New Efficient Identity-Based Encryptions From Factorization[*]

Jun Shao[1], Licheng Wang[2], Xiaolei Dong[3], and Zhenfu Cao[3]

[1] School of Computer and Information Engineering, Zhejiang Gongshang University
[2] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications
[3] Department of Computer Science and Engineering, Shanghai Jiaotong University
chn.junshao@gmail.com, wanglc@bupt.edu.cn, {zfcao,dong-xl}@cs.sjtu.edu.cn

Abstract. Identity Based Encryption (IBE) systems are often constructed using pairings or lattices. Three exceptions are due to Cocks in 2001, Boneh, Gentry and Hamburg in 2007, and Paterson and Srinivasan in 2009. The main goal of this paper to propose new IBE schemes, which may give a way to find IBEs without pairing or lattice. Essentially, the security of our IBE schemes is rooted in the intractability assumption of integer factorization. We believe that our constructions have some essential differences from all existing IBEs.

Keywords: identity-based encryption, integer factorization, without pairing/lattice

1 Introduction

Cryptographers have spent long time for finding practical identity-based encryptions (IBEs) after the birth of the primitive. According to Shamir's seminal conception [13], an IBE scheme should enable some trusted their party, named as private key generator (PKG), to extract a private key securely for arbitrary strings which represent identities. Surprisingly, when we look back the long term struggling for IBEs, it seems that the biggest obstacle for easily fetching practical solutions of IBEs is the adjunct word *arbitrary*, instead of security issues.

The first efficient IBE scheme, denoted by BF01 [1], based on pairings was proposed at CRYPTO 2001. This work wakes our enthusiasm on pairing-based cryptography, such as improved constructions of IBEs, extended construction of fuzzy IBE, Attribute-Based Encryption (ABE), Predicate-Based Encryption (PBE), Functional Encryption (FE), etc. Recently, lattice-based cryptography attracts a lot of attention due to its claimed quantum attack resistant property, and people have already made great progress on building IBEs, as well as ABE and FE, from lattice-based assumptions.

No matter how successful are pairing-based cryptography and lattice-based cryptography, it is still an interesting problem to find an efficient IBE without using pairings or lattices. The first attempt, denoted by Cocks01 [5], is based on quadratic residue problems modulo a composite $n = p \cdot q$ (where p and q are large primes) and was published shortly after the publishing of BF01. The Cocks system, however, produces long ciphertexts: an encryption of an ℓ-bit message consists of $2\ell \cdot \log n$ bits. Since then it had been an open problem to construct a space efficient IBE system without pairings until 2007. At FOCS 2007, Boneh, Gentry and Hamburg [7] proposed a space efficient IBE scheme, denoted by BGH07, in which a ciphertext of an ℓ-bit message consists merely $1 + \ell + \log n$ bits. BGH07, however, has rather large private keys, and both the encryption and

[*] This work was supported by the National Natural Science Foundation of China (NSFC) (nos. 61033014, 61371083, 61373154, 61370194) and the NSFC A3 Foresight Program (no. 61161140320).

decryption algorithms require non-trivial computational effort [11], observably *slower than* in the Cocks system [7]. Note that in 2009, Paterson and Srinivasan [11] also proposed another IBE scheme, denoted by PS09, based on factorization assumption and discrete logarithm related assumptions simultaneously. Although PS09 is efficient both in space and in encryption/decrytion, but the private key extracting algorithm is *inefficient* since PKG needs to solve two discrete logarithm problem over F_p and F_q. It is feasible only if both $p-1$ and $q-1$ are B-smooth and B is not too large. But on the other hand B should large enough for resisting knowing factorization methods. Therefore, it is still a challenge to find *efficient* IBEs without using pairing or lattice. Here, the adjunct word *efficient* means at least three aspects, i.e., efficient in space, in encryption/decryption speed and in private key generation cost.

