鍵更新可能な属性ベース暗号及びその応用に関する研究

A Study on Attribute-Based Encryption with Attribute Update and Its Applications

電気電子情報通信工学専攻 久野 真太郎
shintaro kuno

1 序論

近年, 生活をする上でなくてはならない存在になりつつあるインターネットには多くの脅威が存在する. 例えば, 情報を送る途中で第三者に盗聴されたり, 情報を改竄されたりといった恐れがある. これらの脅威を防ぐ方法の一つとして, 暗号技術が用いられる.

暗号技術のひとつに属性ベース暗号 (Attribute-Based Encryption : ABE)[2, 4] という暗号がある. 属性ベース暗号は暗号化された情報 (暗号文) を復号できる受信者の集合を細かく設定することができる. 復号を許可する受信者の条件は, 受信者を表す属性のもと木構造で表される. この木構造をアクセスポリシーと呼び, このアクセスポリシーを復号するための情報 (復号鍵) とする属性ベース暗号を鍵ポリシー属性ベース暗号 (Key-Policy Attribute Based Encryption : KP-ABE), 暗号化するための情報 (暗号化鍵) とする属性ベース暗号を暗号文ポリシー属性ベース暗号 (Ciphertext-Policy Attribute Based Encryption : CP-ABE) という.

属性ベース暗号の復号鍵は, 鍵生成局と呼ばれる信頼できる第三者機関に発行してもらわなければならない. そのため, 復号鍵の情報を変更したい場合はその都度毎回鍵生成局に復号鍵の発行を依頼する.

本研究では, 鍵生成局を介さず鍵更新可能な属性ベース暗号の提案, 及びその応用を提案する. 一つ目の研究では, 既存の属性ベース暗号をもとに復号鍵のアクセスポリシーや属性の集合といった情報を鍵生成局への依頼なしに追加可能な属性ベース暗号を提案する. 二つ目の研究では, 位置情報ベース暗号という新たな概念を提案し, このモデルを満たすサイズ効率のよい方式を提案する. この提案方式は, 属性ベース暗号に鍵の更新機能を持たせる方式について研究した際に得られた知見によって, 構成することに成功した.

1.1 動的な属性情報更新機能を持つ属性ベース暗号

既存の属性ベース暗号では, 一度発行された復号鍵の情報を変更したい場合, 毎回鍵生成局に復号鍵の発行を依頼する. そのため, 属性ベース暗号では時間や場所といった動的に変化する属性を扱うことができない. 本研究では, 復号鍵に含まれるアクセスポリシー, または属性の集合といった情報を変更可能な属性ベース暗号を提案する. 提案方式では, 利用者が初めから持っている復号鍵に対し, 更新鍵と呼ばれる属性を更新するための鍵を組み合わせることにより, 鍵生成局なしに属性の情報の更新を可能にする. この更新鍵は更新鍵を管理している端末にアクセスすることで配布される. 復号鍵に対し随時更新鍵を変更することで, 一部のアクセスポリシーや属性の集合といった情報を変更することができるようになり, 時間や場所といった動的に変化する属性も扱うことができるようになる.

本論文内では, 鍵ポリシー属性ベース暗号と暗号文ポリシー属性ベース暗号のそれぞれに対し, 動的な属性情報更新機能を持つ方式

を提案する. また, それぞれの動的な属性情報更新機能を持つ属性ベース暗号に対する安全性モデル提案する. そして, 動的な属性情報更新機能を持つ鍵ポリシー属性ベース暗号の提案方式を Decisional Bilinear Diffie-Hellman (DBDH) 仮定のもと, 動的な属性情報更新機能を持つ暗号文ポリシー属性ベース暗号の提案方式を Decisional Parallel Bilinear Diffie-Hellman Exponent (DPBDHE) 仮定のもと, 安全であることを証明する.

1.2 位置情報ベース暗号

近年, スマートフォンなどの携帯端末の普及により屋外でインターネットを利用するユーザが増え, 位置情報に応じた情報を提供するサービスが盛んになっている. もし, ある場所から任意の半径以内にいるユーザのみがデータファイルを復号できるといった暗号が存在すれば, 位置情報を利用したサービスをより効率的に行うことが可能となる. 上記のような暗号は既存の暗号を用いて実現することが可能である. しかし, これらの暗号方式を利用し実現した場合, マップの面積に比例して公開パラメータや復号鍵, 暗号文のサイズが非常に大きなものとなってしまう. そこで, 位置情報を利用したサービスの一つとして, 上記の問題を解決するサイズ効率のよい暗号方式を提案する. 本論文内では, まず初めに “位置情報ベース暗号 (Position-Based Encryption : PBE)” の概念を提案する. 次に, このモデルを満たすサイズ効率のよい方式を動的な属性情報更新機能を持つ属性ベース暗号について研究した際に得られた知見を用いて提案する. そして, 位置情報ベース暗号に対する IND-CPA 安全性モデル (もとの平文の内容を一部分の知ることができない安全性) を提案し, 提案方式が IND-CPA 安全を満たすことを証明する. また, 提案方式と既存の暗号を用いて実現した方式との性能評価を行う.

