# Improved (Almost) Tightly-Secure Structure-Preserving Signatures

Charanjit S. Jutla[1], Miyako Ohkubo[2], and Arnab Roy[3]

[1] IBM T. J. Watson Research Center, Yorktown Heights, NY, USA
csjutla@us.ibm.com
[2] Security Fundamentals Laboratories, CSR, NICT, Japan
m.ohkubo@nict.go.jp
[3] Fujitsu Laboratories of America, Sunnyvale, CA, USA
aroy@us.fujitsu.com

**Abstract.** Structure Preserving Signatures (SPS) allow the signatures and the messages signed to be further encrypted while retaining the ability to be proven valid under zero-knowledge. In particular, SPS are tailored to have *structure* suitable for Groth-Sahai NIZK proofs. More precisely, the messages, signatures, and verification keys are required to be elements of groups that support efficient bilinear-pairings (*bilinear groups*), and the signature verification consists of just evaluating one or more bilinear-pairing product equations. Since Groth-Sahai NIZK proofs can (with zero-knowledge) prove the validity of such pairing product equations, it leads to interesting applications such as blind signatures, group signatures, traceable signatures, group encryption, and delegatable credential systems.

In this paper, we further improve on the SPS scheme of Abe, Hofheinz, Nishimaki, Ohkubo and Pan (CRYPTO 2017) while maintaining only an $O(\lambda)$-factor security reduction loss to the SXDH assumption. In particular, we compress the size of the signatures by almost 40%, and reduce the number of pairing-product equations in the verifier from fifteen to seven. Recall that structure preserving signatures are used in applications by encrypting the messages and/or the signatures, and hence these optimizations are further amplified as proving pairing-product equations in Groth-Sahai NIZK system is not frugal. While our scheme uses an important novel technique introduced by Hofheinz (EuroCrypt 2017), i.e. *structure-preserving adaptive partitioning*, our approach to building the signature scheme is different and this leads to the optimizations mentioned. Thus we make progress towards an open problem stated by Abe et al (CRYPTO 2017) to design more compact SPS-es with smaller number of group elements.

**Keywords:** Structure-preserving signatures, bilinear pairings, SXDH, Matrix-DDH, Groth-Sahai, Cramer-Shoup, QA-NIZK

## 1 Introduction

Structure-Preserving Signatures (SPS), introduced in [AFG+10], allow the signatures and the messages signed to be further encrypted while retaining the ability to be proven valid under zero-knowledge. In particular, SPS are tailored to have *structure* suitable for Groth-Sahai NIZK proofs [GS12]. More precisely, the messages, signatures, and verification keys are required to be elements of groups that support efficient bilinear-pairings (*bilinear groups*), and the signature verification consists of just evaluating one or more bilinear-pairing product equations. Since GS-NIZK proofs can (with zero-knowledge) prove the validity of such pairing product equations, it leads to interesting applications such as blind signatures [AO09,AFG+10], group signatures [AHO10], traceable signatures [ACHO11], group encryption [CLY09], and delegatable credential systems [Fuc11].

While there is a long sequence of works starting with Groth in 2006 [Gro06], and with the formalization of definition of SPS in [AFG+10], recently there have been major efficiency improvements in terms of signature size, number of pairing-product equations and verification time [KPW15,LPY15,JR17]. With the exception of [HJ12], most of these works that are based on static assumptions such as SXDH or $k$-LIN, incur a security reduction loss of factor $O(q)$ or even $O(q^2)$, where $q$ is the number of signature queries. Recently, in a remarkable work, Abe et al [AHN+17] show a SPS scheme which is quite compact and yet has only a $O(\lambda)$ factor security loss, where $\lambda$ is the security parameter[4]. The security is based on the SXDH assumption in asymmetric bilinear-pairing groups, which is essentially the decisional Diffie-Hellman (DDH) assumption in each of the two asymmetric groups.

In this work, we further improve on the SPS scheme of [AHN+17] while maintaining only a $O(\lambda)$-factor security reduction loss. In particular, we compress the size of the signatures by almost 40% of that in [AHN+17], and reduce the number of pairing-product equations in the verifier from fifteen to seven (see Table 1 for more details). Recall, structure-preserving signatures are used in applications by encrypting the messages and/or the signatures, and hence these optimizations are further amplified as proving pairing-product equations in Groth-Sahai NIZK system is not frugal. While our scheme uses an important novel technique introduced in [AHN+17], i.e. *structure-preserving adaptive partitioning*, our approach to building the signature scheme is different and this leads to the optimizations mentioned. It was mentioned as an open problem in [AHN+17] to design more compact SPSes with smaller number of group elements.

At a high level, signature schemes usually encrypt a secret and prove in zero-knowledge that such a secret is encrypted in the signature. Since we consider security under chosen-message attacks (EUF-CMA), this entails some type of simulation-soundness requirement on the zero-knowledge proof. For example, the encryption scheme may then be required to be CCA2. In the standard model,

[4] The work of [HJ12] only encountered a constant factor security loss. However, the scheme produces signatures that require hundreds of group elements.

CCA2 encryption schemes have more or less followed two paradigms: (a) The Naor-Yung paradigm [NY90] of double CPA encryption, and a simulation-sound NIZK proof that the double encryption is valid [Sah99], or (b) An augmented ElGamal Encryption (reminiscent of [Dam92]) along with a hash proof that the augmentation is valid [CS98]. However until very recently, known solutions to both these approaches have had two limitations, i.e. these schemes were inherently tag-based and hence not amenable to structure-preservation, and further they had at least $O(q)$-factor security loss in reduction to standard assumptions. In the context of signature schemes, IBEs and CCA2-encryption, a recent flurry of works [CW13,BKP14,LPJY15,AHY15,GHKW16,Hof17], starting with Chen and Wee's almost tightly-secure IBE scheme [CW13], do manage to handle the second concern but these works (except one) rely on tag-based approaches[5], and hence do not lead to (almost) tightly-secure SPS. The one exception being the recent work [AHN$^+$17] mentioned above. The work [AHN$^+$17] however does build on earlier string of works in obtaining tight-security, and in particular it enhances a technique of [Hof17], *called adaptive-partitioning*, so as to enable structure-preservation.

We now briefly discuss message-space partitioning techniques, which is used in both [AHN$^+$17] and our new SPS. Chen and Wee consider partitioning the message space (resp. identity space in IBEs) repeatedly into two sets based on a bit derived from the message or a tag. In this iterative reduction process, they adjust signatures for messages in one of the two sets so that after logarithmic number of steps (say, in the size of the tag space) all modified signatures hide the secret. The partitioning scheme is however based on the message or tag, and hence this does not lead to structure-preserving signatures. Hofheinz [Hof17] introduced "adaptive partitioning" in which the partitioning is decided dynamically based on an encrypted partitioning-bit embedded in the signature. This leads to public-keys that are constant sized (as opposed to $O(\lambda)$-sized), but the strategy is still "tag"-based, and hence not structure-preserving.

In [AHN$^+$17], simulation-soundness (for the Naor-Yung encryption paradigm) is achieved using Groth-Sahai NIZK proofs for "OR"-systems. The scheme has almost tight-security reduction due to adaptive partitioning and yet it is structure-preserving as tags (or hashes) are not used. Very concisely, the public-key contains a commitment to a bit $x$ which is initially set to zero. Each signature also contains an encryption of a bit $y$, which is set arbitrarily in the scheme (i.e. real world). The "OR" system proves that either $y == x$ or the double encryptions of the secret are consistent. Simulation-soundness is achieved by ensuring that inconsistent double encryptions are only generated in signatures where the simulator was able to ensure $y = x$. This requires an intricate sequence of reduction steps where $y^i$ (i.e. $y$ in $i$-th signature) is first set to $M^i_j$ (i.e. the $j$-bit in the message $M^i$) and $x$ is set to be the complement of a guess of $y^*$ (i.e. adver-

[5] A tag is usually either computed using a 1-1 or collision-resistant function or is chosen afresh at random. In some cases it is clear that the resulting scheme is not SPS, but there are cases of the latter variety [KPW15,LPY15,JR17] that lead to SPS, but where it is not clear if a tight reduction can be obtained or not.

sary's $y$). Since $x \neq y^*$ with probability at least half, this enforces soundness of consistency of double encryption, and the result follows by complexity leveraging. The security argument also requires enacting a strategy of "dynamically" augmenting/strengthening the language that is verified.

**Table 1.** Comparison with existing SPS schemes with table adapted from [AHN+17]. $(n_1, n_2)$ denotes $n_1$ $\mathbb{G}_1$ elements and $n_2$ $\mathbb{G}_2$ elements. The table gives message, signature and public key sizes and finally the security loss in the reduction to the listed assumption(s). For [HJ12], the parameter $d$ limits number of signing to $2^d$. The parameters $q$ and $\lambda$ represent the number of signing queries and the security parameter, respectively.

| | $\|M\|$ | $\|\sigma\|$ | $\|pk\|$ | Sec. Loss | Assumption |
|---|---|---|---|---|---|
| [HJ12] | 1 | $10d + 6$ | 13 | 8 | DLIN |
| [ACD+12] | $(n_1, 0)$ | $(7, 4)$ | $(5, n_1 + 12)$ | $O(q)$ | SXDH, XDLIN |
| [ACD+12] | $(n_1, n_2)$ | $(8, 6)$ | $(n_2 + 6, n_1 + 13$ | $O(q)$ | SXDH, XDLIN |
| [LPY15] | $(n_1, 0)$ | $(10, 1)$ | $(16, 2n_1 + 5)$ | $O(q)$ | SXDH, XDLIN |
| [KPW15] | $(n_1, n_2)$ | $(7, 3)$ | $(n_2 + 1, n_1 + 7)$ | $O(q^2)$ | SXDH |
| [KPW15] | $(n_1, 0)$ | $(6, 1)$ | $(0, n_1 + 6)$ | $O(q^2)$ | SXDH |
| [JR17] | $(n_1, 0)$ | $(5, 1)$ | $(0, n_1 + 6)$ | $O(q \log q)$ | SXDH |
| [AHN+17] | $(n_1, 0)$ | $(13, 12)$ | $(18, n_1 + 11)$ | $O(\lambda)$ | SXDH |
| [AHN+17] | $(n_1, n_2)$ | $(14, 14)$ | $(n_2 + 19, n_1 + 12)$ | $O(\lambda)$ | SXDH |
| This paper | $(n_1, 0)$ | $(11, 6)^{a\,b}$ | $(7, n_1 + 16)$ | $O(\lambda)$ | SXDH |
| This paper | $(n_1, n_2)$ | $(12, 8)$ | $(n_2 + 8, n_1 + 17)$ | $O(\lambda)$ | SXDH |

[a] Based on the optimization in Section 5.2; otherwise $(11, 7)$.
[b] The batched-pairing optimization of Sec. 5.3 has $(12, 7)$.

In our work, we advantageously use simple split-CRS[6] (quasi-adaptive) QA-NIZK for affine languages introduced in [JR13], wherein the verifier CRS does not depend on the affine component of an affine language. This greatly simplifies the security proof while also yielding smaller signatures and verification (PPE) equation sizes. In particular, we do not employ the strategy of augmenting/strengthening the language that is verified, but more or less follow the strategy of obtaining signature schemes using augmented ElGamal encryption along with hash proofs. Moreover, using the enhanced adaptive partitioning technique of [AHN+17] we are able to do this without using tags or hashes of messages and hence our scheme is structure-preserving and simultaneously (almost) tightly-secure. The strategy of obtaining SPS from split-CRS QA-NIZK for affine languages was first used in [JR17], but that scheme incurred an $O(q \log q)$-factor loss in security in reduction to the SXDH assumption. Another advantage of using the split-CRS QA-NIZK of [JR13] is that it is also true-simulation sound (i.e. it is unbounded simulation-sound when the simulator only issues proofs on

[6] In a split-CRS QA-NIZK, the CRS can be split into two parts, a prover CRS and a verifier CRS. to prove a statement only the prover CRS is required, and to verify a statement and its proof only the verifier CRS is required.

**Table 2.** Comparison of factors relevant to computational efficiency in SPS schemes with smaller signature sizes. Third column indicates the no. of scalar multiplications in $\mathbb{G}_1, \mathbb{G}_2$ for signing. Multi-scalar multiplications are counted with a weight 1.5. For [JR17] a constant pairing is included. Column "Batched" shows the no. of pairings in a verification when pairing product equations are aggregated by batch verification techniques [BFI$^+$10].

| | $\lvert M\rvert$ | #(s.mult) in signing | #(PPEs) | #(Pairings) | |
|---|---|---|---|---|---|
| | | | | Plain | Batched |
| [KPW15] | $(n_1, 0)$ | $(6, 1)$ | 3 | $n_1 + 11$ | $n_1 + 10$ |
| [JR17] | | $(6, 1)$ | 2 | $n_1 + 8$ | $n_1 + 6$ |
| [AHN$^+$17] | | $(15, 15)$ | 15 | $n_1 + 57$ | $n_1 + 16$ |
| This paper | | $(13.5, 7.5)$ | 7 | $n_1 + 33$ | $n_1 + 22$ |
| This paper, Sec. 5.3 | | $(15, 8.5)$ | 10 | $n_1 + 39$ | $n_1 + 16$ |
| [KPW15] | $(n_1, n_2)$ | $(8, 3.5)$ | 4 | $n_1 + n_2 + 15$ | $n_1 + n_2 + 14$ |
| [AHN$^+$17] | | $(17.5, 16)$ | 16 | $n_1 + n_2 + 61$ | $n_1 + n_2 + 18$ |
| This paper | | $(15, 8.5)$ | 8 | $n_1 + n_2 + 4$ | $n_1 + 24$ |
| This paper, Sec. 5.3 | | $(16.5, 9.5)$ | 11 | $n_1 + n_2 + 43$ | $n_1 + n_2 + 18$ |

true statements), and this allows us to give an SPS that does not need discrete logarithm of message (group) elements. This was required in the construction of [AHN$^+$17], and thus the final scheme required boot-strapping using a Partial One-time Signature (POS) scheme (or more complicated GS-NIZK proofs of PPEs). Moreover, while [AHN$^+$17] also use the POS for boosting an SPS for a single coordinate message to an SPS for vector messages, we directly construct our SPS for message vectors, which saves us a couple of elements in the signature. We leverage the constant size of QA-NIZKs to achieve this saving. In order to maintain $O(\lambda)$ security we first map the message vector to an $O(\lambda)$-length bit-string and then let the reduction games hop through each bit position of this bit-string.

