Weil Pairing を用いた ID ベース暗号の仕組みと問題点

工藤麻美　(指導教員: 金子 晃)

1　はじめに

1984 年，Shamir は公開鍵暗号方式の公開鍵を，任意の文字列で作れないかと考えた．その当初の動機は，e-mail システムの認証処理を簡単にするためだった．

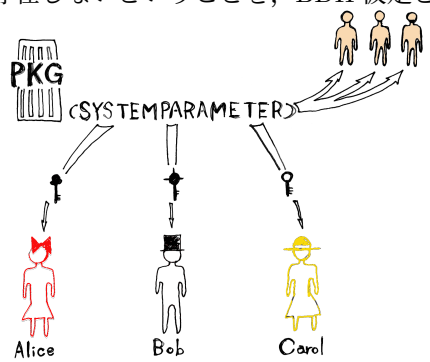
例えば，Alice が Bob のメールアドレス bob@hotmail.com 宛にメールを送るとき，Alice は文字列 “bob@hotmail.com” を Bob の公開鍵として使ってメッセージを暗号化する．そのとき Alice は Bob の公開鍵の証明書を入手する必要はない．Bob が暗号化されたメールを受け取ったら，Bob は PKG(Private Key Generator) と呼ばれる第三者に連絡を取り，彼の秘密鍵を入手する．そして Bob は暗号化されたメールを読むことができるようになる．既存の安全な e-mail 基盤とは異なり，Bob がまだ自分の公開鍵を setup していなくても，Alice は Bob に暗号化したメールを送ることができる．

ここでは，このようなシステムを有限体上の楕円曲線を用いて作る方法を紹介する．

2　双線形 Diffie-Hellman 仮定

$\mathbb{G}_1, \mathbb{G}_2$ を大きな素数 q を位数とする巡回群とし，$\mathbb{G}_1$ は加法的に，$\mathbb{G}_2$ は乗法的に表現する．また，$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ という多項式時間で計算可能な非退化な双線形写像 $\hat{e}$ が定義されているとする．すなわち，$\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$，更に非退化の仮定を強めて，$P$ が $\mathbb{G}_1$ の生成元であるとき，$\hat{e}(P, P)$ は $\mathbb{G}_2$ の生成元になると仮定する．この写像を用いて，双線形 Diffie-Hellman 仮定が以下のように定義できる．

BDH 仮定: P を $\mathbb{G}_1$ の生成元とする．BDH 問題とは，$\langle P, aP, bP, cP\rangle$ に対して $\hat{e}(P, P)^{abc} \in \mathbb{G}_2$ を求める問題である．BDH 問題を多項式時間で解けるアルゴリズムが存在しないということを，BDH 仮定と呼ぶ．



3　ID ベース暗号の仕組み

BDH 仮定が成り立つという前提の下で，ID ベース暗号は次の 4 つの確率的アルゴリズム (Setup,Extract,Encrypt,Decrypt) の組で作れる．

Setup: セキュリティパラメータ k を選び，システムパラメータ params とマスターキー s を返す．(マスターキーは PKG だけが知っているものである．)

Extract: params とマスターキー s を入力すると，任意の文字列 $\mathsf{ID} \in \{0,1\}^*$ に対応する秘密鍵 d を生成する．

Encrypt: params, ID と平文 M を入力すると暗号文 C を返す．

Decrypt: params, ID，暗号文 C と秘密鍵 d を入力すると平文 M を返す．

このようなシステムを実現できる双線形写像のひとつの例を Weil Pairing を用いて作ることができる．

4　安全性の概念

公開鍵暗号の安全性の概念には色々あるが、ここでは暗号文単独攻撃に対する一方向性と，選択暗号文攻撃に対する強秘匿性を考える．これらは公開鍵暗号で一般的に認められている安全性の概念である．ただし ID ベース暗号では更に選択 ID 攻撃というものを加えてこれらの安全性を考察する．

5　Weil Pairing を使った ID ベース暗号

5.1　Weil Pairing

ある素数 q に対して，p を $p = 2 \mod 3$ と $p = 6q-1$ を満たす素数とする．E を $y^2 = x^3 + 1$ で定義される $\mathbb{F}_p$ 上の楕円曲線とする．この曲線に関するいくつかの事実を述べる．

Fact1: x^3+1 は $\mathbb{F}_p$ 上の置換なので $\mathbb{F}_p$ 上の楕円曲線 E は $p+1$ 個の点を持つ．O を無限遠点とする．$P \in E/\mathbb{F}_p$ を位数 $q = (p+1)/6$ の点とする．この点が生成する群を G_q で表す．

Fact2: $1 \neq \zeta \in \mathbb{F}_{p^2}$ を $x^3 - 1 = 0 \mod p$ の解とする．そのとき，写像 $\phi(x, y) = (\zeta x, y)$ は曲線 E 上の点の群の自己同型写像である．$P = (x, y) \in E/\mathbb{F}_p$ のとき $\phi(P) \in E/\mathbb{F}_{p^2}$ だが，$\phi(P) \notin E/\mathbb{F}_p$ となる．したがって $P \in E/\mathbb{F}_p$ は $\phi(P) \in E/\mathbb{F}_{p^2}$ と線形独立である．

