Somewhere Statistically Binding Commitment Schemes with Applications

Prastudy Fauzi[1], Helger Lipmaa[1,2], Zaira Pindado[3], and Janno Siim[2]

[1] Simula UiB, Bergen, Norway
[2] University of Tartu, Tartu, Estonia
[3] Universitat Pompeu Fabra, Barcelona, Spain

Abstract. We define a new primitive that we call a *somewhere statistically binding* (SSB) commitment scheme, which is a generalization of dual-mode commitments but has similarities with SSB hash functions (Hubacek and Wichs, ITCS 2015) without local opening. In (existing) SSB hash functions, one can compute a hash of a vector v that is statistically binding in one coordinate of v. Meanwhile, in SSB commitment schemes, a commitment of a vector v is statistically binding in some coordinates of v and is statistically hiding in the other coordinates. The set of indices where binding holds is predetermined but known only to the commitment key generator. We show that the primitive can be instantiated by generalizing the succinct Extended Multi-Pedersen commitment scheme (González et al., Asiacrypt 2015). We further introduce the notion of functional SSB commitment schemes and, importantly, use it to get an efficient quasi-adaptive NIZK for arithmetic circuits and efficient oblivious database queries.

Keywords: Oblivious transfer, QA-NIZK, SSB commitment scheme

1 Introduction

By relying on non-falsifiable assumptions, it is known how to construct very efficient zero-knowledge succinct arguments of knowledge (zk-SNARKs) for all NP-languages [Gro10, Lip12, GGPR13, Gro16]. Recently, zk-SNARKs have become extremely popular due to applications in verifiable computation and cryptocurrencies. Unfortunately, their reliance on non-falsifiable assumptions is inevitable due to Gentry and Wichs' impossibility result [GW11]. In the soundness proof of most known zk-SNARKs (e.g., [Gro10, Lip12, GGPR13, DFGK14, Lip19]), one uses a non-falsifiable knowledge assumption to efficiently recover the whole witness $\mathtt{w}$ of the prover P, and based on that establishes where exactly P cheated; based on the knowledge of $\mathtt{w}$ one then breaks a computational assumption.

On the other hand, quasi-adaptive NIZKs (QA-NIZKs, [JR13]) are based on falsifiable assumptions and result in very efficient, succinct, arguments for a limited class of subspace languages, [LPJY14, JR14, KW15, LPJY15]. González *et al.* [GHR15, GR16, DGP$^+$19] introduced an interesting technique to construct argument-succinct QA-NIZK arguments (i.e., QA-NIZK arguments that have a long commitment but otherwise are succinct) for a larger class of languages, including NP-complete problems [DGP+19]. They essentially extract only the minimal amount of information, needed to establish that the malicious prover cheated (e.g., by showing that one concrete gate in the circuit was wrongly computed), and then use this information to break a computational assumption. Importantly, their QA-NIZK argument is based on falsifiable assumptions.

For the simplicity of exposition, consider the succinct pairing-based QA-NIZK argument from González *et al.* [GHR15] that a committed string is a bit-string. It implicitly uses a succinct commitment scheme (named *Extended Multi-Pedersen* (EMP) in [GR16]) that enables one to make *at most one* coordinate of the committed n-dimensional vector statistically binding (SB), while other coordinates stay statistically hiding (SH). Since Booleanity is a quadratic relation, $b_i \in \{0, 1\}$ iff $b_i(b_i - 1) = 0$, one commits to the bit-string twice in different pairing groups so that the quadratic relation can be verified using asymmetric pairings. In [GHR15], a commitment C is given by using an SB commitment scheme and another succinct commitment D given by using EMP. One can unequivocally extract the whole witness from C while one can extract only a succinct guilt witness (a single non-bit coefficient) from D; the latter will be however sufficient. Then, [GHR15] gives (1) a QA-NIZK subspace argument to show that both commitments are to the same vector, and (2) a succinct QA-NIZK argument for quadratic relations that only uses the succinct EMP commitment. Both QA-NIZK arguments are succinct.

González *et al.* [GHR15] used the following reduction of the soundness to falsifiable assumptions. Let $\mathcal{A}$ be an adversary that succeeds in breaking the bit-string argument by constructing the following adversary $\mathcal{B}$. $\mathcal{B}$ picks a random coordinate i and extracts (an exponentiation of) the coefficient x_i of the committed vector $\boldsymbol{x}$ from C. If the coefficient is Boolean, then $\mathcal{B}$ aborts; otherwise, with probability $\geq 1/n$, $\mathcal{B}$ has extracted a succinct guilt witness showing that $\mathcal{A}$ cheated. One then defines a new game, where the commitment key of EMP is changed so that the chosen coordinate is also SB in the EMP commitment. Assuming that distinguishing two commitment keys is hard (we will call this the *index-set hiding* (ISH) assumption), $\mathcal{A}$ will also succeed in the new game.

In the new game, the *succinct* commitment D, which is SB in one coordinate, witnesses the fact that $\mathcal{A}$ successfully cheated. One uses D as a succinct guilt witness that $\mathcal{A}$ has broken an underlying falsifiable assumption (e.g., KerMDH [MRV16]). Since D is succinct, the resulting QA-NIZK argument is argument-succinct, and thus one obtains an argument-succinct non-interactive zero-knowledge argument under a falsifiable assumption (note that this does not contradict [GW11]). One additional cost of this approach is the n-times security loss in the reduction.

The described construction is very interesting but does not formalize the properties needed from the EMP commitment scheme. Using terminology introduced in the current paper, in the above construction, we need a succinct *somewhere statistically binding* (SSB) property that guarantees that the chosen coordinate is SB while the remaining coordinates can be computationally binding (CB). On the other hand, to get zero-knowledge, the commitment needs to be *almost-everywhere statistically hiding* (AESH), that is, computationally hiding (CH) at the chosen coordinate, and statistically hiding at any other coordinates. We also need *index-set hiding* (ISH), which means the attacker does not know which particular coordinate is SB.

Quadratic Equations and CIRCUIT-SAT. The same technique is used in the context of CIRCUIT-SAT, e.g., in Daza *et al.* [DGP+19] (and later improved by González and Ràfols [GR19]) where instead of proving quadratic equations corresponding to $b_i \in \{0, 1\}$, the proof is for quadratic equations in $\mathbb{Z}_p$. They use a long ElGamal commitment to all n wire values of the circuit that in the soundness setting is PB in all n coordinates. Again, they randomly pick one of the gates to guess which equation does not hold and use the properties of ElGamal encryption to extract (exponentiations of) all the wire values to check if the guessed equation holds, otherwise abort. Moreover, in this construction, there is another commitment of the witness that is similar to SSB commitment. The size of the latter commitment is $q + 1$, where q is the number of elements they need to extract in the security proof. The q extracted elements are linear functions evaluated on the witness and they are used to break an underlying assumption. We later show in Corollary 1 that algebraic commitments of size $q+1$ are optimal to extract q functions. The Daza *et al.* technique, in this sense, uses a functional variant of the EMP commitment.

Our Contributions. Formalizing the properties of EMP [GHR15, GR16], we define a *somewhere statistically binding (SSB) commitment scheme* to n-dimensional vectors. In the commitment key generation phase of an SSB commitment scheme one chooses an index-set $\mathcal{S} \subseteq [1 \mathinner{..} n]$ of size at most $q \leq n$ and defines a commitment key ck that depends on n, q and $\mathcal{S}$. A commitment to an n-dimensional vector $\boldsymbol{x}$ will be statistically binding and extractable at coordinates indexed by $\mathcal{S}$ and perfectly hiding and trapdoor at all other coordinates. Moreover, commitment keys corresponding to any two index-sets $\mathcal{S}_1$ and $\mathcal{S}_2$ of size at most q must be computationally indistinguishable. Thus, an *SSB commitment scheme* is required to be SSB, *somewhere statistically extractable* (SSE), *almost everywhere statistically hiding* (AESH), *almost everywhere statistical trapdoor* (AEST), and *index-set hiding* (ISH). An SSB commitment scheme generalizes dual-mode commitment schemes [DN02, CV05, GS08, DFL+09] (where $n = 1$ and $q \in \{0, 1\}$ determines the mode) and the EMP commitment scheme of [GHR15, GR16] (where $q = 1$ and n is arbitrary).

In Section 4, we define algebraic commitment schemes (ACS), where the commitments keys are matrices. We prove that some basic properties of SSB commitments hold for ACSs and show that these commitments are what we call *QA-NIZK friendly*, i.e., suitable for working with QA-NIZK arguments. This is because they behave like linear maps and the properties of SSB commitments can be expressed in terms of membership to linear subspaces. Next, we generalize the *Extended Multi-Pedersen* (EMP) commitment scheme of [GHR15, GR16]. Importantly, a single EMP commitment consists of $q + 1$ group elements and is thus succinct given small q. We prove that EMP satisfies most of the mentioned security requirements under a standard MDDH assumption [EHK+13].

In Section 5, we define *functional SSB* commitments, which are statistically binding on some components that are outputs of some functions $\mathcal{S} = \{f_i\}_i$ where $|\mathcal{S}| \leq q$. It is a generalization of SSB commitments, where the extracted values are the result of some linear functions of the committed values, instead of the values itself. We show that results that hold for SSB commitments also naturally hold for functional SSB commitments. The notion of functional SSB commitments for families of linear functions was already used indirectly in some constructions such as [DGP+19]; however, they were not formally defined and their security properties were not analyzed. We also see that a minor modification of EMP works as a functional SSB commitment if we consider only linear functions.

Application: Oblivious database queries. We consider a novel (but natural) application that we call oblivious database queries (ODQ). In an ODQ protocol, a sender has a private database $\boldsymbol{x}$ and a receiver wants to query the database to learn $f_1(\boldsymbol{x}), \ldots, f_q(\boldsymbol{x})$ without revealing the functions f_i. This can be directly realized with linear EMP if we restrict f_i to be linear functions. The receiver sends a commitment key (which encodes $\mathcal{S} = \{f_i\}_i$) to the sender who responds with a commitment to the database $\boldsymbol{x}$. The receiver can then extract the query results with an extraction key (SSE property). Unfortunately, linear EMP only has F-extractability [BCKL08] (more precisely, one can only extract the message as a vector of group elements, not a vector of integers), and thus we are only able to extract $\{g^{f_i(\boldsymbol{x})}\}_i$ where g is a generator of some cyclic group. The protocol is secure in the semi-honest model. In particular, the receiver's privacy follows from the function set hiding property (analog to ISH in functional SSB commitments), which holds under the DDH assumption. Sender's privacy holds information-theoretically since using AESH property, we are able to perfectly simulate the commitment. We also achieve near-optimal download rate (the ratio between output size and sender's message size) which is $q/(q+1) \approx 1$ but sub-optimal total rate (ratio between output size and total transcript size) of approximately $1/(n+q)$.

A similar approach also gives us oblivious linear function evaluation (OLE) [DKM12, GNN17, DGN+17] where sender has a private linear function f and receiver wants to learn $f(\boldsymbol{x})$ of his private input $\boldsymbol{x}$. However, in this case, both download rate and total rate are sub-optimal.

Recently, Döttling et al. [DGI+19] proposed an oblivious matrix-vector product protocol in the semi-honest model using trapdoor hash functions. In their case, the receiver has $\boldsymbol{x}$, the sender has a matrix $\boldsymbol{M}$, and the receiver wants to learn $\boldsymbol{Mx}$. If we interpret linear functions $\{f_i\}_i$ as a matrix $\boldsymbol{M}$, then ODQ can be seen as an OMV protocol where the roles of sender and receiver are switched. They gave a construction under the Learning with Errors (LWE) and the Quadratic Residuosity (QR) problem, which work over fields with small characteristic or rings modulo a smooth integer. Interestingly, they also achieve download rate 1 but sub-optimal total rate. Thus our work can be viewed as complementary to their result.

We give a more technical explanation of ODQ and OLE protocols in Section 6.

Application: Shorter QA-NIZK for arithmetic circuits. Recently, Daza *et al.* [DGP$^+$19] constructed an efficient commit-and-prove QA-NIZK argument for Square Span Programs (SSP, [DFGK14]) under falsifiable assumptions, which can be used to prove Boolean circuit satisfiability. We present a QA-NIZK for Square Arithmetic Programs (SAP, [GM17]) in Section 7 that follows a similar strategy but can be used for arithmetic circuit satisfiability with comparable efficiency and also proven under falsifiable assumptions. Both constructions use a linear-length perfectly binding commitment of the witness, but are otherwise succinct arguments; the arguments also contain perfectly hiding commitments that come from zk-SNARK techniques for proving satisfiability of quadratic equations and a functional SSB commitment to extract certain linear functions of the witness in the security reduction.

We note that the construction in [DGP$^+$19] uses linear EMP commitment schemes indirectly. We formalize and generalize them in our framework as functional SSB commitments and then use them as a black box in our QA-NIZK application. This significantly simplifies the understanding of the scheme in two ways. Firstly, the techniques used in the security proof are natural functionalities of *algebraic commitment schemes* that we present in the paper, e.g., using a commitment key consisting of two orthogonal matrices to enable extraction. Secondly, the notation of our commitments is more compact, which helps to see that soundness is guaranteed by the SSB, $[\cdot]$-SSE, and FSH properties of functional SSB and zero-knowledge is guaranteed by AESH.

We give an intuition of the proof and soundness strategy in the following. The proof consists of two subarguments: one based on SNARK techniques where many quadratic equations are proved to be satisfied using a single polynomial divisibility relation with polynomials evaluated at a secret point s, and a proof of subspace membership showing that all the commitments in the argument open to the same witness. We have one linear perfectly binding commitment C, which is an ElGamal encryption of the witness. Similarly to zk-SNARKs, the witness is extracted in the security proof and used to detect which quadratic equation of the language does not hold. However, our commitment is only F-extractable, which is not enough to break the underlying falsifiable assumption. Note that zk-SNARKs typically use a non-falsifiable assumption at this point to avoid this issue. We instead use a linear EMP commitment D in pairing group $\mathbb{G}_2$ that perfectly hides the witness in the honest proof (setting $\mathcal{S} = \emptyset$).

In the security proof, we change to an indistinguishable game (by the FSH property) where the commitment key now encodes some linear functions that depend on the secret point s. This will allow us to F-extract linear combinations of the form $\sum_i w_i \alpha_i(s)$ where $\{w_i\}_i$ is the witness and $\alpha_i(s)$ are coefficients of the function we choose. Essentially it allows us to trick the prover into computing some secret linear function of the witness. We see that the extra knowledge from the commitment D allows us to break a variant of the target strong Diffie-

Hellman (TSDH) assumption [BB04]. We also prove that the new assumption is falsifiable and equivalent to the TSDH assumption under a knowledge assumption in Appendix D.

Relation to SSB hash functions. The SSB requirement makes the EMP commitment scheme look similar to SSB hash functions [HW15, OPWW15], in which one can compute a hash of a vector v such that the computed hash is statistically binding in one coordinate of v. However, there are also obvious differences. First, to obtain zero-knowledge, we need hiding (AESH) that is not required from hash functions. This is, intuitively, a natural distinction and corresponds to the difference between collision-resistant hash families and statistically hiding commitment schemes.

Second, [HW15, OPWW15] require that an SSB hash has the local opening property, meaning that the committer can efficiently open just one coordinate of the committed vector. In the QA-NIZK application, we do not need this property: in the described QA-NIZK for bit-string (and related QA-NIZKs for other languages from [GR16, DGP+19]), the commitment key $\mathtt{ck}$ is created by a trusted third party, and there is no need for the honest parties to ever open the commitment. Instead, in the soundness proof, we need *somewhere statistical extractability* (SSE), stating that the creator of $\mathtt{ck}$ (e.g., the adversary $\mathcal{B}$) must be able to extract the succinct guilt witness. SSE is not needed in the case of SSB hashes. Although not needed in our concrete applications, it is also desirable to have the *almost everywhere statistical trapdoor* (AEST) property, where the creator of $\mathtt{ck}$ is able to replace non-SB coordinates with anything she wishes. Finally, we allow $\mathtt{ck}$ to be long, but require commitments to be succinct.

The properties of SSB and local opening are orthogonal: it is possible to construct efficient SSB hashes without local opening [OPWW15] and efficient vector commitments [LY10, CF13] (which have a local opening) without the SSB property.

Connection to OT. SSB commitments are directly related to two-message OT protocols as defined in [AIR01]. Essentially, SSB commitments are non-interactive analogs of such protocols, the commitment key corresponding to the first OT message ot_1, and the commitment corresponding to the second OT message ot_2. Importantly, while in OT, the ot_1 generator is always untrusted, in our applications, it is sufficient to consider a trusted $\mathtt{ck}$ generator. This allows for more efficient constructions.

Thus, all secure two-message OT protocols such as [Lip05, GR05] are also secure SSB commitment schemes. Unfortunately, none of the known efficient two-message OT protocols are QA-NIZK-friendly, and thus they are unsuitable for our main application.

Relation to PCP-Based SNARKs. The QA-NIZK application of SSB commitments is based on the observation that the language of bit-strings (resp., CircuitSAT) has a local verifiability property, similar to PCP [AS92, ALM+92]: one can establish, by checking one random coordinate of the bit-string (resp., all adjacent wires of a random gate), whether an input belongs to the language or not. Typical PCP-based zero-knowledge arguments like [Kil94] use PCPs with small soundness error; as a drawback, such PCPs have a long proof and an inefficient reduction from CircuitSAT. Daza *et al.* [DGP+19] and the current paper use a trivial PCP with a large soundness error but with a trivial reduction from CircuitSAT. The use of SSB commitments means that the efficiency loss is logarithmic in n (one needs to use $\approx 2 \log n$-bit longer group elements) while in the case of earlier PCP-based arguments the efficiency loss is much larger. Nevertheless, the use of SSB commitments is not limited to trivial PCP; one can use them together with any PCP that has a small number of queries and short proof length.

2 Preliminaries

For a set S, let $\mathbb{P}(S)$ denote the power set (i.e., the set of subsets) of S, and let $\mathbb{P}(S, q)$ denote the set of q-size subsets of S. For an n-dimensional vector $\boldsymbol{\alpha}$ and $i \in [1 \mathinner{..} n]$, let α_i be its ith coefficient. Let $\boldsymbol{e}_i$ be the ith unit vector of implicitly understood dimension. For a tuple $\mathcal{S} = (\sigma_1, \ldots, \sigma_q)$ with $\sigma_i < \sigma_{i+1}$, let $\boldsymbol{\alpha}_{\mathcal{S}} = (\alpha_{\sigma_1}, \ldots, \alpha_{\sigma_q})$. Let $\boldsymbol{\alpha}_{\emptyset}$ be the empty string.

Let PPT denote probabilistic polynomial-time and let $\lambda \in \mathbb{N}$ be the security parameter. All adversaries will be stateful. Let $\mathsf{RND}_\lambda(\mathcal{A})$ denote the random tape of the algorithm $\mathcal{A}$ for a fixed λ. We denote by $\mathsf{negl}(\lambda)$ an arbitrary negligible function, and by $\mathsf{poly}(\lambda)$ an arbitrary polynomial function. Functions f, g are negligibly close, denoted $f \approx_\lambda g$, if $|f - g| = \mathsf{negl}(\lambda)$.

2.1 Bilinear groups

In the case of groups, we will use additive notation together with the bracket notation [EHK+13], that is, for $\iota \in \{1, 2, T\}$ we define $[a]_\iota := a[1]_\iota$, where $[1]_\iota$ is a fixed generator of the group $\mathbb{G}_\iota$. A *bilinear group generator* $\mathsf{Pgen}(1^\lambda)$ returns $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \hat{e}, [1]_1, [1]_2)$, where p (a large prime) is the order of cyclic Abelian groups $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$. Moreover, $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is an efficient non-degenerate bilinear pairing, such that $\hat{e}([a]_1, [b]_2) = [ab]_T$. Denote $[a]_1[b]_2 := \hat{e}([a]_1, [b]_2)$, and $[1]_T := [1]_1[1]_2$. We use matrix-vector notation freely, writing say $[\boldsymbol{M}_1]_1[\boldsymbol{M}_2]_2 = [\boldsymbol{M}_1\boldsymbol{M}_2]_T$ for any compatible matrices $\boldsymbol{M}_1$ and $\boldsymbol{M}_2$.

We use F-extraction notation to mean extraction of the function F. For example if F is exponentiation then we have $[\cdot]_\iota$-extraction, where we extract elements in the group $\mathbb{G}_\iota$.

Several of our cryptographic primitives have their own parameter generator Pgen. In all concrete instantiations of the primitives, we instantiate Pgen with the bilinear group generator, which is then denoted Pgen_{bg}.

Distribution families $\mathcal{D}^0 = \{\mathcal{D}^0_\lambda\}_\lambda$ and $\mathcal{D}^1 = \{\mathcal{D}^1_\lambda\}_\lambda$ are *computationally indistinguishable*, if $\forall$ PPT $\mathcal{A}$, $|\Pr[x \leftarrow_{\$} \mathcal{D}^0_\lambda : \mathcal{A}(x) = 1] - \Pr[x \leftarrow_{\$} \mathcal{D}^1_\lambda : \mathcal{A}(x) = 1]| \approx_\lambda 0$.

Let $\ell, k \in \mathbb{N}$, with $\ell \geq k$, be small constants. Let p be a large prime. Following [EHK+13], we call $\mathcal{D}_{\ell k}$ a *matrix distribution* if it outputs, in polynomial time, matrices $\boldsymbol{A}$ in $\mathbb{Z}_p^{\ell \times k}$ of full rank k. We denote $\mathcal{D}_{k+1,k}$ by $\mathcal{D}_k$. Let $\mathcal{U}_{\ell k}$ denote the uniform distribution over $\mathbb{Z}_p^{\ell \times k}$.

Let Pgen be as before, and let $\iota \in \{1,2\}$. $\mathcal{D}_{\ell k}$-*MDDH*$_{\mathbb{G}_\iota}$ [EHK+13] holds relative to Pgen, if $\forall$ PPT $\mathcal{A}$, $\mathsf{Adv}^{\mathrm{mddh}}_{\mathcal{A},\mathcal{D}_{\ell k},\iota,\mathsf{Pgen}}(\lambda) := |\varepsilon^0_{\mathcal{A}}(\lambda) - \varepsilon^1_{\mathcal{A}}(\lambda)| \approx_\lambda 0$, where

$$\varepsilon^\beta_{\mathcal{A}}(\lambda) := \Pr\left[\begin{array}{l} \mathsf{p} \leftarrow \mathsf{Pgen}(1^\lambda); \mathbf{A} \leftarrow_\$ \mathcal{D}_{\ell k}; \mathtt{w} \leftarrow_\$ \mathbb{Z}_p^k; \\ \boldsymbol{y}_0 \leftarrow_\$ \mathbb{Z}_p^\ell; \boldsymbol{y}_1 \leftarrow \mathbf{A}\mathtt{w} : \mathcal{A}(\mathsf{p}, [\mathbf{A}, \boldsymbol{y}_\beta]_\iota) = 1 \end{array}\right] .$$

Common distributions for the MDDH assumption are $\mathcal{U}_k := \mathcal{U}_{k+1,k}$ and the linear distribution $\mathcal{L}_k$ over $\boldsymbol{A} = \left(\begin{smallmatrix} \boldsymbol{A'} \\ 1 \ \dots \ 1 \end{smallmatrix}\right)$, where $\boldsymbol{A'} \in \mathbb{Z}_p^{k \times k}$ is a diagonal matrix with $a'_{ii} \leftarrow_\$ \mathbb{Z}_p$.

2.2 Quasi-adaptive NIZK

A quasi-adaptive non-interactive zero-knowledge (QA-NIZK) proof [JR13] enables one to prove membership in a language defined by a relation $\mathcal{R}_\rho$, which is determined by some parameter ρ sampled from a distribution $\mathcal{D}_{\mathsf{gk}}$. A distribution $\mathcal{D}_{\mathsf{gk}}$ is *witness-sampleable* if there exists an efficient algorithm that samples (ρ, ω_ρ) from a distribution $\mathcal{D}^{\mathsf{par}}_{\mathsf{gk}}$ such that ρ is distributed according to $\mathcal{D}_{\mathsf{gk}}$, and membership of ρ in the *parameter language* $\mathcal{L}_{\mathsf{par}}$ can be efficiently verified by using this witness ω_ρ.

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

Quasi-Adaptive Completeness:

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

Computational Quasi-Adaptive Soundness:

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

Computational Strong Quasi-Adaptive Soundness:

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

Perfect Quasi-Adaptive Zero-Knowledge:

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

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

We assume that $\mathtt{crs}$ contains an encoding of ρ, which is thus available to V.

