Improved (Almost) Tight-Secure Simulation-Sound QA-NIZK with Applications

Masayuki Abe[1(✉)], Charanjit S. Jutla[2(✉)], Miyako Ohkubo[3(✉)], and Arnab Roy[4(✉)]

[1] NTT Corporation, Tokyo, Japan
abe.masayuki@lab.ntt.co.jp
[2] IBM T. J. Watson Research Center, Yorktown Heights, USA
csjutla@us.ibm.com
[3] Security Fundamentals Laboratories, CSR, NICT, Tokyo, Japan
m.ohkubo@nict.go.jp
[4] Fujitsu Laboratories of America, Sunnyvale, USA
aroy@us.fujitsu.com

Abstract. We construct the first (almost) tightly-secure unbounded-simulation-sound quasi-adaptive non-interactive zero-knowledge arguments (USS-QA-NIZK) for linear-subspace languages with compact (number of group elements independent of the security parameter) common reference string (CRS) and compact proofs under standard assumptions in bilinear-pairings groups. In particular, under the SXDH assumption, the USS-QA-NIZK proof size is only seventeen group elements with a factor $O(\log Q)$ loss in security reduction to SXDH. The USS-QA-NIZK primitive has many applications, including structure-preserving signatures (SPS), CCA2-secure publicly-verifiable public-key encryption (PKE), which in turn have applications to CCA-anonymous group signatures, blind signatures and unbounded simulation-sound Groth-Sahai NIZK proofs. We show that the almost tight security of our USS-QA-NIZK translates into constructions of all of the above applications with (almost) tight-security to standard assumptions such as SXDH and, more generally, $\mathcal{D}_k$-MDDH. Thus, we get the first publicly-verifiable (almost) tightly-secure multi-user/multi-challenge CCA2-secure PKE with practical efficiency under standard bilinear assumptions. Our (almost) tight SPS construction is also improved in the signature size over previously known constructions.

Keywords: QA-NIZK · Simulation-soundness · Tight security
Public-key encryption · CCA · Structure-preserving signatures

1 Introduction

Over the last decade, pairing-based cryptography has facilitated many new cryptographic protocols and applications that are provably-secure under static

T. Peyrin and S. Galbraith (Eds.): ASIACRYPT 2018, LNCS 11272, pp. 627–656, 2018.
https://doi.org/10.1007/978-3-030-03326-2_21

assumptions. Some of these static assumptions (SXDH, DLIN, MDDH) are now considered standard, as they generalize decisional-Diffie-Hellman (DDH) assumption to pairings-based groups. Some of the ground-breaking ideas include the Groth-Sahai (GS) non-interactive zero-knowledge (NIZK) proofs [GS12], fully-secure identity-based-encryption (IBE) [Wat09], structure-preserving signatures (SPS) [AFG+10], quasi-adaptive NIZK arguments (QA-NIZK) [JR13], and tightly-secure IBE [CW13]. In particular, structure-preserving signatures use Groth-Sahai NIZK proof structure to enable a wide-range of privacy-preserving applications, such as, group signatures [AHO10], blind signatures [AO09a, AFG+10], group encryption [CLY09], among others. Recent works [JR17, JOR18] have employed QA-NIZK to get more efficient SPS, and tightly-secure unbounded-simulation-sound QA-NIZK (USS-QA-NIZK [LPJY14,KW15]) to get tightly-secure CCA2-secure public-key encryption (PKE) in the multi-user and multi-challenge setting [LPJY15].

In this work we focus on the basic primitive of USS-QA-NIZK for linear-subspaces of vector spaces of bilinear groups, which has important implications as a structure-preserving version of it directly implies structure-preserving signatures. Further, it is already known to imply CCA2-secure PKE [LPJY15], which in turn leads to several new applications such as CCA-anonymous group signatures [AHO10], and UC-commitments [FLM11]. Further, an (almost) tightly-secure USS-QA-NIZK implies (almost) tightly-secure version of all the above applications. While an (almost) tightly-secure USS-QA-NIZK was given in [LPJY15] it required a large common reference string (CRS), which was of the order of the security parameter λ. In this work, we give the first (almost) tightly-secure USS-QA-NIZK for linear-subspaces with compact (number of group elements independent of λ) CRS and compact proofs. Moreover, the earlier construction only worked under the DLIN assumption in symmetric groups, and required non-standard assumptions in the asymmetric pairing-group setting, whereas we give a construction which is tightly-secure under the SXDH assumption in asymmetric groups. Asymmetric groups usually allow leaner constructions, which we validate below. At the same time, we make the CRS compact. Our construction of USS-QA-NIZK is also structure-preserving.

Related Techniques. In [KW15], Kiltz and Wee observed that QA-NIZK can be seen as a generalization of hash proof systems [CS98] to public-verifiability by publishing a "partial commitment" to the secret hash-key $\mathbf{k}$ in the second group $\mathbb{G}_2$ of a pairings-based groups $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$. Simulation of proofs of statements then just requires hash computation using the secret hash-key $\mathbf{k}$. Computational-soundness is slightly more tricky to prove than in the hash-proof setting, but essentially an adversary cannot generate hash proofs of false statements given only the "partial commitment" to $\mathbf{k}$ and the projection-key (of the hash-proof system). In the simulation-soundness setting, the simulation of fake proofs would give additional information to the adversary about secret-hash key $\mathbf{k}$, and hence to obtain a USS-QA-NIZK, [KW15] encrypt the hash-proofs and employ a dual-system [Wat09] technique to achieve soundness. This methodology should be

contrasted with the "OR" proof methodology of [LPJY15] (for USS-QA-NIZK) and [CCS09] (for unbounded simulation-sound GS-NIZK).

While the USS-QA-NIZK of [KW15] leads to compact proofs (of size only $(2k + 2)$ under k-linear assumption), the security reduction to the underlying hardness assumption is not tight. The reason behind this being that the dual-system approach is itself not tight as at its heart it employs one-time simulation-soundness along with two-universal hash-proof systems [JR15], similar to Cramer-Shoup CCA2-encryption [CS98]. A nested-version of dual-system approach does lead to (almost) tight IBE [CW13], but then requires non-compact (master) public keys.

However, the concept of identity-space partitioning introduced in [CW13] is also applicable to signature schemes, and this technique repeatedly splits the message space into two based on the message or a tag. This idea was further enhanced in [Hof17] to adaptive partitioning in which the partitioning is decided dynamically based on an encrypted partitioning-bit. [AHN+17] refined this technique by introducing new ideas using "OR" GS-NIZK systems and made the scheme structure-preserving. Since signature schemes, especially the ones considered in the above works, usually encrypt a secret and prove in zero-knowledge that such a secret is encrypted in the signature, the question arises if this refined adaptive-partitioning methodology can be employed to the USS-QA-NIZK of [KW15] discussed above that encrypted the hash-proofs. One main difference between NIZK proofs embedded in signature schemes is that they need only be "designated-prover" NIZK proofs. In other words, such NIZK proofs while still providing public verifiability, need only give the proving capability to a designated party, namely the CRS (or public-key) generator itself. Hence, such designated-prover NIZK proofs are much easier to devise and it is not immediately clear if such restricted NIZK proofs can be extended to usual NIZK proofs (especially in the tight USS-NIZK setting).

Finally, we argue that the recent constructions of tight CCA2-secure PKE [GHK17, Hof17] (along with [CCS09]) also do not easily imply tight USS-NIZK. [CCS09] requires proving an OR-statement where one of the disjuncts is that a CCA2-PKE ciphertext is well-formed. For [GHK17], this statement is not Groth-Sahai friendly as its own "qualified"-OR proof in the ciphertexts employs a mapping that maps group elements to $\mathbb{Z}_q$ elements. This should be contrasted with Cramer-Shoup CCA2-PKE, which also has such a tag, but that is publicly computable from other elements in the ciphertext. This is not the case for [GHK17] as the mapping is from private elements. As for [Hof17], it uses disjunctive hash-proofs from [ABP15] which require the hash proof to be in the target group; GS-proofs of such statements are only possible in the Witness-Indistinguishable setting.

Our Contributions. We show that a different "OR" system than considered in [AHN+17] (or later works such as [JOR18]) does allow one to give (almost) tight (structure-preserving) USS-QA-NIZK for linear-subspaces with compact proof sizes and compact CRS-es. This "OR" system can be proved in the generic framework of [Ràf15], allowing us to obtain USS-QA-NIZKs under the SXDH

assumption in asymmetric pairings groups, which was not previously known even for non-compact CRS. We also mention that while our structure-preserving USS-QA-NIZK construction loses a factor of $O(\lambda)$ in the security reduction, we give another variant employing tags (and hence not structure-preserving) that only has a $O(\log Q)$ factor loss in security reduction, where Q is the number of adversarial requests for simulated proofs. In yet another variant, we consider the "designated prover" setting as described above, and give a leaner structure-preserving construction with a tighter reduction as well, i.e. with only a $O(\log Q)$ factor loss.

As a first application, we show that a labeled version of our tight USS-QA-NIZK construction gives us a tight CCA2-secure *publicly-verifiable* labelled PKE in the multi-user multi-challenge setting[1]. In Table 1, we compare our scheme with the state of the art schemes in [GHKW16, Hof17, GHK17] with the smallest possible assumption for each. While being practical by itself, our scheme is not the best one in terms of efficiency. What separates our scheme from other tightly secure schemes is the public verifiability, which allows anyone, without knowing the secret key, to check if a ciphertext decrypts to some plaintext. Feasibility results for publicly-verifiable tight CCA-PKE can be found in [HJ16] and [ADKNO13], but their ciphertext overhead is hundreds or even more than a thousand of group elements. Ours is the first practical publicly-verifiable scheme having only 19 elements of ciphertext overhead. Our scheme is also secure under the SXDH assumption with only a $O(\log Q)$ loss in security reduction, where Q is the total number of (multi-challenge, multi-user) encryption-oracle requests by the adversary. CCA2-secure PKE and its variants that encrypt long messages have further applications, such as UC commitments, and we refer the reader to [LPJY15] for a good introduction.

Table 1. Comparison of tightly-secure public-key encryption schemes when the underlying assumptions are set to minimum ones, SXDH or DDH. Sizes count the number of group elements and (n_1, n_2) denotes n_1 and n_2 elements in $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. Column 'Pairings?' shows necessity of pairing groups. SAE stands for symmetric authenticated encryption.

	$\lvert pk\rvert$	$\lvert ct\rvert - \lvert m\rvert$	Verifiability	Pairings?	Sec. Loss	Assumption
[GHKW16]	$O(\lambda)$	3	private	no	$O(\lambda)$	DDH
[Hof17]	28	6	private	yes	$O(\lambda)$	DLIN
[GHK17]	6	3	private	no	$O(\lambda)$	DDH+SAE
Ours Sect. 5.1	$(13, 8)$	$(13, 6)$	public	yes	$O(\log Q)$	SXDH

As a second application, we show that our designated-prover variant of structure-preserving USS-QA-NIZK from Sect. 5.2 yields an SPS scheme with

[1] This requires adapting our USS-QA-NIZK to the multi-language USS-QA-NIZK described in [LPJY15], but our scheme readily adapts to that.

the shortest signature size in the literature. Recall that unbounded simulation-soundness guarantees that it is hard to create a valid proof for any no-instances taken out of the legitimate subspace even after seeing simulated proofs for (also no-) instances of one's choice. If we look at the simulation trapdoor as a secret-key and the simulated proofs as signatures, the USS-QA-NIZK can be considered as a signature scheme for message space consisting of no-instances, and the notion of unbounded simulation-soundness is exactly the same as existential unforgeability against adaptive chosen-message attacks. As formally proven in [AAO18], for bringing this idea to reality, we need an efficient mapping from desired message space to these no-instances. Since our USS-QA-NIZK allows simulation of fake proofs and we present a simple and efficient construction of injective mapping from a sequence of group elements to no-instances, this construction suffers no overhead for unilateral messages. This, along with the more efficient (designated-prover) USS-QA-NIZK gives us the shortest SPS known under the SXDH assumption, and with only a $O(\log Q)$ factor loss in security-reduction (see Table 2).

Table 2. Comparison with existing SPS schemes for unilateral messages when assumptions are set to minimal ones. Columns labeled as $|M|$, $|\sigma|$, and $|pk|$ show number of group elements in a message, a signature and a public key. For [HJ16], the parameter d limits number of signing queries to 2^d.

	$\lvert M\rvert$	$\lvert\sigma\rvert$	$\lvert pk\rvert$	Sec. Loss	Assumption
[HJ16]	1	$10d+6$	13	8	DLIN
[ACD+12]	$(n_1, 0)$	$(7, 4)$	$(5, n_1+12)$	$O(Q)$	SXDH, XDLIN
[LPY15]	$(n_1, 0)$	$(10, 1)$	$(16, 2n_1+5)$	$O(Q)$	SXDH, XDLIN
[KPW15]	$(n_1, 0)$	$(6, 1)$	$(0, n_1+6)$	$O(Q^2)$	SXDH
[JR17]	$(n_1, 0)$	$(5, 1)$	$(0, n_1+6)$	$O(Q \log Q)$	SXDH
[AHN+17]	$(n_1, 0)$	$(13, 12)$	$(18, n_1+11)$	$O(\lambda)$	SXDH
[JOR18]	$(n_1, 0)$	$(11, 6)$	$(7, n_1+16)$	$O(\lambda)$	SXDH
[GHKP18]	$(n_1, 0)$	$(8, 6)$	$(2, n_1+9)$	$O(\log Q)$	SXDH
Ours (Sect. 5.2)	$(n_1, 0)$	$(6, 6)$	$(10, n_1+5)$	$O(\log Q)$	SXDH

Finally, we mention some plug-in applications of our tightly-secure PKE and SPS without details. Combining these two applications, we have the first (almost) tightly-secure CCA-anonymous dynamic group signature scheme with compact signature sizes and compact public keys under standard assumptions. Also we can instantiate a generic structure-preserving blind signature scheme of [Fis06] using our SPS to get an (almost) tight round-optimal scheme under $\mathcal{D}_k$-MDDH with compact signature size, whereas previous schemes in standard model were based on non-static assumptions [Fuc09, AO09b]. Finally, our (almost) tight CCA2-secure PKE scheme along with the generic construction of [CCS09], leads

to a first (almost) tightly-secure unbounded simulation-sound Groth-Sahai NIZK proof system with compact CRS and proofs.

2 Preliminaries

We will consider cyclic groups $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ of prime order q, with an efficient bilinear map $\mathsf{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Group elements $\mathbf{g}_1$ and $\mathbf{g}_2$ will typically denote generators of the group $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively. Following [EHK+13], we will use the notations $[a]_1, [a]_2$ and $[a]_T$ to denote $a\mathbf{g}_1, a\mathbf{g}_2$, and $a \cdot \mathsf{e}(\mathbf{g}_1, \mathbf{g}_2)$ respectively and use additive notations for group operations. When talking about a general group $\mathbb{G}$ with generator $\mathbf{g}$, we will just use the notation $[a]$ to denote $a\mathbf{g}$. The notation generalizes to vectors and matrices in a natural component-wise way.

