

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

Alonso González^{*1}, Alejandro Hevia¹, and Carla Ràfols^{**2}

¹ Departamento de Ciencias de la Computación, Universidad de Chile, Chile

² Horst-Görtz Institute for IT Security and Faculty of Mathematics,
Ruhr-Universität Bochum, Germany

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 $e : \hat{\mathbb{G}} \times \hat{\mathbb{H}} \rightarrow \mathbb{T}$. 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 $\hat{\mathbb{G}}^m \times \hat{\mathbb{H}}^n$. In particular, we give a constant-size argument that two sets of Groth-Sahai commitments, defined over different groups $\hat{\mathbb{G}}, \hat{\mathbb{H}}$, 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 $\hat{\mathbb{G}}^m \times \hat{\mathbb{H}}^n$ 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.

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

* Funded by CONICYT, CONICYT-PCHA/Doctorado Nacional/2013-21130937.

** 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.

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. [13]) but based on very strong and controversial assumptions, namely knowledge-of-exponent type of assumptions (which are non-falsifiable, according to Naor’s classification [26]) or the random oracle model.

The Groth-Sahai proof system (GS proofs) [17] 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. [8,9,27])

Among those, a recent line of work [20,21,22,23] has succeeded in constructing constant-size arguments for very specific statements, namely, for membership in subspaces of \hat{G}^m , where \hat{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, [20]). 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 [21] 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{G}, \check{H} , or \mathbb{Z}_q .³

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 [21] (in particular, for two-sided linear equations) in asymmetric bilinear groups. The latter (Type III bilinear groups, according to the classification of [12]) 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 [19] and subsequent improvements. Considerable research effort (e.g. [1,11]) has been put into translating pairing-based

³ 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.

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 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 [22]. 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

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

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 \bar{b} such that $\{b(\bar{b} - 1) = 0, b - \bar{b} = 0\}$. 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, [25]), 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 [9]). Our SKerMDH Assumption says that one cannot find a solution to the KerMDH problem which is “split” between the groups $\hat{\mathbb{G}}$ and $\hat{\mathbb{H}}$. 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, [2]), 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 [21] to aggregate proofs of two-sided linear equations in asymmetric groups. While the original aggregation results of [21] 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 the full version). More specifically, we prove membership in

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

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 the full version). 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 the full version).

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 $\mathcal{L}_{\hat{\mathbf{M}}, \hat{\mathbf{N}}, +}$ with decisional assumptions in $\hat{\mathbb{G}}$ and $\hat{\mathbb{H}}$. 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” loses all meaning, as every vector in $\hat{\mathbb{G}}^m \times \hat{\mathbb{H}}^m$ 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.

	Comms	Proof	CK	CRS(ρ)	#Pairings
GS [16]	$2n(\mathbf{g} + \mathbf{h})$	$4n(\mathbf{g} + \mathbf{h})$	$4(\mathbf{g} + \mathbf{h})$	0	$28n$
GS + $\Psi_{\mathcal{D}_k, \text{com}}$	$2n(\mathbf{g} + \mathbf{h})$	$(2n + 2)(\mathbf{g} + \mathbf{h})$	$4(\mathbf{g} + \mathbf{h})$	$(10n + 4)(\mathbf{g} + \mathbf{h})$	$20n + 8$
$\Pi_{\text{bit}} m = 1$	$(n + 1)\mathbf{g}$	$10(\mathbf{g} + \mathbf{h})$	$(n + 1)\mathbf{g}$	$(6n^2 + 10n + 32)(\mathbf{g} + \mathbf{h})$	$n + 55$
$\Pi_{\text{bit}} m = n$	$2n\mathbf{g}$	$10(\mathbf{g} + \mathbf{h})$	$4\mathbf{g}$	$(12n^2 + 14n + 22)\mathbf{g} + (12n^2 + 12n + 24)\mathbf{h}$	$2n + 54$
$\Pi_{\text{bit}} \text{ weight } 1, m = 1$	$(n + 1)\mathbf{g}$	$10(\mathbf{g} + \mathbf{h})$	$(n + 1)\mathbf{g}$	$(20n + 26)(\mathbf{g} + \mathbf{h})$	$n + 55$

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 $\Psi_{\mathcal{D}_k, \text{com}}$. Row “ $\Pi_{\text{bit}} m = 1$ ” is for our construction for a single commitment of size $n + 1$ to a bit-string of size n , and “ $\Pi_{\text{bit}} m = n$ ” is for our construction for n concatenated GS commitments. Row “ $\Pi_{\text{bit}} \text{ weight } 1$ ” is for our construction for bit-strings of weight 1 with $m = 1$. 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 $\hat{\mathbb{H}}$ is \mathbf{g} and \mathbf{h} , respectively. The table is computed for $\mathcal{D}_k = \mathcal{L}_2$, the 2-Linear matrix distribution.

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 $(q, \hat{\mathbb{G}}, \hat{\mathbb{H}}, \mathbb{T}, e, \hat{g}, \hat{h})$, where $\hat{\mathbb{G}}, \hat{\mathbb{H}}$ and \mathbb{T} are groups of prime order q , the elements \hat{g}, \hat{h} are generators of $\hat{\mathbb{G}}, \hat{\mathbb{H}}$ respectively, and $e : \hat{\mathbb{G}} \times \hat{\mathbb{H}} \rightarrow \mathbb{T}$ is an efficiently computable, non-degenerate bilinear map.

