QA-NIZK Arguments of Same Opening for Bilateral Commitments

Carla Ràfols, Javier Silva

Universitat Pompeu Fabra, Barcelona, Spain.
{carla.rafols,javier.silva}@upf.edu

Abstract. Zero-knowledge proofs of satisfiability of linear equations over a group are often used as a building block of more complex protocols. In particular, in an asymmetric bilinear group we often have two commitments in different sides of the pairing, and we want to prove that they open to the same value. This problem was tackled by González, Hevia and Ràfols (ASIACRYPT 2015), who presented an aggregated proof, in the QA-NIZK setting, consisting of only four group elements. In this work, we present a more efficient proof, which is based on the same assumptions and consists of three group elements. We argue that our construction is optimal in terms of proof size.

Keywords: pairing-based cryptography, zero-knowledge proofs, commitments.

1 Introduction

Bilinear groups have been used to design countless cryptographic protocols, some of them with no equivalent in other settings. In particular, such groups have been very useful to design non-interactive zero-knowledge (NIZK) proofs in the common reference string (CRS) model. The first works to realize that pairings allowed for the construction of efficient NIZK proofs were [20,19,17,5], culminating in the work of Groth–Sahai [21]. The latter presents a NIZK proof system for satisfiability of most types of linear and quadratic equation in bilinear groups, in the CRS model and under standard, constant size and weak assumptions. Groth–Sahai proofs are one of the fundamental building blocks in pairing-based cryptography, with well-known applications as anonymous credentials [13], e-Cash [3], ring-signatures [8], shuffles [18], signatures of knowledge [4], and tight CCA encryption [22].

Groth–Sahai proofs follow the usual commit-and-prove paradigm: first, the prover commits to the solution of the equation, and then produces a “proof” formed of some group elements, which the verifier uses together with the commitments to get convinced of the satisfiability of the equation. The commit-and-prove framework is used implicitly in the original work of Groth and Sahai [21], and formalized explicitly in [13,10]. In this view, a NIZK proof proves some property of a committed value, and many different statements about a single committed value can be proven.[1] This formalization is also a conceptually cleaner approach. It allows to differentiate clearly between the "commit" and the "proof" part among all the elements computed by the prover. In this work we also make the separation between commitment and proof, so when we discuss proof sizes we refer exclusively to the latter part.

For many equation types, the Groth–Sahai proof system is still the state of the art. Few improvements are known, like the general techniques to replace dual mode commitments by ElGamal ciphertexts [10], aggregation of many Groth–Sahai proofs [24,16], which are of limited applicability, or some techniques to encode partial satisfiability [30].

A notable exception are quasi-adaptive NIZK (QA-NIZK) arguments of membership in linear spaces over a source group [27,24,26], introduced by Jutla–Roy [23], which allow to prove satisfiability of linear equations. More precisely, let $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be an asymmetric bilinear group equipped with a pairing. We use implicit notation as in [12], where $[\boldsymbol{y}]_1 \in \mathbb{G}_1^n$ denotes a vector $(y_1\mathcal{P}, \ldots, y_n\mathcal{P})$, for $\mathcal{P}$ a generator of $\mathbb{G}_1$. Such QA-NIZK arguments allow to prove that a vector $[\boldsymbol{y}]_1 \in \mathbb{G}_1^n$ is of the form $\boldsymbol{y} = \mathbf{M}\boldsymbol{w}$, for some public matrix $[\mathbf{M}]_1 \in \mathbb{G}_1^{n \times t}$. These arguments are extremely efficient: under an assumption weaker than DDH, their size is only 1 group element, for most distributions of $[\mathbf{M}]_1$.[2] The same statement proven with Groth–Sahai proofs requires $O(t)$ elements for committing to $\boldsymbol{w}$ and $O(n)$ elements to prove that $\boldsymbol{y}$ is of this form.

Because of their efficiency, these arguments have many applications, for instance to different flavors of identity-based encryption [23] or group signatures [28]. These arguments also have a close relation to structure-preserving signatures [2,25,1]. Membership in linear spaces naturally encodes statements about ciphertexts and commitments: for example, two ElGamal ciphertexts (or more generally, any 'algebraic' commitment scheme, like Pedersen or Groth–Sahai commitments) encrypt the same message if their difference is in a certain linear space dependent of the public key. More generally, QA-NIZK arguments allow to aggregate proof easily: proving that two vectors of ElGamal commitments open pairwise to the same value requires only one group element, using the constructions of Kiltz-Wee [26], and the security relies on Kernel assumptions [29]. On the other hand, with the Groth–Sahai proof system, this requires two elements of each group $\mathbb{G}_1, \mathbb{G}_2$ for each pair of ciphertexts.

In this paper, we consider the problem of proving that two commitments, one in $\mathbb{G}_1$ and one in $\mathbb{G}_2$, open to the same value. This statement appears naturally when one wants to prove quadratic relations in asymmetric bilinear groups. Indeed, suppose that we want to prove that a commitment opens to a bit, that is, that the opening of some commitments satisfies the quadratic equation $X(X-1) = 0$. This often appears as part of a larger proof, for example in ring signatures [8,15,14], e-voting [7] or range proofs [6]. To prove that a commitment opens to a bit, Groth–Sahai proofs proceed as follows:

[1] In contrast, if one thinks of Groth–Sahai proofs as NIZK proofs of satisfiability of quadratic equations, formally commitments cannot be reused across proofs.

[2] More precisely, $[\mathbf{M}]_1$ should be taken from a witness sampleable distribution.

1. Rewrite the equation as $X(Y-1)=0$.
2. Commit to a solution: $[c]_1 = \mathsf{Com}(x; r)$ and $[d]_2 = \mathsf{Com}(y; s)$.
3. Prove satisfiability of the equation $X(Y-1)=0$ using the commitments c, d and providing some additional proof elements.
4. Prove that the commitments c, d open to the same value.

We note that step 4 is proving the linear equation $X = Y$. Informally, the idea is that step 3 is a quadratic check which requires commitments in different groups, and step 4 makes sure there is some consistency between these values. Formally, the need for it arises from the fact that Groth–Sahai proofs work for disjoint sets of variables in $\mathbb{G}_1$ and $\mathbb{G}_2$.

This is one of the main techniques for proving quadratic equations in $\mathbb{Z}_p$ in bilinear groups (in the CRS model and under standard assumptions), and any efficiency improvement in the same opening step (4) would have a direct impact on the overall efficiency. We note that there is another construction, introduced very recently in [9], that proves that a commitment over $\mathbb{G}_1$ opens to either 0 or 1. Their approach consists of using a pairing to compile interactive arguments into non-interactive ones, and they manage to prove that a commitment opens to a bit with 7 group elements. For comparison, the Groth–Sahai approach requires 10 group elements using our approach. Groth–Sahai proofs still seem better for proving that n commitments to a bit: in [9] the proof scales linearly, whereas if we use the aggregated version of our scheme, n proofs require $6n+3$ elements.

1.1 Our Results.

To the best of our knowledge, there are two ways of proving step 4. One is to use standard Groth–Sahai proofs, which requires 2 group elements in each of $\mathbb{G}_1$ and $\mathbb{G}_2$. The alternative is to use QA-NIZK arguments of membership in linear spaces. However, because the statement is split between $\mathbb{G}_1$ and $\mathbb{G}_2$, we need to resort to arguments of membership in bilateral spaces, which show, for two vectors $[\boldsymbol{x}]_1, [\boldsymbol{y}]_2$, and some matrices $[\mathbf{M}]_1, [\mathbf{M}]_2$ that there exists some $\boldsymbol{w}$ such that $\boldsymbol{x} = \mathbf{M}\boldsymbol{w}$ and $\boldsymbol{y} = \mathbf{N}\boldsymbol{w}$. These were constructed by González et al. [16] under some computational assumption in bilinear groups.[3] However, this does not improve step (4) over the cost of Groth–Sahai proofs. The proof of González et al. only improves on the state of the art for the aggregated case, namely to show that n pairs of commitments open (pairwise) to the same value with a proof made of 2 elements in $\mathbb{G}_1$ and 2 elements in $\mathbb{G}_2$, independent of n. However, this is not an improvement for a single pair of commitments.

Noticing the gap between one element for one-sided proofs and four elements for bilateral proofs, a natural question is how much we can reduce the proof size in the bilateral case. In this paper, we give a construction which reduces the

[3] Standard QA-NIZK arguments can be proven sound under Kernel Matrix Diffie-Hellman Assumptions (KerMDH) [29], and bilateral arguments can be proven sound under Split KerMDH, a natural generalization to bilinear groups. In its weakest and most efficient instatiation, KerMDH is weaker than DDH, and SKerMDH is weaker than 2-Lin.

proof size of [16] to three elements, while maintaining the same computational assumption in the soundness proof.

We note that this is the first concrete improvement for step (4) since the publication of the work of Groth–Sahai. Our result is a sophisticated combination of the techniques of Kiltz–Wee [26] and González et al. [16]. Additionally, we argue that our constructions are optimal, by showing that any two-element proof is vulnerable to a simple attack.

1.2 Our Techniques

We briefly review the linear space membership proof of Kiltz–Wee [26]. Their core idea is a clever translation to the bilinear group setting of a hash proof system, which is essentially a NIZK proof in the symmetric key setting. Given a matrix $\mathbf{M} \in \mathbb{Z}_p^{m \times t}$, the starting point is a proof system for the language

$$\mathcal{L}_{\mathbf{M}} = \{[\boldsymbol{c}]_1 \leftarrow \mathbb{G}_1^m \mid \exists \boldsymbol{w} \text{ s. t. } \boldsymbol{c} = \mathbf{M}\boldsymbol{w}\}$$

which works as follows: prover and verifier share a key $\mathbf{K} \leftarrow \mathbb{Z}_p^{m \times (k+1)}$, where k will depend on the hardness assumption used to ensure soundness. The projection $[\mathbf{M}^\top \mathbf{K}]_1$ is published in the CRS. The prover sends $[\boldsymbol{\pi}]_1 = \boldsymbol{w}^\top [\mathbf{M}^\top \mathbf{K}]_1$, and the verifier checks that

$$[\boldsymbol{c}^\top]_1 \mathbf{K} \stackrel{?}{=} [\boldsymbol{\pi}]_1.$$

Intuitively, the proof is sound because if $\boldsymbol{c}$ is not in $\mathbf{Im}(\mathbf{M})$ then $\boldsymbol{c}^\top \mathbf{K}$ is uniformly random given $\mathbf{M}^\top \mathbf{K}$, and thus there is no way for the prover to produce such a proof.

