ID-Based Cryptographic Schemes for User Identification, Digital Signature, and Key Distribution

Lein Harn and Shoubao Yang

Abstract— **In 1984, Shamir introduced the concept of an identity-based cryptosystem. In this system, each user needs to visit a key authentication center (KAC) and identify himself before joining a communication network. Once a user is accepted, the KAC will provide him with a secret key. In this way, if a user wants to communicate with others, he only needs to know the "identity" of his communication partner and the public key of the KAC. There is no public file required in this system. However, Shamir did not succeed in constructing an identity-based cryptosystem, but only in constructing an identity-based signature scheme. In this paper, we propose three identity-based cryptographic schemes based on the discrete logarithm problem: the user identification scheme, the digital signature scheme, and the key distribution scheme.**

I. Introduction

In a network environment, a secret session key needs to be shared between two users to establish a secret communication. While the number of users in the network is increasing, key distribution will become a serious problem. In 1976, Diffie and Hellman [1] introduced the concept of the public key distribution system (PKDS). In the PKDS, each user needs to select a secret key and compute a corresponding public key stored in the public directory. The common secret session key, which will be shared between two users, can then be determined by either user, based on his own secret key and the partner's public key. Although the PKDS provides an elegant way to solve the key distribution problem, the major concern is the authentication of the public keys used in the cryptographic algorithm.

Many attempts have been made to deal with the public key authentication issue. Kohnfelder [2] used the RSA digital signature scheme to provide public key certification. His system involves two kinds of public key cryptography: one is in modular p, where p is a large prime number; the other is in modular n, where $n = pq$, and p and q are large primes. Blom [3] proposed a symmetric key generation system (SKGS) based on secret sharing schemes. The problems of SKGS, however, are the difficulty of choosing a suitable threshold value and the requirement of large memory space for storing the secret shadow of each user.

In 1984, Shamir [4] introduced the concept of an identity-based cryptosystem. In this system, each user needs to visit a key authentication center (KAC) and identify himself before joining the network. Once a user is accepted, the KAC will provide him with a secret key. In this way, a user needs only to know the "identity" of his communication partner and the public key of the KAC, together with his secret key, to communicate with others. There is no public file required in this system. However, Shamir did not succeed in constructing an identity-based cryptosystem, but only in constructing an identity-based signature scheme. Since then, much research has been devoted, especially in Japan, to various kinds of ID-based cryptographic schemes. Okamoto *et al.* [5] proposed an identity-based key distribution system in 1988, and later, Ohta [6] extended their scheme for user identification. These schemes use the RSA public key cryptosystem [7] for operations in modular n, where n is a product of two large primes, and the security of these schemes is based on the computational difficulty of factoring this large composite number n. Tsujii and Itoh [8] have also proposed an ID-based cryptosystem based on the discrete logarithm problem. Most recently, Tsujii and Chao [9] proposed a noninteractive ID-based key sharing system.

In this paper, we propose three identity-based cryptographic schemes based on the discrete logarithm problem in GF(p), where p is a large prime. Our schemes can provide user identification, digital signature, and key distribution. Since our schemes are based on the Agnew *et al.* digital signature scheme [10], we will first review their scheme in the next section. User identification scheme, digital signature scheme, and key distribution scheme will be discussed in Sections III, IV, and V, respectively.

II. Review of the Agnew *et al.* Digital Signature Scheme

We now review a digital signature scheme proposed by Agnew *et al.* [10] in 1990. This scheme was due to ElGamal's signature scheme [11] based on the discrete logarithm problem.

We start with a large prime p and a primitive element α of GF(p), which are all known to the public. In order to provide adequate security, Pohlig and Hellman [12] indicate that p should be selected such that $p - 1$ contains at least one large prime factor. They recommend choosing $p = 2p' + 1$, where p' is a large prime too. A one-way function f also needs to be made public.

