More Short Signatures without Random Oracles

Victor K. Wei and Tsz Hon Yuen

Dept. of Information Engineering, The Chinese Univ. of Hong Kong, Hong Kong
{kwwei,thyuen4}@ie.cuhk.edu.hk

December 31, 2005

Abstract. We construct three new signatures and prove their securities without random oracles. They are motivated, respectively, by Boneh and Boyen [9]'s, Zhang, et al. [45]'s, and Camenisch and Lysyanskaya [14]'s signatures without random oracles. The first two of our signatures are as short as [9, 45]'s state-of-the-art short signatures. Our third signature is reducible to a modified LRSW Assumption [31] but without the LRSW Assumption's hypothesized external signing oracle. New and interesting variants of the q-SDH Assumption, the q-SR (Square Root) Assumption are also presented. New and independently interesting proof techniques extending the two-mode technique of [9] are used, including a combined three-mode simulation and rewinding in the standard model.

1 Introduction

The random oracle has been a popular technique in provable security before and after its formal introduction by Bellare and Rogaway [5]. The results of [20, 21, 36] used rewindings of hashings with observable hashing input-output pairs. The Schnorr signature and many other signatures and Poofs-of-Knowledge (PoK's) results [6, 7] used the Fiat-Shamir paradigm in their reductionist security proofs [33, 23, 32]. The random oracle rewinding technique [38, 37] is a particularly powerful proof technique.

Recently, the results of Barak, et al. [2, 3] and Goldwasser and Kalai [27] proved the insecurity of the random oracle model as it is commonly used in the Fiat-Shamir paradigm. The core contradiction is in the *predictability* of the random oracle, how much can the hash outputs be predicted based on prior computation transcripts. On one hand, proofs in the random oracle model for the Fiat-Shamir paradigm depends on this predictability to simulate the signing oracle. On the other hand, too much predictability enables the attackers to forge. [2, 27] were able to formalize the notion of *predictability* and prove that zero-knowledge cannot exist in the Fiat-Shamir paradigm for a very wide range of real-world hashing families. [3] proceeded to define an essentially necessary and sufficient condition for the existence of real-world hashing families that will enable zero-knowledge proofs in the Fiat-Shamir paradigm. However, [3] expressed pessimism of the construction of such qualified hashing families.

The research on signatures whose reductionist security proofs do no use random oracles has had a long history, and it received renewed vigor since the insecurity proof of the random oracles [2, 27, 3]. The signatures without random oracles in [25, 26, 35, 19, 16, 17, 22, 30, 12] contained various inefficiencies. See [12]'s Table 1 for a good summary.

Cramer and Shoup [18] presented three signatures which achieved good efficiency in $O(\lambda_s)$-bit signature length, $O(\lambda_s)$-bit public key length, servicing any number of Signing Oracle queries, and supporting the generation of any number of signatures in the Real World. Its existential unforgeability against adaptive-chosen-plaintext attackers (ACP-UF) is reducible to the Strong RSA Assumption. The signature consists of three elements from Z_N, where the

RSA modulus N is 1024 (resp. 2048) bits for security level $\lambda_s = 128$ (resp. 256) bits, resulting in 3072-bit (resp. 6144-bit) signatures.

Boneh and Boyen [9] presented short signatures whose ACP-UF is reducible to the q-SDH (Strong Diffie-Hellman) Assumption without random oracles. The signature length is roughly $4\lambda_s$ bits.

Zhang, Chen, Susilo, and Mu [45] presented short signatures whose ACP-UF is reducible to the q-SR (Square Root) Assumption without random oracles. The signature length is also roughly $4\lambda_s$ bits.

Camenisch and Lysyanskaya [14] presented three short signatures without random oracles and reduced their ACP-UF to the LRSW Assumption [31]. Their signature lengths are higher, around $6\lambda_s$ bits or more.

The proofs of [9, 45] are in the standard model, except the attacker must pre-announce the maximum number of Signing Oracle queries it will make. The proof of [14] is in the standard model, except that it assumes the availability of an external (hypothesized) Signing Oracle to the Simulator. This requirement makes the model weak. However, the security of the LRSW Asumption remains plausible against even assuming the attacker has several attack oracles, such as the chosen-target discrete logarithm collision oracle [4], the ROS oracle [39], and the generalized birthday oracle[40].

Rougly speaking, the *Chosen-Target Discrete Logarithm Collision Oracle* outputs nonzero $(a_1, \cdots, a_q)$ satisfying $\prod_i g_i^{a_i} = 1$ given random $g_1, \cdots, g_q$. A related oracle, the *Chosen-Target Discrete Logarithm Oracle* [4] outputs nonzero $(a_{i_1}, \cdots, a_{i'_q})$, $q' \leq q$, such that $\log_g g_{i_j} = a_{i_j}$ for all j, given random g, g_1, $\cdots$, g_q. The *ROS (Randomized Oversampled System) Oracle* [39] outputs nonzero $(a_1, \cdots, a_q)$ such that $\prod_i g_i^{a_i} = 1$ and $\sum_i a_i b_i = 0$, given random (g_1, b_1), $\cdots$, (g_q, b_q). The *Generalized Birthday Oracle* is solves the Generalized Birthyday Problem described in [40].

The signatures of [9, 45] also remain plausible against an attacker in possession of a Chosen-Target Discrete Logarithm Collision Oracle. The signature of Boneh, Lynn, and Shacham [11] can be proven ACP-UF given the hypothesis that the Simulator has an external Signing Oracle similar to [14]. But it is broken if the attacker has a Chosen-Target Discrete Logarithm Collision Oracle.

Our **Contributions** are

1. We construct three new signatures without random oracles, i.e. the correctness and the existential unforgeability against adaptive-chosen-plaintext attackers (ACP-UF) of each is reducible to intractability assumptions without random oracles. The proof for each signature is in the standard model except the attacker pre-announces the maximum number of Signing Oracle queries it will make, just like Boneh and Boyen [9] and Zhang, Chen, Susilo, abd Mu [45] but not like the LRSW Assumption [31].
2. Our three signatures are respectively motivated by the short signatures without random oracles in Boneh and Boyen [9], in Zhang, Chen, Susilo, and Mu [45], and in Camenisch and Lysyanskaya [14]. The security of our three signatures are respectively reducible to the q-SDH' Assumption which is a slight alteration of the q-SDH Assumption [34, 44, 9], the (q, ℓ)-SR (Square Root) Assumption which is modified from [45]'s q-SR Assumption, and the q-wholesale LRSW Assumption which is modified from the LRSW Assumption [31]. These new assumptions are interesting in their own rights.
3. The first two of our new signatures without random oracles are roughly $4\lambda_s$ bits long, as short as the state-of-the-art from [9, 45].

4. Our third new signature is a modification of [14]'s Signature B. We improve the signature such that its security is proved without the external Signing Oracle used in the LRSW Assumption. Our signature is provably secure in the standard model except that the attacker must pre-announce the maximum number of Signing Oracle queries just like [9, 45] but not like [14, 31].
5. During our proofs, we introduce new proof techniques which extend Boneh and Boyen [9]'s two-mode proof technique. For example, we introduce a proof technique which combines three-mode, and rewind simulation in the standard model. These new proof techniques are powerful and are interesting in their own right.

2 Security Model

We review security models [9, 23] for signatures.

Syntax: A signature is a tuple $(\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vf})$ where

– Protocol KGen accepts input the security parameter 1^{λ_s}, outputs system parameters param, and sk-pk pair $(\mathsf{sk}, \mathsf{pk})$.
– Protocol Sign accepts inputs message m and secrete key sk, outputs a signature σ.
– Protocol Vf accepts inputs a message m, a signature σ, and a public key pk, outputs 1 or 0 for valid or $\mathsf{invalid}$.

Definition 1. *(*Correctness*) A signature is* correct *if, for arbitrary message m, we have*

$$\Pr[\mathit{Vf}(m, \mathit{Sign}(m, \mathit{sk}), \mathit{pk}) = 1] = 1$$

Oracles: maximum attacker cabilities. The *Signing Oracle* $\mathcal{SO}$ accepts input public key pk and a message m, outputs a valid signature.

Security notions: The existential unforgeability against adaptive-chosen-plaintext attackers is defined in terms of the following security game:

The **ACP-UF Game**
1. (*Setup Phase*) Simulator $\mathcal{S}$ sets up system parameters and public keys.
2. (*Probe Phase*) Attacker $\mathcal{A}$ queries the Signing Oracle $\mathcal{SO}$ in arbitrary interleaf.
3. (*End Game*) $\mathcal{A}$ delivers a valid message-signature pair (m^*, σ^*) which is not an $\mathcal{SO}$ query output.

The Attacker $\mathcal{A}$ is said to (q_S, T, ϵ)*-forge* if it makes q_S queries to $\mathcal{SO}$, has running time T, and has success probability ϵ where the probability is taken over random choices of system parameters, public keys, and the random bits it consumes.

Definition 2. *A signature scheme is* (q_S, T, ϵ)-ACP-UF (existentially-unforgeable against adaptive-chosen-plaintext attackers)*, if no algorithm $\mathcal{A}$ can (q_S, T, ϵ)-forge. It is* ACP-UF *provided it is (q_S, T, ϵ)-ACP-UF for some (with respect to the security parameter λ_s) polynomially growing q_S, T, and non-negligible ϵ .*

3 New short RO-free signatures from the q-SDH Assumption

We present the first of our three short signatures without random oracles. It is motivated by Boneh and Boyen [9]'s state-of-the-art short signature without random oracles. Below, we discuss intractability assumptions, then review [9]'s signature, before presenting our new signature.

3.1 Intractability assumptions

We present both existing and new intractability assumptions needed in this paper. There are two categories of intractability assumptions: those in the SDH (Strong Diffie-Hellman) family of assumptions, and those assumptions involving hash functions.

3.1.1 SDH-family of intractability assumptions. Let $\hat{\mathbf{e}} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_3$ be a pairing, order$(\mathbb{G}_1) = q_1$ is a prime, g_1 (resp. g_2) be a generator of $\mathbb{G}_1$ (resp. $\mathbb{G}_2$). The original SDH (Strong Diffie-Hellman) Assumption [10] is as follows:

Definition 3. *The q-SDH (Strong Diffie-Hellman) Problem [10] is that, given $g_1 \in \mathbb{G}_1$, $g_2^{x^i} \in \mathbb{G}_2$, $0 \leq i \leq q$, output $(c, g_1^{1/(x+c)})$. An algorithm $\mathcal{A}$ is said to (T, ϵ)-solves the q-SDH Problem if*

$$\Pr[\mathcal{A}(g_1, g_2, g_2^x, \cdots, g_2^{(x^q)}) = (c, g_1^{1/(x+c)})] \geq \epsilon$$

with running time T, where the probability is over the random choice of x and the random bits consumed by $\mathcal{A}$. The (q, T, ϵ)-SDH Assumption is that no algorithm can (q, T, ϵ)-solve the q-SDH Problem.

