Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Network and Computer Applications 27 (2004) 191–199
Journal of NETWORK and COMPUTER APPLICATIONS
www.elsevier.com/locate/jnca

Constructing identity-based cryptosystems for discrete logarithm based cryptosystems

Wei-Bin Lee*, Kuan-Chieh Liao

Department of Information Engineering, Feng Chia University, 100 Wenhwa Road, Seatwen Taichung 407, Taiwan, ROC

Received 29 January 2004; received in revised form 16 March 2004; accepted 24 March 2004

Abstract

In 1984, Shamir proposed the concept of the Identity-Based (ID-Based) cryptosystem. Instead of generating and publishing a public key for each user, the ID-Based scheme permits each user to choose his name or network address as his public key. This is advantageous to public-key cryptosystems because the public-key verification is so easy and direct. In such a way, a large public-key file is not required. Since new cryptographic schemes always face security challenges and many discrete logarithm-based cryptographic systems have been deployed, therefore, the purpose of this paper is to design a transformation process that can transfer all of the discrete logarithm based cryptosystems into the ID-based systems rather than re-invent a new system. In addition, no modification of the original discrete logarithm based cryptosystems is necessary.

Keywords: Public-key cryptosystem; Discrete logarithm; Identity-based cryptosystem; Digital signature; Key distribution

1. Introduction

The development of public-key cryptography is a great revolution in cryptography. The digital signature makes e-commerce possible and the key-exchange protocol solves the difficulty of key distribution in conventional encryption. However, since public keys are exposed to the public, an adversary can successfully enter a corresponding fake public key without being detected if there is no effective authentication method. In order to deal with the public-key authentication issue, the concept of the Identity-Based (ID-Based) cryptosystem

* Corresponding author.
E-mail address: lwb@iecs.fcu.edu.tw (W.-B. Lee).

1084-8045/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2004.03.001

was born. This idea was first introduced by Shamir in 1984 (Shamir, 1984). In the ID-Based system, instead of generating a random pair of public and secret keys, the user chooses his name, network address, social security number, etc. as his public key. Because of this, a user needs only to know the 'identity' of his communication partner, and does not need to run an iterative public-key authentication protocol. Therefore, ID-Based cryptosystems enable any pair of users to communicate securely without keeping a large public file directory, without exchanging private or public keys, and without using services provided by a third party.

While Shamir presented an ID-Based digital signature scheme, he failed to construct an ID-Based cryptosystem. Instead, he conjectured the existence of ID-Based cryptosystems. Since then, much research has been devoted to constructing various kinds of ID-Based cryptosystems. Several ID-Based cryptosystems (Tanaka, 1987; Tsai and Hwang, 1990; Tsujii et al., 1987), ID-Based signature schemes (Abe and Okamoto, 2002; Shamir, 1984), and ID-Based key distribution systems (Gunther, 1989; Matsumoto and lmai, 1989; Okamoto and Tanaka, 1989a,b; Tsujii et al., 1993) 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.

In 1991, Maurer and Yacobi (1991) developed a non-interactive ID-Based public-key distribution system. In their scheme, the public keys are self-authenticated and require no further authentication by certificates. However, some problems with this scheme were found, the scheme was modified (Lim and Lee, 1992; Maurer and Yacobi, 1993), and the final version was presented (Maurer and Yacobi, 1996). In 1998, Tseng and Jan (1998) improved the scheme proposed by Maurer and Yacobi, and provided a non-interactive ID-Based public-key distribution system with multi-objectives such as an ID-Based signature scheme, an identification scheme, and a conference key distribution system. In their scheme, the computational complexity of the system is heavy. Therefore, it is necessary to have a powerful computational capability.

Based on the observation that new cryptographic schemes always face security challenges and confidentiality concerns and many discrete logarithm-based cryptographic systems have been deployed, it is acceptable not to re-invent a new system but to construct a transformation model that introduces the concept of the ID-Based system into all discrete logarithm based cryptosystems. The major contribution of our scheme is the key generation phase, which is just a simple transformation process with low computational complexity. No modification of the original design of the discrete logarithm based cryptosystems is necessary. Therefore, the new scheme has the same security as the original one, and retains all of the advantages of the ID-Based system such as public-key forgery prevention, identification, and key management problem reduction.

This paper is organized into four sections. In Section 2, the new ID-Based model and the signature scheme based on our ID-Based model is proposed. In Section 3, the discussion of the security is given. Finally, conclusions are stated in Section 4.

