STUDIA UNIV. BABEŞ–BOLYAI, INFORMATICA, Volume **XLV**, Number 2, 2000

A MODIFICATION OF THE TSENG-JAN GROUP SIGNATURE SCHEME

CONSTANTIN POPESCU

ABSTRACT. In this paper we present a modification of the Tseng-Jan group signature scheme [18]. Our scheme appears to be secure in comparation with the Tseng-Jan group signature scheme. The proposed scheme is based on the e-th root problem and the discrete logarithm problem. *Keywords*: Group signature, identity, membership certificate.

1. INTRODUCTION

Group signatures allow individual members of a group to sign messages on behalf of the group while remaining anonymous. Furthermore, in case of disputes later a trusted authority, who is given some auxiliary information, can identify the signer. The concept of group signatures was introduced by Chaum and van Heyst [4]. Their schemes have been improved by L. Chen and T. Pedersen [5], who first use a Schoenmaker's protocol [17] to hide a signer's identity. Also, H. Petersen suggested a general method to convert any ordinary digital signature into a group signature scheme [15]. Petersen's method combines the Stadler's verifiable encryption of discrete logarithm [18] and the Schoenmaker's protocol. 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 [2], but this isn't independent of the number of groups. Many group signature schemes have been presented [3], [7], [8], [12], [13], [14], [16]. In [19], Tseng and Jan proposed a group signature scheme, but this was broken in [9] and [10]. In [9], M. Joye, S. Kim and N. Lee showed that the Tseng-Jan scheme is universally forgeable, that is, anyone is able to produce a valid group signature on an arbitrary message. In [10], M. Joye showed that the group signature scheme proposed by Tseng-Jan is not coalition-resistant: two group members can produce untraceable group signatures.

In this paper we present a modification of the Tseng-Jan group signature scheme [19]. Our scheme appears to be secure in comparation with the Tseng-Jan group

2000 *Mathematics Subject Classification.* 94A60.

1998 *CR Categories and Descriptors.* D.4.6. [**Software**]: Operating Systems – *Security and Protection*;

signature scheme. The proposed scheme is based on the e-th root problem and the discrete logarithm problem. The remainder of the paper is organized as follows. In Section 2, we review the scheme proposed by Tseng and Jan. In Section 3 our scheme is described. In Section 4 some security considerations are given and finally, Section 5 concludes with the results of the paper.

2. Tseng-Jan Group Signature Scheme

In this section, we give a short description of the Tseng-Jan group signature scheme and refer to the original paper [19] for more details. The scheme involve four parties: a trusted authority, the group authority, the group members, and verifiers. The trusted authority acts as a third helper to setup the system parameters. The group authority selects the group public/secret keys. He (jointly with the trusted authority) issues membership certificates to new users who wish to join the group. In case of disputes, opens the contentious group signatures to reveal the identity of the actual signer. Finally, group members anonymously sign on group's behalf using their membership certificates and verifiers check the validity of the group signatures using the group public key.

In order to set up the system, a trusted authority selects two large prime numbers $p_1\,(\equiv 3 \bmod 8)$ and $p_2\,(\equiv 7 \bmod 8)$ such that $(p_1-1)/2$ and $(p_2-1)/2$ are smooth, odd and co-prime [11]. Let $N = p_1 p_2$. The trusted authority also defines e, d, v, t satisfying $ed \equiv 1 \,(\mathrm{mod}\ \varphi(N))$ and $vt \equiv 1 \,(\mathrm{mod}\ \varphi(N))$, selects g of large order in $\mathbb{Z}_N^*$, and computes $F = g^v \,(\mathrm{mod}\ N)$. Moreover, the group authority chooses a secret key x and computes the corresponding public key $y = F^x \,(\mathrm{mod} N)$. The public parameters are (N, e, g, F, y). The secret parameters are (p_1, p_2, d, v, t, x).

When a user U_i (with identity information D_i) wants to join the group, the trusted authority computes

$$s_i = et \log_g ID_i \,(\mathrm{mod}\ \varphi(N))$$

where $ID_i = D_i$ or $ID_i = 2D_i$ according to $(D_i \mid N) = 1$ or $(D_i \mid N) = -1$, and the group authority computes

$$x_i = ID_i^x \,(\mathrm{mod}\ N)\,.$$

The user membership certificate is the pair (s_i, x_i). To sign a message M, the user U_i (with certificate (s_i, x_i)) chooses two random numbers r_1 and r_2 and computes

$$\begin{aligned}
A &= y^{r_1} \,(\mathrm{mod}\ N) \\
B &= y^{r_2 e} \,(\mathrm{mod}\ N) \\
C &= s_i + r_1 h(M \parallel A \parallel B) + r_2 e \\
D &= x_i y^{r_2 h(M\parallel A\parallel B)} \,(\mathrm{mod}\ N)
\end{aligned}$$

where $h(\cdot)$ is a publicly known hash function. The group signature on message M is given by the tuple (A, B, C, D). The validity of this signature can then be verified by checking whether

$$D^{e}A^{h(M\|A\|B)}B \equiv y^{C}B^{h(M\|A\|B)} \pmod{N}.$$

Finally, in case of disputes, the group authority can open the signature to recover who issued it by checking which identity ID_i satisfies

$$ID_i^{xe} \equiv D^{e}B^{-h(M\|A\|B)} \pmod{N}.$$

3. Our Group Signature Scheme

This section describes the proposed group signature scheme, which is specified by the key generation, signing messages, verification signatures and opening signatures.

