International Journal of Networking and Computing – www.ijnc.org, ISSN 2185-2847
Volume 13, Number 2, pages 118–130, July 2023

On Multi-user Security of Schnorr Signature in Algebraic Group Model

Masayuki Fukumitsu
Department of Information Security, Faculty of Information Systems, University of Nagasaki
1-1-1 Manabino, Nagayo-cho, Nishisonogi-gun, Nagasaki, 851-2195 Japan
fukumitsu@sun.ac.jp

Shingo Hasegawa
Center for Data-driven Science and Artificial Intelligence, Tohoku University
Multimedia Education and Research Complex, Tohoku University, Kawauchi 41, Aoba-ku, Sendai,
980-8576 Japan
shingo.hasegawa.b7@tohoku.ac.jp

Received: February 13, 2023
Accepted: April 4, 2023
Communicated by Yasuyuki Nogami

Abstract

The security of Schnorr signature Sch has been widely discussed so far. Recently, Fuchsbauer, Plouviez and Seurin gave a tight reduction that proves EUF-CMA of Sch in the random oracle (ROM) with the algebraic group model (AGM) from the discrete logarithm (DL) assumption at EUROCRYPT 2020. Kiltz, Masny and Pan considered multi-user security of Sch at CRYPTO 2016, whereas Fuchsbauer *et al.* considered the single-user security only. More precisely, Kiltz *et al.* constructed a tight reduction from EUF-CMA to MU-EUF-CMA. Combining these two results will likely enable us to construct a tight reduction that proves MU-EUF-CMA security of Sch in AGM+ROM from DL assumption.

Against such an intuition, we show an impossibility on proving MU-EUF-CMA of Sch in AGM+ROM only by combining them in this paper. To estimate our impossibility result, we also discuss why the result by Fuchsbauer *et al.* cannot be applied to MU-EUF-CMA setting. Our result therefore suggests that we are required to develop a new proof technique beyond the algebraic reduction or to find a new form of public keys other than that considered in our impossibility, in order to show MU-EUF-CMA of Sch in AGM+ROM.

Keywords: Schnorr Signature, Algebraic Group Model, Algebraic Reduction, Multi-user Security, Impossibility

1 Introduction

Schnorr signature Sch is one of the simplest and most efficient digital signature schemes. Due to such advantages, Sch is used as a building block of many advanced cryptographic schemes and cryptographic protocols, e.g., [6, 37]. Not only the efficiency and the applicability of Sch but also its security is also discussed so far. Pointcheval and Stern [34] showed the existential unforgeability of Sch against the chosen message attack (EUF-CMA) from the discrete logarithm (DL) assumption. This result is proven under two conditions: in the random oracle model (ROM) and with loose security reduction. The difficulty of removing ROM was already discussed in several papers [30, 12, 28, 19]. In this paper, we focus on the other condition, namely the loose security reduction.

The *loose reduction* is closely related to the loss factor. To explain loss factor, we consider a securiry reduction $\mathcal{R}$ breaking the underlying cryptographic assumption with probability $\epsilon_{\mathcal{R}}$ in time $T_{\mathcal{R}}$ by the black-box access to an adversary $\mathcal{A}$ attacking the designated cryptographic scheme with probability $\epsilon_{\mathcal{A}}$ in time $T_{\mathcal{A}}$. Then, the loss factor is defined so that $\epsilon_{\mathcal{A}}/T_{\mathcal{A}} \leq p \cdot \epsilon_{\mathcal{R}}/T_{\mathcal{R}}$. We say that the security is *loose* when p is polynomial, whereas it is *tight* when the parameter p is constant in the security parameter. The tight security implies that one can set the length of parameters of the cryptographic scheme to be almost the same as that of the cryptographic assumption. In other words, it guarantees the size efficiency of the scheme. Therefore, it is desirable for us that cryptographic schemes have the tight security reduction. However, the question of whether or not the tight security of Sch can be proven is not fully resolved. This open question was just discussed under some restricted conditions. The representative one is the impossibility result under the restriction of reductions given by Paillier and Vergnaud [30]. They showed that the tight security of Sch cannot be proven even in ROM, as long as *algebraic* reduction algorithms are concerned. The algebraic algorithm intuitively means that the algorithm must compute elements of the underlying group using only group operations. This impossibility result was strengthened by [23, 36]. In particular, Seurin [36] showed that the loss factor p must be set as Q_H like [34, 1], which is the number of hash oracle queries by the adversary. As shown above, the restrinction by an algebraic reduction is used to give negative evidence for unresolved problems.

Recently, Fuchsbauer, Plouviez and Seurin [14] gave an affirmative evidence for a tight security reduction of Sch by circumventing the impossibility barrier explained above. Their result was given by restricting an adversary instead of a reduction. More specifically, they showed that Sch is $\mathsf{EUF\text{-}CMA}$ in ROM and in *algebraic group model (AGM)* from DL assumption with a tight reduction. AGM [13] is the security model in which an adversary $\mathcal{A}$ is restricted to be *algebraic*. This implies that they gave such an affirmative result by restricting the behavior of an $\mathsf{EUF\text{-}CMA}$ adversary $\mathcal{A}$, whereas the impossibility results [30, 23, 36] are shown by restricting the type of reductions $\mathcal{R}$.

$\mathsf{EUF\text{-}CMA}$ considers that an adversary $\mathcal{A}$ attacks a single user at once. In the real world, $\mathcal{A}$ shall attack multi-users rather than the single user. To capture the security in the multi-user setting, the multi-user unforgeability against CMA ($\mathsf{MU\text{-}EUF\text{-}CMA}$) was introduced [21]. For the security of Sch in the multi-user setting, Kiltz, Masny and Pan [28] discussed $\mathsf{MU\text{-}EUF\text{-}CMA}$ of Sch in ROM. In particular, they constructed a tight reduction from $\mathsf{EUF\text{-}CMA}$ of Sch to $\mathsf{MU\text{-}EUF\text{-}CMA}$ of Sch. By combining the results by [14] and [28], it is expected that Sch is proven to be $\mathsf{MU\text{-}EUF\text{-}CMA}$ in AGM+ROM with tight reduction.

1.1 Our Contribution

In this paper, we give an impossibility on proving $\mathsf{MU\text{-}EUF\text{-}CMA}$ of Sch in *AGM+ROM* against the above expectation. Our result is given by the following theorem.

Theorem 1 (Informal) *If* Sch *is proven to be* $\mathsf{MU\text{-}EUF\text{-}CMA}$ *in AGM+ROM from* DL *assumption via an algebraic reduction* $\mathcal{R}$ *that generates some specific formed public keys, then* DL *assumption is broken.*

In Theorem 1, we consider the two conditions. The first one is that reductions should be *algebraic* as well as [30, 23, 36]. An algebraic algorithm $\mathcal{R}$ with respect to a target group $\mathbb{G}$ is formally defined as an algorithm such that any element w in $\mathbb{G}$ output by $\mathcal{R}$ is always expressed as the linear combination $\sum_{i=1}^{M} \alpha_i \cdot g$ of elements $(g_1, \cdots, g_M) \in \mathbb{G}^M$ given to $\mathcal{R}$. Additionally, $\mathcal{R}$ is required to output its coefficient vector $(\alpha_1, \ldots, \alpha_M) \in \mathbb{Z}^M$ when $\mathcal{R}$ outputs w. As we mentioned above, the algebraic property is employed to discuss the (un)provable security of several cryptographic schemes [10, 30, 23, 36, 13, 14]. Moreover, the known security reductions proving the single-user security of Sch fall into this type [34, 14].

The second one concerns the type of public keys which are returned by $\mathcal{R}$ when $\mathcal{R}$ invokes an $\mathsf{MU\text{-}EUF\text{-}CMA}$ adversary $\mathcal{A}$. We briefly describe the behavior of a security reduction $\mathcal{R}$ supposed in Theorem 1. As security reductions constructed in [34, 28], a reduction $\mathcal{R}$, which proves $\mathsf{MU\text{-}EUF\text{-}CMA}$

of Sch from DL assumption, is given a DL instance $(\mathbb{G}, q, g, y)$ of a group description $(\mathbb{G}, q, g)$ of a group $\mathbb{G}$ of prime order q with a generator g and $y \in \mathbb{G}$. Then $\mathcal{R}$ would invoke an $\mathsf{MU\text{-}EUF\text{-}CMA}$ adversary $\mathcal{A}$ in a black-box manner with multiple public keys $\{\mathsf{pk}_i^*\}_{i=1}^N$ as input for $\mathcal{A}$. Since $\mathcal{R}$ is assumed to be algebraic and pk_i^* belongs to the target group $\mathbb{G}$, $\mathcal{R}$ must output the coefficient vectors of all pk_i^*. On the other hand, the group elements given to $\mathcal{R}$ are only $(g, y) \in \mathbb{G}$. These imply that any $\mathsf{pk}_i^* \in \mathbb{G}$ can be expressed as

$$\mathsf{pk}_i^* = \alpha_i \cdot g + \beta_i \cdot y,$$

with the coefficient vector $(\alpha_i, \beta_i) \in \mathbb{Z}_q^2$. The second condition is that $\beta_i = 1$ for all pk_i^*, namely the form of pk_i^* is assumed to be

$$\mathsf{pk}_i^* = \alpha_i \cdot g + y.$$

Note that the similar construction of public keys can be seen in the security proofs concerning $\mathsf{MU\text{-}EUF\text{-}CMA}$ of Sch [28, 21].

