SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Algebraic Group Model 上での Schnorr 署名の Multi-User Security に関する一考察

A Note on the Multi-User Security of Schnorr Signature in Algebraic Group Model

福光 正幸 *　　長谷川 真吾 †
Masayuki FUKUMITSU　　Shingo HASEGAWA

キーワード Schnorr 署名, Multi-User Security, Algebraic Reduction, Algebraic Group Model

あらまし

Schnorr 署名 [5] は代表的なディジタル署名の実例の一つであり, この安全性証明可能性について, これまでに多くの議論がなされてきた. まず Pointcheval, Stern [4] は離散対数 (Discrete Logarithm) 仮定が成り立つ状況での安全性を証明した. しかし彼らの証明では, Random Oracle Model を仮定していたり, 構成した帰着 (Reduction) には Security Loss が発生していたりといくつかの条件が課せられていた. 一方, Paillier, Vergnaud [3] は, 文献 [4] の Random Oracle や Security Loss の条件を回避できないとする結果を示した. この安全性証明可能性や不可能性について, Kiltz, Masny, Pan [2] が Schnorr 署名の基となっている Fiat-Shamir 変換型署名に対する枠組みを導入し, その上で整理した. さらに, 文献 [2] では, 複数の公開鍵が攻撃対象となりうる MU-EUF-CMA (Multi-User Existential Unforgeability against Chosen Message Attack) 安全性について同時に議論していた.

近年, 上述の否定的な結果に対し, Fuchsbauer, Plouviez, Seurin [1] は, Algebraic Group Model に限定することで, Schnorr 署名の安全性を Security Loss なしで証明した. ここで, Algebraic Group Model とは, 攻撃者が Algebraic Algorithm, すなわち, 攻撃者が出力する任意の群 $\mathbb{G}$ の元は, 入力された $\mathbb{G}$ の元の線形和で記述できるアルゴリズムに制限するモデルのことをいう. しかし, 彼らの結果で想定している安全性は, 通常の EUF-CMA であり, MU-EUF-CMA 安全性は達成していなかった.

本研究では, Algebraic Group Model における, Schnorr 署名の MU-EUF-CMA 安全性の証明可能性について議論する. 我々はこれまでに, 文献 [1] の結果を文献 [2] の枠組みに適用することで, Algebraic Group Model 上の EUF-CMA 安全性までの結果を整理したきた [6]. 本稿では, 文献 [6] の続きとして, Algebraic Algorithm の場合, Schnorr 署名の EUF-CMA 安全性から MU-EUF-CMA 安全性に持ち上げることができるかどうかについて議論する. 具体的には, Algebraic Algorithm を考慮した場合, 従来研究における MU-EUF-CMA 安全性証明の技法が適用できないことを示していく.

* 北海道情報大学 情報メディア学部, 〒 069-8585 北海道江別市西野幌 59 番 2, Faculty of Information Media, Hokkaido Information University, Nishi Nopporo 59-2, Ebetsu, Hokkaido. 069-8585
† 東北大学 大学院情報科学研究科, 〒 980-8576 宮城県仙台市青葉区川内 41, Graduate School of Information Sciences, Tohoku University, Kawauchi 41, Aoba-ku, Sendai, Miyagi. 980-8576

参考文献

[1] G. Fuchsbauer, A. Plouviez, and Y. Seurin, “Blind Schnorr signatures and signed ElGamal encryption in the algebraic group model,” Proc. Advances in Cryptology – EUROCRYPT 2020, Cham, pp.63–95, 2020.

[2] E. Kiltz, D. Masny, and J. Pan, “Optimal security proofs for signatures from identification schemes,” Proc. Advances in Cryptology – CRYPTO 2016, Berlin, Heidelberg, pp.33–61, 2016.

[3] P. Paillier and D. Vergnaud, “Discrete-log-based signatures may not be equivalent to discrete log,” Proc. Advances in Cryptology - ASIACRYPT 2005, pp.1–20, 2005.

[4] D. Pointcheval and J. Stern, “Security arguments for digital signatures and blind signatures,” Journal of Cryptology, vol.13, no.3, pp.361–396, 2000.

[5] C.P. Schnorr, “Efficient signature generation by smart cards,” Journal of Cryptology, vol.4, no.3, pp.161–174, 1991.

[6] 福光 正幸, 長谷川 真吾, “Algebraic group model における Fiat-Shamir 変換,” Proc. コンピュータセキュリティシンポジウム 2021（CSS2021）, pp.1–8, 2021.