Groth-Sahai Proofs Revisited Again:
A Bug in “Optimized” Randomization

Keita Xagawa

NTT Secure Platform Laboratories
xagawa.keita@lab.ntt.co.jp
May 20, 2016

Abstract. The Groth-Sahai proof system (EUROCRYPT 2008, SIAM Journal of Computing 41(5) [GS12]) provides efficient non-interactive witness-indistinguishable (NIWI) and zero-knowledge (NIZK) proof systems for languages over bilinear groups and is a widely-used versatile tool to design efficient cryptographic schemes and protocols.

We revisit randomization of the prover in the GS proof system. We find an unnoticed bug in the “optimized” randomization in the symmetric bilinear setting with several assumptions, say, the DLIN assumption or the matrix-DH assumption. This bug leads to security issues of the GS NIWI proof system with “optimized” randomization for multi-scalar multiplication equations and the GS NIZK proof system with “optimized” randomization for certain cases of pairing product equations and multi-scalar multiplication equations.

Keywords: Non-interactive proof systems, the Groth-Sahai proof system, symmetric bilinear groups, the DLIN assumption

1 Introduction

Non-interactive witness-indistinguishable (NIWI) protocols and non-interactive zero-knowledge (NIZK) protocols [BFM88] are fundamental tools in cryptology and allow us to design complex cryptographic primitives/protocols in modular approach, e.g., group signatures [BMW03,BSZ05], universal designated-verifier signatures [SBWP03], and policy-based signatures [BF14].

In 2008, Groth and Sahai [GS12] proposed a new framework for NIWI/NIZK proof systems for languages related to bilinear groups, pairing product equations (PPEs), multi-scalar multiplication equations (MMEs), and quadratic equations (QEs). Designers of cryptographic protocols rapidly adopted the Groth-Sahai (GS) proof systems, because they have been longing for efficient and practical NI-WI/NIZK proof systems for such languages, and they have constructed more efficient protocols. After the GS proof system appeared, several efficient (and complex) cryptographic primitives proposed by employing the GS proof system and its improvements as a basic tool.

1.1 Our Contribution

We revisit randomization of a prover in the GS proof system and found an unnoticed bug in the “optimized” randomization in the symmetric setting; the “optimized” randomization is sometimes insufficient to hide the witness. This case happens when we construct a NIWI proof system for MMEs based on the DLIN assumption (or the matrix DH assumptions). This bug leads to security issues as follows:

- We disprove *perfect witness-indistinguishability with a hiding CRS (composable witness-indistinguishability)* of the GS NIWI proof system for MMEs based on the DLIN assumption [GS12, Section 6.3], which we call $\mathsf{GS}'_{\mathsf{Sym}}$.
- We disprove *computational witness-indistinguishability* of the GS NIWI proof system in [GS12, Section 10], which we call $\mathsf{GS}''_{\mathsf{Sym}}$.
- We point out that the simulation for composable zero-knowledge property fails in the case of the NIZK proof systems [GS12, Section 11] for certain cases of MMEs and PPEs based on the DLIN assumption, because the NIZK proof systems employed the NIWI proof system for MMEs.

Table 1 and Table 2 summarize the effect of the bug in the NIWI and NIZK proof systems instantiated from the DLIN assumption.

Remark 1.1. It is easy to remove the bug by avoiding the "optimized" randomization.

Remark 1.2. We check the security the NIWI proof systems with "optimized" randomization for special MMEs, which is employed in the NIZK proof systems for special PPEs, *in the generic-group model.* See Appendix A for the details.

Table 1. Properties of the NIWI GS proof systems with "optimized" randomization based on the DLIN assumption

Languages	$\mathsf{GS}'_{\mathsf{Sym}}$ [GS12, Section 6.3]	$\mathsf{GS}''_{\mathsf{Sym}}$ [GS12, Section 10]
PPE	Composable WI	Composable WI
MME	Not composable WI	Not computational WI
QE	Composable WI	Composable WI

Table 2. Properties of the NIZK GS proof systems with "optimized" randomization based on the DLIN assumption

Languages	Properties
PPE with $T = \mathcal{O}_T$	Composable ZK
PPE with $T = \sum_i e(\mathcal{P}_i, \mathcal{Q}_i)$	Simulation Fails
MME with $T = \mathcal{O}$	Simulation Fails
MME with $T \neq \mathcal{O}$	Simulation Fails
QE with $T = 0$	Composable ZK
QE with $T \neq 0$	Composable ZK

1.2 Related Works

Groth and Sahai [GS12] proposed the GS proof system in the prime/composite-order bilinear groups. They instantiated the proof systems from the subgroup decision, symmetric external Diffie-Hellman (SXDH), and decision-linear (DLIN) assumptions. Ghadafi, Smart, and Warinschi [GSW10] revisited the GS proofs; they corrected errors on functions in the conference version of [GS12] and adapted the GS proof system to the Type-2 pairing group with the symmetric DLIN assumption.

Freeman [Fre10], Seo [Seo12], and Seo and Cheon [SC12], and Herold, Hesse, Hofheinz, Ràfols, and Rupp [HHH+14] studied projecting (and canceling) bilinear groups in order to translate cryptographic schemes/protocols in the composite-order bilinear groups into those in the prime-order bilinear groups. As byproducts, they improved efficiency of the GS proof system in the prime-order bilinear groups by removing redundancy in the GS proof system. Escala, Herold, Kiltz, Ràfols, and Villar [EHK+13] studied several matrix-DH assumptions in the symmetric bilinear groups and proposed the GS proof system in the symmetric bilinear groups based on the matrix-DH assumptions. Escala and Groth [EG14] improved the efficiency of the GS proof system instantiated from the SXDH assumption.

To the best of our knowledge, there are no papers pointing out the bug of the "optimized" randomization. Papers referring [GS12] basically employed the GS proof system as the tool *in the black-box manner.* A few exceptions are papers studying the GS proof system itself or its properties. We notice that Seo [Seo12, Section 5.1] and Jutla and Roy [JR14, Section 5] avoided the bug of the "optimzied" randomization.

1.3 Organization

Section 2 briefly reviews definitions of NIWI and NIZK proof systems. Section 3 is a reminder of bilinear groups. Section 4 reviews the GS proof systems. Section 5 gives concrete attacks against the GS NIWI proof systems for MMEs based on the DLIN assumption and discusses the effect of the bug. Appendix A discusses the security of the NIWI proof systems for special MMEs in the generic-group model.

1.4 Notation

Let $N \in \mathbb{N}$ be a positive integer. For two matrices $\boldsymbol{X} \in \mathbb{Z}_N^{m\times n_1}$ and $\boldsymbol{Y} \in \mathbb{Z}_N^{m\times n_2}$, $(\boldsymbol{X} \mid \boldsymbol{Y}) \in \mathbb{Z}_N^{m\times(n_1+n_2)}$ is the concatenation of the columns of $\boldsymbol{X}$ and $\boldsymbol{Y}$. For two matrices $\boldsymbol{X} \in \mathbb{Z}_N^{m_1\times n}$ and $\boldsymbol{Y} \in \mathbb{Z}_N^{m_2\times n}$, $(\boldsymbol{X};\boldsymbol{Y}) \in \mathbb{Z}_N^{(m_1+m_2)\times n}$ is the concatenation of the rows of $\boldsymbol{X}$ and $\boldsymbol{Y}$. In what follows, $\vec{X}$ represents column vector $(X_1,\dots,X_k)^\top$ and $\boldsymbol{x}$ represents row vector $(x_1,\dots,x_k)$. Let K be a $\mathbb{Z}_N$-module. For a vector $\vec{X} \in K^k$, we denote a space spanned by $\vec{A}$ as $\langle\vec{X}\rangle = \{\boldsymbol{w}\vec{X} \mid \boldsymbol{w} \in \mathbb{Z}_N^k\}$.

2 Non-Interactive Proof Systems

We briefly review the syntax of non-interactive zero-knowledge and witness-indistinguishable proof systems.

Group-dependent languages: Let R be an efficiently computable *ternary* relation instead of binary relation, which consists from $(gk, x, w) \in \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^*$. We call gk a setup key, x a statement, and w a witness. By fixing gk, we define L_{gk} as a language induced by the relation R and gk, that is, $L_{gk} = \{x \in \{0,1\}^* \mid \exists w \text{ such that } (gk, x, w) \in R\}$.

Non-interactive proofs: A non-interactive proof system for a relation R (with setup) consists of the following algorithms; The group generation algorithm, $\mathsf{G}_{\mathsf{group}}$, on inputs 1^λ outputs (gk, sk), which is a pair of gk, the description of groups, and sk, some secret information of gk; The binding CRS generation algorithm, $\mathsf{G}_{\mathsf{bind}}$, takes gk, sk as input and outputs a common reference string, crs; The prover algorithm, P, takes gk, crs, string x, and witness w, and outputs a proof, π; and the verification algorithm, V, takes gk, crs, x, π and outputs its decision $0/1$, where 0 and 1 represents rejection and acceptance, respectively. We say that $(\mathsf{G}_{\mathsf{group}}, \mathsf{G}_{\mathsf{bind}}, \mathsf{P}, \mathsf{V})$ is *a non-interactive proof system* for R (with setup $\mathsf{G}_{\mathsf{group}}$) if it is complete and sound defined below.

