Identity-Based Cryptosystems and Quadratic Residuosity

Marc Joye

Proxy: Fabrice Benhamouda

PKC 2016 · Tapei, Taiwan

Identity-Based Encryption

Definition

An identity-based encryption scheme is a set of 4 algorithms

1. Setup
   - Input: security parameter κ
   - Output: master public/secret key mpk/msk

Identity-Based Encryption

Definition

An identity-based encryption scheme is a set of 4 algorithms

1. Setup
   - Input: security parameter κ
   - Output: master public/secret key mpk/msk
2. Encryption
   - Input: master public key mpk, identity id, message m
   - Output: $C = \mathscr{E}(mpk, id, m)$

Identity-Based Encryption

Definition

An identity-based encryption scheme is a set of 4 algorithms

1. Setup
   - Input: security parameter κ
   - Output: master public/secret key mpk/msk
2. Encryption
   - Input: master public key mpk, identity id, message m
   - Output: $C = \mathscr{E}(mpk, id, m)$
3. Key derivation
   - Input: identity id, master secret key msk
   - Output: user's private key usk

Identity-Based Encryption

Definition

An identity-based encryption scheme is a set of 4 algorithms

1. Setup
   - Input: security parameter κ
   - Output: master public/secret key mpk/msk
2. Encryption
   - Input: master public key mpk, identity id, message m
   - Output: $C = \mathscr{E}(mpk, id, m)$
3. Key derivation
   - Input: identity id, master secret key msk
   - Output: user's private key usk
4. Decryption
   - Input: decryption key usk, ciphertext C
   - Output: $m = \mathscr{D}(usk, C)$

This Talk

- Study of Cocks IBE scheme
  - Clifford Cocks (mathematician, GCHQ)

Our Main Contribution

Discovery of the algebraic structure underlying Cocks encryption

- better understanding of its properties and its security
- new applications

Outline

1. Cocks IBE Scheme
2. Algebraic Structure
3. Applications
4. Conclusion

Preliminaries

If p prime number, $a \in \mathbb{F}_p$, Legendre symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \mod p \\ 1 & \text{if } a \text{ is a square } (a = b^2 \bmod p) \\ -1 & \text{else} \end{cases}$$

Preliminaries

If p prime number, $a \in \mathbb{F}_p$, Legendre symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \mod p \\ 1 & \text{if } a \text{ is a square } (a = b^2 \bmod p) \\ -1 & \text{else} \end{cases}$$

If $N = pq$ RSA modulus, $a \in \mathbb{Z}_N$, Jacobi symbol:

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{q}\right)$$

(efficiently computable)

Preliminaries

If p prime number, $a \in \mathbb{F}_p$, Legendre symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \mod p \\ 1 & \text{if } a \text{ is a square } (a = b^2 \bmod p) \\ -1 & \text{else} \end{cases}$$

If $N = pq$ RSA modulus, $a \in \mathbb{Z}_N$, Jacobi symbol:

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{q}\right)$$

(efficiently computable)

$$a \text{ is a square mod } N \iff \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$$

Preliminaries

If p prime number, $a \in \mathbb{F}_p$, Legendre symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \mod p \\ 1 & \text{if } a \text{ is a square } (a = b^2 \bmod p) \\ -1 & \text{else} \end{cases}$$

If $N = pq$ RSA modulus, $a \in \mathbb{Z}_N$, Jacobi symbol:

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{q}\right)$$

(efficiently computable)

$$a \text{ is a square mod } N \iff \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1 \implies \left(\frac{a}{N}\right) = 1$$

Cocks Cryptosystem

- First pairing-free IBE scheme (2001)
  - works in standard RSA groups
  - semantically secure under QR assumption (in the ROM)

Quadratic Residuosity Assumption

Let $N = pq$ be an RSA-type modulus. The distributions of

$$\mathbb{J}_N = \left\{ a \in \mathbb{Z}_N^\times \mid \left(\tfrac{a}{N}\right) = 1 \right\} \text{ and } \mathbb{QR}_N = \left\{ a \in \mathbb{Z}_N^\times \mid \left(\tfrac{a}{p}\right) = \left(\tfrac{a}{q}\right) = 1 \right\}$$

are indistinguishable

Cocks Cryptosystem (cont'd)

