2Z-1

暗号文の提供者を不特定多数とする検索者を限定したキーワード検索可能暗号方式

冨田　幸嗣[†]　　毛利　公美[‡]　　白石　善明[†]

[†]名古屋工業大学　　[‡]岐阜大学

1. はじめに

2004 年に公開鍵暗号方式の検索可能暗号[1]が提案された．その後，Anonymous HIBE を基にした方式[2]など様々な検索可能暗号方式が提案されている．データの提供者と保管者が異なるクラウドサービスでは，データを保管者に知られないようにするためには暗号化を行い，暗号文のままデータを検索できるのが望ましい．

検索可能暗号で検索者を限定できる方式がある．システムのセットアップのときの指定数を上限とする検索者で，提供者が不特定多数となるブロードキャスト暗号をもとにした方式[3]や，提供者が一人である ID ベースブロードキャスト暗号をもとにした方式[4]が提案されている．

本稿では，暗号文の提供者が不特定多数で検索者に上限数がない検索可能暗号方式を提案する．

2. 準備

2.1 双線形写像

$\mathbb{G}_1, \mathbb{G}_2$を素数位数$p$の巡回群とする．双線型写像 $\mathrm{e}: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$は任意の$a, b \in \mathbb{Z}_p$，$P, Q \in \mathbb{G}_1$に対して，以下の性質を満たす．

- 双線形性
  $\mathrm{e}(aP, bQ) = \mathrm{e}(P, Q)^{ab}$ が成立する．
- 非縮退性
  $\mathrm{e}(P, Q) = 1$ならば$P = 0$または$Q = 0$.
- 計算可能性
  $\mathrm{e}(P, Q)$ を計算する多項式時間アルゴリズムが存在する．

2.2 BDH 仮定

$\mathbb{G}_1$の生成元Pと任意の整数$a, b, c \in \mathbb{Z}$について$< P, aP, bP, cP >$から$\mathrm{e}(P, P)^{abc}$を求める問題を BDH 問題(Bilinear Diffie-Hellman Problem)という．BDH 問題を解く効率的な多項式時間アルゴリズムが存在しないという仮定を BDH 仮定という．

3. 提案方式：暗号文の提供者を不特定多数とする検索者を限定したキーワード検索可能暗号

3.1 構成エンティティ

[提供者]

キーワードWと検索者のIDを指定し，Wの暗号文Cを作成する．暗号文は保管者に管理してもらう．

[検索者]

特定のキーワードの暗号文を検索する．それぞれの検索者は固有の ID を持つ．

保管者にトラップドアを入力として問い合わせ，保管者から暗号文が特定のキーワードを暗号化したものであるか否か返答を受ける．

[保管者]

提供者からキーワードの暗号文を受け取り保管する．検索者からトラップドアによる問い合わせを受け，返答を行う．

[PKG]

公開パラメータとマスター鍵を作成し，公開パラメータを公開する．マスター鍵と検索者から受け取ったIDから秘密鍵を作成し，秘密鍵を検索者に渡す．

3.2 定義

提案方式は以下の 5 つのアルゴリズムから成る．

KeyGen(k)　セキュリティパラメータkを入力として，公開パラメータparamsとマスター鍵mskを出力する．

Extract (params, msk, ID)　公開パラメータparamsとマスター鍵msk，検索者のIDを入力として秘密鍵d_{ID}を出力する．

Encrypt (params, ID, W)　公開パラメータ params，検索者の ID，キーワード W を入力として暗号文 C を出力する．

Trapdoor(params, d_{ID}, W)　公開パラメータparamsと秘密鍵d_{ID}，キーワードWを入力としてトラップドア$T_{W,\mathrm{ID}}$を出力する．

Test(params, C, $T_{W,\mathrm{ID}}$)　公開パラメータparamsと暗号文C，キーワードWと検索者のIDから作られたトラップドア$T_{W,\mathrm{ID}}$を入力として，暗号文CがキーワードWと検索者のIDから生成された暗号文であるか否かを 1 ビット

Keyword Searchable Encryption with Access Control in Multi-User Setting

† Koji TOMIDA and Yoshiaki SHIRAISHI・Nagoya Institute of Technology

‡ Masami MOHRI・Gifu University

(0/1)で出力する．

3.3 構成

構成要素として双線形写像$\mathrm{e}:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_2$，ハッシュ関数$\mathrm{H}_1:\{0,1\}^*\to\mathbb{G}_1$，$\mathrm{H}_2:\mathbb{G}_2\to\{0,1\}^n$，$\mathrm{H}_3:\{0,1\}^*\to\mathbb{Z}_p^*$を用いる．$n$は自然数である．

KeyGen(k) セキュリティパラメータkを入力とし，kビットの素数pを選ぶ．pを位数とする2つの群$\mathbb{G}_1,\mathbb{G}_2$を決定し，双線形写像eを出力する．ランダムに$s\in\mathbb{Z}_p^*$と生成元$P\in\mathbb{G}_1$を選択し$P_{pub}=sP$を計算する．3つのハッシュ関数$\mathrm{H}_1$，$\mathrm{H}_2$，$\mathrm{H}_3$を決定する．公開パラメータ params $=<p,n,P,P_{pub},\mathrm{H}_1,\mathrm{H}_2,\mathrm{H}_3,\mathrm{e}>$，マスター鍵msk $=s$を出力する．

