Copyright© 2022 The Institute of Electronics,
Information and Communication Engineers

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

追跡可能集約署名プロトコルのためのクラウド上シミュレータの提案とプロトタイプ実装

Proposal and Prototype Implementation of a Cloud-Based Simulator for Traceable Aggregate Signature Protocol

宋　子豪*　安西　陸*　坂本 純一†*　吉田 直樹*　松本 勉*
Zihao Song　Riku Anzai　Junichi Sakamoto　Naoki Yoshida　Tsutomu Matsumoto

キーワード 高機能暗号，センサーネットワーク，集約署名，シミュレータ，ソフトウェア実装

あらまし

近年, 半導体のコストダウンとセンサーデバイスの小型化により，IoT デバイスの多くが工場や都市インフラ管理システムの末端センサーとして使用されている. これらのデバイスの特徴として, 低性能かつ安価で通信帯域やデータ量に制限のあるものが多い. また IoT センサーネットワークの特徴として末端デバイスからの情報を一度集約し上位ノードへ転送するエッジと呼ばれる中間ノードを持つことがある[1]．このようなネットワークに対し，少量の追加計算と通信コストでデータの改ざんを検出できる技術として高機能暗号の一種である集約署名の導入が検討されている[2][3]. しかし, 単に集約署名を適用した場合, 各ノード間の通信帯域や通信遅延の許容範囲などのパラメータ次第では集約署名の効率や具体的な追加通信データ量，不正なデバイスの追跡効率などが変化し，単純計算によって最適な集約署名の適応方法を求めるのは難しい. 我々はいくつかの前提下で任意のデバイス数を含むネットワークモデルに対し集約署名を実用化する際に必要となるパラメータを評価できる図１のような構成のコンテナ技術ベースのシミュレータを提案し, 実装したプロトタイプを使ってシミュレーションした結果を示す.

*横浜国立大学，〒240-8501 横浜市保土ケ谷区常盤台 79-7
Yokohama National University, 79-7 Tokiwadai, Hodogaya-ku, Yokohama 240-8501, Japan
†国立研究開発法人産業技術総合研究所，〒135-0064 東京都江東区青海 2-3-26
National Institute of Advanced Industrial Science and Technology, 2-3-26 Aomi, Koto-ku, Tokyo 135-0064, Japan

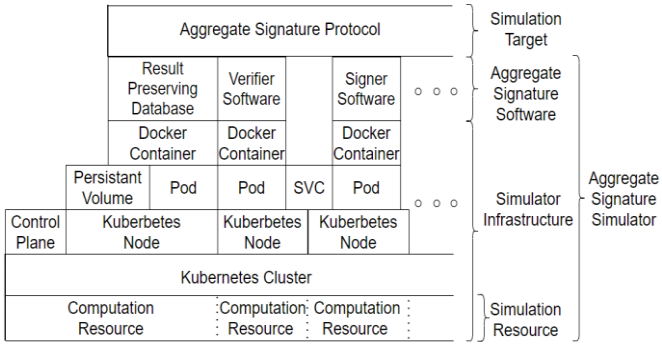

図 1. シミュレータの構成

参考文献

[1] P. Schulz et al., "Latency Critical IoT Applications in 5G: Perspective on the Design of Radio Interface and Network Architecture," IEEE Communications Magazine, vol. 55, no. 2, pp. 70-78, IEEE, 2017
[2] D. Boneh, X. Boyen, “Short Signatures Without Random Oracles,” In: Cachin C., Camenisch J.L. (eds) Advances in Cryptology, EUROCRYPT 2004. Lecture Notes in Computer Science, vol 3027, pp 56-73, Springer, 2004
[3] D. Boneh, C. Gentry, B. Lynn, H. Shacham, “Aggregate and Verifiably Encrypted Signatures from Bilinear Maps,” Lecture Notes in Computer Science, vol 2656, pp 416-432, Springer, 2003

本研究の一部は，内閣府が進める戦略的イノベーション創造プログラム（SIP）「ＩｏＴ社会に対応したサイバー・フィジカル・セキュリティ」（管理法人：NEDO）によって実施されたものである.