6-5　鍵失効機能付き ID ベース暗号

江村恵太

ID ベース暗号（Identity-Based Encryption: IBE）とは、任意の値を公開鍵に設定可能な公開鍵暗号であり、メールアドレスや機器番号などを公開鍵として利用することで公開鍵証明書の検証コストを削減できることから、新世代ネットワークでの応用などが期待されている。本稿では、特に秘密鍵を失効する機能を持つ鍵失効機能付き ID ベース暗号（Revocable IBE: RIBE）について、筆者が提案した方式を紹介する。筆者は、既存方式（Boldyreva, Goyal, and Kumar, ACM CCS 2008）では考慮されていなかった新たな安全性である復号鍵漏洩耐性（Decryption key exposure resilient）を持つ方式を提案するとともに、既存方式に対する攻撃を示した。また、階層型 RIBE への拡張及び一度削除された秘密鍵に紐付いた ID に対して秘密鍵を再発行可能な方式、検索可能暗号への応用についても紹介する。

1　はじめに

ID ベース暗号とは、任意の値を公開鍵に設定可能な公開鍵暗号である。通常の公開鍵暗号では、公開鍵がランダムな値であるため公開鍵検証基盤による公開鍵証明書が必要となる一方、ID ベース暗号ではメールアドレスや名前などの Identity を公開鍵（以下 ID と表記）とすることが可能であり、そのため公開鍵証明書のコストを削減することができる。ID ベース暗号では、鍵生成センタ（Key Generation Center, KGC）が ID に対する秘密鍵を発行、この秘密鍵を用いることで ID を公開鍵として作成された暗号文を復号する。

Boneh と Franklin[1] により、初めての ID ベース暗号方式が提案された。この Boneh と Franklin は、期間 T における非失効ユーザにのみ、ID‖T を新たな ID とみなして秘密鍵を再発行することで、鍵失効機能を実現した方式も紹介した。この方式では、暗号化時に期間 T を付加した ID を公開鍵とすることで、期間 T における秘密鍵を持たないユーザをシステムから削除することができる。しかしながら、期間ごとに KGC が（N-R）個（N: 全ユーザ数、R: 削除ユーザ数）の秘密鍵を発行する必要があるため、スケーラビリティの面で問題があるといえる。この問題を解決するため、Boldyreva ら [2] は KGC の計算コストが期間ごとに O（Rlog（N/R））である鍵失効機能付き ID ベース暗号（Revocable IBE, RIBE）を提案した。図 1 に RIBE の簡単な流れを説明する。各ユーザは通常の ID ベース暗号と同様に（long-term）秘密鍵 sk_{ID} を KGC から発行される。暗号化の際には公開鍵となる ID に加え、期間 T も指定する。KGC は各期間 T において、鍵更新用の情報 ku_T を Broadcast する。期間 T で削除されていないユーザのみ、sk_{ID} と ku_T から復号鍵 $dk_{ID,T}$ を計算することができる。各ユーザは木構造の葉にそれぞれ割り当てられ、放送暗号（Broadcast Encryption）フレームワークのひとつである Complete Subtree（CS）法 [3] を利用することで、ku_T のサイズが人数の log オーダに抑えられる。

2　復号鍵漏洩耐性

筆者は文献 [4][5] にて、Boldyreva らの安全性定義が Boneh-Franklin 方式では達成されていた安全性である復号鍵漏洩耐性（Decryption key exposure resilient）をとらえていないことに着目した。本章では、この復号鍵漏洩耐性について紹介する。なお Boneh-Franklin の論文では、この復号鍵漏洩耐性について言及していないことを明記しておく。