For two vector or matrices A and B, we will denote the product $A^\top B$ as $A \cdot B$. The pairing product $\mathsf{e}([A]_1, [B]_2)$ evaluates to the matrix product $[AB]_T$ in the target group with pairing as multiplication and target group operation as addition.

2.1 Matrix-DDH Assumptions and Boosting

We recall the *Matrix Decisional Diffie-Hellman* or MDDH assumptions from [EHK+13]. A matrix distribution $\mathcal{D}_{l,k}$, where $l > k$, is defined to be an efficiently samplable distribution on $\mathbb{Z}_q^{l \times k}$ which is full-ranked with overwhelming probability. The $\mathcal{D}_{l,k}$*-MDDH assumption* in group $\mathbb{G}$ states that with samples $\mathbf{A} \leftarrow \mathcal{D}_{l,k}, \mathbf{s} \leftarrow \mathbb{Z}_q^k$ and $\mathbf{s}' \leftarrow \mathbb{Z}_q^l$, the tuple $([\mathbf{A}], [\mathbf{A}\mathbf{s}])$ is computationally indistinguishable from $([\mathbf{A}], [\mathbf{s}'])$. A matrix distribution $\mathcal{D}_{k+1,k}$ is simply denoted by $\mathcal{D}_k$.

It was shown in [JR16] that a $\mathcal{D}_k$-MDDH assumption can be *boosted* to generate additional (computationally) independently random elements.

For an $l \times k$ matrix $\mathbf{A}$, we denote $\bar{\mathbf{A}}$ to be the top $k \times k$ square sub-matrix of $\mathbf{A}$ and $\underline{\mathbf{A}}$ to be the bottom $(l-k) \times k$ sub-matrix of $\mathbf{A}$.

Theorem 1 (Boosting [JR16]). *Let $\mathcal{D}_k$ be a matrix distribution on $\mathbb{Z}_q^{(k+1)\times k}$. Define another matrix distribution $\mathcal{D}_{l,k}$ on $\mathbb{Z}_q^{l\times k}$ as follows: First sample matrices $\mathbf{A} \leftarrow \mathcal{D}_k$ and $\mathbf{R} \leftarrow \mathbb{Z}_q^{(l-k)\times k}$ and then output $\begin{pmatrix} \bar{\mathbf{A}} \\ \mathbf{R} \end{pmatrix}$. Then the $\mathcal{D}_k$-MDDH assumption implies the $\mathcal{D}_{l,k}$-MDDH assumption with an $(l-k)$ security reduction.*

They called *boosting* to be the process of stretching $\mathcal{D}_k$ to $\mathcal{D}_{l,k}$ as above. In our construction we will need to boost $\mathcal{D}_k$ to $\mathcal{D}_{2k,k}$.

2.2 Quasi-Adaptive NIZK Proofs

A witness relation is a binary relation on pairs of inputs, the first called a word and the second called a witness. Each witness relation R defines a corresponding

language L which is the set of all words x for which there exists a witness w, such that $R(x, w)$ holds.

We will consider Quasi-Adaptive NIZK proofs [JR13] for a probability distribution $\mathcal{D}$ on a collection of (witness-) relations $\mathcal{R} = \{R_\rho\}$ (with corresponding languages L_ρ). Recall that in a quasi-adaptive NIZK, the CRS can be set after the language parameter has been chosen according to $\mathcal{D}$. Please refer to [JR13] for detailed definitions.

For our USS-QA-NIZK construction we will also need a property called true-simulation-soundness. We recall the definitions of these concepts below.

Definition 1 (QA-NIZK [JR13]). *We call a tuple of efficient algorithms* $(\mathsf{pargen}, \mathsf{crsgen}, \mathsf{prover}, \mathsf{ver})$ *a* quasi-adaptive non-interactive zero-knowledge *(QA-NIZK) proof system for witness-relations* $\mathcal{R}_\eta = \{R_\rho\}$ *with parameters sampled from a distribution* $\mathcal{D}$ *over associated parameter language* Lpar*, if there exist simulators* crssim *and* sim *such that for all non-uniform PPT adversaries* $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$*, we have (in all of the following probabilistic experiments, the experiment starts by setting* η *as* $\eta \leftarrow \mathsf{pargen}(1^\lambda)$*, and choosing* ρ *as* $\rho \leftarrow \mathcal{D}_\eta$*):*

Quasi-Adaptive Completeness:

$$\Pr\left[\begin{array}{l}\mathrm{CRS} \leftarrow \mathsf{crsgen}(\eta, \rho) \\ (x, w) \leftarrow \mathcal{A}_1(\mathrm{CRS}, \rho) \\ \pi \leftarrow \mathsf{prover}(\mathrm{CRS}, x, w)\end{array} : \begin{array}{c}\mathsf{ver}(\mathrm{CRS}, x, \pi) = 1 \textbf{ if} \\ R_\rho(x, w)\end{array}\right] = 1$$

Quasi-Adaptive Soundness:

$$\Pr\left[\begin{array}{l}\mathrm{CRS} \leftarrow \mathsf{crsgen}(\eta, \rho) \\ (x, \pi) \leftarrow \mathcal{A}_2(\mathrm{CRS}, \rho)\end{array} : \begin{array}{c}x \notin L_\rho \textbf{ and} \\ \mathsf{ver}(\mathrm{CRS}, x, \pi) = 1]\end{array}\right] \approx 0$$

Quasi-Adaptive Zero-Knowledge:

$$\Pr\left[\mathrm{CRS} \leftarrow \mathsf{crsgen}(\eta, \rho) \ : \ \mathcal{A}_3^{\mathsf{prover}(\mathrm{CRS}, \cdot, \cdot)}(\mathrm{CRS}, \rho) = 1\right]$$
$$\approx$$
$$\Pr\left[(\mathrm{CRS}, \mathsf{trap}) \leftarrow \mathsf{crssim}(\eta, \rho) \ : \ \mathcal{A}_3^{\mathsf{sim}^*(\mathrm{CRS}, \mathsf{trap}, \cdot, \cdot)}(\mathrm{CRS}, \rho) = 1\right],$$

where $\mathsf{sim}^*(\mathrm{CRS}, \mathsf{trap}, x, w) = \mathsf{sim}(\mathrm{CRS}, \mathsf{trap}, x)$ *for* $(x, w) \in R_\rho$ *and both oracles (i.e.* prover *and* sim^**) output failure if* $(x, w) \notin R_\rho$*.*

Definition 2 (True-Simulation-Sound [Har11]). *A QA-NIZK is called* **true-simulation-sound** *if soundness holds even when an adaptive adversary has access to simulated proofs on language members. More precisely, for all PPT* $\mathcal{A}$*,*

$$\Pr\left[\begin{array}{l}(\mathrm{CRS}, \mathsf{trap}) \leftarrow \mathsf{crssim}(\eta, \rho) \\ (x, \pi) \leftarrow \mathcal{A}^{\mathsf{sim}(\mathrm{CRS}, \mathsf{trap}, \cdot, \cdot)}(\mathrm{CRS}, \rho)\end{array} : \begin{array}{c}x \notin L_\rho \textbf{ and} \\ \mathsf{ver}(\mathrm{CRS}, x, \pi) = 1\end{array}\right] \approx 0,$$

where the experiment aborts if the oracle is called with some $x \notin L_\rho$*.*

The construction of [JR14] yielded k element proofs of any linear subspace language membership and [KW15] generalized it to any $\mathcal{D}_k$-MDDH assumption. Both constructions are true-simulation-sound.

We now define the unbounded simulation-soundness (USS) property, which we seek to achieve in this paper. The prover and verifier can additionally accept a label which is bound to the proof.

Definition 3 (Unbounded Simulation-Soundness). *A QA-NIZK is called (labeled)* **unbounded simulation sound** *if soundness holds even when an adaptive adversary has access to simulated proofs on arbitrary words of its choice. More precisely, for all PPT $\mathcal{A}$,*

$$\Pr\left[\begin{array}{l}(\mathrm{CRS},\mathsf{trap}) \leftarrow \mathsf{crssim}(\eta,\rho)\\ (x,\mathtt{lbl},\pi) \leftarrow \mathcal{A}^{\mathsf{sim}(\mathrm{CRS},\mathsf{trap},\cdot,\cdot)}(\mathrm{CRS},\rho)\end{array} : \begin{array}{c} x \notin L_\rho \ \wedge (x,\mathtt{lbl}) \notin \mathcal{Q}\\ \mathsf{ver}(\mathrm{CRS},x,\pi)=1\end{array}\right] \approx 0,$$

where the set $\mathcal{Q}$ records (word, label) tuples queried to the simulator.

A stronger notion called *Enhanced Unbounded Simulation-Soundness in the multi-CRS setting* was formalized by [LPJY15], where soundness holds even if the discrete logs of the language are given to the adversary and the adversary has access to multiple CRS-es and corresponding oracles. We note that our construction satisfies this property as well.

Our main construction is also *Structure-Preserving* as the CRS and proof elements are all in the base groups of the bilinear map and verification consists only of pairing product equations.

2.3 Public-Key Encryption Schemes

Let GEN be an algorithm that, on input security parameter λ, outputs par that includes parameters of pairing groups.

Definition 4 (Public-key encryption). *A Public-Key Encryption (PKE) scheme consists of probabilistic polynomial-time algorithms* $\mathsf{PKE} := (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$*:*

- *Key generation algorithm* $\mathsf{KeyGen}(\mathsf{par})$ *takes* $\mathsf{par} \leftarrow \mathsf{GEN}(1^\lambda)$ *as input and generates a pair of public and secret keys* $(\mathsf{pk},\mathsf{sk})$*. Message space* $\mathcal{M}$ *is determined by* pk*.*
- *Encryption algorithm* $\mathsf{Enc}(\mathsf{pk},\mathsf{M})$ *returns a ciphertext* ct*.*
- *Decryption algorithm* $\mathsf{Dec}(\mathsf{sk},\mathsf{ct})$ *is deterministic and returns a message* M*.*

For correctness, it must hold that, for all $\mathsf{par} \leftarrow \mathsf{GEN}(1^\lambda)$*,* $(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{KeyGen}(\mathsf{par})$*, messages* $\mathsf{M} \in \mathcal{M}$*, and* $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk},\mathsf{M})$*,* $\mathsf{Dec}(\mathsf{sk},\mathsf{ct}) = \mathsf{M}$*.*

Definition 5 (IND-mCPA Security [BBM00]). *A PKE scheme* PKE *is* indistinguishable against multi-instance chosen-plaintext attack *(*IND-mCPA-secure)

if for any $q_e \geq 0$ *and for all* PPT *adversaries* $\mathcal{A}$ *with access to oracle* $\mathcal{O}_e$ *at most* q_e *times the following advantage function* $\mathsf{Adv}^{\mathsf{mcpa}}_{\mathsf{PKE}}(\mathcal{A})$ *is negligible,*

$$\mathsf{Adv}^{\mathsf{mcpa}}_{\mathsf{PKE}}(\mathcal{A}) := \left| \Pr\left[b' = b \;\middle|\; \begin{array}{l} \mathsf{par} \leftarrow \mathsf{GEN}(1^\lambda); (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(\mathsf{par}); \\ b \leftarrow \{0,1\}; b' \leftarrow \mathcal{A}^{\mathcal{O}_e(\cdot,\cdot)}(\mathsf{pk}) \end{array} \right] - \frac{1}{2} \right|,$$

where $\mathcal{O}_e(\mathsf{M}_0, \mathsf{M}_1)$ *runs* $\mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{M}_b)$*, and returns* ct^* *to* $\mathcal{A}$*.*

There exist public-key encryption schemes that are structure-preserving, IND-mCPA secure, and have tight reductions based on compact assumptions. Examples are ElGamal encryption [ElG84] and Linear encryption [BBS04] based on the DDH assumption and the Decision Linear assumption, respectively. In particular, we will use the scheme of [EHK+13], which is based on the $\mathcal{D}_k$-MDDH assumption. We will use the linear homomorphic property of this PKE in the construction - adding the ciphertexts implicitly adds the underlying plaintexts.

We now recall the definition of IND-CCA2 secure public key encryption scheme in the multi-challenge multi-user setting [BBM00], where the par are shared by multiple users while generating their own keys using KeyGen.

Definition 6 (Multi-CCA [BBM00] (or see [LPJY15])).
A public-key encryption scheme is (μ, q_e)*-IND-CCA secure, for integers* $\mu, q_e \in poly(\lambda)$*, if no PPT adversary has non-negligible advantage in the following game:*

1. *The challenger first generates* $\mathsf{par} \leftarrow \mathsf{GEN}(1^\lambda)$ *and runs* $(\mathsf{sk}^{(i)}, \mathsf{pk}^{(i)}) \leftarrow \mathsf{KeyGen}(\mathsf{par})$ *for* $i = 1$ *to* μ*. It gives* $\{\mathsf{pk}^{(i)}\}_{i=1}^{\mu}$ *to the adversary* $\mathcal{A}$ *and retains* $\{\mathsf{sk}^{(i)}\}_{i=1}^{\mu}$*. In addition, the challenger initializes a set* $\mathcal{D} \leftarrow \phi$ *and a counter* $j_q \leftarrow 0$*. Finally, it chooses a random bit* $d \leftarrow \{0,1\}$*.*
2. *The adversary* $\mathcal{A}$ *adaptively makes queries to the following oracles on multiple occasions:*
   - *Encryption query:* $\mathcal{A}$ *chooses an index* $i \in [1..\mu]$ *and a pair* (M_0, M_1) *of equal length messages. If* $j_q = q_e$*, the oracle returns* $\perp$*. Otherwise, it computes* $C \leftarrow \mathsf{Enc}(\mathsf{pk}^{(i)}, M_d)$ *and returns* C*. In addition, it sets* $\mathcal{D} := \mathcal{D} \cup \{(i, C)\}$ *and* $j_q := j_q + 1$*.*
   - *Decryption query:* $\mathcal{A}$ *can also invoke the decryption oracle on arbitrary ciphertexts* C *and indices* $i \in [1..\mu]$*. If* $(i, C) \in \mathcal{D}$*, the oracle returns* $\perp$*. Otherwise, the oracle returns* $M \leftarrow \mathsf{Dec}(\mathsf{sk}^{(i)}, C)$*, which may be* $\perp$ *if* C *is an invalid ciphertext.*
3. *The adversary* $\mathcal{A}$ *outputs a bit* d' *and is deemed successful if* $d' = d$*. As usual,* $\mathcal{A}$*'s advantage is measured as the distance* $\mathsf{Adv}^{\mathsf{mcca}}(\mathcal{A}) = |2 \Pr[d' = d] - 1|$*.*

2.4 Structure-Preserving Signatures

Let GEN be a common parameter generation algorithm that outputs par for given security parameter λ.