Our scheme also utilizes Groth-Sahai NIZK proofs for "OR"-systems. In particular, we follow [AHN$^+$17] by having a commitment to bit $x$ in the public-key, and including an encryption of bit $y$ in each signature. The "OR" system now proves that either $x == y$ or the augmentation in augmented ElGamal encryption is correct. In other words, the signature contains $\rho = g^r$, $\hat{\rho} = g^{br}$, and an (ElGamal) encryption of a secret $k_0$ using randomness $r$ (and ElGamal secret key $d$). In Cramer-Shoup CCA2-encryption scheme the hash proof system proves that $\rho$ and $\hat{\rho}$ are consistent, i.e. $\hat{\rho} = \rho^b$ where $g^b$ is in the public-key. Here we prove the same using Groth-Sahai NIZK and further only as a consequent of $x \neq y$. At a high level, the security reduction works iteratively as follows (for simplicity, assume that the discrete log $m$ of each message $M$ is available to the simulator): in each round $j$, $y^i$ is set to $m^i_j$. Next $x$ is guessed to be the complement of $y^*$. With probability half the guess is correct, and then only in messages where $y^i_j == x$ the simulator uses a DDH challenge to replace $d = d_1 + b \cdot d_2$ by $d' = d_1 + b' \cdot d_2$. This of course requires soundness of $\hat{\rho}^* = (\rho^*)^b$, which would indeed hold because the guess $x$ is not equal to $y^*$, and further one can easily

switch between Groth-Sahai binding and hiding commitments as all "OR"-proofs in signed messages always remain true. The security proof requires careful use of pairwise independence to replace $k_0$ by a random function of the prefix of the message bits $m^i_{\leq j}$, but otherwise uses standard arguments.

We now briefly remark about the efficiency implications of tight-security reductions. For standard bilinear pairings groups, this point has been well argued in [AHN+17], where for instance the authors point out that the next standard level of security for pairings friendly groups from 128-bit security is 192-bits or 256-bits. Moreover, as SPS schemes are just building blocks for applications, the loss in efficiency is amplified. The authors point out that computing a pairing in the 192-bit security level is slowed by a factor of 6 to 12 as compared to those in 128-bit security levels. As shown in Table 2, with batching of pairings computations in the various pairing-product equations required for signature verification, both [AHN+17] and our new construction has only at most 2.5 factor more pairings than the most efficient [JR17] non-tight scheme. Thus, our scheme (or the [AHN+17] scheme) running at 128-bit security can verify 2.5 to 4.5 times faster than [JR17] running at 192-bit security. Moreover, our new scheme has signatures that are shorter than [AHN+17] by a factor of 2/3 (see Table 1).

## 2 Preliminaries

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

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

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

### 2.1 Quasi-Adaptive NIZK Proofs

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

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

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

For our SPS construction we will also need a property called true-simulation-soundness and an extension of QA-NIZKs called strong split-CRS QA-NIZK. We recall the definitions of these concepts below.

**Definition 1 (Strong Split-CRS QA-NIZK [JR13]).** *We call a tuple of efficient algorithms* $(\mathsf{pargen}, \mathsf{crsgen}_v, \mathsf{crsgen}_p, \mathsf{prover}, \mathsf{ver})$ *a* **strong split-CRS QA-NIZK** *proof system for an ensemble of distributions* $\{\mathcal{D}_\eta\}$ *on collection of witness-relations* $\mathcal{R}_\eta = \{R_\rho\}$ *with associated parameter language* $\mathcal{L}_{par}$ *if there exists probabilistic polynomial time simulators* $(\mathsf{crssim}_v, \mathsf{crssim}_p, \mathsf{sim})$*, such that for all non-uniform PPT adversaries* $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$*, and* $\eta \leftarrow \mathsf{pargen}(1^\lambda)$*, we have:*

**Quasi-Adaptive Completeness:**

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

**Quasi-Adaptive Soundness:**

$$\Pr\left[\begin{array}{l|c} (\mathsf{CRS}_v, st) \leftarrow \mathsf{crsgen}_v(\eta),\ \rho \leftarrow \mathcal{D}_\eta & \\ \mathsf{CRS}_p \leftarrow \mathsf{crsgen}_p(\eta, \rho, st) & \mathsf{ver}(\mathsf{CRS}_v, x, \pi) = 1 \textbf{ and} \\ (x, \pi) \leftarrow \mathcal{A}_2(\eta, \mathsf{CRS}_v, \mathsf{CRS}_p, \rho) & \textbf{not } (\exists w : R_\rho(x, w)) \end{array}\right] \approx 0$$

**Quasi-Adaptive Zero-Knowledge:**

$$\Pr\left[\begin{array}{l|l} (\mathsf{CRS}_v, st) \leftarrow \mathsf{crsgen}_v(\eta) & \\ \rho \leftarrow \mathcal{D}_\eta & \mathcal{A}_3^{\mathsf{prover}(\mathsf{CRS}_p, \cdot, \cdot)}(\eta, \mathsf{CRS}_v, \mathsf{CRS}_p, \rho) = 1 \\ \mathsf{CRS}_p \leftarrow \mathsf{crsgen}_p(\eta, \rho, st) & \end{array}\right]$$

$$\approx$$

$$\Pr\left[\begin{array}{l|l} (\mathsf{CRS}_v, \mathsf{trap}, st) \leftarrow \mathsf{crssim}_v(\eta) & \\ \rho \leftarrow \mathcal{D}_\eta & \mathcal{A}_3^{\mathsf{sim}^*(\mathsf{trap}, \cdot, \cdot)}(\eta, \mathsf{CRS}_v, \mathsf{CRS}_p, \rho) = 1 \\ \mathsf{CRS}_p \leftarrow \mathsf{crssim}_p(\eta, \rho, st) & \end{array}\right],$$

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

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

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

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

In this paper, we use a strong split-CRS QA-NIZK ($\mathsf{pargen}, \mathsf{crsgen}_v, \mathsf{crsgen}_p$, $\mathsf{prover}$, $\mathsf{ver}$) for affine linear subspace languages $\{L_{[\mathbf{M}]_1,[\mathbf{a}]_1}\}$, consisting of words of the form $[\mathbf{Mx}+\mathbf{a}]_1$, with parameters sampled from a robust and efficiently witness-samplable distribution $\mathcal{D}$ over the associated parameter language $\mathcal{L}_{\mathrm{par}}$ and with soundness under a $\mathcal{D}_k$-MDDH assumption. Robustness means that the top square matrix of $\mathbf{M}$ is full-ranked with overwhelming probability. The construction is described in [JR17], with a single element proof under the SXDH assumption.

### 2.2 Groth-Sahai NIWI Proofs

The Groth-Sahai NIWI (non-interactive witness-indistinguishable) and NIZK Proof system provides highly efficient proofs for groups with efficient bilinear pairings [GS12]. We refer the reader to the cited paper for detailed definitions, constructions and proofs. Here we give a brief overview. As usual, and in line with Section 2.1, a non-interactive proof system for a witness relation $R$ consists of four probabilistic polynomial time algorithms: $\mathsf{pargen}$, $\mathsf{crsgen}$, $\mathsf{prover}$, $\mathsf{ver}$. Groth-Sahai proof system satisfies perfect completeness and soundness. Moreover, it satisfies *composable witness indistinguishability*. This requires that there be an efficient probabilistic algorithm $\mathsf{crssim}$ such that for all non-uniform polynomial time adversaries $\mathcal{A}$ we have *CRS indistinguishability*, i.e.,

$$\begin{aligned}&\Pr\left[\eta \leftarrow \mathsf{pargen}(1^\lambda), \mathsf{crs} \leftarrow \mathsf{crsgen}(\eta) \ : \ \mathcal{A}(\mathsf{crs}) = 1\right]\\ \approx &\Pr\left[\eta \leftarrow \mathsf{pargen}(1^\lambda), \mathsf{simcrs} \leftarrow \mathsf{crssim}(\eta) \ : \ \mathcal{A}(\mathsf{simcrs}) = 1\right],\end{aligned}$$

and for all adversaries $\mathcal{A}$ we also have (perfect *witness-indistinguishability*)

$$\begin{aligned}&\Pr[\eta \leftarrow \mathsf{pargen}(1^\lambda), \mathsf{simcrs} \leftarrow \mathsf{crssim}(\eta); \ (x, w_0, w_1) \leftarrow \mathcal{A}(\mathsf{simcrs});\\ &\quad \pi \leftarrow \mathsf{prover}(\mathsf{simcrs}, x, w_0) \ : \ \mathcal{A}(\pi) = 1]\\ =&\Pr[\eta \leftarrow \mathsf{pargen}(1^\lambda), \mathsf{simcrs} \leftarrow \mathsf{crssim}(\eta); \ (x, w_0, w_1) \leftarrow \mathcal{A}(\mathsf{simcrs});\\ &\quad \pi \leftarrow \mathsf{prover}(\mathsf{simcrs}, x, w_1) \ : \ \mathcal{A}(\pi) = 1],\end{aligned}$$

where we require that both $(x, w_0)$ and $(x, w_1)$ are in $R$.

Groth-Sahai system is a commit and prove system, i.e. all free variables are first committed to, and then equations are proven w.r.t. the variables in the commitment. In other words $\mathsf{prover}$ above may have two components, one a randomized commitment algorithm and another an actual prover. An integer (or $\mathbb{Z}_q$) variable can be committed to in either group $\mathbb{G}_1$ or $\mathbb{G}_2$. These randomized commitments algorithms are denoted by $\mathrm{com}_1(\mathsf{crs}, x; r)$ or $\mathrm{com}_2(\mathsf{crs}, x; r)$. In the context of Groth-Sahai NIWI proofs, the algorithm $\mathsf{crsgen}$ is referred to as $BG$, i.e binding generator, since such $\mathsf{crs}$ lead to binding commitments. The algorithm $\mathsf{crssim}$ is referred to as $HG$, i.e. hiding generator, as such $\mathsf{simcrs}$ lead to hiding commitments.

The GS proof system is itself structure-preserving for proving satisfiability of linear multi-scalar equations and a non-linear quadratic equation. It is also

known that its CRS indistinguishability is tightly reduced to the SXDH assumption [GS12]. The maximum (absolute-value) of the difference in the two probabilities (over all efficient adversaries) will be denoted by $\mathrm{ADV}^{\mathrm{CRSIND}}$. More details about the actual commitment schemes can be found in Section 5.2. For full details the reader is referred to [GS12].

### 2.3 Public-Key Encryption Schemes

Let $\mathsf{GEN}$ be an algortihm that, on input security parameter $\lambda$, outputs $\mathsf{par}$ that includes parameters of pairing groups.

**Definition 3 (Public-key encryption).** *A Public-Key Encryption scheme (PKE) consists of proabilistic polynomial-time algorithms* $\mathsf{PKE} := (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$*:*

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

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

**Definition 4 (IND-mCPA Security [BBM00]).** *A PKE scheme* $\mathsf{PKE}$ *is* indistinguishable against multi-instance chosen-plaintext attack (IND-mCPA-secure) *if for any* $q_e \geq 0$ *and for all* PPT *adversaries* $\mathcal{A}$ *with access to oracle* $\mathcal{O}_e$ *at most* $q_e$ *times the following advantage function* $\mathsf{Adv}^{\mathsf{mcpa}}_{\mathsf{PKE}}(\mathcal{A})$ *is negligible,*

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

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

There exist public-key encryption schemes that are structure-preserving, IND-mCPA secure, and have tight reductions based on compact assumptions. Examples are ElGamal encryption [ElG84] and Linear encryption [BBS04] based on the DDH assumption and the Decision Linear assumption, respectively.

### 2.4 Structure-Preserving Signatures

**Definition 5 (Structure-Preserving Signature).** *A structure-preserving signature scheme SPS is defined as a triple of probabilistic polynomial time (PPT) algorithms* $SPS = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$*:*

- *The probabilistic key generation algorithm* $\mathsf{Gen}(par)$ *returns the public/secret key* $(pk, sk)$*, where* $pk \in \mathbb{G}^{n_{pk}}$ *for some* $n_{pk} \in poly(\lambda)$*. We assume that* $pk$ *implicitly defines a message space* $M := \mathbb{G}^n$ *for some* $n \in poly(\lambda)$*.*

– *The probabilistic signing algorithm* $\mathsf{Sign}(sk, [m])$ *returns a signature* $\sigma \in \mathbb{G}^{n_\sigma}$ *for* $n_\sigma \in poly(\lambda)$.
– *The deterministic verification algorithm* $\mathsf{Verify}(pk, [m], \sigma)$ *only consists of pairing product equations and returns 1 (accept) or 0 (reject).*

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

**Definition 6 (Existential Unforgeability against Chosen Message Attack).** *To an adversary A and scheme SPS we associate the advantage function:*

$$\mathrm{ADV}^{CMA}_{SPS}(A) := \Pr\left[\begin{array}{c}(pk, sk) \leftarrow \mathsf{Gen}(par) \\ ([m^*], \sigma^*) \leftarrow A^{SignO(\cdot)}(pk)\end{array} \;:\; \begin{array}{c}[m^*] \notin Q_{msg} \textbf{ and} \\ \mathsf{Verify}(pk, [m^*], \sigma^*) = 1\end{array}\right]$$

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

## 3 The New (Almost) Tightly-Secure SPS Scheme

The new scheme is conveniently described in Figure 1. While a brief overview of the new scheme was given in the introduction, we now describe it in more detail.

