Signatures without RO

Anonymous Submission

No Institute Given

1 Preliminaries

Definition 1 (3-round Tag-based Identification Scheme). *A 3-round identification (ID) scheme is defined as* $\mathsf{ID} := (\mathsf{IGen}, \mathsf{P} = (\mathsf{P}_1, \mathsf{P}_2), \mathsf{ChSet}, \mathsf{V})$.

- *The probabilistic generation algorithm* IGen *takes the public parameter* 1^k *as input and returns a public key and secret key* (pk, sk)*. We assume that* pk *defines the challenge set* ChSet.
- *The prover algorithm* $\mathsf{P} = (\mathsf{P}_1, \mathsf{P}_2)$ *is split into two algorithms.* P_1 *takes the secret key* sk *and a tag* τ *from the tag space* M *as the input and returns the commitment* Com *and a state* St. P_2 *takes the secret key* sk*, the state* St *and a challenge* C *as an input and returns a response* s.
- *The deterministic verifier algorithm* V *takes the public key* pk*, the tag* τ*, the commitment* Com*, the challenge* C *and the response* s *as an input and outputs a decision, 1 (acceptance) or 0 (rejection).*

For correctness we require that for all $k \in \mathbb{N}$, $(pk, sk) \in \mathsf{IGen}(1^k)$, *all* $(Com, St) \in \mathsf{P}_1(sk, \tau)$, *all* $C \in \mathsf{ChSet}$ *and all* $s \in \mathsf{P}_2(sk, St, C)$, *we have*

$$\mathsf{V}(pk, Com, C, s) = 1.$$

Prover		**Verifier**
$(Com, St) \xleftarrow{\$} \mathsf{P}_1(sk, \tau)$	$\xrightarrow{\tau, Com}$	
	$\xleftarrow{C}$	$C \xleftarrow{\$} \mathsf{ChSet}$
$s \xleftarrow{\$} \mathsf{P}_2(sk, St, C)$	$\xrightarrow{s}$	
		$d := \mathsf{V}(pk, Com, C, s)$

Figure 1. 3-round Tag-based Identification Scheme

Definition 2 (Alternative Verification). *We say the deterministic function* $\tilde{\mathsf{V}}$ *is an alternative verification for an identification scheme* ID*, if* $\tilde{\mathsf{V}}$ *takes the*

secret key sk, the tag τ, the commitment Com, the challenge C and the response s as an input and outputs a decision, 1 (acceptance) or 0 (rejection).
For correctness we require that for all $k \in \mathbb{N}$, $(pk, sk) \in \mathsf{IGen}(1^k)$, all $(Com, St) \in \mathsf{P}_1(sk, \tau)$, all $C \in \mathsf{ChSet}$ and all $s \in \mathsf{P}_2(sk, St, C)$, we have

$$\tilde{\mathsf{V}}(sk, \tau, Com, C, s) = 1.$$

Definition 3 (Alternative Impersonation). *A 3-round tag based identification scheme is said to be $(t, q, \epsilon) - \mathsf{IMP}^{\tilde{\mathsf{V}}}$ secure, if for all adversary $\mathcal{A}$ running in time at most t we have*

$$\Pr[q\text{-}\mathsf{IMP\text{-}ALT}^{\tilde{\mathsf{V}}}_{\mathsf{ID}}(\mathcal{A})] = 1] \leq \epsilon.$$

<u>**Game** $q\text{-}\mathsf{IMP\text{-}ALT}^{\tilde{\mathsf{V}}}_{\mathsf{ID}}(\mathcal{A})$</u>

$(sk, pk) \xleftarrow{\$} \mathsf{IGen}$
$\mathcal{Q} \leftarrow \emptyset$
for $i \in [q]$
  $\tau_i \xleftarrow{\$} \mathsf{M}$
  $(Com_i, St_i) \xleftarrow{\$} \mathsf{P}_1(sk, \tau_i)$
  $C_i \xleftarrow{\$} \mathsf{ChSet}$
  $s_i \xleftarrow{\$} \mathsf{P}_2(sk, St_i, C_i)$
  $\mathcal{Q} \leftarrow \mathcal{Q} \cup (\tau_i, Com_i, C_i, s_i)$
$(\tau^*, Com^*, C^*, s^*) \leftarrow \mathcal{A}(pk, \mathcal{Q})$
if $\tilde{\mathsf{V}}(sk, \tau^*, Com^*, C^*, s^*) = 1$ **then return** 1
else return 0

Figure 2.

