Quasigroups and Related Systems **22** (2014), 133 – 140

Group signature protocol based on masking public keys

Nikolay A. Moldovyan and Alexander A. Moldovyan

Abstract. There is proposed and discussed the group signature protocol characterized in using the collective signature scheme and masking the public keys of the signers. The masking is performed depending on parameters computed depending on both the public keys and the hash function from document to be signed.

1. Introduction

Digital signature protocols are widely used in the information technologies to solve a variety of different problems. For practical application there are proposed the following types of the signature protocols: usual (individual) signature [6, 11]; blind signature [3, 4]; aggregate signature [10]; group signature [1]; collective signature [8] et. al. The last three protocols relates to the concept of multisignatures introduced in papers [2, 9]. The multisignature concept was generalized to the threshold group signatures in paper [5] when each t of k signers are able to sign a document. The group signature and the collective signature protocols are different in the following. The group signature to an electronic message is the signature on behalf of some set of of k signers (members of the group) headed by a person called dealer. The group signature is generated by a subset of t ($t \leqslant k$) signers. Any one can verify validity of the group signature. The group signature verification procedure does not provide possibility to open the signature, i.e. to identify the members of the group that created the signature. In the case of disputes the signature can be opened by the dealer (with or without the help of signers). The dealer is a trusted party of the group signature protocol. He creates the secret parameters used by the signers.

The collective signature to a document is the signature on behalf of each of m declared signers. The collective signature means that each of the declared signers has signed the document. The collective signature can be considered as some digest of m individual signatures. No trusted party participates in the collective signature protocol. The secret used by each of the signers is private. It is sup-

2010 Mathematics Subject Classification: 11T71, 94A60, 94A62
Keywords: Cryptographic protocol, public key, digital signature, group signature, collective signature, discrete logarithm problem, one-way function
This work was financially supported by Government of Russian Federation, Grant 074-U01

posed the participants of the collective signature protocol use their private keys corresponding to their public keys used to verify their individual signatures, i.e. the collective signature protocols and individual signature protocols can use the same public key infrastructure. The last represents an important advantage of the collective signatures.

This paper proposes a new design of the group signature protocols based on difficulty of the discrete logarithm problem. Novelty of the design consists in using both the collective signature scheme and the transformation masking the public keys of the signers. The described approach provides possibility to create the group signature protocols that are free from participation of a trusted party and use the standard public key infrastructure, i.e. each of the signers can use the same private key when computing his individual signature and participating in computation of the group signature. Thus, the proposed group signature protocol requires no distribution of the secret keys and uses the standard public key infrastructure. Therefore the set of signers included in the group can be arbitrarily changed by the dealer whose public key is used as public key of the group.

Each group signature contains an additional parameter that can be used only by the dealer to open the signature without help of the signers. Practical application scenario for the proposed protocol is as follows. An official information Bureau with geographically distributed staff is headed by a director (dealer) and issues electronic documents. The documents are signed on behalf of the Bureau. Usually different documents are prepared by different subsets of the employees. Produced documents are signed with collective signature of the respective subsets of the employees and presented to the director. He approves the documents with transforming the collective signatures into the group signatures.

2. The proposed signature protocol

In the proposed protocol there are used the following parameters: 1) sufficiently large prime p (for example, having the size 2500 bits), such that number $p-1$ contains large prime divisor q (for example, having the size 256 bits); 2) number α order of which modulo p is equal to q. Each signer of the group generates his private key as a random number x (for example, having the size 256 bits) and computes his public key $y = \alpha^x \bmod p$. The public key of the dealer $Y = \alpha^X \bmod p$, where X is his private key, represents the public key of the group which is used by verifier while performing the group signature verification procedure.

The group signature generation procedure includes both the mechanism of masking (modifying) the public keys of the signers, which is performed with help of the dealer, and the mechanism of forming the collective signature described in paper [8]. The modified public keys are used in the second mechanism that is performed as follows. It is computed the collective randomization parameter E that is one of elements of the group signature. Depending on the value E each signer computes his share in the collective signature S_c, taking into account his

modified public key. The collective signature S_c represents the preliminary value of the group signature element S. The value S_c is used by dealer to produce the final value S.

