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

強フォワード秘匿性を満たす匿名一方向認証鍵交換
Anonymous One-Sided Authenticated Key Exchange with Strong Forward Secrecy

石橋 錬 * 米山 一樹 *
Ren Ishibashi Kazuki Yoneyama

キーワード 認証鍵交換, 一方向安全性, 匿名性, 強フォワード秘匿性, 耐量子, 同種写像

あらまし

認証鍵交換 (AKE) はインターネットのような認証されていない通信路を用いて複数のパーティ間で共通のセッション鍵を共有するための暗号プロトコルである。通常の公開鍵基盤ベースの AKE では，各パーティは自分自身の長期秘密鍵を保持し，それに対応する長期公開鍵を発行する。鍵交換のセッションでは，各パーティは短期秘密鍵を生成し，それに対応する短期公開鍵を相手に送信する。セッション鍵は，これらの鍵と鍵導出関数から導出される。通常の AKE はセッション鍵の秘匿と相互認証を目的としている。

一方，Tor や Riffle のような匿名ネットワークのように相互認証が望ましくない通信も普及しており，また，HTTPS のトランザクションでは，認証されていないクライアントが，認証されたサーバと通信するのが一般的である。このように片側認証を前提とし，匿名性を保証する暗号プロトコルとして一方向 AKE が知られている。一方向 AKE はクライアント・サーバの 2 者間通信を想定しており，クライアントは長期秘密鍵を持たない AKE である。Goldberg らは各秘密情報の非自明な漏洩を許したとしてもセッション鍵の秘匿性と匿名性を保証する一方向 AKE 安全性モデル [GSU12] を定式化し，ランダムオラクルモデルで安全な具体的方式を提案した。その後，Ishibashi と Yoneyama [IY22] は、KEM に基づく標準モデルで安全な一般構成を提案し，具体的構成として耐量子方式を与えている．

一方，AKE に求められる安全性として，長期秘密鍵が漏れた後でも過去のセッション鍵の秘匿性を保証するフォワード秘匿性がある。特に，攻撃者が通信を改ざんしたセッションについても保証できる強フォワード秘匿性が望ましい。しかし，Goldberg らの既存の安全性モデルは攻撃者が改ざんしていないセッションに攻撃対象が限定される弱フォワード秘匿性しか保証していない。そのため，これまでの既存方式は全て弱フォワード秘匿性を満たす方式であり，強フォワード秘匿性を満たす方式は知られていない。

本稿では，強フォワード秘匿性を捉えた一方向 AKE の安全性モデルを提案し，強フォワード秘匿性を満たす匿名一方向 AKE の一般構成と，その具体的方式を提案する。我々の一般構成は KEM と非適応的選択文書攻撃に対して存在的偽造不可能な決定的電子署名に基づいており，初めての標準モデルにおける方式やランダムオラクルモデルにおける耐量子方式を実現することができる。

参考文献

[IY22] R. Ishibashi, K. Yoneyama,: Post-Quantum Anonymous One-Sided Authenticated Key Exchange without Random Oracles, *PKC 2022*, 2022.

[GSU12] I. Goldberg, D. Stebila, B. Ustaoglu,: Anonymity and one-way authentication in key exchange protocols, *Designs, Codes and Cryptography*, pp. 1–25, 2012.

* 茨城大学, 〒 316-8511 茨城県日立市中成沢町 4-12-1, Ibaraki University, 4-12-1, Nakanarusawacho, Hitachi-shi, Ibaraki 316-8511, Japan,