Efficient Tightly-Secure Structure-Preserving Signatures and Unbounded Simulation-Sound QA-NIZK Proofs

Mojtaba Khalili[1,⋆] and Daniel Slamanig[2]

[1] Isfahan University of Technology, Iran
m.khalili@ec.iut.ac.ir
[2] AIT Austrian Institute of Technology, Vienna, Austria
daniel.slamanig@ait.ac.at

Abstract. We show how to construct structure-preserving signatures (SPS) and unbounded quasi-adaptive non-interactive zero-knowledge (USS QA-NIZK) proofs with a tight security reduction to simple assumptions, being the first with a security loss of $\mathcal{O}(1)$. Specifically, we present a SPS scheme which is more efficient than existing tightly secure SPS schemes and from an efficiency point of view is even comparable with other non-tight SPS schemes. In contrast to existing work, however, we only have a lower security loss of $\mathcal{O}(1)$, resolving an open problem posed by Abe et al. (CRYPTO 2017). In particular, our tightly secure SPS scheme under the SXDH assumption requires 11 group elements. Moreover, we present the first tightly secure USS QA-NIZK proofs with a security loss of $\mathcal{O}(1)$ which also simultaneously have a compact common reference string and constant size proofs (5 elements under the SXDH assumption, which is only one element more than the best non-tight USS QA-NIZK).

From a technical perspective, we present a novel randomization technique, inspired by Naor-Yung paradigm and adaptive partitioning, to obtain a randomized pseudorandom function (PRF). In particular, our PRF uses two copies under different keys but with shared randomness. Then we adopt ideas of Kiltz, Pan and Wee (CRYPTO 2015), who base their SPS on a randomized PRF, but in contrast to their non-tight reduction our approach allows us to achieve tight security. Similarly, we construct the first compact USS QA-NIZK proofs adopting techniques from Kiltz and Wee (EUROCRYPT 2015). We believe that the techniques introduced in this paper to obtain tight security with a loss of $\mathcal{O}(1)$ will have value beyond our proposed constructions.

1 Introduction

Structure-preserving signatures. A structure preserving signature (SPS) scheme [AFG$^+$10] is an interesting cryptographic primitive which is compatible with efficient pairing-based non-interactive zero-knowledge proofs due to Groth

[⋆] Work partly done while visiting Universitat Pompeu Fabra, Barcelona, Spain.

and Sahai [GS08]. More precisely, a SPS scheme is defined over bilinear groups and the messages, public keys and signatures are required to be source group elements. Furthermore, the signature verification consists of only group membership testing and evaluating pairing product equations (PPEs). This feature allows to use them in the construction of many efficient cryptographic tools, such as blind signatures [AFG+10, FHS15], group signatures [AFG+10, LPY15], traceable signatures [ACHO11], group encryption [CLY09], homomorphic signatures [LPJY13], delegatable anonymous credentials [Fuc11], compact verifiable shuffles [CKLM12], network coding signatures [ALP12], oblivious transfer [GH08], tightly secure encryption [HJ12] and anonymous e-cash [BCF+11]. Since SPS are used in the aforementioned and many other cryptographic tools as a basic component, it is essential to make them highly efficient and secure. So, much effort has been put into designing efficient SPS schemes based on simple assumptions.

The first constant-size SPS scheme presented by Abe et al. in [AFG+10] was inspired by previous constructions in [Gro06, GH08, CLY09]. This was followed by a line of research to obtain SPS with short signatures in the generic group model (GGM) [AGHO11, AGOT14, Gha16, Gha17], lower bounds [AGHO11, AGO11, AAOT18], impossibility results [ACDD14], security under well-known assumptions [ACD+12, CDH12, HJ12, KPW15, LPY15, JR17] or tight security proofs [AHN+17, JOR18, GHKP18, AJOR18]. In addition to the most common definition of the SPS, there are also some extended notions of SPS in the literature, such as fully structure-preserving signatures [AKOT15, Gro15, WZM+16] and structure-preserving signatures on equivalence classes [HS14, FG18]. Beyond signatures, effort has also been made to construct other structure-preserving primitives, such as commitments [Gro09, AFG+10, AHO12, LPJY13, AKOT15], public key encryption [CHK+11, ADK+13, LPQ17], certificateless encryption [ZWC19] or smooth projective hash functions [BC16].

Quasi-adaptive NIZK proofs and simulation soundness. Quasi-adaptive NIZK proofs for linear subspaces[3] [JR13, JR14, LPJY14, LPJY15, KW15, GHKW16, AJOR18] are another important tool used in the design of the many cryptographic protocols that need NIZK proofs [BFM88] for giving membership proofs in the subspace of a pre-defined language. Actually, in *quasi-adaptive* NIZK proofs, the common reference string (CRS) depends on the language parameters, which leads to more efficient proofs compared to using Groth-Sahai proofs [GS08]. Some schemes, such as CCA2-secure public key encryption (PKE) schemes [LPJY15], which in turn are used as a building block in other applications such as CCA-anonymous group signatures [AHO10] or UC-secure commitments [CF01, FLM11], require QA-NIZK proofs with a strong property. In particular, they require that even if the adversary has access to an oracle providing proofs for true or false statements, he cannot construct a proof for a new false statement. This property is known as unbounded simulation sound-

[3] In this paper we consider only linear languages in the QA-NIZK setting (the most common setting), but there are works on QA-NIZK for other languages such as quadratic [DGP+19] or shuffles and range proofs [GR16].

ness (USS) [Sah99]. In addition to the applications already mentioned, Abe et al. in [AJOR18] demonstrate an application of their USS QA-NIZK[4] to obtain SPS schemes, CCA2-secure publicly-verifiable PKE schemes, which in turn can be used to obtain round-optimal blind signatures in the CRS model using the framework of Fischlin [Fis06], and unbounded simulation-sound Groth-Sahai NIZK proofs [CCS09].

Earlier approaches to QA-NIZK proofs only satisfied a weaker notion called one-time simulation-soundness. The first USS QA-NIZK scheme based on the Decision Linear (DLin) assumption [BBS04] was presented by Libert et al. [LPJY14]. In an outstanding work, Kiltz and Wee in [KW15] introduced very efficient USS QA-NIZK proofs, whose proofs only require 4 group elements. Unfortunately, their scheme has a security loss of $\mathcal{O}(Q)$, where Q is number of adversarial queries to the proof oracle.

Tight security reductions. In this paper we are interested in tightly secure schemes that at the same time have reasonable efficiency. Tight security means that if an adversary can break a primitive, one can convert the adversary in one against a hard problem with about the same running time and same advantage. Generally, one distinguishes between tight reductions where the security loss is a (small) constant, i.e., $\mathcal{O}(1)$, or so called almost tight reductions, where the security loss grows only (as a small function) in the security parameter λ, e.g., $\mathcal{O}(\lambda)$. Tight reductions are desirable not only from a theoretical perspective, but also a practical one - in a tightly secure primitive, one can use smaller key-lengths (as one does not have to account for a potentially huge tightness gap) and thus gain higher efficiency. This is even more important when the primitive is combined with other tools in the same algebraic setting (e.g., bilinear group), as it is the case for SPS or QA-NIZKs. The desired goal clearly is not only to achieve tight security under simple and well studied assumptions, but also to remain as efficient as possible. In recent years, tight reductions have been considered for many cryptographic primitives, such as PKE schemes [HJ12, GHKW16, Hof17], signature schemes [HJ12, ADK$^+$13, CW13, Hof16, Hof17, GJ18], IBE schemes [CW13, HKS15, AHY15, CGW17, HJP18], key exchange schemes [BHJ$^+$15, GJ18, HHK18], or NIZK proofs [HJ12, GHKW16].

Tight security for SPS. Recently, much effort has been put into designing efficient tightly secure SPS schemes starting with the work of Abe et al. [AHN$^+$17]. Abe et al. have presented an interesting method called structure-preserving adaptive partitioning, which is a modification of an earlier technique called adaptive partitioning by Hofheinz [Hof17]. Their SPS scheme has a security loss of $\mathcal{O}(\lambda)$. Recently, Jutla et al. in [JOR18] gave a tightly secure SPS scheme using the approach of [AHN$^+$17] with improved efficiency by using more efficient QA-NIZK proofs. More recently, Gay et al. in [GHKP18] improved the efficiency of tightly secure SPS schemes by relying on a different approach. Gay et al. adapt a key encapsulation mechanism (KEM) scheme from [GHK17] to obtain a message au-

[4] The construction of [AJOR18] is structure-preserving for simulated proofs.

thentication code (MAC), and then convert it into an SPS scheme (as previously done for non-tight SPS, e.g., in [KPW15]) by using an adapted variant of the generic MAC-to-signatures conversion introduced by Bellare and Goldwasser in [BG90]. Also, this approach leads to a tightly secure scheme with a security loss of $\mathcal{O}(\log(Q))$, where Q is the number of signing queries by the adversary. Very recently, Abe et al. in [AJOR18] introduced a more efficient tightly secure SPS scheme with the same loss. In particular, Abe et al. presented a designated-prover structure-preserving USS QA-NIZK, which can be translated to an SPS scheme. All known tightly-secure SPS schemes, except the one in [HJ12] (which, however, is not practical), are almost tight, and also the shortest among them has twice as much elements in the signature as the best known non-tight SPS scheme. There is an open problem raised by Abe et al. at [AHN$^+$17] to design structure-preserving signatures with a reduction loss $\mathcal{O}(1)$ and smaller number of group elements.

Tight security for USS QA-NIZK proofs. Studying the tightness of security reductions for USS QA-NIZK proofs was initiated by Libert et al. in [LPJY15], and continued in recent works of Gay et al. in [GHKW16], and Abe et al. in [AJOR18]. Technically, the construction of [LPJY15] uses Groth-Sahai proofs [GS08] and linearly homomorphic structure-preserving signatures (LH-SPS) [LPJY13] as building block, and its simulation soundness relies on an OR-proof systems, which allows the prover to show that its CRS is perfectly binding or he knows the the LH-SPS secret key. Gay et al. in [GHKW16] use a hash proof system [CS02] to construct designated-verifier QA-NIZK (DV-QA-NIZK) proofs. There is a known semi-generic transformation [KW15], which can be applied to DV-QA-NIZK to obtain a tightly secure simulation-sound QA-NIZK proof. The most recent work of Abe et al. in [AJOR18] also relies on an OR-proof system using the framework of Ràfols [Ràf15]. Abe et al. encrypt a basic QA-NIZK proof using an augmented ElGamal encryption scheme, and also use an OR-proof to hide the simulation trapdoors in simulated proofs. Unfortunately, the constructions of [LPJY15] and [GHKW16] have a CRS of size $\mathcal{O}(\lambda)$, and the construction of [AJOR18], while it has a compact CRS, has proofs whose size depends on the parameters of the language.

Summarizing, in context of tightly secure QA-NIZK proofs, there is still a gap to obtain tightly secure ones, i.e., $\mathcal{O}(1)$ loss, and that are compact, i.e., where the CRS does not depend on the security parameter and at the same time proofs are constant-size. Also, there is still a gap between the number of group elements used by ordinary SPS schemes (i.e., non-tight schemes) and tightly secure ones as well as the open problem of obtaining a reduction loss $\mathcal{O}(1)$ for a constant-size SPS. In this paper, we try to further reduce these gaps.

1.1 Our Contributions

Overview. We present a more efficient construction of an SPS scheme with a tight security reduction. In particular, under the SXDH assumption our scheme needs 11 group elements and has a reduction loss of $\mathcal{O}(1)$. This gives an improvement compared to the state-of-the-art tightly secure SPS scheme of Abe et al. in [AJOR18] with signature size of 12 group elements, and Gay et al. in [GHKP18] with a size of 14 group elements, wheres both have a larger reduction loss of $\mathcal{O}(\log Q)$. So, we answer the open problem of Abe et al. in [AHN+17] affirmatively, and obtain a more efficient scheme with security reduction loss of $\mathcal{O}(1)$. In Table 1 we provide a comparison with (tightly secure) SPS schemes from simple assumptions, where we put our focus on unilateral variants[5], i.e., where all n messages either come from $\mathbb{G}_1$ or $\mathbb{G}_2$, as there is a generic conversion to bilateral ones due to Kiltz, Pan and Wee [KPW15], which is used by essentially all existing works in the literature. Nevertheless, for completeness, in Section 5 we discuss how our scheme can be extended to sign bilateral messages in a tightness-preserving way. Looking ahead, our SPS scheme also yields the most efficient SPS with constant security loss for bilateral messages with signature size $(7, 7)$. The most efficient one so far in [AJOR18] has signature size $(12, 8)$ and a larger reduction loss of $\mathcal{O}(\log Q)$.

Scheme	**Signature Size**	**PK size**	**Loss**	**Assumption**
[HJ12]	$10\ell + 6$	13	$\mathcal{O}(1)$	DLIN
[ACD+12]	$(7, 4)$	$(5, n + 12)$	$\mathcal{O}(Q)$	SXDH, XDLIN
[LPY15]	$(10, 1)$	$(16, 2n + 5)$	$\mathcal{O}(Q)$	SXDH, XDLINX
[KPW15]	$(6, 1)$	$(0, n + 6)$	$\mathcal{O}(Q^2)$	SXDH
[JR17]	$(5, 1)$	$(0, n + 6)$	$\mathcal{O}(Q \log(Q))$	SXDH
[AHN+17]	(13, 12)	$(18, n + 11)$	$\mathcal{O}(\lambda)$	SXDH
[JOR18]	(11, 6)	$(7, n + 16)$	$\mathcal{O}(\lambda)$	SXDH
[GHKP18]	(8, 6)	$(2, n + 9)$	$\mathcal{O}(\log Q)$	SXDH
[AJOR18]	(6, 6)	$(2, n + 5)$	$\mathcal{O}(\log Q)$	SXDH
Our scheme	(6, 5)	$(4, 2n + 11)$	$\mathcal{O}(1)$	SXDH

Table 1. Comparison of (tightly secure) SPS schemes under standard assumptions, where n denotes the length of the message vector and λ the security parameter. The notation (u, v) means u elements in $\mathbb{G}_1$ and v elements in $\mathbb{G}_2$. We note that for the tree-based signatures in [HJ12], ℓ denotes the depth of the tree limiting the number of signing queries by the adversary to 2^ℓ.

Moreover, we present the first tightly secure unbounded simulation-sound QA-NIZK proofs which additionally have a compact CRS and constant proof size. Specifically, our security reduction has a loss of $\mathcal{O}(1)$ and proofs in our scheme have only 5 group elements. All cryptographic schemes, e.g., CCA2-secure PKE in the multi-challenge, multi-user setting [LPJY15], built on top of our USS QA-NIZK proof will be positively affected by its efficiency and security. In the Table 2 we compare our USS QA-NIZK with previous works, for languages $\mathbf{y} = \mathbf{M}\mathbf{x}$, where $\mathbf{M} \in \mathbb{Z}_p^{n \times t}$.

[5] In Table 1 we consider messages $[\mathbf{m}]_2 \in \mathbb{G}_2^n$, but this can easily be adopted to $[\mathbf{m}]_1 \in \mathbb{G}_1^n$ by switching the roles of the groups.

Scheme	Proof Size	CRS size	Loss	Assumption
[LPJY14]	20	$\mathcal{O}(\lambda)$	$\mathcal{O}(Q)$	DLIN
[KW15]	4	$\mathcal{O}(t)$	$\mathcal{O}(Q)$	SXDH
[LPJY15]	42	$\mathcal{O}(\lambda)$	$\mathcal{O}(\lambda)$	DLIN
[GHKW16]	3	$\mathcal{O}(\lambda)$	$\mathcal{O}(\lambda)$	SXDH
[AJOR18]	$\mathcal{O}(n+t)$	$\mathcal{O}(n+t)$	$\mathcal{O}(\log(Q))$	SXDH
Our scheme	5	$\mathcal{O}(n+t)$	$\mathcal{O}(1)$	SXDH

Table 2. Comparison of (tightly secure) USS QA-NIZK schemes, where $\mathbf{M} \in \mathbb{Z}_p^{n\times t}$ denotes the language parameters.

1.2 Overview of our Approach

A main concept in the construction of signatures and USS QA-NIZK proofs, like [CCS09, KPW15, JR17, AHN$^+$17, JOR18, AJOR18], is to hide a secret using an encryption and prove using a NIZK proof that the signer knows the secret encrypted in the ciphertext. This similarity between signatures and USS QA-NIZK proofs is due to the fact that both have similar requirements. As discussed in [AJOR18], unbounded simulation-soundness of a QA-NIZK system corresponds to unforgeability against adaptive chosen message attacks of a signature scheme, where the adversary has an unbounded access to a signing oracle for his messages and finally cannot find a valid signature for any fresh message.

