

# Fuzzy Identity-Based Encryption

岩手県立大学大学院 ソフトウェア情報学研究科

分散システム学講座

及川一樹

- Amit Sahai and Brent Waters. Fuzzy Identity-Based Encryption. In Eurocrypt 2005, LNCS 3494, pp. 457–473, Springer-Verlag, 2005.

# 1 Introduction (1)

- Identity-Based Encryption (IBE) [1]
  - 公開鍵を事前取得しなくても、IDを公開鍵として利用可能な暗号
    - 例: メールの暗号化
  - スキーム
    - 前提:
      - PKG (Private Key Generator)がグローバルパラメータ生成 (setup)
      - グローバルパラメータはシステム利用者全員が知っている
    - 暗号時:
      - 受取人のIDを公開鍵として暗号化 (encrypt)
    - 復号時:
      - PKGに対して身元を証明し、自分のIDに対応する秘密鍵を取得 (extract)
      - PKGより取得した秘密鍵を用いてメッセージを復号 (decrypt)

# 1 Introduction (2)

- Fuzzy Identity-Based Encryption
  - これまでのIBEは一意的な識別子を利用していた
  - Fuzzy IBEでは属性の集合をIDとして利用する
    - $\omega$  : ユーザのID
    - $\omega'$  : 暗号化に利用されたID
    - $\omega$ と $\omega'$ の距離が、一定の距離未満の場合にのみ復号できる
  - IDに対して一定量の誤差を許容する
- Fuzzy IBEの応用例
  - バイオメトリクスID
  - 属性ベース暗号 (Attribute-Based Encryption, ABE)

# 1 Introduction (3)

- バイオメトリクスID
  - 身体的な特徴をIDとして利用する
    - 虹彩
    - 指紋
  - バイオメトリクスの測定にはノイズが含まれる
    - 従来 of IBE:
      - ノイズを含むバイオメトリクス情報に対して秘密鍵が必要
      - 無数の秘密鍵が必要となるため、利用できない
    - Fuzzy IBE:
      - 誤差を許容する特性を持つため、ノイズを無視できる
      - 少ない鍵の数で実現できる

# 1 Introduction (4)

- バイオメトリクスとIBEスキームは相性が良い
  - 簡単にPKGから秘密鍵を取得できる
    - “及川一樹”のようなIDに対応する秘密鍵を取得する権限があるかどうかを、PKGに立証するのは難しい
    - バイオメトリクスであれば検証は容易
      - 但し、バイオメトリクス技術の安全性に依存する
  - バイオメトリクス情報はユニーク
    - “及川一樹”のような名前がIDだと、同姓同名に対応できない
  - 利用者はIDを常に携帯している

# 1 Introduction (5)

- 属性ベース暗号
  - 属性の集合を利用して暗号化を行う
  - 例:
    - {"岩手県立大学", "学生"}で暗号化
    - 上記の属性をすべて持つユーザ以外は復号できない
      - 及川一樹 → ○
      - 高田先生 → ×
      - 岩手大学の学生 → ×

# Security Against Collusion Attacks

- 結託攻撃に対する安全性
    - 利用者が結託して鍵を合成し、各利用者には権威のない属性の集合で暗号化された文章の復号が出来てはならない
  - 属性ベース暗号を例に説明:
    - {"岩手県立大学", "学生"}で暗号化
    - 上記の属性をすべて持つユーザ以外は復号できない
      - 及川一樹 → ○
      - 高田先生 → ×
      - 岩手大学の学生 → ×
    - 高田先生と岩手大学の学生が結託し、以下の鍵を合成
      - 高田先生の"岩手県立大学"という属性の鍵
      - 岩手大学の学生の"学生"という属性の鍵
- 合成鍵では暗号文は復号できない

