効率的な時間特定暗号とその拡張
Efficient Time-Specific Encryption and Its Extension

電気電子情報通信工学専攻 笠松　宏平
Kohei KASAMATSU

1　暗号技術について

信頼できないネットワークを安全に使うために, 通信内容の機密性の確保や改ざんの防止は必要不可欠である. 暗号技術はその安全なネットワークの実現の中心的な役割を果たす. 本研究ではその暗号技術の一つである公開鍵暗号 (Public Key Encryption) を扱う. この公開鍵暗号は事前の秘密情報の共有なしに安全な通信を行うことを可能にする技術であり, 実社会で使用されている SSL などのプロトコルの根幹を支える技術である.

しかし, この公開鍵暗号では受信者の公開鍵と秘密鍵が正当なものである保障が必要である. 通常, その保障をするためには公開鍵基盤 (Public Key Infrastructure) と呼ばれる信頼できる機関が使われるが, その仕組みの維持には大きな負担がかかる. その負荷を軽減するために, ID ベース暗号 (Identity-Based Encryption) [11, 4] が提案された. この方式は, すでに公に信頼されている情報 (例えば, メールアドレスがそれにあたる) を公開鍵として用いることにより, 鍵管理の負担を軽減することができる. 多くの研究者が (その鍵管理の負担を軽減できる) ID ベース暗号の強力な機能に着目し, その方式を応用した様々な機能付き暗号方式を提案している. 本稿ではその機能付き暗号方式の一つである時間特定暗号 (Time-Specific Encryption) の効率的な構成法およびその時間特定暗号の拡張方式を提案する.

2　本研究の背景と動機

本研究の動機である時間特定暗号 (Time-Specific Encryption) の効率的な構成の必要性およびその拡張方式の有用性について述べる.

時間特定暗号の効率的な構成の必要性.　SCN 2010 において, Paterson と Quaglia [10] は時間特定暗号の概念を示した. 時間特定暗号は受信者が復号できる時間期間を指定できる機能を持つ公開鍵暗号の一種である. この時間特定暗号が使われる典型的なシナリオでは, 時報局と呼ばれる信頼できる第三者機関がシステムパラメータと周期的に暗号文を復号するために使われる時刻鍵を配信する. 時間特定暗号において, 送信者はメッセージ M を暗号化する時に, 復号可能期間と呼ばれる任意の時間期間 $[t_L, t_R]$ を指定する. ただし, t_L は開始時刻, t_R は終了時刻を示す. そして, もし $t \in [t_L, t_R]$ を満たすある時刻 t に対する時刻鍵 SK_t を持つならば, 受信者は復号可能期間 $[t_L, t_R]$ の暗号文を復号できる. このシナリオからもわかるように, この機能によって, システム設計者はある時間期間内のみ情報やコンテンツを提供するシステムを効率的に実現できる. そのシステムの例としては電子オークションやプレスリリースシステムがある.

さらに, Paterson と Quaglia [10] は 2 つの洗練された時間特定暗号の構成法を提案した. 1 つ目は既存の ID ベース暗号 [11, 4] を用いた時間特定暗号の一般的構成法であり, 2 つ目は放送型暗号 (Broadcast Encryption, BE) [7, 5] を用いた時間特定暗号の一般的構成法である. (一般的構成法とは既存の暗号方式を構成要素として用いて, 別の暗号方式を構成する手法である.) しかしながら, この一般的構成法により構成された時間特定暗号はあるデータサイズ (そして計算コスト) が公開パラメータの寿命 T[1]に対して線形に増加するという意味で非効率である. より詳細には, ID ベース暗号を用いた一般的構成法により得られる時間特定暗号の暗号文サイズは T に対して線形に増加し, 放送型暗号を用いた一般的構成により得られる方式の公開パラメータサイズも T に対して線形に増加する. 一般的に, T は大きい値であるため, その非効率さは時間特定暗号の導入の障害になる可能性がある. したがって, その既存の構成法にはまだ改善の余地が残されている. 本研究ではその非効率さを改善する新しい時間特定暗号の構成法を提案する.

