Information Processing Letters 113 (2013) 789–792

Contents lists available at SciVerse ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Improvement on Meshram et al.'s ID-based cryptographic mechanism

Liaojun Pang [a,b,*], Huixian Li [b,c], Qingqi Pei [d], Yumin Wang [d]

[a] School of Life Science and Technology, Xidian University, Xi'an 710071, China
[b] Department of Computer Science, Wayne State University, Detroit, MI 48202, USA
[c] School of Computer Science and Engineering, Northwestern Polytechnical University, Xi'an 710072, China
[d] State Key Lab. of Integrated Service Networks, Xidian University, Xi'an 710071, China

ARTICLE INFO

Article history:
Received 16 August 2012
Received in revised form 20 July 2013
Accepted 23 July 2013
Available online 29 July 2013
Communicated by J. Xu

Keywords:
Cryptography
ID-based cryptosystem
Deadlock
GDLP
IFP

ABSTRACT

Meshram et al. proposed an ID-based cryptosystem based on the generalized discrete logarithm problem (GDLP) and the integer factorization problem (IFP) in 2012, and their contribution lies in that they firstly proposed an idea to construct the ID-based cryptosystem without using the bilinear pair. This scheme can achieve the security goal of protecting data and prevent the adversary from snooping the encrypted data or the user's private key. However, our analyses show that their scheme is still incorrect and has a deadlock problem, because the user cannot carry out the encryption process as expected because it is required for the user to own the key authentication center's private information which is designed to be secret to users. A solution to the deadlock problem is given and an improved scheme is proposed.

1. Introduction

Secure communication requires secure key distribution between users, and the design of effective session key distribution protocols is a hot topic in the field of cryptography [1]. The public key cryptosystem can effectively solve the session key distribution problem in an open network environment, but each user should authenticate the public key of the partner before using it. The public key infrastructure (PKI) is proposed to implement the authentication of the public key, but it leads to large management overheads.

The concept of the identity-based (ID-based) cryptosystem was introduced by Shamir in 1984. According to Shamir's idea, the public key of each user is just extracted from his public identity information, such as e-mail address, ID number [2]. Using each user's public identity as his public key can avoid the problem of authentication of the public key, and it enables users to establish the session key in the non-interactive form. However, Shamir only succeeded in constructing an identity-based signature scheme. Only when Boneh et al. [3] constructed ID-based encryption from the Weil pairing, did the ID-based cryptosystem become practical. However, the bilinear pair operations make the cryptosystems unsuitable to low-performance devices [4].

In 2012, Meshram et al. [5] proposed an ID-based cryptosystem under the security assumptions of the generalized discrete logarithm problem (GDLP) and the integer factorization problem (IFP) without adopting the bilinear pair. However, although their idea is excellent, Meshram et al.'s ID-based cryptosystem is incorrect. This scheme can achieve the security goal of protecting data and prevent the adversary from snooping the encrypted data or the user's private key, but, it also prevents the user from decrypting the ciphertext if the user does not own the key authentication center (KAC)'s private information which is designed to be secret to users. That is to say, without knowing a part of the private key of the key authentication

* Corresponding author at: School of Life Science and Technology, Xidian University, Xi'an 710071, China.
E-mail addresses: ljpang@mail.xidian.edu.cn, liaojun.pang@wayne.edu (L. Pang).

0020-0190/$ – see front matter
http://dx.doi.org/10.1016/j.ipl.2013.07.019

center, the user, who receives a ciphertext sent to him, is unable to decrypt it only with his own private key. In a word, although Meshram et al.'s scheme is secure for protecting data and the user's private key, it has a deadlock problem.

So, in this paper, we shall firstly explain the deadlock problem existing in Meshram et al.'s scheme, and then we shall give a solution to it.

2. Review of Meshram et al.'s identity-based cryptosystem

To describe it briefly, Meshram et al.'s ID-based cryptosystem can be summarized as four related sub-algorithms, namely *Setup*, *Extraction*, *Encryption* and *Decryption*. The *Setup* algorithm is run by KAC to generate its public and private keys. On receiving the register application of a user, KAC shall run the *Extraction* algorithm to generate the private key of this user if the user is identified to be legal. If some user wants to securely send a message to another user, he can run the *Encryption* algorithm to encrypt the message with the identity of the latter. On receiving the ciphertext, the receiver can run the *Decryption* algorithm to decrypt the ciphertext with his private key. Most of the existing ID-based cryptosystems are described in this form [4], so it is easy for readers to understand our description of Meshram et al.'s ID-based cryptosystem, which is shown as follows:

Setup. KAC carries out the following steps:

1. Randomly choose two large (distinct) primes, p and q, roughly of the same size. Let $N = p \cdot q$ and let $n = |N|$ be the bit number of N. (Note: Meshram et al. use t to denote the number of bits of N, but analyses on their scheme show that $t = n$.) Then, compute the Euler-phi function $\varphi(N) = (p-1)(q-1)$.
2. Randomly choose an integer e such that $1 \leqslant e \leqslant \varphi(N)$ and $\gcd(e, \varphi(N)) = 1$, and then use the extended Euclidean algorithm to compute the unique integer d such that $1 \leqslant d \leqslant \varphi(N)$ and $ed \equiv 1 \pmod{\varphi(N)}$.
3. Generate an n-dimensional vector $\vec{a} = (a_1, a_2, \ldots, a_n)$ over $Z^*_{\varphi(N)}$ such that $1 \leqslant a_i \leqslant \varphi(N)$ $(1 \leqslant i \leqslant n)$ and $a_i \neq a_j \bmod \varphi(N)$ $(i \neq j)$. Meshram et al. also gave a simple way to generate such $\vec{a}$ in their paper, and thus we will not repeat it here.
4. Compute another n-dimensional vector $\vec{h} = (h_1, h_2, \ldots, h_n)$ where $h_i = e^{a_i} \bmod N$ $(1 \leqslant i \leqslant n)$.
5. KAC uses $(N, e, \vec{h})$ as his public key and informs it to each entity, and at the same time uses $(\vec{a}, d)$ as his private key and keeps it secret.

Extraction. KAC carries out the following steps to compute the private key of the entity i, whose identity is a k-dimensional binary vector $\mathrm{ID}_i = (x_{i1}, x_{i2}, \ldots, x_{ik})$ such that $x_{ij} \in \{0, 1\}$ $(1 \leqslant j \leqslant k)$:

1. Compute the entity i's extended ID, EID_i, by the following formula:

$$\mathrm{EID}_i = (\mathrm{ID}_i)^e \bmod N = (y_{i1}, y_{i2}, \ldots, y_{in}) \quad \big(y_{ij} \in \{0, 1\}, 1 \leqslant j \leqslant n\big).$$

2. The entity i's private key, s_i, is computed by the inner product of $\vec{a}$ and EID_i as follows:

$$s_i = \vec{a}\,\mathrm{EID}_i = \sum_{j=1}^{n} a_j y_{ij} \pmod{\varphi(N)}.$$

Note that ID_i is used as the public key of the entity i.

Encryption. Assume that entity 2 wants to send message M to entity 1, and entity 2 can encrypt M as follows:

1. Compute entity 1's extended ID, $\mathrm{EID}_1 = (\mathrm{ID}_1)^e = (y_{11}, y_{12}, \ldots, y_{1n})$ from his identity ID_1.
2. Compute

$$\gamma_1 = \prod_{i=1}^{n} h_i^{y_{1i}} \pmod N = \prod_{i=1}^{n} (e^{a_i})^{y_{1i}} \pmod N = e^{\sum_{i=1}^{n} a_i y_{1i} \pmod{\varphi(N)}} \pmod N = e^{s_1} \pmod N$$

   from EID_1 and KAC's public key information $\vec{h}$.
3. Compute $C_0 = M^{e^{s_1}} \pmod N$.
4. Compute the ciphertext $C = C_0^e \pmod N$.

Decryption. Entity 1 does the following steps to recover the plaintext M from the ciphertext C:

1. Compute $\gamma = C^d \pmod N$.
2. Use his private key s_1 to recover M as follows:

$$\gamma^{d^{s_1}} \pmod N \equiv C_0^{d^{s_1}} \pmod N \equiv \big(M^{e^{s_1}}\big)^{d^{s_1}} \pmod N \equiv M^{(ed)^{s_1}} \pmod N \equiv M \pmod N.$$

3. Analyses on Meshram et al.'s cryptosystem

Meshram et al. did a good work, and proposed the above ID-based cryptosystem based on GDLP and IFP. Without adopting the bilinear pair operations, their cryptosystem must be more suitable to low-performance devices than the ones based on the bilinear pair. However, our analyses show that there is still weakness in their cryptosystem.

The weakness that we talk about is that entity 1, who receives a ciphertext sent to him, is unable to decrypt it as expected. Let us recall the *Decryption* algorithm mentioned above. To decrypt the ciphertext C, entity 1 should firstly compute $\gamma = C^d \pmod N$ (see step 1 of the *Decryption* algorithm), where d is a part of the private key of KAC (see step 5 of the *Setup* algorithm) and unknown to entity 1. Similarly, in step 2 of the *Decryption* algorithm, entity 1 needs to use both d and his private key s_1 to compute $\gamma^{d^{s_1}} \equiv M \pmod N$. That is to say, to succeed in decryption, entity 1 must own both d and s_1, and this makes entity 1 unable to carry out the *Decryption* algorithm because d is only known to KAC. It is worth noting that we cannot solve this problem by simply switching e and d used in Meshram et al.'s cryptosystem, because switching e and d will lead to another similar problem that entity 2 is unable to encrypt messages without knowing d. Therefore, although Meshram et al.'s cryptosystem is excellent, some