# 本論文の概要

- 本論文ではFuzzy IBEの構築を行う
- 主な手法
  - IDを集合として表現
  - 双線形写像
  - Shamirの秘密分散手法

## 2 Other Approaches

- エラー訂正
  - 普通のIBEを利用するために、バイオメトリクスの読み取りノイズを修正する方法
- 属性毎の鍵
  - 各属性をIDとして、普通のIBEを利用し、属性ベース暗号を実現する方法
  - 結託攻撃に対して脆弱
- ノイズも含めた大量の鍵
  - $|\omega \cap \omega'| \geq d$  となるような、すべての $\omega'$ の秘密鍵を格納する ( $d$ : エラー許容閾値)
  - 秘密鍵の量が $d$ に対して指数関数的に増加

# 3 Preliminaries

Bilinear Maps

Shamir's Secret Sharing Method

# Bilinear maps

- 双線形写像 (Bilinear maps)

$\mathbb{G}_1, \mathbb{G}_2$  を素数位数の群とするとき

双線形写像  $e: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$  とは、以下の特徴を持つ写像のこと

- 双線形性:

$g$  を  $\mathbb{G}_1$  の生成元とするとき、 $e(g^a, g^b) = e(g, g)^{ab}$  が成り立つ

- 非縮退性:

$g$  が  $\mathbb{G}_1$  の生成元ならば、 $e(g, g)$  も  $\mathbb{G}_2$  の生成元

ここでは特に以下の特徴も併せ持つ写像のことを指す

- 計算可能性:

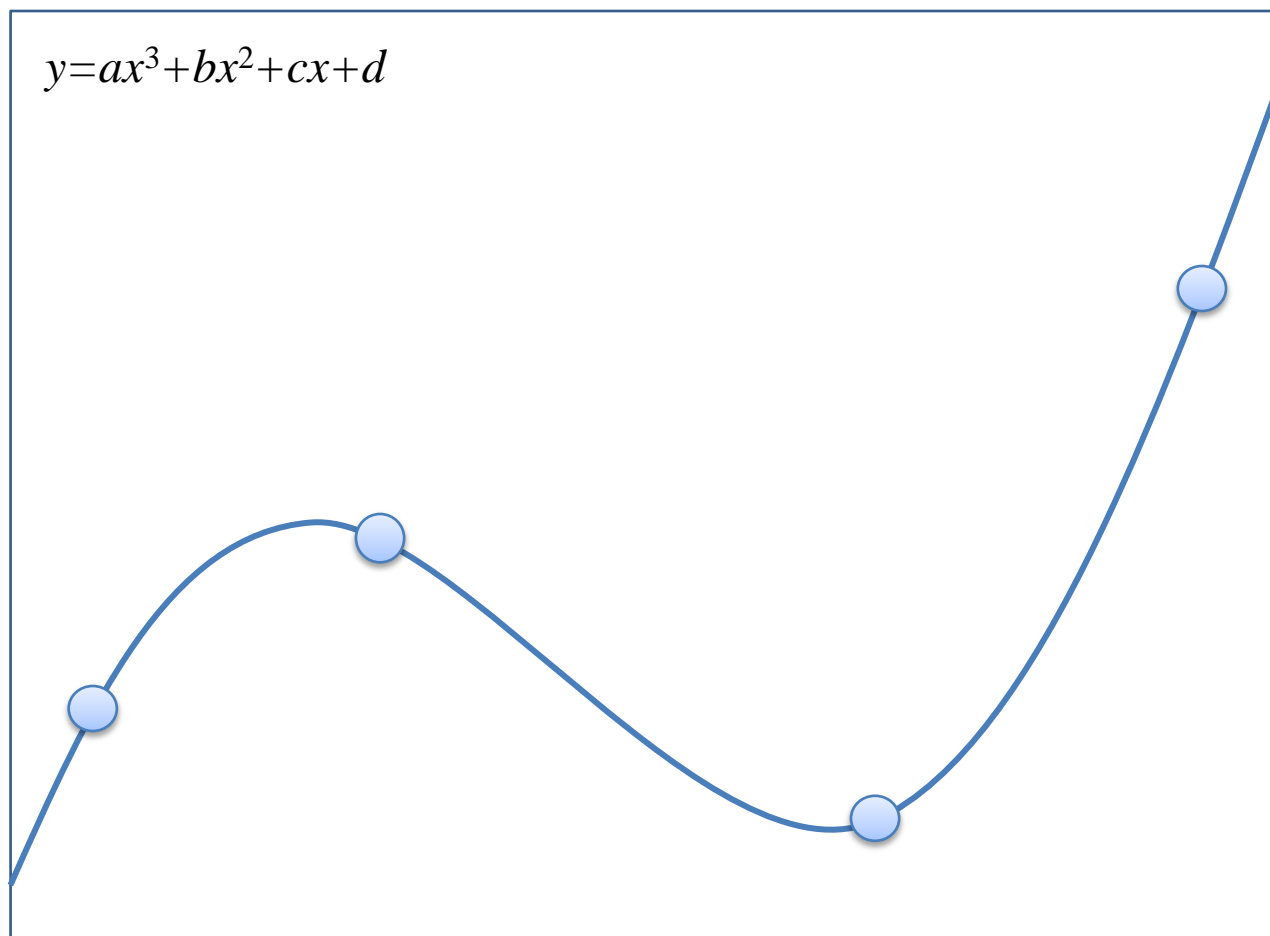
すべての  $P, Q \in \mathbb{G}_1$  において  $e(P, Q)$  が効率的に計算できる

