Adaptable Group-Oriented Signature

Chunbo Ma[*], Jun Ao[**], Dake He[***]

[*](*School of Computer and Communications Engineering, Southwest Jiaotong University, Chengdu, Sichuan, 610031,P. R. China*)

[**](*Laboratory for Radar Signal Processing, Xidian University, Xi'an, Shanxi, 710071, P. R. China*)

[***](*Lab. of Information Security and National Computing Grid, Southwest Jiaotong University, Chengdu, Sichuan 610031,P. R. China*)

Abstract: A new type of signature is presented in this paper, named adaptable group-oriented signature. In contrast with traditional group-oriented signature, the new one laid a strong emphasis on how to improve the signer's efficiency. In fact, this new type of group-oriented signature can be seen as a type of designated verifier signature. In contrast with the ordinary designated verifier signature, it does not designate one member but several members to independently verify the signature. The designated members, who can independently verify the signature, come into a group. This scheme can ensure the anonymity of the verifiers. This type of signature can be used in such system that the compute resource is limited, such as the broadcast protocols of the mobile telephone in the mobile networks.

Key words: adaptable; broadcast; group-oriented signature; ID based; authentication; efficiency; designated verifier

1. Introduction

In distributed networks, the traditional group-oriented signature is that only when all members in an authorized subset of a given group operate collectively, they can generate, conform or deny a signature on behalf of the group. The key skill used in traditional group-oriented is secret sharing. The aim of this type of signature is to improve the signature security. In many applications, the signer should sign a same message for lots of members, and how to improve the signing efficiency comes to be a problem. For example, we hope a mobile telephone has broadcast function, that is, it can send its signature to several members in the mobile networks. In such situations, the compute resource is limited, so signing a same message one by one for all designated members overload the signer.

If a signer wants a designated member to verify his signature, he can use designated verifier signature, such as Chameleon signature [10][11]. If the signer wants several members to independently verify his signature, then he can sign the same message one by one for every member. But with this method, the efficiency is very low.

In practical networks, there exist several group models constructed by the members.

Firstly, in distributed networks, all users come into a group, that is, there is no member outside the group in this model. There is no member outsider the group wants to verify the signature, such as a small scale LAN.

Secondly, in distributed networks, the users in the different companies or institutions naturally come into different groups (this is the second model). In this condition, if the signer wants to provide such type signature service, he should have effect ways to prevent the members outside the designated group from verifying the signature.

Thirdly, in distributed networks, the signer just wants several members to verify his signature no matter whether these members are in one natural group or not (third model). What the signer should do is that he should define a group for these members. Then he should find effect way to prevent the member outside the defined group from verifying the signature. We can see the third model as a generalizing for the first and second models.

The efficiency of a cryptosystem is not only in his arithmetic but also in the way to manage the public keys. To date, the ID based cryptosystem can be seen as the substitute for the traditional PKI. Generally speaking, it is much easier to manage the ID based cryptosystem than the traditional PKI. In traditional PKI, there is no relation between the identity of user A and its public key, and the public key just is a random string. When user B wants to send a message to A, B should get A's authenticated public key. In order to solve this problem, it is necessary to establish a public key list. The virtue of the ID based cryptosystem is that any user can get his public key from his identity information, such as his email address. So, it makes the public key management and authentication much easier.

In the ID based cryptosystem, if the verifier outputs "True", then it means:

1) The sender generates this signature with his private key, which based on his identity.
2) The sender's ID has been authenticated by TTP (Trusted Third Party). With the certificate sent by TTP, the sender can generates his signature.

It is very important to complete two events in the same time for the ID based signature scheme, because it avoids the certificate transmitting and saves communication bandwidth.

Considering the public key management, a novel ID based adaptive group-oriented signature is presented in this paper. In this scheme, before signing a message, the signer defines a group by embedding a group tab in the public key of the designated members. In contrast with the first and the second models, the signer can freely define a group containing the members he wants designated. In first and second models, the group is defined by the system. To any member, he can't get any information about other designated verifier from the published values. Then the anonymity is realized.

2. Related Works

Desmedt fist presents the concept of group-oriented cryptography [1] in 1987. The problem he wants to solve is that when a sender encrypts a message for a group of members, how to make the members to decrypt the ciphertext by cooperation. This concept used in signature, then group-oriented signature comes. Generally speaking, the key skill of traditional group oriented signature is secret sharing. Papers [2][3] are some researches about this type of signature.

