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

復号制御付 ID ベース暗号の安全性に関する考察
Security notions of decryption-controllable identity-based encryption

宮永 英和 * 藤岡 淳 † 佐々木 太良 † 岡野 裕樹 ‡
Hidekazu MIYANAGA Atsushi FUJIOKA Taroh SASAKI Yuki OKANO
永井 彰 ‡ 鈴木 幸太郎 § 米山 一樹 ¶
Akira NAGAI Koutarou SUZUKI Kazuki YONEYAMA

キーワード ID ベース暗号，複数デバイス，復号制御

あらまし

近年，1 人のユーザがコンピュータ・スマートフォンなど複数のデバイスを所持する機会が増えており,ID ベース暗号でも 1 つの ID で複数のデバイスで復号などを行うことを考える必要があることから，SCIS2021 においてデバイスの追加・取消が可能な ID ベース暗号である復号制御付 ID ベース暗号とこれらの利用状況に対応した安全性を一つ定義した [1]. また，ISEC2021 (11 月) において選択的安全性と適応的安全性を考慮し新たに 3 つの安全性を定義し，これらの安全性について強弱関係の一部を証明した [2]．本稿では ISEC2021 (11 月) で示していない残りの強弱関係を証明し，定義した 4 つの安全性定義の強弱関係を示す.

復号機能付 IBE の安全性定義には，公開パラメータ pp を受け取る前に攻撃対象を予め宣言する選択的安全性と，pp を受け取った後に攻撃対象を後から自由に選択できる適応的安全性がある．すなわち，受信者の ID 情報である ID と指定期間 T について選択的安全性 (**S**elective secure) ，適応的安全性 (**A**daptive secure) を考慮すると，以下の 4 つである [2].

1. IND-aIDaT-CCA 安全 $\cdots$ 攻撃者は pp を受け取った後に ID^*, T^* を宣言する
2. IND-aIDsT-CCA 安全 $\cdots$ 攻撃者は pp を受け取る前に T^* を宣言し，受け取った後に ID^* を宣言する
3. IND-sIDaT-CCA 安全 $\cdots$ 攻撃者は pp を受け取る前に ID^* を宣言し，受け取った後に T^* を宣言する
4. IND-sIDsT-CCA 安全 $\cdots$ 攻撃者は pp を受け取る前に ID^*,T^* を宣言する

安全性定義の強弱関係を示すためにはそれぞれの安全性に対して帰着関係と分離関係を示せばよく，自明な関係については，ISEC2021 (11 月) で報告した．本稿では，IND-aIDsT-CCA 安全と IND-sIDaT-CCA 安全の強弱関係について述べ，IND-aIDsT-CCA 安全と IND-sIDaT-CCA 安全では双方向で分離関係が成り立つことを示す.

参考文献

[1] 宮永英和, 藤岡淳, 佐々木太良, 岡野裕樹, 永井彰, 米山一樹. 複数デバイスでの ID ベース暗号の利用に関する考察. 2021 年暗号と情報セキュリティシンポジウム予稿集 (SCIS2021), 3B1-3, 2021.

[2] 宮永英和, 藤岡淳, 佐々木太良, 岡野裕樹, 鈴木幸太郎, 米山一樹. 復号制御付 ID ベース暗号の安全性に関する考察. 信学技報, ISEC2021-43, 2021.

* 神奈川大学大学院，221-8686 神奈川県横浜市神奈川区六角橋 3-27-1, Kanagawa University Graduate School, 3-27-1, Rokkakubashi, Kanagawa-ku, Yokohama, Kanagawa, Japan (r202170162ui@jindai.jp)
† 神奈川大学, 221-8686 神奈川県横浜市神奈川区六角橋 3-27-1, Kanagawa University, 3-27-1, Rokkakubashi, Kanagawa-ku, Yokohama, Kanagawa, Japan ({fujioka,taroh}@kanagawa-u.ac.jp)
‡ NTT 社会情報研究所，180-8585 東京都武蔵野市緑町 3-9-11, NTT Social Informatics Laboratories, 3-9-11, Midoricho, Musashino-shi, Tokyo 180-8585, Japan ({yuki.okano.te,akira.nagai.td}@hco.ntt.co.jp)
§ 豊橋技術科学大学，441-8580 愛知県豊橋市天伯町雲雀ヶ丘 1-1, Toyohashi University of Technology, 1-1, Hibarigaoka, Tenpaku-cho, Toyohashi-shi, Aichi 441-8580, Japan (suzuki@cs.tut.ac.jp)
¶ 茨城大学, 316-8511 茨城県日立市中成沢町 4-12-1, Ibaraki University, 4-12-1, Nakanarusawa-cho, Hitachi-shi, Ibaraki 316-8511, Japan (kazuki.yoneyama.sec@vc.ibaraki.ac.jp)