Kiltz–Wee take this idea and remove the need for a shared secret key by using a bilinear group. Now the CRS includes $[\mathbf{A}, \mathbf{K}\mathbf{A}]_2$, for a matrix $\mathbf{A} \in \mathbb{Z}_p^{(k+1) \times k}$. This partially fixes $\mathbf{K}$ without revealing it, the goal being that the verifier can use these elements to verify without needing to know $\mathbf{K}$ as before. The proof is still the same, but the verification is now

$$e([\boldsymbol{c}^\top]_1, [\mathbf{K}\mathbf{A}]_2) \stackrel{?}{=} e([\boldsymbol{\pi}]_1, [\mathbf{A}]_2).$$

By assuming the hardness of a Kernel problem on $\mathbf{A}$, i.e., it is hard to find non-trivial cokernel elements of $\mathbf{A}$, we are essentially back to the argument of the hash proof system. For the right choice of distribution of $\mathbf{A}$, the assumption is believed to hold starting at $k = 1$, so in this case we have that the proof is formed of 2 group elements.

However, this can be taken one step further. Assuming that the distribution of $[\mathbf{M}]_1$ is witness sampleable, that is, that we can efficiently sample $\tilde{\mathbf{M}}$ such that $[\tilde{\mathbf{M}}]_1$ is distributed as $[\mathbf{M}]_1$, then it is enough to use the truncated matrix $\overline{\mathbf{A}} \in \mathbb{Z}_p^{k \times k}$ instead of $\mathbf{A}$, thus using $\mathbf{K} \in \mathbb{Z}_p^{m \times k}$, which yields proofs consisting of only one group element.

We now consider the natural generalization of this approach to bilateral proofs, as developed by González et al. [16].[4] Consider the following language:

$$\mathcal{L}_{\mathbf{M},\mathbf{N}} = \{([\boldsymbol{c}]_1, [\boldsymbol{d}]_2) \leftarrow \mathbb{G}_1^m \times \mathbb{G}_2^n \mid \exists \boldsymbol{w} \text{ s. t. } \boldsymbol{c} = \mathbf{M}\boldsymbol{w}, \boldsymbol{d} = \mathbf{N}\boldsymbol{w}\}.$$

To account for two-sided statements, we consider one key $\mathbf{K}$ for $\mathbb{G}_1$ and one key $\mathbf{L}$ for $\mathbb{G}_2$, and so we publish the following elements in the CRS:

$$[\mathbf{M}^\top \mathbf{K} + \mathbf{Z}, \mathbf{A}, \mathbf{L}\mathbf{A}]_1, [\mathbf{N}^\top \mathbf{L} - \mathbf{Z}, \mathbf{A}, \mathbf{K}\mathbf{A}]_2,$$

where $\mathbf{Z} \in \mathbb{Z}_p^{t \times k}$. The prover produces the proofs $[\boldsymbol{\pi}]_1 = \boldsymbol{w}^\top [\mathbf{M}^\top \mathbf{K} + \mathbf{Z}]_1$ and $[\boldsymbol{\theta}]_2 = \boldsymbol{w}^\top [\mathbf{N}^\top \mathbf{L} - \mathbf{Z}]_2$, and the verifier checks the equation

$$e([\boldsymbol{c}^\top]_1, [\mathbf{K}\mathbf{A}]_2) + e([\mathbf{L}\mathbf{A}]_1, [\boldsymbol{d}]_2) \stackrel{?}{=} e([\boldsymbol{\pi}]_1, [\mathbf{A}]_2) + e([\mathbf{A}]_1, [\boldsymbol{\theta}]_2). \tag{1}$$

Intuitively, the term $\mathbf{Z}$ in the CRS elements produces terms in the verification equation that will not cancel out unless $\boldsymbol{w}$ is the same in both sides. In a similar way as above, the soundness of this scheme reduces to the hardness of a Split Kernel problem, which is a Kernel problem with the solution split between $\mathbb{G}_1$ and $\mathbb{G}_2$. However, Split Kernel problems are easy for $k = 1$, and so we must take at least $k = 2$. This has a direct impact on the sizes of the keys $\mathbf{K}$ and $\mathbf{L}$, and so this approach yields proofs of two group elements in $\mathbb{G}_1$, and two in $\mathbb{G}_2$, and two verification equations.

Our strategy to reduce the proof size is to use only one element in $\mathbb{G}_2$, so instead of having $\boldsymbol{\theta} = (\theta, \hat{\theta})$ as above, we reuse the same θ. To make it work, we require the condition that the columns of $\mathbf{N}^\top \mathbf{L}$ are equal, so that $\boldsymbol{\theta} = (\theta, \theta)$, and it is enough to send it once. This introduces extra complexity in the CRS generation, and the simulation of the CRS for the adversary in the soundness security reduction, particularly in the aggregated case. We present the proof directly for the most efficient case, $k = 2$.

To solve these new issues, we need to reformulate the problem slightly. Instead of considering the pair of commitments $([\boldsymbol{c}]_1, [\boldsymbol{d}]_2)$ as the statement, we consider just $[\boldsymbol{c}]_1$, and build a proof of F-knowledge of $F(\boldsymbol{w}) = [\boldsymbol{w}]_{1,2}$. Indeed, in applications the commitment $[\boldsymbol{d}]_2$ is an artifact of the proof, as when proving quadratic statements we need to split the commitments between $\mathbb{G}_1$ and $\mathbb{G}_2$ to exploit the pairing. Regarding zero-knowledge, this change implies that the simulator knows the opening of one of the commitments. We note that both openings are required for proving zero-knowledge in Groth–Sahai proofs.

We stress that our modified formalization is due to the intricacies of the soundness reduction, and has no actual impact in most applications. This is because, as we have seen in the proof of $X(X-1) = 0$ above, the commitment in $\mathbb{G}_2$ is a byproduct of the proof, and thus can be seen as part of it, while the 'meaningful' statement is about the commitment in $\mathbb{G}_1$.

Interestingly, our trick of reusing θ does not work for both sides, and in fact in Section 5 we show an attack for any two-element proof of this form. We

[4] The actual construction requires some masking terms to ensure zero-knowledge, but we omit these for simplicity of the presentation.

argue that the general form of any proof of bilateral same opening consisting of only two elements must have a verification equations that looks essentially like equation (1) above, but with π, θ scalars instead of vectors; then we show a simple algebraic attack that exploits the two-sided nature of the proof.

2 Preliminaries

Let $\mathcal{G}$ be some probabilistic polynomial time algorithm which on input 1^λ, where λ is the security parameter, returns the *group key* which is the description of an asymmetric bilinear group $gk := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \mathcal{P}_1, \mathcal{P}_2)$, where $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ are additive groups of prime order p, the elements $\mathcal{P}_1, \mathcal{P}_2$ are generators of $\mathbb{G}_1, \mathbb{G}_2$ respectively, $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is an efficiently computable, non-degenerate bilinear map, and there is no efficiently computable isomorphism between $\mathbb{G}_1$ and $\mathbb{G}_2$.

Elements in $\mathbb{G}_\gamma$ are denoted implicitly as $[a]_\gamma := a\mathcal{P}_\gamma$, where $\gamma \in \{1, 2, T\}$ and $\mathcal{P}_T := e(\mathcal{P}_1, \mathcal{P}_2)$. For simplicity, we often write $[a]_{1,2}$ for the pair $[a]_1, [a]_2$, and $[a, b]_\gamma$ for $([a]_\gamma, [b]_\gamma)$. The pairing operation will be written as a product, that is, $[a]_1 \cdot [b]_2 = [a]_1[b]_2 = e([a]_1, [b]_2) = [ab]_T$. Vectors and matrices are denoted in boldface. Given a matrix $\mathbf{T} = (t_{i,j})$, $[\mathbf{T}]_\gamma$ is the natural embedding of $\mathbf{T}$ in $\mathbb{G}_\gamma$, that is, the matrix whose (i, j)th entry is $t_{i,j}\mathcal{P}_\gamma$. We denote by $|\mathbb{G}_\gamma|$ the bit-size of the elements of $\mathbb{G}_\gamma$.

2.1 Quasi-Adaptive Non-Interactive Zero-Knowledge Proofs

A Quasi-Adaptive NIZK proof system [23] enables to prove membership in a language defined by a relation $\mathcal{R}_\rho$, which is in turn determined by some parameter ρ sampled from a distribution $\mathcal{D}_{gk}$. We say that $\mathcal{D}_{gk}$ is *witness sampleable* if there exists an efficient algorithm that samples (ρ, ω) from a distribution $\mathcal{D}_{gk}^{\mathsf{par}}$ such that ρ is distributed according to $\mathcal{D}_{gk}$, and membership of ρ in the *parameter language* $\mathcal{L}_{\mathsf{par}}$ can be efficiently verified with ω. While the Common Reference String (CRS) can be set based on ρ, the zero-knowledge simulator is required to be a single PPT algorithm that works for any relation $\mathcal{R}_{gk}$. We assume that CRS contains an encoding of ρ, which is thus available to V.

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

Quasi-Adaptive Completeness:

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

Computational Quasi-Adaptive Soundness:

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

Perfect Quasi-Adaptive Zero-Knowledge:

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

where

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

We will prove that our schemes have F-knowledge soundness, which we define in the context of witness sampleable distributions. Intuitively, F-knowledge means that, with access to some extraction key, it is possible to extract a function F of the witness from the statement and the proof. We note that our definition differs from the definition in [10], as we give the extraction key generator access to the witness ω that proves membership of ρ in $\mathcal{L}_{\mathsf{par}}$ (in practice, this means that it has access to the discrete logarithms of the commitment key) and allow to extract information from not only the statement, but also the proof.

Given a function F, a scheme is F-knowledge sound if there exist a soundness PPT extraction key generator E_1 and a DPT extractor E_2 such that for any non-uniform PPT adversary $\mathcal{A}_2$, we have:

Computational Quasi-Adaptive F-knowledge Soundness:

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{K}_0(1^\lambda); \rho \leftarrow \mathcal{D}_{gk}; \\ (\mathsf{CRS}, xk) \leftarrow \mathsf{E}_1(gk,(\rho,\omega)); \\ (x,\pi) \leftarrow \mathcal{A}_2(gk,\mathsf{CRS}) \end{array} : \begin{array}{c} \mathsf{V}(\mathsf{CRS},x,\pi) = 1 \text{ and} \\ \mathsf{E}_{2xk}(x,\pi) \neq F(x,w) \end{array}\right] \approx 0,$$

and the distributions of the CRS produced by K_1 and E_1 are the same.

