Round-Efficient Sub-linear Zero-Knowledge Arguments for Linear Algebra

Jae Hong Seo

Department of Mathematical Sciences and ISaC-RIM,
Seoul National University, Seoul, 151-747, Korea
jhsbhs0@snu.ac.kr

Abstract. The round complexity of interactive zero-knowledge arguments is an important measure along with communication and computational complexities. In the case of zero-knowledge arguments for linear algebraic relations over finite fields, Groth proposed (at CRYPTO 2009) an elegant methodology that achieves sub-linear communication overheads and low computational complexity. He obtained zero-knowledge arguments of sub-linear size for linear algebra using reductions from linear algebraic relations to equations of the form $z = \mathbf{x} *' \mathbf{y}$, where $\mathbf{x}$, $\mathbf{y} \in \mathbb{F}_p^n$ are committed vectors, $z \in \mathbb{F}_p$ is a committed element, and $*' : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p$ is a bilinear map. These reductions impose additional rounds on zero-knowledge arguments of sub-linear size. We focus on minimizing such additional rounds, and we reduce the rounds of sub-linear zero-knowledge arguments for linear algebraic relations as compared with Groth's zero-knowledge arguments for the same relations. To reduce round complexity, we propose a general transformation from a t-round zero-knowledge argument, satisfying mild conditions, to a $(t-2)$-round zero-knowledge argument; this transformation is of independent interest.

Keywords: Round-efficient zero-knowledge arguments, sub-linear zero-knowledge arguments, linear algebra.

1 Introduction

The round complexity of interactive zero-knowledge arguments is an important measure along with communication and computation complexities. In computer networks, interactions between entities consume the most time; hence, it is important to reduce the round complexity of protocols, and many researches have attempted devise round-efficient protocols [1,4,6,8,13,3,17,2,5,14,18,7].

To optimize round complexity, interactive zero-knowledge arguments can be usually transformed into non-interactive zero-knowledge arguments by using the Fiat-Shamir heuristic, i.e., a cryptographic hash function is used by the prover to compute the verifier's challenges. To prove the soundness property in such non-interactive zero-knowledge arguments, we should assume the so-called random oracle model such that the cryptographic hash functions are viewed as random

D. Catalano et al. (Eds.): PKC 2011, LNCS 6571, pp. 387–402, 2011.

oracles. Recently, non-interactive zero-knowledge arguments have been proposed without the random oracle model [10,11]; however, they require communication overheads of quasi-linear size or non-standard assumptions in bilinear groups.

Groth proposed interactive zero-knowledge arguments of sub-linear size for linear algebra [9]. They attain sub-linear communication size and require fewer assumptions than the non-interactive zero-knowledge arguments mentioned above, i.e., they require only the discrete logarithm assumption and common reference strings. Therefore, we start from [9] to obtain round-efficient zero-knowledge arguments of sub-linear size under minimal assumptions.

The techniques used in [9] yield zero-knowledge arguments of sub-linear size; however, they require several additional rounds. We believe that such additional rounds are not necessary to obtain zero-knowledge arguments of sub-linear size for statements involving linear algebra. In addition, we attempt to obtain round-efficient zero-knowledge arguments of sub-linear size for linear algebraic relations.

Our Contributions. The proposed method for obtaining round-efficient zero-knowledge arguments of sub-linear size for linear algebraic relations involves two steps.

First, we reduce arguments for linear algebra to two types of equations that use two different types of bilinear maps; one bilinear map is defined from $\mathbb{F}_p^n \times \mathrm{Mat}_{n\times n}(\mathbb{F}_p)$ to $\mathbb{F}_p^n$, and the other, from $\mathbb{F}_p^n \times \mathbb{F}_p^n$ to $\mathbb{F}_p^n$. In [9], all arguments are reduced to one type of bilinear equations. On the other hand, we do not try to reduce one type of bilinear equations to the other; however, we construct specific short-round zero-knowledge arguments for each type of bilinear equations. Thus, we can obtain shorter rounds than those of [9]. As a result we reduce the three-to-one rounds of zero-knowledge arguments, as compared with those of [9].

Second, we propose a general transformation from a t-round zero-knowledge argument A to a $(t-2)$-round zero-knowledge argument A' if A satisfies some mild conditions that are satisfied by our zero-knowledge arguments and virtually the zero-knowledge arguments in [9]. We show that the rounds of all zero-knowledge arguments in [9] can be reduced by two using the proposed transformation for the same relation. Although the proposed transformation reduces the round complexity of zero-knowledge arguments, it increases the communication and computational complexities. However, for each reduction, the proposed transformation requires, at most 3 times more communication overheads than the original zero-knowledge arguments in [9].

Outline. In the next section, we introduce the notations, useful tools, and basic definitions used in this paper. In Section 3 we construct zero-knowledge arguments for two types of bilinear equations. In Section 4, we present a general transformation from t-round zero-knowledge arguments to $(t-2)$-round arguments with conditions when zero-knowledge arguments are eligible for transformation. In Section 5, we apply the general transformation to the zero-knowledge arguments obtained in Section 3. Finally, in Section 6, we compare the results with the zero-knowledge arguments of [9].

2 Preliminaries

Notation. We use $[a, b]$ to denote a set of integers, at least a and at most b. For a set S and an element $a \in S$, $a \xleftarrow{\$} S$ implies that a is randomly chosen from S. For an algorithm A, $A(x) \rightarrow s$ implies that A outputs s when its input is x.

Generalized Pedersen Commitment. We use the generalization of the Pedersen commitment scheme [16]. To commit to a vector in $\mathbb{F}_p^n$, we use a generalized Pedersen commitment $\mathsf{Com}(\cdot;\cdot) : \mathbb{F}_p^n \times \mathbb{F}_p \rightarrow G$, where p is a prime, $\mathbb{F}_p$ is a finite field of characteristic p, and G is a group of order p. The generalized Pedersen commitment scheme consists of two algorithms, the key generation algorithm K and the commitment algorithm C. K takes the security parameter λ as input, and it outputs $(G, g_1, \cdots, g_n, h)$, where G is a cyclic group of order p and $g_1, \cdots, g_n, h$ are randomly chosen generators of G. C takes a vector $\mathbf{x} = (\zeta^{(1)}, \cdots, \zeta^{(n)}) \in \mathbb{F}_p^n$ and a randomizer $r \in \mathbb{F}_p$ as input, and it outputs $\mathsf{Com}(\mathbf{x}; r) := h^r \prod_{j=1}^{n} g_j^{\zeta^{(j)}}$. The generalized Pedersen commitment scheme is a perfectly hiding and computationally binding commitment scheme under the discrete logarithm assumption in G.

The usefulness of the generalized Pedersen commitment scheme is attributed to its homomorphic property: For $\forall \mathbf{x}, \mathbf{y} \in \mathbb{F}_p^n$ and $r, s \in \mathbb{F}_p$,

$$\mathsf{Com}(\mathbf{x} + \mathbf{y}; r + s) = \mathsf{Com}(\mathbf{x}; r) \cdot \mathsf{Com}(\mathbf{y}; s).$$

Schwartz-Zippel Lemma. We use the Schwartz-Zippel lemma to prove the soundness property of arguments. The schwartz-Zippel lemma enables us to carry out a useful equality test for two multi-variate polynomials. Given two multi-variate d-degree polynomials, $f_1(x_1, \cdots, x_k)$ and $f_2(x_1, \cdots, x_k)$, we can test whether $f_1(e_1, \cdots, e_k) \stackrel{?}{=} f_2(e_1, \cdots, e_k)$ for randomly chosen $e_1, \cdots, e_k$ from $\mathbb{F}_p$. If $f_1 = f_2$, then the equality will always hold for all $e_1, \cdots, e_k$; however, if $f_1 \neq f_2$, then the equality will hold with probability at most d/p.