To obtain simulation-soundness, it seems that one requires CCA2 security from the used encryption scheme. Therefore, one can either consider specific schemes such as augmented ElGamal combined with a hash proof system as done in Cramer-Shoup encryption [CS98], or rely on the Naor-Yung paradigm [NY90], which combines two ciphertexts from any CPA secure encryption scheme to the same message under independent keys and a simulation-sound NIZK proof for consistency. The earlier versions of these approaches required a tag (needing a collision-resistant hash) and so the resulting scheme is no longer structure-preserving, and also resulted in a non-tight reduction (e.g. [JR13]). While there are schemes that solve the first problem[6] (e.g. [KPW15, LPY15, JR17]), to overcome both limitations, only recently some interesting works have been done [AHN$^+$17, JOR18, AJOR18, GHKP18]. All of them rely on the use of a partitioning technique, where in the security proof one gradually transforms the conditions necessary for a successful forgery until a valid forgery is impossible. This requires multiple game hops which determine the actual security loss. In case of [AHN$^+$17, JOR18, AJOR18] the partitioning is done on the bits of the messages, leading to a loss of $\mathcal{O}(\lambda)$. In [GHKP18], the bits of the number Q of signing queries are considered, which leads to a loss of $\mathcal{O}(\log Q)$.

In this paper, we introduce a novel approach, again inspired by the Naor-Yung paradigm and partitioning techniques, but using alternative methods to

[6] In these schemes instead of hashing, the tag is chosen randomly, and its representation in one of the source groups of a bilinear group is included as part of the signature.

obtain a quantitatively better security reduction. In particular, similar to the Naor-Yung paradigm, we use two signatures or QA-NIZK proofs, but both instances share the same randomness and the same tag. As these values can be publicly verified, in contrast to encryption, we do not explicitly need to add a proof of well-formedness. The second difference is that we do partitioning on the verification space. Actually, analogous to what is done by Kiltz, Pan and Wee [KPW15], in the security proof we switch the verification equation under the Kernel Diffie-Hellman assumption and then embed an additional secret whose presence we then verify for the forgery given by the adversary. Our key technique is that once having embedded the additional secret, we switch to a verification equation where we only verify one of the two signatures (proofs), which one we decide randomly, and argue the adversary will not notice this change. We can then apply our core lemma, which allows us to randomize the parts of both signatures (proofs) that include the additional secret. Actually, in the core lemma, based on a random bit, we partition the space of verification, and in a sequence of games we will hide this secret information theoretically from the adversary, which then concludes the proof. Thereby, the strategy used to prove the core lemma is somehow reminiscent of the adaptive partitioning technique by Hofheinz [Hof17] and similar to the approach in [GHKP18] (whereas Gay et al. require $\log Q$ hybrids instead of 2 as in our case). Essentially, we can view our approach as encrypting the additional secret using ElGamal and then using random self reducibility of MDDH (or LinSum to be specific) to make these parts random. This finally hides the secret information theoretically and leaves the adversary only with guessing it.

Subsequently, we give an intuition behind our constructions on a more technical level.

First, we recall the construction of [KW15, KPW15], who present a core lemma, which shows that the following distributions (for $\beta = 0$ or $\beta = 1$) are indistinguishable under the MDDH assumption:

$$([\beta\mu\mathbf{a}^{\perp} + \mathbf{r}^{\top}(\mathbf{P}_0 + \tau\mathbf{P}_1)]_1, [\mathbf{r}^{\top}\mathbf{B}^{\top}]_1),$$

for secret keys $\mathbf{K}_0, \mathbf{K}_1 \in \mathbb{Z}_p^{(k+1)\times(k+1)}$, where $\mathbf{P}_0 = \mathbf{B}^{\top}\mathbf{K}_0$, $\mathbf{P}_1 = \mathbf{B}^{\top}\mathbf{K}_1$ for $\mathbf{B} \leftarrow \mathcal{D}_k$, and $\mathbf{r} \xleftarrow{R} \mathbb{Z}_p^k$, and $\mu \xleftarrow{R} \mathbb{Z}_p$, and random tag $\tau \xleftarrow{R} \mathbb{Z}_p$. Also, we have $\mathbf{a}^{\perp}\mathbf{A} = 0$, where $\mathbf{A} \leftarrow \mathcal{D}_k$. Actually, the part $[\mathbf{r}^{\top}(\mathbf{P}_0 + \tau\mathbf{P}_1]_1)$ acts as a randomized PRF, which is used to mask a one-time signature $[(1, \mathbf{m})]_1\mathbf{K}$ for message $[\mathbf{m}]_1 \in \mathbb{G}_1^{\ell}$, in case of the SPS scheme in [KPW15]. Also, in case of USS QA-NIZK proof in [KW15], Kiltz and Wee use this randomized PRF to hide information outside of the span of $\mathbf{M}$ in a simulated proof $[\mathbf{y}]_1^{\top}\mathbf{K}$ for statement $[\mathbf{y}]_1 \in \mathbb{G}^n$.

Now, we need a new randomization technique to construct a randomized PRF, and add some randomness to our schemes, while allowing a tight reduction. In particular, we present a core lemma that says that the following distributions are indistinguishable under the LinSum assumption, an assumption implied by the MDDH assumption, (for $\beta = 0$ and $\beta = 1$):

$$[\mathbf{u}_0]_1 = [\beta\mu_0\mathbf{a}^\perp + \mathbf{r}^\top\mathbf{K}_2]_1, \quad [\mathbf{u}_1]_1 = [\beta\mu_1\mathbf{a}^\perp + \mathbf{r}^\top\mathbf{K}_3]_1,$$

for secret keys $\mathbf{K}_2, \mathbf{K}_3 \in \mathbb{Z}_p^{k\times(k+1)}$, where $\mu_0, \mu_1 \overset{R}{\longleftarrow} \mathbb{Z}_p$, and $\mathbf{r} \overset{R}{\longleftarrow} \mathbb{Z}_p^k$.

As we will show, when we use our core lemma, we can only verify one of $[\mathbf{u}_0]_1$ and $[\mathbf{u}_1]_1$. Therefore, we have to switch from the original verification to another verification algorithm, in which we verify only one equation. We will show that this gives the adversary at most a negligible advantage. This then allows us to modify the signatures and proofs in a way that the adversary ends up only having negligible probability of producing a valid forgery.

Our USS QA-NIZK proof. We can use the core lemma to hide a part of the trapdoor keys in simulated proofs and obtain unbounded simulation-soundness against multiple simulation queries in QA-NIZKs. Actually, we start with a basic QA-NIZK proof with known form (cf. [KW15, AJOR18]) of

$$\pi = \mathbf{x}^\top([\mathbf{P}]_1 + \tau[\mathbf{P}']_1),$$

for CRS $\mathbf{P} = \mathbf{M}^\top\mathbf{K}$ and $\mathbf{P}' = \mathbf{M}^\top\mathbf{K}'$, where $\mathbf{x} \in \mathbb{Z}_p^t$ is a witness for statement $\mathbf{y} = \mathbf{M}\mathbf{x}$. Here, we have $\mathbf{K}, \mathbf{K}' \in \mathbb{Z}_p^{n\times(k+1)}$, and $\mathbf{M} \in \mathbb{Z}_p^{n\times t}$, and all $\tau \in \mathbb{Z}_p$. Now, with the knowledge of the trapdoor keys one can compute a simulated proof as

$$\pi = [\mathbf{y}^\top]_1(\mathbf{K} + \tau\mathbf{K}'),$$

which is only one-time simulation sound for new tag τ [KW15]. But, to be compatible with our core lemma we need to double this basic form, which preserves the one-time simulation-soundness, and looks as follows:

$$\pi_0 = [\mathbf{y}^\top]_1(\mathbf{K}_0 + \tau\mathbf{K}_2)$$

$$\pi_1 = [\mathbf{y}^\top]_1(\mathbf{K}_1 + \tau\mathbf{K}_3).$$

The simulation-soundness holds because under $\mathbf{M}^\top\mathbf{K}_0$, $\mathbf{M}^\top\mathbf{K}_1$, $\mathbf{M}^\top\mathbf{K}_2$ and $\mathbf{M}^\top\mathbf{K}_3$ the following values for a new tag $\tau^* \neq \tau$ are information theoretically hidden when $\mathbf{y}^{*\top}$ is outside of the span of $\mathbf{M}$:

$$\pi_0^* = [\mathbf{y}^{*\top}]_1(\mathbf{K}_0 + \tau^*\mathbf{K}_2)$$

$$\pi_1^* = [\mathbf{y}^{*\top}]_1(\mathbf{K}_1 + \tau^*\mathbf{K}_3).$$

Then, we try to leak zero information about trapdoor keys, even when we give proofs for statement outside of the span of $\mathbf{M}$. In particualr, we are going to obtain unbounded simulated proofs using an additional random part. This approach is also used in previous works by Kiltz and Wee [KW15], and Abe et al. [AJOR18], while the former obtain a non-tight scheme, and latter obtain proof sizes which depend on the language parameters.

We add our PRF to the basic QA-NIZK proof, and compute the simulated proofs as:

$$[\mathbf{u}_0]_1 = [\mathbf{y}^\top(\mathbf{K}_0 + \tau\mathbf{K}_1) + \mathbf{r}^\top\mathbf{K}_4]_1, \quad [\mathbf{u}_1]_1 = [\mathbf{y}^\top(\mathbf{K}_1 + \tau\mathbf{K}_3) + \mathbf{r}^\top\mathbf{K}_5]_1$$

for $\tau \in \mathbb{Z}_p$ which is computed using a collision-resistant hash function as $\tau = H_k([\mathbf{y}]_1, [\mathbf{r}]_1)$. In particular, we can use our core lemma to hide a part of the trapdoor keys and prevent the adversary to give a proof of a false statement. Note that here we put a part of the trapdoor keys in the CRS. But as we will show, the CRS leaks no information about that part, for proofs outside of the span of $\mathbf{M}$. Also, we proceed as [KW15, KPW15] to obtain public verifiability for our construction.

Our SPS scheme. Similarly, we can use our core lemma to hide a part of the secret keys in our one-time signature, and obtain unforgeability against multiple Sign queries. Here, we need to be structure-preserving, so we cannot proceed as we do in the QA-NIZK, i.e., use a hash function. So, we first use our randomization part to mask our one-time signature as:

$$[\mathbf{u}_0]_1 = [(1, \mathbf{m}^\top)\mathbf{K}_0 + \boldsymbol{\rho}^\top\mathbf{K}_2]_1, \quad [\mathbf{u}_1]_1 = [(1, \mathbf{m}^\top)\mathbf{K}_1 + \boldsymbol{\rho}^\top\mathbf{K}_3]_1,$$

for secret keys $\mathbf{K}_0, \mathbf{K}_1 \in \mathbb{Z}_p^{(\ell+1)\times(k+1)}$, $\mathbf{K}_2, \mathbf{K}_3 \in \mathbb{Z}_p^{k\times(k+1)}$, $\boldsymbol{\rho} \xleftarrow{R} \mathbb{Z}_p^k$and message $[\mathbf{m}]_1 \in \mathbb{G}_1^\ell$. However, so far our signature is malleable, as we do not use tags.[7] So, we let $\boldsymbol{\rho} = [\mathbf{A}_0]_1\mathbf{r}$ for randomness $\mathbf{r} \xleftarrow{R} \mathbb{Z}_p^k$, and language parameter $\mathbf{A}_0 \in \mathbb{Z}_p^{k\times k}$. Then we give a membership proof that the vector $\boldsymbol{\rho}$ is in the linear space of $[\mathbf{A}_0]_1$ using a NIZK argument inspired by [GHKP18]. Actually, all tightly secure SPS schemes use such NIZK proofs in their construction. However, while other schemes need an OR-proof system, specially for their partitioning technique, we only need a simple NIZK argument (using a simplified revised version of [GHKP18]), which allows to save some group elements.

1.3 Roadmap

We recall some background including notation and basic definitions in Section 2. In Section 3 we present our core lemma and then in the following Section 4 and Section 5 we present our USS QA-NIZK proofs and SPS scheme respectively.

2 Preliminaries

In this section we recall background required for our constructions.

[7] This is similar to the construction in [GHKP18] which also has this malleability for part of the signature. Gay et al. then use an OR-proof to obtain non-malleability.

2.1 Notation

Let GGen be a probabilistic polynomial time (PPT) algorithm that on input 1^λ returns a description $\mathcal{G} = (\mathbb{G}, p, P)$ of an additive cyclic group $\mathbb{G}$ of order p for a λ-bit prime p, whose generator is P. We use implicit representation of group elements as introduced in [EHK+17]. For $a \in \mathbb{Z}_p$, define $[a] = aP \in \mathbb{G}$ as the implicit representation of a in $\mathbb{G}$. We will always use this implicit notation of elements in $\mathbb{G}$, i.e., we let $[a] \in \mathbb{G}$ be an element in $\mathbb{G}$. Note that from $[a] \in \mathbb{G}$ it is generally hard to compute the value a (discrete logarithm problem in $\mathbb{G}$).

Let BGGen be a PPT algorithm that returns a description $\mathsf{BG} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, P_1, P_2, e)$ of an asymmetric bilinear group where $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are cyclic groups of order p , P_1 and P_2 are generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively, and $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is an efficiently computable (non-degenerate) bilinear map. For $s \in \{1, 2, T\}$ and $a \in \mathbb{Z}_p$, define $[a]_s = aP_s \in \mathbb{G}_s$ as the implicit representation of a in $\mathbb{G}_s$. For two matrices (vectors) $\mathbf{A}, \mathbf{B}$ define $e([\mathbf{A}]_1, [\mathbf{B}]_2) := [\mathbf{A}^\top \mathbf{B}]_T \in \mathbb{G}_T$. By $\overline{\mathbf{B}}$ we denote the upper square matrix of $\mathbf{B}$. Let $r \overset{R}{\leftarrow} \mathcal{S}$ denote sampling r from set $\mathcal{S}$ uniformly at random, λ be the security parameter, and ϵ any negligible function of λ.

2.2 Assumptions

Definition 1 (Decisional Diffie-Hellman (DDH) Assumption). *Let* GGen *be a group generator. We say that* DDH *assumption holds if for all polynomial time adversaries $\mathcal{A}$ we have:*

$$\mathbf{Adv}_{\mathcal{G}}^{\mathsf{DDH}}(\mathcal{A}) := |\Pr\big[\mathcal{A}(\mathcal{G}, [x], [y], [xy]) = \big] - \Pr\big[\mathcal{A}(\mathcal{G}, [x], [y], [r]) = \big]| \leq \epsilon(\lambda)$$

where the probability is taken over $x, y \overset{R}{\leftarrow} \mathbb{Z}_p$ and $\mathcal{G} \leftarrow \mathsf{GGen}(1^\lambda)$.

Definition 2 (Symmetric external Diffie-Hellman (SXDH) assumption). *The symmetric external Diffie-Hellman* (SXDH) *assumption holds relative to* BGGen *when DDH is hard in $\mathbb{G}_s$ for $s \in \{1, 2\}$.*

We recall the definition of the Matrix Decision Diffie-Hellman assumption [EHK+17] and a natural computational analogue of it, called the Kernel-Diffie-Hellman assumption [MRV16].

Definition 3 (Matrix Distribution). *Let $k \in \mathbb{N}$. We call $\mathcal{D}_k$ a matrix distribution if it outputs matrices in $\mathbb{Z}_p^{(k+1)\times k}$ of full rank k in polynomial time.*

Definition 4 ($\mathcal{D}_k$-Matrix Diffie-Hellman Assumption $\mathcal{D}_k$-MDDH). *Let $\mathcal{D}_k$ be a matrix distribution. We say that the $\mathcal{D}_k$-Matrix Diffie-Hellman ($\mathcal{D}_k$-*MDDH*) Assumption holds relative to* BGGen *in group $\mathbb{G}_s$ if for all PPT adversaries $\mathcal{A}$,*

$$\mathbf{Adv}_{\mathcal{D}_k, \mathbb{G}_s}^{\mathsf{MDDH}}(\mathcal{A}) := |\Pr\big[\mathcal{A}(\mathsf{BG}, [\mathbf{A}]_s, [\mathbf{A}\mathbf{w}]_s) = 1\big] - \Pr\big[\mathcal{A}(\mathsf{BG}, [\mathbf{A}]_s, [\mathbf{u}]_s) = 1\big]| \leq \epsilon(\lambda)$$

where the probability is taken over $\mathsf{BG} \leftarrow \mathsf{BGGen}(1^\lambda), \mathbf{A} \leftarrow \mathcal{D}_k, \mathbf{w} \leftarrow \mathbb{Z}_p^k, \mathbf{u} \leftarrow \mathbb{Z}_p^{k+1}$.

