Concise Multi-challenge CCA-Secure Encryption and Signatures with Almost Tight Security

Benoît Libert[1,⋆], Marc Joye[2], Moti Yung[3], and Thomas Peters[4,⋆⋆]

[1] Ecole Normale Supérieure de Lyon,
Laboratoire de l'Informatique du Parallélisme, France
[2] Technicolor, USA
[3] Google Inc. and Columbia University, USA
[4] Université catholique de Louvain, Crypto Group, Belgium

Abstract. To gain strong confidence in the security of a public-key scheme, it is most desirable for the security proof to feature a *tight* reduction between the adversary and the algorithm solving the underlying hard problem. Recently, Chen and Wee (Crypto '13) described the first Identity-Based Encryption scheme with almost tight security under a standard assumption. Here, "almost tight" means that the security reduction only loses a factor $O(\lambda)$ —where λ is the security parameter— instead of a factor proportional to the number of adversarial queries. Chen and Wee also gave the shortest signatures whose security almost tightly relates to a simple assumption in the standard model. Also recently, Hofheinz and Jager (Crypto '12) constructed the first CCA-secure public-key encryption scheme in the multi-user setting with tight security. These constructions give schemes that are significantly less efficient in length (and thus, processing) when compared with the earlier schemes with loose reductions in their proof of security. Hofheinz and Jager's scheme has a ciphertext of a few hundreds of group elements, and they left open the problem of finding truly efficient constructions. Likewise, Chen and Wee's signatures and IBE schemes are somewhat less efficient than previous constructions with loose reductions from the same assumptions. In this paper, we consider space-efficient schemes with security almost tightly related to standard assumptions. We construct an efficient CCA-secure public-key encryption scheme whose chosen-ciphertext security in the multi-challenge, multi-user setting almost tightly relates to the DLIN assumption (in the standard model). Quite remarkably, the ciphertext size decreases to 69 group elements under the DLIN assumption whereas the best previous solution required about 400 group elements. Our scheme is obtained by taking advantage of a new almost tightly secure signature scheme (in the standard model) which is based on the recent concise proofs of linear subspace membership in the quasi-adaptive non-interactive zero-knowledge setting (QA-NIZK) defined by Jutla and Roy (Asiacrypt '13). Our signature scheme reduces the length

⋆ Part of this work was done while this author was with Technicolor (France).
⋆⋆ This author was supported by the CAMUS Walloon Region Project.

P. Sarkar and T. Iwata (Eds.): ASIACRYPT 2014, PART II, LNCS 8874, pp. 1–21, 2014.

of the previous such signatures (by Chen and Wee) by 37% under the Decision Linear assumption, by almost 50% under the K-LIN assumption, and it becomes only 3 group elements long under the Symmetric eXternal Diffie-Hellman assumption. Our signatures are obtained by carefully combining the proof technique of Chen and Wee and the above mentioned QA-NIZK proofs.

Keywords: CCA-secure encryption, multi-user, multi-challenge, signature, IND-CCA2 security, QA-NIZK proofs, tight security, efficiency.

1 Introduction

Security of public-key cryptographic primitives is established by demonstrating that any successful probabilistic polynomial time (PPT) adversary $\mathcal{A}$ implies a PPT algorithm $\mathcal{B}$ solving a hard problem. In order to be convincing, such "reductionist" arguments should be as *tight* as possible. Ideally, algorithm $\mathcal{B}$'s probability of success should be about as large as the adversary's advantage. The results of Bellare and Rogaway [9] initiated an important body of work devoted to the design of primitives validated by tight security reductions in the random oracle model [22,23,38,20,21,10,24,48,1,37] and in the standard model [21,7,48].

Tight security proofs may be hard to achieve and are even known not to exist at all in some situations [23,37,33]. On the positive side, long-standing open problems have been resolved in the recent years. Hofheinz and Jager [31] showed the first public-key encryption scheme whose chosen-ciphertext security [45,46] in the multi-user setting tightly relates to a standard hardness assumption, which solved a problem left open by Bellare, Boldyreva and Micali [6] although their ciphertext is a few hundreds group elements long. Chen and Wee [19] answered an important open question raised by Waters [51] by avoiding the concrete security loss, proportional to the number of adversarial queries, that affected the security reductions of all prior identity-based encryption (IBE) [14,49] schemes based on simple assumptions, including those based on the dual system paradigm [52,39]. The results of [19] also implied the shortest signatures almost tightly related to simple assumptions[1] in the standard model. In the terminology of [19], "almost tight security" refers to reductions where the degradation factor only depends on the security parameter λ, and not on the number q of adversarial queries, which is potentially much larger as it is common to assume $\lambda = 128$ and $q \approx 2^{30}$.

The tighter security results of Chen and Wee [19] overcame an important barrier since, as pointed out in [19], all earlier short signatures based on standard assumptions in the standard model [51,34,32,53,12] suffered a $\Theta(q)$ loss in terms of exact security. On the other hand, the Chen-Wee schemes are less efficient than previous solutions based on similar assumptions [51,39,18,12]. Likewise,

[1] By "simple assumptions," we mean non-interactive (and thus falsifiable [43]) assumptions that can be described using a *constant* number of group elements. In particular, the number of input elements in the description of the assumption does not depend on the number of adversarial queries.

encryption schemes with tight multi-challenge chosen-ciphertext security [31,3] come at the expense of much longer ciphertexts than constructions (e.g., [25]) in the single-challenge setting.[2] In order to exploit concrete security improvements in the choice of parameters, it is desirable to keep schemes as efficient —from both computational and space viewpoints— as their counterparts backed by loose reductions. This paper aims at rendering the constructions and techniques of [31,19] truly competitive with existing signatures and encryption schemes based on simple assumptions in the standard model.

Our Contributions. In this paper, we construct a new public-key encryption scheme with almost tight chosen-ciphertext (IND-CCA2) security in the multi-user, multi-challenge setting [6] under the DLIN assumption. As in the setting of Chen and Wee, the underlying reduction is not as tight as those of [31,3] since we lose a factor of $O(\lambda)$. On the other hand, our construction provides much shorter ciphertexts than previous tightly IND-CCA2-secure systems [31,3] based on the same assumption. Moreover, our security bound does not depend on the number of users or on the number of challenges, so that our scheme can be safely instantiated in environments involving arbitrarily many users encrypting as many ciphertexts as they like.

As a tool for achieving our encryption scheme (and a result of independent interest), we devise a variant of the Chen-Wee signature scheme [19], which has been proved almost tightly secure under the DLIN assumption, with shorter signatures in prime-order groups. Under the DLIN assumption, each signature consists of 6 groups elements, instead of 8 in [19]. Under the K-linear assumption (which is believed weaker than DLIN when $K > 2$), we reduce the signature length of [19] from $4K$ to $2K + 2$ and thus save $\Theta(K)$ group elements.

By combining our technique and the recent non-interactive proof systems of Jutla and Roy [36], we can further shorten our signatures and obtain 5 group elements per signature under the DLIN assumption and $2K + 1$ elements under the K-linear assumption. Our DLIN-based (resp. K-linear-based) system thus improves upon the Chen-Wee constructions [19] by 37% (resp. nearly 50%) in terms of signature length. Under the Symmetric eXternal Diffie-Hellman assumption (namely, the hardness of DDH in $\mathbb{G}$ and $\hat{\mathbb{G}}$ for asymmetric pairings $e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$), the same optimizations yield signatures comprised of only 3 group elements, which only exceeds the length of Waters signatures [51] by one group element. Since the SXDH-based signatures of [19] live in $\mathbb{G}^4$, we also shorten them by one element (or 25%) under the same assumption. Our SXDH-based scheme turns out to yield the shortest known signature with nearly tight security under a simple assumption.

While randomizable in their basic variant, our schemes can be made strongly unforgeable in a direct manner, without any increase of the signature length.

[2] Using a hybrid argument, Bellare, Boldyreva and Micali [6] showed that any CCA2-secure encryption scheme in the single-challenge setting remains secure if the adversary is given arbitrarily many challenge ciphertexts. However, the reduction is linearly affected by the number q of challenge ciphertexts.

In particular, we do not need generic transformations based on chameleon hash functions, such as the one of Boneh *el al.* [15], which tend to lengthen signatures by incorporating the random coins of the chameleon hashing algorithm. Using the SXDH assumption and asymmetric pairings, we thus obtain the same signature length as the CDH-based strongly unforgeable signatures of Boneh, Shen and Waters [15] with the benefit of a much better concrete security (albeit under a stronger assumption).

Then, our signature schemes can be applied to construct a new efficient public-key encryption scheme with almost tight chosen-ciphertext (IND-CCA) security in the multi-user, multi-challenge setting [6]. Indeed, the randomizable signatures described in this paper easily lend themselves to the construction of new unbounded simulation-sound proof systems (where the adversary remains unable to prove false statements after having seen polynomially many simulated proofs for possibly false statements) with almost tight security. In turn, this yields the most efficient constructions, to date, of IND-CCA-secure public-key encryption schemes in the multi-challenge setting. By following the approach of [29,31], we can obtain an almost tightly simulation-sound proof system by showing that either: *(i)* a set of pairing product equations is satisfiable; and *(ii)* committed group elements form a valid signature on the verification key of a one-time signature. In this case, our randomizable signatures are very interesting candidates since they reduce the number of signature components that must appear in committed form. In addition, the specific algebraic properties of our signature scheme make it possible to construct an optimized simulation-extractable proof system that allows proving knowledge of the plaintext using only 62 group elements, which reduces our ciphertexts to only 69 group elements under the DLIN assumption. This dramatically improves upon previous tightly secure constructions based on the same assumption [31,3] which require several hundreds of group elements per ciphertext. Moreover, unlike [3], our system can also be instantiated in asymmetric pairing configurations. We stress that, unlike [42] (which has a loose security reduction), our simulation-sound proof system does not provide constant-size proofs of linear subspace membership. Still, for the specific application of nearly tight CCA-security, our proof system suffices to obtain relatively concise ciphertexts.

