An extended abstract of this paper appears in *Advances in Cryptology – Asiacrypt'15*. This is the full version.

QA-NIZK Arguments in Asymmetric Groups: New Tools and New Constructions

Alonso González* Alejandro Hevia† Carla Ràfols‡

September 17, 2015

Abstract

A sequence of recent works have constructed constant-size quasi-adaptive (QA) NIZK arguments of membership in linear subspaces of $\hat{\mathbb{G}}^m$, where $\hat{\mathbb{G}}$ is a group equipped with a bilinear map $e : \hat{\mathbb{G}} \times \check{\mathbb{H}} \to \mathbb{T}$. Although applicable to any bilinear group, these techniques are less useful in the asymmetric case. For example, Jutla and Roy (Crypto 2014) show how to do QA aggregation of Groth-Sahai proofs, but the types of equations which can be aggregated are more restricted in the asymmetric setting. Furthermore, there are natural statements which cannot be expressed as membership in linear subspaces, for example the satisfiability of quadratic equations.

In this paper we develop specific techniques for asymmetric groups. We introduce a new computational assumption, under which we can recover all the aggregation results of Groth-Sahai proofs known in the symmetric setting. We adapt the arguments of membership in linear spaces of $\hat{\mathbb{G}}^m$ to linear subspaces of $\hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n$. In particular, we give a constant-size argument that two sets of Groth-Sahai commitments, defined over different groups $\hat{\mathbb{G}}, \check{\mathbb{H}}$, open to the same scalars in $\mathbb{Z}_q$, a useful tool to prove satisfiability of quadratic equations in $\mathbb{Z}_q$. We then use one of the arguments for subspaces in $\hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n$ and develop new techniques to give constant-size QA-NIZK proofs that a commitment opens to a bit-string. To the best of our knowledge, these are the first constant-size proofs for quadratic equations in $\mathbb{Z}_q$ under standard and falsifiable assumptions. As a result, we obtain improved threshold Groth-Sahai proofs for pairing product equations, ring signatures, proofs of membership in a list, and various types of signature schemes.

Keywords: QA-NIZK Arguments, Asymmetric Groups.

*Departamento de Ciencias de la Computación, Universidad de Chile, Chile. E-mail: alonso.gon@gmail.com, Gratefully acknowledges the support of CONICYT, CONICYT-PCHA/Doctorado Nacional/2013-21130937.

†Departamento de Ciencias de la Computación, Universidad de Chile, Chile. E-mail: ahevia@dcc.uchile.cl, URL: http://www.dcc.uchile.cl/~ahevia. Gratefully acknowledges partial support part by INRIA Chile.

‡Horst Görtz Institut für IT Sicherheit, Ruhr-Universität Bochum, Germany. E-mail: carla.rafols@rub.de. Part of this work was done while visiting Centro de Modelamiento Matemático, U. Chile. Gratefully acknowledges the support of CONICYT via Basal in Applied Mathematics.

Contents

1 Introduction

Ideally, a NIZK proof system should be both expressive and efficient, meaning that it should allow to prove statements which are general enough to be useful in practice using a small amount of resources. Furthermore, it should be constructed under mild security assumptions. As it is usually the case for most cryptographic primitives, there is a trade off between these three design goals. For instance, there exist constant-size proofs for any language in NP (e.g. [15]) but based on very strong and controversial assumptions, namely knowledge-of-exponent type of assumptions (which are non-falsifiable, according to Naor's classification [31]) or the random oracle model.

The Groth-Sahai proof system (GS proofs) [19] is an outstanding example of how these three goals (expressivity, efficiency, and mild assumptions) can be combined successfully. It provides a proof system for satisfiability of quadratic equations over bilinear groups. This language suffices to capture almost all of the statements which appear in practice when designing public-key cryptographic schemes over bilinear groups. Although GS proofs are quite efficient, proving satisfiability of m equations in n variables requires sending some commitments of size $\Theta(n)$ and some proofs of size $\Theta(m)$ and they easily get expensive unless the statement is very simple. For this reason, several recent works have focused on further improving proof efficiency (e.g. [10, 11, 32])

Among those, a recent line of work [22, 23, 25, 27] has succeeded in constructing constant-size arguments for very specific statements, namely, for membership in subspaces of $\hat{\mathbb{G}}^m$, where $\hat{\mathbb{G}}$ is some group equipped with a bilinear map where the discrete logarithm is hard. The soundness of the schemes is based on standard, falsifiable assumptions and the proof size is independent of both m and the witness size. These improvements are in a *quasi-adaptive* model (QA-NIZK, [22]). This means that the common reference string of these proof systems is specialized to the linear space where one wants to prove membership.

Interestingly, Jutla and Roy [23] also showed that their techniques to construct constant-size NIZK in linear spaces can be used to aggregate the GS proofs of m equations in n variables, that is, the total proof size can be reduced to $\Theta(n)$. Aggregation is also quasi-adaptive, which means that the common reference string depends on the set of equations one wants to aggregate. Further, it is only possible if the equations meet some restrictions. The first one is that only linear equations can be aggregated. The second one is that, in asymmetric bilinear groups, the equations must be one-sided linear, i.e. linear equations which have variables in only one of the $\mathbb{Z}_q$ modules $\hat{\mathbb{G}}, \check{\mathbb{H}}$, or $\mathbb{Z}_q$.[1]

Thus, it is worth to investigate if we can develop new techniques to aggregate other types of equations, for example, quadratic equations in $\mathbb{Z}_q$ and also recover all the aggregation results of [23] (in particular, for two-sided linear equations) in asymmetric bilinear groups. The latter (Type III bilinear groups, according to the classification of [14]) are the most attractive from the perspective of a performance and security trade off, specially since the recent attacks on discrete logarithms in finite fields by Joux [21] and subsequent improvements. Considerable research effort (e.g. [2, 13]) has been put into translating pairing-based cryptosystems from a setting with more structure in which design is simpler (e.g. composite-order or symmetric bilinear groups) to a more efficient setting (e.g. prime order or asymmetric bilinear groups). In this line, we aim not only at obtaining new results in the asymmetric setting but also to translate known results and develop

[1] Jutla and Roy show how to aggregate two-sided linear equations in symmetric bilinear groups. The asymmetric case is not discussed, yet for one-sided linear equations it can be easily derived from their results. This is not the case for two-sided ones, see Sect. 4.

new tools specifically designed for it which might be of independent interest.

1.1 Our Results

In Sect. 3, we give constructions of constant-size QA-NIZK arguments of membership in linear spaces of $\hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n$. Denote the elements of $\hat{\mathbb{G}}$ (respectively of $\check{\mathbb{H}}$) with a hat (resp. with an inverted hat), as $\hat{x} \in \hat{\mathbb{G}}$ (respectively, as $\check{y} \in \check{\mathbb{H}}$). Given $\hat{\mathbf{M}} \in \hat{\mathbb{G}}^{m\times t}$ and $\check{\mathbf{N}} \in \check{\mathbb{H}}^{n\times t}$, we construct QA-NIZK arguments of membership in the language

$$\mathcal{L}_{\hat{\mathbf{M}},\check{\mathbf{N}}} := \{(\hat{\mathbf{x}},\check{\mathbf{y}}) \in \hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n : \exists \mathbf{w} \in \mathbb{Z}_q^t,\ \hat{\mathbf{x}} = \hat{\mathbf{M}}\mathbf{w},\ \check{\mathbf{y}} := \check{\mathbf{N}}\mathbf{w}\},$$

which is the subspace of $\hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n$ spanned by $\begin{pmatrix}\hat{\mathbf{M}}\\ \check{\mathbf{N}}\end{pmatrix}$. This construction is based on the recent constructions of [25]. When $m = n$, we construct QA-NIZK arguments of membership in

$$\mathcal{L}_{\hat{\mathbf{M}},\check{\mathbf{N}},+} := \{(\hat{\mathbf{x}},\check{\mathbf{y}}) \in \hat{\mathbb{G}}^m \times \check{\mathbb{H}}^m : \exists \mathbf{w} \in \mathbb{Z}_q^t,\ \mathbf{x}+\mathbf{y} = (\mathbf{M}+\mathbf{N})\mathbf{w}\},$$

which is the linear subspace of $\hat{\mathbb{G}}^m \times \check{\mathbb{H}}^m$ of vectors $(\hat{\mathbf{x}},\check{\mathbf{y}})$ such that the sum of their discrete logarithms is in the image of $\mathbf{M}+\mathbf{N}$ (the sum of discrete logarithms of $\hat{\mathbf{M}}$ and $\check{\mathbf{N}}$).

From the argument for $\mathcal{L}_{\hat{\mathbf{M}},\check{\mathbf{N}}}$, we easily derive another constant-size QA-NIZK argument in the space

$$\mathcal{L}_{\mathsf{com},\hat{\mathbf{U}},\check{\mathbf{V}},\nu} := \left\{(\hat{\mathbf{c}},\check{\mathbf{d}}) \in \hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n : \exists(\mathbf{w},\mathbf{r},\mathbf{s}),\ \hat{\mathbf{c}} = \hat{\mathbf{U}}\begin{pmatrix}\mathbf{w}\\ \mathbf{r}\end{pmatrix},\ \check{\mathbf{d}} = \check{\mathbf{V}}\begin{pmatrix}\mathbf{w}\\ \mathbf{s}\end{pmatrix}\right\},$$

where $\hat{\mathbf{U}} \in \hat{\mathbb{G}}^{m\times\tilde{m}}$, $\check{\mathbf{V}} \in \check{\mathbb{H}}^{n\times\tilde{n}}$ and $\mathbf{w} \in \mathbb{Z}_q^\nu$. Membership in this space captures the fact that two commitments (or sets of commitments) in $\hat{\mathbb{G}},\check{\mathbb{H}}$ open to the same vector $\mathbf{w} \in \mathbb{Z}_q^\nu$. This is significant for the efficiency of quadratic GS proofs in asymmetric groups since, because of the way the proofs are constructed, one can only prove satisfiability of equations of degree one in each variable. Therefore, to prove a quadratic statement one needs to add auxiliary variables with commitments in the other group. For instance, to prove that $\hat{\mathbf{c}}$ opens to $b \in \{0,1\}$, one proves that some commitment $\check{\mathbf{d}}$ opens to $\overline{b}$ such that $\{b(\overline{b}-1) = 0, b-\overline{b} = 0\}$. Our result allows us to aggregate the n proofs of the second statement.

To construct these arguments we introduce a new assumption, the *Split Kernel Matrix Diffie-Hellman Assumption* (SKerMDH). This assumption is derived from the recently introduced Kernel Matrix Diffie-Hellman Assumption (KerMDH, [30]), which says that it is hard to find a vector in the co-kernel of $\hat{\mathbf{A}} \in \hat{\mathbb{G}}^{\ell\times k}$ when $\mathbf{A}$ is such that it is hard to decide membership in $\mathbf{Im}(\hat{\mathbf{A}})$ (i.e. when $\mathbf{A}$ is an instance of a Matrix DH Assumption [11]). Our SKerMDH Assumption says that one cannot find a solution to the KerMDH problem which is "split" between the groups $\hat{\mathbb{G}}$ and $\check{\mathbb{H}}$. We think this assumption can be useful in other protocols in asymmetric bilinear groups. A particular case of Kernel MDH Assumption is the *Simultaneous Double Pairing Assumption* (SDP, [3]), which is a well established assumption in symmetric bilinear maps, and its "split" variant is the SSDP Assumption (see Sect. 2.1).

In Sect. 4 we use the SKerMDH Assumption to lift the known aggregation results in symmetric groups to asymmetric ones. More specifically, we show how to extend the results of [23] to aggregate proofs of two-sided linear equations in asymmetric groups. While the original aggregation results of

[23] were based on decisional assumptions, our proof shows that they are implied by computational assumptions.

Next, in Sect. 5, we address the problem of aggregating the proof of quadratic equations in $\mathbb{Z}_q$. For concreteness, we study the problem of proving that a commitment in $\hat{\mathbb{G}}$ opens to a bit-string of length n. Such a construction was unknown even in symmetric bilinear groups (yet, it can be easily generalized to this setting, see Appendix C). More specifically, we prove membership in

$$\mathcal{L}_{\hat{\mathbf{U}},\mathsf{bits}} := \{\hat{\mathbf{c}} \in \hat{\mathbb{G}}^{n+m} : \hat{\mathbf{c}} := \hat{\mathbf{U}}_1\mathbf{b} + \hat{\mathbf{U}}_2\mathbf{w}, (\mathbf{b},\mathbf{w}) \in \{0,1\}^n \times \mathbb{Z}_q^m\},$$

where $(\hat{\mathbf{U}}_1, \hat{\mathbf{U}}_2) \in \hat{\mathbb{G}}^{(n+m)\times n} \times \hat{\mathbb{G}}^{(n+m)\times m}$ are matrices which define a perfectly binding and computationally hiding commitment to $\mathbf{b}$. Specifically, we give instantiations for $m = 1$ (when $\hat{\mathbf{c}}$ is a single commitment to $\mathbf{b}$), and $m = n$ (when $\hat{\mathbf{c}}$ is the concatenation of n Groth-Sahai commitments to a bit).

We stress that although our proof is constant-size, we need the commitment to be perfectly binding, thus the size of the commitment is linear in n. The common reference string which we need for this construction is quadratic in the size of the bit-string. Our proof is compatible with proving linear statements about the bit-string, for instance, that $\sum_{i\in[n]} b_i = t$ by adding a linear number (in n) of elements to the CRS (see Sect. 5.5.2). We observe that in the special case where $t = 1$ the common reference string can be linear in n. The costs of our constructions and the cost of GS proofs are summarized in Table 1.

We stress that our results rely solely on falsifiable assumptions. More specifically, in the asymmetric case we need some assumptions which are weaker than the Symmetric External DH Assumption plus the SSDP Assumption. Interestingly, our construction in the symmetric setting relies on assumptions which are all weaker than the 2-Lin Assumption (see Appendix C).

We think that our techniques for constructing QA-NIZK arguments for bit-strings might be of independent interest. In the asymmetric case, we combine our QA-NIZK argument for $\mathcal{L}_{\hat{\mathbf{M}},\check{\mathbf{N}},+}$ with decisional assumptions in $\hat{\mathbb{G}}$ and $\check{\mathbb{H}}$. We do this with the purpose of using QA-NIZK arguments even when $\mathbf{M}+\mathbf{N}$ has full rank. In this case, strictly speaking "proving membership in the space" looses all meaning, as every vector in $\hat{\mathbb{G}}^m \times \check{\mathbb{H}}^m$ is in the space. However, using decisional assumptions, we can argue that the generating matrix of the space is indistinguishable from a lower rank matrix which spans a subspace in which it is meaningful to prove membership.

Finally, in Sect. 6 we discuss some applications of our results. In particular, our results provide shorter signature size of several schemes, more efficient ring signatures, more efficient proofs of membership in a list, and improved threshold GS proofs for pairing product equations.

2 Preliminaries

Let Gen_a be some probabilistic polynomial time algorithm which on input 1^λ, where λ is the security parameter, returns the description of an asymmetric bilinear group $(q, \hat{\mathbb{G}}, \check{\mathbb{H}}, \mathbb{T}, e, \hat{g}, \check{h})$, where $\hat{\mathbb{G}}, \check{\mathbb{H}}$ and $\mathbb{T}$ are groups of prime order q, the elements $\hat{g}, \check{h}$ are generators of $\hat{\mathbb{G}}, \check{\mathbb{H}}$ respectively, and $e : \hat{\mathbb{G}} \times \check{\mathbb{H}} \to \mathbb{T}$ is an efficiently computable, non-degenerate bilinear map.

We denote by $\mathfrak{g}$ and $\mathfrak{h}$ the bit-size of the elements of $\hat{\mathbb{G}}$ and $\check{\mathbb{H}}$, respectively. Elements $\hat{x} \in \hat{\mathbb{G}}$ (resp. $\check{y} \in \check{\mathbb{H}}$, $z_\mathbb{T} \in \mathbb{T}$) are written with a hat (resp, with inverted hat, sub-index $\mathbb{T}$) and $\hat{0}, \check{0}$ and $0_\mathbb{T}$ denote the neutral elements. Given $\hat{x} \in \hat{\mathbb{G}}, \check{y} \in \check{\mathbb{H}}$, $\hat{x}\check{y}$ refers to the pairing operation, i.e. $\hat{x}\check{y} = e(\hat{x}, \check{y})$.

	Comms	Proof	CK	CRS(ρ)	#Pairings
GS [18]	$2n(\mathfrak{g}+\mathfrak{h})$	$4n(\mathfrak{g}+\mathfrak{h})$	$4(\mathfrak{g}+\mathfrak{h})$	0	$28n$
GS + $\Psi_{\overline{\mathcal{D}_k},\mathsf{com}}$	$2n(\mathfrak{g}+\mathfrak{h})$	$(2n+2)(\mathfrak{g}+\mathfrak{h})$	$4(\mathfrak{g}+\mathfrak{h})$	$(10n+4)(\mathfrak{g}+\mathfrak{h})$	$20n+8$
Π_{bit} $m=1$	$(n+1)\mathfrak{g}$	$10(\mathfrak{g}+\mathfrak{h})$	$(n+1)\mathfrak{g}$	$(6n^2+11n+34)(\mathfrak{g}+\mathfrak{h})$	$n+55$
Π_{bit} $m=n$ (i)	$2n\mathfrak{g}$	$10(\mathfrak{g}+\mathfrak{h})$	$4\mathfrak{g}$	$(12n^2+14n+22)\mathfrak{g}+$ $(12n^2+13n+24)\mathfrak{h}$	$2n+52$
Π_{bit} $m=n$ (ii)	$2n\mathfrak{g}$	$10(\mathfrak{g}+\mathfrak{h})$	$4\mathfrak{g}$	$(6n^2+16n+32)\mathfrak{g}+$ $(6n^2+12n+32)\mathfrak{h}$	$4n+52$
Π_{bit} weight 1, $m=1$	$(n+1)\mathfrak{g}$	$10(\mathfrak{g}+\mathfrak{h})$	$(n+1)\mathfrak{g}$	$(18n+32)\mathfrak{g}+$ $(19n+34)\mathfrak{h}$	$n+55$
Π_{bit} weight 1, $m=n$	$2n\mathfrak{g}$	$10(\mathfrak{g}+\mathfrak{h})$	$4\mathfrak{g}$	$(20n+32)\mathfrak{g}+$ $(18n+32)\mathfrak{h}$	$4n+52$

Table 1: Comparison for proofs of $b_i \in \{0,1\}$, for $i \in [n]$, between GS proofs and our different constructions. Our NIZK construction for bit-strings is denoted by Π_{bit} and the construction for proving that two sets of commitments open to the same value $\Psi_{\overline{\mathcal{D}_k},\mathsf{com}}$. Row "$\Pi_{\mathsf{bit}}$ $m=1$" is for our construction for a single commitment of size $n+1$ to a bit-string of size n. Rows "Π_{bit} $m=n$ (i)" and "Π_{bit} $m=n$ (ii)" are for our construction for n concatenated GS commitments, using the two different CRS distributions described in Sect. 5.5.1. Rows "Π_{bit} weight 1, $m=1$" and "Π_{bit} weight 1, $m=n$" are for our constructions for bit-strings of weight 1 with $m=1$ and $m=n$, respectively. Column "Comms" contains the size of the commitments, "CK" the size of the commitment keys in the CRS, and "CRS(ρ)" the size of the language dependent part of the CRS. The size of elements in $\hat{\mathbb{G}}$ and $\check{\mathbb{H}}$ is $\mathfrak{g}$ and $\mathfrak{h}$, respectively. The table is computed for $\mathcal{D}_k = \mathcal{L}_2$, the 2-Linear matrix distribution.

Vectors and matrices are denoted in boldface and any product of vectors/matrices of elements in $\hat{\mathbb{G}}$ and $\check{\mathbb{H}}$ is defined in the natural way via the pairing operation. That is, given $\hat{\mathbf{X}} \in \hat{\mathbb{G}}^{n\times m}$ and $\check{\mathbf{Y}} \in \check{\mathbb{H}}^{m\times \ell}$, $\hat{\mathbf{X}}\check{\mathbf{Y}} \in \mathbb{T}^{n\times \ell}$. The product $\check{\mathbf{X}}\hat{\mathbf{Y}} \in \mathbb{T}^{n\times \ell}$ is defined similarly by switching the arguments of the pairing. Given a matrix $\mathbf{T} = (t_{i,j}) \in \mathbb{Z}_q^{m\times n}$, $\hat{\mathbf{T}}$ (resp. $\check{\mathbf{T}}$) is the natural embedding of $\mathbf{T}$ in $\hat{\mathbb{G}}$ (resp. in $\check{\mathbb{H}}$), that is, the matrix whose (i,j)th entry is $t_{i,j}\hat{g}$ (resp. $t_{i,j}\check{h}$). Conversely, given $\hat{\mathbf{T}}$ or $\check{\mathbf{T}}$, we use $\mathbf{T} \in \mathbb{Z}_q^{n\times m}$ for the matrix of discrete logarithms of $\hat{\mathbf{T}}$ (resp. $\check{\mathbf{T}}$). We denote by $\mathbf{I}_{n\times n}$ the identity matrix in $\mathbb{Z}_q^{n\times n}$ and $\mathbf{e}_i^n$ the ith element of the canonical basis of $\mathbb{Z}_q^n$ (simply $\mathbf{e}_i$ if n is clear from the context). We make extensive use of the set $[n+k]\times[n+k]\setminus\{(i,i) : i \in [n]\}$ and for brevity we denote it by $\mathcal{I}_{n,k}$.

2.1 Computational Assumptions

Definition 2.1 Let $\ell, k \in \mathbb{N}$ with $\ell > k$. We call $\mathcal{D}_{\ell,k}$ a matrix distribution if it outputs (in poly time, with overwhelming probability) matrices in $\mathbb{Z}_q^{\ell\times k}$. We define $\mathcal{D}_k := \mathcal{D}_{k+1,k}$ and $\overline{\mathcal{D}_k}$ the distribution of the first k rows when $\mathbf{A} \leftarrow \mathcal{D}_k$. ▌

Definition 2.2 [Matrix Diffie-Hellman Assumption [11]] Let $\mathcal{D}_{\ell,k}$ be a matrix distribution and $\Gamma := (q, \hat{\mathbb{G}}, \check{\mathbb{H}}, \mathbb{T}, e, \hat{g}, \check{h}) \leftarrow \mathsf{Gen}_a(1^\lambda)$. We say that the $\mathcal{D}_{\ell,k}$-Matrix Diffie-Hellman ($\mathcal{D}_{\ell,k}$-$\mathsf{MDDH}_{\hat{\mathbb{G}}}$)

Assumption holds relative to Gen_a if for all PPT adversaries D,

$$\mathbf{Adv}_{\mathcal{D}_{\ell,k},\mathsf{Gen}_a}(\mathsf{D}) := \left|\Pr[\mathsf{D}(\Gamma, \hat{\mathbf{A}}, \hat{\mathbf{A}}\mathbf{w}) = 1] - \Pr[\mathsf{D}(\Gamma, \hat{\mathbf{A}}, \hat{\mathbf{u}}) = 1]\right| = \mathsf{negl}(\lambda),$$

where the probability is taken over $\Gamma \leftarrow \mathsf{Gen}_a(1^\lambda)$, $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}, \mathbf{w} \leftarrow \mathbb{Z}_q^k, \hat{\mathbf{u}} \leftarrow \hat{\mathbb{G}}^\ell$ and the coin tosses of adversary D. ▌

The $\mathcal{D}_{\ell,k}$-$\mathsf{MDDH}_{\check{\mathbb{H}}}$ problem is defined similarly. In this paper we will refer to the following matrix distributions:

$$\mathcal{L}_k : \mathbf{A} = \begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_k \\ 1 & 1 & \dots & 1 \end{pmatrix}, \mathcal{L}_{\ell,k} : \mathbf{A} = \begin{pmatrix} \mathbf{B} \\ \mathbf{C} \end{pmatrix}, \ \mathcal{U}_{\ell,k} : \mathbf{A} = \begin{pmatrix} a_{1,1} & \dots & a_{1,k} \\ \vdots & \ddots & \vdots \\ a_{\ell,1} & \dots & a_{\ell,k} \end{pmatrix},$$

where $a_i, a_{i,j} \leftarrow \mathbb{Z}_q$, for each $i, j \in [k]$, $\mathbf{B} \leftarrow \overline{\mathcal{L}}_k$, $\mathbf{C} \leftarrow \mathbb{Z}_q^{\ell-k,k}$.

The $\mathcal{L}_k$-MDDH Assumption is the k-linear family of Decisional Assumptions [20, 33]. The $\mathcal{L}_1$-MDDH_X, $X \in \{\hat{\mathbb{G}}, \check{\mathbb{H}}\}$, is the Decisional Diffie-Hellman (DDH) Assumption in X, and the assumption that it holds in both groups is the Symmetric External DH Assumption (SXDH). The $\mathcal{L}_{\ell,k}$-MDDH Assumption is used in our construction to commit to multiple elements simultaneously. It can be shown tightly equivalent to the $\mathcal{L}_k$-MDDH Assumption. The $\mathcal{U}_{\ell,k}$ Assumption is the *Uniform* Assumption and is weaker than the $\mathcal{L}_k$-MDDH. Additionally, we will be using the following family of computational assumptions:

Definition 2.3 [Kernel Diffie-Hellman Assumption [30]]Let $\Gamma \leftarrow \mathsf{Gen}_a(1^\lambda)$. The Kernel Diffie-Hellman Assumption in $\check{\mathbb{H}}$ ($\mathcal{D}_{\ell,k}$-$\mathsf{KerMDH}_{\check{\mathbb{H}}}$) says that every PPT Algorithm has negligible advantage in the following game: given $\check{\mathbf{A}}$, where $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, find $\hat{\mathbf{x}} \in \hat{\mathbb{G}}^\ell \setminus \{\hat{\mathbf{0}}\}$, such that $\hat{\mathbf{x}}^\top \check{\mathbf{A}} = \mathbf{0}_{\mathbb{T}}$. ▌

The Simultaneous Pairing Assumption in $\check{\mathbb{H}}$ ($\mathsf{SP}_{\check{\mathbb{H}}}$) is the $\mathcal{U}_1$-$\mathsf{KerMDH}_{\check{\mathbb{H}}}$ Assumption and the Simultaneous Double Pairing Assumption ($\mathsf{SDP}_{\check{\mathbb{H}}}$) is the $\mathcal{L}_{2,3}$- $\mathsf{KerMDH}_{\check{\mathbb{H}}}$ Assumption. The Kernel Diffie-Hellman assumption is a generalization and abstraction of these two assumptions to other matrix distributions. The $\mathcal{D}_{\ell,k}$-$\mathsf{KerMDH}_{\check{\mathbb{H}}}$ Assumption is weaker than the $\mathcal{D}_{\ell,k}$-$\mathsf{MDDH}_{\check{\mathbb{H}}}$ Assumption, since a solution allows to decide membership in $\mathsf{Im}(\check{\mathbf{A}})$.

For our construction, we need to introduce a new family of computational assumptions.

Definition 2.4 [Split Kernel Diffie-Hellman Assumption] Let $\Gamma \leftarrow \mathsf{Gen}_a(1^\lambda)$. The Split Kernel Diffie-Hellman Assumption in $\hat{\mathbb{G}}, \check{\mathbb{H}}$ ($\mathcal{D}_{\ell,k}$-$\mathsf{SKerMDH}$) says that every PPT Algorithm has negligible advantage in the following game: given $(\hat{\mathbf{A}}, \check{\mathbf{A}})$, $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, find a pair of vectors $(\hat{\mathbf{r}}, \check{\mathbf{s}}) \in \hat{\mathbb{G}}^\ell \times \check{\mathbb{H}}^\ell$, $\mathbf{r} \neq \mathbf{s}$, such that $\hat{\mathbf{r}}^\top \check{\mathbf{A}} = \check{\mathbf{s}}^\top \hat{\mathbf{A}}$. ▌

As a particular case we consider the *Split Simultaneous Double Pairing Assumption in* $\hat{\mathbb{G}}, \check{\mathbb{H}}$ (SSDP) which is the $\mathcal{L}_2$-$\mathsf{SKerMDH}$ Assumption. Intuitively, the Kernel Diffie-Hellman Assumption says one cannot find a non-zero vector in $\hat{\mathbb{G}}^\ell$ which is in the co-kernel of $\check{\mathbf{A}}$, while the new assumption says one cannot find a pair of vectors in $\hat{\mathbb{G}}^\ell \times \check{\mathbb{H}}^\ell$ such that the difference of the vector of their discrete logarithms is in the co-kernel of $\check{\mathbf{A}}$. The name "split" comes from the idea that the output of a successful adversary would break the Kernel Diffie-Hellman Assumption, but this instance is "split" between the groups $\hat{\mathbb{G}}$ and $\check{\mathbb{H}}$. When $k = 1$, the $\mathcal{D}_{\ell,k}$-$\mathsf{SKerMDH}$ Assumption does not hold. The

assumption is generically as least as hard as the standard,"non-split" assumption in symmetric bilinear groups. This means, in particular, that in Type III bilinear groups, one can use the SSDP Assumption with the same security guarantees as the SDP Assumption, which is a well established assumption (used for instance in [29]).

Lemma 2.5 If $\mathcal{D}_{\ell,k}$-KerMDH holds in generic symmetric bilinear groups, then $\mathcal{D}_{\ell,k}$-SKerMDH holds in generic asymmetric bilinear groups. ∎

Suppose there is a generic algorithm which breaks the $\mathcal{D}_{\ell,k}$-SKerMDH Assumption. Intuitively, given two different encodings of $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, $(\hat{\mathbf{A}}, \check{\mathbf{A}})$, this algorithm finds $\hat{\mathbf{r}}$ and $\check{\mathbf{s}}$, $\mathbf{r} \neq \mathbf{s}$ such that $\hat{\mathbf{r}}^\top \check{\mathbf{A}} = \check{\mathbf{s}}^\top \hat{\mathbf{A}}$. But since the algorithm is generic, it also works when $\hat{\mathbb{G}} = \check{\mathbb{H}}$, and then $\hat{\mathbf{r}} - \hat{\mathbf{s}}$ is a solution to $\mathcal{D}_{\ell,k}$-KerMDH. For a formal proof, see Appendix F.