We also review the previous result of [14]. We discuss the reason why the security reduction of [14] proving $\mathsf{EUF\text{-}CMA}$ in AGM+ROM is difficult to be applied to the multi-user case. This paper suggests that we have to develop a new proof technique beyond the algebraic reduction such as [14, 28], or to find a new form of public keys that does not fall into the condition considered in Theorem 1 in order to overcome our impossibility and prove $\mathsf{MU\text{-}EUF\text{-}CMA}$ of Sch with a tight reduction.

1.2 Related Works

Paillier and Vergnaud [30] also gave the impossibility of proving the security of Sch without ROM inder the restriction that concerned reductions are only algebraic. ROM enables us to employ the useful features on the construction of security reductions, the *observability* and the *programmability.* The observability means that a security reduction $\mathcal{R}$ can observe all pairs of a query and its answer to the hash oracle by the adversary. The programmability enables $\mathcal{R}$ to set arbitrary values as the hash values for queries. Ananth and Bhaskar [3] considered a reduction for Sch without the observability. On the other hand, Fischlin and Fleischhacker [12] showed that Sch cannot be proven to be secure without the programmability. This impossibility was strengthened by [15, 17, 18, 19]. Kiltz, Masny and Pan [28] also summarized the impossibility results on the programmability for generic Fiat-Shamir-type signatures including Sch.

Fuchsbauer, Kiltz and Loss [13] first introduced AGM as a relaxed model of the generic group model. They proved that several DL-based assumptions, including the computational Diffie-Hellman (DH) assumption and the strong DH assumption, are equivalent to the DL assumption in AGM. They also gave the tight reduction in AGM for the BLS signature [9] and the Groth ZK-SNARG [25]. Fuchsbauer, Plouviez and Seurin [14] discussed not only the tight security of Sch but also the Schnorr-based blind signature, although the cryptographic assumption on which that blind signature is based is broken by [8]. Then a new blind signature based on the one-more DL assumption was proposed in AGM [26]. Most recently, [27, 29, 5, 22] discussed the security of cryptographic protocols related to Sch in AGM.

For the tight security of FS signatures, Abdalla, Fouque, Lyubashevsky and Tibouchi [2] introduced the notion of the lossy ID scheme which derives tightly secure Fiat-Shamir-type signatures in ROM. However, the conventional lossy ID schemes are based on decisional assumptions rather than computational assumptions.

[31, 11, 32] proposed tightly secure signatures in the multi-user setting with adaptive corruption by extending the Fiat-Shamir-type transformation. On the other hand, we discuss the security of the original Schnorr signature in the multi-user setting and AGM *without any modification to the Fiat-Shamir-type transformation.* It is also an important open question that whether or not the $\mathsf{MU\text{-}EUF\text{-}CMA}$ security of Sch in AGM with adaptive corruption can be proven.

```
$\mathsf{Game}^{\mathsf{MU\text{-}EUF\text{-}CMA}}_{N,Q_S,\mathsf{DS},\mathcal{A}}(\lambda)$
$\mathsf{L} = \emptyset$
$K \leftarrow\!\$\ \mathsf{Pgen}(1^\lambda)$
$(\mathsf{sk}_i, \mathsf{pk}_i) \leftarrow\!\$\ \mathsf{KGen}(K)$ for $i \in [1, N]$
$(i^*, m^*, \sigma^*) \leftarrow\!\$\ \mathcal{A}^{\mathsf{O}_{\mathsf{Sig}}}(K, \{\mathsf{pk}_i\}_{i=1}^N)$
return $1$ if $(i^*, m^*) \notin \mathsf{L} \wedge \mathsf{Vf}(K, \mathsf{pk}_{i^*}, m^*, \sigma^*) = 1$
```

```
Oracle $\mathsf{O}_{\mathsf{Sig}}(i, m)$
return $\perp$ if $i \notin [1, N]$
$\sigma \leftarrow\!\$\ \mathsf{Sig}(K, \mathsf{sk}_i, \mathsf{pk}_i, m)$
$\mathsf{L} \leftarrow \mathsf{L} \cup \{(i, m)\}$
return $\sigma$
```

Figure 1: Procedure of challenger $\mathcal{C}$ in $\mathsf{MU\text{-}EUFCMA}$ game with signing oracle $\mathsf{O}_{\mathsf{Sig}}$

1.3 Difference from Proceeding Version

The proceeding version appeared in [20]. We extend **Theorem 1** to cover a security reduction which can invoke an adversary polynomially many times, whereas in the proceeding version, we only considered that the number of such an invocation is only one.

2 Preliminaries

For a probabilistic algorithm $\mathcal{A}$, $y \leftarrow\!\$\ \mathcal{A}(x; \omega)$ expresses that $\mathcal{A}$ outputs y on input x with random coins ω. $\mathcal{A}(x)$ is a random variable where random coins ω are internally chosen. For a finite set X, $y \leftarrow\!\$\ X$ means that y is chosen uniformly at random from X. For any algorithm $\mathcal{A}$ (a distribution D, resp.) and any possible input x to $\mathcal{A}$, $[\mathcal{A}(x)]$ means the set of all possible outputs by $\mathcal{A}$ on input x, and $[\mathcal{A}]$ ($[D]$, resp.) does the set of all possible outputs by $\mathcal{A}$ (D, resp.) for any possible input. Abbreviated words *DPT* and *PPT* stand for "deterministic polynomial-time" and "probabilistic polynomial-time", respectively.

We write $\mathbb{N}$ and $\mathbb{Z}$ to denote the sets of all natural numbers and all integers, respectively. For any two integers $a \leq b$, let $[a, b] \subseteq \mathbb{Z}$ be the set of all integers between a and b. For any $N \in \mathbb{N}$, let $\mathbb{Z}_N$ be the ring of residues modulo N. Let $\mathbb{G}$ denote an additive group. For any $g \in \mathbb{G}$ and any $n \in \mathbb{N}$, $n \cdot g$ means $\sum_{i=1}^n g$.

2.1 Digital Signature Schemes

A signature scheme DS is defined by a 4-tuple $(\mathsf{Pgen}, \mathsf{KGen}, \mathsf{Sig}, \mathsf{Vf})$ [24]. Pgen is a PPT parameter generator that generates a public parameter K on a security parameter 1^λ. KGen is a PPT key generator that generates a pair $(\mathsf{sk}, \mathsf{pk})$ of a secret key and its public key on a public parameter K. Sig is a PPT signing algorithm that returns a signature σ on a tuple $(K, \mathsf{sk}, \mathsf{pk}, m)$ of a public parameter, a secret key, its public key and a message. Vf is a DPT verifying algorithm that returns 1 if σ is valid under (pk, m) on a tuple $(K, \mathsf{pk}, m, \sigma)$ of a public parameter, a public key, a message and a signature.

2.1.1 Correctness

The *correctness* of DS is that $\mathsf{Vf}(K, \mathsf{pk}, m, \sigma)$ always returns 1 for any $\lambda \in \mathbb{N}$, any $K \leftarrow\!\$\ \mathsf{Pgen}(1^\lambda)$, any pair $(\mathsf{sk}, \mathsf{pk}) \leftarrow\!\$\ \mathsf{KGen}(K)$, any message m and any $\sigma \leftarrow\!\$\ \mathsf{Sig}(\mathsf{sk}, \mathsf{pk}, m)$.

2.1.2 Security

We consider the multi-user existential unforgeability against the chosen-message attack ($\mathsf{MU\text{-}EUF\text{-}CMA}$). This is defined by the $\mathsf{MU\text{-}EUF\text{-}CMA}$ *game* depicted in Fig. 1. This game is played by a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$. A signature scheme $\mathsf{DS} = (\mathsf{Pgen}, \mathsf{KGen}, \mathsf{Sig}, \mathsf{Vf})$ is said to be (T, ϵ, N, Q_S)-$\mathsf{MU\text{-}EUF\text{-}CMA}$ *secure* if for any adversary $\mathcal{A}$ that runs in time T and makes Q_S signing oracle queries, $\mathcal{A}$ *wins the* $\mathsf{MU\text{-}EUF\text{-}CMA}$ *game*, namely $\mathsf{Game}^{\mathsf{MU\text{-}EUF\text{-}CMA}}_{N,Q_S,\mathsf{DS},\mathcal{A}}(\lambda) = 1$, with at most probability ϵ. For the *random oracle model (ROM)* [7], we denote by the $(T, \epsilon, Q_H, N, Q_S)$-$\mathsf{MU\text{-}EUF\text{-}CMA}$ security the

(T, ϵ, N, Q_S)-$\mathsf{MU\text{-}EUF\text{-}CMA}$ security for an adversary that makes Q_H queries to the hash oracle. $\mathsf{EUF\text{-}CMA}$ in ROM stands for $(T, \epsilon, Q_H, 1, Q_S)$-$\mathsf{MU\text{-}EUF\text{-}CMA}$.