Now, we consider the Q-fold $\mathcal{D}_k$-MDDH assumption. Actually, an instance for the Q-fold $\mathcal{D}_k$-MDDH assumption consists of Q independent instances of the $\mathcal{D}_k$-MDDH assumption (with the same $\mathbf{A}$ but different randomness $\mathbf{w}$). It is known that the two problems are equivalent [EHK+17].

Lemma 1 (Random self-reducibility of $\mathcal{D}_k$-MDDH, [EHK+17]). *Let $Q \in \mathbb{N}$. For any PPT adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$ such that $T(\mathcal{B}) \approx T(\mathcal{A}) + Q \cdot \mathsf{poly}(\lambda)$ with $\mathsf{poly}(\lambda)$ independent of $T(\mathcal{A})$, and*

$$\mathbf{Adv}^{Q\text{-}\mathsf{MDDH}}_{\mathcal{D}_k,\mathbb{G}_s}(\mathcal{A}) < \mathbf{Adv}^{\mathsf{MDDH}}_{\mathcal{D}_k,\mathbb{G}_s}(\mathcal{B}) + \frac{1}{p}$$

where

$$\mathbf{Adv}^{Q\text{-}\mathsf{MDDH}}_{\mathcal{D}_k,\mathbb{G}_s}(\mathcal{A}) := |\Pr\left[\mathcal{A}(\mathsf{BG}, [\mathbf{A}]_s, [\mathbf{AW}]_s) = 1\right] - \Pr\left[\mathcal{A}(\mathsf{BG}, [\mathbf{A}]_s, [\mathbf{U}]_s) = 1\right]|$$

and $\mathbf{W} \xleftarrow{R} \mathbb{Z}_p^{k\times Q}$ and $\mathbf{U} \xleftarrow{R} \mathbb{Z}_p^{(k+1)\times Q}$.

Now, we consider a new instance of the matrix distribution $\mathcal{D}_k$ which leads to a new class of assumptions, which we call k-LinSum. In particular, we choose the matrix distribution as

$$\mathcal{D}_k := \mathcal{LS}_k = \begin{bmatrix} 1 & 0 & \ldots\ldots & 0 \\ 0 & 1 & 0 \ldots & 0 \\ \vdots & \vdots & \vdots \quad \vdots & \vdots \\ 0 & \ldots\ldots & 0 & 1 \\ a_1 & a_2 & \ldots\ldots & a_k \end{bmatrix}. \tag{1}$$

where $a_i \xleftarrow{R} \mathbb{Z}_p$. This assumption is such that the DDH assumption equals 1-LinSum. Actually, k-LinSum implies $k+1$-LinSum, but $k+1$-LinSum is still hard under a k-LinSum oracle (in the generic group model [Sho97, HK07]). Also, the new assumption has random self-reducibility as general case.

Definition 5 (k-Linear Sum Diffie-Hellman Assumption (k-LinSum)). *Let $\mathcal{LS}_k$ be a matrix distribution as in* (1)*. We say that the k-LinSum Assumption holds relative to BGGen in group $\mathbb{G}_s$ if for all PPT adversaries $\mathcal{A}$,*

$$\mathbf{Adv}^{\mathsf{LinSum}}_{\mathcal{L}_k,\mathbb{G}_s}(\mathcal{A}) := |\Pr\left[\mathcal{A}(\mathsf{BG}, [\mathbf{A}]_s, [\mathbf{Aw}]_s) = 1\right] - \Pr\left[\mathcal{A}(\mathsf{BG}, [\mathbf{A}]_s, [\mathbf{u}]_s) = 1\right]| \leq \epsilon(\lambda)$$

where the probability is taken over $\mathsf{BG} \leftarrow \mathsf{BGGen}(1^\lambda), \mathbf{A} \leftarrow \mathcal{L}_k, \mathbf{w} \leftarrow \mathbb{Z}_p^k, \mathbf{u} \leftarrow \mathbb{Z}_p^{k+1}$.

Definition 6 (Kernel Diffie-Hellman Assumption $\mathcal{D}_k$-KerMDH). *Let $\mathcal{D}_k$ be a matrix distribution and $s \in \{1, 2\}$. We say that the $\mathcal{D}_k$-Kernel Diffie-Hellman ($\mathcal{D}_k$-KerMDH) Assumption holds relative to BGGen in group $\mathbb{G}_s$ if for all PPT adversaries $\mathcal{A}$,*

$$\mathbf{Adv}^{\mathsf{KerMDH}}_{\mathcal{D}_k,\mathbb{G}_s}(\mathcal{A}) = \Pr\left[\mathbf{c}^\top\mathbf{A} = \mathbf{0} \wedge \mathbf{c} \neq \mathbf{0} \mid [\mathbf{c}]_{3-s} \leftarrow \mathcal{A}(\mathsf{BG}, [\mathbf{A}]_s)\right] \leq \epsilon(\lambda)$$

where $\mathbf{A} \xleftarrow{R} \mathcal{D}_k$.

Lemma 2 ($\mathcal{D}_k$-MDDH $\implies$ $\mathcal{D}_k$-KerMDH [MRV16]). *Let $k \in \mathbb{N}$ and let $\mathcal{D}_k$ be a matrix distribution. For any PPT adversary $\mathcal{A}$, there exists a PPT adversary $\mathcal{B}$ such that $\mathbf{Adv}^{\mathsf{KerMDH}}_{\mathcal{D}_k,\mathbb{G}_s}(\mathcal{A}) \leq \mathbf{Adv}^{\mathsf{MDDH}}_{\mathcal{D}_k,\mathbb{G}_s}(\mathcal{B})$.*

For each $k \geq 1$, [EHK+17, MRV16] specify (among others) distributions $\mathcal{L}_k$, $\mathcal{SC}_k$, $\mathcal{U}_k$ such that the corresponding $\mathcal{D}_k$-MDDH and $\mathcal{D}_k$-KerMDH form a hierarchy of increasingly weaker assumptions. $\mathcal{D}_k := \mathcal{L}_k$ for $k = 1$ corresponds to the DDH assumption in the respective group $\mathbb{G}_s$ and if $\mathcal{D}_1$-MDDH holds in both source groups, then we have the SXDH assumption. Moreover, $\mathcal{D}_k$-MDDH $\implies$ $\mathcal{D}_1$-KerMDH, latter being also called the 1-KerLin assumption (cf. [KPW15] and [EHK+17, MRV16] for more details).

2.3 Primitives

Definition 7 (Collision-Resistant Hash Function). *A family $\{H_k\}_{k\in\mathcal{K}}$ of hash-functions $H_k : \{0,1\}^* \to \{0,1\}^{\ell(\lambda)}$ indexed by key $k \in \mathcal{K}$ is collision-resistant if for any PPT adversary $\mathcal{A}$ there exists a negligible function ϵ such that:*

$$\mathbf{Adv}^{\mathsf{Coll}}_{H}(\mathcal{A}) := \Pr[k \overset{R}{\leftarrow} \mathcal{K}, (v, v') \leftarrow \mathcal{A}(k) : H_k(v) = H_k(v') \ \wedge \ v \neq v'] < \epsilon(\lambda).$$

Definition 8 (Signature). *A signature scheme consists of the following four algorithms :*

- $\mathsf{Setup}(1^\lambda)$*: On input security parameter 1^λ, outputs a public parameter* pp*, which determines the message space $\mathcal{M}$ and the randomness space $\mathcal{R}$.*
- $\mathsf{KeyGen}(\mathsf{pp})$*: takes as input a public parameter* pp *and generates a public/secret key pair* $(\mathsf{pk}, \mathsf{sk})$.
- $\mathsf{Sign}(\mathsf{sk}, M)$*: takes as input a secret key* sk *and a message M, and outputs a signature σ.*
- $\mathsf{Verify}(\mathsf{pk}, M, \sigma)$*: takes as input a public key* pk*, a message M, and a signature σ, and outputs 1 if accept and 0 otherwise.*

Here, we recall the definition and the security of structure-preserving signatures, as introduced in [AFG+10].

Definition 9 (Structure-Preserving Signature). *A signature scheme is called structure preserving with respect to bilinear group generator* BGGen *if (a) a public parameter includes a bilinear group generated by* BGGen *(b) verification keys consist of group elements in $\mathbb{G}_1$ and $\mathbb{G}_2$ (c) messages consist of group elements in $\mathbb{G}_1$ and $\mathbb{G}_2$ (d) signatures consist of group elements in $\mathbb{G}_1$ and $\mathbb{G}_2$ and (e) the verification algorithm solely evaluates membership in $\mathbb{G}_1$ and $\mathbb{G}_2$, and relations described by pairing product equations.*

Definition 10 (EUF-CMA). *A (structure-preserving) signature scheme is existentially unforgeable under adaptively chosen-message attacks (EUF-CMA secure) if :*

$$\mathbf{Adv}_{\mathsf{SPS}}^{\mathsf{EUF\text{-}CMA}}(\mathcal{A}) := \Pr\left[\begin{array}{l}(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{KeyGen}(\ell) \\ (M^*,\sigma^*) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{Sign}}(\cdot,\mathsf{sk})}(\mathsf{pk})\end{array} : \begin{array}{l} M^* \notin \mathcal{Q}_{msg} \\ \mathsf{Verify}(M^*,\sigma^*,\mathsf{pk}) = 1\end{array}\right] < \epsilon(\lambda)$$

for all PPT adversaries $\mathcal{A}$. Here, $\mathcal{Q}_{msg}$ records all queries that $\mathcal{A}$ sends to $\mathcal{O}_{\mathsf{Sign}}$.

NIZK Proofs. Let $\mathcal{R}_{\mathcal{L}}$ be an efficiently computable relation of pairs (x, w) of words and witnesses. Let $\mathcal{L}$ be the language defined as $\mathcal{L} = \{x|\exists w : \mathcal{R}_{\mathcal{L}}(x,w) = 1\}$. We recall the definition of a NIZK proof system [BFM88] for a relation $\mathcal{R}_{\mathcal{L}}$ where we use the formalization in [GHKP18] (based on [GS08]) for the sake of consistency. We note that we focus on NIZK argument systems, where soundness only holds for computationally bounded adversaries.

- $\mathsf{PGen}(1^\lambda, \mathsf{par})$: On input a security parameter λ and parameters par outputs a common reference string crs.
- $\mathsf{PTGen}(1^\lambda, \mathsf{par})$: On input a security parameter λ and parameters par outputs a common reference string crs and a trapdoor trap.
- $\mathsf{PPro}(\mathsf{crs}, x, w)$: On input a common reference string crs, a statement x, and a witness w such that $\mathcal{R}_{\mathcal{L}}(x,w) = 1$, returns a proof Ω.
- $\mathsf{PVer}(\mathsf{crs}, x, \Omega)$: On input a reference string crs and a proof Ω, Returns accept if Ω is valid and reject otherwise.
- $\mathsf{PSim}(\mathsf{crs}, \mathsf{trap}, x)$: On input common reference string crs, and the trapdoor trap and word x and outputs a simulated proof Ω.

A NIZK argument system needs to satisfy the following properties.

- **Perfect Completeness:** For all possible public parameters par, all $\lambda \in \mathbb{N}$, all words $x \in \mathcal{L}$, and all witnesses w such that $\mathcal{R}_{\mathcal{L}}(x,w) = 1$, we have

$$\Pr\left[\begin{array}{l}\mathsf{crs} \leftarrow \mathsf{PGen}(1^\kappa, \mathsf{par}), \\ \Omega \leftarrow \mathsf{PPro}(\mathsf{crs}, x, w)\end{array} : \mathsf{PVer}(\mathsf{crs}, x, \Omega) = 1\right] = 1.$$

- **Computational Soundness:** For all PPT adversaries $\mathcal{A}$ and for all words $x \notin \mathcal{L}$ we have:

$$\Pr\left[\begin{array}{l}\mathsf{crs} \leftarrow \mathsf{PGen}(1^\kappa, \mathsf{par}), \\ \Omega \leftarrow \mathcal{A}(\mathsf{crs}, x)\end{array} : \mathsf{PVer}(\mathsf{crs}, x, \Omega) = 0\right] \approx 1.$$

- **Composable Zero-Knowledge:** For all PPT adversaries $\mathcal{A}$, we have

$$\Pr\left[\mathsf{crs} \leftarrow \mathsf{PGen}(1^\lambda, \mathsf{par}), : \mathcal{A}(1^\lambda, \mathsf{crs}) = 1\right] \approx$$

$$\Pr\left[(\mathsf{crs}, \mathsf{trap}) \leftarrow \mathsf{PTGen}(1^\lambda, \mathsf{par}), : \mathcal{A}(1^\lambda, \mathsf{crs}) = 1\right].$$

Furthermore, for all for all $x \in \mathcal{L}$ with witness w such that $\mathcal{R}_{\mathcal{L}}(x,w) = 1$, the following are identically distributed:

$$\mathsf{PPro}(\mathsf{crs}, x, w) \quad \text{and} \quad \mathsf{PSim}(\mathsf{crs}, \mathsf{trap}, x)$$

where $(\mathsf{crs}, \mathsf{trap}) \leftarrow \mathsf{PTGen}(1^\lambda, \mathsf{par})$. Note that the composable zero knowledge requires indistinguishability even for adversaries that get access to $(\mathsf{crs}, \mathsf{trap})$.

Quasi-Adaptive NIZK Proofs. Quasi-Adaptive NIZK (QA-NIZK) proofs [JR13, JR14, KW15] are NIZK proofs for a class of languages $\mathcal{L}_\rho$, parametrized by ρ, where the generation of the common reference string (CRS) is allowed to depend on the language parameter ρ. Moreover the common CRS includes a fixed part par, generated by an algorithm PGen. Subsequently, we recall the definitions for unbounded simulation-sound QA-NIZK proofs from [KW15] covering its tag-based variant (for the non-tag based variants all occurrences of tags can just be ignored).

Definition 11 (QA-NIZK). A non-interactive proof system $(\mathsf{Gen}_{\mathsf{par}}, \mathsf{Gen}_{\mathsf{crs}}, \mathsf{Prove}, \mathsf{Verify}, \mathsf{Sim}_\pi)$ for a class of languages $\mathcal{L}_\rho$ is defined as follows:

$\mathsf{Gen}_{\mathsf{par}}(1^\lambda)$: On input a security parameter λ output parameters par.

$\mathsf{Gen}_{\mathsf{crs}}(\mathsf{par}, \rho)$: On input par and ρ return a common reference string crs and a trapdoor trap. We assume that crs implicitly contains par and ρ and that it defines a tag-space $\mathcal{T}$. If $\mathcal{T}$ is not specified then $\mathcal{T} = \{\epsilon\}$ and tags can be ignored in all algorithms.

$\mathsf{Prove}(\mathsf{crs}, \tau, x, w)$: On input a CRS crs, a tag τ, a word x and witness w output a proof π.

$\mathsf{Verify}(\mathsf{crs}, \tau, x, \pi)$: On input a CRS crs, a tag τ, a word x and a proof π output 1 if the proof is accepted and 0 otherwise.

$\mathsf{Sim}_\pi(\mathsf{crs}, \mathsf{trap}, \tau, x)$: On input a CRS crs, a trapdoor trap, a tag τ a word x (not necessarily in $\mathcal{L}_\rho$) output a proof π.

It is said to be a QA-NIZK proof system for an ensemble of distributions $\{\mathcal{D}_{\mathsf{par}}\}$ on collection of witness-relations $\mathcal{R} = \{\mathcal{R}_\rho\}$ with associated language parameter ρ if the following holds:

Perfect Completeness: For all λ, all par output by $\mathsf{Gen}_{\mathsf{par}}(1^\lambda)$, all ρ output by $\mathcal{D}_{\mathsf{par}}$, all (x, y) with $\mathcal{R}_\rho(x, y) = 1$, we have

$$\Pr\left[\begin{array}{l}(\mathsf{crs}, \mathsf{trap}) \leftarrow \mathsf{Gen}_{\mathsf{crs}}(\mathsf{par}, \rho), \\ \pi \leftarrow \mathsf{Prove}(\mathsf{crs}, \tau, x, w)\end{array} : \mathsf{Verify}(\mathsf{crs}, \tau, x, \pi) = 1\right] = 1$$

Perfect Zero-Knowledge: For all λ, all par output by $\mathsf{Gen}_{\mathsf{par}}(1^\lambda)$, all ρ output by $\mathcal{D}_{\mathsf{par}}$, all $(\mathsf{crs}, \mathsf{trap})$ output by $\mathsf{Gen}_{\mathsf{crs}}(\mathsf{par}, \rho)$, all (x, y) with $\mathcal{R}_\rho(x, y) = 1$, the distributions

$$\mathsf{Prove}(\mathsf{crs}, \tau, x, w) \quad \text{and} \quad \mathsf{Sim}_\pi(\mathsf{crs}, \mathsf{trap}, \tau, x)$$

are identical. Note that the formalization of perfect zero-knowledge is similar to that of composable zero knowledge in [GS08] and requires indistinguishability even for adversaries that get access to $(\mathsf{crs}, \mathsf{trap})$.

