From Identification to Signatures via the Fiat-Shamir Transform: Minimizing Assumptions for Security and Forward-Security

Michel Abdalla[1], Jee Hea An[2], Mihir Bellare[3], and Chanathip Namprempre[3]

[1] Magis Networks, Inc., 12651 High Bluff Drive, San Diego, CA 92130, USA.
E-Mail: mabdalla@cs.ucsd.edu. URL: www.michelabdalla.net.
[2] SoftMax, Inc., 10760 Thornmint Road, San Diego, CA 92128, USA.
E-Mail: jeehea@cs.ucsd.edu.
[3] Dept. of Computer Science & Engineering, University of California San Diego, 9500 Gilman Drive, La Jolla, California 92093, USA. E-Mail: {mihir,meaw}@cs.ucsd.edu.
URL: www-cse.ucsd.edu/users/{mihir,cnamprem}.

Abstract. The Fiat-Shamir paradigm for transforming identification schemes into signature schemes has been popular since its introduction because it yields efficient signature schemes, and has been receiving renewed interest of late as the main tool in deriving forward-secure signature schemes. We find minimal (meaning necessary and sufficient) conditions on the identification scheme to ensure security of the signature scheme in the random oracle model, in both the usual and the forward-secure cases. Specifically we show that the signature scheme is secure (resp. forward-secure) against chosen-message attacks in the random oracle model *if and only if* the underlying identification scheme is secure (resp. forward-secure) against impersonation under *passive* (i.e.. eavesdropping only) attacks, and has its commitments drawn at random from a large space. An extension is proven incorporating a random seed into the Fiat-Shamir transform so that the commitment space assumption may be removed.

1 Introduction

The Fiat-Shamir method of transforming identification schemes into signature schemes [11] is popular because it yields efficient signature schemes, and has been receiving renewed interest of late as the main tool in deriving forward-secure signature schemes. We find minimal (meaning necessary and sufficient) conditions on the identification scheme to ensure security of the signature scheme in the random oracle model. The conditions are simple and natural. Below we begin with some background and discussion of known results, and then move to our results, considering first the usual and then the forward-secure case.

Canonical ID schemes. The Fiat-Shamir (FS) transform applies to identification (ID) schemes having a three-move format that we call *canonical*. The prover, holding a secret key sk, sends a message $\textsc{Cmt}$ called a *commitment* to the verifier. The verifier returns a *challenge* $\textsc{Ch}$ consisting of a random string of some length. The prover provides a *response* $\textsc{Rsp}$. Finally, the verifier applies a verification algorithm V to the prover's public key pk and the conversation $\textsc{Cmt}\|\textsc{Ch}\|\textsc{Rsp}$ to obtain a *decision* bit, and accepts iff Dec = 1. The length of the challenge is $c(k)$ where k is the security parameter and c is a function associated to the scheme. A large number of canonical ID schemes are known (e.g., [11, 14, 6, 17, 24, 7, 12, 20, 19, 26, 21]) and are candidates for conversion to signature schemes via the FS transform.

THE FS TRANSFORM. The signer has the public and secret keys pk, sk of the prover of the ID scheme. To sign a message M it computes $\textsc{Cmt}$ just as the prover would, hashes $\textsc{Cmt}\|M$ using a public hash function $H\colon \{0,1\}^* \to \{0,1\}^{c(k)}$ to obtain a "challenge" $\textsc{Ch} = H(\textsc{Cmt}\|M)$, computes a response $\textsc{Rsp}$ just as the prover would, and sets the signature of M to $\textsc{Cmt}\|\textsc{Rsp}$. To verify that $\textsc{Cmt}\|\textsc{Rsp}$ is a signature of M, one first computes $\textsc{Ch} = H(\textsc{Cmt}\|M)$ and then checks that the verifier of the identification scheme would accept, namely $V(pk, \textsc{Cmt}\|\textsc{Ch}\|\textsc{Rsp}) = 1$. Fiat and Shamir's suggestion that one model H as a random oracle [11] is adopted by previous security analyses, both in the standard setting [23, 18] and in the forward-secure setting [4, 2, 15], and also by this paper.

TARGET SECURITY GOAL FOR SIGNATURES. Focusing first on the standard setting (meaning where forward-security is not a goal), the target is to prove that the signature scheme is unforgeable under chosen-message attack [13] in the random oracle model [5]. This requires that it be computationally infeasible for an adversary to produce a valid signature of a new message even after being allowed a chosen-message attack on the signer and provided oracle access to the random hash function.

NON-TRIVIALITY. Previous works [23, 18] have assumed that the ID scheme has the property that the space from which the prover draws its commitments is large, meaning super-polynomial. We refer to a scheme with this property as non-trivial. (A more general definition, in terms of min-entropy, is Definition 3.) We point out in Section 6 that non-triviality of the ID scheme is *necessary* for the security of the signature scheme derived via the FS transform, and thus all discussions related to the FS transform below will assume it. (We will see however that this assumption can be removed by considering a randomized generalization of the FS transform.)

1.1 Main result

In this work we find simple and natural assumptions on the ID scheme that are both sufficient and necessary for the security of the signature scheme, and are related to the security of the underlying ID scheme for the purpose for which it was presumably designed, namely identification.

STATEMENT. We prove the following: The signature scheme resulting from applying the FS transform to a non-trivial ID scheme is secure against chosen-message attack in the random oracle model *if and only if* the underlying identification scheme is secure against impersonation under passive attack. A precise statement is Theorem 1. Let us recall the notion of security used here, following [10], and then compare this to previous work.