Definition 4 (Uniqueness). *We say the identification scheme $\mathsf{ID} := (\mathsf{IGen}, \mathsf{P}, \mathsf{ChSet}, \mathsf{V})$ is unique if for every $(sk, pk) \xleftarrow{\$} \mathsf{IGen}$ and every $(Com, St) \xleftarrow{\$} \mathsf{P}_1(sk, \tau)$,*

$$\left|\{C \in \mathsf{ChSet} \mid \exists\, s : \mathsf{V}(pk, Com, C, s) = 1 \wedge \tilde{\mathsf{V}}(sk, Com, \mathcal{C}, s) \neq 1\}\right| = 1.$$

This means there exist a (not necessarily polynomial time) function we call the uniqueness function such as f that

$$f(pk, Com) = C.$$

Definition 5 (Signature scheme). *To construct a signature* $\mathsf{Sig} := (\mathsf{Gen}, \mathsf{Sgn}, \mathsf{Ver})$*from a 3-round tag-based identification scheme* $\mathsf{ID} := (\mathsf{IGen}, \mathsf{P} = (\mathsf{P}_1, \mathsf{P}_2), \mathsf{ChSet}, \mathsf{V})$ *we proceed as in Figure 4.*

$\underline{\mathsf{Gen}(\mathsf{par}):}$

$(pk_0, sk_0) \xleftarrow{\$} \mathsf{IGen}$
$(pk_1, sk_1) \xleftarrow{\$} \mathsf{IGen}$
$pk \coloneqq (pk_0, pk_1)$
$sk \coloneqq (sk_0, sk_1)$
$\textbf{return } (sk, pk)$

$\underline{\mathsf{Ver}(pk, \sigma, m):}$

$\textbf{if } C_0 + C_1 \neq \mathsf{H}(pk, Com_0, Com_1)$
$\quad \textbf{then return } 0$
$\textbf{if } \mathsf{V}(pk_0, Com_0, C_0, s_0) = 0$
$\quad \textbf{then return } 0$
$\textbf{if } \mathsf{V}(pk_1, Com_1, C_1, s_1) = 0$
$\quad \textbf{then return } 0$
$\textbf{else return } 1$

$\underline{\mathsf{Sgn}(sk, m):}$

$(sk_0, sk_1) \leftarrow sk$
$(Com_0, St_0) \xleftarrow{\$} \mathsf{P}_1(sk_0, m)$
$(Com_1, St_1) \xleftarrow{\$} \mathsf{P}_1(sk_1, m)$
$k = \mathsf{H}(pk, Com_0, Com_1)$
$e \xleftarrow{\$} \mathsf{ChSet}$
$C_0 = d + e$
$C_1 = -e$
$s_0 \xleftarrow{\$} \mathsf{P}_2(sk_0, St_0, C_0)$
$s_1 \xleftarrow{\$} \mathsf{P}_2(sk_1, St_1, C_1)$
$\sigma \coloneqq (Com_0, C_0, s_0, Com_1, C_1, s_1)$
$\textbf{return } \sigma$

Figure 3. Instantiation 1

Definition 6 (RMA security). *We define the existential forgery against the random message attack (EUF-RMA) security experiment, played between a challenger and a forger $\mathcal{F}$.*

1. *The challenger runs* Gen *to generate key pair (pk, sk). The forger receives pk as input.*
2. *The challenger now chooses q random messages and signs them and returns (m_i, σ_i) to the forger where σ_i is m_i signed under sk.*
3. *The forger outputs a message m^* and signature σ^*.*

$\mathcal{F}$ wins the game if $\mathsf{Ver}(pk, \sigma, m) = 1$, that is, σ^* is a valid signature for m^*, and $m^* \neq m_i$ for all i. We say $\mathcal{F}$, (t, q, ϵ)-breaks the EUF-RMA security of the signature, if $\mathcal{F}$ runs in time t, receives at most q signed messages, and has the success probability of ϵ.

Definition 7 (Correlation Interactibilty). *We say an adversary $\mathcal{A}$, $(t, \epsilon)-$breaks the correlation intractability of a hash function $\mathsf{H} : \{0,1\}^{n(\lambda)} \rightarrow \{0,1\}^{m(\lambda)}$ with regards to function g if $\mathcal{A}$ runs in time t and*

$$\Pr[x \xleftarrow{\$} \mathcal{A}, \mathsf{H}(x) = g(x)] \geq \epsilon(\lambda).$$

We call the hash function $(t, \epsilon)-$correlation intractable if such an adversary does not exist.