2. Our proposed scheme

A practical model converting a discrete logarithm-based cryptosystem into an ID-Based system is shown in the subsection. The major contribution of our scheme is the key generation phase. Upon the successful creation of a private key, the ID-Based concept can be easily implemented in discrete logarithm-based cryptosystem.

2.1. System setup stage

There is a trusted center (TC), which is responsible for generating the system parameter and the private key for each registered entity in our system The details of the system setup are described as follows.

1. TC chooses a threshold value t represents that any t entities in our system will not conspire together. The security parameter t also determines the minimum bit length of the entity's identity number in our scheme.
2. Let p be a large prime number, where $p-1$ is divisible by a prime q and $\log_2 q > t$, let g be an element of order q in Z_p, x be TC's secret key, and $y = g^x \bmod p$ be the corresponding public key.
3. $\{k_1, k_2, k_3, \ldots, k_t\}$ is the secret information randomly chosen by TC, where $\sum_{i=1}^{t} k_i < q$. And the corresponding public information is $\{K_1, K_2, K_3, \ldots, K_t\}$, where $K_i = g^{ki} \times \bmod p$, for $i = 1, 2, \ldots, t$.
4. Each entity A has a designed unique t-bit identity $\mathrm{ID}_A = \{\mathrm{ID}_{A1}, \mathrm{ID}_{A2}, \ldots, \mathrm{ID}_{At}\}$, where $\mathrm{ID}_{Ai} \in \{0, 1\}$, for $i = 1, 2, 3, \ldots, t$.

Since $\log_2 q > t$, if q is a 160 bits prime number, and p is a 512 bits prime number, the maximal bit length of t is therefore 159 bits. On the other hand, the maximum threshold value we can define is 159. This of course influences the applications for the scheme. Hence, the parameter chosen strategy depends not only on the strength of the discrete logarithm problem but also on how many members will not conspire together.

2.2. Key generation stage

Without loss of generality, assume that the User A wants to join the system Then, TC and User A carry out the following procedure to generate the private key. Besides, the steps for private key generation are shown in Fig. 1.

Step 1. User A sends TC his identity $\mathrm{ID}_A = \{\mathrm{ID}_{A1}, \mathrm{ID}_{A2}, \mathrm{ID}_{A3}, \ldots, \mathrm{ID}_{At}\}$, where $\mathrm{ID}_{Ai} \in \{0, 1\}$, for $i = 1, 2, 3, \ldots, t$.

Step 2. TC checks whether the identity ID_A conforms to a certain format. If it holds, then TC uses his secret information to compute $K_A = \sum_{i=1}^{t} k_i \mathrm{ID}_{Ai} \bmod q$, and

$$\sigma_A = x + K_A k_A \bmod q, \tag{1}$$

where $K_A = \prod_{i=1}^{t} K_i^{\mathrm{ID}_{Ai}} \bmod p$.

Step 3. TC secretly sends σ_A to user A as A's private key.

Step 4. User A checks whether the following equation holds

$g^{\sigma_A} = y K_A^{K_A} \bmod p$, where $K_A = \prod_{i=1}^{t} K_i^{\mathrm{ID}_{Ai}} \bmod p$ can be computed from public information without any problem.

2.3. Our ID-based transformation model

All discrete logarithm based schemes can be easily transferred into ID-Based systems according to our key generation method. Without loss of generality, let p be a large prime

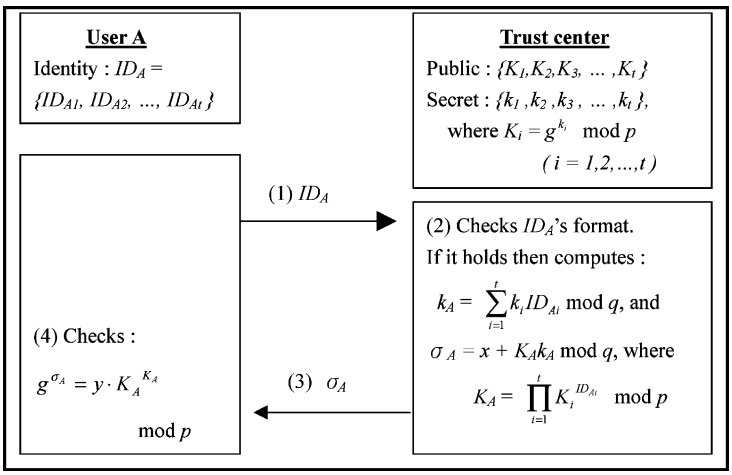

Fig. 1. Private key generation.

number, where $p-1$ is divisible by a prime q, g be an generator of order q in Z_p. Discrete logarithm based system can be defined as $\mathrm{DL} = \{(p, g, X, Y) : Y \equiv g^X (\mathrm{mod}\, p)\}$, where p, g, and Y are public, and X is secret. Then our ID-Based transformation model is constructed as follows:

(1) *Define the format of the identity*

As the original concept of the ID-Based scheme, each entity uses his identity as his public key. Then the user only needs to confirm the identity of his communication partner. Hence, the first step is to check whether the identity conforms to a certain format.