通常の ID ベース暗号の安全性モデルでは、攻撃者はチャレンジ Identity と呼ばれる値（以下 ID* と表記）

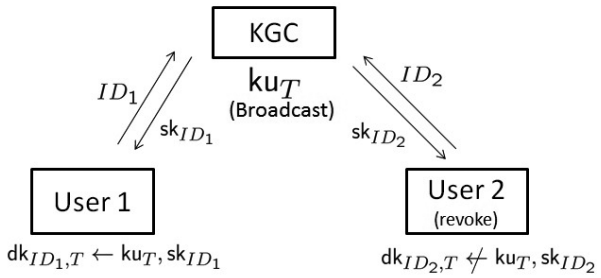

図 1　鍵失効機能付き ID ベース暗号の枠組み

を選択し、その ID* を公開鍵とした暗号文から平文に関する情報を得られないことが要求される。また、攻撃者は ID* 以外の ID に対して秘密鍵の取得を許される。RIBE においては、ID* に加えてチャレンジ期間（以下 T* と表記）も攻撃者が指定し、T* において ID* を公開鍵とした暗号文から平文に関する情報を得られないことが要求される。このとき攻撃者は ID* に対する秘密鍵 sk_{ID^*} を取得しない、または sk_{ID^*} を取得した場合は T* において ID* を削除することが要求される。ここで Boldyreva らの安全性定義では、攻撃者は $dk_{ID,T}$ (ID,T) ≠ (ID*,T*) を取得することは許されない。

筆者は、Boneh-Franklin 方式では攻撃者に $dk_{ID,T}$ (ID,T) ≠ (ID*,T*) を与えたとしても安全である一方、Boldyreva らの方式では ID* に対する秘密鍵 sk_{ID^*} が $dk_{ID^*,T}$（T ≠ T*）から漏洩するため安全とはならないことを示した。また、Boneh-Franklin 方式はスケーラビリティを満たさないため、初めてスケーラブルな RIBE 方式で復号鍵漏洩耐性を持つ方式も提案した。Boldyreva らの方式では、$dk_{ID,T}$ に sk_{ID} の一部がそのまま含まれていたため、$dk_{ID^*,T}$（T ≠ T*）から sk_{ID^*} が漏洩していた。筆者は復号鍵計算時に再ランダム化を行うことにより、ku_T と $dk_{ID,T}$ から sk_{ID} が漏洩しないように工夫することで、復号鍵漏洩耐性を持たせている。詳細は文献 [4][5] を参照されたい。

次に PBC ライブラリ [6] を用いて実装した結果を図 2 に示す。Revoke は削除するユーザの ID とその付加情報を削除リストに掲載するアルゴリズム、KeyUp は削除リストに掲載されたユーザ以外のユーザが復号鍵を作成できるように ku_T を計算するアルゴリズム、DKG は sk_{ID} と ku_T から復号鍵 $dk_{ID,T}$ を計算するアルゴリズムである。

削除ユーザの情報を単純に削除リストに掲載するアルゴリズムである Revoke の計算時間は削除数 R に比例して増大していくものの、その計算コストは非常に小さい。KeyUp アルゴリズムの計算は kuT のサイズ O(Rlog（N/R)) に応じて増大していくが、KGC が期間 T において一度だけ行えばよいため、実用的な範囲に収まっているといえる。ユーザが実行する必要がある DKG アルゴリズムは削除メンバ数 R に依存せず、非常に効率的に実行可能であるといえる。

N	100000	100000	100000	100000
R	0	100	1000	10000
Revoke	-	0.00004	0.00044	0.00774
KeyUp	0.00620	5.84936	39.36161	267.76918
DKG	0.00853	0.00851	0.00859	0.00905

図 2　実装結果（単位：秒）[4]

3　その他の方式

本章では、階層型 RIBE への拡張、一度削除された秘密鍵に紐付いた ID に対して秘密鍵を再発行可能な方式、RIBE の検索可能暗号への応用について紹介する。詳細は各論文を参照されたい。

ID ベース暗号では、KGC が各ユーザに秘密鍵を発行するという一階層の構造を持っている。この構造を多階層に拡張したのが階層型 ID ベース暗号である。階層は木構造で表現され、親ノードのユーザが子ノードのユーザに対して KGC の枠割を果たす。筆者は、この階層型 ID ベース論文に鍵失効機能を付加した鍵失効可能階層型 ID ベース暗号を構成した [7][8][10]–[13]。

通常の RIBE では一度鍵が失効されたユーザの再追加は考慮されていない。そのため鍵が失効された後、別の ID を用いる必要があった。しかしながら、ID として指紋や光彩などの生体情報を用いる場合、その変更は困難であり、そのため同じ ID が使用可能であることが望ましい。筆者は、一度削除された秘密鍵に紐付いた ID に対して秘密鍵を再発行可能な方式を提案した [9]。この方式では ID に加えてタグ情報を用いるため、同じ ID でも異なるタグであれば、あたかも異なる ID として鍵の発行が可能となる。なお同方式内では、タグとしてユーザが配置される木構造の葉ノード名を使用している。

