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

帰着効率がタイトな helper 付き Unruh 変換の提案と効率的なディジタル署名の構成
Unruh Transform using Helper with Tight Reduction and Construction of Efficient Digital Signatures

加藤　拓 *　　古江　弘樹 *　　高木　剛 *
Taku Kato　　Hiroki Furue　　Tsuyoshi Takagi

キーワード　耐量子計算機暗号, ディジタル署名, Fiar-Shamir 変換, Unruh 変換, Picnic3

あらまし

ディジタル署名は IDentification Scheme (IDS) を変換して構成することが可能である．そこで用いられる変換として Fiat-Shamir 変換と Unruh 変換があげられる [7]．この二つの変換を比べると, 一般に Fiat-Shamir 変換により得られるディジタル署名の方が署名長が短くなるという特徴があるが, 安全性証明の帰着効率については Unruh 変換の方が優れている．Unruh 変換は ROM, QROM において EUF-CMA 安全であり, 帰着効率がタイトな安全性証明を持つ．

安全性証明の帰着先の計算問題の一つに多変数多項式求解 (MQ) 問題がある．Sakumoto ら [6] は MQ 問題の困難性に帰着可能な IDS を提案した．この IDS に Fiat-Shamir 変換を用いて構成されるディジタル署名としては MQDSS [2], MUDFISH [1] がある．一方 Kales ら [4] は, MQDSS に対して安全性証明の帰着効率がタイトでないことを利用した攻撃を提案した．このような攻撃の可能性を回避するためにも, 帰着効率がタイトな安全性証明を持つディジタル署名を構成することが重要である．そのため Furue ら [3] は Unruh 変換を用いて, 帰着効率がタイトな安全性証明を持つディジタル署名を構成した．しかし署名長が MUDFISH に比べて, 約 2 倍となるデメリットを持つ．MUDFISH では, helper 付き IDS という特殊な IDS を用いることで, Fiat-Shamir 変換を用いる MQDSS より署名長を削減した．

よって本研究では helper 付き IDS に対する Unruh 変換 (helper 付き Unruh 変換) を構成し, 高い安全性となるタイトな帰着を持つディジタル署名を提案する．Helper 付き Unruh 変換では cut-and-choose と呼ばれる手法を利用して, 既存の Unruh 変換と同様に証明者の正当性を認証するラウンドと helper の正当性を認証するラウンドに分割する．

本研究では MUDFISH の IDS に対して helper 付き Unruh 変換を適用した．128 ビットセキュリティにおいて Furue らのディジタル署名の署名長は 29.6KB であるが, 提案手法では 18.7KB であり, 約 6 割に削減した．

更に本研究では, Picnic3 というディジタル署名の IDS に対して helper 付き Unruh 変換を適用することを提案する．安全性証明について Picnic3 は帰着効率がタイトでないが, 提案手法はタイトである．また 128 ビットセキュリティにおいて Picnic3 の署名長は 12.3KB であるが, 提案手法では 9.2KB であり, 7 割以下に削減した．更に署名生成及び認証アルゴリズムの計算時間も削減した．

参考文献

[1] Beullens, W.: Sigma protocols for mq, pkp and sis, and fishy signature schemes. In: EUROCRYPT 2020. LNCS 12107, pp. 183 - 211. (2020)
[2] Chen, M.S., Hülsing, A., Rijneveld, J., Samardjiska, S., Schwabe, P.: From 5-pass MQ-based identification to MQ-based signatures. In: ASIACRYPT 2016. LNCS 10032, pp. 135 - 165. (2016)
[3] Furue, H., Duong, D., Takagi, T.: An efficient MQ-based signature with tight security proof. In: IJNC. vol. 10(2), pp. 308 - 324 (2020)
[4] Kales, D., Zaverucha, G.: Forgery attacks on MQDSSv2.0 (2019)
[5] Kales, D., Zaverucha, G.: Improving the performance of the picnic signature scheme. IACR Cryptology ePrint Archive 2020/427 (2020)
[6] Sakumoto, K., Shirai, T., Hiwatari, H.: Public-key identification schemes based on multivariate quadratic polynomials. In: CRYPTO 2011. LNCS 6841, pp. 706 - 723. (2011)
[7] Unruh, D.: Non-interactive zero-knowledge proofs in the quantum random oracle model. In: EUROCRYPT 2015. LNCS 9057, pp. 755 - 784. (2015)

* 東京大学大学院 情報理工学系研究科 数理情報学専攻 〒 113–8656 東京都文京区本郷 7-3-1, Department of Mathematical Informatics, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan