Ring signature with divided private key

Stelian Flonta
(Technical University of Cluj-Napoca, Cluj-Napoca, Romania
sflonta@colim.ro)

Liviu-Cristian Miclea
(Technical University of Cluj-Napoca, Cluj-Napoca, Romania
Liviu.Miclea@aut.utcluj.ro)

Abstract: The ring signature is a group signature without a group manager, so that a signer realizes a signature in the name of the group. In some situations it is necessary for a message to be signed by more than one persons. The scheme of the ring signature with divided key is an algorithm which ensures realizing a key signature by a group of k entities from a group of n entities. Because of the way this scheme is elaborated, each signer has his own private key, which he uses in the signing phase. Checking the key is realized by using a single common public key. The signature scheme is based on the problem of the discrete logarithm. This cryptographic primitive ensures the anonymity of the signature, which is a ring signature.

Keywords: Ring signature, divided private key
Categories: D4.6, E.3

1 Introduction

The cryptographic primitives in this paper are based on a ring signature scheme, which relies on the problem of the discrete logarithm. The first part of the paper presents ideas from the specialty literature which treat the subject of ring signature. Creating the scheme of the ring signature with divided key to two is then detailed. The central paragraph refers to a ring signature with divided private key to k entities. An important aspect is the fact that this scheme ensures anonymity of the signer entities. In the end, the ideas of implementation and the authors' contributions are stated.

2 Related work

After the introduction of the notion of electronic group signature scheme, various versions of this model have been elaborated. Some schemes [Chor 85, Gennaro 96] obtained robustness by the means of divinding the private keys. There exist versions based on the discrete logarithm over a commutative group structure or on the RAS system [Camenisch 97 pp. 465-479, Camenisch 97 pp. 410-424 , Chen 94, H Wang 09, Xiaoming 09] . Camenisch [Xu 00] elaborates an efficient group signature scheme having the property that members can be added or removed from the group after the initialization of the algorithm and generalizes this idea, so that a signature is realized by a subset with at least k members from the possible n who form the group. This is the idea which leads to the group signature with threshold scheme, meaning that for a valid signature to be done in the name of a group, it is necessary for it to be realized by k members, where $k \leq n$. In the present paper, realizing a common signature by k members is done by dividing the private key to k. This is the reason why the name is ring signature with divided private key. If the elaborated scheme ensures absolute anonymity (there is no group manager) of the signers, then it is of the ring type [H Wang 09, Xiaoming 09].

3 Ring signature with divided private key to two signers

A simple generalization of the electronic ring signature scheme [G Wang 09] is described in this paragraph. In this case, the private key is divided and distributed to two signers. For the signature to be valid, it is necessary for the two signers to put their private keys in common by the means of a certain algorithm. It must be pointed out that the signing algorithm does not make the private keys public, they are known only by the authorized users.

The Algorithm for Key Generation

The algorithm for generating the keys is done by a trusted center, which must assure the confidentiality for the private keys and a corresponding management. Two high prime numbers are chosen $\{p,q\}$, where $p = zq + 1$ and $z \in \mathbb{Z}^*$. Also, a generator $g \in \mathbb{Z}^*{}_p$ of order q of $\mathbb{Z}^*{}_p$ is chosen. The choice is done so that the problem of the discrete logarithm to be difficult to solve. For each user $Bob_i, i = 1,...,n$, $x_i \in \mathbb{Z}^*{}_q$ $, i = 1,...,n$ are chosen in a random way. $h_i = g^{x_i} \pmod{p}, i = 1,...,n$ is then computed. The keys assigned to each user $Bob_i, i = 1,...,n$ are $\{x_i, h_i\}, i = 1,...,n$, where x_i are private and h_i are public. Of course, $\{p,q,g\}$ are also public.

The Algorithm for signing the message

For the signing of message m, $h = h_1 \cdot h_2 \cdot h_3 \cdot ...h_n \bmod p$ is computed. u, v, y from $\mathbb{Z}_q{}^*$ are chosen and $r_1 = g^u \left(\frac{h}{h_a \cdot h_b} \right)^v \bmod p$,

$r_2 = g^y \bmod p$, $s_1 = -r_1 \cdot r_2 \cdot v^{-1} \bmod q$ are computed by Bob_a, Bob_b together.

Each signer Bob_a, Bob_b computes:

$s_{2a} = y^{-1}(\frac{1}{2} u s_1 + x_a r_1 r_2 - \frac{1}{2} H(m, r_1, r_2)) \bmod q$ respectively

$s_{2b} = y^{-1}(\frac{1}{2} u s_1 + x_b r_1 r_2 - \frac{1}{2} H(m, r_1, r_2)) \bmod q$ after which they compute together:

$$s_2 = (s_{2a} + s_{2b}) \bmod q = y^{-1}(u s_1 + (x_a + x_b) r_1 r_2 - H(m, r_1, r_2)) \bmod q$$

.

The signature of the message m is $(h_1, h_2, h_3, ..., h_n, r_1, r_2, s_1, s_2)$.

The algorithm for checking the signature

The ring signature is valid if the following relation is true:

$$g^{H(m,r_1,r_2)} \equiv h^{r_1 r_2} \cdot r_1^{s_1} \cdot r_2^{-s_2} \bmod p .$$

Proof:

The next computations demonstrate that the presented scheme is correct:

$$h^{r_1 r_2} \cdot r_1^{s_1} \cdot r_2^{-s_2} (\bmod p) \equiv$$

$$\equiv h^{r_1 r_2} \cdot (g^u (h / h_a h_b)^v)^{-r_1 r_2 v^{-1}} \cdot$$

$$\cdot (g^y)^{-y^{-1}(us_1 + (x_a + x_b) r_1 r_2 - H(m, r_1, r_2))(\bmod q)} (\bmod p) \equiv$$

$$\equiv h^{r_1 r_2} \cdot g^{-u r_1 r_2 v^{-1}} \cdot h^{-r_1 r_2} \cdot (h_a h_b)^{r_1 r_2} \cdot$$

$$\cdot (g)^{-(us_1 + (x_a + x_b) r_1 r_2 - H(m, r_1, r_2))(\bmod q)} (\bmod p) \equiv$$

$$\equiv g^{-u r_1 r_2 v^{-1} (\bmod p)} \cdot (h_a h_b)^{r_1 r_2 (\bmod p)} \cdot$$

$$\cdot (g)^{-(us_1 + (x_a + x_b) r_1 r_2 - H(m, r_1, r_2))(\bmod q)} (\bmod p) \equiv$$

$$\equiv g^{us_1} \cdot g^{(x_a + x_b) r_1 r_2} \cdot$$

$$\cdot (g)^{-(us_1 + (x_a + x_b) r_1 r_2 - H(m, r_1, r_2))(\bmod q)} (\bmod p) \equiv$$

$$\equiv g^{us_1 (\bmod q)} \cdot g^{(x_a + x_b) r_1 r_2 (\bmod q)} \cdot$$

$$\cdot (g)^{-(us_1 + (x_a + x_b) r_1 r_2 - H(m, r_1, r_2))(\bmod q)} (\bmod p) \equiv$$

$$\equiv g^{H(m, r_1, r_2)} (\bmod p)$$

Along the calculus, $g^{us_1} \cdot g^{(x_a + x_b) r_1 r_2}$ was substituted by $g^{us_1 (\bmod q)} \cdot g^{(x_a + x_b) r_1 r_2 (\bmod q)}$. This is possible because the order of g is equal to q.

4 Ring signature with divided key to k signers

Another generalization of the electronic ring signature [G Wang 09] scheme is described in this paragraph. In this case, the private key is divided and distributed to k signers. For the signature to be valid, it is necessary for the k signers to put their private keys in common by the means of a certain algorithm. It must be pointed out that the signing algorithm does not make the private keys public, they are known only by the authorized users. It is obvious that the number k is smaller than n.

Version 1

The Algorithm for Key Generation

A trusted center proceeds with the generation and management of the keys in a similar way as described in the previous paragraph.

Two high prime numbers are chosen $\{p, q\}$, where $p = zq + 1$ and $z \in \mathbb{Z}^*$. Also, a generator $g \in \mathbb{Z}^*_p$ of order q of $\mathbb{Z}^*_p$ is chosen. The choice is done so that the problem of the discrete logarithm to be difficult to solve. For each user $Bob_i, i = 1,\ldots,n$, $x_i \in \mathbb{Z}^*_q, i = 1,\ldots,n$ are chosen in a random way. $h_i = g^{x_i} \pmod{p}, i = 1,\ldots,n$ is then computed. The keys assigned to each user $Bob_i, i = 1,\ldots,n$ are $\{x_i, h_i\}, i = 1,\ldots,n$, where x_i are private and h_i are public. Of course, $\{p, q, g\}$ are also public.

The Algorithm for signing the message

For the signing of message m, $h = h_1 \cdot h_2 \cdot h_3 \cdot \ldots h_n \bmod p$ is computed. u, v, y from $\mathbb{Z}_q^*$ are chosen and, $r_1 = g^u \left(\dfrac{h}{h_{a_1} \cdot h_{a_2} \cdot \ldots \cdot h_{a_k}} \right)^v \bmod p$, $r_2 = g^y \bmod p$, and $s_1 = -r_1 \cdot r_2 \cdot v^{-1} \bmod q$ are computed by $Bob_{a_1}, Bob_{a_2}, \ldots, Bob_{a_k}$ together.

Each signer $Bob_{a_1}, Bob_{a_2}, ..., Bob_{a_k}$ computes:

$$s_{2a_1} = y^{-1}(\frac{1}{k}us_1 + x_{a_1}r_1r_2 - \frac{1}{k}H(m, r_1, r_2)) \bmod q$$ respectively

$$s_{2a_2} = y^{-1}(\frac{1}{k}us_1 + x_{a_2}r_1r_2 - \frac{1}{k}H(m, r_1, r_2)) \bmod q$$

……………………………………………………………..

$$s_{2a_k} = y^{-1}(\frac{1}{k}us_1 + x_{a_k}r_1r_2 - \frac{1}{k}H(m, r_1, r_2)) \bmod q$$ after which they compute

$$s_2 = (s_{2a_1} + s_{2a_2} + ... + s_{2a_k}) \bmod q =$$

$$= y^{-1}(us_1 + (x_{a_1} + x_{a_2} + ... + x_{a_k})r_1r_2 - H(m, r_1, r_2)) \bmod q$$

The signature of the message m is $(h_1, h_2, h_3, ..., h_n, r_1, r_2, s_1, s_2)$

The algorithm for checking the signature

The ring signature is valid if the following relation is true:

$$g^{H(m, r_1, r_2)} \equiv h^{r_1 r_2} \cdot r_1^{s_1} \cdot r_2^{-s_2} \bmod p$$

Proof:

The next computations demonstrate that the presented scheme is correct:

$$h^{r_1 r_2} \cdot r_1^{s_1} \cdot r_2^{-s_2} (\bmod p) \equiv$$

$$\equiv h^{r_1 r_2} \cdot (g^{u} (h / h_{a_1} \cdot h_{a_2} \cdot \ldots \cdot h_{a_k})^{v})^{-r_1 r_2 v^{-1}} \cdot$$

$$\cdot (g^{y})^{-y^{-1}(us_1 + (x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2 - H(m, r_1, r_2))(\bmod q)} (\bmod p) \equiv$$

$$\equiv h^{r_1 r_2} \cdot g^{-u r_1 r_2 v^{-1}} \cdot h^{-r_1 r_2} \cdot (h_{a_1} \cdot h_{a_2} \cdot \ldots \cdot h_{a_k})^{r_1 r_2} \cdot$$

$$\cdot (g)^{-(us_1 + (x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2 - H(m, r_1, r_2))(\bmod q)} (\bmod p) \equiv$$

$$\equiv g^{-u r_1 r_2 v^{-1} (\bmod p)} \cdot (h_{a_1} \cdot h_{a_2} \cdot \ldots \cdot h_{a_k})^{r_1 r_2 (\bmod p)} \cdot$$

$$\cdot (g)^{-(us_1 + (x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2 - H(m, r_1, r_2))(\bmod q)} (\bmod p) \equiv$$

$$\equiv g^{us_1} \cdot g^{(x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2} \cdot$$

$$\cdot (g)^{-(us_1 + (x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2 - H(m, r_1, r_2))(\bmod q)} (\bmod p) \equiv$$

$$\equiv g^{us_1 (\bmod q)} \cdot g^{(x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2 (\bmod q)} \cdot$$

$$\cdot (g)^{-(us_1 + (x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2 - H(m, r_1, r_2))(\bmod q)} (\bmod p) \equiv$$

$$\equiv g^{H(m, r_1, r_2)} (\bmod p)$$

Along the calculus, $g^{us_1} \cdot g^{(x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2}$ was substituted by $g^{us_1 (\bmod q)} \cdot g^{(x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2 (\bmod q)}$. This is possible because the order of g is equal to q.

Version 2

The Algorithm for Key Generation

A trusted center proceeds with the generation and management of the keys in a similar way as described in the previous paragraph.