Fact3: 点 P と点 $\phi(P)$ は線形独立なので，これらは $\mathbb{Z}_q \times \mathbb{Z}_q$ と同型な群を生成する．この群の点を $E[q]$ で表す．

μ_q を位数 $q = (p+1)/6$ の全ての元を含む $\mathbb{F}^*_{p^2}$ の部分群とする．曲線 $E/\mathbb{F}_{p^2}$ 上の Weil Pairing とは楕円曲線の因子と有理関数を用いて定義されるある写像 $e : E[q] \times E[q] \to \mu_q$ である．ここで Weil Pairing e を使って前述の条件を満たす写像 $\hat{e} : G_q \times G_q \to \mu_q$ を次のように定義することができる．

$$\hat{e}(P, Q) = e(P, \phi(Q))$$

写像 $\hat{e}$ は次の性質を満たす：

1. 双線形：全ての $P, Q \in G_q$ と全ての $a, b \in \mathbb{Z}$ に対して $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ となる．
2. 非退化：$\forall P \neq O$ に対して $\hat{e}(P, P) \in \mathbb{F}_{p^2}$ は位数 q の元であり，μ_q の生成元である．
3. 計算可能：$P, Q \in G_q$ が与えられたとき，$\hat{e}(P, Q)$ を計算する確率的多項式時間のアルゴリズムが存在する．

5.2　MapToPoint

この暗号システムは任意の文字列 $\mathsf{ID} \in \{0,1\}^*$ を位数 q の点 $Q_{\mathsf{ID}} \in E/\mathbb{F}_p$ へ写すためのハッシュ関数に依存した単純なアルゴリズムを使う．このアルゴリズムを MapToPoint と呼ぶ．

5.3 BasicIdent

まず簡単のため，選択 ID 攻撃付き暗号文単独攻撃に対して一方向性を満たす簡単なシステムについて記述する．これを BasicIdent と呼ぶ．このシステムは４つのアルゴリズム Setup, Extract, Encrypt, Decrypt から成る．

Setup:
Step 1: ある素数 $q > 3$ に対して $p = 2 \mod 3$ と $p = 6q - 1$ を満たす大きい k bit の素数 p を選ぶ．E を $y^2 = x^3 + 1$ で定義される $\mathbb{F}_p$ 上の楕円曲線とする．位数 q の任意の点 $P \in E/\mathbb{F}_p$ を選ぶ．
Step 2: ランダムに $s \in \mathbb{Z}_q^*$ を選び，$P_{\rm pub} = sP$ とおく．
Step 3: ハッシュ関数 $H : \mathbb{F}_{p^2} \to \{0,1\}^n$ を選ぶ．ハッシュ関数 $G : \{0,1\}^* \longrightarrow \mathbb{F}_p$ を選ぶ．安全性解析では H と G をランダムオラクルとして見る．
平文空間は $M = \{0,1\}^n$ ，暗号文空間は $C = E/\mathbb{F}_p \times \{0,1\}^n$ ，システムパラメータは $\mathsf{prams} = \langle p, n, P, P_{\rm pub}, G, H\rangle$, マスターキーは $s \in \mathbb{Z}_q$ となる．
Extract: 与えられた $\mathsf{ID} \in \{0,1\}^*$ に対して，このアルゴリズムは秘密鍵 d を次のようにして作る．
Step 1: $\mathsf{MapToPoint}_G$ を使って ID を位数 q の点 $Q_{\mathsf{ID}} \in E/\mathbb{F}_p$ に移す．
Step 2: 秘密鍵 d_{ID} を $d_{\mathsf{ID}} = sQ_{\mathsf{ID}}$ とおく．ここで s はマスターキーである．
Encrypt: 公開鍵 ID のもとで次のように $M \in \mathcal{M}$ を暗号化する．
(1)$\mathsf{MapToPoint}_G$ を用いて ID を位数 q の点 $Q_{\mathsf{ID}} \in E/\mathbb{F}_p$ に写す．
(2)$r \in \mathbb{Z}_q$ をランダムに選ぶ．
(3) 暗号文を次のようにおく．

$$C = \langle rP, M \oplus H(g_{\mathsf{ID}}^r)\rangle$$

ここに，$g_{\mathsf{ID}} = \hat{e}(Q_{\mathsf{ID}}, P_{\rm pub}) \in \mathbb{F}_{p^2}$
Decrypt: $C = \langle U, V\rangle \in C$ を公開鍵 ID を使って作成した暗号文とする．もし $U \in E/\mathbb{F}_p$ が位数 q の点でなかったら，その暗号文を拒絶する．そうでなければ，秘密鍵 d_{ID} を使って次の計算により，C を復号する．