Concurrent to our work, Blazy, Kiltz and Pan [11] independently gave different constructions of signature schemes with tight security under the SXDH, DLIN and other simple assumptions. Their technique extends to provide (hierarchical) identity-based encryption schemes. Under the DLIN and SXDH assumption, our optimized signatures are as short as theirs. Our approach bears similiarities with theirs in that each signature can be seen as a NIZK proof that a message authentication code is valid w.r.t. a committed key.

Our Techniques. Underlying our results is a methodology of getting security proofs with a short chain of transitions from actual games to ideal ones. Our constructions build upon a signature scheme of Jutla and Roy [35, Section 5], which is itself inspired by [16, Appendix A.3]. In [35], each signature is a CCA2-secure encryption of the private key, where the message is included in the label [50] of

the ciphertext. The signer also computes a non-interactive zero-knowledge proof that the encrypted value is the private key. The security proof uses the dual system encryption method [52,40,28] and proceeds with a sequence of hybrid games heading for a game where all signatures encrypt a random value while the NIZK proofs are simulated.

While Camenisch *el al.* [16] used Groth-Sahai proofs, Jutla and Roy obtained a better efficiency using *quasi-adaptive* NIZK (QA-NIZK) proofs, i.e., where the common reference string (CRS) may depend on the specific language for which proofs are being generated but a single CRS simulator works for the entire class of languages. For the common task of proving that a vector of n group elements belongs to a linear subspace of rank t, Jutla and Roy [35] gave computationally sound QA-NIZK proofs of length $\Theta(n-t)$ where the Groth-Sahai (GS) techniques entail $\Theta(n+t)$ group elements per proof. They subsequently refined their techniques, reducing the proof's length to a constant [36], regardless of the number of equations or the number of variables. Libert *el al.* [42] independently obtained similar improvements using different techniques.

Our signature schemes rely on the observation that the constant-size QA-NIZK proofs of [42,36] make it possible to encode the label (which contains the message) in a bit-by-bit manner without affecting the signature length. In turn, this allows applying the technique of Chen and Wee [19] so as to avoid the need for q transitions, where q is the number of signing queries. As in the security proof of [19], the signing oracle uses a semi-functional private key which is obtained by shifting a normal private key by a factor consisting of a random function that depends on increasingly many bits of the message in each transition. In the last game, the random function depends on all the message bits, so that the shifting factor is thus totally unpredictable by the adversary.

Our encryption of almost tightly CCA2-secure encryption scheme is based on a modification of the Naor-Yung [45] paradigm due to [26,3]. The latter consists in combining an IND-CPA encryption and a simulation-extractable proof of knowledge of the plaintext. In order to build an optimized simulation-extractable proof, we take advantage of the simple algebraic structure of our signature scheme and its randomizability properties. Our proof system is a simplification of the one in [3] and shows that either: (i) A commitment is an extractable commitment to a function of the encryption exponents; or (ii) Another commitment contained in the proof contains a valid signature on the verfication key of a one-time signature. Our signature scheme allows implementing this very efficiently. Specifically, a real proof used by the encryption algorithm involves a commitment to a pseudo-signature —which can be generated without the signing key— whereas a simulated proof uses a real signature instead of a pseudo-signature. The perfect witness indistinguishability of Groth-Sahai proofs on a NIWI CRS guarantees that the adversary will not be able to distinguish committed pseudo-signatures from real signatures.

2 Background and Definitions

2.1 Hardness Assumptions

We consider groups $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$ of prime-order p endowed with a bilinear map $e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$. In this setting, we rely on the standard Decision Linear assumption, which is a special case of the K-linear assumption for $K = 2$.

Definition 1 ([13]). *The* Decision Linear Problem *(DLIN) in a group $\mathbb{G}$, is to distinguish between the distributions $(g^a, g^b, g^{ac}, g^{bd}, g^{c+d})$ and $(g^a, g^b, g^{ac}, g^{bd}, g^z)$, with $a, b, c, d \xleftarrow{R} \mathbb{Z}_p$, $z \xleftarrow{R} \mathbb{Z}_p$. The Decision Linear assumption asserts the intractability of DLIN for any PPT distinguisher.*

It will sometimes be convenient to use the following assumption, which is implied by DLIN, as observed in [17].

Definition 2. *The* Simultaneous Double Pairing problem *(SDP) in $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$ is, given a tuple of group elements $(\hat{g_z}, \hat{g_r}, \hat{h_z}, \hat{h_u}) \in \hat{\mathbb{G}}^4$, to find a non-trivial triple $(z, r, u) \in \mathbb{G}^3 \backslash \{(1_\mathbb{G}, 1_\mathbb{G}, 1_\mathbb{G})\}$ satisfying the equalities $e(z, \hat{g_z}) \cdot e(r, \hat{g_r}) = 1_{\mathbb{G}_T}$ and $e(z, \hat{h_z}) \cdot e(u, \hat{h_u}) = 1_{\mathbb{G}_T}$.*

2.2 One-Time Linearly Homomorphic Structure-Preserving Signatures

In structure-preserving signatures [5,4], messages and public keys all consist of elements of a group over which a bilinear map $e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$ is efficiently computable. Constructions based on simple assumptions were put forth in [2,3].

Libert *el al.* [41] considered structure-preserving schemes with linear homomorphic properties. This section recalls the one-time linearly homomorphic structure-preserving signature (LHSPS) of [41].

Keygen(λ, n): Given a security parameter λ and the dimension $n \in \mathbb{N}$ of the subspace to be signed, choose bilinear group $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$ of prime order p. Then, choose $\hat{g_z}, \hat{g_r}, \hat{h_z}, \hat{h_u} \xleftarrow{R} \hat{\mathbb{G}}$. For $i = 1$ to n, pick $\chi_i, \gamma_i, \delta_i \xleftarrow{R} \mathbb{Z}_p$ and compute $\hat{g}_i = \hat{g_z}^{\chi_i} \hat{g_r}^{\gamma_i}$, $\hat{h}_i = \hat{h_z}^{\chi_i} \hat{h_u}^{\delta_i}$. The private key is $\mathsf{sk} = \{(\chi_i, \gamma_i, \delta_i)\}_{i=1}^n$ while the public key is $\mathsf{pk} = \big(\hat{g_z},\ \hat{g_r},\ \hat{h_z},\ \hat{h_u},\ \{(\hat{g}_i, \hat{h}_i)\}_{i=1}^n\big) \in \hat{\mathbb{G}}^{2n+4}$.

Sign($\mathsf{sk}, (M_1, \ldots, M_n)$): To sign a vector $(M_1, \ldots, M_n) \in \mathbb{G}^n$ using the key $\mathsf{sk} = \{(\chi_i, \gamma_i, \delta_i)\}_{i=1}^n$, output $\sigma = (z, r, u) \in \mathbb{G}^3$, where $z = \prod_{i=1}^n M_i^{-\chi_i}$, $r = \prod_{i=1}^n M_i^{-\gamma_i}$ and $u = \prod_{i=1}^n M_i^{-\delta_i}$.

SignDerive($\mathsf{pk}, \{(\omega_i, \sigma^{(i)})\}_{i=1}^\ell$): Given pk as well as ℓ tuples $(\omega_i, \sigma^{(i)})$, parse $\sigma^{(i)}$ as $\sigma^{(i)} = \big(z_i, r_i, u_i\big)$ for $i = 1$ to ℓ. Compute and return $\sigma = (z, r, u)$, where $z = \prod_{i=1}^\ell z_i^{\omega_i}$, $r = \prod_{i=1}^\ell r_i^{\omega_i}$, $u = \prod_{i=1}^\ell u_i^{\omega_i}$.

Verify($\mathsf{pk}, \sigma, (M_1, \ldots, M_n)$): Given a signature $\sigma = (z, r, u) \in \mathbb{G}^3$ and a vector $(M_1, \ldots, M_n)$, return 1 if and only if $(M_1, \ldots, M_n) \neq (1_\mathbb{G}, \ldots, 1_\mathbb{G})$ and (z, r, u) satisfy the relations $1_{\mathbb{G}_T} = e(z, \hat{g_z}) \cdot e(r, \hat{g_r}) \cdot \prod_{i=1}^n e(M_i, \hat{g}_i)$, and $1_{\mathbb{G}_T} = e(z, \hat{h_z}) \cdot e(u, \hat{h_u}) \cdot \prod_{i=1}^n e(M_i, \hat{h}_i)$.

The one-time security of the scheme (in the sense of [41]) was proved [41] under the SDP assumption under a tight reduction. In short, the security notion implies the infeasibility of deriving a signature on a vector outside the subspace spanned by the vectors authenticated by the signer. Here, "one-time" security means that a given public key allows signing only one subspace.

3 Shorter Signatures Almost Tightly Related to the DLIN Assumption

This section shows that LHSPS schemes and constant-size QA-NIZK proofs for linear subspaces can be used to construct shorter signatures with nearly optimal reductions under the DLIN assumption.

The scheme builds on ideas used in a signature scheme suggested by Jutla and Roy [35, Section 5], where each signature is a CCA2-secure encryption —using the message to be signed as a label— of the private key augmented with a QA-NIZK proof (as defined in [35]) that the encrypted value is a persistent hidden secret. As in [52,40,28], the security proof uses a sequence of games which gradually moves to a game where all signatures contain an encryption of a random value while the QA-NIZK proofs are simulated. At each step of the transition, increasingly many signatures are generated without using the private key and the CCA2-security of the encryption scheme ensures that this should not affect the adversary's probability to output a signature that does encrypt the private key. In the security proof of [35], the latter approach implies that: *(i)* the number of transitions depends on the number of signing queries; and *(ii)* a CCA2-secure encryption scheme is needed since, at each transition, the reduction has to decrypt the ciphertext contained in the forgery.

