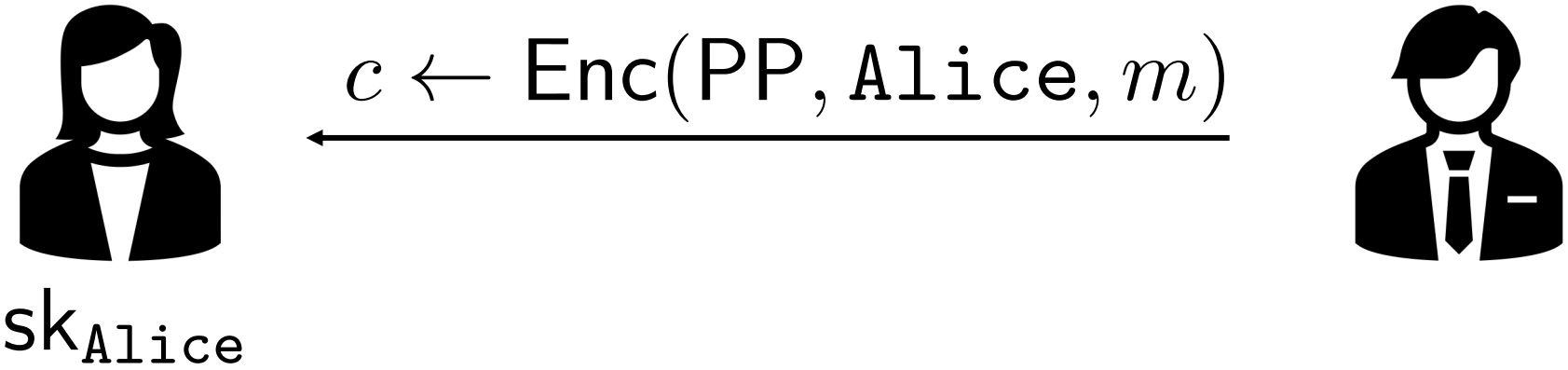
Failing to Generalize Cocks' IBE

Mark Zhandry
NTT Research

Identity-Based Encryption (IBE)

[Shamir'84]



Cocks' IBE

[Cocks'01]

$$\mathsf{PP} = N \;\; (= p \cdot q)$$

$$\mathsf{sk}_{\texttt{Alice}} = x \text{ such that } x^2 = H(\texttt{Alice}) \bmod N$$

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

$$\mathsf{Enc}(\mathsf{PP}, \texttt{Alice}, m) = \frac{4t^2 + H(\texttt{Alice})}{4t} \text{ where } \underbrace{\left(\frac{t}{N}\right)}_{\text{Jacobi symbol}} = m$$

$$\mathsf{Dec}(\mathsf{PP}, x, c) = \left(\frac{c + x}{N}\right)$$

Correctness of Cocks' IBE

[Cocks'01]

$$c + x = \frac{4t^2 + H(\texttt{Alice})}{4t} + x = \frac{4t^2 + 4tx + x^2}{4t} = \frac{(t + x/2)^2}{t}$$

$$\left(\frac{c + x}{N}\right) = \left(\frac{t + x/2}{N}\right)^2 \left(\frac{t}{N}\right)^{-1} = \left(\frac{t}{N}\right) = m$$

Cocks' IBE

[Cocks'01]

$$\mathsf{PP} = N \ \ (= p \cdot q)$$

$$\mathsf{sk}_{\texttt{Alice}} = x \text{ such that } x^2 = H(\texttt{Alice}) \bmod N$$

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

$$\mathsf{Enc}(\mathsf{PP}, \texttt{Alice}, m) = \frac{4t^2 + H(\texttt{Alice})}{4t} \text{ where } \left(\frac{t}{N}\right) = m$$

$$\mathsf{Dec}(\mathsf{PP}, x, c) = \left(\frac{c + x}{N}\right)$$

Can think of Cocks' IBE as encrypting to $x^2 - H(\texttt{Alice})$

Our Goal

$\mathsf{PP} = N \ \ (= p \cdot q)$

$k > 2$

$\mathsf{sk}_{\texttt{Alice}} = x \text{ such that } x^k = H(\texttt{Alice}) \bmod N$

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

$\mathsf{Enc}(\mathsf{PP}, \texttt{Alice}, m) = ???$

Keep “linear” decryption

$$\mathsf{Dec}(\mathsf{PP}, x, c) = \left(\frac{c + x}{N} \right)$$

That is, encrypt to roots of polynomial $x^k - H(\texttt{Alice})$

Why Higher-Order Roots?