SECURITY OF IDENTIFICATION SCHEMES. As with any primitive, a notion of security considers adversary goals (what it has to do to win) and adversary capability (what attacks it is allowed). Naturally, for an ID scheme, the adversary goal is impersonation: it wins if it can interact with the verifier in the role of a prover and convince the latter to accept. There are two natural attacks to consider: passive and active. Passive attacks correspond to eavesdropping, meaning the adversary is in possession of transcripts of conversations between the real prover and the verifier. Active attacks mean that it gets to play the role of a verifier, interacting with the real prover in an effort to extract information. Security against impersonation under active attack is the attribute usually desired of an ID scheme to be used in practice for the purpose of identification. It is however the weaker attribute of security against impersonation under passive attack that we show is tightly coupled to the security of the derived signature scheme.

1.2 Comparison with previous work

Past security analyses identify assumptions on a non-trivial ID scheme that suffice to prove that corresponding the FS-transform based signature scheme is secure, as follows. The pioneering work of Pointcheval and Stern [23] assumes that the identification scheme is honest verifier zero-knowledge and also, in their Forking Lemma, assume a property that implies that it is a "proof of knowledge" [10, 3], namely that there is an algorithm that can produce two transcripts which start with the same commitment $(\textsc{Cmt}, \textsc{Ch}, \textsc{Rsp})$, $(\textsc{Cmt}, \textsc{Ch}', \textsc{Rsp}')$ such that, if both are accepted by the verifier V, the underlying secret key can be determined. (This property is called *collision intractability* in [9].) We refer to an ID scheme meeting these conditions as **PS**-secure.

Ohta and Okamoto [18] assume that the identification scheme is honest-verifier (perfect) zero-knowledge and that it is computationally infeasible for a cheating prover to convince the verifier to accept. We refer to such an ID scheme as **OO**-secure.

RELATIONS. Figure 1 puts our result in context with previous works. It considers the three assumptions made on non-trivial identification schemes for the purpose of proving security of the corresponding FS-transform based signature scheme: **PS**-security [23]; **OO**-security [18]; and the assumption of security against impersonation under passive attacks. As the picture indicates, all three suffice to prove security of the signature scheme in the random oracle model. However, the assumption we make is not only necessary but also sufficient, while the others are provably not necessary. Furthermore, our assumption is weaker than the other assumptions, shown to imply them but not be implied by them. Let us discuss this further.

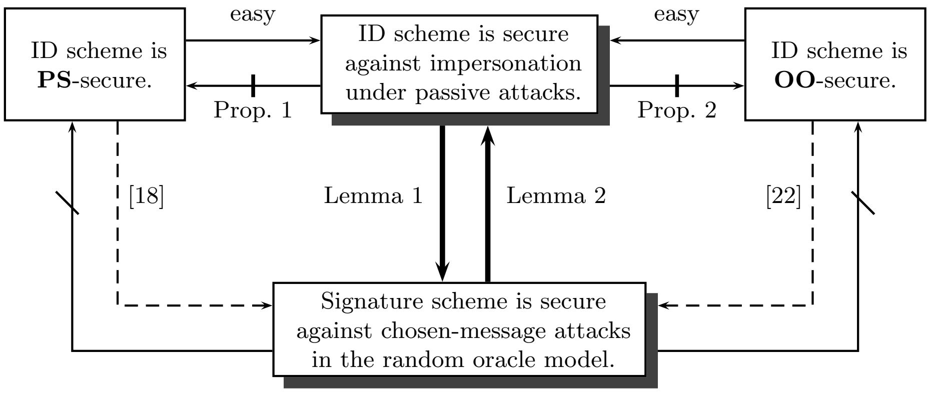

Fig. 1. We depict relations among assumptions on non-trivial ID schemes that have been used to prove security of the corresponding signature scheme. An arrow denotes an implication while a barred arrow denotes a separation. The dotted arrows are existing relations, annotated with citations to the papers establishing them. The full arrows are either relations established in this paper, or are easy.

It is well known that **PS** or **OO** security imply security against impersonation under passive attacks. The converse, however, is not true: in Section 4, we present examples that show that a non-trivial ID scheme could be secure against impersonation under passive attack yet be neither **PS** nor **OO** secure. Thus, our assumption on the ID scheme is weaker than previous ones. On the other hand, the fact that this assumption is necessary says that it is minimal. A consequence is that there exist (non-trivial) ID schemes that are neither **PS**-secure nor **OO**-secure, yet the corresponding signature scheme is secure, showing that the previous assumptions are not necessary conditions for the security of the signature scheme.

In practice, these gaps may not be particularly limiting, because practical ID schemes for the most part are **PS**-secure or **OO**-secure. However our result can simplify future or even existing constructions of identification based signature schemes, and clarifies the theoretical picture.

Assumptions related to the problem. Fiat and Shamir [11] suggested that their transform be applied to an ID scheme. However, previous security analyses have made assumptions that are in fact not inherent to the notion of identification itself. By this we mean assumptions such as honest verifier zero-knowledge or that underlying the forking lemma. These types of properties are convenient tools in the analysis of ID schemes, but not the end goals of identification. In particular, as we show in Section 4, there exist ID schemes, secure even against active attack, that are not honest verifier zero-knowledge and fail to meet the conditions of the forking lemma. In contrast, our necessary and sufficient condition, namely security against impersonation under passive attacks, is a natural end goal of identification. Our results thus support the original intuition that seems to have guided [11], namely that the security of the signature scheme stems from the security of the identification scheme relative to the job for which the latter was intended.

1.3 Generalized transform

As previously mentioned, the non-triviality assumption on an ID scheme is necessary to guarantee that the FS transform yields a secure signature scheme. We define a randomized generalization of the Fiat-Shamir transform (described in detail in Construction 1). We show that this modification allows the non-triviality assumption to be removed. Specifically, we prove that the signature scheme resulting from our generalized Fiat-Shamir transform is secure against chosen-message attack in the random oracle model *if and only if* the underlying identification scheme is secure against impersonation under passive attack. A precise statement is presented in Theorem 2.

