On the Anonymization of Cocks IBE Scheme

Gheorghe A. Schipor(✉)

Faculty of Computer Science,
"Alexandru Ioan Cuza" University of Iaşi, 700506 Iaşi, România
adrian.schipor@info.uaic.ro

Abstract. Identity based encryption is a relative new method of encryption in which the public key is calculated using an identity. Cocks proposed such a scheme, but his scheme doesn't provide anonymity. In this paper is proposed an extended version of the Cocks IBE scheme that provides anonymity. The ciphertext expansion and the computational time of the scheme proposed here is very close to that of the Cocks IBE scheme, and like the Ateniese-Gasti scheme, it provides universal anonymity.

Keywords: Identity based encryption · Anonymity · Identity · Public-key cryptography

1 Introduction

Until 1976, all known cryptographic algorithms were symmetric, the key used for encryption was the same as the key used for decryption. Whitfield Diffie and Martin Hellman laid the foundations of public key cryptography by their key exchange protocol, even if, in 1997, the British Government revealed that a similar scheme was created, in secret and independently, a few years earlier by James H. Ellis, Clifford Cocks and Malcolm J. Williamson.

The first who mentioned about an asymmetric scheme in which the public key can be calculated using the identity of the intended recipient was Adi Shamir, in 1984 [7], although he was unable to develop such a system. The problem remained opened until 2001, when Boneh and Franklin developed an IBE scheme based on elliptic curves [2]. Soon after, Cocks managed to develop another IBE scheme based on quadratic residuosity problem [8].

The scheme proposed by Cocks encrypts the plaintext bit by bit, every bit being mapped into a pair of two big integers, so it's very bandwidth consuming. However, as mentioned in [8] by Cocks, his scheme can be used in practice to encrypt short session keys.

We say that a cryptographic scheme is anonymous if nobody can say who is the recipient only by having the ciphertext and the public key. If anyone can anonymize the ciphertext using only the public key, the scheme is universally anonymous [12]. Galbraith showed that the Cocks IBE scheme is not anonymous, so the question that came was if the Cocks IBE scheme can be extended to provide anonymity but to not be much more expensive than the original scheme. Di Crescenzo and

B. Ors and B. Preneel (Eds.): BalkanCryptSec 2014, LNCS 9024, pp. 194–202, 2015.
DOI: 10.1007/978-3-319-21356-9_13

Saraswat were the first who extended the Cocks IBE scheme to support anonymity. However, their scheme is impractical to use when large data must be encrypted because it requires a large number of keys [6]. In 2009, Ateniese and Gasti proposed another scheme that extends Cocks IBE scheme and provides anonymity. More, only the public key is used to anonymize the ciphertext so their scheme is universally anonymous. However, every bit of plaintext is mapped into two lists of big integers [1], so the ciphertext expansion is very big.

In this paper I propose a more efficient scheme that extends the Cocks IBE scheme to provide anonymity. The ciphertext expansion of the scheme proposed here is very close to that of the Cocks IBE scheme, sending for a bit, besides the two big integers required by Cocks IBE scheme, only two small integers who usually can be represented on 8 bits. Also, the computational time of the scheme proposed in this paper is close to that of the original scheme, reducing the time to (de)anonymize the ciphertext with more than half of the amount of time required by Ateniese-Gasti scheme to realise these operations.

2 Cocks IBE Scheme

The Cocks IBE scheme requires a big integer n, which is the product of two primes numbers p and q, each of them congruent to 3 modulo 4. Also, it requires a hash function $H : \{0,1\}^* \mapsto \mathbb{Z}_n$. n is the public parameter, and (p, q) represents the master key.

Key Generation: The public key for an identity ID is $a = H(ID)$, with the Jacobi symbol $(\frac{a}{n}) = 1$. The private key corresponding to the public key a is calculated as

$$r = a^{(\phi(n)+4)/8} \mod n.$$

Encryption: A bit b is first encoded in $x = (-1)^b$. Two independent values $t, v \in \mathbb{Z}_n^*$ are chosen at random such that $(\frac{t}{n}) = (\frac{v}{n}) = x$, and the ciphertext is computed as

$$(s_1, s_2) = (t + \frac{a}{t} \mod n, v - \frac{a}{v} \mod n).$$

Decryption: To decrypt the pair (s_1, s_2) the recipient must decide which of the two choices he needs to decrypt, choosing s_1 if $r^2 \equiv a \mod n$ and s_2 if $r^2 \equiv -a \mod n$. The decrypted text is

