Information Processing Letters ••• (••••) •••–•••

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Breaking an ID-based encryption based on discrete logarithm and factorization problems

Chik How Tan *, Theo Fanuela Prabowo, Duc-Phong Le

Temasek Laboratories, National University of Singapore, 5A Engineering Drive 1, #09-02, Singapore 117411, Singapore

ARTICLE INFO

Article history:
Received 3 March 2015
Received in revised form 28 September 2015
Accepted 29 September 2015
Available online xxxx
Communicated by M. Yamashita

Keywords:
Cryptography
Cryptanalysis
ID-based encryption
Discrete logarithm problem
Factorization problem

ABSTRACT

Identity-based (ID-based) cryptography is very useful as it can simplify the certificate management in public key cryptosystem. Since 2001, researchers have introduced various practical and efficient ID-based encryption schemes. Most of them are based on pairings, under the Diffie–Hellman assumptions. Recently, Meshram [1] proposed a new ID-based encryption scheme which was not based on pairing-based cryptography. He proved that his scheme was secure against adaptive chosen plaintext attack, as its security was based on the difficulty of discrete logarithm and integer factorization problems. However, in this paper, we show that this new ID-based encryption scheme is insecure by presenting a method to recover the secret master key.

1. Introduction

The idea of identity-based (ID-based) cryptography was introduced by Shamir [2] in 1984. It simplifies certificate management in public key cryptosystem by using the identity (e.g., email address, IP address, etc.) of a user as the public key. The private key of a user is computed and provided secretly to the user by a trusted third party called the private key generator (PKG). The first practical ID-based encryption [3] was introduced by Boneh and Franklin in 2001.

Most efficient ID-based encryptions [3–5] are based on pairings, under the variances of Diffie–Hellman assumptions. In [1], Meshram proposed a new ID-based encryption scheme whose security was based on the difficulty of the discrete logarithm problem and the integer factorization problem. His scheme did not rely on pairing-based cryptography and was provably secure against adaptive chosen plaintext attack.

Despite the scheme in [1] being provably secure, in this paper, we point out that under the setting of this ID-based encryption scheme, the integer factorization problem is no longer difficult to solve. We also present a simple polynomial-time algorithm that allows us to fully recover the master key with only t queries to the PKG, where t is part of the system parameters.

The rest of the paper is organized as follows. Section 2 briefly reviews Meshram's ID-based encryption scheme [1], as well as the complexity assumptions on which his scheme is based. In Section 3, we describe our attacks. We also give some numerical examples in this section. In Section 4, we point out some flaws in the security proof given in [1]. Finally, we conclude the paper in Section 5.

2. A review of Meshram's ID-based encryption scheme

In this section, we briefly recall Meshram's ID-based encryption scheme [1]. Before presenting the scheme, we first review the complexity assumptions on which the scheme was based.

* Corresponding author.
E-mail addresses: tsltch@nus.edu.sg (C.H. Tan), tsltfp@nus.edu.sg (T.F. Prabowo), tslld@nus.edu.sg (D.-P. Le).

http://dx.doi.org/10.1016/j.ipl.2015.09.014
0020-0190/

2.1. Complexity assumptions

The integer factorization problem and the discrete logarithm problem are defined as follows:

Definition 2.1 *(Integer factorization problem).* Given a positive integer n, the integer factorization problem is to find the prime factorization of n.

Definition 2.2 *(Discrete logarithm problem).* Let G be a finite cyclic group of order n. Let α be a generator of G, and let $\beta \in G$. The discrete logarithm problem is to find the unique integer x with $0 \le x \le n-1$, such that $\beta = \alpha^x$.

The security of Meshram's ID-based encryption scheme was based on the assumption that it is very difficult to solve the above two problems in general.

