6.8 A Cryptosystem Based on Weil Pairing
ID-based Cryptosystem

Rong-Jaye Chen

Department of Computer Science, National Chiao Tung University

ECC 2008
Outline

1. ID-based cryptosystem
   - Certificate-based cryptosystem
   - ID-based encryption scheme

2. Weil pairing

3. Modified Weil pairing

4. PKG (TA in the textbook)

5. Encryption and decryption
ID-based cryptosystem

**Private Key Generator (PKG)**

- Setup: generate params and master key
- Authentication (ID$_{Bob}$)

**Extract**
- generate $KR_{IDBob}$ by $ID_{Bob}$ and master key

**Alice**
- Encrypt
- (params, $ID_{Bob}$)
- Verify

**Bob**
- Decrypt
- Sign
- $KR_{IDBob}$

**ID$_{Bob}$ is arbitrary and meaningful**
- ex: Bob@hotmall.com
- or 0912345678
Certificate-based cryptosystem

Certificate Authority (CA)

Certificate(Bob, $K_{U_{Bob}}$) → Authentication ($K_{U_{Bob}}$)

Bob

Encrypt

$K_{U_{Bob}}$

Alice

Verify

Decrypt

$K_{R_{Bob}}$

$K_{U_{Bob}}$ is random
ID-based encryption scheme - (1)

- Proposed by Boneh and Franklin (Crypto 2001)
  - First complete and efficient scheme

- Bilinear pairing

  \[ G_1 : \text{additive group generated by } P, \ \text{ord}(P) = q \]
  \[ G_2 : \text{multiplicative group with same order } q \]

  Assume the DLP in \( G_1 \) and \( G_2 \) are hard

  Let \( e : G_1 \times G_1 \rightarrow G_2 \) satisfies:
  1. Bilinear: \[ e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q), \]
     \[ e(P, Q_1 + Q_2) = e(P, Q_1)e(P, Q_2) \]
  2. Non-degenerate: \( \exists P, Q \in G_1 \), such that \( e(P, Q) \neq 1 \)
  3. Computability

- Bilinear Diffie-Hellman (BDH) Assumption

  Given \( P, aP, bP, cP \in G_1 \), compute \( e(P, P)^{abc} \) is HARD!
ID-based encryption scheme - (2)

ID-based encryption

Setup

1. Choose \( P \in E/F_p \) of order \( q \)
2. Pick a random \( s \in \mathbb{Z}_q^* \) and set \( P_{pub} = sP \)
3. Two hash functions:
   - \( H_1 : \{0, 1\}^* \to G_1^* \) (MapToPoint)
   - \( H_2 : G_2 \to \{0, 1\}^n \) for some \( n \)

Extract

- Given a \( ID \in \{0, 1\}^* \), build private key \( S_{ID} \) as follows:
  \[
  Q_{ID} = H_1(ID)
  \]

  Set \( d_{ID} = sQ_{ID} \), where \( s \) is the master key
ID-based encryption scheme - (3)

Encrypt

- Use MapToPoint to map $ID$ to $Q_{ID}$
- Choose a random $r \in \mathbb{Z}_q^*$
- $C = < rP, M \oplus H_2( e(Q_{ID}, P_{pub})^r ) >$

Decrypt

- Let $C = < U, V >$, if $U$ is not a point of order $q$ then reject
- $M = V \oplus H_2(e(d_{ID}, U))$

$$e(d_{ID}, U) = e(sQ_{ID}, rP) = e(Q_{ID}, P)^{sr} = e(Q_{ID}, sP)^r = e(Q_{ID}, P_{pub})^r$$
Weil pairing

- Define Weil pairing

\[ e : E[m] \times E[m] \rightarrow U_m \]

where \( E[m] = \{ P \mid mP = O, P \in E \} \) is called the \( m \)-torsion group, \( U_m \) is the group of the \( m \)th roots of unity.

Given \( P, Q \in E[m] \), \( \exists D_P, D_Q \in Div^0 \) such that

\[ D_P \sim (P) - (O) \quad \text{and} \quad D_Q \sim (Q) - (O) \]

Also, \( \exists f_P, f_Q \) such that \( div(f_P) = mD_P \) and \( div(f_Q) = mD_Q \)

Suppose \( \text{supp}(D_P) \cap \text{supp}(D_Q) = \emptyset \)

Then

\[ e(P, Q) = \frac{f_P(D_Q)}{f_Q(D_P)} \]
Modified Weil pairing

- $E/F_P : y^2 = x^3 + 1$, $p \equiv 2 \pmod{3}$
- $\omega \in F_{p^2} :$ a primitive 3rd root of 1

$\beta : E(F_{p^2}) \rightarrow E(F_{p^2}), \quad (x, y) \mapsto (\omega x, y), \quad \infty \mapsto \infty$

Suppose $ord(P) = n$. Then $ord(\beta(P)) = n$

Define the Modified Weil pairing

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

$e_n$ is the usual Weil pairing and $P_1, P_2 \in E[n]$

$\therefore E$ is supersingular $\therefore |E(F_p)| = p + 1$

We add the further assumption that $p = 6l - 1$ for some prime $l$. Then $6P$ has order $l$ or 1 for each $P \in E(F_p)$
PKG (TA in the textbook)

1. Chooses a large prime \( p = 6l - 1 \)
2. Chooses \( P \) of order \( l \) in \( E(F_p) \)
3. Chooses hash functions \( H_1 \) and \( H_2 \)
   \[
   H_1(\text{a string}) \rightarrow \text{a point of order } l \text{ on } E \\
   H_2(\text{an element of order } l \text{ in } F_p^*) \rightarrow \text{a string of length } n
   \]
4. Chooses a secret random \( s \in F_l^* \) and computes \( P_{pub} = sP \)
5. Makes \( p, H_1, H_2, n, P, P_{pub} \) public, while keeping \( s \) secret
PKG does for a user with identity $ID$

1. Computes $Q_{ID} = H_1(ID)$ . This is a point on $E$
2. Sends $D_{ID} = sQ_{ID}$ to this user.
Encryption and decryption

Alice wants to send a message $M$ to Bob

1. Looks up Bob’s identity, eg. $ID = \text{bob@computer.com}$ (written as a binary string) and computes $Q_{ID} = H_1(ID)$

2. Chooses a random $r \in F_{l}^*$

3. Computes $g_{ID} = \tilde{e}(Q_{ID}, P_{pub})$

4. Lets the ciphertext be

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

Bob decrypts a ciphertext $(u, v)$

1. Uses his private key $D_{ID}$ to compute

   $$h_{ID} = \tilde{e}(D_{ID}, u)$$

2. Computes $m = v \oplus H_2(h_{ID})$
Correctness of decryption

- The decryption works

\[\tilde{e}(D_{ID}, u) = \tilde{e}(sQ_{ID}, rP) = \tilde{e}(Q_{ID}, P)^{sr} = \tilde{e}(Q_{ID}, P_{pub})^r = g_{ID}^r\]

\[\therefore m = v \oplus H_2(\tilde{e}(D_{ID}, u)) = (M \oplus H_2(g_{ID}^r)) \oplus H_2(g_{ID}^r) = M\]