2.2 Groth-Sahai NIZK Proofs

The GS proof system allows to prove satisfiability of a set of quadratic equations in a bilinear group. The admissible equation types must be in the following form:

$$\sum_{j=1}^{m_y} f(\alpha_j, \mathsf{y}_j) + \sum_{i=1}^{m_x} f(\mathsf{x}_i, \beta_i) + \sum_{i=1}^{m_x}\sum_{j=1}^{m_y} f(\mathsf{x}_i, \gamma_{i,j}\mathsf{y}_j) = t, \tag{1}$$

where A_1, A_2, A_T are $\mathbb{Z}_q$-vector spaces equipped with some bilinear map $f : A_1 \times A_2 \to A_T$, $\boldsymbol{\alpha} \in A_1^{m_y}$, $\boldsymbol{\beta} \in A_2^{m_x}$, $\boldsymbol{\Gamma} = (\gamma_{i,j}) \in \mathbb{Z}_q^{m_x \times m_y}$, $t \in A_T$. The modules and the map f can be defined in different ways as: (a) in pairing-product equations (PPEs), $A_1 = \hat{\mathbb{G}}$, $A_2 = \check{\mathbb{H}}$, $A_T = \mathbb{T}$, $f(\hat{x}, \check{y}) = \hat{x}\check{y} \in \mathbb{T}$, in which case $t = 0_{\mathbb{T}}$, (b1) in multi-scalar multiplication equations in $\hat{\mathbb{G}}$ (MMEs), $A_1 = \hat{\mathbb{G}}$, $A_2 = \mathbb{Z}_q$, $A_T = \hat{\mathbb{G}}$, $f(\hat{x}, y) = y\hat{x} \in \hat{\mathbb{G}}$, (b2) MMEs in $\check{\mathbb{H}}$ (MMEs), $A_1 = \mathbb{Z}_q$, $A_2 = \check{\mathbb{H}}$, $A_T = \check{\mathbb{H}}$, $f(x, \check{y}) = x\check{y} \in \check{\mathbb{H}}$, and (c) in quadratic equations in $\mathbb{Z}_q$ (QEs), $A_1 = A_2 = A_T = \mathbb{Z}_q$, $f(x, y) = xy \in \mathbb{Z}_q$. An equation is linear if $\boldsymbol{\Gamma} = \mathbf{0}$, it is *two-sided linear* if both $\boldsymbol{\alpha} \neq \mathbf{0}$ and $\boldsymbol{\beta} \neq \mathbf{0}$, and *one-sided* otherwise.

We briefly recall some facts about GS proofs in the SXDH instantiation used in the rest of the paper. Let $\Gamma \leftarrow \mathsf{Gen}_a(1^\lambda)$, $\mathbf{u}_2, \mathbf{v}_2 \leftarrow \mathcal{L}_1$, $\mathbf{u}_1 := \mathbf{e}_1 + \mu\mathbf{u}_2$, $\mathbf{v}_1 := \mathbf{e}_1 + \epsilon\mathbf{v}_2$, $\mu, \epsilon \leftarrow \mathbb{Z}_q$. The common reference string is $\mathsf{crs}_{\mathrm{GS}} := (\Gamma, \hat{\mathbf{u}}_1, \hat{\mathbf{u}}_2, \check{\mathbf{v}}_1, \check{\mathbf{v}}_2)$ and is known as the *perfectly sound CRS*. There is also a *perfectly witness-indistinguishable CRS*, with the only difference being that $\mathbf{u}_1 := \mu\mathbf{u}_2$ and $\mathbf{v}_1 := \epsilon\mathbf{v}_2$ and the simulation trapdoor is (μ, ϵ). These two CRS distributions are computationally indistinguishable. Implicitly, $\mathsf{crs}_{\mathrm{GS}}$ defines the maps:

$$\iota_1 : \hat{\mathbb{G}} \cup \mathbb{Z}_q \to \hat{\mathbb{G}}^2, \qquad \iota_1(\hat{x}) := (\hat{x}, \hat{0})^\top, \qquad \iota_1(x) := x\hat{\mathbf{u}}_1.$$
$$\iota_2 : \check{\mathbb{H}} \cup \mathbb{Z}_q \to \check{\mathbb{H}}^2, \qquad \iota_2(\check{y}) := (\check{y}, \check{0})^\top, \qquad \iota_2(y) := y\check{\mathbf{v}}_1.$$

The maps ι_X, $X \in \{1, 2\}$ can be naturally extended to vectors of arbitrary length $\boldsymbol{\delta} \in A_X^m$ and we write $\iota_X(\boldsymbol{\delta})$ for $(\iota_X(\delta_1)||\ldots||\iota_X(\delta_m))$.

The perfectly sound CRS defines perfectly binding commitments for any variable in A_1 or A_2. Specifically, the commitment to $x \in A_1$ is $\hat{\mathbf{c}} := \iota_1(x) + r_1(\hat{\mathbf{u}}_1 - \hat{\mathbf{e}}_1) + r_2\hat{\mathbf{u}}_2 \in \hat{\mathbb{G}}^2$, and to $y \in A_2$ is $\check{\mathbf{d}} := \iota_2(y) + s_1(\check{\mathbf{v}}_1 - \check{\mathbf{e}}_1) + s_2\check{\mathbf{v}}_2$, where $r_1, r_2, s_1, s_2 \leftarrow \mathbb{Z}_q$, except if $A_1 = \mathbb{Z}_q$ (resp. $A_2 = \mathbb{Z}_q$) in which case $r_1 = 0$ (resp. $s_1 = 0$).

2.3 Quasi-Adaptive NIZK Arguments

We recall the definition of Quasi Adaptive NIZK (QA-NIZK) Arguments of Jutla et al. [22]. A QA-NIZK proof system enables to prove membership in a language defined by a relation $\mathcal{R}_\rho$, which in turn is completely determined by some parameter ρ sampled from a distribution $\mathcal{D}_\Gamma$. We say that $\mathcal{D}_\Gamma$ is *witness samplable* if there exist an efficient algorithm that samples (ρ, ω) such that ρ is distributed according to $\mathcal{D}_\Gamma$, and membership of ρ in the *parameter language* $\mathcal{L}_{\mathsf{par}}$ can be efficiently verified with ω. While the Common Reference String can be set based on ρ, the zero-knowledge simulator is required to be a single probabilistic polynomial time algorithm that works for the whole collection of relations $\mathcal{R}_\Gamma$.

A tuple of algorithms $(\mathsf{K}_0, \mathsf{K}_1, \mathsf{P}, \mathsf{V})$ is called a QA-NIZK proof system for witness-relations $\mathcal{R}_\Gamma = \{\mathcal{R}_\rho\}_{\rho \in \mathrm{sup}(\mathcal{D}_\Gamma)}$ with parameters sampled from a distribution $\mathcal{D}_\Gamma$ over associated parameter language $\mathcal{L}_{\mathsf{par}}$, if there exists a probabilistic polynomial time simulator $(\mathsf{S}_1, \mathsf{S}_2)$, such that for all non-uniform PPT adversaries A_1, A_2, A_3 we have:

Quasi-Adaptive Completeness:

$$\Pr\left[\begin{array}{l}\Gamma \leftarrow \mathsf{K}_0(1^\lambda); \rho \leftarrow \mathcal{D}_\Gamma; \psi \leftarrow \mathsf{K}_1(\Gamma, \rho); (x, w) \leftarrow \mathsf{A}_1(\Gamma, \psi); \\ \pi \leftarrow \mathsf{P}(\psi, x, w) : \mathsf{V}(\psi, x, \pi) = 1 \text{ if } \mathcal{R}_\rho(x, w)\end{array}\right] = 1.$$

Computational Quasi-Adaptive Soundness:

$$\Pr\left[\begin{array}{l}\Gamma \leftarrow \mathsf{K}_0(1^\lambda); \rho \leftarrow \mathcal{D}_\Gamma; \psi \leftarrow \mathsf{K}_1(\Gamma, \rho); \\ (x, \pi) \leftarrow \mathsf{A}_2(\Gamma, \psi) : \mathsf{V}(\psi, x, \pi) = 1 \text{ and } \neg(\exists w : \mathcal{R}_\rho(x, w))\end{array}\right] \approx 0.$$

Perfect Quasi-Adaptive Zero-Knowledge:

$$\Pr[\Gamma \leftarrow \mathsf{K}_0(1^\lambda); \rho \leftarrow \mathcal{D}_\Gamma; \psi \leftarrow \mathsf{K}_1(\Gamma, \rho) : \mathsf{A}_3^{\mathsf{P}(\psi, \cdot, \cdot)}(\Gamma, \psi) = 1] =$$
$$\Pr[\Gamma \leftarrow \mathsf{K}_0(1^\lambda); \rho \leftarrow \mathcal{D}_\Gamma; (\psi, \tau) \leftarrow \mathsf{S}_1(\Gamma, \rho) : \mathsf{A}_3^{\mathsf{S}(\psi, \tau, \cdot, \cdot)}(\Gamma, \psi) = 1]$$

where

- $\mathsf{P}(\psi, \cdot, \cdot)$ emulates the actual prover. It takes input (x, w) and outputs a proof π if $(x, w) \in \mathcal{R}_\rho$. Otherwise, it outputs $\perp$.
- $\mathsf{S}(\psi, \tau, \cdot, \cdot)$ is an oracle that takes input (x, w). It outputs a simulated proof $\mathsf{S}_2(\psi, \tau, x)$ if $(x, w) \in \mathcal{R}_\rho$ and $\perp$ if $(x, w) \notin \mathcal{R}_\rho$.

Note that ψ is the CRS in the above definitions. We assume that ψ contains an encoding of ρ, which is thus available to V.

2.4 QA-NIZK Argument for Linear Spaces

In this section we recall the two constructions of QA-NIZK arguments of membership in linear spaces given by Kiltz and Wee [25], for the language:

$$\mathcal{L}_{\hat{\mathbf{M}}} := \{\hat{\mathbf{x}} \in \hat{\mathbb{G}}^n : \exists \mathbf{w} \in \mathbb{Z}_q^t,\ \hat{\mathbf{x}} = \hat{\mathbf{M}}\mathbf{w}\}.$$

$\underline{\mathsf{K}_1(\Gamma, \hat{\mathbf{M}}, n) \qquad (\mathsf{S}_1(\Gamma, \hat{\mathbf{M}}, n))}$
$\mathbf{A} \leftarrow \widetilde{\mathcal{D}_k}, \boldsymbol{\Delta} \leftarrow \mathbb{Z}_q^{\tilde{k} \times n}$
$\check{\mathbf{A}}_\Delta := \boldsymbol{\Delta}^\top \check{\mathbf{A}}, \hat{\mathbf{M}}_\Delta := \boldsymbol{\Delta}\hat{\mathbf{M}}$
Return $\mathsf{crs} := (\hat{\mathbf{M}}_\Delta, \check{\mathbf{A}}_\Delta, \check{\mathbf{A}})$
$(\tau_{sim} := \boldsymbol{\Delta})$

$\underline{\mathsf{P}(\mathsf{crs}, \hat{\mathbf{x}}, \mathbf{w}) \ \backslash\backslash \hat{\mathbf{x}} = \hat{\mathbf{M}}\mathbf{w}}$
Return $\hat{\boldsymbol{\sigma}} := \hat{\mathbf{M}}_\Delta \mathbf{w}$.

$\underline{\mathsf{V}(\mathsf{crs}, \hat{\mathbf{x}}, \hat{\boldsymbol{\sigma}})}$
Return $(\hat{\mathbf{x}}^\top \check{\mathbf{A}}_\Delta = \hat{\boldsymbol{\sigma}}^\top \check{\mathbf{A}})$

$\underline{\mathsf{S}_2(\mathsf{crs}, \hat{\mathbf{x}}, \tau_{sim})}$
Return $\hat{\boldsymbol{\sigma}} := \boldsymbol{\Delta}\hat{\mathbf{x}}$

Figure 1: The figure describes $\Psi_{\mathcal{D}_k}$ when $\widetilde{\mathcal{D}_k} = \mathcal{D}_k$ and $\tilde{k} = k+1$ and $\Psi_{\overline{\mathcal{D}}_k}$ when $\widetilde{\mathcal{D}_k} = \overline{\mathcal{D}}_k$ and $\tilde{k} = k$. Both are QA-NIZK arguments for $\mathcal{L}_{\hat{\mathbf{M}}}$. $\Psi_{\mathcal{D}_k}$ is the construction of [25, Sect. 3.1], which is a generalization of Libert *et al*'s QA-NIZK [27] to any $\mathcal{D}_k$-$\mathsf{KerMDH}_{\check{\mathbb{H}}}$ Assumption. $\Psi_{\overline{\mathcal{D}}_k}$ is the construction of [25, Sect. 3.2.].

Algorithm $\mathsf{K}_0(1^\lambda)$ just outputs $\Gamma := (q, \hat{\mathbb{G}}, \check{\mathbb{H}}, \mathbb{T}, e, \hat{g}, \check{h}) \leftarrow \mathsf{Gen}_a(1^\lambda)$, the rest of the algorithms are described in Fig. 1.

Theorem 2.6 [Theorem 1 of [25]] If $\widetilde{\mathcal{D}_k} = \mathcal{D}_k$ and $\tilde{k} = k+1$, Fig. 1 describes a QA-NIZK proof system with perfect completeness, computational adaptive soundness based on the $\mathcal{D}_k$-$\mathsf{KerMDH}_{\check{\mathbb{H}}}$ Assumption, perfect zero-knowledge, and proof size $k+1$. ∎

Theorem 2.7 [Theorem 2 of [25]] If $\widetilde{\mathcal{D}_k} = \overline{\mathcal{D}}_k$ and $\tilde{k} = k$, and $\mathcal{D}_\Gamma$ is a witness samplable distribution, Fig. 1 describes a QA-NIZK proof system with perfect completeness, computational adaptive soundness based on the $\mathcal{D}_k$-$\mathsf{KerMDH}_{\check{\mathbb{H}}}$ Assumption, perfect zero-knowledge, and proof size k. ∎

3 New QA-NIZK Arguments in Asymmetric Groups

In this section we construct three QA-NIZK arguments of membership in different subspaces of $\hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n$. Their soundness relies on the Split Kernel Assumption.

3.1 Argument of Membership in Subspace Concatenation

Figure 2 describes a QA-NIZK Argument of Membership in the language

$$\mathcal{L}_{\hat{\mathbf{M}},\check{\mathbf{N}}} := \{(\hat{\mathbf{x}}, \check{\mathbf{y}}) : \exists \mathbf{w} \in \mathbb{Z}_q^t, \ \hat{\mathbf{x}} = \hat{\mathbf{M}}\mathbf{w}, \check{\mathbf{y}} = \check{\mathbf{N}}\mathbf{w}\} \subseteq \hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n.$$

We refer to this as the *Concatenation Language*, because if we define $\mathbf{P}$ as the concatenation of $\hat{\mathbf{M}}, \check{\mathbf{N}}$, that is $\mathbf{P} := \begin{pmatrix} \hat{\mathbf{M}} \\ \check{\mathbf{N}} \end{pmatrix}$, then $(\hat{\mathbf{x}}, \check{\mathbf{y}}) \in \mathcal{L}_{\hat{\mathbf{M}},\check{\mathbf{N}}}$ iff $\begin{pmatrix} \hat{\mathbf{x}} \\ \check{\mathbf{y}} \end{pmatrix}$ is in the span of $\mathbf{P}$.

Soundness Intuition. If we ignore for a moment that $\hat{\mathbb{G}}, \check{\mathbb{H}}$ are different groups, $\Psi_{\mathcal{D}_k,\mathsf{spl}}$ (resp. $\Psi_{\overline{\mathcal{D}}_k,\mathsf{spl}}$) is almost identical to $\Psi_{\mathcal{D}_k}$ (resp. to $\Psi_{\overline{\mathcal{D}}_k}$) for the language $\mathcal{L}_{\hat{\mathbf{P}}}$, and $\boldsymbol{\Delta} := (\boldsymbol{\Lambda} || \boldsymbol{\Xi})$, where $\boldsymbol{\Lambda} \in \mathbb{Z}_q^{\tilde{k} \times m}, \boldsymbol{\Xi} \in \mathbb{Z}_q^{\tilde{k} \times n}$. Further, the information that an unbounded adversary can extract from the CRS about $\boldsymbol{\Delta}$ is:

1. $\left\{ \mathbf{P}_\Delta = \boldsymbol{\Lambda}\mathbf{M} + \boldsymbol{\Xi}\mathbf{N}, \mathbf{A}_\Delta = \boldsymbol{\Delta}^\top \mathbf{A} = \begin{pmatrix} \boldsymbol{\Lambda}^\top \mathbf{A} \\ \boldsymbol{\Xi}^\top \mathbf{A} \end{pmatrix} \right\}$ from $\mathsf{crs}_{\Psi_{\mathcal{D}_k}}$,

$\underline{\mathsf{K}_1(\Gamma, \hat{\mathbf{M}}, \check{\mathbf{N}}, m, n) \quad (\mathsf{S}_1(\Gamma, \hat{\mathbf{M}}, \check{\mathbf{N}}, m, n))}$

$\mathbf{A} \leftarrow \widetilde{\mathcal{D}_k}$

$\mathbf{\Lambda} \leftarrow \mathbb{Z}_q^{\tilde{k} \times m}, \mathbf{\Xi} \leftarrow \mathbb{Z}_q^{\tilde{k} \times n}, \mathbf{Z} \leftarrow \mathbb{Z}_q^{\tilde{k} \times t}$

$\check{\mathbf{A}}_\Lambda := \mathbf{\Lambda}^\top \check{\mathbf{A}}$

$\hat{\mathbf{A}}_\Xi := \mathbf{\Xi}^\top \hat{\mathbf{A}}$

$\hat{\mathbf{M}}_\Lambda := \mathbf{\Lambda}\hat{\mathbf{M}} + \hat{\mathbf{Z}}$

$\check{\mathbf{N}}_\Xi := \mathbf{\Xi}\check{\mathbf{N}} - \check{\mathbf{Z}}$

Return $\mathsf{crs} := (\hat{\mathbf{M}}_\Lambda, \check{\mathbf{A}}_\Lambda, \check{\mathbf{A}}, \check{\mathbf{N}}_\Xi, \hat{\mathbf{A}}_\Xi, \hat{\mathbf{A}})$.

$(\tau_{sim} := (\mathbf{\Lambda}, \mathbf{\Xi}).)$

$\underline{\mathsf{P}(\mathsf{crs}, \hat{\mathbf{x}}, \check{\mathbf{y}}, \mathbf{w})}$

$\backslash\backslash(\hat{\mathbf{x}} = \hat{\mathbf{M}}\mathbf{w}, \check{\mathbf{y}} = \check{\mathbf{N}}\mathbf{w})$

$\mathbf{z} \leftarrow \mathbb{Z}_q^{\tilde{k}}$

$\hat{\boldsymbol{\rho}} := \hat{\mathbf{M}}_\Lambda \mathbf{w} + \hat{\mathbf{z}}$

$\check{\boldsymbol{\sigma}} := \check{\mathbf{N}}_\Xi \mathbf{w} - \check{\mathbf{z}}$

Return $(\hat{\boldsymbol{\rho}}, \check{\boldsymbol{\sigma}})$.

$\underline{\mathsf{V}(\mathsf{crs}, (\hat{\mathbf{x}}, \check{\mathbf{y}}), (\hat{\boldsymbol{\rho}}, \check{\boldsymbol{\sigma}}))}$

Return $(\hat{\mathbf{x}}^\top \check{\mathbf{A}}_\Lambda - \hat{\boldsymbol{\rho}}^\top \check{\mathbf{A}} = \check{\boldsymbol{\sigma}}^\top \hat{\mathbf{A}} - \check{\mathbf{y}}^\top \hat{\mathbf{A}}_\Xi)$.

$\underline{\mathsf{S}_2(\mathsf{crs}, (\hat{\mathbf{x}}, \check{\mathbf{y}}), \tau_{sim})}$

$\mathbf{z} \leftarrow \mathbb{Z}_q^{\tilde{k}}$

$\hat{\boldsymbol{\rho}} := \mathbf{\Lambda}\hat{\mathbf{x}} + \hat{\mathbf{z}}$

$\check{\boldsymbol{\sigma}} := \mathbf{\Xi}\check{\mathbf{y}} - \check{\mathbf{z}}$

Return $(\hat{\boldsymbol{\rho}}, \check{\boldsymbol{\sigma}})$.

Figure 2: Two QA-NIZK Arguments for $\mathcal{L}_{\hat{\mathbf{M}}, \check{\mathbf{N}}}$. $\Psi_{\mathcal{D}_k, \mathsf{spl}}$ is defined for $\widetilde{\mathcal{D}_k} = \mathcal{D}_k$ and $\tilde{k} = k+1$, and is a generalization of [25] Sect. 3.1 in two groups. The second construction $\Psi_{\overline{\mathcal{D}}_k, \mathsf{spl}}$ corresponds to $\widetilde{\mathcal{D}_k} = \overline{\mathcal{D}_k}$ and $\tilde{k} = k$, and is a generalization of [25] Sect. 3.2 in two groups. Computational soundness is based on the $\mathcal{D}_k$-SKerMDH Assumption. The CRS size is $(\tilde{k}k + \tilde{k}t + mk)\mathfrak{g} + (\tilde{k}k + \tilde{k}t + nk)\mathfrak{h}$ and the proof size $\tilde{k}(\mathfrak{g} + \mathfrak{h})$. Verification requires $2\tilde{k}k + (m+n)k$ pairing computations.

2. $\left\{\mathbf{M}_\Lambda = \mathbf{\Lambda}\mathbf{M} + \mathbf{Z}, \mathbf{N}_\Xi = \mathbf{\Xi}\mathbf{N} - \mathbf{Z}, \begin{pmatrix} \mathbf{A}_\Lambda \\ \mathbf{A}_\Xi \end{pmatrix} = \begin{pmatrix} \mathbf{\Lambda}^\top \mathbf{A} \\ \mathbf{\Xi}^\top \mathbf{A} \end{pmatrix}\right\}$ from $\mathsf{crs}_{\Psi_{\mathcal{D}_k, \mathsf{spl}}}$.

Given that the matrix $\mathbf{Z}$ is uniformly random, $\mathsf{crs}_{\Psi_{\mathcal{D}_k}}$ and $\mathsf{crs}_{\Psi_{\mathcal{D}_k, \mathsf{spl}}}$ reveal the same information about $\mathbf{\Delta}$ to an unbounded adversary. Therefore, as the proof of soundness is essentially based on the fact that parts of $\mathbf{\Delta}$ are information theoretically hidden to the adversary, the original proof of [25] can be easily adapted for the new arguments. The proofs can be found in Appendix A.

Theorem 3.1 If $\widetilde{\mathcal{D}_k} = \mathcal{D}_k$ and $\tilde{k} = k + 1$, Fig. 2 describes a QA-NIZK proof system with perfect completeness, computational adaptive soundness based on the $\mathcal{D}_k$-SKerMDH Assumption, and perfect zero-knowledge. ∎

Theorem 3.2 If $\widetilde{\mathcal{D}_k} = \overline{\mathcal{D}}_k$ and $\tilde{k} = k$, and $\mathcal{D}_\Gamma$ is a witness samplable distribution, Fig. 2 describes a QA-NIZK proof system with perfect completeness, computational adaptive soundness based on the $\mathcal{D}_k$-SKerMDH Assumption, and perfect zero-knowledge. ∎

3.2 Argument of Sum in Subspace

We can adapt the previous construction to the *Sum in Subspace* Language,

$$\mathcal{L}_{\hat{\mathbf{M}}, \check{\mathbf{N}}, +} := \{(\hat{\mathbf{x}}, \check{\mathbf{y}}) \in \hat{\mathbb{G}}^m \times \check{\mathbb{H}}^m : \exists \mathbf{w} \in \mathbb{Z}_q^t,\ \mathbf{x} + \mathbf{y} = (\mathbf{M} + \mathbf{N})\mathbf{w}\}.$$

We define two proof systems $\Psi_{\mathcal{D}_k, +}$, $\Psi_{\overline{\mathcal{D}}_k, +}$ as in Fig. 2, but now with $\mathbf{\Lambda} = \mathbf{\Xi}$. Intuitively, soundness follows from the same argument because the information about $\mathbf{\Lambda}$ in the CRS is now $\mathbf{\Lambda}^\top \mathbf{A}, \mathbf{\Lambda}(\mathbf{M} + \mathbf{N})$.

3.3 Argument of Equal Opening in Different Groups

Given the results for Subspace Concatenation of Sect. 3.1, it is direct to construct constant-size NIZK Arguments of membership in:

$$\mathcal{L}_{\mathsf{com},\hat{\mathbf{U}},\check{\mathbf{V}},\nu} := \left\{(\hat{\mathbf{c}},\check{\mathbf{d}}) \in \hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n : \exists(\mathbf{w},\mathbf{r},\mathbf{s}), \hat{\mathbf{c}} = \hat{\mathbf{U}}\begin{pmatrix}\mathbf{w}\\ \mathbf{r}\end{pmatrix}, \check{\mathbf{d}} = \check{\mathbf{V}}\begin{pmatrix}\mathbf{w}\\ \mathbf{s}\end{pmatrix}\right\},$$

where $\hat{\mathbf{U}} \in \hat{\mathbb{G}}^{m\times\tilde{m}}$, $\check{\mathbf{V}} \in \check{\mathbb{H}}^{n\times\tilde{n}}$ and $\mathbf{w} \in \mathbb{Z}_q^{\nu}$. The witness is $(\mathbf{w},\mathbf{r},\mathbf{s}) \in \mathbb{Z}_q^{\nu} \times \mathbb{Z}_q^{\tilde{m}-\nu} \times \mathbb{Z}_q^{\tilde{n}-\nu}$. This language is interesting because it can express the fact that $(\hat{\mathbf{c}},\check{\mathbf{d}})$ are commitments to the same vector $\mathbf{w} \in \mathbb{Z}_q^{\nu}$ in different groups.

The construction is an immediate consequence of the observation that $\mathcal{L}_{\mathsf{com},\hat{\mathbf{U}},\check{\mathbf{V}},\nu}$ can be rewritten as some concatenation language $\mathcal{L}_{\hat{\mathbf{M}},\check{\mathbf{N}}}$. Denote by $\hat{\mathbf{U}}_1$ the first ν columns of $\hat{\mathbf{U}}$ and $\hat{\mathbf{U}}_2$ the remaining ones, and $\check{\mathbf{V}}_1$ the first ν columns of $\check{\mathbf{V}}$ and $\check{\mathbf{V}}_2$ the remaining ones. If we define:

$$\hat{\mathbf{M}} := (\hat{\mathbf{U}}_1||\hat{\mathbf{U}}_2||\hat{\mathbf{0}}_{m\times(\tilde{n}-\nu)}) \qquad \check{\mathbf{N}} := (\check{\mathbf{V}}_1||\check{\mathbf{0}}_{n\times(\tilde{m}-\nu)}||\check{\mathbf{V}}_2).$$

then it is immediate to verify that $\mathcal{L}_{\mathsf{com},\hat{\mathbf{U}},\check{\mathbf{V}},\nu} = \mathcal{L}_{\hat{\mathbf{M}},\check{\mathbf{N}}}$.

In the rest of the paper, we denote as $\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}$ the proof system for $\mathcal{L}_{\mathsf{com},\hat{\mathbf{U}},\check{\mathbf{V}},\nu}$ which corresponds to $\Psi_{\overline{\mathcal{D}}_k,\mathsf{spl}}$ for $\mathcal{L}_{\hat{\mathbf{M}},\check{\mathbf{N}}}$, where $\hat{\mathbf{M}},\check{\mathbf{N}}$ are the matrices defined above. Note that for commitment schemes we can generally assume $\hat{\mathbf{U}},\check{\mathbf{V}}$ to be drawn from some witness samplable distribution.

4 Aggregating Groth-Sahai Proofs in Asymmetric Groups

In this section we discuss two different ways to aggregate GS equations. The first is a direct application of the proof of equal commitment opening and is only valid for two-sided linear equations in $\mathbb{Z}_q$, the second is an extension of the results of Jutla and Roy for all other types of linear equations.

4.1 Aggregating Two-Sided Linear Equations in $\mathbb{Z}_q$

We note that proving that n pairs of GS commitments open (pairwise) to the same elements in $\mathbb{Z}_q$ is simply a special case of the proof of equal commmitment opening in Sect. 3.3. Indeed, the concatenation of n GS commitments is just a commitment to a vector of scalars. In particular, given $\mathsf{crs}_{\mathrm{GS}} = (\Gamma,\hat{\mathbf{u}}_1,\hat{\mathbf{u}}_2,\check{\mathbf{v}}_1,\check{\mathbf{v}}_2)$, it is easy to see that n commitments to $x_i \in \mathbb{Z}_q$, which are of the form: $\hat{\mathbf{c}}_i = x_i\hat{\mathbf{u}}_1 + r_i\hat{\mathbf{u}}_2$ for some $r_i \in \mathbb{Z}_q$ (recall that $\iota_1(x_i) = x_i\hat{\mathbf{u}}_1$), can be written as

$$\begin{pmatrix}\hat{\mathbf{c}}_1\\ \vdots\\ \hat{\mathbf{c}}_n\end{pmatrix} = \begin{pmatrix}\hat{\mathbf{u}}_1 & \dots & \hat{\mathbf{0}}\\ \vdots & \ddots & \vdots\\ \hat{\mathbf{0}} & \dots & \hat{\mathbf{u}}_1\end{pmatrix}\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix} + \begin{pmatrix}\hat{\mathbf{u}}_2 & \dots & \hat{\mathbf{0}}\\ \vdots & \ddots & \vdots\\ \hat{\mathbf{0}} & \dots & \hat{\mathbf{u}}_2\end{pmatrix}\begin{pmatrix}r_1\\ \vdots\\ r_n\end{pmatrix},$$

and similarly the concatenation of n commitments $\check{\mathbf{d}}_i$, $i \in [\ell]$ can be written as $\check{\mathbf{V}}_1\mathbf{y} + \check{\mathbf{V}}_2\mathbf{s}$, where $\hat{\mathbf{V}}_i$ is the blockwise concatenation of n copies of $\check{\mathbf{v}}_i$.