$$x = (\frac{s_i + 2r}{n}), i \in \{1, 2\}.$$

3 Cocks IBE Anonymization

3.1 Galbraith's Test

Galbraith showed that Cocks IBE does not provide anonymity. Let $a \in \mathbb{Z}_n$ be the private key and $M_a[n] = \{(t + \frac{a}{t}) \mod n | t \in \mathbb{Z}_n^* \wedge (t/n) = (-1)^b\}$ be the set of all ciphertext values sampled using the public key $a \in \mathbb{Z}_n^*$. He proposed the following test:

$$GT(a, c, n) = (\frac{c^2 - 4a}{n}), c \in \mathbb{Z}_n$$

If c is sampled from $M_a[n]$, the test will return 1 always, because $c^2 - 4a$ is a square in $\mathbb{Z}_n$. If c is not sampled from $M_a[n]$ the test will return 1 with probability negligibly close to 1/2 [1]. This holds because Perron showed that for a prime p, the difference between the squares and non squares from $\mathbb{Z}_p$ is just 1 if $p \equiv 3 \mod 4$.

For two public keys $a, b \in \mathbb{Z}_n^*$ and $c \in \mathbb{Z}_n$ a value of the ciphertext sampled using one of the two keys, the Galbraith's test over the public key a can be summarized as

$$GT(a, c, n) = \begin{cases} +1 \implies Prob[c \in M_a[n]] = 1/2 \\ -1 \implies c \notin M_{(a,n)}. \end{cases}$$

An adversary can apply Galbraith's test for multiple ciphertext values to determine whether the given ciphertext is intended for a or b [1].

In [1], Ateniese and Gasti proved that is no better test against anonymity over an encrypted bit, so the scheme proposed in this paper, like that of Ateniese and Gasti, is based on the Galbraith's test.

3.2 Ateniese-Gasti Scheme

The scheme proposed by Ateniese and Gasti in [1] extends Cocks IBE to provide anonymity. Also, their scheme is the first universally anonymous IBE, so anyone can anonymize the ciphertext using only the public key of the recipient.

Anoymization: Let (s_1, s_2) be the corresponding ciphertext of a bit b encrypted with the public key $a \in \mathbb{Z}_n^*$. To anonymize a component $s_i, i \in \{1, 2\}$ of the pair (s_1, s_2) one must proceed as follows:

1. choose k from the geometric distribution over the set $\{1, 2, 3, ...\}$ with the probability parameter $\frac{1}{2}$;
2. choose T random and set $Z = T + s_i \mod n$;
3. compute the mask as

$$(Z, T_1, T_2, ..., T_{k-1}, \boldsymbol{T}, T_{k+1}, ..., T_m),$$
$$GT(a_i, Z - T_j, n) = -1, 1 \leq j < k$$
$$GT(a_i, Z - T_j, n) = \pm 1, k < j \leq m,$$
$$i \in \{1, 2\}, a_1 = a, a_2 = -a.$$

The pair $((Z_1, T_{1_1}, T_{1_2}, ..., T_{1_k}, ..., T_{1_m}), (Z_2, T_{2_1}, T_{2_2}, ..., T_{2_k}, ..., T_{2_m}))$ represents the anonymized ciphertext.

Deanonymization: Given the anonymized ciphertext

$$((Z_1, T_{1_1}, T_{1_2}, ..., T_{1_k}, ..., T_{1_m}), (Z_2, T_{2_1}, T_{2_2}, ..., T_{2_k}, ..., T_{2_m})),$$

the recipient must first discard one of the two tuples based on whether a or $-a$ is a square in $\mathbb{Z}_n$, and find the smallest index $1 \leq j \leq m$ such that $GT(a_i, Z_i - T_{i_j}, n) = 1, i \in \{1, 2\}$. The initial value of ciphertext is $Z_i - T_{i_j}$.

Security: Ateniese and Gasti showed that their scheme does not reveal any information about the plaintext and an adversary cannot determine which public key was used to encrypt the plaintext, even thought the adversary selects the public keys and the plaintext.

4 A New Method of Anonymization

Like the scheme proposed by Ateniese and Gasti, the scheme proposed bellow is based on the Cocks IBE scheme and is universally anonymous. Also, the ciphertext expansion and the computational time of this scheme is very close to that of the Cocks IBE scheme.

