

## 1 定義

$E$  を  $y^2 = x^3 + 1$  で定義される  $F_q$  上の楕円曲線とする、ここで  $q \equiv 2 \pmod{3}$  とする。 $E[n]$  を  $E[n] = \{P \in E(\overline{F_q}) : [n]P = \infty\}$  として定義する、ここで  $\overline{F_q}$  は  $F_q$  の代数的閉包。 $\omega \in F_{q^2}$  を 1 の原始三乗根とする。以下のようにして distortion map を定義する:

$$\phi : E(F_{q^2}) \rightarrow E(F_{q^2}), (x, y) \mapsto (\omega x, y), \phi(\infty) = \infty$$

以下のようにして modified Weil pairing を定義する:

$$\tilde{e}_n(P_1, P_2) = e_n(P_1, \phi(P_2))$$

ここで  $e_n$  は Weil pairing、 $P_1, P_2 \in E[n]$

## 2 ID ベース暗号

1.  $q = 6l - 1$  をみたす素数  $q$  を選ぶ
2.  $E(F_q)$  内から位数  $l$  をもつ点  $P$  を選ぶ
3.  $H_1$  を、インプットとして任意の長さの 2 進数文字列を受け取り、アウトプットとして位数  $l$  をもつ  $E$  上の点を返すハッシュ関数とする。 $H_2$  を、インプットとして位数  $l$  をもつ  $F_{q^2}^\times(F_{q^2})$  の単元からなる集合) の元を受け取り、アウトプットとして長さ  $n$  の 2 進数文字列を返すハッシュ関数とする、ここで  $n$  は平文の長さ
4. 乱数  $s \in F_l^\times$  を選び、 $P_{pub} = sP$  を計算する
5.  $q, H_1, H_2, n, P, P_{pub}$  を公開し、 $s$  を秘密にする

ID として文字列  $ID$  をもつユーザーが秘密鍵を欲しい場合、信頼できる第三者が以下を行う。

1.  $Q_{ID} = H_1(ID)$  を計算する
2.  $D_{ID} = sQ_{ID}$  を計算する
3.  $D_{ID}$  をそのユーザーに渡す

アリスが平文  $M$  をボブに送りたい場合、アリスは以下を行う。

1. ボブの ID が  $ID$  である場合、 $Q_{ID} = H_1(ID)$  を計算する
2. 乱数  $r \in F_l^\times$  を選ぶ
3.  $g_{ID} = \tilde{e}_l(Q_{ID}, P_{pub})$  を計算する
4. 暗号文を以下のように定義する:

$$c = (rP, M \oplus H_2(g_{ID}^r))$$

ボブが暗号文  $(u, v)$  を復号化したい場合、ボブは以下を行う。

1. 秘密鍵  $D_{ID}$  を使用して、 $h_{ID} = \tilde{e}_l(D_{ID}, u)$  を計算する
2.  $m = v \oplus H_2(h_{ID})$  を計算する

$m$  が復号文となる。

## 参考文献

- [1] Lawrence C. Washington. Elliptic Curves Number Theory and Cryptography, Second Edition
- [2] J.H. Silverman, Jill Pipher, Jeffrey Hoffstein. An Introduction to Mathematical Cryptography
- [3] Craig Costello. Pairings for beginners.
- [4] Ben Lynn. ON THE IMPLEMENTATION OF PAIRING-BASED CRYPTOSYSTEMS.
- [5] R. W. Mak. Identity-based encryption using supersingular curves with the Weil pairing.