2.2 Algebraic Group Model and Algebraic Reduction

Since the notions of the algebraic group model and the algebraic reduction are defined by an algebraic algorithm, we recap the notion of the *algebraic* algorithm [30, 13]. Its intuitive meaning is that $\mathcal{A}$ can execute operations defined over $\mathbb{G}_K$ only to generate a new element in $\mathbb{G}_K$. Paillier and Vergnaud formally defined that an algebraic algorithm is an algorithm such that any element w in $\mathbb{G}_K$ computed by the algebraic algorithm must be expressed by the linear combination of given group elements in $\mathbb{G}_K$. More precisely, if $\mathcal{A}$ takes M group elements $g_1, \ldots, g_M \in \mathbb{G}_K$ with a parameter K before outputting a group element $w \in \mathbb{G}_K$, then there exists $(\alpha_1, \ldots, \alpha_M) \in \mathbb{Z}^M$ such that $w = \sum_{k=1}^{M} \alpha_k \cdot g_k$ and $\mathcal{A}$ also outputs $(\alpha_1, \ldots, \alpha_M)$ with w. $(\alpha_1, \ldots, \alpha_M)$ is called a *coefficient vector of w under the basis* $(g_1, \ldots, g_M)$. We write $w_{\{\sum_{k=1}^{M} \alpha_k \cdot g_k\}}$ to denote the pair $(w, \boldsymbol{\alpha})$ of the element $w \in \mathbb{G}_K$ and its coefficient vector $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_M) \in \mathbb{Z}^M$ under the basis $\boldsymbol{g} = (g_1, \ldots, g_M)$, i.e., $w = \sum_{k=1}^{M} \alpha_k \cdot g_k$.

Consider a reduction algorithm $\mathcal{R}$ that wins some security game with black-box access to an adversary $\mathcal{A}$ winning another security game. Then, the *algebraic group model (AGM) with respect to* $\{\mathbb{G}_K\}_K$ [13] means that $\mathcal{A}$ is restricted to be algebraic with respect to $\{\mathbb{G}_K\}_K$. Such $\mathcal{A}$ is called an *algebraic adversary.* On the other hand, *algebraic reduction with respect to* $\{\mathbb{G}_K\}_K$ [30] does that $\mathcal{R}$ is restricted to be algebraic with respect to $\{\mathbb{G}_K\}_K$.

3 Schnorr Signature and Related Properties

In this section, we recap Schnorr signature Sch [35]. We denote by $\mathsf{Pgen}^{\mathbb{G}}$ a PPT group generator such that on input 1^λ, it returns a tuple $(\mathbb{G}, q, g)$ of a group description $\mathbb{G}$ and a prime q of length λ that denotes the order of $\mathbb{G}$, and a generator g of $\mathbb{G}$. Since the length of q is λ, we have $2^{\lambda-1} < q < 2^\lambda$. Let $\mathsf{KGen}^{\mathsf{DL}}$ be a PPT algorithm that outputs $(x, y) \in \mathbb{Z}_q \times \mathbb{G}$ such that $y = x \cdot g$ on input $(\mathbb{G}, q, g) \in [\mathsf{Pgen}^{\mathbb{G}}]$. Then the discrete logarithm assumption is defined as follows:

Definition 1. *The* (T, ϵ)-discrete logarithm (DL) assumption *holds if there exists no algorithm $\mathcal{A}$ running in time T that on input $(\mathbb{G}, q, g, y)$, returns $x^* \in \mathbb{Z}_q$ such that $(x^*, y) \in [\mathsf{KGen}^{\mathsf{DL}}]$ with probability ϵ, where $(\mathbb{G}, q, g) \leftarrow\$ \mathsf{Pgen}^{\mathbb{G}}(1^\lambda)$ and $(x, y) \leftarrow\$ \mathsf{KGen}^{\mathsf{DL}}(\mathbb{G}, q, g)$.*

Schnorr signature Sch is formalized in the following way:

- $\mathsf{Pgen}^{\mathsf{Sch}}$ and $\mathsf{KGen}^{\mathsf{Sch}}$ coincide with $\mathsf{Pgen}^{\mathbb{G}}$ and $\mathsf{KGen}^{\mathsf{DL}}$, respectively.
- $\mathsf{Sig}^{\mathsf{Sch}}$ issues a signature $\sigma = (\mathsf{cha}, \mathsf{res}) \in \mathbb{Z}_q^2$ on input $(\mathbb{G}, q, g, \mathsf{sk}, \mathsf{pk}, m)$ so that

$$\begin{aligned} &\mathsf{st} \leftarrow\$ \mathbb{Z}_q, \\ &\mathsf{cmt} = \mathsf{st} \cdot g, \\ &\mathsf{cha} = H(\mathsf{cmt}, m), \text{ and} \\ &\mathsf{res} = \mathsf{st} + \mathsf{cha} \cdot \mathsf{sk} \bmod q. \end{aligned}$$

- $\mathsf{Vf}^{\mathsf{Sch}}$ returns 1 on input $(\mathbb{G}, q, g, \mathsf{pk}, m, (\mathsf{cha}, \mathsf{res}))$ if $\mathsf{cha} = H(\mathsf{res} \cdot g - \mathsf{cha} \cdot \mathsf{pk}, m)$.

We say that *a tuple* $(\mathsf{cmt}, \mathsf{cha}, \mathsf{res}) \in \mathbb{G} \times \mathbb{Z}_q \times \mathbb{Z}_q$ *satisfies the verification formula* $\mathsf{Vf}^{\mathsf{Sch}}$ *with respect to* $(\mathbb{G}, q, g, y)$ if it holds that $\mathsf{cmt} = \mathsf{res} \cdot g - \mathsf{cha} \cdot y$ over $\mathbb{G}$. Such a tuple $(\mathsf{cmt}, \mathsf{cha}, \mathsf{res})$ is called a *transcript.*

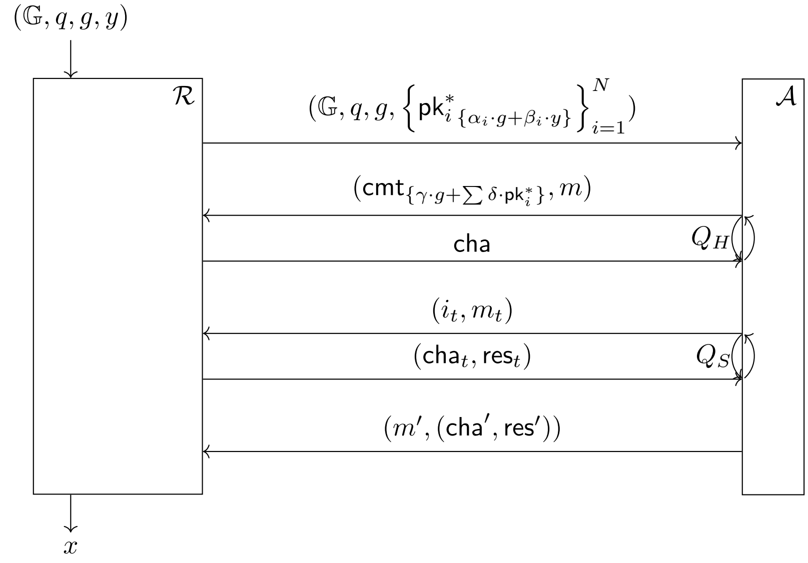
$(\mathbb{G}, q, g, y)$
$\mathcal{R}$
$\mathcal{A}$
$(\mathbb{G}, q, g, \left\{\mathsf{pk}^*_{i\,\{\alpha_i \cdot g + \beta_i \cdot y\}}\right\}_{i=1}^{N})$
$(\mathsf{cmt}_{\{\gamma \cdot g + \sum \delta \cdot \mathsf{pk}^*_i\}}, m)$
cha
Q_H
(i_t, m_t)
$(\mathsf{cha}_t, \mathsf{res}_t)$
Q_S
$(m', (\mathsf{cha}', \mathsf{res}'))$
x

Figure 2: Overview of the reduction $\mathcal{R}$ which proves MU-EUF-CMA of Sch in AGM+ROM from DL assumption