Lemma 1. *Let $f(x_1, \cdots, x_k)$ be a non-zero multivariate polynomial of degree d over $\mathbb{F}_p$. Then,*

$$Pr[f(e_1, \cdots, e_k) = 0] \leq \frac{d}{p},$$

where the probability goes over $e_1, \cdots, e_k$ randomly chosen from $\mathbb{F}_p$.

Special Honest Verifier Zero-Knowledge Arguments. In this paper, we are interested in Special Honest Verifier Zero-Knowlege (SHVZK) arguments of knowledge in the common reference string model. SHVZK arguments feature completeness, the SHVZK property, and witness-extended emulation. In particular, all the SHVZK arguments proposed in this paper have perfect completeness and perfect SHVZK. We refer to [12] for the formal definition of SHVZK arguments.

3 SHVZK Arguments for Equations with Vectors and Matrices

In this section we consider 6 types of equations over committed matrices $X_i, Y_i, Z \in \mathrm{Mat}_{n\times n}(\mathbb{F}_p)$, committed vectors $\mathbf{x}_i, \mathbf{y}_i, \mathbf{z} \in \mathbb{F}_p^n$, and committed elements $z \in \mathbb{F}_p$, with public $a_i \in \mathbb{F}_p$.

$$\begin{array}{lll} Z = \sum_{i=1}^m a_i X_i Y_i, & Z = \sum_{i=1}^m a_i X_i \circ Y_i, & \mathbf{z}^\top = \sum_{i=1}^m a_i X_i \mathbf{y}_i^\top, \\ \mathbf{z} = \sum_{i=1}^m a_i \mathbf{x}_i Y_i, & \mathbf{z} = \sum_{i=1}^m a_i \mathbf{x}_i \circ \mathbf{y}_i, & z = \sum_{i=1}^m a_i \mathbf{x}_i \mathbf{y}_i^\top, \end{array}$$

where $\circ$ is a entry-wise product, the so-called Hadamard product.

We propose SHVZK arguments for committed vectors and matrices of elements from $\mathbb{F}_p$ satisfying the equations stated above, which are typically used in linear algebra. In particular, we focus on the three lower equations because we can consider the three upper equations as a set of n equations of the corresponding types below. More precisely, there exists an 1-round reduction from several equations of the upper form to the corresponding lower equations without a public coefficient a_i [9]. Going a further, we can consider the last two lower equations as a bilinear equation of the form

$$\mathbf{z} = \sum_{i=1}^m a_i \mathbf{x}_i * \mathbf{y}_i,$$

where $* : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p^n$ is a bilinear map. One example of $*$ is the Hadamard product of two vectors in $\mathbb{F}_p^n$, and another example of $*$ is the standard inner product of two vectors in $\mathbb{F}_p^n$, obtained by filling zeros in $\mathbb{F}_p^{n-1}$ of the range $\mathbb{F}_p^n$. That is, $\mathbf{x} * \mathbf{y} := (\langle \mathbf{x}, \mathbf{y} \rangle, 0, \cdots, 0)$, where $\langle , \rangle$ is the standard inner product. Similarly, we can consider a product of a vector and a matrix as a bilinear map defined from $\mathbb{F}_p^n \times \mathrm{Mat}_{n\times n}(\mathbb{F}_p)$ to $\mathbb{F}_p^n$. For simplification, we assume that all public coins a_i are 1 because both the prover and the verifier can compute the commitment to $a_i \mathbf{x}_i$ from the committed $\mathbf{x}$ and public a_i.

First, we consider an equation $\mathbf{z} = \sum_{i=1}^m \mathbf{x}_i Y_i$, and next, we will consider a bilinear equation $\mathbf{z} = \sum_{i=1}^m \mathbf{x}_i * \mathbf{y}_i$. Let us consider an equation $\mathbf{z} = \sum_{i=1}^m \mathbf{x}_i Y_i$. We provide a 3-round SHVZK argument for a minimal case $\mathbf{z} = \mathbf{x}Y$; then, we provide a 2-round reduction from a general case to the minimal case.

3.1 SHVZK Arguments for $\mathbf{z} = \sum_{i=1}^m \mathbf{x}_i Y_i$

The Minimal Case. As the first step, we consider the statement $\mathbf{z} = \mathbf{x}Y$. Let $\mathbf{y}^{(j)}$ be the j-th row vector of Y, and $\mathbf{x} = (\zeta^{(1)}, \cdots, \zeta^{(n)})$.
Common Input (CI): $C_{\mathbf{x}} = \mathsf{Com}(\mathbf{x}; r), C_{\mathbf{y}^{(i)}} = \mathsf{Com}(\mathbf{y}^{(i)}; s^{(i)})$ for $i \in [1, n]$, $C_{\mathbf{z}} = \mathsf{Com}(\mathbf{z}; t)$ where $\mathbf{x}, \mathbf{y}^{(1)}, \cdots, \mathbf{y}^{(n)} \leftarrow \mathbb{F}_p^n$ and $s^{(1)}, \cdots, s^{(n)}, t \leftarrow \mathbb{F}_p$.
Prover Input (PI): $\mathbf{x}, \mathbf{y}^{(1)}, \cdots, \mathbf{y}^{(n)}, \mathbf{z}, r, s^{(1)}, \cdots, s^{(n)}$ and t where $\mathbf{z} \leftarrow \mathbb{F}_p^n$ and $t \leftarrow \mathbb{F}_p$.

Goal: Prove the knowledge of $\mathbf{x}$, Y and $\mathbf{z}$ such that $\mathbf{z} = \mathbf{x}Y$.

Prover		Verifier
Choose $\hat{\mathbf{x}} = (\hat{\zeta}^{(1)}, \cdots, \hat{\zeta}^{(n)}), \mathbf{y}^{(0)} \xleftarrow{\$} \mathbb{F}_p^n,\ \hat{r}, s^{(0)}, \hat{t} \xleftarrow{\$} \mathbb{F}_p.$		
Compute $C_{\hat{\mathbf{x}}} := \mathsf{Com}(\hat{\mathbf{x}}; \hat{r}),$ $C_{\mathbf{y}^{(0)}} := \mathsf{Com}(\mathbf{y}^{(0)}; s^{(0)}),$ $C_{\hat{\mathbf{z}}} := \mathsf{Com}(0; \hat{t}) \prod_{j=1}^{n} (C_{\mathbf{y}^{(j)}})^{\hat{\zeta}^{(j)}}.$		
Send	$\xrightarrow{C_{\hat{\mathbf{x}}}, C_{\mathbf{y}^{(0)}}, C_{\hat{\mathbf{z}}}}$	
		Choose $e \xleftarrow{\$} \mathbb{F}_p.$
	$\xleftarrow{e}$	Send
Compute $\tilde{\mathbf{x}} := \hat{\mathbf{x}} + e\mathbf{x},$ $\tilde{r} := \hat{r} + er,$ $\tilde{\mathbf{y}} := \sum_{j=0}^{n} e^j \mathbf{y}^{(j)},$ $\tilde{s} := \sum_{j=0}^{n} e^j s^{(j)},$ $\tilde{t} := \hat{t} + e(t - \sum_{j=1}^{n} \zeta^{(j)} s^{(j)}).$		
Send	$\xrightarrow{\tilde{\mathbf{x}}, \tilde{r}, \tilde{\mathbf{y}}, \tilde{s}, \tilde{t}}$	

The verifier accepts the argument if

$$
\begin{aligned}
&(1)\ \mathsf{Com}(\tilde{\mathbf{x}}; \tilde{r}) = C_{\hat{\mathbf{x}}} C_{\mathbf{x}}^{e}, \\
&(2)\ \mathsf{Com}(\tilde{\mathbf{y}}; \tilde{s}) = \textstyle\prod_{j=0}^{n} (C_{\mathbf{y}^{(j)}})^{e^j}, \\
&(3)\ \mathsf{Com}(0; \tilde{t}) \textstyle\prod_{j=1}^{n} (C_{\mathbf{y}^{(j)}})^{\tilde{\zeta}^{(j)}} = C_{\hat{\mathbf{z}}} C_{\mathbf{z}}^{e},
\end{aligned}
$$

where $\tilde{\mathbf{x}} = (\tilde{\zeta}^{(1)}, \cdots, \tilde{\zeta}^{(n)})$.