In particular, proving that n GS commitments open to the same value can be also seen as the

aggregation of the proof of n GS equations of the form $\mathsf{x}_\ell - \mathsf{y}_\ell = 0$. The aggregation of any other set of two-sided linear equations in $\mathbb{Z}_q$ easily reduces to this case using the homomorphic properties of GS commitments. Indeed, given n equations of the form:

$$\boldsymbol{\alpha}_\ell^\top \mathsf{y} + \mathsf{x}^\top \boldsymbol{\beta}_\ell = t_\ell,\ \ell \in [n],$$

and the commitments to a satisfying assignment (where the commitments to every coordinate of x (resp. y) are in $\hat{\mathbb{G}}$ (resp. $\check{\mathbb{H}}$), it is easy to derive a commitment to $\mathsf{x}^\top \boldsymbol{\beta}_\ell - t_\ell$ in $\hat{\mathbb{G}}$ and a commitment to $\boldsymbol{\alpha}_\ell^\top \mathsf{y}$ in $\check{\mathbb{H}}$ for all $\ell \in [n]$. Obviously, the equations are satisfied if for each ℓ, these commitments open to the same value.

We insist that two-sided linear equations in $\mathbb{Z}_q$ are essential to prove quadratic statements in asymmetric bilinear groups. In particular, this result can be used to reduce the proof size that n commitments open to a bit-string from $6n(\mathfrak{g}+\mathfrak{h})$ to $(4n+2)(\mathfrak{g}+\mathfrak{h})$.

4.2 QA Aggregation of Other Equation Types

Jutla and Roy [23] show how to aggregate GS proofs of two-sided linear equations in symmetric bilinear groups. In the original construction of [23] soundness is based on a decisional assumption (a weaker variant of the 2-Lin Assumption). Its natural generalization in asymmetric groups (where soundness is based on the SXDH Assumption) only enables to aggregate the proofs of one-sided linear equations.

In this section, we revisit their construction. We give an alternative, simpler, proof of soundness under a computational assumption which avoids altogether the "Switching Lemma" of [23]. Further, we extend it to two-sided equations in the asymmetric setting. For one-sided linear equations we can prove soundness under any kernel assumption and for two-sided linear equations, under any split kernel assumption.[2]

Let A_1, A_2, A_T be $\mathbb{Z}_q$-vector spaces compatible with some Groth-Sahai equation as detailed in Sect. 2.2. Let $\mathcal{D}_\Gamma$ be a witness samplable distribution which outputs n pairs of vectors $(\vec{\alpha}_\ell, \vec{\beta}_\ell) \in A_1^{m_y} \times A_2^{m_x}$, $\ell \in [n]$, for some $m_x, m_y \in \mathbb{N}$. Given some fixed pairs $(\vec{\alpha}_\ell, \vec{\beta}_\ell)$, we define, for each $\tilde{\mathbf{t}} \in A_T^n$, the set of equations $\mathcal{S}_{\tilde{\mathbf{t}}}$ as:

$$\mathcal{S}_{\tilde{\mathbf{t}}} = \left\{ E_\ell(\vec{\mathsf{x}}, \vec{\mathsf{y}}) = \tilde{t}_\ell : \ell \in [n] \right\}, \qquad E_\ell(\vec{\mathsf{x}}, \vec{\mathsf{y}}) := \sum_{j \in [m_y]} f(\alpha_{\ell,j}, \mathsf{y}_j) + \sum_{i \in [m_x]} f(\mathsf{x}_i, \beta_{\ell,i}).$$

We note that, as in [23], we only achieve *quasi-adaptive aggregation*, that is, the common reference string is specific to a particular set of equations. More specifically, it depends on the constants $\boldsymbol{\alpha}_\ell, \boldsymbol{\beta}_\ell$ (but not on $\tilde{t}_\ell$, which can be chosen by the prover) and it can be used to aggregate the proofs of $\mathcal{S}_{\tilde{\mathbf{t}}}$, for any $\tilde{\mathbf{t}}$.

Given the equation types for which we can construct NIZK GS proofs, there always exists (1) $t_\ell \in A_1$, such that $\tilde{t}_\ell = f(t_\ell, \mathsf{base}_2)$ or (2) $\tilde{t}_\ell \in A_2$, such that $\tilde{t}_\ell = f(\mathsf{base}_1, t_\ell)$, where $\mathsf{base}_i = 1$ if $A_i = \mathbb{Z}_q$, $\mathsf{base}_1 = \hat{g}$ if $A_1 = \hat{\mathbb{G}}$ and $\mathsf{base}_2 = \check{h}$ if $A_2 = \check{\mathbb{H}}$. This is because $\tilde{t}_\ell = 0_{\mathbb{T}}$ for PPEs, and $A_T = A_i$, for some $i \in [2]$, for other types of equations. For simplicity, in the construction we assume that (1) is the case, otherwise change $\iota_2(a_{\ell,i}), \iota_1(t_\ell)$ for $\iota_1(a_{\ell,i}), \iota_2(t_\ell)$ in the construction

[2]The results of [23] are based on what they call the "Switching Lemma". As noted in [30], it is implicit in the proof of this lemma that the same results can be obtained under computational assumptions.

below.

$\mathsf{K}_0(1^\lambda)$**:** Return $\Gamma := (q, \hat{\mathbb{G}}, \check{\mathbb{H}}, \mathbb{T}, e, \hat{g}, \check{h}) \leftarrow \mathsf{Gen}_a(1^\lambda)$.

$\mathcal{D}_\Gamma$**:** $\mathcal{D}_\Gamma$ is some distribution over n pairs of vectors $(\boldsymbol{\alpha}_\ell, \boldsymbol{\beta}_\ell) \in A_1^{m_x} \times A_2^{m_y}$.

$\mathsf{K}_1(\Gamma, \mathcal{S}_{\tilde{\mathbf{t}}})$**:** Let $\mathbf{A} = (a_{i,j}) \leftarrow \mathcal{D}_{n,k}$. Define

$$\mathsf{crs} := \left(\mathsf{crs}_{\mathrm{GS}}, \left\{ \sum_{\ell \in [n]} \iota_1(a_{\ell,i}\boldsymbol{\alpha}_\ell), \sum_{\ell \in [n]} \iota_2(a_{\ell,i}\boldsymbol{\beta}_\ell), \left\{ \iota_2(a_{\ell,i}) : \ell \in [n] \right\} : i \in [k] \right\} \right)$$

$\mathsf{P}(\Gamma, \mathcal{S}_{\tilde{\mathbf{t}}}, \mathbf{x}, \mathbf{y})$**:** Given a solution $\vec{\mathsf{x}} = \mathbf{x}$, $\vec{\mathsf{y}} = \mathbf{y}$ to $\mathcal{S}_{\tilde{\mathbf{t}}}$, the prover proceeds as follows:

- Commit to all $x_j \in A_1$ as $\hat{\mathbf{c}}_j \leftarrow \mathsf{Comm}_{\mathrm{GS}}(x_j)$, and to all $\mathsf{y}_j \in A_2$ as $\check{\mathbf{d}}_j \leftarrow \mathsf{Comm}_{\mathrm{GS}}(y_j)$.
- For each $i \in [k]$, run the GS prover for the equation $\sum_{\ell \in [n]} a_{\ell,i} E_\ell(\vec{\mathsf{x}}, \vec{\mathsf{y}}) = \sum_{\ell \in [n]} f(t_\ell, a_{\ell,i})$ to obtain the proof, which is a pair $(\hat{\boldsymbol{\Theta}}_i, \check{\boldsymbol{\Pi}}_i)$.

Output $(\{\hat{\mathbf{c}}_j : j \in [m_x]\}, \{\check{\mathbf{d}}_j : j \in [m_y]\}, \{(\check{\boldsymbol{\Pi}}_i, \hat{\boldsymbol{\Theta}}_i) : i \in [k]\})$.

$\mathsf{V}(\mathsf{crs}, \mathcal{S}_{\tilde{\mathbf{t}}}, \{\hat{\mathbf{c}}_j\}_{j \in [m_x]}, \{\check{\mathbf{d}}_j\}_{j \in [m_y]}, \{\hat{\boldsymbol{\Theta}}_i, \check{\boldsymbol{\Pi}}_i\}_{i \in [k]})$**:** For each $i \in [k]$, run the GS verifier for equation

$$\sum_{\ell \in [n]} a_{\ell,i} E_\ell(\vec{\mathsf{x}}, \vec{\mathsf{y}}) = \sum_{\ell \in [n]} f(t_\ell, a_{\ell,i}).$$

Theorem 4.1 The above protocol is a QA-NIZK proof system for two-sided linear equations. ∎

Proof: Completeness. Observe that

$$\sum_{\ell \in [n]} a_{\ell,i} E_\ell(\vec{\mathsf{x}}, \vec{\mathsf{y}}) = \sum_{j \in [m_y]} f(a_{\ell,i}\alpha_{\ell,j}, \mathsf{y}_j) + \sum_{j \in [m_x]} f(\mathsf{x}_j, a_{\ell,i}\beta_{\ell,j}). \tag{2}$$

Completeness follows from the observation that to efficiently compute the proof, the GS Prover [19] only needs, apart from a satisfying assignment to the equation, the randomness used in the commitments plus a way to compute the inclusion map of all involved constants, in this case $\iota_1(a_{\ell,i}\alpha_{\ell,j})$, $\iota_2(a_{\ell,i}\beta_{\ell,j})$ and the latter is part of the CRS.

Soundness. We change to a game Game_1 where we know the discrete logarithm of the GS commitment key, as well as the discrete logarithms of $(\boldsymbol{\alpha}_\ell, \boldsymbol{\beta}_\ell)$, $\ell \in [n]$. This is possible because they are both chosen from a witness samplable distribution.

We now prove that an adversary against the soundness in Game_1 can be used to construct an adversary B against the $\mathcal{D}_{n,k}$-SKerMDH Assumption, where $\mathcal{D}_{n,k}$ is the matrix distribution used in the CRS generation.

B receives a challenge $(\hat{\mathbf{A}}, \check{\mathbf{A}}) \in \hat{\mathbb{G}}^{n \times k} \times \check{\mathbb{H}}^{n \times k}$. Given all the discrete logarithms that B knows, it can compute a properly distributed CRS even without knowledge of the discrete logarithm of $\hat{\mathbf{A}}$. The soundness adversary outputs commitments $\{\hat{\mathbf{c}}_j\}_{j \in [m_x]}, \{\check{\mathbf{d}}_j\}_{j \in [m_y]}$ together with proofs $\{\hat{\boldsymbol{\Theta}}_i, \check{\boldsymbol{\Pi}}_i\}_{i \in [k]}$, which are accepted by the verifier.

Let $\mathbf{x}$ (resp. $\hat{\mathbf{x}}$) be the vector of openings of $\{\hat{\mathbf{c}}_j\}_{j\in[m_x]}$ in A_1 (resp. in the group $\hat{\mathbb{G}}$) and $\mathbf{y}$ (resp. $\check{\mathbf{y}}$) the vector of openings of $\{\check{\mathbf{d}}_j\}_{j\in[m_y]}$ in A_2 (resp. in the group $\check{\mathbb{H}}$). If $A_1 = \hat{\mathbb{G}}$ (resp. $A_2 = \check{\mathbb{H}}$) then $\mathbf{x} = \hat{\mathbf{x}}$ (resp. $\mathbf{y} = \check{\mathbf{y}}$). The vectors $\hat{\mathbf{x}}$ and $\check{\mathbf{y}}$ are efficiently computable by B who knows the discrete logarithm of the commitment keys. We claim that the pair $(\hat{\boldsymbol{\rho}}, \check{\boldsymbol{\sigma}}) \in \hat{\mathbb{G}}^n \times \check{\mathbb{H}}^n$, $\hat{\boldsymbol{\rho}} := (\boldsymbol{\beta}_1^\top \hat{\mathbf{x}} - \hat{t}_1, \ldots, \boldsymbol{\beta}_n^\top \hat{\mathbf{x}} - \hat{t}_n), \check{\boldsymbol{\sigma}} := (\boldsymbol{\alpha}_1^\top \check{\mathbf{y}}, \ldots, \boldsymbol{\alpha}_n^\top \check{\mathbf{y}})$, solves the $\mathcal{D}_{n,k}$-$\mathsf{SKerMDH}$ challenge.

First, observe that if the adversary is successful in breaking the soundness property, then $\boldsymbol{\rho} \neq \boldsymbol{\sigma}$. Indeed, if this is the case there is some index $\ell \in [n]$ such that $E_\ell(\mathbf{x}, \mathbf{y}) \neq \tilde{t}_\ell$, which means that $\sum_{j\in[m_y]} f(\alpha_{\ell,j}, \mathsf{y}_j) \neq \sum_{j\in[m_x]} f(\mathsf{x}_j, \beta_{\ell,j}) - f(t_\ell, \mathsf{base}_2)$. If we take discrete logarithms in each side of the equation, this inequality is exactly equivalent to $\boldsymbol{\rho} \neq \boldsymbol{\sigma}$.

Further, because GS proofs have perfect soundness, $\mathbf{x}$ and $\mathbf{y}$ satisfy the equation $\sum_{\ell\in[n]} a_{\ell,i} E_\ell(\vec{\mathsf{x}}, \vec{\mathsf{y}}) = \sum_{\ell\in[n]} f(t_\ell, a_{\ell,i})$, for all $i \in [k]$, Thus, for all $i \in [k]$,

$$\sum_{\ell\in[n]} \check{a}_{\ell,i} \left(\boldsymbol{\beta}_\ell^\top \hat{\mathbf{x}} - \hat{t}_\ell\right) = \sum_{\ell\in[n]} \hat{a}_{\ell,i} \left(\boldsymbol{\alpha}_\ell^\top \check{\mathbf{y}}\right), \tag{3}$$

which implies that $\hat{\boldsymbol{\rho}}\check{\mathbf{A}} = \check{\boldsymbol{\sigma}}\hat{\mathbf{A}}$.

Zero-Knowledge. The same simulator of GS proofs can be used. Specifically the simulated proof corresponds to k simulated GS proofs. ∎

4.2.1 One-Sided Equations.

In the case when $\boldsymbol{\alpha}_\ell = \mathbf{0}$ and $\tilde{t}_\ell = f(t_\ell, \mathsf{base}_2)$ for some $t_\ell \in A_1$, for all $\ell \in [n]$, proofs can be aggregated under a standard Kernel Assumption (and thus, in asymmetric bilinear groups we can choose $k = 1$). Indeed, in this case, in the soundness proof, the adversary B receives $\check{\mathbf{A}} \in \check{\mathbb{H}}^{n\times k}$, an instance of the $\mathcal{D}_{n,k} - \mathsf{KerMDH}_{\check{\mathbb{H}}}$ problem. The adversary B outputs $\hat{\boldsymbol{\rho}} := (\boldsymbol{\beta}_1^\top \hat{\mathbf{x}} - \hat{t}_1, \ldots, \boldsymbol{\beta}_n^\top \hat{\mathbf{x}} - \hat{t}_n)$ as a solution to the challenge. To see why this works, note that, when $\boldsymbol{\alpha}_\ell = \mathbf{0}$ for all $\ell \in [n]$, equation (3) reads $\sum_{\ell\in[n]} \check{a}_{\ell,i} \left(\boldsymbol{\beta}_\ell^\top \hat{\mathbf{x}} - \hat{\mathbf{t}}_\ell\right) = \mathbf{0}_\mathbb{T}$ and thus $\hat{\boldsymbol{\rho}}\check{\mathbf{A}} = \mathbf{0}_\mathbb{T}$. The case when $\boldsymbol{\beta}_\ell = \mathbf{0}$ and $\tilde{t}_\ell = f(\mathsf{base}_1, t_\ell)$ for some $t_\ell \in A_2$, for all $\ell \in [n]$, is analogous.

4.2.2 Public Parameters.

The size of the CRS of the construction above depends on the number of elements needed to represent $\hat{\mathbf{A}}$. In this sense, it is interesting to sample $\hat{\mathbf{A}}$ from some family of matrix assumptions with good representation size. As we assume that $n > k$, it is interesting to instantiate this scheme with the *Circulant Matrix Distribution* of [30], which has a representation size of n — independent of k.

5 QA-NIZK Arguments for Bit-Strings

We construct a constant-size QA-NIZK for proving that a perfectly binding commitment opens to a bit-string. That is, we prove membership in the language:

$$\mathcal{L}_{\hat{\mathbf{U}},\mathsf{bits}} := \{\hat{\mathbf{c}} \in \hat{\mathbb{G}}^{n+m} : \hat{\mathbf{c}} := \hat{\mathbf{U}}_1\mathbf{b} + \hat{\mathbf{U}}_2\mathbf{w}, (\mathbf{b}, \mathbf{w}) \in \{0,1\}^n \times \mathbb{Z}_q^m\},$$

where $\hat{\mathbf{U}} := (\hat{\mathbf{U}}_1, \hat{\mathbf{U}}_2) \in \hat{\mathbb{G}}^{(n+m)\times n} \times \hat{\mathbb{G}}^{(n+m)\times m}$ defines perfectly binding and computationally hiding commitment keys. The witness for membership is $(\mathbf{b}, \mathbf{w})$ and $\hat{\mathbf{U}} \leftarrow \mathcal{D}_\Gamma$, where $\mathcal{D}_\Gamma$ is some witness samplable distribution.

To prove that a commitment in $\hat{\mathbb{G}}$ opens to a vector of bits $\mathbf{b}$, the usual strategy is to compute another commitment $\check{\mathbf{d}} \in \check{\mathbb{H}}^{\bar{n}}$ to a vector $\bar{\mathbf{b}} \in \mathbb{Z}_q^n$ and prove (1) $b_i(\bar{b}_i - 1) = 0$, for all $i \in [n]$, and (2) $b_i - \bar{b}_i = 0$, for all $i \in [n]$. For statement (2), since $\hat{\mathbf{U}}$ is witness samplable, we can use our most efficient QA-NIZK from Sect. 3.3 for equal opening in different groups. Under the SSDP Assumption, which is the $\mathsf{SKerMDH}$ Assumption of minimal size conjectured to hold in asymmetric groups, the proof is of size $2(\mathfrak{g} + \mathfrak{h})$. Thus, the challenge is to aggregate n equations of the form $b_i(\bar{b}_i - 1) = 0$. We note that this is a particular case of the problem of aggregating proofs of quadratic equations, which was left open in [23].

We finally remark that the proof must include $\check{\mathbf{d}}$ and thus it may be not of size independent of n. However, it turns out that $\check{\mathbf{d}}$ needs not be perfectly binding, in fact $\bar{n} = 2$ suffices.

5.1 Intuition

A prover wanting to show satisfiability of the equation $\mathsf{x}(\mathsf{y} - 1) = 0$ using GS proofs, will commit to a solution $\mathsf{x} = b$ and $\mathsf{y} = \bar{b}$ as $\hat{\mathbf{c}} = b\hat{\mathbf{u}}_1 + r\hat{\mathbf{u}}_2$ and $\check{\mathbf{d}} = \bar{b}\check{\mathbf{v}}_1 + s\check{\mathbf{v}}_2$, for $r, s \leftarrow \mathbb{Z}_q$, and then give a pair $(\hat{\boldsymbol{\theta}}, \check{\boldsymbol{\pi}}) \in \hat{\mathbb{G}}^2 \times \check{\mathbb{H}}^2$ which satisfies the following verification equation[3]:

$$\hat{\mathbf{c}} \left(\check{\mathbf{d}} - \check{\mathbf{v}}_1\right)^\top = \hat{\mathbf{u}}_2 \check{\boldsymbol{\pi}}^\top + \hat{\boldsymbol{\theta}} \check{\mathbf{v}}_2^\top. \tag{4}$$

The reason why this works is that, if we express both sides of the equation in the basis of $\mathbb{T}^{2\times 2}$ given by $\{\hat{\mathbf{u}}_1\check{\mathbf{v}}_1^\top, \hat{\mathbf{u}}_2\check{\mathbf{v}}_1^\top, \hat{\mathbf{u}}_1\check{\mathbf{v}}_2^\top, \hat{\mathbf{u}}_2\check{\mathbf{v}}_2^\top\}$, the coefficient of $\hat{\mathbf{u}}_1\check{\mathbf{v}}_1^\top$ is $b(\bar{b}-1)$ on the left side and 0 on the right side (regardless of $(\hat{\boldsymbol{\theta}}, \check{\boldsymbol{\pi}})$). Our observation is that the verification equation can be abstracted as saying:

$$\hat{\mathbf{c}} \left(\check{\mathbf{d}} - \check{\mathbf{v}}_1\right)^\top \in \mathsf{Span}(\hat{\mathbf{u}}_2\check{\mathbf{v}}_1^\top, \hat{\mathbf{u}}_1\check{\mathbf{v}}_2^\top, \hat{\mathbf{u}}_2\check{\mathbf{v}}_2^\top) \subset \mathbb{T}^{2\times 2}. \tag{5}$$

Now consider commitments to $(b_1, \ldots, b_n)$ and $(\bar{b}_1, \ldots, \bar{b}_n)$ constructed with some commitment key $\{(\hat{\mathbf{g}}_i, \check{\mathbf{h}}_i) : i \in [n+1]\} \subset \hat{\mathbb{G}}^{\overline{n}} \times \check{\mathbb{H}}^{\overline{n}}$, for some $\overline{n} \in \mathbb{N}$, to be determined later, and defined as $\hat{\mathbf{c}} := \sum_{i\in[n]} b_i\hat{\mathbf{g}}_i + r\hat{\mathbf{g}}_{n+1}$, $\check{\mathbf{d}} := \sum_{i\in[n]} \bar{b}_i\check{\mathbf{h}}_i + s\check{\mathbf{h}}_{n+1}$, $r, s \leftarrow \mathbb{Z}_q$. Suppose for a moment that $\{\hat{\mathbf{g}}_i\check{\mathbf{h}}_j^\top : i, j \in [n+1]\}$ is a set of linearly independent vectors. Then,

$$\hat{\mathbf{c}} \left(\check{\mathbf{d}}^\top - \sum_{j\in[n]} \check{\mathbf{h}}_j^\top\right) \in \mathsf{Span}\{\hat{\mathbf{g}}_i\check{\mathbf{h}}_j^\top : (i,j) \in \mathcal{I}_{n,1}\} \tag{6}$$

if and only if $b_i(\bar{b}_i - 1) = 0$ for all $i \in [n]$, because $b_i(\bar{b}_i - 1)$ is the coordinate of $\hat{\mathbf{g}}_i\check{\mathbf{h}}_i^\top$ in the left side of the equation.

Equation 6 suggests to use one of the constant-size QA-NIZK Arguments for linear spaces to get a constant-size proof that $b_i(\bar{b}_i - 1) = 0$ for all $i \in [n]$. Unfortunately, these arguments are only defined for membership in subspaces in $\hat{\mathbb{G}}^m$ or $\check{\mathbb{H}}^m$ but not in $\mathbb{T}^m$. Our solution is to include information in the CRS to "bring back" this statement from $\mathbb{T}$ to $\hat{\mathbb{G}}$, i.e. the matrices $\hat{\mathbf{C}}_{i,j} := \hat{\mathbf{g}}_i\mathbf{h}_j^\top$, for each $(i,j) \in \mathcal{I}_{n,1}$. Then, to prove that $b_i(\bar{b}_i - 1) = 0$ for all $i \in [n]$, the prover computes $\hat{\boldsymbol{\Theta}}_{b(\bar{b}-1)}$

[3]For readers familiar with the Groth-Sahai notation, equation (4) corresponds to $\mathbf{c} \bullet (\mathbf{d} - \iota_2(1)) = \mathbf{u}_2 \bullet \boldsymbol{\pi} + \boldsymbol{\theta} \bullet \mathbf{v}_2$.

as a linear combination of $\mathcal{C} := \{\hat{\mathbf{C}}_{i,j} : (i,j) \in \mathcal{I}_{n,1}\}$ (with coefficients which depend on $\mathbf{b}, \overline{\mathbf{b}}, r, s$) such that

$$\hat{\mathbf{c}} \left(\check{\mathbf{d}} - \sum_{j \in [n]} \check{\mathbf{h}}_j \right)^\top = \hat{\mathbf{\Theta}}_{b(\bar{b}-1)} \check{\mathbf{I}}_{\overline{n} \times \overline{n}}, \tag{7}$$

and gives a QA-NIZK proof of $\hat{\mathbf{\Theta}}_{b(\bar{b}-1)} \in \mathsf{Span}(\mathcal{C})$.

This reasoning assumes that $\{\hat{\mathbf{g}}_i \mathbf{h}_j^\top\}$ (or equivalently, $\{\hat{\mathbf{C}}_{i,j}\}$) are linearly independent, which can only happen if $\overline{n} \geq n+1$. If that is the case, the proof cannot be constant because $\hat{\mathbf{\Theta}}_{b(\bar{b}-1)} \in \hat{\mathbb{G}}^{\overline{n} \times \overline{n}}$ and this matrix is part of the proof. Instead, we choose $\hat{\mathbf{g}}_1, \ldots, \hat{\mathbf{g}}_{n+1} \in \hat{\mathbb{G}}^2$ and $\check{\mathbf{h}}_1, \ldots, \check{\mathbf{h}}_{n+1} \in \check{\mathbb{H}}^2$, so that $\{\hat{\mathbf{C}}_{i,j}\} \subseteq \hat{\mathbb{G}}^{2 \times 2}$. Intuitively, this should still work because the prover receives these vectors as part of the CRS and he does not know their discrete logarithms, so to him, they behave as linearly independent vectors.

With this change, the statement $\hat{\mathbf{\Theta}}_{b(\bar{b}-1)} \in \mathsf{Span}(\mathcal{C})$ seems no longer meaningful, as $\mathsf{Span}(\mathcal{C})$ is all of $\hat{\mathbb{G}}^{2 \times 2}$ with overwhelming probability. But this is not the case, because by means of decisional assumptions in $\hat{\mathbb{G}}^2$ and in $\check{\mathbb{H}}^2$, we switch to a game where the matrices $\hat{\mathbf{C}}_{i,j}$ span a non-trivial space of $\hat{\mathbb{G}}^{2 \times 2}$. Specifically, to a game where $\hat{\mathbf{C}}_{i^*,i^*} \notin \mathsf{Span}(\mathcal{C})$ and $i^* \leftarrow [n]$ remains hidden to the adversary. Once we are in such a game, perfect soundness is guaranteed for equation $b_{i^*}(\bar{b}_{i^*} - 1) = 0$ and a cheating adversary is caught with probability at least $1/n$. We think this technique might be of independent interest.

The last obstacle is that, using decisional assumptions on the set of vectors $\{\check{\mathbf{h}}_j\}_{j \in [n+1]}$ is incompatible with using the discrete logarithms of $\check{\mathbf{h}}_j$ to compute the matrices $\hat{\mathbf{C}}_{i,j} := \hat{\mathbf{g}}_i \mathbf{h}_j^\top$ given in the CRS. To account for the fact that, in some games, we only know $\mathbf{g}_i \in \mathbb{Z}_q$ and, in some others, only $\mathbf{h}_j \in \mathbb{Z}_q$, we replace each matrix $\hat{\mathbf{C}}_{i,j}$ by a pair $(\hat{\mathbf{C}}_{i,j}, \check{\mathbf{D}}_{i,j})$ which is uniformly distributed conditioned on $\mathbf{C}_{i,j} + \mathbf{D}_{i,j} = \mathbf{g}_i \mathbf{h}_j^\top$. This randomization completely hides the group in which we can compute $\mathbf{g}_i \mathbf{h}_j^\top$. Finally, we use our QA-NIZK Argument for sum in a subspace (Sect. 3.2) to prove membership in this space.

5.2 Instantiations

We discuss in detail two particular cases of languages $\mathcal{L}_{\hat{\mathbf{U}},\mathsf{bits}}$. First, in Sect. 5.3 we discuss the case when

(a) $\hat{\mathbf{c}}$ is a vector in $\hat{\mathbb{G}}^{n+1}$, $\hat{\mathbf{u}}_{n+1} \leftarrow \mathcal{L}_{n+1,1}$ and $\hat{\mathbf{U}}_1 := \begin{pmatrix} \hat{\mathbf{I}}_{n \times n} \\ \hat{\mathbf{0}}_{1 \times n} \end{pmatrix} \in \hat{\mathbb{G}}^{(n+1) \times n}$, $\hat{\mathbf{U}}_2 := \hat{\mathbf{u}}_{n+1} \in \hat{\mathbb{G}}^{n+1}$, $\hat{\mathbf{U}} = (\hat{\mathbf{U}}_1 || \hat{\mathbf{U}}_2)$.