We also define a stronger notion of zero-knowledge, called composable zero-knowledge [17]. Essentially, this means that real and simulated proofs are indistinguishable even when the simulation trapdoor is known. More formally, a scheme is composable zero-knowledge if there exists a PPT simulator $(\mathsf{S}_1,\mathsf{S}_2)$ such that for any non-uniform PPT adversary $\mathcal{A}_3$ we have:

Composable Quasi-Adaptive Zero-Knowledge:

$$\Pr\left[\begin{array}{c} gk \leftarrow \mathsf{K}_0(1^\lambda); \rho \leftarrow \mathcal{D}_{gk}; (\mathsf{CRS},\tau) \leftarrow \mathsf{S}_1(gk,\rho); \\ (x,w) \leftarrow \mathcal{A}_3(gk,\mathsf{CRS},\tau); \pi \leftarrow \mathsf{P}(gk,\mathsf{CRS},x,w) \end{array} : \mathcal{A}_3(\pi) = 1\right] =$$
$$= \Pr\left[\begin{array}{c} gk \leftarrow \mathsf{K}_0(1^\lambda); \rho \leftarrow \mathcal{D}_{gk}; (\mathsf{CRS},\tau) \leftarrow \mathsf{S}_1(gk,\rho); \\ (x,w) \leftarrow \mathcal{A}_3(gk,\mathsf{CRS},\tau); \pi \leftarrow \mathsf{S}_2(gk,\mathsf{CRS},\tau,x) : \end{array} : \mathcal{A}_3(\pi) = 1\right].$$

and the CRS produced by K_1 and S_1 are indistinguishable.

2.2 Assumptions

Definition 1. *Let $\ell, k \in \mathbb{N}$. We call $\mathcal{D}_{\ell,k}$ a matrix distribution if it outputs (in PPT time, with overwhelming probability) matrices in $\mathbb{Z}_p^{\ell\times k}$. We define $\mathcal{D}_k := \mathcal{D}_{k+1,k}$.*

The following applies for $\mathbb{G}_\gamma$, where $\gamma \in \{1, 2\}$.

Assumption 1 (Matrix Decisional Diffie-Hellman Assumption in $\mathbb{G}_\gamma$ [11]) *For all non-uniform PPT adversaries $\mathcal{A}$,*

$$|\Pr[\mathcal{A}(gk, [\mathbf{A}, \mathbf{A}\boldsymbol{w}]_\gamma) = 1] - \Pr[\mathcal{A}(gk, [\mathbf{A}, \boldsymbol{z}]_\gamma) = 1]| \approx 0,$$

where the probability is taken over $gk \leftarrow \mathcal{G}(1^\lambda)$, $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}, \boldsymbol{w} \leftarrow \mathbb{Z}_p^k, [\boldsymbol{z}]_\gamma \leftarrow \mathbb{G}_\gamma^\ell$ and the coin tosses of adversary $\mathcal{A}$.

Intuitively, the $\mathcal{D}_{\ell,k}$-MDDH assumption means that it is hard to decide whether a vector is in the image space of a matrix or it is a random vector, where the matrix is drawn from $\mathcal{D}_{\ell,k}$. In this paper we will refer to the following matrix distributions:

$$\mathcal{L}_k : \mathbf{A} = \begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_k \\ 1 & 1 & \dots & 1 \end{pmatrix}, \qquad \mathcal{RL}_k : \mathbf{A} = \begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_k \\ r_1 & r_2 & \dots & r_k \end{pmatrix},$$

where $a_i, r_i \leftarrow \mathbb{Z}_p$ for $i = 1, \dots, k$. The $\mathcal{L}_k$-MDDH Assumption is the k-linear family of Decisional Assumptions and corresponds to the Decisional Diffie-Hellman (DDH) Assumption in $\mathbb{G}_\gamma$ when $k = 1$. The SXDH Assumption states that DDH holds in $\mathbb{G}_\gamma$ for $\gamma = 1, 2$.

Additionally, we will be using the following family of computational assumptions:

Assumption 2 (Kernel Diffie-Hellman Assumption in $\mathbb{G}_\gamma$ [29]) *For all non-uniform PPT adversaries $\mathcal{A}$:*

$$\Pr\left[[\boldsymbol{x}]_{3-\gamma} \leftarrow \mathcal{A}(gk, [\mathbf{A}]_\gamma) : \boldsymbol{x} \neq 0 \wedge \boldsymbol{x}^\top \mathbf{A} = \mathbf{0}\right] \approx 0,$$

where the probability is taken over $gk \leftarrow \mathcal{G}(1^\lambda)$, $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$ and the coin tosses of adversary $\mathcal{A}$.

The $\mathcal{D}_{\ell,k}$-$\mathsf{KerMDH}_{\mathbb{G}_\gamma}$ Assumption is not stronger than the $\mathcal{D}_{\ell,k}$-$\mathsf{MDDH}_{\mathbb{G}_\gamma}$ Assumption, since a solution to the former allows to decide membership in $\mathbf{Im}([\mathbf{A}]_\gamma)$. In asymmetric bilinear groups, there is a natural variant of this assumption.

Assumption 3 (Split Kernel Diffie-Hellman Assumption [16]) *For all non-uniform PPT adversaries $\mathcal{A}$:*

$$\Pr\left[[\boldsymbol{r}]_1, [\boldsymbol{s}]_2 \leftarrow \mathcal{A}(gk, [\mathbf{A}]_{1,2}) : \boldsymbol{r} \neq \boldsymbol{s} \wedge \boldsymbol{r}^\top \mathbf{A} = \boldsymbol{s}^\top \mathbf{A}\right] \approx 0,$$

where the probability is taken over $gk \leftarrow \mathcal{G}(1^\lambda)$, $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$ and the coin tosses of adversary $\mathcal{A}$.

While the Kernel Diffie-Hellman Assumption says one cannot find a non-zero vector in one of the groups which is in the co-kernel of $\mathbf{A}$, the split assumption says one cannot find different vectors in $\mathbb{G}_1^\ell \times \mathbb{G}_2^\ell$ such that the difference of the vector of their discrete logarithms is in the co-kernel of $\mathbf{A}$. As a particular case, [16] considers the *Split Simultaneous Double Pairing Assumption in* $\mathbb{G}_1, \mathbb{G}_2$ (SSDP) which is the $\mathcal{RL}_2$-SKerMDH Assumption.

3 Linear Relations in a Bilinear Group

3.1 Algebraic Commitment Schemes

We present the type of commitments for which our QA-NIZK arguments can be used. These generalize many common schemes, like (multi-)Pedersen commitments and Groth–Sahai commitments. Our commitments are in the source groups, $\mathbb{G}_\gamma$ for $\gamma = 1, 2$, of a bilinear group. Let $\mathbf{F} \in \mathbb{Z}_p^{m \times n}$ and $\mathbf{U} \in \mathbb{Z}_p^{m \times \ell}$ be full-rank matrices. The commitment key is $ck = [\mathbf{F}, \mathbf{U}]_\gamma$, and the commitment to a message $\boldsymbol{x} \in \mathbb{Z}_p^n$ with randomness $\boldsymbol{r} \in \mathbb{Z}_p^\ell$ is defined as

$$\mathsf{Com}_{ck}(\boldsymbol{x}; \boldsymbol{r}) = [\mathbf{F}\boldsymbol{x} + \mathbf{U}\boldsymbol{r}]_\gamma.$$

Choosing the appropriate distributions for $([\mathbf{F}]_\gamma, [\mathbf{U}]_\gamma)$, we can have two commitment keys, one that produces a perfectly binding commitment scheme and one that produces a perfectly hiding commitment scheme, and these two key distributions are computationally indistinguishable under a MDDH assumption (see [11] for details). In the description of our schemes and the soundness proofs we will use the perfectly binding key, switching to perfectly hiding to argue that our schemes are zero-knowledge.

The most well-known example is Groth–Sahai commitments to integers: given $x \in \mathbb{Z}_p$ and randomness $r \in \mathbb{Z}_p$, this is an instantiation of the commitment defined above, with the matrices $\mathbf{F} \leftarrow \mathbb{Z}_p^2, \mathbf{U} \leftarrow \mathbb{Z}_p^2$ when in perfectly binding mode, and $\mathbf{F} \leftarrow \mathbb{Z}_p^2, \mathbf{U} = \lambda\mathbf{F}$ for $\lambda \leftarrow \mathbb{Z}_p$, when in perfectly hiding mode.

3.2 Linear Equations in a Bilinear Group

A set of linear equations split between the two sides of a bilinear group can be written as

$$\begin{pmatrix} [\boldsymbol{c}]_1 \\ [\boldsymbol{d}]_2 \end{pmatrix} = \begin{pmatrix} [\mathbf{M}]_1 \\ [\mathbf{N}]_2 \end{pmatrix} \boldsymbol{X},$$

where $\boldsymbol{X}$ is the vector of unknowns, $[\boldsymbol{c}, \mathbf{M}]_1$ are the coefficients in $\mathbb{G}_1$ and $[\boldsymbol{d}, \mathbf{N}]_2$ are the coefficients in $\mathbb{G}_2$. Thus, proving satisfiability of this system is equivalent to proving that there exist some vector $\boldsymbol{w}$ such that

$$\boldsymbol{w} \in \mathbf{Im} \begin{pmatrix} \mathbf{M} \\ \mathbf{N} \end{pmatrix}.$$

Thus, these proofs are usually seen as proofs of membership in a linear subspace, in this case split between $\mathbb{G}_1$ and $\mathbb{G}_2$. The problem of same opening of two algebraic commitments,

$$[\boldsymbol{c}]_1 = \mathsf{Com}_{ck_1}(\boldsymbol{x};\boldsymbol{r}) = [\mathbf{F}\boldsymbol{x} + \mathbf{U}\boldsymbol{r}]_1, \qquad [\boldsymbol{d}]_1 = \mathsf{Com}_{ck_2}(\boldsymbol{x};\boldsymbol{s}) = [\mathbf{G}\boldsymbol{x} + \mathbf{V}\boldsymbol{s}]_2$$

can be seen in this framework of membership in linear spaces, where

$$\begin{pmatrix} [\boldsymbol{c}]_1 \\ [\boldsymbol{d}]_2 \end{pmatrix} = \left(\begin{array}{c|c|c} [\mathbf{F} & \mathbf{U} & \mathbf{0}]_1 \\ [\mathbf{G} & \mathbf{0} & \mathbf{V}]_2 \end{array}\right) \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{r} \\ \boldsymbol{s} \end{pmatrix}.$$

Since we are particularly interested in the case of same opening, we present our constructions directly for this application, although it would be easy to generalize to any matrices $[\mathbf{M}]_1, [\mathbf{N}]_2$, as long as they verify some conditions on their dimensions. As a warm-up, we develop first a non-aggregated version of the proof, as the main ideas are easier to visualize in this case.

4 Non-Aggregated Scheme

Given $x \in \mathbb{Z}_p$ and two commitments $[\boldsymbol{c}]_1, [\boldsymbol{d}]_2$ to x, we provide a proof of both commitments opening to the same element x. More precisely, given a group description gk and commitment keys $ck_1 = [\boldsymbol{f}, \boldsymbol{u}]_1 \in \mathbb{G}_1^{2\times 2}$ and $ck_2 = [\boldsymbol{g}, \boldsymbol{v}]_2 \in \mathbb{G}_2^{2\times 2}$, we want to prove F-knowledge in the language

$$\mathcal{L}_{gk,ck_1} = \{[\boldsymbol{c}]_1 \in \mathbb{G}_1^2 \mid \exists x, r \text{ s. t. } [\boldsymbol{c}]_1 = \mathsf{Com}_{ck_1}(x;r) = [x\boldsymbol{f} + r\boldsymbol{u}]_1\},$$

where $F(x,r) = [x]_{1,2}$.