Theorem 1. *the above argument has perfect completeness, perfect SHVZK and witness-extended emulation.*

The proof of Theorem 1 is deferred to the full version of this paper.

2-Round Reduction to Minimal Case. We consider the statement $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i Y_i$. We follow Groth's 2-round reduction methodology from the general case $z = \sum_{i=1}^{m} \mathbf{x}_i \mathbf{y}_i$ to the minimal case $z = \mathbf{x}\mathbf{y}$. Let us briefly explain key idea before describing the argument in detail. First, we consider the product of following elements.

$$
\mathbf{x}' = \sum_{k=1}^{m} e^{k-1} \mathbf{x}_k \text{ and } \mathbf{y}'^{(j)} = \sum_{i=1}^{m} e^{m-i} \mathbf{y}_i^{(j)} \text{ for } j \in [1, n],
$$

where e is a random element in $\mathbb{F}_p$ and $\mathbf{y}_i^{(j)}$ be the j-th row vector of Y_i. Let $\mathbf{x}_i = (\zeta_i^{(1)}, \cdots, \zeta_i^{(n)})$. Then, the product is as follows:

$$
\mathbf{x}'Y' = \sum_{j=1}^{n} (\mathbf{y}'^{(j)} \sum_{k=1}^{m} e^{k-1} \zeta_k^{(j)}) = \sum_{\ell \in [0, 2m-2]} e^{\ell} (\sum_{j=1}^{n} \sum_{\substack{i,j: \\ \ell = m-i+k-1}} \mathbf{y}_i^{(j)} \zeta_k^{(j)})
$$

In the above equation, the part corresponding to $\ell = m-1$ is exactly equal to $\sum_{i=1}^{m} \mathbf{x}_i Y_i$. The prover sends commitments to $\mathbf{z}_\ell$ which is suppose to be $\sum_{j=1}^{n} \sum_{\substack{i,j: \\ \ell=m-i+k-1}} \mathbf{y}_i^{(j)} \zeta_k^{(j)}$ (set $\mathbf{z}_{m-1}$ by $\mathbf{z}$) before receiving the challenge e. Next, both the prover and the verifier compute commitments to $\mathbf{x}'$, Y', and $\sum_{\ell \in [0,2m-2]} e^\ell \mathbf{z}_\ell$ by using Com's additive homomorphic property; then, they run the minimal case with them as input. If the verifier accepts the transcript of the argument, then it means that the following equality holds with overwhelming probability:

$$\sum_{\ell \in [0,2m-2]} e^\ell \Big(\sum_{j=1}^{n} \sum_{\substack{i,j: \\ \ell=m-i+k-1}} \mathbf{y}_i^{(j)} \zeta_k^{(j)}\Big) \;=\; \sum_{\ell \in [0,2m-2]} e^\ell \mathbf{z}_\ell.$$

Since all commitments are chosen by the prover before he see the random challenge e, by Schwartz-Zippel lemma all coefficients of e^ℓ in the left side of above equality are equal to corresponding coefficients of the right side of above equality without probability at most $\frac{2m-2}{p}$. Therefore, $\mathbf{z} = \sum_{i \in [1,m]} \mathbf{x}_i Y_i$ with overwhelming probability.

Now, we provide the complete description of 2-round reduction from $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i Y_i$ to the minimal case $\mathbf{z} = \mathbf{x}Y$.

Common Input: $C_{\mathbf{x}_i} = \mathsf{Com}(\mathbf{x}_i; r_i), C_{\mathbf{y}_i^{(1)}} = \mathsf{Com}(\mathbf{y}_i^{(1)}; s_i^{(1)})$ for $i \in [1,m], j \in [1,n]$, $C_{\mathbf{z}} = \mathsf{Com}(\mathbf{z}; t)$.

Prover Input: $\mathbf{x}_i, r_i, \mathbf{y}_i^{(j)}, s_i^{(j)}$ for $i \in [1,m], j \in [1,n]$, and $\mathbf{z}, t$.

Goal: Prove the knowledge of $\mathbf{x}_i$, Y_i and $\mathbf{z}$ such that $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i Y_i$.

	Prover		Verifier
Choose	For $\ell \in [0, m-2] \cup [m, 2m-2], t_\ell \xleftarrow{\$} \mathbb{F}_p$.		
Set	$t_{m-1} := t - \sum_{i=1}^{m} \sum_{j=1}^{n} \zeta_i^{(j)} s_i^{(j)}$.		
Compute	$C_\ell := \mathsf{Com}(0; t_\ell) \prod_{\ell=m+k-i-1} \prod_{j=1}^{n} (C_{\mathbf{y}_i^{(j)}})^{\zeta_k^{(j)}}$.		
Then,	$C_{m-1} = C_{\mathbf{z}}$.		
Send		$\xrightarrow{C_0, \cdots, C_{2m-2}}$	
			Choose $e \xleftarrow{\$} \mathbb{F}_p$.
		$\xleftarrow{e}$	Send
Define	$C_{\mathbf{x}'} := \prod_{k=1}^{m} (C_{\mathbf{x}_k})^{e^{k-1}}$,		Define $C_{\mathbf{x}'}$,
	$C_{\mathbf{y}'(j)} := \prod_{i=1}^{m} (C_{\mathbf{y}_i^{(j)}})^{e^{m-i}}$,		$C_{\mathbf{y}'(j)}$,
	$C_{\mathbf{z}'} := \prod_{\ell=0}^{2m-2} (C_\ell)^{e^\ell}$.		$C_{\mathbf{z}'}$
Compute	an opening of $C_{\mathbf{x}'}$,		
	$\mathbf{x}' = \sum_{k=1}^{m} e^{k-1} \mathbf{x}_k,\ r' = \sum_{k=1}^{m} e^{k-1} r_k$,		
	an opening of $C_{\mathbf{y}'(j)}$,		
	$\mathbf{y}'^{(j)} = \sum_{i=1}^{m} e^{m-i} \mathbf{y}_i^{(j)},\ s_i'^{(j)} = \sum_{i=1}^{m} e^{m-i} s_i^{(j)}$,		
	and a randomizer of $C_{\mathbf{z}'}$,		
	$t' = \sum_{\ell=0}^{2m-2} e^\ell (t_\ell + \sum_{\ell=m+k-i-1} \sum_{j=1}^{n} \zeta_k^{(j)} s_i^{(j)})$.		
Run	minimal case with $C_{\mathbf{x}'}, C_{\mathbf{y}'(j)}$ and $C_{\mathbf{z}'}$		

Theorem 2. *The above argument has perfect completeness, perfect SHVZK and witness-extended emulation.*

Sketch of proof. Let $\mathbf{x}'$ be an opening vector of $C_{\mathbf{x}'}$, $\mathbf{y}'^{(j)}$ be an opening vector of $C_{\mathbf{y}'^{(j)}}$, and Y' be a matrix consisting of $\mathbf{y}'^{(j)}$ as its j-th row. Then, the product of a vector $\mathbf{x}'$ and a matrix Y' is equal to

$$\mathbf{x}' \cdot Y' = \sum_{j=1}^{n}((\sum_{k=1}^{m} e^{k-1}\zeta_k^{(j)}) \cdot (\sum_{i=1}^{m} e^{m-i}\mathbf{y}_i^{(j)})) = \sum_{j=1}^{n}\sum_{\ell=0}^{2m-2} e^{\ell}(\sum_{\ell=m+k-i-1} \zeta_k^{(j)}\mathbf{y}_i^{(j)}).$$

The right side of equality is equal to an opening vector of $C_{\mathbf{z}'}$; hence, the above argument has perfect completeness by perfect completeness of the SHVZK argument for the minimal case.