Shamir first presents the concept of ID based cryptography [4], and designs the first signature based on ID. It can greatly decrease the complexity of public key authentication and in fact it is similar to email system. In his scheme, the private key mode reverses to that of traditional PKI. That is the private key is generated by the master key and member's public key. In order to preserve the private key secret, this process is kept secret. However, practical identity-based encryption (IBE) schemes were not found until Boneh and Franklin [5] published their work in 2001. The Boneh-Franklin scheme bases its security on the Bilinear Diffie-Hellman Problem, and is quite fast and efficient when using Weil or Tate pairings on supersingular elliptic curves or abelian varieties. From then on, the pairings come to be an important tools to construct cryptosystem, and lots of researches are published, such as [8][9].

Chunbo Ma et al. present the concept of group inside signature [6]. In their scheme, any one in the same group with the signer can verify the signature generated by the signer. This type of signature can be transmitted by broadcast on the Internet. Embedding a group tab in the private key is the key skill to construct this signature. With this method, the efficiency of signing a message is improved enormously. This signature is corresponding to the first model.

Chunbo Ma et al. present another group-oriented signature in paper [7]. This signature is corresponding to the second model. In this scheme, any member in the designated group can independently verify the signature generated by the signer.

The member's group in paper [7] is naturally generated, and it may be a company or an institution on the Internet. It is necessary to embed a group tab in corresponding member's private key, in this aspect, it is similarly to that of paper [6]. The flaw of this method is that the signer can't designate several members in different groups to verify his signature.

3. Background

3.1. Bilinear pairings

Let G_1 be a cyclic additive group generated by P, whose order is a prime q and G_2 be a cyclic multiplicative group of the same order q. Assume that the discrete logarithm in both G_1 and G_2 is intractable. A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$ and satisfies the following properties:

1) *Bilinear:* $e(aP, bP^{'}) = e(P, P^{'})^{ab}$. For all the P, $P^{'} \in G_1$ and $a, b \in Z_q$, the equation holds;

2) *Non-degenerate:* There exists $P^{'} \in G_1$, if $e(P, P^{'}) = 1$, then $P = \mathrm{O}$;

3) *Computable:* For $P, P^{'} \in G_1$, there is an efficient algorithm to compute $e(P, P^{'})$.

Typically, the map e will be derived from either the Weil or Tate pairing on an elliptic curve over a finite field. Pairings and other parameters should be selected in proactive for efficiency and security.

3.2. Gap Diffie-Hellman group

Let G_1, P and q be as above. Assume that the inversion and multiplication in G_1 can be computed efficiently. We first introduce the following problems in G_1.

1) *Discrete Logarithm Problem (DLP)*: Given two elements P and Q, to find an integer $n \in Z_q^*$, such that $Q = nP$ whenever such an integer exists.

2) *Computation Diffie-Hellman Problem (CDHP)*: Given P, aP, bP for $a, b \in Z_q^*$, to compute abP.

3) *Decision Diffie-Hellman Problem (DDHP)*: Given P, aP, bP, cP for $a, b, c \in Z_q^*$, to decide whether $c = ab \bmod q$.

Definition 1: *The advantage of an algorithm* Λ *in solving the CDHP in* G_1 *is the probability*

$$P_r[\Lambda(P, aP, bP) = abP : a, b \overset{R}{\leftarrow} Z_q^*]$$

If no probabilistic algorithm can solve CDHP (Computational Diffie-Hellman) with non-negligible advantage within polynomial time but DDHP (Decision Diffie-Hellman Problem) can be solved in polynomial time, the group G called GDH (Gap Diffie-Hellamn Group). This type of group can be constructed in the field of Hyper Elliptic or Super Singular Elliptic Curve [12].

3.3. GDH group on elliptic curves

An elliptic curve serve as the basis for a GDH signature scheme if we can sue it to construct some group G with large prime order on which CDH is difficult but DDH is easy. First, we characterize a necessary condition for CDH intractability on a subgroup of elliptic curve E.

Definition 2: *Let E be an elliptic curve over* F_{k^n} *with* l *points,* k *be a prime and* n *be a positive exponent. Let* P *in E be a point of prime order* q*, where* q^2 *can't be divided exactly by* l*. We say that the subgroup* $< P >$ *has a security multiplier* α*, for some integer* $\alpha > 0$*, if* $a \mid k^{n\alpha} - 1$ *and* q *cannot be divided exactly by* $k^{nt} - 1$ *for all* $t = 1, 2, \cdots, \alpha - 1$*, that is, the order of* k^n *in* F_q^* *is* α.