2 諸定義

2.1 安全性の指標

2.1.1 安全性のモデル

識別不可能性 (IND) 暗号文 C を平文 M_0 か M_1 のどちらかをランダムに暗号化したものとする. この M_0, M_1, C が与えられた攻撃者が C は M_0 か M_1 のどちらを暗号化したかのかがわからないという性質. また識別不可能性と強秘匿性の安全性強度は同等である.

2.1.2 攻撃者の強度のモデル

選択平文攻撃 (CPA) 攻撃者は任意の平文を暗号化することができるとする攻撃. 公開鍵暗号において公開鍵は公開されているので, 攻撃者は選択平文攻撃を行える.

暗号が選択平文攻撃ができる攻撃者に対し識別不可能性を持つ場合, IND-CPA 安全を持つという.

2.2 DBDH 仮定

生成元を g とし, セキュリティパラメータに従った素数位数 p の群 $\mathbb{G}_1$ を決め, $a, b, c \in \mathbb{Z}_p$ をランダムに選択する. g^a, g^b, g^c, T が与えられたとき T が $e(g,g)^{abc} \in \mathbb{G}_2$ かランダムに選択した値 $R \in \mathbb{G}_2$ かを識別するのが困難な仮定を DBDH 仮定と呼ぶ.

2.3 DPBDHE 仮定

生成元を g とし, セキュリティパラメータに従った素数位数 p の群 $\mathbb{G}_1$ を決め, $a, s, b_1, \ldots, b_q \in \mathbb{Z}_p$ をランダムに選択する. $\forall_{1\leq j\leq q}, \forall_{1\leq j,k\leq q,k\neq j}$ とし,

$$\begin{aligned}\overrightarrow{y} \;=\; & (g, g^s, g^a, \ldots, g^{(a^q)}, \ , g^{(a^{q+2})}, \ldots, g^{(a^{2q})}, \\ & g^{s\cdot b_j}, g^{a/b_j}, \ldots, g^{(a^q/b_j)}, \ , g^{(a^{q+2}/b_j)}, \ldots, g^{(a^{2q}/b_j)}, \\ & g^{a\cdot s\cdot b_k/b_j}, \ldots, g^{(a^q\cdot s\cdot b_k/b_j)})\end{aligned}$$

が与えられたとき, T が $e(g,g)^{a^{q+1}s} \in \mathbb{G}_2$ かランダムに選択した値 $R \in \mathbb{G}_2$ かを識別するのが困難な仮定を DqPBDHE 仮定と呼ぶ.

3　動的な属性情報更新機能を持つ属性ベース暗号

復号鍵に含まれるアクセスポリシー, または属性の集合といった情報を変更可能な属性ベース暗号を提案し, 安全性を証明した.

3.1　動的な属性情報更新機能を持つ鍵ポリシー属性ベース暗号

Goyal らの方式 [2] をもとに動的な属性情報更新機能を持つ鍵ポリシー属性ベース暗号を提案した. また, 提案方式の安全性について以下の定理を証明した. 定理 1 の対偶により, Goyal らの方式が IND-CPA 安全を持つならば提案方式も IND-CPA 安全を持つことが言える.

定理 1 *Selective-set* モデルにおいて提案方式の *IND-CPA* 安全をアドバンテージ ϵ で破る攻撃者が存在するならば, *Goyal* らの鍵ポリシー属性ベース暗号をアドバンテージ $\frac{\epsilon}{2}$ で破る攻撃者が存在する.

3.2　動的な属性情報更新機能を持つ暗号文ポリシー属性ベース暗号

Waters の方式 [5] をもとに動的な属性情報更新機能を持つ暗号文ポリシー属性ベース暗号を提案した. また, 提案方式の安全性について以下の定理を証明した. 定理 2 の対偶により, Waters の方式が IND-CPA 安全を持つならば提案方式も IND-CPA 安全を持つことが言える.

定理 2 *Selective-set* モデルにおいて提案方式の *IND-CPA* 安全をアドバンテージ ϵ で破る攻撃者が存在するならば, *Waters* の暗号文ポリシー属性ベース暗号をアドバンテージ $\frac{\epsilon}{2}$ で破る攻撃者が存在する.