As a first step, we follow the signature scheme of [JR13] (which itself is built on Cramer-Shoup CCA2-encryption) where the split-CRS QA-NIZK for affine languages is used. The affine component is a secret $k_0$ which is only part of the prover CRS of the QA-NIZK and is not part of the verifier CRS (and hence public key of SPS). The secret $k_0$ or its group representation is encrypted using an augmented ElGamal encryption scheme. In other words, the signer picks $r$, computes $s = br$, and outputs $\rho = [r]_1$, and $\hat{\rho} = [s]_1$, where $b$ is a secret key (normally, in a Cramer-Shoup style CCA-secure encryption scheme $[b]_1$ would be part of the public key). Since, we cannot use tags (for example by hashing $\rho, \hat{\rho}$) in a structure-preserving scheme, the last component of the augmented ElGamal encryption $\gamma$ is just computed as $[k_0]_1 + d\rho + \mathbf{k} \cdot \boldsymbol{\mu}$, where $\mathbf{k}$ is another vector of secret keys of length $n$, $\boldsymbol{\mu} \in \mathbb{G}_1^n$ is a length $n$ (adversarially supplied) input message and '$\cdot$' denotes inner product.

The signer provides a QA-NIZK $\Pi_3$ that $\gamma$ and $\hat{\rho}$ are well-formed, as the language $L_3$ (see Figure 1) is an affine subspace language. However, so far the signature components constructed are malleable, as we do not use tags. To this end, the signer also encrypts a bit $z$ using another ElGamal encryption with keys $(pke, ske)$. Call the encryption $\zeta$. The bit $z$ is just set to zero. However, in addition, the signer proves using a Groth-Sahai NIWI that either $z$ is same as $x$ (where $x$ is a bit committed in the public key) or $s = br$. To this end, it also provides a Groth Sahai commitment to $br$ (i.e. $t$ in Figure 1). Since, for the Groth-Sahai proof $s$ and $t$ must also be committed using Groth-Sahai commitments (named $c_s$ and $c_t$), the signer must prove that these relate to the same $r$ in the augmented ElGamal encryption. This is achieved by proving a

QA-NIZK for the linear subspace language $L_1$ (see Fig 1). Finally, it must also be proven that the ElGamal encryption of $z$, i.e $\zeta$ is indeed that of $z$ used in the Groth-Sahai "OR" proof. This can be proven by either a Groth-Sahai proof or a QA-NIZK for language $L_2$.

Thus, the signer produces the following signature on $\boldsymbol{\mu}$:

$$(\rho, \hat{\rho}, \gamma, \zeta, c_s, c_t, c_z, \pi, \pi_1, \pi_2, \pi_3) \in \mathbb{G}_1^{11} \times \mathbb{G}_2^7$$

The verification of the signature just involves checking all the proofs, i.e. the Groth-Sahai "OR" proof $\pi$ for language $L$, and the three QA-NIZK proofs $\pi_1$, $\pi_2$, $\pi_3$ for languages $L_1, L_2, L_3$.

The (almost) tight security of this scheme is proved in the next section. The crux of the proof is in Lemmas 1 and 2. The hybrid games for these lemmas are summarized in Figures 3 and 4. Further, the main transitions in the various hybrid games in these two lemmas are depicted in Figures 5 and 6.

## 4 Security of the SPS Scheme

In this section we state and prove the security of the scheme $SPS_{\text{SXDH}}$ described in Figure 1.

**Theorem 1.** *For any efficient adversary $\mathcal{A}$, which makes at most $Q$ signature queries before attempting a forgery, its probability of success in the EUF-CMA game against the scheme $SPS_{\text{SXDH}}$ is at most*

$$\text{ADV}^{\text{TSS}}_{\Pi_3} + 12L(\text{ADV}^{\text{TSS}}_{\Pi_1} + \text{ADV}^{\text{TSS}}_{\Pi_2}) + 8L \cdot \text{ADV}_{\text{SXDH}}$$

$$+(12L+1)\text{ADV}^{\text{CRSIND}}_{\Pi} + 2L \cdot \text{ADV}^{mCPA}_{ElGamal} + \frac{6L + (q_s+1)^2 + 1}{q}$$

*Here $L$ is the least integer greater than the bit size of $q$, and $q_s$ is an upper bound on the number of signature queries issued by the adversary.*

*Remark 1.* $\text{ADV}^{\text{TSS}}_{\Pi_i}$ of a QA-NIZK $\Pi_i$ reduces to SXDH by a factor of $(n-t)$ where the (affine) linear subspace language is of dimension $t$ within a full space of dimension $n$. Also, $\text{ADV}^{\text{CRSIND}}_{\Pi}$ of a Groth-Sahai NIZK $\Pi$ reduces to SXDH by a factor of 1. Thus the overall reduction in Theorem 1 to SXDH is $O(\lambda)$.

*Proof.* We go through a sequence of Games $\mathbf{G_0}$ to $\mathbf{G_3}$ which are described below and summarized in Figure 2. In the following, $\text{Prob}_i[X]$ will denote probability of predicate X holding in probability space defined in game $\mathbf{G_i}$ and $\mathsf{WIN}_i$ will denote the winning condition for the adversary in game $\mathbf{G_i}$.

**Game $\mathbf{G_0}$**: This game exactly replicates the real construction to the adversary. So the adversary's advantage in $\mathbf{G_0}$ (defined as $\mathsf{WIN}_0$ below) is the EUF-CMA advantage we seek to bound.

$$\mathsf{WIN}_0 \stackrel{\triangle}{=} (\boldsymbol{\mu}^* \notin \mathcal{M}) \textbf{ and } \mathsf{Verify}(pk,\ \boldsymbol{\mu}^*,\ \sigma^*)$$

**Gen** $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2, n)$ :
Sample $crs$ as a Groth-Sahai NIWI BG-CRS.
Sample $(\mathsf{CRS}_p^i, \mathsf{CRS}_v^i, \mathsf{trap}_i) \leftarrow \Pi_i.\mathsf{crssim}()$ for $i = 1, 2, 3$.

Sample $r_x \leftarrow \mathbb{Z}_q$. Set $x = 1$ and $c_x = com_2(crs, x; r_x)$.
Sample $(b, k_0, d) \leftarrow \mathbb{Z}_q^3$, $\mathbf{k} \leftarrow \mathbb{Z}_q^n$ and $(pke, ske) \leftarrow ElGamal.Gen(\mathbb{G}_2)$.

Set $pk := (crs,\ \mathsf{CRS}_v^1,\ \mathsf{CRS}_v^2,\ \mathsf{CRS}_v^3,\ c_x)$.
Set $sk := (b,\ k_0,\ \mathbf{k},\ d,\ \mathsf{trap}_1,\ \mathsf{trap}_2,\ \mathsf{trap}_3,\ pke,\ r_x)$.

Return $(pk, sk)$.

**Sign** $(sk,\ \boldsymbol{\mu} \in \mathbb{G}_1^n)$:
Sample $(r, r_s, r_t, r_z) \leftarrow \mathbb{Z}_q^4$.
Set $s = t = br$, $c_s = com_1(crs, s; r_s)$ and $c_t = com_1(crs, t; r_t)$.
Let $\rho = [r]_1$, $\hat{\rho} = [s]_1$, $\gamma = \mathbf{k} \cdot \boldsymbol{\mu} + [k_0 + dr]_1$.

Set $z = 0$, $c_z = com_2(crs, z; r_z)$ and sample $\zeta \leftarrow ElGamal.Enc(pke, z)$.

Let $\pi := \Pi.\mathsf{prover}(crs,\ (c_s, c_t, c_z, c_x),\ (r_s, r_t, r_z, r_x))$.
Let $\pi_1 := \Pi_1.\mathsf{sim}(\mathsf{trap}_1,\ (\rho, c_t, \hat{\rho}, c_s))$.
Let $\pi_2 := \Pi_2.\mathsf{sim}(\mathsf{trap}_2,\ (\zeta, c_z))$.
Let $\pi_3 := \Pi_3.\mathsf{sim}(\mathsf{trap}_3,\ (\boldsymbol{\mu}, \rho, \hat{\rho}, \gamma))$.

Return $\sigma := (\rho, \hat{\rho}, \gamma, \zeta, c_s, c_t, c_z, \pi, \pi_1, \pi_2, \pi_3) \in \mathbb{G}_1^{11} \times \mathbb{G}_2^7$.

**Verify** $(pk,\ \boldsymbol{\mu},\ \sigma)$ :
Check all the NIZK proofs:
$\Pi.\mathsf{ver}(crs,\ (c_s, c_t, c_z, c_x),\ \pi)$ **and** $\Pi_1.\mathsf{ver}(\mathsf{CRS}_v^1,\ (\rho, \hat{\rho}, c_t, c_s),\ \pi_1)$ **and** $\Pi_2.\mathsf{ver}(\mathsf{CRS}_v^2,\ (\zeta, c_z),\ \pi_2)$ **and** $\Pi_3.\mathsf{ver}(\mathsf{CRS}_v^3,\ (\boldsymbol{\mu}, \rho, \hat{\rho}, \gamma),\ \pi_3)$.

**Languages:**

$\Pi$ is a GS-NIZK for $L \stackrel{\text{def}}{=} \{(c_s, c_t, c_z, c_x) \mid \exists (s, t, z, x, r_s, r_t, r_z, r_x) : (s-t)(z-x) = 0$ **and** $c_s = com_1(s; r_s)$ **and** $c_t = com_1(t; r_t)$ **and** $c_z = com_2(z; r_z)$ **and** $c_x = com_2(x; r_x)\}$.

$\Pi_1$ is a QA-NIZK for $L_1 \stackrel{\text{def}}{=} \{(\rho, c_t, \hat{\rho}, c_s) \mid \exists (r, s, r_t, r_s) : \rho = [r]_1$ **and** $c_t = com_1(br; r_t)$ **and** $\hat{\rho} = [s]_1$ **and** $c_s = com_1(s; r_s)\}$, with parameters $(b, com_1)$.

$\Pi_2$ is a QA-NIZK for $L_2 \stackrel{\text{def}}{=} \{(\zeta, c_z) \mid \exists (z, r_e, r_z) : \zeta = ElGamal.Enc(pke, [z]_2; r_e)$ **and** $c_z = com_2(z; r_z)\}$, with parameters $(com_2, pke)$.

$\Pi_3$ is a QA-NIZK for $L_3 \stackrel{\text{def}}{=} \{(\boldsymbol{\mu}, \rho, \hat{\rho}, \gamma) \mid \exists (\mathbf{m}, r) : \boldsymbol{\mu} = [\mathbf{m}]_1$ **and** $\rho = [r]_1$ **and** $\hat{\rho} = [br]_1$ **and** $\gamma = [\mathbf{k} \cdot \mathbf{m} + k_0 + dr]_1\}$, with parameters $(b, \mathbf{k}, k_0, d)$.

**Fig. 1.** Structure Preserving Signature $SPS_{\text{SXDH}}$

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

Games 0-1 $crs \leftarrow$ GS-NIWI-BG

Games 2-3 $simcrs \leftarrow$ GS-NIWI-HG

Sample $\beta \leftarrow \{0,1\},\ r_x \leftarrow \mathbb{Z}_q$

Set $x = 1$

Games 0-1 $c_x = com_2(crs, x; r_x)$

Games 2-3 $c_x = com_2(simcrs, 0; r_x)$

Sample $d \leftarrow \mathbb{Z}_q$

---

$\mathsf{Sign}(sk,\ \boldsymbol{\mu}^i \in \mathbb{G}_1^n) :$

Sample $\rho^i \leftarrow \mathbb{G}_1$.

Simulate a random function $\text{RP} : \mathbb{G}_1^n \to \{0,1\}^L$. Let $\nu^i = \text{RP}(\boldsymbol{\mu}^i)$.