Wei [42] presented the following variant, the SDH' Assumption, which better suits our purposes in this paper.

Definition 4. *The q-SDH' (Strong Diffie-Hellman') Problem [42] is that, given g_2, $g_2^x \in \mathbb{G}_2$, $g_1^{x^i} \in \mathbb{G}_1$, $0 \leq i \leq q$, output $(c, g_1^{1/(x+c)})$. An algorithm $\mathcal{A}$ is said to (T, ϵ)-solves the q-SDH' Problem if*

$$\Pr[\mathcal{A}(g_2, g_2^x, g_1, g_1^x, \cdots, g_1^{(x^q)}) = (c, g_1^{1/(x+c)})] \geq \epsilon$$

with running time T, where the probability is over the random choice of x and the random bits consumed by $\mathcal{A}$. The (q, T, ϵ)-SDH' Assumption is that no algorithm can (q, T, ϵ)-solve the q-SDH' Problem.

The following relationship between the q-SDH Assumption and the q-SDH' Assumption is straightforward, and its proof is omitted.

Lemma 1 *Assume a homomorphic map $\psi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$ with $\psi(g_2) = g_1$ is given. Then the* (q, T, ϵ)-SDH Assumption *implies the* (T, q, ϵ)-SDH' Assumption.

3.1.2 Intractability assumptions about hash functions.

Definition 5. *Let $\mathcal{H}$ be a mapping. The $\mathcal{H}$-*Collision Problem *is to output (m, m') satisfying $m \neq m$ and $\mathcal{H}(m) = \mathcal{H}(m')$. An algorithm $\mathcal{A}$ is said to (T, ϵ)-*solve *the $\mathcal{H}$-Collision Problem if*

$$\Pr[\mathcal{A}(\mathcal{H}) = (m, m') \wedge m \neq m \wedge \mathcal{H}(m) = \mathcal{H}(m')] = \epsilon$$

*with running time T, and the probability is over random bits $\mathcal{A}$ consumes. $\mathcal{H}$ is called a (T, ϵ)-*Collision Resistant hash function *if no algorithm can* (T, ϵ)-solve the $\mathcal{H}$-Collision Problem.

Definition 6. *Let $\mathcal{H} : \{0,1\}^\ell \to \{0,1\}^\ell \setminus \{0^\ell\}$ be a mapping. The $(\mathcal{H}, q, \ell)$-*Sum Second Pre-Image *($(\mathcal{H}, q, \ell)$-*SSPI) Problem *is, given distinct nonzero $a_1, \cdots, a_q \in \{0,1\}^\ell \setminus \{0^\ell\}$, output b and (i,j), $1 \le i < j \le q$, satisfying $\mathcal{H}(b) = a_i \oplus a_j$. An algorithm $\mathcal{A}$ is said to (T, ϵ)-*solve *the $(\mathcal{H}, q, \ell)$-SSPI Problem if*

$$\Pr[\mathcal{A}(\mathcal{H}, q, a_1, \cdots, a_q) = (b, i, j) \wedge 1 \le i < j \le q \wedge \mathcal{H}(b) = a_i \oplus a_j \neq 0] = \epsilon$$

*with running time T, and the probability is over random choices of distinct nonzero $a_1, \cdots, a_q$ and random bits $\mathcal{A}$ consumes. A mapping $\mathcal{H}$ is called a (q, ℓ, T, ϵ)-*SSPIR *((q, ℓ, T, ϵ)-*Sum Second Pre-Image Resistant) hash function *if $\mathcal{H} : \{0,1\}^\ell \to \{0,1\} \setminus \{0^\ell\}$ and the $(\mathcal{H}, q, \ell, T, \epsilon)$-SSPI Assumption holds.*

3.2 Review: The SDH Signature from Boneh and Boyen [9]

We review Boneh and Boyen [9]'s short signature without random oracles. Let $\hat{\mathbf{e}} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_3$ be a pairing, order$(\mathbb{G}_1)$ = order$(\mathbb{G}_2) = q_1$, g_2 is a generator of $\mathbb{G}_2$. Let $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ be a homomorphic mapping with $\psi(g_2) = g_1$. Let $\{0,1\}^{\ell_1}$ be the space of messages, and $\mathcal{H} : \{0,1\}^{\ell_1} \to \mathbb{Z}_{q_1}$ be a hash function from the message space to $\mathbb{Z}_{q_1}$.

The following is the signature from [9]. We quote their long-message version to suit the purpose of this paper.

Signature $\mathsf{Sig}_{\mathsf{SDH}}$ [9]:

1. $\mathsf{sk} = (x, y)$, $\mathsf{pk} = (g_1, g_2, g_2^x, g_2^y, \hat{\mathbf{e}}, \mathcal{H})$.
2. **Signing Protocol** Given sk, pk, and message m, randomly generate $R \in Z_{q_1}^*$. Output the signature $(m, \sigma = g_1^{1/(x+\mathcal{H}(m)+Ry)})$.
3. **Verification Protocol** Upon receiving a signature (R, σ) for message m, verify $\hat{\mathbf{e}}$ $(\sigma, g_2^{x+\mathcal{H}(m)+Ry})$ $=\hat{\mathbf{e}}$ (g_1, g_2).

Boneh and Boyen [9] proved that the SDH Assumption implies the unforgeability of $\mathsf{Sig}_{\mathsf{SDH}}$. Again we use their long-message version.

Theorem 2. *[9] Assume a homomorphic map $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ with $\psi(g_2) = g_1$ is known. Then signature scheme $\mathsf{Sig}_{\mathsf{SDH}}$ is* correct *and (q_S, T, ϵ)-*ACP-UF *provided the $(q_S, T + O(q_s^2), (\epsilon/4) - (q_S/q_1))$-*SDH Assumption *holds and $\mathcal{H}$ is $(T + O(q_s^2), (\epsilon/4) - (q_S/q_1))$-*collision resistant.

Note $O(q_S^2)$ is the time cost to convert an SDH Problem instance to the public parameters of the signature. Using a similar proof, we can also easily reduce the unforgeability of $\mathsf{Sig}_{\mathsf{SDH}}$ to the SDH' Assumption:

Theorem 3. *Assume a homomorphic map $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ with $\psi(g_2) = g_1$ is known. The signature scheme $\mathsf{Sig}_{\mathsf{SDH}}$ is* correct *and (q_S, T, ϵ)-*ACP-UF *provided the $(q_S, T + O(q_S^2), (\epsilon/2) - (q_S/q_1))$-*SDH' Assumption *holds and $\mathcal{H}$ is $(T + O(q_s^2), (\epsilon/4) - (q_S/q_1))$-*collision resistant*.*

3.3 New short signature: the Product SDH Signature

We present the first of our three new short signatures without random oracles. It is motivated by Boneh and Boyen [9]'s state-of-the-art short signature. Let $\hat{\mathbf{e}} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_3$ be a pairing, order$(\mathbb{G}_1) = q_1$ is a prime, g is a generator of $\mathbb{G}_1$. Let $\{0,1\}^{\ell_1}$ be the message space, $\mathcal{H} : \{0,1\}^{\ell_1} \to \{0,1\}^\ell \setminus \{0^\ell\}$, $\ell < \log_2 q_1$.

Signature $\mathsf{Sig}_{\mathsf{PSDH}}$:

1. $\mathsf{sk} = (x, y)$, $\mathsf{pk} = (g, g^x, g^y, g^{xy}, \hat{\mathbf{e}}, \mathcal{H})$.
2. **Signing Protocol** Given sk, pk, and message $m \in \{0,1\}^{\ell_1}$, randomly generate nonzero $m_1, m_2 \in \{0,1\}^{\ell}$ with $m_1 \oplus m_2 = \mathcal{H}(m)$. Output the signature
$$(m_1, \sigma = g^{1/((x+m_1)(y+m_2))})$$
3. **Verification Protocol** Upon receiving a signature (m_1, σ) for message m, compute $m_2 = \mathcal{H}(m) \oplus m_1$, verify $m_1 \neq 0$, $m_2 \neq 0$, and $\hat{\mathbf{e}}(\sigma, g^{(x+m_1)(y+m_2)}) = \hat{\mathbf{e}}(g, g)$.

The unforgeability of $\mathsf{Sig}_{\mathsf{PSDH}}$ is reducible to the SDH' Assumption:

Theorem 4. *The signature scheme* $\mathsf{Sig}_{\mathsf{PSDH}}$ *is* correct *and* (q_S, T, ϵ)-ACP-UF *provided the following all hold:*

1. *the* $(q_S, T + O(q_S^2), \epsilon/6 - q_S/q_1)$-SDH' Assumption *holds;*
2. $\mathcal{H}$ *is a* $(q_S, \ell, T + O(q_S^2), \epsilon/6 - q_S/q_1)$-SSPIR (Sum Second Pre-Image Resistant) hash function*;*
3. $\mathcal{H}$ *is a* $(T + O(q_S^2), \epsilon/6 - q_S/q_1)$-Collision Resistant hash function*.*

Combining with Lemma 1, we reduce the unforgeability of $\mathsf{Sig}_{\mathsf{PSDH}}$ to the SDH Assumption:

Corollary 5 *Assume a homomorphic mapping* $\psi(g_2) = g_1$ *is given. The signature scheme* $\mathsf{Sig}_{\mathsf{PSDH}}$ *is* correct *and* (q_S, T, ϵ)-ACP-UF *provided the following all hold:*

1. *the* $(q_S, T + O(q_S^2), \epsilon/6 - q_S/q_1)$-SDH Assumption *holds;*
2. $\mathcal{H}$ *is a* $(q_S, \ell, T + O(q_S^2), \epsilon/6 - q_S/q_1)$-SSPIR hash function*;*
3. $\mathcal{H}$ *is a* $(T + O(q_S^2), \epsilon/6 - q_S/q_1)$-Collision Resistant hash function*.*

Proof of Theorem 4: The correctness is trivial. Next we use an ACP-UF attacker to build a Simulator $\mathcal{S}$ to solve the intractability problems.