3.1. **Key Generation.** Our scheme consists of four kinds of participants: a *trusted center* who setup the system parameters, a *group authority* who issues membership certificates to new users who wish to join the group and identifies a signer, a *signer* for issuing group signatures and a *receiver* for verifying them using the group public key.

A trusted center selects two large primes p_1, p_2 as in [19]. Let $n = p_1p_2$. The trusted center also selects a large integer e (160 bits) with $\gcd(e, \varphi(n)) = 1$ and selects g of large order in $\mathbb{Z}_n^*$, where $\mathbb{Z}_n$ is the integer ring. The group authority chooses a secret key x and computes the corresponding public key $y = g^x \pmod{n}$. The public parameters are (n, e, g, y) and the secret parameters are (p_1, p_2, x). Let $ID_i \in \mathbb{Z}_n$ be an identity information of a user U_i. Finally, let h be a collision-resistant hash function. Suppose now that a user wants to join the group. We assume that communication between the user and the trusted center (between the user and the group authority) is secure, i.e., private and authentic.

When a user U_i wants to join the group, the trusted center computes

$$s_i = ID_i^{\frac{1}{e}} \pmod{n}$$

and the group authority computes

$$x_i = (ID_i + eg)^{x} \pmod{n}.$$

The user membership certificate is the pair (s_i, x_i).

3.2. **Signing Messages.** To sign a message M, the user U_i, with certificate (s_i, x_i), chooses two random numbers r_1 and r_2 and computes

$$A = y^{r_2 e} \pmod{n}$$

$$B = x_i y^{s_i + r_1} \pmod{n}$$

$$C = x_i y^{r_2} \pmod{n}$$

$$D = s_i h(M \parallel A) + r_1 h(M \parallel A).$$

The symbol $\|$ denotes the concatenation of two binary strings (or of the binary representation of group elements and integers). The group signature on message M is given by the tuple (A, B, C, D).

3.3. **Verification Signatures.** The validity of this signature can then be verified by checking whether

$$C^{eh(M\|A)} y^{eD} \equiv B^{eh(M\|A)} A^{h(M\|A)} \pmod{n}.$$

If this equation holds, he accepts the signature (A, B, C, D), otherwise it is rejected.

3.4. **Opening Signatures.** Finally, in case of disputes, the group authority can open the signature to recover who issued it by checking which identity ID_i satisfies

$$(ID_i + eg)^{xe} \equiv C^e A^{-1} \pmod{n}.$$

4. Security Considerations

A receiver, a group authority and a trusted center, who have no membership certificate (s_i, x_i) of a user U_i, can not generate a group signature. Trusted center knows s_i, but he can not determine x_i, because only the group authority knows the secret key x. The group authority knows x_i, but he can not determine s_i, because only the trusted center knows the e-th root of ID_i.

Given a group signature (A, B, C, D), identifying the actual signer is computationally hard for every one but the group authority.Since no one knows which pair (s_i, x_i) corresponds to which group member, anonymity is guaranteed.

Deciding whether two different signatures are computed by the same group member is computationally hard. The problem of linking two signatures (A, B, C, D) and (A', B', C', D') reduces to looking if either s_i or x_i is common to the two tuples. This is however impossible under Decisional Diffie-Hellman Assumption (see [1], [6]).

Trusted center and a receiver can not determine a signer of the group signature, because only the group authority knows the secret key x. If p_1 and p_2 are sufficiently large, even trusted center can not get x from the public key y. Therefore, an adversary can not forge our group signature scheme on an arbitrary message M.

5. Conclusions

This paper has presented a modification of the Tseng-Jan group signature scheme proposed in [19]. Our scheme appears to be secure in comparation with the Tseng-Jan group signature scheme. The security of the proposed scheme depends on the e-th root problem and the discrete logarithm problem.

References

[1] D. Boneh, *The decision Diffie-Hellman problem*, In Algorithmic Number Theory (ANTS-III), Lecture Notes in Computer Sciences 1423, Springer-Verlag, pp. 48-63, 1998.

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

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

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

[5] 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.

[6] W. Diffie, M. Hellman, *New Directions in Cryptography*, IEEE Transaction Information Theory, IT-22, 6, pp. 644-654, 1976.

[7] 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.

[8] 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.

[9] M. Joye, S. Kim, N. Lee, *Cryptanalysis of Two Group Signature Schemes*, 1999 (5 pages).

[10] M. Joye, *On the Difficulty of Coalition-Resistance in Group Signature Schemes*, Technical Report, LCIS-99-6B, 1999.

[11] U. Maurer, Y. Yacobi, *Non-interactive public-key cryptography*, In Advances in Cryptology-EUROCRYPT'91, LNCS 547, Springer-Verlag, 1991, pp. 498-507.

[12] S. Park, I. Lee, D. Won, *A practical group signature*, Proc. of JWISC'95, Japan, 1995, pp. 127-133.

[13] S. Park, D. Won, *A practical identity-based group signature*, Proc. of ICEIC'95, China, 1995, pp. II-64-II-67.

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

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

[16] C. Popescu, *Group signature schemes based on the difficulty of computation of approximate e-th roots*, Proceedings of Protocols for Multimedia Systems (PROMS 2000), Poland, pp. 325-331, 2000.

[17] B. Schoenmakers, *Efficient Proofs of Or*, Manuscript, 1993.

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

[19] Y. Tseng, J. Jan, *A novel ID-based group signature*, In T.L. Hwang and A.K. Lenstra, editors, 1998 International Computer Symposium, Workshop on Cryptology and Information Security, Tainan, 1998, pp. 159-164.

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

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