Information Processing Letters 115 (2015) 351–358

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

An efficient ID-based cryptographic encryption based on discrete logarithm problem and integer factorization problem

Chandrashekhar Meshram

Department of Mathematics, R.T.M. Nagpur University, Nagpur (M.S.), India

ARTICLE INFO

Article history:
Received 18 May 2014
Received in revised form 6 October 2014
Accepted 13 October 2014
Available online 24 October 2014
Communicated by Jinhui Xu

Keywords:
Cryptography
Identity-based encryption
Integer factorization problem
Discrete logarithm problem
Random oracle

ABSTRACT

ID-based encryption (identity-based) is a very useful tool in cryptography. It has many potential applications. The security of traditional ID-based encryption scheme wholly depends on the security of secret keys. Exposure of secret keys requires reissuing all previously assigned encryptions. This limitation becomes more obvious today as key exposure is more common with increasing use of mobile and unprotected devices. Under this background, mitigating the damage of key exposure in ID-based encryption is an important problem. To deal with this problem, we propose to integrate forward security into ID-based encryption. In this paper, we propose a new construction of ID-based encryption scheme based on integer factorization problem and discrete logarithm problem is semantically secure against chosen plaintext attack (CPA) in random oracle model. We demonstrate that our scheme outperforms the other existing schemes in terms of security, computational cost and the length of public key.

1. Introduction

An ID-based encryption provides a convenient way to do public key encryption without the burden of distributing public keys. In an ID-based encryption scheme, the sender of a message can encrypt the message using the identity of the receiver as the public key. Therefore, there is no need for the receiver to show his public key certificate to the sender. Such a cryptosystem is particularly useful in applications where message receivers are not always available to present public key certificates. In 1984 Shamir [18] introduced the concepts of ID-based cryptography to simplify the key management problem. In ID-based cryptography, the unambiguous identity of a user (such as e-mail address, social security number etc.) is used as the public key, while the private key associated with that identity (the public key) is computed and issued secretly to the user by a trusted third party called private key generator (PKG). In such a setting, the only thing that should be certificated is the public parameters of the PKG, so ID-based cryptography drastically reduces the needs for certificates. It was not until 2001 that two ID-based encryption schemes were proposed by Cocks [6] and Boneh and Franklin [1], respectively. In their seminal paper [3], Boneh and Franklin used a category of bilinear maps as the basis of their construction. This leads a number of ID-based encryption schemes [1,2,20], among others based on bilinear maps.

Although there have been a number of efficient ID-based encryption schemes, these schemes are still significantly slower than regular public key cryptosystems. For example, the Boneh–Franklin scheme can be 400 times slower than ElGamal in terms of encryption [9]. In practice, applications often need fast encryption and decryption operations. Consequently, the time costs of existing ID-based encryption schemes may not meet the need of practice.

After 2003, several ID-based encryption schemes [4,5,10,13,14,16,17,19] have been proposed. But in these schemes, the public key of each entity is not only an identity, but also some random number selected either by the entity or by the trusted authority. But which makes

E-mail address: cs_meshram@rediffmail.com.

http://dx.doi.org/10.1016/j.ipl.2014.10.007
0020-0190/© 2014 Elsevier B.V. All rights reserved.

the ID-based encryption an active research field in recent years.

The first efficient ID-based encryption scheme was proposed by Boneh and Franklin [3,4]. The novel approach they use is based on a class of bilinear maps. Following their work, a number of ID-based encryption schemes using bilinear maps were proposed. For example, Boneh and Boyen [1] designed a secure ID-based encryption scheme without random oracles; Waters [20] presented an efficient and secure ID-based encryption scheme without random oracles; Boneh and Boyen [2] gave another efficient ID-based encryption scheme without random oracles, which is secure in the selective identity model. Nevertheless, as pointed out in [9], even the efficient schemes like [3] are still significantly slower than regular public key cryptosystems like ElGamal. In contrast, our ID-based encryption scheme is almost as fast as the ElGamal cryptosystem both in encryption and in decryption. Heng and Kurosawa [11,12] used a polynomial based approach to construct an ID-based encryption scheme. Their scheme does not need random oracles and is semantically secure under the integer factorization problem and discrete logarithm problem assumption. However, their scheme is significantly slower than ElGamal as well.