Definition 7 (Structure-Preserving Signature). *A structure-preserving signature scheme SPS is a triple of probabilistic polynomial time (PPT) algorithms* $\mathsf{SPS} = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$*:*

- *Key generation algorithm* $\mathsf{KeyGen}(\mathsf{par})$ *takes common parameter* par *and returns a public/secret key,* (pk, sk)*, where* $pk \in \mathbb{G}^{n_{pk}}$ *for some* $n_{pk} \in poly(\lambda)$*. It is assumed that* pk *implicitly defines a message space* $\mathcal{M} := \mathbb{G}^n$ *for some* $n \in poly(\lambda)$*.*
- *Signing algorithm* $\mathsf{Sign}(sk, M)$ *takes secret key* sk *and a message* $M \in \mathcal{M}$ *as input and returns a signature* $\sigma \in \mathbb{G}^{n_\sigma}$ *for* $n_\sigma \in poly(\lambda)$*.*
- *Verification algorithm* $\mathsf{Verify}(pk, M, \sigma)$ *takes public key* pk*, message* $M \in \mathcal{M}$*, and signature* σ *and outputs* 1 *or* 0*. It only evaluates group membership operations and pairing product equations.*

Perfect correctness holds if for all $(pk, sk) \leftarrow \mathsf{KeyGen}(\mathsf{par})$ *and all messages* $M \in \mathcal{M}$ *and all* $\sigma \leftarrow \mathsf{Sign}(sk, M)$ *we have* $\mathsf{Verify}(pk, M, \sigma) = 1$*.*

Definition 8 (Existential Unforgeability against Chosen Message Attack). *To an adversary A and scheme SPS we associate the advantage function:*

$$\mathsf{Adv}^{\mathsf{cma}}_{\mathsf{SPS}}(A) := \Pr\left[\begin{array}{l}\mathsf{par} \leftarrow \mathsf{GEN}(1^\lambda) \\ (pk, sk) \leftarrow \mathsf{KeyGen}(\mathsf{par}) \\ (M^*, \sigma^*) \leftarrow A^{SignO(\cdot)}(pk)\end{array} : \begin{array}{c} M^* \notin Q_{msg} \textbf{ and} \\ \mathsf{Verify}(pk, M^*, \sigma^*) = 1\end{array}\right]$$

where SignO(M) runs $\sigma \leftarrow \mathsf{Sign}(sk, M)$*, adds* M *to* Q_{msg} *(initialized with* $\emptyset$*) and returns* σ *to A. An SPS is said to be (unbounded) EUF-CMA-secure if for all PPT adversaries A,* $\mathsf{Adv}^{\mathsf{cma}}_{\mathsf{SPS}}(A)$ *is negligible.*

3 The New (Almost) Tightly-Secure USS-QA-NIZK

The new USS-QA-NIZK scheme is formally described in Fig. 1, with the CRS and proof simulators described in Fig. 2. While a brief overview of the new scheme was given in the introduction, we now describe it in more detail.

We essentially combine techniques from the USS-QA-NIZK scheme of Kiltz and Wee [KW15] and the tightly secure SPS scheme of Jutla, Ohkubo and Roy [JOR18]. Following [KW15], we encrypt a basic QA-NIZK proof of the given word $\mathbf{y} = [\mathbf{Mx}]_1$ using an augmented ElGamal encryption scheme:

$$\boldsymbol{\rho} := [\bar{\mathbf{B}}\mathbf{r}]_1^\top,\ \hat{\boldsymbol{\rho}} := [\underline{\mathbf{B}}\mathbf{r}]_1^\top,\ \gamma := \mathbf{x}^\top[\mathbf{p}_1]_1 + \mathbf{r}^\top[\mathbf{p}_2]_1$$

Notice that unlike [KW15], we did not use an integer tag in the encryption. This helps us keep the construction structure preserving. We also include a QA-NIZK Π_2 certifying that $(\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma)$ is well-formed. Now we extend this tuple with elements which enable adaptive partitioning as in [JOR18]. This includes a double ElGamal encryption of a bit z, along with a QA-NIZK proof of equality of plaintexts. The final piece is an OR-NIZK proof that proves either $(\boldsymbol{\rho}, \hat{\boldsymbol{\rho}})$ is

consistent, or that z is same as a bit x which is given encrypted in the public key. Intuitively, in several games in the proof, the OR proof enables us to randomize the ciphertexts in the partitions where the disjunct $z = x$ holds, while restricting the adversary to attempt a win only in the other partitions. Instantiations of OR-NIZKs are given in Sect. 4.

The (almost) tight security of this scheme is proved in the next section. We prove that this construction has an $O(\lambda)$ reduction to $\mathcal{D}_k$-MDDH. In Sect. 3.2, we provide another construction which builds upon this one and enjoys a better $O(\log Q)$ reduction, where Q is the number of simulated proofs given out. Finally, in Sect. 3.3, we describe some optimizations which reduce the size of the proofs even further.

3.1 Security of the USS-QA-NIZK Scheme

In this section we state and prove the security of the USS-QA-NIZK scheme Π described in Fig. 1, with simulators described in Fig. 2.

Theorem 2. *For any efficient adversary $\mathcal{A}$, which makes at most Q simulator queries before attempting a forged proof, its probability of success ($\mathrm{ADV}^{\mathsf{uss}}_{\Pi}(Q)$) in the USS game against the scheme Π is at most*

$$\mathrm{ADV}^{\mathsf{tss}}_{\Pi_2} + 12L \cdot \mathrm{ADV}^{\mathsf{tss}}_{\Pi_1} + 8L \cdot \mathrm{ADV}_{\mathcal{D}_{2k,k}\text{-MDDH}} + (12L+1)\mathrm{ADV}^{\mathsf{zk}}_{\Pi_0}$$

$$+4L \cdot \mathrm{ADV}^{\mathsf{mcpa}}_{\mathsf{PKE}} + \frac{6L + (Q+1)^2 + 1}{q} + \frac{Q}{2^L}$$

Here L is the least integer greater than the bit size of q and hence is $O(\lambda)$.

Remark 1. $\mathrm{ADV}^{\mathsf{tss}}_{\Pi_i}$ of a QA-NIZK Π_i reduces to $\mathcal{D}_k$-MDDH by a factor of $(n-t)$ where the (affine) linear subspace language is of dimension t within a full space of dimension n. Also, $\mathrm{ADV}^{\mathsf{zk}}_{\Pi_0}$ of the OR-NIZK Π_0 reduces to $\mathcal{D}_k$-MDDH by a factor of 1.

Finally, $\mathcal{D}_{2k,k}$-MDDH reduces to $\mathcal{D}_k$-MDDH by a factor of k by boosting (See Sect. 2.1). Thus the overall reduction in Theorem 2 to $\mathcal{D}_k$-MDDH is $O(\lambda)$.

Proof Intuition. At the highest level, we go through a sequence of games (0–4), starting from Game 0 which is the NIZK simulator of Fig. 2 playing against a USS adversary and ending with Game 4, where the adversary has information theoretically negligible chance of winning. Essentially, in going from Game 2 to Game 3, the γ component is masked with an independently random element which depends on the input word, except for a randomly chosen point τ, where the mask is 0. Then finally in Game 4, the quantity $\mathbf{k}_1$ is shifted by a random vector in the kernel of the language matrix $\mathbf{M}$. This still keeps the CRS unchanged and since the simulated proofs have been masked by independently random elements (except at the point τ which occurs with negligible probability), they are also independent of this random kernel vector. However, the random kernel vector shows up in the winning condition of Game 4 and makes it statistically hard for the adversary to satisfy verification with a non-member word.

$\mathsf{crsgen}\ (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2, [\mathbf{M}]_1 \in \mathbb{G}_1^{n\times t})$:
Sample $\mathrm{CRS}^0 \leftarrow \Pi_0.\mathsf{crsgen}(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2)$.
Boost the given distribution $\mathcal{D}_{k+1,k}$ to $\mathcal{D}_{2k,k}$.
Sample $\mathbf{B} \leftarrow \mathcal{D}_{2k,k}$-MDDH and $(\mathbf{k}_1, \mathbf{k}_2) \leftarrow \mathbb{Z}_q^n \times \mathbb{Z}_q^k$.
Set $\mathbf{p}_1 := \mathbf{M}^\top \mathbf{k}_1$ and $\mathbf{p}_2 := \bar{\mathbf{B}}^\top \mathbf{k}_2$
Sample $(\mathrm{CRS}_p^i, \mathrm{CRS}_v^i) \leftarrow \Pi_i.\mathsf{crsgen}(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2, \cdot)$ for $i = 1, 2$, with parameters described below.

Sample $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{PKE.KeyGen}(\mathbb{G}_1)$ for $i = 1, 2$.
Sample $\mathbf{r}_x \leftarrow \mathbb{Z}_q^k$. Set $x := 0$ and $\mathsf{ct}_x := \mathsf{PKE.Enc}(\mathsf{pk}_1, x; \mathbf{r}_x)$.

Set $\mathrm{CRS}_p := (\mathrm{CRS}^0, \mathrm{CRS}_p^1, \mathrm{CRS}_p^2, [\mathbf{B}]_1, [\mathbf{p}_1]_1, [\mathbf{p}_2]_1, \mathsf{pk}_1, \mathsf{pk}_2, \mathsf{ct}_x)$.
Set $\mathrm{CRS}_v := (\mathrm{CRS}^0, \mathrm{CRS}_v^1, \mathrm{CRS}_v^2, [\mathbf{B}]_1, \mathsf{pk}_1, \mathsf{pk}_2, \mathsf{ct}_x)$.

Return $(\mathrm{CRS}_p, \mathrm{CRS}_v)$.

$\mathsf{prover}\ (\mathrm{CRS}_p,\ \mathbf{y} = [\mathbf{M}\mathbf{x}]_1,\ \mathbf{x})$:
Sample $(\mathbf{r}, \mathbf{r}_z^1, \mathbf{r}_z^2) \leftarrow \mathbb{Z}_q^k \times \mathbb{Z}_q^k \times \mathbb{Z}_q^k$.
Set $\boldsymbol{\rho} := [\bar{\mathbf{B}}\mathbf{r}]_1^\top,\ \hat{\boldsymbol{\rho}} := [\underline{\mathbf{B}}\mathbf{r}]_1^\top,\ \gamma := \mathbf{x}^\top [\mathbf{p}_1]_1 + \mathbf{r}^\top [\mathbf{p}_2]_1$.

Set $z := 0,\ \mathsf{ct}_z^1 := \mathsf{PKE.Enc}(\mathsf{pk}_1, z; \mathbf{r}_z^1)$ and $\mathsf{ct}_z^2 := \mathsf{PKE.Enc}(\mathsf{pk}_2, z; \mathbf{r}_z^2)$.

Set $\pi_0 := \Pi_0.\mathsf{prover}(\mathrm{CRS}^0,\ (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \mathsf{ct}_z^1 - \mathsf{ct}_x),\ (\mathbf{r}, 0))$.
Set $\pi_1 := \Pi_1.\mathsf{prover}(\mathrm{CRS}_p^1,\ (\mathsf{ct}_z^1, \mathsf{ct}_z^2),\ (0, \mathbf{r}_z^1, \mathbf{r}_z^2))$.
Set $\pi_2 := \Pi_2.\mathsf{prover}(\mathrm{CRS}_p^2,\ (\mathbf{y}, \boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma),\ (\mathbf{x}, \mathbf{r}))$.

Return $\pi := (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \mathsf{ct}_z^1, \mathsf{ct}_z^2, \pi_0, \pi_1, \pi_2)$.

$\mathsf{ver}\ (\mathrm{CRS}_v,\ \mathbf{y},\ \pi)$:
Check all the NIZK proofs:
$\Pi_0.\mathsf{ver}(\mathrm{CRS}^0,\ (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \mathsf{ct}_z^1 - \mathsf{ct}_x),\ \pi_0)$
and $\Pi_1.\mathsf{ver}(\mathrm{CRS}_v^1,\ (\mathsf{ct}_z^1, \mathsf{ct}_z^2),\ \pi_1)$
and $\Pi_2.\mathsf{ver}(\mathrm{CRS}_v^2,\ (\mathbf{y}, \boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma),\ \pi_2)$.

Languages:
Π_0 is an OR-NIZK for $L_0 \stackrel{\text{def}}{=} \{(\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \mathsf{ct}) \mid \exists(\mathbf{r}, \mathbf{r}_c) :\ (\ \boldsymbol{\rho} = [\bar{\mathbf{B}}\mathbf{r}]_1^\top$ **and** $\hat{\boldsymbol{\rho}} = [\underline{\mathbf{B}}\mathbf{r}]_1^\top)$ **or** $\mathsf{ct} = \mathsf{PKE.Enc}(\mathsf{pk}_1, 0; \mathbf{r}_c)\}$. Instantiation is given in Fig. 5.

Π_1 is a QA-NIZK for $L_1 \stackrel{\text{def}}{=} \{(\mathsf{ct}_z^1, \mathsf{ct}_z^2) \mid \exists(z, \mathbf{r}_z^1, \mathbf{r}_z^2) :\ \mathsf{ct}_z^1 = \mathsf{PKE.Enc}(\mathsf{pk}_1, z; \mathbf{r}_z^1)$ **and** $\mathsf{ct}_z^2 = \mathsf{PKE.Enc}(\mathsf{pk}_2, z; \mathbf{r}_z^2)\}$, with parameters $(\mathsf{pk}_1, \mathsf{pk}_2)$. Instantiations as in [JR14,KW15].

Π_2 is a QA-NIZK for $L_2 \stackrel{\text{def}}{=} \{(\mathbf{y}, \boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma) \mid \exists(\mathbf{x}, \mathbf{r}) :\ \mathbf{y} = [\mathbf{M}\mathbf{x}]_1$ **and** $\boldsymbol{\rho} = [\bar{\mathbf{B}}\mathbf{r}]_1^\top$ **and** $\hat{\boldsymbol{\rho}} = [\underline{\mathbf{B}}\mathbf{r}]_1^\top$ **and** $\gamma = \mathbf{x}^\top [\mathbf{p}_1]_1 + \mathbf{r}^\top [\mathbf{p}_2]_1\}$, with parameters $([\mathbf{M}]_1, [\mathbf{B}]_1, [\mathbf{p}_1]_1, [\mathbf{p}_2]_1)$. Instantiations as in [JR14,KW15].

Fig. 1. Tightly-secure USS-QA-NIZK Π.

$\mathsf{crssim}\ (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2, [\mathbf{M}]_1 \in \mathbb{G}_1^{n\times t})$:
Sample $\text{CRS}^0 \leftarrow \Pi_0.\mathsf{crsgen}(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2)$.
Boost the given distribution $\mathcal{D}_{k+1,k}$ to $\mathcal{D}_{2k,k}$.
Sample $\mathbf{B} \leftarrow \mathcal{D}_{2k,k}$-MDDH and $(\mathbf{k}_1, \mathbf{k}_2) \leftarrow \mathbb{Z}_q^n \times \mathbb{Z}_q^k$.
Set $\mathbf{p}_1 := \mathbf{M}^\top \mathbf{k}_1$ and $\mathbf{p}_2 := \bar{\mathbf{B}}^\top \mathbf{k}_2$
Sample $(\text{CRS}_p^1, \text{CRS}_v^1) \leftarrow \Pi_1.\mathsf{crsgen}(\cdots)$ and $(\text{CRS}_p^2, \text{CRS}_v^2, \mathsf{trap}^2) \leftarrow \Pi_2.\mathsf{crssim}(\cdots)$.