In the following, we take "parameter-switching" approach to show the security. In the soundness setting, we employ the binding CRS generation algorithm $\mathsf{G}_{\mathsf{bind}}$ and we show the soundness on the CRS output by $\mathsf{G}_{\mathsf{bind}}$. In the WI setting, we employ the hiding CRS generation algorithm $\mathsf{G}_{\mathsf{hide}}$ instead of $\mathsf{G}_{\mathsf{bind}}$.

We follow the definitions in [GS12].

Perfect completeness: We say that the system is *perfectly complete* if the following holds: For any unbounded adversary A, we have that

$$\Pr\left[\begin{array}{c}(gk, sk) \leftarrow \mathsf{G}_{\mathsf{group}}(1^\lambda); crs \leftarrow \mathsf{G}_{\mathsf{bind}}(gk, sk); (x, w) \leftarrow \mathsf{A}(gk, crs); \pi \leftarrow \mathsf{P}(gk, crs, x, w) : \\ \mathsf{V}(gk, crs, x, \pi) = 1 \text{ if } (gk, x, w) \in R\end{array}\right] = 1.$$

Perfect culpable soundness: The soundness is relaxed by employing a promise version of the problem corresponding to a language L [GOS06, Gro06]. Let $L_{\mathrm{co}} \subset \{0,1\}^* \setminus L$. The system is *perfectly L_{co}-sound* if any adversary A cannot output a pair of an improper string and a valid proof (x, π) for $x \in L_{\mathrm{co}}$. We note that the adversary might be able to produce a valid proof π on $x \in (\{0,1\}^* \cap L) \setminus L_{\mathrm{co}}$.

Formally, we say that the system is perfectly L_{co}-sound if for any unbounded adversary A, the following holds:

$$\Pr\left[\begin{array}{c}(gk, sk) \leftarrow \mathsf{G}_{\mathsf{group}}(1^{\lambda}); crs \leftarrow \mathsf{G}_{\mathsf{bind}}(gk, sk); (x, \pi) \leftarrow \mathsf{A}(gk, crs) : \\ \mathsf{V}(gk, crs, x, \pi) = 0 \text{ if } x \in L_{\mathrm{co}}\end{array}\right] = 1.$$

If $L_{\mathrm{co}} = \{0, 1\}^* \setminus L$, we say the system perfectly sound.

Composable witness-indistinguishability: We say that the system is *composable witness-indistinguishable* if any PPT adversary cannot distinguish a binding CRS produced by $\mathsf{G}_{\mathsf{bind}}$ and a hiding CRS produced by $\mathsf{G}_{\mathsf{hide}}$ and if any unbounded adversary cannot distinguish a proof proved by the prover on a witnesses w_0 of x or a proof on a witness w_1 of x when the CRS is hiding.

Formally, the system is said to be *composable witness-indistinguishable* if the followings hold: For any PPT adversary A,

$$\begin{aligned}&\Pr\left[(gk, sk) \leftarrow \mathsf{G}_{\mathsf{group}}(1^{\lambda}); crs \leftarrow \mathsf{G}_{\mathsf{bind}}(gk, sk) : \mathsf{A}(gk, crs) = 1\right] \\ \approx_c &\Pr\left[(gk, sk) \leftarrow \mathsf{G}_{\mathsf{group}}(1^{\lambda}); (crs, \tau) \leftarrow \mathsf{G}_{\mathsf{hide}}(gk, sk) : \mathsf{A}(gk, crs) = 1\right]\end{aligned}$$

and for any unbounded adversary A,

$$\begin{aligned}&\Pr\left[(gk, sk) \leftarrow \mathsf{G}_{\mathsf{group}}(1^{\lambda}); (crs, \tau) \leftarrow \mathsf{G}_{\mathsf{hide}}(gk, sk); (x, w_0, w_1) \leftarrow \mathsf{A}(gk, crs); \pi \leftarrow \mathsf{P}(gk, crs, x, w_0) : \mathsf{A}(\pi) = 1\right] \\ = &\Pr\left[(gk, sk) \leftarrow \mathsf{G}_{\mathsf{group}}(1^{\lambda}); (crs, \tau) \leftarrow \mathsf{G}_{\mathsf{hide}}(gk, sk); (x, w_0, w_1) \leftarrow \mathsf{A}(gk, crs); \pi \leftarrow \mathsf{P}(gk, crs, x, w_1) : \mathsf{A}(\pi) = 1\right],\end{aligned}$$

where we require $(gk, x, w_0), (gk, x, w_1) \in R$.

Composable zero-knowledge: We say that the system is *composable zero-knowledge* if any PPT adversary cannot distinguish a binding CRS produced by $\mathsf{G}_{\mathsf{bind}}$ and a hiding CRS produced by $\mathsf{G}_{\mathsf{hide}}$ and if any powerful adversary cannot distinguish a proof generated by the prover on a witnesses w of $x \in L$ from a proof simulated by the simulator $\widetilde{\mathsf{P}}$ employing τ when the CRS is hiding.

Formally, the system is said to be *composable zero-knowledge* if the followings hold: For any PPT adversary A,

$$\begin{aligned}&\Pr\left[(gk, sk) \leftarrow \mathsf{G}_{\mathsf{group}}(1^{\lambda}); crs \leftarrow \mathsf{G}_{\mathsf{bind}}(gk, sk) : \mathsf{A}(gk, crs) = 1\right] \\ \approx_c &\Pr\left[(gk, sk) \leftarrow \mathsf{G}_{\mathsf{group}}(1^{\lambda}); (crs, \tau) \leftarrow \mathsf{G}_{\mathsf{hide}}(gk, sk) : \mathsf{A}(gk, crs) = 1\right]\end{aligned}$$

and for any unbounded adversary A,

$$\begin{aligned}&\Pr\left[(gk, sk) \leftarrow \mathsf{G}_{\mathsf{group}}(1^{\lambda}); (crs, \tau) \leftarrow \mathsf{G}_{\mathsf{hide}}(gk, sk); (x, w) \leftarrow \mathsf{A}(gk, crs, \tau); \pi \leftarrow \mathsf{P}(gk, crs, x, w) : \mathsf{A}(\pi) = 1\right] \\ = &\Pr\left[(gk, sk) \leftarrow \mathsf{G}_{\mathsf{group}}(1^{\lambda}); (crs, \tau) \leftarrow \mathsf{G}_{\mathsf{hide}}(gk, sk); (x, w) \leftarrow \mathsf{A}(gk, crs, \tau); \pi \leftarrow \widetilde{\mathsf{P}}(gk, crs, \tau, x) : \mathsf{A}(\pi) = 1\right],\end{aligned}$$

where we require $(gk, x, w) \in R$.

3 Bilinear Groups

We review bilinear groups and their properties. We employ additive notion for Affine groups throughout of the paper because it fits with linear algebra.

Definition 3.1 (bilinear groups). A bilinear group *for a commutative ring* $\mathbb{Z}_N = \mathbb{Z}_N$ *is* $\mathfrak{G} = (\mathbb{Z}_N, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$*, where* $(\mathbb{G}_i, \mathcal{P}_i)$ *(for* $i = 1, 2, T$*) is a description of a cyclic group of order* N*,* $\mathcal{P}_i$ *is a generator of* $\mathbb{G}_i$ *(for* $i = 1, 2, T$*), and* $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ *is a map satisfying the following properties:*

- *(bilinearity:) For any* $Q_1 \in \mathbb{G}_1, Q_2 \in \mathbb{G}_2, \alpha, \beta \in \mathbb{Z}_N$*, we have* $e(\alpha Q_1, \beta Q_2) = \alpha\beta \cdot e(Q_1, Q_2)$.
- *(Non-degeneracy:)* $\mathcal{P}_T = e(\mathcal{P}_1, \mathcal{P}_2)$.

We will write zero elements in $\mathbb{G}_i$ by O_i for $i = 1, 2, T$.