(2) *Calculate the private key according to our key generation procedure*

User A, for example, will receive his private value σ_A according to our key generation process. Since $\{K_1, K_2, K_3, \ldots, K_t\}$ and y are made public in the proposed scheme, everyone can easily compute the corresponding public value of user A by performing the following computations:

$Y_A = g^{\sigma_A} = yK_A^{K_A} \bmod p$, where

$$K_A = \prod_{i=1}^{t} K_i^{\mathrm{ID}_{Ai}} \bmod p. \tag{2}$$

Accordingly, our transformation process is to convert $\mathrm{DL} = \{(p, g, X, Y) : Y \equiv g^X (\mathrm{mod}\, p)\}$ into an ID-Based model as $\mathrm{DL}_{\text{ID-Based}} = \{(p, g, \sigma_A, Y_A) : Y_A = g^{\sigma_A} (\mathrm{mod}\, p)\}$, where σ_A is treated as the private key and Y_A is the corresponding public key. Because the public key Y_A is derived from Eq. (2), therefore, the identity is the only user's key involved in transformation process, so our model can be easily extended any discrete logarithm based scheme into the ID-based one.

2.4. Example

Here we give an example of the ID-Based signature scheme to illustrate our idea. ElGamal signature (ElGamal, 1985) is the first signature based on the discrete algorithm.

Many variants such as Schnorr (1991) and DSA (National Institute of Standards and Technology, 1994) have been designed based on the same assumption. We now review ElGamal signature scheme as follows:

Let m be a document that user A wants to sign, x_A is A's secret key, and $y_A = g^{x_A} \bmod p$ is the corresponding public key. For $K = \{(p, g, x_A, y_A) : y_A = g^{x_A} (\bmod p)\}$ and let $w \in Z_q^*$ is a secret random number, then ElGamal signature can be defined as $\mathrm{sig}_K(m, w) = (r, s)$, where

$$r = g^w \bmod p,$$

and

$$s = w^{-1}(m - x_A r) \bmod q.$$

For m, $r \in Z_p^*$ and $s \in Z_q$, verification is defined as follows:

$$\mathrm{ver}_K(m, r, s) = \text{true} \Leftrightarrow g^m = r^s y_A^r \bmod p.$$

To illustrate our idea, the new ID-Based ElGamal signature will be transferred as follows:

1. Define the identity format for user A as ID_A.
2. Apply our key generation phase, then User A, for example, will receive his private value σ_A. Up to now, $K = \{(p, g, x_A, y_A) : y_A = g^{x_A} (\bmod p)\}$ is converted into an ID-Based model as $K^* = \{(p, g, \sigma_A, Y_A) : Y_A = g^{\sigma_A} (\bmod p)\}$, where σ_A can be obtained as Eq. (1), and Y_A can be computed according to Eq. (2). Therefore, ElGamal signature can be transformed as $\mathrm{sig}_{K^*}(m, w) = (r, s)$, where

$$r = g^w \bmod p,$$

and

$$s = w^{-1}(m - \sigma_A r) \bmod q.$$

For m, $r \in Z_p^*$ and $s \in Z_q$, verification is transformed as follows?

$\mathrm{ver}_{K^*}(m, r, s) = \text{true} \Leftrightarrow g^m = r^s (Y_A)^r \bmod p$, where Y_A can be computed according to Eq. (2).

By the same way, we can easily embed the concept of the ID-Based scheme into other signature schemes based on the discrete logarithm, such as the Schnorr and the DSA signature schemes.