Set $z^i = 0$

Games 0-1 $c_z^i = com_2(crs, z^i; r_z^i)$

Games 2-3 $c_z^i = com_2(simcrs, 0; r_z^i)$

Let $(\hat{\rho}^i, \gamma^i) :=$

Games 0-2 $\quad (b\rho^i,\ \mathbf{k} \cdot \boldsymbol{\mu}^i + [k_0]_1 + d\rho^i)$

Game 3 $\quad (b\rho^i,\ \mathbf{k} \cdot \boldsymbol{\mu}^i + [\text{RF}_L(\nu^i)]_1 + d\rho^i)$

$\cdots$

---

$\mathsf{WIN} \triangleq$

Games 0'-3 **if** $COL$ (as defined in the text) **return true; else**

$\sigma^* = (\rho^*, \hat{\rho}^*, \gamma^*, \zeta^*, c_s^*, c_t^*, c_z^*, \pi^*, \pi_1^*, \pi_2^*, \pi_3^*) :$

$(\mu^* \notin \mathcal{M})$ **and** $\mathsf{Verify}(pk,\ \mu^*,\ \sigma^*)$

Games 1-3 **and** $\gamma^* == \mathbf{k} \cdot \boldsymbol{\mu}^* + [k_0]_1 + d\rho^*$

Games 1-3 **and** $\hat{\rho}^* == b\rho^*$

**Fig. 2.** Top level games and winning conditions

**Game $\mathbf{G_0'}$**: In Game $\mathbf{G_0'}$, the challenger lazily simulates (by maintaining a table) a random function RP from $\mathbb{G}_1^n$ to $L$-bit strings. Define $COL$ to be the predicate which returns true when there is a collision, i.e., when any pair of message vectors from the set of signature queries union the adversarial response message at the end get mapped to the same output L-bit string. In this game, the adversary is allowed to win outright if $COL$ is true at the end:

$$\mathsf{WIN}_0' \triangleq \ COL \textbf{ or } ((\boldsymbol{\mu}^* \notin \mathcal{M}) \textbf{ and } \mathsf{Verify}(pk,\ \boldsymbol{\mu}^*,\ \sigma^*))$$

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

**Game $\mathbf{G_1}$**: The challenge-response in this game is the same as $\mathbf{G_0}$. The winning condition is now defined as:

$$\begin{aligned}\mathsf{WIN}_1 \triangleq\ & COL \textbf{ or} \\ & \mathsf{WIN}_0 \textbf{ and } \sigma^* = (\rho^*, \hat{\rho}^*, \gamma^*, \cdots) \text{ s.t.} \\ & (\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d\cdot\rho^*) \\ & \textbf{ and } (\hat{\rho}^* == b\rho^*)\end{aligned}$$

The difference in advantages of the adversary is upper bounded by the unbounded true-simulation-soundness of $\Pi_3$:

$$|\mathrm{Prob}_1[\mathsf{WIN}_1] - \mathrm{Prob}_0[\mathsf{WIN}_0]| \leq \mathrm{ADV}^{\mathrm{TSS}}_{\Pi_3} \tag{1}$$

**Game $\mathbf{G_2}$**: In this game, the Groth-Sahai CRS is generated as a hiding CRS, i.e., $simcrs$. Moreover, since all zero is a solution of the equation $(s-t)(z-x)=0$, by witness-indistinguishability property of Groth-Sahai under the hiding CRS, all proofs and commitments can be generated with all zero witness (i.e., $(s,t,z,x) = (0,0,0,0)$). The winning condition $\mathsf{WIN}_2$ remains the same as $\mathsf{WIN}_1$.

$$|\mathrm{Prob}_2[\mathsf{WIN}_2] - \mathrm{Prob}_1[\mathsf{WIN}_1]| \leq \mathrm{ADV}^{\mathrm{CRSIND}}_{\Pi} \tag{2}$$

**Game $\mathbf{G_3}$**: In this game, the challenger also lazily maintains a function $\mathrm{RF}_L$ mapping $L$-bit strings to $\mathbb{Z}_q$. The function $\mathrm{RF}_L$ has the property that it is a random and independent function from $L$-bit strings to $\mathbb{Z}_q$ except possibly at one value in the domain (on which the challenger has defined $\mathrm{RF}_L$) where the value of $\mathrm{RF}_L$ can be $k_0$. In $\mathbf{G_3}$, each signature component $\gamma^i$ is generated as $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_L(\mathrm{RP}(\boldsymbol{\mu^i}))]_1 + d\rho^i$, instead of $\mathbf{k}\cdot\boldsymbol{\mu^i} + [k_0]_1 + d\rho^i$. For ease of exposition, we will denote $\mathrm{RP}(\boldsymbol{\mu^i})$ as $\nu^i$. The winning condition $\mathsf{WIN}_3$ remains the same as $\mathsf{WIN}_2$.

**Lemma 1.** $|\mathrm{Prob}_3[\mathsf{WIN}_3] - \mathrm{Prob}_2[\mathsf{WIN}_2]| \leq$

$$\begin{aligned}&12L(\mathrm{ADV}^{\mathrm{TSS}}_{\Pi_1} + \mathrm{ADV}^{\mathrm{TSS}}_{\Pi_2}) + 8L\cdot\mathrm{ADV}_{\mathrm{SXDH}} \\ &+12L\cdot\mathrm{ADV}^{\mathrm{CRSIND}}_{\Pi} + 2L\cdot\mathrm{ADV}^{mCPA}_{ElGamal} + \frac{6L}{q}\end{aligned}$$

We will prove this lemma in Section 4.1. We now claim that $\text{Prob}_3[\mathsf{WIN}_3] \leq 1/q$. To prove this claim, we observe that $k_0$ is absent from the public key as well as from all the signature responses, except at most one response by property of $\text{RF}_L$ and RP and the conjunct $COL$, which ensures that no RP collision occurred. Let's say this is the $j$-th query. For all queries $i \neq j$, we observe that $RF_L(\mu^i)$ is uniformly random and independent of both $k$ and $k_0$. So all the $\gamma^i$s, for $i \neq j$, might as well be sampled independently randomly.

Coming back to the special $j$-th query, we claim that $[k_0]_1 + \mathbf{k} \cdot \boldsymbol{\mu}^*$ is uniformly random and independent of $[k_0]_1 + \mathbf{k} \cdot \boldsymbol{\mu}_j$, given that $\mu^* \neq \mu_j$. This linear algebra fact is most conveniently seen by the following information- theoretic argument: Let $\alpha \stackrel{\text{def}}{=} [k_0]_1 + \mathbf{k} \cdot \boldsymbol{\mu}_j$ and $\beta \stackrel{\text{def}}{=} [k_0]_1 + \mathbf{k} \cdot \boldsymbol{\mu}^*$. Now sample $\mathbf{k} \leftarrow \mathbb{Z}_q^n$, and $k' \leftarrow \mathbb{Z}_q$ independently and randomly. Set $k_0$ such that $[k_0]_1 = [k']_1 - \mathbf{k} \cdot \boldsymbol{\mu}_j$. Then, $k_0$ is still distributed randomly and independently. Then we have $\alpha = [k']_1$ and $\beta = [k']_1 + \mathbf{k} \cdot (\boldsymbol{\mu}^* - \boldsymbol{\mu}_j)$. Thus $\alpha$ is uniformly random and independent of $k$, while $\beta$ has an independent uniformly random distribution due to the additional term $\mathbf{k} \cdot (\boldsymbol{\mu}^* - \boldsymbol{\mu}_j)$, where $\mathbf{k}$ is uniformly random and $\boldsymbol{\mu}^* - \boldsymbol{\mu}_j$ is non-zero. Thus the probability of the adversary producing $\gamma^* - d \cdot \rho^* = \mathbf{k}\boldsymbol{\mu}^* + [k_0]_1$ is bounded in probability by $1/q$:

$$\text{Prob}_3[\mathsf{WIN}_3] \leq 1/q.$$

### 4.1 Proof of Lemma 1

To prove Lemma 1, we go through a series of $L$ games, each of which has several sub-games. We will identify $\mathbf{G_2}$ with $\mathbf{G_{2,1,0}}$ and $\mathbf{G_3}$ with $\mathbf{G_{2,L,10}}$. These games are summarized in Figure 3 with a table of transitions given in Figure 5.

In the following, we will consider various functions $\text{RF}_j$, $j \in [0..L]$. $\text{RF}_j$ maps $j$-bit length strings to $\mathbb{Z}_q$. Define $\text{RF}_0(\epsilon) = k_0$, where $\epsilon$ denotes the empty string. We will maintain the induction hypothesis (over $j \in [0..L]$) that the function $\text{RF}_j$ is a random function from its domain to its range except possibly for at most one string in the domain where its value is $k_0$. Clearly, the base case holds ($j = 0$).

**Game $\mathbf{G_{2,j,0}}$**: For all signature responses $i$, let $\nu^i|_{j-1}$ be the $(j-1)$-length prefix of $\nu^i$. We generate $\gamma^i$ as $\mathbf{k} \cdot \boldsymbol{\mu}^i + [\text{RF}_{j-1}(\nu^i|_{j-1})]_1 + d\rho^i$.

In the base case, i.e., when $j = 1$, $\mathbf{G_{2,j,0}}$ is indeed the same as $\mathbf{G_2}$ by definition of $\text{RF}_0(\epsilon)$. For the inductive case, we defer the proof of equivalence of $\mathbf{G_{2,j,0}}$ and $\mathbf{G_{2,j-1,10}}$ till the description of the latter game.

**Game $\mathbf{G_{2,j,1}}$**: We also sample $(d_1, d_2) \leftarrow \mathbb{Z}_q^2$ and substitute $d$ with $d_1 + d_2 b$, instead of sampling it from random. Consequently, we change the winning condition's $\gamma^*$-test conjunct to $\gamma^* == \mathbf{k} \cdot \boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^*$, which is same as the earlier winning condition as the winning condition also has the conjunct $\hat{\rho}^* = b\rho^*$. Also set $z^i$ to be $\nu^i_k = \text{RP}(\boldsymbol{\mu}^i)_k$, the k-th bit of output of applying the simulated random function to the query message $\boldsymbol{\mu}^i$.

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

Games (2,j,3-7) $crs \leftarrow$ GS-NIWI-BG

Games (2,j,0-2, 8-10) $simcrs \leftarrow$ GS-NIWI-HG

Sample $\beta \leftarrow \{0,1\},\ r_x \leftarrow \mathbb{Z}_q$

Games (2,j,0-2,10) Set $x = 1$

Games (2,j,3-9) Set $x = 1 - \beta$

Games (2,j,3-7) $c_x = com_2(crs, x; r_x)$

Games (2,j,0-2, 8-10) $c_x = com_2(simcrs, 0; r_x)$

Games (2,j,0, 7-10) Sample $d \leftarrow \mathbb{Z}_q$

Games (2,j,1-6) Sample $(d_1,\ d_2) \leftarrow \mathbb{Z}_q^2$

---

$\mathsf{Sign}(sk,\ \boldsymbol{\mu}^i \in \mathbb{G}_1^n)$ :

Sample $\rho^i \leftarrow \mathbb{G}_1$.

Simulate a random function $\text{RP} : \mathbb{G}_1^n \to \{0,1\}^L$. Let $\nu^i = \text{RP}(\boldsymbol{\mu}^i)$.

Game (2,j,0,10) Set $z^i = 0$

Games (2,j,1-9) Set $z^i = \nu_j^i$

Games (2,j,3-7) $c_z^i = com_2(crs, z^i; r_z^i)$

Games (2,j,0-2, 8-10) $c_z^i = com_2(simcrs, 0; r_z^i)$

Let $(\hat{\rho}^i, \gamma^i) :=$

Games (2,j,0) $(b\rho^i,\ \mathbf{k} \cdot \boldsymbol{\mu}^i + [\text{RF}_{j-1}(\nu^i|_{j-1})]_1 + d\rho^i)$

Games (2,j,1-4) $\left(b\rho^i,\ \mathbf{k} \cdot \boldsymbol{\mu}^i + [\text{RF}_{j-1}(\nu^i|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i\right)$

Games (2,j,5-6) $\left(b\rho^i,\ \mathbf{k} \cdot \boldsymbol{\mu}^i + \begin{bmatrix} \text{RF}_{j-1}(\nu^i|_{j-1}),\ \text{if } (\nu_j^i == \beta) \\ \text{RF}'_{j-1}(\nu^i|_{j-1}),\ \text{if } (\nu_j^i \neq \beta) \end{bmatrix}_1 + d_1\rho^i + d_2\hat{\rho}^i\right)$

Games (2,j,7-10) $(b\rho^i,\ \mathbf{k} \cdot \boldsymbol{\mu}^i + [\text{RF}_j(\nu^i|_j)]_1 + d\rho^i)$

$\cdots$

---

$\mathsf{WIN} \triangleq$ **if** $(COL)$ **return true; else**

Games (2,j,2-8) **if** $CheckAbort$(as defined in the text) **return false; else**

$\sigma^* = (\rho^*, \hat{\rho}^*, \gamma^*, \zeta^*, c_s^*, c_t^*, c_z^*, \pi^*, \pi_1^*, \pi_2^*, \pi_3^*)$ :

$(\mu^* \notin \mathcal{M})$ **and** $\mathsf{Verify}(pk,\ \mu^*,\ \sigma^*)$

**and**

Games (2,j,0,7-10) $\gamma^* == \mathbf{k} \cdot \boldsymbol{\mu}^* + [k_0]_1 + d\rho^*$

Games (2,j,1-6) $\gamma^* == \mathbf{k} \cdot \boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^*$

Games (2,j,0-3,6-10) **and** $\hat{\rho}^* == b\rho^*$

**Fig. 3.** Going from Game 2 to 3

Difference in advantage is the IND-mCPA security of the ElGamal encryption scheme, in switching all the $z^i$ plaintexts. Rest of the changes are information theoretic as $x$ is committed with a hiding CRS and $d$ has the same distribution.

**Game $\mathbf{G_{2,j,2}}$**: The challenger samples a bit $\beta$ randomly from $\{0,1\}$. In the winning condition we introduce a predicate called *CheckAbort* which behaves as follows: it returns true and forces the adversary to lose outright if the decryption of $\zeta^*$ is zero or one and equals $\beta$. In the case that decryption of $\zeta^*$ is not zero or one, then it still forces the adversary to lose at random with probability half. If the *CheckAbort* predicate does not force a loss for the adversary, then the rest of the winning condition remains the same as the previous game.

Since $\beta$ is information theoretically hidden from the adversary, the adversary's advantage goes down by exactly a factor of 2.

**Game $\mathbf{G_{2,j,3}}$**: The challenger sets $x = 1 - \beta$. It goes back to binding-CRS crs for $\Pi$. Thus, $z^i$ as set above is used in GS-commitment $c_z^i$ to $z^i$.