In this case, the vectors $\hat{\mathbf{g}}_i$ in the intuition are defined as $\hat{\mathbf{g}}_i = \mathbf{\Delta} \hat{\mathbf{u}}_i$, where $\mathbf{\Delta} \leftarrow \mathbb{Z}_q^{2 \times (n+1)}$, and the commitment to $\mathbf{b}$ is computed as $\hat{\mathbf{c}} := \sum_{i \in [n]} b_i \hat{\mathbf{u}}_i + w \hat{\mathbf{u}}_{n+1}$. Then in Sect. 5.5.1 we discuss how to generalize the construction for a) to

(b) $\hat{\mathbf{c}}$ is the concatenation of n GS commitments. That is, given the GS CRS $\mathsf{crs}_{\mathrm{GS}} = (\Gamma, \hat{\mathbf{u}}_1, \hat{\mathbf{u}}_2, \check{\mathbf{v}}_1, \check{\mathbf{v}}_2)$,

we define,

$$\hat{\mathbf{U}}_1 := \begin{pmatrix} \hat{\mathbf{u}}_1 & \dots & \hat{\mathbf{0}} \\ \vdots & \ddots & \vdots \\ \hat{\mathbf{0}} & \dots & \hat{\mathbf{u}}_1 \end{pmatrix} \in \hat{\mathbb{G}}^{2n\times n}, \hat{\mathbf{U}}_2 := \begin{pmatrix} \hat{\mathbf{u}}_2 & \dots & \hat{\mathbf{0}} \\ \vdots & \ddots & \vdots \\ \hat{\mathbf{0}} & \dots & \hat{\mathbf{u}}_2 \end{pmatrix} \in \hat{\mathbb{G}}^{2n\times n}.$$

Although the proof size is constant, in both of our instantiations the commitment size is $\Theta(n)$. Specifically, $(n+1)\mathfrak{g}$ for case a) and $2n\mathfrak{g}$ for case b).

5.3 The Scheme

$\mathsf{K}_0(1^\lambda)$**:** Return $\Gamma := (q, \hat{\mathbb{G}}, \check{\mathbb{H}}, \mathbb{T}, e, \hat{g}, \check{h}) \leftarrow \mathsf{Gen}_a(1^\lambda)$.

$\mathcal{D}_\Gamma$**:** The distribution $\mathcal{D}_\Gamma$ over $\hat{\mathbb{G}}^{(n+1)\times(n+1)}$ is some witness samplable distribution which defines the relation $\mathcal{R}_\Gamma = \{\mathcal{R}_{\hat{\mathbf{U}}}\} \subseteq \hat{\mathbb{G}}^{n+1} \times (\{0,1\}^n \times \mathbb{Z}_q)$, where $\hat{\mathbf{U}} \leftarrow \mathcal{D}_\Gamma$, such that $(\hat{\mathbf{c}}, \langle \mathbf{b}, w\rangle) \in \mathcal{R}_{\hat{\mathbf{U}}}$ iff $\hat{\mathbf{c}} = \hat{\mathbf{U}}\binom{\mathbf{b}}{w}$. The relation $\mathcal{R}_{par}$ consists of pairs $(\hat{\mathbf{U}}, \mathbf{U})$ where $\hat{\mathbf{U}} \leftarrow \mathcal{D}_\Gamma$.

$\mathsf{K}_1(\Gamma, \hat{\mathbf{U}})$**:** Let $\mathbf{h}_{n+1} \leftarrow \mathbb{Z}_q^2$ and for all $i \in [n]$, $\mathbf{h}_i := \epsilon_i \mathbf{h}_{n+1}$, where $\epsilon_i \leftarrow \mathbb{Z}_q$. Define $\check{\mathbf{H}} := (\check{\mathbf{h}}_1 || \dots || \check{\mathbf{h}}_{n+1})$. Choose $\mathbf{\Delta} \leftarrow \mathbb{Z}_q^{2\times(n+1)}$, define $\hat{\mathbf{G}} := \mathbf{\Delta}\hat{\mathbf{U}}$ and $\hat{\mathbf{g}}_i := \mathbf{\Delta}\hat{\mathbf{u}}_i \in \hat{\mathbb{G}}^2$, for all $i \in [n+1]$. Let $\mathbf{a} \leftarrow \mathcal{L}_1$ and define $\check{\mathbf{a}}_\Delta := \mathbf{\Delta}^\top \check{\mathbf{a}} \in \check{\mathbb{H}}^{n+1}$. For any pair $(i,j) \in \mathcal{I}_{n,1}$, let $\mathbf{T}_{i,j} \leftarrow \mathbb{Z}_q^{2\times 2}$ and set:

$$\hat{\mathbf{C}}_{i,j} := \hat{\mathbf{g}}_i \mathbf{h}_j^\top - \hat{\mathbf{T}}_{i,j} \in \hat{\mathbb{G}}^{2\times 2}, \qquad \check{\mathbf{D}}_{i,j} := \check{\mathbf{T}}_{i,j} \in \check{\mathbb{H}}^{2\times 2}.$$

Note that $\hat{\mathbf{C}}_{i,j}$ can be efficiently computed as $\mathbf{h}_j \in \mathbb{Z}_q^2$ is the vector of discrete logarithms of $\check{\mathbf{h}}_j$.

Let $\Psi_{\overline{\mathcal{D}}_k,+}$ be the proof system for Sum in Subspace (Sect. 3.2) and $\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}$ be an instance of our proof system for Equal Opening (Sect. 3.3).

Let $\mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k,+}} \leftarrow \mathsf{K}_1(\Gamma, \{\hat{\mathbf{C}}_{i,j}, \check{\mathbf{D}}_{i,j}\}_{(i,j)\in\mathcal{I}_{n,1}})$ and [4] $\mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}} \leftarrow \mathsf{K}_1(\Gamma, \hat{\mathbf{G}}, \check{\mathbf{H}}, n)$. The common reference string is given by:

$$\begin{aligned} \mathsf{crs}_P &:= \left(\hat{\mathbf{U}}, \hat{\mathbf{G}}, \check{\mathbf{H}}, \{\hat{\mathbf{C}}_{i,j}, \check{\mathbf{D}}_{i,j}\}_{(i,j)\in\mathcal{I}_{n,1}}, \mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k,+}}, \mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}\right), \\ \mathsf{crs}_V &:= \left(\check{\mathbf{a}}, \check{\mathbf{a}}_\Delta, \mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k,+}}, \mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}\right). \end{aligned}$$

$\mathsf{P}(\mathsf{crs}_P, \hat{\mathbf{c}}, \langle \mathbf{b}, w_g\rangle)$**:** Pick $w_h \leftarrow \mathbb{Z}_q$, $\mathbf{R} \leftarrow \mathbb{Z}_q^{2\times 2}$ and then:

1. Define

$$\hat{\mathbf{c}}_\Delta := \hat{\mathbf{G}}\begin{pmatrix} \mathbf{b} \\ w_g \end{pmatrix}, \qquad \check{\mathbf{d}} := \check{\mathbf{H}}\begin{pmatrix} \mathbf{b} \\ w_h \end{pmatrix}.$$

[4] We identify matrices in $\hat{\mathbb{G}}^{2\times 2}$ (resp. in $\check{\mathbb{H}}^{2\times 2}$) with vectors in $\hat{\mathbb{G}}^4$ (resp. in $\check{\mathbb{H}}^4$).

2. Compute $(\hat{\mathbf{\Theta}}_{b(\bar{b}-1)}, \check{\mathbf{\Pi}}_{b(\bar{b}-1)}) :=$

$$\sum_{i\in[n]} \Big(b_i w_h(\hat{\mathbf{C}}_{i,n+1}, \check{\mathbf{D}}_{i,n+1}) + w_g(b_i - 1)(\hat{\mathbf{C}}_{n+1,i}, \check{\mathbf{D}}_{n+1,i}) \Big)$$
$$+ \sum_{i\in[n]} \sum_{\substack{j\in[n] \\ j\neq i}} b_i(b_j - 1)(\hat{\mathbf{C}}_{i,j}, \check{\mathbf{D}}_{i,j})$$
$$+ w_g w_h(\hat{\mathbf{C}}_{n+1,n+1}, \check{\mathbf{D}}_{n+1,n+1}) + (\hat{\mathbf{R}}, -\check{\mathbf{R}}). \tag{8}$$

3. Compute a proof $(\hat{\boldsymbol{\rho}}_{b(\bar{b}-1)}, \check{\boldsymbol{\sigma}}_{b(\bar{b}-1)})$ that $\mathbf{\Theta}_{b(\bar{b}-1)} + \check{\mathbf{\Pi}}_{b(\bar{b}-1)}$ belongs to the space spanned by $\{\mathbf{C}_{i,j} + \mathbf{D}_{i,j}\}_{(i,j)\in\mathcal{I}_{n,1}}$, and a proof $(\hat{\boldsymbol{\rho}}_{b-\bar{b}}, \check{\boldsymbol{\sigma}}_{b-\bar{b}})$ that $(\hat{\mathbf{c}}_\Delta, \check{\mathbf{d}})$ open to the same value, using $\mathbf{b}, w_g$, and w_h.

$\mathsf{V}(\mathsf{crs}_V, \hat{\mathbf{c}}, \langle \hat{\mathbf{c}}_\Delta, \check{\mathbf{d}}, (\hat{\mathbf{\Theta}}_{b(\bar{b}-1)}, \check{\mathbf{\Pi}}_{b(\bar{b}-1)}), \{(\hat{\boldsymbol{\rho}}_X, \check{\boldsymbol{\sigma}}_X)\}_{X\in\{b(\bar{b}-1), b-\bar{b}\}} \rangle)$**:**

1. Check if $\hat{\mathbf{c}}^\top \check{\mathbf{a}}_\Delta = \hat{\mathbf{c}}_\Delta^\top \check{\mathbf{a}}$.
2. Check if
$$\hat{\mathbf{c}}_\Delta \left(\check{\mathbf{d}} - \sum_{j\in[n]} \check{\mathbf{h}}_j \right)^\top = \hat{\mathbf{\Theta}}_{b(\bar{b}-1)} \check{\mathbf{I}}_{2\times 2} + \hat{\mathbf{I}}_{2\times 2} \check{\mathbf{\Pi}}_{b(\bar{b}-1)}. \tag{9}$$
3. Verify that $(\hat{\boldsymbol{\rho}}_{b(\bar{b}-1)}, \check{\boldsymbol{\sigma}}_{b(\bar{b}-1)}), (\hat{\boldsymbol{\rho}}_{b-\bar{b}}, \check{\boldsymbol{\sigma}}_{b-\bar{b}})$ are valid proofs for $(\hat{\mathbf{\Theta}}_{b(\bar{b}-1)}, \check{\mathbf{\Pi}}_{b(\bar{b}-1)})$ and $(\hat{\mathbf{c}}_\Delta, \check{\mathbf{d}})$ using $\mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k,+}}$ and $\mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}$ respectively.

If any of these checks fails, the verifier outputs 0, else it outputs 1.

$\mathsf{S}_1(\Gamma, \hat{\mathbf{U}})$**:** The simulator receives as input a description of an asymmetric bilinear group Γ and a matrix $\hat{\mathbf{U}} \in \hat{\mathbb{G}}^{(n+1)\times(n+1)}$ sampled according to distribution $\mathcal{D}_\Gamma$. It generates and outputs the CRS in the same way as K_1, but additionally it also outputs the simulation trapdoor

$$\tau = \left(\mathbf{H}, \mathbf{\Delta}, \tau_{\Psi_{\overline{\mathcal{D}}_k,+}}, \tau_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}} \right),$$

where $\tau_{\Psi_{\overline{\mathcal{D}}_k,+}}$ and $\tau_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}$ are, respectively, $\Psi_{\overline{\mathcal{D}}_k,+}$'s and $\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}$'s simulation trapdoors.

$\mathsf{S}_2(\mathsf{crs}_P, \hat{\mathbf{c}}, \tau)$**:** Compute $\hat{\mathbf{c}}_\Delta := \mathbf{\Delta}\hat{\mathbf{c}}$. Then pick random $\overline{w}_h \leftarrow \mathbb{Z}_q$, $\mathbf{R} \leftarrow \mathbb{Z}_q^{2\times 2}$ and define $\mathbf{d} := \overline{w}_h \mathbf{h}_{n+1}$. Then set:

$$\hat{\mathbf{\Theta}}_{b(\bar{b}-1)} := \hat{\mathbf{c}}_\Delta \left(\mathbf{d} - \sum_{i\in[n]} \mathbf{h}_i \right)^\top + \hat{\mathbf{R}}, \qquad \check{\mathbf{\Pi}}_{b(\bar{b}-1)} := -\check{\mathbf{R}}.$$

Finally, simulate proofs $(\hat{\boldsymbol{\rho}}_X, \check{\boldsymbol{\sigma}}_X)$ for $X \in \{b(\bar{b}-1), b-\bar{b}\}$ using $\tau_{\Psi_{\overline{\mathcal{D}}_k,+}}$ and $\tau_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}$.

5.4 Proof of Security

Completeness is proven in Appendix B.1. The following theorem guarantees Soundness.

Theorem 5.1 Let $\mathsf{Adv}_{\mathcal{PS}}(\mathsf{A})$ be the advantage of an adversary A against the soundness of the proof system described above. There exist PPT adversaries $\mathsf{B}_1, \mathsf{B}_2, \mathsf{B}_3, \mathsf{P}_1^*, \mathsf{P}_2^*$ such that

$$\begin{aligned}\mathsf{Adv}_{\mathcal{PS}}(\mathsf{A}) \quad \leq n \quad & \Big(6/q + \mathsf{Adv}_{\mathcal{U}_1,\hat{\mathbb{G}}}(\mathsf{B}_1) + \mathsf{Adv}_{\mathcal{U}_1,\check{\mathbb{H}}}(\mathsf{B}_2) + \mathsf{Adv}_{\mathsf{SP}_{\check{\mathbb{H}}}}(\mathsf{B}_3) \\ & + \mathsf{Adv}_{\Psi_{\overline{\mathcal{D}}_k,+}}(\mathsf{P}_1^*) + \mathsf{Adv}_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}(\mathsf{P}_2^*)\Big).\end{aligned}$$

∎

The proof follows from the indistinguishability of the following games:

- Real This is the real soundness game. The output is 1 if the adversary breaks the soundness, i.e. the adversary submits some $\hat{\mathbf{c}} = \hat{\mathbf{U}}\binom{\mathbf{b}}{w_g}$, for some $\mathbf{b} \notin \{0,1\}^n$ and $w \in \mathbb{Z}_q$, and the corresponding proof which is accepted by the verifier.
- Game_0 This game is identical to Real except that algorithm K_1 does not receive $\hat{\mathbf{U}}$ as a input but it samples $(\hat{\mathbf{U}}, \mathbf{U}) \in \mathcal{R}_{par}$ itself according to $\mathcal{D}_\Gamma$.
- Game_1 This game is identical to Game_0 except that the simulator picks a random $i^* \in [n]$, and uses $\mathbf{U}$ to check if the output of the adversary A is such that $b_{i^*} \in \{0,1\}$. It aborts if $b_{i^*} \in \{0,1\}$.
- Game_2 This game is identical to Game_1 except that now the vectors $\hat{\mathbf{g}}_i$, $i \in [n]$ and $i \neq i^*$, are uniform vectors in the space spanned by $\hat{\mathbf{g}}_{n+1}$.
- Game_3 This game is identical to Game_2 except that now the vector $\check{\mathbf{h}}_{i^*}$ is a uniform vector in $\check{\mathbb{H}}^2$, sampled independently of $\check{\mathbf{h}}_{n+1}$.

It is obvious that the first two games are indistinguishable. The rest of the argument goes as follows (the remaining proofs are in Appendix B.2).

Lemma 5.2 $\Pr[\mathsf{Game}_1(\mathsf{A}) = 1] \geq \frac{1}{n}\Pr[\mathsf{Game}_0(\mathsf{A}) = 1]$. ∎

Lemma 5.3 There exists a $\mathcal{U}_1$-$\mathsf{MDDH}_{\hat{\mathbb{G}}}$ adversary B such that $|\Pr[\mathsf{Game}_1(\mathsf{A}) = 1] - \Pr[\mathsf{Game}_2(\mathsf{A}) = 1]| \leq \mathsf{Adv}_{\mathcal{U}_1,\hat{\mathbb{G}}}(\mathsf{B}) + 2/q$. ∎

Proof: The adversary B receives $(\hat{\mathbf{s}}, \hat{\mathbf{t}})$ an instance of the $\mathcal{U}_1$-$\mathsf{MDDH}_{\hat{\mathbb{G}}}$ problem. B defines all the parameters honestly except that it embeds the $\mathcal{U}_1$-$\mathsf{MDDH}_{\hat{\mathbb{G}}}$ challenge in the matrix $\hat{\mathbf{G}}$.

Let $\hat{\mathbf{E}} := (\hat{\mathbf{s}}||\hat{\mathbf{t}})$. B picks $i^* \leftarrow [n]$, $\mathbf{W}_0 \leftarrow \mathbb{Z}_q^{2\times(i^*-1)}$, $\mathbf{W}_1 \leftarrow \mathbb{Z}_q^{2\times(n-i^*)}$, $\hat{\mathbf{g}}_{i^*} \leftarrow \hat{\mathbb{G}}^2$, and defines $\hat{\mathbf{G}} := (\hat{\mathbf{E}}\mathbf{W}_0||\hat{\mathbf{g}}_{i^*}||\hat{\mathbf{E}}\mathbf{W}_1||\hat{\mathbf{s}})$. In the real algorithm K_1, the generator picks the matrix $\mathbf{\Delta} \in \mathbb{Z}_q^{2\times(n+1)}$. Although B does not know $\mathbf{\Delta}$, it can compute $\hat{\mathbf{\Delta}}$ as $\hat{\mathbf{\Delta}} = \hat{\mathbf{G}}\mathbf{U}^{-1}$, given that $\mathbf{U}$ is full rank and was sampled by B, so it can compute the rest of the elements of the common reference string using the discrete logarithms of $\hat{\mathbf{U}}$, $\check{\mathbf{H}}$ and $\check{\mathbf{a}}$.

In case $\hat{\mathbf{t}}$ is uniform over $\hat{\mathbb{G}}^2$, by the Schwartz-Zippel lemma $\det(\hat{\mathbf{E}}) = 0$ with probability at most $2/q$. Thus, with probability at least $1 - 2/q$, the matrix $\hat{\mathbf{E}}$ is full-rank and $\hat{\mathbf{G}}$ is uniform over $\hat{\mathbb{G}}^{2\times(n+1)}$ as in Game_1. On the other hand, in case $\hat{\mathbf{t}} = \gamma\hat{\mathbf{s}}$, all of $\hat{\mathbf{g}}_i$, $i \neq i^*$, are in the space spanned by $\hat{\mathbf{g}}_{n+1}$ as in Game_2. ∎

Lemma 5.4 There exists a $\mathcal{U}_1$-$\mathsf{MDDH}_{\check{\mathbb{H}}}$ adversary B such that $|\Pr[\mathsf{Game}_2(\mathsf{A})=1]-\Pr[\mathsf{Game}_3(\mathsf{A})=1]| \leq \mathsf{Adv}_{\mathcal{U}_1,\check{\mathbb{H}}}(\mathsf{B})$. ∎

Lemma 5.5 There exists a $\mathsf{SP}_{\check{\mathbb{H}}}$ adversary B and soundness adversaries $\mathsf{P}_1^*, \mathsf{P}_2^*$ for $\Psi_{\overline{\mathcal{D}}_k,+}$ and $\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}$ such that

$$\Pr[\mathsf{Game}_3(\mathsf{A})=1] \leq 4/q + \mathbf{Adv}_{\mathsf{SP}_{\check{\mathbb{H}}}}(\mathsf{B}) + \mathbf{Adv}_{\Psi_{\overline{\mathcal{D}}_k,+}}(\mathsf{P}_1^*) + \mathbf{Adv}_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}(\mathsf{P}_2^*).$$

∎

Proof: $\Pr[\det((\mathbf{g}_{i^*}||\mathbf{g}_{n+1}))=0] = \Pr[\det((\mathbf{h}_{i^*}||\mathbf{h}_{n+1}))=0] \leq 2/q$, by the Schwartz-Zippel lemma. Then, with probability at least $1-4/q$, $\mathbf{g}_{i^*}\mathbf{h}_{i^*}^\top$ is linearly independent from $\{\mathbf{g}_i\mathbf{h}_j^\top : (i,j) \in [n+1]^2 \setminus \{(i^*,i^*)\}\}$ which implies that $\mathbf{g}_{i^*}\mathbf{h}_{i^*}^\top \notin \mathsf{Span}(\{\mathbf{C}_{i,j}+\mathbf{D}_{i,j} : (i,j) \in \mathcal{I}_{n,1}\}\})$. Additionally $\mathsf{Game}_3(\mathsf{A})=1$ implies that $b_{i^*} \notin \{0,1\}$ while the verifier accepts the proof produced by A, which is $(\hat{\mathbf{c}}_\Delta, \check{\mathbf{d}}, (\hat{\mathbf{\Theta}}_{b(\bar{b}-1)}, \check{\mathbf{\Pi}}_{b(\bar{b}-1)}), \{(\hat{\boldsymbol{\rho}}_X, \check{\boldsymbol{\sigma}}_X)\}_{X\in\{b(\bar{b}-1),b-\bar{b}\}})$. Since $\{\check{\mathbf{h}}_{i^*}, \check{\mathbf{h}}_{n+1}\}$ is a basis of $\check{\mathbb{H}}^2$, we can define $\overline{w}_h, \overline{b}_{i^*}$ as the unique coefficients in $\mathbb{Z}_q$ such that $\check{\mathbf{d}} = \overline{b}_{i^*}\check{\mathbf{h}}_{i^*} + \overline{w}_h\check{\mathbf{h}}_{n+1}$. We distinguish three cases:

1) If $\hat{\mathbf{c}}_\Delta \neq \mathbf{\Delta}\hat{\mathbf{c}}$, we can construct an adversary B against the $\mathsf{SP}_{\check{\mathbb{H}}}$ Assumption that outputs $\hat{\mathbf{c}}_\Delta - \mathbf{\Delta}\hat{\mathbf{c}} \in \ker(\check{\mathbf{a}}^\top)$.
2) If $\hat{\mathbf{c}}_\Delta = \mathbf{\Delta}\hat{\mathbf{c}}$ but $b_{i^*} \neq \overline{b}_{i^*}$. Given that $(b_i\mathbf{g}_{i^*}, \overline{b}_{i^*}\mathbf{h}_{i^*})$ is linearly independent from $\{(\mathbf{g}_{i^*}, \mathbf{h}_{i^*}), (\mathbf{g}_{n+1}, \mathbf{h}_{n+1})\}$ whenever $b_{i^*} \neq \overline{b}_{i^*}$, an adversary P_2^* against $\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}$ outputs the pair $(\hat{\boldsymbol{\rho}}_{b-\bar{b}}, \check{\boldsymbol{\sigma}}_{b-\bar{b}})$ which is a fake proof for $(\hat{\mathbf{c}}_\Delta, \check{\mathbf{d}})$.
3) If $\hat{\mathbf{c}}_\Delta = \mathbf{\Delta}\hat{\mathbf{c}}$ and $b_{i^*} = \overline{b}_{i^*}$, then $b_{i^*}(\overline{b}_{i^*}-1) \neq 0$. If we express $\mathbf{\Theta}_{b(\bar{b}-1)} + \mathbf{\Pi}_{b(\bar{b}-1)}$ as a linear combination of $\mathbf{g}_i\mathbf{h}_j^\top$, the coordinate of $\mathbf{g}_{i^*}\mathbf{h}_{i^*}^\top$ is $b_{i^*}(\overline{b}_{i^*}-1) \neq 0$ and thus $\mathbf{\Theta}_{b(\bar{b}-1)} + \mathbf{\Pi}_{b(\bar{b}-1)} \notin \mathsf{Span}(\{\mathbf{C}_{i,j}+\mathbf{D}_{i,j} : (i,j) \in \mathcal{I}_{n,1}\})$. The adversary P_1^* against $\Psi_{\overline{\mathcal{D}}_k,+}$ outputs the pair $(\hat{\boldsymbol{\rho}}_{b(\bar{b}-1)}, \check{\boldsymbol{\sigma}}_{b(\bar{b}-1)})$ which is a fake proof for $(\hat{\mathbf{\Theta}}_{b(\bar{b}-1)}, \check{\mathbf{\Pi}}_{b(\bar{b}-1)})$.

∎

This concludes the proof of soundness. Now we prove Zero-Knowledge.

Theorem 5.6 The proof system is perfect quasi-adaptive zero-knowledge. ∎

Proof: First, note that the vector $\check{\mathbf{d}} \in \check{\mathbb{H}}^2$ output by the prover and the vector output by S_2 follow exactly the same distribution. This is because the rank of $\check{\mathbf{H}}$ is 1. In particular, although the simulator S_2 does not know the opening of $\hat{\mathbf{c}}$, which is some $\mathbf{b} \in \{0,1\}^n$, there exists $w_h \in \mathbb{Z}_q$ such that $\check{\mathbf{d}} = \check{\mathbf{H}}\left(\begin{smallmatrix}\mathbf{b}\\ w_h\end{smallmatrix}\right)$. Since $\mathbf{R}$ is chosen uniformly at random in $\mathbb{Z}_q^{2\times 2}$, the proof $(\hat{\mathbf{\Theta}}_{b(\bar{b}-1)}, \check{\mathbf{\Pi}}_{b(\bar{b}-1)})$ is uniformly distributed conditioned on satisfying check 2) of algorithm V. Therefore, these elements of the simulated proof have the same distribution as in a real proof. This fact combined with the perfect zero-knowledge property of $\Psi_{\overline{\mathcal{D}}_k,+}$ and $\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}$ concludes the proof. ∎

5.5 Extensions

5.5.1 CRS Generation for Individual Commitments

A natural way to extend our construction to individual commitments (distribution (b) from Sect. 5.2) is the following. The only change is that the matrix $\boldsymbol{\Delta}$ is sampled uniformly from $\mathbb{Z}_q^{2\times 2n}$ (the distribution of $\check{\mathbf{H}}$ is not changed). Thus, the matrix $\hat{\mathbf{G}} := \boldsymbol{\Delta}\hat{\mathbf{U}}$ has $2n$ columns instead of $n+1$ and $\hat{\mathbf{c}}_\Delta := \hat{\mathbf{G}}\left(\begin{smallmatrix}\mathbf{b}\\ \mathbf{w}_g\end{smallmatrix}\right)$ for some $\mathbf{w}_g \in \mathbb{Z}_q^n$. In the soundness proof, the only change is that in Game_2, the extra columns are also changed to span a one-dimensional space, *i.e.* in this game $\hat{\mathbf{g}}_i$, $i \in [2n-1]$ and $i \neq i^*$, are uniform vectors in the space spanned by $\hat{\mathbf{g}}_{2n}$. With this approach, the proof size is still constant and the changes to the original construction are minimal but the CRS is considerably larger. Further, we do not know how to make the CRS linear for bit-strings of weight 1.

Therefore, we propose an alternative way to extend our result to individual commitments. In this new construction, the matrix $\hat{\mathbf{G}}$ is independent from $\hat{\mathbf{U}}$ and for all $i \in [n]$, $\hat{\mathbf{g}}_i = \mu_i \hat{\mathbf{g}}_{n+1}$, $\mu_i \leftarrow \mathbb{Z}_q$ and $\hat{\mathbf{g}}_{n+1} \leftarrow \mathbb{Z}_q^2$.

The proof is defined in a slightly different way. Now one computes $\hat{\mathbf{c}}_\Delta := \hat{\mathbf{G}}\left(\begin{smallmatrix}\mathbf{b}\\ w'_g\end{smallmatrix}\right)$, $w'_g \leftarrow \mathbb{Z}_q$, and one proves that the three commitments, $\hat{\mathbf{c}}, \hat{\mathbf{c}}_\Delta, \check{\mathbf{d}}$ open to the same value. Intuitively, this replaces in the original construction the proofs that $\boldsymbol{\Delta}\hat{\mathbf{c}} = \hat{\mathbf{c}}_\Delta$ and that $\boldsymbol{\Delta}\hat{\mathbf{c}}$ and $\check{\mathbf{d}}$ open to the same value. More specifically, this is proven by showing that $\left(\left(\begin{smallmatrix}\hat{\mathbf{c}}\\ \hat{\mathbf{c}}_\Delta\end{smallmatrix}\right), \check{\mathbf{d}}\right) \in \mathcal{L}_{\hat{\mathbf{M}},\check{\mathbf{N}}}$, where.

$$\hat{\mathbf{M}} := \begin{pmatrix} \hat{\mathbf{U}}_1 & \hat{\mathbf{U}}_2 & \hat{\mathbf{0}}_{2n\times 1} & \hat{\mathbf{0}}_{2n\times 1} \\ \hat{\mathbf{G}}_1 & \hat{\mathbf{0}}_{2\times n} & \hat{\mathbf{g}}_{n+1} & \hat{\mathbf{0}}_{2\times 1} \end{pmatrix} \text{ and } \check{\mathbf{N}} := \begin{pmatrix} \check{\mathbf{H}}_1 & \check{\mathbf{0}}_{2\times n} & \check{\mathbf{0}}_{2\times 1} & \check{\mathbf{h}}_{n+1} \end{pmatrix}.$$

The advantage of this alternative approach is that the matrix $\hat{\mathbf{G}}$ has now $n+1$ columns as in the original construction as opposed to $2n$ in the first extension to individual commitments.