Setup $mpk = \{N, u, \mathcal{H}\}, \quad msk = \{p, q\}$ where:

- $N = pq$ an RSA modulus
- $u \in \mathbb{J}_N \setminus \mathbb{QR}_N$
- $\mathcal{H} \colon \{0,1\}^* \to \mathbb{J}_N$ hash function (RO)

Key derivation compute $D_{id} = \mathcal{H}(id)$ and returns

$$usk = \delta_{id} = \begin{cases} (D_{id})^{1/2} & \text{if } D_{id} \in \mathbb{QR}_N \\ (uD_{id})^{1/2} & \text{if } D_{id} \in \mathbb{J}_N \setminus \mathbb{QR}_N \end{cases}$$

Remark: Original cryptosystem defined with $p, q \equiv 3 \pmod 4$ and $u = -1$

Cocks Cryptosystem (cont'd)

Setup $mpk = \{N, u, \mathcal{H}\}, \quad msk = \{p, q\}$ where:

- $N = pq$ an RSA modulus
- $u \in \mathbb{J}_N \setminus \mathbb{QR}_N$
- $\mathcal{H}\colon \{0,1\}^* \to \mathbb{J}_N$ hash function (RO)

Key derivation compute $D_{id} = \mathcal{H}(id)$ and returns

$$usk = \delta_{id} = \begin{cases} (D_{id})^{1/2} & \text{if } D_{id} \in \mathbb{QR}_N \\ (uD_{id})^{1/2} & \text{if } D_{id} \in \mathbb{J}_N \setminus \mathbb{QR}_N \end{cases}$$

Remark: Original cryptosystem defined with $p, q \equiv 3 \pmod 4$ and $u = -1$

Cocks Cryptosystem (cont'd)

mpk

Alice

message $m \in \{-1, 1\}$

$t \quad \in_R \mathbb{Z}_N$ s.t.

$$\left(\frac{t}{N}\right) = m$$

$$c = t + \frac{\mathcal{H}(id)}{t} \bmod N \quad \xrightarrow{C=(c\quad)}$$

Bob

$\delta_{id} = \mathcal{H}(id)^{1/2} \bmod N$

$$\gamma = c$$

$$m = \left(\frac{\gamma + 2\delta_{id}}{N}\right)$$

Cocks Cryptosystem (cont'd)

mpk

Alice

message $m \in \{-1, 1\}$

$t, \bar{t} \in_R \mathbb{Z}_N$ s.t.

$$\left(\frac{t}{N}\right) = \left(\frac{\bar{t}}{N}\right) = m$$

$$c = t + \frac{\mathcal{H}(id)}{t} \bmod N$$

$$\bar{c} = \bar{t} + \frac{u\mathcal{H}(id)}{\bar{t}} \bmod N$$

$$\xrightarrow{C=(c,\bar{c})}$$

Bob

$\delta_{id} = \mathcal{H}(id)^{1/2} \bmod N$

or $\delta_{id} = (u\mathcal{H}(id))^{1/2} \bmod N$

$\gamma = c$ or $\bar{c}$

$$m = \left(\frac{\gamma + 2\delta_{id}}{N}\right)$$

Outline

Pell Curve

- Consider the Pell curve given by the Pell equation

$$x^2 - \Delta y^2 = 1$$

over $\mathbb{F}_p$, where $\Delta = \delta^2 \in \mathbb{F}_p^\times$

Pell Curve

- Consider the Pell curve given by the Pell equation

$$x^2 - \Delta y^2 = 1$$

  over $\mathbb{F}_p$, where $\Delta = \delta^2 \in \mathbb{F}_p^\times$
- Set of points (x, y) on the Pell curve
    - forms a group $\mathscr{C}(\mathbb{F}_p)$
    - order $p - 1$
    - neutral element: $\mathcal{O} = (0, 1)$