3 SSB Commitment Schemes

Next, we will generalize and formalize the vector commitment scheme of González *et al.* [GHR15, GR16] as an SSB commitment scheme. An SSB commitment scheme generalizes dual-mode commitment schemes [DFL$^+$09] akin to the Groth-Sahai commitment scheme for scalars [GS08]. They are also related to mixed commitment schemes [DN02] and hybrid commitment schemes [CV05].

In an SSB commitment scheme, the commitment key (that is, the CRS) depends on n, q, and an index-set $\mathcal{S} \subseteq [1 \mathinner{..} n]$ of cardinality $\leq q$ (in the case of Groth-Sahai commitments [GS08], $n = q = 1$ while in the current paper $n = \mathsf{poly}(\lambda)$ and $q \geq 1$ is a small constant). At coordinates described by $\mathcal{S}$, an SSB commitment scheme must be *statistically binding* and *F-extractable* [BCKL08] for a well-chosen function F, while at all other coordinates it must be *statistically hiding* and *trapdoor*. Moreover, it must be index-set hiding, i.e., commitment keys corresponding to any two index-sets $\mathcal{S}_1$ and $\mathcal{S}_2$ of size $\leq q$ are required to be computationally indistinguishable.

Note that Groth-Sahai commitments correspond to a *bimodal* setting where either all coefficients are statistically hiding or statistically binding, and these two extremes are indistinguishable. SSB commitments correspond to a more fine-grained *multimodal* setting where some $\leq q$ coefficients are statistically binding and other coefficients are statistically hiding, and all possible selections of statistically binding coefficients are mutually indistinguishable. Our terminology is inspired by [HW15, OPWW15] who defined somewhere statistically binding hashing; however, the consideration of the hiding property makes the case of SSB commitments sufficiently different.

3.1 Formalization and Definitions

An *F-extractable SSB commitment scheme* $\mathsf{COM} = (\mathsf{Pgen}, \mathsf{KC}, \mathsf{Com}, \mathsf{tdOpen}, \mathsf{Ext}_F)$ consists of the following polynomial-time algorithms:

Parameter generation: $\mathsf{Pgen}(1^\lambda)$ returns parameters p (e.g., description of a bilinear group).

Commitment key generation: for parameters p, a positive integer $n \in \mathsf{poly}(\lambda)$, an integer $q \in [1 \mathinner{..} n]$, and a tuple $\mathcal{S} \subseteq [1 \mathinner{..} n]$ with $|\mathcal{S}| \leq q$, $\mathsf{KC}(\mathsf{p}, n, q, \mathcal{S})$ outputs a commitment key $\mathtt{ck}$ and a trapdoor $\mathtt{td} = (\mathtt{ek}, \mathtt{tk})$ consisting of an *extraction key* $\mathtt{ek}$, and a *trapdoor key* $\mathtt{tk}$. Also, $\mathtt{ck}$ implicitly specifies p, n, q, the message space $\mathtt{MSP}$, the randomizer space $\mathtt{RSP}$, and the commitment space $\mathtt{CSP}$, such that $F(\mathtt{MSP}) \subseteq \mathtt{ESP}$. For invalid input, KC outputs $(\mathtt{ck}, \mathtt{td}) = (\perp, \perp)$.

Commitment: for $\mathsf{p} \in \mathsf{Pgen}(1^\lambda)$, a commitment key $\mathtt{ck} \neq \perp$, a message $\boldsymbol{x} \in \mathtt{MSP}^n$, and a randomizer $r \in \mathtt{RSP}$, $\mathsf{Com}(\mathtt{ck}; \boldsymbol{x}; r)$ outputs a commitment $c \in \mathtt{CSP}$.

Trapdoor opening: for $\mathsf{p} \in \mathsf{Pgen}(1^\lambda)$, $\mathcal{S} \subseteq [1 \mathinner{..} n]$ with $|\mathcal{S}| \leq q$, $(\mathtt{ck}, (\mathtt{ek}, \mathtt{tk})) \in \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S})$, two messages $\boldsymbol{x}, \boldsymbol{x}^* \in \mathtt{MSP}^n$, and a randomizer $r \in \mathtt{RSP}$, $\mathsf{tdOpen}(\mathsf{p}, \mathtt{tk}; \boldsymbol{x}, r, \boldsymbol{x}^*)$ returns a randomizer $r^* \in \mathtt{RSP}$.

Abbreviation	Property	Definition
ISH	Index-set hiding	The commitment key reveals nothing about the index-set $\mathcal{S}$
SSB	Somewhere statistically binding	A commitment to $\boldsymbol{x}$ statistically binds the values $\boldsymbol{x}_{\mathcal{S}}$
AESH	Almost everywhere statistically hiding	The commitment is statistically hiding in the indices outside the set $\mathcal{S}$
F-SSE	Somewhere statistical F-extractability	Given a commitment to $\boldsymbol{x}$ and the extraction key, one can extract the values $F(\boldsymbol{x}_S)$

Table 1. Properties of an SBB commitment scheme

Extraction: for $\mathsf{p} \in \mathsf{Pgen}(1^{\lambda})$, $\mathcal{S} = (\sigma_1, \ldots, \sigma_{|\mathcal{S}|}) \subseteq [1 \mathinner{..} n]$ with $1 \leq |\mathcal{S}| \leq q$, $(\mathtt{ck}, (\mathtt{ek}, \mathtt{tk})) \in \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S})$, $F : \mathtt{MSP} \rightarrow \mathtt{ESP}$ and $c \in \mathtt{CSP}$, $\mathsf{Ext}_F(\mathsf{p}, \mathtt{ek}; c)$ returns a tuple $(y_{\sigma_1}, \ldots, y_{\sigma_{|\mathcal{S}|}}) \in \mathtt{ESP}^{|\mathcal{S}|}$. We allow F to depend on p.

Note that SSB commitment schemes are non-interactive and work in the CRS model; the latter is needed to achieve trapdoor opening and extractability. With the current definition, *perfect completeness* is straightforward: to verify that C is a commitment of $\boldsymbol{x}$ with randomizer r, one just recomputes $C' \leftarrow \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}; r)$ and checks whether $C = C'$.

An F-extractable SSB commitment scheme COM is *secure* if it satisfies the following security requirements. (See Table 1 for a brief summary.)

Index-Set Hiding (ISH): $\forall \lambda$, PPT $\mathcal{A}$, $n \in \mathsf{poly}(\lambda)$, $q \in [1 \mathinner{..} n]$, $\mathsf{Adv}^{\mathsf{ish}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) := 2 \cdot |\varepsilon^{\mathsf{ish}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) - 1/2| \approx_{\lambda} 0$, where $\varepsilon^{\mathsf{ish}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) :=$

$$\Pr\left[\begin{array}{l}\mathsf{p} \leftarrow \mathsf{Pgen}(1^{\lambda}); (\mathcal{S}_0, \mathcal{S}_1) \leftarrow \mathcal{A}(\mathsf{p}, n, q) \text{ s.t. } \forall i \in \{0,1\}, \mathcal{S}_i \subseteq [1 \mathinner{..} n] \wedge |\mathcal{S}_i| \leq q; \\ \beta \leftarrow_{\$} \{0,1\}; (\mathtt{ck}_{\beta}, \mathtt{td}_{\beta}) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}_{\beta}) : \mathcal{A}(\mathtt{ck}_{\beta}) = \beta\end{array}\right] .$$

Somewhere Statistically Binding (SSB): $\forall \lambda$, unbounded $\mathcal{A}$, $n \in \mathsf{poly}(\lambda)$, $q \in [1 \mathinner{..} n]$, $\mathsf{Adv}^{\mathrm{ssb}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) \approx_{\lambda} 0$, where $\mathsf{Adv}^{\mathrm{ssb}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) :=$

$$\Pr\left[\begin{array}{l}\mathsf{p} \leftarrow \mathsf{Pgen}(1^{\lambda}); \mathcal{S} \leftarrow \mathcal{A}(\mathsf{p}, n, q) \text{ s.t. } \mathcal{S} \subseteq [1 \mathinner{..} n] \wedge |\mathcal{S}| \leq q; \\ (\mathtt{ck}, \mathtt{td}) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}); (\boldsymbol{x}_0, \boldsymbol{x}_1, r_0, r_1) \leftarrow \mathcal{A}(\mathtt{ck}) \text{ s.t. } \boldsymbol{x}_{0\mathcal{S}} \neq \boldsymbol{x}_{1\mathcal{S}}; \\ \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}_0; r_0) = \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}_1; r_1)\end{array}\right] .$$

COM is *somewhere perfectly binding* (SPB) if $\mathsf{Adv}^{\mathrm{ssb}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) = 0$.

Almost Everywhere Statistically Hiding (AESH): $\forall \lambda$, unbounded adversary $\mathcal{A}$, $n \in \mathsf{poly}(\lambda)$, $q \in [1 \mathinner{..} n]$, $\mathsf{Adv}^{\mathsf{aesh}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) := 2 \cdot |\varepsilon^{\mathsf{aesh}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) - 1/2| \approx_{\lambda} 0$, where $\varepsilon^{\mathsf{aesh}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) :=$

$$\Pr\left[\begin{array}{l}\mathsf{p} \leftarrow \mathsf{Pgen}(1^{\lambda}); \mathcal{S} \leftarrow \mathcal{A}(\mathsf{p}, n, q) \text{ s.t. } \mathcal{S} \subseteq [1 \mathinner{..} n] \wedge |\mathcal{S}| \leq q; \\ (\mathtt{ck}, \mathtt{td}) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}); (\boldsymbol{x}_0, \boldsymbol{x}_1) \leftarrow \mathcal{A}(\mathtt{ck}) \text{ s.t. } \boldsymbol{x}_{0\mathcal{S}} = \boldsymbol{x}_{1\mathcal{S}}; \\ \beta \leftarrow_{\$} \{0,1\}; r \leftarrow_{\$} \mathtt{RSP} : \mathcal{A}(\mathsf{Com}(\mathtt{ck}; \boldsymbol{x}_{\beta}; r)) = \beta\end{array}\right] .$$

COM is *almost everywhere perfectly hiding* (AEPH) if $\mathsf{Adv}^{\mathsf{aesh}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) = 0$. If $\mathcal{A}$ is PPT instead of unbounded, COM is *almost everywhere computationally hiding* (AECH).

Somewhere Statistical F-Extractability (F-SSE): $\forall \lambda$, $n \in \mathsf{poly}(\lambda)$, $q \in [1 \mathinner{..} n]$, $\mathcal{S} = (\sigma_1, \dots, \sigma_{|\mathcal{S}|})$ with $|\mathcal{S}| \le q$, $(\mathtt{ck}, (\mathtt{ek}, \mathtt{tk})) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S})$, and PPT $\mathcal{A}$, $\mathsf{Adv}^{\mathrm{sse}}_{\mathcal{A},F,\mathsf{COM},n,q}(\lambda) :=$

$$\Pr\left[\boldsymbol{x}, r \leftarrow \mathcal{A}(\mathtt{ck}) : \mathsf{Ext}_F(\mathsf{p}, \mathsf{ek}; \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}; r)) \neq (F(x_{\sigma_1}), \dots, F(x_{\sigma_{|\mathcal{S}|}}))\right] \approx_\lambda 0 \enspace .$$

Additionally, an SSB commitment scheme can but does not have to be *trapdoor*.

Almost Everywhere Statistical Trapdoor (AEST): $\forall \lambda$, $n \in \mathsf{poly}(\lambda)$, $q \in [1 \mathinner{..} n]$, and unbounded $\mathcal{A}$, $\mathsf{Adv}^{\mathrm{aest}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) \approx_\lambda 0$, where $\mathsf{Adv}^{\mathrm{aest}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) =$

$$\Pr\left[\begin{aligned} &\mathsf{p} \leftarrow \mathsf{Pgen}(1^\lambda); \mathcal{S} \leftarrow \mathcal{A}(\mathsf{p}, n, q) \text{ s.t. } \mathcal{S} \subseteq [1 \mathinner{..} n] \wedge |\mathcal{S}| \le q;\\ &(\mathtt{ck}, \mathtt{td} = (\mathtt{ek}, \mathtt{tk})) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}); (\boldsymbol{x}_0, r_0, \boldsymbol{x}_1) \leftarrow \mathcal{A}(\mathtt{ck}) \text{ s.t. } \boldsymbol{x}_{0\mathcal{S}} = \boldsymbol{x}_{1\mathcal{S}};\\ &r_1 \leftarrow \mathsf{tdOpen}(\mathsf{p}, \mathtt{tk}; \boldsymbol{x}_0, r_0, \boldsymbol{x}_1) : \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}_0; r_0) \neq \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}_1; r_1) \end{aligned}\right] \enspace .$$

It is *almost everywhere perfect trapdoor (AEPT)* if $\mathsf{Adv}^{\mathrm{aest}}_{\mathsf{COM},n,q}(\lambda) = 0$.

It is important to consider the case $|\mathcal{S}| \le q$ instead of only $|\mathcal{S}| = q$. For example, when $q = n$, the PB commitment key ($|\mathcal{S}| = n$) has to be indistinguishable from the PH commitment key ($|\mathcal{S}| = 0$). Moreover, in the applications to construct QA-NIZK argument systems [GHR15, GR16, DGP$^+$19], one should not be able to distinguish between the cases $|\mathcal{S}| = 0$ and $|\mathcal{S}| = q$.

F-extractability [BCKL08] allows one to model the situation where $x_i \in \mathbb{Z}_p$ but we can only extract the corresponding bracketed value $[x_i]_\iota \in \mathbb{G}_\iota$; similar limited extractability is satisfied say by the Groth-Sahai commitment scheme for scalars [GS08]. Note that in this case, F depends on p. Interestingly, extractability implies SSB, see Appendix B.1 for a proof.

Lemma 1 (F-SSE & F is injective $\Rightarrow$ SSB). *Let* COM *be an SSB commitment scheme. Fix n and q. Assume F is injective. For all PPT $\mathcal{A}$, there exists a PPT $\mathcal{B}$ such that* $\mathsf{Adv}^{\mathrm{ssb}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) \le 2 \cdot \mathsf{Adv}^{\mathrm{sse}}_{\mathcal{B},F,\mathsf{COM},n,q}(\lambda)$*.*

If $q = 0$ then AESH is equal to the standard statistical hiding (SH) requirement, and AEST is equal to the standard statistical trapdoor requirement. If $q = n$ then SSB is equal to the standard statistical binding (SB) requirement, and F-SSE is equal to the standard statistical F-extractability requirement. We will show that any secure SSB commitment scheme must also be computationally hiding and binding in the following sense.

Computational Binding (CB): $\forall$ PPT $\mathcal{A}$, $n \in \mathsf{poly}(\lambda)$, $q \in [1 \mathinner{..} n]$, where $\mathsf{Adv}^{\mathrm{cb}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) :=$

$$\Pr\left[\begin{aligned} &\mathsf{p} \leftarrow \mathsf{Pgen}(1^\lambda); \mathcal{S} \leftarrow \mathcal{A}(\mathsf{p}, n, q) \text{ s.t. } \mathcal{S} \subseteq [1 \mathinner{..} n] \wedge |\mathcal{S}| \le q;\\ &(\mathtt{ck}, \mathtt{td}) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}); (\boldsymbol{x}_0, \boldsymbol{x}_1, r_0, r_1) \leftarrow \mathcal{A}(\mathtt{ck})\\ &\ \text{s.t. } \boldsymbol{x}_0 \neq \boldsymbol{x}_1; \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}_0; r_0) = \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}_1; r_1) \end{aligned}\right] \approx_\lambda 0 \enspace .$$

Computational Hiding (CH): $\forall$ PPT $\mathcal{A}$, $n \in \mathsf{poly}(\lambda)$, $q \in [1 \mathinner{..} n]$, $\mathsf{Adv}^{\mathrm{ch}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) := 2 \cdot |\varepsilon^{\mathsf{ch}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) - 1/2| \approx_\lambda 0$, where $\varepsilon^{\mathsf{ch}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) :=$

$$\Pr\left[\begin{aligned} &\mathsf{p} \leftarrow \mathsf{Pgen}(1^\lambda); \mathcal{S} \leftarrow \mathcal{A}(\mathsf{p}, n, q) \text{ s.t. } \mathcal{S} \subseteq [1 \mathinner{..} n] \wedge |\mathcal{S}| \le q;\\ &(\mathtt{ck}, \mathtt{td}) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}); (\boldsymbol{x}_0, \boldsymbol{x}_1) \leftarrow \mathcal{A}(\mathtt{ck}); \beta \leftarrow_{\$} \{0, 1\};\\ &r \leftarrow_{\$} \mathsf{RSP} : \mathcal{A}(\mathsf{Com}(\mathtt{ck}; \boldsymbol{x}_\beta; r)) = \beta \end{aligned}\right] \enspace .$$

Theorem 1. *Let* COM *be an SSB commitment scheme. Fix* n *and* q.

(i) (ISH + SSB $\Rightarrow$ *CB) For all PPT* $\mathcal{A}$*, there exist PPT* $\mathcal{B}_1$ *and unbounded* $\mathcal{B}_2$*, such that* $\mathsf{Adv}^{\mathrm{cb}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) \leq \mathsf{Adv}^{\mathrm{ish}}_{\mathcal{B}_1,\mathsf{COM},n,q}(\lambda) + n/(q - 4 \cdot \mathsf{Adv}^{\mathrm{ish}}_{\mathcal{B}_1,\mathsf{COM},n,q}(\lambda)) \cdot \mathsf{Adv}^{\mathrm{ssb}}_{\mathcal{B}_2,\mathsf{COM},n,q}(\lambda)$.

(ii) (ISH + AESH $\Rightarrow$ *CH) For all PPT* $\mathcal{A}$*, there exist PPT* $\mathcal{B}_1$ *and unbounded* $\mathcal{B}_2$*, such that* $\mathsf{Adv}^{\mathrm{ch}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) \leq \mathsf{Adv}^{\mathrm{ish}}_{\mathcal{B}_1,\mathsf{COM},n,q}(\lambda) + \mathsf{Adv}^{\mathrm{aesh}}_{\mathcal{B}_2,\mathsf{COM},n,q}(\lambda)$.

Proof. Let $\Pr[\mathrm{Game}_i(\mathcal{A}) = 1]$ denote the probability $\mathcal{A}$ wins in Game_i.

(i: ISH + SSB $\Rightarrow$ CB) We prove the theorem using a sequence of hybrid games, defined as follows, where $\varepsilon_i := \Pr[\mathrm{Game}_i(\mathcal{A}) = 1]$.

$\underline{\mathrm{Game}_1}$: The original computational binding game. For given n and q, by definition $\mathcal{A}$ can break CB with probability $\varepsilon_1 = \mathsf{Adv}^{\mathrm{cb}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda)$.

$\underline{\mathrm{Game}_2}$: Game_1, but instead of $\mathtt{ck}$, $\mathcal{A}$ gets $\mathtt{ck}'$ where $(\mathtt{ck}', \mathtt{td}') \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}_1)$ for $\mathcal{S}_1 \leftarrow_{\$} \mathbb{P}([1\,..\,n], q)$. Note that a distinguisher $\mathcal{B}_1$ for Game_1 and Game_2 can be used to break the ISH game with advantage $\varepsilon_{\mathsf{ish}} = \mathsf{Adv}^{\mathrm{ish}}_{\mathcal{B}_1,\mathsf{COM},n,q}(\lambda)$. Hence $|\varepsilon_1 - \varepsilon_2| \leq \varepsilon_{\mathsf{ish}}$, which implies that $\varepsilon_2 \geq \varepsilon_1 - \varepsilon_{\mathsf{ish}}$.

We now require the following lemma.

Lemma 2. *Assume* $\mathcal{A}$ *outputs* $(\boldsymbol{x}_0, r_0, \boldsymbol{x}_1, r_1)$ *with* $\boldsymbol{x}_0 \neq \boldsymbol{x}_1$*. Then* $\Pr[(\boldsymbol{x}_0)_{\mathcal{S}_1} \neq (\boldsymbol{x}_1)_{\mathcal{S}_1}$ *in* $\mathrm{Game}_2] \geq q/n - 4 \cdot \varepsilon_{\mathsf{ish}}$.

Proof. Assume for any $\mathcal{S}_1$ of size q sampled uniformly at random, $\mathcal{A}$ can output distinct $\boldsymbol{x}_0, \boldsymbol{x}_1$ such that $\Pr[(x_0)_{\mathcal{S}_1} \neq (x_1)_{\mathcal{S}_1}$ in $\mathrm{Game}_2] = \varepsilon$.

We construct an adversary $\mathcal{B}$ that uses $\mathcal{A}$ to break ISH as follows.

1. Given p, n, q, $\mathcal{B}$ sets $\mathcal{S}_1 \leftarrow_{\$} \mathbb{P}([1\,..\,n], q)$ and receives $S_0 \leftarrow \mathcal{A}(\mathsf{p}, n, q)$.
2. $\mathcal{B}$ sends $(\mathcal{S}_0, \mathcal{S}_1)$ to the ISH challenger, and receives $\mathtt{ck}$ corresponding to $\mathcal{S}_\beta$.
3. $\mathcal{B}$ gets $(\boldsymbol{x}_0, r_0, \boldsymbol{x}_1, r_1) \leftarrow \mathcal{A}(\mathtt{ck})$.
   - If $\mathcal{A}$ doesn't win, abort.
   - If $(\boldsymbol{x}_0)_{\mathcal{S}_1} \neq (\boldsymbol{x}_1)_{\mathcal{S}_1}$ return $\beta' \leftarrow_{\$} \{0, 1\}$.
   - Else return 1.

Note that $\beta = 0$ corresponds to Game_1, and $\beta = 1$ corresponds to Game_2. Moreover, for $\beta = 0$, $\mathcal{A}$'s output $(\boldsymbol{x}_0, r_0, \boldsymbol{x}_1, r_1)$ is independent of S_1, in which case $\Pr[(\boldsymbol{x}_0)_{\mathcal{S}_1} \neq (\boldsymbol{x}_1)_{\mathcal{S}_1}] \geq |\mathcal{S}_1|/n = q/n$. Hence we get that if $\mathcal{A}$ wins,

$$\begin{aligned}
\Pr[\mathrm{Game}_{ISH}(\mathcal{B}) = 1] &= \frac{1}{2}\Pr[\mathrm{Game}_{ISH}(\mathcal{B}) = 1 | \beta = 0] + \frac{1}{2}\Pr[\mathrm{Game}_{ISH}(\mathcal{B}) = 1 | \beta = 1] \\
&= \frac{1}{2}\Pr[(x_0)_{\mathcal{S}_1} \neq (x_1)_{\mathcal{S}_1} \text{ in } \mathrm{Game}_1 \wedge \beta' = 0] \\
&+ \frac{1}{2}\Pr[(x_0)_{\mathcal{S}_1} = (x_1)_{\mathcal{S}_1} \text{ in } \mathrm{Game}_2] \\
&+ \frac{1}{2}\Pr[(x_0)_{\mathcal{S}_1} \neq (x_1)_{\mathcal{S}_1} \text{ in } \mathrm{Game}_2 \wedge \beta' = 1] \\
&\geq \frac{q}{4n} + \frac{1 - \epsilon}{2} + \frac{\epsilon}{4} \\
&= \frac{1}{2} + \frac{q - n\epsilon}{4n} \quad .
\end{aligned}$$

Hence $4 \cdot \varepsilon_{\mathsf{ish}} \geq q/n - \epsilon$, as required. □

It is easy to see that an adversary that wins Game$_2$ with $(\boldsymbol{x}_0)_{\mathcal{S}_1} \neq (\boldsymbol{x}_1)_{\mathcal{S}_1}$ also wins the SSB game. Hence there exists an adversary $\mathcal{B}_2$ such that

$$\begin{aligned}\mathsf{Adv}^{\mathrm{ssb}}_{\mathcal{B}_2,\mathsf{COM},n,q}(\lambda) &\geq \varepsilon_2 \cdot \Pr[(\boldsymbol{x}_0)_{\mathcal{S}_1} \neq (\boldsymbol{x}_1)_{\mathcal{S}_1} \text{ in Game}_2 | \boldsymbol{x}_0 \neq \boldsymbol{x}_1] \\ &\geq (\varepsilon_1 - \varepsilon_{\mathsf{ish}})(q/n - 4 \cdot \varepsilon_{\mathsf{ish}}) \text{ (due to Lemma 2).}\end{aligned}$$

This is equivalent to $\varepsilon_1 \leq \varepsilon_{\mathsf{ish}} + \frac{n}{q-4\cdot n\cdot\varepsilon_{\mathsf{ish}}} \cdot \mathsf{Adv}^{\mathrm{ssb}}_{\mathcal{B}_2,\mathsf{COM},n,q}(\lambda)$.