In order to compute the discrete log problem on elliptic curve, we usually map the discrete log problem in $< P >$ to a discrete log problem in some extension of F_{k^n}, say $F_{k^{nt}}$. For CDH to be hard in the subgroup $< P >$, we must have that the security multiplier α for this subgroup is not too small. On the other hand, to get an efficient DDH algorithm in $< P >$, we need that α is not too large. As we will see in paper [12], choose supersingular elliptic curves with $\alpha = 6$, we can obtain short signature but the security is dependent on a discrete log problem in $F_{k^{6n}}$. In order to insure the difficulty of discrete log problem in $F_{k^{6n}}$, we request k^n to be sufficiently large. We can also choose other elliptic curves or hyperelliptic curves to obtain higher security.

4. Group-oriented Signature

Assume that there are n users $a_0, a_1, a_2, \cdots, a_n$ in the distributed network. We denote the set of $a_1, a_2, \cdots, a_n$ by A. Let $a_0 \in A$ be the signer who wants to sign a message m and sends it to certain user's group $B = \{a_1, a_2, \cdots, a_i\}$, where $i < 0 \leq n$. The signer a_0 wants that only the designated members can independently verify his signature. The group B is defined by signer a_0.

4.1 Initialize

Let G_1 be a GDH Group generated by P, whose order is a prime q and G_2 be a cyclic multiplicative group of the same order q. A bilinear pairing is a map e : $G_1 \times G_1 \to G_2$. Define two cryptographic hash functions:

$$H_0 : \ \{0,1\}^* \to G_1 \quad H_1 : \ \{0,1\}^* \times G_1 \to Z_q^* .$$

There exist a KGC (Key Generating Center), which function is to generate private keys for corresponding members.

4.2 Key Generation

Let ID_i denote the identity of $a_i \in A$. KGC random selects $s \in Z_q^*$, then a_i's private key is $S_i = sH_0(ID_i)$ and the corresponding public key is $P_i = H_0(ID_i)$. Any member can compute the public key. The private key generated by KGC is sent to corresponding member in secure way. KGC publishes sP.

4.3 Group-oriented Signature Generation

The signer a_0 random selects $r, k, t \in Z_q^*$, and publishes the value $T_i = kH_0(ID_i)$, where $a_i \in B$. Then a_0 compute $h = H_1(m)$ and publishes $V_0 = tsP$, $V_1 = tkP$, $V_2 = rksH_0(ID_0)$ and $T_0 = kH_0(ID_0)$.

The signer a_0 performs the following computing.

$$\sigma = (r + h)sH_0(ID_0) \qquad (1).$$

The signer a_0 generates the signature $(m, \sigma, V_0, V_1, V_2)$ for the message m. This signature will be transmitted to the designated members by broadcast over Internet.

4.4 Signature Verification

The verification can be divided into two steps, the first step is to judge who can verify the signature, and the second step is how to verify it.

4.4.1 Judge Verifier

The aim of this step is to judge who can verify the signature. Using the value $T_i = kH_0(ID_i)$, any one can perform the following step.

$$e(T_i, V_0) \overset{?}{=} e(S_i, V_1) \qquad (2).$$

If the equation holds, then the corresponding member has the ability to verify the signature. The signer a_0 publishes i values, that is, only i members have the ability to go on verification.

4.4.2 Verify Signature

The member $a_i \in B$, who passes above step, can perform the verification as follows.

$$e(\sigma, T_i) \overset{?}{=} e(V_2, P_i)e(hT_0, S_i) \qquad (3).$$

If above equation hold, then the signature is valid.

5. Security Analysis

a) Correctness.

(i) Judge verifier. To the equation (2), we have $e(T_i, V_0) = e(kH_0(ID_i), tsP) = e(sH_0(ID_i), tkP) = e(S_i, V_1)$. Only the designated $a_i \in B$ has the corresponding S_i, so only a_i himself can verify that whether he is fit for the next verification step or not. After confirming his verification ability, a_i uses T_i to perform the following step.

(ii) Verify signature. To the equation (3), we have

$$\begin{aligned} e(\sigma, T_i) &= e((r+h)sH_0(ID_0), kH_0(ID_i)) \\ &= e(rskH_0(ID_i), H_0(ID_i))e(hkH_0(ID_0), sH_0(ID_i)) \\ &= e(V_2, P_i)e(hT_0, S_i). \end{aligned}$$

With (2) and (3), we can see that only the designated member corresponding to T_i can verify the signature.

b) Anonymity. With the equation (2), any $a_j \notin B$ can't distinguish who is the designated verifier, because he has no S_i corresponding to T_i. The difficulty he gets s from S_j, sP, V_0, V_1, and V_2 is equal to solving discrete logarithm on elliptic curves. For the designated verifier $a_l, a_i \in B$ and $a_j \neq a_i$, a_j can't distinguish whether a_i can verify the signature or not.

c) We use the attack model and modified lemmas and theorems described in paper [13] to prove our signature security. We should prove the unforgeability of signature σ. We use the following attack model: a polynomial time algorithm ϖ simulates the adversary and a polynomial time algorithm θ simulates the function of the signer and KGC.