In this paper, we propose two efficient constructions of IBEs based on the intractability assumption of integer factorization (IF) problem and the related residue decisional Diffie-Hellman (RDDH) problem (See Definition 3). Note that the assumption of intractability of RDDH problem is also rooted in the assumption of intractability of IF problem. Thus, in essential, the security of our scheme is rooted in IF assumption only. Intuitively, our constructions are based on an elaborate coupling of IF assumption and RDDH assumption: the latter enables users to perform Elgamal-like [8] encryption/decryption in Scheme I or Cramer-Shoup-like [6] encryption/decryption in Scheme II, while the former enables PKG to extract proper private keys according to arbitrary given identities. Our schemes are compact and efficient: the ciphertext expansion factor is 2 in Scheme I and 4 in Scheme II, and the encryption (resp. decryption) needs only several modular exponentiations. In particular, the costs in private key generation algorithm `Ext` in both schemes are very efficient: PKG needs only solving the so-called k-residue discrete logarithm problem with the complexity $\mathcal{O}(\alpha(\log n)^2(\log\log n))$, where $\alpha = \sum_{i=1}^{s}\alpha_i$ under the setting $k = \prod_{i=1}^{s} p_i^{\alpha_i}$ with small distinct primes p_i and positive α_i $(i = 1, \cdots, s)$. Note that the costs in `Setup` algorithm in all aforementioned schemes are efficient. In summary, our main contribution is given in Table 1.

Table 1. IBE Constructions Without Pairings/Lattices

Schemes	Efficient In				
	Ciphertext Size	Private-key Size	Enc/Dec Speed	Ext Cost	Setup Cost
Cocks01	No	Yes	Yes	Yes	Yes
BGH07	Yes	No	No	Yes	Yes
PS09	Yes	Yes	Yes	No	Yes
Ours	Yes	Yes	Yes	Yes	Yes

2 Schemes Description

2.1 IBE Scheme I: Extracting Private Keys Deterministically

Our first IBE scheme consists of the following four algorithms:

`Setup`: To generate the master key pairs (mpk, msk), the PKG performs the following steps.

1. Choose three distinct large safe primes p', p'' and q'.
2. Let $n' = p' \cdot q'$ and $e = n' \cdot p''$.
3. Choose two positive integers k_p and k_q such that

(a) both k_p and k_q merely contain small odd prime factors.
(b) both $p = 2k_p \cdot p' + 1$ and $q = 2k_q \cdot q' + 1$ are primes.
(c) $\gcd(k_p, p') = \gcd(k_q, q') = \gcd(k_p, k_q) = 1$.

4. Let $k = k_p \cdot k_q$ and $n = p \cdot q$.
5. Choose $a \in \mathbb{Z}_n^*$ such that $\left(\frac{a}{n}\right) = -1$.
6. Choose $g \in \mathbb{Z}_n^*$ such that $\mathrm{ord}_p(g) = k_p$ and $\mathrm{ord}_q(g) = k_q$ (see [3] and [4] for details on how to do this efficiently.)
7. Choose a hash function $H : \{0,1\}^* \to \mathbb{Z}_n$.
8. Let $mpk = (n, e, a, g, H)$ and $msk = (p, q, k_p, k_q)$

`Ext`: On input an identity `id`, the PKG computes the corresponding private key $sk_{\mathtt{id}}$ as follows:

1. Let $h' = H(id)$.
2. If $\left(\frac{h'}{n}\right) = -1$ then let $h = h' \cdot a \bmod n$ else let $h = h'$.
3. Compute $y = h^{2e} \bmod n$.
4. Find $x < k$ by solving the k-residue discrete logarithm problem $y \equiv g^x \pmod{n}$. [1]
5. Let $sk_{\mathtt{id}} = x$.

`Enc`: On input a message m from $\mathbb{Z}_n$ and an identity `id`, the encryptor performs the following steps:

1. Let $h' = H(id)$.
2. If $\left(\frac{h'}{n}\right) = -1$ then let $h = h' \cdot a \bmod n$ else let $h = h'$.
3. Compute $y = h^{2e} \bmod n$.
4. Choose $r \in \mathbb{Z}_n$ at random and compute the ciphertext $c = (c_1, c_2)$ as follows

$$c_1 = g^r \bmod n, \quad c_2 = y^r \cdot m \bmod n.$$

`Dec`: On input a ciphertext $c = (c_1, c_2)$ under an identity `id` and a private key $sk_{\mathtt{id}}$, the user with identity `id` computes the message m by $m = c_2 / c_1^{sk_{\mathtt{id}}} \bmod n$.