Now, we show that the above argument has perfect SHVZK. We describe a simulator $\mathcal{S}$ with inputs $CI = (C_{\mathbf{x}_i}, C_{\mathbf{y}_i^{(j)}}, C_{\mathbf{z}})$ and challenges, e_1 and e_2, that outputs the simulated argument with the same probability distribution to the real argument. First, $\mathcal{S}$ chooses $C_1, \cdots, C_{2m-2}$ as random commitment to $\mathbf{0}$ except $C_{m-1} = C_{\mathbf{z}}$, and it computes $C_{\mathbf{x}'}$, $C_{\mathbf{y}'^{(j)}}$ and $C_{\mathbf{z}'}$ by using e_1 according to their definition. Second, $\mathcal{S}$ feeds $C_{\mathbf{x}'}$, $C_{\mathbf{y}'^{(j)}}$, $C_{\mathbf{z}'}$, and e_2 to the simulator for the SHVZK argument for the minimal case. The simulated argument by $\mathcal{S}$ is identical to the real argument due to perfect SHVZK property of the minimal case and perfectly hiding property of Com,.

As the last step, we show that the argument has a witness-extended emulation. We can respectively obtain opening vectors $\mathbf{x}'$, $\mathbf{y}'^{(1)}, \cdots, \mathbf{y}'^{(n)}$ and $\mathbf{z}'$ of $C_{\mathbf{x}'}, C_{\mathbf{y}'^{(1)}}, \cdots, C_{\mathbf{y}'^{(n)}}$ and $C_{\mathbf{z}'}$ on random challenge e by using a witness-extended emulation for the SHVZK argument for the minimal case, so that these opening vectors satisfy $\mathbf{z}' = \mathbf{x}' \cdot Y'$. By definition of $C_{\mathbf{x}'}, C_{\mathbf{y}'^{(1)}}, \cdots, C_{\mathbf{y}'^{(n)}}$ and $C_{\mathbf{z}'}$, we have following equalities.

$$C_{\mathbf{x}'} = \prod_{k=1}^{m}(C_{\mathbf{x}_k})^{e^{k-1}}, \quad C_{\mathbf{y}'^{(j)}} = \prod_{i=1}^{m}(C_{\mathbf{y}_i^{(j)}})^{e^{m-i}}, \quad C_{\mathbf{z}'} = \prod_{\ell=1}^{2m-2}(C_\ell)^{e^\ell}.$$

By binding property of Com,

$$\mathbf{x}' = \sum_{k=1}^{m} e^{k-1}\mathbf{x}_k, \quad \mathbf{y}'^{(j)} = \sum_{i=1}^{m} e^{m-i}\mathbf{y}_i^{(j)}, \quad \mathbf{z}' = \sum_{\ell=0}^{2m-2} e^{\ell}\mathbf{z}_\ell,$$

where $\mathbf{x}_k$, $\mathbf{y}_i^{(j)}$, and $\mathbf{z}_\ell$ are openings vectors of $C_{\mathbf{x}_k}$, $C_{\mathbf{y}_i^{(j)}}$, and C_ℓ, respectively. We consider a vector $(1, e, \cdots, e^{2m-2})$ for random challenge e. When we have $2m-1$ such vectors for random challenge e, they are linearly independent with overwhelming probability, so that we can extract all $\mathbf{z}_0, \cdots, \mathbf{z}_{2m-2}$ from $2m-1$ equations on random e. Similarly, we can extract $\mathbf{x}_k$, $\mathbf{y}_i^{(j)}$ for all $k, i \in [1, m]$, $j \in [1, n]$ since m equations of $(1, e, \cdots, e^{m-1})$ for random e are linearly independent with overwhelming probability.

Now, we show that the extracted values $\mathbf{x}_k$, $\mathbf{y}_i^{(j)}$ and $\mathbf{z}$ satisfy $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i Y_i$. We already know that the extracted values satisfy $\mathbf{x}' = \sum_{k=1}^{m} e^{k-1}\mathbf{x}_k$, $\mathbf{y}'^{(j)} =$

$\sum_{i=1}^{m} e^{m-i}\mathbf{y}_i^{(j)}$, and $\mathbf{z}' = \sum_{\ell=0}^{2m-2} e^{\ell}\mathbf{z}_\ell$. The Schwartz-Zippel Lemma tells us the e^{m-1}'s coefficient of $\mathbf{x}'Y'$ should be equal to that of $\mathbf{z}'$ with overwhelming probability when we consider both $\mathbf{x}'Y'$ and $\mathbf{z}'$ as polynomials of e. The coefficient of e^{m-1} in $\mathbf{x}'Y'$ is $\sum_{j=1}^{n}\sum_{i=1}^{m}\zeta_i^{(j)}\mathbf{y}_i^{(j)}$ and the coefficient of e^{m-1} in $\mathbf{z}'$ is $\mathbf{z}_{m-1} = \mathbf{z}$. Therefore, we conclude that

$$\mathbf{z} = \sum_{j=1}^{n}\sum_{i=1}^{m}\zeta_i^{(j)}\mathbf{y}_i^{(j)} = \sum_{i=1}^{m}\mathbf{x}_i Y_i \qquad \square$$

3.2 SHVZK Arguments for $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i * \mathbf{y}_i$

We consider a SHVZK argument for $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i * \mathbf{y}_i$, where $* : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p^n$ is a bilinear map. Groth [9] proposed a SHVZK argument for $z = \sum_{i=1}^{m} \mathbf{x}_i *' \mathbf{y}_i$, where $*' : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p$ is a bilinear map. By simple extension from Groth's SHVZK argument for $z = \sum_{i=1}^{m} \mathbf{x}_i *' \mathbf{y}_i$, we can obtain 5-round SHVZK arguments for $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i * \mathbf{y}_i$. In particular, if we restrict $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i * \mathbf{y}_i$ to the case that $z = \sum_{i=1}^{m} \mathbf{x}_i \mathbf{y}_i^{\top}$, then it is totally same to that of [9]. Our key observation of this bilinear equation is that Hadamard product is already a bilinear map. In [9], the case that $\mathbf{z} = \sum_{i\in[1,m]} \mathbf{x}_i \circ \mathbf{y}_i$ is reduced to of the form $z = \sum_{i\in[1,m]} \mathbf{x}_i *' \mathbf{y}_i$, where $*'$ is a bilinear map, so that it requires total 6-round; however, we need just 5-round for zero-knowledge arguments.[1] We leave details of arguments in the full version of this paper.

4 General Transformation for Reducing Rounds of SHVZK Arguments

In this section, we present a general transformation from a t-round SHVZK argument $A = (K, \mathsf{P}, \mathsf{V})$, satisfying some condition, to a $(t-2)$-round SHVZK argument A', where K is a common reference string generator, and P and V are polynomial time interactive algorithms called the prover and the verifier, respectively. In Definition 1 we formally define the condition that is required to reduce an argument A to A'.

First, let us define the terms used in Definition 1. We write $< \mathsf{P}(x), \mathsf{V}(y) > \to tr$ for the public transcript tr produced by P and V with inputs x and y. The transcript tr can be written as $tr = (p_0; e_1; p_1; \cdots; e_m; p_m)$, where p_i is a value sent by the prover and e_i is a value sent by the verifier. We assumed that P is an interactive algorithm; hence, we can set p_i as an output of some function $P_i(PI, CI, \rho, e_1, \cdots, e_{i-1})$, where PI is the input prover's input PI, CI is the

[1] In [9], Groth constructed a SHVZK argument for the standard inner product and the Hadamard product by building a SHVZK argument for a bilinear equation $z = \sum_{i=1} \mathbf{x}_i * \mathbf{y}_i$ where $* : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p$ is a bilinear map. That is, $*$ can be considered as the standard inner product, or it can be considered as $\mathbf{x} * \mathbf{y} = \mathbf{x}(\mathbf{y} \circ \mathbf{t})^{\top}$, where $\mathbf{t}$ is a public vector chosen by the verifier. This approach requires one additional round for transmitting $\mathbf{t}$ to prove a SHVZK argument for the Hadamard product.

common input, ρ is the randomness of the prover, $e_1, \cdots, e_{i-1}$ are the challenges sent by V, and p_0 is an output of the function $P_0(PI, CI, \rho)$. Further, we assume that all e_i are independently and randomly chosen because we only consider SHVZK arguments. At the end of the interactions between P and V, the verifier accepts or rejects the statement. We write this procedure of the verifier as an algorithm with inputs CI and tr, $\mathsf{Ver}(CI, tr) \to \{0, 1\}$, where 0 and 1 correspond to V rejecting and accepting the statements, respectively.