Since $s^i = t^i$ for all $i$, by Groth-Sahai witness-indistinguishability the difference in the adversary's advantage is at most $\mathrm{ADV}^{\mathrm{CRSIND}}_{\Pi}$. (Note that Groth-Sahai NIWI has perfect composable witness-indistinguishability.)

**Game $\mathbf{G_{2,j,4}}$**: The challenger removes the conjunct $\hat{\rho}^* == b\rho^*$ from the winning condition.

We first check that QA-NIZK $\Pi_1$ and $\Pi_2$ are in true-simulation mode, i.e., the simulator for these QA-NIZK is only issuing simulated proofs on true statements. For $\Pi_1$ it is indeed the case as $s = b \cdot r = t$. For $\Pi_2$ it is also true, since the GS commitment of $z^i$ is same as $z^i$ encrypted in $\zeta^i$. Now, since $\mathsf{dec}(\zeta^*) \neq x$ is in the scope of this removed conjunct, by true-simulation soundness of $\Pi_2$, $z^* \neq x$ is also in the scope of the removed conjunct. This implies by soundness of the NIWI that $s^* = t^*$. Next, by true-simulation soundness of $\Pi_1$, $\hat{\rho}^* = b\rho^*$. Thus this conjunct is indeed redundant and can be removed. The difference in advantage is at most $\mathrm{ADV}^{\mathrm{TSS}}_{\Pi_1} + \mathrm{ADV}^{\mathrm{TSS}}_{\Pi_2}$.

**Game $\mathbf{G_{2,j,5}}$**: We change the computation of $\gamma^i$ from

$$\mathbf{k} \cdot \boldsymbol{\mu}^i + [\mathrm{RF}_{j-1}(\nu^i|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$$

to

$$\mathbf{k} \cdot \boldsymbol{\mu}^i + \begin{bmatrix} \mathrm{RF}_{j-1}(\nu^i|_{j-1}), \text{ if } (\nu^i_j == \beta) \\ \mathrm{RF}'_{j-1}(\nu^i|_{j-1}), \text{ if } (\nu^i_j \neq \beta) \end{bmatrix}_1 + d_1\rho^i + d_2\hat{\rho}^i.$$

Here $\mathrm{RF}'_j$ is another independent random function from $j$-bit strings to $\mathbb{Z}_q$.

**Lemma 2.** $|\mathrm{Prob}_{2,j,4}[\mathsf{WIN}_{2,j,4}] - \mathrm{Prob}_{2,j,5}[\mathsf{WIN}_{2,j,5}]| \leq$

$$4(\mathrm{ADV}^{\mathrm{TSS}}_{\Pi_1} + \mathrm{ADV}^{\mathrm{TSS}}_{\Pi_2}) + 4 \cdot \mathrm{ADV}_{\mathrm{SXDH}} + 4 \cdot \mathrm{ADV}^{\mathrm{CRSIND}}_{\Pi} + \frac{3}{q}$$

We will prove this lemma in the next subsection using another sequence of hybrid games.

**Game $\mathbf{G_{2,j,6}}$**: We now start rolling the games back. In this game we add back the condition $\hat{\rho}^* == b\rho^*$ into the winning condition.

Since $z^* \neq x$ in the scope of this clause, the difference in advantage is $\mathrm{ADV}^{\mathrm{TSS}}_{\Pi_1} + \mathrm{ADV}^{\mathrm{TSS}}_{\Pi_2}$ due to the true-simulation soundness of the QA-NIZKs and the perfect soundness of GS-NIZK $\Pi$.

**Game $\mathbf{G_{2,j,7}}$**: Challenger (lazily) defines $\mathrm{RF}_j$ as follows:

$$\mathrm{RF}_j(\nu^i|_j) \stackrel{\mathrm{def}}{=} \begin{Bmatrix} \mathrm{RF}_{j-1}(\nu^i|_{j-1}), \text{ if } (\nu^i_j = \beta) \\ \mathrm{RF}'_{j-1}(\nu^i|_{j-1}), \text{ if } (\nu^i_j \neq \beta) \end{Bmatrix}$$

Since $\mathrm{RF}'$ is random and independent of $\mathrm{RF}$, the induction hypothesis related to $\mathrm{RF}$ continues to hold: if $\tau$ is the only $(j-1)$-bit string on which $\mathrm{RF}_{j-1}(\tau)$ equals $k_0$, then $(\tau;\beta)$ is the only $j$-bit string on which $\mathrm{RF}_j$ equals $k_0$.

The challenger also goes back to sampling $d$ from random, instead of setting it to $d_1 + bd_2$. $\gamma^i$ is now computed as $(\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_j(\nu^i|_j)]_1 + d\rho^i)$. It also changes the winning condition $\gamma^*$-conjunct to $\gamma^* == \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d\rho^*$, which holds as $\hat{\rho}^* = b\rho^*$.

Changes in this game are statistically indistinguishable from the previous and hence the advantage of the adversary remains the same.

**Game $\mathbf{G_{2,j,8}}$**: The challenger goes back to generating the hiding CRS for $\Pi$. Further, the Groth-Sahai NIWI proofs and commitments are now generated using all zero witnesses (i.e., using 0 in place of $x$ and $z^i$).

The difference in adversary's advantage is at most $\mathrm{ADV}^{\mathrm{CRSIND}}_{\Pi}$.

**Game $\mathbf{G_{2,j,9}}$**: In the winning condition, we remove the *CheckAbort* disjunct where the adversary lost outright in the previous games, i.e., if the decryption of $\zeta^*$ was 0/1 and equaled $\beta$, or with probability half if the decryption was non-0/1.

Since $\beta$ is information theoretically hidden from the adversary, the adversary's advantage goes up by exactly a factor of 2.

**Game $\mathbf{G_{2,j,10}}$**: The challenger sets $z^i = 0$, which also changes the El-Gamal encryption of $z^i$. It also sets $x$ back to 1.

The difference in adversary's advantage is the IND-mCPA security of the El-Gamal encryption scheme, in switching all the $z^i$ plaintexts. Rest of the changes are statistically indistinguishable as $x$ is committed with a hiding CRS.

We now observe that game $\mathbf{G_{2,j,10}}$ is same as $\mathbf{G_{2,j+1,0}}$ for $j < L$ and same as $\mathbf{G_3}$ for $j = L$. This concludes our proof.

### 4.2 Proof of Lemma 2

The various hybrid games to prove this lemma are depicted in Figure 4 with a table of transitions given in Figure 6.

**Game $\mathbf{H_0}$**: The game $\mathbf{H_0}$ is defined to exactly the same as game $\mathbf{G_{2,j,4}}$.

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

Games $H_{0,3-5,10-14}$ $\quad crs \leftarrow$ GS-NIWI-BG

Games $H_{1-2,6-9}$ $\quad crs \leftarrow$ GS-NIWI-HG

---

$\mathsf{Sign}(sk,\ \boldsymbol{\mu}^i \in \mathbb{G}_1) : \quad \cdots$

Let $(\hat{\rho}^i, \gamma^i) :=$

Games (2,j,4) $\quad \left(b\rho^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i\right)$

Game $H_0$ $\quad \begin{pmatrix} b\rho^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i, & \text{if } (\nu_j^i == \beta) \\ b\rho^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i, & \text{if } (\nu_j^i \neq \beta) \end{pmatrix}$

Game $H_1$ $\quad \begin{pmatrix} b\rho^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i, & \text{if } (\nu_j^i == \beta) \\ b(\rho_1^i + \rho_2^i),\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i|_{j-1})]_1 + (d_1 + d_2 b)\rho_1^i + (d_1 + d_2 b)\rho_2^i, & \text{if } (\nu_j^i \neq \beta) \end{pmatrix}$

Game $H_2, H_3$ $\quad \begin{pmatrix} b\rho^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i, & \text{if } (\nu_j^i == \beta) \\ b\rho_1^i + b'\rho_2^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i|_{j-1})]_1 + (d_1 + d_2 b)\rho_1^i + (d_1 + d_2 b')\rho_2^i, & \text{if } (\nu_j^i \neq \beta) \end{pmatrix}$

Game $H_4, H_5, H_6$ $\quad \begin{pmatrix} b\rho^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i|_{j-1})]_1 + d\rho^i, & \text{if } (\nu_j^i == \beta) \\ b\rho_1^i + b'\rho_2^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i|_{j-1})]_1 + d\rho_1^i + d'\rho_2^i, & \text{if } (\nu_j^i \neq \beta) \end{pmatrix}$

Game $H_7$ $\quad \begin{pmatrix} b\rho^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i|_{j-1})]_1 + d\rho^i, & \text{if } (\nu_j^i == \beta) \\ b\rho_1^i + b\rho_2^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i|_{j-1})]_1 + d\rho_1^i + d'\rho_2^i, & \text{if } (\nu_j^i \neq \beta) \end{pmatrix}$

Game $H_8$ $\quad \begin{pmatrix} b\rho^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i|_{j-1})]_1 + d\rho^i, & \text{if } (\nu_j^i == \beta) \\ b\rho_1^i + b\rho_2^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF'_{j-1}(\nu^i|_{j-1})]_1 + d\rho_1^i + d'\rho_2^i, & \text{if } (\nu_j^i \neq \beta) \end{pmatrix}$

Game $H_9, H_{10}$ $\quad \begin{pmatrix} b\rho^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i|_{j-1})]_1 + d\rho^i, & \text{if } (\nu_j^i == \beta) \\ b\rho_1^i + b'\rho_2^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF'_{j-1}(\nu^i|_{j-1})]_1 + d\rho_1^i + d'\rho_2^i, & \text{if } (\nu_j^i \neq \beta) \end{pmatrix}$

Game $H_{11}, H_{12}$ $\quad \begin{pmatrix} b\rho^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i, & \text{if } (\nu_j^i == \beta) \\ b\rho_1^i + b'\rho_2^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF'_{j-1}(\nu^i|_{j-1})]_1 + (d_1 + d_2 b)\rho_1^i + (d_1 + d_2 b')\rho_2^i, & \text{if } (\nu_j^i \neq \beta) \end{pmatrix}$

Game $H_{13}$ $\quad \begin{pmatrix} b\rho^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i, & \text{if } (\nu_j^i == \beta) \\ b(\rho_1^i + \rho_2^i),\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF'_{j-1}(\nu^i|_{j-1})]_1 + (d_1 + d_2 b)\rho_1^i + (d_1 + d_2 b)\rho_2^i, & \text{if } (\nu_j^i \neq \beta) \end{pmatrix}$

Game $H_{14}$ $\quad \begin{pmatrix} b\rho^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i, & \text{if } (\nu_j^i == \beta) \\ b\rho^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + [RF'_{j-1}(\nu^i|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i, & \text{if } (\nu_j^i \neq \beta) \end{pmatrix}$

Games (2,j,5) $\quad \left(b\rho^i,\ \mathbf{k}\cdot\boldsymbol{\mu}^i + \begin{bmatrix} RF_{j-1}(\nu^i|_{j-1}),\ \text{if } (\nu_j^i == \beta) \\ RF'_{j-1}(\nu^i|_{j-1}),\ \text{if } (\nu_j^i \neq \beta) \end{bmatrix}_1 + d_1\rho^i + d_2\hat{\rho}^i\right)$

$\cdots$

---

$\mathsf{WIN} \triangleq$ **if** $(COL)$ **return true; else if** $(CheckAbort)$ **return false; else**

$\sigma^* = (\rho^*, \hat{\rho}^*, \gamma^*, \zeta^*, c_s^*, c_t^*, c_z^*, \pi^*, \pi_1^*, \pi_2^*, \pi_3^*) :$

$(\boldsymbol{\mu}^* \notin \mathcal{M})$ **and** $\mathsf{Verify}(pk,\ \boldsymbol{\mu}^*,\ \sigma^*)$

**and**

Games $H_0$-$H_3$, $H_{11}$-$H_{14}$ $\quad \gamma^* == \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^*$

Games $H_4$-$H_{10}$ $\quad \gamma^* == \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d\rho^*$