Apparently, the above IBE scheme is consistent considering that $\mathrm{ord}_n(g) = k$ and $y \equiv g^{sk_{\mathtt{id}}} \pmod{n}$.

Remark 1 (Security of private key extracting). Note that even if the returned private key $sk_{\mathtt{id}}$ is even, one cannot factor n by using the so-called square-root attack. Suppose that $sk_{\mathtt{id}} = x = 2z$, we have $h^{2e} \equiv g^{2z} \pmod{n}$ according the definition of `Ext`. At first, it is easy to see that $\left(\frac{h}{n}\right) = 1$ holds for arbitrary identities. Next, let us prove that in the case of $\left(\frac{h}{p}\right) = \left(\frac{h}{q}\right) = -1$, it is impossible $p | h^e - g^z$ (resp. $q | h^e - g^z$). Otherwise, we have

$$g^z \equiv h^e \pmod{p} \quad (\text{resp.} \quad g^z \equiv h^e \pmod{q}).$$

Raise the both sides of the above formula to the power of k_p (resp. k_q) and then calculate the Legendre symbol w.r.t. p (resp. q), we get the following contradiction

$$1 \equiv \left(\frac{g^{z \cdot k_p}}{p}\right) \equiv \left(\frac{h}{p}\right)^{e \cdot k_p} \equiv -1 \pmod{p} \quad (\text{resp.} \quad 1 \equiv \left(\frac{g^{z \cdot k_q}}{q}\right) \equiv \left(\frac{h}{q}\right)^{e \cdot k_q} \equiv -1 \pmod{q}).$$

[1] With knowing p, q, k_p, k_q, this can be done via solving the k_p-residue discrete logarithm problem $y \equiv g^{x_p} \pmod{p}$, the k_q-residue discrete logarithm problem $y \equiv g^{x_q} \pmod{q}$, and then letting $x = \mathbf{CRT}(k_p, x_p, k_q, x_q)$ (See [4, 3] for details).

Thus, the only possible situation is that $p|h^e+g^z$ and $q|h^e+g^z$ hold simultaneously. Similarly, in case of $\left(\frac{h}{p}\right) = \left(\frac{h}{q}\right) = 1$, the only possible situation is that $p|h^e - g^z$ and $q|h^e - g^z$ hold simultaneously. Therefore, in both cases, $(h^e \pm g^z, n)$ must be 1 or n, without revealing any non-trivial factor of n.

We are now trying to prove the above scheme secure against CPA attacks. It may be based on the assumption that the following problems are intractable. The main goal of this paper to propose new constructions on IBEs, which may give a way to find IBEs without pairings or lattices.

Definition 1 (k-Residue Discrete Logarithm, k-RDL [4]). *For prime p and two positive integers b, k such that $k|p-1$ and $\mathrm{ord}_p(b) = k$, the k-discrete logarithm problem is to find x $(0 \le x < k)$ satisfying $b^x \equiv y \pmod{p}$ for a given integer $y \in \mathbb{Z}_p^*$. We call x as y's k-discrete logarithm w.r.t. base b and modulus p. When k contains only small prime factors, we call x as y's k-residue discrete logarithm (k-RDL) w.r.t. base b and modulus p, denoted as $x = RDL^k_{b,p}(y)$.*

With knowing p and k's standard factorization $k = \prod_{i=1}^{s} p_i^{\alpha_i}$, the k-RDL problem can be solved within the complexity $\mathcal{O}(\alpha(\log p)^2(\log\log p))$, where $\alpha = \sum_{i=1}^{s} \alpha_i$ (See [3, 4] for details). This fact is the basis of our construction. However, without knowing k and the factorization of n, we do not know how to solve k-RDL problem over $\mathbb{Z}_n$ efficiently.