Sample $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{PKE.KeyGen}(\mathbb{G}_1)$ for $i = 1, 2$.
Sample $\mathbf{r}_x \leftarrow \mathbb{Z}_q^k$. Set $x := 0$ and $\mathsf{ct}_x := \mathsf{PKE.Enc}(\mathsf{pk}_1, x; \mathbf{r}_x)$.

Set $\text{CRS}_p := (\text{CRS}^0, \text{CRS}_p^1, \text{CRS}_p^2, [\mathbf{B}]_1, [\mathbf{p}_1]_1, [\mathbf{p}_2]_1, \mathsf{pk}_1, \mathsf{pk}_2, \mathsf{ct}_x)$.
Set $\text{CRS}_v := (\text{CRS}^0, \text{CRS}_v^1, \text{CRS}_v^2, [\mathbf{B}]_1, \mathsf{pk}_1, \mathsf{pk}_2, \mathsf{ct}_x)$.
Set $\mathsf{trap} := (\mathbf{k}_1, \mathsf{trap}^2)$

Return $(\text{CRS}_p, \text{CRS}_v, \mathsf{trap})$.

$\mathsf{sim}\ (\text{CRS}_p,\ \mathsf{trap}, \mathbf{y})$:
Sample $(\mathbf{r}, \mathbf{r}_z^1, \mathbf{r}_z^2) \leftarrow \mathbb{Z}_q^k \times \mathbb{Z}_q^k \times \mathbb{Z}_q^k$.
Set $\boldsymbol{\rho} := [\bar{\mathbf{B}}\mathbf{r}]_1^\top,\ \hat{\boldsymbol{\rho}} := [\underline{\mathbf{B}}\mathbf{r}]_1^\top,\ \gamma := \mathbf{y}^\top \mathbf{k}_1 + \mathbf{r}^\top [\mathbf{p}_2]_1$.

Set $z := 0,\ \mathsf{ct}_z^1 := \mathsf{PKE.Enc}(\mathsf{pk}_1, z; \mathbf{r}_z^1)$ and $\mathsf{ct}_z^2 := \mathsf{PKE.Enc}(\mathsf{pk}_2, z; \mathbf{r}_z^2)$.

Set $\pi_0 := \Pi_0.\mathsf{prover}(\text{CRS}^0,\ (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \mathsf{ct}_z^1 - \mathsf{ct}_x),\ (\mathbf{r}, 0))$.
Set $\pi_1 := \Pi_1.\mathsf{prover}(\text{CRS}_p^1,\ (\mathsf{ct}_z^1, \mathsf{ct}_z^2),\ (0, \mathbf{r}_z^1, \mathbf{r}_z^2))$.
Set $\pi_2 := \Pi_2.\mathsf{sim}(\text{CRS}_p^2,\ \mathsf{trap}^2,\ (\mathbf{y}, \boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma))$.

Return $\pi := (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \mathsf{ct}_z^1, \mathsf{ct}_z^2, \pi_0, \pi_1, \pi_2)$.

Fig. 2. CRS and Proof simulators for Π.

Going from Game 2 to 3 requires another set of hybrid games in which we introduce the mask elements into the γ's. The games proceed bit by bit based on a random bit-string $\text{RP}(\mathbf{y})$ of length L, which is obtained by applying a random injective function RP to the input word $\mathbf{y}$. In every hybrid j, which runs from 0 to L, the mask depends on the first j bits of $\text{RP}(\mathbf{y})$. The mask function is inductively defined as follows:

$$\text{RF}_j(\text{RP}(\mathbf{y})|_j) \stackrel{\text{def}}{=} \begin{Bmatrix} \text{RF}_{j-1}(\text{RP}(\mathbf{y})|_{j-1}), & \text{if } (\text{RP}(\mathbf{y})_j = \tau_j) \\ \text{RF}'_{j-1}(\text{RP}(\mathbf{y})|_{j-1}), & \text{if } (\text{RP}(\mathbf{y})_j \neq \tau_j) \end{Bmatrix},$$

where RF_j is a random function from $\{0,1\}^j$ to $\mathbb{Z}_q$, except at a point $\tau|_j$, the first j bits of τ, where its value is 0. RF'_{j-1} is another independently random function from $\{0,1\}^{j-1}$ to $\mathbb{Z}_q$. The 0-th hybrids start as Game 2 with the '0' mask, which is the value of $\text{RF}_0(\epsilon)$. The L-th hybrids end in Game 3 with the mask depending on all the bits of $\text{RP}(\mathbf{y})$, hence essentially the whole word.

The adaptive partitioning technique of [Hof17] helps us switching from RF_{j-1} to RF_j with a constant number of MDDH reductions. Essentially, in the j-th hybrid, the j-th bit of $\text{RP}(\mathbf{y})$ induces two partitions of the message space: (1) where the

bit is τ_j, soundness is enforced to hold in the winning condition and (2) where the bit is $1-\tau_j$, all such simulated proofs can be switched in one go with a constant number of MDDH transitions. Formal details follow.

Proof. We go through a sequence of Games $\mathbf{G}_0$ to $\mathbf{G}_4$ which are described below and summarized in Fig. 3. In the following, $\Pr_i[X]$ will denote probability of predicate X holding in probability space defined in game $\mathbf{G}_i$ and WIN_i will denote the winning condition for the adversary in game $\mathbf{G}_i$.

Game $\mathbf{G}_0$: This game exactly replicates the simulator in Fig. 2 to the adversary. So the adversary's advantage in $\mathbf{G}_0$ (defined as WIN_0 below) is the USS advantage we seek to bound.

$$\mathsf{WIN}_0 \triangleq (\mathbf{y}^* \notin \{\mathbf{y}^i\}_i \cup \mathrm{span}([\mathbf{M}]_1)) \textbf{ and } \mathsf{ver}(\mathrm{CRS}_v,\ \mathbf{y}^*,\ \pi^*)$$

Game $\mathbf{G}_0{}'$: In Game $\mathbf{G}_0{}'$, the challenger lazily simulates (by maintaining a table) a random function RP from $\mathbb{G}_1^n$ to $\{0,1\}^L$. Define Col to be the predicate which returns true when there is a collision, i.e., when any pair of message vectors from the set of signature queries union the adversarial response message at the end get mapped to the same output L-bit string. In this game, the adversary is allowed to win outright if Col is true at the end:

$$\mathsf{WIN}_0' \triangleq \mathsf{Col} \textbf{ or } ((\mathbf{y}^* \notin \{\mathbf{y}^i\}_i \cup \mathrm{span}([\mathbf{M}]_1)) \textbf{ and } \mathsf{ver}(\mathrm{CRS}_v,\ \mathbf{y}^*,\ \pi^*))$$

The difference in advantage is at most the collision probability, which is bounded by $(Q+1)^2/q$.

Game $\mathbf{G}_1$: In this game the CRS of Π_2 is generated in the simulation mode and the trapdoor is kept by the challenger to generate simulated proofs. The challenge-response in this game is the same as $\mathbf{G}_0$. The winning condition is now defined as:

$$\begin{aligned}\mathsf{WIN}_1 \triangleq\ & \mathsf{Col} \textbf{ or} \\ & \mathsf{WIN}_0 \textbf{ and } \pi^* = (\boldsymbol{\rho}^*, \hat{\boldsymbol{\rho}}^*, \gamma^*, \mathsf{ct}_z^{1*}, \mathsf{ct}_z^{2*}, \pi_0^*, \pi_1^*, \pi_2^*) \text{ s.t.} \\ & (\gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + \boldsymbol{\rho}^*\mathbf{k}_2) \textbf{ and } (\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)\end{aligned}$$

The difference in advantages of the adversary is upper bounded by the unbounded true-simulation-soundness of Π_2:

$$|\Pr_1[\mathsf{WIN}_1] - \Pr_0[\mathsf{WIN}_0]| \leq \mathrm{ADV}^{\mathsf{tss}}_{\Pi_2} \tag{1}$$

Game $\mathbf{G}_2$: In this game, the OR-NIZK CRS is generated as a simulation CRS and the witness of $(\boldsymbol{\rho}^i, \hat{\boldsymbol{\rho}}^i, \mathsf{ct}_z^{1i} - \mathsf{ct}_x) \in L_0$, is switched to $(\mathbf{0}, \mathbf{r}_z^{1i} - \mathbf{r}_x)$. The winning condition WIN_2 remains the same as WIN_1.

$$|\Pr_2[\mathsf{WIN}_2] - \Pr_1[\mathsf{WIN}_1]| \leq \mathrm{ADV}^{\mathsf{zk}}_{\Pi_0} \tag{2}$$

$\mathsf{crssim}() : \cdots$

Games 0-1 $\quad \mathrm{CRS}^0 \leftarrow \Pi_0.\mathsf{crsgen}()$

Games 2-4 $\quad (\mathrm{CRS}^0, \mathsf{trap}^0) \leftarrow \Pi_0.\mathsf{crssim}()$

Game 0 $\quad \mathrm{CRS}^2 \leftarrow \Pi_2.\mathsf{crsgen}()$

Games 1-4 $\quad (\mathrm{CRS}^2, \mathsf{trap}^2) \leftarrow \Pi_2.\mathsf{crssim}()$

$\quad$ Sample $(\mathbf{k}'_1,\ \mathbf{u}) \leftarrow \mathbb{Z}_q^n \times \mathbb{Z}_q^{n-t}$

Games 1-3 $\quad$ Set $\mathbf{k}_1 := \mathbf{k}'_1$

Game 4 $\quad$ Set $\mathbf{k}_1 := \mathbf{k}'_1 + \mathbf{M}^{\perp}\mathbf{u}$

$\quad \cdots$

$\mathsf{sim}(\mathbf{y}^i \in \mathbb{G}_1^n) :$

$\quad$ Set $(\boldsymbol{\rho}^i, \hat{\boldsymbol{\rho}}^i, \gamma^i) :=$

Games 0-2 $\quad ([\bar{\mathbf{B}}\mathbf{r}^i]_1^\top,\ [\underline{\mathbf{B}}\mathbf{r}^i]_1^\top,\ \mathbf{y}^{i\top}\mathbf{k}_1 + \boldsymbol{\rho}^i\mathbf{k}_2)$

Game 3 $\quad ([\bar{\mathbf{B}}\mathbf{r}^i]_1^\top,\ [\underline{\mathbf{B}}\mathbf{r}^i]_1^\top,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [\mathrm{RF}_L(\nu^i)]_1 + \boldsymbol{\rho}^i\mathbf{k}_2)$

Game 4 $\quad ([\bar{\mathbf{B}}\mathbf{r}^i]_1^\top,\ [\underline{\mathbf{B}}\mathbf{r}^i]_1^\top,\ \mathbf{y}^{i\top}\mathbf{k}'_1 + \mathbf{y}^{i\top}\mathbf{M}^{\perp}\mathbf{u} + [\mathrm{RF}_L(\nu^i)]_1 + \boldsymbol{\rho}^i\mathbf{k}_2)$

$\quad \cdots$

$\mathsf{WIN} \stackrel{\text{def}}{=}$

Games 0'-4 $\quad$ **if** (Col) **return true; else**

$\quad \pi^* = (\boldsymbol{\rho}^*, \hat{\boldsymbol{\rho}}^*, \gamma^*, \mathsf{ct}_z^{1*}, \mathsf{ct}_z^{2*}, \pi_0^*, \pi_1^*, \pi_2^*) :$

$\quad\quad (\mathbf{y}^* \notin \{\mathbf{y}^i\}_i \cup \mathrm{span}([\mathbf{M}]_1))$ **and** $\mathsf{ver}(\mathrm{CRS}_v,\ \mathbf{y}^*,\ \pi^*)$

Games 1-3 $\quad\quad$ **and** $\gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + \boldsymbol{\rho}^*\mathbf{k}_2$

Game 4 $\quad\quad$ **and** $\gamma^* = \mathbf{y}^{*\top}\mathbf{k}'_1 + \mathbf{y}^{*\top}\mathbf{M}^{\perp}\mathbf{u} + \boldsymbol{\rho}^*\mathbf{k}_2$

Games 1-4 $\quad\quad$ **and** $(\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$

Fig. 3. Top level games and winning conditions

Game $\mathbf{G}_3$: In this game, the challenger first chooses a uniformly random string $\tau \in \{0,1\}^L$ and also lazily maintains a function RF_L mapping $\{0,1\}^L$ to $\mathbb{Z}_q$. The function RF_L has the property that it is a random and independent function from $\{0,1\}^L$ to $\mathbb{Z}_q$, except at τ where its value is 0. In $\mathbf{G}_3$, each signature component γ^i is generated as $\mathbf{y}^{i\top}\mathbf{k}_1 + [\mathrm{RF}_L(\mathrm{RP}(\mathbf{y}^i))]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$, instead of $\mathbf{y}^{i\top}\mathbf{k}_1 + \boldsymbol{\rho}^i\mathbf{k}_2$. For ease

of exposition, we will denote $\mathrm{RP}(\mathbf{y}^i)$ as ν^i. The winning condition WIN_3 remains the same as WIN_2.

Lemma 1. $|\Pr_3[\mathit{WIN}_3] - \Pr_2[\mathit{WIN}_2]| \leq$

$$12L \cdot \mathrm{ADV}^{\mathsf{tss}}_{\Pi_1} + 8L \cdot \mathrm{ADV}_{\mathcal{D}_{2k,k}\text{-MDDH}}$$

$$+12L \cdot \mathrm{ADV}^{\mathsf{zk}}_{\Pi_0} + 4L \cdot \mathrm{ADV}^{\mathsf{mcpa}}_{\mathsf{PKE}} + \frac{6L}{q}$$

We prove this lemma in the full paper by going through a finer set of hybrid games.

Game $\mathbf{G}_4$: In this game, the challenger samples $(\mathbf{k}'_1, \mathbf{u}) \leftarrow \mathbb{Z}_q^n \times \mathbb{Z}_q^{n-t}$, and generates $\mathbf{k}_1$ differently as $\mathbf{k}'_1 + \mathbf{M}^\perp\mathbf{u}$, where $\mathbf{M}^\perp$ is a $\mathbb{Z}_q^{t\times(n-t)}$ matrix such that $\mathbf{M}^\top\mathbf{M}^\perp = \mathbf{0}^{t\times(n-t)}$. Observe that the public key component $[\mathbf{p}]_1$ becomes $[\mathbf{M}^\top\mathbf{k}_1]_1 = [\mathbf{M}^\top\mathbf{k}'_1]_1$. So $\mathbf{u}$ does not show up in the public key.

Consequently, the computations of γ^i's are changed to $\mathbf{y}^{i\top}\mathbf{k}'_1 + \mathbf{y}^{i\top}\mathbf{M}^\perp\mathbf{u} + [\mathrm{RF}_L(\nu^i)]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$. Also, the winning condition check on γ^* is modified accordingly to $\gamma^* = \mathbf{y}^{*\top}\mathbf{k}'_1 + \mathbf{y}^{*\top}\mathbf{M}^\perp\mathbf{u} + \boldsymbol{\rho}^*\mathbf{k}_2$.

