Failing to Generalize Cocks' IBE

Mark Zhandry
NTT Research
mzhandry@gmail.com

Abstract

In Cocks' IBE, users' secret keys are solutions to quadratic equations. We attempt to generalize Cocks' IBE to the case where users' secret keys are the roots of higher-degree polynomials. Using higher-order roots could allow for some improvements over Cocks' IBE, such as reducing the number of ciphertext components from two to one, or generalizing to broadcast encryption. We show a solution that is correct for degree 3. However, we show that analogous generalizations to even higher degrees are likely impossible. Even worse, we show that our degree 3 scheme is insecure, despite being a natural generalization of Cocks' degree 2 scheme. The attack we develop applies to a wide range of generalizations of Cocks' IBE.

1 Introduction

Cocks' IBE [Coc01] is an elegant IBE proposal based on the hardness of factoring, and along with the IBE of Boneh and Franklin [BF01] is one of the first two IBE schemes discovered. However, unlike pairings that were popularized by [BF01] and became ubiquitous in cryptography, the techniques underlying Cocks' IBE have received comparatively little follow-up work. In this work, we attempt to leverage the ideas in Cocks' IBE for new applications. Unfortunately, we fail. However, our exploration yields some interesting insights into the security of generalizations of Cocks' IBE.

Review of Cocks' IBE. The public key contains an RSA modulus N, and the secret key for identity id is a square root x of $a = H(\mathsf{id}) \bmod N$, where H is a hash function. The ciphertext for a message $m \in \{-1, 1\}$ is a single component $c \in \mathbb{Z}_N$, and decryption outputs $\left(\frac{c+x}{N}\right)$, the Jacobi symbol of $c + x$ and N.[1] Security is proved under the quadratic residuosity assumption.

Our Goal: Generalizing Cocks' IBE. Our aim was to generalize Cocks' IBE so that secret keys are now kth roots of $H(\mathsf{id})$, while decryption is still $\left(\frac{c+x}{N}\right)$. This could give some advantages:

- It is unknown how to hash into the set of quadratic residues of $\mathbb{Z}_N$ without revealing the square root. This means that not all identities id will have secret keys in Cocks' scheme. In order to account for this, Cocks' IBE actually creates *two* ciphertext components c_0, c_1, corresponding to hashes a_0, a_1, respectively, one of which has a square root. Instead, if secret keys are, say, cube roots of a, then for appropriate N almost all $a \in \mathbb{Z}_N$ will have cube roots. This would allow for having only a single ciphertext component.

[1] Usually Cocks' IBE is described as computing the Jacobi symbol of $c + 2x$ rather than $c + x$. However, our version is equivalent and keeps the notation a bit simpler.

- We can think of Cocks' IBE as encrypting to the quadratic polynomial $x^2 - a$, such that any root of the polynomial allows for decryption. Our hypothetical generalization allows for encrypting to higher-degree polynomials $x^k - a$. If we could further generalize to encrypting to truly arbitrary polynomials, still with a single ciphertext component, this would lead to a natural *broadcast encryption* scheme with constant-sized ciphertexts. To encrypt to a set of identities $\mathsf{id}_1, \cdots, \mathsf{id}_r$, simply encrypt to the polynomial $(x^k - H(\mathsf{id}_1))(x^k - H(\mathsf{id}_2)) \cdots (x^k - H(\mathsf{id}_r))$, a polynomial of degree kr. If the secret key for id is a kth root of $H(\mathsf{id})$, then exactly the users $\mathsf{id}_1, \cdots, \mathsf{id}_r$ will be able to decrypt.

Remark 1. *In [BLS13], a different generalization of Cocks' IBE was considered, where secret keys are e-th roots x of $H(\mathsf{id})$, and decryption now performs $\left(\frac{d(x)}{N}\right)_e$. Here, $e \geq 2$ is a prime, $d(\cdot)$ is a polynomial of degree $e-1$ which is described in the ciphertext, and $\left(\frac{d(x)}{N}\right)_e$ is the e-th-power residue symbol. They prove security under the e-th residuosity assumption, a natural extension of quadratic residuosity. However, their goals are somewhat orthogonal to ours. In particular, since d has degree $e-1$, communicating d in the ciphertext means that ciphertexts contain e terms in $\mathbb{Z}_N$, rather than just 1. Toward compressing the ciphertexts in their scheme, [BLS13] present a variant where decryption still involved an e-th power residue symbol but secret keys are square roots of $H(\mathsf{id})$, but show the scheme is insecure. This compressed scheme can be seen as dual to our goals.*