Setting up: Simulator $\mathcal{S}$ receives a q_S-SDH' Problem instance: a_2, a_2^w, $\{a_1^{w^i} : 0 \leq i \leq q_S\}$. $\mathcal{S}$ flips a fair coin c_{mode} and proceeds below:

1. If $c_{mode} = 1$, $\mathcal{S}$ randomly picks distinct nonzero $\hat{m}_1, \cdots, \hat{m}_{q_S} \in \{0,1\}^{\ell}$, computes $g = a_1^{f_2(w)}$ where $f_2(w) = \prod_{i=1}^{q_S}(w + \hat{m}_i)$, and computes $\hat{\sigma}_i = a_1^{1/(w+\hat{m}_i)}$, $1 \leq i \leq q_S$. Note the complexity of the above transformation of the problem instance is $O(q_S^2)$. $\mathcal{S}$ randomly picks y, sets $x = w$, publishes $\mathsf{pk} = (g,\ g^x,\ g^y,\ g^{xy})$.
2. If $c_{mode} = 2$, $\mathcal{S}$ randomly picks distinct nonzero $\hat{m}_1, \cdots, \hat{m}_{q_S} \in \{0,1\}^{\ell}$, computes $g = a_1^{f_2(w)}$ where $f_2(w) = \prod_{i=1}^{q_S}(w + \hat{m}_i)$, and computes $\hat{\sigma}_i = a_1^{1/(w+\hat{m}_i)}$, $1 \leq i \leq q_S$. Then it randomly picks x, sets $y = w$, publishes $\mathsf{pk} = (g,\ g^x,\ g^y,\ g^{xy})$.

Simulating $\mathcal{SO}$: If $c_{mode} = 1$, do the following: Upon the τ-th $\mathcal{SO}$ query input m_τ, $1 \leq \tau \leq q_S$, abort if $\mathcal{H}(m_\tau) = m_\tau$. Else set $m_{1,\tau} = \hat{m}_\tau$, $m_{2,\tau} = \mathcal{H}(m_\tau) \oplus m_{1,\tau}$ and output the signature $(m_{1,\tau}, \sigma_\tau = (\hat{\sigma}_\tau)^{1/((y+m_{2,\tau}))})$.

If $c_{mode} = 2$, do the following: Upon the τ-th $\mathcal{SO}$ query input m_τ, $1 \leq \tau \leq q_S$, abort if $\mathcal{H}(m_\tau) = m_\tau$. Else set $m_{2,\tau} = \hat{m}_\tau$, $m_{1,\tau} = \mathcal{H}(m_\tau) \oplus m_{2,\tau}$ and output the signature $(m_{1,\tau}, \sigma_\tau = (\hat{\sigma}_\tau)^{1/((x+m_{1,\tau}))})$.

The **simulation deviation** [24]: It can be shown that any pairwise simulation deviation among (1) Real World, (2) Ideal World-1 where $c_{mode} = 1$, and (3) Ideal-World-2 where $c_{mode} = 2$, is negligible. The proof is tedious and mechanical. We omit it here.

The **extractions**: With probability ϵ, Attacker $\mathcal{A}$ eventually delivers a valid message-signature pair (m^*, (m_1^*, σ^*)), $m^* \neq m_\tau$, $\forall\tau$. Compute $m_2^* = \mathcal{H}(m^*) \oplus m_1^*$. When the pair is valid, one of the following events must happen:

- Event A1: $m_1^* \neq m_{1,\tau}$ for any τ. If also $c_{mode} = 1$, then the SDH' Problem instance is solved by the tuple $(m_1^*, (\sigma^*)^{(y+m_{2,\tau}^*)})$.
- Event A2: $m_2^* \neq m_{1,\tau}$ for any τ. If also $c_{mode} = 2$, then the SDH' Problem instance is solved by the tuple $(m_2^*, (\sigma^*)^{(x+m_{1,\tau}^*)})$.
- Event B: $m_1^* = \hat{m}_\tau$ and $m_2^* = \hat{m}_{\tau'}$ for some $1 \leq \tau, \tau' \leq q_S$, $\tau \neq \tau'$. The $(\mathcal{H}, q_S, \ell)$-SSPI Problem is solved by (m^*, τ, τ') where $\mathcal{H}(m^*) = \hat{m}_\tau \oplus \hat{m}_{\tau'}$.
- Event C: $m_1^* = \hat{m}_\tau$ and $m_2^* = \hat{m}_{\tau'}$ for some $1 \leq \tau, \tau' \leq q_S$, $\tau = \tau'$. Then $m^* \neq m_\tau$, $\mathcal{H}(m^*) = \mathcal{H}(m_\tau)$ and $\mathcal{H}$ is not collision-resistant.

The *Exact Security*: The probability of each event is independent of the value of c_{mode}, due to the negligibility of the simulation deviation. The sum of the probabilities of all events above is greater than or equal to ϵ. Let probability Event A denote probability Event A1 *or* probability Event A2. Then at least one of the following composite event has probability lower bounded by $\epsilon/6 - q_S/q_1$

1. $\{ \{\text{Event A1} \wedge c_{mode} = 1\} \vee \{\text{Event A2} \wedge c_{mode} = 2\} \} \wedge \mathcal{A}$ forges
2. Event B $\wedge$ $\mathcal{A}$ forges
3. Event C $\wedge$ $\mathcal{A}$ forges

Note the total probability of aborting during $\mathcal{SO}$ simulation is q_S/q_1. The Theorem is obtained. □

Efficiency discussions We have in mind, in $\mathsf{Sig}_{\mathsf{PSDH}}$, to use $\log_2 q_1 \approx 2\lambda_s$ and $\ell \approx 2\lambda_s$. Justifications below: Using high-security pairings suggested by Koblitz and Menezes [29], with security level $\lambda_s = 128, 192, 256$ bits, q_1 should be at least $2\lambda_s$ bits to ward off the Pollard-ρ attack. The value of ℓ should be at least λ_s to ward off the birthday attack on second pre-image resistance. To ward off hash collisions with probability $\epsilon \approx 2^{-\lambda_s}$, the output of $\mathcal{H}$ should be at least $2\lambda_s$ bits, relative to contemporary hashing technology and taking care to mitigate Wang, Xiaoyun's attacks.

The signature length is $4\lambda_s$ bits, similar to the state-of-the-art in [9, 45].

4 Another new short signature: Product Square Root (PSR) signature

We present the second of our three new short signatures without random oracles. It is motivated by Zhang, et al. [45]'s state-of-the-art short signature from the q SR (Square Root) Assumption. Below, we discuss intractability assumptions both new and old, then review Zhang, et a;. [45]'s signature, before presenting our new signature.

Let $\hat{\mathbf{e}} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_3$ be a pairing, $\text{order}(\mathbb{G}_1) = q_1$ is a prime, g is a generator of $\mathbb{G}_1$.

4.1 Intractability Assumptions

We present several needed assumptions. The q-SR Assumption is from [45]. The other assumptions are new.

Definition 7. *The* q-Square Root (q-SR) Problem *is, given random* g, g^x, Z_τ, a_τ *satisfying* $\hat{\mathbf{e}}(Z_\tau,\ Z_\tau) = \hat{\mathbf{e}}(g^{x+a_\tau},\ g)$, $1 \le \tau \le q$, *output* (a, Z), *satisfying* $\hat{\mathbf{e}}(Z, Z) = \hat{\mathbf{e}}(g^{x+a}, g)$, $a \notin \{a_1, \cdots, a_q\}$. *An algorithm* $\mathcal{A}$ *is said to* (T, ϵ)*-solve the q-SR Problem if*

$$\Pr[\mathcal{A}(g, g^x, g^{(x+a_1)^{1/2}}, \cdots, g^{(x+a_q)^{1/2}}) = (a, g^{(x+a)^{1/2}}) \ \wedge\ a \textit{ is distinct from all } a_i\textit{'s}] \ge \epsilon$$

with running time T*, where the probability is taken over qualified random choices of* x, a_1, $\cdots$, a_q*, and random bits consumed by* $\mathcal{A}$*. The* (q, T, ϵ)*-SR Assumption is that no algorithm can solve the* (T, ϵ)*-solve the q-SR Problem.*

Definition 8. *The* (q, ℓ) Short Input Square Root Problem, *abbreviated the* (q, ℓ)-SR Problem *is, given random* g, g^x, *distinct nonzero* $\{a_1, \cdots, a_q\}$, *and* $\{Z_1 = g^{(x+a_1)^{1/2}}, \cdots, Z_q = g^{(x+a_{q_S})^{1/2}}\}$, *to output* (a, Z), *satisfying* $\hat{\mathbf{e}}(Z, Z) = \hat{\mathbf{e}}(g^{x+a}, g)$, $a \in \{0, 1\}^\ell \setminus \{a_1, \cdots, a_q\}$. *An algorithm* $\mathcal{A}$ *is said to* (T, ϵ)*-solve the* (q, ℓ)*-SR Problem if*

$$\Pr[\mathcal{A}(g, g^x, a_1, g^{(x+a_1)^{1/2}}, \cdots, a_q, g^{(x+a_q)^{1/2}}) = (a, g^{(x+a)^{1/2}}) \ \wedge\ a \in \{0, 1\}^\ell \setminus \{a_1, \cdots, a_q\}] \ge \epsilon$$

with running time T*, where the probability is taken over qualified random choices of* x, $\{a_1, \cdots, a_q\} \subset \{0, 1\}^\ell$*, and random bits consumed by* $\mathcal{A}$*. The* (q, ℓ, T, ϵ)*-SR Assumption is that no algorithm can solve the* (T, ϵ)*-solve the* (q, ℓ)*-SR Problem.*

Definition 9. *The* (q, ℓ) Short Input Square Root Quadratic Non-Residue Problem, abbreviated the (q, ℓ)-SRQNR) Problem *is, given random* g, g^x, *distinct nonzero* $\{a_1, \cdots, a_q\}$, *and* $\{Z_1 = g^{(x+a_1)^{1/2}}, \cdots, Z_q = g^{(x+a_{q_S})^{1/2}}\}$, *to output* (a, Z, γ), *satisfying* $\gamma \in QNR(q_1)$, $\hat{\mathbf{e}}(Z, Z) = \hat{\mathbf{e}}(g^{x+a}, g^\gamma)$, $a \in \{0, 1\}^\ell \setminus \{a_1, \cdots, a_{q_S}\}$. *An algorithm* $\mathcal{A}$ *is said to* (T, ϵ)*-solve the* (q, ℓ)*-SRQNR Problem if*

$$\Pr[\mathcal{A}(g, g^x, a_1, g^{(x+a_1)^{1/2}}, \cdots, a_q, g^{(x+a_q)^{1/2}}) = (a, Z, \gamma) \ \wedge\ \gamma \in QNR(q_1) \ \wedge\ \hat{\mathbf{e}}(Z, Z) = \hat{\mathbf{e}}(g^{x+a}, g^\gamma) \wedge a \in \{0, 1\}^\ell \setminus \{a_1, \cdots, a_{q_S}\}] \ge \epsilon$$

with running time T*, where the probability is taken over qualified random choices of* x, $\{a_1, \cdots, a_q\} \subset \{0, 1\}^\ell$*, and random bits consumed by* $\mathcal{A}$*. The* (q, ℓ, T, ϵ)*-SRQNR Assumption is that no algorithm can solve the* (T, ϵ)*-solve the* (q, ℓ)*-SRQNR Problem.*

Intractability assumptions about hash functions.