1. θ sets up the scheme. The resulting system parameters are published.
2. ϖ issues the following queries as he wants:
   a) Hash function query. θ computes the value of the hash function for the requested input and sends the value to ϖ.
   b) Private key query: Given public key P_i, θ returns the corresponding private key S_i to ϖ.
   c) Sign query: Given public key P_i and a message m, θ returns a signature, which is obtained by running signature process.
3. A outputs (P_i, m, σ), where (P_i, m) has not been queried before. If σ is a valid signature of m corresponding to certain group member's public key P_i, ϖ will succeed.

Lemma 1[13]: *if there is an algorithm ϖ_0 for an adaptively chosen message and member identity attack to our signature σ with running time t_0 and advantage ε_0, then there is an algorithm ϖ_1 for an adaptively chosen message and certain member attack to our signature σ which has running time $t_1 \le t_0$ and advantage $\varepsilon_1 \le \varepsilon_0 / q - 1$, where q is the order of Z_q.*

Proof: Without any loss of generality, we assume that for any member's public key P_i, ϖ_0 queries the private key and the signature at most once.

Since the output of ϖ_0 is (P_{out}, m, σ), then $\Pr[(P_{out}, m, \sigma)$ is valid $] \ge \varepsilon_0$. Assume that ϖ_1 attacks certain member P_{a_i}, then $\Pr[P_{out} = P_{a_i} \mid (P_{out}, m, \sigma) is \quad valid] \ge 1/q - 1$. So $\Pr[P_{out} = P_{a_i} \cap (P_{out}, m, \sigma) is \quad valid] \ge \varepsilon_0 / q - 1$, that is $\varepsilon_1 \le \varepsilon_0 / q - 1$. It is obvious that $t_1 \le t_0$

Lemma 2: *If there is an algorithm ϖ_1 for an adaptively chosen message and certain member P_{a_i} attack to our signature σ, which queries hash function, signing and private key at most q_H, q_S and q_k times, respectively, and has running time t_1 with advantage $\varepsilon_1 \ge 10(q_S + 1)(q_S + q_H)/(q - 1)$, then the attacker can solve DLP within time $t_2 \le 120686 q_H t_1 / \varepsilon_1$, where q is the order of Z_q^*.*

Proof: We use the theorem 3 in paper [14] to proof this lemma:

Let ϖ be a probabilistic polynomial time Turing machine whose input only consists of public data. We denote respectively by Q and R the number of queries that ϖ can ask to the random oracle and the number of queries that ϖ can ask to the signer. Assume that, within a tie bound T, ϖ produces, with probability $\varepsilon \geq 10(R+1)(Q+R)/2^k$, a valid signature (m,σ_1,h,σ_2). If the triple (σ_1,h,σ_2) can be simulated without knowing the secret key, with an indistinguishable distribution probability, then there is another machine $\varpi^{'}$ which has control over the machine obtained from ϖ replacing interaction with the signer by simulation and produces two valid signatures (m,σ_1,h,σ_2) and $(m,\sigma_1,h^{'},\sigma_2^{'})$ such that $h \neq h^{'}$ in expected time $T^{'} \leq 120686QT/\varepsilon$, where k is the security parameter.

Now we prove the lemma 2: From theorem 3 in paper [14], if an algorithm ϖ_1 could forge a signature $(P_{a_i},\sigma_1,h,\sigma_2)$ with advantage $\varepsilon_1 \geq 10(q_S+1)(q_S+q_H)/(q-1)$, then there is an algorithm ϖ_2, by choosing different h, to obtain another valid signature $(P_{a_i},\sigma_1,h^{'},\sigma_2^{'})$ within time $t_2 \leq 120686q_H t_1/\varepsilon_1$, where $h \neq h^{'}$. Let $q \geq 2^k+1$, and k is the security parameter, these two valid signatures are $(P_{a_i},\sigma_1,h^{'},\sigma_2^{'})$ and $(P_{a_i},\sigma_1,h,\sigma_2)$. Then we have $\sigma_2 = \sigma_1 + hsH_0(ID_i)$ and $\sigma_2^{'} = \sigma_1 + h^{'}sH_0(ID_i)$. Subtracting the equations, $\sigma_2 - \sigma_2^{'} = (h-h^{'})sH_0(ID_i)$. So $sH_0(ID_i) = (\sigma_2 - \sigma_2^{'})/(h-h^{'})$. The running time of ϖ_2 is $t_2 \leq 120686q_H t_1/\varepsilon_1$.