2.2. Meshram's ID-based encryption scheme

We describe Meshram's ID-based encryption scheme below:

Setup The setup algorithm is as follows:

- Let t be a positive integer and $H : \{0,1\}^* \mapsto \{0,1\}^t$ be a cryptographic hash function.
- Generate a large number $N = pq$, where p and q are primes such that q is t bits long and $q|(p-1)$.
- Generate an element g of order q in the multiplicative group $Z_N^\times$.
- Generate a random secret vector $X = (x_1, x_2, \ldots, x_t)$, where $x_i \in Z_N^\times$ for all $1 \le i \le t$.
- Compute the corresponding public vector $Y = (y_1, y_2, \ldots, y_t)$, where $y_i := g^{x_i} \bmod N$ for all $1 \le i \le t$.

The PKG keeps $\{p, q, X\}$ as the secret master key and publishes $\{N, g, Y, H\}$ as the system parameter.

Key Extraction To generate the private key and public key for an identity $ID \in \{0,1\}^*$, the key extraction algorithm works as follows:

- Compute $H(ID) =: (h_1, h_2, \ldots, h_t)$, where $h_i \in \{0,1\}$ for all $1 \le i \le t$.
- Compute the private key as follows:

$$x_{ID} := \sum_{i=1}^{t} h_i x_i \bmod N.$$

- Compute the corresponding public key as follows:

$$y_{ID} := \prod_{i=1}^{t} (y_i)^{h_i} \bmod N = g^{x_{ID}} \bmod N.$$

Note that the knowledge of the master key is required to compute the user's private key, but it is not required to compute the public key.

Encryption To encrypt a message $M \in \{0,1\}^*$ for an identity ID, the algorithm chooses a random $r \in Z_N^\times$ and computes

$$C_1 := g^r \bmod N; \quad C_2 := M(y_{ID})^r \bmod N.$$

Then, the ciphertext is given by

$$C := (C_1, C_2).$$

Decryption To decrypt a ciphertext $C = (C_1, C_2)$ for an identity ID, the user simply computes

$$\left(\frac{C_2}{C_1^{x_{ID}}}\right) \bmod N = \left(M \frac{(y_{ID})^r}{(g^r)^{x_{ID}}}\right) \bmod N = M \bmod N.$$

3. Attacking the scheme

3.1. Factorizing N

In this subsection, we show that the integer factorization problem is easy to solve in the setting of Meshram's ID-based encryption scheme.

Proposition 3.1. *Let $N = pq$, where p and q are primes and $q \mid (p-1)$. Suppose $g \in Z_N^\times$ is of order q. Then,* $\gcd(g-1, N) = q$.

Proof. Since g is of order q, we have

$$g^q \equiv 1 \bmod N.$$

Moreover, since $q \mid N$, we see that

$$g^q \equiv 1 \bmod q. \tag{1}$$

By Fermat's Little Theorem (see [6, Chapter 2]), we have

$$g^q \equiv g \bmod q. \tag{2}$$

From eq. (1) and eq. (2), it follows that $g \equiv 1 \bmod q$, or equivalently $q \mid (g-1)$. Since $g \not\equiv 1 \bmod N$, we must have $\gcd(g-1, N) = q$. □

Proposition 3.1 allows us to recover the secret prime factor q. We can then compute the other prime factor as $p = N/q$. Hence, the public key N is totally factored.

Example. Let $q = 251$, $p = 4519 (= 18 \times 251 + 1)$. Then $N = pq = 1134269$, and $\phi(N) = (p-1)(q-1) = 4518 \times 250 = 1129500$. Choose $g = 148593$ as a generator of order q in $Z_N^\times$.[1] Given g and N, the prime factor q can be recovered by computing the greatest common divisor of $g-1$ and N, that is, $q = \gcd(148592, 1134269) = 251$.

3.2. Recovering the secret vector X

In this subsection, we describe a concrete method to recover the secret vector X.

- An adversary randomly selects t identities $ID_1, ID_2, \ldots, ID_t$ such that the t vectors $H(ID_1), H(ID_2), \ldots, H(ID_t)$ are linearly independent over Z_N.

[1] A generator g of order q in $Z_N^\times$ can be found by taking a random element of $Z_N^\times$ and then raising it to the power of $\phi(N)/q$.

Please cite this article in press as: C.H. Tan et al., Breaking an ID-based encryption based on discrete logarithm and factorization problems, Inf. Process. Lett. (2015), http://dx.doi.org/10.1016/j.ipl.2015.09.014