(Unbound) Simulation-Soundness: For all λ and all PPT adversaries $\mathcal{A}$

$$\mathbf{Adv}^{\mathsf{USS}}_{\mathsf{QA}}(\mathcal{A}) := \Pr\left[\begin{array}{l} \mathsf{par} \leftarrow \mathsf{Gen}_{\mathsf{par}}(1^\lambda), \rho \leftarrow \mathcal{D}_{\mathsf{par}}, \\ (\mathsf{crs}, \mathsf{trap}) \leftarrow \mathsf{Sim}_{\mathsf{crs}}(\mathsf{par}, \rho), \\ (x^*, \tau^*, \pi^*) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{Prove}}(\cdot,\cdot)}(\mathsf{par}, \mathsf{crs}, \rho) \end{array} : \begin{array}{l} y^* \notin \mathcal{L}_\rho \quad \wedge \\ \tau^* \notin \mathcal{Q}_{tag} \ \wedge \\ \mathsf{Verify}(\mathsf{crs}, \tau^*, \\ x^*, \pi^*) = 1 \end{array}\right] < \epsilon(\lambda)$$

where $\mathcal{O}_{\mathsf{Prove}}(\tau, x)$ returns $\mathsf{Sim}_\pi(\mathsf{crs}, \mathsf{trap}, \tau, y)$ and adds τ to the set $\mathcal{Q}_{tag}$.

3 Our Core Lemma

In this section we provide our core lemma. Instead of directly proving security of the SPS scheme and USS QA-NIZK proofs, we first prove the security of our core lemma and later use it to prove the security of both schemes.

Essentially, our core lemma is a randomization technique which says that going from a specific distribution to a random distribution is indistinguishable under the LinSum assumption. We present our core lemma in Figure 3 and note that the strategy to prove the core lemma is somehow reminiscent of the adaptive partitioning technique by Hofheinz [Hof17] and similar to the approach in [GHKP18] (whereas Gay et al. require $\log Q$ hybrids instead of 2 as in our case). We additionally parametrize our core lemma with a input bit b determining which of the two values $[w_0]_1$ and $[w_1]_1$ in tag is actually verified. Note that in the core lemma, for the QA-NIZK case we include $[\mathbf{x}_0]_1$ and $[\mathbf{x}_1]_1$ in the parameters pp. While this would also work for the SPS case, we remove them as in the security game of the SPS scheme, the reduction does not need to know these values, as they will vanish in public keys (in this case, one can also remove the first verification equation, but it does not affect the security).

Lemma 3 (Core Lemma). *If the Q-fold k-LinSum assumption holds, then going from experiment EXP_0^{core} to EXP_1^{core} can only increase the winning chances of an adversary negligibly. Namely, for any PPT adversary A, there exist a PPT adversary $\mathcal{B}$, such that*

$$\mathbf{Adv}^{core}_{\mathsf{BG}}(\mathcal{A}) < 8 \cdot \mathbf{Adv}^{Q\text{-}\mathsf{LinSum}}_{\mathcal{LS}_k, \mathbb{G}_1}(\mathcal{B})$$

where Q is the number of queries to CTAG.

Proof. We prove the claim using a sequence of games.
Game 0: This game corresponds to $\mathsf{EXP}_0^{\mathrm{core}}$ and we have:

$$\mathbf{Adv}_0 = \mathbf{Adv}^{\mathsf{EXP}_0^{\mathrm{core}}}(\mathcal{A})$$

Game 1: In this game, we use the received bit $b \in \{0,1\}$ to determine which equation should be verified. Then we receive a Q-fold k-LinSum tuple $[\mathbf{x}_{1-b}]_1$, $[\mathbf{r}_i^\top]_1$, $[z_i]_1$ with $[z_i]_1$ being either $[\mathbf{r}_i^\top \mathbf{x}_{1-b}]$ or $[\zeta_i]_1$ for random values $\mathbf{r}_i \in \mathbb{Z}_p^k$, and $\zeta_i \in \mathbb{Z}_p$ and set $[w_{1-b}]_1 := [z_i]_1$.

```
Experiment $\mathsf{EXP}^{\mathrm{core}}_{\beta}(b), \beta \in \{0,1\}$:
$\mathsf{ct} := 0$
$\mathsf{BG} \leftarrow \mathsf{BGGen}(1^{\lambda})$
$\mathbf{x}_0, \mathbf{x}_1 \xleftarrow{R} \mathbb{Z}_p^k$
// $\mathsf{F}_0, \mathsf{F}_1$ are truly random functions
$\mathsf{F}_i : \mathbb{Z}_p \rightarrow \mathbb{Z}_p, i \in \{0,1\}$
if SPS
  $\mathsf{pp} := \mathsf{BG}$
elseif QA-NIZK
  $\mathsf{pp} := (\mathsf{BG}, [\mathbf{x}_0]_1, [\mathbf{x}_1]_1)$
$\mathsf{tag} \leftarrow \mathcal{A}^{\mathsf{CTAG}()}(\mathsf{pp})$
return $\mathsf{CVER}(\mathsf{tag})$
```

```
$\mathsf{CTAG}()$ :
$\mathsf{ct} := \mathsf{ct} + 1$
$\mathbf{r} \xleftarrow{R} \mathbb{Z}_p^k$
$[w_0]_1 := [\mathbf{r}^{\top}\mathbf{x}_0 + \beta\mathsf{F}_0(\mathsf{ct})]_1$
$[w_1]_1 := [\mathbf{r}^{\top}\mathbf{x}_1 + \beta\mathsf{F}_1(\mathsf{ct})]_1$
$\mathsf{tag} := ([\mathbf{r}^{\top}]_1, [w_0]_1, [w_1]_1)$
return $\mathsf{tag}$
```

```
$\mathsf{CVER}(\mathsf{tag})$ :
Parse $\mathsf{tag} = ([\mathbf{r}^{\top}]_1, [w_0]_1, [w_1]_1)$
if $[w_b]_1 = [\mathbf{r}^{\top}]_1\mathbf{x}_b$
  or $\exists \mathsf{ct}' \leq \mathsf{ct} : [w_b]_1 = [\mathbf{r}^{\top}]_1\mathbf{x}_b + \beta\mathsf{F}_b(\mathsf{ct}')$
return 1
else return 0
```

Fig. 1. Experiment for our core lemma.

We set $b_1 = b$. Using the Q-fold $\mathcal{LS}_k$-LinSum assumption we have:

$$|\mathbf{Adv}_0 - \mathbf{Adv}_1| < \mathbf{Adv}^{Q\text{-}\mathsf{LinSum}}_{\mathcal{LS}_k,\mathbb{G}_1}(\mathcal{B})$$

Game 2: In this game, we use the received bit $b \in \{0,1\}$ to determine which equation should be verified. If $b \neq b_1$, we abort and otherwise, as we know $\mathbf{x}_{1-b_1}$, we construct $w_{1-b_1} = \mathbf{r}^{\top}\mathbf{x}_{1-b_1} + \mathsf{F}_{1-b_1}(\mathsf{ct})$ in each query of the adversary, for fresh $\mathbf{r} \in \mathbb{Z}_p^k$.

The view of the adversary does not change, and we have:

$$\mathbf{Adv}_2 = 2 \cdot \mathbf{Adv}_1$$

Game 3: In this game, we use the received bit $b \in \{0,1\}$ to determine which equation should be verified. If $b = b_1$, we abort and otherwise, we receive a Q-fold k-LinSum tuple $[\mathbf{x}_{1-b}]_1$, $[\mathbf{r}_i^{\top}]_1$, $[z_i]_1$ with $[z_i]_1$ being either $[\mathbf{r}_i^{\top}\mathbf{x}_{1-b}]$ or $[\zeta_i]_1$ for random values $\mathbf{r}_i \in \mathbb{Z}_p^k$, and $\zeta_i \in \mathbb{Z}_p$ and set $[w_{1-b}]_1 = [z_i]_1$. Also, in this game, and next games, we additionally check a verification as $[w_b]_1 = [\mathbf{r}^{\top}]_1\mathbf{x}_b + \mathsf{F}_b(\mathsf{ct}')$. Using the Q-fold k-LinSum assumption we have:

$$|\frac{1}{2} \cdot \mathbf{Adv}_3 - \mathbf{Adv}_2| < \mathbf{Adv}^{Q\text{-}\mathsf{LinSum}}_{\mathcal{LS}_k,\mathbb{G}_1}(\mathcal{B})$$

Game 4: In this game, we use the received bit $b \in \{0,1\}$ to determine which equation should be verified. If $b = b_1$, we abort and otherwise, as we know $\mathbf{x}_{1-b}$, we construct $w_{1-b} = \mathbf{r}^{\top}\mathbf{x}_{1-b} + \mathsf{F}_{1-b}(\mathsf{ct})$ in each query of the adversary, for fresh $\mathbf{r} \in \mathbb{Z}_p^k$.

The view of the adversary does not change, and we have:

$$\mathbf{Adv}_4 = 2 \cdot \mathbf{Adv}_3$$

Game 4 corresponds to $\mathsf{EXP}^{\mathrm{core}}_1$, which concludes the proof. □

4 Our USS QA-NIZK Proof

In this section we present our construction for USS QA-NIZK proofs for linear spaces. Therefore, let us briefly discuss parameter generation and the description of the languages. $\mathsf{Gen}_{\mathsf{par}}$ on input 1^λ runs BGGen and returns $\mathsf{par} := \mathsf{BG}$ as the description of a bilinear group. The probability distribution $\mathcal{D}_{\mathsf{par}}$ returns a matrix $\rho = [\mathbf{M}]_1 \in \mathbb{G}^{n\times t}$, for integers $n > t$. Given par and ρ, the language $\mathcal{L}_{\mathbf{M}}$ is defined as

$$\mathcal{L}_{\mathbf{M}} = \left\{ [\mathbf{y}]_1 \in \mathbb{G}_1^n : \exists \mathbf{x} \in \mathbb{Z}_p^t \text{ s.t. } \mathbf{y} = \mathbf{M}\mathbf{x} \right\}.$$

In Figure 3 we present an USS QA-NIZK scheme under simple assumptions.

- $\underline{\mathsf{Gen}_{\mathsf{par}}(1^\lambda)}$: Given a security parameter 1^λ, return $\mathsf{par} := (\mathsf{BG}, H_k)$ where $\mathsf{BG} \leftarrow \mathsf{BGGen}(1^\lambda)$ and $H_k : \{0,1\}^* \to \mathbb{Z}_p$ with $k \overset{R}{\leftarrow} \mathcal{K}$ is a collision-resistant hash function.
- $\underline{\mathsf{Gen}_{\mathsf{crs}}(\mathsf{par}, \mathbf{M})}$: Pick $\mathbf{A} \overset{R}{\leftarrow} \mathcal{D}_k$, $\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3 \overset{R}{\leftarrow} \mathbb{Z}_p^{n\times(k+1)}$, and $\mathbf{K}_4, \mathbf{K}_5 \overset{R}{\leftarrow} \mathbb{Z}_p^{k\times(k+1)}$ and return $\mathsf{trap} = (\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3)$ and $\mathsf{crs} = ([\mathbf{A}]_2, [\mathbf{P}_0]_1 = [\mathbf{M}^\top\mathbf{K}_0]_1, [\mathbf{P}_1]_1 = [\mathbf{M}^\top\mathbf{K}_1]_1, [\mathbf{P}_2]_1 = [\mathbf{M}^\top\mathbf{K}_2]_1, [\mathbf{P}_3]_1 = [\mathbf{M}^\top\mathbf{K}_3]_1, [\mathbf{P}_4]_1 = [\mathbf{K}_4]_1, [\mathbf{P}_5]_1 = [\mathbf{K}_5]_1, [\mathbf{K}_0\mathbf{A}]_2, [\mathbf{K}_1\mathbf{A}]_2, [\mathbf{K}_2\mathbf{A}]_2, [\mathbf{K}_3\mathbf{A}]_2, [\mathbf{K}_4\mathbf{A}]_2, [\mathbf{K}_5\mathbf{A}]_2)$.
- $\underline{\mathsf{Prove}(\mathsf{crs}, [\mathbf{y}]_1, \mathbf{x})}$: On input crs, a word $[\mathbf{y}]_1 \in \mathbb{G}_1^n$ and corresponding witness $\mathbf{x} \in \mathbb{Z}_p^t$, pick $\mathbf{r} \overset{R}{\leftarrow} \mathbb{Z}_p^k$, compute $\tau = H_k([\mathbf{y}]_1, [\mathbf{r}]_1)$ and return proof $\pi = ([\mathbf{u}_0]_1, [\mathbf{u}_1]_1, \boldsymbol{\rho} = [\mathbf{r}^\top]_1)$ with:

$$[\mathbf{u}_0]_1 := [\mathbf{x}^\top(\mathbf{P}_0 + \tau\mathbf{P}_2) + \mathbf{r}^\top\mathbf{P}_4)]_1$$

$$[\mathbf{u}_1]_1 := [\mathbf{x}^\top(\mathbf{P}_1 + \tau\mathbf{P}_3) + \mathbf{r}^\top\mathbf{P}_5)]_1$$

- $\underline{\mathsf{Verify}(\mathsf{crs}, [\mathbf{y}]_1, \pi)}$: On input crs, a word $[\mathbf{y}]_1 \in \mathbb{G}_1^n$ and proof $\pi = ([\mathbf{u}_0]_1, [\mathbf{u}_1]_1, \boldsymbol{\rho} = [\mathbf{r}]_1)$, compute $\tau = H_k([\mathbf{y}]_1, \boldsymbol{\rho})$ and return 1 if the following holds and 0 otherwise:

$$e([\mathbf{u}_0]_1, [\mathbf{A}]_2) = e([\mathbf{y}^\top]_1, [\mathbf{K}_0\mathbf{A}]_2 + \tau[\mathbf{K}_2\mathbf{A}]_2) + e(\boldsymbol{\rho}, [\mathbf{K}_4\mathbf{A}]_2) \quad (1)$$

$$e([\mathbf{u}_1]_1, [\mathbf{A}]_2) = e([\mathbf{y}^\top]_1, [\mathbf{K}_1\mathbf{A}]_2 + \tau[\mathbf{K}_3\mathbf{A}]_2) + e(\boldsymbol{\rho}, [\mathbf{K}_5\mathbf{A}]_2) \quad (2)$$

- $\underline{\mathsf{Sim}_\pi(\mathsf{crs}, \mathsf{trap}, [\mathbf{y}]_1)}$: On input crs, trapdoor $\mathsf{trap} = (\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3)$ and word $[\mathbf{y}]_1 \in \mathbb{G}_1^n$, pick $\mathbf{r} \overset{R}{\leftarrow} \mathbb{Z}_p$, compute $\tau = H_k([\mathbf{y}]_1, [\mathbf{r}]_1)$ and return proof $\pi = ([\mathbf{u}_0]_1, [\mathbf{u}_1]_1, \boldsymbol{\rho} = [\mathbf{r}^\top]_1)$ with:

$$[\mathbf{u}_0]_1 := [\mathbf{y}^\top(\mathbf{K}_0 + \tau\mathbf{K}_2) + \mathbf{r}^\top\mathbf{P}_4]_1$$

$$[\mathbf{u}_1]_1 := [\mathbf{y}^\top(\mathbf{K}_1 + \tau\mathbf{K}_3) + \mathbf{r}^\top\mathbf{P}_5]_1$$

Fig. 2. Our USS QA-NIZK scheme.

Theorem 1. *If the $\mathcal{D}_k$-KerMDH and k-LinSum assumptions holds, our USS QA-NIZK scheme from Figure 3 is perfectly zero-knowledge and tightly unbounded simulation-sound. In particular, for any efficient adversary $\mathcal{A}$, which makes at most Q simulator queries, there exist adversaries $\mathcal{B}$, $\mathcal{B}_1$ and $\mathcal{B}_2$ such that:*

$$\mathbf{Adv}^{\mathsf{USS}}_{\mathsf{QA}}(\mathcal{A}) \leqslant \mathbf{Adv}^{\mathsf{coll}}_{H}(\mathcal{B}) + \mathbf{Adv}^{\mathsf{KerMDH}}_{\mathcal{D}_k,\mathbb{G}_2}(\mathcal{B}_1) + \mathbf{Adv}^{\mathsf{EXP}^{core}}_{\mathsf{BG}}(\mathcal{B}_2) + \frac{Q}{p}$$

Proof. As Prove and Sim_π are identically distributed, we have perfectly zero-knowledge. In the following we prove unbounded simulation-soundness of the scheme.