Theorem 2: *If there is an algorithm ϖ_0 for an adaptively chosen message and member identity attack to our signature σ which queries hash function, signing and private key at most q_H, q_S and q_k times, respectively, and has running time t_1 with advantage $\varepsilon_0 \geq 10(q_S+1)(q_S+q_H)$, then the attacker can solve DLP within time $t_2 \leq 120686q_H t_0(q-1)/\varepsilon_0$, where q is the order of Z_q.*

In this paper, we assume that the KGC distributes the private key to corresponding member in secure way, so we consider the private key is safe. That is, the attacker can get the private key with the probability of no more than $1/2^k$. The only way to get certain member's private key is to solve s with the public values. The assumption that the DLP is intractable is contrary to above result, so the signature σ can't be forged.

6. Conclusion

This paper generalizes the result of [6] and [7], and designs a new type of signature:

adaptable group-oriented signature. In the new scheme, the signer can define the group freely to make all members in the defined group can independently verify his signature. What the most different from the paper [6][7] is that the designated group does not naturally come into being, but defines by the signer. In the instance that the signer should sign the same message for several members, this scheme can effectively improve the signing efficiency. In practice, this scheme can be used in the distributed networks, whose member has limited compute ability. At the end of the paper, we give the brief discuss about the security of the signature scheme.

References

1. Desmedt Y. Society and Group Oriented Cryptography: A New Concept. Proceedings of CRYPTO 87, Lecture Notes in Computer Science, papers 120-127, 1988.
2. Pedersen T P. A Threhold Cryptosystem Without a Trusted Party. Proceedings of EUROCRYPT'91, Lecture Notes in Computer Science, paper 522-526,1992.
3. Shoup V. Practical threshold signatures. Advance in Cryptology-Eurocrypt'00, LNCS 1807, pp.207-220
4. Shamir A. Identity-based cryptosystems and signature schemes. In Proc. of Cryptology-CRYPTO'84, 1984: 47~53.
5. Boneh D, Lynn B, and Shacham H. Short signatures from the Weil pairing. *Advances in Cryptology -- Asiacrypt'2001*, Lecture Notes in Computer Science 2248, Springer-Verlag (2002), pp. 514—532
6. Ma C. B, Ao F. L, He D. K. Certificateless Group Inside Signature. Proceedings of ISADS'05 (The 7th International Symposium on Autonomous Decentralized Systems, Chengdu. P. R. China), pagers: 194~200
7. Chunbo Ma, Jun Ao, Dake He. "Broadcast group oriented signature". Proceedings of ICICS2005 (5th International Conference on Information, Communications and Signal Processing, 6-9 December 2005 in Bangkok, Thailand), to appear.
8. Kenneth G. Paterson. ID-based Signature from pairings on elliptic curves. Http://eprint.iacr.org/2002/004.
9. Dan Boneh and Xavier Boyen. Secure identity based encryption without random oracles. In Advances in Cryptology-Crypto 2004, LNCS, Springer-Verlag, 2004, 3152: 443~456.
10. Krawczyk H and Rabin T. Chameleon signatures. In Proceedings of NDSS2000, San Diego, California, USA, 2000, 143-154.
11. Chunbo Ma, Dake He. "A New Chameleon Multisignature Based on Bilinear Pairing". Proceedings of GCC'04(3rd International Conference on Grid and Cooperative Computing, Wuhan. P. R. China), Lecture Notes in Computer Science. Springer Verlag, 2004, 3252: 329-335
12. Boneh D, Lynn B, and Shacham H. Short signatures from the Weil pairing. Advances in Cryptology -- Asiacrypt'2001, Gold Coast, Australia, Lecture Notes in Computer Science, 2248, Springer-Verlag, 2001, 514—532.
13. Jae Choon Cha and Jung Hee Cheon, An identity-based signature from gap Diffie-Hellman group. Proc. of PKC 2003, Miami, FL, USA, Lecture Notes in Computer Science, 2567, 2002, 18-30.
14. Pointcheval D and Stern J. Security arguments for digital signature and blind signatures. J. of Cryptology, 2000, 13(3):361-396.