表 1: 位置情報ベース暗号方式の比較

方式	公開パラメータサイズ	秘密鍵サイズ	暗号文サイズ
BE[1] を用いた PBE	$2mn$	1	2
提案方式	$6(m+n)-11$	$3(m+n)-6$	3

$m \times n$ マップ

単位：群の要素数

4　位置情報ベース暗号

本研究では, まず位置情報ベース暗号という概念を提案した. そして, このモデルを満たすサイズ効率のよい方式を閾値暗号文ポリシー属性ベース暗号と呼ばれる属性ベース暗号の一種をもとに提案したまた, その安全性について以下の定理を証明した. 定理 3 の待遇により, 提案方式に用いた閾値暗号文ポリシー属性ベース暗号が IND-CPA 安全を持つならば, 提案方式も IND-CPA 安全を持つことが言える. また, 提案方式と既存の暗号を用いて実現した方式との性能評価を行った.

定理 3 提案方式の *IND-CPA* 安全をアドバンテージ ϵ で破る攻撃者が存在するならば, 提案方式に用いる閾値暗号文ポリシー属性ベース暗号をアドバンテージ ϵ で破る攻撃者が存在する.

4.1　性能評価

提案方式と既存の暗号を用いて実現した方式との性能評価を行う. 今回評価するにあたり, Boneh らにより提案された放送暗号 [1] を用いて実現した位置情報ベース暗号と比較する. この評価結果を表 1 に記す.

5 結論

本研究では, 既存の属性ベース暗号 [2, 5] に鍵の属性を更新する機能を付加した方式を提案した. そして, 動的な属性情報更新機能を持つ属性ベース暗号に対する安全性モデルを提案し, 仮定のもと提案方式が安全であることを証明した. また, 動的な属性情報更新機能を持つ暗号文ポリシー属性ベース暗号を用いたアプリケーションの例を示した.

さらに, 新たに位置情報ベース暗号という概念を提案し, このモデルを満たすサイズ効率のよい提案方式を既存の閾値暗号文属性ベース暗号 [3] から構成し, IND-CPA 安全を満たすことを証明した. そして, 提案方式と閾値暗号文ポリシー属性ベース暗号, 暗号文ポリシー属性ベース暗号, 放送暗号を用いて実現した方式との性能評価を行った. また, 提案方式の拡張と位置情報ベース暗号を用いたアプリケーションの例について示した.

謝辞

本研究を進めるにあたり，日々有益かつ適切な御助言を賜りました指導教官の今井秀樹教授に心から感謝致します. 独立行政法人産業技術総合研究所情報セキュリティ研究センターのナッタポン アッタラパドゥン氏には, 研究に対しての考え方や非常に有益な議論と助言をして頂いたことに深く感謝いたします. 中央大学研究開発機構研究員の北川隆氏には, 論文の執筆や発表練習などで多大な助言をして頂きましたことに感謝いたします.

発表論文

- 久野 真太郎, ナッタポン アッタラパドゥン, 北川 隆, 今井 秀樹, “動的な属性情報更新可能な属性ベース暗号,” 暗号と情報セキュリティシンポジウム 2010 (SCIS 2010), 4C2-1,2010.
- 久野 真太郎, ナッタポン アッタラパドゥン, 北川 隆, 今井 秀樹, “動的な属性情報更新機能を持つ暗号文ポリシー属性ベース暗号,” 暗号と情報セキュリティシンポジウム 2011 (SCIS 2011), 2A4-3, 2011.
- 久野 真太郎, ナッタポン アッタラパドゥン, 北川 隆, 今井 秀樹, “位置情報ベース暗号,” 暗号と情報セキュリティシンポジウム 2012 (SCIS 2012), 1A1-4, 2012.

参考文献

[1] Dan Boneh, Craig Gentry, and Brent Waters, “Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys,” CRYPTO 2005, LNCS 3621, pp. 258–275, 2005.

[2] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,” Proc. of the ACM conference on computer and communications security 2006, pp. 89–98, 2006.

[3] Javier Herranz, Fabien Laguillaumie, and Carla Rafols, “Constant size Ciphertexts in Threshold Attribute-Based Encryption,” PKC2010, LSCN, 6056, pp. 19–34, 2010.

[4] Amit Sahai and Brent Waters, “Fuzzy Identity Based Encryption,” In Advances in Cryptology - Eurocrypt, volume 3494 of LNCS, pages 457–473, Springer, 2005.

[5] Brent Waters, “Ciphertext-Policy Attribute-Based Encryption : An Expressive, Efficient, and Provably Secure Realization,” Cryptology ePrint Archive, Report 2008/290, http://eprint.iacr.org/2008/290, 2008.