# Shamir's Secret Sharing (1)

- 秘密分散 (Adi Shamirが1979年に最初に提案[2])
  - 情報を $n$ 個のピースに分割
  - $k$  個以上のピースを集めることにより元のデータを復元
  - $k$  個未満のピースでは元のデータを復元不能
- Shamirの秘密分散法
  - ラグランジュ多項式を利用 (ラグランジュ補間で利用される多項式)
  - $n$ 点を通る1変数多項式は、 $n-1$ 次1変数多項式として一意に定まる
    - $y=ax+b$
    - $y=ax^2+bx+c$

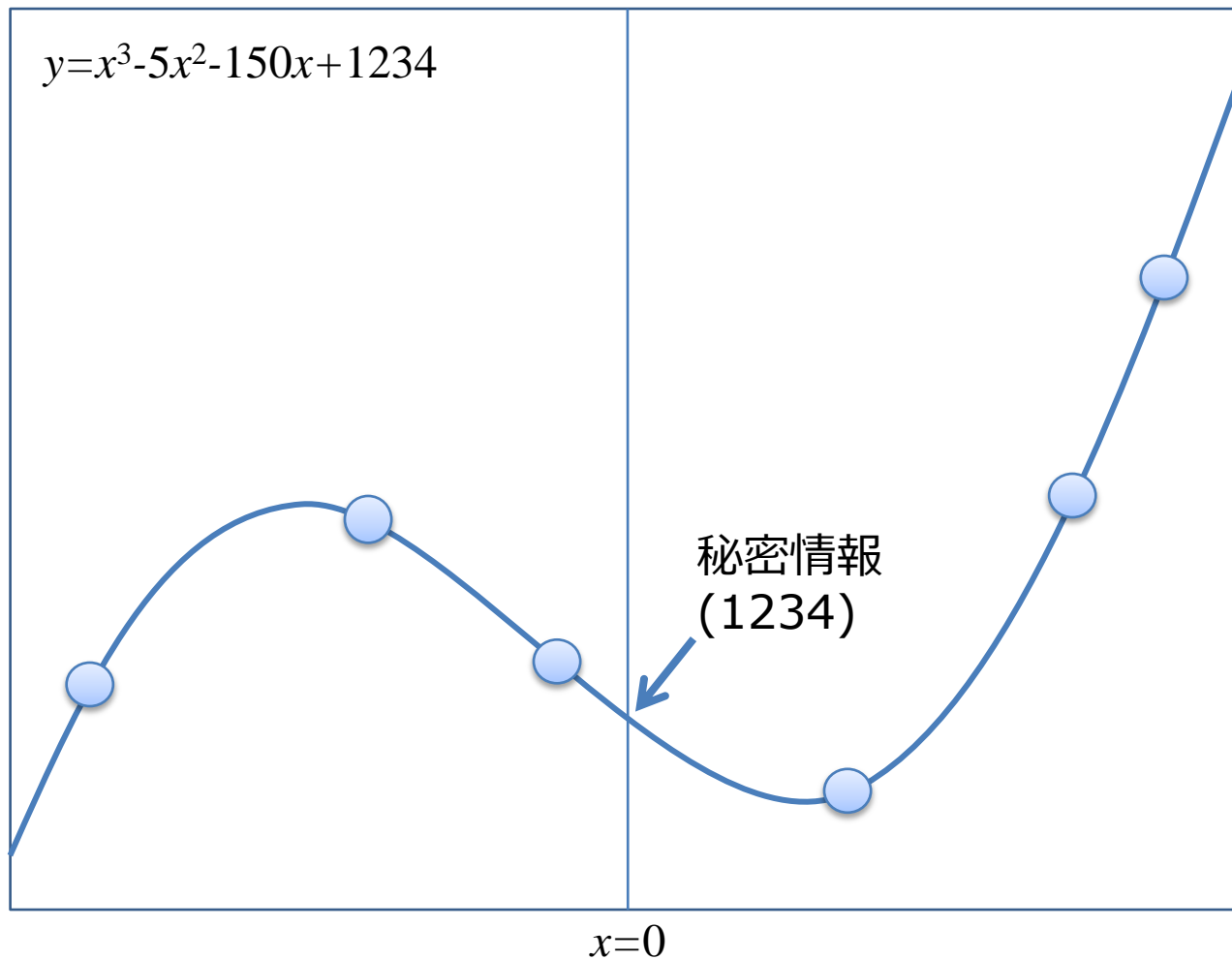
# Shamir's Secret Sharing (2)

- ラグランジュ補間



# Shamir's Secret Sharing (3)

- Shamirの秘密分散の概要



# Shamir's Secret Sharing (4)

- Shamirの秘密分散法

- 準備

1. 秘密情報を $S$ , 分割数を $n$ , 復元可能ピース数の閾値を $k$ とする
2. 定数項が $S$ となるような  $k-1$ 次の1変数多項式をランダムに生成  
 $q(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1} \quad (a_0 = S)$
3.  $\{(1, q(1)), (2, q(2)), \dots, (n, q(n))\}$  を計算

- 復元

1. 入手したピースを  $\{(x_0, y_0), (x_1, y_1), \dots, (x_{k-1}, y_{k-1})\}$  とする
2. ラグランジュの補間多項式を求める

$$f(x) = \sum_{j=0}^{k-1} y_j \ell_j(x), \quad \ell_j(x) = \prod_{i=0, i \neq j}^{k-1} \frac{x - x_i}{x_j - x_i}$$