1.1 proof

Theorem 1. *Let* ID *be a unique identification scheme and* H *be a (t'', ϵ'') correlation intractable hash function. Suppose there exists a (t, q, ϵ)-forger $\mathcal{F}$*

breaking the security of $\mathsf{Sig}_{\mathsf{ID},\mathsf{H}}$ *against the existential forgery under the random message attack. Then there exists an adversary that* (t', q, ϵ')*-breaks the* $\mathsf{IMP}^{\tilde{\mathsf{V}}}$ *security of* ID *with* $t' \approx t$ *and*

$$\epsilon' \geq \frac{3}{4}\epsilon.$$

This results follows from Lemma 1 and 2 and a hybrid argument.

Definition 8 (Partially valid signature). *signature* $\sigma = (Com_0, C_0, s_0, Com_1, C_1, s_1)$ *is partially valid if* $\tilde{\mathsf{V}}(pk_0, Com_0, C_0, s_0) = 1$ *or* $\tilde{\mathsf{V}}(pk_1, Com_1, C_1, s_1) = 1$ *not partially valid if* $\tilde{\mathsf{V}}(pk_0, Com_0, C_0, s_0) = 0$ *and* $\tilde{\mathsf{V}}(pk_1, Com_1, C_1, s_1) = 0$.

Let (m_i, σ_i) denote the i-th random message and it's signature. Let (m^*, σ^*) be the forgery output by $\mathcal{F}$.
We distinguish between Type I forger returning (m^*, σ^*) where (m^*, σ^*) is patially valid and Type II forger returning (m^*, σ^*) where (m^*, σ^*) is not partially valid.

Type I forger

Lemma 1. *Let* $\mathcal{F}$ *be a type I forger that* (t, q, ϵ)*-breaks the RMA security of the signature. Then there exists adversary* $\mathcal{A}$ *that* (t', q, ϵ')*-breaks the* $\mathsf{IMP}^{\tilde{\mathsf{V}}}$ *security of the ID scheme with* $t \approx t'$ *and*

$$\epsilon' \geq \frac{1}{2}\epsilon.$$

Game 0.

We define Game 0 as the existential unforgeability experiment with forger $\mathcal{F}$. By definition, we have

$$\Pr[X_0] = \epsilon.$$

Game 1.

We modify this game such that the game chooses a random bit b at the beginning. When $\mathcal{F}$ outputs a forgery (m^*, σ^*) the game parses the signature as

$$(Com_0^*, C_0^*, s_0^*, Com_1^*, C_1^*, s_1^*)$$

and aborts if $\tilde{\mathsf{V}}(pk_b, Com_b^*, C_b^*, s_b^*) = 1$. We denote this even with abort.
Since the forger is of type I and outputs a partially valid signature, we have $\Pr[\mathsf{abort}] \leq \frac{1}{2}$, which implies

$$\Pr[X_1] = \Pr[X_0 \wedge \neg\mathsf{abort}] \geq \frac{1}{2}\Pr[X_0].$$

Game 2.

In this Game we change the way signatures are calculate. The game first signs every signature as before then changes every signature $\sigma_i = (Com_{0,i}, C_{0,i}, s_{0,i}, Com_{1,i}, C_{1,i}, s_{1,i})$ for message m_i as follows.

$$(Com_{1-b,i}, St_{1-b,i}) \xleftarrow{\$} \mathsf{P}_1(sk_{1-b}, m_i)$$

$$k_i = \mathsf{H}(pk, Com_{0,i}, Com_{1,i})$$

$$C_{1-b,i} = k_i - C_{b,i}$$

$$s_{1-b,i} \xleftarrow{\$} \mathsf{P}_2(sk_{1-b}, St_{1-b,i}, C_{1-b,i})$$

Finally the game returns the newly calculated signature σ_i to $\mathcal{F}$.
Game 2 is perfectly indistinguishable from game 1 from the adversary's point of view. Thus we have

$$\Pr[X_2] = \Pr[X_1].$$

The Alternative Impersonation Adversary.

Now adversary $\mathcal{A}$ simulates game 2. The $\mathcal{A}$ receives pk_b and $(\tau_i, Com_{b,i}, S_{i,b})$ from the alternative impersonation game and proceeds to calculate the public key and signatures on message $m_i := \tau_i$ as in game 2.
It remains to show how $\mathcal{A}$ can break the alternative impersonation from the forged signature $\sigma^* = (Com_0^*, C_0^*, s_0^*, Com_1^*, C_1^*, s_1^*)$ on message m^* output by $\mathcal{F}$. We know that $\tilde{\mathsf{V}}(sk_b, m^*, Com_b^*, C_b^*, s_b^*) = 1$ (by game 1). So $\mathcal{A}$ can win the alternative impersonation game by outputing $(m^*, Com_b^*, C_b^*, s_b^*)$.

