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

指数部検査を省略したFSU方式のピア事後指定安全性
Post-Specified Peer Security of FSU Scheme without Exponent Check

小山 幸保 * 藤岡 淳 * 佐々木 太良 * 岡野 裕樹 † 永井 彰 †
Yukiho Koyama Atsushi Fujioka Taroh Sasaki Yuki Okano Akira Nagai

キーワード ID ベース認証鍵交換，post-specified peer モデル，ペアリング

あらまし

本論文では，SCIS2020 で発表された ID ベース認証鍵交換 (IBAKE) 方式である FSUw/oCheck [1] が post-specified peer モデルで安全かを検証した．

IBAKE は，通信相手の ID を知るタイミングによって安全性モデルが pre-specified peer モデルと post-specified peer モデルに分類できる．pre-specified peer モデルは，方式を実行する前に通信相手の ID を知っていることが前提のものであり，post-specified peer モデルは，サーバの IP アドレスなどの通信相手のアドレスのみを知る状態で方式を実行し，実行途中で通信相手の ID を知るというものである．これは，通信前に通信相手の ID を知ることができない場合に有効である．

pre-specified peer モデルと post-specified peer モデルを同時に満たす Combined モデル [2] は，認証鍵交換 (AKE) に対してのみ定義されている．Combined モデルでは，敵対者に EphemeralPublicKeyReveal というクエリが許されており，これは，敵対者がセッションとは無関係に入手できるものである．つまり，通信相手の ID を知らない状態で一時公開鍵を生成することを意味し，post-specified peer モデルを表している．そこで本論文では，IBAKE の安全性モデルに EphemeralPublicKeyReveal を追加することで IBAKE に対する Combined モデルを提案する．

IBAKE の既存方式に，gap Bilinear Diffie-Hellman (GBDH) 仮定およびランダムオラクルモデルの下で id-eCK 安全な非対称ペアリング版 FSU があり，これは 4 回のペアリングを要する．一方，非対称ペアリング版 FSU の指数部検査を除いた FSUw/oCheck は，id-eCK 安全となるために必要な数学的な仮定が 1-{1,2}-{1,2} 型非対称 GBDH 仮定となるが，ペアリングを 2 回に抑えることができる．また，XDTH 仮定および q-Gap-BCA 仮定，ランダムオラクルモデルの下で id-eCK 安全な TFNS [3] は，ペアリングが 1 回であるが，通信前に始動側のユーザが応答側のユーザの ID を得る必要があるため post-specified peer 安全になり得ないと予想される．

本論文では，IBAKE の一方式である FSUw/oCheck が 1-{1,2}-{1,2} 型非対称 GBDH 仮定，ランダムオラクルモデル，post-specified peer モデルにおいて安全であることを提案した Combined モデルを用いて検証する．

参考文献

[1] 岩井光輝, 川口武瑠, 佐々木太良, 藤岡淳, 鈴木幸太郎, 永井彰, 富田潤一. 非対称 pairing 版 FSU における指数部検査の必要性. In *SCIS 2020*. 3B1-1, 2020.

[2] Alfred Menezes and Berkant Ustaoglu. Comparing the pre- and post-specified peer models for key agreement. *Int. J. Appl. Cryptogr.*, Vol. 1, No. 3, pp. 236–250, 2009.

[3] Junichi Tomida, Atsushi Fujioka, Akira Nagai, and Koutarou Suzuki. Strongly secure identity-based key exchange with single pairing operation. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, Vol. 104-A, No. 1, pp. 58–68, 2021.

* 神奈川大学, 221-8686 神奈川県横浜市神奈川区六角区橋 3–27–1, Kanagawa University, 3–27–1, Rokkakuba-shi, Kanagawa-ku, Yokohama, Kanagawa, Japan (r201804292bg@jindai.jp, {fujioka, taroh}@kanagawa-u.ac.jp)
† NTT 社会情報研究所, 180–8585 東京都武蔵野市緑町 3–9–11, NTT Social Informatics Laboratories, 3–9–11 Midori-cho, Musashino-shi, Tokyo 180–8585 Japan ({yuki.okano.te, akira.nagai.td}@hco.ntt.co.jp)