4 Impossibility on Proving MU-EUF-CMA of Schnorr signature in AGM+ROM

In this section, we show that Schnorr signature Sch cannot be proven to be MU-EUF-CMA in AGM+ROM from DL assumption under some restrictions, whereas EUF-CMA in AGM+ROM is justified in [14]. For our purpose, we first define the situation where Sch *is proven to be* MU-EUF-CMA *in AGM+ROM from* DL *assumption as far as algebraic reductions are concerned.* This is defined by a PPT black-box algebraic reduction $\mathcal{R}$ that proves MU-EUF-CMA in AGM+ROM from DL assumption. $\mathcal{R}$ aims to break DL assumption with non-negligible probability in AGM+ROM if a successful MU-EUF-CMA adversary $\mathcal{A}$ is provided in a black-box manner. The behavior of $\mathcal{R}$ is elaborated in the following way. Let $(\mathbb{G}, q, g, y)$ be a tuple of a group description $(\mathbb{G}, q, g)$ and a group element $y \in \mathbb{G}$ that is given to $\mathcal{R}$. To break DL assumption with non-negligible probability, $\mathcal{R}$ can invoke an adversary $\mathcal{A}$ that breaks MU-EUF-CMA with non-negligible probability. $\mathcal{R}$ invokes $\mathcal{A}$ with a tuple $(\mathbb{G}, q, g, \{\mathsf{pk}^*_i\}_{i=1}^{N})$ of the group description $(\mathbb{G}, q, g)$ and N public keys $\{\mathsf{pk}^*_i\}_{i=1}^{N}$ as initial input for $\mathcal{A}$. Here, we suppose that $\mathcal{R}$ is *fixed-parameter* in the sense that the group description given to $\mathcal{A}$ is always the same as the one given to $\mathcal{R}$. Since we now consider a result in ROM, $\mathcal{A}$ would make queries to the hash oracle $\mathsf{O}^{\mathcal{A}}_{H}$ and the signing oracle $\mathsf{O}^{\mathcal{A}}_{\mathsf{Sig}}$ which are emulated by $\mathcal{R}$. In particular, we need to consider that $\mathcal{R}$ may fail to emulate $\mathsf{O}^{\mathcal{A}}_{\mathsf{Sig}}$ since it is a PPT algorithm. If $\mathcal{R}$ fails to emulate $\mathsf{O}^{\mathcal{A}}_{H}$ or $\mathsf{O}^{\mathcal{A}}_{\mathsf{Sig}}$ for some query by $\mathcal{A}$, $\mathcal{A}$ can abort the MU-EUF-CMA game. Otherwise, $\mathsf{O}^{\mathcal{A}}_{\mathsf{Sig}}$ answers a signature $(\mathsf{cha}_t, \mathsf{res}_t) \in \mathbb{Z}_q^2$ of the message m_t under the public key $\mathsf{pk}^*_{i_t}$ for the t-th signing oracle query $(i_t, m_t) \in [1, N] \times \{0,1\}^{\ell_m}$. If $\mathsf{O}^{\mathcal{A}}_{\mathsf{Sig}}$ succeeds in answering all signing oracle queries by $\mathcal{A}$, $\mathcal{A}$ finally wins the game with non-negligible probability with the output tuple $(i^*, m^*, (\mathsf{cha}^*, \mathsf{res}^*))$. $\mathcal{A}$ is regarded as deterministic or probabilistic with fixed random coins as the treatment in [33].

Now, both $\mathcal{R}$ and $\mathcal{A}$ are algebraic with respect to $\{\mathbb{G}\}_{(\mathbb{G},q,g) \in [\mathsf{Pgen}^{\mathsf{Sch}}]}$, since $\mathcal{R}$ is assumed to be an algebraic reduction. We employ AGM. Therefore when $\mathcal{R}$ and $\mathcal{A}$ output elements in $\mathbb{G}$ such as $\mathsf{cmt} \in \mathbb{G}$, they should also output coefficient vectors under the input elements in $\mathbb{G}$. Especially, $\mathcal{R}$ should invoke the MU-EUF-CMA adversary $\mathcal{A}$ on the initial input $(\mathbb{G}, q, g, \{\mathsf{pk}^*_i\}_{i=1}^{N})$ with the coefficient vectors $(\alpha_i, \beta_i) \in \mathbb{Z}_q \times \mathbb{Z}_q$ of $\mathsf{pk}^*_i \in \mathbb{G}$ under the basis (g, y). Namely, each pk^*_i is of the form

$$\alpha_i \cdot g + \beta_i \cdot y.$$

This is because pk^*_i is an element in $\mathbb{G}$ output by the algebraic algorithm $\mathcal{R}$, and g and y are the

```
Specific Adversary: $\tilde{\mathcal{A}}^{\mathsf{O}_H^{\mathcal{A}},\mathsf{O}_{\mathsf{Sig}}^{\mathcal{A}}}(\mathbb{G}, q, g, \{\mathsf{pk}_i^*\}_{i=1}^N)$
1 : $(m, \tilde{i}, i^*) \leftarrow\!\$\ \mathsf{O}_{\mathsf{rand}}(\mathbb{G}, q, g, \{\mathsf{pk}_i^*\}_{i=1}^N)$
2 : $(\mathsf{cha}, \mathsf{res}) \leftarrow\!\$\ \mathsf{O}_{\mathsf{Sig}}^{\mathcal{A}}(\tilde{i}, m)$
3 : $\mathsf{cmt} \leftarrow \mathsf{res} \cdot g - \mathsf{cha} \cdot \mathsf{pk}_{\tilde{i}}^*$
4 : $\textbf{abort if } \mathsf{cha} \neq \mathsf{O}_H^{\mathcal{A}}(\mathsf{cmt}_{\{\mathsf{res}\cdot g - \mathsf{cha}\cdot\mathsf{pk}_{\tilde{i}}^*\}}, m)$
5 : $\textbf{find } \mathsf{res}' \in \mathbb{Z}_q \textbf{ s.t. } \mathsf{cmt} = \mathsf{res}' \cdot g - \mathsf{cha} \cdot \mathsf{pk}_{i^*}^*$
6 : $\textbf{return } (i^*, m, (\mathsf{cha}, \mathsf{res}'))$
```

```
$\mathcal{M}^{\mathcal{R}}(\mathbb{G}, q, g, y)$
1 : $\mathsf{L}_{\mathsf{rand}} = \emptyset$
2 : $\textbf{for } k \in [1, I]:$
3 :     $(m_k, \tilde{i}_k, i_k^*) \leftarrow\!\$\ \{0,1\}^{\ell_m} \times \{(i, i') \in [1, N]^2 \mid i \neq i'\}$
4 : $k \leftarrow 0$
5 : $\textbf{return } \mathcal{R}^{\tilde{\mathcal{A}}}(\mathbb{G}, q, g, y)$
```

```
Simulator: $\tilde{\mathcal{A}}^{\mathsf{O}_H^{\mathcal{A}},\mathsf{O}_{\mathsf{Sig}}^{\mathcal{A}}}(\mathbb{G}, q, g, \{\mathsf{pk}_{i\,\{\alpha_i\cdot g+y\}}^*\}_{i=1}^N)$
1 : $(m, \tilde{i}, i^*) \leftarrow \mathsf{Sim}_{\mathsf{L}_{\mathsf{rand}}}^{\{(m_k, \tilde{i}_k, i_k^*)\}}(\mathbb{G}, q, g, \{\mathsf{pk}_i^*\}_{i=1}^N)$
        $\mathsf{Sim}_{\mathsf{L}_{\mathsf{rand}}}^{\{(m_k, \tilde{i}_k, i_k^*)\}}(\mathbb{G}, q, g, \{\mathsf{pk}_i^*\}_{i=1}^N)$
        $\textbf{if } \mathsf{L}_{\mathsf{rand}}[\mathbb{G}, q, g, \{\mathsf{pk}_i^*\}_{i=1}^N] = \bot:$
            $k \leftarrow k + 1$
            $\mathsf{L}_{\mathsf{rand}}[\mathbb{G}, q, g, \{\mathsf{pk}_i^*\}_{i=1}^N] \leftarrow (m_k, \tilde{i}_k, i_k^*)$
        $\textbf{return } \mathsf{L}_{\mathsf{rand}}[\mathbb{G}, q, g, \{\mathsf{pk}_i^*\}_{i=1}^N]$
2 : $(\mathsf{cha}, \mathsf{res}) \leftarrow\!\$\ \mathsf{O}_{\mathsf{Sig}}^{\mathcal{A}}(\tilde{i}, m)$
3 : $\mathsf{cmt} \leftarrow \mathsf{res} \cdot g - \mathsf{cha} \cdot \mathsf{pk}_{\tilde{i}}^*$
4 : $\textbf{abort if } \mathsf{cha} \neq \mathsf{O}_H^{\mathcal{A}}(\mathsf{cmt}_{\{\mathsf{res}\cdot g - \mathsf{cha}\cdot\mathsf{pk}_{\tilde{i}}^*\}}, m)$
5 : $\mathsf{res}' \leftarrow \mathsf{res} + (\alpha_{i^*} - \alpha_{\tilde{i}})\mathsf{cha} \bmod q$
6 : $\textbf{return } (i^*, m, (\mathsf{cha}, \mathsf{res}'))$
```

Figure 3: Specific MU-EUF-CMA adversary $\tilde{\mathcal{A}}$ and meta-reduction $\mathcal{M}$ with simulator of $\tilde{\mathcal{A}}$

only elements in $\mathbb{G}$ given to $\mathcal{R}$ before invoking $\mathcal{A}$. The overview of $\mathcal{R}$ is depicted in Fig. 2.

Moreover, $\mathcal{R}$ is supposed to be *sequentially multi-instance (SMI)* [4, 16]. Namely, $\mathcal{R}$ can invoke $\mathcal{A}$ polynomially many times, but the concurrent invocations of clones of $\mathcal{A}$ is prohibited. We denote by I the number of invocations of $\mathcal{A}$ by $\mathcal{R}$.

We now show the impossibility of proving MU-EUF-CMA of Sch in AGM+ROM. More precisely, Sch cannot be proven to be MU-EUF-CMA from DL assumption in AGM+ROM when each β_i of the public keys pk_i^* given to an MU-EUF-CMA adversary is fixed to the same value such as 1.

We now show our main theorem in the following way.

Theorem 1 (DL $\not\to$ MU-EUF-CMA in AGM+ROM)**.** *Assume that there exists a PPT fixed-parameter, SMI and algebraic black-box reduction $\mathcal{R}$ such that $\mathcal{R}$ proves* MU-EUF-CMA *of* Sch *in AGM+ROM from* DL *assumption, it invokes an* MU-EUF-CMA *adversary at most I times, and the initial input $\{\mathsf{pk}_i^*\}_{i=1}^N$ for an* MU-EUF-CMA *adversary is of the form $\mathsf{pk}_i^* = \alpha_i \cdot g + y$ for the pair $(g, y) \in \mathbb{G}^2$ which is given to $\mathcal{R}$ as the* DL *adversary. Then, there exists a PPT algorithm $\mathcal{M}$ that breaks* DL *assumption with non-negligible probability.*

Proof. Let $\mathcal{R}$ be a PPT black-box reduction that is fixed-parameter, SMI and algebraic, and proves MU-EUF-CMA of Sch in AGM+ROM from DL assumption. As we have mentioned above, $\mathcal{R}$ can break DL assumption with non-negligible probability $\epsilon_{\mathcal{R}}$ if it is provided an adversary $\mathcal{A}$ that breaks MU-EUF-CMA with non-negligible probability. We now consider the algebraic MU-EUF-CMA adversary $\tilde{\mathcal{A}}$ of the specific type. If $\tilde{\mathcal{A}}$ wins the MU-EUF-CMA game with non-negligible probability, $\mathcal{R}$ can break DL assumption in AGM+ROM. Therefore, we aim to construct a PPT algorithm $\mathcal{M}$ that makes $\mathcal{R}$ break DL assumption with probability $\epsilon_{\mathcal{R}}$ by simulating $\tilde{\mathcal{A}}$. We call $\mathcal{M}$ *meta-reduction.* We now describe the specific adversary $\tilde{\mathcal{A}}$.

Specific MU-EUF-CMA Advesary $\tilde{\mathcal{A}}$ We depict the specific adversary $\tilde{\mathcal{A}}$ in the left side of Fig. 3. The strategy of $\tilde{\mathcal{A}}$ is as follows. $\tilde{\mathcal{A}}$ makes a signing oracle query $(\tilde{i}, m)$ to obtain its signature $(\mathsf{cha}, \mathsf{res})$ under $\mathsf{pk}_{\tilde{i}}^*$, and then converts $(\mathsf{cha}, \mathsf{res})$ into a signature $(\mathsf{cha}, \mathsf{res}')$ of m under another public key $\mathsf{pk}_{i^*}^*$. It follows from $(\tilde{i}, m) \neq (i^*, m)$ that $(i^*, m, (\mathsf{cha}, \mathsf{res}'))$ can be a forgery of the MU-EUF-CMA adversary $\tilde{\mathcal{A}}$. Since $\tilde{\mathcal{A}}$ should be deterministic as mentioned above, the random values $(m, \tilde{i}, i^*)$ are sampled by using the virtual oracle $\mathsf{O}_{\mathsf{rand}}$ that samples a message $m \leftarrow\!\$\ \{0,1\}^{\ell_m}$ and indices $(\tilde{i}, i^*) \leftarrow\!\$\ \{(i, i') \in [1, N]^2 \mid i \neq i'\}$ on a tuple $(\mathbb{G}, q, g, \{\mathsf{pk}_i^*\}_{i=1}^N)$ at Line 1 [1].

[1] A similar technique appears in [18].

Since $\tilde{\mathcal{A}}$ is supposed to be algebraic with respect to $\{\mathbb{G}\}_{(\mathbb{G},q,g)\in[\mathsf{Pgen}^{\mathsf{Sch}}]}$, $\tilde{\mathcal{A}}$ must output a coefficient vector under the input elements $(g, \{\mathsf{pk}_i^*\}_{i=1}^N)$ when $\tilde{\mathcal{A}}$ outputs some element in $\mathbb{G}$. At Line 4, $\tilde{\mathcal{A}}$ outputs $\mathsf{cmt} \in \mathbb{G}$ as a hash query. By the setting of $\mathsf{cmt} = \mathsf{res} \cdot g - \mathsf{cha} \cdot \mathsf{pk}_{\tilde{i}}^*$ at Line 3, $(\mathsf{res}, -\mathsf{cha})$ can be naturally a coefficient vector of cmt under $(g, \mathsf{pk}_{\tilde{i}}^*)$. Thus $\tilde{\mathcal{A}}$ satisfies the condition of the algebraic $\mathsf{MU\text{-}EUF\text{-}CMA}$ adversary.

It should be noted that Line 5 seems not to be done in polynomial-time. Although $\tilde{\mathcal{A}}$ is not required to be a PPT algorithm, we will show that $\mathcal{M}$ simulates $\tilde{\mathcal{A}}$ in polynomial-time by utilizing the algebraic property of $\mathcal{R}$.

Construction of Meta-reduction $\mathcal{M}$ We construct a PPT meta-reduction $\mathcal{M}$ as in Fig. 3. The basic strategy of $\mathcal{M}$ is making $\mathcal{R}$ break DL assumption with probability $\epsilon_{\mathcal{R}}$, and the key technical issue is how $\mathcal{M}$ simulates $\tilde{\mathcal{A}}$ in polynomial-time. In particular, we realize the simulation of $\tilde{\mathcal{A}}$ on the right side of Fig. 3 by utilizing the algebraic property of $\mathcal{R}$. Since $\mathcal{R}$ is algebraic with respect to $\{\mathbb{G}\}_{(\mathbb{G},q,g)\in[\mathsf{Pgen}^{\mathsf{Sch}}]}$ and $\mathcal{R}$ outputs N public keys $\mathsf{pk}_i^* \in \mathbb{G}$ $(i \in [1, N])$ to invoke $\tilde{\mathcal{A}}$ simulated by $\mathcal{M}$, $\mathcal{R}$ would output the coefficient vectors of all pk_i^* under the group elements (g, y) given to $\mathcal{R}$. Namely each pk_i^* is expressed as

$$\mathsf{pk}_i^* = \alpha_i \cdot g + y, \tag{1}$$

for some $\alpha_i \in \mathbb{Z}_q$ by the assumption on the statement. Then, the valid signature $(\mathsf{cha}, \mathsf{res})$ of m under $\mathsf{pk}_{\tilde{i}}^*$ obtained at Line 2 can be converted into a signature $(\mathsf{cha}, \mathsf{res}')$ of m under $\mathsf{pk}_{i^*}^*$ at Line 5. This is because $(\mathsf{cha}, \mathsf{res})$ satisfies that $\mathsf{cha} = \mathsf{O}_H^{\mathcal{A}}(\mathsf{cmt}, m)$ for $\mathsf{cmt} = \mathsf{res} \cdot g - \mathsf{cha} \cdot \mathsf{pk}_{\tilde{i}}^*$, and then Line 5 implies that

$$\begin{aligned}
\mathsf{cmt} &= \mathsf{res} \cdot g - \mathsf{cha} \cdot \mathsf{pk}_{\tilde{i}}^* \\
&= \mathsf{res} \cdot g - \mathsf{cha}(\alpha_{\tilde{i}} \cdot g + y) \\
&= \mathsf{res} \cdot g - \mathsf{cha}(\alpha_{\tilde{i}} \cdot g + y) + \alpha_{i^*}\mathsf{cha} \cdot g - \alpha_{i^*}\mathsf{cha} \cdot g \\
&= (\mathsf{res} - \alpha_{\tilde{i}}\mathsf{cha} + \alpha_{i^*}\mathsf{cha}) \cdot g - \mathsf{cha}(\alpha_{i^*} \cdot g + y) \\
&= \mathsf{res}' \cdot g - \mathsf{cha} \cdot \mathsf{pk}_{i^*}^*.
\end{aligned} \tag{2}$$

Therefore, $(\mathsf{cha}, \mathsf{res}')$ is a valid signature of m under $\mathsf{pk}_{i^*}^*$.