In this cryptosystem, each user selects a random exponent from GF(p) as its private key. Suppose A randomly selects a number x_A from [0, $p - 1$] with $gcd(x_A, p - 1) = 1$. Then A computes

$$y_A = \alpha^{x_A} \bmod p$$

Manuscript received May 1992.

L. Harn is with the Computer Science Telecommunications Program, University of Missouri–Kansas City, Kansas City, MO 64110.

S. Yang is with the Department of Computer Science, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China.

IEEE Log Number 9206688.

as A's public key. Assuming A wants to sign a message m, where $0 \leq m \leq p-1$, A randomly selects a number k from $[0, p-1]$ and computes

$$r = \alpha^k \bmod p.$$

A now solves the congruence

$$m' = kr + x_A s \bmod p - 1,$$

or

$$s = (m' - kr)x_A^{-1} \bmod p - 1$$

for the integer s, where $0 \leq s \leq p-1$ and $m' = f(m)$. The one-way function f is used to increase the redundancy of m to avoid ElGamal's attack 5 [11]. The signature for message m is then the ordered pair (r, s).

Upon receiving the set of $\{m, r, s\}$, any user can verify the signature of message m as

$$\alpha^{m'} = r^r y_A^s \bmod p, \qquad \text{where } m' = f(m).$$

III. Identity- Based User Identification Scheme

Gunther and Boveri [13] proposed a user identification scheme based on ElGamal's signature scheme. However, in order to authenticate a user, additional zero-knowledge proof protocols, such as the Chaum, Evertse, and van de Graaf protocol [14], are required. In our scheme, user identification can be achieved directly through a challenge-response-type procedure.

Generally, an identity-based cryptosystem consists of three phases: the initiation phase, user registration phase, and application phase. The first two phases are applicable to all different applications. Since the digital signature and key distribution schemes are derived from the user identification scheme, we present the user identification scheme first. The procedure to identify user i can be described as follows.

Initiation Phase: The key authentication center (KAC) selects a one-way function f, a large prime p, and a primitive element α of GF(p), which are all known to the public. p should be selected such that $p = 2p' + 1$, where p' is also a large prime. A random number $x \in [1, p-1]$, with $gcd(x, p-1) = 1$, is selected as KAC's private key which is used to compute KAC's public key, $Y = \alpha^x \bmod p$. We note that due to the property of $gcd(x, p-1) = 1$, the public key Y is also a primitive element of GF(p).

User Registration Phase: Each user of the communication facility needs to visit the KAC before he can communicate with other users secretly. At this registration phase, user i will present his identity ID_i to the KAC. If user i is acceptable, the KAC computes an extended identity EID_i for user i as

$$EID_i = f(ID_i),$$

and the signature (r_i, s_i) of EID_i as

$$s_i = (EID_i - k_i r_i)x^{-1} \bmod p - 1$$

where $r_i = \alpha^{k_i} \bmod p$ and k_i is randomly selected from $[1, p-1]$. We note here that due to ElGamal's attack 5 [11], which allows an intruder to use a known legitimate signature of a certain message to generate legitimate signatures for other messages, our scheme is designed to sign the extended user identity EID_i, rather than directly signing the original user identity ID_i. We also note that no k_i should be used repeatedly. Otherwise, the collusion of users can uncover the KAC secret key x. As we will see later, s_i is actually user i's secret key.

User Identification Phase: At this stage, let us see how user i proves his identity to a verifier without revealing his secret key s_i. We use a challenge-response-type interactive protocol here. The procedure can be described as follows.

Step 1: User i sends (ID_i, r_i) to the verifier.

Step 2: The verifier randomly selects an odd number $\nu \in [1, p-1]$ such that $gcd(\nu, p-1) = 1$ (i.e., $\nu^{-1} \bmod p-1$ does exist), and computes

$$W = Y^\nu \bmod p, \text{ where } Y \text{ is KAC's , public key.}$$

W is sent back to user i.