Here, our key observation is that, by using a QA-NIZK proof system where the proof length is independent of the dimension of the considered linear subspace, the approach of [35] can be combined with the proof technique of Chen and Wee [19] so as to reduce the number of game transitions while retaining short signatures. In addition, the techniques of [19] allow us to dispense with the need for a CCA2-secure encryption scheme. The security analysis actually departs from that of [35] and rather follows the one of Chen and Wee [19]. The techniques of [35,16,28] argue that, even if the adversary is given signatures where the private key is blinded by a semi-functional component, its forgery will retain the distribution of a normal signature unless some indistinguishability assumption is broken. Here, we follow [19] and blind the outputs of the signing oracle by a random function of increasingly many bits of the message. Instead of using the same argument as in [35], however, we argue that the adversary's forgery will always have the same distribution as the signatures produced by the signing oracle. In the last game of the hybrid sequence, we prove that the adversary cannot retain the same behavior as the signing oracle since the latter's outputs are blinded by a random function of *all* message bits. In order to come up with the same kind of signature as the signing oracle, the adversary would have to predict the value of the random function on the forgery message $M^\star$, which is information-theoretically infeasible.

As in [19], by guessing exactly one bit of the target message, the reduction can efficiently test whether the forgery has the same distribution as outputs of the signing oracle while remaining able to embed a DLIN instance in outputs of signing queries. For L-bit messages, by applying arguments similar to those of [44,19], we need L game transitions to reach a game where each signature encrypts a random —and thus unpredictable— function of the message. As a result, we obtain DLIN-based signatures comprised of only 6 group elements.

Keygen(λ): Choose bilinear groups $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$ of prime order p together with $f, g, h, u_1, u_2 \xleftarrow{R} \mathbb{G}$.

1. For $\ell = 1$ to L, choose $V_{\ell,0}, V_{\ell,1}, W_{\ell,0}, W_{\ell,1} \xleftarrow{R} \mathbb{G}$ to assemble row vectors

$$\boldsymbol{V} = (V_{1,0}, V_{1,1}, \ldots, V_{L,0}, V_{L,1}),\ \boldsymbol{W} = (W_{1,0}, W_{1,1}, \ldots, W_{L,0}, W_{L,1}) \in \mathbb{G}^{2L}\ .$$

2. Define the matrix $\mathbf{M} = \big(M_{i,j}\big)_{i,j} \in \mathbb{G}^{(4L+2)\times(4L+3)}$ given by

$$\mathbf{M} = \left(\begin{array}{c|c|c|c|c} \boldsymbol{V}^\top & \mathbf{Id}_{f,2L} & \mathbf{1}^{2L\times 2L} & \mathbf{1}^{2L\times 1} & \mathbf{1}^{2L\times 1} \\ \hline \boldsymbol{W}^\top & \mathbf{1}^{2L\times 2L} & \mathbf{Id}_{h,2L} & \mathbf{1}^{2L\times 1} & \mathbf{1}^{2L\times 1} \\ \hline g & \mathbf{1}^{1\times 2L} & \mathbf{1}^{1\times 2L} & u_1 & 1 \\ \hline g & \mathbf{1}^{1\times 2L} & \mathbf{1}^{1\times 2L} & 1 & u_2 \end{array}\right) \quad (1)$$

with $\mathbf{Id}_{f,2L} = f^{\mathbf{I}_{2L}} \in \mathbb{G}^{2L\times 2L}$, $\mathbf{Id}_{h,2L} = h^{\mathbf{I}_{2L}} \in \mathbb{G}^{2L\times 2L}$, and where $\mathbf{I}_{2L} \in \mathbb{Z}_p^{2L\times 2L}$ is the identity matrix.

3. Generate a key pair $(\mathsf{sk}_{hsps}, \mathsf{pk}_{hsps})$ for the one-time linearly homomorphic signature of Section 2.2 in order to sign vectors of dimension $n = 4L+3$. Let $\mathsf{sk}_{hsps} = \{(\chi_i, \gamma_i, \delta_i)\}_{i=1}^{4L+3}$ be the private key, of which the corresponding public key is $\mathsf{pk}_{hsps} = \big(\hat{g_z},\ \hat{g_r},\ \hat{h_z},\ \hat{h_u},\ \{(\hat{g}_i, \hat{h}_i)\}_{i=1}^{4L+3}\big)$.
4. Using $\mathsf{sk}_{hsps} = \{\chi_i, \gamma_i, \delta_i\}_{i=1}^{4L+3}$, generate one-time homomorphic signatures $\{(Z_j, R_j, U_j)\}_{j=1}^{4L+2}$ on the rows $\boldsymbol{M}_j = (M_{j,1}, \ldots, M_{j,4L+3})$ of $\mathbf{M}$. For each $j \in \{1, \ldots, 4L+2\}$, these are obtained as

$$(Z_j, R_j, U_j) = \left(\prod_{i=1}^{4L+3} M_{j,i}^{-\chi_i},\ \prod_{i=1}^{4L+3} M_{j,i}^{-\gamma_i},\ \prod_{i=1}^{4L+3} M_{j,i}^{-\delta_i}\right),$$

and, as part of the common reference string for the QA-NIZK proof system of [42], they will be included in the public key.

5. Choose $\omega_1, \omega_2 \xleftarrow{R} \mathbb{Z}_p$ and compute $\Omega_1 = u_1^{\omega_1} \in \mathbb{G}$, $\Omega_2 = u_2^{\omega_2} \in \mathbb{G}$.

The private key consists of $SK = (\omega_1, \omega_2)$ and the public key is

$$PK = \Big(f,\ g,\ h,\ u_1,\ u_2,\ \Omega_1,\ \Omega_2,\ \boldsymbol{V},\ \boldsymbol{W},\ \mathsf{pk}_{hsps} = \big(\hat{g_z},\ \hat{g_r},\ \hat{h_z},\ \hat{h_u},\ \{(\hat{g}_i, \hat{h}_i)\}_{i=1}^{4L+3}\big), \{(Z_j, R_j, U_j)\}_{j=1}^{4L+2}\Big)\ .$$

Sign($\boldsymbol{SK}, \boldsymbol{M}$): Given $M = M[1] \ldots M[L] \in \{0,1\}^L$ and $SK = (\omega_1, \omega_2)$:

1. Choose $r, s \xleftarrow{R} \mathbb{Z}_p$ and compute

$$\sigma_1 = g^{\omega_1+\omega_2} \cdot H(\boldsymbol{V}, M)^r \cdot H(\boldsymbol{W}, M)^s\,, \quad \sigma_2 = f^r\,, \quad \sigma_3 = h^s\,, \tag{2}$$

where $H(\boldsymbol{V}, M) = \prod_{\ell=1}^{L} V_{\ell,M[\ell]}$ and $H(\boldsymbol{W}, M) = \prod_{\ell=1}^{L} W_{\ell,M[\ell]}$.

2. Using $\{(Z_j, R_j, U_j)\}_{j=1}^{4L+2}$, derive a one-time homomorphic signature (Z, R, U) which will serve as a non-interactive argument showing that the vector

$$(\sigma_1, \sigma_2^{1-M[1]}, \sigma_2^{M[1]}, \ldots, \sigma_2^{1-M[L]}, \sigma_2^{M[L]}, \sigma_3^{1-M[1]}, \sigma_3^{M[1]}, \\ \ldots, \sigma_3^{1-M[L]}, \sigma_3^{M[L]}, \Omega_1, \Omega_2) \tag{3}$$

is in the row space of $\mathbf{M}$, which ensures that $(\sigma_1, \sigma_2, \sigma_3)$ is of the form (2). Namely, compute

$$\begin{cases} Z = Z_{4L+1}^{\omega_1} \cdot Z_{4L+2}^{\omega_2} \cdot \prod_{i=1}^{L} \left(Z_{2i-\overline{M[i]}}^{r} \cdot Z_{2L+2i-\overline{M[i]}}^{s}\right) \\ R = R_{4L+1}^{\omega_1} \cdot R_{4L+2}^{\omega_2} \cdot \prod_{i=1}^{L} \left(R_{2i-\overline{M[i]}}^{r} \cdot R_{2L+2i-\overline{M[i]}}^{s}\right) \\ U = U_{4L+1}^{\omega_1} \cdot U_{4L+2}^{\omega_2} \cdot \prod_{i=1}^{L} \left(U_{2i-\overline{M[i]}}^{r} \cdot U_{2L+2i-\overline{M[i]}}^{s}\right). \end{cases} \tag{4}$$

Return the signature $\sigma = \big(\sigma_1, \sigma_2, \sigma_3, Z, R, U\big) \in \mathbb{G}^6$.

Verify($\boldsymbol{PK}, \boldsymbol{M}, \boldsymbol{\sigma}$): Parse σ as $\big(\sigma_1, \sigma_2, \sigma_3, Z, R, U\big) \in \mathbb{G}^6$ and return 1 iff

$$e(Z, \hat{g_z}) \cdot e(R, \hat{g_r}) = e(\sigma_1, \hat{g}_1)^{-1} \cdot e(\sigma_2, \prod_{i=1}^{L} \hat{g}_{2i+M[i]})^{-1} \\ \cdot e(\sigma_3, \prod_{i=1}^{L} \hat{g}_{2L+2i+M[i]})^{-1} \cdot e(\Omega_1, \hat{g}_{4L+2})^{-1} \cdot e(\Omega_2, \hat{g}_{4L+3})^{-1}$$

$$e(Z, \hat{h_z}) \cdot e(U, \hat{h_u}) = e(\sigma_1, \hat{h_1})^{-1} \cdot e(\sigma_2, \prod_{i=1}^{L} \hat{h}_{2i+M[i]})^{-1} \\ \cdot e(\sigma_3, \prod_{i=1}^{L} \hat{h}_{2L+2i+M[i]})^{-1} \cdot e(\Omega_1, \hat{h}_{4L+2})^{-1} \cdot e(\Omega_2, \hat{h}_{4L+3})^{-1}\,.$$

Each signature consists of 6 elements of $\mathbb{G}$, which is as short as Lewko's DLIN-based signatures [39, Section 4.3] where the security proof incurs a security loss proportional to the number of signing queries. Under the same assumption, the Chen-Wee signatures [19] require 8 group elements.

We emphasize that our security proof allows using any QA-NIZK proof system for linear subspaces and not only the one of [42] (which we used in order to keep the description as simple and self-contained as possible). Our constructions can thus be optimized if we replace the QA-NIZK proof system of [42] —which entails $K+1$ group elements under the K-LIN assumption— by those recently suggested by Jutla and Roy, where only K group elements per proof are needed.