We note that the process of applying our generalized transform to a given ID scheme can be alternatively viewed as first modifying the ID scheme by enhancing its commitment space and then applying the FS transform.

1.4 Results for forward security

An important paradigm in the construction of forward-secure signature schemes, beginning with [4] and continuing with [2, 15], has been to first design a forward-secure identification scheme and then obtain a forward-secure signature scheme via the FS transform. The analyses in these works are however ad hoc.

We prove an analogue of our main result that says that the signature scheme resulting from applying FS transform to a non-trivial ID scheme is forward-secure against chosen-message attacks in the random oracle model *if and only if* the underlying identification scheme is forward-secure against impersonation under passive attack. An extension based on the generalized FS transform, analogous to that mentioned above, also holds. This brings the characterization described above to forward-secure signature schemes, and helps to unify previous results [4, 2, 15]. Our result can simplify future or even existing constructions of identification based forward-secure signature schemes, saving repetition in the analytical work. (One should note however that non-modular analyses may have the benefit of yielding better concrete security than is obtained by our general result [2, 15].)

1.5 Discussion and remarks

Other transforms. There are other methods of transforming ID schemes into signature schemes. A variant of the FS transform suggested by Micali and Reyzin [16] applies only to a subclass of canonical ID schemes. A transform suggested by Cramer and Damgård [9] has the advantage of not requiring random oracles in the analysis, but is relatively inefficient. Overall the FS transform has remained the most attractive, due to its wide applicability, the efficiency of the resulting signature scheme, and its robustness in the face of extra goals such as forward security, and thus is our focus.

THE PROOFS. This abstract outlines proof ideas where space permits. Full proofs can be found in [1]. We note that our proofs appear to be simpler than previous ones even though our results are stronger. We believe that this is true because our assumptions, although weaker, have extracted more of the properties of the ID scheme that are truly relevant to the security of the signature scheme, thereby leaving less to be proven.

2 Definitions

NOTATION. If $A(\cdot, \cdot, \ldots)$ is a randomized algorithm, then $y \leftarrow A(x_1, x_2, \ldots; R)$ means y is assigned the unique output of the algorithm on inputs $x_1, x_2, \ldots$ and coins R, while $y \leftarrow A(x_1, x_2, \ldots)$ is shorthand for first picking R at random and then setting $y \leftarrow A(x_1, x_2, \ldots; R)$. We let $\mathsf{Coins}_A(k)$ denote the space from which R is drawn —it is a set of binary strings of some appropriate length— where k is the underlying security parameter. If S is a set then $s \stackrel{R}{\leftarrow} S$ indicates that s is chosen uniformly at random from S. If $x_1, x_2, \ldots$ are strings then $x_1 \| x_2 \| \cdots$ denotes an encoding under which the constituent strings are uniquely recoverable. It is assumed any string x can be uniquely parsed as an encoding of some sequence of strings. The empty string is denoted ε.

CANONICAL IDENTIFICATION SCHEMES. We use the term *canonical* to describe a three-move protocol in which the verifier's move consists of picking and sending a random string of some length, and the verifier's final decision is a deterministic function of the conversation and the public key (cf. Figure 2). The specification of a *canonical identification scheme* will take the form $\mathcal{ID} = (K, P, V, c)$ where K is the *key generation* algorithm, taking input a security parameter $k \in \mathsf{N}$ and returning a public and secret key pair (pk, sk); P is the *prover* algorithm taking input sk and the current conversation prefix to return the next message to send to the verifier; c is a function of k indicating the length of the verifier's challenge; V is a deterministic algorithm taking pk and a complete conversation transcript to return a boolean decision Dec on whether or not to accept. We associate to $\mathcal{ID}$ and each (pk, sk) a randomized *transcript generation oracle* which takes no inputs and returns a random transcript of an "honest" execution, namely:

Function $\mathsf{Tr}^{\mathcal{ID}}_{pk,sk,k}$
 $R_P \stackrel{R}{\leftarrow} \mathsf{Coins}_P(k)$
 $\text{CMT} \leftarrow P(sk; R_P)$; $\text{CH} \stackrel{R}{\leftarrow} \{0,1\}^{c(k)}$; $\text{RSP} \leftarrow P(sk, \text{CMT}\|\text{CH}; R_P)$;
 Return $\text{CMT}\|\text{CH}\|\text{RSP}$

The scheme must obey a standard completeness requirement, namely that for every k, we have $\Pr[V(pk, \text{CMT}\|\text{CH}\|\text{RSP}) = 1] = 1$, the probability being over $(pk, sk) \leftarrow K(k)$ and $\text{CMT}\|\text{CH}\|\text{RSP} \leftarrow \mathsf{Tr}^{\mathcal{ID}}_{pk,sk,k}$.

Prover		Verifier
Input: sk		Input: pk
	$\xrightarrow{\textsc{Cmt}}$	
		$\textsc{Ch} \stackrel{R}{\leftarrow} \{0,1\}^{c(k)}$
	$\xleftarrow{\textsc{Ch}}$	
	$\xrightarrow{\textsc{Rsp}}$	
		$\mathrm{Dec} \leftarrow V(pk, \textsc{Cmt}\|\textsc{Ch}\|\textsc{Rsp})$

Fig. 2. A canonical identification protocol.

Security against impersonation under passive attacks considers an adversary —here called an impersonator— whose goal is to impersonate the prover without the knowledge of the secret key. In practice, such an adversary generally has access not only to the public key but also to conversations between the real prover and an honest verifier, possibly via eavesdropping over the network. We model this setting by viewing an impersonator as a probabilistic algorithm I and giving to it the public key and the transcript-generation oracle defined above. This oracle gives I the ability to obtain some number of transcripts of honest executions of the protocol. After reviewing the transcripts, the impersonator must then participate in the three-move protocol with an honest verifier and try to get the verifier to accept.