Anonymization: To anonymize a component $s_i, i \in \{1, 2\}$ of the pair (s_1, s_2) with the public key $a \in \mathbb{Z}_n^*$, one must proceed as follows:

1. choose a bit d random;
2. if d is 1 then:
   (a) choose k from the geometric distribution over the set $\{1, 2, 3, ...\}$ with the probability parameter $\frac{1}{2}$;
   (b) $plus_i \leftarrow 1$, $j \leftarrow 0$, $s_{anon_i} \leftarrow s_i$;
   (c) $s_{anon_i} = s_{anon_i} + 1 \mod n$;
   (d) if $GT(a_i, s_{anon_i}, n) = 1$, then $plus_i \leftarrow plus_i + 1$, else $j \leftarrow j + 1$;
   (e) if $j = k$, then output $(s_{anon_i}, plus_i)$, else jump to (c);
3. else, $s_{anon_i} \leftarrow s_i$, choose $plus_i$ random from the geometric distribution over the set $\{1, 2, 3, ...\}$ with the probability parameter $\frac{1}{2}$ and output $(s_{anon_i}, plus_i)$.

The pair $((s_{anon_1}, plus_1), (s_{anon_2}, plus_2))$ represents the ciphertext anonymized.

Deanonymization: Given the anonymized ciphertext

$$((s_{anon_1}, plus_1), (s_{anon_2}, plus_2)),$$

the recipient must first choose the valid component based on whether a or $-a$ is a square in $\mathbb{Z}_n$. After that, the recipient must test if $GT(a, s_{anon_i}, n)$ equals -1 or 1. If $GT(a, s_{anon_i}, n) = 1$, then the component was not anonymized, so he can jump to decryption. Else, the component was anonymized so he must substract 1 from s_{anon_i} until he reaches the $plus_i$-th element such that $GT(a_i, s_{anon_i} - 1 - ..., n) = 1$. That value represents the initial ciphertext.

4.1 Security

At the base of the security of this scheme is the fact that the probability to anonymize a component is $\frac{1}{2}$. Let $a, b \in \mathbb{Z}_n^*$ be two public keys, and $s_{anon} \in M_a[n]$ be a component of the anonymized ciphertext. The probability that $GT(a, s_{anon}, n) = 1$ is $\frac{1}{2}$. The probability that $GT(b, s_{anon}, n) = 1$ is also $\frac{1}{2}$ because of the distribution of the Jacobi symbols in $\mathbb{Z}_n$. So an adversary cannot say what public key was used to encrypt the plaintext because for him each of the public keys has the same probability to be used. An adversary can be in one of the following four cases:

Case 1:

$$\begin{cases} GT(a, s_{anon}, n) = 1 \\ GT(b, s_{anon}, n) = 1 \end{cases}$$

The adversary cannot say what public key was used to encrypt the plaintext. For each of the two public keys, the ciphertext seems to not be anonymized. The adversary can suppose that the plaintext was encrypted with the public key a and not anonymized(the probability to be so is $\frac{1}{2}$) and $GT(b, s_{anon}, n)$ is 1 because of the distribution of the Jacobi symbols in $\mathbb{Z}_n$. Also, the adversary can suppose that the plaintext was encrypted with the public key b and not anonymized(the probability to be so is $\frac{1}{2}$) and $GT(a, s_{anon}, n)$ is 1 because of the distribution of the Jacobi symbols in $\mathbb{Z}_n$. It can be easily seen that the adversary cannot say with probability greater than 1/2 which case is the good one.

Case 2:

$$\begin{cases} GT(a, s_{anon}, n) = -1 \\ GT(b, s_{anon}, n) = 1 \end{cases}$$

The adversary can suppose that the plaintext was encrypted with the public key a and anonymized(the probability to be so is $\frac{1}{2}$) and $GT(b, s_{anon}, n)$ is 1 because of the distribution of the Jacobi symbols in $\mathbb{Z}_n$. Also, the adversary can suppose that the plaintext was encrypted with the public key b and not anonymized(the probability to be so is $\frac{1}{2}$) and $GT(a, s_{anon}, n)$ is -1 because of the distribution of the Jacobi symbols in $\mathbb{Z}_n$. Therefore, the adversary cannot say with probability greater than 1/2 which case is the good one.

Case 3:

$$\begin{cases} GT(a, s_{anon}, n) = 1 \\ GT(b, s_{anon}, n) = -1 \end{cases}$$

Similar with the **Case 2**.

