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

複数の鍵生成局を持つ鍵失効機能付き ID ベース暗号
Revocable Identity-Based Encryption With Multiple Private Key Generators

鈴木 裕大 * 藤岡 淳 * 佐々木 太良 * 岡野 裕樹 † 永井 彰 †
Yudai Suzuki Atushi Fujioka Taroh Sasaki Yuki Okano Akira Nagai

キーワード 複数鍵生成局，ID ベース暗号，鍵失効機能 適応的安全性，選択的安全性

1 あらまし

昨今，公開鍵暗号のうち ID ベース暗号 (Identity-Based Encryption: IBE) の研究が盛んに行われている．IBE とは，メールアドレスなど自分だけが持っている個人特有の文字列 (ID) を用いて公開鍵を作成する暗号のことである．この暗号では個人の識別子から公開鍵と秘密鍵を生成する PKG (Private Key Generator: 鍵生成局) といわれる第三者機関が必要となる．この方式を用いることで，中間者攻撃を回避できる．しかし既存の IBE には，PKG が１つしかないことにより，全てのユーザが同じ PKG を利用しなければならないという問題がある．この問題を解決する方法として PKG を複数用意し，各ユーザが利用する PKG を選択するという方法が提案されている [1].

また，複号に利用する秘密鍵が漏洩したときに鍵を無効にする方法が無いという問題もある．この問題については鍵失効機能付き ID ベース暗号 (RIBE: Revocable Identity-Based Encryption) というものがある [2].

本研究では，

研究内容 1 複数の鍵生成局を持つ RIBE の方式を提案

研究内容 2 複数の鍵生成局を持つ RIBE についての安全性を定義

研究内容 3 提案した方式が定義した安全性を満たすことを証明

を行うことで，上記２つの問題点を同時に解決する RIBE について考察する．

研究内容 1 では，PKG が 1 つの RIBE の暗号化にユーザに ID を用いていたのに対し，PKG を複数利用するにあたり，各 PKG に対して固有の識別子 pid を付与し，個人の識別子 ID と共に暗号化などに用いることで複数の鍵生成局を持つ RIBE を提案する．

研究内容 2 では，PKG が 1 つの RIBE の安全性で選択的 ID を用いていた安全性定義に対して選択的 PID と適応的 PID のそれぞれを加えた．また同様に，PKG が１つの RIBE の安全性で適応的 ID を用いていた安全性定義に対して選択的 PID と適応的 PID のそれぞれを加えた．

研究内容 3 では，PKG が１つの RIBE が ID に選択的 ID 安全性を満たすならば，研究内容 1 で提案した PKG が複数の RIBE が選択的 ID 安全性を満たし，かつ選択的 pid 安全性ないし，適応的 pid 安全性を満たすことを証明する．また，適応的 ID 安全性を満たす場合も同様に選択的 pid 安全性ないし，適応的 pid 安全性を満たすことを証明する．

* 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-shi, Kanagawa 221–8686, Japan ({r201704247ie,fujioka,taroh}@jindai.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 Midori-cho, Musashino-shi, Tokyo 180–8585 Japan ({yuki.okano.te,akira.nagai.td}@hco.ntt.co.jp)

参考文献

[1] A. Fujioka and K. Yoneyama. Single Private-Key Generator Security Implies Multiple Private-Key Generators Security. ProvSec 2018, LNCS Vol. 11192 pp. 56–74. Springer, 2018.

[2] J. H. Seo and K. Emura. Revocable Identity-Based Encryption Revisited: Security Model And Construction. PKC2013, LNCS Vol. 7778 pp. 216–234. Springer, 2013.