Definition 2 (k-Residue Computational Diffie-Hellman Problem, k-RCDH). *Suppose that $n = p \cdot q$ (where p and q are large primes), and $\mathrm{ord}_n(g) = k$, but both k and the factorization of n are unknown. Given $g^a, g^b \pmod{n}$, the objective of k-residue computational Diffie-Hellman problem is to find $g^{ab} \pmod{n}$.*

Definition 3 (k-Residue Decisional Diffie-Hellman Problem, k-RDDH). *Suppose that $n = p \cdot q$ (where p and q are large primes), and $\mathrm{ord}_n(g) = k$, but both k and the factorization of n are unknown. Given $g^a, g^b, g^c \pmod{n}$, the objective of k-residue decisional Diffie-Hellman problem is to determine whether $g^c = g^{ab} \pmod{n}$.*

2.2 IBE Scheme II: Extracting Private Keys Non-Deterministically

The above IBE scheme follows the well-known Elgamal encryption/decryption diagram that is merely achieve IND-CPA security. It is easy to extend it to an IND-CCA2 secure IBE scheme by using the typical transformation techniques, such as the FO technique [9, 10], etc. However, an even natural idea is to derive new IBE variant by replacing the ElGamal-like diagram in the above construction with another well-known encryption/decryption diagram – the Cramer-Shoup scheme [6] that is IND-CCA2 secure in the standard model.

Our second IBE scheme consists of the following four algorithms:

`Setup`: To generate the master key pairs (mpk, msk), the PKG performs the following steps.

1. Choose three distinct large safe primes p', p'' and q'.
2. Let $n' = p' \cdot q'$ and $e = n' \cdot p''$.
3. Choose two positive integers k_p and k_q such that
   (a) both k_p and k_q merely contain small odd prime factors.
   (b) both $p = 2k_p \cdot p' + 1$ and $q = 2k_q \cdot q' + 1$ are primes.
   (c) $\gcd(k_p, p') = \gcd(k_q, q') = \gcd(k_p, k_q) = \gcd(p', q') = 1$.
4. Let $k = k_p \cdot k_q$ and $n = p \cdot q$.

5. Choose $a \in \mathbb{Z}_n^*$ such that $\left(\frac{a}{n}\right) = -1$.
6. Choose $g_1 \in \mathbb{Z}_n^*$ such that $\mathrm{ord}_p(g_1) = k_p$ and $\mathrm{ord}_q(g_1) = k_q$ (see [3] and [4] for details on how to do this efficiently.)
7. Choose $g_2 \in \mathbb{Z}_n^*$ such that g_2 is a common primitive root w.r.t the modulus p and the modulus q.
8. Choose two hash functions $H_0 : \{0,1\}^* \to \mathbb{Z}_n^3$ and $H : \mathbb{Z}_n^3 \to \mathbb{Z}_n$.
9. Let $mpk = (n, e, a, g_1, g_2, H_0, H)$ and $msk = (p, q, k_p, k_q)$

`Ext`: On input an identity `id`, the PKG computes the corresponding private key $sk_{\mathtt{id}}$ as follows:

1. Let $(c, d, h') = H_0(\mathtt{id})$.
2. If $\left(\frac{h'}{n}\right) = -1$ then let $h = h' \cdot a \bmod n$ else let $h = h'$.
3. Compute $y = h^{2e} \bmod n$.
4. Find $z < k$ by solving the k-residue discrete logarithm problem $y \equiv g_1^z \pmod n$.
5. Choose $x_2 \in \mathbb{Z}_n$ at random.
6. Find $x_1 < k$ by solving the k-residue discrete logarithm problem $(c/g_2^{x_2})^{2e} \equiv g_1^{x_1} \pmod n$.
7. If x_1 is even then goto Step 5.
8. Choose $y_2 \in \mathbb{Z}_n$ at random.
9. Find $y_1 < k$ by solving the k-residue discrete logarithm problem $(d/g_2^{y_2})^{2e} \equiv g_1^{y_1} \pmod n$.
10. If y_1 is even then goto Step 8.
11. Let $sk_{\mathtt{id}} = (x_1, x_2, y_1, y_2, z)$.