Definition 3.2 (Bilinear group generator). *Let $\lambda > 1$ be an integer. A bilinear group generator $\mathcal{G}_\lambda$ takes a security parameter 1^λ and outputs a bilinear group $\mathfrak{G} = (\mathbb{Z}_N, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$.*

We call a bilinear group with $\mathbb{G}_1 = \mathbb{G}_2$ and $\mathcal{P}_1 = \mathcal{P}_2$ *a symmetric bilinear group.* We also call a bilinear group generator which outputs a symmetric bilinear group always *a symmetric bilinear group generator.*

Definition 3.3 (DLIN assumption). *Fix $i = 1$ or 2. We say that* the decision linear (DLIN) assumption holds relative to $\mathcal{G}_\lambda$ and $\mathbb{G}_i$ *if for any PPT adversary* A*, its advantage*

$$\mathsf{Adv}_{\mathcal{G}_\lambda, \mathbb{G}_i, \mathsf{A}}(\lambda) := \left| \begin{array}{c} \Pr[\mathsf{A}(\mathfrak{G}, \mathcal{P}_i, \alpha\mathcal{P}_i, \beta\mathcal{P}_i, z_1\alpha\mathcal{P}_i, z_2\beta\mathcal{P}_i, (z_1+z_2)\mathcal{P}_i) = 1] \\ -\Pr[\mathsf{A}(\mathfrak{G}, \mathcal{P}_i, \alpha\mathcal{P}_i, \beta\mathcal{P}_i, z_1\alpha\mathcal{P}_i, z_2\beta\mathcal{P}_i, z_3\mathcal{P}_i) = 1] \end{array} \right|$$

is negligible in the security parameter λ, where the probability is taken over $\mathfrak{G} = (\mathbb{Z}_N, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow \mathcal{G}_\lambda$, $\alpha, \beta, z_1, z_2, z_3 \leftarrow \mathbb{Z}_N$, and the coins of A.

4 Review of the Groth-Sahai Proof System

We briefly review the Groth-Sahai proof systems [GS12].

Let $\mathfrak{G} = (\mathbb{Z}_N, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ be a bilinear group. Consider $\mathbb{Z}_N$-modules A_1, A_2, and A_T. Let $f : A_1 \times A_2 \to A_T$ be a bilinear map. For two vectors $\vec{a} = (a_1, \dots, a_k)^\top \in A_1^k$ and $\vec{b} = (b_1, \dots, b_k)^\top \in A_2^k$, we denote $\sum_{i \in [1,k]} f(a_i, b_i) \in A_T$ by $\vec{a}^\top \cdot \vec{b}$. We consider an equation defined as

$$t = \vec{a}^\top \cdot \vec{y} + \vec{x}^\top \cdot \vec{b} + \vec{x}^\top \cdot \boldsymbol{\Gamma} \vec{y},$$

where $\vec{x} \in A_1^m$ and $\vec{y} \in A_2^n$ are variables, $\vec{a} \in A_1^n$, $\vec{b} \in A_2^m$, $\boldsymbol{\Gamma} \in \mathbb{Z}_N^{m \times n}$, and $t \in A_T$ are constants.

Groth and Sahai considered four types of equations:

- Pairing Product Equations (PPEs): $A_1 = \mathbb{G}_1$, $A_2 = \mathbb{G}_2$, $A_T = \mathbb{G}_T$, and $f(X, Y) = e(X, Y) \in \mathbb{G}_T$.
- Multi-scalar Multiplication Equations (MMEs) over $\mathbb{G}_1$: $A_1 = A_T = \mathbb{G}_1$, $A_2 = \mathbb{Z}_N$, and $f(X, y) = yX \in \mathbb{G}_1$.
- Multi-scalar Multiplication Equations (MMEs) over $\mathbb{G}_2$: $A_1 = \mathbb{Z}_N$, $A_2 = A_T = \mathbb{G}_2$, and $f(x, Y) = xY \in \mathbb{G}_2$.
- Quadratic Equations (QEs): $A_1 = A_2 = A_T = \mathbb{Z}_N$ and $f(x, y) = xy \in \mathbb{Z}_N$.

4.1 CRS and Commitments

The group key *gk* defines a bilinear group $\mathfrak{G} = (\mathbb{Z}_N, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$. The CRS *crs* defines $(\mathbb{Z}_N, A_1, A_2, A_T, f, B_1, B_2, B_T, F, \iota_1, p_1, \iota_2, p_2, \iota_T, p_T, \vec{U}, \vec{V}, \boldsymbol{H}_1, \dots, \boldsymbol{H}_\eta)$ specified below.

A part of the CRS specifies three $\mathbb{Z}_N$-modules B_1, B_2, and B_T, and bilinear function $F : B_1 \times B_2 \to B_T$. We denote zero of B_i as O_{B_i}. For two vectors $\vec{a} = (a_1, \dots, a_k)^\top \in B_1^k$ and $\vec{b} = (b_1, \dots, b_k)^\top \in B_2^k$, we define "$\bullet$" by $\vec{a}^\top \bullet \vec{b} = \sum_{i \in [1,k]} F(a_i, b_i) \in B_T$.

In addition, the CRS contains $\vec{U} \in B_1^{\hat{m}}$, $\vec{V} \in B_2^{\hat{n}}$, and $\mathbb{Z}_N$-linear functions $\iota_i : A_i \to B_i$ for $i = 1, 2, T$. The commitment key for A_1 consists of $\vec{U} \in B_1^{\hat{m}}$ and $\iota_1 : A_1 \to B_1$. That for A_2 consists of $\vec{V} \in B_2^{\hat{n}}$ and $\iota_2 : A_2 \to B_2$. The CRS implicitly defines $\mathbb{Z}_N$-linear functions $p_i : B_i \to A_i$ for $i = 1, 2, T$.

The final part of the CRS is matrices $\boldsymbol{H}_1, \dots, \boldsymbol{H}_\eta$ to randomize the proof. The matrices generate all solutions of $\vec{U}^\top \bullet \boldsymbol{H}\vec{V} = O_{B_T}$, that is, $\langle \boldsymbol{H}_1, \dots, \boldsymbol{H}_\eta \rangle = \{\boldsymbol{H} \in \mathbb{Z}_N^{\hat{m} \times \hat{n}} \mid \vec{U}^\top \bullet \boldsymbol{H}\vec{V} = O_{B_T}\}$ in the WI setting.

We require the following properties :

- For any $\vec{a} \in A_1^k$ and $\vec{b} \in A_2^k$, $\iota_T(\vec{a}^\top \cdot \vec{b}) = \iota_1(\vec{a})^\top \bullet \iota_2(\vec{b})$.
- For any $\vec{A} \in B_1^k$ and $\vec{B} \in B_2^k$, $p_T(\vec{A}^\top \bullet \vec{B}) = p_1(\vec{A})^\top \cdot p_2(\vec{B})$.
- In the soundness setting, binding CRS yields $\langle \vec{U} \rangle \subseteq \ker(p_1)$ and $\langle \vec{V} \rangle \subseteq \ker(p_2)$.
- In the WI setting, hiding CRS yields $\iota_1(A_1) \subseteq \langle \vec{U} \rangle$ and $\iota_2(A_2) \subseteq \langle \vec{V} \rangle$.
- Binding CRS and hiding CRS are computationally indistinguishable under certain assumption, say, the DLIN assumption.

Commitments: To commit $x \in A_1$ with randomness $\boldsymbol{r} \leftarrow \mathbb{Z}_N^{\hat{m}}$, we compute $C_x = \iota_1(x) + \boldsymbol{r}\vec{U}$. For simplicity of the notation, we write the commitments of $\vec{x} \in A_1^m$ with randomness $\boldsymbol{R} = (\boldsymbol{r}_1; \ldots; \boldsymbol{r}_m) \in \mathbb{Z}_N^{m \times \hat{m}}$ by

$$\vec{C} = \iota_1(\vec{x}) + \boldsymbol{R}\vec{U} \in B_1^m.$$

To commit $y \in A_2$ with randomness $\boldsymbol{s} \leftarrow \mathbb{Z}_N^{\hat{n}}$, we compute $D_y = \iota_2(y) + \boldsymbol{s}\vec{V}$. For simplicity of the notation, we write the commitments of $\vec{y} \in B^n$ with randomness $\boldsymbol{S} = (\boldsymbol{s}_1; \ldots; \boldsymbol{s}_n) \in \mathbb{Z}_N^{n \times \hat{n}}$ by

$$\vec{D} = \iota_2(\vec{y}) + \boldsymbol{S}\vec{V} \in B_2^n.$$

4.2 Proof and Verification

Prover: The prover first commits $\vec{x} \in A_1^m$ and $\vec{y} \in A_2^n$ into $\vec{C} \in B_1^m$ and $\vec{D} \in B_2^n$ by using randomness $\boldsymbol{R} \in \mathbb{Z}_N^{m \times \hat{m}}$ and $\boldsymbol{S} \in \mathbb{Z}_N^{n \times \hat{n}}$, respectively. The prover picks $\boldsymbol{T} \leftarrow \mathbb{Z}_N^{\hat{n} \times \hat{m}}$ and $r_1, \ldots, r_\eta \leftarrow \mathbb{Z}_N$ and computes

$$\begin{aligned} \vec{\mathit{\Pi}} &:= \boldsymbol{R}^\top \iota_2(\vec{b}) + \boldsymbol{R}^\top \boldsymbol{\Gamma} \iota_2(\vec{y}) + \boldsymbol{R}^\top \boldsymbol{\Gamma} \boldsymbol{S} \vec{V} - \boldsymbol{T}^\top \vec{V} + \textstyle\sum_{i=1}^{\eta} r_i \boldsymbol{H}_i \vec{V} \in B_2^{\hat{m}} \\ \vec{\mathit{\Theta}} &:= \boldsymbol{S}^\top \iota_1(\vec{a}) + \boldsymbol{S}^\top \boldsymbol{\Gamma}^\top \iota_1(\vec{x}) + \boldsymbol{T}\vec{U} \in B_1^{\hat{n}}. \end{aligned}$$

Finally, the prover sends $\pi = (\vec{C}, \vec{D}, \vec{\mathit{\Pi}}, \vec{\mathit{\Theta}})$ as commitments and proofs.