We denote by \mathbf{g} and \mathbf{h} the bit-size of the elements of $\hat{\mathbb{G}}$ and $\hat{\mathbb{H}}$, respectively. Elements $\hat{x} \in \hat{\mathbb{G}}$ (resp. $\check{y} \in \hat{\mathbb{H}}, z_{\mathbb{T}} \in \mathbb{T}$) 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 $\hat{x} \in \hat{\mathbb{G}}, \check{y} \in \hat{\mathbb{H}}$, $\hat{x}\check{y}$ refers to the pairing operation, i.e. $\hat{x}\check{y} = e(\hat{x}, \check{y})$. Vectors and matrices are denoted in boldface and any product of vectors/matrices of elements in $\hat{\mathbb{G}}$ and $\hat{\mathbb{H}}$ is defined in the natural way via the pairing operation. That is, given $\hat{\mathbf{X}} \in \hat{\mathbb{G}}^{n \times m}$ and $\check{\mathbf{Y}} \in \hat{\mathbb{H}}^{m \times \ell}$, $\hat{\mathbf{X}}\check{\mathbf{Y}} \in \mathbb{T}^{n \times \ell}$. 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 $\hat{\mathbb{H}}$), that is, the matrix whose (i, j) th entry is $t_{i,j}\hat{g}$ (resp. $t_{i,j}\hat{h}$). 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 i th 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 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 (Matrix Diffie-Hellman Assumption [9]). Let $\mathcal{D}_{\ell,k}$ be a matrix distribution and $\Gamma := (q, \hat{\mathbb{G}}, \check{\mathbb{H}}, \mathbb{T}, e, \hat{g}, \check{h}) \leftarrow \text{Gen}_a(1^\lambda)$. We say that the $\mathcal{D}_{\ell,k}$ -Matrix Diffie-Hellman ($\mathcal{D}_{\ell,k}$ -MDDH $_{\hat{\mathbb{G}}}$) Assumption holds relative to Gen_a if for all PPT adversaries \mathcal{D} ,

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

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

The $\mathcal{D}_{\ell,k}$ -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 [18,28]. 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 3 (Kernel Diffie-Hellman Assumption [25]). Let $\Gamma \leftarrow \text{Gen}_a(1^\lambda)$. The Kernel Diffie-Hellman Assumption in $\check{\mathbb{H}}$ ($\mathcal{D}_{\ell,k}$ -KerMDH $_{\check{\mathbb{H}}}$) says that every PPT Algorithm has negligible advantage in the following game: given $\hat{\mathbf{A}}$, where $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, find $\hat{\mathbf{x}} \in \hat{\mathbb{G}}^\ell \setminus \{\hat{\mathbf{0}}\}$, such that $\hat{\mathbf{x}}^\top \hat{\mathbf{A}} = \mathbf{0}_{\mathbb{T}}$.

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

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

Definition 4 (Split Kernel Diffie-Hellman Assumption). Let $\Gamma \leftarrow \text{Gen}_a(1^\lambda)$. The Split Kernel Diffie-Hellman Assumption in $\hat{\mathbb{G}}, \check{\mathbb{H}}$ ($\mathcal{D}_{\ell,k}$ -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 $\hat{\mathbf{r}}^\top \hat{\mathbf{A}} = \check{\mathbf{s}}^\top \check{\mathbf{A}}$.

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 -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 $\hat{\mathbf{A}}$, 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 $\hat{\mathbf{A}}$. 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 $\mathcal{D}_{\ell,k}$ -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 [24]).

Lemma 1. *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 $\hat{\mathbf{r}}^\top \hat{\mathbf{A}} = \check{\mathbf{s}}^\top \check{\mathbf{A}}$. But since the algorithm is generic, it also works when $\hat{\mathbb{G}} = \check{\mathbb{H}}$, and then $\hat{\mathbf{r}} - \check{\mathbf{s}}$ is a solution to $\mathcal{D}_{\ell,k}$ -KerMDH. We provide a formal proof in the full version.

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:

$$\sum_{j=1}^{m_y} f(\alpha_j, \gamma_j) + \sum_{i=1}^{m_x} f(x_i, \beta_i) + \sum_{i=1}^{m_x} \sum_{j=1}^{m_y} f(x_i, \gamma_{i,j} \gamma_j) = t, \quad (1)$$

where A_1, A_2, A_T are \mathbb{Z}_q -vector spaces equipped with some bilinear map $f : A_1 \times A_2 \rightarrow A_T$, $\boldsymbol{\alpha} \in A_1^{m_y}$, $\boldsymbol{\beta} \in A_2^{m_x}$, $\boldsymbol{\Gamma} = (\gamma_{i,j}) \in \mathbb{Z}_q^{m_x \times m_y}$, $t \in A_T$. 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 $\Gamma \leftarrow \text{Gen}_a(1^\lambda)$, $\mathbf{u}_2, \mathbf{v}_2 \leftarrow \mathcal{L}_1$, $\mathbf{u}_1 := \mathbf{e}_1 + \mu \mathbf{u}_2$, $\mathbf{v}_1 := \mathbf{e}_1 + \epsilon \mathbf{v}_2$, $\mu, \epsilon \leftarrow \mathbb{Z}_q$. The common reference string is $\text{crs}_{\text{GS}} := (\Gamma, \hat{\mathbf{u}}_1, \hat{\mathbf{u}}_2, \check{\mathbf{v}}_1, \check{\mathbf{v}}_2)$ 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, crs_{GS} defines the maps:

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

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

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. [20]. A QA-NIZK proof system enables to prove membership in a language defined by a relation \mathcal{R}_ρ , which in turn is completely determined by some parameter ρ sampled from a distribution \mathcal{D}_Γ . We say that \mathcal{D}_Γ is *witness samplable* if there exist an efficient algorithm that samples (ρ, ω) such that ρ is distributed according to \mathcal{D}_Γ , and membership of ρ in the *parameter language* \mathcal{L}_{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}_Γ .