Definition 1. *Let $A = (K, \mathsf{P}, \mathsf{V})$ be an argument for a relation R with completeness and soundness. For A, we use following notation:*

$$\begin{cases} < \mathsf{P}, \mathsf{V} > & \to tr = (p_0; e_1; p_1; \cdots; e_m; p_m) \\ \mathsf{Ver}(CI, tr) & \to \{0, 1\} \end{cases}$$

If there exist functions F_i and P'_i such that $F_i(p'_i, e_i) = P_i(PI, CI, \rho, e_1, \cdots, e_i)$ for some $i \in [1, m]$, where $p'_i = P'_i(PI, CI, \rho, e_1, \cdots, e_{i-1})$, then we define the reduced argument of A, $A' = (K', \mathsf{P}', \mathsf{V}')$ of A at i with F_i and P'_i for the relation R as follows:

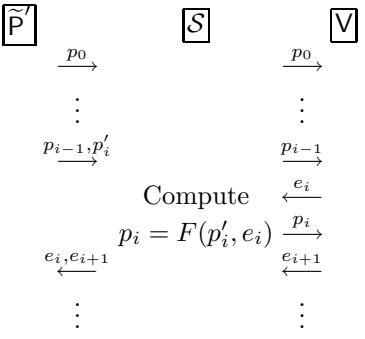
$$\begin{cases} K' & = K \\ < \mathsf{P}', \mathsf{V}' > & \to tr' = (p_0; \cdots; e_{i-1}; p_{i-1}, p'_i; e_i, e_{i+1}; p_{i+1}; \cdots; p_m) \\ \mathsf{Ver}'(CI, tr') & = \mathsf{Ver}(CI, (p_0; \cdots; p_{i-1}; e_i; F_i(p'_i; e_i); e_{i+1}; \cdots; p_m)) \end{cases}$$

The following lemma shows that a reduced argument also has the completeness and soundness if the original argument has. Although the reduced arguments have completeness and soundness, we need additional requirements for the reduced arguments to have the SHVZK property. We will consider the extra requirements for the SHVZK property after we state Lemma 2.

Lemma 2. *Let A be an argument for a relation R with completeness and soundness, and let A' be a reduced argument of A at i with F_i and P'_i for the relation R. Then, A' has completeness and soundness. Moreover, if A has a witness-extended emulation, then A' also has the same.*

Proof. Since $\mathsf{Ver}'(CI, tr') = \mathsf{Ver}(CI, tr)$ and A has completeness, A' also has completeness.

Let us consider the soundness of the argument A'. Assume that there exists a cheating prover $\widetilde{\mathsf{P}}'$ of argument A', with success probability ϵ. We construct a simulator $\mathcal{S}$ using $\widetilde{\mathsf{P}}'$ to cheat the verifier V of the argument A, with success probability ϵ. Now, we explain the role of $\mathcal{S}$. $\mathcal{S}$ interacts with $\widetilde{\mathsf{P}}'$ on behalf of the verifier of A', and it simultaneously interacts with a verifier V on behalf of the prover of A. $\mathcal{S}$ transfers $\widetilde{\mathsf{P}}'$'s message p_k to V and V's challenge e_{k+1} to $\widetilde{\mathsf{P}}'$ in order for $k \in [0, i-2]$. Then, $\mathcal{S}$ receives p_{i-1} and p'_i from $\widetilde{\mathsf{P}}'$, sends p_{i-1} to V, receives e_i from V, computes $p_i = F(p'_i, e_i)$, and sends it to V. V sends a challenge e_{i+1} to $\mathcal{S}$; then, $\mathcal{S}$ sends e_i and e_{i+1} to $\widetilde{\mathsf{P}}'$. Next, $\mathcal{S}$ transfers all the messages between $\widetilde{\mathsf{P}}'$ and V. The operations of $\mathcal{S}$' is shown below.



In $\widetilde{\mathsf{P}}'$'s view, simulated challenges are identical to real arguments. Therefore, the transcript tr' between $\widetilde{\mathsf{P}}'$ and $\mathcal{S}$ is accepted with probability ϵ, i.e., $\mathsf{Ver}'(CI, tr') = 1$ with probability ϵ. As aforementioned $\mathsf{Ver}'(CI, tr') = \mathsf{Ver}(CI, tr)$; hence V accepts with probability ϵ.

Now, we show that A' has a witness-extended emulation whenever A has a witness-extended emulation. We showed that we can construct a simulator $\mathcal{S}$ that performs the role of the prover of A by using the prover P' of A'. Therefore, the witness-extended emulation of A can extract a witness of A from $\mathcal{S}$. A and A' are arguments for the same relation R; hence, the lemma is complete. □

Now, we consider the SHVZK property of the reduced argument A' of A at i with F_i and P'_i. To show that A' has the SHVZK property, we should construct a simulator that can generate the prover's output $(p_0, \cdots, p'_i, \cdots, p_m)$ according to the randomness ρ of the prover from given the common input CI and all challenges $e_1, \cdots, e_m$. The following lemma shows the requirements for the SHVZK property of A'. We introduce the simple notations used to concisely state Lemma 3. For fixed PI ,CI, and $e_1, \cdots, e_m$, we define two probabilities $X_{(p_0,\cdots,p_i,\cdots,p_m)}$ and $Y_{(p_0,\cdots,p'_i,\cdots,p_m)}$. $X_{(p_0,\cdots,p_i,\cdots,p_m)}$ denotes the probability that the prover of the original argument A outputs $(p_0, \cdots, p_i, \cdots, p_m)$ for fixed $PI, CI, e_1, \cdots, e_m$. Similarly, $Y_{(p_0,\cdots,p_i,\cdots,p_m)}$ denotes the probability that the prover of the reduced argument A' outputs $(p_0, \cdots, p'_i, \cdots, p_m)$ for fixed $PI, CI, e_1, \cdots, e_m$. The probability of $X_{(p_0,\cdots,p_i,\cdots,p_m)}$ and $Y_{(p_0,\cdots,p'_i,\cdots,p_m)}$ goes over the prover's randomness ρ.

Lemma 3. *The reduced argument A' of A at i with F_i and P'_i has the SHVZK property if the original argument A has the SHVZK property, and there exists an algorithm Alg which runs as follows:*

Alg with input $CI, e_1, \cdots, e_n$, and $(p_0, \cdots, p_i, \cdots, p_m)$ outputs p'_i satisfying $p_i = F_i(p'_i, e_i)$, with probability

$$\frac{Y_{(p_0,\cdots,p'_i,\cdots,p_m)}}{X_{(p_0,\cdots,p_i,\cdots,p_m)}},$$

where Alg uses independent randomness.

Proof. We construct a simulator $\mathsf{Sim}^{A'}$ that generates all the output of the prover of argument A', $(p_0, \cdots, p'_i, \cdots, p_m)$. Thereafter, we show that for each $(p_0, \cdots, p'_i, \cdots, p_m)$, the probability that $\mathsf{Sim}^{A'}$ outputs $(p_0, \cdots, p'_i, \cdots, p_m)$, $\Pr[\mathsf{Sim}^{A'} \rightarrow (p_0, \cdots, p'_i, \cdots, p_m)]$, is equal to $Y_{(p_0, \cdots, p'_i, \cdots, p_m)}$. Then, the proof is complete.