Definition 1. [**Security of an identification scheme under passive attacks**] Let $\mathcal{ID} = (K, P, V, c)$ be a canonical identification scheme, and let I be an impersonator, st be its state, and k be the security parameter. Define the *advantage* of I as

$$\mathbf{Adv}^{\text{imp-pa}}_{\mathcal{ID},I}(k) \;=\; \Pr[\,\mathbf{Exp}^{\text{imp-pa}}_{\mathcal{ID},I}(k) = 1\,]\;,$$

where the experiment in question is

$\mathbf{Exp}^{\text{imp-pa}}_{\mathcal{ID},I}(k)$

$\quad (pk, sk) \leftarrow K(k)\,;\; st\|\textsc{Cmt} \leftarrow I^{\mathsf{Tr}^{\mathcal{ID}}_{pk,sk,k}}(pk)\,;\; \textsc{Ch} \stackrel{R}{\leftarrow} \{0,1\}^{c(k)}$

$\quad \textsc{Rsp} \leftarrow I(st, \textsc{Ch})\,;\; \mathrm{Dec} \leftarrow V(pk, \textsc{Cmt}\|\textsc{Ch}\|\textsc{Rsp})\,;\; \texttt{Return}\ \mathrm{Dec}$

We say that $\mathcal{ID}$ is *polynomially-secure against impersonation under passive attacks* if $\mathbf{Adv}^{\text{imp-pa}}_{\mathcal{ID},I}(\cdot)$ is negligible for every probabilistic poly(k)-time impersonator I. ▮

Signature schemes. We recall the standard definition of security of a digital signature scheme under chosen-message attacks (cf. [13]) adapted to the random oracle model as per [5].

The specification of a *digital signature scheme* will take the form $\mathcal{DS} = (K, S, Vf, c)$ where: K is the *key generation* algorithm, taking input a security parameter $k \in \mathsf{N}$ and returning a public and secret key pair (pk, sk); S is the *signing* algorithm taking input sk and a message $M \in \{0,1\}^*$ to be signed and returning a signature; Vf is the *verification* algorithm taking input pk, a message M and a candidate signature σ for M and returning a boolean decision. The signing and verifying algorithms have oracle access to a function $H\colon \{0,1\}^* \to \{0,1\}^{c(k)}$ (which in the random oracle model will be a random function) so that c in the scheme description is a function of k whose value is the output-length of the hash function being used. The signing algorithm may be randomized, drawing coins from a space $\mathsf{Coins}_S(k)$, but the verification algorithm is deterministic. It is required that valid signatures are always accepted.

The adversary F —called a forger in this setting— gets the usual signing oracle plus direct access to the random oracle and wins if it outputs a valid signature of a new message. Below, we let $[\{0,1\}^* \to \{0,1\}^c]$ denote the set of all maps from $\{0,1\}^*$ to $\{0,1\}^c$. The notation $H \stackrel{R}{\leftarrow} [\{0,1\}^* \to \{0,1\}^c]$ is used to mean that we select a hash function H at random from this set. The discussion following the definition clarifies how this random selection from an infinite space is implemented.

Definition 2. [**Security of a digital signature scheme**] Let $\mathcal{DS} = (K, S, \mathcal{V}, c)$ be a digital signature scheme, let F be a forger and k the security parameter. Define the experiment

$\mathbf{Exp}^{\text{frg-cma}}_{\mathcal{DS},F}(k)$
$H \stackrel{R}{\leftarrow} [\{0,1\}^* \to \{0,1\}^c]$
$(pk, sk) \leftarrow K(k)$; $(M, \sigma) \leftarrow F^{S^H_{sk}(\cdot), H(\cdot)}(pk)$; $\mathrm{Dec} \leftarrow Vf^H(pk, M, \sigma)$
`If` M was previously queried to $S^H_{sk}(\cdot)$ `then return` 0 `else return` Dec

Define the *advantage* of F as

$$\mathbf{Adv}^{\text{frg-cma}}_{\mathcal{DS},F}(k) \;=\; \Pr[\,\mathbf{Exp}^{\text{frg-cma}}_{\mathcal{DS},F}(k) = 1\,]\ .$$

$\mathcal{DS}$ is *polynomially-secure against chosen-message attacks* if $\mathbf{Adv}^{\text{frg-cma}}_{\mathcal{DS},F}(\cdot)$ is negligible for every probabilistic poly(k)-time forger F. ▮

A special convention is needed with regard to how one can measure the time taken by the first step of $\mathbf{Exp}^{\text{frg-cma}}_{\mathcal{DS},F}(k)$ where one picks at random a function H from an infinite space. This selection of the hash function is not viewed as being performed all at once. Rather, the hash function is built dynamically using a table. In particular, for each hash-oracle query M, we check if the entry $H(M)$ exists. If so, we return it. Otherwise, we pick a random element y from $\{0,1\}^c$, make a table entry $H(M) = y$, and return y.

Concrete security issues. In addition to our main results which speak in the usual language of polynomial security, we make concrete security statements so as to better gauge the practical impact of our reductions. Below, we discuss the parameters and conventions used.

When we refer to the running time of an adversary such as an impersonator or forger, we mean the time-complexity of the *entire* associated experiment, including the time taken to pick keys, compute replies to oracle queries, implement a random hash function as described above, and even compute the final outcome of the experiment.

For identification, the parameters of interest are the running time of the adversary and the number of queries q it makes to its transcript oracle. For signatures, the parameters of interest are the forger's running time, the number of sign-oracle queries, denoted q_s, and the number of hash-oracle queries, denoted q_h. All of these are functions of the security parameter k.

