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

低リソースデバイス制御のための匿名放送型認証技術の提案
Practical anonymous broadcast authentification from DLP and lattices

青野　良範 *†　　四方　順司 ‡*
Yoshinori Aono　　Junji Shikata

キーワード 匿名放送型認証，Multi-receiver encryption, 離散対数問題，格子

あらまし

5G 以降の IoT ネットワークにおいて想定される，特定のエリア内に存在する複数台のデバイスに対してコマンドを一斉送信し制御するための匿名放送型認証（ABA）プロトコルを提案する．

主な要件定義 (1) 中央サーバからコマンドを送信し，指定した複数台の機器を同時に制御可能 (2) 通信路上のメッセージの改ざん耐性 (3) マルウェア感染などで複数の機器の情報が漏洩した場合でもコマンドが偽造不可能 (4) 各機器は自身がコマンドの対象であるかどうかを判断できるが，自分以外の機器が対象であるかどうかは判断できない．

以上 4 点の他，数値的な目標として $N = 10^6 \sim 10^7$ 台のデバイスを同時に制御できること，1 回のコマンドのサイズが小さく，デバイス側での処理をできる限り軽くすることなどが要件として与えられている．

構成の方針 匿名放送型認証においては，コマンドサイズの下界 $\Omega(N)$ が既に知られている [2]．これは，N 台のデバイスをランダムに指定した場合，コマンドのエントロピーが最低でも N [bit] となることから本質的なものであると考えられる．一方で，制御デバイスの指定が完全にランダムであることは実用上考えにくく，特定のメーカーの連続した番号等，ある程度の規則性を持った指定方法が使われると考えられる．そのため，K 個の ABA を直列に組み合わせ，全ての認証が通った場合にコマンドを実行するなどの単純な改良により，匿名性をある程度犠牲にしてコマンドサイズを $O(K \cdot N^{1/K})$ 程度に下げることができると期待される．

技術的な概要 まず，バーナム暗号ベースの Multi-receiver Encryption を構成する．この方式は自身以外のデバイスが受信する平文に関して情報理論的安全性を持つ．この方式を黒澤ら [3, Sect. 5] の方法により，繰り返し使用可能な ElGamal 暗号ベースの方式に変換したもの，および Ding[1] の LWE ベース鍵交換の方法により、格子ベースの方法を提案する．これらの ABA を直列に複数個組み合わせることで，低リソース環境での利用が期待される ABA を構成する．

* 横浜国立大学先端科学高等研究院, 〒 240-8501 神奈川県横浜市保土ケ谷区常盤台 79-5 Institute of Advanced Sciences, Yokohama National University 79-5 Tokiwadai, Hodogaya-ku, Yokohama 240-8501, Japan. aono-yoshinori-xf@ynu.ac.jp
† 情報通信研究機構 セキュリティ基盤研究室, 〒 184-8795 東京都小金井市貫井北町 4-2-1 NICT, 4-2-1, Nukui-Kitamachi, Koganei, Tokyo, Japan.
‡ 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 Graduate School of Environment and Information Sciences, Yokohama National University 79-7 Tokiwadai, Hodogaya-ku, Yokohama 240-8501, Japan

References

[1] Jintai Ding. “A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem”. In: *IACR Cryptol. ePrint Arch.* 2012/688 (2012).

[2] Yohei Watanabe Hirokazu Kobayashi and Junji Shikata. “Asymptotically Tight Lower Bounds in Anonymous Broadcast Encryption and Authentication”. In: *Cryptography and Coding - 18th IMA International Conference, IMACC 2021, Proceedings.*

[3] Kaoru Kurosawa et al. “Some Bounds and a Construction for Secure Broadcast Encryption”. In: *Advances in Cryptology - ASIACRYPT ’98*. Ed. by Kazuo Ohta and Dingyi Pei. Vol. 1514. Lecture Notes in Computer Science. Springer, 1998, pp. 420–433.