Verifier: Upon receiving commitments $\vec{C} = (C_1, \ldots, C_m)^\top$ and $\vec{D} = (D_1, \ldots, D_n)^\top$ and proofs $\vec{\mathit{\Pi}} = (\mathit{\Pi}_1, \ldots, \mathit{\Pi}_{\hat{m}})^\top$ and $\vec{\mathit{\Theta}} = (\mathit{\Theta}_1, \ldots, \mathit{\Theta}_{\hat{n}})^\top$, the verifier checks if $C_i, \mathit{\Theta}_i \in B_1$ and $D_i, \mathit{\Pi}_i \in B_2$, and

$$\iota_1(\vec{a})^\top \bullet \vec{D} + \vec{C}^\top \bullet \iota_2(\vec{b}) + \vec{C}^\top \bullet \boldsymbol{\Gamma}\vec{D} = \iota_T(t) + \vec{U}^\top \bullet \vec{\mathit{\Pi}} + \vec{\mathit{\Theta}}^\top \bullet \vec{V}. \tag{1}$$

4.3 Groth and Sahai's Optimization in Symmetric Case

We next review the simplification for the symmetric case in [GS12, Section 6.3]. We suppose that $\hat{m} \geq \hat{n}$ and $\vec{V} = (U_1, \ldots, U_{\hat{n}})^\top$.

We define padding functions rpad and cpad that pads matrices by 0. [1]

Definition 4.1 (Padding functions rpad **and** cpad**).** *For any $\mathbb{Z}_N$-module $\mathcal{M}$ with zero $0_\mathcal{M}$, we define two padding functions:*

- $\mathrm{rpad}_\mathcal{M} : \mathcal{M}^{\hat{n} \times k} \to \mathcal{M}^{\hat{m} \times k}$ *that pads a matrix with $\hat{m} - \hat{n}$ $0_\mathcal{M}$-rows*
- $\mathrm{cpad}_\mathcal{M} : \mathcal{M}^{k \times \hat{n}} \to \mathcal{M}^{k \times \hat{m}}$ *that pads a matrix with $\hat{m} - \hat{n}$ $0_\mathcal{M}$-columns*

Apparently, they are $\mathbb{Z}_N$-linear. Notice that, for any $\boldsymbol{K} \in \mathbb{Z}_N^{\hat{n} \times \hat{m}}$, $\mathrm{cpad}_{\mathbb{Z}_N}(\boldsymbol{K}^\top) = \mathrm{rpad}_{\mathbb{Z}_N}(\boldsymbol{K})^\top$, $\mathrm{rpad}_B(\boldsymbol{K}\vec{U}) = \mathrm{rpad}_{\mathbb{Z}_N}(\boldsymbol{K})\vec{U}$, and $\boldsymbol{K}^\top \vec{V} = \mathrm{cpad}_{\mathbb{Z}_N}(\boldsymbol{K}^\top)\vec{U} = \mathrm{rpad}_{\mathbb{Z}_N}(\boldsymbol{K})^\top \vec{U}$. For brevity of notations, we omit the subscriptions from rpad and cpad in what follows.

[1] This operations are denoted by $(\cdot)'$ in [GS12].

Groth and Sahai defined a new proof as

$$\begin{aligned}\vec{\Phi} &:= \mathrm{rpad}(\vec{\Theta}) + \vec{\Pi}\\ &= \mathrm{rpad}\Big(\boldsymbol{S}^\top \iota_1(\vec{a}) + \boldsymbol{S}^\top \boldsymbol{\Gamma}^\top \iota_1(\vec{x}) + \boldsymbol{T}\vec{U}\Big)\\ &\quad + \boldsymbol{R}^\top \iota_2(\vec{b}) + \boldsymbol{R}^\top \boldsymbol{\Gamma} \iota_2(\vec{y}) + \boldsymbol{R}^\top \boldsymbol{\Gamma} \boldsymbol{S} \vec{V} - \boldsymbol{T}^\top \vec{V} + \textstyle\sum_{i=1}^{\eta} r_i \boldsymbol{H}_i \vec{V}\\ &= \boldsymbol{R}^\top \iota_2(\vec{b}) + \boldsymbol{R}^\top \boldsymbol{\Gamma} \iota_2(\vec{y}) + \mathrm{cpad}(\boldsymbol{S})^\top \iota_1(\vec{a}) + \mathrm{cpad}(\boldsymbol{S})^\top \boldsymbol{\Gamma}^\top \iota_1(\vec{x}) + \boldsymbol{R}^\top \boldsymbol{\Gamma} \mathrm{cpad}(\boldsymbol{S}) \vec{U}\\ &\quad + (\mathrm{rpad}(\boldsymbol{T}) - \mathrm{rpad}(\boldsymbol{T})^\top)\vec{U} + \textstyle\sum_{i=1}^{\eta} r_i \mathrm{cpad}(\boldsymbol{H}_i)\vec{U}.\end{aligned}$$

The verifier checks if

$$\iota_1(\vec{a})^\top \bullet \vec{D} + \vec{C}^\top \bullet \iota_2(\vec{b}) + \vec{C}^\top \bullet \boldsymbol{\Gamma}\vec{D} = \iota_T(T) + \vec{U}^\top \bullet \vec{\Phi}. \tag{2}$$

instead of eq. (1).

We denote by $\mathsf{GS}_{\mathsf{Sym}}$ the simplified GS NIWI proof system in this subsection. The following theorem says the distribution of $\vec{\Phi}$ is uniformly random conditioned on the verification equation. Thus, the system $\mathsf{GS}_{\mathsf{Sym}}$ is composable WI.

Theorem 4.1 (Adaption of [GS12, Theorem 8]). *In the WI setting where $\iota_1(A_1) \subseteq \langle \vec{U} \rangle$ and $\iota_2(A_2) \subseteq \langle \vec{V} \rangle$ and $\boldsymbol{H}_1, \ldots, \boldsymbol{H}_\eta$ generates all matrices $\boldsymbol{H}$ such that $\vec{U}^\top \bullet \boldsymbol{H}\vec{V} = O_{B_T}$, all satisfying witnesses $\vec{x}$, $\vec{y}$, $\boldsymbol{R}, \boldsymbol{S}$ yield proofs $\vec{\Phi} \in \langle \vec{U} \rangle^{\hat{n}} \times \langle \vec{V} \rangle^{\hat{m}-\hat{n}}$ that is uniformly distributed conditioned on the verification equation (1).*

Corollary 4.1. *Suppose that hiding CRS and binding CRS are computationally indistinguishable under certain assumption. Then, $\mathsf{GS}_{\mathsf{Sym}}$ is composable WI.*

4.4 "Optimized" Randomization

In [GS12, Section 6.3], Groth and Sahai observed that if $\bullet$ is symmetric, $\vec{U}^\top \bullet (\mathrm{rpad}(\boldsymbol{T}) - \mathrm{rpad}(\boldsymbol{T})^\top)\vec{U} = O_{B_T}$ for any $\boldsymbol{T} \in \mathbb{Z}_N^{\hat{n}\times\hat{m}}$. [2] They then removed the randomization term $(\mathrm{rpad}(\boldsymbol{T}) - \mathrm{rpad}(\boldsymbol{T})^\top)\vec{U}$ from the proof $\vec{\Phi}$. Formally speaking, they defined an "optimized" proof as

$$\begin{aligned}\vec{\Phi}' &:= \boldsymbol{R}^\top \iota_2(\vec{b}) + \boldsymbol{R}^\top \boldsymbol{\Gamma} \iota_2(\vec{y}) + \mathrm{cpad}(\boldsymbol{S})^\top \iota_1(\vec{a}) + \mathrm{cpad}(\boldsymbol{S})^\top \boldsymbol{\Gamma}^\top \iota_1(\vec{x}) + \boldsymbol{R}^\top \boldsymbol{\Gamma} \mathrm{cpad}(\boldsymbol{S}) \vec{U}\\ &\quad + \textstyle\sum_{i=1}^{\eta} r_i \mathrm{cpad}(\boldsymbol{H}_i)\vec{U}\end{aligned} \tag{3}$$

We denote by $\mathsf{GS}'_{\mathsf{Sym}}$ the GS NIWI proof system $\mathsf{GS}_{\mathsf{Sym}}$ employing this "optimized" randomization.