$$V \oplus H(\hat{e}(d_{\mathsf{ID}}, U)) = M$$

まず始めに健全性を証明する．全てが上のように計算できたとき，次のようになっている．
1. 暗号化の際，M は g_{ID} のハッシュと XOR される．
2. 復号の際，V は $\hat{e}(d_{\mathsf{ID}}, U)$ のハッシュと XOR される．

$$\hat{e}(d_{\mathsf{ID}}, U) = \hat{e}(sQ_{\mathsf{ID}}, rP) = \hat{e}(Q_{\mathsf{ID}}, P)^{sr}$$
$$= \hat{e}(Q_{\mathsf{ID}}, sP)^r = \hat{e}(Q_{\mathsf{ID}}, P_{\rm pub})^r = g_{\mathsf{ID}}^r$$

したがって，暗号文に Decrypt を適用すると，もとの平文を復元できる．

BasicIdent は BDH 仮定が成り立つ限り，選択 ID 攻撃付き暗号文単独攻撃に対して一方向性を持つことが，BDH 仮定とランダムオラクルモデルの下で証明できる．

5.4 選択暗号文攻撃に対して安全な ID ベース暗号

BasicIdent に藤崎-岡本 [2] のテクニックを適用して選択暗号文攻撃に対しても強秘匿性を持つ暗号システムを作る．

ここで，藤崎-岡本のテクニックとは次のようなものである．公開鍵 pk のもとで，ランダムビット r を使って平文 M を暗号化したものを $\varepsilon_{pk}(M; r)$ と表すとする．次で定義される ε^{hy} は，ε が一方向性を満たすとき，選択暗号文攻撃に対して強秘匿となる，というものである．ここで，σ はランダムに生成されたもので，H_1, G_1 はハッシュ関数である．

$$\varepsilon_{pk}^{hy}(M) = \varepsilon_{pk}(\sigma; H_1(\sigma, M)) \,||\, G_1(\sigma) \oplus M$$

BasicIdent にこのテクニックを適用すると，システムは次のようになる．
Setup: BasicIdent の手続きに加え，ハッシュ関数 $H_1 : \{0,1\}^n \times \{0,1\}^n \to \mathbb{F}_q$ とハッシュ関数 $G_1 : \{0,1\}^n \to \{0,1\}^n$ を選ぶ．
Extract: BasicIdent と同じようにする．
Encrypt: 公開鍵 ID を用い，平文 $M \in \{0,1\}^n$ を暗号化する．
1. $\mathsf{MapToPoint}_G$ を使って ID を位数 q の点 $Q_{\mathsf{ID}} \in E/\mathbb{F}_p$ に写す．
2. $\sigma \in \{0,1\}^n$ をランダムに選ぶ．
3. $r = H_1(\sigma, M)$ とおく．
4. 暗号文を次のようにおく

$$C = \langle rP, \sigma \oplus H(g_{\mathsf{ID}}^r), G_1(\sigma) \oplus M\rangle$$

ここで，$g_{\mathsf{ID}} = \hat{e}(Q_{\mathsf{ID}}, P_{\rm pub}) \in \mathbb{F}_{p^2}$, $r = H_1(\sigma, M)$.
Decrypt: $C = \langle U, V, W\rangle$ を公開鍵 ID を使って暗号化した暗号文とする．秘密鍵 d_{ID} を使って C を復号するために次のようにする．
1. $V \oplus H(\hat{e}(d_{\mathsf{ID}}, U)) = \sigma$ を計算する．
2. $W \oplus G_1(\sigma) = M$ を計算する．
3. $r = H_1(\sigma, M)$ とおく．$U = rP$ となるか試し，もし違ったら暗号文を拒絶する．
4. M を C の復号として出力する．

6 まとめと今後の課題

Weil Pairing を使った ID ベース暗号の仕組と安全性などを紹介し，C 言語による実装を行った．今後は最近活発に研究されている ID ベース暗号の具体的な応用について，新たな試みを行いたい．また，新しい効率的なペアリングの探求も行いたい．

参考文献

[1] Dan Boneh, Matt Franklin, *Identity-Based Encryption from the Weil Pairing*, Springer-Verlag, pp.213-229, 2001.
[2] E. Fujisaki and T. Okamoto, “Secure integration of asymmetric and symmetric encryption scheme”, Springer-Verlag, pp.537-554, 1999.
[3] L. C. Washington, *Elliptic Curves, Number Theory and Cryptography*, CHAPMAN &HALL/CRC.
[4] Yasuyuki MURAKAMI, Ryuichi SAKAI, Masao KASAHARA, *A New Probabilistic ID-Based Non-interactive Key Sharing Scheme*, IEICE Transaction Vol.E83-A No.1 pp.2-9, 2000.
[5] I.F.Blake, G.Seroussi, N.P.Smart, *Elliptic Curves in Cryptography*, Cambridge Univ Pr.