Definition 10. *Let* $\mathcal{H}$ *be a mapping,* $\mathcal{H} : \{0, 1\}^\ell \to \{0, 1\}^\ell$*. The* $\mathcal{H}$-Iterated Collision Problem *is to output* $(m, m', k, k') \in (\{0, 1\}^\ell)^2 \times (\mathbb{Z}^+)^2$ *satisfying* $m \ne m$ *and* $\mathcal{H}^k(m) = \mathcal{H}^{k'}(m')$*. An algorithm* $\mathcal{A}$ *is said to* (T, ϵ)-solve *the* $\mathcal{H}$*-Iterated Collision Problem if*

$$\Pr[\mathcal{A}(\mathcal{H}) = (m, m', k, k') \in (\{0, 1\}^\ell)^2 \times (\mathbb{Z}^+)^2 \wedge m \ne m \wedge \mathcal{H}^k(m) = \mathcal{H}^{k'}(m')] \ge \epsilon$$

with running time T*, and the probability is over random bits* $\mathcal{A}$ *consumes.* $\mathcal{H}$ *is called a* (T, ϵ)-Iterated Collision Resistant hash function *if no algorithm can* (T, ϵ)-solve the $\mathcal{H}$-Iterated Collision Problem.

Definition 11. *Let $\mathcal{H} : \{0,1\}^\ell \to \{0,1\}^\ell$ be a mapping. The* $(\mathcal{H}, q, \ell)$-Sum Iterated Second Pre-Image Problem ($(\mathcal{H}, q, \ell)$-SISPI Problem) *is, given random distinct nonzero $a_1, \cdots, a_q \in \{0,1\}^\ell$, to output (b, i, j, k), $1 \le i, j \le q$, k is a positive integer, satisfying $\mathcal{H}^k(b) = a_i \oplus a_j \neq 0$. An algorithm $\mathcal{A}$ is said to* (T, ϵ)-solve *the $(\mathcal{H}, q, \ell)$-SISPI Problem if*

$$\Pr[\mathcal{A}(\mathcal{H}, q, a_1, \cdots, a_q) \\ = (b, i, j, k) \wedge 1 \le i \le j \le q \wedge \mathcal{H}^k(b) = a_i \oplus a_j \neq 0] = \epsilon$$

with running time T, and the probability is over random choices of distinct nonzero $a_1, \cdots, a_q$ and random bits $\mathcal{A}$ consumes. A mapping $\mathcal{H}$ is called a (q, ℓ, T, ϵ)-SISPIR hash function ((q, ℓ, T, ϵ)-Sum Iterated Second Pre-Image Resistant hash function) *if no algorithm can (T, ϵ)-solve the $(\mathcal{H}, q, \ell)$-SISPI Problem.*

4.2 Review: Zhang, et al. [45]'s q-Square Root signature

We review Zhang, et al. [45]'s short signature without random oracles from the q-SR Assumption. Let $\hat{\mathbf{e}} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_3$ be a pairing, order$(\mathbb{G}_1) = q_1$ is a prime. Let the message space be $\{0,1\}^{\ell_1}$, $\mathcal{H} : \{0,1\}^{\ell_1} \to \mathbb{Z}_{q_1}^*$. For simplicity, let $\ell_1 = \ell$.

Signature $\mathsf{Sig}_{\mathsf{SR}}$:

1. $\mathsf{sk} = x$, $\mathsf{pk} = (g, g^x, \hat{\mathbf{e}}, \mathcal{H})$.
2. *Signing Protocol* Given sk, pk, and message m, randomly generate R satisfying $x + \mathcal{H}(m)y + R \in QR(q_1)$. Output the signature $(R,\ \sigma = g^{(x+\mathcal{H}(m)y+R)^{1/2}})$. Randomly choose either square root of $x + \mathcal{H}(m)y + R$.
3. *Verification Protocol* Upon receiving a signature (R, σ) for message m, verify $\hat{\mathbf{e}}(\sigma,\ \sigma) = \hat{\mathbf{e}}(g^{x+\mathcal{H}(m)y+R},\ g)$.

Note we use a long-message variant above. Zhang, et al. [45] reduced the unforgeability of $\mathsf{Sig}_{\mathsf{SR}}$ to the q-SR Assumption:

Theorem 6. [45] *The signature scheme $\mathsf{Sig}_{\mathsf{SR}}$ is* correct *and* (q_S, T, ϵ)-ACP-UF *provided the* $(q, T+O(q_S), (\epsilon/4)-(q_S/q_1))$-SR Assumption *holds and $\mathcal{H}$ is a* $(q, T+O(q_S), (\epsilon/4)-(q_S/q_1))$-collision resistant hash function.

4.3 New signature from the Product Square-Root (PSR) Assumption: $\mathsf{Sig}_{\mathsf{PSR}}$

We present the second of our three new short signatures without random oracles. This signature is modified from Zhang, et al. [45]'s short signature without random oracles.

Let $\hat{\mathbf{e}} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_3$ be a pairing, order$(\mathbb{G}_1) = q_1$ is a prime. Let the message space be $\{0,1\}^{\ell_1}$. Let $\ell < \log_2 q_1$. For simplicity let $\ell_1 = \ell$.

Signature $\mathsf{Sig}_{\mathsf{PSR}}$:

1. $\mathsf{sk} = (x, y)$, $\mathsf{pk} = (g, g^x, g^y, \hat{\mathbf{e}}, \mathcal{H})$, where $\mathcal{H} : \{0,1\}^\ell \to \{0,1\}^\ell$.
2. *Signing Protocol*: Given sk, pk, and message m, do the following:
   (a) Initialize $k = 0$.
   (b) If $\mathcal{H}^{k+1}(m) \neq 0$, randomly pick nonzero m_1, m_2 from $\{0,1\}^\ell$ satisfying $m_1 \oplus m_2 = \mathcal{H}^{k+1}(m)$ and go to next Step. Else increment k by one and go to the beginning of this Step.

(c) If $x+m_1, y+m_2 \in QR(q_1)$, then output the signature $(m_1, '0^k1', \sigma = g^{(x+m_1)^{1/2}(y+m_2)^{1/2}})$ by randomly choosing either square root in each case, and terminate. Else increment k by one and go back to the previous step. Note $'0^k1'$ is the string with k zeros followed by a $'1'$.

3. *Verification Protocol*: Upon receiving a signature $(m_1, '0^k1', \sigma)$ for message m, parse the signature, recover k from the second entry, compute $m_2 = \mathcal{H}^{k+1}(m) \oplus m_1$, verify $m_1, m_2 \in \{0,1\}^{\lambda_s} \setminus \{0\}$, $m_1 \neq m_2$, and $\hat{\mathbf{e}}(\sigma, \sigma) = \hat{\mathbf{e}}(g^{x+m_1}, g^{y+m_2})$.

Theorem 7. *The signature scheme* Sig_{PSR} *is* correct *and* (q_S, T, ϵ)-ACP-UF *provided the following all hold:*

1. *the* $(q_S, \ell, T + O(q_S), (\epsilon/8) - (8q_S/q_1))$-SR (Square Root) Assumption *holds;*
2. *the* $(q_S, \ell, T + O(q_S), (\epsilon/8) - (8q_S/q_1))$-SRQNR (Square Root Quadratic Non-Residue) Assumption *holds;*
3. $\mathcal{H}$ *is a* $(q_S, \ell, T/2 + O(q_S), ((\epsilon/8) - (8q_S/q_1))$-SISPIR (Sum Iterated Second Pre-Image Resistant) hash function*;*
4. $\mathcal{H}$ *is a* $(\ell, T/2 + O(q_S), ((\epsilon/8) - (8q_S/q_1))$-Iterated Collision Resistant hash function*;*

where q_S *is the number of signing oracle queries.*

Proof: The correctness is trivial. Next we use a successful ACP-UF attacker to build a solver of the intractability problem.

Setting up: Simulator $\mathcal{S}$ receives, simultaneously, the following problem instances:

1. a (q, ℓ)-SR Problem instance: g', $(g')^{w'}$, distinct nonzero $\{\hat{m}_1, \cdots, \hat{m}_{q_S}\}$, $\{\hat{\sigma}_1 = (g')^{(w'+\hat{m}_1)^{1/2}}, \cdots, \hat{\sigma}_{q_S} = (g')^{(w'+\hat{m_{q_S}})^{1/2}}$.
2. a (q, ℓ)-SRQNR Problem instance: g'', $(g'')^{w''}$, distinct nonzero $\{\hat{m}_1, \cdots, \hat{m}_{q_S}\}$, $\{\hat{\sigma}_1 = (g'')^{(w''+\hat{m}_1)^{1/2}}, \cdots, \hat{\sigma}_{q_S} = (g'')^{(w''+\hat{m}_{q_S})^{1/2}}$.

$\mathcal{S}$ flips a four-way fair coin c_{mode} and proceeds below:

If $c_{mode} = 1$, $\mathcal{S}$ sets $g = g'$ and $g^x = (g')^{w'}$, randomly picks y and z, publishes $\mathsf{pk} = (g, g^x, g^y, g^z, g^{yz})$.

If $c_{mode} = 2$, $\mathcal{S}$ sets $g = g'$ and $g^y = (g')^{w'}$, randomly picks x and z, publishes $\mathsf{pk} = (g, g^x, g^y, g^z, g^{yz})$.

If $c_{mode} = 3$, $\mathcal{S}$ sets $g = g''$ and $g^x = (g'')^{w''}$, randomly picks y and z, publishes $\mathsf{pk} = (g, g^x, g^y, g^z, g^{yz})$.

If $c_{mode} = 4$, $\mathcal{S}$ sets $g = g''$ and $g^y = (g'')^{w''}$, randomly picks x and z, publishes $\mathsf{pk} = (g, g^x, g^y, g^z, g^{yz})$.