In the mechanism of masking the public keys there is used the internal public key of the dealer, which represents the pair of numbers (n, e), and is generated, like in the RSA cryptosystem [11], as follows. The dealer generates two strong [7] primes r and w, computes $n = wr$ and $\phi(n) = (w-1)(r-1)$, selects number e that is mutually prime with $\phi(n)$, and calculates his private value $d = e^{-1} \bmod \phi(n)$. The internal public key (n, e) is actual only for the signers of the group headed by the dealer. It is not used in the group signature verification procedure. The generalized scheme of the proposed group signature protocol includes the following steps:

i. Taking into account the document M to be signed the dealer masks the public keys of the assigned signers. To mask the public key y_i of the ith signer the dealer computes the exponent $\lambda_i = (H + y_i)^d \bmod n$, where H is the hash-function value computed from M, and sends the value λ_i to the ith signer.

ii. The assigned subset of signers and leader computes the collective randomization parameter E.

iii. Using the value λ_i each ith signer computes his share in the collective signature and sends it to the dealer.

iv. The dealer verifies the share of all assigned signers and computes his share in the group signature. Then he computes the group signature as triple (U, E, S), where S is sum (modulo q) of all shares; U is the product (modulo p) of the modified public keys of all signers.

The value U contains the information about all signers participating in the given group signature to the document M. In the case of disputes the identification of the signers can be performed by the dealer. Except the dealer opening of the given group signature can be performed only by all signers participating in the signature. If one of them is not agree the group signature be opened the others are not able to open the signature.

One of possible particular implementations of the group signature protocol is described as follows. Suppose there are m signers assigned by dealer to process the document M and to generate the group signature to M. The signature generation procedure includes the following steps:

1. Using some specified 256-bit hash-function F_H the dealer computes the hash value from the document $H = F_H(M)$ and the masking exponents $\lambda_i = (H + y_i)^d \bmod n$ for all public keys $y_i = \alpha^{x_i} \bmod p$, where x_i is private key of the ith signer, and sends the value λ_i to the ith signer $(i = 1, 2, \ldots, m)$. Then dealer computes the first element of the group signature

$$U = \prod_{i=1}^{m} y_i^{\lambda_i} \bmod p.$$

The value U represents the masked collective public key of the assigned subset of

signers.

2. Each ith signer ($i = 1, 2, \ldots, m$) computes the hash value $H = F_H(M)$, verifies that equation $\lambda_i^e = y_i + H \bmod n$ holds (it means the value λ_i has been provided by the dealer), generates a random number $k_i < q$, computes the value $R_i = \alpha^{k_i} \bmod p$, and sends R_i to the dealer.

3. Dealer generates the random number $K < n$ and computes values $R' = \alpha^K \bmod p$,

$$R = R' \prod_{i=1}^{m} R_i \bmod p = \alpha^{K+\sum_{i=1}^{m} k_i \bmod q} \bmod p,$$

and $E = F_H(H||R||U)$, where E is the second element of the group signature; $||$ denotes the concatenation operation. Then he sends the value E to each signer.

4. Each ith signer ($i = 1, 2, \ldots, m$) computes his share $S_i = k_i + \lambda_i x_i E \bmod q$ in the third element of the group signature and sends it to the dealer.

5. Dealer computes the collective signature S_c of the assigned set of signers: $S_c = \sum_{i=1}^{m} S_i \bmod q$ and verifies it with formula $R/R' = U^{-E}\alpha^{S_c} \bmod p$. If S_c is valid, he computes his share $S' = K + XE \bmod q$ and the third element of the group signature $S = S' + S_c \bmod q$.

The verification of the group signature (U, E, S) to document M is performed with the public key of the group Y that coincides with the public key of the dealer. The verification procedure includes the following steps:

1. The verifier computes the hash value from the document M: $H = F_H(M)$.

2. Using the group public key Y and signature (U, E, S) he computes the value $R^* = (UY)^{-E}\alpha^S \bmod p$.

3. Then he computes the value $E^* = F_H(H||R^*||U)$ and compares the values E^* and E. If $E^* = E$, then the verifier concludes the group signature is valid.