A tuple of algorithms $(\mathsf{K}_0, \mathsf{K}_1, \mathsf{P}, \mathsf{V})$ is called a QA-NIZK proof system for witness-relations $\mathcal{R}_\Gamma = \{\mathcal{R}_\rho\}_{\rho \in \text{sup}(\mathcal{D}_\Gamma)}$ with parameters sampled from a distribution \mathcal{D}_Γ over associated parameter language \mathcal{L}_{par} , if there exists a probabilistic polynomial time simulator $(\mathsf{S}_1, \mathsf{S}_2)$, such that for all non-uniform PPT adversaries $\mathsf{A}_1, \mathsf{A}_2, \mathsf{A}_3$ we have:

Quasi-Adaptive Completeness:

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

Computational Quasi-Adaptive Soundness:

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

Perfect Quasi-Adaptive Zero-Knowledge:

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

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 [22], for the language:

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

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

$$\begin{array}{l} \mathsf{K}_1(\Gamma, \hat{\mathbf{M}}, n) \quad (\mathsf{S}_1(\Gamma, \hat{\mathbf{M}}, n)) \quad \mathsf{P}(\text{crs}, \hat{\mathbf{x}}, \mathbf{w}) \quad \backslash \backslash \hat{\mathbf{x}} = \hat{\mathbf{M}}\mathbf{w} \quad \mathsf{S}_2(\text{crs}, \hat{\mathbf{x}}, \tau_{sim}) \\ \hline \mathbf{A} \leftarrow \widetilde{\mathcal{D}}_k, \mathbf{\Delta} \leftarrow \mathbb{Z}_q^{\tilde{k} \times n} \quad \text{Return } \hat{\sigma} := \hat{\mathbf{M}}_\Delta \mathbf{w}. \quad \text{Return } \hat{\sigma} := \mathbf{\Delta} \hat{\mathbf{x}} \\ \mathbf{\check{A}}_\Delta := \mathbf{\Delta}^\top \mathbf{A}, \hat{\mathbf{M}}_\Delta := \mathbf{\Delta} \hat{\mathbf{M}} \\ \text{Return crs} := (\hat{\mathbf{M}}_\Delta, \mathbf{\check{A}}_\Delta, \mathbf{\check{A}}) \quad \mathsf{V}(\text{crs}, \hat{\mathbf{x}}, \hat{\sigma}) \\ (\tau_{sim} := \mathbf{\Delta}) \quad \text{Return } (\hat{\mathbf{x}}^\top \mathbf{\check{A}}_\Delta = \hat{\sigma}^\top \mathbf{\check{A}}) \end{array}$$

Fig. 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 [22, Sect. 3.1], which is a generalization of Libert *et al*'s QA-NIZK [23] to any \mathcal{D}_k -KerMDH $_{\hat{\mathbb{H}}}$ Assumption. $\Psi_{\overline{\mathcal{D}}_k}$ is the construction of [22, Sect. 3.2].

Theorem 1 (Theorem 1 of [22]). *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 -KerMDH $_{\hat{\mathbb{H}}}$ Assumption, perfect zero-knowledge, and proof size $k + 1$.*

Theorem 2 (Theorem 2 of [22]). *If $\widetilde{\mathcal{D}}_k = \overline{\mathcal{D}}_k$ and $\tilde{k} = k$, and \mathcal{D}_Γ 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 -KerMDH $_{\hat{\mathbb{H}}}$ 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} .

$\begin{aligned} & \mathbf{K}_1(\Gamma, \hat{\mathbf{M}}, \check{\mathbf{N}}, m, n) \quad (\mathbf{S}_1(\Gamma, \hat{\mathbf{M}}, \check{\mathbf{N}}, m, n)) \\ & \mathbf{A} \leftarrow \widetilde{\mathcal{D}}_k \\ & \mathbf{\Lambda} \leftarrow \mathbb{Z}_q^{\tilde{k} \times m}, \mathbf{\Xi} \leftarrow \mathbb{Z}_q^{\tilde{k} \times n}, \mathbf{Z} \leftarrow \mathbb{Z}_q^{\tilde{k} \times t} \\ & \check{\mathbf{A}}_\Lambda := \mathbf{\Lambda}^\top \check{\mathbf{A}} \\ & \check{\mathbf{A}}_\Xi := \mathbf{\Xi}^\top \check{\mathbf{A}} \\ & \hat{\mathbf{M}}_\Lambda := \mathbf{\Lambda} \hat{\mathbf{M}} + \hat{\mathbf{Z}} \\ & \check{\mathbf{N}}_\Xi := \mathbf{\Xi} \check{\mathbf{N}} - \check{\mathbf{Z}} \\ & \text{Return } \text{crs} := (\hat{\mathbf{M}}_\Lambda, \check{\mathbf{A}}_\Lambda, \check{\mathbf{A}}, \check{\mathbf{N}}_\Xi, \\ & \quad \check{\mathbf{A}}_\Xi, \hat{\mathbf{A}}). \\ & (\tau_{sim} := (\mathbf{\Lambda}, \mathbf{\Xi})). \end{aligned}$	$\begin{aligned} & \mathbf{P}(\text{crs}, \hat{\mathbf{x}}, \check{\mathbf{y}}, \mathbf{w}) \\ & \text{\\}(\hat{\mathbf{x}} = \hat{\mathbf{M}}\mathbf{w}, \check{\mathbf{y}} = \check{\mathbf{N}}\mathbf{w}) \\ & \mathbf{z} \leftarrow \mathbb{Z}_q^{\tilde{k}} \\ & \hat{\rho} := \hat{\mathbf{M}}_\Lambda \mathbf{w} + \hat{\mathbf{z}} \\ & \check{\sigma} := \check{\mathbf{N}}_\Xi \mathbf{w} - \check{\mathbf{z}} \\ & \text{Return } (\hat{\rho}, \check{\sigma}). \\ & \mathbf{V}(\text{crs}, (\hat{\mathbf{x}}, \check{\mathbf{y}}), (\hat{\rho}, \check{\sigma})) \\ & \text{Return } (\hat{\mathbf{x}}^\top \check{\mathbf{A}}_\Lambda - \hat{\rho}^\top \check{\mathbf{A}} \\ & \quad = \check{\sigma}^\top \check{\mathbf{A}} - \check{\mathbf{y}}^\top \check{\mathbf{A}}_\Xi). \end{aligned}$	$\begin{aligned} & \mathbf{S}_2(\text{crs}, (\hat{\mathbf{x}}, \check{\mathbf{y}}), \tau_{sim}) \\ & \mathbf{z} \leftarrow \mathbb{Z}_q^{\tilde{k}} \\ & \hat{\rho} := \mathbf{\Lambda} \hat{\mathbf{x}} + \hat{\mathbf{z}} \\ & \check{\sigma} := \mathbf{\Xi} \check{\mathbf{y}} - \check{\mathbf{z}} \\ & \text{Return } (\hat{\rho}, \check{\sigma}). \end{aligned}$
---	---	--