Simulation of Specific Adversary $\tilde{\mathcal{A}}$ We now confirm that the behavior of the simulator of $\tilde{\mathcal{A}}$ (in the right side of Fig. 3) is identical to that of the original $\tilde{\mathcal{A}}$ (in the left side of Fig. 3) from the viewpoint of $\mathcal{R}$. The differences between the simulator and the original appear at Lines 1 and 5. At Line 1 of the simulator, the tuple $(m, \tilde{i}, i^*)$ is given from $\mathsf{Sim}_{\mathsf{L}_{\mathsf{rand}}}^{\{(m_k,\tilde{i}_k,i_k^*)\}}$ instead of $\mathsf{O}_{\mathsf{rand}}$. We first consider a case where the input tuple $(\mathbb{G}, q, g, \{\mathsf{pk}_i^*\}_{i=1}^N)$ does not apper at any previous invocation of $\tilde{\mathcal{A}}$. Namely, $\mathsf{Sim}_{\mathsf{L}_{\mathsf{rand}}}^{\{(m_k,\tilde{i}_k,i_k^*)\}}$ returns a tuple $(m_k, \tilde{i}, i^*)$ which is sampled at Line 3 in $\mathcal{M}$ so that $m \leftarrow\!\!\$ \ \{0,1\}^{\ell_m}$ and $(\tilde{i}, i^*) \leftarrow\!\!\$ \ \{(i, i') \in [1, N]^2 \mid i \neq i'\}$. Since the tuple $(\mathbb{G}, q, g, \{\mathsf{pk}_i^*\}_{i=1}^N)$ is a new tuple given to $\tilde{\mathcal{A}}$, $(m_k, \tilde{i}, i^*)$ is a tuple which has not been used to simulate $\tilde{\mathcal{A}}$ until this invocation of $\tilde{\mathcal{A}}$. This implies that the distribution of $(m_k, \tilde{i}, i^*)$ by $\mathsf{Sim}_{\mathsf{L}_{\mathsf{rand}}}^{\{(m_k,\tilde{i}_k,i_k^*)\}}$ coincides with the one by $\mathsf{O}_{\mathsf{rand}}$ for the viewpoint of $\mathcal{R}$. We next consider the opposite case. Namely, $(\mathbb{G}, q, g, \{\mathsf{pk}_i^*\}_{i=1}^N)$ has been given to $\tilde{\mathcal{A}}$ for some previous invocation of $\tilde{\mathcal{A}}$. In this case, both $\mathsf{O}_{\mathsf{rand}}$ and $\mathsf{Sim}_{\mathsf{L}_{\mathsf{rand}}}^{\{(m_k,\tilde{i}_k,i_k^*)\}}$ return the same tuple $(m, \tilde{i}, i)$ for the same tuple $(\mathbb{G}, q, g, \{\mathsf{pk}_i^*\}_{i=1}^N)$. Thus, the behavior at line 1 of the simulator is the same as that of the original specific adversary.

From Eq. (2), $\mathsf{res}' = \mathsf{res} + (\alpha_{i^*} - \alpha_{\tilde{i}})\mathsf{cha} \bmod q$ set as at Line 5 satisfies that $\mathsf{cmt} = \mathsf{res}' \cdot g - \mathsf{cha} \cdot \mathsf{pk}_{i^*}^*$. This is the goal of Line 5 of the original $\tilde{\mathcal{A}}$. These imply that $\mathcal{M}$ perfectly simulates the original specific adversary $\tilde{\mathcal{A}}$.

For Multi-invocation of $\tilde{\mathcal{A}}$ by $\mathcal{R}$ Observe that the simulator of $\tilde{\mathcal{A}}$ is constructed to be deterministic. This implies that for the same input $(\mathbb{G}, q, g, \{\mathsf{pk}_i^*\}_{i=1}^N, \mathsf{O}_{\mathsf{Sig}}^{\mathcal{A}}(\tilde{i}, m), \mathsf{O}_H^{\mathcal{A}}(\mathsf{cmt}_{\{\mathsf{res} \cdot g - \mathsf{cha} \cdot \mathsf{pk}_{\tilde{i}}^*\}}, m))$ to

```
$\mathcal{R}_{\mathsf{FPS}}(g, q, g, y)$
1 : $L_H, L_{\mathsf{alg}}, L_{\mathsf{Sig}} \leftarrow \emptyset$
2 : $(m^*, (\mathsf{cha}^*, \mathsf{res}^*)) \leftarrow\!\$\ \mathcal{A}^{\mathsf{O}_H^{\mathcal{A}}, \mathsf{O}_{\mathsf{Sig}}^{\mathcal{A}}}(g, q, g, y)$
3 : $\mathsf{cmt}^* \leftarrow \mathsf{cha}^* \cdot g - \mathsf{res}^* \cdot y$
4 : abort if $m^* \in L_{\mathsf{Sig}} \vee \mathsf{Vf}^{\mathsf{Sch}}(g, q, g, y, m^*, (\mathsf{cha}^*, \mathsf{res}^*)) \neq 1$   // During that, running $\mathsf{O}_H^{\mathcal{A}}(\mathsf{cmt}^*, m^*)$
5 : $(\gamma^*, \delta^*) \leftarrow L_{\mathsf{alg}}[\mathsf{cmt}^*, m^*]$
6 : return $(\mathsf{res}^* - \delta^*)/(\mathsf{cha}^* + \gamma^*)$
```

```
$\mathsf{O}_H^{\mathsf{FPS}}(\mathsf{cmt}_{\{\gamma \cdot g + \delta \cdot y\}}, m)$
1 : if $L_H[\mathsf{cmt}, m] = \perp$
2 :     $L_H[\mathsf{cmt}, m] \leftarrow\!\$\ \mathbb{Z}_q$
3 :     abort if $L_H[\mathsf{cmt}, m] = -\delta$
4 :     $L_{\mathsf{alg}}[\mathsf{cmt}, m] \leftarrow (\gamma, \delta)$
5 : return $L_H[\mathsf{cmt}, m]$
```

```
$\mathsf{O}_{\mathsf{Sig}}^{\mathsf{FPS}}(m)$
1 : $\mathsf{cha}, \mathsf{res} \leftarrow\!\$\ \mathbb{Z}_q$
2 : $\mathsf{cmt} \leftarrow \mathsf{res} \cdot g - \mathsf{cha} \cdot y$
3 : abort if $L_H[\mathsf{cmt}, m] \neq \perp$
4 : $L_H[\mathsf{cmt}, m] \leftarrow \mathsf{cha}$
5 : $L_{\mathsf{Sig}} \leftarrow L_{\mathsf{Sig}} \cup \{m\}$
6 : return $(\mathsf{cha}, \mathsf{res})$
```

Figure 4: Fuchsbauer-Plouviez-Seurin's Reduction $\mathcal{R}$ [14]

$\tilde{\mathcal{A}}$, $\tilde{\mathcal{A}}$ behaves the same, even when $\mathcal{R}$ invokes $\tilde{\mathcal{A}}$ many times and rewinds it. Therefore, the multiple invocations and the rewind of $\tilde{\mathcal{A}}$ by $\mathcal{R}$ do not affect the winning probability of $\mathcal{R}$.

Success Probability of $\mathcal{M}$ Since $\mathcal{M}$ simulates the specific MU-EUF-CMA adversary $\tilde{\mathcal{A}}$ correctly, $\mathcal{R}$ run by $\mathcal{M}$ can break DL assumption with the non-negligible probability $\epsilon_{\mathcal{R}}$ as the assumption on $\mathcal{R}$. Thus $\mathcal{M}$ can break DL assumption with the non-negligible probability $\epsilon_{\mathcal{R}}$. □

For the restriction of N public keys $\{\mathsf{pk}_i^*\}_{i=1}^N$ that are given to the adversary, the similar construction of public keys can be seen in the reduction by [28] which proves MU-EUF-CMA of Sch from DL assumption in ROM (not in AGM). Namely, Theorem 1 implies that the known proof technique to prove MU-EUF-CMA of Sch cannot be applied in the AGM setting.

5 Discussions

In this secion, we review the previous result by [14] of proving the securiry of Sch.