The original argument A has the SHVZK property; hence, there exists a simulator Sim^{A} that can generate all the output of the prover of A, $(p_0, \cdots, p_i, \cdots, p_m)$, from the given common input CI and challenges $e_1, \cdots, e_m$ with the probability $X_{(p_0, \cdots, p_i, \cdots, p_m)}$. Now, we construct $\mathsf{Sim}^{A'}$ by using Sim^{A} and Alg. First, $\mathsf{Sim}^{A'}$ runs Sim^{A} with inputs CI and $e_1, \cdots, e_m$, and $(p_0, \cdots, p_i, \cdots, p_m)$ is obtained. Then, it runs Alg with inputs CI, $e_1, \cdots, e_m$, and $(p_0, \cdots, p_i, \cdots, p_m)$, and it receives Alg's output p'_i. Lastly, $\mathsf{Sim}^{A'}$ outputs $(p_0, \cdots, p'_i, \cdots, p_m)$.

We consider $\Pr[\mathsf{Sim}^{A'} \rightarrow (p_0, \cdots, p'_i, \cdots, p_m)]$ for each $(p_0, \cdots, p'_i, \cdots, p_m)$;

$$
\begin{aligned}
&\Pr[\mathsf{Sim}^{A'} \rightarrow (p_0, \cdots, p'_i, \cdots, p_m)] \\
&= \Pr[\mathsf{Sim}^{A} \rightarrow (p_0, \cdots, p_i, \cdots, p_m) \text{ such that } p_i = F_i(p'_i, e_i), \text{ and } Alg \rightarrow p'_i] \\
&= \Pr[\mathsf{Sim}^{A} \rightarrow (p_0, \cdots, p_i, \cdots, p_m) \text{ such that } p_i = F_i(p'_i, e_i)] \\
&\cdot\ \Pr[Alg(CI, e_1, \cdots, e_m, (p_0, \cdots, p_m)) \rightarrow p'_i] \\
&= X_{(p_0, \cdots, p_i, \cdots, p_m)} \cdot \frac{Y_{(p_0, \cdots, p'_i, \cdots, p_m)}}{X_{(p_0, \cdots, p_i, \cdots, p_m)}} \\
&= Y_{(p_0, \cdots, p'_i, \cdots, p_m)}.
\end{aligned}
$$

The probabilities go over all the randomness used by Sim^{A} and Alg. The second equality holds because the two algorithms Sim^{A} and Alg use independent randomness. □

5 Applying Transformation to SHVZK Arguments for Linear Algebra

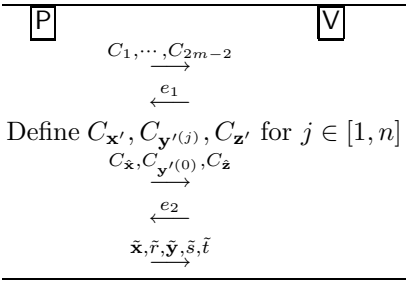
5.1 Application I: SHVZK Arguments for $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i \boldsymbol{Y}_i$

In this section, we apply the general transformation to SHVZK arguments for $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i Y_i$ presented in Section 3.1. Before applying the general transformation, we modify SHVZK arguments for $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i Y_i$. This modification does not affect the argument itself; however, it adds redundant computations on the prover side, thereby enabling us to easily apply the general transformation. Let us briefly review 5-round SHVZK arguments for $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i Y_i$. P and V perform the 2-move reduction to the minimal case; then, P starts the minimal case SHVZK by sending $C_{\hat{\mathbf{x}}}, C_{\mathbf{y}'^{(0)}}, C_{\hat{\mathbf{z}}}$, where

$$
C_{\hat{\mathbf{x}}} = \mathsf{Com}(\hat{\mathbf{x}}; \hat{r}), C_{\mathbf{y}'^{(0)}} = \mathsf{Com}(\mathbf{y}'^{(0)}; s'^{(0)}) \text{ for } \hat{\mathbf{x}}, \mathbf{y}'^{(0)} \xleftarrow{\$} \mathbb{F}_p^n, \hat{r}, s'^{(0)} \xleftarrow{\$} \mathbb{F}_p,
$$

$$
C_{\hat{\mathbf{z}}} = \mathsf{Com}(0; \hat{t}) \prod_{j=1}^{n} (C_{\mathbf{y}'^{(j)}})^{\hat{\zeta}^{(j)}} \text{ for } \hat{t} \xleftarrow{\$} \mathbb{F}_p, \text{ where } \hat{\mathbf{x}} = (\hat{\zeta}^{(1)}, \cdots, \hat{\zeta}^{(n)}).
$$

This process is shown below.



We modify this process by computing $C_{\hat{\mathbf{x}}}, C_{\mathbf{y}^{(0)}}$, and $C_{\hat{\mathbf{z}}}$ as follows:

Step (1). Compute $C_{\hat{\mathbf{x}}_k}$, $C_{\mathbf{y}'^{(0)}}$, and C'_ℓ as

$$C_{\hat{\mathbf{x}}_k} = \mathsf{Com}(\hat{\mathbf{x}}_k, \hat{r}_k) \text{ for } k \in [1, m], \text{ where } \hat{\mathbf{x}}_k \xleftarrow{\$} \mathbb{F}_p^n, \hat{r}_k \xleftarrow{\$} \mathbb{F}_p,$$
$$C_{\mathbf{y}'^{(0)}} = \mathsf{Com}(\mathbf{y}'^{(0)}; s'^{(0)}) \text{ where } \mathbf{y}'^{(0)} \xleftarrow{\$} \mathbb{F}_p^n, s'^{(0)} \xleftarrow{\$} \mathbb{F}_p,$$
$$C'_\ell = \mathsf{Com}(0; \hat{t}_\ell)\Big(\prod_{i,k:\ell=m+k-i-1} \prod_{j=1}^{n} C_{\mathbf{y}_i^{(j)}}^{\hat{\zeta}_k^{(j)}}\Big), \text{ where } \hat{\mathbf{x}}_k = (\hat{\zeta}_k^{(1)}, \cdots, \hat{\zeta}_k^{(n)}).$$

Step (2). Compute $C_{\hat{\mathbf{x}}}$ and $C_{\hat{\mathbf{z}}}$ using $C_{\hat{\mathbf{x}}_k}$, C'_ℓ, and the first challenge e_1 as follows:

$$C_{\hat{\mathbf{x}}} = \prod_{k=1}^{m} (C_{\hat{\mathbf{x}}_k})^{e_1^{k-1}}, \quad C_{\hat{\mathbf{z}}} = \prod_{\ell=0}^{2m-2} C_\ell'^{e_1^\ell}.$$

Then, $C_{\hat{\mathbf{x}}} = \prod_{k=1}^{m} (C_{\hat{\mathbf{x}}_k})^{e_1^{k-1}} = \mathsf{Com}(\sum_{k=1}^{m} e_1^{k-1} \hat{\mathbf{x}}_k; \sum_{k=1}^{m} e_1^{k-1} \hat{r}_k)$. $\sum_{k=1}^{m} e_1^{k-1} \hat{\mathbf{x}}_k$ and $\sum_{k=1}^{m} e_1^{k-1} \hat{r}_k$ are uniformly distributed; hence, $C_{\hat{\mathbf{x}}}$ has the same distribution as that before modification. The $C_{\hat{\mathbf{z}}}$ case is slightly complicated.