Under the DLIN (resp. K-linear) assumption, each signature is only comprised of 5 (resp. $2K+1$) group elements. We thus shorten signatures by 37% under the DLIN assumption. Under the K-Linear assumption, our improvement is more dramatic since, when K increases, our signatures become almost 50% shorter as we reduce the signature length of [19] from $4K$ to $2K+1$.

Under the SXDH assumption (namely, the 1-linear assumption), a direct adaptation of the above scheme entails 4 elements of $\mathbb{G}$ per signature, which is as long as [19]. However, as explained in the full version of the paper, the QA-NIZK proof system of Jutla and Roy [36] can supersede the one of [42] since, under the SXDH assumption, it only requires one group element per proof, instead of two in [42]. The signature thus becomes a triple $(\sigma_1, \sigma_2, Z) = (u^{\omega} \cdot H(\boldsymbol{V}, M)^r, f^r, Z)$, where Z is a QA-NIZK proof of well-formedness for (σ_1, σ_2).

Theorem 1. *The above signature scheme provides existential unforgeability under chosen-message attacks if the DLIN assumption holds in $\mathbb{G}$ and $\hat{\mathbb{G}}$. For L-bit messages, for any adversary $\mathcal{A}$, there exist DLIN distinguishers $\mathcal{B}$ and $\mathcal{B}'$ in $\hat{\mathbb{G}}$ and $\mathbb{G}$ such that $\mathbf{Adv}_{\mathcal{A}}(\lambda) \leq \mathbf{Adv}^{\mathrm{DLIN}}_{\mathcal{B}}(\lambda) + 2 \cdot L \cdot \mathbf{Adv}^{\mathrm{DLIN}}_{\mathcal{B}'}(\lambda) + \frac{2}{p}$ and with running times $t_{\mathcal{B}}, t_{\mathcal{B}'} \leq t_{\mathcal{A}} + q \cdot \mathsf{poly}(\lambda, L)$.*

Proof. The proof considers several kinds of valid signatures.

Type A signatures are produced by the real signing algorithm. Namely, if $\boldsymbol{V} = f^{\boldsymbol{v}}$ and $\boldsymbol{W} = h^{\boldsymbol{w}}$ for vectors $\boldsymbol{v} = (v_{1,0}, v_{1,1}, \ldots, v_{L,0}, v_{L,1}) \in \mathbb{Z}_p^{2L}$, $\boldsymbol{w} = (w_{1,0}, w_{1,1}, \ldots, w_{L,0}, w_{L,1}) \in \mathbb{Z}_p^{2L}$ and if we define $F(\boldsymbol{v}, M) = \sum_{\ell=1}^{L} v_{\ell, M[\ell]}$ and $F(\boldsymbol{w}, M) = \sum_{\ell=1}^{L} w_{\ell, M[\ell]}$, these signatures are such that

$$g^{\omega_1+\omega_2} = \sigma_1 \cdot \sigma_2^{-F(\boldsymbol{v},M)} \cdot \sigma_3^{-F(\boldsymbol{w},M)}$$

and (Z, R, U) is a valid linearly homomorphic signature on the vector (3).

Type B signatures are valid signatures that are not Type A signatures. These are of the form

$$\sigma_1 = g^{\omega_1+\omega_2+\tau} \cdot H(\boldsymbol{V}, M)^r \cdot H(\boldsymbol{W}, M)^s\,, \qquad \sigma_2 = f^r\,, \qquad \sigma_3 = h^s\,,$$

for some $\tau \in_R \mathbb{Z}_p$, $r, s \in_R \mathbb{Z}_p$, and

$$\begin{cases} Z = g^{-\tau \cdot \chi_1} \cdot Z_{4L+1}^{\omega_1} \cdot Z_{4L+2}^{\omega_2} \cdot \prod_{i=1}^{L} \left(Z^r_{2i-\overline{M[i]}} \cdot Z^s_{2L+2i-\overline{M[i]}} \right) \\ R = g^{-\tau \cdot \gamma_1} \cdot R_{4L+1}^{\omega_1} \cdot R_{4L+2}^{\omega_2} \cdot \prod_{i=1}^{L} \left(R^r_{2i-\overline{M[i]}} \cdot R^s_{2L+2i-\overline{M[i]}} \right) \\ U = g^{-\tau \cdot \delta_1} \cdot U_{4L+1}^{\omega_1} \cdot U_{4L+2}^{\omega_2} \cdot \prod_{i=1}^{L} \left(U^r_{2i-\overline{M[i]}} \cdot U^s_{2L+2i-\overline{M[i]}} \right) \end{cases}.$$

Note that Type B signatures also satisfy the verification algorithm since (Z, R, U) is a valid homomorphic signature on the vector (3). The term g^{τ} will be henceforth called the *semi-functional component* of the signature. Type B signatures include the following sub-classes.

Type B-k signatures ($1 \leq k \leq L$) are generated by choosing $r, s \xleftarrow{R} \mathbb{Z}_p$ and setting

$$\sigma_1 = g^{\omega_1+\omega_2} \cdot R_k(M_{|_k}) \cdot H(\boldsymbol{V}, M)^r \cdot H(\boldsymbol{W}, M)^s\,, \quad \sigma_2 = f^r\,, \quad \sigma_3 = h^s\,,$$

with $H(\boldsymbol{V}, M) = \prod_{\ell=1}^{L} V_{\ell,M[\ell]}$ and where $H(\boldsymbol{W}, M) = \prod_{\ell=1}^{L} W_{\ell,M[\ell]}$ and $R_k\colon \{0,1\}^k \to \mathbb{G}, M_{|_k} \mapsto R_k(M_{|_k})$ is a random function that depends on the first k bits of M. The (Z, R, U) components are simulated QA-NIZK proofs of subspace membership. They are obtained using $\{(\chi_i, \gamma_i, \delta_i)\}_{i=1}^{4L+3}$ to generate a homomorphic signature on the vector (3) by computing

$$\begin{cases} Z = \sigma_1^{-\chi_1} \cdot \sigma_2^{-\sum_{i=1}^{L} \chi_{2i+M[i]}} \cdot \sigma_3^{-\sum_{i=1}^{L} \chi_{2L+2i+M[i]}} \cdot \Omega_1^{-\chi_{4L+2}} \cdot \Omega_2^{-\chi_{4L+3}} \\ R = \sigma_1^{-\gamma_1} \cdot \sigma_2^{-\sum_{i=1}^{L} \sigma_{2i+M[i]}} \cdot \sigma_3^{-\sum_{i=1}^{L} \gamma_{2L+2i+M[i]}} \cdot \Omega_1^{-\gamma_{4L+2}} \cdot \Omega_2^{-\gamma_{4L+3}} \\ U = \sigma_1^{-\delta_1} \cdot \sigma_2^{-\sum_{i=1}^{L} \delta_{2i+M[i]}} \cdot \sigma_3^{-\sum_{i=1}^{L} \delta_{2L+2i+M[i]}} \cdot \Omega_1^{-\delta_{4L+2}} \cdot \Omega_2^{-\delta_{4L+3}} \end{cases}.$$

To prove the result, we consider the following sequence of games. For each i, we call S_i the event that the adversary wins in Game i. We also define E_i to be the event that, in Game i, $\mathcal{A}$'s forgery has the same type as the signatures it observes. Namely, if $\mathcal{A}$ obtains a Type A (resp. Type B-k) signature at each query, it should output a Type A (resp. Type B-k) forgery.

Game 0: This game is the real game. Namely, the adversary obtains Type A signatures at each signing query. At the end of the game, however, the challenger $\mathcal{B}$ checks if $\mathcal{A}$'s forgery is a Type A signature and we define E_0 the event that the forgery $\sigma^\star$ is a Type A forgery. We obviously have $\Pr[S_0] = \Pr[S_0 \wedge E_0] + \Pr[S_0 \wedge \neg E_0]$. Lemma 1 shows that, if the DLIN assumption holds in $\hat{\mathbb{G}}$, the adversary can only output a Type B signature with negligible probability. We have $\Pr[S_0 \wedge \neg E_0] \leq \mathbf{Adv}^{\mathrm{DLIN}}_{\hat{\mathbb{G}}}(\lambda) + 1/p$. We are thus left with the task of bounding $\Pr[S_0 \wedge E_0]$. To this end, we proceed using a sequence of L games.

Game 1: This game is identical to Game 0 with the difference that, at each signing query, the signature components (Z, R, U) are obtained as simulated QA-NIZK proofs of linear subspace membership. Namely, instead of computing (Z, R, U) as per (4), the challenger uses $\{\chi_i, \gamma_i, \delta_i\}_{i=1}^{4L+3}$ to compute (Z, R, U) as a one-time linearly homomorphic signature on the vector (3). Clearly (Z, R, U) retains the same distribution as in Game 0, so that $\mathcal{A}$'s view remains unchanged. We have $\Pr[S_1 \wedge E_1] = \Pr[S_0 \wedge E_0]$, where E_1 is the counterpart of event E_0 in Game 1.

Game 2.k ($1 \leq k \leq L$): In Game 2.k, all signing queries are answered by returning Type B-k signatures. For each k, we call $E_{2.k}$ the event that $\mathcal{A}$ outputs a Type B-k forgery in Game 2.k. Lemma 2 provides evidence that Game 2.1 is computationally indistinguishable from Game 1 under the DLIN assumption in $\mathbb{G}$: we have $|\Pr[S_{2.1} \wedge E_{2.1}] - \Pr[S_1 \wedge E_1]| \leq 2 \cdot \mathbf{Adv}^{\mathrm{DLIN}}_{\mathbb{G}}(\lambda)$. In the full version of the paper, we show that, under the DLIN assumption in $\mathbb{G}$, the probability of $\mathcal{A}$'s forgery to be of the same type as the outputs of signing queries is about the same in Game 2.k and in Game 2.$(k-1)$. We thus have $|\Pr[S_{2.k} \wedge E_{2.k}] - \Pr[S_{2.(k-1)} \wedge E_{2.(k-1)}]| \leq 2 \cdot \mathbf{Adv}^{\mathrm{DLIN}}_{\mathbb{G}}(\lambda)$.