Our Results. First, we show a scheme that allows for encrypting to solutions to cubic equations with single-element ciphertexts, while still using the Jacobi symbol. However, we show two major limitations of the scheme:

- First, the scheme is totally insecure. More generally, we show that *any* scheme where (1) decryption has the form $\left(\frac{d(x)}{N}\right)_e$ and (2) works for all x that are roots of a known polynomial $s(x)$ of degree k such that (3) k and e are relatively prime, then the scheme is insecure. This significantly generalizes the aforementioned attack of [BLS13].
- The above leaves open the possibility of a generalized scheme with $e = 2$ and k even or perhaps even a power of 2. Given that we were able to generalize from $k = 2$ (Cocks' scheme) to $k = 3$, it may initially seem hopeful that we could further generalize to higher k. Indeed, the scheme of [BLS13] which is dual to ours has a natural generalization to all e. Surprisingly, we show that it is not possible to generalize our scheme based on cube roots to even $k = 4$.

Taken together, this shows that our initial goal is likely impossible: while we can generalize Cocks' IBE to $k = 3$, it is insecure, and any further generalizations along similar lines seem impossible.

2 Our Scheme

$\mathsf{Gen}()$: Choose two random primes p, q such that $p-1, q-1$ are relatively prime to 3. Let $N = pq$. Output $\mathsf{mpk} = N$ and $\mathsf{sk} = (p, q)$.

$\mathsf{Extract}(\mathsf{sk}, \mathsf{id})$: Assume a hash function $H : \{0,1\}^* \to \mathbb{Z}_N^*$. Let $a = H(\mathsf{id})$. Use p, q to compute

$$\mathsf{sk}_{\mathsf{id}} = x = a^{1/3} \bmod N \ .$$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, m)$**:** Here, $m \in \{-1, 1\}$. First let $a = H(\mathsf{id})$. Next, choose a random v such that

$$\left(\frac{v^3 - a}{N}\right) = m \ .$$

Here, $(\frac{x}{N})$ is the Jacobi symbol. Do this by choosing random v until the desired equality holds. In expectation, only about two v will be sampled. Then the ciphertext is

$$c = \frac{v(v^3 + 8a)}{4(v^3 - a)} \bmod N \ .$$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{id}, \mathsf{sk}_{\mathsf{id}} = x, c)$**:** Output $(\frac{c-x}{N})$.

Correctness: First, observe that, if x is the cube root of a, then

$$\frac{(v^2 - 2vx - 2x^2)^2}{4(v^3 - a)} = \frac{v^4 - 4v^3x + 8vx^3 + 4x^4}{4(v^3 - a)} = \frac{v^4 - 4v^3x + 8av + 4ax}{4(v^3 - a)}$$
$$= \frac{v^4 + 8av}{4(v^3 - a)} - x = c - x$$

Therefore,

$$\left(\frac{c - x}{N}\right) = \left(\frac{(v^2 - 2vx - 2x^2)^2 4^{-1}(v^3 - a)^{-1}}{N}\right) = \left(\frac{v^2 - 2vx - 2x^2}{N}\right)^2 \left(\frac{2}{N}\right)^{-2} \left(\frac{v^3 - a}{N}\right)^{-1}$$
$$= \left(\frac{v^3 - a}{N}\right) = m$$

3 Our Attack

Attacking our scheme. Some algebraic manipulation shows that

$$c^3 - a = \frac{(v^6 - 20av^3 - 8a^2)^2}{64(v^3 - a)^3}$$

Therefore, to decrypt without knowing the secret key, compute

$$\left(\frac{c^3 - a}{N}\right) = \left(\frac{(v^6 - 20av^3 - 8a^2)^2 64^{-1}(v^3 - a)^{-3}}{N}\right) = \left(\frac{v^3 - a}{N}\right) = m$$

A generalization. Consider any scheme where decryption using secret key x has the form

$$m \leftarrow \left(\frac{d(x)}{N}\right)_e$$

where $d(x) = \sum_i d_i x^i$, and the d_i are derived from the scheme and the ciphertext in some way. Note that the e-th power residue symbol $\left(\frac{d(x)}{N}\right)_e$ outputs e-th roots of unity, so we are assuming messages are encoded as e-th roots of unity. Suppose there is a publicly known degree-k polynomial s, such that decryption succeeds for *any* root of $s(x)$, even roots involving extension "fields" of $\mathbb{Z}_N$. We will call such a scheme a (k, e)-scheme. Note that the insecure compressed version of [BLS13] is a $(2, e)$ scheme for odd primes e.[2] Our scheme in Section 2 is a $(3, 2)$-scheme.