(ii: ISH + AESH $\Rightarrow$ CH) Assume that for given n and q, $\mathcal{A}$ can break CH with probability $\mathsf{Adv}^{\mathrm{ch}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda)$. Consider the following sequence of games with $\varepsilon_i := \Pr[\text{Game}_i(\mathcal{A}) = 1]$.

Game$_1$: In this game, $\mathcal{A}$ breaks CH with probability ε_1. That is, given p, $\mathcal{A}(\mathsf{p}, n, q)$ outputs $\mathcal{S}_0$ such that $|\mathcal{S}_0| \leq q$, and for $(\mathtt{ck}_0, \mathtt{td}_0) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}_0)$, $\mathcal{A}(\mathtt{ck}_0)$ outputs $(\boldsymbol{x}_0, \boldsymbol{x}_1)$, s.t. $\Pr[\beta \leftarrow_{\$} \{0,1\} : \mathcal{A}(\mathsf{Com}(\mathtt{ck}_0; \boldsymbol{x}_\beta; r)) = \beta] = \varepsilon_1$.

Game$_2$: In this game, instead of $\mathtt{ck}_0$, $\mathcal{A}$ obtains $\mathtt{ck}_1$ where $(\mathtt{ck}_1, \mathtt{td}_1) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}_1)$ for $\mathcal{S}_1 = \emptyset$. Clearly, for any PPT $\mathcal{A}$ that tries to distinguish Game$_1$ and Game$_2$, there exists a PPT $\mathcal{B}_1$, such that $|\varepsilon_2 - \varepsilon_1| \leq \mathsf{Adv}^{\mathrm{ish}}_{\mathcal{B}_1,\mathsf{COM},n,q}(\lambda)$.

Let us consider the following AESH adversary $\mathcal{B}_2$ in Game$_2$.

1. Given p, n, q, $\mathcal{B}_2$ sets $\mathcal{S}_1 \leftarrow \emptyset$ and receives $S_0 \leftarrow \mathcal{A}(\mathsf{p}, n, q)$.
2. $\mathcal{B}_2$ computes $(\mathtt{ck}_1, \mathtt{td}_1) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}_1)$ and receives $(\boldsymbol{x}_0, \boldsymbol{x}_1) \leftarrow \mathcal{A}(\mathtt{ck})$.
3. $\mathcal{B}_2$ forwards $(\boldsymbol{x}_0, \boldsymbol{x}_1)$ to the AESH challenger, and receives $c \leftarrow \mathsf{Com}(\mathtt{ck}_1, \boldsymbol{x}_\beta; r)$ for some $\beta \leftarrow_{\$} \{0,1\}$, $r \leftarrow_{\$} \mathtt{RSP}$.
4. $\mathcal{B}$ gets and outputs $\beta' \leftarrow \mathcal{A}(c)$.

If $\mathcal{A}$ returns the correct β' then clearly also $\mathcal{B}_2$ returns the correct β'. For the success of $\mathcal{B}_2$, it is also needed that $\boldsymbol{x}_{0\mathcal{S}_1} = \boldsymbol{x}_{1\mathcal{S}_1}$, which clearly holds since $\mathcal{S}_1 = \emptyset$. Thus, $\mathsf{Adv}^{\mathrm{aesh}}_{\mathcal{B}_2,\mathsf{COM},n,q}(\lambda) = \varepsilon_2$. Hence, $\mathsf{Adv}^{\mathrm{ch}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) \leq |\varepsilon_2 - \varepsilon_1| + \varepsilon_2 \leq \mathsf{Adv}^{\mathrm{ish}}_{\mathcal{B}_1,\mathsf{COM},n,q}(\lambda) + \mathsf{Adv}^{\mathrm{aesh}}_{\mathcal{B}_2,\mathsf{COM},n,q}(\lambda)$. □

4 QA-NIZK-Friendly and EMP Commitments

Recall that the main driving application of the current paper is QA-NIZK, specifically the way González *et al.* [GHR15, GR16, DGP$^+$19] constructed QA-NIZKs for quadratic equations (including SSP, [DFGK14]). To be useful in this application, one will need an SSB commitment that satisfies some additional algebraic properties.

4.1 QA-NIZK-friendly Commitments

González *et al.* [GHR15, GR16, DGP$^+$19] implicitly use an SSB commitment scheme COM to construct efficient QA-NIZK argument systems based on falsifiable assumptions. We will show that the soundness of their QA-NIZK system depends on the ISH, SSB, and SSE properties, while the zero-knowledge property depends on the AESH and CH properties. On the other hand, honest parties never need to actually open the commitment; the opening (more precisely, extraction) is only done inside the security proof by using the SSE property. (In this sense, one could also call them trapdoor hash functions [DGI+19] with the SSB and AESH properties.)

The notion of *algebraic commitment schemes (ACSs)*, where the commitment keys are matrices, was already defined in [RS20] and used implicitly in other works ([CGM16], [CFS17]). Since ACSs behave like linear maps, they are very natural to work with. We give a more general definition in the following where the matrices are sampled from general distributions.

Definition 1. *Let $\iota \in \{1, 2\}$, and let n, m, k be small integers. Let $\mathcal{D}_1$ be a distribution of matrices from $\mathbb{G}_\iota^{k\times n}$ and let $\mathcal{D}_2$ be a distribution of matrices from $\mathbb{G}_\iota^{k\times m}$. A commitment scheme* COM *is a* $(\mathcal{D}_1, \mathcal{D}_2)$-algebraic commitment scheme (ACS) *for vectors in $\mathbb{Z}_p^n$, if for commitment key $\mathsf{ck} = [\boldsymbol{U}_1, \boldsymbol{U}_2]_\iota \leftarrow_\$ \mathcal{D}_1 \times \mathcal{D}_2$ the commitment of a vector $\boldsymbol{x} \in \mathbb{Z}_p^n$ is computed as a linear map of $\boldsymbol{x}$ and randomness $\boldsymbol{r} \leftarrow_\$ \mathbb{Z}_p^m$, i.e., $\mathsf{Com}_{\mathsf{ck}}(\boldsymbol{x}, \boldsymbol{r}) := [\boldsymbol{U}_1]_\iota \boldsymbol{x} + [\boldsymbol{U}_2]_\iota \boldsymbol{r} \in \mathbb{G}_\iota^k$.*

We will see that given different commitment key matrices, their distributions are computationally indistinguishable under the MDDH assumption, and each concrete distribution defines which coordinates of the commitments are SB or SH.

ACS are SSB commitment schemes. We will show that algebraic commitments are computationally hiding under MDDH. They are also perfectly binding in those components that correspond to the linearly independent columns of $\boldsymbol{U}_1$. If they are also pair-wise to columns of $\boldsymbol{U}_2$, the system of equations has maximum rank and unique solution.

Moreover, for extraction assume that $\mathrm{span}\{\boldsymbol{U}_1\} \cap \mathrm{span}\{\boldsymbol{U}_2\} = \{\boldsymbol{0}\}$. Intuitively, $\boldsymbol{U}_1$ defines the space of the opening $\boldsymbol{x}$, while $\boldsymbol{U}_2$ defines the randomness space. To extract in q positions, we hence need ek is such that $\mathsf{ek}[\boldsymbol{U}_2]_\iota = \boldsymbol{0}$ and $\mathsf{ek}[\boldsymbol{U}_1]_\iota = (\boldsymbol{b}_i)_{i=1}^n$, where $\boldsymbol{b}_i$ is $\boldsymbol{e}_i$ in q positions and $\boldsymbol{0}$ elsewhere. Then by the linearity of ACS, $\mathsf{ek} \cdot \mathsf{Com}_{\mathsf{ck}}(\boldsymbol{x}, \boldsymbol{r}) = \mathsf{ek} \cdot [\boldsymbol{U}_1]_\iota \boldsymbol{x} = [\boldsymbol{x}]_\iota$.

Lemma 3. *Let $n \geq 1$ and $q \leq n$. Let* COM *be an ACS with commitment key* $\mathsf{ck} = [\boldsymbol{U}_1, \boldsymbol{U}_2]_\iota$ *sampled from $\mathcal{D}_1 \times \mathcal{D}_2$ as defined in Definition 1.*

(i) COM *is AECH under $\mathcal{D}_2$-MDDH$_{\mathbb{G}_\iota}$.*
(ii) COM *is ISH under $\mathcal{D}_1, \mathcal{D}_2$-MDDH$_{\mathbb{G}_\iota}$.*
(iii) COM *is SPB if $\boldsymbol{U}_1$ has rank q and* $\mathrm{span}\{\boldsymbol{U}_1\} \cap \mathrm{span}\{\boldsymbol{U}_2\} = \{\boldsymbol{0}\}$.
(iv) COM *is $[\cdot]_\iota$-SPE if $\boldsymbol{U}_1$ has rank q and* $\mathrm{span}\{\boldsymbol{U}_1\} \cap \mathrm{span}\{\boldsymbol{U}_2\} = \{\boldsymbol{0}\}$.

The full proof of Lemma 3 is deferred to Appendix B.2. The proof shows how to extract q elements from a ACS; we also show that the optimal size for an ACS COM to be extractable in q components is $q + 1$ and the optimal size for the commitment key $\boldsymbol{U}_2$ is $(q + 1) \times 1$.

Corollary 1. *The minimum size of the $k \times m$ matrix to guarantee $[\cdot]_\iota$-extraction of $n \geq 1$ elements is $k = n + 1$, $m = 1$.*

Proof. Information theoretically the commitment size should be no less than the dimension of the opening in order to extract it completely, so $k \geq n$. The orthogonal space has to be at least of dimension 1 in order to provide extraction, so the minimal difference is $k - m \geq 1$. We have $k \geq n + m$ directly by the linear independence of the columns in matrices $\boldsymbol{U}_1, \boldsymbol{U}_2$. Hence, the minimal constants are $m = 1$, $k = n + 1$. □

Application of algebraic commitments. The motivation behind algebraic commitments is that most of their properties can be expressed in terms of membership or non-membership to certain linear subspaces. We consider such commitment schemes *QA-NIZK-friendly*, since they perfectly combine with QA-NIZK arguments for linear spaces.

Several QA-NIZK arguments in the literature describe the same structure that we describe in the following, given a relation $\mathcal{R}_{\mathcal{L}}$ for a language $\mathcal{L} \in \mathsf{NP}$:

1. An algebraic perfectly binding commitment COM of some vector $\boldsymbol{w}$.
2. An $[\cdot]_\iota$-extractable, SB and ISH algebraic commitment scheme COM' of $\boldsymbol{w}$.
3. An efficient QA-NIZK argument scheme $\mathit{\Pi}'$ for the opening of COM' is valid witness of some statement $\boldsymbol{x}$ such that $\mathcal{R}_{\mathcal{L}}(\boldsymbol{x}, \boldsymbol{w}) = 1$.
4. An efficient QA-NIZK argument system $\mathit{\Pi}$ of same opening of COM and COM' ([KW15, GHR15]).

The first commitment COM is linear in n and uniquely defines the witness vector. On the other hand, COM' provides extraction of q values of the witness in the security proof of the argument $\mathit{\Pi}'$. Finally, once $\mathit{\Pi}'$ is proven, $\mathit{\Pi}$ implies that the opening of COM also satisfies the relation $\mathcal{R}_{\mathcal{L}}$.

Properties 1, 2, 4 can be proven using a single QA-NIZK argument of constant size with an adequate matrix, which is more efficient since QA-NIZK arguments are constant proofs. Furthermore, extra linear conditions can be aggregated using the same argument by adding necessary rows to the parametrized matrix that defines the linear space of the language.

4.2 The EMP Commitment Scheme

González et al. [GHR15] proposed a variant of the standard vector Pedersen commitment scheme [Ped92], calling it *Extended Multi-Pedersen* (EMP) in [GR16]. In this section, we will depict a general version of the EMP commitment scheme (González *et al.* [GR16] mostly considered the case $q = 1$; they also did not formalize its security by using notions like ISH) in group $\mathbb{G}$. We redefine EMP by using a division of the generator matrix $\boldsymbol{g}$ as a product of two matrices $\boldsymbol{R}$ and $\boldsymbol{M}$; this representation results in very short security proofs for EMP. To simplify notation, we will write Ext instead of $\mathsf{Ext}_{[\cdot]}$. We use a distribution $\mathcal{D}_{q+1}^{p,n,\mathcal{S}}$ that outputs $n+1$ vectors $\boldsymbol{g}^{(i)}$, such that if $i \in \mathcal{S}' = \mathcal{S} \cup \{n+1\}$ then $\boldsymbol{g}^{(i)}$ is distributed uniformly over $\mathbb{Z}_p^{q+1}$, and otherwise $\boldsymbol{g}^{(i)}$ is a random element from the span of $\boldsymbol{g}^{(n+1)}$.[4]

Definition 2. *Let $p = p(\lambda)$, $n = \mathsf{poly}(\lambda)$, and let $q \leq n$ be a small positive integer. Let $\mathcal{S} \subseteq [1\,..\,n]$ with $|\mathcal{S}| \leq q$. Then the distribution $\mathcal{D}_{q+1}^{p,n,\mathcal{S}}$ is defined*

[4] We use dimensions with $+1$ like $q + 1$ and $n + 1$ since in later uses of EMP, $+1$ corresponds to the randomizer.

as the first part of $\mathcal{D}_{gen}(p, n, \mathcal{S}, q)$ in Fig. 1 (i.e., just $\boldsymbol{g}$, without the associated extraction key or trapdoor).

We note that [GR16] uses a distribution $\mathcal{D}_{q+1,k}$ instead of the uniform distribution $\mathcal{U}_{q+1}$ over $\mathbb{Z}_p^{q+1}$. This means that taking a larger k gives a weaker security assumption in return of worse efficiency. Our version of EMP also works with a general distribution, but for ease of presentation we only use the distribution $\mathcal{U}_{q+1}$.

```
$\mathcal{D}_{gen}(p, n, \mathcal{S}, q)$
$\mathcal{S}' \leftarrow \mathcal{S} \cup \{n+1\}$; // $\mathcal{S}' = \{\sigma_1, \ldots, \sigma_{q+1}\}$
$\boldsymbol{R} \leftarrow_{\$} \mathbb{Z}_p^{(q+1)\times(q+1)}$; $\boldsymbol{M} \leftarrow \mathbf{0}_{(q+1)\times(n+1)}$; $M_{q+1,n+1} \leftarrow 1$;
for $j = 1$ to $n$ do
  if $j \notin \mathcal{S}'$ then $M_{q+1,j} = \delta_j \leftarrow_{\$} \mathbb{Z}_p$; else let $i$ be such that $j = \sigma_i$; $M_{i,\sigma_i} \leftarrow 1$;
endfor
$\boldsymbol{g} \leftarrow \boldsymbol{RM}$; tk $\leftarrow (\delta_j)_{j \in [1\,..\,n] \setminus \mathcal{S}}$; // $\boldsymbol{g} \in \mathbb{Z}_p^{(q+1)\times(n+1)}$;
return $(\boldsymbol{g}, \boldsymbol{R}, \mathtt{tk})$;
```

Fig. 1. The algorithm generating $\mathcal{D}_{q+1}^{p,n,\mathcal{S}}$, with associated extraction key $\boldsymbol{R}$ and trapdoor `tk`

Example 1. In the Groth-Sahai commitment scheme, $n = q = 1$, so $\mathcal{D}_{gen}$ first samples $\boldsymbol{R} = \left(\begin{smallmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{smallmatrix}\right) \leftarrow_{\$} \mathbb{Z}_p^{2\times 2}$. If $\mathcal{S} = \{1\}$ then $\boldsymbol{M} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\boldsymbol{g} = \boldsymbol{RM} = \left(\begin{smallmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{smallmatrix}\right)$. On the other hand, if $\mathcal{S} = \emptyset$, then $\boldsymbol{M} = \left(\begin{smallmatrix} 0 & 0 \\ \delta_1 & 1 \end{smallmatrix}\right)$ and $\boldsymbol{g} = \boldsymbol{RM} = \left(\begin{smallmatrix} \delta_1 r_{12} & r_{12} \\ \delta_1 r_{22} & r_{22} \end{smallmatrix}\right)$, for $\delta_1 \leftarrow_{\$} \mathbb{Z}_p$.

Consider the case $n = 3$, $q = 2$, and $\mathcal{S} = \{3\}$. Then

$$\boldsymbol{M} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \delta_1 & \delta_2 & 0 & 1 \end{pmatrix} \ , \ \boldsymbol{g} = \boldsymbol{RM} = \begin{pmatrix} \delta_1 r_{13} & \delta_2 r_{13} & r_{11} & r_{13} \\ \delta_1 r_{23} & \delta_2 r_{23} & r_{21} & r_{23} \\ \delta_1 r_{33} & \delta_2 r_{33} & r_{31} & r_{33} \end{pmatrix} \ ,$$

for $\delta_1, \delta_2 \leftarrow_{\$} \mathbb{Z}_p$, $\boldsymbol{R} \leftarrow_{\$} \mathbb{Z}_p^{3\times 3}$.

The following lemma shows that distributions $[\mathcal{D}_{q+1}^{p,n,\mathcal{S}}]$ for different sets $\mathcal{S}$ are indistinguishable under the MDDH assumption. See Appendix B.3 for a proof.

Lemma 4. *Let $\iota \in \{1, 2\}$. Let $p = p(\lambda)$ be created by $\mathsf{Pgen}(1^\lambda)$, $n = \mathsf{poly}(\lambda)$, and let $q \leq n$ be a positive integer. Let $\mathcal{S} \subseteq [1\,..\,n]$ with $|\mathcal{S}| \leq q$. The distribution families $\mathcal{D}^0 := \{[\mathcal{D}_{q+1}^{p,n,\mathcal{S}}]\}_\lambda$ and $\mathcal{D}^1 := \{[\mathcal{D}_{q+1}^{p,n,\emptyset}]\}_\lambda$ are computationally indistinguishable under the $\mathcal{U}_{q+1}$-MDDH$_{\mathbb{G}_\iota}$ assumption relative to Pgen: for any PPT $\mathcal{A}$, there exists a PPT $\mathcal{B}$, such that $\mathsf{Adv}^{\mathrm{indist}}_{\mathcal{A},\mathcal{D}^0,\mathcal{D}^1}(\lambda) \leq |\mathcal{S}| \cdot \mathsf{Adv}^{\mathrm{mddh}}_{\mathcal{B},\mathcal{U}_{q+1},\mathsf{Pgen}}(\lambda)$.*

We define EMP in Fig. 2. We show that it is indeed an SSB commitment scheme.

Theorem 2. *Let Pgen_{bg} be a bilinear group generator. Fix λ, n, and q. The EMP commitment scheme is (i) ISH under the $\mathcal{U}_{(q+1)\times(n+1)}$-MDDH$_{\mathbb{G}_\iota}$ assumption, (ii) F-SSE for $F = [\cdot]$ (thus, F depends on p), (iii) AEPT, (iv) SPB, (v) AEPH, (vi) CB and CH under the $\mathcal{U}_{(q+1)\times(n+1)}$-MDDH$_{\mathbb{G}_\iota}$ assumption.*

```
$\mathsf{KC}(\mathsf{p}, n, q, \mathcal{S})$: // $\mathcal{S} \subseteq \{1, 2, \ldots, n\}$ with $|\mathcal{S}| \leq q$
    Sample $(\boldsymbol{g}, \boldsymbol{R}, \mathtt{tk}_\iota) \leftarrow_{\$} \mathcal{D}_{gen}(p, n, \mathcal{S}, q)$ s.t. $\boldsymbol{R}$ has full rank;
    $\mathtt{ck} \leftarrow [\boldsymbol{g}]; \mathtt{ek} \leftarrow \boldsymbol{R};$ // $\boldsymbol{g} \in \mathbb{Z}_p^{(q+1)\times(n+1)}$, $\boldsymbol{R} \in \mathbb{Z}_p^{(q+1)\times(q+1)}$
    $\mathtt{td} \leftarrow (\mathtt{ek}, \mathtt{tk});$ return $(\mathtt{ck}, \mathtt{td})$;

$\mathsf{tdOpen}(\mathsf{p}, \mathtt{tk}_\iota; \boldsymbol{x}, r, \boldsymbol{x}^*)$
    $r^* \leftarrow \sum_{i \in [1\,..\,n] \setminus \mathcal{S}} (x_i - x_i^*)\delta_i + r$;
    return $r^*$;

$\mathsf{Ext}(\mathsf{p}, \mathsf{ek}; [\mathbf{c}])$
    $[\boldsymbol{x}'] \leftarrow \boldsymbol{R}^{-1}[\mathbf{c}]$;
    return $[\boldsymbol{x}_{\mathcal{S}}] \leftarrow [\boldsymbol{x}'_{[1\,..\,|\mathcal{S}|]}]$;

$\mathsf{Com}(\mathsf{ck}; \boldsymbol{x} \in \mathbb{Z}_p^n; r \in \mathbb{Z}_p)$
    return $[\boldsymbol{g}]\binom{\boldsymbol{x}}{r}$; // $= \sum_{j=1}^n x_j [\boldsymbol{g}^{(j)}] + r[\boldsymbol{g}^{(n+1)}] \in \mathbb{G}^{q+1}$
```

Fig. 2. The EMP commitment scheme COM

Proof. **(i: ISH)** Due to the properties of $\mathcal{D}_{q+1}^{p,n,\mathcal{S}}$, $\boldsymbol{g}^{(\mathcal{S} \cup \{n+1\})}$ has columns distributed uniformly over $\mathbb{Z}_p^{q+1}$ and hence by the Schwartz-Zippel lemma has full rank with probability $\geq 1 - (q+1)/p$. It follows from Lemma 4 that for any PPT $\mathcal{A}$, there exists a PPT $\mathcal{B}$, such that $\mathsf{Adv}^{\mathrm{ish}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) \leq q \cdot \mathsf{Adv}^{\mathrm{mddh}}_{\mathcal{B},\mathcal{U}_{(q+1)\times(n+1)},\iota,\mathsf{Pgen}}(\lambda) + (q+1)/p$.

(ii: $[\cdot]$-SSE) We have $[\mathbf{c}] = [\boldsymbol{g}]\binom{\boldsymbol{x}}{r} = [\boldsymbol{R}\boldsymbol{M}]\binom{\boldsymbol{x}}{r}$ for *some* $\binom{\boldsymbol{x}}{r}$, where $\boldsymbol{R}$ has full rank. But then $[\boldsymbol{x}'] = \boldsymbol{R}^{-1}[\mathbf{c}] = [\boldsymbol{M}]\binom{\boldsymbol{x}}{r}$. Let $\mathcal{S} = \{\sigma_i\}$. By the definition of $\boldsymbol{M}$, clearly $x'_i = \boldsymbol{M}_i\binom{\boldsymbol{x}}{r} = x_{\sigma_i}$ for $i \leq |\mathcal{S}|$.

(iii: AEPT) Let $\boldsymbol{x} \neq \boldsymbol{x}^*$ but $\boldsymbol{x}_{\mathcal{S}} = \boldsymbol{x}^*_{\mathcal{S}}$. Then $\mathsf{Com}(\mathsf{ck}; \boldsymbol{x}; r) - \mathsf{Com}(\mathsf{ck}; \boldsymbol{x}^*; r^*) = \boldsymbol{R}\boldsymbol{M}\binom{\boldsymbol{x}-\boldsymbol{x}^*}{r-r^*} = \boldsymbol{R}\binom{\mathbf{0}_q}{\sum_{i \in [1\,..\,n] \setminus \mathcal{S}} (x_i - x_i^*)\delta_i + (r - r^*)} = \mathbf{0}_{q+1}$, since from tdOpen, $r^* = \sum_{i \in [1\,..\,n] \setminus \mathcal{S}} (x_i - x_i^*)\delta_i + r$.

(iv: SPB) Since $F = [\cdot]$ is injective (because the bilinear group has a prime order), this follows from Item ii and Lemma 1.

(v: AEPH) Let $\boldsymbol{x}, \boldsymbol{x}^*$ be such that $\boldsymbol{x}_{\mathcal{S}} = \boldsymbol{x}^*_{\mathcal{S}}$. Then $\boldsymbol{M}\binom{\boldsymbol{x}}{r} = (\boldsymbol{x}_{\mathcal{S}}^\top, 0, \ldots, 0, r + \sum_{i \in [1\,..\,n] \setminus \mathcal{S}} x_i \sigma_i)^\top$ and similarly $\boldsymbol{M}\binom{\boldsymbol{x}^*}{r^*} = ((\boldsymbol{x}^*_{\mathcal{S}})^\top, 0, \ldots, 0, r^* + \sum_{i \in [1\,..\,n] \setminus \mathcal{S}} x_i^* \sigma_i)^\top$. Thus, both have first q elements equal and the last element is uniformly random. Clearly then also $\mathsf{Com}(\mathsf{ck}; \boldsymbol{x}; r) = \boldsymbol{R}\boldsymbol{M}\binom{\boldsymbol{x}}{r}$ and $\mathsf{Com}(\mathsf{ck}; \boldsymbol{x}^*; r^*) = \boldsymbol{R}\boldsymbol{M}\binom{\boldsymbol{x}^*}{r^*}$ are indistinguishable.