The proof of soundness must be modified in the following way. In the proof of Lemma 5.3 one sets $\hat{\mathbf{g}}_{n+1} := \hat{\mathbf{s}}$ and $\hat{\mathbf{g}}_{i^*} := \hat{\mathbf{t}}$, similarly as done in Lemma 5.4. This guarantees that, as in the original construction, in the last game $\hat{\mathbf{g}}_{i^*}$ (resp. $\check{\mathbf{h}}_{i^*}$) is linearly independent of the rest of columns of $\hat{\mathbf{G}}$ (resp. $\check{\mathbf{H}}$). In the last game we need to show that $\hat{\mathbf{c}}_\Delta = b_{i^*}\hat{\mathbf{g}}_{i^*} + \tilde{w}_g\hat{\mathbf{g}}_{n+1}$ and $\check{\mathbf{d}} = b_{i^*}\check{\mathbf{h}}_{i^*} + \tilde{w}_h\check{\mathbf{h}}_{n+1}$, for some $\tilde{w}_g, \tilde{w}_h \in \mathbb{Z}_q$ and that $b_{i^*} \in \{0,1\}$. Note that the fact that $\left(\left(\begin{smallmatrix}\hat{\mathbf{c}}\\ \hat{\mathbf{c}}_\Delta\end{smallmatrix}\right), \check{\mathbf{d}}\right) \in \mathcal{L}_{\hat{\mathbf{M}},\check{\mathbf{N}}}$ implies that there is some $\boldsymbol{\gamma} \in \mathbb{Z}_q^{2n+2}$ such that $\begin{pmatrix}\hat{\mathbf{c}}\\ \hat{\mathbf{c}}_\Delta\\ \check{\mathbf{d}}\end{pmatrix} = \begin{pmatrix}\hat{\mathbf{M}}\\ \check{\mathbf{N}}\end{pmatrix}\boldsymbol{\gamma}$, and the fact that $\hat{\mathbf{c}}$ is perfectly binding together with the form of $\hat{\mathbf{M}}, \check{\mathbf{N}}$ implies that $\boldsymbol{\gamma} = \begin{pmatrix}\mathbf{b}\\ \boldsymbol{\gamma}'\end{pmatrix}$. In particular, $\hat{\mathbf{c}}_\Delta = \hat{\mathbf{G}}\left(\begin{smallmatrix}\mathbf{b}\\ \gamma_{2n+1}\end{smallmatrix}\right) = b_{i^*} + \tilde{w}_g\hat{\mathbf{g}}_{n+1}$ and $\check{\mathbf{d}} = \check{\mathbf{H}}\left(\begin{smallmatrix}\mathbf{b}\\ \gamma_{2n+2}\end{smallmatrix}\right) = b_{i^*}\check{\mathbf{h}}_{i^*} + \tilde{w}_h\check{\mathbf{h}}_{n+1}$ for some unique b_{i^*}. To conclude the proof of soundness we just need to argue that $b_{i^*} \neq \{0,1\}$, leads to a contradiction. This follows from the same argument as the original proof.

For zero-knowledge, observe that $\hat{\mathbf{c}}_\Delta$ is just a uniform vector in $\mathsf{Span}(\hat{\mathbf{g}}_{n+1})$. The simulator just picks a random $\hat{\mathbf{c}}_\Delta$ and simulates the proof that $\left(\left(\begin{smallmatrix}\hat{\mathbf{c}}\\ \hat{\mathbf{c}}_\Delta\end{smallmatrix}\right), \check{\mathbf{d}}\right) \in \mathcal{L}_{\hat{\mathbf{M}},\check{\mathbf{N}}}$ with the appropriate trapdoor. The rest of the proof is identical to the simulated proof in the original construction.

5.5.2 Linear Equations Satisfied by Bit-Strings

Because of the homomorphic properties of the commitments, we can easily extend it to prove that the bit-string $\mathbf{b}$ satisfies $\sum_{i\in[n]} \beta_i b_i = t$, for some $\boldsymbol{\beta} \in \mathbb{Z}_q^n, t \in \mathbb{Z}_q$. If the commitment $\hat{\mathbf{c}}$ is

a concatenation of GS commitments to b_i, this can be done in the usual way with GS proofs. But if $\hat{\mathbf{U}}$ is drawn from distribution (a) (see Sect. 5.2) this can also be done as follows. Define $\mathbf{B} := \left(\begin{smallmatrix} \beta_1 & \cdots & \beta_n & 0 \\ 0 & \cdots & 0 & 1 \end{smallmatrix}\right) \in \mathbb{Z}_q^{2\times(n+1)}$ and let $\hat{\mathbf{e}}_i^\ell$ denote the i th vector of the canonical basis of $\hat{\mathbb{G}}^\ell$. We claim the following:

$$\mathbf{B}\hat{\mathbf{c}} - t\hat{\mathbf{e}}_1^2 \in \mathsf{Span}\left(\mathbf{B}\hat{\mathbf{u}}_{n+1}\right) \Leftrightarrow \sum_{i\in[n]} \beta_i b_i = t.$$

This is justified because $\mathbf{B}\mathbf{u}_i = \mathbf{B}\mathbf{e}_i^{n+1} = (1,0)^\top$, and then $\mathbf{B}\hat{\mathbf{c}} - t\hat{\mathbf{e}}_1^2 = w\mathbf{B}\hat{\mathbf{u}}_{n+1} + \sum_{i\in[n]} b_i\mathbf{B}\hat{\mathbf{u}}_i - t\hat{\mathbf{e}}_1^2$. So to be able to prove that $\sum_{i\in[n]} \beta_i b_i = t$, we just need to add to the CRS the necessary elements to prove membership in $\mathcal{L}_{B\hat{\mathbf{u}}_{n+1}} := \{\hat{\mathbf{x}} \in \hat{\mathbb{G}}^2 : \exists w \in \mathbb{Z}_q, \hat{\mathbf{x}} = \mathbf{B}\hat{\mathbf{u}}_{n+1}w\}$ using one of the constructions of Sect. 2.4.

5.5.3 Bit-Strings of Weight 1

In the special case when the bit-string has only one 1 (this case is useful in some applications, see Sect. 6), the size of the CRS can be made linear in n, instead of quadratic. To prove this statement we would combine our proof system for bit-strings of section 5.3 and a proof that $\sum_{i\in[n]} b_i = 1$ as described above when $m = 1$ or using GS-proofs when $m = n$. In the definition of $(\hat{\mathbf{\Theta}}_{b(\bar{b}-1)}, \check{\mathbf{\Pi}}_{b(\bar{b}-1)})$ in Eq. 8, one sees that for all pairs $(i,j) \in [n]\times[n]$, the coefficient of $(\hat{\mathbf{C}}_{i,j}, \check{\mathbf{D}}_{i,j})$ is $b_i(b_j - 1)$. If i^* is the only index such that $b_{i^*} = 1$, then we have:

$$\sum_{i\in[n]}\sum_{j\in[n]} b_i(b_j-1)(\hat{\mathbf{C}}_{i,j}, \check{\mathbf{D}}_{i,j}) = \sum_{j\neq i^*}(\hat{\mathbf{C}}_{i^*,j}, \check{\mathbf{D}}_{i^*,j}) =: (\hat{\mathbf{C}}_{i^*,\neq}, \check{\mathbf{D}}_{i^*,\neq}).$$

Therefore, one can replace in the CRS the pairs of matrices $(\hat{\mathbf{C}}_{i,j}, \check{\mathbf{D}}_{i,j})$ by $(\hat{\mathbf{C}}_{i,\neq}, \check{\mathbf{D}}_{i,\neq})$, $i \in [n]$. The resulting CRS is linear in n.

6 Applications

Many protocols use proofs that a commitment opens to a bit-string as a building block. Since our commitments are still of size $\Theta(n)$, our results may not apply to some of these protocols (*e.g.* range proofs). Yet, there are several applications where bits need to be used independently and our results provide significant improvements. Table 2 summarizes them.

6.1 Signatures

Some application examples are the signature schemes of [4, 5, 8, 12]. For example, in the revocable attribute-based signature scheme of Escala *et. al* [12], every signature includes a proof that a set of GS commitments, whose size is the number of attributes, opens to a bit-string. Further, the proof of membership in a list which is discussed below can also be used to reduce the size of Ring Signature scheme of [9], which is the most efficient ring signature in the standard model. To sign a message m, among other things, the signer picks a one-time signature key and certifies the one-time verification key by signing it with a Boneh-Boyen signature under vk_α. Then, the signer commits to vk_α and shows that vk_α belongs to the list of Boneh-Boyen verification keys $(vk_1, \ldots, vk_n)$ of the parties in the ring R.

Proof System	Author	Proof Size
Threshold GS	Ràfols [32] (1)	$(m_x + 3(n-t) + 2\bar{n})\mathfrak{g}$
	Ràfols [32] (2)	$2(n-t+1)\mathfrak{h} + 2n(\mathfrak{g}+\mathfrak{h})$
	This work	$2(n+1)\mathfrak{g} + 10(\mathfrak{g}+\mathfrak{h})$
Dynamic List (Ring Signature)	Chandran et al. [9]	$(16\sqrt{n}+4)(\mathfrak{g}+\mathfrak{h})$
	Ràfols [32]	$(8\sqrt{n}+6)\mathfrak{g} + 12\sqrt{n}\mathfrak{h}$
	This work	$(4\sqrt{n}+14)\mathfrak{g} + (8\sqrt{n}+14)\mathfrak{h}$
Static List	This work (first scheme)	$(4\sqrt{n}+16)\mathfrak{g} + (2\sqrt{n}+22)\mathfrak{h}$
	This work (second scheme)	$(6\sqrt[3]{n}+36)\mathfrak{g} + (6\sqrt[3]{n}+60)\mathfrak{h}$

Table 2: Comparison of the application of our techniques and results from the literature. In rows labeled as "Threshold GS" we give the size of the proof of satisfiability of t-out-of-n sets $\mathcal{S}_i$, where m_x is the sum of the number of variables in $\hat{\mathbb{G}}$ in each set $\mathcal{S}_i$, and $\bar{n}$ is the total number of two-sided and quadratic equations in some $\bigcup_{i\in[n]} \mathcal{S}_i$. For all rows, we must add to the proof size the cost of a GS proof of each equation in one of the sets $\mathcal{S}_i$. In the other rows n is the size of the list.

6.2 Threshold GS Proofs for PPEs

There are two approaches to construct threshold GS proofs for PPEs, i.e. proofs of satisfiability of t-out-of-n equations. One is due to [16] and consists of compiling the n equations into a single equation which is satisfied only if t of the original equations are satisfied. For the case of PPEs, this method adds new variables and proves that each of them opens to a bit. Our result reduces the cost of this approach, but we omit any further discussion as it is quite inefficient because the number of additional variables is $\Theta(m_{var} + n)$, where m_{var} is the total number of variables in the original n equations.

The second approach is due to Ràfols [32]. The basic idea behind [32], which extends [17], follows from the observation that for each GS equation type tp, the CRS space $\mathcal{K}$ is partitioned into a perfectly sound CRS space $\mathcal{K}^b_{\mathsf{tp}}$ and a perfectly witness indistinguishable CRS space $\mathcal{K}^h_{\mathsf{tp}}$.

In particular, to prove satisfiability of t-out-of-n sets of equations from $\{\mathcal{S}_i : i \in [n]\}$ of type tp, it suffices to construct an algorithm $\mathsf{K}_{\mathsf{corr}}$ which on input $\mathsf{crs}_{\mathrm{GS}}$ and some set of indexes $A \subset [n]$, $|A| = t$, generates n GS common reference strings $\{\mathsf{crs}_i, i \in [n]\}$ and simulation trapdoors $\tau_{i,sim}$, $i \in A^c$, in a such a way that[5]:

a) it can be publicly verified the set of perfectly sound keys, $\{\mathsf{crs}_i : \mathsf{crs}_i \in \mathcal{K}^b_{\mathsf{tp}}\}$ is of size at least t,

b) there exists a simulator $\mathsf{S}_{\mathsf{corr}}$ who outputs $(\mathsf{crs}_i, \tau_{i,sim})$ for all $i \in [n]$, and the distribution of $\{\mathsf{crs}_i : i \in [n]\}$ is the same as the one of the keys output by $\mathsf{K}_{\mathsf{corr}}$ when $\mathsf{crs}_{\mathrm{GS}}$ is the perfectly witness-indistinguishable CRS.

The prover of t-out-of-n satisfiability can run $\mathsf{K}_{\mathsf{corr}}$ and, for all $i \in [n]$, compute a real (resp. simulated) proof for $\mathcal{S}_i$ with respect to crs_i when $i \in A$ (resp. when $i \in A^c$).

[5] More technically, this is the notion of *Simulatable Verifiable Correlated Key Generation* in [32], which extends the definition of Verifiable Correlated Key Generation of [17].

Ràfols gives two constructions for PPEs, the first one can be found in [32], App. C and the other follows from [32, Sect. 7][6]. Our algorithm $\mathsf{K}_{\mathsf{corr}}$ for PPEs[7] goes as follows:

- Define $(b_1, \ldots, b_n)$ as $b_i = 1$ if $i \in A$ and $b_i = 0$ if $i \in A^c$. For all $i \in [n]$, let $\hat{\mathbf{z}}_i := \mathsf{Comm}(b_i) = b_i\hat{\mathbf{u}}_1 + r_i\hat{\mathbf{u}}_2$, $r_i \in \mathbb{Z}_q$, and define $\tau_{sim,i} = r_i$, for all $i \in A^c$. Define $\mathsf{crs}_i := (\Gamma, \hat{\mathbf{z}}_i, \hat{\mathbf{u}}_2, \check{\mathbf{v}}_1, \check{\mathbf{v}}_2)$.
- Prove that $\{\hat{\mathbf{c}}_i\}$ opens to $\mathbf{b} \in \{0,1\}^n$ and that $\sum_{i\in[n]} b_i = t$.

The simulator just defines $\mathbf{b} = \mathbf{0}$. The reason why this works is that when $b_i = 1$, $(\hat{\mathbf{z}}_i - \hat{\mathbf{u}}_1) \in \mathsf{Span}(\hat{\mathbf{u}}_2)$, therefore $\mathsf{crs}_i \in \mathcal{K}^b_{PPE}$ and when $b_i = 0$, $(\hat{\mathbf{z}}_i - \hat{\mathbf{u}}_1) \notin \mathsf{Span}(\hat{\mathbf{u}}_2)$ so $\mathsf{crs}_i \in \mathcal{K}^h_{PPE}$.

6.3 More Efficient Proof of Membership in a List

Chandran *et al.* construct a ring signature of size $\Theta(\sqrt{n})$ [9], which is the most efficient ring signature in the standard model. Their construction uses as a subroutine a non-interactive proof of membership in some list $L = (\hat{l}_1, \ldots, \hat{l}_n)$ which is of size $\Theta(\sqrt{n})$. The trick of Chandran *et al.* to achieve this asymptotic complexity is to view L as a matrix $\hat{\mathbf{L}} \in \hat{\mathbb{G}}^{m\times m}$, for $m = \sqrt{n}$, where the i, j th element of $\hat{\mathbf{L}}$ is $\hat{l}_{i,j} := \hat{l}_{(i,j)}$ and $(i, j) := (i - 1)m + j$. Given a commitment $\hat{\mathbf{c}}$ to some element $\hat{l}_\alpha$, where $\alpha = (i_\alpha, j_\alpha)$, their construction in asymmetric bilinear groups works as follows :

1. Compute GS commitments in $\check{\mathbb{H}}$ to $b_1 \ldots, b_m$ and $b'_1, \ldots, b'_m$, where $b_i = 1$ if $i = i_\alpha$ and 0 otherwise, and $b'_j = 1$ if $j = j_\alpha$, and 0 otherwise.
2. Compute a GS proof that $b_i \in \{0, 1\}$ and $b'_j \in \{0, 1\}$ for all $i, j \in [m]$, and that $\sum_{i\in[m]} b_i = 1$, and $\sum_{j\in[m]} b'_j = 1$.
3. Compute GS commitments to $\hat{x}_1 := \hat{l}_{(i_\alpha,1)}, \ldots, \hat{x}_m := \hat{l}_{(i_\alpha,m)}$.
4. Compute a GS proof that $\hat{x}_j = \sum_{i\in[m]} b_i\hat{l}_{(i,j)}$, for all $j \in [m]$, is satisfied.
5. Compute a GS proof that $\hat{l}_\alpha = \sum_{j\in[m]} b'_j\hat{x}_j$ is satisfied.

With respect to the naive use of GS proofs, Step 2 was improved by Ràfols [32]. Using our proofs for bit-strings of weight 1 from Sect. 5.5, we can further reduce the size of the proof in step 2, see table.

We note that although in step 4 the equations are all two-sided linear equations, proofs can only be aggregated if the list comes from a witness samplable distribution and the CRS is set to depend on that specific list. This is not useful for the application to ring signatures, since the CRS should be independent of the ring R (which defines the list). If aggregation is possible then the size of the proof in step 4 is reduced from $(2\mathfrak{g} + 4\mathfrak{h})\sqrt{n}$ to $4\mathfrak{g} + 8\mathfrak{h}$. A complete description of the proof can be found in Appendix D, where we also show that when the CRS depends on the list and the list is witness samplable, the proof can be further reduced to $\Theta(\sqrt[3]{n})$.

[6] The construction in [32, Sect. 7] is for other equation types but can be used to prove that t-out-of-n of $\mathsf{crs}_1, \ldots, \mathsf{crs}_n$ are perfectly binding for PPEs.

[7] Properly speaking the construction is for PPEs which are left-simulatable in the terminology of [32].

References

[1] M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, and M. Ohkubo. Structure-preserving signatures and commitments to group elements. In T. Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 209–236, Santa Barbara, CA, USA, Aug. 15–19, 2010. Springer, Heidelberg, Germany. 42

[2] M. Abe, J. Groth, M. Ohkubo, and T. Tango. Converting cryptographic schemes from symmetric to asymmetric bilinear groups. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 241–260, Santa Barbara, CA, USA, Aug. 17–21, 2014. Springer, Heidelberg, Germany. 4

[3] M. Abe, K. Haralambiev, and M. Ohkubo. Signing on elements in bilinear groups for modular protocol design. Cryptology ePrint Archive, Report 2010/133, 2010. `http://eprint.iacr.org/2010/133`. 5

[4] O. Blazy, G. Fuchsbauer, D. Pointcheval, and D. Vergnaud. Signatures on randomizable ciphertexts. In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, editors, *PKC 2011*, volume 6571 of *LNCS*, pages 403–422, Taormina, Italy, Mar. 6–9, 2011. Springer, Heidelberg, Germany. 24

[5] O. Blazy, D. Pointcheval, and D. Vergnaud. Compact round-optimal partially-blind signatures. In I. Visconti and R. D. Prisco, editors, *Security and Cryptography for Networks - 8th International Conference, SCN 2012, Amalfi, Italy, September 5-7, 2012. Proceedings*, volume 7485 of *Lecture Notes in Computer Science*, pages 95–112. Springer, 2012. 24

[6] D. Boneh, X. Boyen, and E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext. In R. Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 440–456, Aarhus, Denmark, May 22–26, 2005. Springer, Heidelberg, Germany. 46

[7] D. Boneh, D. Freeman, J. Katz, and B. Waters. Signing a linear subspace: Signature schemes for network coding. In S. Jarecki and G. Tsudik, editors, *PKC 2009*, volume 5443 of *LNCS*, pages 68–87, Irvine, CA, USA, Mar. 18–20, 2009. Springer, Heidelberg, Germany. 42

[8] P. Camacho. Fair exchange of short signatures without trusted third party. In E. Dawson, editor, *CT-RSA 2013*, volume 7779 of *LNCS*, pages 34–49, San Francisco, CA, USA, Feb. 25 – Mar. 1, 2013. Springer, Heidelberg, Germany. 24

[9] N. Chandran, J. Groth, and A. Sahai. Ring signatures of sub-linear size without random oracles. In L. Arge, C. Cachin, T. Jurdzinski, and A. Tarlecki, editors, *ICALP 2007*, volume 4596 of *LNCS*, pages 423–434, Wroclaw, Poland, July 9–13, 2007. Springer, Heidelberg, Germany. 24, 25, 26

[10] A. Escala and J. Groth. Fine-tuning Groth-Sahai proofs. In H. Krawczyk, editor, *PKC 2014*, volume 8383 of *LNCS*, pages 630–649, Buenos Aires, Argentina, Mar. 26–28, 2014. Springer, Heidelberg, Germany. 4

[11] A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar. An algebraic framework for Diffie-Hellman assumptions. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147, Santa Barbara, CA, USA, Aug. 18–22, 2013. Springer, Heidelberg, Germany. 4, 5, 7

[12] A. Escala, J. Herranz, and P. Morillo. Revocable attribute-based signatures with adaptive security in the standard model. In A. Nitaj and D. Pointcheval, editors, *AFRICACRYPT 11*, volume 6737 of *LNCS*, pages 224–241, Dakar, Senegal, July 5–7, 2011. Springer, Heidelberg, Germany. 24

[13] D. M. Freeman. Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In H. Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 44–61, French Riviera, May 30 – June 3, 2010. Springer, Heidelberg, Germany. 4

[14] S. D. Galbraith, K. G. Paterson, and N. P. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16):31133121, 2008. 4

[15] R. Gennaro, C. Gentry, B. Parno, and M. Raykova. Quadratic span programs and succinct NIZKs without PCPs. In T. Johansson and P. Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 626–645, Athens, Greece, May 26–30, 2013. Springer, Heidelberg, Germany. 4

[16] J. Groth. Simulation-sound NIZK proofs for a practical language and constant size group signatures. In X. Lai and K. Chen, editors, *ASIACRYPT 2006*, volume 4284 of *LNCS*, pages 444–459, Shanghai, China, Dec. 3–7, 2006. Springer, Heidelberg, Germany. 25

[17] J. Groth, R. Ostrovsky, and A. Sahai. Non-interactive zaps and new techniques for NIZK. In C. Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 97–111, Santa Barbara, CA, USA, Aug. 20–24, 2006. Springer, Heidelberg, Germany. 25

[18] J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In N. P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432, Istanbul, Turkey, Apr. 13–17, 2008. Springer, Heidelberg, Germany. 7

[19] J. Groth and A. Sahai. Efficient noninteractive proof systems for bilinear groups. *SIAM J. Comput.*, 41(5):1193–1232, 2012. 4, 15

[20] D. Hofheinz and E. Kiltz. Secure hybrid encryption from weakened key encapsulation. In A. Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 553–571, Santa Barbara, CA, USA, Aug. 19–23, 2007. Springer, Heidelberg, Germany. 8

[21] A. Joux. A new index calculus algorithm with complexity $L(1/4+o(1))$ in small characteristic. In T. Lange, K. Lauter, and P. Lisonek, editors, *SAC 2013*, volume 8282 of *LNCS*, pages 355–379, Burnaby, BC, Canada, Aug. 14–16, 2014. Springer, Heidelberg, Germany. 4

[22] C. S. Jutla and A. Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In K. Sako and P. Sarkar, editors, *ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 1–20, Bengalore, India, Dec. 1–5, 2013. Springer, Heidelberg, Germany. 4, 10

[23] C. S. Jutla and A. Roy. Switching lemma for bilinear tests and constant-size NIZK proofs for linear subspaces. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014, Part II*, volume 8617 of *LNCS*, pages 295–312, Santa Barbara, CA, USA, Aug. 17–21, 2014. Springer, Heidelberg, Germany. 4, 5, 6, 14, 17

[24] E. Kiltz, J. Pan, and H. Wee. Structure-preserving signatures from standard assumptions, revisited. In R. Gennaro and M. J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216

of *LNCS*, pages 275–295, Santa Barbara, CA, USA, Aug. 16–20, 2015. Springer, Heidelberg, Germany. 44

[25] E. Kiltz and H. Wee. Quasi-adaptive NIZK for linear subspaces revisited. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 101–128, Sofia, Bulgaria, Apr. 26–30, 2015. Springer, Heidelberg, Germany. 4, 5, 10, 11, 12, 30

[26] B. Libert, T. Peters, M. Joye, and M. Yung. Linearly homomorphic structure-preserving signatures and their applications. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 289–307, Santa Barbara, CA, USA, Aug. 18–22, 2013. Springer, Heidelberg, Germany. 42, 43, 44, 45

[27] B. Libert, T. Peters, M. Joye, and M. Yung. Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures. In P. Q. Nguyen and E. Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 514–532, Copenhagen, Denmark, May 11–15, 2014. Springer, Heidelberg, Germany. 4, 11, 43

[28] B. Libert, T. Peters, M. Joye, and M. Yung. Compactly hiding linear spans: Tightly secure constant-size simulation-sound QA-NIZK proofs and applications. Cryptology ePrint Archive, Report 2015/242, 2015. `http://eprint.iacr.org/2015/242`. 47

[29] B. Libert, T. Peters, and M. Yung. Group signatures with almost-for-free revocation. In R. Safavi-Naini and R. Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 571–589, Santa Barbara, CA, USA, Aug. 19–23, 2012. Springer, Heidelberg, Germany. 9

[30] P. Morillo, C. Ràfols, and J. L. Villar. Matrix computational assumptions in multilinear groups. Cryptology ePrint Archive, Report 2015/353, 2015. `http://eprint.iacr.org/2015/353`. 5, 8, 14, 16, 33

[31] M. Naor. On cryptographic assumptions and challenges (invited talk). In D. Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 96–109, Santa Barbara, CA, USA, Aug. 17–21, 2003. Springer, Heidelberg, Germany. 4

[32] C. Ràfols. Stretching groth-sahai: NIZK proofs of partial satisfiability. In Y. Dodis and J. B. Nielsen, editors, *TCC 2015, Part II*, volume 9015 of *LNCS*, pages 247–276, Warsaw, Poland, Mar. 23–25, 2015. Springer, Heidelberg, Germany. 4, 25, 26

[33] H. Shacham. A cramer-shoup encryption scheme from the linear assumption and from progressively weaker linear variants. Cryptology ePrint Archive, Report 2007/074, 2007. `http://eprint.iacr.org/`. 8

[34] V. Shoup. Lower bounds for discrete logarithms and related problems. In W. Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 256–266, Konstanz, Germany, May 11–15, 1997. Springer, Heidelberg, Germany. 46

A Proofs of Theorems 3.1 and 3.2

Theorem A.1 [Theorem 3 repeated] If $\widetilde{\mathcal{D}_k} = \mathcal{D}_k$ and $\tilde{k} = k+1$, Fig. 2 describes a QA-NIZK proof system with perfect completeness, computational adaptive soundness based on the $\mathcal{D}_k$-SKerMDH Assumption, and perfect zero-knowledge. ∎

Proof: (Soundness.) B receives a challenge $(\hat{\mathbf{A}}, \check{\mathbf{A}})$, $\mathbf{A} \leftarrow \mathcal{D}_k$, and then it chooses $\boldsymbol{\Lambda} \leftarrow \mathbb{Z}_q^{(k+1)\times m}, \boldsymbol{\Xi} \leftarrow \mathbb{Z}_q^{(k+1)\times n}$, samples $(\hat{\mathbf{M}}, \check{\mathbf{N}}) \leftarrow \mathcal{D}_\Gamma$ and computes $\mathsf{crs} := (\hat{\mathbf{M}}_\Lambda, \check{\mathbf{A}}_\Lambda, \check{\mathbf{A}}, \check{\mathbf{N}}_\Xi, \hat{\mathbf{A}}_\Xi, \hat{\mathbf{A}})$ in the natural way. An adversary F against the soundness outputs a vector $(\hat{\mathbf{x}}^*, \check{\mathbf{y}}^*) \notin \mathcal{L}_{\hat{\mathbf{M}},\check{\mathbf{N}}}$ and a valid proofs $(\hat{\boldsymbol{\rho}}^*, \check{\boldsymbol{\sigma}}^*)$. At this point, B computes its own proof $(\hat{\boldsymbol{\rho}}^\dagger, \check{\boldsymbol{\sigma}}^\dagger)$ using $\boldsymbol{\Lambda}$ and $\boldsymbol{\Xi}$. The adversary B will output as a response to the $\mathcal{D}_k$-$\mathsf{SKerMDH}$ challenge the pair $(\hat{\mathbf{r}}, \check{\mathbf{s}}) := (\hat{\boldsymbol{\rho}}^* - \hat{\boldsymbol{\rho}}^\dagger, \check{\boldsymbol{\sigma}}^\dagger - \check{\boldsymbol{\sigma}}^*)$. We now see that with all but probability $1/q$, this is a valid solution. Indeed, if $(\hat{\mathbf{r}}, \check{\mathbf{s}}) \neq 0$, we are done, because since both are valid proofs, subtraction of the verification equations yields

$$(\hat{\boldsymbol{\rho}}^* - \hat{\boldsymbol{\rho}}^\dagger)^\top \check{\mathbf{A}} = (\check{\boldsymbol{\sigma}}^\dagger - \check{\boldsymbol{\sigma}}^*)^\top \hat{\mathbf{A}}.$$

By definition $\mathbf{r} \neq \mathbf{s}$ if and only if $\boldsymbol{\rho}^* + \boldsymbol{\sigma}^* \neq \boldsymbol{\rho}^\dagger + \boldsymbol{\sigma}^\dagger$. But

$$\boldsymbol{\rho}^\dagger + \boldsymbol{\sigma}^\dagger = \boldsymbol{\Lambda}\mathbf{x}^* + \boldsymbol{\Xi}\mathbf{y}^* = \boldsymbol{\Delta}\mathbf{w}, \qquad \boldsymbol{\Delta} := (\boldsymbol{\Lambda}||\boldsymbol{\Xi}),\ \mathbf{w} := \begin{pmatrix}\mathbf{x}\\ \mathbf{y}\end{pmatrix} \tag{10}$$

Since $\mathbf{Z}$ is a uniform random value, the CRS reveals (information theoretically) only $\left\{\boldsymbol{\Delta}\left(\begin{smallmatrix}\mathbf{M}\\ \mathbf{N}\end{smallmatrix}\right), \boldsymbol{\Delta}^\top\mathbf{A}\right\}$ about $\boldsymbol{\Delta}$. But since a) $(\hat{\mathbf{x}}, \check{\mathbf{y}}) \notin \mathcal{L}_{\hat{\mathbf{M}},\check{\mathbf{N}}}$, $\mathbf{w}$ is not in the image of $\left(\begin{smallmatrix}\mathbf{M}\\ \mathbf{N}\end{smallmatrix}\right)$ and b) $\mathbf{A}$ has more rows than columns, it follows by a standard argument that $\boldsymbol{\Delta}\mathbf{w}$ is undetermined from the adversary's point of view. ▌

Theorem A.2 [Theorem 4 repeated] If $\widetilde{\mathcal{D}_k} = \overline{\mathcal{D}}_k$ and $\tilde{k} = k$, and $\mathcal{D}_\Gamma$ is a witness samplable distribution, Fig. 2 describes a QA-NIZK proof system with perfect completeness, computational adaptive soundness based on the $\mathcal{D}_k$-$\mathsf{SKerMDH}$ Assumption, and perfect zero-knowledge. ▌

Proof: (Soundness.) Define $\tilde{m} := m + n$ and $\mathbf{P} := \left(\begin{smallmatrix}\mathbf{M}\\ \mathbf{N}\end{smallmatrix}\right)$. An adversary B against $\mathcal{D}_k$-$\mathsf{SKerMDH}$ Assumption receives a challenge $(\hat{\mathbf{A}}, \check{\mathbf{A}})$, $\mathbf{A} \leftarrow \mathcal{D}_k$. It samples $(\hat{\mathbf{M}}, \check{\mathbf{N}}, \mathbf{M}, \mathbf{N}) \in \mathcal{R}_{par}$ and computes $\mathbf{P}^\perp \in \mathbb{Z}_q^{\tilde{m}\times(\tilde{m}-r)}$, where $r = \mathsf{rank}(\mathbf{P})$, a basis of the kernel of $\mathbf{P}^\top$. By definition, $\mathbf{P}^\top = (\mathbf{M}^\top||\mathbf{N}^\top)$ and $\mathbf{P}^\top\mathbf{P}^\perp = \mathbf{0}$, thus we can write $\mathbf{P}^\perp = \left(\begin{smallmatrix}\mathbf{E}\\ \mathbf{F}\end{smallmatrix}\right)$, for some matrices such that $\mathbf{M}^\top\mathbf{E} = -\mathbf{N}^\top\mathbf{F}$.