Simulating $\mathcal{SO}$: Upon receiving the query message m_τ, proceed as follows:

If $c_{mode} = 1$, do the following:

1. Initialize $k_\tau = 0$.
2. Set $m_{1,\tau} = \hat{m}_\tau$, compute $m_{2,\tau} = \mathcal{H}^{k_\tau+1}(m_\tau) \oplus m_{1,\tau}$. Abort the entire simulation process if $m_{2,\tau} = 0$ or $m_{2,\tau} = m_{2,\tau}$ (for the preservation of the negligibility of the simulation deviation). Else flip a fair coin $coin_{\tau,k_\tau}$ and go to next Step.
3. If $coin_{\tau,k_\tau} = 1$ and $y + m_{2,\tau} \in QR(q_1)$, then output the signature $(m_{1,\tau}, '0^{k_\tau}1', \sigma = \hat{\sigma}_\tau^{(x+m_{1,\tau})^{1/2}(y+m_{2,\tau})^{1/2}})$ and exit this $\mathcal{SO}$ query. (Randomly choose either square root in each case.) Else increment k_τ by one and return to Step (2) above.

If $c_{mode} = 2$, simulate $\mathcal{SO}$ similarly to the case $c_{mode} = 1$, except with the roles of x and y swapped. If $c_{mode} = 3$, simulate as in the case $c_{mode} = 1$. If $c_{mode} = 4$, simulate as in the case $c_{mode} = 2$.

Simulation deviation: There are three *worlds* to consider: (1) Real World, (2) Ideal World-1 where $c_{mode} = 1$, and (3) Ideal-World-2 where $c_{mode} = 2$. The simulation deviation between the two Ideal Worlds is negligible due to symmetry. That the simulation deviation between the Real World and either Ideal World is negligible is proved below.

Without loss of generality, let $c_{mode} = 1$. Given any $\mathcal{SO}$ output for query m_τ, denoted $(m_{1,\tau},' 0^{k_\tau} 1', \sigma = g^{(x+m_{1,\tau})^{1/2}(y+m_{2,\tau})^{1/2}})$, there exists a sequence of random bits consumed by Signer in the Real World that produces the same output with the same probability, as follows: Real World Signer, for each k, $0 \le k < k_\tau$, randomly generates nonzero $\tilde{m}_{1,k}$, $\tilde{m}_{2,k} \in \{0,1\}^\ell$ satisfying $\mathcal{H}^{k+1}(m_\tau) = \tilde{m}_{1,k} \oplus \tilde{m}_{2,k}$. But it occurs that $(x+\tilde{m}_{1,k}, y+\tilde{m}_{2,k}) \notin QR(q_1)^2$ for each $k < k_\tau$. Then Real World Signer generates, in the k_τ-th try, $(\tilde{m}_{i,k_\tau}, \tilde{m}_{2,k_\tau}) = (\hat{m}_\tau, m_{2,\tau}) \in QR(q_1)^2$. The probability of the above event equals the probability of $\mathcal{SO}$ outputting the same signature, i.e. $(3/4)^{k_\tau}(1/4)$. Therefore the simulation deviation between Real World and Ideal World-1 is negligible.

Extractions: With probability ϵ, Attacker $\mathcal{A}$ eventually delivers a valid message-signature pair (m^*, (m_1^*, $0^k 1'$, σ^*)), $m^* \neq m_\tau$, $\forall \tau$. Compute $m_2^* = \mathcal{H}^{k^*}(m) \oplus m_1^*$. At least one of the following event occurs:

- Event A1: $m_1^* \neq m_{1,\tau}$ for any τ. If also $c_{mode} = 1$ and $y+m_2^* \in QR(q_1)$, then $(m_1^*, (\sigma^*)^{y+m_2^*})$ solves the SR Problem instance. Else if also $c_{mode} = 3$ and $y + m_2^* \in QNR(q_1)$, then $(m_1^*, \sigma^*, y + m_2^*)$ solves the SRQNR Problem instance.
- Event A2: $m_2^* \neq m_{2,\tau}$ for any τ. If also $c_{mode} = 2$ and $x+m_1^* \in QR(q_1)$, then $(m_2^*, (\sigma^*)^{x+m_1^*})$ solves the SR Problem instance. Else if also $c_{mode} = 4$ and $x + m_1^* \in QNR(q_1)$, then $(m_2^*, \sigma^*, x + m_1^*)$ solves the SRQNR Problem instance.
- Event B: $m_1^* = m_{1,\tau'}$ and $m_2^* = m_{2,\tau''}$ for some $\tau' \neq \tau''$. Then $\mathcal{H}^{k^*+1}(m^*) = \hat{m}_{\tau'} \oplus \hat{m}_{\tau''}$ and $(m^*, \tau', \tau'', k^* + 1)$ solves the SISPI Problem.
- Event C: $m_1^* = m_{1,\tau'}$ and $m_2^* = m_{2,\tau''}$ for some $\tau' = \tau''$. Then $\mathcal{H}^{k^*+1}(m^*) = \mathcal{H}^{k_\tau+1}(m_\tau)$ and the tuple $(m^*, m_\tau, k^* + 1, k_\tau + 1)$ solves the $\mathcal{H}$ Iterated Collision Problem.

The *Exact Security*: The probability of each event is independent of the value of c_{mode}, due to the negligibility of the simulation deviation. The sum of the probabilities of all events above is greater than or equal to ϵ. Let probability Event A denote probability Event A1 *or* probability Event A2. Then at least one of the following composite event has probability lower bounded by $\epsilon/8 - 8q_S/q_1$

1. $\{$Event A1 $\wedge\ c_{mode} = 1\} \vee \{$Event A2 $\wedge\ c_{mode} = 2\}$ (then $\mathcal{S}$ solves the SR Problem)
2. $\{$Event A1 $\wedge\ c_{mode} = 3\} \vee \{$Event A2 $\wedge\ c_{mode} = 4\}$ (then $\mathcal{S}$ solves the SRQNR Problem)
3. Event B (then $\mathcal{S}$ solves the SISPI Problem)
4. Event C (then $\mathcal{S}$ solves the $\mathcal{H}$ Iterated Collision Problem)

Note the total probability of aborting during $\mathcal{SO}$ simulation is $\langle k \rangle 2q_S/q_1$, where the expected value $\langle k \rangle = \sum_{k=1}^{\infty}(3/4)^k(1/k) = 4$. The Theorem is obtained. □

Efficiency discussions We have in mind, in $\mathsf{Sig}_{\mathsf{PSR}}$, to use $\log_2 q_1 \approx 2\lambda_s$ and $\ell \approx 2\lambda_s$. This signature length is $4\lambda_s$ bits, similar to the state-of-the-art in [9, 45]. Justifications are similar to those for $\mathsf{Sig}_{\mathsf{PSDH}}$ and omitted.

Verification's online complexity: Verifying $\mathsf{Sig}_{\mathsf{PSR}}$ costs one pairing and one multi-base exponentiations in $\mathbb{G}_3$: $\hat{\mathbf{e}}(g^{x+m_1}, g^{y+m_2}) = \hat{\mathbf{e}}(g^x, g^y)\hat{\mathbf{e}}(g^x, g)^{m_2}\hat{\mathbf{e}}(g, g^y)^{m_1}\hat{\mathbf{e}}(g, g)^{m_1 m_2}$

5 Yet another RO-free signature: the CL04B-wh Signature

Camenisch and Lysyanskaya [14] presented three signatures without random oracles, Schemes A, B, and C. We modify their Scheme B, hereby named $\mathsf{Sig}_{\mathsf{CL04B}}$, into a variant we name $\mathsf{Sig}_{\mathsf{CL04B\text{-}wh}}$. We prove the security of $\mathsf{Sig}_{\mathsf{CL04B\text{-}wh}}$ without random oracles and without the external signing oracle $O_{X,Y}(\cdot)$ used in all previous results containing the LRSW Assumption.

Let $\hat{\mathbf{e}} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_3$ be a pairing, order$(\mathbb{G}_1) = q_1$ is a prime, g is a generator of $\mathbb{G}_1$.

5.1 Intractability assumptions

First we review some existing, and define some new, intractability assumptions:

Definition 12. *[31] The* LRSW Problem *is: Given random $g, X = g^x, Y = g^y$, and an oracle $O_{X,Y}(\cdot)$ which, upon input m, returns a random tuple (m, a, b, c) satisfying $\hat{\mathbf{e}}(b, g) = \hat{\mathbf{e}}(a, Y)$, $\hat{\mathbf{e}}(c, g) = \hat{\mathbf{e}}(ab^m, X)$; output (m^*, a^*, b^*, c^*) satisfying $\hat{\mathbf{e}}(b^*, g) = \hat{\mathbf{e}}(a^*, g^y)$, $\hat{\mathbf{e}}(c^*, g) = \hat{\mathbf{e}}(a^*(b^*)^{m^*}, g^x)$, m^* has never been queried to $O_{X,Y}$. The* LRSW Assumption *is that no PPT algorithm can solve the LRSW Problem with non-negligible probability.*

The following new variant of the LRSW Assumption will be useful. Note its formulation is without the external signing oracle $O_{X,Y}(\cdot)$.

Definition 13. *The* q-wholesale LRSW (q-whLRSW) Problem *is: Given random g, g^x, g^y, random $(m_\tau, a_\tau, b_\tau, c_\tau)$ satisfying $\hat{\mathbf{e}}(b_\tau, g) = \hat{\mathbf{e}}(a_\tau, g^y)$, $\hat{\mathbf{e}}(c_\tau, g) = \hat{\mathbf{e}}(a_\tau b_\tau^{m_\tau}, g^x)$, $1 \leq \tau \leq q$; output (m^*, a^*, b^*, c^*) satisfying $\hat{\mathbf{e}}(b^*, g) = \hat{\mathbf{e}}(a^*, g^y)$, $\hat{\mathbf{e}}(c^*, g) = \hat{\mathbf{e}}(a^*(b^*)^{m^*}, g^x)$, $m^* \neq m_\tau\ \forall \tau$. An algorithm $\mathcal{A}$ is said to (T, ϵ)-solve the q-whLRSW Problem if*

$$\begin{aligned}\Pr[&\mathcal{A}(g, g^x, g^y, (m_1, a_1, b_1, c_1), \cdots, (m_q, a_q, b_q, c_q)) = (m, a, b, c)\\ &\wedge\ \hat{\mathbf{e}}(b, g) = \hat{\mathbf{e}}(a, g^y) \wedge \hat{\mathbf{e}}(c, g) = \hat{\mathbf{e}}(ab^m, g^x) \wedge m \neq m_\tau \forall \tau] = \epsilon\end{aligned}$$

with running time T, where the probability is taken over qualified random choices of x, y, (m_1, a_1, b_1, c_1), $\cdots$, (m_q, a_q, b_q, c_q) and random bits consumed by $\mathcal{A}$. The (q, T, ϵ)-whLRSW Assumption is that no algorithm can (T, ϵ)-solve the q-whLRSW Problem.