3. Security analysis and discussions

The discrete logarithm problem has played an important role in the construction of some cryptographic protocols. Due to the intractability of the discrete logarithm problem for a large prime p and a generator g, it is infeasible to compute x from the observation of $g^x \bmod p$. Many of the most widely used public-key cryptosystems are based on the assumption that the discrete logarithm is indeed hard to compute (Gordon, 1991; LaMacchia and Odlyzko, 1911; Wells, 1984). The main objective of developers is to

design a protocol that is as difficult to break as the underlying discrete logarithm problem. On the other hand, the verifiable security guarantees that there is no efficient attack on it. Hence, discrete logarithm based schemes are widely deployed. It is meaningful to construct a practice model that embeds the concept of an ID-Based system into all of the cryptosystems based on the discrete logarithm.

In the following, some possible attacks against the proposed scheme are presented:

(1) Because the $\{k_1, k_2, k_3, \ldots, k_t\}$, where $\sum_{i=1}^{t} k_i < q$ is randomly chosen by TC, $K_A = \sum_{i=1}^{t} k_i \mathrm{ID}_{Ai} \bmod q$ and $k_B = \sum_{i=1}^{t} k_i \mathrm{ID}_{Bi} \bmod q$ are possibly equivalent. In order to prevent the collision, the sequence of integers $k_1, k_2, k_3, \ldots,$ and k_t must be chosen carefully. It should be a super increasing list, which means that the sequence satisfies the following property:

$$\sum_{i=1}^{j-1} k_i < k_j,$$

where $j = 2, 3, \ldots, t$.

(2) No one can create a valid private key σ'_A by himself. It is clear that the private key σ'_A should guarantee that the congruence

$$g^{\sigma'_A} = yK_A^{K_A} \bmod p,$$

holds. Even if someone knows the particular value $yK_A^{K_A}$, the calculation of σ'_A for the above equation implies the computation of the discrete logarithm. Since $\sigma_A = x + K_A k_A \bmod q$, the knowledge of TC's private key x is necessary to obtain a valid σ_A. Thus, it is computationally infeasible for anyone to create a private key without the assistance of TC.

(3) No less than t members can conspire together to obtain TC's secret information $\{k_1, k_2, k_3, \ldots, k_t\}$, or TC's secret key x.

If we have the following t linear equations

$$\sigma_A = x + K_A k_A \bmod q = x + K_A(k_1 \mathrm{ID}_{A1} + k_2 \mathrm{ID}_{A2} + \cdots + k_t \mathrm{ID}_{At}) \bmod q,$$

$$\sigma_B = x + K_B(k_1 \mathrm{ID}_{B1} + k_2 \mathrm{ID}_{B2} + \cdots + k_t \mathrm{ID}_{Bt}) \bmod q,$$

$$\sigma_C = x + K_C(k_1 \mathrm{ID}_{C1} + k_2 \mathrm{ID}_{C2} + \cdots + k_t \mathrm{ID}_{Ct}) \bmod q,$$

$$\vdots$$

we have $t + 1$ unknown numbers x, $k_1, k_2, \ldots,$ and k_t. Hence we need $t + 1$ polynomial equations to obtain x, $k_1, k_2, k_3, \ldots,$ and k_t. It is clear that more than $t + 1$ participants should cooperate together to obtain TC's secret information $\{k_1, k_2, k_3, \ldots, k_t\}$, or TC's secret key x. This is obviously a contradiction to our assumption that no t or above entities will conspire together.

(4) Because the private key is derived by

$$\sigma_A = x + K_A k_A \bmod q = x + K_A(k_1 \mathrm{ID}_{A1} + k_2 \mathrm{ID}_{A2} + \cdots + k_t \mathrm{ID}_{At}) \bmod q.$$

Then, the users might conspire together to obtain TC's secret key x, by using some special identity values, such as (1,0,0,…,0), (0,1,0,…,0) (1,1,0,…,0), etc. But our proposed

scheme can resist the attack, because TC will check whether the identity conforms to a certain format in the key generation stage.

Therefore, we show that the key generation phase is secure if secret information $k_1, k_2, k_3, \ldots, k_t$, and x do not leak out. No one except TC can generate the valid secret key. According to the previous discussions, our ID-Based system is as secure as the original discrete logarithm-based cryptosystem.

In our scheme, since the public key of each entity is just the identity, it perfectly satisfied the original concept of the Shamir's ID-Based scheme. Moreover, the computation load of the trust center is just some modular multiplications and modular additions by computing

$$k_A = \prod_{i=1}^{t} K_i^{\mathrm{ID}_{Ai}} \bmod p,$$

$$K_A = \sum_{i=1}^{t} k_i \mathrm{ID}_{Ai} \bmod q,$$

and

$$\sigma_A = x + K_A k_A \bmod q,$$

and the computation load of each user is just two modular exponentiations and some modular multiplications by computing

$$K_A = \prod_{i=1}^{t} K_i^{\mathrm{ID}_{Ai}} \bmod p,$$

and

$$g^{\sigma_A} = y K_A^{K_A} \bmod p.$$

From the above discussion, our construction is an efficient and secure ID-Based scheme to be based on the discrete logarithm problem.