(vi: CB and CH): Follows from Theorem 1, Item i, SPB and AEPH. □

5 Functional SSB Commitments

In this section we generalize the notion of SSB commitment from being statistically binding on an index-set $\mathcal{S} \subseteq [1\,..\,n]$ to being statistically binding on outputs of the functions $\{f_i\}_{i=1}^q$ from some function family $\mathcal{F}$. We construct a functional SSB commitment for the case when $\mathcal{F}$ is the set of linear functions. In particular, this covers functions $f_j(\boldsymbol{x}) = x_j$ and hence we also have the index-set functionality of EMP commitment. We show this can be straight-forwardly used to get oblivious linear function evaluation (OLE) [DKM12, GNN17, DGN+17]

```
$\mathsf{KC}_\iota(\mathsf{p}, n, q, \boldsymbol{M} \in \mathbb{Z}_p^{q \times n})$:
    Set implicitly $\mathtt{MSP} = \mathtt{RSP} = \mathbb{Z}_p^n$ and $\mathtt{CSP} = \mathbb{G}_\iota^{q+1}$;
    Sample $\boldsymbol{R} \leftarrow_\$ \mathbb{Z}_p^{(q+1)\times(q+1)}$ so that it has full rank;
    Sample $\boldsymbol{r} \leftarrow_\$ \mathbb{Z}_p^n$;
    Set $\boldsymbol{M}' \leftarrow \left(\begin{smallmatrix} \boldsymbol{M} & \boldsymbol{0} \\ \boldsymbol{r}^\intercal & 1 \end{smallmatrix}\right) \in \mathbb{Z}_p^{(q+1)\times(n+1)}$;
    $\mathtt{ck} \leftarrow [\boldsymbol{R}\boldsymbol{M}']_\iota \in \mathbb{G}_\iota^{(q+1)\times(n+1)}$;
    $\mathtt{td} \leftarrow (\mathtt{ek} \leftarrow \boldsymbol{R}^{-1}, \mathtt{tk} \leftarrow \boldsymbol{r})$; return $(\mathtt{ck}, \mathtt{td})$;

$\mathsf{Com}(\mathtt{ck}; \boldsymbol{x} \in \mathbb{Z}_p^n; r \in \mathbb{Z}_p)$
    return $\mathtt{ck}\left(\begin{smallmatrix} \boldsymbol{x} \\ r \end{smallmatrix}\right)$;

$\mathsf{tdOpen}(\mathsf{p}, \mathtt{tk}_\iota; \boldsymbol{x}, r, \boldsymbol{x}^*)$ // $\boldsymbol{M}\boldsymbol{x} = \boldsymbol{M}\boldsymbol{x}^*$
    $r^* \leftarrow \sum_{i \in [1 \,..\, n]} (x_i - x_i^*)\mathtt{tk}_i + r$;
    return $r^*$;

$\mathsf{CKV}(n, q, \mathtt{ck} = [\boldsymbol{g}]_\iota)$
    return $\mathtt{ck} \overset{?}{\in} \mathbb{G}_\iota^{(q+1)\times(n+1)}$
    $\wedge\, [\boldsymbol{g}^{(n+1)}]_\iota \neq [\boldsymbol{0}]_\iota$;

$\mathsf{Ext}(\mathsf{p}, \mathtt{ek}; [\mathbf{c}]_\iota)$
    return $\mathtt{ek}[\boldsymbol{c}]_\iota$ without the last element;
```

Fig. 3. Functional SSB commitment for linear functions

and oblivious database query (ODQ). OLE allows the receiver to learn $f(\boldsymbol{x})$ where $\boldsymbol{x}$ is the receiver's private vector and f is the sender's private linear function. ODQ essentially switches the roles of receiver and sender: the receiver wants to learn $f(\boldsymbol{x})$ where $\boldsymbol{x}$ is the sender's private database and f is the receiver's linear query function. Moreover, we allow batch evaluation of queries in ODQ. In Section 7, we construct a QA-NIZK with a linear SSB commitment.

In our definition, given a family of functions $\mathcal{F}$ we require that the commitment key $\mathtt{ck}$ will hide the functions $\{f_i\}_{i=1}^q \subset \mathcal{F}$ and given a commitment $\mathsf{Com}(\mathtt{ck}; \boldsymbol{x}; r)$ and an extraction key $\mathtt{ek}$ it is possible to F-extract $f_i(\boldsymbol{x})$ for $i \in [1 \,..\, q]$. The commitment uniquely determines the outputs of the functions (due to the SSB property) and commitments to messages which produce equal function outputs are statistically indistinguishable (due to the AESH property). Our definition is similar to Döttling et al.'s [DGI$^+$19] definition for trapdoor hash functions for a family of predicates $\mathcal{F}$.

Definition of functional SSB. An *F-extractable functional SSB commitment scheme* $\mathsf{COM} = (\mathsf{Pgen}, \mathsf{KC}, \mathsf{CKV}, \mathsf{Com}, \mathsf{tdOpen}, \mathsf{Ext}_F)$ for a function family $\mathcal{F}$ follows the definitions of SSB commitments in Section 3.1, but with the following changes: (i) $\mathcal{S}$ is now a set of functions rather than a set of indices. (ISH then becomes function set hiding (FSH)). (ii) For $\mathcal{S} = \{f_i\}_{i=1}^q \subseteq \mathcal{F}$ and vector $\boldsymbol{x}$ we redefine $\boldsymbol{x}_\mathcal{S} := (f_1(\boldsymbol{x}), \ldots, f_q(\boldsymbol{x}))$. The full definitions are given in Appendix C.1. Relations that hold between properties of SSB commitments also hold for functional SSB commitments; the proofs are very similar.

Linear EMP. We construct a functional SSB commitment for a family of linear functions $\mathcal{F}$. Our construction follows the ideas in [DGP$^+$19] although they never formalized it as a commitment scheme and only dealt with some concrete functions.

We represent q linear functions by a matrix $\boldsymbol{M} \in \mathbb{Z}_p^{q \times n}$ where each row of the matrix contains coefficients of one function. From a commitment to vector $\boldsymbol{x} \in \mathbb{Z}_p^n$, our construction allows to extract $[\boldsymbol{M}\boldsymbol{x}]_\iota$. In particular, if we take $\boldsymbol{M} = (\boldsymbol{e}_{i_1} | \dots | \boldsymbol{e}_{i_q})^\top$ where $\boldsymbol{e}_{i_j} \in \mathbb{Z}_p^n$ is the i_jth unit vector, then $[\boldsymbol{M}\boldsymbol{x}]_\iota = (x_{i_1}, \dots, x_{i_q})^\top$. A detailed construction is given in Fig. 3. Moreover, if we take an ACSP, the commitment key is $\mathtt{ck} = [\boldsymbol{U}_1, \boldsymbol{U}_2]_\iota \in \mathbb{G}_\iota^{(q+1) \times n} \times \mathbb{G}_\iota^{(q+1) \times 1}$, which is optimal size for extraction in q coordinates.

There are only two differences with the EMP construction in Section 4.2:

(i) in EMP $\boldsymbol{M}$ is a matrix in reduced row echelon form (with multiples of the column vector $(0, \dots, 0, 1)^T$ possibly inserted in between), and

(ii) functional SSB also has a key verification algorithm CKV which guarantees security even if the commitment key generators are untrusted (see Theorem 6).

Key verification is not possible with EMP precisely because we would need to show that $\boldsymbol{M}$ is a matrix with a very specific structure. For functional SSB we only need to know that $\mathtt{ck} = [\boldsymbol{g}]_\iota$ has the correct size and non-zero last column. This turns out to be sufficient to show that the commitment key is well-formed and an unbounded extractor can extract some suitable matrix $\boldsymbol{M}$ which will define the linear functions. We prove security of linear EMP in Appendix C.2.

6 Application of Functional SSB Commitments: ODQ & OLE

A very straight-forward application of linear EMP is oblivious database queries (ODQ). We consider a scenario where the sender knows a private database $\boldsymbol{x}$ and the receiver knows a set of private linear functions $f_i(X_1, \dots, X_n) = b_i + \sum_{j=1}^n a_{i,j} X_j$ for $i \in [1 \mathinner{..} q]$ that he wants to evaluate on that database.

Our ODQ protocol works as follows:

- Receiver defines matrices $\boldsymbol{A} = (a_{ij}) \in \mathbb{Z}_p^{q \times n}$, $\boldsymbol{B} = \mathrm{diag}(b_1, \dots, b_q) \in \mathbb{Z}_p^{q \times q}$, and constructs a matrix $\boldsymbol{M} = (\boldsymbol{A} \mid \boldsymbol{B}) \in \mathbb{Z}_p^{q \times (n+q)}$. Following the KC algorithm it creates the commitment key $\mathtt{ck}$, the extraction key $\mathtt{ek}$, and sends $\mathtt{ck}$ to the sender.
- Sender has $\boldsymbol{x} \in \mathbb{Z}_p^n$ and $\mathtt{ck}$ as input. It sets $\boldsymbol{x}' = \left(\begin{smallmatrix}\boldsymbol{x} \\ \mathbf{1}_q\end{smallmatrix}\right)$, picks random $r \leftarrow_{\$} \mathbb{Z}_p$ and sends $\mathsf{COM} = \mathtt{ck} \left(\begin{smallmatrix}\boldsymbol{x}' \\ r\end{smallmatrix}\right)$ to the receiver.
- Receiver extracts $[\boldsymbol{M} \cdot \boldsymbol{x}']$ from COM using the Ext algorithm with $\mathtt{ek}$.

Privacy and Correctness. We follow privacy and correctness definitions proposed by Döttling et al. [DGI+19] (see Section 5.1 of their paper for full definitions). From the SSE property we know that the receiver can recover $[\boldsymbol{M} \left(\begin{smallmatrix}\boldsymbol{x} \\ \mathbf{1}_q\end{smallmatrix}\right)]_\iota = [\boldsymbol{A}\boldsymbol{x} + \boldsymbol{b}]_\iota$ and thus correctness holds. Receiver's (computational) privacy follows directly from the FSH property, that is, any two function sets of size at most q are indistinguishable. Sender's privacy is defined through simulatability of the protocol transcript given only receiver's input $\boldsymbol{M}$ and receiver's output $[\boldsymbol{M}\boldsymbol{x}']$ to the simulator. Simulatability is slightly stronger than the AEPH property but still holds for linear EMP commitments. As a first message, the simulator can generate ck with $\boldsymbol{M}$ and store $\boldsymbol{R}$. An honestly computed second message has the form

$$[\boldsymbol{R}\left(\begin{smallmatrix}\boldsymbol{M} & \boldsymbol{0}\\ \boldsymbol{r}^\intercal & 1\end{smallmatrix}\right)]\left(\begin{smallmatrix}\boldsymbol{x}'\\ r\end{smallmatrix}\right) = \boldsymbol{R}\left[\begin{smallmatrix}\boldsymbol{M}\boldsymbol{x}'\\ \boldsymbol{x}'\boldsymbol{r}^\top + r\end{smallmatrix}\right]$$

and therefore we can simulate it by sampling $r^* \leftarrow_\$ \mathbb{Z}_p$ and computing $\boldsymbol{R}\left(\begin{smallmatrix}[\boldsymbol{M}\boldsymbol{x}']\\ r^*\end{smallmatrix}\right)$. Thus sender's privacy also holds.

Efficiency. We define download rate as the ratio between output size and sender's message and total rate as the ratio between output size and total transcript size. The total rate of our protocol is $|[\boldsymbol{M}\boldsymbol{x}']|/(|\mathsf{ck}| + |\mathsf{COM}|) = q/((n+q+2)(q+1))$. However, we achieve very good download rate $|[\boldsymbol{M}\boldsymbol{x}']|/|\mathsf{COM}| = q/(q+1)$ which tends to 1. This is similar to Döttling et al. [DGI+19] where they achieve an optimal download rate but sub-optimal total rate.

OLE. We can achieve OLE in a very similar way. Suppose that now the sender has a function $f(X_1, \dots, X_n) = b + \sum_{i=1}^n a_i X_i$ and the receiver has $\boldsymbol{x}$. Then the receiver can send a commitment key with $\boldsymbol{M} = (x_1, \dots, x_n, 1)$ and the sender responds with a commitment to $(a_1, \dots, a_n, b)$. The receiver extracts to obtain $[f(\boldsymbol{x})]_\iota$. The proof is identical to the ODQ case. However, the resulting OLE is less efficient with download rate $1/2$ and total rate $1/(2n+4)$.

7 Application: QA-NIZK Argument for Quadratic Equations

We present a QA-NIZK argument which uses functional SSB commitments as an important technical tool in the security proof. Daza et al. [DGP+19] presented a commit-and-prove QA-NIZK argument for square span programs (SSP, [DFGK14]) which can be used to encode the Boolean circuit satisfiability language. Their construction uses a specific setting of linear EMP commitments without explicitly formalizing it. Our QA-NIZK is for square arithmetic programs (SAP) [GM17] which can be used to encode the arithmetic circuit satisfiability language and follows a similar overall strategy. However, we use the linear EMP commitment scheme as a black-box and thus have a more compact and clear presentation. Our argument has roughly the same complexity as the argument in [DGP+19]: both have a linear-length perfectly binding commitment of the witness, a succinct argument, and a security proof based on falsifiable assumptions. The proof size in the original construction in [DGP+19] is 4 elements in $\mathbb{G}_1$ and 6 elements in $\mathbb{G}_2$, while our construction's proof size is 5 elements in $\mathbb{G}_1$ and 7 elements in $\mathbb{G}_2$.

A rough intuition of our commit-and-prove QA-NIZK is as follows. The statement of our language contains a linear-length perfectly binding (and $[\cdot]_1$-extractable) commitment $[\boldsymbol{c}]_1$ of the SAP witness. For simplicity, we use ElGamal encryption in this role. As is usual for commit-and-prove arguments, $[\boldsymbol{c}]_1$ can be reused for many different SAP relations. The commitment key is going to be a parameter for the QA-NIZK language. The argument itself is succinct and contains the following elements:

- A succinct SNARK-type argument $[V, H, W]_1$, $[V]_2$ for the SAP relation that would typically be only secure under some knowledge assumption.
- A succinct linear EMP commitment $[\tilde{\boldsymbol{c}}]_2$ that commits to the SAP witness and to the randomness of the SNARK proof.
- A succinct linear subspace argument [GHR15] that shows that commitments open to consistent values. In particular, it guarantees that the opening of the perfectly binding commitment $[\boldsymbol{c}]_1$ is also used in the SNARK proof and in $[\tilde{\boldsymbol{c}}]_2$.

We use extractability of $[\boldsymbol{c}]_1$ and $[\tilde{\boldsymbol{c}}]_2$ to avoid non-falsifiable assumptions. The linear EMP commitment is in perfectly hiding mode in the honest proof ($\mathcal{S} = \emptyset$). Intuitively, in the security reduction we need to compute some elements of the form $[\sum_i a_i y_i]_2$ where $(a_1, \ldots, a_n)$ is the witness and $[y_1, \ldots, y_n]_2$ are elements that can be computed from the challenge of some falsifiable assumption. Since our perfectly binding commitment is only $[\cdot]_1$-extractable, we can at best extract $[a_i]_1$ which is not enough to break the assumption. Instead, in the security games we switch the EMP commitment key from the perfectly hiding mode to the mode that encodes the function $f(a_1, \ldots, a_n) = \sum_i a_i [y_i]_2$ (the commitment keys are indistinguishable due to the FSH property) and thus we can extract $[\sum_i a_i y_i]_2$ from $[\tilde{\boldsymbol{c}}]_2$. As we will see, the actual reduction requires us to extract multiple such linear combinations.

7.1 Preliminaries

Perfectly binding commitment. We are going to use ElGamal encryption as our perfectly binding commitment. In particular, the commitment key is $\mathtt{ck} = [\boldsymbol{u}]_1 = [1, u]_1^\top$ where $u \leftarrow_\$ \mathbb{Z}_p$ and $\mathsf{Com}_{\mathtt{ck}}(\boldsymbol{a} \in \mathbb{Z}_p^n; \boldsymbol{r} \in \mathbb{Z}_p^n) = ([\boldsymbol{c}_1]_1, \ldots, [\boldsymbol{c}_n]_1)$ where $[\boldsymbol{c}_i]_1 = ([r_i]_1, [a_i]_1 + r_i[u]_1)^\top$ and $\boldsymbol{r} \leftarrow_\$ \mathbb{Z}_p^n$. In matrix form $[\boldsymbol{c}_i]_1 = a_i[\boldsymbol{e}_2]_1 + r_i[\boldsymbol{u}]_1$ where $\boldsymbol{e}_2 = (0, 1)^\top$. To extract the message, we can simply decrypt each individual ciphertext, that is $[a_i]_1 = [c_{i,2}]_1 - u[c_{i,1}]_1$ where $[\boldsymbol{c}_i]_1 = [c_{i,1}, c_{i,2}]_1^\top$. Note that we can only $[\cdot]_1$-extract and cannot recover a_i itself.

Square Arithmetic Program (SAP). A square arithmetic program is a tuple $\mathtt{SAP} = (\mathsf{p}, n, d, \mathbf{V} \in \mathbb{Z}_p^{n \times d}, \mathbf{W} \in \mathbb{Z}_p^{n \times d})$. We define a commit-and-prove language for $\mathtt{SAP}$ as the following language with n variables and d quadratic equations

$$\mathscr{L}_{\mathtt{SAP},\mathtt{ck}} = \left\{ [\boldsymbol{c}]_1 \in \mathbb{G}_1^{2n} \;\middle|\; \begin{array}{c} \exists \boldsymbol{a}, \boldsymbol{r} \in \mathbb{Z}_p^n \colon [\boldsymbol{c}]_1 = \mathsf{Com}_{ck}(\boldsymbol{a}, \boldsymbol{r}) \wedge \\ \left\{ \left(\boldsymbol{a}^\top \boldsymbol{v}_j\right)^2 - \boldsymbol{a}^\top \boldsymbol{w}_j = 0 \right\}_{j=1}^{d} \end{array} \right\}$$

where Com_{ck} is a perfectly binding commitment scheme, $\boldsymbol{v}_j$ is j-th column of the matrix $\boldsymbol{V}$ and $\boldsymbol{w}_j$ is the j-th column of the matrix $\boldsymbol{W}$. We note that satisfiability of any arithmetic circuit can be encoded in this form [GM17].

SNARK for SAP. Let $\chi_1, \ldots, \chi_d \in \mathbb{Z}_p$ be unique interpolation points. We define

$$v(X) = \sum_{i=1}^{n} a_i v_i(X), \quad w(X) = \sum_{i=1}^{n} a_i w_i(X) \tag{1}$$

where $v_i(X)$, $w_i(X)$ are polynomials of degree less than d such that $v_i(\chi_j) = v_{ij}$ and $w_i(\chi_j) = -w_{ij}$. Moreover, let us define $p(X) = v(X)^2 - w(X)$ and $t(X) = \prod_{j=1}^{d}(X - \chi_j)$. We have that $p(\chi_j) = (\boldsymbol{a}^\top \boldsymbol{v}_j)^2 - \boldsymbol{a}^\top \boldsymbol{w}_j$ and thus the j-th SAP equation is satified exactly when χ_j is a root of $p(X)$. In particular, when all interpolation points are roots of $p(X)$, then $t(X)$ divides $p(X)$ and all the SAP equations are satisfied.

We can use these polynomial representations to construct a SNARK. Our CRS will contain $\{[s^i]_{1,2}\}_{i=1}^{d}$ where $s \leftarrow_\$ \mathbb{Z}_p$ is a secret point. The prover will compute $[V]_{1,2} = [V(s)]_{1,2}$, $[W]_1 = [W(s)]_1$ and $[H]_1 = [H(s)]_1$ where $V(X) = v(X) + \delta_v t(X)$, $W(X) = w(X) + \delta_w t(X)$, and $H(X) = (V(X)^2 - W(X))/t(X)$. Elements δ_v and δ_w are picked randomly to hide the witness. The verifier checks that the equation $[V]_1[V]_2 - [W]_1[1]_2 = [H]_1[t(s)]_2$ is satisfied. Intuitively, we can use this to show that $t(X)$ divides $P(X) := V(X)^2 - W(X)$. It is easy to see that if $t(X) \mid P(X)$ then also $t(X) \mid p(X)$ and thus the SAP relation is satisfied.

BLS argument. As a subargument, we use a QA-NIZK argument $(\mathsf{K}_{\mathsf{bls}}, \mathsf{P}_{\mathsf{bls}}, \mathsf{V}_{\mathsf{bls}})$ defined in [GHR15] for the bilateral linear subspace (BLS) language $\mathcal{L}_{[\boldsymbol{M}]_1,[\boldsymbol{N}]_2} := \{([\boldsymbol{x}]_1, [\boldsymbol{y}]_2) \mid \exists \boldsymbol{w} \in \mathbb{Z}_p^t : \boldsymbol{x} = \boldsymbol{M}\boldsymbol{w} \wedge \boldsymbol{y} = \boldsymbol{N}\boldsymbol{w}\}$ for $\boldsymbol{M} \in \mathbb{Z}_p^{n \times t}$, $\boldsymbol{N} \in \mathbb{Z}_p^{m \times t}$, to prove that commitments open to the same value. It has perfect completeness, strong quasi-adaptive soundness under the SKer-MDH assumption, and perfect zero-knowledge. The proof size is 2 elements in $\mathbb{G}_1$ and 2 elements in $\mathbb{G}_2$. We refer the reader to the original paper for more details. We leave it as an open question if the slightly more efficient construction by Rafols and Silva [RS20] can be used.

New target assumption. The q-target strong Diffie-Hellman assumption [BB04] says that given $\{[s^i]_{1,2}\}_{i=1}^{q}$ for a random s, it is computationally hard to find $[\nu]_T = [1/(s-r)]_T$ for any $r \in \mathbb{Z}_p$. We generalize this assumption and intuitively say that it is hard to compute $[\nu]_T = [c/(s-r)]_T$ where $r \in \mathbb{Z}_p$ and c is a constant independent of s. In order to satisfy the latter requirement, we include a challenge value $[z]_2$ and let the adversary additionally output $[c]_1$ and $[c']_2$ such that $zc = c'$. Intuitively, then c cannot depend on s^i since otherwise c' should depend on zs^i which is not a part of the challenge. For technical reasons, c in our assumption has a slightly more structured form $\beta_1^2 - \beta_2$.

Definition 3 (q-SATSDH). *The q-Square Arithmetic Target Strong Diffie-Hellman assumption holds relative to* Pgen, *if* $\forall$ *PPT adversaries* $\mathcal{A}$,

$$\Pr\left[\begin{array}{l} \mathsf{p} \leftarrow \mathsf{Pgen}(1^\lambda); s, z \leftarrow_\$ \mathbb{Z}_p; \\ \Big(r, [\beta_1, \beta_2]_1, [\tilde{\beta}_1, \tilde{\beta}_2]_2, [\nu]_T\Big) \leftarrow \mathcal{A}\big(\mathsf{p}, \{[s^i]_{1,2}\}_{i=1}^{q}, [z]_2\big) : \\ \tilde{\beta}_1 = z\beta_1 \wedge \tilde{\beta}_2 = z\beta_2 \wedge \beta_1^2 \neq \beta_2 \wedge \nu = \frac{\beta_1^2 - \beta_2}{s-r} \end{array}\right] \approx_\lambda 0.$$

We prove in Appendix D that our new assumption is falsifiable and equivalent to TSDH assumption under a knowledge assumption.