- $gk := (p, \mathcal{P}_1, \mathcal{P}_2, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow \mathcal{G}(1^\lambda)$.
- $\mathsf{K}_0(gk)$: set $ck_1 = [\boldsymbol{f}, \boldsymbol{u}]_1 \leftarrow \mathcal{D}_{\mathsf{par}}$, where $\mathcal{D}_{\mathsf{par}}$ is witness sampleable, that is, there exists an efficiently sampleable distribution $\tilde{\mathcal{D}}_{\mathsf{par}}$ outputting $(\tilde{\boldsymbol{f}}, \tilde{\boldsymbol{u}})$ such that $[\tilde{\boldsymbol{f}}, \tilde{\boldsymbol{u}}]_1$ is distributed as $[\boldsymbol{f}, \boldsymbol{u}]_1$.
- $\mathsf{K}_1(gk, ck_1)$: set $ck_2 = [\boldsymbol{g}, \boldsymbol{v}]_2$, where $\boldsymbol{g}, \boldsymbol{v} \leftarrow \mathbb{Z}_p^2$. Choose $a_1, a_2 \leftarrow \mathbb{Z}_p$ and also $\boldsymbol{k}_u, \hat{\boldsymbol{k}}_u, \boldsymbol{l}_v, \hat{\boldsymbol{l}}_v \leftarrow \mathbb{Z}_p^2$ conditioned on

  $$\boldsymbol{l}_v^\top \boldsymbol{v} = \hat{\boldsymbol{l}}_v^\top \boldsymbol{v}, \tag{2}$$

  Finally, choose $z_2 \leftarrow \mathbb{Z}_p$ and set

  $$w = \frac{\boldsymbol{k}_u^\top \boldsymbol{f}}{\boldsymbol{l}_v^\top \boldsymbol{g}}, \qquad z_1 = z_2 w,$$
  $$\hat{w} = \frac{\hat{\boldsymbol{k}}_u^\top \boldsymbol{f}}{\hat{\boldsymbol{l}}_v^\top \boldsymbol{g}}, \qquad \hat{z}_1 = z_2 \hat{w}.$$

  Algorithm K_1 outputs the following CRS:

  $$\begin{pmatrix} gk, ck_1, [\boldsymbol{k}_u^\top \boldsymbol{u}]_1, [\hat{\boldsymbol{k}}_u^\top \boldsymbol{u}]_1, [a_1 w]_1, [a_2 \hat{w}]_1, [a_1 w \boldsymbol{l}_v]_1, [a_2 \hat{w} \hat{\boldsymbol{l}}_v]_1, [z_1]_1, [\hat{z}_1]_1, \\ ck_2, [\boldsymbol{l}_v^\top \boldsymbol{v}]_2, [a_1]_2, [a_2]_2, [a_1 \boldsymbol{k}_u]_2, [a_2 \hat{\boldsymbol{k}}_u]_2, [z_2]_2 \end{pmatrix}.$$

- $\mathsf{P}(\mathrm{CRS}, ([\boldsymbol{c}]_1, x, r) \in \mathcal{R})$: commit to x in $\mathbb{G}_2$ by choosing $s \leftarrow \mathbb{Z}_p$ and setting
$$[\boldsymbol{d}]_2 = \mathsf{Com}_{ck_2}(x, s) = [x\boldsymbol{g} + s\boldsymbol{v}]_2.$$
Choose $\delta \leftarrow \mathbb{Z}_p$ and output $[\boldsymbol{d}]_2$ and
$$\begin{aligned} [\pi]_1 &= [r\boldsymbol{k}_u^\top \boldsymbol{u} + \delta z_1]_1, & [\theta]_2 &= [s\boldsymbol{l}_v^\top \boldsymbol{v} + \delta z_2]_2, \\ [\hat{\pi}]_1 &= [r\hat{\boldsymbol{k}}_u^\top \boldsymbol{u} + \delta \hat{z}_1]_1, \end{aligned}$$
- $\mathsf{V}(\mathrm{CRS}, [\boldsymbol{c}]_1, ([\boldsymbol{d}, \theta]_2, [\pi, \hat{\pi}]_1)$: The algorithm outputs 1 iff the following equations hold:
$$\begin{aligned} e\left([\boldsymbol{c}^\top]_1, [a_1\boldsymbol{k}_u]_2\right) - e([a_1 w \boldsymbol{l}_v^\top]_1, [\boldsymbol{d}]_2) &\overset{?}{=} e([\pi]_1, [a_1]_2) - e([a_1 w]_1, [\theta]_2), \\ e\left([\boldsymbol{c}^\top]_1, [a_2\hat{\boldsymbol{k}}_u]_2\right) - e([a_2 \hat{w} \hat{\boldsymbol{l}}_v^\top]_1, [\boldsymbol{d}]_2) &\overset{?}{=} e([\hat{\pi}]_1, [a_2]_2) - e([a_2 \hat{w}]_1, [\theta]_2). \end{aligned}$$

Completeness. Both equations are analogous, and it is easy to see that for honest provers, using that $\boldsymbol{f}^\top \boldsymbol{k}_u = w(\boldsymbol{l}_v^\top \boldsymbol{g})$, we have that
$$\begin{aligned} &\boldsymbol{c}^\top(a_1\boldsymbol{k}_u) - (a_1 w \boldsymbol{l}_v^\top)\boldsymbol{d} = (x\boldsymbol{f}^\top + r\boldsymbol{u}^\top)(a_1\boldsymbol{k}_u) - (a_1 w \boldsymbol{l}_v^\top)(x\boldsymbol{g} + s\boldsymbol{v}) = \\ &= a_1 x \boldsymbol{f}^\top \boldsymbol{k}_u - a_1 x (w \boldsymbol{l}_v^\top \boldsymbol{g}) + (r\boldsymbol{u}^\top \boldsymbol{k}_u) a_1 - a_1 w (s\boldsymbol{v}^\top \boldsymbol{l}_v) = \pi a_1 - a_1 w \theta. \end{aligned}$$

F-extractor. We now define the algorithm that, given the extraction key $xk = (\boldsymbol{f}, \boldsymbol{g}, \boldsymbol{u}, \boldsymbol{v})$, outputs a function of the witness, in this case $F(x, r) = [x]_{1,2}$.

- $\mathsf{Ext}_{xk}([\boldsymbol{c}]_1, [\boldsymbol{d}]_2)$: knowing $\boldsymbol{f}, \boldsymbol{u}$, we can find a vector $\boldsymbol{u}^\perp$ such that $\boldsymbol{u}^\top \boldsymbol{u}^\perp = 0$ and $\boldsymbol{f}^\top \boldsymbol{u}^\perp = 1$, and compute $[\boldsymbol{c}^\top]_1 \boldsymbol{u}^\perp = [x]_1$. Similarly, we obtain $[x]_2$ from $[\boldsymbol{d}]_2$, using $\boldsymbol{g}, \boldsymbol{v}$.

Theorem 1. *The above scheme is computationally F-knowledge sound under the $\mathcal{RL}_2$-$\mathsf{SKerMDH}$ assumption. More precisely, there exists an adversary $\mathcal{B}$ against the $\mathcal{RL}_2$-$\mathsf{SKerMDH}$ problem such that for any PPT adversary $\mathcal{A}$, we have that*
$$\mathsf{Adv}_{F-\mathsf{KnowledgeSoundness}}(\mathcal{A}) \leq \mathsf{Adv}_{\mathcal{RL}_2\text{-}\mathsf{SKerMDH}}(\mathcal{B}).$$

Proof. We assume the existence of an adversary $\mathcal{A}$ against the F-knowledge soundness of the scheme (that is, $\mathcal{A}$ is able to produce a statement and and an accepting proof such that $\mathsf{Ext}_{xk}([\boldsymbol{c}]_1, [\boldsymbol{d}]_2) = ([x]_1, [y]_2)$ and $x \neq y$), and we use it to build an adversary $\mathcal{B}$ against the $\mathcal{RL}_2$-$\mathsf{SKerMDH}$ problem. $\mathcal{B}$ receives the challenge matrix
$$[\mathbf{A}]_{1,2} = [\boldsymbol{a}_1 || \boldsymbol{a}_2]_{1,2} = \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \\ r_1 & r_2 \end{bmatrix}_{1,2},$$
and builds the environment for $\mathcal{A}$ as follows. $\mathcal{B}$ samples $\boldsymbol{f}, \boldsymbol{u} \leftarrow \tilde{\mathcal{D}}_{\mathsf{par}}$ and $\boldsymbol{k}'_u, \hat{\boldsymbol{k}}'_u \leftarrow \mathbb{Z}_p^2$, and $\boldsymbol{u}^\perp \leftarrow \mathbb{Z}_p^2$ conditioned on $\boldsymbol{u}^\top \boldsymbol{u}^\perp = 0$. Implicitly, $\mathcal{B}$ defines
$$\boldsymbol{k}_u = \boldsymbol{k}'_u + a_1^{-1} r_1 \boldsymbol{u}^\perp, \qquad \hat{\boldsymbol{k}}_u = \hat{\boldsymbol{k}}'_u + a_2^{-1} r_2 \boldsymbol{u}^\perp.$$

Observe that this implies that

$$a_1 \boldsymbol{k}_u = a_1 \boldsymbol{k}'_u + r_1 \boldsymbol{u}^\perp, \qquad a_2 \hat{\boldsymbol{k}}_u = a_2 \hat{\boldsymbol{k}}'_u + r_2 \boldsymbol{u}^\perp, \tag{3}$$

which $\mathcal{B}$ can compute in $\mathbb{G}_2$. For the other side, $\mathcal{B}$ samples $\boldsymbol{g}, \boldsymbol{v} \leftarrow \mathbb{Z}_p^2$ and $\boldsymbol{l}'_v \leftarrow \mathbb{Z}_p^2$, and let $\boldsymbol{v}^\perp \in \mathbb{Z}_p^2$ be the unique vector such that $\boldsymbol{v}^\top \boldsymbol{v}^\perp = 0$ and

$$\boldsymbol{f}^\top \boldsymbol{u}^\perp = \boldsymbol{g}^\top \boldsymbol{v}^\perp. \tag{4}$$

$\mathcal{B}$ defines

$$w = \frac{\boldsymbol{k}'^\top_u \boldsymbol{f}}{\boldsymbol{l}'^\top_v \boldsymbol{g}}, \qquad \hat{w} = \frac{\hat{\boldsymbol{k}}'^\top_u \boldsymbol{f}}{\boldsymbol{l}'^\top_v \boldsymbol{g}}, \tag{5}$$

