STUDIA UNIV. "BABEŞ-BOLYAI", INFORMATICA, Volume XLIV, Number 1, 1999

GROUP SIGNATURES BASED ON THE e-TH ROOT AND THE DISCRETE LOGARITHM PROBLEM

CONSTANTIN POPESCU

ABSTRACT. The concept of group signatures was introduced by Chaum and Heyst at Eurocrypt'91. It allows a member of a group to sign messages anonymously on behalf of the group. Furthermore, in case of disputes later a trusted authority can identify the signer. In this paper, we present a group signature based on the e-th root problem and the discrete logarithm problem. The group signature is verified by identities of group members. The signature can be opened, in case of dispute later, with the help of the deciphering function of a group authority's public key cryptosystem. *Keywords*: Group signature, identity, enciphering function, deciphering function.

1. INTRODUCTION

A group signature scheme allows members of a group to sign messages on behalf of the group such that everybody can verify the signature but no one can find out which group member provided it. However, there is a trusted third party, called the group manager, who can in case of a later dispute reveal the identity of the originator of a signature. The group manager can either be a single entity or a member of coalitions of several entities.

In [3] four different schemes were proposed. Three of them require the group manager to contact each group member in order to find out who signed a message. These scheme provide computational anonymity, whereas the fourth scheme provides information theoretical anonymity. For two of the schemes it is not possible to add a new member after the scheme is set up. In none of the proposed schemes it is possible to distribute the functionality of the group manager efficiently.

Group signatures could for instance be used by a company for authenticating price lists, press releases, or digital contracts. The customers need to know only a single company public key to verify signatures. The company can hide any internal organizational structures and responsibilities, but still can find out which employee has signed a particular document. Group signatures have been proposed by Chaum and Heyst [3]. Their schemes have been improved by L. Chen and T. Pedersen [4], who first use a Schoenmaker's protocol [9] to hide a signer's identity. Also, H. Petersen suggested a general method to convert any ordinary digital signature into a group signature scheme [8]. Petersen's method combines the Stadler's verifiable

encryption of discrete logarithm [10] and the Schoenmaker's protocol. Recently, J. Camenisch and M. Stadler presented the first group signature scheme whose public key and signatures have length independent of the number of group members of one group [1], [2], but this isn't independent of the number of groups. Also, S. Kim, S. Park and D. Won published the group signatures for hierarchical multigroups [5], convertible group signatures [6] and the ID-based group signature [7].

In this paper we present a group signature based on the e-th root problem and the discrete logarithm problem. The group signature is verified by identities of group members. The signature can be opened, in case of dispute later, with the help of the deciphering function of a group authority's public key cryptosystem. Our scheme consists of four kinds of participants: a trusted center for generating secret key of all users, a group authority for identifying a signer, a signer for issuing group signatures and a receiver for verifying them.

2. The Group Signature Scheme

In this section we propose a group signature scheme based on the ideas presented at the end of Section 1. The proposed group signature scheme is specified by the key generation, signing messages, verifying signatures and opening signatures.

2.1. **Key Generation.** Trusted center generates secret keys of users. First, one chooses a modulus $n = p \cdot q$, where p and q are two large primes. Trusted center selects a large integer e (160 bits) with $\gcd(e, \Phi(n)) = 1$ and $g \in \mathbb{Z}_n$ with the order q. One publishes n, g and e. Let $ID_i \in \mathbb{Z}_n$ be an identity information of a user, where $\mathbb{Z}_n$ is the integer ring. One computes a secret key x_i with

$$ID_i = x_i^e \pmod{n}$$

The group authority generates his key pair (x, y) with $y = g^x \pmod{n}$, publishes the public key y and keeps x secret. The group authority (GA) chooses a public-key cryptosystem, $(E_{GA}(\cdot), D_{GA}(\cdot))$, where $E_{GA}(\cdot)$ is the enciphering function and $D_{GA}(\cdot)$ is the deciphering function. The enciphering function $E_{GA}(\cdot)$ is public. The signer and the receiver use the group authority's public key y to encrypt the messages.

2.2. **Signing Messages.** Let $G = \{ID_1, ..., ID_k\}$ be a set of identities of group members and $H(\cdot)$ be a secure hash function. A member ID_1 generates a group signature as follows. The symbol $\|$ denotes the concatenation of two binary strings (or of the binary representation of group elements and integers).