Fig. 2. Two QA-NIZK Arguments for $\mathcal{L}_{\hat{\mathbf{M}}, \check{\mathbf{N}}}$. $\Psi_{\mathcal{D}_k, \text{spl}}$ is defined for $\widetilde{\mathcal{D}}_k = \mathcal{D}_k$ and $\tilde{k} = k + 1$, and is a generalization of [22] Sect. 3.1 in two groups. The second construction $\Psi_{\overline{\mathcal{D}}_k, \text{spl}}$ corresponds to $\widetilde{\mathcal{D}}_k = \overline{\mathcal{D}}_k$ and $\tilde{k} = k$, and is a generalization of [22] 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.

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

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

Given that the matrix \mathbf{Z} is uniformly random, $\text{crs}_{\Psi_{\mathcal{D}_k}}$ and $\text{crs}_{\Psi_{\mathcal{D}_k, \text{spl}}}$ 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 [22] can be easily adapted for the new arguments. The proofs can be found in the full version.

Theorem 3. *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 4. *If $\widetilde{\mathcal{D}}_k = \overline{\mathcal{D}}_k$ and $\tilde{k} = k$, and \mathcal{D}_Γ 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,

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

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:

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

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 $\mathcal{L}_{\text{com}, \hat{\mathbf{U}}, \check{\mathbf{V}}, \nu}$ 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:

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

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

In the rest of the paper, we denote as $\Psi_{\overline{\mathcal{D}}_k, \text{com}}$ the proof system for $\mathcal{L}_{\text{com}, \hat{\mathbf{U}}, \check{\mathbf{V}}, \nu}$ which corresponds to $\Psi_{\overline{\mathcal{D}}_k, \text{spl}}$ 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

Jutla and Roy [21] show how to aggregate GS proofs of two-sided linear equations in symmetric bilinear groups. In the original construction of [21] 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 [21]. 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.⁴

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}_Γ be a witness samplable distribution which outputs n pairs of vectors $(\alpha_\ell, \beta_\ell) \in A_1^{m_y} \times A_2^{m_x}$, $\ell \in [n]$, for some $m_x, m_y \in \mathbb{N}$. Given some fixed pairs $(\alpha_\ell, \beta_\ell)$, we define, for each $\tilde{\mathbf{t}} \in A_T^n$, the set of equations $\mathcal{S}_{\tilde{\mathbf{t}}}$ as:

$$\mathcal{S}_{\tilde{\mathbf{t}}} = \{E_\ell(\mathbf{x}, \mathbf{y}) = \tilde{t}_\ell : \ell \in [n]\}, \quad E_\ell(\mathbf{x}, \mathbf{y}) := \sum_{j \in [m_y]} f(\alpha_{\ell,j}, y_j) + \sum_{i \in [m_x]} f(x_i, \beta_{\ell,i}).$$

We note that, as in [21], 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 α_ℓ, β_ℓ (but not on \tilde{t}_ℓ , 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 $\tilde{t}_\ell = f(t_\ell, \text{base}_2)$ or (2) $\tilde{t}_\ell \in A_2$, such that $\tilde{t}_\ell = f(\text{base}_1, t_\ell)$, where $\text{base}_i = 1$ if $A_i = \mathbb{Z}_q$, $\text{base}_1 = \hat{g}$ if $A_1 = \hat{\mathbb{G}}$ and $\text{base}_2 = \check{h}$ 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 $\nu_2(a_{\ell,i}), \nu_1(t_\ell)$ for $\nu_1(a_{\ell,i}), \nu_2(t_\ell)$ in the construction below.

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

\mathcal{D}_Γ : \mathcal{D}_Γ is some distribution over n pairs of vectors $(\alpha_\ell, \beta_\ell) \in A_1^{m_x} \times A_2^{m_y}$.

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

$$\text{crs} := \left(\text{crs}_{\text{GS}}, \left\{ \sum_{\ell \in [n]} \nu_1(a_{\ell,i} \alpha_\ell), \sum_{\ell \in [n]} \nu_2(a_{\ell,i} \beta_\ell), \{\nu_2(a_{\ell,i}) : \ell \in [n]\} : i \in [k] \right\} \right)$$

⁴ The results of [21] are based on what they call the “Switching Lemma”. As noted in [25], it is implicit in the proof of this lemma that the same results can be obtained under computational assumptions.

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

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

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

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

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

Theorem 5. *The above protocol is a QA-NIZK proof system for two-sided linear equations.*

Proof. Completeness. Observe that

$$\sum_{\ell \in [n]} a_{\ell, i} E_{\ell}(\mathbf{x}, \mathbf{y}) = \sum_{j \in [m_y]} f(a_{\ell, i} \alpha_{\ell, j}, y_j) + \sum_{j \in [m_x]} f(x_j, a_{\ell, i} \beta_{\ell, j}). \quad (2)$$

Completeness follows from the observation that to efficiently compute the proof, the GS Prover [17] only needs, a part 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 $(\alpha_{\ell}, \beta_{\ell})$, $\ell \in [n]$. 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 \mathbf{B} against the $\mathcal{D}_{n, k}$ -SKerMDH Assumption, where $\mathcal{D}_{n, k}$ is the matrix distribution used in the CRS generation.