(note that $\boldsymbol{l}'_v$ is the same in both), and implicitly

$$\boldsymbol{l}_v = \boldsymbol{l}'_v + (a_1 w)^{-1} r_1 \boldsymbol{v}^\perp, \qquad \hat{\boldsymbol{l}}_v = \boldsymbol{l}'_v + (a_2 \hat{w})^{-1} r_2 \boldsymbol{v}^\perp,$$

which means that

$$a_1 w \boldsymbol{l}_v = a_1 w \boldsymbol{l}'_v + r_1 \boldsymbol{v}^\perp, \qquad a_2 \hat{w} \hat{\boldsymbol{l}}_v = a_2 \hat{w} \boldsymbol{l}'_v + r_2 \boldsymbol{v}^\perp, \tag{6}$$

and these can be computed in $\mathbb{G}_1$. Note that, by construction,

$$\frac{a_1 \boldsymbol{f}^\top \boldsymbol{k}_u}{a_1 w \boldsymbol{g}^\top \boldsymbol{l}_v} = \frac{a_1 \boldsymbol{f}^\top \boldsymbol{k}'_u + r_1 \boldsymbol{f}^\top \boldsymbol{u}^\perp}{a_1 w \boldsymbol{g}^\top \boldsymbol{l}'_v + r_1 \boldsymbol{g}^\top \boldsymbol{v}^\perp} = 1,$$

where we have used equalities (5) and (4), and therefore $w = \frac{\boldsymbol{f}^\top \boldsymbol{k}_u}{\boldsymbol{g}^\top \boldsymbol{l}_v}$. A similar argument shows that $\hat{w} = \frac{\boldsymbol{f}^\top \hat{\boldsymbol{k}}_u}{\boldsymbol{g}^\top \hat{\boldsymbol{l}}_v}$. $\mathcal{B}$ can also compute

$$[\boldsymbol{k}_u^\top \boldsymbol{u}]_1 = [\boldsymbol{k}'^\top_u \boldsymbol{u}]_1, \qquad [\hat{\boldsymbol{k}}_u^\top \boldsymbol{u}]_1 = [\hat{\boldsymbol{k}}'^\top_u \boldsymbol{u}]_1, \qquad [\boldsymbol{l}_v^\top \boldsymbol{v}]_2 = [\boldsymbol{l}'^\top_v \boldsymbol{v}]_2 = [\hat{\boldsymbol{l}}_v^\top \boldsymbol{v}]_2.$$

Finally, choose $z_2 \leftarrow \mathbb{Z}_p$ and set

$$z_1 = w z_2, \qquad \hat{z}_1 = \hat{w} z_2,$$

completing the CRS. The CRS is then sent to adversary $\mathcal{A}$, who outputs a statement $[\boldsymbol{c}]_1$ and a proof $[\boldsymbol{d}]_2, [\pi]_1, [\hat{\pi}]_1, [\theta]_2$ such that

$$\begin{aligned} \boldsymbol{c}^\top (a_1 \boldsymbol{k}_u) - (a_1 w \boldsymbol{l}_v^\top) \boldsymbol{d} &= \pi a_1 - (a_1 w)\theta, \\ \boldsymbol{c}^\top (a_2 \hat{\boldsymbol{k}}_u) - (a_2 \hat{w} \hat{\boldsymbol{l}}_v^\top) \boldsymbol{d} &= \hat{\pi} a_2 - (a_2 \hat{w})\theta. \end{aligned}$$

Notice that, using the equalities (3) and (6), we can rewrite these expressions in terms of the columns of $\mathbf{A}$. Indeed, these are equivalent to

$$\begin{aligned} \boldsymbol{c}^\top (\boldsymbol{k}'_u || \hat{\boldsymbol{k}}'_u || \boldsymbol{u}^\perp) \boldsymbol{a}_1 - \boldsymbol{d}^\top (w \boldsymbol{l}'_v || \hat{w} \boldsymbol{l}'_v || \boldsymbol{v}^\perp) \boldsymbol{a}_1 &= (\pi, \hat{\pi}, 0) \boldsymbol{a}_1 - (w\theta, \hat{w}\theta, 0) \boldsymbol{a}_1, \\ \boldsymbol{c}^\top (\boldsymbol{k}'_u || \hat{\boldsymbol{k}}'_u || \boldsymbol{u}^\perp) \boldsymbol{a}_2 - \boldsymbol{d}^\top (w \boldsymbol{l}'_v || \hat{w} \boldsymbol{l}'_v || \boldsymbol{v}^\perp) \boldsymbol{a}_2 &= (\pi, \hat{\pi}, 0) \boldsymbol{a}_2 - (w\theta, \hat{w}\theta, 0) \boldsymbol{a}_2. \end{aligned}$$

We rearrange this as a solution of the $\mathcal{RL}_2$-$\mathsf{SKerMDH}$ problem that the reduction $\mathcal{B}$ can compute:

$$e([(\boldsymbol{c}^\top \boldsymbol{k}'_u - \pi || \boldsymbol{c}^\top \hat{\boldsymbol{k}}'_u - \hat{\pi} || \boldsymbol{c}^\top \boldsymbol{u}^\perp)]_1, [\mathbf{A}]_2) = e([(w(\boldsymbol{d}^\top \boldsymbol{l}'_v - \theta) || \hat{w}(\boldsymbol{d}^\top \boldsymbol{l}'_v - \theta) || \boldsymbol{d}^\top \boldsymbol{v}^\perp)]_2, [\mathbf{A}]_1).$$

It remains to argue that this is not the trivial solution. To do so, we look at the third component. As $\{\boldsymbol{f}, \boldsymbol{u}\}$ and $\{\boldsymbol{g}, \boldsymbol{v}\}$ are bases of $\mathbb{Z}_p^2$, we can write $\boldsymbol{c} = x\boldsymbol{f} + r\boldsymbol{u}$ and $\boldsymbol{d} = y\boldsymbol{g} + s\boldsymbol{v}$ for some $x, y, r, s \in \mathbb{Z}_p$. Since the proof provided by the adversary is false, it must be that $x \neq y$. Then, in the first equation, the third component on the left is $\boldsymbol{c}^\top \boldsymbol{u}^\perp = x\boldsymbol{f}^\top \boldsymbol{u}^\perp$, while the corresponding component on the right is $\boldsymbol{d}^\top \boldsymbol{v}^\perp = y\boldsymbol{g}^\top \boldsymbol{v}^\perp$. Since $\boldsymbol{f}^\top \boldsymbol{u}^\perp = \boldsymbol{g}^\top \boldsymbol{v}^\perp$ and $x \neq y$, these values are different. We conclude that we have found a nontrivial solution of the $\mathcal{RL}_2$-$\mathsf{SKerMDH}$ problem. □

Theorem 2. *The above scheme is composable zero-knowledge, with simulation trapdoor* $\tau = (\boldsymbol{k}_u, \hat{\boldsymbol{k}}_u, \boldsymbol{l}_v)$.

Proof. We switch to a game in which the commitments in $\mathbb{G}_2$ are perfectly hiding instead of perfectly binding, and prove that in this case the scheme has perfect zero-knowledge. The CRS simulator generates the CRS as in the honest execution of the protocol, and also outputs $\tau = (\boldsymbol{k}_u, \hat{\boldsymbol{k}}_u, \boldsymbol{l}_v)$ as the simulation trapdoor. The proof simulator chooses $\delta \leftarrow \mathbb{Z}_p$ and uses τ to produce:

$$[\boldsymbol{d}_{\mathsf{sim}}]_2 = \mathsf{Com}_{ck_2}(0; s) = s[\boldsymbol{v}]_2$$

$$[\pi_{\mathsf{sim}}]_1 = [\boldsymbol{c}^\top]_1 \boldsymbol{k}_u + \delta[z_1] \qquad [\theta_{\mathsf{sim}}]_2 = [\boldsymbol{d}_{\mathsf{sim}}^\top] \boldsymbol{l}_v + \delta[z_2]$$

$$[\hat{\pi}_{\mathsf{sim}}]_1 = [\boldsymbol{c}^\top]_1 \hat{\boldsymbol{k}}_u + \delta[\hat{z}_1]$$

We have that $\boldsymbol{d}_{\mathsf{sim}}$ is distributed as $\boldsymbol{d}$, as the commitment is perfectly hiding, and $\pi_{\mathsf{sim}}, \hat{\pi}_{\mathsf{sim}}, \theta_{\mathsf{sim}}$ are uniformly random elements conditioned on satisfying the verification equations for any fixed $\boldsymbol{c}, \boldsymbol{d}$, which is the same distribution that $\pi, \hat{\pi}, \theta$ have in an honest execution. □

5 Aggregated Scheme

Given $\boldsymbol{x} \in \mathbb{Z}_p^n$ and two commitments $[\boldsymbol{c}]_1, [\boldsymbol{d}]_2$ to $\boldsymbol{x}$, we provide a proof of both commitments opening to the same vector $\boldsymbol{x}$. More precisely, given a group description gk and commitment keys $ck_1 = [\mathbf{F}, \mathbf{U}]_1$, and $ck_2 = [\mathbf{G}, \mathbf{V}]_2$, where $\mathbf{F} \in \mathbb{Z}_p^{m_1 \times n}, \mathbf{G} \in \mathbb{Z}_p^{m_2 \times n}$ and $\mathbf{U} \in \mathbb{Z}_p^{m_1 \times \ell_1}, \mathbf{V} \in \mathbb{Z}_p^{m_2 \times \ell_2}$, we want to prove F-knowledge in the language

$$\mathcal{L}_{gk, ck_1} = \{[\boldsymbol{c}]_1 \in \mathbb{G}_1^{m_1} \mid \exists \boldsymbol{x}, \boldsymbol{r} \text{ s. t. } [\boldsymbol{c}]_1 = \mathsf{Com}_{ck_1}(\boldsymbol{x}; \boldsymbol{r})\},$$

where $F(\boldsymbol{x}, \boldsymbol{r}) = [\boldsymbol{x}]_{1,2}$.

- $gk := (p, \mathcal{P}_1, \mathcal{P}_2, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow \mathcal{G}(1^\lambda)$.

