r_{1,i}) - e_{1,i}\right)$$

Security Argument. Using the Extended Forking Lemma, we prove in the following that the signature scheme derived from the MQ-based zero-knowledge identification scheme is secure against adaptively chosen message attacks. We assume that an adversary produces a valid signature $(\sigma_0, h_1, \sigma_1, h_2, \sigma_2)$ for a message m. By applying Theorem 1 we can find a second forgery $(\sigma_0, h_1, \sigma_1, h_2', \sigma_2')$ with a non-negligible probability, such that $h_2 \neq h_2'$. That leads to the existence of an index i with $1 \leq i \leq \delta$, such that $h_{2,i} \neq h_{2,i}'$. W.l.o.g. assume $h_{2,i} = 0$ and $h_{2,i}' = 1$. Now, the adversary gets the answers for two distinct challenges, namely $r_{0,i}$ and $r_{1,i}$. Finally, by adding the last two values, the secret key can be disclosed. This contradicts the intractability of the MQ problem.

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. Aguilar Melchor, C., Gaborit, P., Schrek, J.: A new zero-knowledge code based identification scheme with reduced communication. CoRR, abs/1111.1644 (2011)
3. Cayrel, P.-L., Lindner, R., Rückert, M., Silva, R.: Improved Zero-Knowledge Identification with Lattices. In: Heng, S.-H., Kurosawa, K. (eds.) ProvSec 2010. LNCS, vol. 6402, pp. 1–17. Springer, Heidelberg (2010)
4. Cayrel, P.-L., Véron, P., El Yousfi Alaoui, S.M.: A Zero-Knowledge Identification Scheme Based on the q-ary Syndrome Decoding Problem. In: Biryukov, A., Gong, G., Stinson, D.R. (eds.) SAC 2010. LNCS, vol. 6544, pp. 171–186. Springer, Heidelberg (2011)

5. 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)
6. El Gamal, T.: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 10–18. Springer, Heidelberg (1985)
7. Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof-systems. In: STOC 1985, pp. 291–304. ACM (1985)
8. Lampe, R., Patarin, J.: Analysis of some natural variants of the PKP algorithm. Cryptology ePrint Archive, Report 2011/686 (2011), http://eprint.iacr.org/
9. 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)
10. Pointcheval, D.: A New Identification Scheme Based on the Perceptrons Problem. In: Guillou, L.C., Quisquater, J.-J. (eds.) EUROCRYPT 1995. LNCS, vol. 921, pp. 319–328. Springer, Heidelberg (1995)
11. Pointcheval, D., Poupard, G.: A new NP-complete problem and public-key identification. Des. Codes Cryptography 28, 5–31 (2003)
12. Pointcheval, D., Stern, J.: Security Proofs for Signature Schemes. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 387–398. Springer, Heidelberg (1996)
13. Pointcheval, D., Stern, J.: Security arguments for digital signatures and blind signatures. J. Cryptology 13(3), 361–396 (2000)
14. Sakumoto, K., Shirai, T., Hiwatari, H.: Public-Key Identification Schemes Based on Multivariate Quadratic Polynomials. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 706–723. Springer, Heidelberg (2011)
15. Shamir, A.: An Efficient Identification Scheme Based on Permuted Kernels (Extended Abstract). In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 606–609. Springer, Heidelberg (1990)
16. Silva, R., Cayrel, P.-L., Lindner, R.: Zero-knowledge identification based on lattices with low communication costs. XI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais 8, 95–107 (2011)
17. Stern, J.: A New Identification Scheme Based on Syndrome Decoding. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 13–21. Springer, Heidelberg (1994)
18. Stern, J.: Designing Identification Schemes with Keys of Short Size. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 164–173. Springer, Heidelberg (1994)
19. Yao, A.C., Zhao, Y.: Digital signatures from challenge-divided sigma-protocols. Cryptology ePrint Archive, Report 2012/001 (2012), http://eprint.iacr.org/