When we reach Game 2.L, we know that $|\Pr[S_{2.L} \wedge E_{2.L}] - \Pr[S_{2.0} \wedge E_{2.0}]| \leq 2 \cdot L \cdot \mathbf{Adv}_{\mathbb{G}}^{\mathrm{DLIN}}(\lambda)$ by the triangle inequality. However, in Game 2.L, it is easy to prove that, even though $\mathcal{A}$ only obtains Type B-k signatures throughout the game, its probability to output a Type B-k forgery is negligible even with an unbounded computational power. Indeed, a legitimate adversary that outputs a forgery on a new message $M^\star$ has no information on $R_L(M^\star)$. Hence, it can only produce a Type B-k forgery by pure chance and we thus have $\Pr[S_{2.L} \wedge E_{2.L}] \leq 1/p$. □

Lemma 1. *In Game* 0*, any PPT adversary outputting a Type B forgery with non-negligible probability implies an algorithm breaking the DLIN assumption in* $\hat{\mathbb{G}}$ *with nearly the same advantage.* (The proof is in the full version of the paper).

Lemma 2. *If the DLIN assumption holds in* $\mathbb{G}$*,* $\mathcal{A}$*'s probability to output a Type B-*1 *signature in Game* 2.1 *is about the same as its probability to output a Type A signature in Game* 1*.*

Proof. Let us assume that events $S_{2.1} \wedge E_{2.1}$ and $S_1 \wedge E_1$ occur with noticeably different probabilities in Game 2.1 and Game 1, respectively. We construct a DLIN distinguisher $\mathcal{B}$ in $\mathbb{G}$. Our algorithm $\mathcal{B}$ takes as input (f, g, h, f^a, h^b, T) with the task of deciding if $T = g^{a+b}$ or $T \in_R \mathbb{G}$. Similarly to [19, Lemma 6], the reduction $\mathcal{B}$ uses the random self-reducibility of DLIN to build q tuples $(F_j = f^{a_j}, H_j = h^{b_j}, T_j)$ such that, for each $j \in \{1, \ldots, q\}$, we have

$$T_j = \begin{cases} g^{a_j + b_j} & \text{if } T = g^{a+b} \\ g^{a_j + b_j + \tau_0} & \text{if } T \in_R \mathbb{G} \end{cases}$$

for some $\tau_0 \in_R \mathbb{Z}_p$. This is done by picking $\rho_0 \xleftarrow{R} \mathbb{Z}_p$ and $\rho_{a_j}, \rho_{b_j} \xleftarrow{R} \mathbb{Z}_p$, for $j \in \{1, \ldots, q\}$, and setting

$$(F_j, H_j, T_j) = \left((f^a)^{\rho_0} \cdot f^{\rho_{a_j}}, (h^b)^{\rho_0} \cdot h^{\rho_{b_j}}, T^{\rho_0} \cdot g^{\rho_{a_j} + \rho_{b_j}}\right), \quad \forall j \in \{1, \ldots, q\} \ .$$

In addition, $\mathcal{B}$ generates an extra tuple $(u_1, u_2, \Omega_1, \Omega_2) \in \mathbb{G}^4$ by choosing random exponents $\alpha_{u,1}, \alpha_{u,2} \xleftarrow{R} \mathbb{Z}_p$ and setting

$$u_1 = f^{\alpha_{u,1}}, \qquad u_2 = h^{\alpha_{u,2}}, \qquad \Omega_1 = (f^a)^{\alpha_{u,1}}, \qquad \Omega_2 = (h^b)^{\alpha_{u,2}} \ .$$

Before generating the public key of the scheme, $\mathcal{B}$ flips a coin $b^\dagger \xleftarrow{R} \{0,1\}$ hoping that the first bit of the target message $M^\star = M[1]^\star \ldots M[L]^\star \in \{0,1\}^L$ will coincide with $b^\dagger$. To construct PK, $\mathcal{B}$ chooses $\boldsymbol{\alpha} = (\alpha_{1,0}, \alpha_{1,1}, \ldots, \alpha_{L,0}, \alpha_{L,1}) \xleftarrow{R} \mathbb{Z}_p^{2L}$, $\boldsymbol{\beta} = (\beta_{1,0}, \beta_{1,1}, \ldots, \beta_{L,0}, \beta_{L,1}) \xleftarrow{R} \mathbb{Z}_p^{2L}$ and $\zeta \xleftarrow{R} \mathbb{Z}_p$. It defines the vectors $\boldsymbol{V} = (V_{1,0}, V_{1,1}, \ldots, V_{L,0}, V_{L,1})$, $\boldsymbol{W} = (W_{1,0}, W_{1,1}, \ldots, W_{L,0}, W_{L,1})$ as

$$\begin{cases} (V_{\ell,0}, V_{\ell,1}) = (f^{\alpha_{\ell,0}}, f^{\alpha_{\ell,1}}), \ (W_{\ell,0}, W_{\ell,1}) = (h^{\beta_{\ell,0}}, h^{\beta_{\ell,1}}) & \text{if } \ell \neq 1, \\ (V_{1,1-b^\dagger}, V_{1,b^\dagger}) = (f^{\alpha_{1,1-b^\dagger}} \cdot g^\zeta, f^{\alpha_{1,b^\dagger}}), \ (W_{1,1-b^\dagger}, W_{1,b^\dagger}) = (h^{\beta_{1,1-b^\dagger}} \cdot g^\zeta, h^{\beta_{1,b^\dagger}}) \ . \end{cases}$$

The rest of PK, including $(\mathsf{sk}_{hsps}, \mathsf{pk}_{hsps})$ and $\{(Z_i, R_i, U_i)\}_{i=1}^{4L+2}$, is generated as in the real setup. The adversary $\mathcal{A}$ is run on input of

$$PK = \Big(f,\ g,\ h,\ u_1,\ u_2,\ \Omega_1 = {u_1}^a,\ \Omega_2 = {u_2}^b,\ \boldsymbol{V},\ \boldsymbol{W},$$
$$\mathsf{pk}_{hsps} = \big(\hat{g_z},\ \hat{g_r},\ \hat{h_z},\ \hat{h_u},\ \{(\hat{g}_i, \hat{h}_i)\}_{i=1}^{4L+3}\big),\ \{(\hat{Z}_j, \hat{R}_j, \hat{U}_j)\}_{j=1}^{4L+2}\Big)$$

and $\mathcal{B}$ keeps $(\{\chi_i, \gamma_i, \delta_i\}_{i=1}^{4L+3})$ to itself. Note that $a, b \in \mathbb{Z}_p$ are part of the original DLIN instance and are not available to $\mathcal{B}$. However, $\mathcal{B}$ will use the challenge value T —which is either g^{a+b} or a random element of $\mathbb{G}$— to answer signing queries.

During the game, signing queries are answered as follows. In order to handle the j-th signing query $M^j = M[1]^j \dots M[L]^j \in \{0,1\}^L$, the answer of $\mathcal{B}$ depends on the first bit $M[1]^j$ of M^j. Specifically, $\mathcal{B}$ considers the following cases.

– If $M[1]^j = b^\dagger$, $\mathcal{B}$ chooses $r, s \xleftarrow{R} \mathbb{Z}_p$ and sets

$$\sigma_1 = T \cdot H(\boldsymbol{V}, M)^r \cdot H(\boldsymbol{W}, M)^s\,, \qquad \sigma_2 = f^r\,, \qquad \sigma_3 = h^s\,,$$

where $H(\boldsymbol{V}, M) = \prod_{\ell=1}^{L} V_{\ell, M[\ell]}$ and $H(\boldsymbol{W}, M) = \prod_{\ell=1}^{L} W_{\ell, M[\ell]}$. The (Z, R, U) components of the private key are computed by generating a homomorphic structure-preserving signature on the vector

$$(\sigma_1, \sigma_2^{1-M[1]}, \sigma_2^{M[1]}, \dots, \sigma_2^{1-M[L]}, \sigma_2^{M[L]}, \sigma_3^{1-M[1]}, \sigma_3^{M[1]}, \dots, \sigma_3^{1-M[L]}, \sigma_3^{M[L]}, \Omega_1, \Omega_2)\,,$$

by computing

$$\begin{cases} Z = \sigma_1^{-\chi_1} \cdot \sigma_2^{-\sum_{i=1}^{L} \chi_{2i+M[i]}} \cdot \sigma_3^{-\sum_{i=1}^{L} \chi_{2L+2i+M[i]}} \cdot \Omega_1^{-\chi_{4L+2}} \cdot \Omega_2^{-\chi_{4L+3}} \\ R = \sigma_1^{-\gamma_1} \cdot \sigma_2^{-\sum_{i=1}^{L} \gamma_{2i+M[i]}} \cdot \sigma_3^{-\sum_{i=1}^{L} \gamma_{2L+2i+M[i]}} \cdot \Omega_1^{-\gamma_{4L+2}} \cdot \Omega_2^{-\gamma_{4L+3}} \\ U = \sigma_1^{-\delta_1} \cdot \sigma_2^{-\sum_{i=1}^{L} \delta_{2i+M[i]}} \cdot \sigma_3^{-\sum_{i=1}^{L} \delta_{2L+2i+M[i]}} \cdot \Omega_1^{-\delta_{4L+2}} \cdot \Omega_2^{-\delta_{4L+3}} \end{cases} \tag{5}$$

Note that, if $T = g^{a+b+\tau}$ for some $\tau \in_R \mathbb{Z}_p$, (Z, R, U) can be written

$$\begin{cases} Z = g^{-\chi_1 \cdot \tau} \cdot Z_{4L+1}^a \cdot Z_{4L+2}^b \cdot \prod_{i=1}^{L} \left(Z_{2i-\overline{M[i]}}^r \cdot Z_{2L+2i-\overline{M[i]}}^s\right) \\ R = g^{-\gamma_1 \cdot \tau} \cdot R_{4L+1}^a \cdot R_{4L+2}^b \cdot \prod_{i=1}^{L} \left(R_{2i-\overline{M[i]}}^r \cdot R_{2L+2i-\overline{M[i]}}^s\right) \\ U = g^{-\delta_1 \cdot \tau} \cdot U_{4L+1}^a \cdot U_{4L+2}^b \cdot \prod_{i=1}^{L} \left(U_{2i-\overline{M[i]}}^r \cdot U_{2L+2i-\overline{M[i]}}^s\right) \end{cases}.$$

We observe that $(\sigma_1, \sigma_2, \sigma_3, Z, R, U)$ matches the distribution of signatures in both Game 2.1 if $\tau \neq 0$ and Game 1 if $\tau = 0$. Indeed, in the former case, we implicitly define the constant function $R_0(\varepsilon) = g^\tau$ and define the function R_1 so that $R_1(b^\dagger) = R_0(\varepsilon)$.