Two high prime numbers are chosen $\{p,q\}$, where $p = zq+1$ and $z \in \mathbb{Z}^*$. Also, a generator $g \in \mathbb{Z}^*{}_p$ of order q of $\mathbb{Z}^*{}_p$ is chosen. The choice is done so that the problem of the discrete logarithm to be difficult to solve. For each user $Bob_i, i=1,\ldots,n$, $x_i \in \mathbb{Z}^*{}_q$ $, i=1,\ldots,n$ are chosen in a random way. $h_i = g^{x_i} \pmod{p}, i=1,\ldots,n$ is then computed. The keys assigned to each user $Bob_i, i=1,\ldots,n$ are $\{x_i, h_i\}, i=1,\ldots,n$, where x_i are private and h_i are public. Of course, $\{p,q,g\}$ are also public.

The Algorithm for signing the message

For the signing of message m, $h = h_1 \cdot h_2 \cdot h_3 \cdot \ldots h_n \bmod p$ is computed. u,v,y from $\mathbb{Z}_q^*$ are chosen and,

$r_1 = g^u \left(\dfrac{h}{h_{a_1} \cdot h_{a_2} \cdot \ldots \cdot h_{a_k}} \right)^v \bmod p$, $r_2 = g^y \bmod p$, and

$s_1 = -r_1 \cdot r_2 \cdot v^{-1} \bmod q$ are computed by $Bob_{a_1}, Bob_{a_2}, \ldots, Bob_{a_k}$ together.

Each signer $Bob_{a_1}, Bob_{a_2}, \ldots, Bob_{a_k}$ computes:

$s_{2a_1} = y^{-1}(\frac{1}{k}us_1 + x_{a_1}r_1r_2 - H(m, r_1, r_2)) \bmod q$ respectively

$s_{2a_2} = y^{-1}(\frac{1}{k}us_1 + x_{a_2}r_1r_2 - H(m, r_1, r_2)) \bmod q$

………………………………………………………………..

$s_{2a_k} = y^{-1}(\frac{1}{k}us_1 + x_{a_k} r_1 r_2 - H(m, r_1, r_2)) \bmod q$ after which they compute

$$s_2 = (s_{2a_1} + s_{2a_2} + \ldots + s_{2a_k}) \bmod q =$$

$$= y^{-1}(us_1 + (x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2 - k \cdot H(m, r_1, r_2)) \bmod q$$

The signature of the message m is $(h_1, h_2, h_3, \ldots, h_n, r_1, r_2, s_1, s_2)$.

The algorithm for checking the signature

The ring signature is valid if the following relation is true:

$$g^{k \cdot H(m, r_1, r_2)} \equiv h^{r_1 r_2} \cdot r_1^{s_1} \cdot r_2^{-s_2} \bmod p$$

Proof:

The next computations demonstrate that the presented scheme is correct:

$$h^{r_1 r_2} \cdot r_1^{s_1} \cdot r_2^{-s_2} (\operatorname{mod} p) \equiv$$

$$\equiv h^{r_1 r_2} \cdot (g^{u} (h / h_{a_1} \cdot h_{a_2} \cdot \ldots \cdot h_{a_k})^{v})^{-r_1 r_2 v^{-1}} \cdot$$

$$\cdot (g^{y})^{-y^{-1}(us_1 + (x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2 - k \cdot H(m, r_1, r_2))(\operatorname{mod} q)} (\operatorname{mod} p) \equiv$$

$$\equiv h^{r_1 r_2} \cdot g^{-u r_1 r_2 v^{-1}} \cdot h^{-r_1 r_2} \cdot (h_{a_1} \cdot h_{a_2} \cdot \ldots \cdot h_{a_k})^{r_1 r_2} \cdot$$

$$\cdot (g)^{-(us_1 + (x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2 - k \cdot H(m, r_1, r_2))(\operatorname{mod} q)} (\operatorname{mod} p) \equiv$$

$$\equiv g^{-u r_1 r_2 v^{-1} (\operatorname{mod} p)} \cdot (h_{a_1} \cdot h_{a_2} \cdot \ldots \cdot h_{a_k})^{r_1 r_2 (\operatorname{mod} p)} \cdot$$

$$\cdot (g)^{-(us_1 + (x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2 - k \cdot H(m, r_1, r_2))(\operatorname{mod} q)} (\operatorname{mod} p) \equiv$$

$$\equiv g^{us_1} \cdot g^{(x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2} \cdot$$

$$\cdot (g)^{-(us_1 + (x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2 - k \cdot H(m, r_1, r_2))(\operatorname{mod} q)} (\operatorname{mod} p) \equiv$$