Case 4:

$$\begin{cases} GT(a, s_{anon}, n) = -1 \\ GT(b, s_{anon}, n) = -1 \end{cases}$$

For each of the two public keys, the ciphertext seems to be anonymized. The adversary can suppose that the plaintext was encrypted with the public key a and anonymized(the probability to be so is $\frac{1}{2}$) and $GT(b, s_{anon}, n)$ is -1 because of the distribution of the Jacobi symbols in $\mathbb{Z}_n$. Also, the adversary can suppose that the plaintext was encrypted with the public key b and anonymized(the probability to be so is $\frac{1}{2}$) and $GT(a, s_{anon}, n)$ is -1 because of the distribution of the Jacobi symbols in $\mathbb{Z}_n$. Therefore, the adversary cannot say with probability greater than 1/2 which case is the good one.

Anonymization Method: The method to anonymize a component should not reveal any informations about the used public key, so an adversary must find a valid deanonymized ciphertext for every public key $p_k \in \mathbb{Z}_n^*$ and to not make distinction between these ciphertexts.

It is easy to prove that the method used to anonymize the ciphertext doesn't reveal informations about the used public key. If an adversary has two public keys $a, b \in \mathbb{Z}_n^*$ and an anonymized(for both keys) component $(s_{anon}, plus_i)$, he can subtract 1 from s_{anon} until he reach the k-th element with $GT(a, s_{anon} - 1 - ..., n) = 1$ or until he reach the k-th elemenet with $GT(b, s_{anon} - 1 - ..., n) = 1$. With both public keys he can determine a valid value. When a component is not anonymized, it is chosen $plus_i$ from the geometric distribution with the probability parameter $\frac{1}{2}$. This is because the Jacobi symbols are uniformly distributed in $\mathbb{Z}_n$, so we can consider that until we reach at the k-th element for that the value of Galbraith's test is -1(when the component is anonymized), we pass over same number of elements for that the value of Galbraith's test is 1. So the method used to anonymize a component does not reveal any information about the pubic key used to encrypt the plaintext.

Choosen Plaintext Attack: An IBE scheme is ANON-IND-ID-CPA-secure if is IND-ID-CPA-secure and an adversary cannot determine the key used for encryption even if he selects the plaintext and the identities and receives the plaintext encrypted with the public key corresponding to one of the chosen identities [13,14].

The scheme presented is IND-ID-CPA-secure because extends Cocks IBE scheme, which is IND-ID-CPA-secure, and the anonymization is done using only the public key and the ciphertext.

It remains to prove that an adversary cannot determine the key used for encryption when he selects the keys and the plaintext. In [13] is presented an experiment for this. The adversary has access to a random oracle H and to an oracle $KeyDer$ that returns the private key corresponding to any identity ID, but cannot request the private keys [1,13]:

Experiment $Exp_{IBE,A}^{ibe-ano-cpa}(n)$:
pick random oracle H;
$(ID_0, ID_1, msg, state) \leftarrow A^{KeyExtr(.),H}(find, PKG_{pub})$;
$b \leftarrow \{0,1\}$;
$W \leftarrow \{0,1\}^{|msg|}$;
$c \leftarrow Enc^H(ID_b, W, PKG_{pub})$;
$b' \leftarrow A^{KeyExtr(.),H}(guess, c, state)$;
if $b' = b$ return 1, else return 0.
The advantage of A is defined as

$$Adv_{IBE,A}^{ibe-ano-cpa}(n) =$$

$$Prob[Exp_{IBE,A}^{ibe-ano-cpa-1}(n) = 1] - Prob[Exp_{IBE,A}^{ibe-ano-cpa-0}(n) = 1].$$

We say that a scheme is IBE-ANO-CPA-secure if $Adv_{IBE,A}^{ibe-ano-cpa}(n)$ is a negligible function in n for all polynomial-time adversaries A [13].

In the proposed scheme every component from the pair corresponding to an encrypted bit is anonymized independently and even if both components encrypts the same value, since the Cocks IBE scheme is IND-ID-CPA-secure, the advantage of an adversary to win the experiment is only negligibly, even if he choose the plaintext and the keys. An adversary will be in one of the four cases presented, so he cannot find the key used for encryption because the components are anonymized independently and for every key he can find a valid value of ciphertext. To summarize,

$$Adv_{new-ibe-cocks,A}^{ibe-ano-cpa}(n) = \frac{1}{2} + negl(n)$$

for every adversary A, where *new-ibe-cocks* is the scheme presented.