Pell Curve

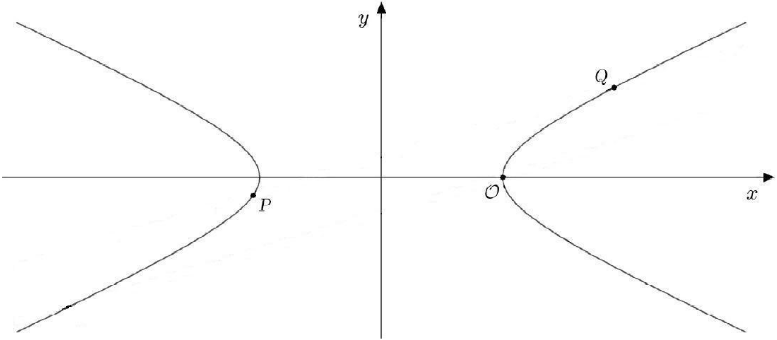
- Consider the Pell curve given by the Pell equation

$$x^2 - \Delta y^2 = 1$$

  over $\mathbb{F}_p$, where $\Delta = \delta^2 \in \mathbb{F}_p^\times$
- Set of points (x, y) on the Pell curve
  - forms a group $\mathscr{C}(\mathbb{F}_p) \cong \mathbb{F}_p^\times$
  - order $p - 1$
  - neutral element: $\mathcal{O} = (0, 1)$

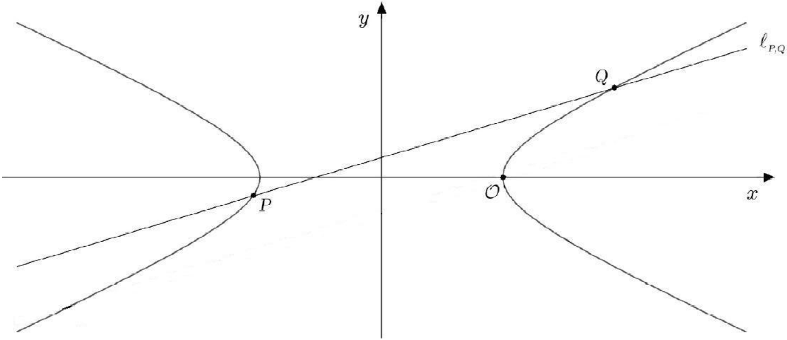
Group Law

- Geometric interpretation



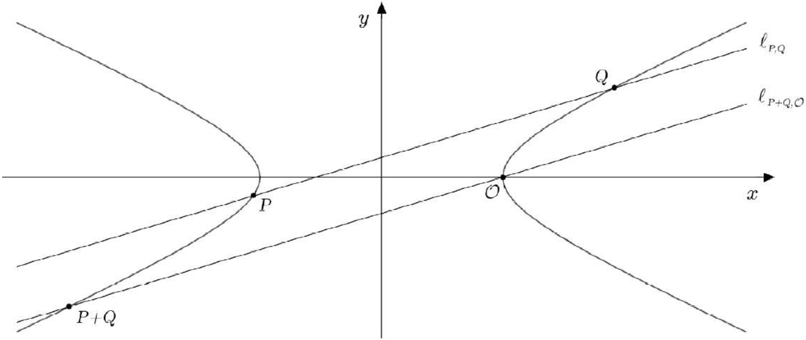
Group Law

- Geometric interpretation



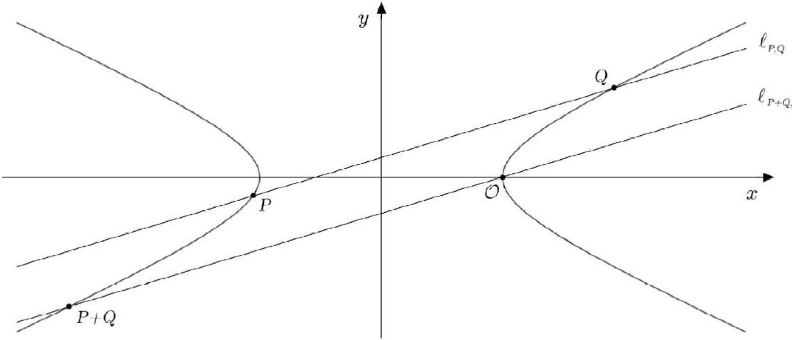
Group Law

- Geometric interpretation



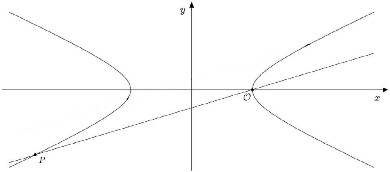
Group Law

- Geometric interpretation



- Algebraically: $(x_1, y_1) \oplus (x_2, y_2) = (x_1x_2 + \Delta y_1y_2, x_1y_2 + x_2y_1)$