$$\equiv g^{us_1 (\operatorname{mod} q)} \cdot g^{(x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2 (\operatorname{mod} q)} \cdot$$

$$\cdot (g)^{-(us_1 + (x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2 - k \cdot H(m, r_1, r_2))(\operatorname{mod} q)} (\operatorname{mod} p) \equiv$$

$$\equiv g^{k \cdot H(m, r_1, r_2)} (\operatorname{mod} p)$$

Along the calculus, $g^{us_1} \cdot g^{(x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2}$ was substituted by $g^{us_1 (\operatorname{mod} q)} \cdot g^{(x_{a_1} + x_{a_2} + \ldots + x_{a_k}) r_1 r_2 (\operatorname{mod} q)}$. This is possible because the order of g is equal to q.

The two versions differ in the signing stage and check stage of the message. According to *Version 1*, the number k of the signers is established by computations. This means that ensuring that k entities have signed is done by computations regarding to s_2.

Version 2 contains the information related to the number of signers in computations regarding s_2 and in the formula for checking the message, which also ensures that the signature has been realized by k entities. It is remarkable that the number of the k signers can be equal to the number n of the members of the group. Moreover, the private keys x_i do not have to be distinct.

5 Anonymity of the ring signature with divided key to k signers

The property of anonymity refers to the fact that the signers remain anonymous after they have signed a message and their identity cannot be established starting from the signature or other public information.

In the version where the signer is a single entity Bob_t, a possibility of determining his identity is offered by the public key h_t. Establishing the key h_t, using public information, leads to the discovery of the signer Bob_t.

The analysis of the computations reveals that h_t can be determined from the equation $r_1 = g^u \left(\frac{h}{h_t} \right)^v \bmod p$. Solving this equation has the complexity of the discrete logarithm. Consequently, the complexity is $O(\sqrt{n})$ [1,2].

If the schemes with divided keys are analyzed, the anonymity must be studied from the perspective of the group members who are not signers and relatively to the members of the group who are signers. From the point of view of members who haven't signed or of entities outside the group, the discovery of the signers' identity is similar to solving the problem of the discrete logarithm, fact which leads to a problem of $O(\sqrt{n})$ complexity[1,2]. If a signer Bob_t wishes to determine the identity of other signers, he possesses additional information besides the equation $r_1 = g^u \left(\frac{h}{h_{a_1} \cdot h_{a_2} \cdot \ldots \cdot h_{a_k}} \right)^v \bmod p$, the values of the parameters u, v, y and obviously x_t, and implicitly h_t. Simple computations lead to the finding of the keys $h_{a_1}, h_{a_2}, \ldots, h_{a_k}$, fact which allows the discovery of the signers' identity if the function for associating public keys to signers is public. Consequently, in this case, the signers can know each other, but they remain anonymous to entities exterior to their group.

6 Contribution

The authors have elaborated a scheme for ring signatures, which is a generalization of the scheme in [G Wang 09]. This scheme has two versions. Both of them allow realizing a ring signature by a subset of a defined set of signers. Moreover, ideas of implementation are identified.

References

[Camenisch 97] J. Camenisch: Efficient and generalized group signatures. In: Eurocrypt'97, LNCS 1233, pp. 465-479. Springer-Verlag, 1997.

[Camenisch 97] J. Camenisch, and M. Stadler. Efficient group signature schemes for large groups. In: Crypto'97, LNCS 1294, pp. 410-424. Springer-Verlag, 1997.

[Chen 94] L.Chen, and T.P.Pedersen.New group signature schemes. In:Eurocrypt'94, 1994.

[Chor 85] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In 26th Annual Symposium on oundations of Computer Science, 1985.

[Gennaro 96] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust and efficient sharing of rsa functions. In Advances in Cryptology,1996

[G Wang 09] Guilin Wang, "Network Security", Birmingham, January 2009
www.cs.bham.ac.uk/~gzw/teaching/netsec08/RS.pdf

[H Wang 09] Huaqun Wang, Futai Zhang, and Yanfei Sun, "Cryptanalysis of a Generalized Ring
Signature Scheme", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 6, NO. 2 pp 149-151, APRIL-JUNE 2009

[Xiaoming 09] Wang Xiaoming , „On/Off Threshold Group Signature Scheme", 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, Proceedings pp. 69-73, April 2009

[Xu 00] Q.L.Xu . A Modified Threshold RSA Digital Signature Scheme. Chinese Journal of Computer, 2000, 23(5):449-453.