All query parameters are bounded by the running time, so if the adversary is polynomial time, all the other parameters are poly(k)-bounded. Thus, they can be ignored in the polynomial-time setting.

3 Equivalence Results

To save space (and avoid repetition), we present straightaway our randomized generalization of the Fiat-Shamir transform. The standard Fiat-Shamir transformation is the special case of the construction below in which the seed length is $s(k) = 0$.

Construction 1 (Generalized Fiat-Shamir Transform). Let $\mathcal{ID} = (K, P, V, c)$ be a canonical identification scheme and let $s\colon \mathsf{N} \to \mathsf{N}$ be a function which we call the *seed length*. We associate to these a digital signature scheme $\mathcal{DS} = (K, S, \mathit{Vf}, c)$. It has the same key generation algorithm as the identification scheme, and the output length of the hash function equals the challenge length of the identification scheme. The signing and verifying algorithms are defined as follows:

Algorithm $S^H(sk, M)$	Algorithm $\mathit{Vf}^H(pk, M, \sigma)$
$R \xleftarrow{R} \{0,1\}^{s(k)}$; $R_P \xleftarrow{R} \mathsf{Coins}_P(k)$	Parse σ as $R \Vert \textsc{Cmt} \Vert \textsc{Rsp}$
$\textsc{Cmt} \leftarrow P(sk; R_P)$	$\textsc{Ch} \leftarrow H(R \Vert \textsc{Cmt} \Vert M)$
$\textsc{Ch} \leftarrow H(R \Vert \textsc{Cmt} \Vert M)$	$\mathrm{Dec} \leftarrow V(pk, \textsc{Cmt} \Vert \textsc{Ch} \Vert \textsc{Rsp})$
$\textsc{Rsp} \leftarrow P(sk, \textsc{Cmt} \Vert \textsc{Ch}; R_P)$	Return Dec
Return $R \Vert \textsc{Cmt} \Vert \textsc{Rsp}$	

Note that the signing algorithm is randomized, using a random tape whose length is $s(k)$ plus the length of the random tape of the prover. Furthermore, the chosen random seed is included as part of the signature, to make verification possible. ∎

We use the concept of min-entropy [8] to measure how likely it is for a commitment generated by the prover of an identification scheme to collide with a fixed value. This is used to provide a more precise definition of what in the Introduction was referred to as a non-trivial ID scheme.

Definition 3. [**Min-Entropy of Commitments**] Let $\mathcal{ID} = (K, P, V, c)$ be a canonical identification scheme. Let $k \in \mathsf{N}$, and let (pk, sk) be a key pair generated by K on input k. Let $\mathcal{C}(sk) = \{P(sk; R_P) : R_P \in \mathsf{Coins}_P(k)\}$ be the set of commitments associated to sk. We define the maximum probability that a commitment takes on a particular value via

$$\alpha(sk) = \max_{\text{CMT} \in \mathcal{C}(sk)} \left\{ \Pr\left[P(sk; R_P) = \text{CMT} \ : \ R_P \stackrel{R}{\leftarrow} \mathsf{Coins}_P(k) \right] \right\}$$

Then, the *min-entropy* function associated to $\mathcal{ID}$ is defined as follows:

$$\beta(k) = \min_{sk} \left\{ \log_2 \frac{1}{\alpha(sk)} \right\} ,$$

where minimum is over all (pk, sk) generated by K on input k. We say that $\mathcal{ID}$ is *non-trivial* if $\beta(\cdot) = \omega(\log(\cdot))$ is super-logarithmic. ∎

We remark that for practical identification schemes, the commitment is drawn uniformly from some set. If the size of this set is $\gamma(\cdot)$ then the min-entropy of the scheme is $\log_2(\gamma(\cdot))$. Non-triviality means that this set has super-polynomial size.

The following theorem considers Construction 1 above in the special case where $s(k) = 0$. This case is exactly the Fiat-Shamir transform.

Theorem 1 (Equivalence Under Standard Fiat-Shamir Transform). *Let $\mathcal{ID} = (K, P, V, c)$ be a non-trivial, canonical identification scheme, and let $\mathcal{DS} = (K, S, Vf, c)$ be the associated signature scheme as per Construction 1 with $s(k) = 0$. Then $\mathcal{DS}$ is polynomially-secure against chosen-message attacks in the random oracle model if and only if $\mathcal{ID}$ is polynomially-secure against impersonation under passive attacks.* ∎

The non-triviality assumption above can be removed if one applies the generalized FS transform with a seed length that is not zero but which, when added to the min-entropy, results in a super-logarithmic function.

Theorem 2 (Equivalence Under Generalized Fiat-Shamir Transform). *Let $\mathcal{ID} = (K, P, V, c)$ be a canonical identification scheme, let $s(\cdot)$ be a seed length, and let $\mathcal{DS} = (K, S, Vf, c)$ be the associated signature scheme as per Construction 1. Let $\beta(\cdot)$ be the min-entropy function associated to $\mathcal{ID}$. Assume $s(\cdot) + \beta(\cdot) = \omega(\log(\cdot))$. Then $\mathcal{DS}$ is polynomially-secure against chosen-message attacks in the random oracle model if and only if $\mathcal{ID}$ is polynomially-secure against impersonation under passive attacks.* ∎

Theorem 1 is the special case of Theorem 2 in which $s(\cdot) = 0$ and $\beta(\cdot)$ is super-logarithmic. Accordingly, it suffices to prove Theorem 2. The proof of Theorem 2 follows easily from the two lemmas below. The first lemma relates the exact security of the signature scheme to that of the underlying identification scheme.