5.2 Review: The CL04B signature [14]

Signature $\mathsf{Sig}_{\mathsf{CL04B}}$:

1. $\mathsf{sk} = (x, y, z)$, $\mathsf{pk} = (g, g^x, g^y, g^z, \hat{\mathbf{e}})$.
2. **Signing Protocol** Given sk, pk, and message $m = (m_1, m_2)$, randomly generate a, compute $A = a^z$, $b = a^y$, $B = a^{yz}$, $c = a^{x+m_1xy+m_2xyz}$. Output the signature (a, A, b, B, c).
3. **Verification Protocol** Upon receiving a signature (a, A, b, B, c) for message m, verify

$$\begin{gathered}\hat{\mathbf{e}}(A, g) = \hat{\mathbf{e}}(a, g^z), \quad \hat{\mathbf{e}}(b, g) = \hat{\mathbf{e}}(a, g^y), \quad \hat{\mathbf{e}}(B, g) = \hat{\mathbf{e}}(A, g^y),\\ \hat{\mathbf{e}}(B, g) = \hat{\mathbf{e}}(b, g^z), \quad \hat{\mathbf{e}}(c, g) = \hat{\mathbf{e}}(ab^{m_1}B^{m_2}, g^x)\end{gathered}$$

Camenisch and Lysyanskaya [14] supplied the following security result:

Theorem 8. *[14] Signature $\mathsf{Sig}_{\mathsf{CL04B}}$ is* correct *and* ACP-UF *provided the* LRSW Assumption *holds.*

5.3 New RO-free signature: The CL04B-wh Signature

Camenisch and Lysyanskaya [14]'s second signature, $\mathsf{Sig}_{\mathsf{CL04B}}$, is provable in the plain model provided the LRSW Assumption holds. But the LRSW Assumption is formulated with an (external) oracle $O_{X,Y}(\cdot)$. Below, we prove a slightly modified version of $\mathsf{Sig}_{\mathsf{CL04B}}$, which we name $\mathsf{Sig}_{\mathsf{CL04B\text{-}wh}}$, to be secure in the plain model provided the q-whLRSW Assumption holds. Note the q-whLRSW Assumption is specified without any oracle similar to $O_{X,Y}(\cdot)$.

Signature $\mathsf{Sig}_{\mathsf{CL04B\text{-}wh}}$:

1. $\mathsf{sk} = (x, y, z)$, $\mathsf{pk} = (g, g^x, g^y, g^z, \hat{\mathbf{e}})$.
2. **Signing Protocol** Given sk, pk, and message m, randomly generate a, compute $A = a^z$, $b = a^y$, $B = a^{yz}$, $c = a^{x+(m+zR)xy}$. Output the signature (R, a, A, b, B, c).
3. **Verification Protocol** Upon receiving a signature (R, a, A, b, B, c) for message m, verify

$$\hat{\mathbf{e}}(A, g) = \hat{\mathbf{e}}(a, g^z), \quad \hat{\mathbf{e}}(b, g) = \hat{\mathbf{e}}(a, g^y), \quad \hat{\mathbf{e}}(B, g) = \hat{\mathbf{e}}(A, g^y),$$
$$\hat{\mathbf{e}}(B, g) = \hat{\mathbf{e}}(b, g^z), \quad \hat{\mathbf{e}}(c, g) = \hat{\mathbf{e}}(ab^m B^R, g^x)$$

Theorem 9. *The signature scheme* $\mathsf{Sig}_{\mathsf{CL04B\text{-}wh}}$ *is* correct *and* (q_S, T, ϵ)-ACP-UF *provided the* $(q_S, 2T + O(q_S), (2\epsilon^2/9) - (q_S^2 + q_S)/q_1)$-whLRSW Assumption *holds.*

Proof: The correctness is trivial. Next we use a successful ACP-UF attacker to build a solver of the intractability problem. In a nutshell. assume a PPT attacker $\mathcal{A}$ who can win the ACP-UF Game in average time T and probability ϵ. We use $\mathcal{A}$ to build a Simulator $\mathcal{S}$ who can solve the q_S-whLRSW Problem.

Setup: $\mathcal{S}$ received a q_S-whLRSW Problem instance: g, g^u, g^v, $(\hat{m}_\tau, \hat{a}_\tau, \hat{b}_\tau, \hat{c}_\tau)$, $1 \le \tau \le q_S$. $\mathcal{S}$ aborts if there are duplicates among $\hat{m}_\tau$'s. Note the probability of this abort is q_s^2/q_1. If it does not abort, $\mathcal{S}$ flips a three-way fair coin c_{mode} and sets up as follows:

1. If $c_{mode} = 1$, $\mathcal{S}$ randomly picks z, sets $\mathsf{pk} = (g^u, g^v, g^z)$.
2. If $c_{mode} = 2$, $\mathcal{S}$ picks x, y, sets $\mathsf{pk} = (g^x, g^y, g^u)$.
3. If $c_{mode} = 3$, $\mathcal{S}$ picks x, y, sets $\mathsf{pk} = (g^x, g^y, g^v)$.

Simulating $\mathcal{SO}$: If $c_{mode} = 1$, do the following: Upon the τ-th $\mathcal{SO}$ query input m_τ, $1 \le \tau \le q_S$, solve for R_τ in $\hat{m}_\tau = m_\tau + R_\tau z$. Output the signature $(R_\tau, a_\tau = \hat{a}_\tau, b_\tau = \hat{b}_\tau, c_\tau = \hat{c}_\tau)$.

If $c_{mode} = 2$ or 3, do the following: Upon the τ-th $\mathcal{SO}$ query input m_τ, $1 \le \tau \le q_S$, randomly pick α_τ, R_τ. Output the signature $(R_\tau, a_\tau = g^{\alpha_\tau}, b_\tau = g^{\alpha_\tau y}, c_\tau = g^{\alpha_\tau(1+(m_\tau+R_\tau z)xy)} = (g^z)^{R_\tau xy} g^{\alpha_\tau(1+m_\tau xy)})$.

The **simulation deviation**: It can be shown that the pairwise simulation deviation between any two of the following *worlds* are negligible: (1) Real World, (2) Ideal World-1 where $c_{mode} = 1$, (3) Ideal-World-2 where $c_{mode} = 2$, and (4) Ideal-World-3 where $c_{mode} = 3$. The proof is tedious but mechanical. We omit it.

Extraction: With probability ϵ, Attacker $\mathcal{A}$ eventually delivers a valid message-signature pair (m^*, (a^*, A^*, b^*, B^*, c^*)), $m^* \ne m_\tau$, $\forall\tau$. There are two events:

- Event A: $m^* + R^* z \ne \hat{m}_\tau$, $\forall\tau$.
- Event B: $m^* + R^* z = \hat{m}_\tau$, form some τ.

For $i = 1, 2, 3$, let $\epsilon_{i,A}$ (resp. $\epsilon_{c_{mode},B}$) denote the probability that $c_{mode} = i$ and Event A (resp. Event B). The negligibility of simulation deviations implies that $\epsilon_{1,A} = \epsilon_{2,A} = \epsilon_{3,A} = \epsilon_A$ and $\epsilon_{1,B} = \epsilon_{2,B} = \epsilon_{3,B} = \epsilon_B$. Note $\epsilon = 3\epsilon_A + 3\epsilon_B$.

In Event A, the tuple $(m^* + R^* z, a^*, b^*, c^*)$ solves the q_S-whLRSW Problem instance at hand. In Event B, we have $m^* + R^* z = \hat{m}_\tau = m_\tau + R_\tau z$, $m^* \neq m_\tau$, and the discrete logarithm $z = -(R^* - R_\tau)^{-1}(m^* - m_\tau)$ is solved where $z = u$ if $c_{mode} = 2$, and $z = v$ if $c_{mode} = 3$.

Finally, we rewind $\mathcal{A}$ to the beginning and resimulate it with a new randomness tape but with the same inputs of system parameters and q_S-whLRSW Problem instance, and flipping a new three-way fair coin c'_{mode}. Combining the result of both simulation *forks*, we obtain

1. The probability of Event A and c_{mode}=1 in the first fork or the second fork is $1 - (1 - \epsilon_A/3)^2 = (2/3)\epsilon_A - (1/9)\epsilon_A^2$. With this probability, we solve the q_S-whLRSW Problem instance at hand.
2. The probability of Event B in the first fork and the second fork, and $(c_{mode}, c'_{mode}) = (2, 3)$ or (3,2) is $(2/9)\epsilon_B^2$. With this probability, we obtains both u and v, and consequently solve the q_S-whLRSW Problem instance.

Exact Security In summary, we have a probability at least $(2/9)\epsilon^2$ of solving the q_S-whLRSW Problem instance, with time complexity twice that of the attacker algorithm $\mathcal{A}$ plus $O(q_S)$. The constant coefficient 2/9 can be further optimized, but we forgo that pursuit in order to simplify our core presentation. □

Efficiency discussions The length of signature $\mathsf{Sig}_{\mathsf{CL04B\text{-}wh}}$ is 5 $\mathbb{G}_1$ elements and one Z_{q_1} element, for a total of $5(5/2)\lambda_s + 2\lambda_2 = (29/2)\lambda_s$ bits according to [29]. The online verification complexity is 10 pairings, plus one exponentiation.

6 Discussions

Several signature schemes can be provably ACP-UF if the Simulator $\mathcal{S}$ is given an external Signing Oracle. We provide the details for two such signatures below: Boneh, Lynn, and Shacham [11]'s signature, and Zhang, Chen, Susilo, and Mu [45]'s second signture.

6.1 Zhang, Chen, Susilo, and Mu [45]'s second signture

Using our variable-length coding technique for k in $\mathsf{Sig}_{\mathsf{PSR}}$, we can improve the efficiency of Zhang, et al. [45]'s second signature with the modification below, named $\mathsf{Sig}_{\mathsf{SR}^*}$. Let $\hat{\mathbf{e}}: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_3$ be a pairing, order$(\mathbb{G}_1) = q_1$ be a prime, g be a generator of $\mathbb{G}_1$. The *Common Reference String* is denoted $\mathsf{crs} = r_1 r_2 r_3 \cdots$, each $r_i \in \{0, 1\}$.