Games $H_3$-$H_4$, $H_{10}$-$H_{11}$ $\quad$ **and** $\hat{\rho}^* == b\rho^*$

**Fig. 4.** Going from Game (2,j,4) to (2,j,5).

| # | $crs$ | $\beta$ | $x$ | $z^i$ | witness | $d$ | If $\nu_j^i \neq \beta$ $\gamma^i$ | If $\nu_j^i = \beta$ $\gamma^i$ | forgery check | abort | reduction |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2.j.0 | HG | - | 1 | 0 | $\hat{\rho} = b\rho$ | $d$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_{j-1}(\nu^i\|_{j-1})]_1 + d\rho^i)$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_{j-1}(\nu^i\|_{j-1})]_1 + d\rho^i)$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d\rho^* \wedge \hat{\rho}^* = b\rho^*$ | - | |
| 2.j.1 | HG | - | 1 | $\nu_j^i$ | $\hat{\rho} = b\rho$ | $(d_1, d_2)$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^*$ $\wedge \hat{\rho}^* = b\rho^*$ | - | IND-mCPA |
| 2.j.2 | HG | $\beta$ | 1 | $\nu_j^i$ | $\hat{\rho} = b\rho$ | $(d_1, d_2)$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^* \wedge \hat{\rho}^* = b\rho^*$ | $Dec(\zeta^*) = \beta$ | down by a factor of 2 |
| 2.j.3 | BG | $\beta$ | $1-\beta$ | $\nu_j^i$ | $\hat{\rho} = b\rho$ | $(d_1, d_2)$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^* \wedge \hat{\rho}^* = b\rho^*$ | $Dec(\zeta^*) = \beta$ | crsind |
| 2.j.4 | BG | $\beta$ | $1-\beta$ | $\nu_j^i$ | $x = z$ | $(d_1, d_2)$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^* \wedge$ $\square$ | $Dec(\zeta^*) = \beta$ | TSS |
| 2.j.5 | BG | $\beta$ | $1-\beta$ | $\nu_j^i$ | $x = z$ | $(d_1, d_2)$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}'_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^*$ | $Dec(\zeta^*) = \beta$ | Lemma 2 |
| 2.j.6 | BG | $\beta$ | $1-\beta$ | $\nu_j^i$ | $\hat{\rho} = b\rho$ | $(d_1, d_2)$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}'_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^* \wedge \boxed{\hat{\rho}^* = b\rho^*}$ | $Dec(\zeta^*) = \beta$ | TSS |
| 2.j.7 | BG | $\beta$ | $1-\beta$ | $\nu_j^i$ | $\hat{\rho} = b\rho$ | $d$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_j(\nu^i\|_j)]_1 + d\rho^i)$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_j(\nu^i\|_j)]_1 + d\rho^i)$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d\rho^*$ $\wedge \hat{\rho}^* = b\rho^*$ | $Dec(\zeta^*) = \beta$ | stat.ind |
| 2.j.8 | HG | $\beta$ | $1-\beta$ | $\nu_j^i$ | $\hat{\rho} = b\rho$ | $d$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_j(\nu^i\|_j)]_1 + d\rho^i)$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_j(\nu^i\|_j)]_1 + d\rho^i)$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d\rho^* \wedge \hat{\rho}^* = b\rho^*$ | $Dec(\zeta^*) = \beta$ | crsind |
| 2.j.9 | HG | $\beta$ | $1-\beta$ | $\nu_j^i$ | $\hat{\rho} = b\rho$ | $d$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_j(\nu^i\|_j)]_1 + d\rho^i)$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_j(\nu^i\|_j)]_1 + d\rho^i)$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d\rho^* \wedge \hat{\rho}^* = b\rho^*$ | $\square$ | up by a factor of 2 |
| 2.j.10 | HG | $\beta$ | 1 | 0 | $\hat{\rho} = b\rho$ | $d$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_j(\nu^i\|_j)]_1 + d\rho^i)$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_j(\nu^i\|_j)]_1 + d\rho^i)$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d\rho^* \wedge \hat{\rho}^* = b\rho^*$ | | IND-mCPA |

**Fig. 5.** Summary of the game transitions in Lemma 1.

| # | $crs$ | $\beta$ | witness | $\hat{\rho}^i$ | If $\nu_j^i \neq \beta$ $\gamma^i$ | $\hat{\rho}^i$ | If $\nu_j^i = \beta$ $\gamma^i$ | forgery check | abort | reduction |
|---|---|---|---|---|---|---|---|---|---|---|
| 2.j.4 | BG | $\beta$ | $x = z$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\mathrm{RF}_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^*$ | $Dec(\zeta^*) = \beta$ | |
| $\mathbf{H_0}$ | BG | $\beta$ | $x = z$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^*$ | $Dec(\zeta^*) = \beta$ | |
| $\mathbf{H_1}$ | HG | $\beta$ | $x = z$ | $b(\rho_1^i + \rho_2^i)$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + (d_1 + d_2 b)\rho_1^i + (d_1 + d_2 b)\rho_2^i$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^*$ | $Dec(\zeta^*) = \beta$ | crsind |
| $\mathbf{H_2}$ | HG | $\beta$ | $x = z$ | $b\rho_1^i + b'\rho_2^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + (d_1 + d_2 b)\rho_1^i + (d_1 + d_2 b')\rho_2^i$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^*$ | $Dec(\zeta^*) = \beta$ | SXDH |
| $\mathbf{H_3}$ | BG | $\beta$ | $x = z$ | $b\rho_1^i + b'\rho_2^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + (d_1 + d_2 b)\rho_1^i + (d_1 + d_2 b')\rho_2^i$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^* \wedge \hat{\rho}^* = b\rho^*$ | $Dec(\zeta^*) = \beta$ | crsind, TSS |
| $\mathbf{H_4}$ | BG | $\beta$ | $x = z$ | $b\rho_1^i + b'\rho_2^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d\rho_1^i + d'\rho_2^i$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d\rho^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d\rho^* \wedge \hat{\rho}^* = b\rho^*$ | $Dec(\zeta^*) = \beta$ | stat.ind |
| $\mathbf{H_5}$ | BG | $\beta$ | $x = z$ | $b\rho_1^i + b'\rho_2^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d\rho_1^i + d'\rho_2^i$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d\rho^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d\rho^* \wedge$ _____ | $Dec(\zeta^*) = \beta$ | TSS |
| $\mathbf{H_6}$ | HG | $\beta$ | $x = z$ | $b\rho_1^i + b'\rho_2^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d\rho_1^i + d'\rho_2^i$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d\rho^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d\rho^*$ | $Dec(\zeta^*) = \beta$ | crsind |
| $\mathbf{H_7}$ | HG | $\beta$ | $x = z$ | $b\rho_1^i + b\rho_2^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d\rho_1^i + d'\rho_2^i$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d\rho^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d\rho^*$ | $Dec(\zeta^*) = \beta$ | SXDH |
| $\mathbf{H_8}$ | HG | $\beta$ | $x = z$ | $b\rho_1^i + \overline{b\rho_2^i}$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF'_{j-1}(\nu^i\|_{j-1})]_1 + d\rho_1^i + d'\rho_2^i$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d\rho^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d\rho^*$ | $Dec(\zeta^*) = \beta$ | stat.ind |
| $\mathbf{H_9}$ | HG | $\beta$ | $x = z$ | $b\rho_1^i + \overline{b'\rho_2^i}$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [\overline{RF'_{j-1}(\nu^i\|_{j-1})}]_1 + d\rho_1^i + d'\rho_2^i$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d\rho^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d\rho^*$ | $Dec(\zeta^*) = \beta$ | SXDH |
| $\mathbf{H_{10}}$ | BG | $\beta$ | $x = z$ | $b\rho_1^i + \overline{b'\rho_2^i}$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF'_{j-1}(\nu^i\|_{j-1})]_1 + d\rho_1^i + d'\rho_2^i$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d\rho^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d\rho^* \wedge \hat{\rho}^* = b\rho^*$ | $Dec(\zeta^*) = \beta$ | crsind, TSS |
| $\mathbf{H_{11}}$ | BG | $\beta$ | $x = z$ | $b\rho_1^i + b'\rho_2^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF'_{j-1}(\nu^i\|_{j-1})]_1 + (d_1 + d_2 b)\rho_1^i + (d_1 + d_2 b')\rho_2^i$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + \underline{d_1\rho^i + d_2\hat{\rho}^i}$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^* \wedge \hat{\rho}^* = b\rho^*$ | $Dec(\zeta^*) = \beta$ | stat.ind |
| $\mathbf{H_{12}}$ | BG | $\beta$ | $x = z$ | $b\rho_1^i + b'\rho_2^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF'_{j-1}(\nu^i\|_{j-1})]_1 + (d_1 + d_2 b)\rho_1^i + (d_1 + d_2 b')\rho_2^i$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^* \wedge$ _____ | $Dec(\zeta^*) = \beta$ | TSS |
| $\mathbf{H_{13}}$ | BG | $\beta$ | $x = z$ | $\underline{b(\rho_1^i + \rho_2^i)}$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF'_{j-1}(\nu^i\|_{j-1})]_1 + (d_1 + d_2 b)\rho_1^i + \underline{(d_1 + d_2 b)\rho_2^i}$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^*$ | $Dec(\zeta^*) = \beta$ | SXDH |
| $\mathbf{H_{14}}$ | BG | $\beta$ | $x = z$ | $\underline{b\rho_1^i}$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF'_{j-1}(\nu^i\|_{j-1})]_1 + \underline{d_1\rho^i + d_2\hat{\rho}^i}$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^*$ | $Dec(\zeta^*) = \beta$ | WI |
| 2.j.5 | BG | $\beta$ | $x = z$ | $\overline{b\rho_1^i}$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF'_{j-1}(\nu^i\|_{j-1})]_1 + \overline{d_1\rho^i + d_2\hat{\rho}^i}$ | $b\rho^i$ | $\mathbf{k}\cdot\boldsymbol{\mu}^i + [RF_{j-1}(\nu^i\|_{j-1})]_1 + d_1\rho^i + d_2\hat{\rho}^i$ | $\gamma^* = \mathbf{k}\cdot\boldsymbol{\mu}^* + [k_0]_1 + d_1\rho^* + d_2\hat{\rho}^*$ | $Dec(\zeta^*) = \beta$ | |

**Fig. 6.** Summary of the game transitions in Lemma 2.

**Game $\mathbf{H_1}$**: In this game, the challenger generates the Groth-Sahai NIWI-CRS as simcrs, i.e., using the simulator CRS generator. Further, for each query $i$, if $\nu_j^i$ is not equal to $\beta$, then instead of just picking $r^i$, the challenger picks $r_1^i$ and $r_2^i$ at random, and sets $\rho^i = \rho_1^i + \rho_2^i = [r_1^i + r_2^i]_1$. Similarly, it sets $s^i = t^i = b(r_1^i + r_2^i)$, and thus $\hat{\rho}^i = b[r_1^i + r_2^i]_1$ and a similar change in the generation of $\gamma^i$. Finally, in generating the Groth-Sahai commitments and proof $\Pi$, the challenger uses all zero witnesses.

By the witness-indistinguishability property of GS-NIWI, and since rest of the game is statistically the same as the previous game, the adversary's advantage of winning is at most $\mathrm{ADV}_{\Pi}^{\mathrm{CRSIND}}$.

**Game $\mathbf{H_2}$**: In this game, the adversary also picks a $b'$ randomly and independently from $\mathbb{Z}_q$. Next, for each query $i$, if $\nu_j^i$ is not equal to $\beta$, then the challenger picks $r_1^i$ and $r_2^i$ at random, and sets $\rho^i = [r_1^i + r_2^i]_1$. It sets $s^i = br_1^i + b'r_2^i$, $t^i = b(r_1^i + r_2^i)$. It sets $\hat{\rho}^i = b[r_1^i]_1 + b'[r_2^i]_1$ and a similar change in generation of $\gamma^i$ (see Figure 4).

We now prove that the absolute value of the difference of the advantage in adversary's winning probability in $\mathbf{H_2}$ and $\mathbf{H_1}$ is at most the maximum advantage of winning in an SXDH game. In other words,

$$|\mathrm{Prob}_{\mathbf{H_2}}(\mathsf{WIN}_{\mathbf{H_2}}) - \mathrm{Prob}_{\mathbf{H_1}}(\mathsf{WIN}_{\mathbf{H_1}})| \leq \mathrm{ADV}_{\mathrm{SXDH}}.$$

To this end, for each Adversary $\mathcal{A}$ playing against the challenger in games $\mathbf{H_1}$ and $\mathbf{H_2}$, we will build another adversary $\mathcal{B}$ that plays against the SXDH challenge. Say, the adversary $\mathcal{B}$ receives an SXDH challenge $(\mathbf{g}, \mathbf{x}, \mathbf{y}, \mathbf{w})$, all elements in $\mathbb{G}_1$, where either $\mathbf{w}$ is a real DDH element, i.e., $\mathbf{w} = (\log_{\mathbf{g}} \mathbf{x})(\log_{\mathbf{g}} \mathbf{y})\mathbf{g}$ or $\mathbf{w}$ is a fake DDH element, i.e., is random and independent of the other three elements.

Adversary $\mathcal{B}$ next emulates the challenger $\mathcal{C}$ against $\mathcal{A}$ as follows. It starts emulating $\mathcal{C}$ by letting the first element of the challenge being the group generator for $\mathbb{G}_1$. Next, it emulates rest of $\mathcal{C}$ perfectly, except for queries $i$ where $\nu_j^i$ is not equal to $\beta$. In this case, it picks $r_1^i$ and $r_2^i$ at random, and sets $\rho^i = r_1^i\mathbf{g} + r_2^i\mathbf{x}$. It sets $\hat{\rho}^i = r_1^i\mathbf{y} + r_2^i\mathbf{w}$. It does not need to set $s^i$ and $t^i$, as these quantities are only needed in GS commitments and proof, but in game $\mathbf{H_1}$ we switched to all zero witnesses. The quantity $\gamma^i$ is also generated using the just defined $\rho^i$ and $\hat{\rho}^i$ (as well as $d_1$ and $d_2$). Also, the CRS of the QA-NIZK $\Pi_1$ which includes $b$ in its language parameter, can also be simulated using the group element $\mathbf{x}$ only.

Now, it is easy to check that if the SXDH challenge was real, then $\mathcal{B}$ emulated game $\mathbf{H_1}$ to $\mathcal{A}$, and if the SXDH challenge was fake, then $\mathcal{B}$ emulated $\mathbf{H_2}$ to $\mathcal{A}$. This proves the claim above.

**Game $\mathbf{H_3}$**: In this game, the Challenger goes back to generating the GS-NIWI CRS as crs, i.e., using the binding CRS generator. It also generates all GS-commitments and proofs using real witnesses, i.e., $s^i$, $t^i$, $z^i$ and $x$. it also reintroduces the conjunct $\hat{\rho}^* == b\rho^*$ in the winning condition.