Compact Representation



- Slope
  - line through $\boldsymbol{P}$ and $\mathcal{O}$: $y = s(x-1)$
  - for efficiency, let $t := \Delta s = \frac{\Delta y}{x-1}$

$$\psi : \mathbb{F}_p \cup \{\infty\} \to \mathscr{C}(\mathbb{F}_p), \begin{cases} t \mapsto \boldsymbol{P} = \left(\frac{t^2+\Delta}{t^2-\Delta}, \frac{2t}{t^2-\Delta}\right) \\ \infty \mapsto \mathcal{O} \end{cases}$$

Remark: ψ not defined at $\pm\delta$ when $\Delta \in \mathbb{QR}_p$

The Group $\mathcal{Z}_{N,\Delta}$

- We recall that $\Delta = \delta^2 \in \mathbb{QR}_p$
- Define the group $(\mathcal{F}_{p,\Delta}, \circledast)$ with neutral element ∞, where

$$
\begin{aligned}
\mathcal{F}_{p,\Delta} &= (\mathbb{F}_p \setminus \{\pm\delta\}) \cup \{\infty\} \\
&= \{\psi^{-1}(\boldsymbol{P}) \mid \boldsymbol{P} \in \mathscr{C}(\mathbb{F}_p)\} \\
&= \{t \in \mathbb{F}_p \mid t^2 \neq \Delta\} \cup \{\infty\}
\end{aligned}
$$

under the law $\circledast$: $t_1 \circledast t_2 = \dfrac{t_1 t_2 + \Delta}{t_1 + t_2}$

The Group $\mathcal{Z}_{N,\Delta}$

- We recall that $\Delta = \delta^2 \in \mathbb{QR}_p$
- Define the group $(\mathcal{F}_{p,\Delta}, \circledast)$ with neutral element ∞, where

$$\begin{aligned}\mathcal{F}_{p,\Delta} &= (\mathbb{F}_p \setminus \{\pm\delta\}) \cup \{\infty\} \\ &= \{\psi^{-1}(\boldsymbol{P}) \mid \boldsymbol{P} \in \mathscr{C}(\mathbb{F}_p)\} \\ &= \{t \in \mathbb{F}_p \mid t^2 \neq \Delta\} \cup \{\infty\} \cong \mathbb{F}_p^{\times}\end{aligned}$$

under the law $\circledast$: $t_1 \circledast t_2 = \dfrac{t_1 t_2 + \Delta}{t_1 + t_2}$

The Group $\mathcal{Z}_{N,\Delta}$

- We recall that $\Delta = \delta^2 \in \mathbb{QR}_p$
- Define the group $(\mathcal{F}_{p,\Delta}, \circledast)$ with neutral element ∞, where

$$\begin{aligned} \mathcal{F}_{p,\Delta} &= (\mathbb{F}_p \setminus \{\pm\delta\}) \cup \{\infty\} \\ &= \{\psi^{-1}(\boldsymbol{P}) \mid \boldsymbol{P} \in \mathscr{C}(\mathbb{F}_p)\} \\ &= \{t \in \mathbb{F}_p \mid t^2 \neq \Delta\} \cup \{\infty\} \cong \mathbb{F}_p^\times \end{aligned}$$

under the law $\circledast$: $t_1 \circledast t_2 = \dfrac{t_1 t_2 + \Delta}{t_1 + t_2}$

- By Chinese remaindering, for $N = pq$, consider

$$\mathcal{Z}_{N,\Delta} := \mathcal{F}_{p,\Delta} \times \mathcal{F}_{q,\Delta} \cong \mathbb{Z}_N^\times$$