Signature $\mathsf{Sig}_{\mathsf{SR}^*}$:

1. $\mathsf{sk} = x$, $\mathsf{pk} = (g, g^x, \hat{\mathbf{e}}, \mathcal{H}, \mathsf{crs}, \ell)$.
2. *Signing Protocol*: Upon inputs sk and message $m \in \{0, 1\}^\ell$, compute the smallest nonnegative integer k such that $x + (m || r_1 \cdots r_k) \in QR(q_1)$. Output the signature $('0^k 1', \sigma = g^{(x + (m||r_1 \cdots r_k))^{1/2}})$. Randomly choose either square root. Note the binary string $'0^k 1'$ consists of k zeros followed by a one.
3. *Verification Protocol*: Upon receiving signature $('0^k 1', \sigma)$ for message m, recover k from the first entry, and verify $\hat{\mathbf{e}}(\sigma, \sigma) = \hat{\mathbf{e}}(g^{x + (m||r_1 \cdots r_k)}, g)$.

Below, we define a new intractability assumption, and then reduce the security of $\mathsf{Sig}_{\mathsf{SR}^*}$ to it.

Definition 14. *The* Oracled Square Root (OSR) Problem *is: Given random $g, X = g^x$, random common reference string* crs*, and the Square Root Oracle $SRO_X(\cdot)$ which, upon input m, returns the tuple $('0^k1', g^{(x+(m||r_1\cdots r_k))^{1/2}})$ such that k is the smallest nonnegative integer satisfying $x + (m||r_1 \cdots r_k) \in QR(q_1)$; output $(m^*, '0^{k^*}1', g^{(x+(m^*||r_1\cdots r_{k^*}))^{1/2}})$, $x + (m^*||r_1 \cdots r_k) \in QR(q_1)$, m^* has never been queried to $SRO_X(\cdot)$. An algorithm $\mathcal{A}$ is said to (q_S, T, ϵ)-solve the OSR Problem if*

$$\Pr[\mathcal{A}^{SRO_X(\cdot)}(g, X, \mathsf{crs}) = (m^*, '0^{k^*}1', g^{(x+(m^*||r_1\cdots r_{k^*}))^{1/2}}) \\ \wedge x + (m^*||r_1 \cdots r_k) \in QR(q_1) \wedge m^* \textit{ has never been queried to } SRO_X(\cdot)] = \epsilon$$

with running time T, the number of queries to $SRO_X(\cdot)$ is q_S, and the probability is taken all random choices of g, X, crs *and the random bits $\mathcal{A}$ consumes. The (q_S, T, ϵ)-*OSR Assumption *is that no PPT algorithm can (q_S, T, ϵ)-solve the OSR Problem.*

Theorem 10. *The signature scheme* $\mathsf{Sig}_{\mathsf{SR}^*}$ *is* correct *and (q_S, T, ϵ)-ACP-UF provided the $(q_S, T + O(q_S), \epsilon)$-*OSR Assumption *holds.*

The proof is straightforward and omitted. Note $O(q_S)$ is the cost to simulate q_S Signing Oracle queries. Note the OSR Assumption remains plausible with respect to many contemporary attack technologies even if the attacker has a Chosen-Target Discrete Logarithm Collision [4] oracle and an ROS (Randomized Oversampled System) oracle [39] and a Generalized Birthday oracle [40].

Its correctness is straightforward. Its ACP-UF (existential unforgeability against adaptive-chosen-plaintext attackers) can be proved similar to [45]'s Theorem 2. The expected value of k is $\langle k \rangle = \sum_{i=1}^{\infty} k2^{-k} = 2$. The signature length is one $\mathbb{G}_1$ element plus $1 + \langle k \rangle = 3$ bits, or $(5/2)\lambda_s + 3$ bits according to [29]. The Signing complexity is two square-root tests in Z_{q_1} and one exponentiation in $\mathbb{G}_1$. The Verification complexity can be optimized by this technique

$$\hat{\mathbf{e}}(g^{x+(m||r_1\cdots r_k)}, g) = \hat{\mathbf{e}}(g^x, g)\hat{\mathbf{e}}(g, g)^{(m||r_1\cdots r_k)} \\ = \hat{\mathbf{e}}(g^x, g)((((\hat{\mathbf{e}}(g, g)^m)^2\hat{\mathbf{e}}(g, g)^{r_1})^2\hat{\mathbf{e}}(g, g)^{r_2})\cdots)^2\hat{\mathbf{e}}(g, g)^{r_k}$$

The online complexity consists of one exponentiation in $\mathbb{G}_3$, for $\hat{\mathbf{e}}(g, g)^m$, plus $\langle k \rangle$ square-and-multiply's in $\mathbb{G}_3$, plus one multiplication in $\mathbb{G}_3$, plus one pairing. for $\hat{\mathbf{e}}(\sigma, \sigma)$. Other parts can be precomputed. For $\lambda_s = 128$ (resp. 256), signature $\mathsf{Sig}_{\mathsf{SR}^*}$ is 323 (resp. 643) bits long, and its online verification costs is one pairing with 320-bit (resp. 640-bit) $\mathbb{G}_1$ elements and one exponentiation with 3072-bit (resp. 15360-bit) $\mathbb{G}_3$ elements according to [29]'s Table 1.

6.2 Boneh, Lynn, and Shacham [11]'s signature without random oracles

Here we prove the security of Boneh, Lynn, and Shacham [11]'s signature without random oracles. The signature is reviewed first:

signature scheme $\mathsf{Sig}_{\mathsf{BLS}}$:
1. $\mathsf{sk} = x$, $\mathsf{pk} = (g, g^x, \hat{\mathbf{e}}, \mathcal{H})$.
2. *Signing Protocol*: Given message m and sk, output $\sigma = \mathcal{H}(m)^x$.
3. *Verification Protocol*: Given signature σ for message m, verify $\hat{\mathbf{e}}(\sigma, g) = \hat{\mathbf{e}}(\mathcal{H}(m), g^x)$.

Security analysis We define an intractability assumption, and prove the security of $\mathsf{Sig}_{\mathsf{BLS}}$. First, an intractability assumption:

Definition 15. *The* Oracled Hashed Computational Diffie-Hellman (OCDH($\mathcal{H}$)) Problem *is: Given random $g, X = g^x$, hash function $\mathcal{H}$, and the Oracled Hashed CDH (OCDH($\mathcal{H}$)) Oracle $CDHO_{\mathcal{H},X}(\cdot)$ which, upon input m, returns the tuple $\mathcal{H}(m)^x$. An algorithm $\mathcal{A}$ is said to (q_S, T, ϵ)-solve the OCDH($\mathcal{H}$) Problem if*

$$\Pr[\mathcal{A}^{CDHO_{\mathcal{H},X}(\cdot)}(g, X) = (m^*, \mathcal{H}(m^*)^x) \\ \wedge\ m^* \text{ has never been queried to } CDHO_{\mathcal{H},X}(\cdot)] = \epsilon$$

with running time T, the number of queries to $CDHO_{\mathcal{H},X}(\cdot)$ is q_S, and the probability is taken all random choices of g, X, and the random bits $\mathcal{A}$ consumes. The (q_S, T, ϵ)-OCDH($\mathcal{H}$) Assumption *is that no PPT algorithm can (q_S, T, ϵ)-solve the OCDH($\mathcal{H}$) Problem.*

The following Theorem is straightforward, and we omit its proof.

Theorem 11. *The signature scheme* $\mathsf{Sig}_{\mathsf{BLS}}$ *is* correct *and (q_S, T, ϵ)-ACP-UF provided the* $(q_S, T + O(q_S), \epsilon)$-OCDH($\mathcal{H}$) Assumption *holds.*

Note $O(q_S)$ is the cost to simulate q_S Signing Oracle queries.

The length of $\mathsf{Sig}_{\mathsf{BLS}}$ is $(5/2)\lambda_s$ bits, using high-security pairings parameters suggested by Koblitz and Menezes [29]. The online verification complexity consists of two pairings, or alternatively one pairing and one exponentiation in $\mathbb{G}_3$. The size of a $\mathbb{G}_3$ element is 3072 (resp. 15360) bits for $\lambda_s = 128$ (resp. 256) [29].

A necessary condition for ACP-UF of $\mathsf{Sig}_{\mathsf{BLS}}$ To improve understanding, we present a necessary condition for the ACP-UF of $\mathsf{Sig}_{\mathsf{BLS}}$, based on a property of the hashing function $\mathcal{H}$. However, we cannot prove the condition is sufficient.

Definition 16. *Let p and q be primes, $q|(p-1)$, $g \in Z_p$, order$(g) = q$. A hash function $\mathcal{H}$: $\{0,1\}^\ell \to \langle g \rangle \subset Z_p$, is a (p, q, g, T, ϵ)-*Chosen-Target Discrete Logarithm Collision Resistant ((T, ϵ)-CTDLCR(p, q, g)) Hashing Function *if no algorithm $\mathcal{A}(p, q, g)$ can output $a_1, \cdots, a_n \in \{0,1\}^\ell$, and $(b_1, \cdots, b_n)$, not all $b_i = 0 \bmod q$, satisfying $\prod_{i=1}^n \mathcal{H}(a_i)^{b_i} = 1$ in running time T and success probability ϵ, where the probability is taken over random choices of $g \in Z_p$, order$(g) = q$, and random bits $\mathcal{A}$ consumes.*

The following relationship between the above two intractability assumptions is trivial:

Theorem 12. *Given primes p and q, $q|(p-1)$, the The* (q_S, T, ϵ)-OCDH($\mathcal{H}$) Assumption *implies that $\mathcal{H}$ is a* $((T - q_S T_{SO}, \epsilon)$-CTDLCR$(p, q))$ Hashing Function*, where T_{SO} is the running time of the Hashed CDH Oracle $CDHO_{\mathcal{H},X}(\cdot)$.*

Combining Theorems 11 and 12, we easily obtain:

Corollary 13 *If $\mathsf{Sig}_{\mathsf{BLS}}$ is* (q_S, T, ϵ)-ACP-UF*, then $\mathcal{H}$ is a* $((T - q_S T_{SO}, \epsilon)$-CTDLCR$(p, q))$ Hashing Function*, where T_{SO} is the running time of the Hashed CDH Oracle $CDHO_{\mathcal{H},X}(\cdot)$.*

Therefore, solving the Chosen-Target Discrete Logarithm Collision Problem implies the forgery of $\mathsf{Sig}_{\mathsf{BLS}}$. But it does not imply the forgery of any of $\mathsf{Sig}_{\mathsf{SDH}}$, $\mathsf{Sig}_{\mathsf{PSDH}}$, $\mathsf{Sig}_{\mathsf{SR}}$, $\mathsf{Sig}_{\mathsf{PSR}}$, $\mathsf{Sig}_{\mathsf{CL04B}}$, $\mathsf{Sig}_{\mathsf{CL04B\text{-}wh}}$, $\mathsf{Sig}_{\mathsf{SR}^*}$ – not yet, that is.