`Enc`: On input a message m from $\mathbb{Z}_n$ and an identity `id`, the encryptor performs the following steps:

1. Let $(c, d, h') = H_0(\mathtt{id})$.
2. If $\left(\frac{h'}{n}\right) = -1$ then let $h = h' \cdot a \bmod n$ else let $h = h'$.
3. Compute $y = h^{2e} \bmod n$.
4. Choose $r \in \mathbb{Z}_n$ at random and computes the ciphertext $c = (u_1, u_2, w, v)$ as follows.

$$u_1 = g_1^r \bmod n, \quad u_2 = g_2^r, \quad w = h^{2e \cdot r} m, \quad \alpha = H(u_1, u_2, w) \quad \text{and} \quad v = c^r d^{r\alpha}.$$

`Dec`: On input a ciphertext $c = (u_1, u_2, w, v)$ under an identity `id` and a private key $sk_{\mathtt{id}} = (x_1, x_2, y_1, y_2, z)$, the user with identity `id` performs the following steps:

1. Let $\alpha = H(u_1, u_2, w)$.
2. Validate the ciphertext by checking the following equality

$$u_1^{x_1 + y_1\alpha} u_2^{2e(x_2 + y_2\alpha)} \overset{?}{\equiv} v^{2e} \pmod n.$$

3. If the validation pass, output $m = w/u_1^z \bmod n$; otherwise, output $\perp$.

Remark 2. In the above scheme, with the purpose to evade square-root attacks, we adopt two mechanisms in setting private key $sk_{\mathtt{id}} = (x_1, x_2, y_1, y_2, z)$. The first is to let $\left(\frac{h}{n}\right) = 1$. Then even if z is even, one cannot launch a successful square-root attack from the equality $h^{2e} \equiv g_1^x \pmod n$ (cf. Remark 1). The second is to let both x_1 and y_1 be odd. By doing so, one has no way to obtain an non-trivial equality $A^2 \equiv B^2 \pmod n$ for some different A and B from the parities of x_1, x_2, y_1 and y_2.

Remark 3. Note that it is also possible to derive an IBE scheme by coupling our method with the idea for building the so-called miniature CCA2 PKE scheme due to Boyen [2]. In fact, it is also possible to derive identity-based signatures (IBSs) by coupling our method with some DL-based or DDH-based signature schemes, such as the well-known Elgamal signature [8], Schnorr signature [12], etc. In addition, we are now considering how to develop similar constructions but without keeping k secret.

References

1. D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In *CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer-Verlag, 2001.
2. Xavier Boyen. Miniature CCA2 PK encryption: tight security without redundancy. In *ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 485–501. Springer-Verlag, 2007.
3. Zhenfu Cao. *Public-key Cryptography (in Chinese)*. Heilongjiang Education Press, 1993.
4. Zhenfu Cao, Xiaolei Dong, Licheng Wang, and Jun Shao. More efficient cryptosystems from k^{th} power residues. *Cryptology ePrint Archive: Report 2013/569*, pages 1–22, 2013.
5. C. Cocks. An identity-based encryption scheme based on quadratic residues. In *Proceedings of Cryptography and Coding*, volume 2260 of *Lecture Notes in Computer Science*, pages 360–363. Springer-Verlag, 2001.
6. Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *CRYPTO 1998*, volume 1462 of *Lecture Notes in Computer Science*, pages 13–25. Springer-Verlag, 1998.
7. C. Gentry D. Boneh and M. Hamburg. Space-efficient ibe without pairings. In *FOCS 2007*, pages 647–657. IEEE Computer Society, 2007.
8. Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.
9. E. Fujisaki and T. Okamoto. How to enhance the security of public-key encryption at minimum cost. In *PKC 1999*, volume 1560 of *Lecture Notes in Computer Science*, pages 53–68. Springer-Verlag, 1999.
10. E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *CRYPTO 1999*, volume 1666 of *Lecture Notes in Computer Science*, pages 537–554. Springer-Verlag, 1999.
11. K.G. Paterson and S. Srinivasan. On the relations between non-interactive key distribution, identity-based encryption and trapdoor discrete log groups. *Designs, Codes and Cryptography*, 52(2009):219–241, 2009.
12. C. P. Schnorr. Efficient identification and signatures for smart cards. In *CRYPTO 1989*, volume 435 of *Lecture Notes in Computer Science*, pages 239–252. Springer-Verlag, 1990.
13. A. Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO 1984*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer-Verlag, 1985.