Witness indistinguishability: If $\hat{m} = \hat{n}$, that is, if $\vec{V} = \vec{U}$, then the randomization term $\sum_{i=1}^{\eta} r_i \mathrm{cpad}(\boldsymbol{H}_i)\vec{U}$ is uniformly distributed over $\{\vec{R} \in \langle \vec{U} \rangle^{\hat{m}} \mid \vec{U}^\top \bullet \vec{R} = O_{B_T}\}$ and there is no problem.

However, if $\hat{m} > \hat{n}$, the "optimized" randomization forgets to randomize with $U_{\hat{n}+1}, \ldots, U_{\hat{m}}$, because the last $\hat{m} - \hat{n}$ columns of $\mathrm{cpad}(\boldsymbol{H}_i)$ is zero. We give attacks exploing this point in Section 5.

5 Concrete Attacks against NIWI Proof Systems for MMEs

We notice that there are two versions of the NIWI proof systems for MMEs based on the DLIN assumption with "optimized" randomization; one is a direct adaption of $\mathsf{GS}'_{\mathsf{Sym}}$ in [GS12, Section 6.3] and the other is in [GS12, Section 10].

[2] $\vec{U}^\top \bullet (\mathrm{rpad}(\boldsymbol{T}) - \mathrm{rpad}(\boldsymbol{T})^\top)\vec{U} = \vec{U}^\top \bullet \mathrm{rpad}(\boldsymbol{T})\vec{U} - \vec{U}^\top \mathrm{rpad}(\boldsymbol{T})^\top \bullet \vec{U} = \vec{U}^\top \bullet \mathrm{rpad}(\boldsymbol{T})\vec{U} - (\vec{U}^\top \bullet \mathrm{rpad}(\boldsymbol{T})\vec{U})^\top = O_{B_T}$ by the symmetric property of $\bullet$.

5.1 Review of the Parameters of the GS Proof System for MMEs based on the DLIN Assumption

The parameters are defined in [GS12, Section 10]. Let $\mathfrak{G} = (\mathbb{Z}_N, \mathbb{G}, \mathbb{G}_T, e)$ be a symmetric-bilinear group. Define $B = \mathbb{G}^3$ and $B_T \subseteq \mathbb{G}_T^{3\times 3}$. Define $F : B \times B \to B_T$ by a mapping a pair $\boldsymbol{\mathcal{P}} = (\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3)$ and $\boldsymbol{Q} = (Q_1, Q_2, Q_3)$ to

$$\frac{1}{2}\left(\boldsymbol{\mathcal{P}}^\top \cdot \boldsymbol{Q} + \boldsymbol{Q}^\top \cdot \boldsymbol{\mathcal{P}}\right) = \frac{1}{2}\begin{pmatrix} 2e(\mathcal{P}_1, Q_1) & e(\mathcal{P}_1, Q_2) + e(\mathcal{P}_2, Q_1) & e(\mathcal{P}_1, Q_3) + e(\mathcal{P}_3, Q_1) \\ e(\mathcal{P}_1, Q_2) + e(\mathcal{P}_2, Q_1) & 2e(\mathcal{P}_2, Q_2) & e(\mathcal{P}_2, Q_3) + e(\mathcal{P}_3, Q_2) \\ e(\mathcal{P}_1, Q_3) + e(\mathcal{P}_3, Q_1) & e(\mathcal{P}_2, Q_3) + e(\mathcal{P}_3, Q_2) & 2e(\mathcal{P}_3, Q_3) \end{pmatrix}.$$

Let $U_1 = (\alpha\mathcal{P}, O, \mathcal{P})$ and $U_2 = (O, \beta\mathcal{P}, \mathcal{P})$, where $\alpha, \beta \leftarrow \mathbb{Z}_N$. Let $U_3 = (W_1, W_2, W_3) \in B = \mathbb{G}^3$ with

$$U_3 = \begin{cases} z_1 U_1 + z_2 U_2 & \text{for soundness} \\ z_1 U_1 + z_2 U_2 - (O, O, \mathcal{P}) & \text{for WI,} \end{cases}$$

for randomly chosen $z_1, z_2 \leftarrow \mathbb{Z}_N$. We define $\vec{U} = (U_1, U_2, U_3)^\top \in B^3$ and $\vec{V} = (V_1, V_2)^\top = (U_1, U_2)^\top \in B^2$. From the DLIN assumption, we cannot efficiently distinguish U_3 for soundness from U_3 for WI. The hiding CRS generator outputs $\vec{U}$ with U_3 for WI and the binding CRS generator outputs $\vec{U}$ with U_3 for soundness.

For simplicity of notation, we define $U^* = U_3 + (O, O, \mathcal{P})$. We define three $\mathbb{Z}_N$-linear functions

$$\begin{aligned} \iota_1 &: X \in \mathbb{G} \mapsto (O, O, X) \in B, \\ \iota_2 &: y \in \mathbb{Z}_N \mapsto yU^* \in B, \\ \iota_T &: Z \in \mathbb{G} \mapsto F\big(\iota_1(Z), \iota_2(1)\big) \in B_T. \end{aligned}$$

We omit the definitions of projecting functions p_1, p_2, p_T.

Finally, Groth and Sahai prepared a matrix $\boldsymbol{H}_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \\ 0 & 0 \end{pmatrix}$ as the basis of the solutions of $\{\boldsymbol{H} \in \mathbb{Z}_N^{3\times 2} \mid \vec{U}^\top \bullet \boldsymbol{H}\vec{V} = O_{B_T}\}$ for MMEs.

Remark 5.1. Precisely speaking, they chose $\boldsymbol{H}_1 = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$ in [GS12, page 1223]. It should be transposed.

5.2 Distinguishing Attack against $\mathbf{GS}'_{\mathsf{Sym}}$ for MMEs

Recall the structure of the proof (3):

$$\vec{\varPhi}' := \boldsymbol{R}^\top \iota_2(\vec{b}) + \boldsymbol{R}^\top\boldsymbol{\varGamma}\iota_2(\vec{y}) + \mathsf{cpad}(\boldsymbol{S})^\top\iota_1(\vec{a}) + \mathsf{cpad}(\boldsymbol{S})^\top\boldsymbol{\varGamma}^\top\iota_1(\vec{x}) + \boldsymbol{R}^\top\boldsymbol{\varGamma}\mathsf{cpad}(\boldsymbol{S})\vec{U} + r_1\mathsf{cpad}(\boldsymbol{H}_1)\vec{U}.$$

We can simplify it as

$$\vec{\varPhi}' = \boldsymbol{R}^\top \iota_2(\vec{b}) + \boldsymbol{R}^\top\boldsymbol{\varGamma}\iota_2(\vec{y}) + \boldsymbol{R}^\top\boldsymbol{\varGamma}\boldsymbol{S}\vec{V} + \mathsf{rpad}\Big(\boldsymbol{S}^\top\iota_1(\vec{a}) + \boldsymbol{S}^\top\boldsymbol{\varGamma}^\top\iota_1(\vec{x})\Big) + r_1\boldsymbol{H}_1\vec{V}.$$

Since the last element of the output of $\mathsf{rpad}(\cdot)$ is always O_B and $r_1\boldsymbol{H}_1\vec{V} = (r_1U_2, -r_1U_1, O_B)^\top$ does nothing on the last B-element, the proof reveals the last B-element of $\boldsymbol{R}^\top\iota_2(\vec{b}) + \boldsymbol{R}^\top\boldsymbol{\varGamma}\iota_2(\vec{y}) + \boldsymbol{R}^\top\boldsymbol{\varGamma}\boldsymbol{S}\vec{V}$.

Theorem 5.1. $\mathrm{GS}'_{\mathsf{Sym}}$ *for MMEs is not perfect WI in the WI setting. Thus, it is not composable WI.*

Proof. We show that we can determine which witness is used if we can solve the DL problem in $\mathbb{G}$. Let us consider an equation $\vec{a}^\top \cdot \vec{y} + \vec{x}^\top \cdot \vec{b} + \vec{x}^\top \cdot \boldsymbol{\varGamma}\vec{y} = t \in \mathbb{G}$ with $\vec{b} \neq \vec{0}$ or $\boldsymbol{\varGamma} \neq \boldsymbol{O}$. We suppose that there exist two witnesses $(\vec{x}_0, \vec{y}_0)$ and $(\vec{x}_1, \vec{y}_1)$ with $\vec{x}_0 \neq \vec{x}_1$. The simplest example is the equation $\mathcal{P} \cdot y + X \cdot 1 = O$ with witnesses $(\mathcal{P}, -1)$ and $(O, 0)$.