Adversary B samples $\mathbf{R} \in \mathbb{Z}_q^{(\tilde{m}-r-1)\times(k+1)}$ and defines

$$\hat{\mathbf{A}}' := \begin{pmatrix}\hat{\mathbf{A}}\\ \mathbf{R}\hat{\mathbf{A}}\end{pmatrix} \in \hat{\mathbb{G}}^{(k+\tilde{m}-r)\times k}, \qquad \check{\mathbf{A}}' := \begin{pmatrix}\check{\mathbf{A}}\\ \mathbf{R}\check{\mathbf{A}}\end{pmatrix} \in \check{\mathbb{H}}^{(k+\tilde{m}-r)\times k}.$$

Then B samples $(\widetilde{\boldsymbol{\Lambda}}||\widetilde{\boldsymbol{\Xi}}) \leftarrow \mathbb{Z}_q^{k\times\tilde{m}}$. Let $\mathbf{A}_0$ be the first k rows of $\mathbf{A}'$ (or $\mathbf{A}$) and $\mathbf{A}'_1$ the rest of the rows, and $\mathbf{T}_{\mathbf{A}'} = \mathbf{A}'_1\mathbf{A}_0^{-1}$. Then B implicitly sets $(\boldsymbol{\Lambda}||\boldsymbol{\Xi}) := (\widetilde{\boldsymbol{\Lambda}}||\widetilde{\boldsymbol{\Xi}}) + \mathbf{T}^\top_{\mathbf{A}'}(\mathbf{E}^\top||\mathbf{F}^\top)$, and computes:

$$\begin{pmatrix}\check{\mathbf{A}}_\Lambda\\ \hat{\mathbf{A}}_\Xi\end{pmatrix} = \begin{pmatrix}\boldsymbol{\Lambda}^\top\check{\mathbf{A}}_0\\ \boldsymbol{\Xi}^\top\hat{\mathbf{A}}_0\end{pmatrix} := \begin{pmatrix}(\widetilde{\boldsymbol{\Lambda}}^\top + \mathbf{E}\mathbf{T}_{\mathbf{A}'})\check{\mathbf{A}}_0\\ (\widetilde{\boldsymbol{\Xi}}^\top + \mathbf{F}\mathbf{T}_{\mathbf{A}'})\hat{\mathbf{A}}_0\end{pmatrix} = \begin{pmatrix}(\widetilde{\boldsymbol{\Lambda}}^\top||\mathbf{E})\check{\mathbf{A}}'\\ (\widetilde{\boldsymbol{\Xi}}^\top||\mathbf{F})\hat{\mathbf{A}}'\end{pmatrix} \tag{11}$$

So far the argument is very similar to [25] Sect. 3.2, now comes an important difference. Adversary B also needs to compute $\boldsymbol{\Lambda}\hat{\mathbf{M}} + \hat{\mathbf{Z}}$ and $\boldsymbol{\Xi}\check{\mathbf{N}} - \check{\mathbf{Z}}$. Although the adversary B does not know how to

compute $\boldsymbol{\Xi}\mathbf{N}$ or $\boldsymbol{\Lambda}\mathbf{M}$, it can compute their sum in $\mathbb{Z}_q$ as:

$$\boldsymbol{\Xi}\mathbf{N} + \boldsymbol{\Lambda}\mathbf{M} = \left((\widetilde{\boldsymbol{\Lambda}}||\widetilde{\boldsymbol{\Xi}}) + \mathbf{T}_{\mathbf{A}'}^{\top}(\mathbf{E}^{\top}||\mathbf{F}^{\top})\right)\begin{pmatrix}\mathbf{M}\\ \mathbf{N}\end{pmatrix} = \widetilde{\boldsymbol{\Lambda}}\mathbf{M} + \widetilde{\boldsymbol{\Xi}}\mathbf{N} =: \mathbf{T}.$$

Thus, B picks $\mathbf{Z} \leftarrow \mathbb{Z}_q^{k\times t}$ and outputs $\check{\mathbf{N}}_{\Xi} := \check{\mathbf{T}} - \check{\mathbf{Z}}$ and $\hat{\mathbf{M}}_{\Xi} := \hat{\mathbf{Z}}$. Now, when F outputs a valid proof for some $(\hat{\mathbf{x}}, \check{\mathbf{y}}) \notin \mathcal{L}_{\hat{\mathbf{M}},\check{\mathbf{N}}}$, it holds that:

$$\begin{aligned}\hat{\mathbf{x}}^{\top}\check{\mathbf{A}}_{\Lambda} - \hat{\boldsymbol{\rho}}^{\top}\check{\mathbf{A}}_0 = \check{\boldsymbol{\sigma}}^{\top}\hat{\mathbf{A}}_0 - \check{\mathbf{y}}^{\top}\hat{\mathbf{A}}_{\Xi} \iff\\ \hat{\mathbf{x}}^{\top}(\widetilde{\boldsymbol{\Lambda}}^{\top}||\mathbf{E})\check{\mathbf{A}}' - (\hat{\boldsymbol{\rho}}^{\top}||\hat{\mathbf{0}}_{1\times(\tilde{m}-r)})^{\top}\check{\mathbf{A}}' = (\check{\boldsymbol{\sigma}}^{\top}||\check{\mathbf{0}}_{1\times(\tilde{m}-r)})\hat{\mathbf{A}}' - \check{\mathbf{y}}^{\top}(\boldsymbol{\Xi}^{\top}||\mathbf{F})\hat{\mathbf{A}}' \iff\\ \hat{\mathbf{c}}^{\top}\check{\mathbf{A}}' = \check{\mathbf{d}}^{\top}\hat{\mathbf{A}}',\end{aligned}$$

where $\hat{\mathbf{c}}^{\top} := (\hat{\mathbf{x}}^{\top}\widetilde{\boldsymbol{\Lambda}} - \hat{\boldsymbol{\rho}}^{\top}||\hat{\mathbf{x}}^{\top}\mathbf{E})$ and $\check{\mathbf{d}}^{\top} := (\check{\mathbf{y}}^{\top}\widetilde{\boldsymbol{\Xi}} - \check{\boldsymbol{\sigma}}^{\top}|| - \check{\mathbf{y}}^{\top}\mathbf{F})$.

Obviously

$$\mathbf{c} - \mathbf{d} \in \ker((\mathbf{A}')^{\top}) \iff (\mathbf{c} - \mathbf{d})^{\top}\mathbf{A}' = 0 \iff (\mathbf{c}_1^{\top} + \mathbf{c}_2^{\top}\mathbf{R}) - (\mathbf{d}_1^{\top} + \mathbf{d}_2^{\top}\mathbf{R}) \in \ker(\mathbf{A}^{\top}).$$

while, by assumption, $(\hat{\mathbf{x}}, \check{\mathbf{y}}) \notin \mathcal{L}_{\hat{\mathbf{M}},\check{\mathbf{N}}}$ and thus $\hat{\mathbf{x}}^{\top}\mathbf{E} \neq -\check{\mathbf{y}}^{\top}\mathbf{F}$, so $\mathbf{c} - \mathbf{d} \neq 0$. We conclude with an information-theoretic argument: because $\mathbf{R}$ is only revealed to B through $\mathbf{RA}$ the probability that $(\mathbf{c}_1^{\top} + \mathbf{c}_2^{\top}\mathbf{R}) \neq (\mathbf{d}_1^{\top} + \mathbf{d}_2^{\top}\mathbf{R})$ is $1 - 1/q$, so w.h.p, $(\hat{\mathbf{c}}_1^{\top} + \hat{\mathbf{c}}_2^{\top}\mathbf{R}), (\check{\mathbf{d}}_1^{\top} + \check{\mathbf{d}}_2^{\top}\mathbf{R})$ solves $\mathcal{D}_k$-$\mathsf{SKerMDH}$. ∎

B Additional details for QA-NIZK for Bit-Strings

B.1 Completeness

It is obvious by definition that for any $\hat{\mathbf{c}} \in \mathcal{L}_{\hat{\mathbf{U}},\mathsf{bits}}$ the vector $\hat{\mathbf{c}}_{\Delta}$ generated by an honest prover passes the verification test described in 1).

Note that, by definition of $\hat{\mathbf{C}}_{i,j}$ and $\check{\mathbf{D}}_{i,j}$, $\hat{\mathbf{C}}_{i,j}\check{\mathbf{I}}_{2\times 2} + \hat{\mathbf{I}}_{2\times 2}\check{\mathbf{D}}_{i,j} = \hat{\mathbf{g}}_i\check{\mathbf{h}}_j$. Since $b_i(b_i - 1) = 0$ for each

$i \in [n]$,

$$
\begin{aligned}
&\hat{\mathbf{c}}_{\Delta} \left(\check{\mathbf{d}} - \sum_{i\in[n]} \check{\mathbf{h}}_i \right)^{\top} \\
&= \sum_{i\in[n]} \left(b_i w_h \hat{\mathbf{g}}_i \check{\mathbf{h}}_{n+1}^{\top} + w_g (b_i - 1) \hat{\mathbf{g}}_{n+1} \check{\mathbf{h}}_i^{\top} + \sum_{j\in[n]} b_i (b_j - 1) \hat{\mathbf{g}}_i \check{\mathbf{h}}_j^{\top} \right) \\
&\quad + w_g w_h \hat{\mathbf{g}}_{n+1} \check{\mathbf{h}}_{n+1}^{\top} \\
&= \sum_{i\in[n]} \left(b_i w_h \hat{\mathbf{g}}_i \check{\mathbf{h}}_{n+1}^{\top} + w_g (b_i - 1) \hat{\mathbf{g}}_{n+1} \check{\mathbf{h}}_i^{\top} + \sum_{\substack{j\in[n] \\ j\neq i}} b_i (b_j - 1) \hat{\mathbf{g}}_i \check{\mathbf{h}}_j^{\top} \right) \\
&\quad + w_g w_h \hat{\mathbf{g}}_{n+1} \check{\mathbf{h}}_{n+1}^{\top} + \hat{\mathbf{R}} \check{\mathbf{I}}_{2\times 2} - \hat{\mathbf{I}}_{2\times 2} \check{\mathbf{R}} \\
&= \hat{\mathbf{\Theta}}_{b(\bar{b}-1)} \check{\mathbf{I}}_{2\times 2} + \hat{\mathbf{I}}_{2\times 2} \check{\mathbf{\Pi}}_{b(\bar{b}-1)}.
\end{aligned}
$$

Finally, the rest of the proof follows from completeness of $\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}$ and $\Psi_{\overline{\mathcal{D}}_k,+}$.

B.2 Soundness Proof

Lemma B.1 [Lemma 5.2 repeated] $\Pr\left[\mathsf{Game}_1(\mathsf{A}) = 1\right] \geq \frac{1}{n} \Pr\left[\mathsf{Game}_0(\mathsf{A}) = 1\right]$. ∎

Proof: The probability that $\mathsf{Game}_1(\mathsf{A}) = 1$ is the probability that a) $\mathsf{Game}_0(\mathsf{A}) = 1$ and b) $b_{i^*} \notin \{0, 1\}$. The view of adversary A is independent of i^*, while, if $\mathsf{Game}_0(\mathsf{A}) = 1$, then there is at least one index $\ell \in [n]$ such that such that $b_\ell \notin \{0, 1\}$. Thus, the probability that the event described in b) occurs conditioned on $\mathsf{Game}_0(\mathsf{A}) = 1$, is greater than or equal to $1/n$ and the lemma follows. ∎

Lemma B.2 [Lemma 5.4 repeated] There exists a $\mathcal{U}_1$-$\mathsf{MDDH}_{\check{\mathbb{H}}}$ adversary B such that $|\Pr\left[\mathsf{Game}_2(\mathsf{A}) = 1\right] - \Pr\left[\mathsf{Game}_3(\mathsf{A}) = 1\right]| \leq \mathsf{Adv}_{\mathcal{U}_1,\check{\mathbb{H}}}(\mathsf{B})$. ∎

Proof: The adversary B receives an instance of the $\mathcal{U}_1$-$\mathsf{MDDH}_{\check{\mathbb{H}}}$ problem, which is a pair $(\check{\mathbf{s}}, \check{\mathbf{t}})$, where $\check{\mathbf{s}}$ is a uniform vector of $\check{\mathbb{H}}^2$ and $\check{\mathbf{t}}$ is either a uniform vector in $\check{\mathbb{H}}^2$ or $\check{\mathbf{t}} = \gamma\check{\mathbf{s}}$, for random $\gamma \in \mathbb{Z}_q$.

Adversary B defines $\check{\mathbf{h}}_{n+1} := \check{\mathbf{s}}$ and the rest of the columns of $\check{\mathbf{H}}$ are honestly sampled with the sole exception of $\check{\mathbf{h}}_{i^*}$, which is set to $\check{\mathbf{t}}$.

Given that adversary B can only compute $\mathbf{g}_i \check{\mathbf{h}}_j^{\top} \in \check{\mathbb{H}}^{2\times 2}$, it defines $\check{\mathbf{D}}_{i,j} := \mathbf{g}_i \check{\mathbf{h}}_j^{\top} - \check{\mathbf{T}}_{i,j}$ and $\hat{\mathbf{C}}_{i,j} := \hat{\mathbf{T}}_{i,j}$, for $\mathbf{T}_{i,j} \leftarrow \mathbb{Z}_q^{2\times 2}$ and $(i, j) \in \mathcal{I}_{n,1}$. Note that this does not change the distribution of $(\check{\mathbf{D}}_{i,j}, \hat{\mathbf{C}}_{i,j})$, which is the uniform one conditioned on $\mathbf{C}_{i,j} + \mathbf{D}_{i,j} = \mathbf{g}_i \mathbf{h}_j^{\top}$.

The rest of the parameters are computed using $\mathbf{a} \leftarrow \mathcal{L}_1$, the matrix $\boldsymbol{\Delta} \in \mathbb{Z}_q^{2\times(n+1)}$ and the discrete logarithms of $\hat{\mathbf{G}}$. It is immediate to see that adversary B perfectly simulates Game_2 when $\check{\mathbf{t}} = \gamma\check{\mathbf{s}}$ and Game_3 when $\check{\mathbf{t}}$ is uniform. ▮

B.3 Efficiency

If we take $\mathcal{D}_k = \mathcal{L}_2$, the proof is of size of $2(\mathfrak{g}+\mathfrak{h})$ for $\hat{\mathbf{c}}_\Delta, \hat{\mathbf{d}}$, $4(\mathfrak{g}+\mathfrak{h})$ for $(\hat{\boldsymbol{\Theta}}_{b(\bar{b}-1)}, \check{\boldsymbol{\Pi}}_{b(\bar{b}-1)})$, and $4(\mathfrak{g}+\mathfrak{h})$ for $\hat{\boldsymbol{\rho}}_{b(\bar{b}-1)}, \hat{\boldsymbol{\rho}}_{b-\bar{b}}$ and $\check{\boldsymbol{\sigma}}_{b(\bar{b}-1)}, \check{\boldsymbol{\sigma}}_{b-\bar{b}}$. The whole proof size is $10(\mathfrak{g}+\mathfrak{h})$.

The CRS is of size $4(\mathfrak{g}+\mathfrak{h})$ for each pair $(\hat{\mathbf{C}}_{i,j}, \check{\mathbf{D}}_{i,j})$, so it adds up to $4(\mathfrak{g}+\mathfrak{h})((n+1)^2-n)$. To represent the matrix $\hat{\mathbf{U}}$ we need $n+1$ elements of $\hat{\mathbb{G}}$, $2(n+1)$ elements of $\hat{\mathbb{G}}$ for $\hat{\mathbf{G}}$ and $2(n+1)$ elements of $\check{\mathbb{H}}$ for $\check{\mathbf{H}}$. The size of $\mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k,+}}$ is $2(\mathfrak{g}+\mathfrak{h})((n+1)^2-n)+12(\mathfrak{g}+\mathfrak{h})$ and the size of $\mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}$ is $2(\mathfrak{g}+\mathfrak{h})(n+2)+8(\mathfrak{g}+\mathfrak{h})$. To represent $\check{\mathbf{a}}$ and $\check{\mathbf{a}}_\Delta$ we need $n+2$ elements of $\check{\mathbb{H}}$ In total, the CRS requires $6n^2+11n+33$ elements of $\hat{\mathbb{G}}$ and $6n^2+11n+34$ elements of $\check{\mathbb{H}}$.

The verifier computes $n+3$ pairings in the first step of the verification algorithm, 12 pairings in the second step, and $24+16$ pairings in the third step. The whole verification algorithm requires $n+55$ pairing computations.

C QA-NIZK Arguments for Bit-Strings in Symmetric Bilinear Groups

C.1 Symmetric Bilinear Groups

Throughout this section, $(q, \hat{\mathbb{G}}, \mathbb{T}, e, \hat{g}) \leftarrow \mathsf{Gen}_s(1^\lambda)$ is a description of a symmetric bilinear group, where $\hat{\mathbb{G}}, \mathbb{T}$ are groups of prime order q, the element $\hat{g}$ is a generator of $\hat{\mathbb{G}}$, and $e : \hat{\mathbb{G}} \times \hat{\mathbb{G}} \to \mathbb{T}$ is an efficiently computable, non-degenerate bilinear map.

We retake the definition and the examples of Matrix Diffie-Hellman Assumptions given in section 2, except that we drop the sub-indexes $\hat{\mathbb{G}}, \check{\mathbb{H}}$ as here $\hat{\mathbb{G}} = \check{\mathbb{H}}$. As a computational assumption, we will use the Kernel Assumption in symmetric bilinear groups.

Definition C.1 [Kernel Diffie-Hellman Assumption [30]] Let $\Gamma \leftarrow \mathsf{Gen}_s(1^\lambda)$. The Kernel Diffie-Hellman Assumption in $\hat{\mathbb{G}}$ ($\mathcal{D}_{\ell,k}$-KerMDH) says that every PPT Algorithm has negligible advantage in the following game: given $\hat{\mathbf{A}}$, $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, find a vector $\hat{\mathbf{r}} \in \check{\mathbb{H}}^\ell$, $\mathbf{r} \neq \mathbf{0}$, such that $\hat{\mathbf{r}}^\top \check{\mathbf{A}} = \mathbf{0}_\mathbb{T}$. ▮

A well-known instance of it is the Simultaneous Double Pairing (SDP) Assumption, which is the $\mathcal{L}_{3,2}$-KerMDH Assumption, using the notation defined in Sect. 2.1. Recall that:

$$\mathcal{L}_{3,2} : \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ a_3 & a_4 \end{pmatrix} \qquad a_1, a_2, a_3, a_4 \leftarrow \mathbb{Z}_q.$$

C.2 Intuition

In the symmetric case, a GS Proof that a commitment opens to a bit consists of a proof that the committed value b is such that $b(b-1)=0$. That is, compared to the asymmetric case, one does not need to commit to another value $\overline{b}$ and prove that $b(\overline{b}-1)=0$ and $b-\overline{b}=0$, which would be less efficient in terms of proof size. It is natural to ask if we can do the same when we extend our construction to the symmetric setting, that is, if we can use the same key to commit to both groups, set $\hat{\mathbf{c}}=\hat{\mathbf{d}}$ (now, $\hat{\mathbb{G}}=\check{\mathbb{H}}$) and only give a proof that $b_i(b_i-1)=0$ for all $i\in[n]$. Unfortunately, this approach completely fails, as we use in several places in a crucial way that $\hat{\mathbf{g}}_i$ and $\hat{\mathbf{h}}_i$ are sampled independently. For instance, this is essential to be able to use decisional assumptions in the image of $\hat{\mathbf{G}}$, or in the image of $\hat{\mathbf{H}}$.

Therefore, the construction in the symmetric case follows the same lines as in the asymmetric one. However, the construction is still a bit simpler in the symmetric case as there is no need to "split" $\mathbf{g}_i\mathbf{h}_j^\top$ as the matrices $\mathbf{C}_{i,j},\mathbf{D}_{i,j}$. Recall that, following the intuition given in Sect. 5.1, this was done to allow any simulator knowing one and only one of $\hat{\mathbf{g}}_i$ and $\check{\mathbf{h}}_j$ discrete logarithms to create a properly distributed CRS. In the symmetric case, this happens "for free", as $\hat{\mathbf{g}}_i\mathbf{h}_j^\top$ can be computed also as $\mathbf{g}_i\hat{\mathbf{h}}_j^\top$. As a consequence, we do not need to use our proof system from Sect. 3.2 and we can avoid the use of the Split Kernel Assumption.

In the construction below the matrix $\hat{\mathbf{U}}$ is such that its last two columns are sampled from $\mathcal{L}_{n+2,2}$ and the matrix $\mathbf{B}$ is sampled from $\mathcal{L}_{3,2}$, but they can easily be replaced by other matrix assumptions. However, with this choice, if $\mathcal{D}_k$ is also weaker than the 2-Lin Assumption, then security is based on assumptions which are all weaker than the 2-Lin Assumption. The construction can also be extended to the case where $\hat{\mathbf{c}}$ is the concatenation of several GS commitments. We omit any further details, as the extension is very similar as in the asymmetric case.

C.3 QA-NIZK Arguments For Bit-Strings

$\mathsf{K}_0(1^\lambda)$**:** Return $\Gamma:=(q,\hat{\mathbb{G}},\mathbb{T},e,\hat{g})\leftarrow\mathsf{Gen}_s(1^\lambda)$.

$\mathcal{D}_\Gamma$**:** The distribution $\mathcal{D}_\Gamma$ over $\hat{\mathbb{G}}^{(n+2)\times(n+2)}$ is the one induced by the following sampling procedure. To sample $\hat{\mathbf{U}}\leftarrow\mathcal{D}_\Gamma$, pick $\mathbf{A}\leftarrow\mathcal{L}_{n+2,2}$, for some given $\mathcal{L}_{n+2,2}$ matrix distribution and let the last two columns of $\mathbf{U}$ be equal to $\mathbf{A}$, i.e. $(\mathbf{u}_{n+1}||\mathbf{u}_{n+2})=\mathbf{A}$. Set $\mathbf{u}_i:=\mathbf{e}_i$, where $\mathbf{e}_i$ is the i th vector of the canonical basis of $\mathbb{Z}_q^{n+2}$. Finally, set $\hat{\mathbf{U}}:=(\hat{\mathbf{u}}_1||\ldots||\hat{\mathbf{u}}_{n+2})$. The distribution $\mathcal{D}_\Gamma$ defines the relation $\mathcal{R}_\Gamma=\{\mathcal{R}_{\hat{\mathbf{U}}}\}\subseteq\hat{\mathbb{G}}^{n+2}\times(\{0,1\}^n\times\mathbb{Z}_q^2)$, where $\hat{\mathbf{U}}\leftarrow\mathcal{D}_\Gamma$, such that $(\hat{\mathbf{c}},\langle\mathbf{b},\mathbf{w}\rangle)\in\mathcal{R}_{\hat{\mathbf{U}}}$ iff $\hat{\mathbf{c}}=\hat{\mathbf{U}}\binom{\mathbf{b}}{\mathbf{w}}$. The relation $\mathcal{R}_{par}$ consists of pairs $(\hat{\mathbf{U}},\mathbf{U})$ where $\hat{\mathbf{U}}\leftarrow\mathcal{D}_\Gamma$.

$\mathsf{K}_1(\Gamma,\hat{\mathbf{U}})$**:** Let $\hat{\mathbf{h}}_{n+1},\hat{\mathbf{h}}_{n+2}\leftarrow\mathbb{Z}_q^3$ and for all $i\in[n]$, $\hat{\mathbf{h}}_i:=\epsilon_{i,1}\hat{\mathbf{h}}_{n+1}+\epsilon_{i,2}\hat{\mathbf{h}}_{i,2}$, where $\epsilon_{i,1},\epsilon_{i,2}\leftarrow\mathbb{Z}_q$. Define $\hat{\mathbf{H}}:=(\hat{\mathbf{h}}_1||\ldots||\hat{\mathbf{h}}_{n+2})$. Choose $\boldsymbol{\Delta}\leftarrow\mathbb{Z}_q^{3\times(n+2)}$, define $\hat{\mathbf{G}}:=\boldsymbol{\Delta}\hat{\mathbf{U}}$ and define $\hat{\mathbf{g}}_i:=\boldsymbol{\Delta}\hat{\mathbf{u}}_i\in\hat{\mathbb{G}}^3$, for all $i\in[n+2]$. For any pair $(i,j)\in\mathcal{I}_{n,2}$, define:

$$\hat{\mathbf{C}}_{i,j}:=\hat{\mathbf{g}}_i\mathbf{h}_j^\top\in\hat{\mathbb{G}}^{3\times3},$$

where $\mathbf{h}_j$ is the vector of discrete logarithms of $\hat{\mathbf{h}}_j$.

Let $\Psi_{\overline{\mathcal{D}}_k}$ be an instance of a QA-NIZK proof system for proving membership in linear subspaces of $\hat{\mathbb{G}}^9$ (in symmetric groups), and let $\mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k}}\leftarrow\mathsf{K}_1(\Gamma,\{\hat{\mathbf{C}}_{i,j}\}_{(i,j)\in\mathcal{I}_{n,2}},9)$. Let $\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}$

be an instance of our QA-NIZK proof system from Sect. 3.3 adapted to the symmetric case and pick $\mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}} \leftarrow \mathsf{K}_1(\Gamma, \hat{\mathbf{G}}, \hat{\mathbf{H}}, n)$.

Let $\mathbf{B} \leftarrow \mathcal{L}_{3,2}$ and define $\mathbf{B}_\Delta := \boldsymbol{\Delta}^\top \mathbf{B} \in \hat{\mathbb{G}}_T^{(n+2)\times 2}$.

The common reference string is given by

$$\mathsf{crs}_P := \left(\hat{\mathbf{U}}, \hat{\mathbf{G}}, \hat{\mathbf{H}}, \mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k}}, \mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}\right), \mathsf{crs}_V := \left(\hat{\mathbf{B}}_\Delta, \hat{\mathbf{B}}, \mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k}}, \mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}\right).$$

$\mathsf{P}(\mathsf{crs}_P, \hat{\mathbf{c}}, (\mathbf{b}, \mathbf{w}_g))$**:** Pick $\mathbf{w}_h \leftarrow \mathbb{Z}_q^2$ and then:

1. Define
$$\hat{\mathbf{c}}_\Delta := \hat{\mathbf{G}} \begin{pmatrix} \mathbf{b} \\ \mathbf{w}_g \end{pmatrix}, \qquad \hat{\mathbf{d}} := \hat{\mathbf{H}} \begin{pmatrix} \mathbf{b} \\ \mathbf{w}_h \end{pmatrix}.$$
2. Compute
$$\begin{aligned} \hat{\mathbf{\Pi}}_{b(\bar{b}-1)} \quad := \quad & \sum_{i\in[n]} \sum_{\substack{j\in[n],\\ j\neq i}} b_i(b_j-1)\hat{\mathbf{C}}_{i,j} + \sum_{i\in[2]} \sum_{j\in[n]} w_{g,i}(b_j-1)\hat{\mathbf{C}}_{n+i,j} + \\ & \sum_{i\in[n]} \sum_{j\in[2]} b_i w_{h,j} \hat{\mathbf{C}}_{i,n+j} + \sum_{i\in[2]} \sum_{j\in[2]} w_{g,i} w_{h,j} \hat{\mathbf{C}}_{n+i,n+j}, \end{aligned}$$
3. Compute a proof $\hat{\boldsymbol{\sigma}}_{b(\bar{b}-1)}$ that $\hat{\mathbf{\Pi}}_{b(\bar{b}-1)}$ belongs to the space spanned by $\{\hat{\mathbf{C}}_{i,j}\}_{(i,j)\in\mathcal{I}_{n,2}}$, and a proof $\hat{\boldsymbol{\sigma}}_{b-\bar{b}}$ that $(\hat{\mathbf{c}}_\Delta, \hat{\mathbf{d}})$ open to the same value using $\mathbf{b}, \mathbf{w}_g$, and $\mathbf{w}_h$.