We now show that the adversary's advantage in winning in $\mathbf{H_3}$ is different from its advantage in winning in game $\mathbf{H_2}$ by

$$\mathrm{ADV}_{\Pi_1}^{\mathrm{TSS}} + \mathrm{ADV}_{\Pi_2}^{\mathrm{TSS}} + \mathrm{ADV}_{\Pi}^{\mathrm{CRSIND}}.$$

We first prove that the real witnesses , i.e., $s^i$, $t^i$, $z^i$ and $x$ satisfy the equation $(s-t)(z-x) == 0$. Indeed, if $z^i_j = \nu^i_j$ is equal to $\beta = 1 - x$, i.e., $z^i_j \neq x$, then the challenger generated $s^i = t^i$, thus the quadratic equation holds. On the other hand, $z^i_j = x$, in which case also the quadratic equation holds. Thus, by witness-indistinguishability, the adversary's advantage in distinguishing between the two games is at most $\mathrm{ADV}^{\mathrm{CRSIND}}_{\Pi}$.

Next, we prove that the other conjuncts in the winning condition already imply $\hat{\rho}^* == b\rho^*$. To ascertain this, we must first check that the QA-NIZK $\Pi_1$ and $\Pi_2$ are in true-simulation mode. For cases such that $\nu^i_j$ is equal to $\beta$, this is true as $t^i = s^i$. In the other cases, note that challenger sets $\hat{\rho}^i = b[r^i_1]_1 + b'[r^i_2]_1 = [s^i]_1$. Also $t^i = b(r^i)$, where $r^i = r^i_1 + r^i_2$, and $\rho^i = [r^i]_1$. Thus, the two QA-NIZK are indeed in true-simulation mode. Then, by the true-simulation soundness of these two, and the perfect soundness of the Groth-Sahai NIWI it follows that $\hat{\rho}^* == b\rho^*$ is implied by the other conjuncts in the winning condition: since $\mathsf{dec}(\zeta^*) \neq x$ holds by true-simulation soundness of $\Pi_2$, $z^* \neq x$ also holds. This implies by soundness of the NIWI that $s^* = t^*$. Next, by true-simulation soundness of $\Pi_1$, $\hat{\rho}^* = b\rho^*$. This completes the proof of the claim.

**Game $\mathbf{H_4}$**: In this game, instead of pikcing $d_1$ and $d_2$ at random, the challenger picks $d, d'$ uniformly and randomly. Note $d, d'$ are independent of $b$ and $b'$. The challenger changes the $\gamma^*$-test conjunct in the winning condition by replacing $d_1\rho^* + d_2\hat{\rho}^*$ by $d\rho^*$. Further, in each signature query output it modifies the computation of $\gamma^i$ as follows: if $\nu^i_j == \beta$ then $d_1\rho^i + d_2\hat{\rho}^i$ is replaced by $d\rho^i$. Otherwise, it replaces $(d_1 + d_2 b)\rho^i_1 + (d_1 + d_2 b')\rho^i_2$ by $(d)\rho^i_1 + (d')\rho^i_2$, where $\rho^i_1 = [r^i_1]_1$ and $\rho^i_2 = [r^i_2]_1$.

First note that since $\hat{\rho}^* = b\rho^*$ is a conjunct in the winning condition, replacing $d_1\rho^* + d_2\hat{\rho}^*$ by $d\rho^*$ is equivalent if $d_1 + bd_2$ is replaced by $d$. It is easy to see (by pairwise independence) that the adversary's view in the two games $\mathbf{H_3}$ and $\mathbf{H_4}$ is statistically indistinguishable, except if $b = b'$ which happens with probability at most $1/q$.

**Game $\mathbf{H_5}$**: In this game the challenger again removes the conjunct $\hat{\rho}^* = b\rho^*$ from the winning condition.

We again, first check that the QA-NIZK $\Pi_1$ and $\Pi_2$ are in true-simulation mode. This is indeed the case, as the only change from game $\mathbf{H_3}$ to $\mathbf{H_4}$ was in $\gamma^i$ computation which is not used in $\Pi_1$ and $\Pi_2$. Then by the same argument as given in $\mathbf{H_3}$ indistinguishability from $\mathbf{H_2}$, the adversary's advantage is different from advantage in game $\mathbf{H_4}$ by at most $\mathrm{ADV}^{\mathrm{TSS}}_{\Pi_1} + \mathrm{ADV}^{\mathrm{TSS}}_{\Pi_2}$.

**Game $\mathbf{H_6}$**: In this game the challenger again generates the GS-NIWI CRS as simcrs, i.e., using the hinding CRS generator. Further, all GS commitments and proofs use the all zero witnesses.

The adversary's advantage in game $\mathbf{H_6}$ is different from its advantage in $\mathbf{H_5}$ by at most $\mathrm{ADV}^{\mathrm{CRSIND}}_{\Pi}$.

**Game $\mathbf{H_7}$**: In this game, the adversary need not pick $b'$. Next, for each query $i$, if $\nu^i_j$ is not equal to $\beta$, then the challenger picks $r^i_1$ and $r^i_2$ at random, and sets

$\rho^i = [r_1^i + r_2^i]_1$. It sets $s^i = t^i = b(r_1^i + r_2^i)$, Note $s^i$ and $t^i$ are not used in the GS commitments or proof. It sets $\hat{\rho}^i = b[r_1^i]_1 + b[r_2^i]_1$. There is no change in the generation of $\gamma^i$ as it uses $d$ and $d'$.

By a reduction argument similar to that given for games $\mathbf{H_1}$ and $\mathbf{H_2}$, the adversary's advantage in distinguishing between $\mathbf{H_6}$ and $\mathbf{H_7}$ is at most $\mathrm{ADV}_{\mathrm{SXDH}}$.

**Game $\mathbf{H_8}$**: In this game the Challenger lazily defines another random and independent function $\mathrm{RF}'_{j-1}$ from $(j-1)$-bit strings to $\mathbb{Z}_q$. Then, for all $i$ such that $\nu_j^i$ is not equal to $\beta$, it replaces in the computation of $\gamma^i$, the function $\mathrm{RF}_{j-1}$ by $\mathrm{RF}'_{j-1}$.

Since in each query $i$, $r_1^i$ and $r_2^i$ are chosen afresh randomly and independently, and since all other terms (i.e., other that $\gamma^i$) use one linear combination of $r_1^i$ and $r_2^i$, namely $r_1^i + r_2^i$, and $\gamma^i$ uses a different linear combination, namely $dr_1^i + d'r_2^i$, then conditioned on $d \neq d'$, the transcripts in games $\mathbf{H_7}$ and $\mathbf{H_8}$ are statistically identical. The probability of $d = d'$ is just $1/q$, and hence that is the statistical distance between the distributions of the transcripts in $\mathbf{H_7}$ and $\mathbf{H_8}$. Thus, this is also an upper bound on the difference in adversary's advantage in the two games.

**Game $\mathbf{H_9}$**: In this game, the adversary also picks a $b'$ randomly and independently from $\mathbb{Z}_q$. Next, for each query $i$, if $\nu_j^i$ is not equal to $\beta$, then the challenger picks $r_1^i$ and $r_2^i$ at random, and sets $\rho^i = [r_1^i + r_2^i]_1$. It sets $s^i = br_1^i + b'r_2^i$, $t^i = b(r_1^i + r_2^i)$. Note $s^i$ and $t^i$ are not used in the GS commitments or proof. It sets $\hat{\rho}^i = b[r_1^i]_1 + b'[r_2^i]_1$. There is no change in generation of $\gamma^i$ (see Figure 4).

Again, by a similar reduction argument to SXDH assumption, the difference in adversary's advantage in games $\mathbf{H_9}$ and $\mathbf{H_8}$ is at most $\mathrm{ADV}_{\mathrm{SXDH}}$.

**Game $\mathbf{H_{10}}$**: In this game, the challenger generates the GS-NIWI CRS as crs, i.e., using the binding CRS generator. It also uses the real witnesses, i.e $s^i, t^i$, $x$ and $z^i$ in generating the GS commitments and proof. In this game, the challenger also re-introduces the conjunct $\hat{\rho}^* == b\rho^*$.

First note that the witnesses $s^i, t^i, z^i, x$ do satisfy the quadratic equation for all queries $i$, by an argument similiar to that given for games $\mathbf{H_3}$ and $\mathbf{H_2}$. Then by repeating the argument there, we also conclude that $\hat{\rho}^* == b\rho^*$ is implied by other conjuncts. Thus, the difference in adversary's advantage is at most

$$\mathrm{ADV}^{\mathrm{TSS}}_{\Pi_1} + \mathrm{ADV}^{\mathrm{TSS}}_{\Pi_2} + \mathrm{ADV}^{\mathrm{CRSIND}}_{\Pi}.$$

**Game $\mathbf{H_{11}}$**: In this game, the challenger picks $d_1, d_2$ randomly and independently (instead of picking $d, d'$) and setting $d = d_1 + bd_2$ and $d' = d_1 + b'd_2$. The challenger also changes the $\gamma^*$-test in the winning condition by replacing $d\rho^*$ by $d_1\rho^* + d_2\hat{\rho}^*$. Further, similar changes are made in the computation of $\gamma^i$ (see Figure 4).

With the conjunct $\hat{\rho}^* == b\rho^*$ in place in the winning condition, the new winning condition is equivalent to the previous winning condition. Moreover, conditioned on $b \neq b'$, the distribution of $d$ and $d'$ remains same as in game $\mathbf{H_{10}}$. Thus, the difference in adversary's advantage is at most $1/q$.

**Game $\mathbf{H_{12}}$**: In this game, the challenger drops the conjunct $\hat{\rho}^* == b\rho^*$ from the winning condition.

Again, by arguments similar to that given for games $\mathbf{H_2}$ and $\mathbf{H_3}$ the difference in adversary's advantage is at most $\mathrm{ADV}^{\mathrm{TSS}}_{\Pi_1} + \mathrm{ADV}^{\mathrm{TSS}}_{\Pi_2}$.

**Game $\mathbf{H_{13}}$**: In this game the challenger does not pick $b'$. The challenger picks $r_1^i$ and $r_2^i$ at random, and sets $\rho^i = [r_1^i + r_2^i]_1$. Similarly, it sets $s^i = t^i = b(r_1^i + r_2^i)$, and thus $\hat{\rho}^i = b[r_1^i + r_2^i]_1$ and a similar change in generation of $\gamma^i$ (see Figure 4).

This is essentially the rewind of going from game $\mathbf{H_1}$ to $\mathbf{H_2}$. Hence, by a similar argument, the difference in adversary's advantage in games $\mathbf{H_{13}}$ and $\mathbf{H_{12}}$ is at most $\mathrm{ADV}_{\mathrm{SXDH}}$.

**Game $\mathbf{H_{14}}$**: In this game, even for $i$ such that $\nu_j^i$ is not equal to $\beta$, the challenger just picks $r^i$, and defines $\rho^i = [r^i]_1$, $s^i = t^i = br^i$, and $\hat{\rho}^i = [s^i]_1$.

There is no statistical difference in the two games $\mathbf{H_{14}}$ and $\mathbf{H_{13}}$. Now, note that game $\mathbf{H_{14}}$ is identical to game $\mathbf{G_{2,j,5}}$. This completes the proof.

## 5 Extensions and Optimizations

We begin this section by extending our construction to messages with elements in both groups. We then describe an optimization which reduces one group element from the ElGamal encryption of $z$. Next, we describe another optimization that moves some of the QA-NIZK proofs to Groth-Sahai proofs. While this may lead to slightly larger signature sizes, it reduces the size of the public-key and consequently may benefit in batching the various pairings in the verification step.

### 5.1 Bilateral Message Vectors

We use the same technique employed by [AHN+17] to extend our SPS to sign bilateral messages, i.e., messages $(\boldsymbol{\mu_1}, \boldsymbol{\mu_2})$ in $\mathbb{G}_1^{n_1} \times \mathbb{G}_2^{n_2}$. Essentially, we sign $\boldsymbol{\mu_2}$ using a Partial One-Time signature scheme (POS) [BS07] of Abe et al [ACD+16] which has a one-time public key $opk$ consisting of one element of $\mathbb{G}_1$ and one-time signature $osig$ consisting of 2 elements of $\mathbb{G}_2$. The public key $opk$ is appended to the message vector $\boldsymbol{\mu}_1$ making it $(n_1 + 1)$-elements long. Then $SPS_{\mathrm{SXDH}}$ is used to sign the extended $\mathbb{G}_1$ vector. The final signature consists of $(opk, osig)$ and the $SPS_{\mathrm{SXDH}}$ signature. Thus the signature has 1 $\mathbb{G}_1$ and 2 $\mathbb{G}_2$ additional elements. The public key is extended by $(n_2 + 1)$ $\mathbb{G}_1$ elements and 1 $\mathbb{G}_2$ element due to the POS public key and an additional $SPS_{\mathrm{SXDH}}$ public key for the extra dimension in $\mathbb{G}_1$.

### 5.2 Double Groth-Sahai Commitments to replace ElGamal

In the SPS scheme described in Figure 1, the signer needs to provide an ElGamal encryption $\zeta$ of $z$, as well as a Groth-Sahai (binding) commitment $c_z$ to $z$ (both in $\mathbb{G}_2$). Under the SXDH assumption, this requires a total of four group elements.

Note, the encryption of $z$ just needs to be IND-mCPA secure, and not CCA-secure.

While in the proof of security in Section 4, the challenger *does* need to decrypt $\zeta^*$ in some hybrid games (namely, games $(2, j, 2-8)$), it is the case that the security proof *does not* need to employ IND-mCPA security in those hybrid games (which is only needed in games $(2, j, 0-1)$ and $(2, j, 9-10)$).

So, it is worthwhile investigating if a double Groth-Sahai commitment which shares randomness might achieve the same IND-mCPA goal: the decryption to be performed using a trapdoor for the second commitment, which will not be used in NIWI proofs. At this point, we briefly describe Groth-Sahai commitments (under SXDH assumption).