– If $M[1]^j = 1 - b^\dagger$, $\mathcal{B}$ implicitly defines

$$R_1(M_{|_1}^j) = R_1(1 - b^\dagger) = \begin{cases} R_0(\varepsilon) \cdot g^{\zeta \cdot \tau_0} & \text{if } T \in_R \mathbb{G} \\ 1 & \text{if } T = g^{a+b} \end{cases}.$$

Namely, $\mathcal{B}$ uses the j-th tuple (F_j, H_j, T_j) to set

$$\sigma_1 = T \cdot F_j^{\sum_{\ell=1}^{L} \alpha_{\ell,M[\ell]}} \cdot H_j^{\sum_{\ell=1}^{L} \beta_{\ell,M[\ell]}} \cdot T_j^{\zeta}\ ,\ \sigma_2 = F_j = f^{a_j}\ ,\ \sigma_3 = H_j = h^{b_j}\ .$$

If $T = g^{a+b}$ (and thus $T_j = g^{a_j+b_j}$), this implicitly defines σ_1 as the product $\sigma_1 = g^{a+b} \cdot H(\boldsymbol{V}, M^j)^{a_j} \cdot H(\boldsymbol{W}, M^j)^{b_j}$, so that $(\sigma_1, \sigma_2, \sigma_3)$ has the same distribution as in Game 1. If $T = g^{a+b+\tau}$ (so that $T_j = g^{a_j+b_j+\tau_0}$), we have

$$\sigma_1 = g^{a+b} \cdot R_1(M_{|_1}^j) \cdot H(\boldsymbol{V}, M^j)^{a_j} \cdot H(\boldsymbol{W}, M^j)^{b_j}\ ,$$

since $R_1(M_{|_1}^j) = R_0(\varepsilon) \cdot g^{\zeta \cdot \tau_0}$, which is distributed as in Game 2.1. In either case, (Z, R, U) are computed using $\mathsf{sk}_{hsps} = \{(\chi_i, \gamma_i, \delta_i)\}_{i=1}^{4L+3}$ as in the previous case (i.e., as per (5)).

In the forgery stage, the adversary $\mathcal{A}$ outputs a new message $M^\star$ and a signature $\sigma^\star = (\sigma_1^\star, \sigma_2^\star, \sigma_3^\star, Z^\star, R^\star, U^\star)$. Our distinguisher $\mathcal{B}$ must determine if $\sigma^\star$ has the same type as the outputs of the simulated signing oracle. At this point, algorithm $\mathcal{B}$ halts and outputs a random bit if $M[1]^\star \neq b^\dagger$. Otherwise, $\mathcal{B}$ can compute $F(\boldsymbol{v}, M^\star) = \sum_{\ell=1}^{L} \alpha_{\ell,M[\ell]^\star}$ and $F(\boldsymbol{w}, M^\star) = \sum_{\ell=1}^{L} \beta_{\ell,M[\ell]^\star}$, which yields $\eta^\star = \sigma_1^\star \cdot {\sigma_2^\star}^{-F(\boldsymbol{v},M^\star)} \cdot {\sigma_3^\star}^{-F(\boldsymbol{w},M^\star)}$. If $\eta^\star = T$, $\mathcal{B}$ considers $(\sigma^\star, M^\star)$ as a forgery of the same type as outputs of the signing oracle and returns 1. Recall that $R_0(\varepsilon) = T/g^{a+b}$, so that $\sigma^\star$ matches the output distribution of the signing oracle in both Game 1 and Game 2.1. Otherwise, $\mathcal{B}$ decides that $\sigma^\star$ has a different distribution than signatures produced by the signing oracle and outputs 0. If the difference between $\mathcal{A}$'s probability to output the same kind of signatures as the signing oracle in Games 2.1 and 2.1 is ϵ, then $\mathcal{B}$'s advantage as a DLIN distinguisher is at least $\epsilon/2$ since $b^\dagger \in \{0, 1\}$ is independent of $\mathcal{A}$'s view. □

We remark that, while its signatures are randomizable, the system can be made strongly unforgeable in a simple manner and without increasing the signature length. In particular, we do not need a chameleon-hash-function-based transformation such as [15]. Using the QA-NIZK proofs of [36], we thus obtain strongly unforgeable signatures based on the SXDH assumption which are short as those of Boneh, Shen and Waters [15] with a nearly tight reduction. The details are given in the full version of the paper.

4 Almost Tightly CCA-Secure Encryption with Shorter Ciphertexts

Equipped with our signature scheme, we now present a public-key encryption scheme whose IND-CCA2 security in the multi-challenge-multi-user setting is almost tightly related to the DLIN assumption. Like [31], our scheme instantiates a variant of the Naor-Yung paradigm using Groth-Sahai proofs and the cryptosystem of Boneh, Boyen and Shacham (BBS) [13].

The construction can be seen as an instantiation of a technique suggested by Dodis *el al.* [26] as a modification of the Naor-Yung paradigm, where only one IND-CPA secure encryption suffices (instead of two in [45,47]) if it is accompanied with a NIZK proof of knowledge of the plaintext that is simulation-extractable (and not only simulation-sound). In [3], Abe *el al.* used a simulation-extractable proof system showing that either: (i) The IND-CPA encryption scheme encrypts the message containted in an extractable commitment; (ii) Another commitment included in the proof is a valid signature on the verification key VK of a one-time signature. Here, we show that, if this simulation-extractable proof system is combined with the BBS cryptosystem, it can be simplified by removing the commitment to the message and the proof that this commitment contains the encrypted plaintext. The reason is that, in each simulation-extractable proof, the commitments to the encryption exponents suffice to guarantee the extractability of the plaintext.

While our reduction is not quite as tight as in the results of [31,3] since we lose a factor of $\Theta(\lambda)$, our scheme is much more space-efficient as the ciphertext overhead reduces to 68 group elements. As a comparison, the most efficient solution of [3] incurs 398 group elements per ciphertext.

For simplicity, the description below uses symmetric pairings $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ (i.e., $\mathbb{G} = \hat{\mathbb{G}}$) but extensions to asymmetric pairings are possible.

Par-Gen(λ): Choose bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ with generators $g, f, h \xleftarrow{R} \mathbb{G}$. Define common public parameters $\mathsf{par} = ((\mathbb{G}, \mathbb{G}_T), g, f, h)$.

Keygen(par): Parse par as $\big((\mathbb{G}, \mathbb{G}_T), g, f, h\big)$ and conduct the following steps.

1. Choose random exponents $x_1, y_1 \xleftarrow{R} \mathbb{Z}_p$ and set $f_1 = g^{x_1}$, $h_1 = g^{y_1}$.
2. Choose a strongly unforgeable one-time signature $\Sigma = (\mathcal{G}, \mathcal{S}, \mathcal{V})$ with verification keys of length $L \in \mathsf{poly}(\lambda)$.
3. For $\ell = 1$ to L, choose $V_{\ell,0}, V_{\ell,1}, W_{\ell,0}, W_{\ell,1} \xleftarrow{R} \mathbb{G}$ to assemble row vectors

$$\boldsymbol{V} = (V_{1,0}, V_{1,1}, \ldots, V_{L,0}, V_{L,1}),$$
$$\boldsymbol{W} = (W_{1,0}, W_{1,1}, \ldots, W_{L,0}, W_{L,1}) \in \mathbb{G}^{2L} .$$

4. Choose $\omega_1, \omega_2 \xleftarrow{R} \mathbb{Z}_p$, $u_1, u_2 \xleftarrow{R} \mathbb{G}$, and compute $\Omega_1 = u_1^{\omega_1}$, $\Omega_2 = u_2^{\omega_2}$.
5. Define the matrix $\mathbf{M} = \big(M_{i,j}\big)_{i,j} \in \mathbb{G}^{(4L+2)\times(4L+3)}$ as

$$\big(M_{i,j}\big)_{i,j} = \left(\begin{array}{c|c|c|c|c} \boldsymbol{V}^\top & \mathbf{Id}_{f,2L} & \mathbf{1}^{2L\times 2L} & \mathbf{1}^{2L\times 1} & \mathbf{1}^{2L\times 1} \\ \hline \boldsymbol{W}^\top & \mathbf{1}^{2L\times 2L} & \mathbf{Id}_{h,2L} & \mathbf{1}^{2L\times 1} & \mathbf{1}^{2L\times 1} \\ \hline g & \mathbf{1}^{1\times 2L} & \mathbf{1}^{1\times 2L} & u_1 & 1 \\ \hline g & \mathbf{1}^{1\times 2L} & \mathbf{1}^{1\times 2L} & 1 & u_2 \end{array}\right)$$

with $\mathbf{Id}_{f,2L} = f^{\mathbf{I}_{2L}} \in \mathbb{G}^{2L\times 2L}$, $\mathbf{Id}_{h,2L} = h^{\mathbf{I}_{2L}} \in \mathbb{G}^{2L\times 2L}$, where $\mathbf{I}_{2L} \in \mathbb{Z}_p^{2L\times 2L}$ is the identity matrix. Then, generate a key pair $(\mathsf{pk}_{hsps}, \mathsf{sk}_{hsps})$ for the one-time LHSPS scheme of Section 2.2 with $n = 4L + 3$. Let $\mathsf{pk}_{hsps} = \big(g_z,\ g_r,\ h_z,\ h_u,\ \{g_i, h_i\}_{i=1}^{4L+3}\big)$ be the resulting public key and let $\mathsf{sk}_{hsps} = \{\chi_i, \gamma_i, \delta_i\}_{i=1}^{4L+3}$ be the underlying private key.