Because is IBE-ANO-CPA-secure and IND-ID-CPA-secure, *new-ibe-cocks* is ANON-IND-ID-CPA-secure.

4.2 Practical Aspects

If Cocks IBE scheme is used to encrypt a 128 bits session key, the ciphertext length is only $128 * 2 * 1024$ bits, but the ciphertext is not anonymized. Using the Ateniese-Gasti scheme, the ciphertext length is $128 * 2 * m * 1024$ bits. However, using the scheme presented in this paper, the ciphertext length is only $128 * 2 * (1024 + l)$ bits, where l is the number of bits required to represent the second component from an anonymized component. The $plus_i$ component is chosen from the geometric distribution over the set $\{1, 2, 3, ...\}$ with the probability parameter $\frac{1}{2}$, so l can be usually 8. It can be seen that the ciphertext expansion of this scheme is much smaller than the ciphertext expansion of the Ateniese-Gasti scheme, being closer to the Cocks IBE scheme.

Implementation: I implemented all three schemes and compared the results. The implementation was done using the *C* programming language and the big numbers library *GMP*. In all three implementations, I used 512 bits numbers for p and q. Every essential step of the schemes was executed 1000 times. The operating system under I tested the schemes is *Elementary OS*, *Linux Kernel 3.2* and the machine consists of 4GB RAM memory and an Intel Core i5 processor. The results are summarized in the Table 1.

Table 1. Average execution times

	Setup	Extraction	Encryption	Decryption
Cocks	26.77 ms	3.58 ms	18.7 ms	7.45 ms
Ateniese-Gasti	26.77 ms	3.58 ms	33.46 ms	24.46 ms
Proposed scheme	26.77 ms	3.58 ms	23.19 ms	14.38 ms

As you can see, the scheme proposed in this paper is more efficient than the scheme proposed by Ateniese and Gasti, reducing the (de)anonymization time with more than half of the time needed by their scheme. Also, like their scheme, this scheme is universally anonymous because only the public key is used to anonymize the ciphertext, so one could write an algorithm that has as input the ciphertext and the public key and outputs the anonymized ciphertext.

Overall, I propose a universally anonymous IBE scheme that is almost as efficient as Cocks IBE scheme.

References

1. Ateniese, G., Gasti, P.: Universally anonymous IBE based on the quadratic residuosity assumption. In: Fischlin, M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 32–47. Springer, Heidelberg (2009)
2. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. SIAM J. Comput. **32**(3), 586–615 (2003)
3. Martin, L.: Introduction to Identity-Based Encryption. Artech House, Norwood (2008)
4. Tiplea, F.L.: Algebric Foundation of Computer Science. Polirom, Algebric Foundation of Computer Science. Polirom, Romanian (2006)
5. Damgård, I.B.: On the randomness of legendre and jacobi sequences. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 163–172. Springer, Heidelberg (1990)
6. Di Crescenzo, G., Saraswat, V.: Public key encryption with searchable keywords based on jacobi symbols. In: Srinathan, K., Rangan, C.P., Yung, M. (eds.) INDOCRYPT 2007. LNCS, vol. 4859, pp. 282–296. Springer, Heidelberg (2007)
7. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)

8. Benachour, P., Farrell, P.G., Honary, B.: A line code construction for the adder channel with rates higher than time-sharing. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, p. 166. Springer, Heidelberg (2001)
9. Satoh, A., Morioka, S., Takano, K., Munetoh, S.: A compact rijndael hardware architecture with S-Box optimization. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, p. 239. Springer, Heidelberg (2001)
10. Spiegel, M.: Theory and Problems of Statistics. McGraw-Hill, New York (1992)
11. Boneh, D., Gentry, C., Hamburg, M.: Space-Efficient Identity Based Encryption Without Pairings. In: Proceedings FOCS 2007 (2007)
12. Hayashi, R., Tanaka, K.: Universally anonymizable public-key encryption. In: Roy, B.(ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 293–312. Springer, Heidelberg (2005)
13. Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P., Shi, H.: Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 205–222. Springer, Heidelberg (2005)
14. Halevi, S.: A Sufficient Condition for Key-Privacy. Cryptology ePrint Archive, Report 2005/05 (2005)