We now claim that $\Pr_4[\mathsf{WIN}_4] \leq \frac{1}{q} + \frac{Q}{2^L}$. To see this, recall that RF maps any element of $\{0,1\}^L$ to a uniformly random element of $\mathbb{Z}_q$, except τ, which it maps to 0. Now, if none of the adversary queries is actually mapped to τ by RP, no information about it is leaked to the adversary. The probability that for any i, $\mathrm{RP}(\mathbf{y}^i) = \tau$, is upper bounded by $\frac{Q}{2^L}$.

Now, in the case that $\mathrm{RP}(\mathbf{y}^i)$ is not τ for any i, we have that $\mathrm{RF}(\mathrm{RP}(\mathbf{y}^i))$ is uniformly random and independent of everything else. This means that it completely hides the term $\mathbf{y}^{i\top}\mathbf{M}^\perp\mathbf{u}$ in the γ^i components of the signature responses.

As for the adversary's forged proof, $\mathbf{y}^{*\top}\mathbf{M}^\perp$ is non-zero if $\mathbf{y}^*$ is not in the span of $[\mathbf{M}]_1$. Also, $\mathbf{u}$ is not shown in any public key and as we reasoned in the last paragraph, it doesn't show up (whp) in any signature either. Consequently, $\mathbf{y}^{*\top}\mathbf{M}^\perp\mathbf{u}$ is uniformly random in $\mathbb{Z}_q$ and independent of the adversary's view. Therefore, the probability of satisfying $\gamma^* - \mathbf{y}^{*\top}\mathbf{k}'_1 - \boldsymbol{\rho}^*\mathbf{k}_2 = \mathbf{y}^{*\top}\mathbf{M}^\perp\mathbf{u}$ is upper bounded by $1/q$. This proves the claim.

3.2 USS-QA-NIZK Scheme with $O(\log Q)$ Reduction

The scheme is given in Fig. 4 and the top level proof game table is given in the full paper. Since this scheme is very similar to the one given earlier, we only point out the essential points of difference in the construction and proof.

The scheme uses a similar augmented ElGamal encryption of a basic QA-NIZK proof:

$$\boldsymbol{\rho} := [\bar{\mathbf{B}}\mathbf{r}]_1^\top,\ \hat{\boldsymbol{\rho}} := [\underline{\mathbf{B}}\mathbf{r}]_1^\top,\ \gamma := \mathbf{x}^\top[\mathbf{p}_1]_1 + \mathbf{r}^\top[\mathbf{p}_2 + \tau\mathbf{p}_3]_1$$

The additional part is a tagged component reminiscent of the Cramer-Shoup CCA2 encryption scheme [CS02], where τ is a collision resistant hash on rest of the proof components. Rest of it is fairly similar to the earlier construction. Unfortunately, this construction is no longer structure-preserving due to the tag computation.

To prove $O(\log Q)$ reduction, we follow the partitioning strategy of [GHKP18], where the partition is done on the bits of the query index i, instead of a random function applied to the argument. This strategy did not work for our earlier construction because RF mapped to 0 at one point of it's domain and the proof relied on the fact that such a point is exponentially hard to determine since the domain size is exponential in λ.

In the proof of security of this construction, we take account of the fact that RF could map to 0 at a point which can non-negligibly occur in a query. We instead argue that since the tag of such a query response would be different from the tag of the adversary's output proof, the response can still be randomized due to pairwise independence. A detailed proof will be in the full version of the paper.

Theorem 3. *For any efficient adversary $\mathcal{A}$, which makes at most Q simulator queries before attempting a forged proof, its probability of success ($\mathrm{ADV}^{\mathsf{uss}}_{\Pi'}(Q)$) in the USS game against the scheme Π' is at most (Here L is $\log Q$):*

$$\mathrm{ADV}^{\mathsf{tss}}_{\Pi_2} + 12L \cdot \mathrm{ADV}^{\mathsf{tss}}_{\Pi_1} + 8L \cdot \mathrm{ADV}_{\mathcal{D}_{2k,k}\text{-MDDH}} + (12L+1)\mathrm{ADV}^{\mathsf{zk}}_{\Pi_0}$$

$$+4L \cdot \mathrm{ADV}^{\mathsf{mcpa}}_{\mathsf{PKE}} + \frac{6L + (Q+1)^2 + 1}{q}.$$

3.3 Optimizations

In this section, we describe two optimizations which reduce the size of the proofs further by $2k$ elements under the $\mathcal{D}_k$-MDDH assumption.

ElGamal Encryption with Common Randomness. As described in [AHN+17], the randomnesses $\mathbf{r}^1_z$ and $\mathbf{r}^2_z$ of ciphertexts ct^1_z and ct^2_z can be shared and merged into a single k-element $\mathbf{r}_z$. In more details, let's say $\mathsf{ct}^1_z = ([\bar{\mathbf{A}}_1\mathbf{r}^1_z]_1, [z + \underline{\mathbf{A}}_1\mathbf{r}^1_z]_1)$ and $\mathsf{ct}^2_z = ([\bar{\mathbf{A}}_2\mathbf{r}^2_z]_1, [z + \underline{\mathbf{A}}_2\mathbf{r}^2_z]_1)$, which are encryptions of z under public keys $[\mathbf{A}_1]_1$ and $[\mathbf{A}_2]_1$. Then instead of computing the ciphertexts independently, we can merge them into $([\bar{\mathbf{A}}_1\mathbf{r}_z]_1, [z+\underline{\mathbf{A}}_1\mathbf{r}_z]_1), [z+\underline{\mathbf{A}}_2\mathbf{r}_z]_1)$. This saves us k elements. Importantly, we can still enable transitions where we can hold the decryption key of one system, while switching the plaintext of the other.

Merge QA-NIZKs in the Same Group. The reason we did not combine Π_1 and Π_2 is that we needed to use the true-simulation-soundness of one system, while producing proofs over fake instances with the other. However, we show in the full paper, that we can still merge the proofs into one proof over the combined linear system, and still be independently able to use the true-simulation-soundness of its parts. This saves us k elements from Π.

$\mathsf{crsgen}\ (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2, [\mathbf{M}]_1 \in \mathbb{G}_1^{n\times t})$:
Sample $\mathrm{CRS}^0 \leftarrow \Pi_0.\mathsf{crsgen}()$.
Boost the given distribution $\mathcal{D}_{k+1,k}$ to $\mathcal{D}_{2k,k}$.
Sample $\mathbf{B} \leftarrow \mathcal{D}_{2k,k}$-MDDH and $(\mathbf{k}_1, \mathbf{k}_2, \mathbf{k}_3) \leftarrow \mathbb{Z}_q^n \times \mathbb{Z}_q^k \times \mathbb{Z}_q^k$.
Set $\mathbf{p}_1 := \mathbf{M}^\top \mathbf{k}_1, \mathbf{p}_2 := \bar{\mathbf{B}}^\top \mathbf{k}_2$ and $\mathbf{p}_3 := \bar{\mathbf{B}}^\top \mathbf{k}_3$.
Sample $(\mathrm{CRS}_p^i, \mathrm{CRS}_v^i) \leftarrow \Pi_i.\mathsf{crsgen}()$ for $i = 1, 2$.

Sample $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{PKE.KeyGen}(\mathbb{G}_1)$ for $i = 1, 2$.
Sample $\mathbf{r}_x \leftarrow \mathbb{Z}_q^k$. Set $x := 0$ and $\mathsf{ct}_x := \mathsf{PKE.Enc}(\mathsf{pk}_1, x; \mathbf{r}_x)$.
Let crh be a collision resistant hash from $\{0,1\}^*$ to $\mathbb{Z}_q$.

Set $\mathrm{CRS}_p := (\mathrm{CRS}^0, \mathrm{CRS}_p^1, \mathrm{CRS}_p^2, [\mathbf{B}]_1, [\mathbf{p}_1]_1, [\mathbf{p}_2]_1, \mathsf{pk}_1, \mathsf{pk}_2, \mathsf{ct}_x)$.
Set $\mathrm{CRS}_v := (\mathrm{CRS}^0, \mathrm{CRS}_v^1, \mathrm{CRS}_v^2, [\mathbf{B}]_1, \mathsf{pk}_1, \mathsf{pk}_2, \mathsf{ct}_x)$.

Return $(\mathrm{CRS}_p, \mathrm{CRS}_v)$.

$\mathsf{prover}\ (\mathrm{CRS}_p,\ \mathbf{y} = [\mathbf{M}\mathbf{x}]_1,\ \mathbf{x},\ \text{label } \mathtt{lbl})$:
Sample $(\mathbf{r}, \mathbf{r}_z^1, \mathbf{r}_z^2) \leftarrow \mathbb{Z}_q^k \times \mathbb{Z}_q^k \times \mathbb{Z}_q^k$.
Set $\boldsymbol{\rho} := [\bar{\mathbf{B}}\mathbf{r}]_1^\top,\ \hat{\boldsymbol{\rho}} := [\underline{\mathbf{B}}\mathbf{r}]_1^\top$.

Set $z := 0,\ \mathsf{ct}_z^1 := \mathsf{PKE.Enc}(\mathsf{pk}_1, z; \mathbf{r}_z^1)$ and $\mathsf{ct}_z^2 := \mathsf{PKE.Enc}(\mathsf{pk}_2, z; \mathbf{r}_z^2)$.

Set $\pi_0 := \Pi_0.\mathsf{prover}(\mathrm{CRS}^0,\ (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \mathsf{ct}_z^1 - \mathsf{ct}_x),\ (\mathbf{r}, 0))$.
Set $\pi_1 := \Pi_1.\mathsf{prover}(\mathrm{CRS}_p^1,\ (\mathsf{ct}_z^1, \mathsf{ct}_z^2),\ (0, \mathbf{r}_z^1, \mathbf{r}_z^2))$.

Set $\tau := \mathsf{crh}(\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \mathsf{ct}_z^1, \mathsf{ct}_z^2, \pi_0, \pi_1, \mathtt{lbl})$.
Set $\gamma := \mathbf{x}^\top [\mathbf{p}_1]_1 + \mathbf{r}^\top [\mathbf{p}_2 + \tau \mathbf{p}_3]_1$.
Set $\pi_2 := \Pi_2.\mathsf{prover}(\mathrm{CRS}_p^2,\ (\mathbf{y}, \boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \mathrm{tag} = \tau),\ (\mathbf{x}, \mathbf{r}))$.

Return $\pi := (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \mathsf{ct}_z^1, \mathsf{ct}_z^2, \pi_0, \pi_1, \pi_2)$.

$\mathsf{ver}\ (\mathrm{CRS}_v,\ \mathbf{y},\ \pi,\ \mathtt{lbl})$:
Set $\tau := \mathsf{crh}(\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \mathsf{ct}_z^1, \mathsf{ct}_z^2, \pi_0, \pi_1, \mathtt{lbl})$.
Check all the NIZK proofs:
$\Pi_0.\mathsf{ver}(\mathrm{CRS}^0,\ (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \mathsf{ct}_z^1 - \mathsf{ct}_x),\ \pi_0)$
and $\Pi_1.\mathsf{ver}(\mathrm{CRS}_v^1,\ (\mathsf{ct}_z^1, \mathsf{ct}_z^2),\ \pi_1)$
and $\Pi_2.\mathsf{ver}(\mathrm{CRS}_v^2,\ (\mathbf{y}, \boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \mathrm{tag} = \tau),\ \pi_2)$.

Languages:

Π_0 is an OR-NIZK for $L_0 \stackrel{\text{def}}{=} \{(\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \mathsf{ct}) \mid \exists (\mathbf{r}, \mathbf{r}_c) :\ (\boldsymbol{\rho} = [\bar{\mathbf{B}}\mathbf{r}]_1^\top$ **and** $\hat{\boldsymbol{\rho}} = [\underline{\mathbf{B}}\mathbf{r}]_1^\top)$ **or** $\mathsf{ct} = \mathsf{PKE.Enc}(\mathsf{pk}_1, 0; \mathbf{r}_c)\}$.

Π_1 is a QA-NIZK for $L_1 \stackrel{\text{def}}{=} \{(\mathsf{ct}_z^1, \mathsf{ct}_z^2) \mid \exists (z, \mathbf{r}_z^1, \mathbf{r}_z^2) : \mathsf{ct}_z^1 = \mathsf{PKE.Enc}(\mathsf{pk}_1, z; \mathbf{r}_z^1)$ **and** $\mathsf{ct}_z^2 = \mathsf{PKE.Enc}(\mathsf{pk}_2, z; \mathbf{r}_z^2)\}$, with parameters $(\mathsf{pk}_1, \mathsf{pk}_2)$.

Π_2 is a QA-NIZK for $L_2 \stackrel{\text{def}}{=} \{(\mathbf{y}, \boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \mathrm{tag} = \tau) \mid \exists (\mathbf{x}, \mathbf{r}) : \mathbf{y} = [\mathbf{M}\mathbf{x}]_1$ **and** $\boldsymbol{\rho} = [\bar{\mathbf{B}}\mathbf{r}]_1^\top$ **and** $\hat{\boldsymbol{\rho}} = [\underline{\mathbf{B}}\mathbf{r}]_1$ **and** $\gamma = \mathbf{x}^\top [\mathbf{p}_1]_1 + \mathbf{r}^\top [\mathbf{p}_2 + \tau \mathbf{p}_3]_1\}$, with parameters $([\mathbf{M}]_1, [\mathbf{B}]_1, [\mathbf{p}_1]_1, [\mathbf{p}_2]_1, [\mathbf{p}]_3)$.

Fig. 4. Labeled Tightly-secure USS-QA-NIZK Π', with $O(\log Q)$ reduction to $\mathcal{D}_k$-MDDH.

In more details, let the combined language be defined by the matrix $\mathbf{M} = \begin{pmatrix} \mathbf{M}_1^{n_1 \times t} \\ \mathbf{M}_2^{n_2 \times t} \end{pmatrix}$, where both n_1 and n_2 are greater than t. What we show is, provided the words corresponding to $[\mathbf{M}_1]_1$ are not faked then even if the words corresponding to $[\mathbf{M}_2]_1$ are faked, true-simulation-soundness holds for the $[\mathbf{M}_1]_1$ components.

4 NIZK for Disjunction of Linear Subspaces

We have critically used an "OR"-NIZK in our USS-QA-NIZK construction. In this section we describe three flavors of OR-NIZKs. The first one is a standard NIZK where both the prover and verifier are public algorithms. The second one is a designated prover system where only the verifier is public - this flavor is useful for signature schemes where the signing key is held private. The final one is a designated verifier system where the prover is public, but the verifier is private - this is useful in public-key encryption schemes where the public encryption algorithm is required to prove consistency, but only the private decryption algorithm needs to check a proof.