6. Generate one-time linearly homomorphic signatures $\{(z_j, r_j, u_j)\}_{j=1}^{4L+2}$ on the rows of $\mathbf{M}$.
7. Choose a perfectly WI Groth-Sahai CRS $\mathbf{g} = (\boldsymbol{G}_1, \boldsymbol{G}_2, \boldsymbol{G}_3)$ defined by vectors $\boldsymbol{G}_1 = (G_1, 1, G)$, $\boldsymbol{G}_2 = (1, G_2, G)$ and $\boldsymbol{G}_3 \in \mathbb{G}^3$, with $G, G_1, G_2 \xleftarrow{R} \mathbb{G}$ and $\boldsymbol{G}_3 \xleftarrow{R} \mathbb{G}^3$.
8. Define the private key as $SK = (x_1, y_1) \in \mathbb{Z}_p^2$. The public key is

$$PK = \big(g, f_1,\ h_1,\ \boldsymbol{V},\ \boldsymbol{W},\ u_1,\ u_2,\ \Omega_1,\ \Omega_2, \\ \mathsf{pk}_{hsps},\ \{(z_j, r_j, u_j)\}_{j=1}^{4L+2}, \mathbf{g} = (\boldsymbol{G}_1, \boldsymbol{G}_2, \boldsymbol{G}_3),\ \Sigma\big)\,,$$

whereas $\omega_1, \omega_2 \in \mathbb{Z}_p$ and sk_{hsps} are erased.

Encrypt(M, PK): To encrypt $M \in \mathbb{G}$, generate a one-time signature key pair $(\mathsf{SK}, \mathsf{VK}) \leftarrow \mathcal{G}(\lambda)$ and conduct the following steps:

1. Choose $\theta_1, \theta_2 \xleftarrow{R} \mathbb{Z}_p$ and compute $(C_0, C_1, C_2) = (M \cdot g^{\theta_1+\theta_2}, f_1^{\theta_1}, h_1^{\theta_2})$.
2. Choose $r, s \xleftarrow{R} \mathbb{Z}_p$ and compute a pseudo-signature

$$\sigma_1 = H(\boldsymbol{V}, \mathsf{VK})^r \cdot H(\boldsymbol{W}, \mathsf{VK})^s\,, \qquad \sigma_2 = f^r\,, \qquad \sigma_3 = h^s\,,$$

where $H(\boldsymbol{V}, \mathsf{VK}) = \prod_{\ell=1}^{L} V_{\ell,\mathsf{VK}[\ell]}$ and $H(\boldsymbol{W}, \mathsf{VK}) = \prod_{\ell=1}^{L} W_{\ell,\mathsf{VK}[\ell]}$.
3. Define the variables $(W_1, W_2) = (g^{\theta_1}, g^{\theta_2})$ and compute Groth-Sahai commitments $\{\boldsymbol{C}_{W_i}\}_{i=1}^{2}$ to these.
4. Define the bit $b = 1$ and generate $\boldsymbol{C}_b = (1, 1, G^b) \cdot \boldsymbol{G}_1^{r_b} \cdot \boldsymbol{G}_2^{s_b} \cdot \boldsymbol{G}_3^{t_b}$, where $r_b, s_b, t_b \xleftarrow{R} \mathbb{Z}_p$, as a commitment to b. Then, compute a Groth-Sahai commitment $\boldsymbol{C}_{\sigma_1}$ to σ_1 and commitments $\boldsymbol{C}_{\Theta_1}, \boldsymbol{C}_{\Theta_2} \in \mathbb{G}^3$ and $\boldsymbol{C}_{\Gamma_g}$ to

$$\Theta_1 = \Omega_1^{1-b}\,, \quad \Theta_2 = \Omega_2^{1-b}\,, \quad \Gamma_g = g^b\ . \tag{6}$$

The vector

$$(\sigma_1, \sigma_2^{1-\mathsf{VK}[1]}, \sigma_2^{\mathsf{VK}[1]}, \ldots, \sigma_2^{1-\mathsf{VK}[L]}, \sigma_2^{\mathsf{VK}[L]}, \\ \sigma_3^{1-\mathsf{VK}[1]}, \sigma_3^{\mathsf{VK}[1]}, \ldots, \sigma_3^{1-\mathsf{VK}[L]}, \sigma_3^{\mathsf{VK}[L]}, \Theta_1, \Theta_2) \in \mathbb{G}^{4L+3} \tag{7}$$

belongs to the subspace spanned by the first $4L$ rows of the matrix $\mathbf{M} \in \mathbb{G}^{(4L+2)\times(4L+3)}$. Hence, the algorithm can use $r, s \in \mathbb{Z}_p$ to derive a one-time linearly homomorphic signature $(Z, R, U) \in \mathbb{G}^3$ on the vector (7). Note that $(\sigma_1, \sigma_2, \sigma_3, Z, R, U)$ can be seen as a signature on VK, for the degenerated private key $(\omega_1, \omega_2) = (0, 0)$.
5. Generate commitments $\boldsymbol{C}_Z, \boldsymbol{C}_R, \boldsymbol{C}_U \in \mathbb{G}^3$. Then, compute a NIWI proof $\boldsymbol{\pi}_b \in \mathbb{G}^9$ that b satisfies $b^2 = b$ (which ensures that $b \in \{0, 1\}$) and NIWI proofs $\boldsymbol{\pi}_{\mathrm{PPE1}}, \boldsymbol{\pi}_{\mathrm{PPE2}} \in \mathbb{G}^3$ that variables $(\sigma_1, Z, R, U, \Theta_1, \Theta_2)$ satisfy

$$e(Z, g_z) \cdot e(R, g_r) = e(\sigma_1, g_1)^{-1} \cdot e(\sigma_2, \prod_{i=1}^{L} g_{2i+\mathsf{VK}[i]})^{-1} \cdot e(\sigma_3, \prod_{i=1}^{L} g_{2L+2i+\mathsf{VK}[i]})^{-1} \cdot e(\Theta_1, g_{4L+2})^{-1} \cdot e(\Theta_2, g_{4L+3})^{-1},$$

$$e(Z, h_z) \cdot e(U, h_u) = e(\sigma_1, h_1)^{-1} \cdot e(\sigma_2, \prod_{i=1}^{L} h_{2i+\mathsf{VK}[i]})^{-1} \cdot e(\sigma_3, \prod_{i=1}^{L} h_{2L+2i+\mathsf{VK}[i]})^{-1} \cdot e(\Theta_1, h_{4L+2})^{-1} \cdot e(\Theta_2, h_{4L+3})^{-1} .$$

6. Generate NIWI proofs $\boldsymbol{\pi}_g$, $\{\boldsymbol{\pi}_{\Theta_i}\}_{i=1}^2$ that (b, Θ_1, Θ_2), which are committed in $\boldsymbol{C}_b, \boldsymbol{C}_{\Theta_1}, \boldsymbol{C}_{\Theta_2}$, satisfy (6). Each such proof lives in $\mathbb{G}^3$.
7. Generate a simulation-extractable proof that (W_1, W_2) satisfy

$$e(C_1, g) = e(f_1, W_1), \qquad e(C_2, g) = e(h_1, W_2) . \tag{8}$$

   To this end, prove that (W_1, W_2, Γ_g) satisfy

$$e(C_1, \Gamma_g) = e(f_1, W_1), \qquad e(C_2, \Gamma_g) = e(h_1, W_2) . \tag{9}$$

   This requires proofs $\boldsymbol{\pi}_1, \boldsymbol{\pi}_2$ of 3 group elements each.
8. Finally, compute a one-time signature $sig = \mathcal{S}(\mathsf{SK}, C_0, C_1, C_2, \pi)$ and output the ciphertext $C = (\mathsf{VK}, C_0, C_1, C_2, \pi, sig)$, where

$$\pi = (\boldsymbol{C}_b, \boldsymbol{\pi}_b, \boldsymbol{C}_{\sigma_1}, \sigma_2, \sigma_3, \{\boldsymbol{C}_{W_i}\}_{i=1}^2, \boldsymbol{C}_Z, \boldsymbol{C}_R, \boldsymbol{C}_U, \{\boldsymbol{C}_{\Theta_i}\}_{i=1}^2, \boldsymbol{C}_{\Gamma_g}, \boldsymbol{\pi}_g, \{\boldsymbol{\pi}_{\Theta_i}\}_{i=1}^2, \boldsymbol{\pi}_{\text{PPE1}}, \boldsymbol{\pi}_{\text{PPE2}}, \boldsymbol{\pi}_1, \boldsymbol{\pi}_2) \tag{10}$$

   is a simulation-extractable proof of plaintext knowledge consisting of 62 elements of $\mathbb{G}$.

Decrypt($\boldsymbol{SK}, \boldsymbol{C}$): Parse C as $C = (\mathsf{VK}, C_0, C_1, C_2, \pi, sig)$ and do the following.

1. Return $\perp$ if $\mathcal{V}(\mathsf{VK}, (C_0, C_1, C_2, \pi), sig) = 0$ or if π does not properly verify.
2. Using $SK = (x_1, y_1) \in \mathbb{Z}_p^2$, compute and return $M = C_0 \cdot C_1^{-1/x_1} \cdot C_2^{-1/y_1}$.

Note that π forms a proof that either $(\sigma_1, \sigma_2, \sigma_3)$ is a valid signature or $\{\boldsymbol{C}_{W_i}\}_{i=1}^2$ are commitments to $(W_1, W_2) = (g^{\theta_1}, g^{\theta_2})$, where $\theta_1, \theta_2 \in \mathbb{Z}_p$ are the encryption exponents. A simulator holding the private key $(\omega_1, \omega_2) \in \mathbb{Z}_p^2$ of the signature scheme can simulate a proof π of plaintext knowledge by computing $(\sigma_1, \sigma_2, \sigma_3)$ as a real signature, by setting $b = 0$ at step 4 of the encryption algorithm and using the witnesses $(W_1, W_2) = (1_{\mathbb{G}}, 1_{\mathbb{G}})$ to prove relations (9).

We remark that each ciphertext must contain a proof comprised of 62 group elements. In an instantiation using the one-time signature of [31], the entire ciphertexts thus costs 69 group elements. The scheme can also be adapted to asymmetric pairings in a simple manner.

