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

最大鍵漏洩攻撃に対して安全で計算効率のよいPKI-ID混在認証鍵交換
Efficient PKI-ID cross-domain authenticated key exchange secure against maximal exposure attacks

青柳 光太郎 * 岡野 裕樹 † 永井 彰 † 藤岡 淳 ‡ 鈴木 幸太郎 *
Kohtaroh Aoyagi Yuki Okano Akira Nagai Atsushi Fujioka Koutarou Suzuki

キーワード 認証鍵交換, PKI ベース認証, ID ベース認証, ペアリング

あらまし

認証鍵交換方式に関して，公開鍵を用いて認証を行うPKI ベース認証鍵交換方式と，ID を用いて認証を行うID ベース認証鍵交換方式が主に研究されている．認証鍵交換方式の安全性については，すべての鍵漏洩パターンを考慮した eCK (extented Canetti–Krawcyzk) 安全性と呼ばれる強い安全性が提案されている [2]．eCK 安全な PKI ベース認証鍵交換方式として例えば [2]，[4] が提案されており，ID-eCK 安全な ID ベース認証鍵交換方式として例えば [3]，[5] が提案されている．

一方，Ustaoğlu [1] は，PKI ベース認証と ID ベース認証が混在する環境で認証を行う PKI-ID 混在認証鍵交換方式を提案した．Ustaoğlu の方式は，最大鍵漏洩攻撃に対して安全で，ペアリング演算を 2 回必要としている．

本研究では，最大鍵漏洩攻撃に対して安全で，ペアリング演算を 1 回必要とする PKI-ID 混在認証鍵交換方式を提案する．提案方式は NAXOS 構成法を用いて最大鍵漏洩攻撃に対する安全性を実現している．また提案方式は，最大鍵漏洩攻撃に対する安全性を満たす PKI-ID 混在認証鍵交換方式のなかで最も効率の良いものとなっている．

ID ベース認証鍵交換方式は IoT 機器間の通信に用いることが考えられている．一方，インターネットにおいては PKI ベース認証鍵交換方式が用いられている．そのため，提案方式は IoT 機器のネットワークとインターネットを統合する際に有用であると考えられる．

* 豊橋技術科学大学, 〒 441-8580 愛知県豊橋市天伯町雲雀ヶ丘 1 – 1 , Toyohashi University of Technology, 1-1 Hibarigaoka, Tempaku, Toyohashi, Aichi, 441-8580, JAPAN
† 日本電信電話株式会社, 〒 180-8585 東京都武蔵野市緑町 3-9-11, NTT Corporation, 3-9-11, Midoricho, Musashino-shi, Tokyo 180-8585, Japan
‡ 神奈川大学, 〒 221-8686 神奈川県横浜市神奈川区六角橋 3-27-1, Kanagawa University, 3-27-1, Rokkakubashi, Kanagawa-ku, Yokohama, Kanagawa, Japan

参考文献

[1] Ustaoğlu, Berkant, “Integrating identity-based and certificate-based authenticated key exchange protocols,” International Journal of Information Security, 2011

[2] LaMacchia, Brian and Lauter, Kristin and Mityagin, Anton,“Stronger security of authenticated key exchange,” International conference on provable security, 2007

[3] Tomida, Junichi and Fujioka, Atsushi and Nagai, Akira and Suzuki, Koutarou, “Strongly secure identity-based key exchange with single pairing operation,” European Symposium on Research in Computer Security, 2019

[4] Ustaoğlu, Berkant, “Obtaining a secure and efficient key agreement protocol from (H) MQV and NAXOS,” Designs, Codes and Cryptography, 2008

[5] 木下 魁, 永井 彰, 富田 潤一, 鈴木 幸太郎, 藤岡 淳,“TLS1.3 への適用を考慮した ID ベース認証鍵交換方式,” SCIS2020