4.1 Public CRS Setting

In this section we describe a NIZK proof system for languages of the following type:

$$L^{\vee} \stackrel{\text{def}}{=} \left\{ \begin{array}{c} ([\mathbf{x}_0]_1, [\mathbf{x}_1]_1) \in \mathbb{G}_1^{n_0} \times \mathbb{G}_1^{n_1} | \\ \exists \mathbf{r}_0 \in \mathbb{Z}_q^{t_0} : [\mathbf{x}_0]_1 = [\mathbf{A}_0]_1 \mathbf{r}_0 \textbf{ or } \exists \mathbf{r}_1 \in \mathbb{Z}_q^{t_1} : [\mathbf{x}_1]_1 = [\mathbf{A}_1]_1 \mathbf{r}_1 \end{array} \right\}$$

The system is described in Fig. 5 and is based on [Ràf15] with syntax based on [GHKP18]. The proofs of completeness, zero-knowledge and soundness are similar to these papers. We only give a sketch below.

The completeness of the system is straightforward. Zero-knowledge is proved by transitioning to a different way of generating the CRS along with a trapdoor. The transition is enabled by the $\mathcal{D}_k$-MDDH assumption on $([\mathbf{D}]_1, [\mathbf{z}]_1)$ and the resulting CRS and proof simulators are also given in the same figure.

We now prove perfect soundness. Since $\mathbf{z}_0 + \mathbf{z}_1 = \mathbf{z} \notin \text{span}(\mathbf{D})$, at least one of $\mathbf{z}_0$ and $\mathbf{z}_1$ should be outside the span of $\mathbf{D}$. WLOG, let this be $\mathbf{z}_0$. Therefore, there should be a vector $\mathbf{d}^{\perp} \in \mathbb{Z}_q^{k+1}$, such that $\mathbf{D}^{\top}\mathbf{d}^{\perp} = \mathbf{0}$ and $\mathbf{z}_0^{\top}\mathbf{d}^{\perp} = 1$. Right multiplying this vector to the verification equation $\mathbf{A}_0\mathbf{C}_0 = \mathbf{P}_0\mathbf{D}^{\top} + \mathbf{x}_0\mathbf{z}_0^{\top}$ gives us $\mathbf{A}_0\mathbf{C}_0\mathbf{d}^{\perp} = \mathbf{x}_0$. This means $\mathbf{r}_0 \stackrel{\text{def}}{=} \mathbf{C}_0\mathbf{d}^{\perp}$ satisfies the disjunct $\mathbf{x}_0 = \mathbf{A}_0\mathbf{r}_0$.

4.2 Designated Prover Setting

In Fig. 5 we saw an efficient NIZK proof for the "OR" language of Fig. 1, where one of the disjuncts was a predicate on group elements in the CRS of the USS-QA-NIZK, namely that ct_x was a binding commitment to x (using randomness

OR Languages :

Let $L^{\vee} \stackrel{\text{def}}{=} \left\{ \begin{array}{c} ([\mathbf{x}_0]_1, [\mathbf{x}_1]_1) \in \mathbb{G}_1^{n_0} \times \mathbb{G}_1^{n_1} | \\ \exists \mathbf{r}_0 \in \mathbb{Z}_q^{t_0} : \mathbf{x}_0 = [\mathbf{A}_0 \mathbf{r}_0]_1 \textbf{ or } \exists \mathbf{r}_1 \in \mathbb{Z}_q^{t_1} : [\mathbf{x}_1]_1 = [\mathbf{A}_1 \mathbf{r}_1]_1 \end{array} \right\}$.

$\mathsf{crsgen}\ (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2)$:
Sample $\mathbf{D} \leftarrow \mathcal{D}_k$-MDDH and $\mathbf{z} \leftarrow \mathbb{Z}_q^{k+1} \setminus \mathrm{span}(\mathbf{D})$.
Return $\mathrm{CRS} := ([\mathbf{D}]_2, [\mathbf{z}]_2)$.

$\mathsf{prover}\ (\mathrm{CRS},\ ([\mathbf{x}_0]_1, [\mathbf{x}_1]_1),\ (j, \mathbf{r}_j))$:
Sample $(\mathbf{v},\ \mathbf{S}_0, \mathbf{S}_1) \leftarrow \mathbb{Z}_q^k \times \mathbb{Z}_q^{t_0 \times k} \times \mathbb{Z}_q^{t_1 \times k}$.
Set $[\mathbf{z}_{1-j}]_2 := [\mathbf{D}]_2 \mathbf{v}$ and $[\mathbf{z}_j]_2 := [\mathbf{z}]_2 - [\mathbf{z}_{1-j}]_2$.
Set $[\mathbf{C}_j]_2 := \mathbf{S}_j [\mathbf{D}]_2^\top + \mathbf{r}_j [\mathbf{z}_j]_2^\top$ and $[\mathbf{P}_j]_1 := [\mathbf{A}_j]_1 \mathbf{S}_j$.
Set $[\mathbf{C}_{1-j}]_2 := \mathbf{S}_{1-j} [\mathbf{D}]_2^\top$ and $[\mathbf{P}_{1-j}]_1 := [\mathbf{A}_{1-j}]_1 \mathbf{S}_{1-j} - [\mathbf{x}_j]_1 \mathbf{v}^\top$.
Return $\pi := ([\mathbf{z}_0]_2, [\mathbf{C}_0]_2, [\mathbf{P}_0]_1, [\mathbf{C}_1]_2, [\mathbf{P}_1]_1) \in \mathbb{G}_1^{(n_0+n_1)k} \times \mathbb{G}_2^{(t_0+t_1+1)(k+1)}$.

$\mathsf{ver}\ (\mathrm{CRS},\ ([\mathbf{x}_0]_1, [\mathbf{x}_1]_1),\ \pi)$:
Set $[\mathbf{z}_1]_2 := [\mathbf{z}]_2 - [\mathbf{z}_0]_2$.
Check the following equations for all $j \in \{0, 1\}$:
$\mathsf{e}([\mathbf{A}_j]_1, [\mathbf{C}_j]_2) = \mathsf{e}([\mathbf{P}_j]_1, [\mathbf{D}]_2^\top) \cdot \mathsf{e}([\mathbf{x}_j]_1, [\mathbf{z}_j]_2^\top)$.

$\mathsf{crssim}\ (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2)$:
Sample $\mathbf{D} \leftarrow \mathcal{D}_k$-MDDH and $\mathbf{u} \leftarrow \mathbb{Z}_q^k$.
Set $\mathbf{z} := \mathbf{D}\mathbf{u}$
Return $\mathrm{CRS} := ([\mathbf{D}]_2, [\mathbf{z}]_2)$ and $\mathsf{trap} := \mathbf{u}$.

$\mathsf{sim}\ (\mathrm{CRS},\ \mathsf{trap},\ ([\mathbf{x}_0]_1, [\mathbf{x}_1]_1))$:
Sample $(\mathbf{v},\ \mathbf{S}_0, \mathbf{S}_1) \leftarrow \mathbb{Z}_q^k \times \mathbb{Z}_q^{t_0 \times k} \times \mathbb{Z}_q^{t_1 \times k}$.
Set $[\mathbf{z}_0]_2 := [\mathbf{D}]_2 \mathbf{v}$ and $[\mathbf{z}_1]_2 := [\mathbf{z}]_2 - [\mathbf{z}_0]_2$.
Set $[\mathbf{C}_0]_2 := \mathbf{S}_0 [\mathbf{D}]_2^\top$ and $[\mathbf{P}_0]_1 := [\mathbf{A}_0]_1 \mathbf{S}_0 - [\mathbf{x}_0]_1 \mathbf{v}^\top$.
Set $[\mathbf{C}_1]_2 := \mathbf{S}_1 [\mathbf{D}]_2^\top$ and $[\mathbf{P}_1]_1 := [\mathbf{A}_1]_1 \mathbf{S}_1 - [\mathbf{x}_1]_1 (\mathbf{u} - \mathbf{v})^\top$.
Return $\pi := ([\mathbf{z}_0]_2, [\mathbf{C}_0]_2, [\mathbf{P}_0]_1, [\mathbf{C}_1]_2, [\mathbf{P}_1]_1)$.

Fig. 5. NIZK for OR languages based on [Ràf15].

r_x). The quantity r_x cannot be made public in this general setting as proving simulation-soundness requires us to hide x from the public. However, in the application of USS-QA-NIZK to build SPS, the quantity r_x can indeed be given to a "designated" prover, i.e. the signer, and the quantity still remains private. In particular, in a forgery attempt, the adversary does not have access to r_x, as the signer is an honest party. In such a situation, i.e. where r_x in the commitment to x is available to the designated prover, we can give an even more efficient

NIZK. For ease of exposition, we will restrict ourselves to the SXDH asymmetric pairings-group setting in this section. The results can easily be generalized to $\mathcal{D}_k$-MDDH setting.

Consider the "OR" language,

$$\mathcal{L} = \left\{ \begin{array}{c} \boldsymbol{\alpha}, \hat{\boldsymbol{\alpha}}, \boldsymbol{x} \mid \exists r, r_x \in \mathbb{Z}_q : \\ (\boldsymbol{\alpha} = r[1]_1 \textbf{ and } \hat{\boldsymbol{\alpha}} = r[b]_1) \textbf{ or } \boldsymbol{x} = \mathrm{com}(0; r_x) \end{array} \right\}$$

where $\mathrm{com}(x; r_x)$ is a binding commitment to x using randomness r_x (e.g. a GS-commitment or ElGamal encryption), and $[b]_1$ is public.

It is not difficult to see that the above is implied by the following (i.e. $\mathcal{L}_1 \subseteq \mathcal{L}$)

$$\mathcal{L}_1 = \left\{ \begin{array}{c} \boldsymbol{\alpha}, \hat{\boldsymbol{\alpha}}, \boldsymbol{x} \mid \exists x, r_x, \hat{x} \in \mathbb{Z}_q : \\ \hat{\boldsymbol{\alpha}} \cdot x - [b]_1 \cdot \hat{x} = 0 \textbf{ and } [1]_1 \cdot \hat{x} - \boldsymbol{\alpha} \cdot x = 0 \textbf{ and } \boldsymbol{x} = \mathrm{com}(x; r_x) \end{array} \right\}$$

since if $x \neq 0$ in $\mathcal{L}_1$, one can take $r = \hat{x}/x$, and otherwise $\boldsymbol{x}$ is commitment to zero with r_x. Thus soundness of NIZK proof of $\mathcal{L}_1$ implies the tuple is in $\mathcal{L}$.

Now, consider another language $\mathcal{L}_2$,

$$\mathcal{L}_2 = \left\{ \begin{array}{c} \boldsymbol{\alpha}, \hat{\boldsymbol{\alpha}}, \boldsymbol{x} \mid \exists r, x, r_x \in \mathbb{Z}_q : \\ ((\boldsymbol{\alpha} = r[1]_1 \textbf{ and } \hat{\boldsymbol{\alpha}} = r[b]_1) \textbf{ or } (x = 0)) \textbf{ and } \boldsymbol{x} = \mathrm{com}(x; r_x) \end{array} \right\}$$

Thus, in the language the value $\boldsymbol{x}$ is always a commitment to x under r_x. First note that $\mathcal{L}_2$ implies $\mathcal{L}_1$, i.e. $\mathcal{L}_2 \subseteq \mathcal{L}_1$. This is so because if $x = 0$ in $\mathcal{L}_2$, then we just set $\hat{x} = 0$ as well, and if there is a good r, then we set $\hat{x} = r \cdot x$.

Since the "designated" prover always knows x and r_x in the commitment $\boldsymbol{x}$, then if it has an (r, x) which satisfies the "or" part of $\mathcal{L}_2$, it can generate the witnesses required to satisfy membership in $\mathcal{L}_1$ and hence give a valid NIZK proof.

Under the SXDH assumption, $\mathcal{L}_1$ can be proved by using two group elements and in addition two elements for commitment to $\hat{x}$ (and not counting the two for $\boldsymbol{x}$ which is commitment to x) using the technique by Escala and Groth in [EG14]. Namely, the size of π_0 is $(2, 2)$. For this to work, we also need to sample public keys pk_1 of ElGamal encryption (i.e. com) from $\mathbb{G}_2$. Furthermore, pk_1 is taken from CRS^1 (see Fig. 1). We note that this dependency of pk_1 to CRS^1 does not affect the security proof since we can use ciphertext with respect to pk_2 when CRS^1 is set to the simulation mode. We further optimize ct_z^1 and ct_z^2 by applying the common randomness technique from Sect. 3.3. With these modifications, ct_z^1 and ct_z^2 together consist of $(0, 3)$ elements, and proof π_1 is a single element in $\mathbb{G}_2$ (rather than in $\mathbb{G}_1$ in the original construction). Other components, $\boldsymbol{\rho}$, $\hat{\boldsymbol{\rho}}$, γ, and π_2 are unchanged; each of them is represented by a single element in $\mathbb{G}_1$. In total, the proof size will be $(6, 6)$. Under general $\mathcal{D}_k$-MDDH assumption, the optimized proof will consist of $(5k + 1, 4k + 2)$ elements.

Finally we note that in the designated prover setting, the scheme Π_1 can be made $O(\log Q)$-reduction secure, while maintaining its structure-preserving property. Essentially we add an affine constant to γ as done in [JOR18]. In the split-CRS QA-NIZK setting, this constant would only appear in the prover CRS. This still lets the security proof go through as the adversary's view at the final game would be independent of this affine constant.

4.3 Designated Verifier Setting

As the most expensive part (from the size of USS-QA-NIZK perspective and applications) is the size of the "OR"-proof considered in our general construction, we now consider the designated-verifier setting [ES02]. In the designated-verifier setting of a NIZK, the CRS is split into two parts, CRS_p and CRS_v, and only a designated-verifier gets access to CRS_v and the public information is only CRS_p (required by the prover). Alternatively, one can think of designated-verifier NIZKs as hash-proof systems, as the CRS_v is just the secret hash-key, and CRS_p is the projection hash-key – by the fact that hash-proofs can be generated without the witness (but using the secret hash-key), zero-knowledge is automatic; further, soundness is information-theoretic. Since hash-proofs for linear subspace languages are well known [CS98], and we even have hash-proofs for "OR"-languages [ABP15], so we have designated-verifier NIZK proofs for our "OR"-language used in the USS-QA-NIZK construction. Consequently, we have smaller sized (almost) tightly-secure designated-verifier USS-QA-NIZKs.

For this idea to work, we instantiate PKE in $\mathbb{G}_2$ in our construction so that the OR-language consists of relations from both $\mathbb{G}_1$ and $\mathbb{G}_2$. This allows us to use the hash proof system of [ABP15]. The downside of such a construction is that we have more $\mathbb{G}_2$ elements in the proof and the USS-QA-NIZK is itself in the target group $\mathbb{G}_T$, as the construction of [ABP15] generates hashes in the target group. Since these elements require much longer representation we give a more precise estimation. In the original construction of our USS-QA-NIZK with optimizations in Sect. 3.3, a proof consists of $(11, 6)$ elements in the SXDH setting, of which $(3, 6)$ are for proof π_0. In remaining $(8, 0)$ elements, $(4, 0)$ are the ciphertext of PKE and proof π_1. Moving the $(4, 0)$ elements to $\mathbb{G}_2$ and replacing $(3, 6)$ of π_0 with a target group element, the proof size of our designated-verifier USS-QA-NIZK will be $(4, 4)$ source group elements and 1 target group element. Thus it saves $(7, 2)$ elements in exchange of having an extra target group element. Since the target group element is computed from a product of four pairings, it can also be represented by randomized $(4, 4)$ group elements by using the PPE randomization technique of [AFG+16]. However, either representation requires larger space than original $(7, 2)$ elements. Thus, the known approach with [ABP15] does not seem to yield shorter proofs than our original construction in the designated verifier setting.