1

Encrypt to $(x^2 - H(\texttt{Alice}))(x^2 - H(\texttt{Bob}))(x^2 - H(\texttt{Charlie}))$

➡ Broadcast encryption

2

Can't obliviously hash into quadratic residues

➡ with Cocks' scheme, half of users will have no secret keys

With cube roots, for appropriate N, all users have secret keys

3

Cocks' scheme = very interesting technique, worthy of exploration

Related Work: [Boneh-LaVigne-Sabin'13]

$$\mathsf{PP} = N \ \ (= p \cdot q)$$

$$\mathsf{sk}_{\texttt{Alice}} = x \text{ such that } x^k = H(\texttt{Alice}) \bmod N$$

$m \in \mathbb{F}_k$

$$\mathsf{Dec}(\mathsf{PP}, x, c) = \left(\frac{c(x)}{N}\right)_k$$

Degree $k-1$ poly described in ctxt

kth power residue symbol

Our Scheme for Cube Roots

$$a = H(\texttt{Alice})$$

$$\mathsf{sk}_{\texttt{Alice}} = x \text{ such that } x^3 = a \bmod N$$

$$\mathsf{Enc}(\mathsf{PP}, \texttt{Alice}, m) = \frac{t(t^3 - 8a)}{4(t^3 + a)} \bmod N$$

$$\text{where } \left(\frac{t^3 + a}{N}\right) = m$$

Correctness of Our Scheme

$$\left(\frac{c+x}{N}\right) = \left(\frac{(t^2+2tx-2x^2)^2 2^{-2}(t^3+a)^{-1}}{N}\right) = \left(\frac{t^3+a}{N}\right) = m$$

Dream theorem?: There exists a secure generalization of Cocks' IBE to encrypt any polynomial

Proof by example? Perfect protocols for degree 2,3

This Work

Theorem 1: For relatively prime constants k, e, any $(k, e)-$ scheme is insecure

Def of $(k, e)-$ scheme:

$$\mathsf{Dec}(\mathsf{PP}, x, c) = \left(\frac{f(x)}{N}\right)_e$$

f a polynomial derived from c

x any root of public degree-k poly $s(\cdot)$

Theorem 2: No "natural" correct schemes with decryption $\left(\frac{c+x}{N}\right)$ for degree ≥ 4

Theorem 1: For rel. prime k, e, any (k, e)–scheme is insecure

Proof: $f(\alpha_1)f(\alpha_2)\cdots f(\alpha_k)$ symmetric in $\alpha_1, \cdots, \alpha_k$

➡ Write as poly $F(e_1, \cdots, e_k)$ where e_j are elementary symmetric polys in $\alpha_1, \cdots, \alpha_k$

Let $\alpha_1, \cdots, \alpha_k$ be (unknown) roots of $s(\cdot)$

➡ e_j are derived from coefficients of $s(\cdot)$

➡ Can compute $F(e_1, \cdots, e_k) = f(\alpha_1)f(\alpha_2)\cdots f(\alpha_k)$ from public information

Theorem 1: For rel. prime k, e, any $(k, e)-$scheme is insecure

Proof:

$$\left(\frac{F(e_1, \cdots, e_k)}{N}\right)_e^{k^{-1} \bmod e} = \left(\frac{f(\alpha_1) \cdots f(\alpha_k)}{N}\right)_e^{k^{-1} \bmod e}$$

$$= \left(\left(\frac{f(\alpha_1)}{N}\right)_e \cdots \left(\frac{f(\alpha_k)}{N}\right)_e\right)^{k^{-1} \bmod e}$$

$$= \left(m^k\right)^{k^{-1} \bmod e}$$

$$= m$$

Theorem 1: For rel. prime k, e, any (k, e)–scheme is insecure

Example: Our scheme

$$\left(\frac{c^3 + H(\texttt{Alice})}{N} \right) = m$$

Theorem 2: No "natural" correct scheme for degree ≥ 4

Proof: Natural scheme:

$$c + X = v \times g(X)^2 \bmod (X^k - a)$$

where $a = H(\texttt{Alice})$

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

v, g secret, chosen by encrypter

c, v, coefs of g are rational funcs in underlying randomness and a

Theorem 2: No "natural" correct scheme for degree ≥ 4

Proof: Case $k = 4$

Recall $c + X = v \times g(X)^2 \bmod (X^k - a)$

Write $g(X) = g_0 + g_1 X + g_2 X^2 + g_3 X^3$

➡ Need $g(X)^2 \bmod (X^4 - a)$ to be linear

➡

$$2g_0 g_2 + g_1^2 + a g_3^2 = 0$$
$$g_1 g_2 + g_0 g_3 = 0$$

Theorem 2: No "natural" correct scheme for degree ≥ 4

Proof: $2g_0g_2 + g_1^2 + ag_3^2 = 0 \qquad g_1g_2 + g_0g_3 = 0$

$$\Rightarrow \quad 2\left(-\frac{g_1g_2}{g_3}\right)g_2 + g_1^2 + ag_3^2 = 0$$

$$\Rightarrow \quad -2g_1g_2^2 + g_1^2g_3 + ag_3^3 = 0$$

Now write $x = g_1/g_3 \qquad y = g_1g_2/g_3^2$

$$\Rightarrow \quad (-2y^2/x + x^2 + a)g_3^2 = 0$$

$$\Rightarrow \quad y^2 = x^3/2 + ax/2$$

Theorem 2: No "natural" correct scheme for degree ≥ 4

Proof:

$$y^2 = x^3/2 + ax/2$$

Elliptic curve with no-zero discriminant

x, y rational functions of underlying randomness
i.e. rational parameterization of curve

Impossible!

Recap

Theorem 1: For relatively prime constants k, e, any (k, e)– scheme is insecure

Theorem 2: No "natural" correct schemes with decryption $\left(\frac{c+x}{N}\right)$ for degree ≥ 4

No natural $(k, 2)$-scheme with one ciphertext component other than Cocks scheme

Moving to higher e just seems to make things harder

Future Directions?

Use higher-degree decryption?

Use more than 1 ctxt component?