本稿で提案する拡張方式の有用性. 私たちの周りにはある値が指定された範囲内であるかどうかによってアクセス制御をする場面が多く存在する. 例えば, 年齢制限や有効期限の確認はその一例である. 時間の代わりに年齢やカードの発行日を秘密鍵に関連付けることによって, 時間特定暗号はそのようなアクセス制御を効率的に実現できる. しかし, 年齢制限や有効期限の確認を組み合わせるような柔軟な制御を行う場合, 時間特定暗号の機能では不十分である.

本研究ではそのような複数の範囲を復号条件として指定できる時間特定暗号の拡張方式を提案する. この新しい暗号方式を暗号文ポリシー閾値多次元範囲暗号 (Ciphertext-Policy Threshold Multi-Dimensional Range Encryption) と名付け, 以降, 簡略化のために, その方式を範囲暗号と呼ぶ. この方式は次のようにして, 複数の範囲を組み合わせたアクセス制御を行うことができる. 範囲暗号において, ユーザの属性情報は多次元空間における点 $(p_1, p_2, \ldots)$ として表現され, ある信頼できる機関がその点とサービスもしくはユーザごとに決められた閾値に対応した秘密鍵をユーザに配布する. 送信者は復号が許される属性情報の範囲 $([x_1, y_1], [x_2, y_2], \ldots)$ を指定し, その範囲に対応した暗号文を生成する. この範囲指定により, 暗号文の復号条件を指定された範囲内である点の座標の数が閾値以上である秘密鍵を所有することとできる.

3 本研究の貢献

本研究ではフォワード安全暗号 (Forward-Secure Encryption, FSE) を用いた時間特定暗号の新しい構成法を提案する. この提案方式はフォワード安全暗号の機能は時間特定暗号の機能と類似していることに基づいている. 実際に, フォワード安全暗号を直接用いることによって $t_L = 0$ を満たす制限された復号可能期間 $[t_L, t_R]$ のみを許す時間特定暗号を得ることができる. この考察に基づき, 本稿では 2 つの具体的な時間特定暗号方式とフォワード安全暗号を用いた時間特定暗号の一般的構成法を提案する.

[1] より詳細には, T はシステムが公開パラメータ (これはシステム利用者全員が共通して使用する値である) の設定時に指定される値である, この公開パラメータは T 個の時間期間に分割された寿命を持つ. そのとき, 利用者は 0 から $T-1$ までの時刻を指定することができる.

1. Boneh, Boyen, Goh の階層型 ID ベース暗号 [3] (hierarchical identity-based encryption by Boneh, Boyen, Goh, BBG-HIBE) によって得られる既存の FSE (BBG-FSE) [2]を用いた具体的な時間特定暗号方式.

2. Boneh, Boyen の HIBE [1] (HIBE by Boneh, Boyen, BB-HIBE) によって得られる既存の FSE (BB-FSE) [3]を用いた具体的な時間特定暗号方式.

3. 任意のフォワード安全暗号を用いた時間特定暗号の一般的構成法.

この BBG-FSE に基づく時間特定暗号, BB-FSE に基づく時間特定暗号, そして本稿の一般的構成により得られるいくつかの時間特定暗号は既存の方式と比べて, 全てのデータサイズと計算コストが高々公開パラメータの寿命 T に対して対数多項式である点で効率的である. ゆえに, 提案方式は既存方式のある種の非効率さを改善している. さらに, 3 つの提案方式はそれぞれ優れた点を持つ. BBG-FSE に基づく時間特定暗号は著者が知る本稿の一般的構成を用いて得られる時間特定暗号方式を含む他の提案方式の中で最も効率的である. BB-FSE に基づく時間特定暗号は BBG-FSE に基づく時間特定暗号よりも標準的な仮定の下で安全性が保障できる点で優れている. 本稿の一般的構成法は任意の FSE から時間特定暗号を構成できる点で 2 つの提案方式よりも優れている. つまり, 新しい FSE が提案された時, この一般的構成により自動的に新しい時間特定暗号を構成でき, その時に得られる方式は BBG-FSE に基づく時間特定暗号よりも効率的である可能性がある.