Let $\mathbf{g}$ be a generator of group $\mathbb{G}_2$ (a cyclic group of order $q$, with identity $\mathcal{O}$). The commitment public-key pk is of the form

$$u_1 = (\mathbf{g}, Q = \chi\mathbf{g}), \quad u_2 = (\mathcal{U}, \mathcal{V}).$$

where $\chi$ is chosen at random from $\mathbb{Z}_q^*$. Note both $u_1$ and $u_2$ are in $\mathbb{G}_2^2$ which is a $\mathbb{Z}_q$-module. The second element $u_2$ can be chosen in two different ways: $u_2 = \psi u_1$ or $u_2 = \psi u_1 + (\mathcal{O}, \mathbf{g})$. The former choice of $u_2$ gives a perfectly hiding commitment key, whereas the latter choice of $u_2$ gives a perfectly binding commitment key (as we will see), and the two choices are indistinguishable under the DDH assumption in $\mathbb{G}_2$.

Commitments $\mathrm{com}(pk, x; r_x)$ to $x \in \mathbb{Z}_q$ using randomness $r_x \in \mathbb{Z}_q$ work as follows:

$$\mathrm{com} = (r_x, x) \cdot (u_1, u_2),$$

where the latter "$\cdot$"is an inner product.

On a hiding key pk, we have $u_2 = \psi u_1$ and hence $u$ is in the span of $\langle u_1 \rangle$, consequently, we get a perfectly hiding commitment. On a binding key pk, the commitment just becomes an El-Gamal encryption of $x\mathbf{g}$ with randomness $r_x + x\psi$, with secret key $\chi$.

While so far we have described the standard Groth-Sahai commitments, we now describe the alternate double Groth-Sahai commitment. In the double commitment, the public key is expanded to have $u_1' = \chi' u_1$, where $\chi'$ is a random and independent value from $\mathbb{Z}_q$. The value $u_2'$ is again defined in terms of $u_1'$ but using the same factor $\psi$ as used for $u_2$. Thus, $u_2' = \psi u_1$ (hiding) or $u_2' = \psi u_1 + (\mathcal{O}, \mathbf{g})$ (binding).

Now double commitments $\mathrm{dcom}(pk, x; r_x)$ is just $\langle c = (r_x, x) \cdot (u_1, u_2), c' = (r_x, x) \cdot (u_1', u_2') \rangle$.

On a hiding key pk, we have that four-vector $(u_2; u_2')$ is in span of four-vector $(u_1, u_1')$ (being a $\psi$-multiple). and hence dcom is a hiding commitment of $x$. In the binding setting, both commitments are ElGamal encryptions of $x$, first with secret key $\chi$ and the second with secret key $\chi'$ (with common randomness $(r_x + x\psi)$.

We also have the freedom to make one of the first public key hiding and the second binding. However, the double commitment is not hiding in this mixed

case. But, if there are other values that are only committed using the first public key (i.e. do not use double commitment) then those commitments are still hiding. Thus, e.g. in the SPS scheme, both $x$ and $z^i$ are committed in the group $\mathbb{G}_2$. Now, for each $z^i$ we will use double commitment, whereas for $x$ we will only commit using $(u_1, u_2)$. If this latter is in hiding mode and $(u'_1, u'_2)$ is in binding mode, then $c_x$ is a hiding commitment, and $c_z$ for all $i$ is not hiding. Moreover, if $(x, z)$ and $(x', z)$ are both witnesses for $\rho$ satisfying a witness-relation $R$, then the commitments (in this mixed mode) and the proofs are still witness indistinguishable. This is easily seen (under SXDH assumption) because for each commitment there is a unique proof satisfying the verification equation [GS12].

Coming back to the SPS scheme of Fig 1, we first replace the ElGamal encryption $\zeta$ of $z$ by a double commitment of $z$ using the above expanded public key in $\mathbb{G}_2$. Note, only $x$ and $z$ are GS-committed in $\mathbb{G}_2$. Next, the QA-NIZK $\Pi_2$ now has the language

$$L_2 \stackrel{\text{def}}{=} \left\{ \begin{array}{c} (c_z, c'_z) \mid \exists (z, r_z) : c_z = \mathrm{com}_2(z; r_z) \textbf{ and} \\ c'_z = \langle r_z \mathbf{g} + z[\psi]_2,\ r_z(\chi' \mathbf{g}) + z((\chi'\psi + 1)\mathbf{g}) \rangle \end{array} \right\}$$

Note $(\mathbf{g}, \psi\mathbf{g}, \chi'\mathbf{g}, (\chi'\psi + 1)\mathbf{g})$ are public parameters, and the above language is thus a linear-subspace language, and a single group element QA-NIZK proof can be given.

Next, note that decryption of $\zeta^*$ which is required in games $(2, j, 2-8)$ can be performed using secret key $\chi'$. The property that this is a good decryption of $\zeta^*$ holds only if the QA-NIZK $\Pi_2$ is sound and the double commitment is in binding mode; this in turn requires that that $\Pi_2$ be in true-simulation mode. This property is only required in games $(2, j, 4-6)$, so the double commitments must be in binding mode in these games. The only games where the challenger needs to hide $z$ and/or $x$ lie outside these games. However, there are games where $z$ is being decrypted using $\chi'$, and yet we need to transition between hiding and binding modes in $\mathbb{G}_2$. In particular, in games $(2, j, 1-3)$ and similarly in games $(2, j, 8-10)$. So instead, now consider an intermediate game between $(2, j, 1)$ and $(2, j, 2)$ where the commitment pk for $\mathbb{G}_2$ is moved to being mixed, i.e. binding for $\chi'$ and hiding for $\chi$. In this, the adversary's advantage changes by at most $\mathrm{ADV}^{\mathrm{CRSIND}}_{\Pi}$. Next, in game $(2, j, 2)$, the challenger introduces decryption using $\chi'$. In game $(2, j, 3)$ the challenger moves the first public key of the double commitment also to binding mode (after setting $x = 1 - \beta$). This incurs another penalty of $\mathrm{ADV}^{\mathrm{CRSIND}}_{\Pi}$. Hence forth, till game $(2, j, 8)$ the double commitment remains binding. The argument is reversed in games $(2, j, 8-10)$.

While this only saves one group element from the SPS scheme, it is worth recalling that savings can multiply in applications requiring SPS.

### 5.3 Mixing Groth-Sahai and QA-NIZK Proofs

While the scheme in Figure 1 is optimized for the size of the signature, its public key can be larger because of the use of QA-NIZK. In this section, we note that some of the QA-NIZK (or parts) can be replaced by Groth-Sahai NIZK proofs without much increase in size of the signatures.

The QA-NIZK $\Pi_2$ can easily be replaced to be a GS NIZK which just checks the multi-scalar equation that $\zeta = (\zeta_a, \zeta_b)$ satisfy $z\mathbf{g}_2 + ske\ \zeta_a - \zeta_b = 0$, where $z$ is committed in $c_z$ and commitment of El-Gamal secret-key $ske$ is in the public-key of SPS. The GS proof of this multi-scalar equation is only one group element (see e.g. equation (22) in [AHN+17]).

Next, the QA-NIZK $\Pi_1$ can be split into two parts, (i) one proving that $\rho$ and $c_t$ are related, which should remain a QA-NIZK –as this can be costly as a GS proof, and (ii) the other proving the $\hat{\rho}$ is $[s]_1$, which is just one group element as a GS proof. The QA-NIZK $\Pi_3$ remains as it is since true-simulation soundness is required.

So, this scheme requires an extra group element in the proof as $\Pi_1$ has been split. However, this scheme cannot use the optimization of Section 5.2. As for the proof of Theorem 1, note that the proof just employed the GS NIWI property, whereas now we must use the GS NIZK property, for proving $\hat{\rho} = [s]_1$. Fortunately, for such equations it is quite straightforward to convert Groth-Sahai NIWI to NIZK (for more details see [GS12]).

### 5.4 Sharing Groth-Sahai and QA-NIZK Public-Key Components

Note that the Groth-Sahai CRS (for each group) consists of four group elements (under the SXDH assumption), these being $u_1 = (\mathbf{g}, Q = \chi\mathbf{g})$, and $u_2 = (\mathcal{U}, \mathcal{V})$ as described above in Section 5.2.

The verifier CRS size of a QA-NIZK depends on the language (i.e. the number of its defining parameters), but some components of the CRS can be general group parameters and can be shared with GS CRS. From [JR14] recall that in a QA-NIZK for language with parameters $\mathbf{A}$ the prover and verifier CRS, i.e. $\mathbf{CRS}_p$ and $\mathbf{CRS}_v$ are defined as

$$\mathbf{CRS}_p := \mathbf{A} \cdot \begin{bmatrix} \mathsf{D} \\ \mathsf{R} \end{bmatrix} \qquad \mathbf{CRS}_v = \begin{bmatrix} \mathsf{D}\ \mathsf{B} \\ \mathsf{R}\ \mathsf{B} \\ -\mathsf{B} \end{bmatrix} \cdot \mathbf{g}$$

where $\mathsf{B}$ is a $k \times k$ matrix in the $k$-lin setting, and $D$ and $R$ are simulation trapdoors. Since SXDH is the k-lin setting with $k = 1$, $\mathsf{B}$ is just a single element. Moreover, this $B$ matrix can be shared among all the QA-NIZK (in the same group). In fact, it can also be made the same as one component of the GS CRS, namely $\mathcal{U} = \psi\mathbf{g}$.

### 5.5 Batching Pairings in Pairing-Product-Equations

We first analyze the size of the public key in the scheme of Fig 1, especially considering the sharing mentioned in Section 5.4. Now the 2 Groth-Sahai CRSes are of total size $(4, 4)$, including group generators and $\mathcal{U}$ that can be shared for QA-NIZK. The QA-NIZK $\Pi_1$ verifier CRS is then of size $(0, 6)$. The QA-NIZK $\Pi_2$ verifier CRS is of size $(4, 0)$ (or, $(3, 0)$ considering the optimization in Section 5.2). The QA-NIZK $\Pi_3$ verifier CRS is of size $(0, n_1 + 4)$. Since the

commitment to $x$ is of size $(0, 2)$, the public key is of size $(8, n_1 + 16)$ (or $(7, n_1 + 16)$ with optimization).

As for batch-verification, the number of pairing computations for verification can be reduced to pairing with $\mathbf{g}_1, \mathbf{g}_2, \mathcal{U}_1, \mathcal{U}_2, c_x, c_z$, and the elements in the QA-NIZK verification CRSes (other than those shared with GS CRS), which amounts to a total of $(8 + 14 + n_1 + 1) = n_1 + 23$ pairings.

If we use the scheme of Section 5.3 then the number of pairings reduce to $(8 + 7 + n_1 + 1) = n_1 + 16$ pairings (where one of these pairings is a constant pairing from the affine split-CRS QA-NIZK).

## References


[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.

[ACD+16] Masayuki Abe, Melissa Chase, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo. Constant-size structure-preserving signatures: Generic constructions and simple assumptions. *Journal of Cryptology*, 29(4):833–878, October 2016.

[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.

[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.

[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. *IACR Cryptology ePrint Archive*, 2010:133, 2010.

[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.

[AO09] Masayuki Abe and Miyako Ohkubo. A framework for universally composable non-committing blind signatures. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 435–450. Springer, Heidelberg, December 2009.

[BBM00] Mihir Bellare, Alexandra Boldyreva, and Silvio Micali. Public-key encryption in a multi-user setting: Security proofs and improvements. In Bart

Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 259–274. Springer, Heidelberg, May 2000.

[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.

[BFI+10] Olivier Blazy, Georg Fuchsbauer, Malika Izabachène, Amandine Jambert, Hervé Sibert, and Damien Vergnaud. Batch Groth-Sahai. In Jianying Zhou and Moti Yung, editors, *ACNS 10*, volume 6123 of *LNCS*, pages 218–235. Springer, Heidelberg, June 2010.

[BKP14] Olivier Blazy, Eike Kiltz, and Jiaxin Pan. (Hierarchical) identity-based encryption from affine message authentication. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 408–425. Springer, Heidelberg, August 2014.

[BS07] Mihir Bellare and Sarah Shoup. Two-tier signatures, strongly unforgeable signatures, and Fiat-Shamir without random oracles. In Tatsuaki Okamoto and Xiaoyun Wang, editors, *PKC 2007*, volume 4450 of *LNCS*, pages 201–216. Springer, Heidelberg, April 2007.

[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.

[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.

[Dam92] Ivan Damgård. Towards practical public key systems secure against chosen ciphertext attacks. In Joan Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 445–456. Springer, Heidelberg, August 1992.

[EHK+13] Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Villar. An algebraic framework for Diffie-Hellman assumptions. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147. Springer, Heidelberg, August 2013.

[ElG84] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In G. R. Blakley and David Chaum, editors, *CRYPTO'84*, volume 196 of *LNCS*, pages 10–18. Springer, Heidelberg, August 1984.

[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.

[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.

[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.

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

[Har11] Kristiyan Haralambiev. *Efficient cryptographic primitives for non-interactive zero-knowledge proofs and applications*. PhD thesis, New York University, 2011.

[HJ12] Dennis Hofheinz and Tibor Jager. Tightly secure signatures and public-key encryption. In *Crypto*, volume 7417, pages 590–607. Springer, 2012.

[Hof17] Dennis Hofheinz. Adaptive partitioning. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part II*, volume 10211 of *LNCS*, pages 489–518. Springer, Heidelberg, May 2017.

[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.

[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.

[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.

[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.

[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.