Theorem 1. *For any constants k, e that are relatively prime, any (k, e)-scheme is insecure.*

Proof. Consider the polynomial $d(\alpha_1)d(\alpha_2)\dots d(\alpha_k)$. This polynomial is symmetric in $\alpha_1, \dots, \alpha_k$, and therefore can be written as a polynomial $D(e_1, \cdots, e_k)$, where e_j is the jth elementary symmetric polynomial in $(\alpha_1, \dots, \alpha_k)$. The coefficients of D are rational functions in the coefficients of d.

Now let α_i be the roots over some extension $\mathbb{F}$ of the field $\mathbb{Z}_p$ of the polynomial s. In other words, we can write $s(x) \bmod p = (x - \alpha_1)\dots(x - \alpha_k)$ over $\mathbb{F}$. The coefficient of x^j in $s \bmod p$ is therefore exactly $(-1)^{k-j}e_j$. Therefore, $D(e_1, \cdots, e_k) \bmod p = d(\alpha_1)d(\alpha_2)\dots d(\alpha_k) \bmod p$. Applying the same logic over $\mathbb{Z}_q$ shows that $D(e_1, \cdots, e_k) \bmod N = d(\alpha_1)d(\alpha_2)\dots d(\alpha_k) \bmod N$. $D(e_1, \cdots, e_k)$ can be computed from publicly available information. Since α_i are roots of s, we know that $\left(\frac{d(\alpha_i)}{N}\right)_e = m$ by the correctness of a (k, e)-scheme. But then we can decrypt without knowing a roots of s by setting $u = k^{-1} \bmod e$ (which exits since k, e are relatively prime) and computing:

$$\left(\frac{D(e_1, \cdots, e_k)}{N}\right)_e^u = \left(\frac{\prod_i d(\alpha_i)}{N}\right)_e^u = \prod_i \left(\frac{d(\alpha_i)}{N}\right)_e^u = \left(\prod_i m\right)^u = \left(m^k\right)^u = m \qquad \square$$

Note that if $e = k$ (as in Cocks' IBE or the secure uncompressed scheme in [BLS13]), then $\left(\frac{D(e_1, \cdots, e_k)}{N}\right)_e = 1$, and so the attack is useless.

4 Impossibility of Generalizing Our Scheme

Here, we explain how our (insecure) generalization of Cocks' IBE *cannot* be further generalized beyond $k = 3$, eliminating any hope of avoiding our attack by moving to even k. To do so, we explain how we derived our scheme, and explain why it is unlikely to extend to higher degrees.

Recall that we want $\left(\frac{c+x}{N}\right) = m$, and this needs to hold for all roots of $x^k = a$ where $a = H(\mathsf{id})$. In order to ensure this, the encrypter will set $c + X = tf(X)^2 \bmod (X^k - a)$ where $\left(\frac{t}{N}\right) = m$. Note that the encrypter does not know the actual root x, but will instead choose c, f so that the equation holds over the formal variable X. Here, $f(X)$ is some rational function in X, but by standard arguments we can take it to be a polynomial of degree at most $k - 1$. Then decryption works because $\left(\frac{c+x}{N}\right) = \left(\frac{f(x)}{N}\right)^2\left(\frac{t}{N}\right) = m$. Now let us divide by t, and write $c' = c/t, t' = 1/t$ to get

$$c' + t'X = f(X)^2 \bmod (X^k - a)$$

Obtaining Cocks' IBE ($k = 2$)**.** Let $f(X)$ be a random linear polynomial (remember $k = 2$ so the degree of f is 1). This then uniquely determines c', t', from which we can derive c and t. If $\left(\frac{t}{N}\right) = m$, then we output the derived c. Otherwise, we choose a new random linear polynomial and try again. The resulting scheme is identical to Cocks' IBE, up to a change of variables.