5 Applications

In this section, we demonstrate that our tightly secure USS-QA-NIZK can be used to develop CCA2-secure public key encryption and structure-preserving signatures (SPS). Besides being (almost) tightly secure under standard matrix assumptions in bilinear groups, these applications have particular advantage over previous constructions. Our CCA2-secure public-key encryption is *publicly verifiable* and our SPS scheme yields the *shortest signatures*. By plugging our CCA2-secure public key encryption and SPS into the generic frameworks of blind signatures [Fis06], group signatures [Gro07], and simulation-sound NIZKs [CCS09]

we have blind SPS, group SPS, and simulation-sound Groth-Sahai proofs, all of which have (almost) tight reduction to standard matrix assumptions in bilinear groups and efficiency improvements over known schemes. Details for these plug-in applications are given in the full version of this paper.

5.1 (Almost) Tight CCA2-Secure PKE Scheme

In this section we show that the labelled (enhanced) USS-QANIZK for linear-subspaces can be used to build a publicly verifiable labeled CCA-secure public-key encryption (PKE) scheme (described in Fig. 6) which is (almost) tightly-secure in the multi-user, multi-challenge setting. The security reduction to USS-QANIZK is tight and is independent of the number of decryption-oracle requests of the CCA2 adversary.

$\mathsf{KeyGen}\ (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2)$:
[Boost distribution $\mathcal{D}_{k+1,k}$ to $\mathcal{D}_{2k,k}$.]
Sample $\mathbf{B} \leftarrow \mathcal{D}_{2k,k}$-MDDH and $\mathbf{k} \leftarrow \mathbb{Z}_q^k$,
Sample $(\mathrm{CRS}_p, \mathrm{CRS}_v) \leftarrow \Pi'.\mathsf{crsgen}(\langle q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2\rangle, [\mathbf{B}]_1)$,
Set $\mathbf{p} := \bar{\mathbf{B}}^\top \mathbf{k}$, $\mathsf{pk} := (\mathrm{CRS}_p, [\mathbf{B}]_1, [\mathbf{p}]_1)$, $\mathsf{sk} := (\mathrm{CRS}_v, \mathbf{k})$.

Return $(\mathsf{pk}, \mathsf{sk})$.

$\mathsf{Enc}\ (\mathsf{pk} = (\mathrm{CRS}_p, [\mathbf{B}], [\mathbf{p}]_1),\ M \in \mathbb{G}_1,\ \mathtt{lbl})$:
Sample $\mathbf{r} \leftarrow \mathbb{Z}_q^k$, and set $\boldsymbol{\rho} := [\bar{\mathbf{B}}\mathbf{r}]_1^\top,\ \hat{\boldsymbol{\rho}} := [\underline{\mathbf{B}}\mathbf{r}]_1^\top,\ \gamma := M + \mathbf{r}^\top[\mathbf{p}]_1$,
$\pi := \Pi'.\mathsf{prover}(\mathrm{CRS}_p, \langle \boldsymbol{\rho}, \hat{\boldsymbol{\rho}}\rangle, \langle \gamma, \mathtt{lbl}\rangle; \mathbf{r})$.

Return $\mathtt{ctxt} := (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \pi)$.

$\mathsf{Dec}\ (\mathsf{sk} = (\mathrm{CRS}_v, \mathbf{k}),\ \mathtt{ctxt} = (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \pi),\ \mathtt{lbl})$:
If the NIZK proof verification
$\Pi'.\mathsf{ver}(\mathrm{CRS}_v,\ \langle \boldsymbol{\rho}, \hat{\boldsymbol{\rho}}\rangle,\ \langle \gamma, \mathtt{lbl}\rangle,\ \pi)$
returns true then return $\gamma - \boldsymbol{\rho}\mathbf{k}$ else return $\perp$.

Language for Π':
$L \stackrel{\text{def}}{=} \{(\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}) \mid \exists \mathbf{r} :\ \boldsymbol{\rho} = [\bar{\mathbf{B}}\mathbf{r}]_1^\top$ **and** $\hat{\boldsymbol{\rho}} = [\underline{\mathbf{B}}\mathbf{r}]_1^\top\}$ with parameters $([\mathbf{B}]_1)$.

Fig. 6. CCA2 Public-Key Encryption using labelled (strong) USS-QA-NIZK.

Theorem 4. *Under the $\mathcal{D}_k$-MDDH assumption, and using the labeled USS-QANIZK Π' of Fig. 4, the public-key encryption scheme described in Fig. 6 is (μ, q_e) IND-CCA secure with Adversary's advantage $\mathcal{A}$ upper-bounded by*

$$2 \cdot \mathrm{ADV}^{\mathsf{tss}}_{\Pi'} + 6k \cdot \mathrm{ADV}_{\mathcal{D}_k\text{-MDDH}} + 2 \cdot \mathrm{ADV}^{\mathsf{uss}}_{\Pi'}(q_e) + O(1/q).$$

The proof of this theorem can be found in the full paper.

Remark. The public-key encryption construction in Fig. 6, during encryption, uses randomness $\mathbf{r}$ to construct $\boldsymbol{\rho}$. Then, it calls USS-QA-NIZK prover in a black-box manner to obtain π. The USS-QANIZK construction itself picks another $\mathbf{s}$ and constructs its own $\boldsymbol{\rho}$. We remark that in a non-black box construction of tight CCA2-secure public key encryption scheme, i.e. by utilizing the USS-QA-NIZK construction in a non-black fashion, one can use the same $\mathbf{B}$ matrix in the PKE construction above and the USS-QANIZK construction, while keeping $\underline{\mathbf{B}}$ matrices sampled randomly and independently. This leads to a savings of k group elements. The proof of the (almost) tight security of this scheme combines the proof given in the full paper with the proof of the USS-QANIZK tight-security (Theorem 2).

5.2 Direct Construction of Tight SPS from Tight USS-QA-NIZK

Recall that unbounded simulation-soundness assures that, after having simulated proofs for any instances of adversary's choice, it is hard for the adversary to find a valid proof for any fresh no-instances. This corresponds to the notion of unforgeability against adaptive chosen message attacks of a signature scheme where no adversary can find a valid signature for any fresh messages after seeing signatures for any chosen messages. Indeed, syntactically, an unbounded simulation-sound NIZK system can be seen as a signature scheme whose key generation, signature generation, and signature verification functions correspond to CRS simulation, proof simulation, and proof verification functions of the NIZK system, respectively. For this translation to work in reality, it is required that the NIZK system allows simulation for any no-instance in a certain set and there exists a collision resistant mapping (ideally injection) from the desired message space for the signature scheme to the set of no-instances. In [AAO18], this intuition is proven formally in a more general setting (allowing errors in correctness, etc). We use the simplest form of their result with adjustment to the syntax of USS-QA-NIZK.

Let $\Pi := (\mathsf{pargen}, \mathsf{crsgen}, \mathsf{prover}, \mathsf{ver}, \mathsf{crssim}, \mathsf{sim})$ be a designated prover USS-QANIZK system for $\mathcal{L} := \mathrm{span}([\mathbf{M}]_1) \subset \mathbb{G}_1^n$ with soundness advantage $\mathsf{Adv}^{\mathsf{uss}}_{\Pi}(A)$. We assume that Π is *perfectly no-instance simulation correct* with respect to $\mathcal{C} := \mathbb{G}_1^n \setminus \mathrm{span}([\mathbf{M}]_1)$ which means that, for any CRS_v and trap generated by $\Pi.\mathsf{crssim}$, $y \in \mathcal{C}$, $\pi \leftarrow \Pi.\mathsf{sim}(\mathsf{trap}, y)$, $1 \leftarrow \Pi.\mathsf{ver}(\mathrm{CRS}_v, y, \pi)$ holds with probability 1.

Let $[\mathbf{M}]_1 \leftarrow \mathbb{G}_1^{n \times t}$ denote a sampling where matrix $\mathbf{M}$ is chosen uniformly with constraint that its upper square sub-matrix is full rank. For message space $\mathcal{M} := \mathbb{G}_1^t$ and $n \geq 2t+1$, we construct a function $H : \mathcal{M} \to \mathcal{C}$ as follows. Choose $\mathbf{c}$ uniformly from $\mathbb{G}_1^{n-t}$. Then define $H(M)$ for $M \in \mathbb{G}_1^t$ as $M||\mathbf{c}$. For any $\mathbf{M}$ and $M \in \mathbb{G}_1^t$, with probability at least $1 - 1/q$ over the choice of $\mathbf{c}$, there exists no x that satisfies $(M||\mathbf{c})^\top = [\mathbf{M}x]_1$. Thus H is an efficiently computable injection from $\mathcal{M}$ to $\mathcal{C}$. Following this idea, we construct a signature scheme as shown in Fig. 7.

Theorem 5. *With the above USS-QA-NIZK system Π, SIG in Fig. 7 is a signature scheme for message space $\mathcal{M} := \mathbb{G}_1^t$. It is tightly unforgeable against*

Common parameters: $\mathsf{par} := (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2, [\mathbf{M}]_1 \in \mathbb{G}_1^{n\times t})$.

$\mathsf{KeyGen}(1^m)$:
$\lambda := (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2) \leftarrow \Pi.\mathsf{pargen}(1^m)$
$[\mathbf{M}]_1 \leftarrow \mathbb{G}_1^{n\times t}$
$\mathbf{c} \leftarrow \mathbb{G}_1^{n-t}$
$(\mathrm{CRS}, \mathsf{trap}) \leftarrow \Pi.\mathsf{crssim}(\lambda, [\mathbf{M}]_1)$
$\mathsf{pk} := (\mathrm{CRS}, \mathbf{c})$, $\mathsf{sk} := (\mathsf{trap}, \mathbf{c})$
$\mathsf{return}(\mathsf{pk}, \mathsf{sk})$

$\mathsf{Sign}(\mathsf{sk}, M)$:
$(\mathsf{trap}, \mathbf{c}) \leftarrow \mathsf{sk}$
$\mathbf{y} := M||\mathbf{c}$
$\sigma \leftarrow \Pi.\mathsf{sim}(\mathsf{trap}, y)$
$\mathsf{return}(\sigma)$

$\mathsf{Verify}(\mathsf{pk}, M, \sigma)$:
$(\mathrm{CRS}, \mathbf{c}) \leftarrow \mathsf{pk}$
$\mathbf{y} := M||\mathbf{c}$
$b \leftarrow \Pi.\mathsf{ver}(\mathrm{CRS}_v, y, \sigma)$
$\mathsf{return}(b)$

Fig. 7. Signature scheme SIG for unilateral messages in $\mathbb{G}_1^t$ based on USS-QA-NIZK Π for a linear subspace language.

adaptive chosen message attacks, i.e., for every PPT *adversary* $\mathcal{A}$ *breaking the unforgeability of* SIG *with a chosen message attack with advantage* $\mathsf{Adv}^{\mathsf{cma}}_{\mathsf{SIG}}(\mathcal{A})$*, there exists a* PPT *algorithm* $\mathcal{B}$ *that breaks the unbounded simulation soundness of* Π *with advantage* $\mathsf{Adv}^{\mathsf{uss}}_{\Pi}(\mathcal{B}) \geq \mathsf{Adv}^{\mathsf{cma}}_{\mathsf{SIG}}(\mathcal{A}) - 1/q$ *and almost the same running time as* $\mathcal{A}$*. Furthermore, if* Π *is structure preserving, so is* SIG*.*

Proof. To show unforgeability, we construct $\mathcal{B}$ using $\mathcal{A}$ as black-box as follows. Given CRS, $[\mathbf{M}]_1$, $\mathcal{B}$ picks $c \leftarrow \mathbb{G}_1^{n-t}$ and send $\mathsf{pk} := (\mathrm{CRS}, \mathbf{c})$ to $\mathcal{A}$. For message M queried from $\mathcal{A}$, $\mathcal{B}$ sends $\mathbf{y} := M||\mathbf{c}$ to its oracle, receives a simulated proof π, and returns $\sigma := \pi$ to $\mathcal{A}$. Given a forgery M^*, σ_* from $\mathcal{A}$, $\mathcal{B}$ outputs $\mathbf{y}^* := M^*||\mathbf{c}$ and $\pi^* := \sigma^*$. Since $H(M) := M||\mathbf{c}$ is an injection to $\mathbb{G}_1^n \backslash \mathrm{span}([\mathbf{M}]_1)$ with probability at least $1 - 1/q$, $\mathbf{y}^*$ is a fresh instance not in $\mathrm{span}([\mathbf{M}]_1)$, and $(\mathbf{y}^*, \pi^*)$ passes the verification whenever $\mathcal{A}$ succeeds. Hence we have $\mathsf{Adv}^{\mathsf{uss}}_{\Pi}(\mathcal{B}) \geq \mathsf{Adv}^{\mathsf{cma}}_{\mathsf{SIG}}(\mathcal{A}) - 1/q$. Running time of $\mathcal{B}$ is the same as $\mathcal{A}$ except for performing concatenation and parsing. Structure-preserving property is obvious from the construction.

We remark that we can remove the negligible $1/q$ term in the above bound in an enhanced model [LPJY15, JR13] where $\mathbf{M}$ is given to the adversary playing the simulation soundness game.

In Fig. 8 we present an instantiation of SIG in Fig. 7 using our optimized designated prover USS-QA-NIZK from Sect. 4.2 under the SXDH assumption. Designated prover is sufficient in this application as the signing key is private. The signature size is exactly the same as the proof size of the underlying USS-QA-NIZK and it retains structure preserving property. Hence the signature scheme in Fig. 8 is an SPS scheme having signatures consisting of $(6, 6)$ elements for unilateral messages. (Under $\mathcal{D}_k$-MDDH assumption, the signature size will be $(5k + 1, 4k + 2)$). For bilateral messages $(M_1, M_2) \in \mathbb{G}_1^{t_1} \times \mathbb{G}_2^{t_2}$ where $t_1 = t - 1$,

Common parameters: $\mathsf{par} := (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2, [\mathbf{M}]_1 \in \mathbb{G}_1^{n\times t})$.

