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

IoT ネットワークにおける検証者指定署名方式
Multi-Designated Verifier Signatures over IoT Networks

渡邉 洋平 [*] [†] 矢内 直人 [‡] [†] 四方 順司 [§]
Yohei Watanabe Naoto Yanai Junji Shikata

キーワード 遠隔制御システム，放送型認証技術，検証者指定署名

あらまし

次のような IoT ネットワーク上における遠隔制御システムを考える．(1) 情報がシステム管理者から全ての IoT デバイスに同報送信されるような環境，例えば無線環境において，任意の IoT デバイスにのみ，システム管理者が指定したコマンドを実行させることができる; (2) 通信路上の情報の改ざんを検知し，指定されていないコマンドが実行されることを防ぐ．AINA 2021 において，著者らはそのようなシステムの中核をなす暗号技術として，匿名放送型認証技術 (Anonymous Broadcast Authentication: ABA) を提案した [4]．ABA では，送信者が指定した受信者（IoT 機器）のみが認証子の正当性を検証することができ，かつ，認証子からどの受信者が指定されているかがわからないことを保証する匿名性を達成することができる．ABA は共通鍵暗号プリミティブのみから構成され，効率的な時間計算量を達成しているものの，その匿名性のため，上記システムで同報送信される認証コマンド長が指定受信者数に線形依存し，非効率的であった．実際，IMACC 2021 において，Kobayashi らによって ABA の認証子長の下界が導出され，[4] の構成が漸近的に最適であることが示されている [3]．

本稿では，同システムにおける通信計算量の削減を目指し，ABA に代わる暗号技術として，新たな検証者指定署名方式 (Multi-Designated Verifier Signature: MDVS) を提案する．具体的には，新たな MDVS のモデル及び安全性を定式化し，確率的データ構造（例えば，Bloom フィルタ [1] やカッコウフィルタ [2]）とディジタル署名を用いた構成法を提案する．結果として，ABA を利用した場合に比べ，匿名性はないものの，より認証コマンド長が効率的な遠隔制御システムを実現が可能である．

参考文献

[1] B. H. Bloom. Space/time trade-offs in hash coding with allowable errors. *Communication of the ACM*, 13(7):422–426, jul 1970.

[2] B. Fan, D. G. Andersen, M. Kaminsky, and M. D. Mitzenmacher. Cuckoo filter: Practically better than bloom. In *ACM CoNEXT 2014*, CoNEXT '14, page 75–88, New York, NY, USA, 2014. Association for Computing Machinery.

[3] H. Kobayashi, Y. Watanabe, and J. Shikata. Asymptotically tight lower bounds in anonymous broadcast encryption and authentication. In *Cryptography and Coding, IMACC 2021*, 2021. (To appear).

[4] Y. Watanabe, N. Yanai, and J. Shikata. Anonymous broadcast authentication for securely remote-controlling IoT devices. In L. Barolli, I. Woungang, and T. Enokido, editors, *AINA 2021*, pages 679–690, Cham, 2021. Springer International Publishing.

[*] 電気通信大学, 〒 182-8585 東京都調布市調布ヶ丘 1-5-1, The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo, 182-8585, Japan. watanabe@uec.ac.jp

[†] ジャパンデータコム株式会社, 〒 107-0052 東京都港区赤坂 2-23-1 アークヒルズフロントタワー RoP 1201, Japan Datacom Co., Ltd., Room 1201, Ark Hills Front Tower RoP, 2-23-1 Akasaka, Minato-ku, Tokyo, 107-0052, Japan.

[‡] 大阪大学, 〒 565-0871 吹田市山田丘 1-5, Osaka University, 1-5 Yamadaoka, Suita, Osaka, 565-0871, Japan. yanai@ist.osaka-u.ac.jp

[§] 横浜国立大学, 〒 240-8501 神奈川県横浜市保土ヶ谷区常盤台 79-7, Yokohama National University, 79-7 Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa, 240-8501, Japan. shikata-junji-rb@ynu.ac.jp