\mathbf{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 \mathbf{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 $\{\hat{\Theta}_i, \check{\Pi}_i\}_{i \in [k]}$, 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 \mathbf{B} who knows the discrete logarithm of the commitment keys. We claim that the pair $(\hat{\rho}, \check{\sigma}) \in \hat{\mathbb{G}}^n \times \check{\mathbb{H}}^n$, $\hat{\rho} := (\beta_1^{\top} \hat{\mathbf{x}} - \hat{t}_1, \dots, \beta_n^{\top} \hat{\mathbf{x}} - \hat{t}_n)$, $\check{\sigma} := (\alpha_1^{\top} \check{\mathbf{y}}, \dots, \alpha_n^{\top} \check{\mathbf{y}})$, solves the $\mathcal{D}_{n, k}$ -SKerMDH challenge.

First, observe that if the adversary is successful in breaking the soundness property, then $\hat{\rho} \neq \check{\sigma}$. 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 $\sum_{j \in [m_y]} f(\alpha_{\ell,j}, y_j) \neq \sum_{j \in [m_x]} f(x_j, \beta_{\ell,j}) - f(t_\ell, \text{base}_2)$. If we take discrete logarithms in each side of the equation, this inequality is exactly equivalent to $\rho \neq \sigma$.

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

$$\sum_{\ell \in [n]} \check{a}_{\ell,i} (\beta_\ell^\top \hat{\mathbf{x}} - \hat{t}_\ell) = \sum_{\ell \in [n]} \hat{a}_{\ell,i} (\alpha_\ell^\top \hat{\mathbf{y}}), \quad (3)$$

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

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

One-sided Equations. In the case when $\alpha_\ell = \mathbf{0}$ and $\tilde{t}_\ell = f(t_\ell, \text{base}_2)$ 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 \mathbf{B} receives $\hat{\mathbf{A}} \in \mathbb{H}^{n \times k}$, an instance of the $\mathcal{D}_{n,k} - \text{KerMDH}_{\mathbb{H}}$ problem. The adversary \mathbf{B} outputs $\hat{\rho} := (\beta_1^\top \hat{\mathbf{x}} - \hat{t}_1, \dots, \beta_n^\top \hat{\mathbf{x}} - \hat{t}_n)$ as a solution to the challenge. To see why this works, note that, when $\alpha_\ell = \mathbf{0}$ for all $\ell \in [n]$, equation (3) reads $\sum_{\ell \in [n]} \check{a}_{\ell,i} (\beta_\ell^\top \hat{\mathbf{x}} - \hat{t}_\ell) = \mathbf{0}_{\mathbb{T}}$ and thus $\hat{\rho} \hat{\mathbf{A}} = \mathbf{0}_{\mathbb{T}}$. The case when $\beta_\ell = \mathbf{0}$ and $\tilde{t}_\ell = f(\text{base}_1, t_\ell)$ for some $t_\ell \in A_2$, for all $\ell \in [n]$, is analogous.

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:

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

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}_Γ 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 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 [21].

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.

Intuition. A prover wanting to show satisfiability of the equation $x(y - 1) = 0$ using GS proofs, will commit to a solution $x = b$ and $y = \bar{b}$ 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 equation⁵:

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

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:

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

Now consider commitments to (b_1, \dots, b_n) and $(\bar{b}_1, \dots, \bar{b}_n)$ constructed with some commitment key $\{(\hat{\mathbf{g}}_i, \check{\mathbf{h}}_i) : i \in [n+1]\} \subset \hat{\mathbb{G}}^{\bar{n}} \times \check{\mathbb{H}}^{\bar{n}}$, for some $\bar{n} \in \mathbb{N}$, 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,

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

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 $\hat{\mathbf{C}}_{i,j} := \hat{\mathbf{g}}_i \check{\mathbf{h}}_j^\top$, 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 $\hat{\boldsymbol{\Theta}}_{b(\bar{b}-1)}$ as a linear combination of $\mathcal{C} := \{\hat{\mathbf{C}}_{i,j} : (i, j) \in \mathcal{I}_{n,1}\}$ (with coefficients which depend on $\mathbf{b}, \bar{\mathbf{b}}, r, s$) such that

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

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

This reasoning assumes that $\{\hat{\mathbf{g}}_i \check{\mathbf{h}}_j^\top\}$ (or equivalently, $\{\hat{\mathbf{C}}_{i,j}\}$) are linearly independent, which can only happen if $\bar{n} \geq n + 1$. If that is the case, the proof cannot be constant because $\hat{\boldsymbol{\Theta}}_{b(\bar{b}-1)} \in \hat{\mathbb{G}}^{\bar{n} \times \bar{n}}$ and this matrix is part of the

⁵ For readers familiar with the Groth-Sahai notation, equation (4) corresponds to $\mathbf{c} \bullet (\mathbf{d} - \iota_2(1)) = \mathbf{u}_2 \bullet \boldsymbol{\pi} + \boldsymbol{\theta} \bullet \mathbf{v}_2$.

proof. Instead, we choose $\hat{\mathbf{g}}_1, \dots, \hat{\mathbf{g}}_{n+1} \in \hat{\mathbb{G}}^2$ and $\check{\mathbf{h}}_1, \dots, \check{\mathbf{h}}_{n+1} \in \check{\mathbb{H}}^2$, 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 $\hat{\Theta}_{b(\bar{b}-1)} \in \text{Span}(\mathcal{C})$ seems no longer meaningful, as $\text{Span}(\mathcal{C})$ 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 $\hat{\mathbf{C}}_{i^*,i^*} \notin \text{Span}(\mathcal{C})$ 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 $\hat{\mathbf{C}}_{i,j} := \hat{\mathbf{g}}_i \check{\mathbf{h}}_j^\top$ 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 $(\hat{\mathbf{C}}_{i,j}, \hat{\mathbf{D}}_{i,j})$ which is uniformly distributed conditioned on $\hat{\mathbf{C}}_{i,j} + \hat{\mathbf{D}}_{i,j} = \mathbf{g}_i \check{\mathbf{h}}_j^\top$. This randomization completely hides the group in which we can compute $\mathbf{g}_i \check{\mathbf{h}}_j^\top$. Finally, we use our QA-NIZK Argument for sum in a subspace (Sect. 3.2) to prove membership in this space.