For simplicity, we follow [3] and only prove security in the single-user, multi-challenge case. However, as pointed out in [3], the single-user security results can always be simply extended to the scenario of multiple public keys by leveraging the random self-reducibility of the DLIN assumption in a standard manner. In the full version of the paper, we prove the following result.

Theorem 2. *The above scheme is* $(1, q_e)$*-IND-CCA secure provided: (i)* Σ *is a strongly unforgeable one-time signature; and (ii) the DLIN assumption holds in* $\mathbb{G}$*. For any adversary* $\mathcal{A}$*, there exist a one-time signature forger* $\mathcal{B}'$ *and a DLIN distinguisher* $\mathcal{B}$ *with running times* $t_{\mathcal{B}}, t_{\mathcal{B}'} \leq t_{\mathcal{A}} + q_e \cdot \mathsf{poly}(\lambda, L)$ *such that* $\mathbf{Adv}_{\mathcal{A}}^{(1,q_e)\text{-cca}}(\lambda) \leq 2 \cdot \mathbf{Adv}_{\mathcal{B}'}^{n\text{-suf-ots}}(\lambda) + (4 \cdot L + 5) \cdot \mathbf{Adv}_{\mathcal{B}}^{\text{DLIN}}(\lambda) + 5/p$*, where* L *is the verification key length of* Σ *and* q_e *is the number of encryption queries.*

In order to extend the result to the multi-user setting, the main changes are that we need to rely on: *(i)* The random self-reducibility of DLIN, which is used as in [31]; *(ii)* The almost tight security of the signature scheme of Section 3 in the multi-user setting [27], which can also be proved using the random self-reducibility of DLIN. The latter proof notably relies on the tight security of the homomorphic signature of Section 2.2 in the multi-key setting, which is proved in the full version of the paper.

Acknowledgements. We thank the anonymous reviewers for very useful comments. In particular, we are grateful to one reviewer for suggesting a more efficient approach to the scheme of Section 4. The first author's work was supported in part by the ERC Starting Grant ERC-2013-StG-335086-LATTAC. This work has also been supported by the "Programme Avenir Lyon Saint-Etienne de l'Université de Lyon" in the framework of the programme "Inverstissements d'Avenir" (ANR-11-IDEX-0007).

References

1. Abdalla, M., Fouque, P.-A., Lyubashevsky, V., Tibouchi, M.: Tightly-secure signatures from lossy identification schemes. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 572–590. Springer, Heidelberg (2012)
2. Abe, M., Chase, M., David, B., Kohlweiss, M., Nishimaki, R., Ohkubo, M.: Constant-size structure-preserving signatures: Generic constructions and simple assumptions. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 4–24. Springer, Heidelberg (2012)
3. Abe, M., David, B., Kohlweiss, M., Nishimaki, R., Ohkubo, M.: Tagged one-time signatures: Tight security and optimal tag size. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 312–331. Springer, Heidelberg (2013)
4. Abe, M., Fuchsbauer, G., Groth, J., Haralambiev, K., Ohkubo, M.: Structure-preserving signatures and commitments to group elements. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 209–236. Springer, Heidelberg (2010)
5. Abe, M., Haralambiev, K., Ohkubo, M.: Signing on elements in bilinear groups for modular protocol design. In: Cryptology ePrint Archive: Report 2010/133 (2010)
6. Bellare, M., Boldyreva, A., Micali, S.: Public-key encryption in a multi-user setting: Security proofs and improvements. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 259–274. Springer, Heidelberg (2000)

7. Bellare, M., Ristenpart, T.: Simulation without the Artificial Abort: Simplified Proof and Improved Concrete Security for Waters' IBE Scheme. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 407–424. Springer, Heidelberg (2009)
8. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: ACM CCS 1993, pp. 62–73. ACM Press (1993)
9. Bellare, M., Rogaway, P.: The Exact Security of Digital Signatures - How to Sign with RSA and Rabin. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 399–416. Springer, Heidelberg (1996)
10. Bernstein, D.J.: Proving Tight Security for Rabin-Williams Signatures. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 70–87. Springer, Heidelberg (2008)
11. Blazy, O., Kiltz, E., Pan, J. (Hierarchical) identity-based encryption from affine message authentication. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part I. LNCS, vol. 8616, pp. 408–425. Springer, Heidelberg (2014)
12. Böhl, F., Hofheinz, D., Jager, T., Koch, J., Seo, J.H., Striecks, C.: Practical signatures from standard assumptions. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 461–485. Springer, Heidelberg (2013)
13. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004)
14. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. SIAM J. of Computing 32(3), 586–615 (2003)
15. Boneh, D., Shen, E., Waters, B.: Strongly unforgeable signatures based on computational diffie-hellman. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.) PKC 2006. LNCS, vol. 3958, pp. 229–240. Springer, Heidelberg (2006)
16. Camenisch, J., Chandran, N., Shoup, V.: A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 351–368. Springer, Heidelberg (2009)
17. Cathalo, J., Libert, B., Yung, M.: Group encryption: Non-interactive realization in the standard model. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 179–196. Springer, Heidelberg (2009)
18. Chen, J., Lim, H.-W., Ling, S., Wang, H., Wee, H.: Shorter IBE and signatures via asymmetric pairings. In: Abdalla, M., Lange, T. (eds.) Pairing 2012. LNCS, vol. 7708, pp. 122–140. Springer, Heidelberg (2013)
19. Chen, J., Wee, H.: Fully (almost) tightly secure IBE and dual system groups. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 435–460. Springer, Heidelberg (2013)
20. Chevallier-Mames, B.: An efficient CDH-based signature scheme with a tight security reduction. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 511–526. Springer, Heidelberg (2005)
21. Chevallier-Mames, B., Joye, M.: A practical and tightly secure signature scheme without hash function. In: Abe, M. (ed.) CT-RSA 2007. LNCS, vol. 4377, pp. 339–356. Springer, Heidelberg (2006)
22. Coron, J.-S.: On the exact security of full domain hash. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 229–235. Springer, Heidelberg (2000)
23. Coron, J.-S.: Optimal security proofs for PSS and other signature schemes. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 272–287. Springer, Heidelberg (2002)
24. Coron, J.-S.: A variant of Boneh-Franklin IBE with a tight reduction in the random oracle model. Designs, Codes & Cryptography 50(1), 115–133 (2009)

25. Cramer, R., Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 13–25. Springer, Heidelberg (1998)
26. Dodis, Y., Haralambiev, K., López-Alt, A., Wichs, D.: Efficient public-key cryptography in the presence of key leakage. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 613–631. Springer, Heidelberg (2010)
27. Galbraith, S., Malone-Lee, J., Smart, N.: Public-key signatures in the multi-user setting. Information Processing Letters 83(5), 263–266 (2002)
28. Gerbush, M., Lewko, A., O'Neill, A., Waters, B.: Dual form signatures: An approach for proving security from static assumptions. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 25–42. Springer, Heidelberg (2012)
29. Groth, J.: Simulation-sound NIZK proofs for a practical language and constant size group signatures. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 444–459. Springer, Heidelberg (2006)
30. Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 415–432. Springer, Heidelberg (2008)
31. Hofheinz, D., Jager, T.: Tightly secure signatures and public-key encryption. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 590–607. Springer, Heidelberg (2012)
32. Hofheinz, D., Jager, T., Kiltz, E.: Short signatures from weaker assumptions. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 647–666. Springer, Heidelberg (2011)
33. Hofheinz, D., Jager, T., Knapp, E.: Waters signatures with optimal security reduction. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 66–83. Springer, Heidelberg (2012)
34. Hohenberger, S., Waters, B.: Short and stateless signatures from the RSA assumption. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 654–670. Springer, Heidelberg (2009)
35. Jutla, C., Roy, A.: Shorter quasi-adaptive NIZK proofs for linear subspaces. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I. LNCS, vol. 8269, pp. 1–20. Springer, Heidelberg (2013)
36. Jutla, C., Roy, A.: Switching lemma for bilinear tests and constant-size NIZK proofs for linear subspaces. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part II. LNCS, vol. 8617, pp. 295–312. Springer, Heidelberg (2014)
37. Kakvi, S., Kiltz, E.: Optimal security proofs for full domain hash, revisited. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 537–553. Springer, Heidelberg (2012)
38. Katz, J., Wang, N.: Efficiency improvements for signature schemes with tight security reductions. In: ACM-CCS 2003, pp. 155–164. ACM Press (2003)
39. Lewko, A.: Tools for simulating features of composite order bilinear groups in the prime order setting. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 318–335. Springer, Heidelberg (2012)
40. Lewko, A., Waters, B.: New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 455–479. Springer, Heidelberg (2010)
41. Libert, B., Peters, T., Joye, M., Yung, M.: Linearly homomorphic structure-preserving signatures and their applications. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 289–307. Springer, Heidelberg (2013)

42. Libert, B., Peters, T., Joye, M., Yung, M.: Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 514–532. Springer, Heidelberg (2014)
43. Naor, M.: On cryptographic assumptions and challenges. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 96–109. Springer, Heidelberg (2003)
44. Naor, M., Reingold, O.: Number-theoretic constructions of efficient pseudo-random functions. In: FOCS 1997, pp. 458–467. IEEE Press (1997)
45. Naor, M., Yung, M.: Public-key cryptosystems provably secure against chosen ciphertext attacks. In: STOC 1990, ACM Press (1990)
46. Rackoff, C., Simon, D.: Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 433–444. Springer, Heidelberg (1992)
47. Sahai, A.: Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In: FOCS 1999, pp. 543–553. IEEE Press (1999)
48. Schäge, S.: Tight proofs for signature schemes without random oracles. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 189–206. Springer, Heidelberg (2011)
49. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
50. Shoup, V.: A proposal for an ISO standard for public key encryption. Manuscript (December 20, 2001)
51. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)
52. Waters, B.: Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Heidelberg (2009)
53. Yamada, S., Hanaoka, G., Kunihiro, N.: Two-dimensional representation of cover free families and its applications: Short signatures and more. In: Dunkelman, O. (ed.) CT-RSA 2012. LNCS, vol. 7178, pp. 260–277. Springer, Heidelberg (2012)