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

匿名放送型暗号及び認証における非漸近的タイトな下界と最適構成法について
Non-Asymptotically Tight Lower Bounds and Optimal Constructions of Anonymous Broadcast Encryption and Authentication

小林 大航 * 渡邉 洋平 † 峯松 一彦 ‡* 四方 順司 *
Hirokazu Kobayashi Yohei Watanabe Kazuhiko Minematsu Junji Shikata

キーワード 放送型暗号, 匿名性, 下界

あらまし

放送型暗号（Broadcast Encryption; BE）は, 送信者が平文を暗号化するとき, 復号権限を付与する受信者を複数人指定できる方式である. BE に望まれる安全性の一つとして匿名性が考えられており, 匿名性を満たす BE（匿名 BE）は復号権限をもつ受信者の情報を秘匿する. Kobayashi ら（IMACC 2021）は匿名 BE における暗号文長の漸近的にタイトな下界を示している. 本稿では, その結果を拡張し, 匿名 BE における暗号文長の非漸近的にタイトな下界を示すと同時に, Li と Gong（ACNS 2018）による匿名 BE 方式の変形版が最適な構成法であることを示す. また, 同様な解析を匿名放送型認証（ABA）に適用することで, ABA における認証子サイズの非漸近的にタイトな下界を示すと同時に, ABA の最適な構成法を提案する.

* 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. kobayashi-hirokazu-dr@ynu.jp, shikata-junji-rb@ynu.ac.jp, minematsu-kazuhiko-bk@ynu.ac.jp
† 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
‡ NEC セキュアシステム研究所, 〒 211-8666 神奈川県川崎市下沼部 1753, NEC Corporation, 1753 Shimonumabe, Kawasaki, Kanagawa, 211-8666, Japan.