We prove the claim using a sequence of games:
Game 0: This game is the original game and we have:

$$\mathbf{Adv}_0 = \mathbf{Adv}^{\mathsf{USS}}_{\mathsf{QA}}(\mathcal{A})$$

Game 1: In this game we have $\mathcal{Q}_{\text{tag}}$ as all tags τ that we have sent to the adversary. Finally, when the adversary sends his forgery $([\mathbf{u}_0]_1, [\mathbf{u}_1]_1, \boldsymbol{\rho})$ for a new statement $[\mathbf{y}]_1$ with $\tau = H_k([\mathbf{y}]_1, \boldsymbol{\rho})$, if $\tau = \tau_j$ for some $\tau_j \in \mathcal{Q}_{\text{tag}}$, we can break collision resistance of the hash function. Thus, we have:

$$|\mathbf{Adv}_1 - \mathbf{Adv}_0| \leqslant \mathbf{Adv}^{\mathsf{coll}}_{H}(\mathcal{B})$$

Game 2: In this game we verify the following equations instead of the original verification equations (1) and (2).

$$[\mathbf{u}_0]_1 = [\mathbf{y}^\top]_1(\mathbf{K}_0 + \tau\mathbf{K}_2) + \boldsymbol{\rho}\mathbf{K}_4$$

$$[\mathbf{u}_1]_1 = [\mathbf{y}^\top]_1(\mathbf{K}_1 + \tau\mathbf{K}_3) + \boldsymbol{\rho}\mathbf{K}_5$$

For any proof $\pi = ([\mathbf{u}_0]_1, [\mathbf{u}_1]_1, \boldsymbol{\rho})$ that passes the original verification but not verification of Game 2, the values

$$[\mathbf{u}_0]_1 - [\mathbf{y}^\top]_1(\mathbf{K}_0 + \tau\mathbf{K}_2) + \boldsymbol{\rho}\mathbf{K}_4$$

$$[\mathbf{u}_1]_1 - [\mathbf{y}^\top]_1(\mathbf{K}_1 + \tau\mathbf{K}_3) + \boldsymbol{\rho}\mathbf{K}_5$$

are non-zero vectors in the kernel of $\mathbf{A}$. Thus if $\mathcal{A}$ outputs such a proof, we can construct an adversary $\mathcal{B}_1$ that breaks the $\mathcal{D}_k$-KerMDH assumption in $\mathbb{G}_2$. To do this we proceed as follows. The adversary $\mathcal{B}_1$ receives $(\mathsf{BG}, [\mathbf{A}]_2)$, samples all other parameters and simulates Game 2 for $\mathcal{A}$. When $\mathcal{B}_1$ receives a forgery from $\mathcal{A}$ as tuple $([\mathbf{u}_0]_1, [\mathbf{u}_1]_1, \boldsymbol{\rho})$, he passes one of following values to its own challenger:

$$[\mathbf{u}_0]_1 - [\mathbf{y}^\top]_1(\mathbf{K}_0 + \tau\mathbf{K}_2) + \boldsymbol{\rho}\mathbf{K}_4$$

$$[\mathbf{u}_1]_1 - [\mathbf{y}^\top]_1(\mathbf{K}_1 + \tau\mathbf{K}_3) + \boldsymbol{\rho}\mathbf{K}_5$$

We have:

$$|\mathbf{Adv}_2 - \mathbf{Adv}_1| \leqslant \mathbf{Adv}^{\mathsf{KerMDH}}_{\mathcal{D}_k,\mathbb{G}_2}(\mathcal{B}_1)$$

Game 3: In this game we replace $\mathbf{K}_0 := \mathbf{K}_0 + \mathbf{k}_0\mathbf{a}^{\perp}$ and $\mathbf{K}_1 := \mathbf{K}_1 + \mathbf{k}_0\mathbf{a}^{\perp}$, and $\mathbf{K}_2 := \mathbf{K}_2 + \mathbf{k}_1\mathbf{a}^{\perp}$ and $\mathbf{K}_3 := \mathbf{K}_3 + \mathbf{k}_1\mathbf{a}^{\perp}$ (in the CRS generation we can pick $\mathbf{k}_0, \mathbf{k}_1 \in \mathbb{Z}_p^{n\times 1}$ and $\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3 \in \mathbb{Z}_p^{n\times(k+1)}$ and set $\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3$; we have $\mathbf{a}^{\perp}\mathbf{A} = 0$ for $\mathbf{a}^{\perp} \in \mathbb{Z}_p^{1\times(k+1)}$), and $\mathbf{K}_4 := \mathbf{K}_4 + \mathbf{x}_0\mathbf{a}^{\perp}$, and $\mathbf{K}_5 := \mathbf{K}_5 + \mathbf{x}_1\mathbf{a}^{\perp}$ (in the CRS generation we can pick $\mathbf{x}_0, \mathbf{x}_1 \in \mathbb{Z}_p^{k}$ and $\mathbf{K}_4, \mathbf{K}_5 \in \mathbb{Z}_p^{k\times(k+1)}$). So, our proof has the following form:[8]

$$[\mathbf{u}_0]_1 \leftarrow [\mathbf{y}^{\top}(\mathbf{K}_0 + \tau\mathbf{K}_2) + \mathbf{r}^{\top}\mathbf{K}_4]_1 + [\mathbf{y}^{\top}(\mathbf{k}_0 + \tau\mathbf{k}_1) + \mathbf{r}^{\top}\mathbf{x}_0]_1\mathbf{a}^{\perp}$$

$$[\mathbf{u}_1]_1 \leftarrow [\mathbf{y}^{\top}(\mathbf{K}_1 + \tau\mathbf{K}_3) + \mathbf{r}^{\top}\mathbf{K}_5]_1 + [\mathbf{y}^{\top}(\mathbf{k}_0 + \tau\mathbf{k}_1) + \mathbf{r}^{\top}\mathbf{x}_1]_1\mathbf{a}^{\perp}$$

and also we verify the forgery $(\mathbf{y}^*, \pi^*)$ as:

$$[\mathbf{u}_0^*]_1 \leftarrow [\mathbf{y}^{*\top}(\mathbf{K}_0 + \tau\mathbf{K}_2) + \boldsymbol{\rho}^*\mathbf{K}_4]_1 + [\mathbf{y}^{*\top}(\mathbf{k}_0 + \tau\mathbf{k}_1) + \boldsymbol{\rho}^*\mathbf{x}_0]_1\mathbf{a}^{\perp}$$

$$[\mathbf{u}_1]_1 \leftarrow [\mathbf{y}^{*\top}(\mathbf{K}_1 + \tau\mathbf{K}_3) + \boldsymbol{\rho}^*\mathbf{K}_5]_1 + [\mathbf{y}^{*\top}(\mathbf{k}_0 + \tau\mathbf{k}_1) + \boldsymbol{\rho}^*\mathbf{x}_1]_1\mathbf{a}^{\perp}$$

We can rewrite them as:

$$[\mathbf{u}_0^*]_1 \leftarrow [\mathbf{y}^{*\top}(\mathbf{K}_0 + \tau\mathbf{K}_2) + \boldsymbol{\rho}^*\mathbf{K}_4]_1 + c_0\,\mathbf{a}^{\perp}$$

$$[\mathbf{u}_1]_1 \leftarrow [\mathbf{y}^{*\top}(\mathbf{K}_1 + \tau\mathbf{K}_3) + \boldsymbol{\rho}^*\mathbf{K}_5]_1 + c_1\,\mathbf{a}^{\perp}$$

for $c_0 = [\mathbf{y}^{*\top}(\mathbf{k}_0 + \tau\mathbf{k}_1) + \boldsymbol{\rho}^*\mathbf{x}_0]_1$, and $c_1 = [\mathbf{y}^{*\top}(\mathbf{k}_0 + \tau\mathbf{k}_1) + \boldsymbol{\rho}^*\mathbf{x}_1]_1$.
We have:

$$\mathbf{Adv}_3 = \mathbf{Adv}_2$$

Game 4: In this game, we pick $b \overset{R}{\leftarrow} \{0,1\}$, and verify all equations[9], except for the value c_{1-b}.

The view of the adversary does not change, and the transition from Game 3 to Game 4 can only increase the chance of the adversary. We have:

$$\mathbf{Adv}_3 < \mathbf{Adv}_4$$

Game 5: In this game, we construct $\mathbf{u}_0$ and $\mathbf{u}_1$ as follows for the i-th query:

$$[\mathbf{u}_0]_1 \leftarrow [\mathbf{y}^{\top}(\mathbf{K}_0 + \tau\mathbf{K}_2) + \boldsymbol{\rho}\mathbf{K}_4]_1 + [\mathbf{y}^{\top}(\mathbf{k}_0 + \tau\mathbf{k}_1) + \boldsymbol{\rho}\mathbf{x}_0 + \mathsf{F}_0(i)]_1\mathbf{a}^{\perp}$$

$$[\mathbf{u}_1]_1 \leftarrow [\mathbf{y}^{\top}(\mathbf{K}_1 + \tau\mathbf{K}_3) + \boldsymbol{\rho}\mathbf{K}_5]_1 + [\mathbf{y}^{\top}(\mathbf{k}_0 + \tau\mathbf{k}_1) + \boldsymbol{\rho}\mathbf{x}_1 + \mathsf{F}_1(i)]_1\mathbf{a}^{\perp}$$

for truly random functions F_0 and F_1, where $\mathsf{F}_i : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$. Now, we show if $\mathcal{A}$ can distinguish between Game 4 and Game 5, we can construct a distinguisher $\mathcal{B}_2$ for the core lemma. $\mathcal{B}_2$ sends the bit b to core lemma. It receives $\mathsf{pp} = (\mathsf{BG}, [\mathbf{x}_0]_1, [\mathbf{x}_1]_1)$ from the core lemma experiment, and sets the CRS according

[8] Note that the values $\mathbf{x_0}, \mathbf{x_1}$ are not required in the generation of $[\mathbf{K}_i\mathbf{A}]_2$.

[9] Note that we could verify the black part of $[\mathbf{u}_{1-b}]_1$, but we do not require it.

to it and sends his crs to the adversary $\mathcal{A}$. To simulate the Prove oracle, it uses $\mathsf{CTAG}()$ and receives $(\boldsymbol{\rho}, [w_0]_1, [w_1]_1)$. Then he computes $\tau = H([\mathbf{y}]_1, \boldsymbol{\rho})$ and constructs the proofs using these parameters as

$$[\mathbf{u}_0]_1 \leftarrow [\mathbf{y}^\top(\mathbf{K}_0 + \tau\mathbf{K}_2) + \boldsymbol{\rho}\mathbf{K}_4]_1 + [\mathbf{y}^\top(\mathbf{k}_0 + \tau\mathbf{k}_1) + w_0]_1\mathbf{a}^\perp$$
$$[\mathbf{u}_1]_1 \leftarrow [\mathbf{y}^\top(\mathbf{K}_1 + \tau\mathbf{K}_3) + \boldsymbol{\rho}\mathbf{K}_5]_1 + [\mathbf{y}^\top(\mathbf{k}_0 + \tau\mathbf{k}_1) + w_1]_1\mathbf{a}^\perp$$

Finally, given the forgery $([\mathbf{m}^*]_1, \pi^*)$, he derives $\mathsf{tag}^* = (\boldsymbol{\rho}^*, [w_0^*]_1, [w_1^*]_1)$, calls $\mathsf{CVER}(\mathsf{tag}^*)$ and forwards the answer to $\mathcal{A}$.

Based on core lemma, we have:

$$|\mathbf{Adv}_3 - \mathbf{Adv}_4| \leqslant \mathbf{Adv}_{\mathsf{BG}}^{\mathsf{EXP}^{\mathrm{core}}}(\mathcal{B}_2)$$

Game 6: In this game, we are going to show that the adversary has negligible chance to give a fake proof, i.e., $\mathbf{y}^* \notin \mathrm{span}(\mathbf{M})$. Actually, we consider an information theoretic argument. As shown, we mask the parts including $\mathbf{k}_0$ and $\mathbf{k}_1$ in the proofs, except for when the adversary sets i^* as one of the previous queries, say $\hat{i}$ (ct' in the core lemma), which happens with probability $\frac{1}{Q}$ over the choice of $i^* \xleftarrow{R} [1, Q]$. So, the only leaked information from

$$[\mathbf{u}_0]_1 \leftarrow [\mathbf{y}_{\hat{i}}^\top(\mathbf{K}_0 + \tau_{\hat{i}}\mathbf{K}_2) + \mathbf{r}_{\hat{i}}^\top\mathbf{K}_4]_1 + [\mathbf{y}_{\hat{i}}^\top(\mathbf{k}_0 + \tau_{\hat{i}}\mathbf{k}_1) + \mathbf{r}_{\hat{i}}^\top\mathbf{x}_0 + \mathsf{F}_0(\hat{i})]_1\mathbf{a}^\perp$$

$$[\mathbf{u}_1]_1 \leftarrow [\mathbf{y}_{\hat{i}}^\top(\mathbf{K}_1 + \tau_{\hat{i}}\mathbf{K}_3) + \mathbf{r}_{\hat{i}}^\top\mathbf{K}_5]_1 + [\mathbf{y}_{\hat{i}}^\top(\mathbf{k}_0 + \tau_{\hat{i}}\mathbf{k}_1) + \mathbf{r}_{\hat{i}}^\top\mathbf{x}_1 + \mathsf{F}_1(\hat{i})]_1\mathbf{a}^\perp$$

is $\mathbf{y}_{\hat{i}}^\top(\mathbf{k}_0 + \tau_{\hat{i}}\mathbf{k}_1)$. As $\mathbf{a}^\perp\mathbf{A} = 0$, the values of $\mathbf{k}_0$ and $\mathbf{k}_1$ will vanish in the CRS parts $[\mathbf{K}_0\mathbf{A}]_2$, $[\mathbf{K}_1\mathbf{A}]_2$, $[\mathbf{K}_2\mathbf{A}]_2$ and $[\mathbf{K}_3\mathbf{A}]_2$. So, it remains to argue about the information $\mathbf{M}^\top\mathbf{k}_0$ and $\mathbf{M}^\top\mathbf{k}_1$ in the CRS. Note that since $\mathbf{M} \in \mathbb{Z}_p^{n\times t}$ and $\mathbf{k}_0, \mathbf{k}_1 \in \mathbb{Z}_p^n$ (for $n > t$), the value of $\mathbf{k}_0 + \tau^*\mathbf{k}_1$ for a new $\tau^* \neq \tau_{\hat{i}}$ remains hidden under all leaked information. Overall, we conclude that under this information, the value of $\mathbf{y}^{*\top}(\mathbf{k}_0 + \tau^*\mathbf{k}_1)$ is distributed uniformly random for the adversary. So, $\mathcal{A}$ can satisfy condition c_b only with probability of $\frac{Q}{p}$. We have:

$$\mathbf{Adv}_6 = \frac{Q}{p}$$

□

5 Our SPS Scheme

In this section we present our SPS scheme. Before we present our concrete construction, we present a NIZK argument ($\mathit{\Omega}_{\mathbf{A_0}}$) for membership in a linear space, which we require as a building block for our SPS scheme. As we mentioned, we are interested in non-malleability of this NIZK argument [10], like the variant used in [GHKP18]. Actually, our NIZK inherits non-malleability of the NIZK proof in [GHKP18].

[10] The SPS scheme in [JOR18], also uses non-malleability of GS proofs for quadratic equations (cf. section 3).

5.1 NIZK Argument for Membership in a Linear Space

We define a NIZK argument $\Omega_{\mathbf{A_0}}$ inspired by the work in [Ràf15, GHKP18]. While [GHKP18], however, present an OR-proof of membership in one of two spaces, we require a proof for only one space and thus can make the proof significantly simpler. The language we are considering is

$$\mathcal{L}_{\mathbf{A_0}} = \{[\mathbf{x}]_1 \in \mathbb{G}_1^k | \exists \mathbf{r} \in \mathbb{Z}_p^k : [\mathbf{x}]_1 = [\mathbf{A_0}]_1 \mathbf{r}\},$$

for $\mathbf{A_0} \in \mathbb{Z}_p^{k \times k}$.

To instantiate $\Omega_{\mathbf{A_0}}$, we require a QA-NIZK for which we use the following $\mathcal{O}(1)$ tightly secure QA-NIZK from [KW15] for language

$$\mathcal{L}_{\mathbf{M}} = \left\{[\mathbf{y}]_1 \in \mathbb{G}_1^n : \exists \mathbf{x} \in \mathbb{Z}_p^t \text{ s.t. } \mathbf{y} = \mathbf{M}\mathbf{x}\right\},$$

which we recall subsequently.