Recall that Fuchsbauer, Plouviez and Seurin showed that Sch is EUF-CMA in AGM+ROM with tight reduction [14], whereas we have shown the impossibility of proving MU-EUF-CMA of Sch in AGM+ROM via an algebraic reduction in the previous section. We discuss why the Fuchsbauer-Plouviez-Seurin's result is not straightforwardly applied to the MU-EUF-CMA case.

Let us briefly recap the security reduction $\mathcal{R}_{\mathsf{FPS}}$ of [14] that proves EUF-CMA from DL assumption. Their security reduction $\mathcal{R}_{\mathsf{FPS}}$ can be depicted as in Fig. 4 [2]. The procedures of $\mathcal{R}_{\mathsf{FPS}}$ are divided into the followings.

(P.I) As depicted at Line 2 in $\mathcal{R}_{\mathsf{FPS}}$, on a given DL instance $(\mathbb{G}, q, g, y)$, $\mathcal{R}_{\mathsf{FPS}}$ invokes an EUF-CMA adversary $\mathcal{A}$ of Sch with $(\mathbb{G}, q, g, y)$. Here, y is regarded as the challenge public key given to $\mathcal{A}$.

(P.II) As depicted in $\mathsf{O}_H^{\mathsf{FPS}}$, when $\mathcal{A}$ makes a hash oracle query $(\mathsf{cmt}, m) \in \mathbb{G} \times \{0,1\}^{\ell_m}$, $\mathcal{R}_{\mathsf{FPS}}$ returns its hash value $\mathsf{cha} \in \mathbb{Z}_q$ by emulating the hash oracle.

[2] In [14], a signature generated by Sch is defined by (cmt, res), whereas it is defined by (cha, res) in this paper. We slightly modify the actual reduction $\mathcal{R}_{\mathsf{FPS}}$ to deal with our form of signatures. Such a modification would enable us to explain the behavior of $\mathcal{R}_{\mathsf{FPS}}$ succinctly.

(P.III) As depicted in $\mathsf{O}^{\mathsf{FPS}}_{\mathsf{Sig}}$, when $\mathcal{A}$ makes a signing oracle query $m \in \{0,1\}^{\ell_m}$, $\mathcal{R}_{\mathsf{FPS}}$ returns a signature $\sigma = (\mathsf{cha}, \mathsf{res}) \in \mathbb{Z}_q^2$ by emulating the signing oracle.

(P.IV) As depicted at Lines 3–6 in $\mathcal{R}_{\mathsf{FPS}}$, when $\mathcal{A}$ finally returns a forgery $(m^*, (\mathsf{cha}^*, \mathsf{res}^*))$, $\mathcal{R}_{\mathsf{FPS}}$ finds the solution $x \in \mathbb{Z}_q$ of the DL instance $(\mathbb{G}, q, g, y)$.

In a similar manner to [34], the special soundness of Sch is utilized to realize the process (P.IV). The special soundness guarantees that we can extract the solution x of $(\mathbb{G}, q, g, y)$ from the two transcripts $(\mathsf{cmt}^*, \mathsf{cha}^*, \mathsf{res}^*)$ and $(\mathsf{cmt}, \mathsf{cha}, \mathsf{res})$ such that both tuples satisfy the verification formula $\mathsf{Vf}^{\mathsf{Sch}}$ with respect to $(\mathbb{G}, q, g, y)$ and $\mathsf{cmt}^* = \mathsf{cmt}$ and $\mathsf{cha}^* \neq \mathsf{cha}$. Thus $\mathcal{R}_{\mathsf{FPS}}$ aims to find such two transcripts.

The first transcript $(\mathsf{cmt}^*, \mathsf{cha}^*, \mathsf{res}^*)$ is obtained from the forgery $(m^*, (\mathsf{cha}^*, \mathsf{res}^*))$ by setting $\mathsf{cmt}^* = \mathsf{res}^* \cdot g - \mathsf{cha}^* \cdot y$. This part corresponds to Lines 2–3 in $\mathcal{R}_{\mathsf{FPS}}$. If $\mathcal{A}$ wins the $\mathsf{EUF\text{-}CMA}$ game, this transcript $(\mathsf{cmt}^*, \mathsf{cha}^*, \mathsf{res}^*)$ satisfies $\mathsf{Vf}^{\mathsf{Sch}}$ with respect to $(\mathbb{G}, q, g, y)$. On the other hand, $\mathcal{R}_{\mathsf{FPS}}$ aims to obtain another transcript by utilizing the emulation of the hash oracle and the algebraic property of $\mathcal{A}$. Now, we focus on the hash oracle query (cmt^*, m^*) from $\mathcal{A}$ which is expected to be made before $\mathcal{A}$ finally returns the forgery $(m^*, (\mathsf{cha}^*, \mathsf{res}^*))$. Since $\mathcal{A}$ is supposed to be algebraic, $\mathcal{A}$ is required to output a coefficient vector of $\mathsf{cmt}^* \in \mathbb{G}$ for the query (cmt^*, m^*). Moreover, the basis of coefficient vectors is $(g, y) \in \mathbb{G}^2$. This is because (g, y) are only elements in $\mathbb{G}$ given to $\mathcal{A}$. Then the coefficient vector is of the form (γ^*, δ^*) such that $\mathsf{cmt}^* = \gamma^* \cdot g + \delta^* \cdot y$. This implies that $(\mathsf{cmt}^*, -\delta^*, \gamma^*)$ satisfies $\mathsf{Vf}^{\mathsf{Sch}}$ with respect to $(\mathbb{G}, q, g, y)$. Observe that such a pair (δ^*, γ^*) is recorded at Line 4 in $\mathsf{O}^{\mathsf{FPS}}_{H}$ and then it is retrived at Line 5 in $\mathcal{R}$. Therefore we can employ the special soundness if $\mathsf{cha}^* \neq -\delta^*$.

To show $\mathsf{cha}^* \neq -\delta^*$, we consider two situations depending on the appearance of (cmt^*, m^*) in the signing oracle queries. First, consider the situation that (cmt^*, m^*) appears when m^* is queried to the signing oracle. We show that this situation never happens when $\mathcal{A}$ wins the $\mathsf{EUF\text{-}CMA}$ game. The reason is as follows. Due to the mechanism of Sch, for any fixed pair (cmt^*, m^*), the signature $(\mathsf{cha}^*, \mathsf{res}^*)$ of m^* is uniquely determined. In fact, cha^* is the hash value of the fixed pair (cmt^*, m^*), and there exists only one $\mathsf{res}^* \in \mathbb{Z}_q$ such that the transcript $(\mathsf{cmt}^*, \mathsf{cha}^*, \mathsf{res}^*)$ satisfies $\mathsf{Vf}^{\mathsf{Sch}}$ with respect to $(\mathbb{G}, q, g, y)$. Eventually, the reuse of (cmt^*, m^*) derives the reuse of the signature $(\mathsf{cha}^*, \mathsf{res}^*)$. Hence, such a transcript $(m^*, (\mathsf{cha}^*, \mathsf{res}^*))$ cannot be a forgery and leads to the game's loss.

Consider the opposite case where (cmt^*, m^*) does not appear in the signing oracle queries. Then the hash value cha^* is given from the hash oracle. $\mathcal{R}_{\mathsf{FPS}}$ emulates the hash oracle so that $\mathsf{cha}^* \neq -\delta^*$ with only negligible error probability. Therefore, when $\mathcal{A}$ wins the $\mathsf{EUF\text{-}CMA}$ game, we have $\mathsf{cha}^* \neq -\delta^*$ except the negligible probability. This means that the solution x is extractable from the two transcripts $(\mathsf{cmt}^*, \mathsf{cha}^*, \mathsf{res}^*)$ and $(\mathsf{cmt}^*, \gamma^*, -\delta^*)$ with overwhelming probability.

We now observe whether or not the strategy of $\mathcal{R}_{\mathsf{FPS}}$ is straightforwardly applied to $\mathsf{MU\text{-}EUF\text{-}CMA}$ case. In this setting, we cannot guarantee that the pair (cmt, m) that appeared in the signing oracle simulation is not reused as the forgery. In fact, $\mathsf{MU\text{-}EUF\text{-}CMA}$ adversary can return $(i^*, m^*, (\mathsf{cha}^*, \mathsf{res}^*))$ even if $\mathcal{A}$ queried m^* to the signing oracle with another index $i \neq i^*$. Moreover, such behavior of adversaries is employed in the specific forger $\tilde{\mathcal{A}}$ of Theorem 1 to derive the impossibility of $\mathsf{MU\text{-}EUF\text{-}CMA}$ in AGM+ROM.

This discussion suggests to us that we have to develop a new proof technique beyond the algebraic reduction, or to find a new form of public keys other than that considered in Theorem 1 in order to overcome our impossibility and prove $\mathsf{MU\text{-}EUF\text{-}CMA}$ of Sch with a tight reduction.