Step 3: User i computes

$$Z = W^{s_i} \bmod p$$

and sends Z back to the verifier.

Step 4: The verifier uses Z and the extended user identity EID_i of ID_i to verify the following equation:

$$\alpha^{EID_i} = r_i^{r_i} Z^{\nu^{-1}} \bmod p.$$

If the above equation holds, user i is then identified.

Security: In order to analyze the security of the above scheme, we propose five possible attacks here. As we can see, none of them can break our scheme.

Attack 1: Any intruder knows Z, W, p, and $Z = W^{s_i} \bmod p$. Trying to solve s_i from this information is always equivalent to computing the discrete logarithm over GF(p). Thus, user i's secret key s_i will never be revealed to the public.

Attack 2: An intruder might try to impersonate user i by developing some relations between two challenged questions ν and ν'. Since $Z = Y^{\nu s_i} \bmod p$ and $Z' = Y^{\nu' s_i} \bmod p$, by knowing Z, ν, and ν', the intruder can derive Z' as $Z' = Z^{\nu^{-1}\nu'} \bmod p$ without knowing s_i. However, trying to obtain ν from W is equivalent to computing the discrete logarithm.

Attack 3: Given (ID_i, r_i, Y) as public known information and $\alpha^{EID_i} = r_i^{r_i} Y^{s_i} \bmod p$, obviously, it is still computationally infeasible to derive s_i.

Attack 4: Any intruder might try to randomly select an integer s_i' first, and then compute the corresponding r_i' based on the relation

$$\alpha^{EID_i} = r_i'^{r_i'} Y^{s_i'} \bmod p.$$

This is an extremely difficult problem and, in all likelihood, is more difficult than the discrete logarithm problem itself [10].

Attack 5: Suppose there are t conspirators among the users and they try to derive the KAC's secret key x. For each signature pair (r_i, s_i), they can construct the equation as

$$s_i = (EID_i - k_i r_i)x^{-1} \bmod p - 1.$$

Since k_i and x are unknown parameters, and k_i is different for each signature pair, x cannot be uniquely determined.

IV. Identity- Based Digital Signature Scheme

Suppose user i wants to sign a message M. Without losing generality, we assume the user's secret key s_i obtained from KAC is an odd number (i.e., $gcd(s_i, p-1) = 1$).

Digital Signature Generating Procedure

The digital signature generating procedure can be described as follows.

Step 1: Find the one-way result, $M' = f(M, Time)$, where f is the public known one-way function, *Time* is used as a time-stamp, and M is a message to be signed.

Step 2: User i randomly selects a number σ_i from $[0, p-1]$ and computes

$$\delta_i = Y^{\sigma_i} \bmod p.$$

Step 3: Since $gcd(s_i, p-1) = 1$, user i now solves the congruence

$$M' = \sigma_i \delta_i + \eta_i s_i \bmod p - 1$$

or

$$\eta_i = (M' - \sigma_i \delta_i) s_i^{-1} \bmod p - 1$$

for the integer η_i, where $0 \le \eta_i \le p-1$.

The signature of message M is then the ordered triple (r_i, δ_i, η_i), where r_i is the public key of user i obtained from the KAC during the registration time.

Digital Signature Verification

Upon receiving the set $\{M, r_i, \delta_i, \eta_i\}$, any user can verify the signature of message M as

$$Y^{M'} = \delta_i^{\delta_i} \{\alpha^{EID_i} (r_i^{r_i})^{-1}\}^{\eta_i} \bmod p$$

where Y is KAC's public key, $M' = f(M, Time)$, and $EID_i = f(ID_i)$.

Security: In the above scheme, user i possesses a secret key s_i obtained from the KAC during registration time. The corresponding public key Y^{s_i} can be computed by any other user as

$$Y^{s_i} = \alpha^{EID_i} (r_i^{r_i})^{-1} \bmod p.$$

Given this key as public-known information, it is still computationally infeasible to derive s_i. On the other hand, user i can use his secret key s_i to sign messages repeatedly. The security discussion of our scheme is the same as the Agnew *et al.* signature scheme.