さらに, 本研究では 2 章で述べた時間特定暗号の拡張方式である範囲暗号の概念およびその範囲暗号の 2 つの効率的な構成法を提案する. それらは, 上記で説明した BBG-FSE に基づく時間特定暗号, BB-FSE に基づく時間特定暗号を構成部品とした, 具体的な範囲暗号方式である. 既存方式を用いることによって, 復号条件である閾値の機能を制限した範囲暗号を構成することができるが, 提案方式はその既存方式より得られる範囲暗号よりも公開パラメータおよび暗号文サイズの面で効率的である. さらに, 2 つの提案方式はそれぞれ優れた点を持つ. BBG-FSE に基づく時間特定暗号により得られる範囲暗号は効率性の面で BB-FSE に基づく時間特定暗号により得られる範囲暗号に比べて優れている. 一方で, 安全性の面では, BB-FSE に基づく時間特定暗号により得られる範囲暗号の方が優れている. 2 つの提案方式は同じ設計思想の下で構成されているため, この性能と安全性のトレードオフは構成部品である BBG-FSE に基づく時間特定暗号と BB-FSE に基づく時間特定暗号の関係と同じであるといえる.

4 結論

高度な機能と安全性を両立できる暗号技術の一つである時間特定暗号に関して, 本研究ではフォワード安全暗号を用いた 3 つの効率的な構成法を提案した. 提案方式は全てのデータサイズと計算コストが高々公開パラメータの寿命 T に対して対数多項式である点で, 既存方式よりも効率的である. さらに, 時間特定暗号の機能を拡張した範囲暗号方式の概念とその効率的な構成法についても提案した.

---

[2] この FSE は BBG-HIBE に Canetti, Halevi, and Katz [6] のテクニックを用いることによって構成される.

[3] BBG-FSE と同様に, この FSE は BB-HIBE に [6] のテクニックを用いることによって構成される.

今後の課題は安全性の向上およびより柔軟な復号条件の実現である．範囲暗号の安全性モデルには selective と adaptive の 2 種類の定義があり．本稿では selective モデルを扱った．しかし, 攻撃者にとって有利な状況を与えても安全性を担保できる意味で, adaptive モデルの方が望ましい定義である．ゆえに, adaptive 安全性を持つ範囲暗号の構成が望まれる．また, 本研究では範囲暗号の復号条件として範囲に対する閾値機能を実現したが, より高度な論理演算 (論理和や論理積の組み合わせ等) を実現することは範囲暗号を適用可能な領域を広げる意味で有益である．

参考文献

[1] D. Boneh and X. Boyen. Efficient Selective Identity-Based Encryption Without Random Oracles. *Eurocrypt'04*, LNCS, vol. 3027, pp. 223-238, 2004.

[2] D. Boneh, X. Boyen, and E.J. Goh. Hierarchical identity based encryption with constant size ciphertext. *In Eurocrypt'05*, pages 440–456, 2005.

[3] D. Boneh, X. Boyen, and E.J. Goh. Hierarchical identity based encryption with constant size ciphertext. Full version of [2]. Cryptology ePrint Archive: Report 2005/015 (2005).

[4] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. *In Crypto'01*, LNCS, vol. 2139, pages 213–229, 2001.

[5] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. *In Crypto'05*, LNCS, vol. 3621, pages 258–275, 2005.

[6] R. Canetti, S. Halevi, and J. Katz. A forward-secure public-key encryption scheme. *In Eurocrypt'03*, LNCS, vol. 2656, pages 646–646, 2003.

[7] A. Fiat and M. Naor. Broadcast encryption. *In Crypto'93*, LNCS, vol. 773, pages 480–491, 1994.

[8] C. Gentry. Practical identity-based encryption without random oracles. *In Eurocrypt'06*, LNCS, vol. 4004, pages 445–464, 2006.

[9] C. Gentry and B. Waters. Adaptive security in broadcast encryption systems (with short ciphertexts). *In Eurocrypt'09*,LNCS, vol. 5479, pages 171–188, 2009.

[10] K. Paterson and E. Quaglia. Time-specific encryption. *In SCN'10*, LNCS, vol. 6280, pages 1–16, 2010.

[11] A. Shamir. Identity-based cryptosystems and signature schemes. *In Crypto'84*, LNCS, vol. 196, pages 47–53, 1985.

[12] B. Waters. Efficient identity-based encryption without random oracles. *In Eurocrypt'05*, LNCS, vol. 3494, pages 557–557, 2005.

[13] B. Waters. Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions. *In Crypto'09*, LNCS, vol. 5677, pages 619–636, 2009.