- $\mathsf{K}_0(gk)$: set $ck_1 = [\mathbf{F}, \mathbf{U}]_1 \leftarrow \mathcal{D}_{\mathsf{par}}$, where $\mathcal{D}_{\mathsf{par}}$ is witness sampleable, that is, there exists an efficiently sampleable distribution $\tilde{\mathcal{D}}_{\mathsf{par}}$ outputting $(\tilde{\mathbf{F}}, \tilde{\mathbf{U}})$ such that $[\tilde{\mathbf{F}}, \tilde{\mathbf{U}}]_1$ is distributed as $[\mathbf{F}, \mathbf{U}]_1$.
- $\mathsf{K}_1(gk, ck_1)$: set $ck_2 = [\mathbf{G}, \mathbf{V}]_2$, where $\mathbf{G} \leftarrow \mathbb{Z}_p^{m_2 \times n}, \mathbf{V} \leftarrow \mathbb{Z}_p^{m_2 \times \ell_2}$. Also choose $a_1, a_2 \leftarrow \mathbb{Z}_p$ and $\boldsymbol{k}_u, \hat{\boldsymbol{k}}_u \leftarrow \mathbb{Z}_p^{m_1}$. Set $\boldsymbol{l}_v, \hat{\boldsymbol{l}}_v \leftarrow \mathbb{Z}_p^{m_2}$ conditioned on

  $$\boldsymbol{l}_v^\top \mathbf{V} = \hat{\boldsymbol{l}}_v^\top \mathbf{V}, \qquad \boldsymbol{k}_u^\top \mathbf{F} = w(\boldsymbol{l}_v^\top \mathbf{G}), \qquad \hat{\boldsymbol{k}}_u^\top \mathbf{F} = \hat{w}(\hat{\boldsymbol{l}}_v^\top \mathbf{G}), \tag{7}$$

  for some $w, \hat{w} \leftarrow \mathbb{Z}_p$. Choose $z_2 \leftarrow \mathbb{Z}_p$ and set

  $$z_1 = wz_2, \qquad\qquad \hat{z}_1 = \hat{w} z_2.$$

  Algorithm K_1 outputs the following CRS:

  $$\begin{pmatrix} gk, [\mathbf{U}^\top \boldsymbol{k}_u]_1, [\mathbf{U}^\top \hat{\boldsymbol{k}}_u]_1, [a_1 w]_1, [a_2 \hat{w}]_1, [a_1 w \boldsymbol{l}_v]_1, [a_2 \hat{w} \hat{\boldsymbol{l}}_v]_1, [z_1]_1, [\hat{z}_1]_1, \\ [\mathbf{V}^\top \boldsymbol{l}_v]_2, [a_1]_2, [a_2]_2, [a_1 \boldsymbol{k}_u]_2, [a_2 \hat{\boldsymbol{k}}_u]_2, [z_2]_2 \end{pmatrix}.$$

- $\mathsf{P}(\mathrm{CRS}, ([\boldsymbol{c}]_1, (\boldsymbol{x}, \boldsymbol{r})) \in \mathcal{R})$: commit to $\boldsymbol{x}$ in $\mathbb{G}_2$ as $[\boldsymbol{d}]_2$. Choose $\delta \leftarrow \mathbb{Z}_p$ and output $[\boldsymbol{d}]_2$ and

  $$\begin{aligned} [\pi]_1 &= [\boldsymbol{r}^\top \mathbf{U}^\top \boldsymbol{k}_u + \delta z_1]_1, & [\theta]_2 &= [\boldsymbol{s}^\top \mathbf{V}^\top \boldsymbol{l}_v + \delta z_2]_2, \\ [\hat{\pi}]_1 &= [\boldsymbol{r}^\top \hat{\mathbf{U}}^\top \boldsymbol{k}_u + \delta \hat{z}_1]_1, \end{aligned}$$

- $\mathsf{V}(\mathrm{CRS}, [\boldsymbol{c}]_1, ([\boldsymbol{d}, \theta]_2, [\pi, , \hat{\pi}]_1))$: The algorithm outputs 1 iff the following equations hold:

  $$\begin{aligned} e\left([\boldsymbol{c}^\top]_1, [a_1 \boldsymbol{k}_u]_2\right) - e([a_1 w \boldsymbol{l}_v^\top]_1, [\boldsymbol{d}]_2) &\overset{?}{=} e([\pi]_1, [a_1]_2) - e([a_1 w]_1, [\theta]_2), \\ e\left([\boldsymbol{c}^\top]_1, [a_2 \hat{\boldsymbol{k}}_u]_2\right) - e([a_2 \hat{w} \hat{\boldsymbol{l}}_v^\top]_1, [\boldsymbol{d}]_2) &\overset{?}{=} e([\hat{\pi}]_1, [a_2]_2) - e([a_2 \hat{w}]_1, [\theta]_2). \end{aligned}$$

Completeness. It is easy to check that, if the prover is honest,

$$\begin{aligned} \boldsymbol{c}^\top (a_1 \boldsymbol{k}_u) - (a_1 w \boldsymbol{l}_v^\top) \boldsymbol{d} &= (\boldsymbol{x}^\top \mathbf{F}^\top + \boldsymbol{r}^\top \mathbf{U}^\top)(a_1 \boldsymbol{k}_u) - (a_1 w \boldsymbol{l}_v^\top)(\mathbf{G}\boldsymbol{x} + \mathbf{V}\boldsymbol{s}) = \\ &= a_1 \boldsymbol{x}^\top \mathbf{F}^\top \boldsymbol{k}_u - a_1 (w \boldsymbol{l}_v^\top \mathbf{G}) \boldsymbol{x} + a_1 \boldsymbol{r}^\top \mathbf{U}^\top \boldsymbol{k}_u - a_1 w \boldsymbol{l}_v^\top \mathbf{V} \boldsymbol{s} = \pi a_1 - a_1 w \theta. \end{aligned}$$

We have used that $\boldsymbol{k}_u^\top \mathbf{F} = w(\boldsymbol{l}_v^\top \mathbf{G})$. The second equation is completely analogous.

Note on dimensions. For this scheme to work and be secure, we require some relations between the dimensions of the different elements involved.

(1) We want our commitments to be perfectly binding to be able to open the commitments in the source groups, so we require that $m_i \geq n + \ell_i$, for $i = 1, 2$.

(2) To be able to find $\boldsymbol{l}_v, \hat{\boldsymbol{l}}_v$ verifying the equations (7), we need to solve the linear system

$$\begin{pmatrix} \mathbf{G}^\top & \mathbf{0} \\ \mathbf{0} & \mathbf{G}^\top \\ \mathbf{V}^\top & -\mathbf{V} \end{pmatrix} \begin{pmatrix} \boldsymbol{l}_v \\ \hat{\boldsymbol{l}}_v \end{pmatrix} = \begin{pmatrix} \mathbf{F}^\top \boldsymbol{k}_u \\ \mathbf{F}^\top \hat{\boldsymbol{k}}_u \\ \mathbf{0} \end{pmatrix}.$$

Since $\mathbf{F}$ is only known in $\mathbb{G}_1$, the system cannot be fully solved over $\mathbb{Z}_p$. However, we do not need the full solution over $\mathbb{Z}_p$, as only the projection $\mathbf{V}^\top \boldsymbol{l}_v$ needs to be given in $\mathbb{G}_2$, while the full $\boldsymbol{l}_v$ is necessary in $\mathbb{G}_1$. Thus we proceed as follows: we start by sampling $\boldsymbol{t} \leftarrow \mathbb{Z}_p^{\ell_2}$ and setting $\mathbf{V}^\top \boldsymbol{l}_v = \mathbf{V}^\top \hat{\boldsymbol{l}}_v = \boldsymbol{t}$. Then we consider the system

$$\begin{pmatrix} \mathbf{G}^\top & \mathbf{0} \\ \mathbf{0} & \mathbf{G}^\top \\ \mathbf{V}^\top & \mathbf{0} \\ \mathbf{0} & \mathbf{V} \end{pmatrix} \begin{pmatrix} \boldsymbol{l}_v \\ \hat{\boldsymbol{l}}_v \end{pmatrix} = \begin{pmatrix} \mathbf{F}^\top \boldsymbol{k}_u \\ \mathbf{F}^\top \hat{\boldsymbol{k}}_u \\ \boldsymbol{t} \\ \boldsymbol{t} \end{pmatrix}.$$

The matrix is known over $\mathbb{Z}_p$ and the right hand side is known over $\mathbb{G}_1$ (since $\mathbf{F}$ is known over $\mathbb{G}_1$ and the rest is known over $\mathbb{Z}_p$), so the system can be solved over $\mathbb{G}_1$ using Gaussian elimination. The system has solutions if $2m_2 \geq 2n + 2\ell_2$, which is implied by condition (1) above.

(3) In the proof of the zero-knowledge property, we want to be able to switch the commitment in $\mathbb{G}_2$ to perfectly hiding, so we need to ensure that it has enough randomness. Thus $\ell_2 \geq n$.

(4) Consider the matrices $(\mathbf{F}||\mathbf{U})$ and $(\mathbf{G}||\mathbf{V})$. These are of size $m_i \times (n + \ell_i)$, for $i = 1, 2$, respectively. In the soundness reduction we will be interested in finding nonzero vectors $\boldsymbol{u}^\perp, \boldsymbol{v}^\perp$ such that $\boldsymbol{w}^\top \boldsymbol{u}^\perp = 0$ for any vector $\boldsymbol{w}$ outside of the span of the columns of $\mathbf{F}$, and the same for $\boldsymbol{v}^\perp$ and $\mathbf{G}$. Additionally, we will require that

$$\mathbf{F}^\top \boldsymbol{u}^\perp = \mathbf{G}^\top \boldsymbol{v}^\perp.$$

As we have already established that $m_i \geq n + \ell_i$, we might need to add more columns to the matrices $(\mathbf{F}||\mathbf{U})$ and $(\mathbf{G}||\mathbf{V})$ so that they form bases of $\mathbb{Z}_p^{m_i}$, so let $\overline{\mathbf{U}}, \overline{\mathbf{V}} \in \mathbb{Z}_p^{m_i \times (m_i - n)}$ be the augmented matrices such that $(\mathbf{F}||\overline{\mathbf{U}})$ and $(\mathbf{G}||\overline{\mathbf{V}})$ are bases of $\mathbb{Z}_p^{m_i}$ for $i = 1, 2$, respectively. Then the vectors $\boldsymbol{u}^\perp, \boldsymbol{v}^\perp$ are given by the nontrivial solutions of the linear system

$$\begin{pmatrix} \overline{\mathbf{U}}^\top & \mathbf{0} \\ \mathbf{0} & \overline{\mathbf{V}}^\top \\ \mathbf{F}^\top & -\mathbf{G}^\top \end{pmatrix} \begin{pmatrix} \boldsymbol{u}^\perp \\ \boldsymbol{v}^\perp \end{pmatrix} = \mathbf{0}.$$

This matrix is of size $(m_1 + m_2 - n) \times (m_1 + m_2)$, and therefore it has nontrivial solutions.

F-extractor. We now define the algorithm that, given the extraction key $xk = (\mathbf{F}, \mathbf{G}, \mathbf{U}, \mathbf{V})$, outputs a function of the witness, in this case $F(\boldsymbol{x}, \boldsymbol{r}) = [\boldsymbol{x}]_{1,2}$.

- $\mathsf{Ext}_{xk}([\boldsymbol{c}]_1, [\boldsymbol{d}]_2)$: as above, consider $\overline{\mathbf{U}}, \overline{\mathbf{V}}$ so that $(\mathbf{F}||\overline{\mathbf{U}})$ and $(\mathbf{G}||\overline{\mathbf{V}})$ are bases of $\mathbb{Z}_p^{m_i}$ for $i = 1, 2$, respectively. Knowing $\mathbf{F}, \overline{\mathbf{U}}$, we can find a matrix $\mathbf{U}^\perp \in \mathbb{Z}_p^{m_1 \times n}$ such that $\overline{\mathbf{U}}^\top \mathbf{U}^\perp = \mathbf{0}$ and $\mathbf{F}^\top \mathbf{U}^\perp = \mathbf{I}$, and compute $[\boldsymbol{c}^\top]_1 \mathbf{U}^\perp = [\boldsymbol{x}]_1$. Similarly, we obtain $[\boldsymbol{x}]_2$ from $[\boldsymbol{d}]_2$, using $\mathbf{G}, \overline{\mathbf{V}}$.