7.2 Using the SSB functionality in the soundness proof

In the security proof, the soundness game is first changed by randomly picking one of the SAP equations $\left(\boldsymbol{a}^\top \boldsymbol{v}_{j^*}\right)^2 - \boldsymbol{a}^\top \boldsymbol{w}_{j^*} = 0$ for some $j^* \in [1 \mathinner{..} d]$; with probability $\geq 1/d$ this equation does not hold, assuming that the adversary is successful. By the characterization of the SAP, if the j^*-th equation does not hold, then $X - \chi_{j^*} \nmid P(X)$. In particular, let $q_v(X), q_w(X)$ be unique polynomials and $\beta_v, \beta_w \in \mathbb{Z}_p$ be unique values such that $V(X) = q_v(X)(X - \chi_{j^*}) + \beta_v$ and $W(X) = q_w(X)(X - \chi_{j^*}) + \beta_w$. Then we can express the division of $P(X) = V(X)^2 - W(X)$ by $X - \chi_{j^*}$ as follows,

$$\begin{aligned}
P(X) =& V(X)(q_v(X)(X - \chi_{j^*}) + \beta_v) - q_w(X)(X - \chi_{j^*}) - \beta_w \\
=& (X - \chi_{j^*}) \left(V(X) q_v(X) - q_w(X)\right) + V(X)\beta_v - \beta_w \\
=& (X - \chi_{j^*}) \left(V(X) q_v(X) - q_w(X)\right) + (q_v(X)(X - \chi_{j^*}) + \beta_v)\beta_v - \beta_w \\
=& (X - \chi_{j^*}) \left(q_v(X) \left(V(X) + \beta_v\right) - q_w(X)\right) + (\beta_v^2 - \beta_w) \ .
\end{aligned} \tag{2}$$

Since, $X - \chi_{j^*} \nmid P(X)$ we get that $(\beta_v^2 - \beta_w) \neq 0$.

We denote by $\alpha_i(X)$ and $\beta_{v,i}$ the quotient and the remainder of the polynomial division of $v_i(X)$ by $X - \chi_{j^*}$, i.e., $v_i(X) = \alpha_i(X)(X - \chi_{j^*}) + \beta_{v,i}$. Similarly, we can also express $w_i(X) = \hat{\alpha}_i(X)(X - \chi_{j^*}) + \beta_{w,i}$. As a special case, we define $t(X) = \alpha_t(X)(X - \chi_{j^*}) + \beta_t$. The definition of $V(X)$ and Eq. (1) give us

$$V(X) = \left(\sum_{i=1}^{n} a_i \alpha_i(X) + \delta_v \alpha_t\right)(X - \chi_{j^*}) + \sum_{i=1}^{n} a_i \beta_{v,i} + \delta_v \beta_t,$$

and thus

$$q_v(X) = \sum_{i=1}^{n} a_i \alpha_i(X) + \delta_v \alpha_t, \quad \beta_v = \sum_{i=1}^{n} a_i \beta_{v,i} + \delta_v \beta_t. \tag{3}$$

Similarly, we get that

$$q_w(X) = \sum_{i=1}^{n} a_i \hat{\alpha}_i(X) + \delta_w \beta_t, \quad \beta_w = \sum_{i=1}^{n} a_i \beta_{w,i} + \delta_w \beta_t. \tag{4}$$

The security proof extracts the following functions of the witness $\boldsymbol{a}$ and δ_v, δ_w:

- $[q_v(s)]_2 = [\sum_{i=1}^n a_i \alpha_i(s) + \delta_v \beta_t]_2$,
- $[\beta_v z]_2 = [\sum_{i=1}^n a_i z \beta_{v,i} + \delta_v z \beta_t]_2$, and $[\beta_w z]_2 = [\sum_{i=1}^n a_i z \beta_{w,i} + \delta_w z \beta_t]_2$,

where $z, s \in \mathbb{Z}_p$ are secrets of SATSDH assumption. The idea is that we can break the d-SATSDH assumption by computing $[\beta_v]_1 = \sum_{i=1}^n \beta_{v,i}[a_i]_1 + \beta_t[\delta_v]_1$ (note that $[a_i]_1$ and $[\delta_v]_1$ are extractable from the PB commitment and $[V]_1$), $[\beta_w]_1 = \sum_{i=1}^n \beta_{w,i}[a_i]_1 + \beta_t[\delta_w]_1$ and moreover by Eq. (2),

$$\left[\frac{\beta_v^2 - \beta_w}{s - \chi_{j^*}}\right] = \left[\frac{P(s)}{s - \chi_{j^*}}\right]_T - ([V]_1 + [\beta_v]_1)[q_v(s)]_2 + [q_w(s)]_T,$$

where $[\frac{P(s)}{s-\chi_{j^*}}]_T$ can be computed from the verification equation. Together with other extracted elements, this is now enough to break the SATSDH assumption.

We refer to Theorem 4 for more precise details of the reduction.

7.3 QA-NIZK Argument for Arithmetic Quadratic Equations

Given $n, d \in \mathbb{N}$ we construct a QA-NIZK argument for $\mathscr{L}_{\mathsf{SAP},\mathtt{ck}}$.

- $\mathsf{K}_0(\lambda)$ returns $\mathsf{p} \leftarrow \mathsf{Pgen}(1^\lambda)$.
- $\mathcal{D}_{\mathsf{p}}(n, d)$ returns a commitment key $\mathtt{ck} = [\boldsymbol{u}]_1 = [1, u]_1^\top$ where $u \leftarrow_{\$} \mathbb{Z}_p$.
- $\mathsf{K}_1(\mathsf{p}, n, d, \mathtt{ck})$ picks $s \leftarrow_{\$} \mathbb{Z}_p$, then sets $q_v = 3$, $n' = n + 1$, $\boldsymbol{M}_v = \boldsymbol{0} \in \mathbb{Z}_p^{q_v \times n'}$ (i.e., $S_v = \emptyset$) and generates a linear EMP key $\mathtt{ck}' = [\mathbf{K}]_2 \leftarrow \mathsf{KC}_2(\mathsf{p}, n', q_v, \boldsymbol{M}_v) \in \mathbb{G}_2^{4\times(n+2)}$. Finally, it runs $(\mathsf{crs}_{\mathsf{bls}}, \mathsf{td}_{\mathsf{bls}}) \leftarrow \mathsf{K}_{\mathsf{bls}}([\boldsymbol{M}]_1 \in \mathbb{G}_1^{(2n+2)\times(2n+3)}, [\boldsymbol{N}]_2 \in \mathbb{G}_2^{5\times(2n+3)})$ for

$$[\mathbf{M}]_1 = \left[\begin{array}{ccc|ccc|ccc} \boldsymbol{e}_2 & & & \boldsymbol{u} & & & & & \\ & \ddots & & & \ddots & & & \boldsymbol{0} & \\ & & \boldsymbol{e}_2 & & & \boldsymbol{u} & & & \\ \hline v_1(s) & \dots & v_n(s) & & \boldsymbol{0} & & t(s) & 0 & 0 \\ w_1(s) & \dots & w_n(s) & & & & 0 & t(s) & 0 \end{array}\right]_1,$$

$$[\mathbf{N}]_2 = \left[\begin{array}{ccc|c|ccc} v_1(s) & \dots & v_n(s) & \boldsymbol{0} & t(s) & 0 & 0 \\ \mathbf{K}^{(1)} & \dots & \mathbf{K}^{(n)} & & \mathbf{K}^{(n+1)} & 0 & \mathbf{K}^{(n+2)} \end{array}\right]_2.$$

  Return the CRS $\mathtt{crs} = (\mathsf{p}, \mathsf{ck}, \mathsf{ck}', \{[s^i]_{1,2}\}_{i=1}^{d}, \mathsf{crs}_{\mathsf{bls}})$ with trapdoor $(s, \mathsf{td}_{\mathsf{bls}})$.
- The prover P receives an input $(\mathtt{crs}, ([\boldsymbol{c}]_1, \mathbf{V}, \mathbf{W}), (\boldsymbol{a}, \boldsymbol{r}))$. Let $v_i(X)$ and $w_i(X)$ be the interpolation polynomials for the i-th column of $\mathbf{V}$ and $\mathbf{W}$ respectively for $i \in [1 \mathinner{..} n]$, and set $t(X) = \prod_{i=j}^{d}(X - \chi_j)$ where $\{\chi_j\}_j$ are distinct interpolation points. The prover picks $\delta_v, \delta_w, r_v \leftarrow_{\$} \mathbb{Z}_p$ and defines polynomials:

$$\begin{array}{ll} V(X) := \sum_{i=1}^{n} a_i v_i(X) + \delta_v t(X), & W(X) := \sum_{i=1}^{n} a_i w_i(X) + \delta_w t(X) \\ P(X) := V(X)^2 - W(X) & H(X) := P(X)/t(X) \end{array} \quad (5)$$

  The prover computes group elements $[V]_{1,2} = [V(s)]_{1,2}$, $[W]_1 = [W(s)]_1$, $[H]_1 = [H(s)]_1$ and a linear EMP commitment $[\tilde{\boldsymbol{c}}]_2 = \mathsf{Com}(\mathsf{ck}'; (\boldsymbol{a}, \delta_v), r_v)$. All of the above can be computed as a linear combination of the CRS elements, in particular, $H(X)$ is a polynomial of degree $\leq d$. The prover also computes a bls argument ψ for the statement

$$\mathsf{x}_{\mathsf{bls}} := ([\boldsymbol{c}]_1, [V]_1, [W]_1, [V]_2, [\tilde{\boldsymbol{c}}]_2)^\top \in \mathbf{Im}\begin{pmatrix} [\mathbf{M}]_1 \\ [\mathbf{N}]_2 \end{pmatrix}$$

  with witness $(\boldsymbol{a}, \boldsymbol{r}, \delta_v, \delta_w, r_v)^\top \in \mathbb{Z}_p^{2n+3}$. Finally, it outputs the argument $\pi := \left([H]_1, [V]_{1,2}, [W]_1, [\tilde{\boldsymbol{c}}]_2, \psi\right)$.
- The verifier V with input $(\mathtt{crs}, [\boldsymbol{c}]_1, \mathbf{V}, \mathbf{W}, \pi)$ returns 1 if the equation

$$[V]_1[V]_2 - [W]_1[1]_2 = [H]_1[t(s)]_2$$

  holds and $\mathsf{V}_{\mathsf{bls}}(\mathsf{crs}_{\mathsf{bls}}, \mathsf{x}_{\mathsf{bls}}, \psi) = 1$. Otherwise it returns 0.

7.4 Security Proof

The security proof of the argument uses similar techniques as [DGP$^+$19] but it is simplified since we can rely on the properties of SSB commitment. Namely, in the soundness proof we randomly guess $j^* \in [1\,..\,d]$ such that the adversary cheats in the the j^*-th SAP equation, and embed several functions related to this equation to the SSB commitment key. The FSH property guarantees that the prover cannot learn the index j^* and thus the j^*-th SAP equation is not satisfied with probability $\geq 1/d$. The $[\cdot]_2$-SSE property allows us to extract some linear combinations of the claimed witness and break the SATSDH assumption. Zero-knowledge is straightforwardly guaranteed by the AEPH property.

The following two theorems prove the completeness, zero-knowledge, and soundness properties of our QA-NIZK construction.

Theorem 3. *The QA-NIZK argument has perfect completeness and perfect zero-knowledge.*

Proof. Completeness. Since the BLS argument is perfectly complete, we only need to check the last verification equation: the left hand side is $[V]_1[V]_2 - [W]_1[1]_2 = \left[V^2 - W\right]_T = [P(s)]_T$, and the right hand side is $[H]_1[t(s)]_2 = [H(s)]_1[t(s)]_2 = [P(s)]_T$.

Zero-knowledge. We prove it by showing that the proof can be efficiently simulated given the BLS trapdoor $\mathsf{td}_{\mathsf{bls}}$. Since we set $S_v = \emptyset$, then the SSB commitments are perfectly hiding by the AEPH property. Thus we may simulate $[\tilde{\boldsymbol{c}}]_2$ by committing to $\boldsymbol{0}$. Next, V and W are uniformly random and independently distributed in the honest proof. Hence, the simulator can pick $\mu_1, \mu_2 \leftarrow_\$ \mathbb{Z}_p$ and define $[V]_{1,2} = \mu_1[t(s)]_{1,2}$, $[W]_1 = \mu_2[t(s)]_1$. Then, $[H]_1 = \mu_1^2[t(s)]_1 - [\mu_2]_1$ and the verification equation will be satisfied. Finally, the BLS proof ψ can be perfectly simulated (see [GHR15]) using the trapdoor $\mathsf{td}_{\mathsf{bls}}$. □

Theorem 4. *Let $\mathsf{Adv}_{snd}(\mathcal{A})$ be the advantage of any PPT adversary $\mathcal{A}$ against the soundness of the QA-NIZK argument. There exist PPT adversaries $\mathcal{B}_1$ against the DDH assumption in $\mathbb{G}_2$, $\mathcal{B}_2$ against strong soundness of the BLS argument, and $\mathcal{B}_3$ against the d-SATSDH assumption such that*

$$\mathsf{Adv}_{\mathrm{Snd}}(\mathcal{A}) \leq d\big(2\mathsf{Adv}_{\mathsf{DDH},\mathbb{G}_2}(\mathcal{B}_1) + \mathsf{Adv}_{\mathsf{bls}}(\mathcal{B}_2) + \mathsf{Adv}_{d\text{-}\mathsf{SATSDH}}(\mathcal{B}_3)\big).$$

Proof. In order to prove soundness we will prove indistinguishability of the following games.

- Real: This is the real soundness game. The output is 1 if the adversary produces a false accepting proof, i.e., if there is some equation $\left(\boldsymbol{a}^\top \boldsymbol{v}_i\right)^2 - \boldsymbol{a}^\top \boldsymbol{w}_i \neq 0$ and the verifier accepts the proof. Note that $\boldsymbol{a}$ is uniquely determined since commitment $[\boldsymbol{c}]_1$ is perfectly binding.
- Game_0: This game is identical to the previous one, except instead of generating the commitment key as $\mathtt{ck} \leftarrow \mathcal{D}_{\mathsf{p}}(n, d)$, the game samples $u \leftarrow_\$ \mathbb{Z}_p$ himself, sets $\mathtt{ck} = [1, u]_1^\top$, and stores u. Clearly, $\mathcal{A}$'s advantage is the same in Real and Game_0.

- Game_1: This game is identical to the previous one, except that some $j^* \leftarrow_{\$} [1\,..\,d]$ is chosen and the game aborts if $\boldsymbol{a}$ satisfies the j^*-th equation, i.e., $\left(\boldsymbol{a}^\top \boldsymbol{v}_{j^*}\right)^2 - \boldsymbol{a}^\top \boldsymbol{w}_{j^*} = 0$. Note this statement is well-defined since $\boldsymbol{a}$ is uniquely determined by the commitment $[\boldsymbol{c}]_1$.
- Game_2: This game is identical to the previous one except that we change the commitment key ck' by using a different matrix $\mathbf{M}_v \neq \mathbf{0}$ during its generation. For each $i \in [1\,..\,n]$, let us express

$$v_i(X) = \alpha_i(X)(X - \chi_{j^*}) + \beta_{v,i}$$

$$w_i(X) = \hat{\alpha}_i(X)(X - \chi_{j^*}) + \beta_{w,i}$$

and $t(X) = \alpha_t(X)(X - \chi_{j^*}) + \beta_t$. We will pick $[z]_2 \leftarrow_{\$} \mathbb{G}_2$ that is part of the SATSDH challenge and change the EMP commitment key ck' by setting

$$\mathbf{M}_v = \begin{pmatrix} \alpha_1(s) \dots \alpha_n(s) & \alpha_{n+1}(s) \\ \beta_{v,1}z \dots \beta_{v,n}z & 0 \\ \beta_{w,1}z \dots \beta_{w,n}z & 0 \end{pmatrix}.$$

It is important to note that from $\{[s^i]_{1,2}\}_{i=1}^d$ and $[z]_2$ we can only compute $[\mathbf{M}_v]_2$. However, looking at the KC algorithm in Fig. 3, it is clear that ck' can be computed even if only $[\mathbf{M}_v]_2$ is known.

Let us now analyze the games. Obviously, the games Real and Game_0 are indistinguishable.

Lemma 5. $\Pr[\mathsf{Game}_0(\mathcal{A}) = 1] \leq d \cdot \Pr[\mathsf{Game}_1(\mathcal{A}) = 1]$.

Proof. If $\mathcal{A}$ breaks soundness, at least one equation j does not hold. Thus the challenger can guess j with probability at least $\frac{1}{d}$. □

Lemma 6. *There exists an adversary $\mathcal{B}_1$ against DDH in $\mathbb{G}_2$ such that* $|\Pr[\mathsf{Game}_1(\mathcal{A}) = 1] - \Pr[\mathsf{Game}_2(\mathcal{A}) = 1]| \leq 2\mathsf{Adv}_{\mathsf{DDH},\mathbb{G}_2}(\mathcal{B}_1)$.

Proof. Game_1 and Game_2 differ only in the linear EMP commitment key that encode different functions, but these keys are indistinguishable due to the FSH property. In particular, we can bound the advantage of an adversary $\mathcal{B}_1$ against the $DDH_{\mathbb{G}_2}$ assumption as in Theorem 6: $\mathsf{Adv}^{\mathrm{fsh}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) \leq \lceil \log_2(q+1) \rceil \cdot \mathsf{Adv}^{\mathrm{ddh}}_{\mathcal{B}_1,2,\mathsf{Pgen}}(\lambda)$ where in this case $q = 3$. □

Lemma 7. *There exists an adversary $\mathcal{B}_2$ against the strong soundness of the* bls *proof and a d-*SATSDH *adversary $\mathcal{B}_3$ such that*

$$\Pr[\mathsf{Game}_2(\mathcal{A}) = 1] \leq \mathcal{A}_{\mathsf{bls}}(\mathcal{B}_2) + \mathcal{A}_{d\text{-}\mathsf{SATSDH}}(\mathcal{B}_3).$$

Proof. For any adversary $\mathcal{A}$ which breaks soundness, let E be the event that $([\boldsymbol{c}]_1, [V]_1, [W]_1, [V]_2, [\tilde{\boldsymbol{c}}]_2)^\top \in \mathbf{Im}\begin{pmatrix}[\mathbf{M}]_1 \\ [\mathbf{N}]_2\end{pmatrix}$ and $\overline{E}$ be the complementary event. Obviously,

$$\Pr[\mathsf{Game}_3(\mathcal{A}) = 1] \leq \Pr[\mathsf{Game}_3(\mathcal{A}) = 1|E] + \Pr[\mathsf{Game}_3(\mathcal{A}) = 1|\overline{E}]. \qquad (6)$$

For the latter event, we can easily construct from $\mathcal{A}$ a PPT adversary $\mathcal{B}_2$ that breaks strong quasi-adaptive soundness of the BLS argument. Such an adversary receives as an input $(\mathsf{crs}_{\mathsf{bls}}, \varrho = ([\mathbf{M}]_1, [\mathbf{N}]_2), \omega_\rho = (\mathbf{M}, \mathbf{N}))$ sampled according to the distribution specified by Game_3. In particular, $\mathbf{N}$ contains $t(s)$ and thus $\mathcal{B}_2$ can efficiently recover s by finding roots of the polynomial $t(X) - t(s)$. This is sufficient to construct the rest of the CRS chosen in the usual way. Now adversary $\mathcal{B}_2$ can use the output of $\mathcal{A}$ to break the soundness of bls in a straightforward way. Thus, $\Pr[\mathsf{Game}_3(\mathcal{A}) = 1 | \overline{E}] \leq \mathsf{Adv}_{\mathsf{bls}}(\mathcal{B}_2)$.

In the following, we bound the first term of the sum in Eq. (6) by constructing an adversary $\mathcal{B}_3$ which breaks the d-SATSDH assumption in the case that E happens. Note that in this case there exists a witness $(\boldsymbol{a}, \boldsymbol{r}, \delta_v, \delta_w, r_v)^\top$ for membership in $\mathbf{Im}\begin{pmatrix}[\mathbf{M}]_1 \\ [\mathbf{N}]_2\end{pmatrix}$. Furthermore, this witness is unique since

- $[\boldsymbol{c}]_1$ is perfectly binding and thus uniquely fixes $\boldsymbol{a}$ and $\boldsymbol{r}$,
- $[V]_1$ and $\boldsymbol{a}$ uniquely fix δ_v,
- $[W]_1$ and $\boldsymbol{a}$ uniquely fix δ_w, and
- $[\boldsymbol{a}]_1$ and δ_v uniquely fix r_v.

In particular, this uniquely determines the polynomial $P(X) = (v(X) + \delta_v t(X))^2 - w(X) + \delta_w t(X)$.

We now describe the full reduction. Adversary $\mathcal{B}_3$ receives the d-SATSDH assumption challenge $\left(\mathsf{p}, \{\left[s^i\right]_{1,2}\}_{i=1}^q, [z]_2\right)$ and uses this to construct the CRS just as is specified in Game_2. The CRS is then sent to the soundness adversary $\mathcal{A}$ that returns $[\boldsymbol{c}]_1$ and π.

The adversary $\mathcal{B}_3$ extracts $[\boldsymbol{a}]_1, [\delta_v]_1, [\delta_w]_1 \in \mathbb{G}_1$ from $[\boldsymbol{c}]_1$ by using the secret key u and aborts if the j^*-th equation is satisfied. Since verification succeeds, $[V]_1[V]_2 - [W]_T = [H(s)]_1[t(s)]_2$. By the definition of $P(X)$, we have that the left hand side is $[V^2 - W]_T = [P(s)]_T$.

If we divide both sides of the verification equation by $s - \chi_{j^*}$, then

$$\left[\frac{P(s)}{s - \chi_{j^*}}\right]_T = [H]_1 \cdot \left[\frac{t(s)}{s - \chi_{j^*}}\right]_2 = [H]_1 \cdot \left[\prod_{i \neq j^*}(s - \chi_i)\right]_2,$$

so the adversary $\mathcal{B}_3$ can compute $\left[\frac{P(s)}{s - \chi_{j^*}}\right]_T$ from $[H]_1$ and the powers of $[s]_2$ in the CRS. On the other hand, if we use equation (2) on $P(X)$, then

$$\left[\frac{P(s)}{s - \chi_{j^*}}\right]_T = \left[(V(s) + \beta_v)q_v(s) - q_w(s) + \frac{\beta_v^2 - \beta_w}{s - \chi_{j^*}}\right]_T, \tag{7}$$

and we have $\beta_v^2 - \beta_w \neq 0$ (otherwise the j^*-th equation is satisfied, in which case the game aborts). We describe in the following how $\mathcal{B}_3$ can compute the right hand side of Eq. (7) and the elements to break the d-SATSDH Assumption.

According to Eq. (3) and Eq. (4), $\mathcal{B}_3$ can compute $[\beta_v]_1 = \sum_{i=0}^n [a_i]_1 \beta_{v,i} + [\delta_v]_1 \beta_t$, $[\beta_w]_1 = \sum_{i=0}^n [a_i]_1 \beta_{w,i} + [\delta_w]_1 \beta_t$ and also $[V(s) + \beta_v]_1 = [V]_1 + [\beta_v]_1$, because it knows $[V]_1$ from the proof π and the extracted values $[a_i]_1$, and β_i are the reminders of dividing $V_i(X)$ by $X - \chi_{j^*}$.

Since $\mathcal{B}_3$ sampled $\mathtt{ck}'$ itself, it knows the extraction key of the commitment $[\tilde{\boldsymbol{c}}]_2$ and can extract the elements $[q_v(s)]_2 = [\sum_{i=1}^{n+1} a_i \alpha_i(s) + \delta_v \alpha_{n+1}(s)]_2$, $[\beta_v z]_2$ and $[\beta_w z]_2$.

From these values and $[V(s) + \beta_v]_2$, computed above, $\mathcal{B}_3$ can derive $[(V(s) + \beta_v) q_v(s)]_T$ as $[V(s) + \beta_v]_1 \cdot [q_v(s)]_2$. Finally, it can directly compute $[q_w(s)]_T$ from extracted elements $[a_i]_1$ for $i \in [1 \mathinner{..} n]$ and $[\delta_w]_1$, and public $\hat{\alpha}_i(s)$: $[\sum_{i=1}^{n} a_i \hat{\alpha}_i(s) + \delta_w \beta_t]_1$. Thus, from equation (7) $\mathcal{B}_3$ recovers $\left[\frac{\beta_v^2 - \beta_w}{s - \chi_{j^*}}\right]_T$ and returns

$$\left(\chi_{j^*}, [\beta_v]_1, [\beta_w]_1, [z\beta_v]_2, [z\beta_w]_2, \left[\frac{\beta_v^2 - \beta_w}{s - \chi_{j^*}}\right]_T\right),$$

breaking the d-SATSDH assumption. □

Hence by Lemmas 5 to 7 and the triangle inequality we get that

$$1/d \cdot \mathsf{Adv}_{\mathrm{Snd}}(\mathcal{A}) \leq \left(2\mathsf{Adv}_{\mathsf{DDH},\mathbb{G}_2}(\mathcal{B}_2) + \mathsf{Adv}_{\mathsf{bls}}(\mathcal{B}_3) + \mathsf{Adv}_{d\text{-}\mathsf{SATSDH}}(\mathcal{B}_4)\right).$$

□

Acknowledgments. We would like to thank Carla Ràfols and Janno Veeorg for useful discussions. The authors were supported by the Estonian Research Council grant (PRG49) and by Dora Plus Grant funded by the European Regional Development Fund, Republic of Estonia and Archimedes Foundation.