Lemma 1 (ID $\Rightarrow$ SIG). *Let $\mathcal{ID} = (K, P, V, c)$ be a canonical identification scheme, let $s(\cdot)$ be a seed length, and let $\mathcal{DS} = (K, S, Vf, c)$ be the associated signature scheme as per Construction 1. Let $\beta(\cdot)$ be the min-entropy function associated to $\mathcal{ID}$. Let F be an adversary attacking $\mathcal{DS}$ in the random oracle* *model, having time-complexity $t(\cdot)$, making $q_s(\cdot)$ sign-oracle queries and $q_h(\cdot)$ hash-oracle queries. Then there exists an impersonator I attacking $\mathcal{ID}$ such that*

$$\mathbf{Adv}^{\text{frg-cma}}_{\mathcal{DS},F}(k) \leq \big(1+q_h(k)\big) \cdot \mathbf{Adv}^{\text{imp-pa}}_{\mathcal{ID},I}(k) + \frac{[1+q_h(k)+q_s(k)] \cdot q_s(k)}{2^{s(k)+\beta(k)}} \ . \quad (1)$$

Furthermore, I has time-complexity $t(\cdot)$ and makes at most $q_s(\cdot)$ queries to its transcript oracle. ▮

The full proof of Lemma 1 is presented in the full version of the paper [1], but we give a brief sketch of it here. We use a standard approach, namely assuming that a forger F can break the signature scheme, we construct an impersonator I that has access to a transcript generation oracle. The goal of I is to convince an honest verifier that it is a prover without knowing the secret key. I achieves its goal by running the forger F as a subroutine, answering its hash and sign oracle queries. When F outputs a forgery, I can make use of it in its interaction with the verifier. In order to do so, I guesses the "forgery point," at which F makes a hash query (of the form $R\|\textsc{Cmt}\|M$) that contains the message M on which F will attempt to forge, and uses $\textsc{Cmt}$ as its commitment to the verifier. The verifier then replies with a challenge, and I uses this value in its response to F's hash query at the forgery point. I simulates the response to F's other hash and sign queries using the transcript generation oracle and randomness. When F finally outputs a forgery, I uses it to respond to the verifier's challenge. If I guessed F's forgery point correctly and if F's forgery was successful, then the impersonator succeeds. Note that "enough" randomness or min-entropy is needed to successfully simulate the responses to the forger's hash and sign queries.

Going in the opposite direction, the following lemma relates the security of the identification scheme to that of the signature scheme derived from it. In fact, it says that if the signature scheme is secure then so is the identification scheme (regardless of the min-entropy of the ID scheme).

Lemma 2 (ID $\Leftarrow$ SIG). *Let $\mathcal{ID} = (K, P, V, c)$ be a canonical identification scheme, let $s(\cdot)$ be a seed length, and let $\mathcal{DS} = (K, S, Vf, c)$ be the associated signature scheme as per Construction 1. Let I be an adversary attacking $\mathcal{ID}$, having time-complexity $t(\cdot)$ and making $q(\cdot)$ queries to its transcript oracle. Then, in the random oracle model, there exists a forger F attacking $\mathcal{DS}$ such that*

$$\mathbf{Adv}^{\text{imp-pa}}_{\mathcal{ID},I}(k) \leq \mathbf{Adv}^{\text{frg-cma}}_{\mathcal{DS},F}(k) \ . \quad (2)$$

Furthermore, F has time-complexity $t(\cdot)$, makes at most $q(\cdot)$ queries to its sign-oracle and at most $q(\cdot)$ queries to its hash-oracle. ▮

The proof of the lemma above uses a standard reduction technique and is straightforward. We assume that an impersonator mounting a passive attack can break the identification scheme, and build a forger who runs it as a subroutine. Transcript queries are answered by the forger using its signature oracle, and a successful impersonation attempt translates easily into a successful forgery. The proof details can be found in the full version of the paper [1].

4 Separations among Security Assumptions

In this section, we justify the claimed separations among the security conditions in Figure 1. Specifically, we give an example of an ID scheme that is secure against impersonation under passive attack but is not honest-verifier zero-knowledge, and also an example of an ID scheme that is secure against impersonation under passive attack and is not a proof of knowledge. (In this section, proof of knowledge means proof of knowledge of the secret key. More precisely, it refers to some underlying witness-relation $R(pk, sk)$ depending on the protocol.) Since the **PS** and **OO** assumptions include either an assumption of honest verifier zero-knowledge or an assumption of proof of knowledge, this implies that there exists an identification scheme secure against impersonation under passive attack that is not **PS** secure, and there exists an identification scheme secure against impersonation under passive attack that is not **OO** secure, justifying two of the claimed separations in Figure 1, and showing that our assumption on the ID scheme is strictly weaker than previous ones used to prove security of the signature scheme.

Furthermore, this also justifies two more separations claimed in Figure 1, namely that the signature scheme could be secure even if the ID scheme is not **PS** secure or **OO** secure. This follows simply by logic, because if we assume that security of the signature scheme implies, say, **PS**-security of the ID scheme, the existing arrows say that security against impersonation under passive attack implies **PS**-security, which we know from the above to not be true. The analogous argument applies in the case of **OO**.

We now proceed to the examples. Shoup notes that the 2^m-th root identification (a special case of the identification scheme of Ong and Schnorr [20]) is provably not a proof of knowledge if factoring is hard [25]. However, he shows that this scheme is secure against impersonation under active (and hence certainly under passive) attacks if factoring is hard. This yields the following:

Proposition 1. *If factoring is hard, then there exists a non-trivial canonical identification scheme that is secure against impersonation under passive attacks but is not a proof of knowledge.* ∎

Similarly, we show that there exists an identification scheme that is secure against impersonation under passive attacks yet is not honest verifier zero-knowledge. We take the following approach in constructing such an identification scheme. We begin with a canonical identification secure against impersonation under passive attacks and modify it so that it remains secure against impersonation under passive attacks but is not zero-knowledge. A detailed construction is presented in the full version of the paper [1]. The example we construct, though contrived, makes the point that zero-knowledge is not strictly necessary in a secure identification scheme. The following proposition states this more precisely.