Theorem 3. *The above proof system is computationally F-knowledge sound under the $\mathcal{RL}_2$-$\mathsf{SKerMDH}$ assumption. More precisely, there exists an adversary $\mathcal{B}$ against the $\mathcal{RL}_2$-$\mathsf{SKerMDH}$ problem such that for any PPT adversary $\mathcal{A}$, we have that*

$$\mathsf{Adv}_{F-\mathsf{KnowledgeSoundness}}(\mathcal{A}) \leq \mathsf{Adv}_{\mathcal{RL}_2\text{-}\mathsf{SKerMDH}}(\mathcal{B})$$

Proof. Assume that there is an adversary $\mathcal{A}$ against the soundness of the scheme ($\mathcal{A}$ is able to produce a statement and and an accepting proof such that $\mathsf{Ext}_{xk}([\boldsymbol{c}]_1, [\boldsymbol{d}]_2) = ([\boldsymbol{x}]_1, [\boldsymbol{y}]_2)$ and $\boldsymbol{x} \neq \boldsymbol{y}$). We use it to build an adversary $\mathcal{B}$ against the $\mathcal{RL}_2$-$\mathsf{SKerMDH}$ problem. $\mathcal{B}$ receives the challenge matrix

$$[\mathbf{A}]_{1,2} = [\boldsymbol{a}_1||\boldsymbol{a}_2]_{1,2} = \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \\ r_1 & r_2 \end{bmatrix}_{1,2},$$

and builds the environment for $\mathcal{A}$ as follows. We sample $\mathbf{G} \leftarrow \mathbb{Z}_p^{m_2 \times n}, \mathbf{V} \leftarrow \mathbb{Z}_p^{m_2 \times \ell_2}$, and let $\overline{\mathbf{V}}$ be as in (4) above. We choose $w, \hat{w} \leftarrow \mathbb{Z}_p$ and $\boldsymbol{l}'_v \leftarrow \mathbb{Z}_p^{m_2}$ Let $\boldsymbol{v}^\perp \in \mathbb{Z}_p^{m_2}$ such that $\overline{\mathbf{V}}^\top \boldsymbol{v}^\perp = 0$. Implicitly set

$$\boldsymbol{l}_v = \boldsymbol{l}'_v + (a_1 w)^{-1} r_1 \boldsymbol{v}^\perp, \qquad \hat{\boldsymbol{l}}_v = \boldsymbol{l}'_v + (a_2 \hat{w})^{-1} r_2 \boldsymbol{v}^\perp.$$

Observe that this implies that

$$a_1 w \boldsymbol{l}_v = a_1 w \boldsymbol{l}'_v + r_1 \boldsymbol{v}^\perp, \qquad a_2 \hat{w} \hat{\boldsymbol{l}}_v = a_2 \hat{w} \boldsymbol{l}'_v + r_2 \boldsymbol{v}^\perp, \tag{8}$$

which we can compute over $\mathbb{G}_1$. For the other side, we sample $(\mathbf{F}, \mathbf{U}) \leftarrow \tilde{\mathcal{D}}_{\mathsf{par}}$ and define $\overline{\mathbf{U}}$ as in (4) above. We also sample $\boldsymbol{k}'_u, \hat{\boldsymbol{k}}'_u \leftarrow \mathbb{Z}_p^{m_1}$ conditioned on

$$\boldsymbol{k}'^\top_u \mathbf{F} = w(\boldsymbol{l}'^\top_v \mathbf{G}), \qquad \hat{\boldsymbol{k}}'^\top_u \mathbf{F} = \hat{w}(\hat{\boldsymbol{l}}'^\top_v \mathbf{G}). \tag{9}$$

Let $\boldsymbol{u}^\perp \in \mathbb{Z}_p^{m_1}$ such that $\overline{\mathbf{U}}^\top \boldsymbol{u}^\perp = 0$ and

$$\mathbf{F}^\top \boldsymbol{u}^\perp = \mathbf{G}^\top \boldsymbol{v}^\perp. \tag{10}$$

We implicitly define

$$\boldsymbol{k}_u = \boldsymbol{k}'_u + a_1^{-1} r_1 \boldsymbol{u}^\perp, \qquad \hat{\boldsymbol{k}}_u = \hat{\boldsymbol{k}}'_u + a_2^{-1} r_2 \boldsymbol{u}^\perp.$$

which means that

$$a_1 \boldsymbol{k}_u = a_1 \boldsymbol{k}'_u + r_1 \boldsymbol{u}^\perp, \qquad a_2 \hat{\boldsymbol{k}}_u = a_2 \hat{\boldsymbol{k}}'_u + r_2 \boldsymbol{u}^\perp. \tag{11}$$

Note that, by construction,

$$a_1 w \mathbf{G}^\top \boldsymbol{l}_v = a_1 w \mathbf{G}^\top \boldsymbol{l}'_v + r_1 \mathbf{G}^\top \boldsymbol{v}^\perp = a_1 \mathbf{F}^\top \boldsymbol{k}'_u + r_1 \mathbf{F}^\top \boldsymbol{u}^\perp = a_1 \mathbf{F}^\top \boldsymbol{k}_u$$

where we have used equalities (9) and (10), and therefore $\mathbf{F}^\top \boldsymbol{k}_u = w(\mathbf{G}^\top \boldsymbol{l}_v)$ A similar argument shows that $\mathbf{F}^\top \hat{\boldsymbol{k}}_u = \hat{w}(\mathbf{G}^\top \hat{\boldsymbol{l}}_v)$. We can also compute

$$[\boldsymbol{k}_u^\top \mathbf{U}]_1 = [\boldsymbol{k}_u'^\top \mathbf{U}]_1, \qquad [\hat{\boldsymbol{k}}_u^\top \mathbf{U}]_1 = [\hat{\boldsymbol{k}}_u'^\top \mathbf{U}]_1, \qquad [\boldsymbol{l}_v^\top \mathbf{V}]_2 = [\boldsymbol{l}_v'^\top \mathbf{V}]_2 = [\hat{\boldsymbol{l}}_v^\top \mathbf{V}]_2.$$

Finally, choose $z_2 \leftarrow \mathbb{Z}_p$ and set

$$z_1 = w z_2, \qquad \hat{z}_1 = \hat{w} z_2,$$

completing the CRS. The CRS is then sent to adversary $\mathcal{A}$, who outputs a statement $[\boldsymbol{c}]_1, [\boldsymbol{d}]_2$ and a proof $[\pi]_1, [\hat{\pi}]_1, [\theta]_2$ such that

$$\begin{aligned} \boldsymbol{c}^\top (a_1 \boldsymbol{k}_u) - (a_1 w \boldsymbol{l}_v^\top) \boldsymbol{d} &= \pi a_1 - (a_1 w)\theta, \\ \boldsymbol{c}^\top (a_2 \hat{\boldsymbol{k}}_u) - (a_2 \hat{w} \hat{\boldsymbol{l}}_v^\top) \boldsymbol{d} &= \hat{\pi} a_2 - (a_2 \hat{w})\theta. \end{aligned}$$

Notice that, using equalities (11) and (8), we can rewrite these expressions in terms of the columns of $\mathbf{A}$. Indeed, these are equivalent to

$$\begin{aligned} \boldsymbol{c}^\top (\boldsymbol{k}'_u || \hat{\boldsymbol{k}}'_u || \boldsymbol{u}^\perp) \boldsymbol{a}_1 - \boldsymbol{d}^\top (w \boldsymbol{l}'_v || \hat{w} \boldsymbol{l}'_v || \boldsymbol{v}^\perp) \boldsymbol{a}_1 &= (\pi, \hat{\pi}, 0) \boldsymbol{a}_1 - (w\theta, \hat{w}\theta, 0) \boldsymbol{a}_1, \\ \boldsymbol{c}^\top (\boldsymbol{k}'_u || \hat{\boldsymbol{k}}'_u || \boldsymbol{u}^\perp) \boldsymbol{a}_2 - \boldsymbol{d}^\top (w \boldsymbol{l}'_v || \hat{w} \boldsymbol{l}'_v || \boldsymbol{v}^\perp) \boldsymbol{a}_2 &= (\pi, \hat{\pi}, 0) \boldsymbol{a}_2 - (w\theta, \hat{w}\theta, 0) \boldsymbol{a}_2, \end{aligned}$$

We rearrange this as a solution of the $\mathcal{RL}_2$-$\mathsf{SKerMDH}$ problem that the reduction can compute:

$$e([(\boldsymbol{c}^\top \boldsymbol{k}'_u - \pi || \boldsymbol{c}^\top \hat{\boldsymbol{k}}'_u - \hat{\pi} || \boldsymbol{c}^\top \boldsymbol{u}^\perp)]_1, [\mathbf{A}]_2) = e([(w(\boldsymbol{d}^\top \boldsymbol{l}'_v - \theta) || \hat{w}(\boldsymbol{d}^\top \boldsymbol{l}'_v - \theta) || \boldsymbol{d}^\top \boldsymbol{v}^\perp)]_2, [\mathbf{A}]_1).$$

It remains to argue that this is not the trivial solution. To do so, we look at the third component. As the columns of $(\mathbf{F}||\overline{\mathbf{U}})$ and $(\mathbf{G}||\overline{\mathbf{V}})$ are bases of $\mathbb{Z}_p^{m_i}$ for $i = 1, 2$, respectively, we can write $\boldsymbol{c} = \mathbf{F}\boldsymbol{x} + \overline{\mathbf{U}}\boldsymbol{r}$ and $\boldsymbol{d} = \mathbf{G}\boldsymbol{y} + \overline{\mathbf{V}}\boldsymbol{s}$ for some $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}_p^n, \boldsymbol{r}, \boldsymbol{s} \in \mathbb{Z}_p^\ell$. Since the proof provided by the adversary is false, it must be that $\boldsymbol{x} \neq \boldsymbol{y}$. Then, in the first equation, the third component on the left is $\boldsymbol{c}^\top \boldsymbol{u}^\perp = \boldsymbol{x}^\top \mathbf{F}^\top \boldsymbol{u}^\perp$, while the corresponding component on the right is $\boldsymbol{d}^\top \boldsymbol{v}^\perp = \boldsymbol{y}^\top \mathbf{G}^\top \boldsymbol{v}^\perp$. Since $\mathbf{F}^\top \boldsymbol{u}^\perp = \mathbf{G}^\top \boldsymbol{v}^\perp$ and $\boldsymbol{x} \neq \boldsymbol{y}$, these values are different. We conclude that we have found a nontrivial solution of the $\mathcal{RL}_2$-$\mathsf{SKerMDH}$ problem. □

Theorem 4. *The above proof system is composable zero-knowledge, with simulation trapdoor* $\tau = (\boldsymbol{k}_u, \hat{\boldsymbol{k}}_u, \boldsymbol{l}_v)$.