3. 秘密情報  $S' = f(0)$

# 4 Our Construction

# Fuzzy IBEにおけるID

- Fuzzy IBEで利用するIDは属性の集合

$$\omega = \{121, 122, 123, 124, 125\}$$

$$\omega' = \{122\}, \omega'' = \{256\}, \omega''' = \{7, 125\}$$

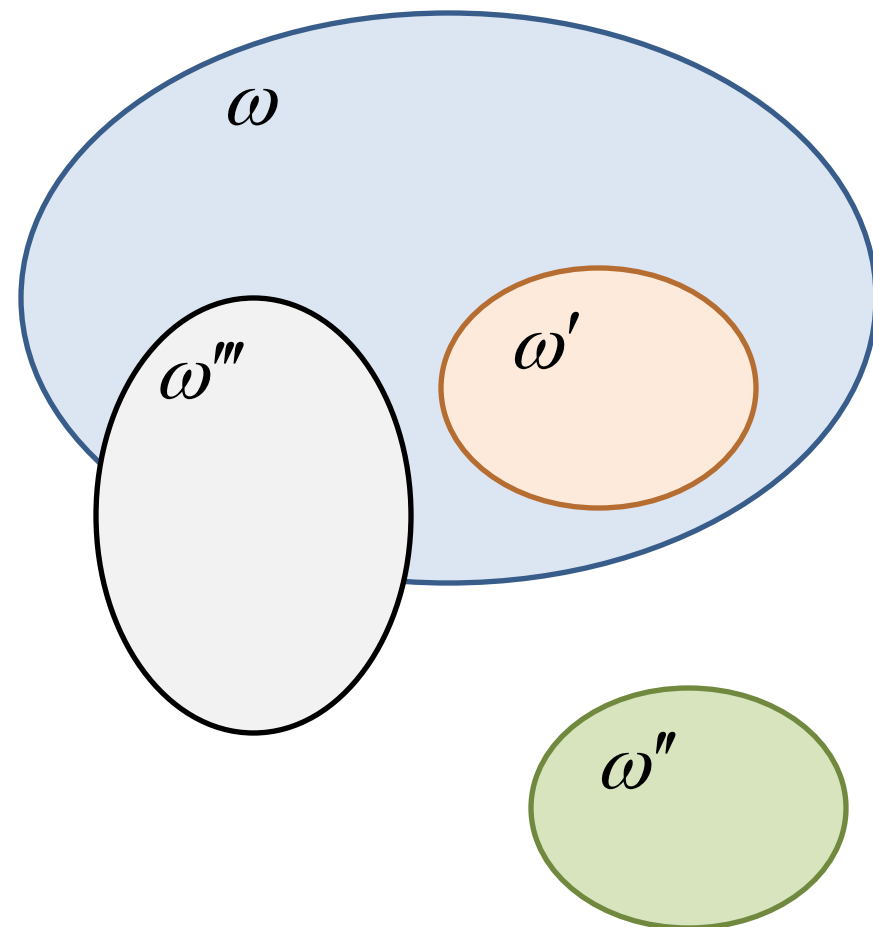
- $\omega'$ で暗号化したものが $\omega$ で復号できる条件  $\rightarrow |\omega \cap \omega'| \geq d$ 
  - $\omega$ と $\omega'$ の要素が一定の数以上一致していることが条件

- 属性ベース暗号の例:

$$\omega = \{\text{IPU, 学生, 高田研}\} \quad (d = 2)$$

$$\omega' = \{\text{IPU, 学生}\}, \omega'' = \{\text{IPU, 教員}\}$$

$$\omega''' = \{\text{IPU, 教員, 高田研}\}$$



# Fuzzy IBEの構築 – はじめに

- 暗号化を行う鍵  $\rightarrow \omega'$ , 復号を行う鍵  $\rightarrow \omega$
- エラー許容閾値  $d$ ,  $|\omega \cap \omega'| \geq d$
- 双線形写像  $e: (\mathbb{G}_1 \times \mathbb{G}_1) \rightarrow \mathbb{G}_2$ 
  - $\mathbb{G}_1$ の生成元  $g$
  - $\mathbb{G}_1$ の素数位数  $p$
- ラグランジュ係数  $\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$
- 属性の全体集合  $\mathcal{U} = \{u_1, u_2, \dots, u_{|\mathcal{U}|}\}$
- IDは  $\mathcal{U}$ の要素のインデックスの集合 (とする)  
 $\omega, \omega' \subseteq \{1, 2, \dots, |\mathcal{U}|\}$