$$\begin{aligned}
C_{\hat{\mathbf{z}}} &= \prod_{\ell=0}^{2m-2} C_\ell'^{e_1^\ell} \\
&= \prod_{\ell=0}^{2m-2} \mathsf{Com}(0; \hat{t}_\ell)^{e_1^\ell} \Big(\prod_{i,k:\ell=m+k-i-1} \prod_{j=1}^{n} C_{\mathbf{y}_i^{(j)}}^{\hat{\zeta}_k^{(j)}}\Big)^{e_1^\ell} \\
&= \mathsf{Com}\Big(0; \sum_{\ell=0}^{2m-2} e_1^\ell \hat{t}_\ell\Big) \prod_{\ell=0}^{2m-2} \prod_{i,k:\ell=m+k-i-1} \prod_{j=1}^{n} (C_{\mathbf{y}_i^{(j)}}^{\hat{\zeta}_k^{(j)}})^{e_1^\ell} \\
&= \mathsf{Com}\Big(0; \sum_{\ell=0}^{2m-2} e_1^\ell \hat{t}_\ell\Big) \prod_{i=1}^{m} \prod_{k=1}^{m} \prod_{j=1}^{n} C_{\mathbf{y}_i^{(j)}}^{\hat{\zeta}_k^{(j)} e_1^{m+k-i-1}} \\
&= \mathsf{Com}\Big(0; \sum_{\ell=0}^{2m-2} e_1^\ell \hat{t}_\ell\Big) \prod_{j=1}^{n} \Big(\prod_{i=1}^{m} C_{\mathbf{y}_i^{(j)}}^{e_1^{m-i}}\Big)^{\sum_{k=1}^{m} e_1^{k-1} \hat{\zeta}_k^{(j)}}
\end{aligned}$$

$$= \mathsf{Com}(0; \sum_{\ell=0}^{2m-2} e_1^{\ell}\hat{t}_{\ell}) \prod_{j=1}^{n} (C_{\mathbf{y}'(j)})^{\hat{\zeta}^{(j)}},$$

where $\hat{x} = (\hat{\zeta}^{(1)}, \cdots, \hat{\zeta}^{(n)})$. $\sum_{\ell=0}^{2m-2} e_1^{\ell}\hat{t}_{\ell}$ is uniformly distributed; hence, $C_{\hat{\mathbf{z}}}$'s distribution in this modification is identical to the original distribution.

Now, we are ready to apply the general transformation to this modified SHVZK argument. In the modified argument, we consider the third move as an output of the function $P_1(PI, CI, \rho, e_1)$, and we can separate $P_1(PI, CI, \rho, e_1)$ into two steps. All the computations associated with the challenge e_1 are contained in *Step (2)* and not in *Step (1)*; thus, the function $P_1(PI, CI, \rho, e_1)$ can be rewritten as $F_1(P_1'(PI, CI, \rho), e_1)$, where P_1' is a function that denotes *Step(1)* and F_1 is a function that denotes *Step(2)*. Therefore, we can apply the general transformation in Definition 1 so that the reduced argument at 1 with F_1 and P_1' for the relation $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i Y_i$ has perfect completeness and witness-extended emulation by Lemma 2.

Next, to show that the reduced argument has perfect SHVZK, we construct an algorithm *Alg* satisfying the condition in Lemma 3. First, we consider the probabilities $X_{(p_0,p_1,p_2)}$ and $Y_{(p_0,p_1',p_2)}$ that are defined in Lemma 3. Since we use the perfect hiding commitment scheme, p_0 and p_1 are independent. Similarly, p_0 and p_1' are independent. Therefore, we obtain

$$\begin{aligned}
\frac{Y_{(p_0,p_1',p_2)}}{X_{(p_0,p_1,p_2)}} &= \frac{\Pr[P_0 = p_0] \cdot \Pr[P_1' = p_1'] \cdot \Pr[P_2 = p_2 | p_0, p_1']}{\Pr[P_0 = p_0] \cdot \Pr[P_1 = p_1] \cdot \Pr[P_2 = p_2 | p_0, p_1]} \\
&= \frac{\Pr[P_1' = p_1']}{\Pr[P_1 = p_1]} \\
&= \Pr[P_1' = p_1' | P_1 = p_1],
\end{aligned}$$

where P_i and P_1' are functions with input PI, CI, the randomness ρ, and appropriate verifier's challenges, and the probabilities go over ρ. The second equality holds since $\Pr[P_2 = p_2 | p_0, p_1'] = \Pr[P_2 = p_2 | p_0, p_1]$, and the last equality holds since the event $P_1'(PI, CI, \rho) = p_1'$ implies $P_1(PI, CI, \rho, e_1) = F_1(p_1', e_1) = p_1$. Now, we construct an algorithm *Alg* that outputs $p_1' = (C_{\hat{\mathbf{x}}_k}, C_{\mathbf{y}'(0)}, C_{\ell}')$ with above probability. *Alg* takes $C_{\hat{\mathbf{x}}}$, $C_{\hat{\mathbf{z}}}$ and e_1 as inputs, and it outputs uniform $C_{\hat{\mathbf{x}}_k}, C_{\mathbf{y}'(0)}$ and C_{ℓ}' satisfying the equalities of *Step(2)*. More precisely, *Alg* randomly chooses $C_{\mathbf{y}'(0)}$, $C_{\hat{\mathbf{x}}_k}$ and C_{ℓ}' for $k \in [2, m]$ and $\ell \in [1, 2m-2]$, and it computes $C_{\hat{\mathbf{x}}_1} = C_{\hat{\mathbf{x}}} \prod_{k=1}^{m} (C_{\hat{\mathbf{x}}_k})^{-e_1^{k-1}}$ and $C_0' = C_{\hat{\mathbf{z}}} \prod_{\ell=1}^{2m-2} (C_{\ell}')^{-e_1^{\ell}}$. Then, $C_{\hat{\mathbf{x}}_k}$ and C_{ℓ}' for $k \in [1, m]$, and $\ell \in [0, 2m-2]$ are uniformly distributed with the restrictions $C_{\hat{\mathbf{x}}} = \prod_{k=1}^{m} (C_{\hat{\mathbf{x}}_k})^{e_1^{k-1}}$ and $C_{\hat{\mathbf{z}}} = \prod_{\ell=0}^{2m-2} C_{\ell}'^{e_1^{\ell}}$. We can easily check that *Alg* satisfies the condition in Lemma 3, and the original argument has the SHVZK property so that, by Lemma 3, the reduced argument has perfect SHVZK.

Therefore, we obtain the following theorem. The complete description of the 3-round SHVZK for $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i Y_i$ is provided in the full version of this paper.

Theorem 3. *The reduced* 3*-round argument obtained by applying the general transformation to the* 5*-round SHVZK argument of the knowledge of committed values* $\mathbf{x}_i$*,* Y_i*, and* $\mathbf{z}$ *such that* $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i Y_i$ *has perfect completeness, perfect SHVZK, and witness-extended emulation.*

Complexity. The proposed argument requires 3 moves. The prover sends $5m-2$ commitments and $2n+3$ field elements to the verifier. The prover's computation is dominated by C_ℓ and C'_ℓ for $\ell \in [0, 2m-2]$, $C_{\mathbf{x}_k}$ for $k \in [1, m]$, and $\mathbf{y}'^{(j)}$. If we naively compute them, they require $2m^2n+mn$ group exponentiations and mn^2 field multiplications. However, if we sue the multi-exponentiation technique [15] for group exponentiation, they require less than $\frac{4m^2n\kappa}{\log m^2n} + \frac{2mn\kappa}{\log n}$ multiplications in G and mn^2 field multiplications, where κ is the size of p. The verifier computes $\frac{12m\kappa}{\log m}$ group multiplications to define $C_{\mathbf{x}'}, C_{\mathbf{z}'}, C_{\hat{\mathbf{x}}}$, and $C_{\hat{\mathbf{z}}}$, $\frac{2mn\kappa}{\log m}$ group multiplications to define $C_{\mathbf{y}'^{(j)}}$ for $j \in [1, m]$, and $\frac{8n\kappa}{\log n}$ group multiplications during the verification procedure. We can use the batch verification technique for reduction from $\frac{8n\kappa}{\log n}$ to $\frac{6n\kappa}{\log n}$ group multiplications.

5.2 Application II: SHVZK Arguments for $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i * \mathbf{y}_i$

We can apply the general transformation to the 5-round SHVZK argument for $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i * \mathbf{y}_i$ to reduce the 3-round SHVZK argument for the same relation. The basic strategy is similar to that in the case of SHVZK arguments for $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i * Y_i$. The details are provided in the full version of this paper.