Suppose that the prover chooses two randomness $\boldsymbol{R} = (\boldsymbol{R}_1 \mid \boldsymbol{R}_2 \mid \boldsymbol{R}_3) \in \mathbb{Z}_N^{m\times 3}$ and $\boldsymbol{S} = (\boldsymbol{S}_1 \mid \boldsymbol{S}_2) \in \mathbb{Z}_N^{n\times 2}$ and generates two commitments

$$\vec{C} = \iota_1(\vec{x}) + \boldsymbol{R}\vec{U} \text{ and } \vec{D} = \iota_2(\vec{y}) + \boldsymbol{S}\vec{V}.$$

The prover then constructs the proof as

$$\begin{aligned}\vec{\varPhi}' &= \mathsf{rpad}\Big(\boldsymbol{S}^\top \iota_1(\vec{a}) + \boldsymbol{S}^\top \boldsymbol{\varGamma}^\top \iota_1(\vec{x})\Big) + \boldsymbol{R}^\top \iota_2(\vec{b}) + \boldsymbol{R}^\top \boldsymbol{\varGamma} \iota_2(\vec{y}) + \boldsymbol{R}^\top \boldsymbol{\varGamma} \boldsymbol{S}\vec{V} + r_1 \boldsymbol{H}_1 \vec{V} \\ &= \begin{pmatrix} *_1 \\ *_2 \\ \boldsymbol{R}_3^\top \iota_2(\vec{b}) + \boldsymbol{R}_3^\top \boldsymbol{\varGamma} \iota_2(\vec{y}) + \boldsymbol{R}_3^\top \boldsymbol{\varGamma}\boldsymbol{S}\vec{V} \end{pmatrix}.\end{aligned}$$

We additionally observe that $\boldsymbol{R}_3^\top \iota_2(\vec{b}) + \boldsymbol{R}_3^\top \boldsymbol{\varGamma}\iota_2(\vec{y}) + \boldsymbol{R}_3^\top \boldsymbol{\varGamma}\boldsymbol{S}\vec{V} = \boldsymbol{R}_3^\top(\iota_2(\vec{b}) + \boldsymbol{\varGamma}\vec{D}) \in B = \mathbb{G}^3$.

Given $\vec{C}$, $\vec{D}$, and $\vec{\varPhi}' = (\varPhi_1', \varPhi_2', \varPhi_3')^\top \in B^3$, we decide which witness is used as follows: Since we are powerful enough to solve the DL problem in $\mathbb{G}$, we can compute $\boldsymbol{R}^{(0)} = (\boldsymbol{R}_1^{(0)} \mid \boldsymbol{R}_2^{(0)} \mid \boldsymbol{R}_3^{(0)})$ and $\boldsymbol{R}^{(1)} = (\boldsymbol{R}_1^{(1)} \mid \boldsymbol{R}_2^{(1)} \mid \boldsymbol{R}_3^{(1)}) \in \mathbb{Z}_N^{n\times 3}$ satisfying $\vec{C} = \iota_1(\vec{x}_0) + \boldsymbol{R}^{(0)}\vec{U} = \iota_1(\vec{x}_1) + \boldsymbol{R}^{(1)}\vec{U}$. Notice that $\boldsymbol{R}^{(0)} \neq \boldsymbol{R}^{(1)}$ holds since $\vec{x}_0 \neq \vec{x}_1$. Now, we can check if

$$\varPhi_3' - (\boldsymbol{R}_3^{(\beta)})^\top(\iota_2(\vec{b}) + \boldsymbol{\varGamma}\vec{D}) = O_B$$

or not.

We note that the probability that $\iota_2(\vec{b}) + \boldsymbol{\varGamma}\vec{D} = \overrightarrow{O_B}$ is negligible since $\vec{b} \neq \vec{0}$ or $\boldsymbol{\varGamma} \neq \boldsymbol{O}$ holds from our choice of the equation. Meanwhile, the LHS of the check equation is $(\boldsymbol{R}_3 - \boldsymbol{R}_3^{(\beta)})^\top(\iota_2(\vec{b}) + \boldsymbol{\varGamma}\vec{D})$. Therefore, when $\boldsymbol{R} \neq \boldsymbol{R}_{(\beta)}$, the probability that $(\boldsymbol{R}_3 - \boldsymbol{R}_3^{(\beta)})^\top(\iota_2(\vec{b}) + \boldsymbol{\varGamma}\vec{D})$ is not O_B is overwhelming. On the other hand, when $\boldsymbol{R} = \boldsymbol{R}_{(\beta)}$, the LHS is always zero. Hence, the system is not perfect WI in the WI setting. □

5.3 Distinguishing Attack against a Variant of $\mathbf{GS}'_{\mathsf{Sym}}$ for MMEs

Let us quote the definitions of commitments and proofs in the GS NIWI proof system for MMEs based on the DLIN assumption from [GS12, Section 10, pp.1224-1225].

> Commit to the scalars $\vec{x} \in \mathbb{Z}_p^m$ and the group elements $\vec{\mathcal{Y}} \in G^n$ as
>
> $$\vec{c} = \iota'(\vec{x}) + R\vec{v} \qquad\qquad \vec{d} = \iota(\vec{\mathcal{Y}}) + S\vec{u}$$
>
> for randomly chosen $R \leftarrow \mathrm{Mat}_{m\times 2}(\mathbb{Z}_p)$, $S \leftarrow \mathrm{Mat}_{n\times 3}(\mathbb{Z}_p)$.
> (...)
> For each multi-scalar multiplication equation $\vec{a}\cdot\vec{\mathcal{Y}} + \vec{x}\cdot\vec{\mathcal{B}} + \vec{x}\cdot\Gamma\vec{\mathcal{Y}} = \mathcal{T}_2$ we use the symmetric map F. (...) The proof is for random $r_1 \leftarrow \mathbb{Z}_p$:

$$\vec{\phi} := R^\top \iota(\vec{\mathcal{B}}) + R^\top \Gamma \iota(\vec{\mathcal{Y}}) + (S')^\top \iota'(\vec{a}) + (S')^\top \Gamma^\top \iota'(\vec{x}) + R^\top \Gamma S' \vec{u} + r_1 H_1 \vec{u}.$$

They considered an MME $\vec{a}^\top \cdot \vec{\mathcal{Y}} + \vec{x}^\top \cdot \vec{\mathcal{B}} + \vec{x}^\top \cdot \Gamma\vec{\mathcal{Y}} = \mathcal{T}_2$, where $A_1 = \mathbb{Z}_N$, $A_2 = \mathbb{G}$, and $A_T = \mathbb{G}$. Removing inconsistency of dimensions, we obtain

$$\vec{\phi} := (R')^\top \iota(\vec{\mathcal{B}}) + (R')^\top \Gamma \iota(\vec{\mathcal{Y}}) + S^\top \iota'(\vec{a}) + S^\top \Gamma^\top \iota'(\vec{x}) + (R')^\top \Gamma S \vec{u} + r_1 H_1' \vec{u},$$

where R' is $\mathsf{rpad}(R)$. By replacing $(\vec{x}, \vec{\mathcal{Y}}, \vec{a}, \vec{\mathcal{B}}, R, S, \Gamma)$ with $(\vec{\mathcal{X}}, \vec{y}, \vec{\mathcal{A}}, \vec{b}, S, R, \Gamma^\top)$, we have, for the MME $\vec{\mathcal{A}}^\top \cdot \vec{y} + \vec{\mathcal{X}}^\top \cdot \vec{b} + \vec{\mathcal{X}}^\top \cdot \Gamma\vec{y} = \mathcal{T}$,

$$\begin{aligned}\vec{c} &:= \iota(\vec{\mathcal{X}}) + R\vec{u} \\ \vec{d} &:= \iota'(\vec{y}) + S\vec{v} \\ \vec{\phi} &:= (S')^\top \iota(\vec{\mathcal{A}}) + (S')^\top \Gamma^\top \iota(\vec{\mathcal{X}}) + R^\top \iota'(\vec{b}) + R^\top \Gamma \iota'(\vec{y}) + (S')^\top \Gamma^\top R\vec{u} + r_1 H_1' \vec{u}.\end{aligned}$$

Thus, we conclude that they alternatively defined the proof as

$$\begin{aligned}\vec{\varPhi}'' := {} & \boldsymbol{R}^\top \iota_2(\vec{b}) + \boldsymbol{R}^\top \boldsymbol{\Gamma} \iota_2(\vec{y}) + \mathsf{cpad}(\boldsymbol{S})^\top \iota_1(\vec{a}) + \mathsf{cpad}(\boldsymbol{S})^\top \boldsymbol{\Gamma}^\top \iota_1(\vec{x}) + \mathsf{cpad}(\boldsymbol{S})^\top \boldsymbol{\Gamma}^\top \boldsymbol{R}\vec{U} \\ & + r_1 \mathsf{cpad}(\boldsymbol{H}_1)\vec{U},\end{aligned}$$

since the proof in $\mathsf{GS}'_{\mathsf{Sym}}$ is defined as

$$\begin{aligned}\vec{\varPhi}' := {} & \boldsymbol{R}^\top \iota_2(\vec{b}) + \boldsymbol{R}^\top \boldsymbol{\Gamma} \iota_2(\vec{y}) + \mathsf{cpad}(\boldsymbol{S})^\top \iota_1(\vec{a}) + \mathsf{cpad}(\boldsymbol{S})^\top \boldsymbol{\Gamma}^\top \iota_1(\vec{x}) + \boldsymbol{R}^\top \boldsymbol{\Gamma} \mathsf{cpad}(\boldsymbol{S})\vec{U} \\ & + r_1 \mathsf{cpad}(\boldsymbol{H}_1)\vec{U}.\end{aligned}$$

We call the proof system with $\vec{\varPhi}''$ as $\mathsf{GS}''_{\mathsf{Sym}}$ for MMEs.