The Subgroup of Squares in $\mathcal{Z}_{N,\Delta}$

Main Observation

(Up to a factor of 2) Cocks ciphertexts are *squares* in $\mathcal{Z}_{N,\Delta}$, where $\Delta = \mathcal{H}(id) \in \mathbb{QR}_N$ [or $\Delta = u\mathcal{H}(id) \in \mathbb{QR}_N$]

- $t_1 \circledast t_2 = \dfrac{t_1 t_2 + \Delta}{t_1 + t_2}$

$$\Longrightarrow \quad t \circledast t = \frac{t^2 + \mathcal{H}(id)}{2t} = \frac{1}{2} \cdot \left(t + \frac{\mathcal{H}(id)}{t} \right) = \frac{c}{2}$$

and likewise, $\bar{t} \circledast \bar{t} = \frac{\bar{t}^2 + u\mathcal{H}(id)}{2\bar{t}} = \frac{1}{2} \cdot \left(\bar{t} + \frac{u\mathcal{H}(id)}{\bar{t}} \right) = \frac{\bar{c}}{2}$

Outline

Re-Randomizing Cocks Ciphertexts

For simplicity, we suppose $\mathcal{H}(id) \in \mathbb{QR}_N \implies \Delta = \mathcal{H}(id)$

- Let message $m = (-1)^b \in \{\pm 1\}$
- Corresponding ciphertext is $c = t + \frac{\Delta}{t}$ with $\left(\frac{t}{N}\right) = m$
- Choosing a random t' and computing $c' = t' + \frac{\Delta}{t'}$, we have

$$\frac{c^*}{2} := \frac{c}{2} \circledast \frac{c'}{2} \equiv \frac{c}{2} \iff \left(\frac{c + c'}{N}\right) = 1$$

$\implies$ t' should be chosen s.t. $\left(\frac{c+c'}{N}\right) = 1$ to get a ciphertext c^* equivalent to c

Computing over Cocks Ciphertexts

For simplicity, we suppose $\mathcal{H}(id) \in \mathbb{QR}_N \implies \Delta = \mathcal{H}(id)$

- Let messages $m_1 = (-1)^{b_1}$ and $m_2 = (-1)^{b_2} \in \{\pm 1\}$
- Define message $m_3 := m_1 \cdot m_2 = (-1)^{b_1 \oplus b_2}$
- Corresponding ciphertexts are denoted c_1, c_2, and c_3

- Then

$$\frac{c_3'}{2} := \frac{c_1}{2} \circledast \frac{c_2}{2} \equiv \frac{c_3}{2} \iff \left(\frac{c_1 + c_2}{N}\right) = 1$$

If necessary, re-randomize e.g. c_1 until above condition is met

Computing over Cocks Ciphertexts

Cocks cryptosystem is homomorphic

- w.r.t. multiplication for messages in $\{\pm 1\}$
- w.r.t. $\oplus$ for messages in $\{0, 1\}$

Making Cocks Ciphertexts Anonymous

- Galbraith: Cocks ciphertext are not anonymous
- With our notation

Proposition

Let $w \in \mathcal{Z}_{N,\Delta}$. If

$$\left(\frac{w^2 - \Delta}{N}\right) = -1$$

then w is not a square in $\mathcal{Z}_{N,\Delta}$

$\implies$ If a ciphertext c satisfies $\left(\frac{(c/2)^2 - \mathcal{H}(id)}{N}\right) = -1$ then it is not for user with identity *id*

Making Cocks Ciphertexts Anonymous

$\circledast$-multiply with probability $1/2$ the value of $\frac{c}{2}$ with an element $\frac{d}{2}$ satisfying $\left(\frac{(d/2)^2-\Delta}{N}\right) = -1$

- At decryption time, legitimate recipient can $\circledast$-divide by $\frac{d}{2}$ in case ciphertext were $\circledast$-multiplied by $\frac{d}{2}$
- Application: Public-key encryption with keyword search (PEKS)

Outline

Summary

- Description of algebraic structure underlying Cocks encryption
- Better understanding of Cocks cryptosystem
- Applications:
  - homomorphic computations
  - anonymous encryption
- (More results in the paper)

Cocks cryptosystem is homomorphic

Comments/Questions?

http://joye.site88.net/