Instantiations. We discuss in detail two particular cases of languages $\mathcal{L}_{\hat{\mathbf{U}}, \text{bits}}$. First, in Sect. 5.1 we discuss the case when

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

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. 5.3 we discuss how to generalize the construction for a) to

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

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

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

5.1 The scheme

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

\mathcal{D}_Γ : The distribution \mathcal{D}_Γ 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 $\hat{\mathbf{c}} = \hat{\mathbf{U}} \begin{pmatrix} \mathbf{b} \\ w \end{pmatrix}$. 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 $\Delta \leftarrow \mathbb{Z}_q^{2 \times (n+1)}$, define $\hat{\mathbf{G}} := \Delta \hat{\mathbf{U}}$ and $\hat{\mathbf{g}}_i := \Delta \hat{\mathbf{u}}_i \in \hat{\mathbb{G}}^2$, for all $i \in [n+1]$. Let $\mathbf{a} \leftarrow \mathcal{L}_1$ and define $\check{\mathbf{a}}_\Delta := \Delta^\top \mathbf{a} \in \check{\mathbb{H}}^{n+1}$. For any pair $(i, j) \in \mathcal{I}_{n,1}$, let $\mathbf{T}_{i,j} \leftarrow \mathbb{Z}_q^{2 \times 2}$ and set:

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

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 $\Psi_{\overline{\mathcal{D}}_{k,\text{com}}}$ be an instance of our proof system for Equal Opening (Sect. 3.3).

Let $\text{crs}_{\Psi_{\overline{\mathcal{D}}_{k,+}}} \leftarrow \mathsf{K}_1(\Gamma, \{\hat{\mathbf{C}}_{i,j}, \check{\mathbf{D}}_{i,j}\}_{(i,j) \in \mathcal{I}_{n,1}})$ and ${}^6 \text{crs}_{\Psi_{\overline{\mathcal{D}}_{k,\text{com}}}} \leftarrow \mathsf{K}_1(\Gamma, \hat{\mathbf{G}}, \check{\mathbf{H}}, n)$. The common reference string is given by:

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

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

1. Define

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

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

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

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

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

1. Check if $\hat{\mathbf{c}}^\top \check{\mathbf{a}}_\Delta = \hat{\mathbf{c}}_\Delta^\top \check{\mathbf{a}}$.

⁶ 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. Check if

$$\hat{\mathbf{c}}_\Delta \left(\check{\mathbf{d}} - \sum_{j \in [n]} \check{\mathbf{h}}_j \right)^\top = \hat{\Theta}_{b(\bar{b}-1)} \check{\mathbf{I}}_{2 \times 2} + \hat{\mathbf{I}}_{2 \times 2} \check{\Pi}_{b(\bar{b}-1)}. \quad (9)$$

3. Verify that $(\hat{\rho}_{b(\bar{b}-1)}, \check{\sigma}_{b(\bar{b}-1)}), (\hat{\rho}_{b-\bar{b}}, \check{\sigma}_{b-\bar{b}})$ are valid proofs for $(\hat{\Theta}_{b(\bar{b}-1)}, \check{\Pi}_{b(\bar{b}-1)})$ and $(\hat{\mathbf{c}}_\Delta, \check{\mathbf{d}})$ using $\text{crs}_{\Psi_{\mathcal{D}_k, +}}$ and $\text{crs}_{\Psi_{\mathcal{D}_k, \text{com}}}$ respectively.

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

$S_1(\Gamma, \hat{\mathbf{U}})$: 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}_Γ . It generates and outputs the CRS in the same way as K_1 , but additionally it also outputs the simulation trapdoor

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

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

$S_2(\text{crs}_P, \hat{\mathbf{c}}, \tau)$: Compute $\hat{\mathbf{c}}_\Delta := \Delta \hat{\mathbf{c}}$. Then pick random $\bar{w}_h \leftarrow \mathbb{Z}_q$, $\mathbf{R} \leftarrow \mathbb{Z}_q^{2 \times 2}$ and define $\check{\mathbf{d}} := \bar{w}_h \mathbf{h}_{n+1}$. Then set:

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

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

5.2 Proof of Security

Completeness is proven in the full version. The following theorem guarantees Soundness.

Theorem 6. *Let $\text{Adv}_{\mathcal{P}_S}(\mathbf{A})$ be the advantage of an adversary \mathbf{A} against the soundness of the proof system described above. There exist PPT adversaries $B_1, B_2, B_3, P_1^*, P_2^*$ such that*

$$\begin{aligned} \text{Adv}_{\mathcal{P}_S}(\mathbf{A}) \leq & n \left(6/q + \text{Adv}_{\mathcal{U}_1, \hat{\mathbb{G}}}(\mathbf{B}_1) + \text{Adv}_{\mathcal{U}_1, \mathbb{H}}(\mathbf{B}_2) + \text{Adv}_{\text{SP}_{\mathbb{H}}}(\mathbf{B}_3) \right. \\ & \left. + \text{Adv}_{\Psi_{\mathcal{D}_k, +}}(P_1^*) + \text{Adv}_{\Psi_{\mathcal{D}_k, \text{com}}}(P_2^*) \right). \end{aligned}$$

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 $\hat{\mathbf{c}} = \hat{\mathbf{U}} \begin{pmatrix} \mathbf{b} \\ w_g \end{pmatrix}$, for some $\mathbf{b} \notin \{0, 1\}^n$ and $w \in \mathbb{Z}_q$, and the corresponding proof which is accepted by the verifier.

