New Efficient Identity-Based Encryption 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 the above scheme, which may give a way to find ibe schemes without pairings or lattice. Essentially, the security of our identity-based encryption scheme is rooted in the intractability assumption of integer factorization. We believe that our construction has 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 [9], 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 the 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 [4], 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 [6] 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 [8], observably *slower than* in the Cocks system [6]. Note that in 2009, Paterson and Srinivasan [8] 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 *very 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 considering the so-called $(p-1)$-factoring method, B should not too small. Therefore, it is still a challenge to find *efficient* IBEs without using pairings or lattices. Here, the adjunct word *efficient* means at least three aspects, i.e., efficient in space, in encryption/decryption speed and in private key generation.

In this paper, we propose an efficient construction of IBE 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 construction is based on an elaborate coupling of IF assumption and RDDH assumption: the latter enables uses to perform Elgamal-like encryption/decryption [7], with a slight modification enlightened by the Cramer-Shoup scheme [5], while the former enables PKG to extract proper private keys according to arbitrary given identities. Our scheme is compact and efficient: the ciphertext expansion factor is 3, and the encryption (resp. decryption) needs only three (resp. two) modular exponentiations. In addition, the private key generation algorithm is 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 $(i = 1, \cdots, s)$. In summary, our 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 Speed	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 Scheme Description

Our scheme consists of the following four algorithms:

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

1. Choose two safe primes p' and q', and then sets $n' = p' \cdot q'$.
2. Choose another safe prime p'' and let $e = n' \cdot p''$.
3. Choose two positive integers k_p and k_q such that
   (a) both k_p and k_q merely contain small 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 $n = p \cdot q$. (Note that we have $\phi(n) = 4kn'$, now.)
5. Choose $g \in \mathbb{Z}_n^*$ such that $\mathrm{ord}_p(g) = k_p$ and $\mathrm{ord}_q(g) = k_q$ (see [2] and [3] for details on how to do this efficiently.)
6. Choose $g_1 \in \mathbb{Z}_n^*$ such that g_1 is a common primitive root w.r.t the modulus p and the modulus q.
7. Choose a hash function $H : \{0,1\}^* \to \mathbb{Z}_n$.
8. Let $mpk = (n, e, g, g_1, H)$ 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. Compute $h = H(\mathtt{id}) \bmod n$.
2. Choose $z \in \mathbb{Z}_n^*$.
3. Let $y = (h/g_1^z)^{4e} \bmod n$.
4. Find $x < k$ by solving the k-residue discrete logarithm problem $y \equiv g^x \pmod{n}$. [1]
5. If x is even then goto Step 2.
6. Let $sk_{\mathtt{id}} = (x, z)$.

`Enc`: On input a message m from $\mathbb{Z}_n$ and an identity `id`, the encryptor computes the ciphertext $c = (c_1, c_2, c_3)$ as follows.

$$c_1 = g^r \bmod n, \quad c_2 = g_1^r \bmod n, \quad c_3 = h^{4e\cdot r} \cdot m \bmod n$$

where $h = H(\mathtt{id}) \bmod n$, and r is a random number from $\mathbb{Z}_n$.

`Dec`: On input a ciphertext $c = (c_1, c_2, c_3)$ under an identity `id` and a private key $sk_{\mathtt{id}} = (x, z)$, the user with identity `id` computes the message m by

$$m = \frac{c_3}{c_1^x c_2^{4e\cdot z}} \bmod n.$$

Apparently, the above IBE scheme is consistent considering that $\mathrm{ord}_n(g) = k$ and

$$c_3 \equiv h^{4e\cdot r} \cdot m \equiv (y \cdot g_1^{4e\cdot z})^r \cdot m \equiv (g^r)^x \cdot (g_1^r)^{4e\cdot z} \cdot m \equiv c_1^x \cdot c_2^{4e\cdot z} \cdot m \pmod{n}.$$

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 the above scheme, which may give a way to find ibe schemes without pairings or lattice.

Definition 1 (k-Residue Discrete Logarithm, k-RDL [3]). *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 $x = RDL_{b,p}^k(y)$.*

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 [2, 3] 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.

[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 $x = \mathbf{CRT}(k_p, x_p, k_q, x_q)$.

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 $g^c = g^{ab} \pmod{n}$.*

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. Zhenfu Cao. *Public-key Cryptography (in Chinese)*. Heilongjiang Education Press, 1993.
3. Zhenfu Cao, Xiaolei Dong, Licheng Wang, and Jun Shao. More efficient cryptosystems from k^{th} power residues. *Cryptology ePrint Archive: Report 2013/550*, pages 1–21, 2013.
4. 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.
5. 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.
6. C. Gentry D. Boneh and M. Hamburg. Space-efficient ibe without pairings. In *FOCS 2007*, pages 647–657. IEEE Computer Society, 2007.
7. Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.
8. 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.
9. 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.