(1) Choose α randomly in $\mathbb{Z}_n$ and compute $c = x_1^{H(m\|\alpha)} \pmod{n}$
(2) Compute $A = g^\beta \pmod{n}$ and $B = c \cdot y^\beta \pmod{n}$, where $\beta \in \mathbb{Z}_n$ randomly
(3) Compute $u = E_{GA}(m \| \alpha)$ and $v = E_{GA}(c \| ID_1)$
(4) For $i = 1, ..., k$ one computes $C_i = ID_i^{H(m\|\alpha)} \pmod{n}$

(5) Choose r randomly in $\mathbb{Z}_n$ and compute

$$m_i = r^e H\left(u \parallel v \parallel C_i\right) \pmod{n},$$

for $i = 1, ..., k$

(6) Compute

$$b = \left(\prod_{i=1}^{k} m_i\right)^{\frac{1}{e}} \pmod{n}$$

and $s = \frac{b}{r} \pmod{n}$

(7) The signer sends a group signature (s, α, v, A, B).

2.3. **Verification Signatures.** We suppose that a receiver knows the identities ID_i's of a group G. The group signature is verified as follows. First, a receiver computes

$$C_i = ID_i^{H(m\|\alpha)} \pmod{n}$$

and then checks whether:

$$s^e \stackrel{?}{=} \prod_{i=1}^{k} H\left(E_{GA}\left(m \parallel \alpha\right) \parallel v \parallel C_i\right) \pmod{n} \tag{1}$$

If this equation holds, one accepts the signature (s, α, v, A, B), otherwise rejects it.

2.4. **Opening Signatures.** Given the group signature (s, α, v, A, B), the group authority can easily computes the identity ID_1 by decrypting v with the help of the deciphering function $D_{GA}(\cdot)$. First, the group authority obtain $c = B/A^x \pmod{n}$. Then he can identify the signer ID_1 by decrypting v, because only the group authority knows the secret key x for deciphering.

3. Security Considerations

A receiver and a group authority, who have no secret keys x_i's of the group G, can not generate a group signature. In order to generate a group signature, the e-th root of $ID_i = x_i^e \pmod{n}$ should be computed. But, since a receiver and a group authority do not know the factor p and q, they can not compute the e-th root of ID_i. It is hard to get another α, v satisfying the equation (1) because $H(\cdot)$ is a secure hash function. Second, trusted center and a receiver can not determine a signer of the group signature, because only the group authority knows the secret key x for deciphering. Since, the secret key x is unknown, the ordinary signature c can not be driven from (A, B). Moreover, if p and q are sufficiently large, trusted center and a receiver can not get x from the public key y.

The security of the proposed scheme depends on the e-th root problem and the discrete logarithm problem.

4. Conclusion

In this paper we proposed a group signature based on the e-th root problem and the discrete logarithm problem. The group signature is verified by identities of group members which a receiver already knows. The signature can be opened, in case of dispute later, with the help of the deciphering function of a group authority's public key cryptosystem.

References

[1] J. Camenisch, M. Stadler, Efficient group signature schemes for large groups, Advances in Cryptology, CRYPTO'97.

[2] J. Camenisch, M. Michels, A group signature scheme based on RSA-variant, BRICS, Denmark, 1998.

[3] D. Chaum, E. Heyst, Group Signatures, Advances in Cryptology, EUROCRYPT'91, Lecture Notes in Computer Sciences 950, Springer-Verlag, 1992, pp. 257-265.

[4] L. Chen, T. Pedersen, New group signature schemes, Advances in Cryptology, EUROCRYPT'94, Lecture Notes in Computer Sciences 547, Springer-Verlag, 1995, pp. 163-173.

[5] S. Kim, S. Park, D. Won, Group signatures for hierarchical multigroups, Information Security Workshop, Lecture Notes in Computer Sciences 1396, Springer-Verlag, 1998, pp. 273-281.

[6] S. Kim, S. Park, D. Won, Convertible group signatures, Advances in Cryptology, ASIACRYPT'96, Lecture Notes in Computer Sciences 1163, Springer-Verlag, 1996, pp. 311-321.

[7] S. Park, S. Kim, D. Won, ID-based group signature schemes, Electronics Letters, 1997, pp. 1616-1617.

[8] H. Petersen, How to convert any digital signature scheme into a group signature scheme, In Security Protocols Workshop, Paris, 1997.

[9] B. Schoenmaker, Efficient Proofs of Or, Manuscript, 1993.

[10] M. Stadler, Publicly verifiable secret sharing, Advances in Cryptology, EUROCRYPT'96, Lecture Notes in Computer Sciences 1070, Springer-Verlag, 1996, pp. 190-199.

University of Oradea, Department of Mathematics, Str. Armatei Romane 5, Oradea, Romania

E-mail address: cpopescu@math.uoradea.ro