Our contribution. As outlined in the above, unfortunately we found that all the existing ID-based encryption schemes based on integer factorization problem and ID-based encryption scheme based on discrete logarithm problem cannot be regarded as secure. Therefore, our main contribution in this paper is to fill this gap by proposing a provably secure ID-based encryption scheme based on integer factorization and discrete logarithm problem. The time costs of encryption and decryption in our ID-based encryption scheme are those of ElGamal. More precisely, except the first encryption operation for each identity, all encryption and decryption operations have the same cost as the corresponding operations of ElGamal. We also provide a formal security proof for semantically secure against CPA under the integer factorization and discrete logarithm problem assumption in the random oracle model using the rewinding technique introduced by Boneh and Franklin [3].

Organization. The rest of this paper is organized as follows: Some preliminaries are introduced in Section 2. Our proposed ID-based encryption scheme based on IFP and DLP is presented in Section 3. Efficiency of the proposed ID-based encryption scheme is discussed in Section 4. The security analysis and security proof of our new scheme are presented in Section 5. The Performance comparison of other ID-based encryption schemes is discussed in Section 6. Finally, Section 7 concludes the paper.

2. Preliminaries

In this section, we describe some background knowledge used in this paper, including discrete logarithm problem and integer factorization problem [18].

2.1. Related definitions

Definition 2.1.1 *(IFP).* Let $N = p * q$ and $\gcd(e, \phi(N)) = 1$, where p and q are randomly safe primes. Given $y \in Z_N^*$, it is computationally intractable to derive x such that $y = x^e \bmod N$ with the knowledge of e and N.

Definition 2.1.2 *(DLP over Z_N^*).* Let $N = p * q$ and g be a primitive root for both Z_p^* and Z_q^*, where p and q are randomly safe primes. Given $y = g^x \bmod N$, it is computationally intractable to derive x.

2.2. Complexity assumption

The security of our scheme relies on a standard complexity-theoretic assumption, the IFP and DLP assumption. We review it as follows.

2.2.1. IFP and DLP assumption

Let g be a generator of a multiple group G, where $|G| = q$. The challenger randomly chooses $a, b, c \in Z_p^*$ and a bit $\sigma \in \{0, 1\}$, uniformly and independently. If $\sigma = 1$ he outputs the tuple $(g, g^a \bmod n, g^b \bmod n, g^{ab} \bmod n)$, otherwise, he outputs the tuple $(g, g^a \bmod n, g^b \bmod n, g^c \bmod n)$, where $n = p * q$. Then the adversary outputs a guess σ' of σ. An adversary has an ϵ advantage if

$$\left|\Pr[\sigma = \sigma'] - \frac{1}{2}\right| = \epsilon.$$

Definition 2.2.1. The decisional ϵ-IFP and DLP assumption holds in G if no PPT adversary has at least ϵ advantage in solving the below game (see Subsection 5.1).

3. Proposed an ID-based encryption scheme based on integer factorization problem and discrete logarithm problem

In this section, we proposed an ID-based encryption scheme based on integer factorization problem (IFP) and discrete logarithm problem (DLP). Our ID-based encryption scheme is defined to be a four-tuple of algorithms, namely: Setup, Extract, Encryption and Decryption. These algorithms are constructed as follows.

3.1. Setup

By taking in security parameter (k, t), this algorithm will be carried out by PKG as follows:

1. Generate large prime number N, such that $N = p * q$ with $q | p - 1$. Also let $G = \{g^0, g^1, g^2, \ldots, g^{q-1}\}$ be a prime order q subgroup of multiple group Z_N^*, where g is a generator with prime order q.
2. Generate t dimension secret vectors $X = (x_1, x_2, x_3, x_4, \ldots, x_t)$, where x_i is randomly selected from Z_N^*.
3. Generate the corresponding t dimension public vectors $Y = (y_1, y_2, y_3, y_4, \ldots, y_t)$, where $y_i = g^{x_i} \bmod N$ and $i \in (1, t)$.
4. Construct an identity cryptographic hash function $H : \{0, 1\}^* \to \{0, 1\}^t$.