4. Conclusions

Based on the fact that re-inventing a new scheme involves many uncertain and unknown threats, and discrete logarithm based schemes are widely deployed, our goal is to construct an ID-Based transformation model for discrete logarithm based scheme rather than re-invent a new one. The concept of the ID-Based system can be easily embedded into all of the discrete logarithm-based cryptosystems without changing their original design. This solution can be directly deployed in the currently used system with very low cost. Therefore, our new scheme is more practical and has the same security as the original discrete logarithm-based system.

References

Abe M, Okamoto T. Delegation chains secure up to constant length. IEICE Trans Fundam 2002;E85-A(1):110–6.
ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inf Theory 1985;31(4):469–72.
Gordon DM. Discrete logarithms using the number field sieve; 1991. Preprint, 28.
Gunther CG. An identity-based key exchange protocol. Cryptology—Eurocrypt'89. New York: Springer; 1989. p. 29–37.
LaMacchia BA, Odlyzko AM. Computation of discrete logarithms in prime fields. Des Codes Cryptogr 1911;1: 46–62.
Lim CH, Lee PJ. Modified Maurer–Yacobi's scheme and its application. Proc Auscrypt'92 1992;308–23.
Matsumoto T, lmai H. On the key predistribution system. Cryptology—Eurocrpt'89. New York: Springer; 1989. p. 29–37.
Maurer UM, Yacobi Y. Non-interactive public key cryptography. Cryptology—Eurocrypt'91. New York: Springer; 1991. p. 498–507.
Maurer UM, Yacobi Y. A remark on a noninteractive public-key distribution system. Proc Eurocrpt'92 1993; 458–60.
Maurer UM, Yacobi Y. A non-interactive public-key distribution system. Des Codes Cryptogr 1996;9(3): 305–16.
National Institute of Standards and Technology, NIST FIPS PUB 186, May 1994. Digital Signature Standard. US Department of Commerce.
Okamoto E, Tanaka K. Identity-based information security management for personal computer networks. IEEE J Sel Areas Commun 1989;7(2):290–4.
Okamoto E, Tanaka K. Key distribution system based on identification information. IEEE J Sel Areas Commun 1989;7(4):481–5.
Schnorr CP. Efficient signature generation for smart cards. J Cryptology 1991;4(3):161–74.
Shamir A. Identity-based cryptosystem and signature schemes. Cryptology—Crypto'84. New York: Springer; 1984. p. 47–53.
Tanaka H. A realization scheme for the identity-based cryptosystem. Proc Crypto'87 1987;340–9.
Tsai YW, Hwang T. ID-based public key cryptosystems based on Okamoto and Tanaka's ID-based one way communication scheme. Electron Lett 1990;26(10):666–8.
Tseng YM, Jan JK. ID-based cryptographic schemes using a non-interactive public-key distribution system. The 14th Annual Computer Security Applications Conference; 1998. p. 237–43.
Tsujii S, Itoh T, Kurosawa K. ID-based cryptosystem using discrete logarithm problem. Electron Lett 1987;23: 1318–20.
Tsujii S, Chao J, Araki K. A simple ID-based for key sharing. IEEE J Sel Areas Commun 1993;11(5):730–4.
Wells Jr AL. A polynomial form for logarithms modulo a prime. IEEE Trans Inf Theory 1984;845–6.

Wei-Bin Lee received his BS degree from the Department of Information and Computer Engineering, Chung-Yuan Christian University, Chungli, Taiwan, in 1991 and his MS degree in Computer Science and Information Engineering from National Chung Cheng University, Chiayi, Taiwan in 1993. He received his PhD degree in 1997 from National Chung Cheng University. Since 1999, he has been with the Department of Information Engineering at Feng Chia University, where he is currently an associate professor. His research interests currently include cryptography, information security management, steganography, and network security. He is an honorary member of the Phi Tau Phi Scholastic Honor Society.

Kuan-Chieh Liao received his BS degree from the Department of Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan, in 2001, and his MS degree in Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan, in 2002. He is currently pursuing his PhD degree in Department of Information Engineering and Computer Science, Feng Chia University. His research interests currently include cryptography, steganography, and network security.