# Fuzzy IBEの構築 – Setup

- PKGが行う処理で、グローバルパラメータを生成する
- 入力
  - $d$  : エラー許容閾値. PKGが保存
- 処理
  - 乱数を $|\mathcal{U}|$ 個生成  $t_1, t_2, \dots, t_{|\mathcal{U}|} \in \mathbb{Z}_p$
  - 乱数  $y \in \mathbb{Z}_p$  を生成
  - 公開パラメータを以下のように生成
$$T_1 = g^{t_1}, \dots, T_{|\mathcal{U}|} = g^{t_{|\mathcal{U}|}}, Y = e(g, g)^y$$
- 出力
  - 公開パラメータ:  $T_1, \dots, T_{|\mathcal{U}|}, Y$
  - マスターキー:  $t_1, \dots, t_{|\mathcal{U}|}, y$

# Fuzzy IBEの構築 – Key Generation

- PKGが行う処理。IDから秘密鍵を生成する。
- 入力
  - $\omega$ : 秘密鍵を生成するID
- 処理
  - $q(0)=y$  となるような  $d-1$ 次多項式  $q$  をランダムに選択
  - 次の式を計算

$$\left\{ D_i = g^{\frac{q(i)}{t_i}} \right\}_{i \in \omega}$$

g: 生成元  
 $t_i$ : マスターキー

- 出力
  - $\{D_i\}_{i \in \omega}$

# Fuzzy IBEの構築 – Encryption

- 入力
  - $\omega'$ : 暗号化に利用するID
  - $M \in \mathbb{G}_2$ : 平文
- 処理
  - 乱数  $s$  を選択
  - 暗号文を次のように計算
$$E = (\omega', E' = MY^s, \{E_i = T_i^s\}_{i \in \omega'})$$
- 出力
  - 暗号文  $E$

$Y, T_i$ : 公開パラメータ

# Fuzzy IBEの構築 – Decryption

- 入力

- 暗号文  $E = (\omega', E' = MY^s, \{E_i = T_i^s\}_{i \in \omega'})$

- 処理

- $d$  個の要素を持つ部分集合  $S = \omega \cap \omega'$  を求める

- 以下の式を解く

$$\begin{aligned}
 E' / \prod_{i \in S} (e(D_i, E_i))^{\Delta_{i,S}(0)} &= Me(g, g)^{sy} / \prod_{i \in S} \left( e(g^{\frac{q(i)}{t_i}}, g^{st_i}) \right)^{\Delta_{i,S}(0)} \\
 &= Me(g, g)^{sy} / \prod_{i \in S} (e(g, g)^{sq(i)})^{\Delta_{i,S}(0)} \\
 &= M
 \end{aligned}$$

- 出力: 平文  $M$

# 復号処理

$$\begin{aligned}
 \prod_{i \in S} \left( e(g, g)^{sq(i)} \right)^{\Delta_{i,S}(0)} &= \prod_{i \in S} e(g, g)^{sq(i)\Delta_{i,S}(0)} \\
 &= e(g, g)^{\sum_{i \in S} sq(i)\Delta_{i,S}(0)} \\
 &= e(g, g)^{sy}
 \end{aligned}$$

暗号文に含まれる  $E'$  は

$$E' = Me(g, g)^{sy}$$

と定義されているので、以下のように平文が求まる

$$Me(g, g)^{sy} / e(g, g)^{sy} = M$$

# 鍵サイズ、エラー許容の柔軟性

- 鍵サイズ
  - グローバルパラメータの要素数はシステム全体の属性数に比例
    - システム全体の属性数 =  $|U|$
  - ユーザの秘密鍵の大きさは、IDの要素数に比例
  - 暗号文の要素数は、暗号化に利用したIDの要素数に比例
- エラー許容の柔軟性
  - 閾値  $d$  は、グローバルパラメータで定数として設定される
    - 柔軟性がない
  - シンプルな解決策
    - $d$  にあわせてPKGを複数用意する
    - ダミーの属性を用意し、パディングとして利用する

(スケーラビリティ向上させた変形も紹介されていたが、省略)

# References

- [1] Dan Boneh and Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. In *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, pp. 213–229, London, UK, 2001. Springer-Verlag.
- [2] Adi Shamir. How to share a secret. *Communications*. ACM, Vol. 22, No. 11, pp. 612–613, 1979.