6 Concluding Remarks

For the security of Schnorr signature Sch, Fuchsbauer, Plouviez and Seurin [14] gave a tight reduction that proves $\mathsf{EUF\text{-}CMA}$ in AGM+ROM from DL assumption, and Kiltz, Masny and Pan [28] constructed a tight reduction from $\mathsf{EUF\text{-}CMA}$ to $\mathsf{MU\text{-}EUF\text{-}CMA}$ in ROM. Then it is expected that we can construct a tight reduction that proves $\mathsf{MU\text{-}EUF\text{-}CMA}$ of Sch in AGM+ROM from DL assumption.

However, against the above expectation, we have given the impossibility of proving MU-EUF-CMA of Sch in AGM+ROM only by combining their results in this paper. Our result is shown by focusing on the algebraic reduction and a specific type of public keys given to an MU-EUF-CMA adversary when a reduction invokes an adversary. We have also reviewed the previous result of [14]. We discuss the reason why the security reduction of [14] proving EUF-CMA in AGM+ROM is difficult to be applied to the multi-user case. Our result suggests that we have to develop a new proof technique or to find a new form of public keys that does not fall into the condition considered in Theorem 1. It remains open whether or not such a technique exists to overcome our impossibility barrier and prove MU-EUF-CMA of Sch with a tight reduction.

Acknowledgements

We would like to thank anonymous reviewers for their valuable comments and suggestions. This work was supported by JSPS KAKENHI Grant Numbers JP19K20272 and JP22K12023.

References

[1] Michel Abdalla, Jee Hea An, Mihir Bellare, and Chanathip Namprempre. From identification to signatures via the Fiat-Shamir transform: Necessary and sufficient conditions for security and forward-security. *Information Theory, IEEE Transactions on*, 54(8):3631–3646, 2008.

[2] Michel Abdalla, Pierre-Alain Fouque, Vadim Lyubashevsky, and Mehdi Tibouchi. Tightly-secure signatures from lossy identification schemes. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, pages 572–590. Springer Berlin Heidelberg, 2012.

[3] Prabhanjan Ananth and Raghav Bhaskar. Non observability in the random oracle model. In Willy Susilo and Reza Reyhanitabar, editors, *Provable Security 2013*, volume 8209, pages 86–103. Springer, Heidelberg, 2013.

[4] Christoph Bader, Tibor Jager, Yong Li, and Sven Schäge. On the impossibility of tight cryptographic reductions. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016*, pages 273–304. Springer Berlin Heidelberg, 2016.

[5] Mihir Bellare and Wei Dai. Chain reductions for multi-signatures and the HBMS scheme. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2021*, pages 650–678, Cham, 2021. Springer International Publishing.

[6] Mihir Bellare and Gregory Neven. Multi-signatures in the plain public-key model and a general forking lemma. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, CCS '06, pages 390–399, New York, NY, USA, 2006. ACM.

[7] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, CCS '93, pages 62–73, New York, NY, USA, 1993. ACM.

[8] Fabrice Benhamouda, Tancrède Lepoint, Julian Loss, Michele Orrù, and Mariana Raykova. On the (in)security of ROS. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021*, pages 33–53, Cham, 2021. Springer International Publishing.

[9] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. *Journal of Cryptology*, 17(4):297–319, 2004.

[10] Dan Boneh and Ramarathnam Venkatesan. Breaking RSA may not be equivalent to factoring. In Kaisa Nyberg, editor, *Advances in Cryptology — EUROCRYPT'98*, pages 59–71. Springer Berlin Heidelberg, 1998.

[11] Denis Diemert, Kai Gellert, Tibor Jager, and Lin Lyu. More efficient digital signatures with tight multi-user security. In Juan A. Garay, editor, *Public-Key Cryptography – PKC 2021*, pages 1–31, Cham, 2021. Springer International Publishing.

[12] Marc Fischlin and Nils Fleischhacker. Limitations of the meta-reduction technique: The case of Schnorr signatures. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, pages 444–460. Springer Berlin Heidelberg, 2013.

[13] Georg Fuchsbauer, Eike Kiltz, and Julian Loss. The algebraic group model and its applications. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018*, pages 33–62, Cham, 2018. Springer International Publishing.

[14] Georg Fuchsbauer, Antoine Plouviez, and Yannick Seurin. Blind Schnorr signatures and signed ElGamal encryption in the algebraic group model. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020*, pages 63–95, Cham, 2020. Springer International Publishing.

[15] Masayuki Fukumitsu and Shingo Hasegawa. Impossibility on the provable security of the Fiat-Shamir-type signatures in the non-programmable random oracle model. In Matt Bishop and Anderson C A Nascimento, editors, *Information Security*, pages 389–407, Cham, 2016. Springer International Publishing.

[16] Masayuki Fukumitsu and Shingo Hasegawa. Impossibility on the provable security of the Fiat-Shamir-type signatures in the non-programmable random oracle model. In M. Bishop and A.C.A. Nascimento, editors, *ISC 2016*, volume 9866 of *LNCS*, pages 389–407. Springer, Heidelberg, 2016.

[17] Masayuki Fukumitsu and Shingo Hasegawa. Black-box separations on Fiat-Shamir-type signatures in the non-programmable random oracle model. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E101.A(1):77–87, 2018.

[18] Masayuki Fukumitsu and Shingo Hasegawa. One-more assumptions do not help Fiat-Shamir-type signature schemes in NPROM. In Stanislaw Jarecki, editor, *Topics in Cryptology – CT-RSA 2020*, pages 586–609, Cham, 2020. Springer International Publishing.

[19] Masayuki Fukumitsu and Shingo Hasegawa. Impossibility on the Schnorr signature from the one-more DL assumption in the non-programmable random oracle model. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E104.A(9):1163–1174, 2021.

[20] Masayuki Fukumitsu and Shingo Hasegawa. On multi-user security of Schnorr signature in algebraic group model. In *2022 10th International Workshop on Information and Communication Security (WICS'22)*, pages 395–301, November 2022.

[21] Steven Galbraith, John Malone-Lee, and Nigel P. Smart. Public key signatures in the multi-user setting. *Information Processing Letters*, 83(5):263–266, 2002.

[22] Chaya Ganesh, Claudio Orlandi, Mahak Pancholi, Akira Takahashi, and Daniel Tschudi. Fiat-Shamir bulletproofs are non-malleable (in the algebraic group model). In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology – EUROCRYPT 2022*, pages 397–426, Cham, 2022. Springer International Publishing.

[23] Sanjam Garg, Raghav Bhaskar, and Satyanarayana V. Lokam. Improved bounds on security reductions for discrete log based signatures. In David Wagner, editor, *Advances in Cryptology – CRYPTO 2008*, pages 93–107. Springer Berlin Heidelberg, 2008.

[24] Shafi Goldwasser, Silvio Micali, and Ronald L Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. Comput.*, 17(2):281–308, 1988.

[25] Jens Groth. On the size of pairing-based non-interactive arguments. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016*, pages 305–326, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[26] Julia Kastner, Julian Loss, and Jiayu Xu. On pairing-free blind signature schemes in the algebraic group model. In Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe, editors, *Public-Key Cryptography – PKC 2022*, pages 468–497, Cham, 2022. Springer International Publishing.

[27] Handan Kılınç Alper and Jeffrey Burdges. Two-round trip Schnorr multi-signatures via delinearized witnesses. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 157–188, Cham, 2021. Springer International Publishing.

[28] Eike Kiltz, Daniel Masny, and Jiaxin Pan. Optimal security proofs for signatures from identification schemes. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016*, pages 33–61, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[29] Jonas Nick, Tim Ruffing, and Yannick Seurin. MuSig2: Simple two-round Schnorr multi-signatures. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 189–221, Cham, 2021. Springer International Publishing.

[30] Pascal Paillier and Damien Vergnaud. Discrete-log-based signatures may not be equivalent to discrete log. In Bimal Roy, editor, *Advances in Cryptology - ASIACRYPT 2005*, pages 1–20. Springer Berlin Heidelberg, 2005.

[31] Jiaxin Pan and Magnus Ringerud. Signatures with tight multi-user security from search assumptions. In Liqun Chen, Ninghui Li, Kaitai Liang, and Steve Schneider, editors, *Computer Security – ESORICS 2020*, pages 485–504, Cham, 2020. Springer International Publishing.

[32] Jiaxin Pan and Benedikt Wagner. Lattice-based signatures with tight adaptive corruptions and more. In Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe, editors, *Public-Key Cryptography – PKC 2022*, pages 347–378, Cham, 2022. Springer International Publishing.

[33] Rafael Pass. Limits of provable security from standard assumptions. In *STOC2011*, pages 109–118, 2011.

[34] David Pointcheval and Jacques Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, 2000.

[35] Claus-Peter Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3):161–174, 1991.

[36] Yannick Seurin. On the exact security of Schnorr-type signatures in the random oracle model. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, pages 554–571. Springer Berlin Heidelberg, 2012.

[37] Tatu Ylonen. The secure shell (ssh) transport layer protocol, 2006.