6.3 Even shorter versions of $\mathsf{Sig}_{\mathsf{PSDH}}$ and $\mathsf{Sig}_{\mathsf{PSR}}$

We can further shorten $\mathsf{Sig}_{\mathsf{PSDH}}$ by the following: Select two hash functions $\mathcal{H}$ and $\mathcal{H}'$. Given message m and sk, the Signing Algorithm computes $m_1 = \mathcal{H}(m) \oplus \mathcal{H}'(m)$, and outputs the signature $\sigma = g^{(x+m_1)^{-1}(y+\mathcal{H}'(m)^{-1})}$. The Verification Algorithm confirms $\hat{\mathbf{e}}(\sigma, g^{(x+m_1)(y+\mathcal{H}'(m))})$ $= \hat{\mathbf{e}}(g, g)$.

We can further shorten $\mathsf{Sig}_{\mathsf{PSR}}$ by the following: Select two hash functions $\mathcal{H}$ and $\mathcal{H}'$. Given message m and sk, the Signing Algorithm computes $m_1 = \mathcal{H}(m) \oplus \mathcal{H}'(m)$, and outputs the signature $\sigma = g^{(x+m_1)^{1/2}(y+\mathcal{H}'(m)^{1/2})}$. The Verification Algorithm confirms $\hat{\mathbf{e}}(\sigma, \sigma) = \hat{\mathbf{e}}(g^{x+m_1}, g^{y+\mathcal{H}'(m)})$.

7 Conclusions

We presented three new signatures without random oracles, and reduced their securities to new or old intractability assumptions. Two of our signatures are as short as state-of-the-art short signatures without random oracles.

The following remain interesting open problems: more varieties of efficient ordinary signatures without random oracles, and efficient signatures for specific applications without random oracles, such as ring signatures [15, 8], group signatures [1, 13], blind signatures [28], group-oriented signatures [41], hierarchical identity-based signatures [43], ..., etc.

Acknowledgements to Professor Zhang, Fangguo, for helpful discussions, and to Hong Kong Earmarked Grants 4232-03E and 4328-02E for financial support.

References

1. G. Ateniese, J. Camenisch, B. de Medeiros, and S. Hohenberger. Practical group signatures without random oracles, 2005. ePrint 2005/304.
2. Boaz Barak. How to go beyond the black-box simuation barrier. In *42d FOCS*, pages 106–115. IEEE Computer Soceity, 2001. Also http://www.wisdom.weizmann.ac.il/ boaz.
3. Boaz Barak, Yehuda Lindell, and Salil P. Vadhan. Lower bounds for non-black-box zero knowledge. In *FOCS 2003*, pages 384–393. IEEE Computer Soceity, 2003.
4. M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko. The one-more-RSA-inversion problem and the security of Chaum's blind signature scheme. *J. of Cryptology*, pages 185–215, 2003.
5. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proc. 1st ACM Conference on Computer and Communications Security*, pages 62–73. ACM Press, 1993.
6. Mihir Bellare and Oded Goldreich. On defining proofs of knowledge. In *CRYPTO 1992*, volume 740 of *LNCS*, pages 390–420, 1992.
7. Mihir Bellare and Oded Goldreich. Proving computational ability. manuscript, 2005. http://www-cse.ucsd.edu/users/mihir/papers/pok.html.
8. Adam Bender, Jonathan Katz, and Ruggero Morselli. Ring signatures: Stronger definitions, and constructions without random oracles. In *TCC'06*, 2005. Also ePrint 2005/304.
9. D. Boneh and X. Boyen. Short signatures without random oracles. In *Proc. EUROCRYPT 2004*, pages 56–73. Springer-Verlag, 2004. Lecture Notes in Computer Science No. 3027.
10. D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *Proc. CRYPTO 2004*, pages 41–55. Springer-Verlag, 2004. Lecture Notes in Computer Science No. 3152.
11. Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. In *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 514–532. Springer-Verlag, 2001.
12. Dan Boneh, Ilya Mironov, and Victor Shoup. A secure signature scheme from bilinear maps. In *CT-RSA 2003*, pages 98–110, 2003.
13. Xavier Boyen and Brent Waters. Compact group signatures without random oracles. Cryptology ePrint Archive, Report 2005/381, 2005. http://eprint.iacr.org/.

14. J. Camenisch and A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In *Proc. CRYPTO 2004*, volume 3152 of *LNCS*, pages 56–72. Springer-Verlag, 2004.
15. Sherman S. M. Chow, Joseph K. Liu, Victor K. Wei, and Tsz Hon Yuen. Ring signatures without random oracles. In *AsiaCCS'06*, 2005. Also ePrint 2005/317.
16. R. Cramer and I. Damgaard. Secure signature schemes based on interactive protocols. In *CRYPTO95*, pages 297–310, 1995.
17. R. Cramer and I. Damgaard. New generation of secure and practical rsabased signature. In *CRYPTO96*, pages 173–185, 1996.
18. R. Cramer and V. Shoup. Signature schemes based on the strong RSA assumption. In *ACM CCS99*, pages 161–185, 1999. Full version appeared in ACM TISSEC, v. 3(3), pp. 161C185, 2000.
19. C. Dwork and M. Naor. An efficient existentially unforgeable signature scheme and its applications. In *CRYPTO94*, pages 234–246, 1994. Full version appeared in J. of Cryptology, v. 11(2), pp. 187C208, 1998.
20. U. Feige, A. Fiat, and A. Shamir. Zero-knowledge proofs of identity. *Journal of Cryptology*, 1(2):77–94, 1988.
21. U. Feige and A. Shamir. Witness indistinguishable and witness hiding protocols. In *Proc. 22nd Annual ACM Sympsoium on Theory of Computing*, pages 416–426. ACM Press, 1990.
22. R. Gennaro, S. Halevi, and T. Rabin. Secure hash-and-sign signatures without the random oracle. In *Eurocrypt99*, pages 123–139, 1999.
23. O. Goldreich. *Foundations of Cryptography*, volume volumes 1 and 2. Cambridge Univesity Press, 2001 and 2005.
24. Oded Goldreich, Amit Sahai, and Salil P. Vadhan. Honest-verifier statistical zero-knowledge equals general statistical zero-knowledge. In *STOC'98*, pages 399–408, 1998.
25. S. Goldwasser, S. Micali, and R. Rivest. A paradoxical solution to the signature problem (extended abstract). In *FOCS'84*, page 441C448, 1984. Journal version in [26].
26. S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. on Computing*, 17(2):281C308, 1988.
27. Shafi Goldwasser and Yael Tauman Kalai. On the (in)security of the Fiat-Shamir paradigm. In *FOCS 2003*, pages 102–. IEEE Computer Soceity, 2003.
28. Aggelos Kiayias and Hong-Sheng Zhou. Two-round concurrent blind signatures without random oracles. Cryptology ePrint Archive, Report 2005/435, 2005. http://eprint.iacr.org/.
29. N. Koblitz and A. Menezes. Pairing-based cryptography at high security levels. In *10th IMA International Conference*, volume 3796 of *LNCS*, pages 13–36, 2005.
30. A. Lysyanskaya. Unique signatures and verifiable random functions from DH-DDH separation. In *CRYPTO02*, pages 597–612, 2002.
31. Anna Lysyanskaya, Ronald L. Rivest, Amit Sahai, and Stefan Wolf. Pseudonym systems. In *Selected Areas in Cryptography (SAC) 1999*, volume 1758 of *LNCS*, pages 184–199. Springer-Verlag, 1999.
32. W. Mao. *Modern Cryptography: Theory and Practice*. Pearson Education, 2004.
33. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press LLC, 1996.
34. S. Mitsunari, R. Sakai, and M. Kasahara. A new traitor tracing. *IEICE Trans. Fundamentals*, E85-A(2):481–484, 2002.
35. M. Naor and M. Yung. Universal one-way hash functions and their cryptographic applications. In *STOC'89*, pages 33–43, 1989.
36. T. Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In *Proc. CRYPTO 92*, pages 31–53. Springer-Verlag, 1993. Lecture Notes in Computer Science No. 740.
37. D. Pointcheval and J. Stern. Provably secure blind signature shcemes. In *Proc. ASIACRYPT 96*, pages 252–265. Springer-Verlag, 1996. Lecture Notes in Computer Science No. 1163.
38. D. Pointcheval and J. Stern. Security proofs for signature schemes. In *Proc. EUROCRYPT 96*, pages 387–398. Springer-Verlag, 1996. Lecture Notes in Computer Science No. 1070.
39. C. P. Schnorr. Security of blind discrete log signatures against interactive attacks. In *ICICS 2001*, volume 2229, pages 1–12. Springer–Verlag, 2001. LNCS.
40. D. Wagner. A generalized birthday problem. In *Proc. CRYPTO 2002*, pages 288–303. Springer-Verlag, 2002. Lecture Notes in Computer Science No. 2442.
41. Hong Wang, Yuqing Zhang, and Gengguo Feng. Short threshold signature schemes without random oracles. In *Indocrypt 2005*, pages 297–310, 2005.
42. Victor K. Wei. Tight reductions among strong Diffie-Hellman Assumptions. Cryptology ePrint Archive, Report 2005/057, 2005. http://eprint.iacr.org/.

43. Tsz Hon Yuen and Victor K. Wei. Constant-size hierarchical identity-based signature/signcryption without random oracles. Cryptology ePrint Archive, Report 2005/412, 2005. http://eprint.iacr.org/.
44. F. Zhang, R. Safavi-Naini, and W. Susilo. An efficient signature scheme from bilinear pairings and its applications. In *Proc. PKC'2004*, pages 277–290. Springer-Verlag, 2004. Lecture Notes in Computer Science No. 2947.
45. Fangguo Zhang, Xiaofeng Chen, Willy Susilo, and Yi Mu. A new short signature scheme without random oracles from bilinear pairings. Cryptology ePrint Archive, Report 2005/386, 2005. http://eprint.iacr.org/.