$\mathsf{KeyGen}(\mathsf{par})$:
Sample $\mathrm{CRS}^0 \leftarrow \Pi_0.\mathsf{crsgen}(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2)$,
$(\mathrm{CRS}_p^1, \mathrm{CRS}_v^1) \leftarrow \Pi_1.\mathsf{crsgen}(\mathsf{par})$, and $(\mathrm{CRS}_p^2, \mathrm{CRS}_v^2, \mathsf{trap}^2) \leftarrow \Pi_2.\mathsf{crssim}(\mathsf{par})$.
Let $([u_1]_2, [u_2]_2, [u_3]_2)$ denote elements of $\mathbb{G}_2$ in CRS^0.
Set $\mathsf{pk}_1 := [u_3]_2$ and $\mathsf{sk}_1 := u_3$.
Sample $\mathsf{sk}_2 \leftarrow \mathbb{Z}_q$ and set $\mathsf{pk}_2 := [\mathsf{sk}_2]_2$.
Sample $\mathbf{B} \leftarrow \mathcal{D}_{2,1}$-MDDH and $(\mathbf{k}_1, \mathsf{k}_2) \leftarrow \mathbb{Z}_{\mathsf{q}}^{\mathsf{n}} \times \mathbb{Z}_{\mathsf{q}}$.
Set $\mathsf{p}_1 := \mathbf{M}^\top \mathbf{k}_1$ and $\mathsf{p}_2 := \bar{\mathbf{B}}^\top \mathsf{k}_2$
Sample $\mathsf{r}_x \leftarrow \mathbb{Z}_q$. Set $x := 0$, $R_x := [\mathsf{r}_x]_2$, and $E_x := [x]_2 + \mathsf{r}_x\, \mathsf{pk}_1$.
Set $\mathrm{CRS}_p := (\mathrm{CRS}^0, \mathrm{CRS}_p^1, \mathrm{CRS}_p^2, [\mathbf{B}]_1, [\mathbf{p}_1]_1, [\mathbf{p}_2]_1, \mathsf{pk}_1, \mathsf{pk}_2, E_x, R_x)$.
Set $\mathrm{CRS}_v := (\mathrm{CRS}^0, \mathrm{CRS}_v^1, \mathrm{CRS}_v^2, [\mathbf{B}]_1, \mathsf{pk}_1, \mathsf{pk}_2, E_x, R_x)$.
Set $\mathsf{trap} := (\mathbf{k}_1, \mathsf{trap}^2)$.
Set $\mathbf{c} \leftarrow \mathbb{G}_1^{n-t}$.
Set $\mathsf{pk} := (\mathrm{CRS}_v, \mathbf{c})$, $\mathsf{sk} := (\mathrm{CRS}_p, \mathsf{trap}, \mathbf{c})$.
Return $(\mathsf{pk}, \mathsf{sk})$.

$\mathsf{Sign}(\mathsf{sk}, M \in \mathbb{G}_1^t)$:
Parse $(\mathsf{trap}, \mathbf{c}) \leftarrow \mathsf{sk}$, and set $\mathbf{y} := M||\mathbf{c}$.
Sample $(\mathbf{r}, \mathsf{r}_z) \leftarrow \mathbb{Z}_q \times \mathbb{Z}_q$.
Set $\rho := [\bar{\mathbf{B}}\mathbf{r}]_1^\top$, $\hat{\rho} := [\underline{\mathbf{B}}\mathbf{r}]_1^\top$, $\gamma := \mathbf{y}^\top \mathbf{k}_1 + \mathsf{r}^\top [\mathsf{p}_2]_1$.
Set $z := 0$. Compute $R_z := [\mathsf{r}_z]_2$.
Compute $E_z^i := [z]_2 + \mathsf{r}_z\, \mathsf{pk}_i$ for $i = 1, 2$.
Set $E_\delta := E_z^1 - E_x$, $R_\delta := R_z - R_x$, $\mathsf{r}_\delta := \mathsf{r}_x - \mathsf{r}_z$.
Set $\pi_0 := \Pi_0.\mathsf{prover}(\mathrm{CRS}^0, (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, E_\delta, R_\delta), (x, \mathsf{r}_\delta, \hat{x}))$.
Set $\pi_1 := \Pi_1.\mathsf{prover}(\mathrm{CRS}_p^1, (E_z^1, E_z^2, R_z), (0, \mathsf{r}_z))$.
Set $\pi_2 := \Pi_2.\mathsf{sim}(\mathrm{CRS}_p^2, \mathsf{trap}^2, (\mathbf{y}, \rho, \hat{\rho}, \gamma))$.
Return $\sigma := (\rho, \hat{\rho}, \gamma, E_z^1, E_z^2, R_z, \pi_0, \pi_1, \pi_2)$.

$\mathsf{Verify}(\mathsf{pk}, M, \sigma)$:
Parse $(\mathrm{CRS}, \mathbf{c}) \leftarrow \mathsf{pk}$, and set $\mathbf{y} := M||\mathbf{c}$.
Parse $(\rho, \hat{\rho}, \gamma, E_z^1, E_z^2, R_z, \pi_0, \pi_1, \pi_2) \leftarrow \sigma$.
Check all the NIZK proofs:
$\Pi_0.\mathsf{ver}(\mathrm{CRS}^0, (\rho, \hat{\rho}, E_\delta, R_\delta), \pi_0)$
and $\Pi_1.\mathsf{ver}(\mathrm{CRS}_v^1, (E_z^1, E_z^2, R_z), \pi_1)$
and $\Pi_2.\mathsf{ver}(\mathrm{CRS}_v^2, (\mathbf{y}, \rho, \hat{\rho}, \gamma), \pi_2)$.

Languages:

Π_0 is a NIZK proof for OR-language $L_0 \stackrel{\text{def}}{=} \{(\rho, \hat{\rho}, E_\delta, R_\delta) \mid \exists x, \mathsf{r}_\delta, \hat{x} \in \mathbb{Z}_q : x\,\hat{\rho} - \hat{x}\,[\underline{\mathbf{B}}]_1 = [0]_1$ **and** $\hat{x}\,[1]_1 - x\,\rho = [0]_1$ **and** $(E_\delta, R_\delta) = \mathrm{com}_2(x; \mathsf{r}_\delta)\}$ by Escala-Groth proof system for multi scalar multiplication equations.

Π_1 is a QA-NIZK for linear language $L_1 \stackrel{\text{def}}{=} \{(E_z^1, E_z^2, R_z) \mid \exists (z, \mathsf{r}_z) : E_z^1 := [z]_2 + \mathsf{r}_z\, \mathsf{pk}_1$ **and** $E_z^2 := [z]_2 + \mathsf{r}_z\, \mathsf{pk}_2\}$ with parameters $(\mathsf{pk}_1, \mathsf{pk}_2)$.

Π_2 is a QA-NIZK for linear language $L_2 \stackrel{\text{def}}{=} \{(\mathbf{y}, \rho, \hat{\rho}, \gamma) \mid \exists (\mathbf{x}, \mathsf{r}) : \mathbf{y} = [\mathbf{M}\mathbf{x}]_1$ **and** $\rho = [\bar{\mathbf{B}}\mathbf{r}]_1^\top$ **and** $\hat{\rho} = [\underline{\mathbf{B}}\mathbf{r}]_1^\top$ **and** $\gamma = \mathbf{x}^\top [\mathbf{p}_1]_1 + \mathsf{r}^\top [\mathsf{p}_2]_1\}$ with parameters $([\mathbf{M}]_1, [\mathbf{B}]_1, [\mathbf{p}_1]_1, [\mathbf{p}_2]_1)$.

Fig. 8. An SPS constructed directly by using the customized USS-QA-NIZK with designated prover (in Sect. 4.2) with optimizations from Sect. 3.3.

we follow a generic construction in [ACD+16, Sect. 6.3] that combines partially one-time signature for a part of messages in $\mathbb{G}_2$. It requires extra $(0, t_2)$ public-key elements, and the signature size increases by $(1, 2)$ elements sacrificing one group element in the message space $\mathbb{G}_1^{t_1}$. A signature thus consists of $(7, 8)$ elements for a bilateral message.

Acknowledgments. We thank the anonymous reviewers for detailed and insightful feedback on the paper. We especially thank Carla Ràfols for her significant effort in helping us revise the paper.

References

[ABP15] Abdalla, M., Benhamouda, F., Pointcheval, D.: Disjunctions for hash proof systems: new constructions and applications. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part II. LNCS, vol. 9057, pp. 69–100. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46803-6_3

[ACD+12] 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). https://doi.org/10.1007/978-3-642-34961-4_3

[ADKNO13] 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.) Public-Key Cryptography – PKC 2013. PKC 2013. LNCS, vol. 7778. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36362-7_20

[ACD+16] Abe, M., Chase, M., David, B., Kohlweiss, M., Nishimaki, R., Ohkubo, M.: Constant-size structure-preserving signatures: generic constructions and simple assumptions. J. Cryptol. **29**(4), 833–878 (2016)

[AFG+10] 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). https://doi.org/10.1007/978-3-642-14623-7_12

[AFG+16] Abe, M., Fuchsbauer, G., Groth, J., Haralambiev, K., Ohkubo, M.: Structure-preserving signatures and commitments to group elements. J. Cryptol. **29**(2), 363–421 (2016)

[AHN+17] Abe, M., Hofheinz, D., Nishimaki, R., Ohkubo, M., Pan, J.: Compact structure-preserving signatures with almost tight security. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part II. LNCS, vol. 10402, pp. 548–580. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63715-0_19

[AHO10] Abe, M., Haralambiev, K., Ohkubo, M.: Signing on elements in bilinear groups for modular protocol design. Cryptology ePrint Archive, Report 2010/133 (2010). http://eprint.iacr.org/2010/133

[AAO18] Abe, M., Ambrona, M., Ohkubo, M.: Impossibility of Black-Box Language Extension, and Signatures from SS-NIZK for any Language (2018, Unpublished manuscript)

[AO09a] Abe, M., Ohkubo, M.: A framework for universally composable non-committing blind signatures. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 435–450. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10366-7_26

[AO09b] Abe, M., Ohkubo, M.: A framework for universally composable non-committing blind signatures. Cryptology ePrint Archive, Report 2009/494 (2009). http://eprint.iacr.org/2009/494

[BBM00] 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). https://doi.org/10.1007/3-540-45539-6_18

[BBS04] Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-28628-8_3

[CCS09] 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). https://doi.org/10.1007/978-3-642-01001-9_20

[CLY09] 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). https://doi.org/10.1007/978-3-642-10366-7_11

[CS98] 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). https://doi.org/10.1007/BFb0055717

[CS02] Cramer, R., Shoup, V.: Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 45–64. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-46035-7_4

[CW13] 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). https://doi.org/10.1007/978-3-642-40084-1_25

[EHK+13] Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.: An algebraic framework for Diffie-Hellman assumptions. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 129–147. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40084-1_8

[ElG84] ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 10–18. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_2

[ES02] Elkind, E., Sahai, A.: A unified methodology for constructing public-key encryption schemes secure against adaptive chosen-ciphertext attack. Cryptology ePrint Archive, Report 2002/042 (2002). http://eprint.iacr.org/2002/042

[Fis06] Fischlin, M.: Round-optimal composable blind signatures in the common reference string model. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 60–77. Springer, Heidelberg (2006). https://doi.org/10.1007/11818175_4

[FLM11] Fischlin, M., Libert, B., Manulis, M.: Non-interactive and re-usable universally composable string commitments with adaptive security. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 468–485. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_25

[Fuc09] Fuchsbauer, G.: Automorphic signatures in bilinear groups and an application to round-optimal blind signatures. Cryptology ePrint Archive, Report 2009/320 (2009). http://eprint.iacr.org/2009/320

[GHKP18] Gay, R., Hofheinz, D., Kohl, L., Pan, J.: More efficient (almost) tightly secure structure-preserving signatures. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part II. LNCS, vol. 10821, pp. 230–258. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78375-8_8

[GHKW16] Gay, R., Hofheinz, D., Kiltz, E., Wee, H.: Tightly CCA-secure encryption without pairings. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016, Part I. LNCS, vol. 9665, pp. 1–27. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49890-3_1

[GHK17] Gay, R., Hofheinz, D., Kohl, L.: Kurosawa-Desmedt meets tight security. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part III. LNCS, vol. 10403, pp. 133–160. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63697-9_5

[Gro07] Groth, J.: Fully anonymous group signatures without random oracles. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 164–180. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-76900-2_10

[GS12] Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. SIAM J. Comput. **41**(5), 1193–1232 (2012)

[Har11] Haralambiev, K.: Efficient cryptographic primitives for non-interactive zero-knowledge proofs and applications. Ph.D. thesis, New York University (2011)

[HJ16] Hofheinz, D., Jager, T.: Tightly secure signatures and public-key encryption. Des. Codes Cryptogr. **80**(1), 29–61 (2016)

[Hof17] Hofheinz, D.: Adaptive partitioning. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017, Part III. LNCS, vol. 10212, pp. 489–518. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56617-7_17

[JOR18] Jutla, C.S., Ohkubo, M., Roy, A.: Improved (almost) tightly-secure structure-preserving signatures. In: Abdalla, M., Dahab, R. (eds.) PKC 2018, Part II. LNCS, vol. 10770, pp. 123–152. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76581-5_5

[JR13] Jutla, C.S., 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). https://doi.org/10.1007/978-3-642-42033-7_1

[JR14] Jutla, C.S., 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). https://doi.org/10.1007/978-3-662-44381-1_17

[JR15] Jutla, C.S., Roy, A.: Dual-system simulation-soundness with applications to UC-PAKE and more. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part I. LNCS, vol. 9452, pp. 630–655. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48797-6_26

[JR16] Jutla, C., Roy, A.: Smooth NIZK arguments with applications to asymmetric UC-PAKE. Cryptology ePrint Archive, Report 2016/233 (2016). http://eprint.iacr.org/2016/233

[JR17] Jutla, C.S., Roy, A.: Improved structure preserving signatures under standard bilinear assumptions. In: Fehr, S. (ed.) PKC 2017, Part II. LNCS, vol. 10175, pp. 183–209. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-662-54388-7_7

[KPW15] Kiltz, E., Pan, J., Wee, H.: Structure-preserving signatures from standard assumptions, revisited. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015, Part II. LNCS, vol. 9216, pp. 275–295. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48000-7_14

[KW15] Kiltz, E., Wee, H.: Quasi-adaptive NIZK for linear subspaces revisited. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part II. LNCS, vol. 9057, pp. 101–128. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46803-6_4

[LPJY14] 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). https://doi.org/10.1007/978-3-642-55220-5_29

[LPJY15] Libert, B., Peters, T., Joye, M., Yung, M.: Compactly hiding linear spans. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part I. LNCS, vol. 9452, pp. 681–707. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48797-6_28

[LPY15] Libert, B., Peters, T., Yung, M.: Short group signatures via structure-preserving signatures: standard model security from simple assumptions. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015, Part II. LNCS, vol. 9216, pp. 296–316. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48000-7_15

[Ràf15] Ràfols, C.: Stretching Groth-Sahai: NIZK proofs of partial satisfiability. In: Dodis, Y., Nielsen, J.B. (eds.) TCC 2015, Part II. LNCS, vol. 9015, pp. 247–276. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46497-7_10

[Wat09] 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). https://doi.org/10.1007/978-3-642-03356-8_36

[EG14] Escala, A., Groth, J.: Fine-tuning Groth-Sahai proofs. In: Krawczyk, H. (ed.) PKC 2014. LNCS, vol. 8383, pp. 630–649. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54631-0_36