Proposition 2. *If factoring is hard, then there exists a non-trivial canonical identification scheme that is secure against impersonation under passive attacks but is not honest-verifier zero-knowledge.* ∎

5 Extension to forward security

We prove an extension of Theorem 2 to the case where the security requirement is forward security.

CANONICAL FORWARD-SECURE IDENTIFICATION SCHEMES. We consider key-evolving identification schemes. The operation of the scheme is divided into time periods, where a different secret is used in each time period. The public key remains the same in every time period. A canonical key-evolving identification scheme is a three-move protocol in which the verifier's only move is to pick and send a random challenge to the prover. Unlike canonical identification schemes with fixed keys, the verifier's final decision, though still deterministic, is not only a function of the conversation with the prover and the public key, but also a function of the the index of the current time period. We say that a canonical key-evolving identification scheme is *forward-secure* if it is infeasible for a passive adversary, even with access to the current secret key, to impersonate the prover with respect to an honest verifier in any of the prior time periods.

As pointed out by Bellare and Miner [4], forward-secure identification schemes are artificial constructs since, due to the online nature of identification protocols, the kind of attack we withstand in this case cannot exist in reality. Nevertheless, the schemes are still very useful in the design of efficient forward-secure signature schemes. Please refer to the full version of the paper [1] for a formal definition of a key-evolving identification scheme and what it means for it to be forward-secure.

FORWARD-SECURE SIGNATURE SCHEMES. A forward-secure signature scheme is in essence a key-evolving signature scheme in which the secret key is updated periodically. As in standard signature schemes, the public key remains the same throughout the lifetime of the scheme. In each time period, a different secret key is used to sign messages. The verification algorithm checks not only the validity of a signature, but also the particular time period in which it was generated. At the end of each time period, an update algorithm is run to compute the new secret key from the current one, which is then erased. Informally, we say that a key-evolving signature scheme is *forward-secure* under chosen-message attack if it is infeasible for an adversary, even with access to the secret key for the current period and to previously signed messages of its choice, cannot forge signatures for a past time period. For a formal definition of a key-evolving signature scheme and what it means for it to be forward-secure, see the full version of the paper [1].

THE EQUIVALENCE. Our transformation of key-evolving ID schemes into key-evolving signature schemes follows the same paradigm of Construction 1, in which the challenge becomes the output of a hash function H. The main difference with respect to that construction is that the secret key is no longer fixed but varies according to the time period. As a result, the current time index j is also given as input to the signing algorithm and attached to the signature to allow for correct verification. The current time index j is also added to the input of the hash function, which now becomes $j \| R \| \textsc{Cmt} \| M$. The update algorithm of the key-evolving signature scheme is exactly the same as that of the identification scheme on which it is based. The following theorem, where min-entropy is defined in a manner similar to that for canonical identification schemes, states precisely the equivalence with regard to forward security of the key-evolving ID scheme and the associated key-evolving signature scheme.

Theorem 3 (Forward security equivalence theorem). *Let $\mathcal{FID} = (K, P, Vid, c, T)$ be a canonical key-evolving identification scheme, let $s(\cdot)$ be a seed length, and let $\mathcal{FSDS} = (K, S, VSig, c, T)$ be the associated key-evolving signature scheme as per the new construction described above. Let $\beta(\cdot)$ be the min-entropy function associated to $\mathcal{FID}$ and assume $s(\cdot) + \beta(\cdot) = \omega(\log(\cdot))$. Then $\mathcal{FSDS}$ is polynomially-forward-secure against chosen-message attack in the random oracle model if and only if $\mathcal{FID}$ is polynomially-forward-secure against impersonation under passive attacks.* ▮

The full paper [1] states and proves a pair of lemmas, one for each direction of the "if and only if". These indicate the concrete security of the underlying reductions. The theorem follows.

As in the case of standard signature and ID schemes, if we consider key-evolving ID schemes in which the commitment is chosen from a large space (i.e., $\beta(\cdot) = \omega(\log(\cdot))$), then the key-evolving signature scheme resulting from the Fiat-Shamir transform (i.e., $s(k) = 0$) is forward-secure against chosen-message attack in the random oracle model *if and only if* the underlying identification scheme is forward-secure against impersonation under passive attacks.

6 The Non-Triviality Condition

We show that applying the FS transform to a trivial identification scheme can result in an insecure signature scheme, which supports our claim in the Introduction that non-triviality of the ID scheme is necessary for security of the signature scheme obtained via the FS transform. This is implied by the following, whose proof is presented in the full version of the paper [1].

Proposition 3. *If factoring Williams integers is hard, then there exists a trivial, canonical identification scheme that is secure against impersonation under passive attacks, but the signature scheme resulting from applying the standard Fiat-Shamir transform is insecure.* ▮

This example also shows why the generalized FS transform that we have introduced is useful. Since the ID scheme is secure against impersonation under passive attacks, the generalized transform does yield a secure signature scheme, even though the triviality of the ID scheme prevented the FS transform from doing so.

Acknowledgments

Work done while the first two authors were at the University of California at San Diego. Third author supported in part by NSF Grant CCR-0098123, a 1996

Packard Foundation Fellowship in Science and Engineering, and an IBM Faculty Partnership Development Award. First and last authors supported in part by third author's grants.