An efficient QA-NIZK with adaptive soundness for WS distributions. We recall that distributions are witness sampleable [JR13] if there exist an efficiently sampleable distribution $\mathcal{D}'_{\mathsf{par}}$ that outputs $\mathbf{M}' \in \mathbb{Z}_p^{n \times t}$ such that $[\mathbf{M}']_1$ has the same distribution as $[\mathbf{M}]_1$. The QA-NIZK proof is presented in Figure 3.

```
$\mathsf{pargen}(1^\lambda)$ :
    $\mathsf{BG} \leftarrow \mathsf{BGGen}(1^\lambda)$
    return $\mathsf{par} := \mathsf{BG}$

$\mathsf{prove}(\mathsf{crs}, [\mathbf{y}]_2 = [\mathbf{Mx}]_2, \mathbf{x})$ :
    $\pi := [\mathbf{x}^\top \mathbf{P}]_2$
    return $\pi$

$\mathsf{sim}(\mathsf{crs}, \mathsf{trap}, [\mathbf{y}]_2)$ :
    $\pi := [\mathbf{y}^\top \mathbf{K}]_2$
    return $\pi$

$\mathsf{crsgen}(\mathsf{par}, [\mathbf{M}]_2 \in \mathbb{G}_2^{n \times t})$ :
    $\mathbf{A} \xleftarrow{R} \mathcal{D}_k$
    $\mathbf{K} \xleftarrow{R} \mathbb{Z}_p^{n \times k}$
    $\mathbf{P} := \mathbf{M}^\top \mathbf{K}$
    $\mathbf{C} := \mathbf{K}\overline{\mathbf{A}}$
    $\mathsf{crs} := ([\mathbf{P}]_2, [\overline{\mathbf{A}}]_1, [\mathbf{C}]_1)$
    $\mathsf{trap} := \mathbf{K}$
    return $(\mathsf{crs}, \mathsf{trap})$

$\mathsf{verify}(\mathsf{crs}, [\mathbf{y}]_{\mathbf{2}}, \pi)$ :
    if $e([\overline{\mathbf{A}}]_1, \pi) = e([\mathbf{C}]_1, [\mathbf{y}^\top]_2)$
        return $1$
    else return $0$
```

Fig. 3. QA-NIZK from [KW15]

Theorem 2 ([KW15]). *The protocol in Figure 3 is a Quasi-adaptive Non-Interactive Zero-Knowledge Argument. Suppose in addition that $\mathcal{D}_{par}$ is a witness sampleable distribution. Then, under the $\mathcal{D}_k$-*KerMDH *Assumption in $\mathbb{G}_1$, the protocol has adaptive soundness.*

Our NIZK proof $\Omega_{\mathbf{A_0}}$. In Figure 4 we present our NIZK argument system.

```
$\mathsf{PGen}(1^\lambda, \mathsf{par})$ :
$\mathbf{A}, \mathbf{D} \xleftarrow{R} \mathcal{D}_k$
$\mathbf{z} \xleftarrow{R} \mathbb{Z}_p^{k+1} \notin \mathrm{span}(\mathbf{D})$
$\mathbf{K} \xleftarrow{R} \mathbb{Z}_p^{(k+1)\times k}$
$\mathbf{M} := \mathbf{D}$
$\mathbf{P} := \mathbf{M}^\top \mathbf{K}$
$\mathbf{C} := \mathbf{K}\overline{\mathbf{A}}$
$\mathsf{crs} := (\mathsf{par}, [\mathbf{D}]_2, [\mathbf{z}]_2, [\mathbf{P}]_2, [\overline{\mathbf{A}}]_1, [\mathbf{C}]_1)$
return crs

$\mathsf{PPro}(\mathsf{crs}, [\mathbf{x}]_1, \mathbf{r})$ :
$\mathbf{v} \xleftarrow{R} \mathbb{Z}_p^k$
$\mathbf{S} \xleftarrow{R} \mathbb{Z}_p^{k\times k}$
$[\mathbf{z}_0]_2 := [\mathbf{D}]_2 \cdot \mathbf{v}$
// QA-NIZK for $[\mathbf{z}_0]_2$
$\pi_1 := \mathbf{v}^\top [\mathbf{P}]_2$
$[\mathbf{z}_1]_2 := [\mathbf{z}]_2 - [\mathbf{z}_0]_2$
$[\mathbf{C}]_2 := \mathbf{S} \cdot [\mathbf{D}]_2^\top + \mathbf{r} \cdot [\mathbf{z}_1]_2^\top$
$[\mathbf{\Pi}]_1 := [\mathbf{A}_0]_1 \cdot \mathbf{S}$
$\pi := ([\mathbf{z}_0]_2, [\mathbf{C}]_2, [\mathbf{\Pi}]_1, \pi_1)$
return $\pi$

$\mathsf{PVer}(\mathsf{crs}, [\mathbf{x}]_1, \pi)$ :
$[\mathbf{z}_1]_2 := [\mathbf{z}]_2 - [\mathbf{z}_0]_2$
// Check QA-NIZK for $[\mathbf{z}_0]_2$
if $e([\overline{\mathbf{A}}]_1, \pi') = e([\mathbf{C}]_1, [\mathbf{z}_0]_2)$
  and $e([\mathbf{A}_0]_1, [\mathbf{C}]_2)$
    $= e([\mathbf{\Pi}]_1, [\mathbf{D}]_2^\top) + e([\mathbf{x}]_1, [\mathbf{z}_1]_2^\top)$
    return 1
else return 0
```

```
$\mathsf{PTGen}(1^\lambda, \mathsf{par})$ :
$\mathbf{A}, \mathbf{D} \xleftarrow{R} \mathcal{D}_k$
$\mathbf{u} \xleftarrow{R} \mathbb{Z}_p^k$
$\mathbf{K} \xleftarrow{R} \mathbb{Z}_p^{k+1\times k}$
$\mathbf{z} := \mathbf{D} \cdot \mathbf{u}$
$\mathbf{M} := \mathbf{D}$
$\mathbf{P} := \mathbf{M}^\top \mathbf{K}$
$\mathbf{C} := \mathbf{K}\overline{\mathbf{A}}$
$\mathsf{crs} := (\mathsf{par}, [\mathbf{D}]_2, [\mathbf{z}]_2, [\mathbf{P}]_2, [\overline{\mathbf{A}}]_1, [\mathbf{C}]_1)$
$\mathsf{trap} := \mathbf{u}$
return $(\mathsf{crs}, \mathsf{trap})$

$\mathsf{PSim}(\mathsf{crs}, \mathsf{trap}, [\mathbf{x}]_1)$ :
$\mathbf{v} \xleftarrow{R} \mathbb{Z}_p^k$
$\mathbf{S} \xleftarrow{R} \mathbb{Z}_p^{k\times k}$
$[\mathbf{z}_0]_2 := [\mathbf{D}]_2 \cdot \mathbf{v}$
// QA-NIZK for $[\mathbf{z}_0]_2$
$\pi_1 := \mathbf{v}^\top [\mathbf{P}]_2$
$[\mathbf{C}]_2 := \mathbf{S} \cdot [\mathbf{D}]_2^\top$
$[\mathbf{\Pi}]_1 := [\mathbf{A}_0]_1 \cdot \mathbf{S} - [\mathbf{x}]_1(\mathbf{u} - \mathbf{v})^\top$
$\pi := ([\mathbf{z}_0]_2, [\mathbf{C}]_2, [\mathbf{\Pi}]_1, \pi_1)$
return $\pi$
```

Fig. 4. NIZK argument $\Omega_{\mathbf{A_0}}$ for language $\mathcal{L}_{\mathbf{A_0}}$

Theorem 3. *The protocol in Figure 4 is a non-interactive zero-knowledge argument for the language $\mathcal{L}_{\mathbf{A}_0}$.*

Proof. We need to prove three properties, perfect completeness, composable zero-knowledge and computational soundness.

Completeness: This is easy to verify.

Zero-Knowledge: The challenger sends an MDDH challenge $([\mathbf{D}]_2, [\mathbf{z}]_2)$ to the adversary $\mathcal{B}$. Then $\mathcal{B}$ sets $\mathbf{A}_0$ itself, $\mathbf{A} \xleftarrow{R} \mathcal{D}_k$, $\mathbf{K} \xleftarrow{R} \mathbb{Z}_p^{(k+1)\times k}$ and computes $[\mathbf{P}]_2 = [\mathbf{D}^\top]_2\mathbf{K}$ and $\mathbf{C} = \mathbf{K}\overline{\mathbf{A}}$. Then $\mathcal{B}$ sends $([\mathbf{A}_0]_1, [\mathbf{z}]_2, [\mathbf{D}]_2, [\mathbf{P}]_2, [\overline{\mathbf{A}}]_1, [\mathbf{C}]_1)$ to $\mathcal{A}$ as crs. When $\mathcal{B}$ receives a real MDDH tuple, where $[\mathbf{z}]_2 = [\mathbf{D} \cdot \mathbf{u}]_2$ for some $\mathbf{u} \leftarrow \mathbb{Z}_p^k$, $\mathcal{B}$ simulates crs as PTGen. In the other case, where $[\mathbf{z}]_2 \xleftarrow{R} \mathbb{G}_2^{k+1}$, using the fact that the uniform distribution over $\mathbb{Z}_p^{k+1}$ and the uniform distribution over $\mathbb{Z}_p^{k+1}\backslash\text{span}(\mathbf{D})$ are $1/p$-statistically close distributions, since $\mathbf{D}$ is of rank k, we can conclude that $\mathcal{B}$ simulates the crs as output by PGen, within a $1/p$-statistical distance.

First, note that PPro and PSim compute the vector $[\mathbf{z}_0]_2$ in the exact same way. The algorithm PPro computes $[\mathbf{C}]_2 = \mathbf{S}\cdot[\mathbf{D}]_2^\top + \mathbf{r}\cdot[\mathbf{z}_1]_2^\top$ and $[\mathbf{\Pi}]_1 = [\mathbf{A}_0]_1\cdot\mathbf{S}$, with $\mathbf{S} \xleftarrow{R} \mathbb{Z}_p^{k\times k}$. Since the following are identically distributed:

$$\mathbf{S} \qquad \text{and} \qquad \mathbf{S} - \mathbf{r}\cdot(\mathbf{u}-\mathbf{v})^\top$$

for $\mathbf{S} \xleftarrow{R} \mathbb{Z}_p^{k\times k}$, we can re-write the commitment and proof computed by PPro as $[\mathbf{C}]_2 = \mathbf{S}\cdot[\mathbf{D}]_2^\top - \mathbf{r}\cdot(\mathbf{u}-\mathbf{v})^\top[\mathbf{D}]_2^\top + \mathbf{r}[\mathbf{z}_1]_2 = [\mathbf{S}\cdot\mathbf{D}]_2^\top$ and $[\mathbf{\Pi}]_1 = [\mathbf{A}_0]_1\cdot\mathbf{S} - [\mathbf{A}_0\mathbf{r}(\mathbf{u}-\mathbf{v})^\top]_2 = [\mathbf{A}_0\cdot\mathbf{S}]_1 - [\mathbf{x}]_1(\mathbf{u}-\mathbf{v})^\top$, which is exactly as the output of PSim.

Computational Soundness: Based on the computational soundness of the QA-NIZK, $\mathbf{z}_0$ is in the span $\mathbf{D}$. So, we have $\mathbf{z}_1 \notin \text{span}(\mathbf{D})$. This implies that there exists a $\mathbf{d}^\perp \in \mathbb{Z}_p^{k+1}$ such that $\mathbf{D}^\top\mathbf{d}^\perp = 0$, and $\mathbf{z}_1^\top\mathbf{d}^\perp = 1$. Furthermore, as the row vectors of $\mathbf{D}$ together with $\mathbf{z}_1$ form a basis of $\mathbb{Z}_p^{k+1}$, we can write $[\mathbf{C}]_2 := [\mathbf{S}\cdot\mathbf{D}^\top + \mathbf{r}\mathbf{z}_1^\top]_2$ for some $\mathbf{S} \xleftarrow{R} \mathbb{Z}_p^{k\times k}$, and $\mathbf{r} \xleftarrow{R} \mathbb{Z}_p^k$. Multiplying the verification equation by $\mathbf{d}$ thus yields $[\mathbf{A}_0\mathbf{r}]_1 = [\mathbf{x}]_1$, which proves a successful forgery outside $\mathcal{L}_{\mathbf{A_0}}$ impossible. □

5.2 Our Construction

In Figure 5 we present a SPS scheme under simple assumptions.

Theorem 4. *If $\Omega_{\mathbf{A}_0}$ is a NIZK argument system for $\mathcal{L}_{\mathbf{A}_0}$, the SPS scheme from Figure 5 is EUF-CMA secure under $\mathcal{D}_k$-KerMDH and $\mathcal{LS}_k$-LinSum assumptions. In particular, for any efficient adversary $\mathcal{A}$, which makes at most Q signing queries, there exist adversaries $\mathcal{B}$, $\mathcal{B}_1$, $\mathcal{B}_2$ and $\mathcal{B}_3$ such that:*

$$\mathbf{Adv}_{\mathsf{SPS}}^{\mathsf{EUF\text{-}CMA}}(\mathcal{A}) \leqslant \mathbf{Adv}_{\mathcal{D}_k,\mathbb{G}_2}^{\mathsf{KerMDH}}(\mathcal{B}) + \mathbf{Adv}_{\Omega_{\mathbf{A}_0}}^{\mathsf{zk}}(\mathcal{B}_1) + \mathbf{Adv}_{\mathcal{D}_k,\mathbb{G}_1}^{Q\text{-}\mathsf{MDDH}}(\mathcal{B}_2)$$
$$+\mathbf{Adv}_{\mathsf{BG}}^{\mathsf{EXP}^{core}}(\mathcal{B}_3) + \frac{Q}{p}$$

Proof. We prove the claim using a sequence of games:
Game 0: This game is the same as original game and we have:

$$\mathbf{Adv}_0 = \mathbf{Adv}_{\mathsf{SPS}}^{\mathsf{EUF\text{-}CMA}}(\mathcal{A})$$

Game 1: In this game we verify the following equations instead of the original verification equations (3) and (4).

$$[\mathbf{u}_0]_1 = [(1,\mathbf{m}^\top)]_1\mathbf{K}_0 + \boldsymbol{\rho}^\top\mathbf{K}_2$$

$$[\mathbf{u}_1]_1 = [(1,\mathbf{m}^\top)]_1\mathbf{K}_1 + \boldsymbol{\rho}^\top\mathbf{K}_3$$

- $\underline{\mathsf{BGGen}(1^\lambda)}$: Given a security parameter 1^λ, return BG.
- $\underline{\mathsf{KeyGen}(\mathsf{BG})}$: Pick $\mathbf{A} \overset{R}{\leftarrow} \mathcal{D}_k$, $\mathbf{K}_2, \mathbf{K}_3 \overset{R}{\leftarrow} \mathbb{Z}_p^{k\times(k+1)}$, and $\mathbf{K}_1, \mathbf{K}_0 \overset{R}{\leftarrow} \mathbb{Z}_p^{(\ell+1)\times(k+1)}$. Also run $\mathsf{crs} := (\mathsf{par}, [\mathbf{D}]_2, [\mathbf{z}]_2, [\mathbf{P}]_2, [\overline{\mathbf{A}}]_1, [\mathbf{C}]_1) \leftarrow \Omega_{\mathbf{A}_0}.\mathsf{PGen}(\mathsf{par}, 1^\lambda)$ with $\mathsf{par} := (\mathsf{BG}, [\mathbf{A}_0]_1)$. Return $\mathsf{sk} = (\mathbf{A}_0, \mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3)$ and $\mathsf{pk} = ([\mathbf{A}]_2, [\mathbf{K}_0\mathbf{A}]_2, [\mathbf{K}_1\mathbf{A}]_2, [\mathbf{K}_2\mathbf{A}]_2, [\mathbf{K}_3\mathbf{A}]_2, \mathsf{crs})$.
- $\underline{\mathsf{Sign}([\mathbf{m}]_1, \mathsf{sk})}$: On input a message $[\mathbf{m}]_1 \in \mathbb{G}_1^\ell$, and signing key sk, pick $\mathbf{r} \overset{R}{\leftarrow} \mathbb{Z}_p^k$, set $\boldsymbol{\rho} := [\mathbf{A}_0\mathbf{r}]_1$, compute $\pi \leftarrow \Omega_{\mathbf{A}_0}.\mathsf{Prove}(\mathsf{crs}, \boldsymbol{\rho}, \mathbf{r})$ and return signature $\sigma = ([\mathbf{u}_1]_1, [\mathbf{u}_0]_1, \boldsymbol{\rho}, \pi)$ with:
$$[\mathbf{u}_0]_1 := [(1, \mathbf{m}^\top)\mathbf{K}_0 + \boldsymbol{\rho}^\top\mathbf{K}_2]_1$$
$$[\mathbf{u}_1]_1 := [(1, \mathbf{m}^\top)\mathbf{K}_1 + \boldsymbol{\rho}^\top\mathbf{K}_3]_1$$
- $\underline{\mathsf{Verify}([\mathbf{m}]_1, \sigma_1, \mathsf{pk})}$: On input a message $[\mathbf{m}]_1 \in \mathbb{G}_1^\ell$, signature $\sigma = ([\mathbf{u}_1]_1, [\mathbf{u}_0]_1, \boldsymbol{\rho}, \pi)$ and public key pk, return 1 if $\Omega_{\mathbf{A}_0}.\mathsf{Verify}(\mathsf{crs}, \boldsymbol{\rho}, \pi) = 1$ and the following checks hold and 0 otherwise:
$$e([\mathbf{u}_0]_1, [\mathbf{A}]_2) = e([(1, \mathbf{m}^\top)]_1, [\mathbf{K}_0\mathbf{A}]_2) + e(\boldsymbol{\rho}^\top, [\mathbf{K}_2\mathbf{A}]_2) \tag{3}$$
$$e([\mathbf{u}_1]_1, [\mathbf{A}]_2) = e([(1, \mathbf{m}^\top)]_1, [\mathbf{K}_1\mathbf{A}]_2) + e(\boldsymbol{\rho}^\top, [\mathbf{K}_3\mathbf{A}]_2) \tag{4}$$

Fig. 5. Our SPS scheme.