The proof is completely analogous to the proof of Theorem 2.

6 Optimality of our Constructions

We argue that our constructions are optimal in terms of proof size, at least based on this general strategy of commit-and-prove schemes, and where the prover is limited to linear algebraic operations on the group elements, and verification is a pairing equation. To the best of our knowledge, this is the approach that is always taken in the literature. We prove optimality by arguing that any such proof formed of two elements (plus the commitments) is vulnerable to an attack.

We now consider any proof in which we have two commitments $[\boldsymbol{c}]_1$ and $[\boldsymbol{d}]_2$ to the values x and y, respectively, and we have a a two-element proof $[\pi]_1, [\theta]_2$ of same opening, that is, $x = y$. We consider a CRS formed of elements in $\mathbb{G}_1$ and $\mathbb{G}_2$, and we assume that each side of the CRS is closed under linear combination. We can do this without loss of generality, since given the CRS it is easy to compute linear combinations of its elements.

Then the general verification equation of such a proof looks like this:

$$e([\boldsymbol{c}^\top]_1, [\boldsymbol{k}_1]_2) + e([\boldsymbol{k}_2^\top]_1, [\boldsymbol{d}]_2) + e([\pi]_1, [k_3]_2) + e([k_4]_1, [\theta]_2) = [0]_T, \qquad (12)$$

where $[\boldsymbol{k}_1, k_3]_2, [\boldsymbol{k}_2, k_4]_1$ are elements (some of them vectors of elements) of the CRS. We note two omissions from this general equation: there is no affine term and there are no “quadratic” terms, i.e., terms in $\boldsymbol{c}^\top \boldsymbol{d}, \pi \boldsymbol{d}, \boldsymbol{c}\theta$ or $\pi\theta$. This is because the linear terms (those in equation (12)) force π and θ to be linear in the witness, and so the terms above are quadratic. The quadratic condition causes the appearance of terms with coefficient xy, which must cancelled out with other quadratic terms of the same coefficient. We note that, unlike in the linear part, this check does not make a distinction when $x = y$ or $x \neq y$, so we conclude that these quadratic terms do not contribute to achieving soundness. The intuition behind this is that we are proving membership in a linear space, and non-linear operations take us out of the space.

This leaves us with the equation (12) above. We now observe a very simple attack on any scheme with a verification equation like this. We set

$$\begin{aligned} [\boldsymbol{c}]_1 &= \boldsymbol{\alpha}[k_4]_1, & [\boldsymbol{d}]_2 &= \boldsymbol{\beta}[k_3]_2, \\ [\pi]_1 &= -\boldsymbol{\beta}^\top[\boldsymbol{k}_2]_1, & [\theta]_2 &= -\boldsymbol{\alpha}^\top[\boldsymbol{k}_1]_2, \end{aligned}$$

where $\boldsymbol{\alpha}, \boldsymbol{\beta} \leftarrow \mathbb{Z}_p^2$. It is trivial to verify that the first term in the equation cancels out with the fourth and the second with the third, and with overwhelming probability the openings of $[\boldsymbol{c}]_1$ and $[\boldsymbol{d}]_2$ do not match. Intuitively, this attack works because of the two-sided nature of the proof: the elements that are given in the CRS to ensure verifiability in one side are used to fool the other. Indeed, in an honest execution the first term is expected to cancel out with the third, and the second with the fourth, while in this attack the pairs are jumbled.

One could also consider one-sided two-element proofs, i.e., of the form $[\pi_1, \pi_2]_1$ or $[\theta_1, \theta_2]_2$, but these can be handled in a very similar way. For example, in the first case, the general verification equation would be

$$e([\boldsymbol{c}^\top]_1, [\boldsymbol{k}_1]_2) + e([\boldsymbol{k}_2^\top]_1, [\boldsymbol{d}]_2) + e([\pi_1]_1, [k_3]_2) + e([\pi_2]_1, [k_4]_2) = [0]_T, \qquad (13)$$

and the attack would consist of setting

$$\begin{aligned} [\boldsymbol{c}]_1 &= \alpha[\boldsymbol{k}_2]_1, & [\boldsymbol{d}]_2 &= \boldsymbol{\beta}(r[k_3]_2 + s[k_4]_2) - \alpha[\boldsymbol{k}_1]_2, \\ [\pi_1]_1 &= -r\boldsymbol{\beta}^\top[\boldsymbol{k}_2]_1, & [\pi_2]_1 &= -s\boldsymbol{\beta}^\top[\boldsymbol{k}_2]_1, \end{aligned}$$

for $\boldsymbol{\beta} \leftarrow \mathbb{Z}_p^2, \alpha, r, s \leftarrow \mathbb{Z}_p$. Thus we conclude that, with this approach, there is no possible proof of same opening of commitments in different groups which consists of less than three group elements, making our constructions optimal.

Acknowledgements. The second author was supported by a PhD grant from the Spanish government, co-financed by the ESF (Ayudas para contratos predoctorales para la formación de doctores 2016).

References

1. M. Abe, M. Ambrona, M. Ohkubo, and M. Tibouchi. Lower bounds on structure-preserving signatures for bilateral messages. In D. Catalano and R. De Prisco, editors, *SCN 18*, volume 11035 of *LNCS*, pages 3–22, Amalfi, Italy, Sept. 5–7, 2018. Springer. 2
2. M. Abe, C. S. Jutla, M. Ohkubo, and A. Roy. Improved (almost) tightly-secure simulation-sound QA-NIZK with applications. In T. Peyrin and S. Galbraith, editors, *ASIACRYPT 2018, Part I*, volume 11272 of *LNCS*, pages 627–656, Brisbane, Queensland, Australia, Dec. 2–6, 2018. Springer. 2
3. M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya. Compact e-cash and simulatable VRFs revisited. In *International Conference on Pairing-Based Cryptography*, pages 114–131. Springer, 2009. 1
4. D. Bernhard, G. Fuchsbauer, and E. Ghadafi. Efficient signatures of knowledge and DAA in the standard model. In M. J. Jacobson Jr., M. E. Locasto, P. Mohassel, and R. Safavi-Naini, editors, *ACNS 13*, volume 7954 of *LNCS*, pages 518–533, Banff, AB, Canada, June 25–28, 2013. Springer. 1
5. X. Boyen and B. Waters. Full-domain subgroup hiding and constant-size group signatures. In *International Workshop on Public Key Cryptography*, pages 1–15. Springer, 2007. 1
6. J. Camenisch, R. Chaabouni, and a. shelat. Efficient protocols for set membership and range proofs. In J. Pieprzyk, editor, *ASIACRYPT 2008*, volume 5350 of *LNCS*, pages 234–252, Melbourne, Australia, Dec. 7–11, 2008. Springer. 2
7. P. Chaidos, V. Cortier, G. Fuchsbauer, and D. Galindo. BeleniosRF: A non-interactive receipt-free electronic voting scheme. In E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi, editors, *ACM CCS 2016*, pages 1614–1625, Vienna, Austria, Oct. 24–28, 2016. ACM Press. 2
8. N. Chandran, J. Groth, and A. Sahai. Ring signatures of sub-linear size without random oracles. In *International Colloquium on Automata, Languages, and Programming*, pages 423–434. Springer, 2007. 1, 2
9. G. Couteau and D. Hartmann. Shorter non-interactive zero-knowledge arguments and zaps for algebraic languages. 3
10. A. Escala and J. Groth. Fine-tuning Groth-Sahai proofs. In H. Krawczyk, editor, *PKC 2014*, volume 8383 of *LNCS*, pages 630–649, Buenos Aires, Argentina, Mar. 26–28, 2014. Springer. 1, 2, 7

11. A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar. An algebraic framework for Diffie-Hellman assumptions. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147, Santa Barbara, CA, USA, Aug. 18–22, 2013. Springer. 8, 9
12. A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. L. Villar. An algebraic framework for Diffie-Hellman assumptions. *Journal of Cryptology*, 30(1):242–288, Jan. 2017. 2
13. G. Fuchsbauer. Commuting signatures and verifiable encryption. In K. G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 224–245, Tallinn, Estonia, May 15–19, 2011. Springer. 1
14. E. M. Ghadafi. Sub-linear blind ring signatures without random oracles. In *IMA International Conference on Cryptography and Coding*, pages 304–323. Springer, 2013. 2
15. A. González. Shorter ring signatures from standard assumptions. In *IACR International Workshop on Public Key Cryptography*, pages 99–126. Springer, 2019. 2
16. A. González, A. Hevia, and C. Ràfols. QA-NIZK arguments in asymmetric groups: New tools and new constructions. In T. Iwata and J. H. Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 605–629, Auckland, New Zealand, Nov. 30 – Dec. 3, 2015. Springer. 2, 3, 4, 5, 8, 9
17. 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. 1, 7
18. J. Groth and S. Lu. A non-interactive shuffle with pairing based verifiability. In K. Kurosawa, editor, *ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 51–67, Kuching, Malaysia, Dec. 2–6, 2007. Springer. 1
19. 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. 1
20. J. Groth, R. Ostrovsky, and A. Sahai. Perfect non-interactive zero knowledge for NP. In S. Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 339–358, St. Petersburg, Russia, May 28 – June 1, 2006. Springer. 1
21. 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. 1
22. D. Hofheinz and T. Jager. Tightly secure signatures and public-key encryption. *Designs, Codes and Cryptography*, 80(1):29–61, 2016. 1
23. C. S. Jutla and A. Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In K. Sako and P. Sarkar, editors, *ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 1–20, Bengalore, India, Dec. 1–5, 2013. Springer. 2, 6
24. 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. 2
25. E. Kiltz, J. Pan, and H. Wee. Structure-preserving signatures from standard assumptions, revisited. In R. Gennaro and M. J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 275–295, Santa Barbara, CA, USA, Aug. 16–20, 2015. Springer. 2
26. 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. 2, 4

27. B. Libert, T. Peters, M. Joye, and M. Yung. Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures. In P. Q. Nguyen and E. Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 514–532, Copenhagen, Denmark, May 11–15, 2014. Springer. 2
28. B. Libert, T. Peters, and M. Yung. Short group signatures via structure-preserving signatures: Standard model security from simple assumptions. In R. Gennaro and M. J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 296–316, Santa Barbara, CA, USA, Aug. 16–20, 2015. Springer. 2
29. P. Morillo, C. Ràfols, and J. L. Villar. The kernel matrix Diffie-Hellman assumption. In J. H. Cheon and T. Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 729–758, Hanoi, Vietnam, Dec. 4–8, 2016. Springer. 2, 3, 8
30. 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. 2