V. Identity- Based Key Distribution Schemes

Gunther and Boveri [13] also show an identity-based key-exchange protocol based on the ElGamal signature scheme. In their protocol, however, the communication key can only be authenticated indirectly. In other words, the protocol does not provide any authentication for the exchanged keys, although unauthorized users cannot share the same session key with a registered user.

In the following, we present two key distribution schemes. The first one only provides indirect key authentication, and the common secret session key shared between two users is always the same. The second one provides direct key authentication, and the common secret key is different from one time to the next.

Key Distribution with Indirect Authentication

Suppose users i and j want to share a common secret session key $K_{i,j}$. User i sends (ID_i, r_i) to user j, while user j sends (ID_j, r_j) to user i. Then user i can compute the key $K_{i,j}$ as

$$\begin{aligned} K_{i,j} &= \{\alpha^{EID_j} (r_j^{r_j})^{-1}\}^{s_i} \bmod p \\ &= (Y^{s_j})^{s_i} \bmod p. \end{aligned}$$

User j can compute the key $K_{j,i}$ as

$$\begin{aligned} K_{j,i} &= \{\alpha^{EID_i} (r_i^{r_i})^{-1}\}^{s_j} \bmod p \\ &= (Y^{s_i})^{s_j} \bmod p. \end{aligned}$$

Since $K_{i,j} = K_{j,i}$, this is the exact common secret session key shared between users i and j. This scheme authenticates the session keys indirectly, because actual authentication is achieved only when the decrypted message sent by the other party is meaningful during communication. However, an intruder cannot impersonate any authorized user to share a common session key with any other authorized user. This is because our method is an identity-based key distribution scheme, and the common secret session key involves two individual secret keys known only to these two users with correct identities.

Key Distribution with Direct Authentication

Here we present an ID-based key exchange protocol which allows two users not only to share a common secret session key, but also to authenticate the exchanged public keys.

Step 1: User i randomly selects a number $\nu_i \in [1, p-1]$, then computes

$$W_i = Y^{\nu_i} \bmod p.$$

By using the signature scheme described in the previous section, user i generates the signature pair (W_i, η_i) for W_i and sends (ID_i, r_i, W_i, η_i) to user j. Note here that W_i is used as both user i's public key and as part of the signature of itself. User j also randomly selects $\nu_j \in [1, p-1]$ and computes

$$W_j = Y^{\nu_j} \bmod p$$

in the same way. Then the signature pair (W_j, η_j) of W_j is computed, and (ID_j, r_j, W_j, η_j), is sent to user i.

Step 2: Upon receiving (ID_j, r_j, W_j, η_j), user i verifies the signature of W_j. If the signature is verified, W_j from user j is authenticated by user i. Consequently, user i computes $K_{i,j}$ as

$$K_{i,j} = W_j^{\nu_i} \bmod p.$$

User j receives (ID_i, r_i, W_i, η_i) and verifies the signature of W_i. If the signature is verified, W_i from user i is authenticated by user j. Consequently, user j computes $K_{j,i}$ as

$$K_{j,i} = W_i^{\nu_j} \bmod p.$$

Since $K_{i,j} = (Y^{\nu_j})^{\nu_i} \bmod p = (Y^{\nu_i})^{\nu_j} \bmod p = K_{j,i}$, $K_{i,j}$ or $K_{j,i}$ is the exact common secret session key shared between users i and j. We also note here that since ν_i and ν_j are randomly selected by users i and j, respectively, the common secret key $K_{i,j}$ will be different from one time to the next.

Because the security of these two schemes is the same as the user identification scheme, we omit the discussion here.