For any signature $\sigma = ([\mathbf{u}_0]_1, [\mathbf{u}_1]_1, \boldsymbol{\rho}, \pi)$ that passes the original verification but not verification of Game 1, the values

$$[\mathbf{u}_0]_1 - [(1, \mathbf{m}^\top)]_1\mathbf{K}_0 + \boldsymbol{\rho}^\top\mathbf{K}_2$$
$$[\mathbf{u}_1]_1 - [(1, \mathbf{m}^\top)]_1\mathbf{K}_1 + \boldsymbol{\rho}^\top\mathbf{K}_3$$

are non-zero vectors in the kernel of $\mathbf{A}$. Thus if $\mathcal{A}$ outputs such a signature, we can construct an adversary $\mathcal{B}$ that breaks the $\mathcal{D}_k$-KerMDH assumption in $\mathbb{G}_2$. To do this we proceed as follows: The adversary $\mathcal{B}$ receives $(\mathsf{BG}, [\mathbf{A}]_2)$, samples all other parameters and simulates Game 1 for $\mathcal{A}$. When $\mathcal{B}$ receives the forgery from $\mathcal{A}$ as tuple $([\mathbf{u}_0]_1, [\mathbf{u}_1]_1, \boldsymbol{\rho}, \pi)$, he passes following values to its own challenger:

$$[\mathbf{u}_0]_1 - [(1, \mathbf{m}^\top)]_1\mathbf{K}_0 + \boldsymbol{\rho}^\top\mathbf{K}_2$$
$$[\mathbf{u}_1]_1 - [(1, \mathbf{m}^\top)]_1\mathbf{K}_1 + \boldsymbol{\rho}^\top\mathbf{K}_3$$

We have:
$$|\mathbf{Adv}_1 - \mathbf{Adv}_0| \leqslant \mathbf{Adv}^{\mathsf{KerMDH}}_{\mathcal{D}_k, \mathbb{G}_2}(\mathcal{B})$$

Game 2: In this game we replace $\mathbf{K}_0 := \mathbf{K}_0 + \mathbf{k}_0\mathbf{a}^\perp$ and $\mathbf{K}_1 := \mathbf{K}_1 + \mathbf{k}_0\mathbf{a}^\perp$ (in the key generation we can pick $\mathbf{k}_0 \in \mathbb{Z}_p^{(\ell+1)\times 1}$ and $\mathbf{K}_0, \mathbf{K}_1 \in \mathbb{Z}_p^{(\ell+1)\times(k+1)}$ and set $\mathbf{K}_0, \mathbf{K}_1$; we have $\mathbf{a}^\perp\mathbf{A} = 0$ for $\mathbf{a}^\perp \in \mathbb{Z}_p^{1\times(k+1)}$), and $\mathbf{K}_2 := \mathbf{K}_2 + \mathbf{x}_0\mathbf{a}^\perp$, and

$\mathbf{K}_3 := \mathbf{K}_3 + \mathbf{x}_1\mathbf{a}^\perp$ (in the key generation we can pick $\mathbf{x}_i \in \mathbb{Z}_p^k$ and $\mathbf{K}_i \in \mathbb{Z}_p^{k\times(k+1)}$). So, signatures have the following form:

$$[\mathbf{u}_0]_1 \leftarrow [(1,\mathbf{m}^\top)\mathbf{K}_0 + \boldsymbol{\rho}^\top\mathbf{K}_2]_1 + [(1,\mathbf{m}^\top)\mathbf{k}_0 + \boldsymbol{\rho}^\top\mathbf{x}_0]_1\mathbf{a}^\perp$$

$$[\mathbf{u}_1]_1 \leftarrow [(1,\mathbf{m}^\top)\mathbf{K}_1 + \boldsymbol{\rho}^\top\mathbf{K}_3]_1 + [(1,\mathbf{m}^\top)\mathbf{k}_0 + \boldsymbol{\rho}^\top\mathbf{x}_1]_1\mathbf{a}^\perp$$

and also we verify the forgery $(\mathbf{m}^*, \sigma^*)$ as:

$$[\mathbf{u}_0^*]_1 \leftarrow [(1,\mathbf{m}^*)^\top]_1\mathbf{K}_0 + \boldsymbol{\rho}^{*\top}\mathbf{K}_2 + ([(1,\mathbf{m}^*)^\top]_1\mathbf{k}_0 + \boldsymbol{\rho}^{*\top}\mathbf{x}_0)\mathbf{a}^\perp$$

$$[\mathbf{u}_1]_1 \leftarrow [(1,\mathbf{m}^*)^\top]_1\mathbf{K}_1 + \boldsymbol{\rho}^{*\top}\mathbf{K}_3 + ([(1,\mathbf{m}^*)^\top]_1\mathbf{k}_0 + \boldsymbol{\rho}^{*\top}\mathbf{x}_1)\mathbf{a}^\perp$$

We can rewrite the latter two equations as:

$$[\mathbf{u}_0^*]_1 \leftarrow [(1,\mathbf{m}^*)^\top]_1\mathbf{K}_0 + \boldsymbol{\rho}^{*\top}\mathbf{K}_2 + c_0\mathbf{a}^\perp$$

$$[\mathbf{u}_1]_1 \leftarrow [(1,\mathbf{m}^*)^\top]_1\mathbf{K}_1 + \boldsymbol{\rho}^{*\top}\mathbf{K}_3 + c_1\mathbf{a}^\perp$$

with $c_0 = ([(1,\mathbf{m}^*)^\top]_1\mathbf{k}_0 + \boldsymbol{\rho}^{*\top}\mathbf{x}_0)$ and $c_1 = ([(1,\mathbf{m}^*)^\top]_1\mathbf{k}_0 + \boldsymbol{\rho}^{*\top}\mathbf{x}_1)$. We have:

$$\mathbf{Adv}_2 = \mathbf{Adv}_1$$

Game 3: In this game, we pick $b \xleftarrow{R} \{0,1\}$, and verify all equations[11], except for the value c_{1-b}.

The view of the adversary does not change, and the transition from Game 2 to Game 3 can only increase the chance of the adversary. We have:

$$\mathbf{Adv}_2 < \mathbf{Adv}_3$$

Game 4: In this game, we use PTGen instead of PGen in the NIZK proof $\Omega_{\mathbf{A}_0}$. Because the output of PSim and PPro are identically distributed, we can argue that the CRS distribution is the only difference in these two games. This difference is justified by zero-knowledge of $\Omega_{\mathbf{A}_0}$.

$$|\mathbf{Adv}_3 - \mathbf{Adv}_4| \leqslant \mathbf{Adv}^{\mathsf{zk}}_{\Omega_{\mathbf{A}_0}}(\mathcal{B}_1)$$

Game 5: In this game, we can pick $\boldsymbol{\rho}$ randomly over $\mathbb{G}_1$ which we do under the Q-fold MDDH assumption[12]. More precisely, given a Q-fold MDDH challenge $[\mathbf{A}_0]_1$, $[\mathbf{z}_i]_1$ with $[\mathbf{z}_i]_1$ being either $[\mathbf{A}_0\mathbf{r}_i]$ or $[\boldsymbol{\zeta}_i]_1$ for random values $\mathbf{r}_i, \boldsymbol{\zeta}_i \in \mathbb{Z}_p^k$, we answer i-th query with $\boldsymbol{\rho}_i = \mathbf{z}_i$. This is possible as the proofs of $\Omega_{\mathbf{A}_0}$ are

[11] Note that we could verify the black part of $[\mathbf{u}_{1-b}]_1$, but we do not require it.

[12] Here, we have $\mathbf{A}_0 \xleftarrow{R} \mathbb{Z}_p^{k\times k}$, but one can easily show that the assumption for this $\mathbf{A}_0$ is at least as hard as MDDH for uniform distribution $\mathcal{D}_k := \mathcal{U}_k$. Actually, compared to matrices from $\mathcal{D}_k$, $\mathbf{A}_0$ only has one less row, and so any distinguisher against former can be turned to another distinguisher against MDDH assumption (the same for Q-fold MDDH).

simulated from the previous game onwards. So, for every PPT adversary $\mathcal{A}$ there exist PPT adversary $\mathcal{B}$, such that

$$|\mathbf{Adv}_4 - \mathbf{Adv}_5| \leqslant \mathbf{Adv}^{Q\text{-}\mathsf{MDDH}}_{\mathcal{D}_k,\mathbb{G}_1}(\mathcal{B}_2)$$

Game 6: In this game, we construct $[\mathbf{u}_0]_1$ and $[\mathbf{u}_1]_1$ as follows for i-th query:

$$[\mathbf{u}_0]_1 \leftarrow [(1,\mathbf{m}_i^\top)\mathbf{K}_0 + \boldsymbol{\rho}_i\mathbf{K}_2]_1 + [(1,\mathbf{m}_i^\top)\mathbf{k}_0 + \boldsymbol{\rho}_i\mathbf{x}_0 + \mathsf{F}_0(i)]_1\mathbf{a}^\perp$$

$$[\mathbf{u}_1]_1 \leftarrow [(1,\mathbf{m}_i^\top)\mathbf{K}_1 + \boldsymbol{\rho}_i\mathbf{K}_3]_1 + [(1,\mathbf{m}_i^\top)\mathbf{k}_0 + \boldsymbol{\rho}_i\mathbf{x}_1 + \mathsf{F}_1(i)]_1\mathbf{a}^\perp$$

for truly random function F_0 and F_1, where $\mathsf{F}_i : \mathbb{Z}_p \to \mathbb{Z}_p$. Now, we show that if $\mathcal{A}$ can distinguish between Game 5 and Game 6, we can construct a distinguisher $\mathcal{B}$ for the core lemma. $\mathcal{B}$ first sends the bit b to the core lemma. It receives $\mathsf{pp} = \mathsf{BG}$ from the core lemma experiment, sets his keys according to it and sends his pk to the adversary $\mathcal{A}$. Note that $\mathcal{B}$ do not need to know $[\mathbf{x}_0]_1$ and $[\mathbf{x}_1]_1$, as they will vanish in $[\mathbf{K}_2]_1\mathbf{A}$ and $[\mathbf{K}_3]_1\mathbf{A}$. To simulate the Sign oracle it uses $\mathsf{CTAG}()$ and receives $(\boldsymbol{\rho}, [w_0]_1, [w_1]_1)$. Then he constructs the signatures using these parameters as:

$$[\mathbf{u}_0]_1 \leftarrow [(1,\mathbf{m}_i^\top)\mathbf{K}_0 + \boldsymbol{\rho}_i\mathbf{K}_2]_1 + [(1,\mathbf{m}_i^\top)\mathbf{k}_0 + w_0]_1\mathbf{a}^\perp$$

$$[\mathbf{u}_1]_1 \leftarrow [(1,\mathbf{m}_i^\top)\mathbf{K}_1 + \boldsymbol{\rho}_i\mathbf{K}_3]_1 + [(1,\mathbf{m}_i^\top)\mathbf{k}_0 + w_1]_1\mathbf{a}^\perp$$

Finally, given the forgery $([\mathbf{m}^*]_1, \sigma^*)$, he derives $\mathsf{tag}^* = (\boldsymbol{\rho}^*, [w_0^*]_1, [w_1^*]_1)$ and calls $\mathsf{CVER}(\mathsf{tag}^*)$ and forwards the answer to $\mathcal{A}$.

Using the core lemma, we have:

$$|\mathbf{Adv}_6 - \mathbf{Adv}_5| \leqslant \mathbf{Adv}^{\mathsf{EXP}^{\mathrm{core}}}_{\mathsf{BG}}(\mathcal{B}_3)$$

Game 7: As shown, we mask the parts including $\mathbf{k}_0$ in the signatures, except for when the adversary set i^* as one of the previous queries, say $\hat{i}$ (ct' in the core lemma), which happens with probability $\frac{1}{Q}$ over the choice of $i^* \xleftarrow{R} [1, Q]$. So, the only leaked information about

$$[\mathbf{u}_0]_1 \leftarrow [(1,\mathbf{m}_{\hat{i}}^\top)\mathbf{K}_0 + \boldsymbol{\rho}_{\hat{i}}\mathbf{K}_2]_1 + [(1,\mathbf{m}_{\hat{i}}^\top)\mathbf{k}_0 + \boldsymbol{\rho}_{\hat{i}}\mathbf{x}_0 + \mathsf{F}_0(\hat{i})]_1\mathbf{a}^\perp$$

$$[\mathbf{u}_1]_1 \leftarrow [(1,\mathbf{m}_{\hat{i}}^\top)\mathbf{K}_1 + \boldsymbol{\rho}_{\hat{i}}\mathbf{K}_3]_1 + [(1,\mathbf{m}_{\hat{i}}^\top)\mathbf{k}_0 + \boldsymbol{\rho}_{\hat{i}}\mathbf{x}_1 + \mathsf{F}_1(\hat{i})]_1\mathbf{a}^\perp$$

is $(1,\mathbf{m}_{\hat{i}}^\top)\mathbf{k}_0$. As for a new message $\mathbf{m}^* \neq \mathbf{m}_{\hat{i}}$ the two values $(1,\mathbf{m}^{*\top})\mathbf{k}_0$ and $(1,\mathbf{m}_{\hat{i}}^\top)\mathbf{k}_0$ are linearly independent. So $\mathcal{A}$ can satisfy condition c_b only with probability of $\frac{Q}{p}$. We have:

$$\mathbf{Adv}_7 = \frac{Q}{p}$$

$\square$

Extension to a bilateral SPS scheme. So far we have considered our SPS scheme only for the case where the message $[\mathbf{m}]_1$ is a vector of elements in $\mathbb{G}_1$. However, there are applications that require schemes which are able to sign bilateral messages, i.e., from both source groups. More formally, when considering the message space $\mathcal{M} := \mathbb{G}_1^{n_1} \times \mathbb{G}_2^{n_2}$ of the SPS scheme, then we call it bilateral if both $n_1 > 0$ and $n_2 > 0$.

Now, we can obtain an SPS scheme for bilateral messages by applying the generic transformation from Kiltz, Pan and Wee [KPW15]. This transformation is based on the Even-Goldreich-Micali framework [EGM96] and the method from Abe et al. [ACD$^+$12]. In particular, to sign a message $\mathbf{m} = ([\mathbf{m}_1]_1, [\mathbf{m}_2]_2) \in \mathbb{G}_1^{n_1} \times \mathbb{G}_2^{n_2}$ it uses a one-time SPS scheme with a freshly sampled public key pk_{ot} living in $\mathbb{G}_2$ and then use an EUF-CMA secure SPS scheme to sign the message $([\mathbf{m}_2]_2, \mathsf{pk}_{ot})$. Using the two-tier SPS scheme from [KPW15] as a one-time SPS, which yields compact keys pk_{ot}, this adds additional costs of k elements from $\mathbb{G}_1$ and $k+1$ elements from $\mathbb{G}_2$ to the signature.