Correctness proof of the protocol is performed with substitution of the signature (U, E, S) in the signature verification procedure:

$$R^* \equiv (UY)^{-E}\alpha^S \equiv U^{-E}Y^{-E}\alpha^{S'+\sum_{i=1}^{m} S_i} \equiv$$

$$\equiv \left(\prod_{i=1}^{m} \alpha^{\lambda_i x_i}\right)^{-E} \alpha^{-XE}\alpha^{S'+\sum_{i=1}^{m} S_i} \equiv$$

$$\equiv \alpha^{-E\sum_{i=1}^{m} \lambda_i x_i}\alpha^{-XE}\alpha^{K+XE+\sum_{i=1}^{m}(k_i+\lambda_i x_i E)} \equiv$$

$$\equiv \alpha^K \alpha^{\sum_{i=1}^{m} k_i} \equiv \alpha^K \prod_{i=1}^{m} \alpha^{k_i} \equiv R' \prod_{i=1}^{m} R_i \equiv R \bmod p \Rightarrow$$

$$\Rightarrow \quad R^* = R \;\Rightarrow\; F_H(M||R^*||U) = F_H(M||R||U) \Rightarrow\; E^* = E.$$

3. Discussion

The proposed group signature protocol needs no dealer's distributing any secrete values among signers of the group. This is one of the advantages of the new protocol compared with known group signature protocols [5]. Another advantage is using the standard public key infrastructure, i.e. the public keys of the signers and dealer can be used in both the individual signature protocol and the proposed group signature protocol. Since in the protocol there is used no secret sharing, no special communication channels are needed to implement the protocol. Therefore using Internet is sufficient and the staff of the group can include geographically distributed employees. Besides, the staff of the group can be often and easily changed (when it is needed).

Including the value U as one of the elements of the group signature provides possibility of the dealer's opening the signature in the case of disputes. The last can be performed as follows. Using his private value d the dealer computes the values $\lambda_i = (H + y_i)^d \bmod n$ and $U_i = y_i^{\lambda_i} \bmod p$, multiplies the masked public keys U_i of all possible subsets of signers, and finds the subset for which the product of the values U_i is equal to U, i.e. to the masked collective public key. No other person can open the group signature since computing the masked public keys requires using the secret value d. Except the dealer, only joint action of all signers participating in the group signature can open it, this trivial case is not critical for majority of practical applications. One can note that opening the signature by all m signers participating in the group signature is possible due the fact that they can present all masking exponents λ_i used while computing the value U and show the formulas $\lambda_i^e = H + y_i \bmod n$ $(i = 1, 2, \ldots, m)$ holds. If it will be required this attack can be eliminated defining computation of the value U (see step 1 of the described protocol) in accordance with the following formula:

$$U = Y^{\lambda} \prod_{i=1}^{m} y_i^{\lambda_i} \bmod p,$$

where $\lambda = (H + Y)^d \bmod n$. This modification leads to changing the formula for computing the share of dealer in the signature element S (see step 5 of the protocol) as follows:

$$S' = K + (1 + \lambda)XE \bmod q.$$

While proving correctness of the results of the procedure of opening the group signature the dealer presents the values λ_i (and λ in the modified version of the protocol), however this does not compromise his private value d connected with his internal public key acting in frame of the group.

To provide 128-bit security, i.e. security equal to 2^{128} modulo p multiplication operations, the size of the primes p and q should be equal to about 2500 and 256 bits, respectively. This defines the signature size equal approximately to 3012 bits, while using 256-bit hash-function F_H. For practical applications it is desired

to have shorter group signatures. We estimate the proposed cryptoscheme implemented with using elliptic curves defined over the finite field $GF(p)$, where p is a 256-bit prime, will provide 128-bit security with the signature size equal to 770 bits and 641 bits (the last figure relates to the case of implementing the protocol on the base of the cryptoschemes providing 128-bit security with 128-bit value E).

In frame of the group it is used local (internal) public key of the dealer, which is denoted as (n, e) and used by signers at step 2 of the protocol. The private key d connected with the public key (n, e) is used by dealer to compute the masking coefficients λ_i (at step 1 of the protocol and while performing procedure of the opening signature). For further investigation it is interesting to simplify the mechanism of masking the public keys of signers in order to eliminate using the internal public key of the dealer. For example, the masking coefficients can be computed as follows $\lambda_i = F_H(H||y_i||\delta)$, where δ is internal secret key of the dealer. This formula provides possibility for dealer to restore the masking coefficients with using the secret value δ and open the signature in the case of disputes.

However this variant of computing the masking coefficients is connected with proposing a new mechanism providing for users possibility to verify the values λ_i at step 2 of the protocol. The dealer can directly sign each value λ_i with his signature using his private key X and, for example, the Schnorr signature algorithm [12]. Using the dealer's public key Y the ith user will be able to verify validity of the dealer's signature to λ_i. Significant disadvantage of this verification mechanism is essential increasing the computational difficulty of the group signature generation procedure. Indeed, the dealer has to generate m additional individual signatures (this requires performing m exponentiation operations modulo p) and each of the m signers participating in the group signature is to perform the Schnorr signature verification procedure (for each signer this requires performing 2 exponentiations modulo p). In total this variant of verifying values λ_i introduces $3m$ additional exponentiations in the group signature generation procedure.