References

ABLZ17. Behzad Abdolmaleki, Karim Baghery, Helger Lipmaa, and Michal Zajac. A subversion-resistant SNARK. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part III*, volume 10626 of *LNCS*, pages 3–33. Springer, Heidelberg, December 2017. doi:10.1007/978-3-319-70700-6_1.

AIR01. William Aiello, Yuval Ishai, and Omer Reingold. Priced oblivious transfer: How to sell digital goods. In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 119–135. Springer, Heidelberg, May 2001. doi:10.1007/3-540-44987-6_8.

ALM$^+$92. Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and hardness of approximation problems. In *33rd FOCS*, pages 14–23. IEEE Computer Society Press, October 1992. doi:10.1109/SFCS.1992.267823.

AS92. Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs; A new characterization of NP. In *33rd FOCS*, pages 2–13. IEEE Computer Society Press, October 1992. doi:10.1109/SFCS.1992.267824.

BB04. Dan Boneh and Xavier Boyen. Secure identity based encryption without random oracles. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 443–459. Springer, Heidelberg, August 2004. doi:10.1007/978-3-540-28628-8_27.

BCKL08. Mira Belenkiy, Melissa Chase, Markulf Kohlweiss, and Anna Lysyanskaya. P-signatures and noninteractive anonymous credentials. In Ran Canetti, editor, *TCC 2008*, volume 4948 of *LNCS*, pages 356–374. Springer, Heidelberg, March 2008. `doi:10.1007/978-3-540-78524-8_20`.

CF13. Dario Catalano and Dario Fiore. Vector commitments and their applications. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *PKC 2013*, volume 7778 of *LNCS*, pages 55–72. Springer, Heidelberg, February / March 2013. `doi:10.1007/978-3-642-36362-7_5`.

CFS17. Alessandro Chiesa, Michael A. Forbes, and Nicholas Spooner. A zero knowledge sumcheck and its applications. Cryptology ePrint Archive, Report 2017/305, 2017. `http://eprint.iacr.org/2017/305`.

CGM16. Melissa Chase, Chaya Ganesh, and Payman Mohassel. Efficient zero-knowledge proof of algebraic and non-algebraic statements with applications to privacy preserving credentials. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part III*, volume 9816 of *LNCS*, pages 499–530. Springer, Heidelberg, August 2016. `doi:10.1007/978-3-662-53015-3_18`.

CV05. Dario Catalano and Ivan Visconti. Hybrid trapdoor commitments and their applications. In Luís Caires, Giuseppe F. Italiano, Luís Monteiro, Catuscia Palamidessi, and Moti Yung, editors, *ICALP 2005*, volume 3580 of *LNCS*, pages 298–310. Springer, Heidelberg, July 2005. `doi:10.1007/11523468_25`.

DFGK14. George Danezis, Cédric Fournet, Jens Groth, and Markulf Kohlweiss. Square span programs with applications to succinct NIZK arguments. In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Part I*, volume 8873 of *LNCS*, pages 532–550. Springer, Heidelberg, December 2014. `doi:10.1007/978-3-662-45611-8_28`.

DFL$^+$09. Ivan Damgård, Serge Fehr, Carolin Lunemann, Louis Salvail, and Christian Schaffner. Improving the security of quantum protocols via commit-and-open. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 408–427. Springer, Heidelberg, August 2009. `doi:10.1007/978-3-642-03356-8_24`.

DGI$^+$19. Nico Döttling, Sanjam Garg, Yuval Ishai, Giulio Malavolta, Tamer Mour, and Rafail Ostrovsky. Trapdoor hash functions and their applications. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part III*, volume 11694 of *LNCS*, pages 3–32. Springer, Heidelberg, August 2019. `doi:10.1007/978-3-030-26954-8_1`.

DGN$^+$17. Nico Döttling, Satrajit Ghosh, Jesper Buus Nielsen, Tobias Nilges, and Roberto Trifiletti. TinyOLE: Efficient actively secure two-party computation from oblivious linear function evaluation. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *ACM CCS 2017*, pages 2263–2276. ACM Press, October / November 2017. `doi:10.1145/3133956.3134024`.

DGP$^+$19. Vanesa Daza, Alonso González, Zaira Pindado, Carla Ràfols, and Javier Silva. Shorter quadratic QA-NIZK proofs. In Dongdai Lin and Kazue Sako, editors, *PKC 2019, Part I*, volume 11442 of *LNCS*, pages 314–343. Springer, Heidelberg, April 2019. `doi:10.1007/978-3-030-17253-4_11`.

DKM12. Nico Döttling, Daniel Kraschewski, and Jörn Müller-Quade. Statistically secure linear-rate dimension extension for oblivious affine function evaluation. In Adam Smith, editor, *ICITS 12*, volume 7412 of

LNCS, pages 111–128. Springer, Heidelberg, August 2012. doi:10.1007/978-3-642-32284-6_7.

DN02. Ivan Damgård and Jesper Buus Nielsen. Perfect hiding and perfect binding universally composable commitment schemes with constant expansion factor. In Moti Yung, editor, *CRYPTO 2002*, volume 2442 of *LNCS*, pages 581–596. Springer, Heidelberg, August 2002. doi:10.1007/3-540-45708-9_37.

EHK$^+$13. Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Villar. An algebraic framework for Diffie-Hellman assumptions. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147. Springer, Heidelberg, August 2013. doi:10.1007/978-3-642-40084-1_8.

GGPR13. Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova. Quadratic span programs and succinct NIZKs without PCPs. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 626–645. Springer, Heidelberg, May 2013. doi:10.1007/978-3-642-38348-9_37.

GHR15. Alonso González, Alejandro Hevia, and Carla Ràfols. QA-NIZK arguments in asymmetric groups: New tools and new constructions. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 605–629. Springer, Heidelberg, November / December 2015. doi:10.1007/978-3-662-48797-6_25.

GM17. Jens Groth and Mary Maller. Snarky signatures: Minimal signatures of knowledge from simulation-extractable SNARKs. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 581–612. Springer, Heidelberg, August 2017. doi:10.1007/978-3-319-63715-0_20.

GNN17. Satrajit Ghosh, Jesper Buus Nielsen, and Tobias Nilges. Maliciously secure oblivious linear function evaluation with constant overhead. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part I*, volume 10624 of *LNCS*, pages 629–659. Springer, Heidelberg, December 2017. doi:10.1007/978-3-319-70694-8_22.

GR05. Craig Gentry and Zulfikar Ramzan. Single-database private information retrieval with constant communication rate. In Luís Caires, Giuseppe F. Italiano, Luís Monteiro, Catuscia Palamidessi, and Moti Yung, editors, *ICALP 2005*, volume 3580 of *LNCS*, pages 803–815. Springer, Heidelberg, July 2005. doi:10.1007/11523468_65.

GR16. Alonso González and Carla Ràfols. New techniques for non-interactive shuffle and range arguments. In Mark Manulis, Ahmad-Reza Sadeghi, and Steve Schneider, editors, *ACNS 16*, volume 9696 of *LNCS*, pages 427–444. Springer, Heidelberg, June 2016. doi:10.1007/978-3-319-39555-5_23.

GR19. Alonso González and Carla Ràfols. Shorter pairing-based arguments under standard assumptions. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 728–757. Springer, Heidelberg, December 2019. doi:10.1007/978-3-030-34618-8_25.

Gro10. Jens Groth. Short pairing-based non-interactive zero-knowledge arguments. In Masayuki Abe, editor, *ASIACRYPT 2010*, volume 6477 of *LNCS*, pages 321–340. Springer, Heidelberg, December 2010. doi:10.1007/978-3-642-17373-8_19.

Gro16. Jens Groth. On the size of pairing-based non-interactive arguments. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 305–326. Springer, Heidelberg, May 2016. doi:10.1007/978-3-662-49896-5_11.

GS08. Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432. Springer, Heidelberg, April 2008. doi:10.1007/978-3-540-78967-3_24.

GW11. Craig Gentry and Daniel Wichs. Separating succinct non-interactive arguments from all falsifiable assumptions. In Lance Fortnow and Salil P. Vadhan, editors, *43rd ACM STOC*, pages 99–108. ACM Press, June 2011. doi:10.1145/1993636.1993651.

HW15. Pavel Hubacek and Daniel Wichs. On the communication complexity of secure function evaluation with long output. In Tim Roughgarden, editor, *ITCS 2015*, pages 163–172. ACM, January 2015. doi:10.1145/2688073.2688105.

JR13. Charanjit S. Jutla and Arnab Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 1–20. Springer, Heidelberg, December 2013. doi:10.1007/978-3-642-42033-7_1.

JR14. Charanjit S. Jutla and Arnab Roy. Switching lemma for bilinear tests and constant-size NIZK proofs for linear subspaces. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part II*, volume 8617 of *LNCS*, pages 295–312. Springer, Heidelberg, August 2014. doi:10.1007/978-3-662-44381-1_17.

Kil94. Joe Kilian. On the complexity of bounded-interaction and noninteractive zero-knowledge proofs. In *35th FOCS*, pages 466–477. IEEE Computer Society Press, November 1994. doi:10.1109/SFCS.1994.365744.

KW15. Eike Kiltz and Hoeteck Wee. Quasi-adaptive NIZK for linear subspaces revisited. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 101–128. Springer, Heidelberg, April 2015. doi:10.1007/978-3-662-46803-6_4.

Lip05. Helger Lipmaa. An oblivious transfer protocol with log-squared communication. In Jianying Zhou, Javier Lopez, Robert H. Deng, and Feng Bao, editors, *ISC 2005*, volume 3650 of *LNCS*, pages 314–328. Springer, Heidelberg, September 2005.

Lip12. Helger Lipmaa. Progression-free sets and sublinear pairing-based non-interactive zero-knowledge arguments. In Ronald Cramer, editor, *TCC 2012*, volume 7194 of *LNCS*, pages 169–189. Springer, Heidelberg, March 2012. doi:10.1007/978-3-642-28914-9_10.

Lip19. Helger Lipmaa. Simulation-Extractable ZK-SNARKs Revisited. Technical Report 2019/612, IACR, May 31, 2019. https://eprint.iacr.org/2019/612, updated on 8 Feb 2020.

LPJY14. Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 514–532. Springer, Heidelberg, May 2014. doi:10.1007/978-3-642-55220-5_29.

LPJY15. Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Compactly hiding linear spans - tightly secure constant-size simulation-sound QA-NIZK proofs and applications. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 681–707. Springer, Heidelberg, November / December 2015. doi:10.1007/978-3-662-48797-6_28.

LY10. Benoît Libert and Moti Yung. Concise mercurial vector commitments and independent zero-knowledge sets with short proofs. In Daniele Micciancio, editor, *TCC 2010*, volume 5978 of *LNCS*, pages 499–517. Springer, Heidelberg, February 2010. doi:10.1007/978-3-642-11799-2_30.

MRV16. Paz Morillo, Carla Ràfols, and Jorge Luis Villar. The kernel matrix Diffie-Hellman assumption. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 729–758. Springer, Heidelberg, December 2016. doi:10.1007/978-3-662-53887-6_27.

OPWW15. Tatsuaki Okamoto, Krzysztof Pietrzak, Brent Waters, and Daniel Wichs. New realizations of somewhere statistically binding hashing and positional accumulators. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 121–145. Springer, Heidelberg, November / December 2015. doi:10.1007/978-3-662-48797-6_6.

Ped92. Torben P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In Joan Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 129–140. Springer, Heidelberg, August 1992. doi:10.1007/3-540-46766-1_9.

RS20. Carla R'afols and Javier Silva. QA-NIZK Arguments of SameOpening for Bilateral Commitments. Preprint. Available from https://eprint.iacr.org/2020/569.pdf, May 2020, 2020.

Vil12. Jorge Luis Villar. Optimal reductions of some decisional problems to the rank problem. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 80–97. Springer, Heidelberg, December 2012. doi:10.1007/978-3-642-34961-4_7.

A Analysis of Existing QA-NIZK Constructions

In this section, we show that some of the existing QA-NIZK arguments implicitly use QA-NIZK-friendly commitments. These constructions rely on falsifiable assumptions; in particular, the commitment has to contain the necessary amount of information for extraction to be possible. More precisely, to extract q group elements from a commitment, the commitment has to contain at least $q+1$ group elements as proved in Corollary 1.

In the following we explain two constructions in detail, the argument for proving bit-strings in [GHR15] and the argument for proving satisfiability of n quadratic equations of d variables in [DGP$^+$19]. As we will see, the second approach uses similar techniques to the first one. Both have the same structure described in Section 4.1 and use QA-NIZK-friendly commitments.

There exist two versions of bit-string arguments, but we focus on the one in [GHR15] because the idea is very similar. In [GHR15] the COM is perfectly binding while in [GR16] it is computationally binding, so in the second case another witness can open the commitment.

The argument for bit-strings in [GHR15]. The argument for bit-strings in [GHR15] guarantees that a commitment COM opens to a bit-vector $\boldsymbol{b} \in \{0,1\}^n$. COM is perfectly binding and, since it is based on standard assumptions, its length is linear in n. Proving $\boldsymbol{b}$ is a bit-vector is equivalent to proving equations $b_i(b_i - 1) = 0$ for all $i \in [1 \mathinner{..} n]$, which in turn is equivalent to proving that vectors $\boldsymbol{b}, \bar{\boldsymbol{b}}$ satisfy (i) $\bar{b}_i - b_i = 0$ and (ii) $\bar{b}_i(b_i - 1) = 0$ for all $i \in [1 \mathinner{..} n]$. The argument [GHR15] consists of the following building blocks:

1. The prover uses a perfectly binding ACS COM with $\boldsymbol{U}_1 = (\boldsymbol{g}^{(1)}, \ldots, \boldsymbol{g}^{(n)})$, $\boldsymbol{U}_2 = \boldsymbol{g}^{(n+1)}$, where $\boldsymbol{g}^{(i)} \leftarrow_{\$} \mathbb{Z}_p^2$, to commit $\boldsymbol{b} \in \mathbb{Z}_p^n$: $[\boldsymbol{c}]_1 = [\boldsymbol{U}_1]_1 \boldsymbol{b} + r[\boldsymbol{U}_2]_1$, for $r \leftarrow_{\$} \mathbb{Z}_p$.
2. The prover computes another commitment of the witness, by using an SSB ACS COM', with $\boldsymbol{U}'_1 = (\boldsymbol{h}^{(1)}, \ldots, \boldsymbol{h}^{(n)})$, $\boldsymbol{U}'_2 = \boldsymbol{h}^{(n+1)}$. Here, $\boldsymbol{h}^{(n+1)} \leftarrow \mathbb{Z}_p^2$, and $\{\boldsymbol{h}^{(i)}\}_{i \in [1 \mathinner{..} n]}$ are sampled uniformly from the span of $\boldsymbol{h}^{(n+1)}$ ($q' = 0$, $\boldsymbol{h}^{(i)} = \varepsilon_i \boldsymbol{h}^{(n+1)}$ where $\varepsilon_i \leftarrow \mathbb{Z}_p$ uniformly sampled. Thus, $[\boldsymbol{d}]_2 \leftarrow [\boldsymbol{U}_1]_2 \boldsymbol{b} + s[\boldsymbol{U}_2]_2$ for $s \leftarrow_{\$} \mathbb{Z}_p$.
3. The prover computes an argument $\mathit{\Pi}'$ with additional commitments $[\mathit{\Omega}_1]_1$ and $[\mathit{\Omega}_2]_2$ of the witness and the randomness used in $\mathsf{COM}, \mathsf{COM}'$, together with a QA-NIZK argument for subspace sum [GHR15] used to prove membership of $\mathit{\Omega}_1 + \mathit{\Omega}_2$. This is a trick for proving all equations in condition (ii) together by the efficient QA-NIZK argument for Sum in [GHR15].
4. The prover computes a succinct QA-NIZK argument $\mathit{\Pi}$ for Equal Opening in Asymmetric Groups [GHR15] to show that $[\boldsymbol{c}]_1$ and $[\boldsymbol{d}]_2$ open to the same value, which proves condition (i).

In the proof of soundness, one uses the game hopping technique as follows. Assume that an adversary $\mathcal{A}$ succeeds in breaking the soundness; thus the verifier accepts, but $b_{i^*} \notin \{0,1\}$ for at least one index $i^* \in [1 \mathinner{..} n]$. First, one changes the distribution of $\boldsymbol{U}_1$ to be SSB with $q' = 1$, hence for some i the column $\boldsymbol{h}^{(i)}$ is linearly independent to the others; the resulting COM' commitment is statistically binding and $[\cdot]_2$-extractable in a single component. Then, the reduction guesses an index $i \leftarrow [1 \mathinner{..} n]$ for which b_i is not a bit, and aborts if $b_i \in \{0,1\}$. In the next game, the reduction itself samples a vector $\boldsymbol{h}^{(i^*)}$ uniformly at random. With an overwhelming probability $\boldsymbol{h}^{(i^*)}$ is linearly independent of $\{\boldsymbol{h}^{(i)}\}_{i=1}^n$. This allows one to extract the element b_{i^*} from the commitment $[\boldsymbol{d}]_2$ and use it to break either the equal opening argument, the subspace sum argument or the split kernel assumption defined as follows.

$\mathcal{D}_{\ell k}$-SKerMDH [GHR15] holds relative to Pgen, if $\forall$ PPT $\mathcal{A}$, $\mathsf{Adv}^{\mathrm{skermdh}}_{\mathcal{A}, \mathcal{D}_{\ell k}, \mathsf{Pgen}}(\lambda) :=$

$$\Pr\left[\begin{matrix} \mathsf{p} \leftarrow \mathsf{Pgen}(1^\lambda); \mathbf{A} \leftarrow_{\$} \mathcal{D}_{\ell k}; ([\boldsymbol{c}_1]_1, [\boldsymbol{c}_2]_2) \leftarrow \mathcal{A}(\mathsf{p}, [\mathbf{A}]_1, [\mathbf{A}]_2) : \\ \mathbf{A}^\top (\boldsymbol{c}_1 - \boldsymbol{c}_2) = \mathbf{0}_k \wedge \boldsymbol{c}_1 - \boldsymbol{c}_2 \neq \mathbf{0}_\ell \end{matrix}\right] \approx_\lambda 0 \ .$$

The Argument for Quadratic Equations in [DGP$^+$19]. The argument in [DGP$^+$19] guarantees that the opening of a perfectly binding commitment

$\mathsf{COM} = [\boldsymbol{c}]_1$ satisfies a set of n quadratic equations in d variables. We use a constant QA-NIZK for proving the equations based on SNARK techniques and the constant QA-NIZK for same opening [GHR15].

1. The prover computes a commitment $[\boldsymbol{c}]_1$ of the witness using a perfectly binding commitment scheme COM. that is a concatenation of n Lifted El-Gamal commitments $[\boldsymbol{c}_i]_1$. In particular, $[\boldsymbol{c}]_1 = ([\boldsymbol{c}_1]_1, \ldots, [\boldsymbol{c}_n]_1)$ computed as $[\boldsymbol{c}_i]_1 = b_i[\boldsymbol{g}_1]_1 + r_i[\boldsymbol{g}_2]_2$ for $r_i \leftarrow \mathbb{Z}_p$. Here the commitment key is $\mathtt{ck} = ([\boldsymbol{g}_1]_1, [\boldsymbol{g}_2]_2)$ where the vectors $\boldsymbol{g}_i$ are sampled uniformly random from $\mathbb{Z}_p^2$. Hence, using our terminology, $\boldsymbol{U}_1 = \boldsymbol{g}_1\boldsymbol{I}$, $\boldsymbol{U}_2 = \boldsymbol{g}_2\boldsymbol{I}$.
2. For the divisibility argument the prover computes a functional SSB commitment $[\boldsymbol{q}_2]_2$ and two perfectly hiding commitments $[V]_1, [V]_2$ of the witness. Concretely, the commitment $[\boldsymbol{q}_2]_2 = [\boldsymbol{H}]_2\boldsymbol{b} + [\boldsymbol{Q}]_2\boldsymbol{r} \in \mathbb{G}^{q+1}$ with commitment key $\mathtt{ck} = ([\boldsymbol{H}]_2, [\boldsymbol{Q}]_2)$ where the columns of $\boldsymbol{H}$ and $\boldsymbol{Q}$ are sampled uniformly random from $\mathbb{Z}_p^{q+1}$.
3. The divisibility argument Π' uses SNARKs to prove satisfiability of quadratic equations.
4. Finally, the prover computes a QA-NIZK argument Π for Equal Opening in Asymmetric Groups [GHR15] to prove that $[\boldsymbol{c}]_1$, $[V]_1$, $[V]_2$, $[\boldsymbol{q}_2]_2$ open to the same value.

In the security proof, the soundness game is changed to another game that chooses $\boldsymbol{g}_1, \boldsymbol{g}_2$ itself in order to open the commitment $[\boldsymbol{c}]_1$ and $[\cdot]_\iota$-extract the whole witness. By the same technique as in previous example, in the latter game, we guess the index i^* where the i^*th equation does not hold. Next, we change to another game where the matrix $\boldsymbol{H}$ is constructed to define some linear functions in their rows. Both distributions are indistinguishable because some randomness is added to each column ($\boldsymbol{h}^{(i)} \leftarrow \boldsymbol{f}^{(i)}(\boldsymbol{w}) + \boldsymbol{r}_i[\boldsymbol{Q}]_2$). Hence, each column is indistinguishable from a uniformly sampled vector in $\mathbb{Z}_p^{q+1}$ but the reduction knows the structure. Moving to another indistinguishable game, the matrix $\boldsymbol{Q}$ is sampled uniformly at random from $\mathbb{Z}_p^{(q+1)\times(q+1)}$ conditioned on having rank 1, i.e., there exists an extractable key. The functions of the witness defined in $\boldsymbol{H}$ can then be extracted without the randomness, because the extraction key is in the orthogonal space of $\boldsymbol{Q}$. Soundness follows because from the i^*th equation we can either break soundness of the same opening argument or the divisibility relation of polynomials. In the second case, we use the functional commitment to extract linear functions of the witness that allow to break a falsifiable assumption derived from the Target Strong DH assumption.

These special properties of perfectly binding and extractability of q functions of the committed value are explained in detail when we present functional SSB commitments in Appendix C.

Required properties of SSB. In both constructions soundness depends on the ISH, SSB, and SSE properties of SSB commitments, while zero-knowledge depends on AESH. In the second example, all the commitments are PH, even the commitment $[\boldsymbol{c}]_1$ that, as in GS proofs, use commitment keys $\boldsymbol{g}_1, \boldsymbol{g}_2$ which in the zero-knowledge setting are two linear dependent vectors. More details can be seen in the analogous construction in Section 7.

B Missing Proofs in Section 3 and Section 4

B.1 Proof of Lemma 1

Proof. Assume that for given n and q, $\mathcal{A}$ breaks SSB with probability $\mathsf{Adv}^{\mathrm{ssb}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda)$. This means that for some $\mathcal{S}$ of cardinality $\leq q$ and honestly generated ck (w.r.t. $\mathcal{S}$), $\mathcal{A}$ outputs $(\boldsymbol{x}_0, \boldsymbol{x}_1, r_0, r_1)$ such that $\boldsymbol{x}_{0\mathcal{S}} \neq \boldsymbol{x}_{1\mathcal{S}}$ and $C := \mathsf{Com}(\mathsf{ck}; \boldsymbol{x}_0; r_0) = \mathsf{Com}(\mathsf{ck}; \boldsymbol{x}_1; r_1)$.