- Game₀** 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}_Γ .
- Game₁** This game is identical to **Game₀** except that the simulator picks a random $i^* \in [n]$, and uses \mathbf{U} to check if the output of the adversary \mathbf{A} is such that $b_{i^*} \in \{0, 1\}$. It aborts if $b_{i^*} \in \{0, 1\}$.
- Game₂** This game is identical to **Game₁** except that now the vectors $\hat{\mathbf{g}}_i, i \in [n]$ and $i \neq i^*$, are uniform vectors in the space spanned by $\hat{\mathbf{g}}_{n+1}$.
- Game₃** This game is identical to **Game₂** 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 the full version).

Lemma 2. $\Pr[\text{Game}_1(\mathbf{A}) = 1] \geq \frac{1}{n} \Pr[\text{Game}_0(\mathbf{A}) = 1]$.

Lemma 3. *There exists a \mathcal{U}_1 -MDDH $_{\hat{\mathbb{G}}}$ adversary \mathbf{B} such that $|\Pr[\text{Game}_1(\mathbf{A}) = 1] - \Pr[\text{Game}_2(\mathbf{A}) = 1]| \leq \text{Adv}_{\mathcal{U}_1, \hat{\mathbb{G}}}(\mathbf{B}) + 2/q$.*

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

Let $\hat{\mathbf{E}} := (\hat{\mathbf{s}} || \hat{\mathbf{t}})$. \mathbf{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 $\Delta \in \mathbb{Z}_q^{2 \times (n+1)}$. Although \mathbf{B} does not know Δ , it can compute $\hat{\Delta}$ as $\hat{\Delta} = \hat{\mathbf{G}}\mathbf{U}^{-1}$, given that \mathbf{U} is full rank and was sampled by \mathbf{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 **Game₁**. 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 **Game₂**.

Lemma 4. *There exists a \mathcal{U}_1 -MDDH $_{\check{\mathbb{H}}}$ adversary \mathbf{B} such that $|\Pr[\text{Game}_2(\mathbf{A}) = 1] - \Pr[\text{Game}_3(\mathbf{A}) = 1]| \leq \text{Adv}_{\mathcal{U}_1, \check{\mathbb{H}}}(\mathbf{B})$.*

Lemma 5. *There exists a $\text{SP}_{\check{\mathbb{H}}}$ adversary \mathbf{B} and soundness adversaries $\mathbf{P}_1^*, \mathbf{P}_2^*$ for $\Psi_{\overline{\mathcal{D}}_k, +}$ and $\Psi_{\overline{\mathcal{D}}_k, \text{com}}$ such that*

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

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 $\mathbf{g}_{i^*} \mathbf{h}_{i^*}^\top \notin \text{Span}(\{\mathbf{C}_{i,j} + \mathbf{D}_{i,j} : (i, j) \in \mathcal{I}_{n,1}\})$. Additionally $\text{Game}_3(\mathbf{A}) = 1$ implies that $b_{i^*} \notin \{0, 1\}$ while the verifier accepts the proof produced by \mathbf{A} , which

is $(\hat{\mathbf{c}}_\Delta, \check{\mathbf{d}}, (\hat{\Theta}_{b(\bar{b}-1)}, \check{\Pi}_{b(\bar{b}-1)}), \{(\hat{\rho}_X, \check{\sigma}_X)\}_{X \in \{b(\bar{b}-1), b-\bar{b}\}\})$. Since $\{\check{\mathbf{h}}_{i^*}, \check{\mathbf{h}}_{n+1}\}$ is a basis of $\check{\mathbb{H}}^2$, we can define \bar{w}_h, \bar{b}_{i^*} as the unique coefficients in \mathbb{Z}_q such that $\check{\mathbf{d}} = \bar{b}_{i^*} \check{\mathbf{h}}_{i^*} + \bar{w}_h \check{\mathbf{h}}_{n+1}$. We distinguish three cases:

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

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

Theorem 7. *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 $\check{\mathbf{d}} = \check{\mathbf{H}} \begin{pmatrix} \mathbf{b} \\ w_h \end{pmatrix}$. Since \mathbf{R} is chosen uniformly at random in $\mathbb{Z}_q^{2 \times 2}$, the proof $(\hat{\Theta}_{b(\bar{b}-1)}, \check{\Pi}_{b(\bar{b}-1)})$ is uniformly distributed conditioned on satisfying check 2) of algorithm \mathbf{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 $\Psi_{\overline{\mathcal{D}}_k, \text{com}}$ concludes the proof.

5.3 Extensions

CRS generation for Individual Commitments. When using individual commitments (distribution \mathbf{b}) from Sect. 5), the only change is that Δ is sampled uniformly from $\mathbb{Z}_q^{2 \times 2n}$ (the distribution of $\check{\mathbf{H}}$ is not changed). Thus, the matrix $\hat{\mathbf{G}} := \Delta \hat{\mathbf{U}}$ has $2n$ columns instead of $n+1$ and $\hat{\mathbf{c}}_\Delta := \hat{\mathbf{G}} \begin{pmatrix} \mathbf{b} \\ \mathbf{w}_g \end{pmatrix}$ 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 $\hat{\mathbf{g}}_{2n}$.

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 5.1 and a proof that $\sum_{i \in [n]} b_i = 1$ as described above. In the definition of $(\hat{\Theta}_{b(\bar{b}-1)}, \check{\Pi}_{b(\bar{b}-1)})$ 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.

Signatures. Some application examples are the signature schemes of [4,5,6,10]. For example, in the revocable attribute-based signature scheme of Escala *et. al* [10], 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 [7], 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, \dots, vk_n) of the parties in the ring R .

