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

追跡可能集約署名に対する潜在的な攻撃とその対処法に関する考察

A Study of A Potential Attack on Fault-Tolerant Aggregate Signature Schemes and How to Deal with It

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

追跡可能集約署名（fault-tolerant aggregate signature schemes, Hartung ら, PKC ’16）とは，集約署名に不正な署名が混入していた場合にその発信元を特定する能力を具備した方式である．集約署名はセンサーネットワークや効率的なルーティングへの応用が期待されている暗号機能であり，そのためにも不正者特定は重要な機能として注目を浴びている．追跡可能集約署名の一般的構成は既にいくつか提案されているが，本稿では石井ら（ACNS SCI ’21）の提案した動的な不正者に耐性を持つマルチラウンドな追跡可能集約署名の拡張を考える．彼らは安全性の定式化のために不正者が毎ラウンド少なくとも 1 人は現れるモデルを考えた．そのような仮定は先述のアプリケーションへの適用を考える際には非現実的であるため，我々は不正者が不正をしないラウンドを許容するモデルを検討した．その結果，追跡可能集約署名を現実に利用する場合に潜在的に起こり得る効率性に対する新たな攻撃を発見し，それに効率的に対処するためのアルゴリズムを提案した．

* 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
† yamashita.kyosuke@aist.go.jp
‡ 東京大学生産技術研究所, 〒 153-8505 東京都目黒区駒場 4-6-1
§ 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