Since $\boldsymbol{x}_{0\mathcal{S}} \neq \boldsymbol{x}_{1\mathcal{S}}$ and F is injective, we get that $\boldsymbol{F}_0 := (F(x_{0\sigma_1}), \ldots, F(x_{0\sigma_{|\mathcal{S}|}})) \neq (F(x_{1\sigma_1}), \ldots, F(x_{1\sigma_{|\mathcal{S}|}})) =: \boldsymbol{F}_1$. Therefore, there exists $\beta \in \{0,1\}$, such that $\mathsf{Ext}_F(\mathsf{p}, \mathsf{ek}; C) \neq \boldsymbol{F}_\beta$. Thus, if $\mathcal{B}$ outputs $(\boldsymbol{x}_\beta, r_\beta)$ for $\beta \leftarrow_{\$} \{0,1\}$, $\mathsf{Adv}^{\mathrm{sse}}_{\beta,F,\mathsf{COM},n,q}(\lambda) \geq \mathsf{Adv}^{\mathrm{ssb}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda)/2$ and hence $\mathsf{Adv}^{\mathrm{ssb}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) \leq 2 \cdot \mathsf{Adv}^{\mathrm{sse}}_{\beta,F,\mathsf{COM},n,q}(\lambda)$. □

B.2 Proof of Lemma 3

Proof. Let $\mathcal{S} \subseteq [1\,..\,n]$, $|\mathcal{S}| \leq q$ be the indices of $\boldsymbol{x}$ one can extract during opening. **(i: AECH)** Let $\mathcal{A}$ be an adversary that breaks AECH with non-negligible probability, say $\varepsilon_{\mathcal{A}}$. Consider the following $\mathbb{G}_\iota$-MDDH adversary $\mathcal{B}$. $\mathcal{B}$ receives a challenge $[\mathbf{A}, \boldsymbol{y}_\beta]_\iota$ where $\mathbf{A} \leftarrow_{\$} \mathcal{D}_2$, $\boldsymbol{y}_0 \leftarrow_{\$} \mathbb{Z}_p^k$, and $\boldsymbol{y}_1 \leftarrow \mathbf{A}\boldsymbol{r}$ for $\boldsymbol{r} \leftarrow_{\$} \mathbb{Z}_p^m$. $\mathcal{B}$ sets $[\boldsymbol{U}_2]_\iota \leftarrow [\mathbf{A}]_\iota$, and generates $\boldsymbol{U}_1$ from the distribution $\mathcal{D}_1$. $\mathcal{B}$ sends $\mathsf{ck} = [\boldsymbol{U}_1, \boldsymbol{U}_2]_\iota$ to $\mathcal{A}$ who replies with two messages $\boldsymbol{x}_0, \boldsymbol{x}_1$, such that $\boldsymbol{x}_{0,\mathcal{S}}, \boldsymbol{x}_{1,\mathcal{S}}$. $\mathcal{B}$ computes $\boldsymbol{c}_0 \leftarrow [\boldsymbol{U}_1]_\iota \boldsymbol{x}_0 + [\boldsymbol{U}_2]_\iota \boldsymbol{r}$, for $\boldsymbol{r} \leftarrow_{\$} \mathbb{Z}_p^m$, and $\boldsymbol{c}_1 \leftarrow [\boldsymbol{U}_1]_\iota \boldsymbol{x}_1 + [\boldsymbol{y}_\beta]_\iota$. $\mathcal{B}$ picks $\beta' \leftarrow \{0,1\}$ and sends $c_{\beta'}$ to $\mathcal{A}$. $\mathcal{A}$ guesses which message was committed by returning $\beta_{\mathcal{A}} \in \{0,1\}$ to $\mathcal{B}$. $\mathcal{B}$ sends $\beta_{\mathcal{A}}$ to the MDDH challenger. Clearly,

$$\begin{aligned}\Pr[\beta_{\mathcal{A}} = \beta] =& \Pr[\beta_{\mathcal{A}} = 0|\beta = 0]/2 + \Pr[\beta_{\mathcal{A}} = 1|\beta = 1]/2\\ =& \varepsilon_{\mathcal{A}}/2 + (\Pr[\beta_{\mathcal{A}} = 1|\beta = 1, \beta' = 0]/2 + \Pr[\beta_{\mathcal{A}} = 1|\beta = 1, \beta' = 1]/2)/2\\ =& \varepsilon_{\mathcal{A}}/2 + \varepsilon_{\mathcal{A}}/4 + \varepsilon_{\mathcal{A}}/8 = 7/8 \cdot \varepsilon_{\mathcal{A}} \ .\end{aligned}$$

Thus if $\mathcal{A}$ succeeded with non-negligible probability, then so did $\mathcal{B}$.

(ii: ISH) Firstly we prove that for any $\mathcal{S}_0$ with $|\mathcal{S}_0| \leq n$, if $\mathcal{S}_1 = \mathcal{S}_0 \cup \{i^*\}$ for some $i^* \notin \mathcal{S}_0$ and $\mathcal{S}_0, \mathcal{S}_1 \subseteq [1\,..\,n]$, then $\mathcal{D}^{0,q}_{1,2} := ([\mathcal{D}^{n,k}_{\mathcal{S}_0}]_\iota, [\mathcal{D}^{m,k}_{\mathcal{S}_0}]_\iota)$ and $\mathcal{D}^{1,q}_{1,2} := ([\mathcal{D}^{n,k}_{\mathcal{S}_1}]_\iota, [\mathcal{D}^{m,k}_{\mathcal{S}_1}]_\iota)$ are computationally indistinguishable under MDDH. Let $\mathcal{A}$ be an adversary that can distinguish $\mathcal{D}^0_{1,2}$ and $\mathcal{D}^1_{1,2}$. We construct the following MDDH adversary $\mathcal{B}$ that receives a challenge $[\mathbf{A}, \boldsymbol{y}_\beta]_\iota$ where $\mathbf{A}_1, \mathbf{A}_2 \leftarrow_{\$} \mathcal{D}^0_{1,2}$, $\boldsymbol{y}_0 \leftarrow_{\$} \mathbb{Z}_p^k$, and $\boldsymbol{y}_1 \leftarrow (\mathbf{A}_1^\top | \mathbf{A}_2^\top)\boldsymbol{r}$ for $\boldsymbol{r} \leftarrow_{\$} \mathbb{Z}_p^m$. $\mathcal{B}$ sets $[\boldsymbol{U}_1]_\iota \leftarrow [\mathbf{A}_1]_\iota$, and $[\boldsymbol{U}_2]_\iota \leftarrow ([\mathbf{A}_2]_\iota | [\boldsymbol{y}_\beta]_\iota)$. $\mathcal{B}$ computes $\boldsymbol{c}_\beta \leftarrow [\boldsymbol{U}_1]_\iota \boldsymbol{x} + [\boldsymbol{U}_2]_\iota \boldsymbol{r}$, for $\boldsymbol{r} \leftarrow_{\$} \mathbb{Z}_p^m$ and sends $\boldsymbol{c}_\beta$ to $\mathcal{A}$ who replies with $\beta_{\mathcal{A}}$. Thus, $\mathcal{B}$ has the same advantage in breaking MDDH as $\mathcal{A}$ has in distinguishing $\mathcal{D}^{0,q}_{1,2}$ and $\mathcal{D}^{1,q}_{1,2}$.

Now, for any sets $\mathcal{S}_0$ and $\mathcal{S}_1$ it holds that $\mathsf{Adv}^{\mathrm{indist}}_{\mathcal{A},\mathcal{D}^0_{1,2},\mathcal{D}^1_{1,2}}(\lambda) \leq (|\mathcal{S}_0 \cup \mathcal{S}_1| - |\mathcal{S}_0 \cap \mathcal{S}_1|) \cdot \mathsf{Adv}^{\mathrm{mddh}}_{\mathcal{B},\mathcal{D}^{n,q}_{1,2},\mathsf{Pgen}}(\lambda)$.

(iii: SPB) Assume that all columns of $\boldsymbol{U}_1$ and $\boldsymbol{U}_2$ are pairwise linearly independent. Consider the matrix system of equations defined by $(\boldsymbol{U}_1, \boldsymbol{U}_2)\left(\begin{smallmatrix}\boldsymbol{x}\\ \boldsymbol{r}\end{smallmatrix}\right) =$

$\mathsf{Com}_{\mathtt{ck}}(\boldsymbol{x}, \boldsymbol{r})$. This system has a unique solution because the matrix has full rank. Hence, each commitment corresponds to a unique vector $\left(\begin{smallmatrix}\boldsymbol{x}\\ \boldsymbol{r}\end{smallmatrix}\right)$. Now, if $\boldsymbol{U}_1$ has q columns pair-wise linear independent and columns of $\boldsymbol{U}_2$ pair-wise linear independent to all of them, consider the system that has a matrix with those q columns of $\boldsymbol{U}_1$ and the whole $\boldsymbol{U}_2$. Its rank is maximum as well and the result follows.

<u>**(iv: $[\cdot]$-SPE)**</u> Since $k > m$, for any matrix $\boldsymbol{U}_2$ of size $k \times m$ there exist matrices $\mathtt{ek} \in \boldsymbol{U}_2^{\perp}$ that define orthogonal spaces of $\boldsymbol{U}_2$ of size $k' \times k$ for $k' \geq k - m$ such that $\mathtt{ek} \cdot \boldsymbol{U}_2 = \begin{pmatrix} \mathbf{0}_{(k-m)\times m} \\ \boldsymbol{a} \end{pmatrix}$ where $\boldsymbol{a} \in \mathbb{Z}_p^{(k'-k+m)\times m}$. This space has at least dimension 1 because $k > m$. Moreover, there exists an appropriate change of basis of the space such that $\mathtt{ek} \cdot \boldsymbol{U}_1 = \left(\begin{array}{c|c} \boldsymbol{I}_q & \boldsymbol{b}_2 \\ \boldsymbol{b}_1 & \end{array}\right)$ where $\boldsymbol{b}_1 \in \mathbb{Z}_p^{(k'-q)\times q}, \boldsymbol{b}_2 \in \mathbb{Z}_p^{k'\times(n-q)}$. This is well-defined since $k - m \geq q$ and if q columns of the matrices are pair-wise linear independent then $k' - q \geq k - m - q \geq 0$. □

B.3 Proof of Lemma 4

Proof. Fix λ. We first prove that for any $\mathcal{S}_0$ with $|\mathcal{S}_0| \leq q-1$, if $\mathcal{S}_1 = \mathcal{S}_0 \cup \{i^*\}$ for $i^* > \max_i\{i \in \mathcal{S}_0\}$ and $\mathcal{S}_0, \mathcal{S}_1 \subseteq [1\,..\,n]$, then $\mathcal{D}_0 := [\mathcal{D}_{q+1}^{p,n,\mathcal{S}_0}]$ and $\mathcal{D}_1 := [\mathcal{D}_{q+1}^{p,n,\mathcal{S}_1}]$ are computationally indistinguishable.

Let $\mathcal{A}$ be an adversary that can distinguish $\mathcal{D}_0$ and $\mathcal{D}_1$. We construct the following MDDH adversary $\mathcal{B}$. The challenger $\mathcal{C}$ of the MDDH game samples $\mathbf{A} \leftarrow_{\$} \mathbb{Z}_p^{q+1}$ and $\mathtt{w} \leftarrow_{\$} \mathbb{Z}_p$. If $\beta = 0$ then $\mathcal{C}$ samples $\boldsymbol{y} \leftarrow_{\$} \mathbb{Z}_p^{q+1}$, otherwise $\mathcal{C}$ sets $\boldsymbol{y} \leftarrow \mathbf{A}\mathtt{w}$. $\mathcal{C}$ sends $(\mathsf{p}, [\mathbf{A}, \boldsymbol{y}]_\iota)$ to $\mathcal{B}$. $\mathcal{B}$ does the following:

```
$\mathcal{B}(\mathsf{p}, [\mathbf{A}, \boldsymbol{y}])$
$[\boldsymbol{g}^{(n+1)}] \leftarrow [\mathbf{A}]$;
for $i$ in $[1\,..\,n]$ do
  if $i = i^*$ then $[\boldsymbol{g}^{(i)}] \leftarrow [\boldsymbol{y}]$;
  elseif $i \in \mathcal{S}_0$ then $\boldsymbol{g}^{(i)} \leftarrow_{\$} \mathbb{Z}_p^{q+1}$;
  else $\delta_i \leftarrow_{\$} \mathbb{Z}_p$; $[\boldsymbol{g}^{(i)}] \leftarrow [\boldsymbol{g}^{(n+1)}]\delta_i$; fi endfor
return $\beta \leftarrow \mathcal{A}(\mathsf{p}, [\boldsymbol{g}])$;
```

Clearly, $[\boldsymbol{g}]$ is distributed according to $\mathcal{D}_\beta$. Thus, $\mathcal{B}$ has the same advantage in breaking MDDH as $\mathcal{A}$ has in distinguishing $\mathcal{D}_0$ from $\mathcal{D}_1$. By using a standard hybrid argument, $\mathsf{Adv}^{\mathrm{indist}}_{\mathcal{A},\mathcal{D}^0,\mathcal{D}^1}(\lambda) \leq |\mathcal{S}| \cdot \mathsf{Adv}^{\mathrm{mddh}}_{\mathcal{B},\mathcal{U}_{q+1},\mathsf{Pgen}}(\lambda)$. □

As a simple generalization of Lemma 4, for any $\mathcal{S}_0, \mathcal{S}_1 \subseteq [1\,..\,n]$ with $\mathcal{S}_i \leq q$, $\mathsf{Adv}^{\mathrm{indist}}_{\mathcal{A},[\mathcal{D}_{q+1}^{p,n,\mathcal{S}_0}],[\mathcal{D}_{q+1}^{p,n,\mathcal{S}_1}]}(\lambda) \leq |\mathcal{S}_1 \triangle \mathcal{S}_2| \cdot \mathsf{Adv}^{\mathrm{mddh}}_{\mathcal{B},\mathcal{U}_{q+1},\mathsf{Pgen}}(\lambda)$.

C Details of Functional SSB Commitments

C.1 Definitions

Essentially the only difference between an SSB commitment and a functional SSB commitment is that in the former $\mathcal{S}$ is a subset of $[1\,..\,q]$ and in the latter

$\mathcal{S}$ is a subset of some function set $\mathcal{F}$. For the sake of completeness we provide the formal definition below.

Definition 4. *An F-*extractable functional SSB commitment scheme $\mathsf{COM} = (\mathsf{Pgen}, \mathsf{KC}, \mathsf{CKV}, \mathsf{Com}, \mathsf{tdOpen}, \mathsf{Ext}_F)$ *for a function family $\mathcal{F}$ consists of the following polynomial-time algorithms:*

Parameter generation: $\mathsf{Pgen}(1^\lambda)$ *returns parameters* p *(for example, group description). We allow F to depend on* p.

Commitment key generation: *for parameters* p*, a positive integer* $n \in \mathsf{poly}(\lambda)$*, an integer* $q \in [1\,..\,n]$*, and a tuple* $\mathcal{S} = (f_1, \dots, f_{|\mathcal{S}|}) \subseteq \mathcal{F}$ *with* $|\mathcal{S}| \leq q$, $\mathsf{KC}(\mathsf{p}, n, q, \mathcal{S})$ *outputs a commitment key* $\mathtt{ck}$ *and a trapdoor* $\mathtt{td} = (\mathtt{ek}, \mathtt{tk})$*. Here,* $\mathtt{ck}$ *implicitly specifies* p*, the message space* $\mathtt{MSP}$*, the randomizer space* $\mathtt{RSP}$*, and the commitment space* $\mathtt{CSP}$*, such that* $F(\mathtt{MSP}) \subseteq \mathtt{CSP}$, $\mathtt{ek}$ *is the* extraction key*, and* $\mathtt{tk}$ *is the* trapdoor key*. For any other input,* KC *outputs* $(\mathtt{ck}, \mathtt{td}) = (\bot, \bot)$.

Commitment key verification: *for a positive integer* $n \in \mathsf{poly}(\lambda)$*, an integer* $q \in [1\,..\,n]$*, and a commitment key* $\mathtt{ck}$, $\mathsf{CKV}(n, q, \mathtt{ck})$ *outputs* 1 *(accept,* $\mathtt{ck}$ *was formed correctly) or* 0 *(reject).*

Commitment: *for* $\mathsf{p} \in \mathsf{Pgen}(1^\lambda)$*, a commitment key* $\mathtt{ck} \neq \bot$*, a message* $\boldsymbol{x} \in \mathtt{MSP}^n$*, and a randomizer* $r \in \mathtt{RSP}$, $\mathsf{Com}(\mathtt{ck}; \boldsymbol{x}; r)$ *outputs a commitment* $c \in \mathtt{CSP}$.

Trapdoor opening: *for* $\mathsf{p} \in \mathsf{Pgen}(1^\lambda)$, $\mathcal{S} \subseteq \mathcal{F}$ *with* $|\mathcal{S}| \leq q$, $(\mathtt{ck}, (\mathtt{ek}, \mathtt{tk})) \in \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S})$*, two messages* $\boldsymbol{x}, \boldsymbol{x}^* \in \mathtt{MSP}^n$*, and a randomizer* $r \in \mathtt{RSP}$, $\mathsf{tdOpen}(\mathsf{p}, \mathtt{tk}; \boldsymbol{x}, r, \boldsymbol{x}^*)$ *returns a randomizer* $r^* \in \mathtt{RSP}$.

Extraction: *for* $\mathsf{p} \in \mathsf{Pgen}(1^\lambda)$, $\mathcal{S} = (f_1, \dots, f_{|\mathcal{S}|}) \subseteq \mathcal{F}$ *with* $1 \leq |\mathcal{S}| \leq q$, $(\mathtt{ck}, (\mathtt{ek}, \mathtt{tk})) \in \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S})$*, and* $c \in \mathtt{CSP}$, $\mathsf{Ext}_F(\mathsf{p}, \mathsf{ek}; c)$ *returns a tuple* $\big(F(f_1(x)), \dots, F(f_{|\mathcal{S}|}(x))\big) \in \mathtt{MSP}^{|\mathcal{S}|}$*;*

For $\{f_i\}_{i=1}^q \subseteq \mathcal{F}$ and vector $\boldsymbol{x}$ let us denote $\boldsymbol{x}_\mathcal{S} = (f_1(\boldsymbol{x}), \dots, f_q(\boldsymbol{x}))$.

Definition 5. *An F-extractable functional SSB commitment scheme* COM *for function family $\mathcal{F}$ is* secure *if it satisfies the following security requirements.*

Perfect Key-Correctness (PKC): *There exists a computationally unbounded extractor* Ext *such that* $\forall \lambda$*,* $n \in \mathsf{poly}(\lambda)$*,* $q \in [1\,..\,n]$*, and subverter* Sub*,* $\mathsf{Adv}^{\mathrm{kc}}_{\mathsf{COM},n,q,\mathcal{S},\mathsf{Ext}}(\lambda) = 0$*, where* $\mathsf{Adv}^{\mathrm{kc}}_{\mathsf{COM},n,q,\mathcal{S}}(\lambda) :=$

$$\Pr\left[\begin{matrix}\mathsf{p} \leftarrow \mathsf{Pgen}(1^\lambda); \mathtt{ck} \leftarrow \mathsf{Sub}(\mathsf{p}, n, q); \mathcal{S} \leftarrow \mathsf{Ext}(\mathtt{ck}) : \mathcal{S} \subseteq \mathcal{F} \wedge \\ |\mathcal{S}| \leq q \wedge \mathsf{CKV}(n, q, \mathtt{ck}) = 1 \wedge \forall \mathtt{td} : (\mathtt{ck}, \mathtt{td}) \notin \mathrm{range}(\mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}))\end{matrix}\right] .$$

Perfect Key-Verifiability (PKV): $\forall \lambda$*,* $n \in \mathsf{poly}(\lambda)$*,* $q \in [1\,..\,n]$*, and* $\mathcal{S} \subseteq \mathcal{F}$ *with* $|\mathcal{S}| \leq q$*,* $\mathsf{Adv}^{\mathrm{kv}}_{\mathsf{COM},n,q,\mathcal{S}}(\lambda) = 0$*, where* $\mathsf{Adv}^{\mathrm{kv}}_{\mathsf{COM},n,q,\mathcal{S}}(\lambda) :=$

$$\Pr\left[\mathsf{p} \leftarrow \mathsf{Pgen}(1^\lambda); (\mathtt{ck}, \mathtt{td}) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}) : \mathsf{CKV}(n, q, \mathtt{ck}) = 0\right] .$$

Function-Set Hiding (FSH): *$\forall$ PPT $\mathcal{A}$, $n \in \mathsf{poly}(\lambda)$, $q \in [1\,..\,n]$, $\mathsf{Adv}^{\mathsf{fsh}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) := 2\cdot|\varepsilon^{\mathsf{fsh}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) - 1/2| = \mathsf{negl}(\lambda)$, where $\varepsilon^{\mathsf{fsh}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) :=$*

$$\Pr\left[\begin{array}{l}\mathsf{p} \leftarrow \mathsf{Pgen}(1^{\lambda});\\ (\mathcal{S}_0, \mathcal{S}_1) \leftarrow \mathcal{A}(\mathsf{p}, n, q) \text{ s.t. } \forall i \in \{0,1\}, \mathcal{S}_i \subseteq \mathcal{F} \wedge |\mathcal{S}_i| \leq q;\\ \beta \leftarrow_{\$} \{0,1\}\,; (\mathtt{ck}_\beta, \mathtt{td}_\beta) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}_\beta) : \mathcal{A}(\mathtt{ck}_\beta) = \beta\end{array}\right] .$$

Somewhere Statistically Binding (SSB): *$\forall\lambda$, unbounded $\mathcal{A}$, $n \in \mathsf{poly}(\lambda)$, $q \in [1\,..\,n]$, $\mathsf{Adv}^{\mathrm{ssb}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) \approx_\lambda 0$, where $\mathsf{Adv}^{\mathrm{ssb}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) :=$*

$$\Pr\left[\begin{array}{l}\mathsf{p} \leftarrow \mathsf{Pgen}(1^{\lambda}); \mathcal{S} \leftarrow \mathcal{A}(\mathsf{p}, n, q) \text{ s.t. } \mathcal{S} \subseteq \mathcal{F} \wedge |\mathcal{S}| \leq q;\\ (\mathtt{ck}, \mathtt{td}) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}); (\boldsymbol{x}_0, \boldsymbol{x}_1, \boldsymbol{r}_0, \boldsymbol{r}_1) \leftarrow \mathcal{A}(\mathtt{ck}) \text{ s.t. } \boldsymbol{x}_{0\mathcal{S}} \neq \boldsymbol{x}_{1\mathcal{S}} :\\ \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}_0; \boldsymbol{r}_0) = \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}_1; \boldsymbol{r}_1)\end{array}\right] .$$

We say that COM is somewhere perfectly binding *(SPB) if $\mathsf{Adv}^{\mathrm{ssb}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) = 0$.*

Almost Everywhere Statistically Hiding (AESH): *$\forall\lambda$, unbounded $\mathcal{A}$, $n \in \mathsf{poly}(\lambda)$, $q \in [1\,..\,n]$, $\mathsf{Adv}^{\mathrm{aesh}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) := 2 \cdot |\varepsilon^{\mathsf{aesh}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) - 1/2| \approx_\lambda 0$, where $\varepsilon^{\mathsf{aesh}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) :=$*

$$\Pr\left[\begin{array}{l}\mathsf{p} \leftarrow \mathsf{Pgen}(1^{\lambda}); \mathcal{S} \leftarrow \mathcal{A}(\mathsf{p}, n, q) \text{ s.t. } \mathcal{S} \subseteq \mathcal{F} \wedge |\mathcal{S}| \leq q;\\ (\mathtt{ck}, \mathtt{td}) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}); (\boldsymbol{x}_0, \boldsymbol{x}_1) \leftarrow \mathcal{A}(\mathtt{ck}) \text{ s.t. } \boldsymbol{x}_{0\mathcal{S}} = \boldsymbol{x}_{1\mathcal{S}};\\ \beta \leftarrow_{\$} \{0,1\}\,; \boldsymbol{r} \leftarrow_{\$} \mathsf{RSP} : \mathcal{A}(\mathsf{Com}(\mathtt{ck}; \boldsymbol{x}_\beta; \boldsymbol{r})) = \beta\end{array}\right] .$$

COM *is* almost everywhere perfectly hiding *(AEPH) if* $\mathsf{Adv}^{\mathrm{aesh}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) = 0$.

