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

対話的追跡機能付き集約署名における署名送信間隔に関する制約と評価
Constraints and Evaluations on Signature Transmission Interval for Aggregate Signatures with Interactive Tracing

石井 龍 *†‡ Ryu Ishii
山下 恭佑 ‡ Kyosuke Yamashita
宋 子豪 § Song Zihao
照屋 唯紀 ‡ Tadanori Teruya
坂井 祐介 ‡ Yusuke Sakai
花岡 悟一郎 ‡ Goichiro Hanaoka
松浦 幹太 * Kanta Matsuura
松本 勉 ‡ § Tsutomu Matsumoto

キーワード センサーネットワーク, 集約署名, 追跡可能集約署名, dynamic traitor tracing

あらまし

集約署名は，複数のデジタル署名を 1 つに集約する方式であり，全体署名長および署名検証時間の短縮という効率性を持つが，不正署名を 1 つでも含んで集約すると集約署名は不正となり，検証者はどのユーザやデバイスが不正署名を生成したかを特定できない．対話的追跡機能付き集約署名は，多数のデバイスが定期的に署名付きデータを送信するシステムで，時々刻々と変わる不正署名の生成デバイスを，集約者と検証者の対話によって特定する方式である．しかし，集約者は，デバイスからの署名を集約するために，検証者からのフィードバックを待つ必要があるため，システムの規模に応じて署名送信間隔に制約が生じる．本研究では，集約者がフィードバック待機なしに集約署名を作成できる方式として Sequential Traitor Tracing を構成要素とする対話的追跡機能付き集約署名を提案する．また，提案方式と既存方式である Dynamic Traitor Tracing を用いた対話的追跡機能付き集約署名について理論評価および実装シミュレーションによる評価を行う．

* 東京大学生産技術研究所, 〒 153-8505 東京都目黒区駒場 4-6-1
† ryuishii@iis.u-tokyo.ac.jp
‡ 産業技術総合研究所 サイバーフィジカルセキュリティ研究センター, 〒 130-0064 東京都江東区青海 2-3-26
§ 横浜国立大学 大学院環境情報研究院, 〒 240-8501 神奈川県横浜市保土ヶ谷区常盤台 79-7