As in the case of $\vec{\varPhi}'$ in $\mathsf{GS}'_{\mathsf{Sym}}$, we observe

$$\begin{aligned}\vec{\varPhi}'' &= \boldsymbol{R}^\top \iota_2(\vec{b}) + \boldsymbol{R}^\top \boldsymbol{\Gamma} \iota_2(\vec{y}) + \mathsf{rpad}\Big(\boldsymbol{S}^\top \iota_1(\vec{a}) + \boldsymbol{S}^\top \boldsymbol{\Gamma}^\top \iota_1(\vec{x}) + \boldsymbol{S}^\top \boldsymbol{\Gamma}^\top \boldsymbol{R}\vec{U}\Big) + r_1 \boldsymbol{H}_1 \vec{V} \\ &= \boldsymbol{R}^\top (\iota_2(\vec{b} + \boldsymbol{\Gamma}\vec{y})) + \mathsf{rpad}\Big(\boldsymbol{S}^\top \iota_1(\vec{a}) + \boldsymbol{S}^\top \boldsymbol{\Gamma}^\top \iota_1(\vec{x}) + \boldsymbol{S}^\top \boldsymbol{\Gamma}^\top \boldsymbol{R}\vec{U}\Big) + r_1 \boldsymbol{H}_1 \vec{V}.\end{aligned}$$

The proof $\vec{\varPhi}''$ reveals $\boldsymbol{R}_3^\top (\iota_2(\vec{b} + \boldsymbol{\Gamma}\vec{y}))$ where $\boldsymbol{R}_3$ is the last column of $\boldsymbol{R}$, since $r_1 \boldsymbol{H}_1 \vec{V}$ does nothing on the last element.

In addition, we notice that $\iota_2(0) = 0U^* = O_B$ and, with overwhelming probability over the coins of CRS generation, for $z \neq 0 \in \mathbb{Z}_N$, $\iota_2(z) = zU^* \neq O_B$. From those observations, we can mount a stronger attack as follows:

Theorem 5.2. $\mathsf{GS}''_{\mathsf{Sym}}$ *for MMEs is not computational WI.*

Proof. We consider an equation $\vec{a}^\top \cdot \vec{y} + \vec{x}^\top \cdot \vec{b} + \vec{x}^\top \cdot \boldsymbol{\Gamma}\vec{y} = t$. We suppose that there exist two witnesses $(\vec{x}_0, \vec{y}_0)$ and $(\vec{x}_1, \vec{y}_1)$ with $\vec{y}_0 \neq \vec{y}_1$. We additionally suppose that $\vec{b} + \boldsymbol{\Gamma}\vec{y}_\eta \in \mathbb{Z}_N^m$ is $\vec{0}$ if $\eta = 0$ and not $\vec{0}$ otherwise. The simplest example is the equation $X \cdot 1 + X \cdot 1 \cdot y = \mathcal{O}$ with witness $(\mathcal{P}, -1)$ and $(\mathcal{O}, 0)$.

Suppose that the prover employs two randomness $\boldsymbol{R} = (\boldsymbol{R}_1 \mid \boldsymbol{R}_2 \mid \boldsymbol{R}_3) \in \mathbb{Z}_N^{n \times 3}$ and $\boldsymbol{S} = (\boldsymbol{S}_1 \mid \boldsymbol{S}_2) \in \mathbb{Z}_N^{m \times 2}$ and obtain two commitments

$$\vec{C} = \iota_1(\vec{x}) + \boldsymbol{R}\vec{U} \text{ and } \vec{D} = \iota_2(\vec{y}) + \boldsymbol{S}\vec{V}.$$

The prover then constructs the proof by computing

$$\begin{aligned}\vec{\varPhi}'' &= \boldsymbol{R}^\top \iota_2(\vec{b}) + \boldsymbol{R}^\top \boldsymbol{\Gamma} \iota_2(\vec{y}) + \mathsf{rpad}\Big(\boldsymbol{S}^\top \iota_1(\vec{a}) + \boldsymbol{S}^\top \boldsymbol{\Gamma}^\top \iota_1(\vec{x}) + \boldsymbol{S}^\top \boldsymbol{\Gamma}^\top \boldsymbol{R}\vec{U}\Big) + r_1 \boldsymbol{H}_1 \vec{V} \\ &= \begin{pmatrix} *_1 \\ *_2 \\ \boldsymbol{R}_3^\top (\iota_2(\vec{b} + \boldsymbol{\Gamma}\vec{y})) \end{pmatrix}.\end{aligned}$$

Let $\varPhi''_3 := \boldsymbol{R}_3^\top (\iota_2(\vec{b} + \boldsymbol{\Gamma}\vec{y}))$.

When $\vec{b} + \boldsymbol{\Gamma}\vec{y} = \vec{0}$, then $\varPhi''_3$ is $\boldsymbol{R}_3^\top \iota_2(\vec{0}) = O_B$; while if $\vec{b} + \boldsymbol{\Gamma}\vec{y} \neq \vec{0}$, then $\varPhi''_3 \neq O_B$ with overwhelming probability over the choice of $\boldsymbol{R}_3$. Therefore, with overwhelming probability, we can distinguish the case that $\vec{b} + \boldsymbol{\Gamma}\vec{y} = \vec{0}$ from the case $\vec{b} + \boldsymbol{\Gamma}\vec{y} \neq \vec{0}$. This breaks the computational WI property. □

5.4 Effects of the Bug: On NIZK Proof Systems Based on the DLIN Assumption

In [GS12, Section 11], Groth and Sahai discussed constructions of NIZK proof systems for MMEs and special PPEs. We summarize the effects of the bug on the NIZK proof systems.

- NIZK proof system for MMEs: This system directly employs the NIWI proof system for MMEs. Therefore, the simulation fails.
- NIZK proof system for PPEs with $t = \sum_i e(\mathcal{P}_i, \mathcal{Q}_i)$ for known $\mathcal{P}_i$, $\mathcal{Q}_i$: This system employs the NIWI proof system for a special MME, $1 \cdot \mathcal{X} - \delta \cdot \mathcal{Q} = \mathcal{O} \in G$. [3] Hence, the simulation fails.

We check the security of the NIWI proof system for the special MME, $1 \cdot \mathcal{X} - \delta \cdot \mathcal{Q} = \mathcal{O} \in G$, *in the generic group model* by using GGA (Generic Group Analyzer) [BFF$^+$14, BFF$^+$15, Fag15]. [4] GGA says that if $\mathcal{Q}$ is chosen randomly by the challenger, then the real proof employing witness $(\mathcal{Q}, 1)$ and the simulated proof employing witness $(\mathcal{O}, 0)$ are indistinguishable in the generic group model. For the detail, see Appendix A.

Acknowledgments

We are grateful to Jens Groth and Amit Sahai for their helpful comments. We thank Carla Ràfols for comments and discussions on their variant of the GS proof system [HHH$^+$14, Appendix F of the ePrint version]. We also thank Masayuki Abe and Miyako Ohkubo for helpful comments and discussions related to this work.

References

BF14. Mihir Bellare and Georg Fuchsbauer. Policy-based signatures. In Krawczyk [Kra14], pages 520–537. See also https://eprint.iacr.org/2013/413.

BFF$^+$14. Gilles Barthe, Edvard Fagerholm, Dario Fiore, John C. Mitchell, Andre Scedrov, and Benedikt Schmidt. Automated analysis of cryptographic assumptions in generic group models. In Garay and Gennaro [GG14a], pages 95–112. See also https://eprint.iacr.org/2014/458.

BFF$^+$15. Gilles Barthe, Edvard Fagerholm, Dario Fiore, Andre Scedrov, Benedikt Schmidt, and Mehdi Tibouchi. Strongly-optimal structure preserving signatures from type II pairings. In Jonathan Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 355–376. Springer, Heidelberg, 2015. See also https://eprint.iacr.org/2015/019.

BFM88. Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications (extended abstract). In Janos Simon, editor, *STOC '88*, pages 103–112. ACM, 1988.

BMW03. Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In Eli Biham, editor, *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 614–629. Springer, Heidelberg, 2003.