Proof System	Author	Proof Size
Threshold GS	Ràfols [27] (1)	$(m_x + 3(n - t) + 2\bar{n})\mathbf{g}$
	Ràfols [27] (2)	$2(n - t + 1)\mathbf{h} + 2n(\mathbf{g} + \mathbf{h})$
	This work	$2(n + 1)\mathbf{g} + 10(\mathbf{g} + \mathbf{h})$
Dynamic List (Ring Signature)	Chandran et al. [7]	$(16\sqrt{n} + 4)(\mathbf{g} + \mathbf{h})$
	Ràfols [27]	$(8\sqrt{n} + 6)\mathbf{g} + 12\sqrt{n}\mathbf{h}$
	This work	$(4\sqrt{n} + 14)\mathbf{g} + (8\sqrt{n} + 14)\mathbf{h}$

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 $\hat{\mathbf{G}}$ 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.

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 [14] 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 [27]. The basic idea behind [27], which extends [15], follows from the observation that for each GS equation type tp , the CRS space \mathcal{K} is partitioned into a perfectly sound CRS space $\mathcal{K}_{\text{tp}}^b$ and a perfectly witness indistinguishable CRS space $\mathcal{K}_{\text{tp}}^h$.

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 K_{corr} which on input crs_{GS} and some set of indexes $A \subset [n]$, $|A| = t$, generates n GS common reference strings $\{\text{crs}_i, i \in [n]\}$ and simulation trapdoors $\tau_{i,\text{sim}}, i \in A^c$, in a such a way that⁷:

- a) it can be publicly verified the set of perfectly sound keys, $\{\text{crs}_i : \text{crs}_i \in \mathcal{K}_{\text{tp}}^b\}$ is of size at least t ,
- b) there exists a simulator S_{corr} who outputs $(\text{crs}_i, \tau_{i,\text{sim}})$ for all $i \in [n]$, and the distribution of $\{\text{crs}_i : i \in [n]\}$ is the same as the one of the keys output by K_{corr} when crs_{GS} is the perfectly witness-indistinguishable CRS.

The prover of t -out-of- n satisfiability can run K_{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 $i \in A^c$).

Ràfols gives two constructions for PPEs, the first one can be found in [27], App. C and the other follows from [27, Sect. 7]⁸. Our algorithm K_{corr} for PPEs⁹ goes as follows:

- Define (b_1, \dots, 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 $\hat{\mathbf{z}}_i := \text{Comm}(b_i) = b_i \hat{\mathbf{u}}_1 + r_i \hat{\mathbf{u}}_2$, $r_i \in \mathbb{Z}_q$, and define $\tau_{\text{sim},i} = r_i$, for all $i \in A^c$. Define $\text{crs}_i := (\Gamma, \hat{\mathbf{z}}_i, \hat{\mathbf{u}}_2, \check{\mathbf{v}}_1, \check{\mathbf{v}}_2)$.
- 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 $b_i = 1$, $(\hat{\mathbf{z}}_i - \hat{\mathbf{u}}_1) \in \text{Span}(\hat{\mathbf{u}}_2)$, therefore $\text{crs}_i \in \mathcal{K}_{PPE}^b$ and when $b_i = 0$, $(\hat{\mathbf{z}}_i - \hat{\mathbf{u}}_1) \notin \text{Span}(\hat{\mathbf{u}}_2)$ so $\text{crs}_i \in \mathcal{K}_{PPE}^h$.

⁷ More technically, this is the notion of *Simulatable Verifiable Correlated Key Generation* in [27], which extends the definition of Verifiable Correlated Key Generation of [15].

⁸ The construction in [27, Sect. 7] is for other equation types but can be used to prove that t -out-of- n of $\text{crs}_1, \dots, \text{crs}_n$ are perfectly binding for PPEs.

⁹ Properly speaking the construction is for PPEs which are left-simulatable in the terminology of [27].

More Efficient Proof of Membership in a List. Chandran *et al.* construct a ring signature of size $\Theta(\sqrt{n})$ [7], 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 $L = (\hat{l}_1, \dots, \hat{l}_n)$ 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{c} to some element \hat{l}_α , 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, \dots, b_m and b'_1, \dots, 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 $\hat{x}_1 := \hat{l}_{(i_\alpha, 1)}, \dots, \hat{x}_m := \hat{l}_{(i_\alpha, m)}$.
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 [27]. Using our proofs for bit-strings of weight 1 from Sect. 5.3, 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 $(2\mathbf{g} + 4\mathbf{h})\sqrt{n}$ to $4\mathbf{g} + 8\mathbf{h}$. A complete description of the proof can be found in the full version, 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 $\Theta(\sqrt[3]{n})$.

References

1. 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, Berlin, Germany. 2
2. 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>. 4
3. Anonymous. Qa-nizk arguments in asymmetric groups: New tools and new constructions (supplementary material), 2015.
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, Berlin, Germany. 21

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. 21
6. 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, Berlin, Germany. 21
7. 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, Berlin, Germany. 21, 23
8. 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, Berlin, Germany. 2
9. 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, Berlin, Germany. 2, 4, 6
10. 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, Berlin, Germany. 21
11. 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, Berlin, Germany. 2
12. S. D. Galbraith, K. G. Paterson, and N. P. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16):31133121, 2008. 2
13. 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, Berlin, Germany. 2
14. 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, Berlin, Germany. 22
15. 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, Berlin, Germany. 22
16. 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, Berlin, Germany. 5
17. J. Groth and A. Sahai. Efficient noninteractive proof systems for bilinear groups. *SIAM J. Comput.*, 41(5):1193–1232, 2012. 2, 13
18. 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, Berlin, Germany. 6
19. 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, Berlin, Germany. 2
20. 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, Bangalore, India, Dec. 1–5, 2013. Springer, Berlin, Germany. 2, 8
 21. 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, Berlin, Germany. 2, 4, 12, 14
 22. 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, Berlin, Germany. 2, 3, 9, 10, 11
 23. 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, Berlin, Germany. 2, 9
 24. 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, Berlin, Germany. 7
 25. 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>. 3, 6, 12
 26. 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, Berlin, Germany. 2
 27. 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, Berlin, Germany. 2, 21, 22, 23
 28. 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/>. 6