It is more practically to exclude verification of the values λ_i from the step 2 of the proposed protocol and to inset the verifying masking exponents procedure in step 5 that is performed by the dealer. After such modification these two steps acquire the following form:

2. Each ith signer $(i = 1, 2, \ldots, m)$ generates a random number $k_i < q$, computes the value $R_i = \alpha^{k_i} \bmod p$, and sends R_i to the dealer.

5. Dealer verifies correctness of each value S_i $(i = 1, 2, \ldots, m)$ with formula $R_i = y_i^{-\lambda_i E}\alpha^{S_i} \bmod p$. If each value S_i is correct, he computes his share $S' = K + XE \bmod q$ and the third element of the group signature $S = S' + \sum_{i=1}^{m} S_i \bmod q$.

To provide possibility for the dealer to open the group signature in the case of disputes without disclosing his private key in the modified protocol one can use the following formula for computing the masking exponents λ_i:

$$\lambda_i = F_H\left(H||y_i||F_H\left(M||y_i||\delta\right)\right).$$

Indeed, while opening a group signature, the dealer justifies each value λ_i

assigned to the opened group signature presenting the value $\Delta = F_H(M||y_i||\delta)$, from which it is computationally infeasible to compute the secret value δ.

4. Conclusion

The paper proposes a new group signature protocol characterized in dealer's participating in the procedure of the signature generation. The described group signature protocol has the following merits:

- it uses the standard public key infrastructure;
- it is free from sharing any secret values;
- the set of signers can be easily changed.

In the considered implementation of the protocol the group signature size is comparatively large, 3012 bits in the case of 128-bit security. This parameter can be reduced to about 640 bits with using computations on elliptic curves to implement the protocol like the described one, however it is a topic of individual consideration.

References

[1] **A. Boldyreva**, *Efficient threshold signature, multisignature and blind signature schemes based on the gap-Diffie-Hellman group signature scheme*, Lecture Nnotes Comp. Sci. **2567** (2003), 31-46.

[2] **C. Boyd**, *Digital multisignatures*, Proceedings IMA Conference on Cryptography and Coding. Clarendon, Oxford, 1989, 241-246.

[3] **J. L. Camenisch, J. M. Piveteau, M. A. Stadler**, *Blind signatures based on the discrete logarithm problem*, Lecture Notes Comp. Sci. **950** (1995), 428 – 432.

[4] **D. Chaum**, *Blind signatures for untraceable payments*, Advances in Cryptology: Proc. of CRYPTO'82. Plenum Press, 1983, 199 – 203.

[5] **Y. Desmedt and Y. Frankel**, *Threshold cryptosystems*, Lecture Notes Comp. Sci. **435** (1990), 307 – 315.

[6] **T. ElGamal**, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Trans. Information Theory **IT–31** (1985), 469 – 472.

[7] **J. Gordon**, *Strong primes are easy to find*, Lecture Notes Comp. Sci. **209** (1985), 216 – 223.

[8] **A. A. Moldovyan and N. A. Moldovyan**, *Blind collective signature protocol based on discrete logarithm problem*, Intern. J. Network Security **11** (2010), 106–113.

[9] **T. Okamoto**, *A digital multisignature scheme using bijective public key cryptosystems*, ACM Transactions on Computer Systems **6** (1988), 432 – 441.

[10] **R. Ostrovsky, S. Lu, A. Sahai, H. Shacham, and B. Waters**, *Sequential aggregate signatures and multisignatures without random oracles*, Lecture Notes Comp. Sci. **4004** (2006), 465 – 485.

[11] **R. L. Rivest, A. Shamir and L. Adleman**, *A method for obtaining digital signatures and public-key cryptosystems*, Commun. ACM **21** (1978), 120 – 126.

[12] **C.P. Schnorr**, *Efficient signature generation by smart cards*, Journal of Cryptology **4** (1991), 161 – 174.

Received Febuary 10, 2014

ITMO University,
Kronverksky pr., 10, St. Petersburg 197101, Russia
E-mail: nmold@mail.ru