Composable Sub-AESH: *there exists a PPT simulator Sim, such that for any unbounded subverter Sub there exists an unbounded extractor $\mathsf{Ext}_{\mathsf{Sub}}$ such that $\forall\lambda$, $n \in \mathsf{poly}(\lambda)$, $q \in [1\,..\,n]$, $\mathsf{p} \in \mathrm{range}(\mathsf{Pgen}(1^{\lambda}))$, and unbounded $\mathcal{A}$, $\mathsf{Adv}^{\mathrm{compsubaesh}}_{\mathsf{COM},\mathsf{Sub},\mathsf{Ext}_{\mathsf{Sub}},\mathsf{Sim},\mathcal{A},n,q}(\lambda) := 2\cdot|\varepsilon^{\mathsf{subaesh}}_{\mathsf{comp}}(\lambda) - 1/2| \approx_\lambda 0$, where $\varepsilon^{\mathsf{subaesh}}_{\mathsf{comp}}(\lambda) :=$*

$$\Pr\left[\begin{array}{l}r \leftarrow_{\$} \mathsf{RND}_\lambda(\mathsf{Sub}); (\mathtt{ck}, \mathsf{aux}_{\mathsf{Sub}} \| \mathcal{S}) \leftarrow (\mathsf{Sub} \| \mathsf{Ext}_{\mathsf{Sub}})(\mathsf{p}, n, q; r); \beta \leftarrow_{\$} \{0,1\}\,;\\ \boldsymbol{x} \leftarrow \mathcal{A}(\mathsf{p}, \mathtt{ck}, \mathsf{aux}_{\mathsf{Sub}}); \textbf{if } \beta = 0 \textbf{ then } \ r' \leftarrow \mathsf{RND}_\lambda(\mathsf{Com});\\ C \leftarrow \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}; r'); \textbf{else } r' \leftarrow_{\$} \mathsf{RND}_\lambda(\mathsf{Sim});\ C \leftarrow \mathsf{Sim}(\mathtt{ck}, \boldsymbol{x}_{\mathcal{S}}, \mathcal{S}; r') :\\ \mathsf{CKV}(n, q, \mathtt{ck}) = 1 \wedge \mathcal{A}(C) = \beta\end{array}\right] .$$

COM *is* composable sub-AEPH *if* $\mathsf{Adv}^{\mathrm{compsubaesh}}_{\mathsf{COM},\mathsf{Sub},\mathsf{Ext}_{\mathsf{Sub}},\mathsf{Sim},\mathcal{A},n,q}(\lambda) = 0$.

Somewhere Statistical F-Extractability (F-SSE): *$\forall\lambda$, $\mathsf{p} \in \mathsf{Pgen}(1^{\lambda})$, $n \in \mathsf{poly}(\lambda)$, $q \in [1\,..\,n]$, $\mathcal{S} = (f_1, \dots, f_{|\mathcal{S}|}) \subseteq \mathcal{F}$ with $|\mathcal{S}| \leq q$, $(\mathtt{ck}, (\mathsf{ek}, \mathtt{tk})) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S})$, and PPT $\mathcal{A}$, $\mathsf{Adv}^{\mathrm{sse}}_{\mathcal{A},F,\mathsf{COM},n,q}(\lambda) \approx_\lambda 0$, where $\mathsf{Adv}^{\mathrm{sse}}_{\mathcal{A},F,\mathsf{COM},n,q}(\lambda) :=$*

$$\Pr\left[\boldsymbol{x}, r \leftarrow \mathcal{A}(\mathtt{ck}) : \mathsf{Ext}_F(\mathsf{p}, \mathsf{ek}; \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}; r)) \neq \big(F(f_1(\boldsymbol{x})), \dots, F(f_{|\mathcal{S}|}(\boldsymbol{x}))\big)\right] .$$

It is somewhere perfect extractable if $\mathsf{Adv}^{\mathrm{sse}}_{\mathcal{A},F,\mathsf{COM},n,q}(\lambda) = 0$.

Almost Everywhere Statistical Trapdoor (AEST): *$\forall \lambda$, $n \in \mathsf{poly}(\lambda)$, $q \in [1\mathinner{..}n]$ and unbounded $\mathcal{A}$, $\mathsf{Adv}^{\mathrm{aest}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda)(\lambda) \approx_\lambda 0$, where $\mathsf{Adv}^{\mathrm{aest}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda)(\lambda) =$*

$$\Pr\left[\begin{array}{l}\mathsf{p} \in \mathsf{Pgen}(1^\lambda); \mathcal{S} \leftarrow \mathcal{A}(\mathsf{p}, n, q) \text{ s.t. } \mathcal{S} \subseteq \mathcal{F} \wedge |\mathcal{S}| \leq q; \\ (\mathtt{ck}, \mathtt{td}) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}); (\boldsymbol{x}_0, \boldsymbol{x}_1, \boldsymbol{r}_0) \leftarrow \mathcal{A}(\mathtt{ck}) \text{ s.t. } \boldsymbol{x}_{0\mathcal{S}} = \boldsymbol{x}_{1\mathcal{S}} : \\ \boldsymbol{r}^* \leftarrow \mathsf{tdOpen}(\mathsf{p}, \mathtt{tk}; \boldsymbol{x}, \boldsymbol{r}, \boldsymbol{x}^*) : \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}; \boldsymbol{r}) \neq \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}^*; \boldsymbol{r}^*)\end{array}\right] .$$

It is AEPT (almost everywhere perfect trapdoor) if $\mathsf{Adv}^{\mathrm{aest}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda)(\lambda) = 1$.

Computational Binding (CB): *$\forall$ PPT $\mathcal{A}$, $n \in \mathsf{poly}(\lambda)$, $q \in [1\mathinner{..}n]$, $\mathsf{Adv}^{\mathrm{cb}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) = \mathsf{negl}(\lambda)$, where $\mathsf{Adv}^{\mathrm{cb}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) :=$*

$$\Pr\left[\begin{array}{l}\mathsf{p} \leftarrow \mathsf{Pgen}(1^\lambda); \mathcal{S} \leftarrow \mathcal{A}(\mathsf{p}, n, q) \text{ s.t. } \mathcal{S} \subseteq \mathcal{F} \wedge |\mathcal{S}| \leq q; \\ (\mathtt{ck}, \mathtt{td}) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}); (\boldsymbol{x}_0, \boldsymbol{x}_1, \boldsymbol{r}_0, \boldsymbol{r}_1) \leftarrow \mathcal{A}(\mathtt{ck}) \text{ s.t. } \boldsymbol{x}_0 \neq \boldsymbol{x}_1 : \\ \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}_0; \boldsymbol{r}_0) = \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}_1; \boldsymbol{r}_1)\end{array}\right] .$$

Computational Hiding (CH): *$\forall$ PPT $\mathcal{A}$, $n \in \mathsf{poly}(\lambda)$, $q \in [1\mathinner{..}n]$, $\mathsf{Adv}^{\mathsf{ch}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) := 2\cdot|\varepsilon^{\mathsf{ch}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) - 1/2| = \mathsf{negl}(\lambda)$, where $\varepsilon^{\mathsf{ch}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) :=$*

$$\Pr\left[\begin{array}{l}\mathsf{p} \leftarrow \mathsf{Pgen}(1^\lambda); \mathcal{S} \leftarrow \mathcal{A}(\mathsf{p}, n, q) \text{ s.t. } \mathcal{S} \subseteq \mathcal{F} \wedge |\mathcal{S}| \leq q; \\ (\mathtt{ck}, \mathtt{td}) \leftarrow \mathsf{KC}(\mathsf{p}, n, q, \mathcal{S}); (\boldsymbol{x}_0, \boldsymbol{x}_1) \leftarrow \mathcal{A}(\mathtt{ck}); \beta \leftarrow_{\$} \{0,1\}; \\ \boldsymbol{r} \leftarrow_{\$} \mathtt{RSP} : \mathcal{A}(\mathsf{Com}(\mathtt{ck}; \boldsymbol{x}_\beta; \boldsymbol{r})) = \beta\end{array}\right] .$$

C.2 Security proofs

Before proving the security of linear EMP, let us recall some well-known decisional assumptions.

Decisional Diffie-Hellman (DDH) Assumption. Let $\iota \in \{1,2\}$. *DDH*$_{\mathbb{G}_\iota}$ holds relative to Pgen, if $\forall$ PPT $\mathcal{A}$, $\mathsf{Adv}^{\mathrm{ddh}}_{\mathcal{A},\iota,\mathsf{Pgen}}(\lambda) := |\varepsilon^0_{\mathcal{A}}(\lambda) - \varepsilon^1_{\mathcal{A}}(\lambda)| = \mathsf{negl}(\lambda)$, where

$$\varepsilon^\beta_{\mathcal{A}}(\lambda) := \Pr\left[\mathsf{p} \leftarrow \mathsf{Pgen}(1^\lambda); x, y, z \leftarrow_{\$} \mathbb{Z}_p : \mathcal{A}(\mathsf{p}, [x, y, xy + \beta z]_\iota) = 1 \quad\right] .$$

Rank Assumption. Let $\iota \in \{1,2\}$. (ℓ, k, r_0, r_1)-*Rank assumption* for $1 \leq r_0 < r_1 \leq \min(\ell, k)$ holds relative to Pgen, if $\forall$ PPT $\mathcal{A}$, $\mathsf{Adv}^{\mathrm{rank}}_{\mathcal{A},\ell,k,r_0,r_1,\iota,\mathsf{Pgen}}(\lambda) := |\varepsilon^0_{\mathcal{A}}(\lambda) - \varepsilon^1_{\mathcal{A}}(\lambda)| = \mathsf{negl}(\lambda)$, if

$$\varepsilon^\beta_{\mathcal{A}}(\lambda) := \Pr\left[\mathsf{p} \leftarrow \mathsf{Pgen}(1^\lambda); \mathbf{A} \leftarrow_{\$} \mathcal{U}^{(r_\beta)}_{\ell k} : \mathcal{A}(\mathsf{p}, [\mathbf{A}]_\iota) = 1 \quad\right] ,$$

where $\mathcal{U}^{(r_\beta)}_{\ell k}$ is the uniform distribution over rank r_β matrices $\mathbb{Z}_p^{\ell \times k}$.

Theorem 5 ([Vil12]). *Let $\iota \in \{1,2\}$. For any $\ell, k, r_0, r_1 \in \mathbb{Z}$ such that $1 \leq r_0 < r_1 \leq \min(\ell, k)$, any PPT $\mathcal{A}$, and any* Pgen,

$$\mathsf{Adv}^{\mathrm{rank}}_{\mathcal{A},\ell,k,r_0,r_1,\iota,\mathsf{Pgen}}(\lambda) \leq \lceil \log_2(r_1/r_0) \rceil \cdot \mathsf{Adv}^{\mathrm{ddh}}_{\mathcal{A},\iota,\mathsf{Pgen}}(\lambda) .$$

Theorem 6. *Let Pgen_{bg} be a bilinear group generator. Fix n and q. The commitment scheme in Fig. 3 is*

(i) PKC,

(ii) PKV,

(iii) FSH relative to Pgen_{bg} under the DDH$_{\mathbb{G}_\iota}$ assumption: for each PPT $\mathcal{A}$, there exists a PPT $\mathcal{B}$, such that $\mathsf{Adv}^{\mathrm{fsh}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) \leq \lceil \log_2(q+1) \rceil \cdot \mathsf{Adv}^{\mathrm{ddh}}_{\mathcal{B},\iota,\mathsf{Pgen}}(\lambda)$.

(iv) F-SSE for $F = [\cdot]_\iota$ (thus, F depends on p),

(v) SPB,

(vi) Sub-AEPH,

(vii) AEPT,

(viii) CB and CH.

Proof. **(i: PKC)** Given a commitment key $\mathsf{ck} = [\boldsymbol{g}] \in \mathbb{G}^{(q+1)\times(n+1)}$ with $[\boldsymbol{g}^{(n+1)}] \neq [\boldsymbol{0}]$, an unbounded extractor can compute $\boldsymbol{g}$. Let us pick some matrix $\boldsymbol{R} \in \mathbb{Z}_p^{(q+1)\times(q+1)}$ such that $\boldsymbol{R}^{(q+1)} = \boldsymbol{g}^{(q+1)}$ and $\boldsymbol{R}$ is full rank. This is always possible since $\boldsymbol{g}^{n+1} \neq \boldsymbol{0}$. Now we can uniquely express $\boldsymbol{g}^{(j)} = \sum_{i=1}^{q+1} M'_{i,j} \boldsymbol{R}^{(i)}$ for $j \in [1 \,..\, n+1]$ and in particular $\boldsymbol{M'}^{(n+1)} = (0, \ldots, 0, 1)^\top$. Therefore $\boldsymbol{M'}$ has the form $\left(\begin{smallmatrix} \boldsymbol{M} & \boldsymbol{0} \\ \boldsymbol{r}^\intercal & 1 \end{smallmatrix}\right)$ for some matrix $\boldsymbol{M} \in \mathbb{Z}_p^{q\times n}$ and $\boldsymbol{r} \in \mathbb{Z}_N^n$. Extractor can output $\boldsymbol{M}$ and moreover ck is well-formed.

(ii: PKV) Honestly generated $\mathsf{ck} = [\boldsymbol{g}]$ is by definition from the set $\mathbb{G}^{(q+1)\times(n+1)}$. Considering that $\boldsymbol{R}$ is full rank and that $\boldsymbol{g}^{(n+1)} = \boldsymbol{R}^{(q+1)}$ by construction, we may conclude that $\boldsymbol{g}^{(n+1)} \neq \boldsymbol{0}$. Thus, honest ck is accepted by CKV.

(iii: FSH) Since given a matrix $\boldsymbol{M'}$ of rank $r \in [1 \,..\, q+1]$, the matrix $\boldsymbol{RM'}$ is a random matrix of rank r with an overwhelming probability. Then, distinguishing commitment keys $\mathsf{ck}_1 = [\boldsymbol{R}_1 \boldsymbol{M'}_1]_\iota$ and $\mathsf{ck}_2 = [\boldsymbol{R}_2 \boldsymbol{M'}_2]_\iota$ is equivalent to breaking the rank assumption. Now, considering Theorem 5 we get that for each adversary $\mathcal{A}$ against FSH, there exists an adversary $\mathcal{B}$ against the DDH in $\mathbb{G}_\iota$ such that the bound $\mathsf{Adv}^{\mathrm{fsh}}_{\mathcal{A},\mathsf{COM},n,q}(\lambda) \simeq \mathsf{Adv}^{\mathrm{rank}}_{\mathcal{B},\iota,\mathsf{Pgen}}(\lambda) \leq \lceil \log_2(r_1/r_0) \rceil \cdot \mathsf{Adv}^{\mathrm{ddh}}_{\mathcal{B},\iota,\mathsf{Pgen}}(\lambda)$ holds. In the worst case one matrix has rank $r_0 = 1$ and the other has rank $r_1 = q+1$, so the worst bound is $\lceil \log_2(q+1) \rceil \cdot \mathsf{Adv}^{\mathrm{ddh}}_{\mathcal{B},\iota,\mathsf{Pgen}}(\lambda)$.

(iv: F-SSE) For any $\boldsymbol{x} \in \mathbb{Z}_p^n$ and $\boldsymbol{r} \in \mathbb{Z}_p^{q+1}$, we have $\mathsf{Com}(\mathsf{ck}; \boldsymbol{x}; r) = [\boldsymbol{RM'}\left(\begin{smallmatrix} \boldsymbol{x} \\ r \end{smallmatrix}\right)]_\iota = [\boldsymbol{c}]_\iota =$. Then, $\mathsf{Ext}(\mathsf{p}, \mathsf{ek} = \boldsymbol{R}^{-1}; [\boldsymbol{c}]_\iota)$ computes $\boldsymbol{R}^{-1}[\boldsymbol{c}]_\iota = [\boldsymbol{M'}\left(\begin{smallmatrix} \boldsymbol{x} \\ r \end{smallmatrix}\right)]_\iota = \left[\begin{smallmatrix} \boldsymbol{Mx} \\ \boldsymbol{r}^\top \boldsymbol{x}+r \end{smallmatrix}\right]_\iota$ and outputs $[\boldsymbol{Mx}]_\iota$ which is exatly what we wanted to extract.

(v: SPB) Clearly, there are no $\boldsymbol{x}_0, \boldsymbol{x}_1 \in \mathbb{Z}_p^n$ such that $\boldsymbol{Mx}_0 \neq \boldsymbol{Mx}_1$ and $[\boldsymbol{c}]_\iota := \mathsf{Com}(\mathsf{ck}; \boldsymbol{x}_0; \boldsymbol{r}_0) = \mathsf{Com}(\mathsf{ck}; \boldsymbol{x}_1; \boldsymbol{r}_1)$ since by the F-SSE property we have that $\mathsf{Ext}(\mathsf{p}, \mathsf{ek} = \boldsymbol{R}^{-1}; [\boldsymbol{c}]_\iota) = [\boldsymbol{Mx}_0]_\iota = [\boldsymbol{Mx}_1]_\iota$.

(vi: Sub-AEPH) Suppose a subverter Sub on input (p, n, q) outputs $(\mathsf{ck} = [\boldsymbol{g}], \mathsf{aux}_{\mathsf{Sub}})$ such that $\mathsf{CKV}(n, q, \mathsf{ck}) = 1$. We know from PKC property that there exists an extractor $\mathsf{Ext}_{\mathsf{Sub}}$ that on the same input outputs $\mathcal{S} = \boldsymbol{M} \in \mathbb{Z}_p^{q\times n}$ such that $\boldsymbol{g} = \boldsymbol{R} \cdot \boldsymbol{M'}$ where $\boldsymbol{M'} = \left(\begin{smallmatrix} \boldsymbol{M} & \boldsymbol{0} \\ \boldsymbol{r}^\top & 1 \end{smallmatrix}\right)$, $\boldsymbol{R} \in \mathbb{Z}_p^{(q+1)(q+1)}$ is some full rank matrix, and $\boldsymbol{r} \in \mathbb{Z}_p^n$. Let adversary $\mathcal{A}$ output $\boldsymbol{x}_0$ on input $(\mathsf{p}, \mathsf{ck}, \mathsf{aux}_{\mathsf{Sub}})$.

In order to prove Sub-AEPH we need to construct a simulator Sim that on input $(\mathtt{ck}, \boldsymbol{x}_{\mathcal{S}} = \boldsymbol{M}\boldsymbol{x}_0, \mathcal{S} = \boldsymbol{M})$ outputs a simulated commitment which is indistinguishable from $C_0 = \mathsf{Com}(\mathtt{ck}, \boldsymbol{x}, r_0)$ where $r_0 \leftarrow_{\$} \mathbb{Z}_p$. Our simulator works as follows. Given $\boldsymbol{y} := \boldsymbol{M}\boldsymbol{x}_0$ and $\boldsymbol{M}$ it solves a linear system of equations to find some solution $\boldsymbol{x}_1$ such that $\boldsymbol{y} = \boldsymbol{M}\boldsymbol{x}_1$ and then outputs a commitment $C_1 = \mathsf{Com}(\mathtt{ck}, \boldsymbol{x}_1; r_1)$ with $r_1 \leftarrow_{\$} \mathbb{Z}_p$.

Let us analyze distributions of C_0 and C_1. We know that $\boldsymbol{x}_0, \boldsymbol{x}_1 \in \mathbb{Z}_p^n$ are such that $\boldsymbol{M}\boldsymbol{x}_0 = \boldsymbol{M}\boldsymbol{x}_1$. For $\beta \in \{0, 1\}$, we can define $[\boldsymbol{u}_\beta] := [\boldsymbol{M'}(\begin{smallmatrix} \boldsymbol{x}_\beta \\ r_\beta \end{smallmatrix})] = \left[\begin{smallmatrix} \boldsymbol{M}\boldsymbol{x}_\beta \\ \boldsymbol{r}^\top \boldsymbol{x}_\beta + r_\beta \end{smallmatrix}\right]$. We see that top q elements of $\boldsymbol{u}_0$ and $\boldsymbol{u}_1$ are equal and the last element is uniformly random. Thus, $\boldsymbol{u}_0$ and $\boldsymbol{u}_1$ are indistinguishable. Since $C_\beta = \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}_\beta; r_\beta) = \boldsymbol{R}[\boldsymbol{u}_\beta]$, then also C_1 and C_2 are indistinguishable.

(vii: AEPT) Let $r_0 \in \mathbb{Z}_p$ and $\boldsymbol{x}_0, \boldsymbol{x}_1 \in \mathbb{Z}_p^n$ such that $\boldsymbol{M}\boldsymbol{x}_0 = \boldsymbol{M}\boldsymbol{x}_1$. In tdOpen, we define $r_1 = \sum_{i \in [1\,..\,n]} (x_{0,i} - x_{1,i}) r_i + r_0$. Then, $\boldsymbol{r}^\top \boldsymbol{x}_1 + r_1 = \boldsymbol{r}^\top \boldsymbol{x}_0 + r_0$. Using, the definition of $\boldsymbol{u}_b$ from the previous property, we see that $\boldsymbol{u}_0 = \boldsymbol{u}_1$ and then also $\mathsf{Com}(\mathtt{ck}; \boldsymbol{x}_0; r_0) = \mathsf{Com}(\mathtt{ck}; \boldsymbol{x}_1; r_1)$.

(viii: CB and CH) Follows directly from analog of Theorem 1. □

D On the q-SATSDH assumption

Let us first see that q-SATSDH is falsifiable. Observe that the challenger knows $z, s \in \mathbb{Z}_p$. Thus, upon receiving $(r, [\beta_1, \beta_2]_1, [\tilde{\beta_1}, \tilde{\beta_2}]_2, [\nu]_T)$ it verifies that: (a) $[1]_1[\tilde{\beta_1}]_2 = [\beta_1]_1[z]_2$, (b) $[1]_1[\tilde{\beta_2}]_2 = [\beta_2]_1[z]_2$, (c) $\frac{1}{z}[\beta_1]_1[\tilde{\beta_1}]_2 \neq [\beta_2]_1[1]_2$, and (d) $(s - r)[\nu]_T = \frac{1}{z}[\beta_1]_1[\tilde{\beta_1}]_2 - [\beta_2]_1[1]_2$.

We prove that if the Knowledge of Exponent Assumption in bilinear groups holds, then both q-TSDH and q-SATSDH assumptions are equivalent. We recall in the following the definition of the Bilinear Bilinear Diffie-Hellman Knowledge of Exponent assumption.

Definition 6 (Bilinear Diffie-Hellman Knowledge of Exponent Assumption, BDH-KE [ABLZ17]). *For all non-uniform PPT adversaries $\mathcal{A}$:*

$$\Pr\left[([\alpha_1]_1, [\alpha_2]_2 \| a) \leftarrow (\mathcal{A} \| \mathcal{X}_{\mathcal{A}})(\mathsf{gk}) : e([\alpha_1]_1, [1]_2) = e([1]_1, [\alpha_2]_2) \wedge a \neq \alpha_1\right] \approx 0,$$

where the probability is taken over $\mathsf{gk} \leftarrow \mathsf{Pgen}(1^\lambda)$ and the coin tosses of adversary $\mathcal{A}$.

Lemma 8. *Given a bilinear group $\mathsf{gk} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$, if the q-SATSDH assumption holds then the q-TSDH assumption holds.*

Proof. Assume that $\mathcal{A}$ is an adversary against the q-TSDH assumption, we construct another adversary $\mathcal{B}$ against q-SATSDH assumption that receives a challenge tuple $(\mathsf{gk}, \{[s^i]_{1,2}\}_{i=1}^q, [z]_2)$ and sends the elements $(\mathsf{gk}, \{[s^i]_{1,2}\}_{i=1}^q)$ to $\mathcal{A}$. $\mathcal{A}$ then returns $(r, [\nu]_T)$ that breaks q-TSDH. The adversary $\mathcal{B}$ chooses $\beta_1, \beta_2 \leftarrow \mathbb{Z}_p$ such that $\beta_1^2 \neq \beta_2$ and returns $\left(r, [\beta_1, \beta_2]_1, \beta_1[z]_2, \beta_2[z]_2, (\beta_1^2 - \beta_2)[\nu]_T\right)$ which breaks the q-SATSDH assumption. □

Lemma 9. *Given a bilinear group* $\mathsf{gk} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ *where* BDHKE *assumption holds, if the* q-TSDH *assumption holds then the* q-SATSDH *assumption holds.*

Proof. Assume that $\mathcal{A}$ is an adversary against the q-SATSDH assumption, we construct an another adversary $\mathcal{B}$ against the q-TSDH assumption that receives a challenge tuple $(\mathsf{gk}, \{[s^i]_{1,2}\}_{i=1}^{q})$. $\mathcal{B}$ chooses $z \leftarrow \mathbb{Z}_p$ and sends the elements $(\mathsf{gk}, \{[s^i]_{1,2}\}_{i=1}^{q}, [z]_2)$ to $\mathcal{A}$. The adversary $\mathcal{A}$ then returns $(r, [\beta_1, \beta_2]_1, [\beta_3, \beta_4]_2, [\nu]_T)$ that breaks q-SATSDH. Now $\mathcal{B}$ computes $[\hat{\beta}_1]_2 = \frac{1}{z}[\beta_3]_2$ and $[\hat{\beta}_2]_2 = \frac{1}{z}[\beta_4]_2$ which satisfy $e([\beta_i]_1, [1]_2) = e([1]_1, [\hat{\beta}_i]_2)$ for $i = 1, 2$. By the BDHKE assumption there exists and extractor of β_1, β_2 that solves the q-TSDH assumption with $\left(r, \frac{1}{\beta_1^2 - \beta_2}[\nu]_T\right)$. □