$\mathsf{V}(\mathsf{crs}_V, \hat{\mathbf{c}}, \langle \hat{\mathbf{c}}_\Delta, \hat{\mathbf{d}}, \hat{\mathbf{\Pi}}_{b(\bar{b}-1)}, \hat{\boldsymbol{\sigma}}_{b(\bar{b}-1)}, \hat{\boldsymbol{\sigma}}_{b-\bar{b}} \rangle)$**:**
1. Check if $\hat{\mathbf{c}}^\top \hat{\mathbf{B}}_\Delta = \hat{\mathbf{c}}_\Delta^\top \hat{\mathbf{B}}$.
2. Check if $\hat{\mathbf{c}}_\Delta (\hat{\mathbf{d}} - \sum_{i\in[n]} \hat{\mathbf{h}}_i)^\top = \hat{\mathbf{\Pi}}_{b(\bar{b}-1)} \hat{\mathbf{I}}_{3\times 3}$.
3. Verify proofs $\hat{\boldsymbol{\sigma}}_{b(\bar{b}-1)}, \hat{\boldsymbol{\sigma}}_{b-\bar{b}}$ for $\hat{\mathbf{\Pi}}_{b(\bar{b}-1)}$ and $(\hat{\mathbf{c}}_\Delta, \hat{\mathbf{d}})$.

If any of these checks fails, the verifier outputs 0, else it outputs 1.

Completeness. It is obvious by definition that any tuple $(\hat{\mathbf{c}}, \hat{\mathbf{c}}_\Delta)$ generated as described passes the verification test described in 1). On the other hand, given that $b_i(b_i - 1) = 0$ for each $i \in [n]$:

$$\begin{aligned}
&\hat{\mathbf{c}}_\Delta \left(\hat{\mathbf{d}} - \sum_{i\in[n]} \hat{\mathbf{h}}_i \right)^\top \\
&= \sum_{i\in[n]} \sum_{j\in[n]} b_i(b_j - 1)\hat{\mathbf{g}}_i \hat{\mathbf{h}}_j^\top + \sum_{i\in[2]} \sum_{j\in[n]} w_{g,i}(b_j - 1)\hat{\mathbf{g}}_{n+i} \hat{\mathbf{h}}_j^\top + \\
&\quad \sum_{i\in[n]} \sum_{j\in[2]} b_i w_{h,j} \hat{\mathbf{g}}_i \hat{\mathbf{h}}_j^\top + \sum_{i\in[2]} \sum_{j\in[2]} w_{g,i} w_{h,j} \hat{\mathbf{g}}_{n+i} \hat{\mathbf{h}}_{n+j}^\top \\
&= \sum_{i\in[n]} \sum_{\substack{j\in[n],\\ j\neq i}} b_i(b_j - 1)\hat{\mathbf{C}}_{i,j} \hat{\mathbf{I}}_{3\times 3} + \sum_{i\in[2]} \sum_{j\in[n]} w_{g,i}(b_j - 1)\hat{\mathbf{C}}_{n+i,j} \hat{\mathbf{I}}_{3\times 3} + \\
&\quad \sum_{i\in[n]} \sum_{j\in[2]} b_i w_{h,j} \hat{\mathbf{C}}_{i,n+j} \hat{\mathbf{I}}_{3\times 3} + \sum_{i\in[2]} \sum_{j\in[2]} w_{g,i} w_{h,j} \hat{\mathbf{C}}_{n+i,n+j} \hat{\mathbf{I}}_{3\times 3}.
\end{aligned}$$

Finally, the rest of the proof of completeness follows from completeness of $\Psi_{\overline{\mathcal{D}}_k}$ and $\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}$.

Soundness. We prove the following theorem.

Theorem C.2 Let $\mathsf{Adv}_{\mathcal{PS}}(\mathsf{A})$ be the advantage of an adversary A against the soundness of the proof system described above. There exist PPT adversaries $\mathsf{B}_1, \mathsf{B}_2, \mathsf{B}_3, \mathsf{P}_1^*, \mathsf{P}_2^*$ such that

$$\mathsf{Adv}_{\mathcal{PS}}(\mathsf{A}) \leq n \left(9/q + 2\mathsf{Adv}_{\mathcal{U}_2}(\mathsf{B}_1) + \mathsf{Adv}_{\mathsf{SDP}}(\mathsf{B}_3) + \mathsf{Adv}_{\Psi_{\overline{\mathcal{D}}_k}}(\mathsf{P}_1^*) + \mathsf{Adv}_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}(\mathsf{P}_2^*) \right).$$

∎

The proof follows from the indistinguishability of the following games:

- Real This is the real soundness game. The output is 1 if the adversary breaks the soundness, i.e. the adversary submits some $\hat{\mathbf{c}} = \hat{\mathbf{U}} \left(\begin{smallmatrix} \mathbf{b} \\ \mathbf{w}_g \end{smallmatrix} \right)$, for some $\mathbf{b} \notin \{0,1\}^n$ and $\mathbf{w} \in \mathbb{Z}_q^2$, and the corresponding proof which is accepted by the verifier.
- Game_0 This game is identical to game Real except that algorithm K_1 does not receive $\hat{\mathbf{U}}$ as a input but it samples $(\hat{\mathbf{U}}, \mathbf{U}) \in \mathcal{R}_{par}$ itself according to $\mathcal{D}_\Gamma$.
- Game_1 This game is identical to Game_0 except that the simulator picks a random $i^* \in [n]$, and uses $\mathbf{U}$ to check if the output of the adversary A is such that $b_{i^*} \in \{0,1\}$. It aborts if $b_{i^*} \in \{0,1\}$.
- Game_2 This game is identical to Game_1 except that now the vectors $\hat{\mathbf{g}}_i$, $i \in [n]$ and $i \neq i^*$, are uniform vectors in the space spanned by $\hat{\mathbf{g}}_{n+1}, \hat{\mathbf{g}}_{n+2}$.
- Game_3 This game is identical to Game_2 except that now the vector $\hat{\mathbf{h}}_{i^*}$ is a uniform vector in $\hat{\mathbb{G}}^3$, sampled independently of $\hat{\mathbf{h}}_{n+1}$, $\hat{\mathbf{h}}_{n+2}$.

It is obvious that the first two games are indistinguishable. The rest of the argument goes as follows.

Lemma C.3 $\Pr[\mathsf{Game}_1(\mathsf{A})] \geq \frac{1}{n}\Pr[\mathsf{Game}_0(\mathsf{A}) = 1]$. ∎

Proof: The probability that $\mathsf{Game}_1(\mathcal{A}) = 1$ is the probability that a) $\mathsf{Game}_0(\mathcal{A}) = 1$ and b) $b_{i^*} \notin \{0,1\}$. The view of adversary A is independent of i^*, while, if $\mathsf{Game}_0(\mathcal{A}) = 1$, then there is at least one index ℓ such that $b_\ell \notin \{0,1\}$. The probability that the event described in b) occurs conditioned on $\mathsf{Game}_0(\mathcal{A}) = 1$, is greater than or equal to $1/n$ and the lemma follows. ∎

Lemma C.4 There exists a $\mathcal{U}_2$-MDDH adversary B such that $|\Pr[\mathsf{Game}_1(\mathsf{A}) = 1] - \Pr[\mathsf{Game}_2(\mathsf{A}) = 1]| \leq \mathsf{Adv}_{\mathcal{U}_2}(\mathsf{B}) + 3/q$. ∎

Proof: The adversary B receives an instance of the $\mathcal{U}_2$-MDDH problem, i.e. $(\hat{\mathbf{A}}, \hat{\mathbf{t}})$, where $\hat{\mathbf{A}}$ is a uniform matrix in $\hat{\mathbb{G}}^{3\times 2}$ and $\hat{\mathbf{t}}$ is either a uniform vector $\hat{\mathbf{t}}$ in $\hat{\mathbb{G}}^3$ or $\hat{\mathbf{t}} = \hat{\mathbf{A}}\boldsymbol{\gamma}$, for $\boldsymbol{\gamma} \leftarrow \mathbb{Z}_q^2$. The simulator B defines all the parameters honestly, except that the $\mathcal{U}_2$-MDDH challenge is embedded in the matrix $\hat{\mathbf{G}}$.

Let $\hat{\mathbf{D}} := (\hat{\mathbf{A}}||\hat{\mathbf{t}})$. Adversary B picks $i^* \leftarrow [n]$, $\mathbf{W}_0 \leftarrow \mathbb{Z}_q^{3\times(i^*-1)}$, $\mathbf{W}_1 \leftarrow \mathbb{Z}_q^{3\times(n-i^*)}$, $\hat{\mathbf{g}}_{i^*} \leftarrow \hat{\mathbb{G}}^3$, and defines $\hat{\mathbf{G}} := (\hat{\mathbf{D}}\mathbf{W}_0||\hat{\mathbf{g}}_{i^*}||\hat{\mathbf{D}}\mathbf{W}_1||\hat{\mathbf{A}})$.

In the real algorithm K_1, the generator picks the matrix $\boldsymbol{\Delta} \in \mathbb{Z}_q^{3\times(n+2)}$. Although B but does not know $\boldsymbol{\Delta}$, it can compute $\hat{\boldsymbol{\Delta}} = \hat{\mathbf{G}}\mathbf{U}^{-1}$, given that $\mathbf{U}$ is full rank and B sampled $(\hat{\mathbf{U}}, \mathbf{U})$ itself. It is easy to see that it can generate the rest of the elements of the common reference string using $\hat{\boldsymbol{\Delta}}$, the discrete logarithms of $\hat{\mathbf{U}}$, $\hat{\mathbf{H}}$ and $\hat{\mathbf{B}}$.

In case $\hat{\mathbf{t}}$ is uniform over $\hat{\mathbb{G}}^3$, by the Schwartz-Zippel lemma $\det(\hat{\mathbf{D}}) = 0$ with probability at most $3/q$. Thus, with probability at least $1 - 3/q$, $\hat{\mathbf{D}}$ is a full rank matrix and $\hat{\mathbf{G}}$ is uniform over $\hat{\mathbb{G}}^{3\times(n+2)}$ as in Game_1. On the other hand, in case $\hat{\mathbf{t}} = \hat{\mathbf{A}}\boldsymbol{\gamma}$, $\{\hat{\mathbf{g}}_{n+1}, \hat{\mathbf{g}}_{n+2}\}$ is a basis for $\mathsf{Span}(\hat{\mathbf{D}})$ and each $\hat{\mathbf{g}}_i$, $i \in [n]$, $i \neq i^*$, is in the space spanned by $\hat{\mathbf{g}}_{n+1}, \hat{\mathbf{g}}_{n+2}$ as in Game_2. ∎

Lemma C.5 There exists a $\mathcal{U}_2$-MDDH adversary B such that $|\Pr[\mathsf{Game}_2(\mathsf{A}) = 1] - \Pr[\mathsf{Game}_3(\mathsf{A}) = 1]| \leq \mathsf{Adv}_{\mathcal{U}_2}(\mathsf{B})$. ∎

Proof: The adversary B receives an instance of the $\mathcal{U}_2$-MDDH problem, i.e. $(\hat{\mathbf{A}}, \hat{\mathbf{t}})$, where $\hat{\mathbf{A}}$ is a uniform matrix of $\hat{\mathbb{G}}^{3\times 2}$ and $\hat{\mathbf{t}}$ is either a uniform vector $\hat{\mathbf{t}}$ in $\hat{\mathbb{G}}^3$ or $\hat{\mathbf{t}} = \hat{\mathbf{A}}\boldsymbol{\gamma}$, $\boldsymbol{\gamma} \leftarrow \mathbb{Z}_q^2$. The simulator B defines $(\hat{\mathbf{h}}_{n+1}||\hat{\mathbf{h}}_{n+2}) := \hat{\mathbf{A}}$ and the rest of the columns of $\hat{\mathbf{H}}$ are honestly sampled with the sole exception of $\hat{\mathbf{h}}_{i^*}$, which is set to $\hat{\mathbf{t}}$. The rest of the parameters are computed by using $\mathbf{B} \leftarrow \mathcal{L}_{3,2}$, the matrix $\boldsymbol{\Delta} \in \mathbb{Z}_q^{3\times(n+2)}$, and the matrix of discrete logarithms of $\hat{\mathbf{U}}$.

It follows directly that adversary B perfectly simulates Game_2 when $\hat{\mathbf{t}} = \hat{\mathbf{A}}\boldsymbol{\gamma}$ and Game_3 when $\hat{\mathbf{t}}$ is uniform the output of B. ∎

Lemma C.6 There exists a SDP adversary B, and soundness adversaries $\mathsf{P}_1^*, \mathsf{P}_2^*$ for $\Psi_{\overline{\mathcal{D}}_k}$ and $\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}$, respectively, such that $\Pr[\mathsf{Game}_3(\mathsf{A}) = 1] \leq 6/q + \mathbf{Adv}_{\mathsf{SDP}}(\mathsf{B}) + \mathbf{Adv}_{\Psi_{\overline{\mathcal{D}}_k}}(\mathsf{P}_1^*) + \mathbf{Adv}_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}(\mathsf{P}_2^*)$. ∎

Proof: Let E be the event that $\{\mathbf{g}_{i^*}, \mathbf{g}_{n+1}, \mathbf{g}_{n+2}\}$ is a basis of $\hat{\mathbb{G}}^3$ and $\{\hat{\mathbf{h}}_{i^*}, \hat{\mathbf{h}}_{n+1}, \hat{\mathbf{h}}_{n+2}\}$ is a basis of $\hat{\mathbb{G}}^3$ (when parameters are generated as in Game_3). Clearly, $\Pr[E] = 1 - 6/q$, and

$$\begin{aligned}\Pr[\mathsf{Game}_3(\mathsf{A}) = 1] &= \Pr[\mathsf{Game}_3(\mathsf{A}) = 1 | E^c] \Pr[E^c] + \Pr[\mathsf{Game}_3(\mathsf{A}) = 1 | E] \Pr[E] \\ &\leq 6/q + \Pr[\mathsf{Game}_3(\mathsf{A}) = 1 | E].\end{aligned}$$

We next show that $\Pr[\mathsf{Game}_3(\mathsf{A}) = 1 | E] \leq \mathbf{Adv}_{\mathsf{SDP}}(\mathsf{B}) + \mathbf{Adv}_{\Psi_{\overline{\mathcal{D}}_k}}(\mathsf{P}_1^*) + \mathbf{Adv}_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}(\mathsf{P}_2^*)$, which concludes the proof.

Indeed, when E occurs, $\mathbf{g}_{i^*}\hat{\mathbf{h}}_{i^*}^\top$ is linearly independent from $\{\mathbf{g}_i\hat{\mathbf{h}}_j^\top : (i,j) \in [n+2]^2 \setminus \{(i^*, i^*)\}\}$. Additionally $\mathsf{Game}_3(\mathsf{A}) = 1$ implies that $b_{i^*} \notin \{0, 1\}$, while the verifier accepts the proof produced by A. Further, in this game, $\{\hat{\mathbf{h}}_{i^*}, \hat{\mathbf{h}}_{n+1}, \hat{\mathbf{h}}_{n+2}\}$ is a basis of $\hat{\mathbb{G}}^3$, so we can define $\overline{\mathbf{w}}_v \in \mathbb{Z}_q^2, \overline{b}_{i^*} \in \mathbb{Z}_q$ as the unique coefficients such that $\hat{\mathbf{d}} = \overline{b}_{i^*}\hat{\mathbf{h}}_{i^*} + \overline{w}_{h,1}\hat{\mathbf{h}}_{n+1} + \overline{w}_{h,2}\hat{\mathbf{h}}_{n+2}$. We distinguish three cases:

1) If $\hat{\mathbf{c}}_\Delta \neq \boldsymbol{\Delta}\hat{\mathbf{c}}$, we can construct an adversary B against the SDP Assumption. The SDP challenge is the matrix $\hat{\mathbf{B}}$ included in the common reference string. The adversary computes $\boldsymbol{\Delta}\hat{\mathbf{c}}$ and outputs $\hat{\mathbf{c}}_\Delta - \boldsymbol{\Delta}\hat{\mathbf{c}}$. This solves the SDP problem since both $\hat{\mathbf{c}}_\Delta$ and $\boldsymbol{\Delta}\hat{\mathbf{c}}$ pass the check 1) of the verification algorithm, so $(\boldsymbol{\Delta}\hat{\mathbf{c}} - \hat{\mathbf{c}}_\Delta)^\top \hat{\mathbf{B}} = (0_\mathbb{T}\ 0_\mathbb{T})$.

2) If $\hat{\mathbf{c}}_\Delta = \boldsymbol{\Delta}\hat{\mathbf{c}}$ but $b_{i^*} \neq \overline{b}_{i^*}$, this means that $(\hat{\mathbf{c}}_\Delta, \hat{\mathbf{d}})$ is not in the space associated to $\mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}$. This is because $(b_{i^*}\hat{\mathbf{g}}_{i^*}, \overline{b}_{i^*}\hat{\mathbf{h}}_{i^*})$ is l.i. from $\{(\hat{\mathbf{g}}_{i^*}, \hat{\mathbf{h}}_{i^*}), (\hat{\mathbf{g}}_{n+1}, \hat{\mathbf{h}}_{n+1}), (\hat{\mathbf{g}}_{n+2}, \hat{\mathbf{h}}_{n+2})\}$ whenever $b_{i^*} \neq \overline{b}_{i^*}$. Thus, we can construct an adversary P_2^* against the soundness of $\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}$ which outputs $\hat{\boldsymbol{\sigma}}$ as a fake proof for $(\hat{\mathbf{c}}_\Delta, \hat{\mathbf{d}})$.

3) If $\hat{\mathbf{c}}_\Delta = \boldsymbol{\Delta}\hat{\mathbf{c}}$, and $b_{i^*} = \overline{b}_{i^*}$, then $b_{i^*}(\overline{b}_{i^*} - 1) \neq 0$ (otherwise this would contradict the fact that $b_i^* \notin \{0, 1\}$). But in this case we can construct an adversary P_1^* against the soundness of $\Psi_{\overline{\mathcal{D}}_k}$ which outputs $\hat{\boldsymbol{\sigma}}_{b(\overline{b}-1)}$ as a fake proof for $\hat{\boldsymbol{\Pi}}_{b(\overline{b}-1)}$. Indeed, $\boldsymbol{\Pi}_{b(\overline{b}-1)} \notin \mathsf{Span}(\{\mathbf{C}_{i,j} : (i,j) \in \mathcal{I}_{n,2}\})$ given that the coordinate of $\boldsymbol{\Pi}_{b(\overline{b}-1)}$ in $\mathbf{g}_{i^*}\hat{\mathbf{h}}_{i^*}^\top$ is $b_{i^*}(\overline{b}_{i^*} - 1) \neq 0$.

This concludes the proof of soundness, we now prove zero-knowledge.

Zero-Knowledge.

- $\mathsf{S}_1(\Gamma, \hat{\mathbf{U}})$: The simulator receives as input a description of a symmetric bilinear group Γ and a matrix $\hat{\mathbf{U}} \in \hat{\mathbb{G}}^{(n+2)\times(n+2)}$ sampled according to distribution $\mathcal{D}_\Gamma$. It generates and outputs the common reference in the same way as K_1, but additionally it also outputs the simulation trapdoor

$$\tau = \left(\mathbf{H}, \boldsymbol{\Delta}, \tau_{\Psi_{\overline{\mathcal{D}}_k}}, \tau_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}\right).$$

- $\mathsf{S}_2(\mathsf{crs}_P, \hat{\mathbf{c}}, \tau)$: Compute $\hat{\mathbf{c}}_\Delta := \boldsymbol{\Delta}\hat{\mathbf{c}}$. Then pick random $(w_{h,1}, w_{h,2})$ and define

$$\mathbf{d} := \mathbf{H} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ w_{h,1} \\ w_{h,2} \end{pmatrix} = w_{h,1}\hat{\mathbf{h}}_{n+1} + w_{h,2}\hat{\mathbf{h}}_{n+2}.$$

  Then set:

$$\hat{\boldsymbol{\Pi}}_{b(\bar{b}-1)} \quad := \quad \hat{\mathbf{c}}_\Delta \left(\mathbf{d} - \sum_{i \in [n]} \hat{\mathbf{h}}_i \right)^\top .$$

  Finally, compute proofs $\hat{\boldsymbol{\sigma}}_{b(\bar{b}-1)}$ and $\hat{\boldsymbol{\sigma}}_{b-\bar{b}}$ for $\hat{\boldsymbol{\Pi}}_{b(\bar{b}-1)}$ and $(\hat{\mathbf{c}}_\Delta, \hat{\mathbf{d}})$ using $\tau_{\Psi_{\overline{\mathcal{D}}_k}}$ and $\tau_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}$.

Lemma C.7 The proof system is perfect quasi-adaptive zero-knowledge. ∎

Proof: First, note that the vector $\hat{\mathbf{d}} \in \hat{\mathbb{G}}^3$ output by the prover and the vector output by S_2 follow exactly the same distribution. This is because the rank of $\hat{\mathbf{H}}$ is 2. In particular, although the simulator S_2 does not know $\mathbf{b} \in \{0,1\}^n$, there exist $w_{h,1}, w_{h,2} \in \mathbb{Z}_q$ such that $\hat{\mathbf{d}} = \mathbf{H} \begin{pmatrix} \mathbf{b} \\ w_{h,1} \\ w_{h,2} \end{pmatrix}$. On the other hand, it is obvious by construction that $\hat{\boldsymbol{\Pi}}_{b(\bar{b}-1)}$ is uniquely determined by $\hat{\mathbf{c}}, \hat{\mathbf{d}}$ and the rest of the argument follows from the perfect zero-knowledge property of $\Psi_{\overline{\mathcal{D}}_k}$ and $\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}$. ∎

C.4 Efficiency

When $\mathcal{D}_k = \mathcal{L}_2$, our proofs consist of 6 group elements for $\hat{\mathbf{c}}_\Delta$ and $\hat{\mathbf{d}}$, 9 group elements for $\hat{\boldsymbol{\Pi}}_{b(\bar{b}-1)}$, and 4 group elements for $\hat{\boldsymbol{\sigma}}_{b(\bar{b}-1)}$ and $\hat{\boldsymbol{\sigma}}_{b-\bar{b}}$. The whole proof consist of 19 elements of $\hat{\mathbb{G}}$.

The CRS consists of 9 group elements for each $\hat{\mathbf{C}}_{i,j}$, which sums up to a total of $9((n+2)^2 - n)$. To represent $\hat{\mathbf{U}}$ we need $2(n+1)$ group elements, $3(n+2)$ elements for matrix $\hat{\mathbf{G}}$, $3(n+2)$ elements for $\hat{\mathbf{H}}$, $2((n+2)^2 - n) + 33$ elements for $\mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k}}$, $2n + 36$ elements for $\mathsf{crs}_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}$, and $4 + 2(n+2)$ elements for $\hat{\mathbf{B}}, \hat{\mathbf{B}}_\Delta$. The whole CRS needs a total of $11n^2 + 45n + 135$ elements of $\hat{\mathbb{G}}$.

The verifier computes $2n + 10$ pairings in the first step of the verification algorithm, 18 pairings in the second step, 38 pairings in the last step. The whole verification algorithm requires $2n + 66$ pairing computations.

D Complete Description of Applications

D.1 More Efficient Proof of Membership in a List of Vectors

For our proof of membership in a (witness samplable, static) list of size $\Theta(\sqrt[3]{n})$ which we describe next, we use as a building block our improvement of the proof of membership in a list of Chandran *et al.* extended to vectors, i.e. to the case where $L = (\hat{\mathbf{l}}_1, \ldots, \hat{\mathbf{l}}_n)$ is a list of vectors of length ℓ. In such a proof, we show that some commitment $\hat{\mathbf{c}}$ opens to a vector $\hat{\mathbf{l}}_\alpha$, where $\alpha = (i_\alpha, j_\alpha)$ (recall that $(i,j) = \sqrt{n}(i-1) + j$).

1. Compute GS commitments in $\check{\mathbb{H}}$ to $b_1 \ldots, b_m$ and $b'_1, \ldots, b'_m$, where $b_i = 1$ if $i = i_\alpha$ and 0 otherwise, and $b'_j = 1$ if $j = j_\alpha$, and 0 otherwise.
2. Compute a proof that $b_i \in \{0,1\}$ and $b'_j \in \{0,1\}$ for all $i, j \in [m]$, using the proof system of Sect. 5.3.
3. Compute GS proofs that $\sum_{i\in[m]} b_i = 1$ and $\sum_{j\in[m]} b'_j = 1$.
4. Compute GS commitments to each coordinate of $\hat{\mathbf{x}}_1 := \hat{\mathbf{l}}_{(i_\alpha,1)}, \ldots, \hat{\mathbf{x}}_m := \hat{\mathbf{l}}_{(i_\alpha,m)}$.
5. Compute an aggregated GS proof that the equations $\hat{\mathbf{x}}_j = \sum_{i\in[m]} b_i \hat{\mathbf{l}}_{(i,j)}$, for all $j \in [m]$, are satisfied, as detailed in Sect. 4.
6. Compute a GS proof that $\hat{\mathbf{l}}_\alpha = \sum_{j\in[m]} b'_j \hat{\mathbf{x}}_j$ is satisfied.

We emphasize that the CRS depends on the list L. This is necessary to aggregate the proofs as in Step 4. More specifically, to aggregate the proof of the equations $\hat{\mathbf{x}}_j = \sum_{i\in[m]} b_i \hat{\mathbf{l}}_{(i,j)}$, $j \in [m]$ (that is, a total of ℓk equations), we need to include in the CRS some information which depends on the coordinates of $\hat{\mathbf{l}}_{(i,j)}$ as explained in Sect. 5.3.

Theorem D.1 If L is witness samplable, the above protocol is a perfectly complete, computationally sound, and computationally zero-knowledge proof system for the language of commitments to elements from the list L. ∎

Proof: Completeness follows directly from the completeness of the building blocks. Soundness follows directly from the perfect soundness of GS proofs together with the computational soundness of aggregation of GS proofs. For computational zero-knowledge, if $\mathsf{crs}_{\mathrm{GS}} := (\Gamma, \hat{\mathbf{u}}_1, \hat{\mathbf{u}}_2, \check{\mathbf{v}}_1, \check{\mathbf{v}}_2)$ is the GS common reference string in the soundness setting as defined in Sect. 2.2, switch to a game where $\check{\mathbf{v}}_1 = \epsilon \check{\mathbf{v}}_2$. Under the DDH Assumption in $\check{\mathbb{H}}$, the new CRS is computationally indistinguishable from the original CRS. In a simulated proof, commit to $b_i = 0$, $b'_j = 0$ for all $i, j \in [m]$. In step 2, simply compute a real proof. In step 3, use the GS simulation algorithm (with trapdoor ϵ) to simulate the proof. In Step 4, set $\hat{\mathbf{x}}_j = \hat{\mathbf{0}}$. Finally, in step 6, simulate a proof using ϵ. It is not hard to see that such a proof can be simulated even without knowledge of an opening of $\hat{\mathbf{c}}$. ∎

D.2 A $\Theta(\sqrt[3]{n})$ Proof of Membership in a Witness Samplable and Static List

We give a proof of membership in a list with improved asymptotic proof size when the list is drawn from a witness samplable distribution and the CRS depends on the list.

The main idea is to combine the previous proof of membership in a list with a Split Kernel Assumption. Specifically, the CRS includes a matrix $\check{\mathbf{A}}$, $\mathbf{A} \leftarrow \mathcal{D}_{m,2}$, whose rows are denoted $\check{\boldsymbol{a}}_1, \ldots, \check{\boldsymbol{a}}_m$ and a list

$$L' := \left(\sum_{i\in[m]} \boldsymbol{a}_i \hat{l}_{(i,1,1)}, \sum_{i\in[m]} \boldsymbol{a}_i \hat{l}_{(i,1,2)}, \ldots, \sum_{i\in[m]} \boldsymbol{a}_i \hat{l}_{(i,m,m)} \right) \in \hat{\mathbb{G}}^{2\times m^2},$$

where $m := \sqrt[3]{n}$, $(i,j,k) = m^2(i-1) + m(j-1) + k \in [n]$. As before, the goal to prove is that a commitment $\hat{\mathbf{c}}$ opens to some $\hat{l}_\alpha \in L = (\hat{l}_1, \ldots, \hat{l}_n)$ and $(i_\alpha, j_\alpha, k_\alpha)$ are such that $\alpha = (i_\alpha, j_\alpha, k_\alpha)$.

1. Commit to $\hat{\mathbf{y}} := \sum_{i\in[m]} \boldsymbol{a}_i \hat{l}_{(i,j_\alpha,k_\alpha)}$ such that $\alpha = (i_\alpha, j_\alpha, k_\alpha)$.
2. Using the proof described in Sect. D.1, show that $\hat{\mathbf{y}}$ is an element of L'.
3. Compute commitments to $\hat{z}_i := \hat{l}_{(i,j_\alpha,k_\alpha)}$, for each $i \in [m]$.
4. Compute a GS proof for the equations $\hat{\mathbf{y}}\check{h} = \sum_{i\in[n]} \check{\boldsymbol{a}}_i \hat{z}_i$.
5. Compute GS commitments in $\check{\mathbb{H}}$ to $b_1 \ldots, b_m \in \{0,1\}$, where $b_i = 1$ if $i = i_\alpha$ and 0 otherwise.
6. Using our proof system from Sect. 5.3 prove that $b_i \in \{0,1\}$ for all $i \in [m]$.
7. Compute GS proofs for the satisfiability of equations $\sum_{i\in[m]} b_i = 1$ and $\hat{l}_\alpha = \sum_{i\in[m]} b_i \hat{z}_i$.