Type II forger

Lemma 2. *Let $\mathcal{F}$ be a type II forger that (t, q, ϵ)-breaks the RMA security of the signature. Then there exists adversary $\mathcal{A}$ that (t', ϵ')-breaks the correlation intractability of the hash function H with $t \approx t'$ and*

$$\epsilon' \geq \epsilon.$$

The correlation intractability adversary $\mathcal{A}$ simulates the unforgeability experiment by running IGen twice and obtaining two pairs of keys we name (sk_0, pk_0) and (sk_1, pk_1). The adversary now return $pk := (pk_0, pk_1)$ to $\mathcal{F}$ as the public key and also chooses random messages $m_1, ..., m_q$ and signs them with the secret key $sk := (sk_0, sk_1)$ to obtain the signatures $\sigma_1, ..., \sigma_q$ and returns the (m_i, σ_i) pairs to $\mathcal{F}$. This game is indistinguishable from the unforgeability game in the view of $\mathcal{F}$.

Breaking the hash intractability.

Eventually, $\mathcal{F}$ returns a message and signature pair (m^*, σ^*), from which $\mathcal{A}$ extracts the solution that breaks the hash intractability as follows. First $\mathcal{A}$ parses σ^* as $(Com_0^*, C_0^*, s_0^*, Com_1^*, C_1^*, s_1^*)$. We assume the signature is valid and because forger type II outputs signatures that are not partially valid, due to the uniqueness of the identification scheme we can write

$$C_0^* = f(pk_0, Com_0^*)$$

$$C_1^* = f(pk_1, Com_1^*).$$

If the forged signature is valid then

$$\mathsf{H}(pk, Com_0^*, Com_1^*) = C_0^* + C_1^* = f(pk_0, Com_0^*) + f(pk_1, Com_1^*) = g(pk, Com_0^*, Com_1^*).$$

So $\mathcal{A}$ can (t, ϵ') break the g-correlation intractability of H where g is defined as

$$g(pk = (pk_0, pk_1), Com_0, Com_1) = f(pk_0, Com_0) + f(pk_1, Com_1).$$

Adversary $\mathcal{A}$ succeeds at giving a solution that breaks the correlation intractability of H whenever $\mathcal{F}$ succeeds at forging a valid signature so

$$\epsilon' \geq \epsilon.$$

1.2 Instantiation from the q-SDH

In the following let $\mathsf{par} \coloneqq (p, q, \mathsf{G})$ be a set of system parameters, where $\mathsf{G} =< g >$ is a cyclic group of prime order p.

Definition 9 (q-SDH). ***[TODO:]***

We describe the identification scheme $\mathsf{ID} \coloneqq (\mathsf{IGen}, \mathsf{P} = (\mathsf{P}_1, \mathsf{P}_2), \mathsf{ChSet}, \mathsf{V})$ as the following

$\mathsf{IGen}(1^k)$: Let g be a random generator of G. The private key is $x \xleftarrow{\$} \mathbb{Z}_q$ and the public key is $y = g^x$.
$\mathsf{P} = (\mathsf{P}_1, \mathsf{P}_2)$
V

$\underline{\mathsf{IGen}(\mathsf{par})\text{:}}$

$sk \coloneqq x \xleftarrow{\$} \mathbb{Z}_p$
$pk \coloneqq y = g^x$
$\mathsf{ChSet} \coloneqq \mathbb{Z}_p$
return (sk, pk)

$\underline{\mathsf{V}(pk, Com, C, s)\text{:}}$

parse $R \coloneqq (h, u, \hat{u})$
if $u = g^s \cdot (y \cdot g^m)^{-c} \wedge \hat{u} = h^s \cdot g^{-c}$
    then return 1
else return 0

$\underline{\tilde{\mathsf{V}}(sk, m, Com, \text{[???:]})\text{:}}$

parse $R \coloneqq (h, u, \hat{u}), sk = x$
if $h = g^{\frac{1}{x+m}}$
    then return 1
else return 0

$\underline{\mathsf{P}_1(sk, m) :}$

$St \coloneqq r \xleftarrow{\$} \mathbb{Z}_p$
$h \coloneqq g^{\frac{1}{x+m}}$
$u \coloneqq g^r$
$\hat{u} \coloneqq h^r$
$R = (h, u, \hat{u})$
return (Com, St)

$\underline{\mathsf{P}_2(sk, St, C) :}$

parse $St = r$
return $s = c \cdot (x + m) + r \mod p$

Figure 4. Instantiation 1