[2] More generally, the authors also consider a natural generalization of their scheme to a (k, e) scheme for $k < e$ and e a prime, and show that this particular generalization is also insecure.

Obtaining Our Scheme ($k = 3$). We cannot let $f(X)$ be a truly random degree 2 polynomial, since $f(X)^2 \bmod (X^3 - a)$ will in general be quadratic. Instead, we need to ensure that the quadratic term of $f(X)^2 \bmod (X^3 - a)$ is zero. Writing $f(X) = g_0 + g_1 X + g_2 X^2$, we get that

$$\begin{aligned} f(X)^2 &= (g_0^2) + (2g_0 g_1)X + (2g_0 g_2 + g_1^2)X^2 + (2g_1 g_2)X^3 + (g_2^2)X^4 \\ &= (g_0^2 + 2a g_1 g_2) + (2g_0 g_1 + a g_2^2)X + (2g_0 g_2 + g_1^2)X^2 \bmod (X^3 - a) \end{aligned}$$

Thus, we can choose $f(X)$ by choosing uniform g_0, g_1, and setting $g_2 = -g_1^2/2g_0$. From the polynomial $f(X)$, we can then derive both c and t. If $\left(\frac{t}{N}\right) = m$, we output c; otherwise we choose a new function $f(X)$ and try again. This is equivalent to the scheme in Section 2 up to a change of variables. It also extends to encrypt to arbitrary cubic polynomials.

Failing Beyond $k = 3$**.** Unfortunately, this approach does not extend beyond $k = 3$. Let us try to solve the case $k = 4$. Setting $f(X) = \sum_{i=0}^{3} g_i X^i$, we then have that

$$\begin{aligned} f(X)^2 &= (g_0^2) + (2g_0 g_1)X + (2g_0 g_2 + g_1^2)X^2 + (2g_1 g_2 + 2g_0 g_3)X^3 + (2g_1 g_3 + g_2^2)X^4 + (2g_2 g_3)X^5 + (g_3^2)X^6 \\ &= (g_0^2 + a(2g_1 g_3 + g_2^2)) + (2g_0 g_1 + 2a g_2 g_3)X + (2g_0 g_2 + g_1^2 + a g_3^2)X^2 + (2g_1 g_2 + 2g_0 g_3)X^3 \bmod (X^4 - a) \end{aligned}$$

For $f(X)^2 \bmod (X^4 - a)$ to be linear, we need both $2g_0 g_2 + g_1^2 + a g_3^2 = 0$ and $2g_1 g_2 + 2g_0 g_3 = 0$. Solutions to such equations exist in abundance. However, it is not clear how to obtain a non-trivial one since we cannot take efficient roots over the composite modulus N. We therefore ask for a *rational parameterization* of the solution space, meaning the coefficients g_i are each rational functions in some parameter v. This allows us to sample from the solution space by choosing a uniform v. However, we now argue that such a rational parameterization does not exist.

First, observe that both equations we need to solve are homogeneous, meaning we can take, say, $g_3 = 1$, and scale the other variables accordingly. Plugging into the second equation gives $g_0 = -g_1 g_2$. Plugging into the first equation gives $-2g_1 g_2^2 + g_1^2 + a = 0$. Now substitute $g_1 = x$ and $g_2 = y/x$, giving $-2y^2/x + x^2 + a = 0$, or equivalently $y^2 = x^3/2 + ax/2$. This is the equation for an elliptic curve with non-zero discriminant, which are known to have no rational parameterizations. Thus, it is impossible to rationally parameterize the set of polynomials $f(X)$. Hence, this approach does not generalize to $k = 4$. Similar arguments extend to all $k > 3$.

References

[BF01] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229. Springer, Heidelberg, August 2001.

[BLS13] Dan Boneh, Rio LaVigne, and Manuel Sabin. Identity-based encryption with eth residuosity and its incompressibility. In *Autumn 2013 TRUST Conference. Washington DC (Oct 9-10, 2013), poster presentation*, 2013.

[Coc01] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In Bahram Honary, editor, *8th IMA International Conference on Cryptography and Coding*, volume 2260 of *LNCS*, pages 360–363. Springer, Heidelberg, December 2001.