The first step is to commit to $\hat{\mathbf{y}} := \sum_{i\in[m]} \boldsymbol{a}_i \hat{l}_{(i,j_\alpha,k_\alpha)}$ and use the previous proof system to prove $\hat{\mathbf{y}} \in L'$. The next step is to commit to $\hat{z}_i := \hat{l}_{(i,j_\alpha,k_\alpha)}$ and prove that $\sum_{i\in[m]} \check{\boldsymbol{a}}_i \hat{z}_i = \check{h}\hat{\mathbf{y}}$ holds. Finally, steps 5 and 6 prove that $\hat{l}_\alpha$ is an element of the list $(\hat{z}_1, \ldots, \hat{z}_m)$. For the last statement, compute GS commitments to b_i, $i \in [m]$, and prove that $\sum_{i\in[m]} b_i \hat{z}_i = \hat{l}_\alpha$, $\sum_{i\in[m]} b_i = 1$ and $b_i \in \{0,1\}$.[8]

Theorem D.2 If L is witness samplable, the above protocol is a perfectly complete, computationally sound, and computationally zero-knowledge proof system for the language of commitments to elements from the list L. ∎

Completeness follows directly from the completeness of the building blocks.

Proof: Completeness follows directly from the completeness of the building blocks. Soundness can be argued as follows. If the list is witness samplable, the CRS can be generated given an instance of the $\mathcal{D}_{m,2} - \mathsf{SKerMDH}$ Assumption, $(\hat{\mathbf{A}}, \check{\mathbf{A}})$. By the soundness of the extension of the proof of Chandran *et al.* of Sect.D.1, it holds that $\hat{\mathbf{y}} = \sum_{i\in[m]} \boldsymbol{a}_i \hat{l}_{(i,j,k)}$ for some $j, k \in [m]$. Because of the perfect soundness of GS proofs it must hold that $\sum_{i\in[m]} \check{\boldsymbol{a}}_i \hat{z}_i = \hat{\mathbf{y}}\check{h} = \sum_{i\in[m]} \check{\boldsymbol{a}}_i \hat{l}_{(i,j,k)}$. It

[8] Such statement can also be proven using again the proof of membership in a list, and the proof will be of size $\Theta(\sqrt[6]{n})$. Note this is not exactly a proof of membership in a list, since only the commitments to the elements in the list are public. However, it is not hard to construct a proof system for that statement using the same ideas as Chandran *et al.*

must also be the case that $\hat{z}_1 = \hat{l}_{(1,j,k)}, \ldots, \hat{z}_m = \hat{l}_{(m,j,k)}$, because otherwise the pair $(\hat{\boldsymbol{\rho}}, \check{\mathbf{0}})$, where $\hat{\boldsymbol{\rho}} := (\hat{z}_1 - \hat{l}_{(1,j,k)}, \ldots, \hat{z}_m - \hat{l}_{(m,j,k)})$ is a solution to the $\mathcal{D}_{m,2}$-SKerMDH challenge, as $\hat{\boldsymbol{\rho}}\check{\mathbf{A}} = \check{\mathbf{0}}\hat{\mathbf{A}}$. Soundness of the last step implies that $b_i \in \{0,1\}$, for all $i \in [m]$, and that $\sum_{i\in[m]} b_i = 1$. Therefore, there exists a unique $i \in [m]$ such that $b_i = 1$. Finally, $\hat{l}_\alpha = \sum_{i\in[m]} b_i \hat{z}_i$ implies that $\hat{\mathbf{c}}$ opens to $\hat{l}_\alpha = \hat{z}_i = \hat{l}_{(i,j,k)}$. Zero-knowledge follows from the same argument as in the proof of Theorem D.1. ∎

E Structure Preserving Linearly Homomorphic Signatures

Linearly-homomorphic structure preserving signatures [1, 7] enable to sign group elements in G, where G is a group and to publicly derive signatures of new elements which are a linear combination of other signed messages. We take the definition from [26], except that we do not identify the elements of G with vectors in $\hat{\mathbb{G}}^n$, for some group $\hat{\mathbb{G}}$. The reason is that G might be some space of the form $\hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n$.

Definition E.1 [SPLHS scheme] A linearly homomorphic structure-preserving signature scheme over the group G consists of a tuple of efficient algorithms Φ=(SignGen, Sign, SignDerive, Verify) for which the message space is $\mathcal{M} := G$, with the following specifications.

$\mathsf{SignGen}(1^\lambda, n)$: is a randomized algorithm that takes as input a security parameter $\lambda \in \mathbb{N}$ and an integer n and outputs a key pair (pk, sk). The public key pk specifies a $\mathbb{Z}_q$ vector space G of dimension n.

$\mathsf{Sign}(sk, \mathbf{m})$**:** is a possibly probabilistic algorithm that takes as input a private key sk and $\mathbf{m} \in G$. It outputs a signature $\boldsymbol{\sigma} \in G$.

$\mathsf{SignDerive}(pk, \{\omega_i, \boldsymbol{\sigma}_i, \mathbf{m}_i\}_{i\in[\ell]})$**:** is a (possibly probabilistic) signature derivation algorithm. It takes as input a public key pk as well as ℓ pairs $(\omega_i, \boldsymbol{\sigma}_i)$, each of which consists of a weight $\omega_i \in \mathbb{Z}_q$ and a signature $\boldsymbol{\sigma}_i \in G$. The output is a signature $\boldsymbol{\sigma} \in G$ on the vector $\mathbf{m} = \sum_{i\in[\ell]} \omega_i \mathbf{m}_i$.

$\mathsf{Verify}(pk, \mathbf{m}, \boldsymbol{\sigma})$**:** is a deterministic algorithm that takes in a public key pk, a signature $\boldsymbol{\sigma}$, and a vector $\mathbf{m}$. It outputs 1 if $\boldsymbol{\sigma}$ is deemed valid and 0 otherwise.

∎

Correctness is expressed by imposing that, for all security parameters $\lambda \in \mathbb{N}$, all integers $n \in \mathrm{poly}(\lambda)$ and all pairs $(pk, sk) \leftarrow \mathsf{SignGen}(1^\lambda, n)$, the following holds:

1. For all $\mathbf{m} \in G$, if $\boldsymbol{\sigma} = \mathsf{Sign}(sk, \mathbf{m})$, then we have $\mathsf{Verify}(pk, \mathbf{m}, \boldsymbol{\sigma}) = 1$.
2. For any $\ell > 0$ and any set of triples $\{(\omega_i, \boldsymbol{\sigma}_i, \mathbf{m}_i)\}_{i\in[\ell]}$, if $\mathsf{Verify}(pk, \mathbf{m}_i, \boldsymbol{\sigma}_i) = 1$ for each $i \in [\ell]$, then $\mathsf{Verify}(pk, \sum_{i\in[\ell]} \omega_i \mathbf{m}_i, \mathsf{SignDerive}(pk, \{(\omega_i, \boldsymbol{\sigma}_i)\})) = 1$

In order to get a uniform definition for different types of forgery, we will say that a pair $(\mathbf{m}^*, \boldsymbol{\sigma}^*)$ is a forgery if $P(\mathbf{m}^*, Q) = 1$, where P is a predicate on $(\mathbf{m}^*, Q)$ and Q is the set of reveal queries

made by the adversary. We stress that the predicate P is not always efficiently computable. For instance, for the scheme of Libert *et al.* ([26]), this predicate is 1 iff $\mathbf{m}^*$ is in the linear span of previous queries, and this is, in general, hard to decide in the group G (although it might be easy for some set Q).

Definition E.2 A SPLHS scheme $\Phi = (\mathsf{SignGen}, \mathsf{Sign}, \mathsf{Verify}, \mathsf{SignDerive})$ is secure against Type P adversaries if no PPT adversary has non-negligible advantage in the game below:

1. The adversary A chooses an integer $n \in \mathbb{N}$ and sends it to the challenger who runs $\mathsf{SignGen}(1^\lambda, n)$ and obtains (pk, sk) before sending pk to A.

2. On polynomially-many occasions, A can interleave the following kinds of queries.

   Signing queries: A chooses a vector $\mathbf{m} \in \mathsf{Gen}$. The challenger picks a handle h and computes $\boldsymbol{\sigma} \leftarrow \mathsf{Sign}(sk, \mathbf{m})$. It stores $(h, \mathbf{m}, \boldsymbol{\sigma})$ in a table T and returns h.

   Derivation queries: A chooses a vector of handles $\vec{h} = (h_1, \ldots, h_\ell)$ and a set of coefficients $\{\omega_i\}_{i\in[\ell]}$. The challenger retrieves the tuples $\{(h_i, \mathbf{m}_i, \boldsymbol{\sigma}_i)\}_{i\in[\ell]}$ from T and returns $\perp$ if one of these does not exist. Otherwise, it computes $\mathbf{m} = \sum_{i\in[\ell]} \omega_i \mathbf{m}_i$ and runs $\boldsymbol{\sigma} \leftarrow \mathsf{SignDerive}(pk, \{(\omega_i, \boldsymbol{\sigma}_i)\}_{i\in[\ell]})$. It also chooses a handle h, stores $(h, \mathbf{m}, \boldsymbol{\sigma})$ in T and returns h to A.

   Reveal queries: A chooses a handle h. If no tuple of the form $(h, \mathbf{m}, \boldsymbol{\sigma})$ exists in T, the challenger returns $\perp$. Otherwise, it returns $\boldsymbol{\sigma}$ to A and adds $(\mathbf{m}, \boldsymbol{\sigma})$ to the set Q.

3. A outputs a signature $\boldsymbol{\sigma}^*$ and a vector $\mathbf{m}^*$. The adversary A wins if $P(\mathbf{m}^*, Q) = 1$.

As advantage is its probability of success taken over all coin tosses. ∎

Libert *et al.* also used a set $\mathcal{T}$ of tags in order to add up many instances of their signature scheme in only one. For simplicity, we omit this parameter.

E.1 One-Time LHSPS Signatures in Different Groups

The one-time linearly homomorphic signature of Libert, Peters and Yung [27] implies a QA-NIZK Argument for linear spaces. Similarly, our constructions of QA-NIZK proofs for membership in concatenated subspace and for sum in subspace (in the case where the space is not from a witness samplable distribution) also have an equivalent one-time structure preserving signature scheme with different security properties.

In particular, for subspace concatenation, "one-time" means that the adversary is unable to sign vectors which are not in the span of previously signed vectors, namely, the adversary cannot output a signature for a pair $(\hat{\mathbf{x}}^*, \check{\mathbf{y}}^*) \in \hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n$ if $((\mathbf{x}^*)^\top || (\mathbf{y}^*)^\top)$ is linearly independent from the vectors $(\mathbf{x}_i^\top || \mathbf{y}_i^\top)$, $i \in [q_s]$, (the concatenation of two vectors), where $(\hat{\mathbf{x}}_i, \check{\mathbf{y}}_i)$ are the signing queries of the adversary. The discussion for the scheme which results from our Sum-in-Subspace QA-NIZK proof, results in a different notion of "one-time" — this is captured in the security definition by a different predicate P —, see discussion below.

In either case, the size of the resulting signatures is $(k+1)(\mathfrak{g}+\mathfrak{h})$ under the $\mathsf{SKerMDH}$ Assumption, but if security against random message attacks is sufficient (meaning that the signatures in the set

Q which are seen by the adversary are sampled uniformly at random), the signature size can be reduced to $k(\mathfrak{g}+\mathfrak{h})$ (essentially, in this case one can sample $\mathbf{A}$ from $\overline{\mathcal{D}}_k$). This is inspired by the one-time constructions of structure-preserving signatures of [24] secure against random message attacks. We omit any further discussion of this case, as it is a straightforward generalization of our QA-NIZK proofs in the witness samplable setting using the ideas of [24].

Our construction is based on the SKerMDH Assumption introduced in section 2. Following the syntactic definition of section E, our scheme assumes $G = \hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n$ and the length of the messages is $n+m$.

- $\mathsf{SignGen}(1^\lambda, m, n)$: Let $(q, \hat{\mathbb{G}}, \check{\mathbb{H}}, \mathbb{T}, e, \hat{g}, \check{h}) \leftarrow \mathsf{Gen}_a(1^\lambda)$. Choose $\mathbf{A} \leftarrow \mathcal{D}_k$, $\mathbf{\Lambda}, \mathbf{\Xi} \leftarrow \mathbb{Z}_q^{(k+1)\times m}$, $\mathbf{A}_\Lambda := \mathbf{\Lambda}^\top \mathbf{A}$, $\mathbf{A}_\Xi := \mathbf{\Xi}^\top \mathbf{A}$ The secret key is $\mathsf{sk} = (\mathbf{\Lambda}, \mathbf{\Xi})$, while the public key is defined to be

$$\mathsf{pk} = (\hat{\mathbf{A}}, \hat{\mathbf{A}}_\Xi, \check{\mathbf{A}}, \check{\mathbf{A}}_\Lambda) \in \hat{\mathbb{G}}^{(k+1)\times k} \times \hat{\mathbb{G}}^{m\times k} \times \check{\mathbb{H}}^{(k+1)\times k} \times \check{\mathbb{H}}^{m\times k}.$$

- $\mathsf{Sign}(\mathsf{sk}, (\hat{\mathbf{x}}, \check{\mathbf{y}}))$: To sign a vector $(\hat{\mathbf{x}}, \check{\mathbf{y}}) \in \hat{\mathbb{G}}^m \times \check{\mathbb{H}}^m$, pick $\mathbf{z} \leftarrow \mathbb{Z}_q^{(k+1)}$ and output the pair $(\hat{\boldsymbol{\rho}}, \check{\boldsymbol{\sigma}}) \in \hat{\mathbb{G}}^{(k+1)} \times \check{\mathbb{H}}^{(k+1)}$, defined as:

$$\hat{\boldsymbol{\rho}} := \mathbf{\Lambda}\hat{\mathbf{x}} + \hat{\mathbf{z}}, \qquad \check{\boldsymbol{\sigma}} := \mathbf{\Xi}\check{\mathbf{y}} - \check{\mathbf{z}}.$$

- $\mathsf{SignDerive}(\mathsf{pk}, \{(\omega_i, \hat{\boldsymbol{\rho}}_i, \check{\boldsymbol{\sigma}}_i)\}_{i=1}^\ell)$: given the public key pk, and ℓ tuples $(\omega_i, \hat{\boldsymbol{\rho}}_i, \check{\boldsymbol{\sigma}}_i)$, output the pair $(\sum_{i=1}^\ell \omega_i \hat{\boldsymbol{\rho}}_i, \sum_{i=1}^\ell \omega_i \check{\boldsymbol{\sigma}}_i) \in \hat{\mathbb{G}}^{(k+1)} \times \check{\mathbb{H}}^{(k+1)}$.
- $\mathsf{Verify}(\mathsf{pk}, (\hat{\mathbf{x}}, \check{\mathbf{y}}), (\hat{\boldsymbol{\rho}}, \check{\boldsymbol{\sigma}}))$ is a deterministic algorithm, that takes as input a public key pk, a signature $(\hat{\boldsymbol{\rho}}, \check{\boldsymbol{\sigma}})$ and returns 1 if and only if $(\hat{\boldsymbol{\rho}}, \check{\boldsymbol{\sigma}})$ satisfies

$$\hat{\boldsymbol{\rho}}^\top \check{\mathbf{A}} + \check{\boldsymbol{\sigma}}^\top \hat{\mathbf{A}} = \hat{\mathbf{x}}^\top \check{\mathbf{A}}_\Lambda + \check{\mathbf{y}}^\top \hat{\mathbf{A}}_\Xi.$$

Correctness. If a signature is correctly generated then

$$\hat{\boldsymbol{\rho}}^\top \check{\mathbf{A}} - \hat{\mathbf{x}}^\top \check{\mathbf{A}}_\Lambda = \hat{\mathbf{z}}^\top \check{\mathbf{A}} \qquad \check{\boldsymbol{\sigma}}^\top \hat{\mathbf{A}} - \check{\mathbf{y}}^\top \hat{\mathbf{A}}_\Xi = -\check{\mathbf{z}}^\top \hat{\mathbf{A}}.$$

Therefore the verification algorithm outputs 1 on a correctly generated signature. The proof of correctness of the signature derivation algorithm follows a similar argument.

Let $Q = \{(\hat{\mathbf{x}}_i, \check{\mathbf{y}}_i)\}_{i\in[q_s]}$ be some set of elements of $\hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n$. We define the predicate P as $P((\hat{\mathbf{x}}, \check{\mathbf{y}}), Q) = 1$ iff $(\mathbf{x}^\top || \mathbf{y}^\top) \in \mathbb{Z}_q^{2m}$ is not in the space spanned by $\{(\mathbf{x}_i^\top || \mathbf{y}_i^\top) : i \in [q_s]\}$.

Theorem E.3 The signature scheme is Type P unforgeable if the SKerMDH Assumption holds in $\hat{\mathbb{G}}, \check{\mathbb{H}}$. ∎

The argument is almost identical to [26]. **Proof:** We show how to construct an algorithm B which takes as input an instance $(\hat{\mathbf{A}}, \check{\mathbf{A}})$ of the SKerMDH Assumption and outputs a pair of vectors $(\hat{\mathbf{r}}, \check{\mathbf{s}}) \in \hat{\mathbb{G}}^3 \times \check{\mathbb{H}}^3$, $\mathbf{r} \neq \mathbf{s}$, such that $\hat{\mathbf{r}}^\top \check{\mathbf{A}} = \check{\mathbf{s}}^\top \hat{\mathbf{A}}$ given oracle access to a forger F against the signature scheme (see Sect. E).

Algorithm B starts by honestly running the key generation algorithm using a randomly chosen $\mathsf{sk} = (\mathbf{\Lambda}, \mathbf{\Xi})$. Any signature query of F on a vector $(\hat{\mathbf{x}}, \check{\mathbf{y}})$ is honestly answered by B, by running

the signing algorithm. The game ends with F outputting a vector $(\hat{\mathbf{x}}^*, \check{\mathbf{y}}^*)$ with a valid signature $(\hat{\boldsymbol{\rho}}^*, \check{\boldsymbol{\sigma}}^*)$. At this point, B computes its own signature $(\hat{\boldsymbol{\rho}}^\dagger, \check{\boldsymbol{\sigma}}^\dagger)$ using the secret key $\mathsf{sk} := (\boldsymbol{\Lambda}, \boldsymbol{\Xi})$. The adversary B will output as a response to the $\mathsf{SKerMDH}$ challenge the pair $(\hat{\boldsymbol{\rho}}^* - \hat{\boldsymbol{\rho}}^\dagger, \check{\boldsymbol{\sigma}}^\dagger - \check{\boldsymbol{\sigma}}^*)$.

We now see that, with overwhelming probability, this is a valid answer to the $\mathsf{SKerMDH}$ challenge. Indeed, since both signatures satisfy the verification equation, we can subtract the verification equation of each pair, obtaining:

$$(\hat{\boldsymbol{\rho}}^* - \hat{\boldsymbol{\rho}}^\dagger)^\top \check{\mathbf{A}} = (\check{\boldsymbol{\sigma}}^\dagger - \check{\boldsymbol{\sigma}}^*)^\top \hat{\mathbf{A}}$$

Therefore, all we need to argue is that $\boldsymbol{\rho}^* - \boldsymbol{\rho}^\dagger \neq \boldsymbol{\sigma}^\dagger - \boldsymbol{\sigma}^*$ with overwhelming probability. This is equivalent to show that the probability that $\boldsymbol{\rho}^* + \boldsymbol{\sigma}^* = \boldsymbol{\rho}^\dagger + \boldsymbol{\sigma}^\dagger$ is negligible. The key point of the argument is that

$$\boldsymbol{\rho}^\dagger + \boldsymbol{\sigma}^\dagger = \boldsymbol{\Lambda}\mathbf{x}^* + \boldsymbol{\Xi}\mathbf{y}^* = \begin{pmatrix} \boldsymbol{\Lambda} & \boldsymbol{\Xi} \end{pmatrix} \begin{pmatrix} \mathbf{x}^* \\ \mathbf{y}^* \end{pmatrix}$$

is information theoretically hidden to F.

The rest of the argument is identical to [26]. The argument goes as follows: since, by assumption, $\begin{pmatrix} \mathbf{x}^* \\ \mathbf{y}^* \end{pmatrix}$ is independent of all previous queries, then there is some information about $\begin{pmatrix} \boldsymbol{\Lambda} & \boldsymbol{\Xi} \end{pmatrix}$ which is information theoretically hidden. Thus, $\boldsymbol{\rho}^\dagger + \boldsymbol{\sigma}^\dagger$ is information theoretically hidden and from the adversary's point of view it is equally likely that it has any out of q potential values. ▌

Signing the Sum of Two Linear Spaces. When $m = n$, we can adapt the previous construction to a different forgery condition namely, we can prove security against a different type of adversary. Namely, in [26] the scheme is secure against an adversary whose goal is to output a forgery for a message which is linearly independent from all of its signing queries. In our case, we require that the adversary cannot output a signature for a pair $(\hat{\mathbf{x}}^*, \check{\mathbf{y}}^*) \in \hat{\mathbb{G}}^m \times \check{\mathbb{H}}^m$ if $\mathbf{x}^* + \mathbf{y}^*$ is linearly independent from the vectors $\mathbf{x}_i + \mathbf{y}_i$, $i \in [q_s]$, where $(\hat{\mathbf{x}}_i, \check{\mathbf{y}}_i)$ are the signing queries of the adversary.

Our construction is like the previous one taking $\boldsymbol{\Xi} = \boldsymbol{\Lambda}$. Indeed, in this case the adversary only learns $\boldsymbol{\Lambda}\mathbf{x}^* + \boldsymbol{\Xi}\mathbf{y}^* = \boldsymbol{\Lambda}(\mathbf{x}^* + \mathbf{y}^*)$, and identically the same argument follows.

F The Split Kernel Assumption

In this section we discuss in more detail the new computational assumption introduced in Sect. 2.1.

We first note that it implies the Kernel MDH Assumption.

Lemma F.1 $\mathcal{D}_{\ell,k}$-$\mathsf{SKerMDH} \Rightarrow \mathcal{D}_{\ell,k}$-$\mathsf{KerMDH}_{\check{\mathbb{H}}}$. ▌

Proof: Suppose there exists an adversary B against the $\mathcal{D}_{\ell,k}$-$\mathsf{KerMDH}_{\check{\mathbb{H}}}$ assumption. We show how to construct an adversary A against the $\mathcal{D}_{\ell,k}$-$\mathsf{SKerMDH}$ Assumption. Adversary A receives as a challenge $(\hat{\mathbf{A}}, \check{\mathbf{A}})$ and forwards $\check{\mathbf{A}}$ to B, who outputs with non-negligible probability a vector $\hat{\mathbf{r}}$ such that $\hat{\mathbf{r}}^\top \check{\mathbf{A}} = \mathbf{0}_{\mathbb{T}}$. Then A simply outputs $(\hat{\mathbf{r}}, \check{\mathbf{0}})$ as a solution to the $\mathcal{D}_{\ell,k}$-$\mathsf{SKerMDH}$ challenge. ▌

We prove that the reciprocal is true in the generic bilinear model. A rough idea of the proof was given already in Sect. 2.1, here we give the formal argument.

We use the natural generalization of Shoup's generic group model [34] to the (a)symmetric bilinear setting, as it was used for instance in [6]. In such a model an adversary can only access elements of $\hat{\mathbb{G}}, \check{\mathbb{H}}$ or $\mathbb{T}$ via a query to a group oracle, which gives him a randomized encoding of the queried element. The group oracle must be consistent with the group operations (allowing to query for the encoding of constants in either group, for the encoding of the sum of previously queried elements in the same group and for the encoding of the product of pairs in $\hat{\mathbb{G}} \times \check{\mathbb{H}}$. More details, can be found for instance in [6].

Lemma F.2 If $\mathcal{D}_{\ell,k}$-KerMDH holds in generic symmetric bilinear groups, then $\mathcal{D}_{\ell,k}$-SKerMDH holds in generic asymmetric bilinear groups. ▌

Proof: Suppose there is an adversary A in the asymmetric generic bilinear group model against the $\mathcal{D}_{\ell,k}$-SKerMDH assumption. We show how to construct an adversary B against the $\mathcal{D}_{\ell,k}$-KerMDH$_{\check{\mathbb{H}}}$ Assumption in the symmetric generic group model.

Adversary B has oracle access to the randomized encodings $\sigma : \mathbb{Z}_q \to \{0,1\}^n$, and $\sigma_T : \mathbb{Z}_q \to \{0,1\}^n$. It receives as a challenge $\{\sigma(a_{ij})\}_{1\le i\le \ell, 1\le j\le k}$.

Adversary B simulates the generic hardness game for A as follows. It defines encodings $\xi_1 : \mathbb{Z}_q \to \{0,1\}^n$, $\xi_2 : \mathbb{Z}_q \to \{0,1\}^n$ and $\xi_T : \mathbb{Z}_q \to \{0,1\}^n$ as $\xi_1 = \sigma$, $\xi_T = \sigma_T$ and ξ_2 a random encoding function. B keeps a list L_{A} with the values that have been queried by A to the group oracle. The list is initialized as $L_{\mathsf{A}} = \{\{(A_{i,j}, \xi_1(a_{ij}), 1), (A_{i,j}, \xi_2(a_{ij}), 2)\}_{1\le i\le \ell, 1\le j\le k}\}$, where $\xi_2(a_{ij}) \in \{0,1\}^n$ are chosen uniformly at random conditioned on being pairwise distinct. Adversary B also keeps a list L_{B} with the queries it makes to its own group oracle. The list L_{B} is initialized as $L_{\mathsf{B}} = \{\{(A_{i,j}, \sigma(a_{ij}), 1)\}_{1\le i\le \ell, 1\le j\le k}\}$

Each element in the list L_{A} is a tuple (P_i, s_i, x_i), where $P_i \in \mathbb{Z}_q[A_{11}, \ldots, A_{\ell k}]$, $x_i \in \{1, 2, T\}$ and $s_i = \xi_{x_i}(P_i(a_{11}, \ldots, a_{\ell k}))$. The polynomial P_i is one of the following: a) $P_i = A_{ij}$, i.e. it is one of the initial values in the query list L_{A} or b) a constant polynomial or c) $P_i = P_c + P_d$ for some $(P_c, s_c, x), (P_d, s_d, x) \in L_{\mathsf{A}}$ or d) $P_i = P_c P_d$ for some $(P_c, s_c, 1), (P_d, s_d, 2) \in L_{\mathsf{A}}$, $x_i = T$. For L_{B} the same holds except that $x_i \in \{1, T\}$ and except that d) is changed to: d) $P_i = P_c P_d$ for some $(P_c, s_c, 1), (P_d, s_d, 1) \in L_{\mathsf{B}}$ and $x_i = T$.

Without loss of generality we can identify the queries of A with pairs (P_i, x_i) meeting the restrictions described above. If (P_i, x_i) was queried before, it replies with the same answer s_i.

Else, when B receives a (valid) query (P_i, x_i), if $x_i \in \{1, T\}$ it simply forwards the query to its own group oracle, who replies with s_i. Then (P_i, s_i, x_i) is appended to L_{B} and to L_{A}. If $x_i = 2$, then it forwards the query to its own group oracle as $(P_i, 1)$. When it receives the answer s_i, B appends $(P_i, s_i, 1)$ to L_{B} and it looks for the set S of all tuples $(P_j, s_j, 1) \in L_{\mathsf{B}}$, $P_j \neq P_i$, such that $s_j = s_i$. For every tuple in S, B checks if there is some $\tilde{s}$ such that $(P_j, \tilde{s}, 2)$ is in L_{A} (note that, because of the way L_{A} is constructed, if such $\tilde{s}$ exists it is the same for all P_j).

If such $\tilde{s}$ exists, it appends $(P_i, \tilde{s}, 2)$ in L_{A} and it replies with $\tilde{s}$. Else it chooses some $\tilde{s}$ uniformly at random conditioned on being distinct from all other values s such that there exist some P such that $(P, s, 2)$ is in L_{A}. Finally, it appends $(P_i, \tilde{s}, 2)$ in L_{A}.

Finally, A will output as a solution to the challenge a pair s_q, s_r such that $(Q, s_q, 1), (R, s_r, 2) \in L_{\mathsf{A}}$. Because of the way L_{A} and L_{B} were constructed, there exists some s'_r such that $(Q, s_q, 1), (R, s'_r, 1) \in L_{\mathsf{A}}$. B queries its group oracle for $(R - Q, 1)$ and obtains as a reply some string s_{R-Q}. Finally, it outputs s_{R-Q} as a solution to its challenge. It easily follows that A and B have exactly the same probability of success. ∎

Finally, we note that the $\mathcal{L}_2$-SKerMDH Assumption is implied by a decisional assumption introduced in [28]. The assumption says that, given $(\hat{\mathbf{A}}, \check{\mathbf{A}})$, where $\mathbf{A} \leftarrow \mathcal{L}_2$, the vector $(\hat{\mathbf{A}}\mathbf{w}, \check{\mathbf{A}}\mathbf{w})$, $\mathbf{w} \leftarrow \mathbb{Z}_q^2$, is computationally indistinguishable from $(\hat{\mathbf{u}}, \check{\mathbf{u}})$, $\mathbf{u} \leftarrow \mathbb{Z}_q^3$. The proof is analogous to the proof that $\mathcal{D}_{\ell,k}$-MDDH $\Rightarrow$ $\mathcal{D}_{\ell,k}$-KerMDH. Suppose that $(\hat{\mathbf{r}}, \check{\mathbf{s}})$ is a solution to the $\mathcal{L}_2$-SKerMDH Assumption, then $\hat{\mathbf{r}}^\top \check{\mathbf{A}}\mathbf{w} - \check{\mathbf{s}}^\top \hat{\mathbf{A}}\mathbf{w} = (\hat{\mathbf{r}}^\top \check{\mathbf{A}} - \check{\mathbf{s}}^\top \hat{\mathbf{A}})\mathbf{w} = 0_{\mathbb{T}}$, while $\hat{\mathbf{r}}^\top \check{\mathbf{u}} - \check{\mathbf{s}}^\top \hat{\mathbf{u}} = 0_{\mathbb{T}}$ only with negligible probability whenever $\mathbf{r} \neq \mathbf{s}$.