また、ID ベース暗号から検索可能暗号が構成できることが知られており、暗号化されたキーワードを検索者が生成したトラップドアを用いて検索する。筆者は、RIBE の知見を活かし、このトラップドアの失効及び同じキーワードに対するトラップドアの再生成が可能な検索可能暗号を提案した [14]。

4　おわりに

本稿では、鍵失効機能を持つ ID ベース暗号について紹介した。ID ベース暗号は、それ自体の機能の有用性に加え、様々な暗号方式を構成する際の部品となることも知られている。そのため、ID ベース暗号における鍵失効機能が、別の暗号方式において有用な機能を実現することも期待される。例えば [14] で提案したように、ID ベース暗号から構成される検索可能暗号に対し、基礎部品となる ID ベース暗号に鍵失効機能を付加することで、検索可能暗号においてもキーワード検索用のトラップドアを失効する機能が付加される。このように、鍵失効機能で得た知見を他の暗号方式に転用することも今後の展開として考えている。また、特に階層型の方式については、更なる効率改善の必要性があり、引き続きこれらの課題の解決に取り

組む所存である。

【参考文献】

1 Dan Boneh and Matthew K. Franklin, “Identity-Based Encryption from the Weil Pairing,” SIAM J. Comput. 32(3), pp.586–615, 2003.
2 Alexandra Boldyreva, Vipul Goyal, and Virendra Kumar, “Identity-based encryption with efficient revocation,” ACM Conference on Computer and Communications Security 2008, pp.417–426, 2008.
3 Dalit Naor, Moni Naor, and Jeffery Lotspiech, “Revocation and Tracing Schemes for Stateless Receivers,” CRYPTO 2001, pp.41–62, 2001.
4 Jae Hong Seo and Keita Emura, “Revocable Identity-Based Cryptosystem Revisited: Security Models and Constructions,” IEEE Trans. Information Forensics and Security 9(7), pp.1193–1205, 2014.
5 Jae Hong Seo and Keita Emura, “Revocable Identity-Based Encryption Revisited: Security Model and Construction,” Public Key Cryptography 2013, pp.216–234, 2013.
6 The PBC (pairing-based cryptography) library, available at http://crypto.stanford.edu/pbc/.
7 Jae Hong Seo and Keita Emura, “Revocable hierarchical identity-based encryption,” Theor. Comput. Sci. 542, pp.44–62, 2014.
8 Jae Hong Seo and Keita Emura, “Efficient Delegation of Key Generation and Revocation Functionalities in Identity-Based Encryption,” CT-RSA 2013, pp.343–358, 2013.
9 Jae Hong Seo and Keita Emura, “Revocable Identity-Based Encryption with Rejoin Functionality,” IEICE Transactions 97-A(8), pp.1806–1809, 2014.
10 Jae Hong Seo and Keita Emura, “Revocable hierarchical identity-based encryption via history-free approach,” Theor. Comput. Sci. 615, pp.45–60, 2016.
11 Jae Hong Seo and Keita Emura, “Revocable Hierarchical Identity-Based Encryption: History-Free Update, Security Against Insiders, and Short Ciphertexts,” CT-RSA 2015, pp.106–123, 2015.
12 Keita Emura, Jae Hong Seo, and Taek-Young Youn, “Semi-Generic Transformation of Revocable Hierarchical Identity-Based Encryption and Its DBDH Instantiation,” IEICE Transactions 99-A(1), pp.83–91, 2016.
13 Jae Hong Seo and Keita Emura, “Adaptive-ID Secure Revocable Hierarchical Identity-Based Encryption,” IWSEC 2015, pp.21–38, 2015.
14 Keita Emura, Le Trieu Phong, and Yohei Watanabe, “Keyword Revocable Searchable Encryption with Trapdoor Exposure Resistance and Re-generateability,” TrustCom 2015, pp.167–174, 2015.

江村恵太　（えむら　けいた）

サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士（情報科学）
暗号理論