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

QUIC への ID ベース認証鍵交換 TFNS の適用と実装評価
Application of ID-Based Authenticated Key Exchange TFNS to QUIC and Its Implementation

村上 啓造 * 岡野 裕樹 * 青木 信雄 † 永井 彰 *
Keizo MURAKAMI Yuki OKANO Nobuo AOKI Akira NAGAI

キーワード QUIC, TLS1.3, ID ベース鍵交換

あらまし

2021 年 5 月に IETF にて RFC9000 として標準化された通信プロトコルである QUIC に対し，ID ベース鍵交換プロトコルである TFNS[1] を適用する方式を提案する．TFNS は一回の鍵交換につきペアリング演算が一度で済むため，従来の ID ベース鍵交換プロトコルに比べ，効率がよい．また，通信相手の ID を事前に知っていれば 1 ラウンドでの鍵交換が可能であるため，QUIC における一往復のハンドシェイクに適用が可能である．TFNS を用いることで，QUIC にて一般的に利用される DH 鍵交換と証明書による認証に比べ，証明書の送受信が不要となるため，通信データ量が削減でき，認証および鍵交換の性能向上が期待できる．QUIC のハンドシェイク部分は TLS1.3 をベースとしており，TLS1.3 へ TFNS を適用した場合の結果は既報 [2] の通りである．QUIC はトランスポート層として UDP を用いる QUIC に TFNS を実際に組み込んで動作検証を行った．本稿では，QUIC の実装として microsoft 社の MsQuic を用い，通信遅延，通信帯域，パケットロス率を段階的に変更し，ハンドシェイクにかかる時間を測定した結果について述べる．

以下に，TLS1.3 over TLS の場合と QUIC の場合の違いを図 1 に示す．

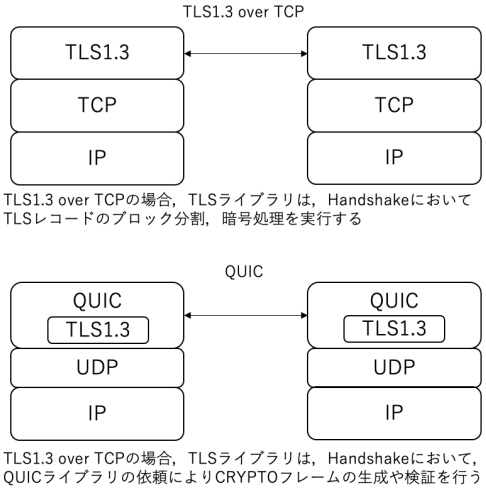

図 1: TLS1.3 over TLS と QUIC の比較

参考文献

[1] J. Tomida, A. Fujioka, A. Nagai, and K. Suzuki,“ Strongly Secure Identity-Based Key Exchange with Single Pairing Operation,”in Computer Security – ESORICS 2019, 2019, pp. 484–503.

[2] 木下魁, 永井彰, 鈴木幸太郎,“ TLS1.3 への ID ベース認証鍵交換の適用と実装評価”コンピュータセキュリティシンポジウム 2019 ,824-830.

* NTT 社会情報研究所, 〒 180-8585 東京都武蔵野市緑町 3-9-11. NTT Social Laboratories, 3-9-11, Midori-cho, Musashino-shi, Tokyo 180-8585, Japan. keizo.murakami.cv@hco.ntt.co.jp
† 広島市立大学, 〒 731-3194 広島市安佐南区大塚東 3-4-1, Hiroshima City Uni- versity, 3-4-1, Ozuka-Higashi, Asaminami-ku, Hiroshima, 731-3194, Japan.