BSZ05. Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of group signatures: The case of dynamic groups. In Alfred Menezes, editor, *CT-RSA 2005*, volume 3376 of *LNCS*, pages 136–153. Springer, Heidelberg, 2005. See also https://eprint.iacr.org/2004/077.

EG14. Alex Escala and Jens Groth. Fine-tuning Groth-Sahai proofs. In Krawczyk [Kra14], pages 630–649. See also https://eprint.iacr.org/2013/662.

EHK$^+$13. Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge L. 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, 2013. See also https://eprint.iacr.org/2013/377.

Fag15. Edvard Fagerholm. *Automated analysis in generic groups*. PhD thesis, 2015. Available at http://repository.upenn.edu/edissertations/1053.

Fre10. David Mandell Freeman. Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 44–61. Springer, Heidelberg, 2010.

GG14a. Juan A. Garay and Rosario Gennaro, editors. *Advances in Cryptology - CRYPTO 2014, 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21 2014. Proceedings, Part I*, volume 8616 of *LNCS*. Springer, Heidelberg, 2014.

[3] The real prover employs a witness $(\mathcal{Q}, 1)$ and the simulator employs a witness $(\mathcal{O}, 0)$.

[4] Available at https://github.com/generic-group-analyzer/gga.

GG14b. Juan A. Garay and Rosario Gennaro, editors. *Advances in Cryptology - CRYPTO 2014, 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21 2014. Proceedings, Part II*, volume 8617 of *LNCS*. Springer, Heidelberg, 2014.

GOS06. Jens Groth, Rafail Ostrovsky, and Amit Sahai. Perfect non-interactive zero knowledge for NP. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 339–358. Springer, Heidelberg, 2006. See also https://eprint.iacr.org/2005/290.

Gro06. Jens Groth. Simulation-sound NIZK proofs for a practical language and constant size group signatures. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT 2006*, volume 4284 of *LNCS*, pages 444–459. Springer, Heidelberg, 2006.

GS12. Jens Groth and Amit Sahai. Efficient noninteractive proof systems for bilinear groups. *SIAM Journal of Computing*, 41(5):1193–1232, 2012. A preliminary version appeared in *EUROCRYPT 2008*, 2008.

GSW10. Essam Ghadafi, Nigel. P. Smart, and Bogdan Warinschi. Groth–Sahai proofs revisited. In Phong Q. Nguyen and David Pointcheval, editors, *PKC 2010*, volume 6056 of *LNCS*, pages 177–192. Springer, Heidelberg, 2010. See also https://eprint.iacr.org/2009/599.

HHH+14. Gottfried Herold, Julia Hesse, Dennis Hofheinz, Carla Ràfols, and Andy Rupp. Polynomial spaces: A new framework for composite-to-prime-order transformations. In Garay and Gennaro [GG14a], pages 261–279. See also https://eprint.iacr.org/2014/445.

JR14. Charanjit S. Jutla and Arnab Roy. Switching lemma for bilinear tests and constant-size NIZK proofs for linear subspaces. In Garay and Gennaro [GG14b], pages 295–312. See also https://eprint.iacr.org/2013/670.

Kra14. Hugo Krawczyk, editor. *Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014. Proceedings*, volume 8383 of *LNCS*. Springer, Heidelberg, 2014.

SBWP03. Ron Steinfeld, Laurence Bull, Huaxiong Wang, and Josef Pieprzyk. Universal designated-verifier signatures. In Chi Sung Laih, editor, *ASIACRYPT 2003*, volume 2894 of *LNCS*, pages 523–542. Springer, Heidelberg, 2003. See also https://eprint.iacr.org/2003/192.

SC12. Jae Hong Seo and Jung Hee Cheon. Beyond the limitation of prime-order bilinear groups, and round optimal blind signatures. In Ronald Cramer, editor, *TCC 2012*, volume 7194 of *LNCS*, pages 133–150. Springer, Heidelberg, 2012. See also https://eprint.iacr.org/2012/198.

Seo12. Jae Hong Seo. On the (im)possibility of projecting property in prime-order setting. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 61–79. Springer, Heidelberg, 2012. See also https://eprint.iacr.org/2013/186.

A On the security of $\mathsf{GS}_{\mathsf{Sym}}$ for special MME

Let us consider an equation

$$-\boldsymbol{Q} \cdot y + X \cdot 1 = \mathcal{O} \in \mathbb{G}$$

and two witnesses $(X, y) = (\boldsymbol{Q}, 1)$ and $(\mathcal{O}, 0)$.

A.1 The special case based on the DLIN assumption

In the WI setting, we have

$$\vec{U} = \begin{pmatrix} (\alpha, 0, 1)\mathcal{P} \\ (0, \beta, 1)\mathcal{P} \\ (z_1\alpha, z_2\alpha, z_1 + z_2 - 1)\mathcal{P} \end{pmatrix}.$$

Let $\boldsymbol{U} = \left(\begin{smallmatrix} \alpha & 0 & 1 \\ 0 & \beta & 1 \\ z_1\alpha & z_2\beta & z_1+z_2-1 \end{smallmatrix}\right)$. In addition, the commitments C and D are uniformly distributed over $\langle \vec{U} \rangle$ and $\langle \vec{V} \rangle$. Therefore, we can represent $C = c_1U_1 + c_2U_2 + c_3U_3$ and $D = d_1U_1 + d_2U_2$, where $c_1, c_2, c_3, d_1, d_2 \leftarrow \mathbb{Z}_N$. We can write $X = y\boldsymbol{Q}$, since $-\boldsymbol{Q} \cdot y + X \cdot 1 = \mathcal{O} \in \mathbb{G}$. Finally, we observe that $C = \iota_1(X) + \boldsymbol{r}\vec{U}$ and $D = \iota_2(y) + \boldsymbol{s}\vec{V}$. Hence, we have $\boldsymbol{r}\mathcal{P} = (C - \iota_1(X))\boldsymbol{U}^{-1}$ and $\boldsymbol{s}\mathcal{P} = (D - \iota_2(y))\boldsymbol{U}^{-1}$. By using $\boldsymbol{r}$ and $\boldsymbol{s}$, we can represent $\vec{\Phi}'$ as

$$\begin{pmatrix} \big(z_1\alpha(-z_1yq + c_1), z_1\alpha(-z_2yq + c_2) + \alpha\rho, z_1\alpha(yq + c_3)\big)\mathcal{P} \\ \big(z_2\beta(-z_1yq + c_1) - \beta\rho, z_2\beta(-z_2yq + c_2), z_2\beta(yq + c_3)\big)\mathcal{P} \\ \big((z_1 + z_2)(-z_1yq + c_1) + q(z_1y - d_1) - \rho, (z_1 + z_2)(-z_2yq + c_2) + q(z_2y - d_2) + \rho, (z_1 + z_2)(yq + c_3)\big)\mathcal{P} \end{pmatrix},$$

where q is the discrete logarithm of $\boldsymbol{Q}$.

Listing 1.1. MME-DLIN-GivenQ.ggt

```
(* MME-DLIN-GivenQ.ggt *)
(* Symmetric Pairing *)
maps G * G -> GT.

(* U, V, Q, C, and D *)
input [
  alpha,beta,z1*alpha,z2*beta,z1+z2-1,q,
  c1*alpha+c3*z1*alpha,c2*beta+c3*z2*beta,c1+c2+c3*(z1+z2-1),
  d1*alpha,d2*beta,d1+d2
] in G.

(* \Phi with y = 0 *)
input_left [
  alpha*c1*z1,alpha*c2*z1-alpha*r,alpha*c3*z1,
  beta*c1*z2+beta*r,beta*c2*z2,beta*c3*z2,
  -d1*q+c1*z1+c1*z2+r,-d2*q+c2*z1+c2*z2-r,c3*z1+c3*z2
] in G.

(* \Phi with y = 1 *)
input_right [
  alpha*c1*z1-alpha*q*z1*z1,alpha*c2*z1-alpha*r-alpha*q*z1*z2,alpha*c3*z1+alpha*q*z1,
  beta*c1*z2+beta*r-beta*q*z1*z2,beta*c2*z2-beta*q*z2*z2,beta*c3*z2+beta*q*z2,
  -d1*q+c1*z1+c1*z2+r+q*z1-q*z1*z1-q*z1*z2,
  -d2*q+c2*z1+c2*z2-r+q*z2-q*z1*z2-q*z2*z2,
  c3*z1+c3*z2+q*z1+q*z2
] in G.
```

We analyze the proofs are indistinguishable in the generic-group model when Q is randomly chosen by employing GGA (Generic Group Analyzer) [BFF$^+$14, BFF$^+$15, Fag15]. [5] Our code for GGA is in Listing 1.1 which reflects calculations in the above. We run the script and obtain

```
$ gga nonparam MME-DLIN-GivenQ.ggt
common input:
(...)
The assumption is valid for all primes
```

as we wanted.

[5] Available at `https://github.com/generic-group-analyzer/gga`.