Theorem 4. *The reduced* 3*-round argument obtained by applying the general transformation to the* 5*-round SHVZK argument of the knowledge of committed values* $\mathbf{x}_i$*,* Y_i *and* $\mathbf{z}$ *such that* $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i * \mathbf{y}_i$ *has perfect completeness, perfect SHVZK, and witness-extended emulation.*

6 Comparison

We compare our results with the SHVZK arguments in [9]. First, we briefly explain the results of [9]. In [9], several SHVZK arguments for linear algebraic equations as well as the 6 types of equations considered in this paper are proposed. For example, an equation where the product of two committed matrices is equal to the identity matrix, an equation where one committed matrix is (known or hidden) a permutation of another committed matrix, the satisfiability of an arithmetic circuit, etc. All such SHVZK arguments for linear algebraic equations need at least one SHVZK argument for one of three types of equations mainly considered in this paper, i.e.,

$$\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i Y_i, \qquad \mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i \circ \mathbf{y}_i, \qquad z = \sum_{i=1}^{m} \mathbf{x}_i \mathbf{y}_i^\top.$$

In particular, an SHVZK argument for $z = \sum_{i=1}^{m} \mathbf{x}_i \mathbf{y}_i^\top$ is used in all the SHVZK arguments for the linear algebraic equations in [9] since all the SHVZK arguments

are reduced to the case where $z = \sum_{i=1}^{m} \mathbf{x}_i \mathbf{y}_i^\top$. In cases where $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i Y_i$ and $z = \sum_{i=1}^{m} \mathbf{x}_i \circ \mathbf{y}_i$, 3-round reduction and 1-round reduction to the case where $z = \sum_{i=1}^{m} \mathbf{x}_i \mathbf{y}_i^\top$ are used, respectively.

For the three types of equations stated above, we obtain 3-round SHVZK arguments that have smaller rounds than those in [9]; however, their communication overheads are similar to those in [9]. In the case where $z = \sum_{i=1}^{m} \mathbf{x}_i \mathbf{y}_i^\top$ we built a 3-round SHVZK argument with four times the communication and computational overheads of those in [9]. Therefore, we can reduce 2 rounds of each SHVZK argument for the linear algebraic equations in [9] with four times communication and computational overheads of those in [9]. Furthermore, in cases where $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i Y_i$ and $\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i \circ \mathbf{y}_i$, we reduced one and three more rounds than $z = \sum_{i=1}^{m} \mathbf{x}_i \mathbf{y}_i^\top$, respectively, by trading small additional computational overheads. Exact comparisons are provided in Table 1.

SHVZK Argument	Rounds		Communication	
	Ours	[9]	Ours	[9]
$\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i Y_i$	3	8	$5m\kappa' + 2n\kappa$	$7m\kappa' + 2n\kappa$
$\mathbf{z} = \sum_{i=1}^{m} \mathbf{x}_i \circ \mathbf{y}_i$	3	6	$8m\kappa' + 2n\kappa$	$2m\kappa' + 2n\kappa$
$z = \sum_{i=1}^{m} \mathbf{x}_i \mathbf{y}_i^\top$	3	5	$8m\kappa' + 2n\kappa$	$2m\kappa' + 2n\kappa$

Table 1. Comparisons

Prover Computation		Verifier Computation	
Ours	[9]	Ours	[9]
$mn^2 + \frac{2mn\kappa\tau}{\log n} + \frac{4m^2n\kappa\tau}{\log mn}$	$9m^2n + 12m\kappa\tau + \frac{4mn\kappa\tau}{\log n}$	$\frac{12m\kappa}{\log m} + \frac{2mn\kappa}{\log m} + \frac{6n\kappa}{\log n}$	$2m\kappa\tau + \frac{24m\kappa\tau}{\log m} + \frac{2mn\kappa\tau}{\log n}$
$4m^2n + \frac{16mn\kappa\tau}{\log n}$	$2m^2n + 4m\kappa\tau + \frac{4n\kappa\tau}{\log n}$	$\frac{20m\kappa}{\log m} + \frac{2n\kappa}{\log n}$	$\frac{8m\kappa\tau}{\log m} + \frac{2n\kappa\tau}{\log n}$
$4m^2n + 12m\kappa\tau + \frac{4mn\kappa\tau}{\log n}$	$m^2n + 4m\kappa\tau + \frac{4n\kappa\tau}{\log n}$	$\frac{20m\kappa\tau}{\log m} + \frac{2n\kappa\tau}{\log n}$	$\frac{8m\kappa\tau}{\log m} + \frac{2n\kappa\tau}{\log n}$

$\mathbf{x}_i, \mathbf{y}_i, \mathbf{z} \in \mathbb{F}_p^n$, $z \in \mathbb{F}_p$, $Y_i \in \mathrm{Mat}_{n\times n}(\mathbb{F}_p)$,
κ': size of group element in G, κ: size of field element in $\mathbb{F}_p$,
τ: cost of multiplication in G measured in multiplication in $\mathbb{F}_p$.

Acknowledgments. We would like to thank Jung Hee Cheon and Jens Groth for helpful discussions and suggestions. This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (2010-0001655).

References

1. Bar-Ilan, J., Beaver, D.: Non-cryptographic fault-tolerant computing in a constant number of rounds. In: ACM PODC, pp. 201–209 (1989)
2. Beaver, D.: Minimal-latency secure function evaluation. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 335–350. Springer, Heidelberg (2000)

3. Beaver, D., Feigenbaum, J., Kilian, J., Rogaway, P.: Locally random reductions: Improvements and applications. Journal of Cryptology 10, 17–36 (1997)
4. Beaver, D., Micali, S., Rogaway, P.: The round complexity of secure protocols. In: STOC, pp. 503–513. ACM, New York (1990)
5. Cachin, C., Camenisch, J., Kilian, J., Müller, J.: One-round secure computation and secure autonomous mobile agents. In: Welzl, E., Montanari, U., Rolim, J.D.P. (eds.) ICALP 2000. LNCS, vol. 1853, p. 512. Springer, Heidelberg (2000)
6. Feige, U., Kilian, J., Naor, M.: A minimal model for secure computation. In: STOC, pp. 554–563 (1994)
7. Gennaro, R., Ishai, Y., Kushilevitz, E., Rabin, T.: The round complexity of verifiable secret sharing and secure multicast. In: STOC, pp. 580–589 (2001)
8. Goldreich, O., Kahan, A.: How to construct contant-round zero-knowledge proof systems for np. Journal of Cryptology 9, 167–190 (1996)
9. Groth, J.: Linear algebra with sub-linear zero-knowledge arguments. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 192–208. Springer, Heidelberg (2009)
10. Groth, J.: Short non-interactive zero-knowledge proofs. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 341–358. Springer, Heidelberg (2010)
11. Groth, J.: Short pairing-based non-interactive zero-knowledge arguments. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 321–340. Springer, Heidelberg (2010)
12. Groth, J.: Honest Verifier Zero-Knowledge Arguments Applied. PhD thesis, Department of Computer Science, University of Aarhus (June 2004)
13. Ishai, Y., Kushilevitz, E.: Private simultaneous messages protocols with applications. In: ISTCS, pp. 174–184 (1997)
14. Ishai, Y., Kushilevitz, E.: Randomizing polynomials: A new representation with applications to round-efficient secure computation. In: FOCS, pp. 294–304 (2000)
15. Lim, C.H.: Efficient multi-exponentiation and application to batch verification of digital signatures (2000), `http://dasan.sejong.ac.kr/~chlim/pub/multi_exp.ps`
16. Pedersen, T.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 129–140. Springer, Heidelberg (1992)
17. Sander, T., Young, A., Yung, M.: Non-interactive cryptocomputing for nc1. In: FOCS, pp. 554–567 (1999)
18. Tzeng, W.-G., Tzeng, Z.-J.: Round-efficient conference key agreement protocols with provable security. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 614–627. Springer, Heidelberg (2000)