Relying on the SXDH assumption ($k = 1$) as used in Table 1 in Section 1, our bilateral SPS scheme additionally requires 1 element from $\mathbb{G}_1$ and 2 elements from $\mathbb{G}_2$ in the signature. This yields an overall signature size of $(7, 7) \in \mathbb{G}_1 \times \mathbb{G}_2$. We stress that the transformation in [KPW15] is tightness-preserving and so our SPS scheme for bilateral messages preserves the security loss of $\mathcal{O}(1)$.

Acknowledgments. We thank the anonymous reviewers from ASIACRYPT 2019 for their valuable feedback and for spotting a problem with the core lemma in a previous version. We also thanks Carla Ràfols for her comments on earlier versions of this work. This work was supported by the EUs Horizon 2020 ECSEL Joint Undertaking project SECREDAS under grant agreement n°783119 and by the Austrian Science Fund (FWF) and netidee SCIENCE project PROFET (grant agreement P31621-N38).

References

AAOT18. Masayuki Abe, Miguel Ambrona, Miyako Ohkubo, and Mehdi Tibouchi. Lower bounds on structure-preserving signatures for bilateral messages. In Dario Catalano and Roberto De Prisco, editors, *SCN 18*, volume 11035 of *LNCS*, pages 3–22. Springer, Heidelberg, September 2018.

ACD$^+$12. Masayuki Abe, Melissa Chase, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo. Constant-size structure-preserving signatures: Generic constructions and simple assumptions. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 4–24. Springer, Heidelberg, December 2012.

ACDD14. Masayuki Abe, Jan Camenisch, Rafael Dowsley, and Maria Dubovitskaya. On the impossibility of structure-preserving deterministic primitives. In Yehuda Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 713–738. Springer, Heidelberg, February 2014.

ACHO11. Masayuki Abe, Sherman S. M. Chow, Kristiyan Haralambiev, and Miyako Ohkubo. Double-trapdoor anonymous tags for traceable signatures. In

Javier Lopez and Gene Tsudik, editors, *ACNS 11*, volume 6715 of *LNCS*, pages 183–200. Springer, Heidelberg, June 2011.

ADK$^+$13. Masayuki Abe, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo. Tagged one-time signatures: Tight security and optimal tag size. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *PKC 2013*, volume 7778 of *LNCS*, pages 312–331. Springer, Heidelberg, February / March 2013.

AFG$^+$10. Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 209–236. Springer, Heidelberg, August 2010.

AGHO11. Masayuki Abe, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Optimal structure-preserving signatures in asymmetric bilinear groups. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 649–666. Springer, Heidelberg, August 2011.

AGO11. Masayuki Abe, Jens Groth, and Miyako Ohkubo. Separating short structure-preserving signatures from non-interactive assumptions. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 628–646. Springer, Heidelberg, December 2011.

AGOT14. Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi. Unified, minimal and selectively randomizable structure-preserving signatures. In Yehuda Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 688–712. Springer, Heidelberg, February 2014.

AHN$^+$17. Masayuki Abe, Dennis Hofheinz, Ryo Nishimaki, Miyako Ohkubo, and Jiaxin Pan. Compact structure-preserving signatures with almost tight security. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 548–580. Springer, Heidelberg, August 2017.

AHO10. Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo. Signing on elements in bilinear groups for modular protocol design. Cryptology ePrint Archive, Report 2010/133, 2010. http://eprint.iacr.org/2010/133.

AHO12. Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo. Group to group commitments do not shrink. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 301–317. Springer, Heidelberg, April 2012.

AHY15. Nuttapong Attrapadung, Goichiro Hanaoka, and Shota Yamada. A framework for identity-based encryption with almost tight security. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 521–549. Springer, Heidelberg, November / December 2015.

AJOR18. Masayuki Abe, Charanjit S. Jutla, Miyako Ohkubo, and Arnab Roy. Improved (almost) tightly-secure simulation-sound QA-NIZK with applications. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part I*, volume 11272 of *LNCS*, pages 627–656. Springer, Heidelberg, December 2018.

AKOT15. Masayuki Abe, Markulf Kohlweiss, Miyako Ohkubo, and Mehdi Tibouchi. Fully structure-preserving signatures and shrinking commitments. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 35–65. Springer, Heidelberg, April 2015.

ALP12. Nuttapong Attrapadung, Benoît Libert, and Thomas Peters. Computing on authenticated data: New privacy definitions and constructions. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 367–385. Springer, Heidelberg, December 2012.

BBS04. Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 41–55. Springer, Heidelberg, August 2004.

BC16. Olivier Blazy and Céline Chevalier. Structure-preserving smooth projective hashing. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 339–369. Springer, Heidelberg, December 2016.

BCF+11. Olivier Blazy, Sébastien Canard, Georg Fuchsbauer, Aline Gouget, Hervé Sibert, and Jacques Traoré. Achieving optimal anonymity in transferable e-cash with a judge. In Abderrahmane Nitaj and David Pointcheval, editors, *AFRICACRYPT 11*, volume 6737 of *LNCS*, pages 206–223. Springer, Heidelberg, July 2011.

BFM88. Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications (extended abstract). In *20th ACM STOC*, pages 103–112. ACM Press, May 1988.

BG90. Mihir Bellare and Shafi Goldwasser. New paradigms for digital signatures and message authentication based on non-interative zero knowledge proofs. In Gilles Brassard, editor, *CRYPTO'89*, volume 435 of *LNCS*, pages 194–211. Springer, Heidelberg, August 1990.

BHJ+15. Christoph Bader, Dennis Hofheinz, Tibor Jager, Eike Kiltz, and Yong Li. Tightly-secure authenticated key exchange. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015, Part I*, volume 9014 of *LNCS*, pages 629–658. Springer, Heidelberg, March 2015.

CCS09. Jan Camenisch, Nishanth Chandran, and Victor Shoup. A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks. In Antoine Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 351–368. Springer, Heidelberg, April 2009.

CDH12. Jan Camenisch, Maria Dubovitskaya, and Kristiyan Haralambiev. Efficient structure-preserving signature scheme from standard assumptions. In Ivan Visconti and Roberto De Prisco, editors, *SCN 12*, volume 7485 of *LNCS*, pages 76–94. Springer, Heidelberg, September 2012.

CF01. Ran Canetti and Marc Fischlin. Universally composable commitments. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 19–40. Springer, Heidelberg, August 2001.

CGW17. Jie Chen, Junqing Gong, and Jian Weng. Tightly secure IBE under constant-size master public key. In Serge Fehr, editor, *PKC 2017, Part I*, volume 10174 of *LNCS*, pages 207–231. Springer, Heidelberg, March 2017.

CHK+11. Jan Camenisch, Kristiyan Haralambiev, Markulf Kohlweiss, Jorn Lapon, and Vincent Naessens. Structure preserving CCA secure encryption and applications. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 89–106. Springer, Heidelberg, December 2011.

CKLM12. Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Sarah Meiklejohn. Malleable proof systems and applications. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 281–300. Springer, Heidelberg, April 2012.

CLY09. Julien Cathalo, Benoît Libert, and Moti Yung. Group encryption: Non-interactive realization in the standard model. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 179–196. Springer, Heidelberg, December 2009.

CS98. Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Hugo Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 13–25. Springer, Heidelberg, August 1998.

CS02. Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In Lars R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 45–64. Springer, Heidelberg, April / May 2002.

CW13. Jie Chen and Hoeteck Wee. Fully, (almost) tightly secure IBE and dual system groups. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 435–460. Springer, Heidelberg, August 2013.

DGP$^+$19. Vanesa Daza, Alonso González, Zaira Pindado, Carla Ràfols, and Javier Silva. Shorter quadratic QA-NIZK proofs. In Dongdai Lin and Kazue Sako, editors, *PKC 2019, Part I*, volume 11442 of *LNCS*, pages 314–343. Springer, Heidelberg, April 2019.

EGM96. Shimon Even, Oded Goldreich, and Silvio Micali. On-line/off-line digital signatures. *Journal of Cryptology*, 9(1):35–67, March 1996.

EHK$^+$17. Alex Escala, Gottfried Herold, Eike Kiltz, Carla Rafols, and Jorge Villar. An algebraic framework for diffie–hellman assumptions. *Journal of cryptology*, 30(1):242–288, 2017.

FG18. Georg Fuchsbauer and Romain Gay. Weakly secure equivalence-class signatures from standard assumptions. In Michel Abdalla and Ricardo Dahab, editors, *PKC 2018, Part II*, volume 10770 of *LNCS*, pages 153–183. Springer, Heidelberg, March 2018.

FHS15. Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig. Practical round-optimal blind signatures in the standard model. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 233–253. Springer, Heidelberg, August 2015.

Fis06. Marc Fischlin. Round-optimal composable blind signatures in the common reference string model. In Cynthia Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 60–77. Springer, Heidelberg, August 2006.

FLM11. Marc Fischlin, Benoît Libert, and Mark Manulis. Non-interactive and reusable universally composable string commitments with adaptive security. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 468–485. Springer, Heidelberg, December 2011.

Fuc11. Georg Fuchsbauer. Commuting signatures and verifiable encryption. In Kenneth G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 224–245. Springer, Heidelberg, May 2011.

GH08. Matthew Green and Susan Hohenberger. Universally composable adaptive oblivious transfer. In Josef Pieprzyk, editor, *ASIACRYPT 2008*, volume 5350 of *LNCS*, pages 179–197. Springer, Heidelberg, December 2008.

Gha16. Essam Ghadafi. Short structure-preserving signatures. In Kazue Sako, editor, *CT-RSA 2016*, volume 9610 of *LNCS*, pages 305–321. Springer, Heidelberg, February / March 2016.

Gha17. Essam Ghadafi. More efficient structure-preserving signatures - or: Bypassing the type-III lower bounds. In Simon N. Foley, Dieter Gollmann, and Einar Snekkenes, editors, *ESORICS 2017, Part II*, volume 10493 of *LNCS*, pages 43–61. Springer, Heidelberg, September 2017.

GHK17. Romain Gay, Dennis Hofheinz, and Lisa Kohl. Kurosawa-desmedt meets tight security. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part III*, volume 10403 of *LNCS*, pages 133–160. Springer, Heidelberg, August 2017.

GHKP18. Romain Gay, Dennis Hofheinz, Lisa Kohl, and Jiaxin Pan. More efficient (almost) tightly secure structure-preserving signatures. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part II*, volume 10821 of *LNCS*, pages 230–258. Springer, Heidelberg, April / May 2018.

GHKW16. Romain Gay, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee. Tightly CCA-secure encryption without pairings. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 1–27. Springer, Heidelberg, May 2016.

GJ18. Kristian Gjøsteen and Tibor Jager. Practical and tightly-secure digital signatures and authenticated key exchange. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 95–125. Springer, Heidelberg, August 2018.

GR16. Alonso González and Carla Ràfols. New techniques for non-interactive shuffle and range arguments. In Mark Manulis, Ahmad-Reza Sadeghi, and Steve Schneider, editors, *ACNS 16*, volume 9696 of *LNCS*, pages 427–444. Springer, Heidelberg, June 2016.

Gro06. Jens Groth. Simulation-sound NIZK proofs for a practical language and constant size group signatures. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT 2006*, volume 4284 of *LNCS*, pages 444–459. Springer, Heidelberg, December 2006.

Gro09. Jens Groth. Homomorphic trapdoor commitments to group elements. Cryptology ePrint Archive, Report 2009/007, 2009. http://eprint.iacr.org/2009/007.

Gro15. Jens Groth. Efficient fully structure-preserving signatures for large messages. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 239–259. Springer, Heidelberg, November / December 2015.

GS08. Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432. Springer, Heidelberg, April 2008.

HHK18. Julia Hesse, Dennis Hofheinz, and Lisa Kohl. On tightly secure non-interactive key exchange. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 65–94. Springer, Heidelberg, August 2018.

HJ12. Dennis Hofheinz and Tibor Jager. Tightly secure signatures and public-key encryption. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 590–607. Springer, Heidelberg, August 2012.

HJP18. Dennis Hofheinz, Dingding Jia, and Jiaxin Pan. Identity-based encryption tightly secure under chosen-ciphertext attacks. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 190–220. Springer, Heidelberg, December 2018.

HK07. Dennis Hofheinz and Eike Kiltz. Secure hybrid encryption from weakened key encapsulation. In Alfred Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 553–571. Springer, Heidelberg, August 2007.

HKS15. Dennis Hofheinz, Jessica Koch, and Christoph Striecks. Identity-based encryption with (almost) tight security in the multi-instance, multi-ciphertext setting. In Jonathan Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 799–822. Springer, Heidelberg, March / April 2015.

Hof16. Dennis Hofheinz. Algebraic partitioning: Fully compact and (almost) tightly secure cryptography. In Eyal Kushilevitz and Tal Malkin, editors, *TCC 2016-A, Part I*, volume 9562 of *LNCS*, pages 251–281. Springer, Heidelberg, January 2016.

Hof17. Dennis Hofheinz. Adaptive partitioning. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part III*, volume 10212 of *LNCS*, pages 489–518. Springer, Heidelberg, April / May 2017.

HS14. Christian Hanser and Daniel Slamanig. Structure-preserving signatures on equivalence classes and their application to anonymous credentials. In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Part I*, volume 8873 of *LNCS*, pages 491–511. Springer, Heidelberg, December 2014.

JOR18. Charanjit S. Jutla, Miyako Ohkubo, and Arnab Roy. Improved (almost) tightly-secure structure-preserving signatures. In Michel Abdalla and Ricardo Dahab, editors, *PKC 2018, Part II*, volume 10770 of *LNCS*, pages 123–152. Springer, Heidelberg, March 2018.

JR13. Charanjit S. Jutla and Arnab Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 1–20. Springer, Heidelberg, December 2013.

JR14. Charanjit S. Jutla and Arnab Roy. Switching lemma for bilinear tests and constant-size NIZK proofs for linear subspaces. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part II*, volume 8617 of *LNCS*, pages 295–312. Springer, Heidelberg, August 2014.

JR17. Charanjit S. Jutla and Arnab Roy. Improved structure preserving signatures under standard bilinear assumptions. In Serge Fehr, editor, *PKC 2017, Part II*, volume 10175 of *LNCS*, pages 183–209. Springer, Heidelberg, March 2017.

KPW15. Eike Kiltz, Jiaxin Pan, and Hoeteck Wee. Structure-preserving signatures from standard assumptions, revisited. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 275–295. Springer, Heidelberg, August 2015.

KW15. Eike Kiltz and Hoeteck Wee. Quasi-adaptive NIZK for linear subspaces revisited. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 101–128. Springer, Heidelberg, April 2015.

LPJY13. Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Linearly homomorphic structure-preserving signatures and their applications. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 289–307. Springer, Heidelberg, August 2013.

LPJY14. Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 514–532. Springer, Heidelberg, May 2014.

LPJY15. Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Compactly hiding linear spans - tightly secure constant-size simulation-sound QA-NIZK proofs and applications. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 681–707. Springer, Heidelberg, November / December 2015.

LPQ17. Benoît Libert, Thomas Peters, and Chen Qian. Structure-preserving chosen-ciphertext security with shorter verifiable ciphertexts. In Serge Fehr, editor, *PKC 2017, Part I*, volume 10174 of *LNCS*, pages 247–276. Springer, Heidelberg, March 2017.

LPY15. Benoît Libert, Thomas Peters, and Moti Yung. Short group signatures via structure-preserving signatures: Standard model security from simple assumptions. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 296–316. Springer, Heidelberg, August 2015.

MRV16. Paz Morillo, Carla Ràfols, and Jorge Luis Villar. The kernel matrix Diffie-Hellman assumption. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 729–758. Springer, Heidelberg, December 2016.

NY90. Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *22nd ACM STOC*, pages 427–437. ACM Press, May 1990.

Ràf15. Carla Ràfols. Stretching groth-sahai: NIZK proofs of partial satisfiability. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015, Part II*, volume 9015 of *LNCS*, pages 247–276. Springer, Heidelberg, March 2015.

Sah99. Amit Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In *40th FOCS*, pages 543–553. IEEE Computer Society Press, October 1999.

Sho97. Victor Shoup. Lower bounds for discrete logarithms and related problems. In Walter Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 256–266. Springer, Heidelberg, May 1997.

WZM$^+$16. Yuyu Wang, Zongyang Zhang, Takahiro Matsuda, Goichiro Hanaoka, and Keisuke Tanaka. How to obtain fully structure-preserving (automorphic) signatures from structure-preserving ones. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 465–495. Springer, Heidelberg, December 2016.

ZWC19. Tao Zhang, Huangting Wu, and Sherman S. M. Chow. Structure-preserving certificateless encryption and its application. In Mitsuru Matsui, editor, *CT-RSA 2019*, volume 11405 of *LNCS*, pages 1–22. Springer, Heidelberg, March 2019.