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. Full version of this paper, available via `http://www-cse.ucsd.edu/users/mihir`.
2. M. Abdalla and L. Reyzin. A new forward-secure digital signature scheme. In T. Okamoto, editor, *Advances in Cryptology – ASIACRYPT 2000*, volume 1976 of *Lecture Notes in Computer Science*, pages 116–129, Berlin, Germany, Dec. 2000. Springer-Verlag.
3. M. Bellare and O. Goldreich. On defining proofs of knowledge. In E. Brickell, editor, *Advances in Cryptology – CRYPTO ' 92*, volume 740 of *Lecture Notes in Computer Science*, pages 390–420, Berlin, Germany, Aug. 1992. Springer-Verlag.
4. M. Bellare and S. Miner. A forward-secure digital signature scheme. In M. Wiener, editor, *Advances in Cryptology – CRYPTO ' 99*, volume 1666 of *Lecture Notes in Computer Science*, pages 431–448, Berlin, Germany, Aug. 1999. Springer-Verlag.
5. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In V. Ashby, editor, *1st ACM Conference on Computer and Communications Security*. ACM Press, Nov. 1993.
6. T. Beth. Efficient zero-knowledge identification scheme for smart cards. In C. Guenther, editor, *Advances in Cryptology – EUROCRYPT ' 1988*, volume 330 of *Lecture Notes in Computer Science*, pages 77–86, Berlin, Germany, May 1988. Springer-Verlag.
7. E. Brickell and K. McCurley. An interactive identification scheme based on discrete logarithms and factoring. In I. Damgård, editor, *Advances in Cryptology – EUROCRYPT ' 90*, volume 473 of *Lecture Notes in Computer Science*, pages 63–71, Berlin, Germany, May 1991. Springer-Verlag.
8. B. Chor and O. Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. In *26th Annual Symposium on Foundations of Computer Science*, pages 429–442, Los Angeles, CA, USA, Oct. 1985. IEEE Computer Society Press.
9. R. Cramer and I. Damgård. Secure signature schemes based on interactive protocols. In D. Coppersmith, editor, *Advances in Cryptology — CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*, pages 297–310, Berlin, Germany, 1995. Springer-Verlag.
10. U. Feige, A. Fiat, and A. Shamir. Zero knowledge proofs of identity. *Journal of Cryptology*, 1(2):77–94, 1988.
11. A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A. Odlyzko, editor, *Advances in Cryptology – CRYPTO ' 86*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194, Berlin, Germany, Aug. 1986. Springer-Verlag.
12. M. Girault. An identity-based identification scheme based on discrete logarithms modulo a composite number. In I. Damgård, editor, *Advances in Cryptology – EUROCRYPT ' 90*, volume 473 of *Lecture Notes in Computer Science*, pages 481–486, Berlin, Germany, May 1991. Springer-Verlag.

13. S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal of Computing*, 17(2):281–308, Apr. 1988.
14. L. Guillou and J. J. Quisquater. A "paradoxical" identity-based signature scheme resulting from zero-knowledge. In S. Goldwasser, editor, *Advances in Cryptology — CRYPTO ' 88*, volume 403 of *Lecture Notes in Computer Science*, pages 216–231, Berlin, Germany, 21–25 Aug. 1988. Springer-Verlag.
15. G. Itkis and L. Reyzin. Forward-secure signatures with optimal signing and verifying. In J. Kilian, editor, *Advances in Cryptology – CRYPTO ' 01*, volume 2139 of *Lecture Notes in Computer Science*, pages 332–354, Berlin, Germany, Aug. 2001. Springer-Verlag.
16. S. Micali and L. Reyzin. Improving the exact security of digital signature schemes. *Journal of Cryptology*, 15(1):1–18, 2002.
17. S. Micali and A. Shamir. An improvement of the Fiat-Shamir identification and signature scheme. In S. Goldwasser, editor, *Advances in Cryptology — CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 244–248, Berlin, Germany, Aug. 1990. Springer-Verlag.
18. K. Ohta and T. Okamoto. On concrete security treatment of signatures derived from identification. In H. Krawczyk, editor, *Advances in Cryptology — CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 354–370, Berlin, Germany, Aug. 1998. Springer-Verlag.
19. T. Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In E. Brickell, editor, *Advances in Cryptology — CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 31–53, Berlin, Germany, Aug. 1993. Springer-Verlag.
20. H. Ong and C. Schnorr. Fast signature generation with a Fiat Shamir–like scheme. In I. Damgård, editor, *Advances in Cryptology – EUROCRYPT ' 90*, volume 473 of *Lecture Notes in Computer Science*, pages 432–440, Berlin, Germany, May 1990. Springer-Verlag.
21. D. Pointcheval. A new identification scheme based on the perceptrons problem. In J. Quisquater and L. Guillou, editors, *Advances in Cryptology – EUROCRYPT ' 95*, volume 921 of *Lecture Notes in Computer Science*, pages 319–328, Berlin, Germany, May 1995. Springer-Verlag.
22. D. Pointcheval and J. Stern. Security proofs for signature schemes. In U. Maurer, editor, *Advances in Cryptology – EUROCRYPT ' 96*, volume 1070 of *Lecture Notes in Computer Science*, pages 387–398, Berlin, Germany, May 1996. Springer-Verlag.
23. D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, 2000.
24. C. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3):161–174, 1991.
25. V. Shoup. On the security of a practical identification scheme. In U. Maurer, editor, *Advances in Cryptology – EUROCRYPT ' 96*, volume 1070 of *Lecture Notes in Computer Science*, pages 344–353, Berlin, Germany, May 1996. Springer-Verlag.
26. J. Stern. A new identification scheme based on syndrome decoding. In D. Stinson, editor, *Advances in Cryptology — CRYPTO '93*, volume 773 of *Lecture Notes in Computer Science*, pages 13–21, Berlin, Germany, 1994. Springer-Verlag.