Extract (params, msk, ID) ID$\in\{0,1\}^*$から$Q_{\mathrm{ID}}=\mathrm{H}_1(\mathrm{ID})\in\mathbb{G}_1$を計算する．マスター鍵mskを用いて秘密鍵$d_{\mathrm{ID}}=sQ_{\mathrm{ID}}$を出力する．

Encrypt (params, ID, W) IDから$Q_{\mathrm{ID}}=\mathrm{H}_1(\mathrm{ID})$を計算し，ランダムに$r\in\mathbb{Z}_p^*$を選択する．暗号文$C=[rP,\mathrm{H}_2(g_{\mathrm{ID}}^r)]$，$g_{\mathrm{ID}}=\mathrm{e}\left(\mathrm{H}_3(W)Q_{\mathrm{ID}},P_{pub}\right)\in\mathbb{G}_2$を出力する．

Trapdoor(params, d_{ID}, W) 秘密鍵d_{ID}とキーワードWから$T_{W,\mathrm{ID}}=\mathrm{H}_3(W)d_{\mathrm{ID}}$を計算し，トラップドアとして出力する．

Test(params, C, $T_{W,\mathrm{ID}}$) $C=[C_1,C_2]$とする．$\mathrm{H}_2(\mathrm{e}(T_{W,\mathrm{ID}},C_1))=C_2$となるかテストする．2値が一致したときに1，そうでないときは0を出力する．

提案方式の流れを図1に示す．

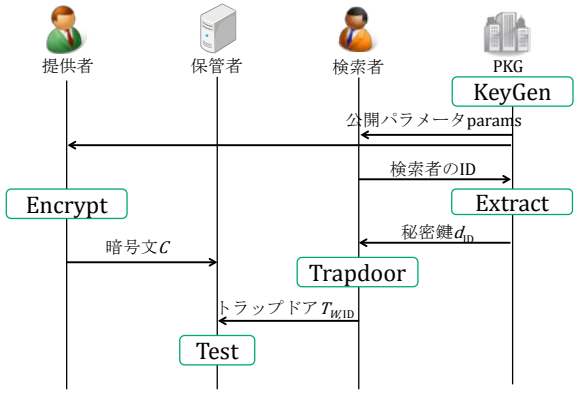

図1 提案方式の流れ

4. 安全性

次のような攻撃者を考える．攻撃者は暗号文や公開パラメータを入手することができ，暗号文からキーワードを入手しようとする．ただし，その暗号文を検索するのに対応したトラップドアは入手できないものとする．それ以外のトラップドアに関しては，任意のIDとキーワードに対応したすべてのトラップドアを適応的に入手できるものとする．

攻撃者が任意のIDと2つのキーワードW_0,W_1を選ぶと，IDと一方のキーワードから作られた暗号文がランダムに与えられるとする．攻撃者がどちらのキーワードの暗号文であるか識別できた場合に，攻撃者は暗号文からキーワードに関する情報を部分的に得ることができたと考えることができる．

攻撃者はW_0,W_1の暗号文の検索に対応するトラップドアを入手することはできないが，手持ちの公開パラメータparamsと暗号文$C=[C_1,C_2]$から$\mathrm{H}_2\left(\mathrm{e}\left(\mathrm{H}_3(W)Q_{\mathrm{ID}},P_{pub}\right)^r\right)$を求めることができれば，暗号文に対応するトラップドアを用いて暗号文を検索したときと同じ結果を得ることができる．$\mathrm{H}_3(W)\in\mathbb{Z}_p^*$であり，$Q_{\mathrm{ID}}=aP,P_{pub}=bP,C_1=rP$から$\mathrm{e}(P,P)^{abr}$を求めることができるかが問題となる．BDH仮定よりこの問題を解くことは困難である．したがって，提案方式は選択キーワード攻撃に対して識別不可能性の意味で安全である．

5. まとめ

本稿では，暗号文の提供者を不特定対数とする検索者を限定したキーワード検索可能暗号方式を提案した．提案方式は提供者と検索者がともに多数の状況に対応し，かつ検索者数に上限がない．提案方式はランダムオラクルモデルにおいて，BDH仮定のもと，選択キーワード攻撃に対して識別不可能性の意味で安全である．

参考文献

[1] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” EUROCRYPT 2004, LNCS, vol.3027, pp.506-522, 2004.

[2] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, “Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions,” CRYPTO 2005, LNCS, vol.3621, pp.205-222, 2005.

[3] N. Attrapadung, J. Furukawa, H. Imai, “Forward-Secure and Searchable Broadcast Encryption with Short Ciphertexts and Private Keys,” ASIACRYPT 2006, LNCS, vol.4284, pp.161-177, 2006.

[4] 片山貴充，高木剛，“アクセス制限可能なキーワード検索可能暗号方式，” 暗号と情報セキュリティシンポジウム SCIS2008，4E2-2，2008.