VI. Conclusion

Three identity-based cryptographic schemes have been discussed in this paper. These schemes use the operations in modular p, where p is a large prime. User identification and the digital signature scheme can be used to authenticate the user and message itself without revealing any secret information. The key distribution scheme can be used to establish any secret communication between any two users.

References

[1] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 644–654, Nov. 1976.

[2] L. Kohnfelder, "Towards a practical public-key cryptosystem," B.S. thesis, Mass. Inst. Technol., Cambridge, MA, 1978.

[3] R. Blom, "An optimal class of symmetric key generation systems," in *Proc. Eurocrypt '84*, Paris, France, Apr. 9–11, 1984, pp. 335–338.

[4] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Crypto '84*, Santa Barbara, CA, Aug. 19–22, 1984, pp. 47–53.

[5] E. Okamoto and K. Tanaka, "Key distribution system based on identification information," *IEEE J. Select. Areas Commun.*, vol. 7, pp. 481–485, May 1989.

[6] K. Ohta, "Efficient identification and signature schemes," *Electron. Lett.*, vol. 24, no. 2, pp. 115–116, Jan. 1988.

[7] R. L. Rivest, A. Shamir, and L. Adelman, "A method for obtaining digital signatures and public-key cryptosystem," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[8] S. Tsujii and T. Itoh, "An ID-based cryptosystem based on the discrete logarithm problem," *IEEE J. Select. Areas Commun.*, vol. 7, pp. 467–473, May 1989.

[9] S. Tsujii and J. Chao, "A new ID-based key sharing system," in *Proc. Crypto '91*, 1991, pp. 6.18–6.24.

[10] G. B. Agnew, R. C. Mullin, and S. A. Vanstone, "Improved digital signature scheme based on discrete exponentiation," *Electron. Lett.*, vol. 26, no. 14, pp. 1024–1025, July 1990.

[11] T. ElGamel, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 469–472, July 1985.

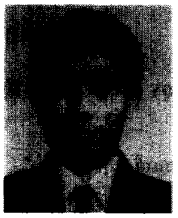
[12] S. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 106–110, 1978.

[13] C. G. Gunther and A. B. Boveri, "An identity-based key-exchange protocol," in *Proc. Eurocrypt '89*, 1989, pp. 29–37.

[14] D. Chaum, J.-H. Evertse, and J. van de Graaf, "An improved protocol for demonstrating possession of discrete logarithms and some generalizations," in *Proc. Eurocrypt '87*, 1987, pp. 121–141.

Lein Harn was born in Taipei, Taiwan, in 1954. He received the B.S. degree from the National Taiwan University in 1977, the M.S. degree from the State University of New York, Stony Brook, in 1980, and the Ph.D. degree from the University of Minnesota, Minneapolis, in 1984, all in electrical engineering.

From 1981 to 1984, he was a Research/Teaching Assistant and was involved in research on signal detection and digital filtering in the Department of Electrical Engineering at the University of Minnesota. Since 1984, he has been an Assistant Professor in the Department of Electrical and Computer Engineering at the University of Missouri-Columbia, and the University of Missouri-Kansas City. From 1986 to 1987, he was a Visiting Associate Professor at the National Cheng Kung University, Taiwan. Currently, he is an Associate Professor at the Computer Science Telecommunications Program, University of Missouri at Kansas City, MO. His research interests include digital filter design, signal processing, data security, cryptography, and VLSI design.



Shoubao Yang was born in Shanghai, China in 1947. He received the B.S. and M.S. degrees in computer science from the University of Science and Technology of China in 1975 and 1990, respectively.

Since 1975, he has been a Research/Teaching Assistant, and then an Assistant Professor at the Department of Computer Science, University of Science and Technology of China. Currently as an Edgar Snow Fellow, he is visiting the Computer Science Telecommunication Programs, University of Missouri-Kansas City. His research interests are computer architecture, fault-tolerance computing, data security, and cryptography.