IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

An Efficient Proxy-Multi Signature Scheme Based On Discrete Logarithm Problem

Swati Verma[1] and Gulab Das[2]

[1]*Department of Mathematics, School of Science, O. P. Jindal University, Raigarh (C.G.), India.*
[2]*Department of Mathematics, Govt. N. P.G. Science College, Raipur (C.G.), India.*

Abstract:

The multi signature is a form of group-orientated cryptography that became first added with the aid of using Desmedt in 1987. The group has a protection coverage that calls for a multi signature to be signed with the aid of using all institution individuals with the understanding of more than one non-public key. However, to any verifier, the multi signature may be established the use of a corresponding institution public key. In general, we expect that everyone organization participants do now not take delivery of as real with each other. On the opposite hand, in the event that they do accept as true with every other, all non-public keys may be shared amongst themselves. In this paper, we proposed new proxy-multi signature scheme primarily based on DLP. We display that our new scheme can withstand existential forgeries in opposition to adaptive chosen-message attacks. Furthermore, the brand new scheme is quite simple and efficient computationally. It has the belongings that the dimension of a multi-signature is unbiased of the variety of the authentic signers. In addition, this proxy- multi signature can be used for suitable type of blockchain structure.

Keywords— Cryptography; Proxy-Signature; Multi-Signature; Discrete logarithm problem; Security.

1. Introduction

The observation of proxy signature first introduced by Mambo et al. in 1996 [11, 12]. However, the idea to proxy signature became already recorded in 1989 [3]. A proxy signature scheme is a critical research within side the subject of virtual signature which includes 3 entities: an authentic signer, a proxy signer and a verifier. It offers equipment to the authentic signer to delegate his signing proper to a selected signer, referred to as proxy signer. After the proxy signer signs the message on behalf of the real signer, the verifier knowing the common public key of the real signer and the proxy signer verifies the validity of the proxy signature after receiving the message. Proposed some other form of proxy signature scheme known as Proxy-multi signature schemes [6, 7, 18]. In the proxy-multi signature scheme, a proxy signer can generate the signature on behalf of a group of real signers [4, 5]. Proxy-multi signatures can play critical function within side the following scenario: An organization releases a record which could contain the monetary department, engineering department, and application office, etc [14, 15, 16]. The record should through signal mutually through those entities, or signed through a proxy signer legal through those entities. One strategy to the later case of this trouble is to apply a proxy multi-signature scheme.

According to whether or not legitimate multi-signatures are generated simplest through the proxy signer, proxy multi-signatures may be categorized into two types. One is a proxy- unprotected multi-signature, wherein except the proxy signer, simplest the cooperation of all individuals within side the authentic organization can create legitimate proxy signatures. The different is a proxy-protected multi-signature; wherein simplest the proxy signer can create legitimate proxy signatures [2]. Then a few proxy multi-signature schemes have been proposed [1, 17].

In this paper, we advise a new proxy-multi signature scheme primarily based totally on issue of fixing discrete logarithm problem. The algorithm of proxy signature is as follows:

Organization: The remaining parts of this paper an organized as follows. In Section 2, we completed security properties of the proxy signature scheme. Next, we proposed our proxy-multi signature scheme in Section 3. In Section 4 and 5, we analyze the security and efficiency of the proposed scheme. We give our concluding remarks in last section.

2. Security Requirements of Proxy Signature Scheme

The protection necessities for any proxy signature are first studied in [11, 12], According to them, a steady proxy signature scheme is expected to meet the following five necessities [7, 8]:

1. ***Verifiability:*** The verifier is satisfied that the authentic signer has given consent to the proxy signer to signal a message.
2. ***Strong unforgeability:*** Nobody else other than the designated proxy signer can create a valid proxy signature on behalf of the original signer.
3. ***Strong identifiability:*** Everyone can define the identity of the proxy signer of the proxy signature.
4. ***Strong undeniability:*** Once a proxy signer creates a valid proxy signature on behalf of an original signer, he cannot repudiate the signature creation against anyone else.
5. ***Prevention of misuse:*** The proxy signer cannot use the proxy key for the purposes other than generating a valid proxy signature. In case of misuse, the obligation of the proxy signer have to be decided explicitly.

2.1 Preliminaries

Discrete Logarithm (DL) assumption:

Let tt_q= (g) be a cyclic multiplicative group generated by g of order q. Then, on inputs (g, g^x) ∈tt^2 where x ∈Z_q is a random number, there is no probabilistic polynomial-time algorithm that outputs the value of x with^{q}non-negligible probability [19]. The DL assumption is widely believed to be true for many cyclic groups, such as the multiplicative subgroup tt_q= (g) of the finite field Z_p, where p is a large prime and q is a prime factor of $p-1$ [19].

3. Proposed Proxy-Multi Signature Scheme

In this section, we propose a new proxy-multi signature scheme, which is based on DLP [13] having different public key and with highly secure channel. There are also three parties in our scheme: the original signer O, the proxy signer P and the verifier V. We assume that each user has a pair of private key and public key and their certificates. The system public parameters consist of a large prime number p, alargeprimefactor$q$of$p$−1, elements $g \in Z_p^*$with prime order q such that the discrete logarithm of g is unknown.

The proposed scheme is divided into four phases: ***Key generation, Proxy key generation, Signing phase*** **and** ***Signature verification phase [6].***

3.1 Key Generation

We define the parameters for generating the message as follows:

- ***U_j* :** the original signer
- ***P* :** the proxy signer
- ***U_i* :** users
- ***p, q* :** prime number with $q/(p-1)$
- *f*: generator of order q in Z_p^*;
- ***h()* :** a secure hash function
- ***m_w* :** warrant
- ***$t\ t_q$= (g) :*** discrete logarithm assumption holds in ***$t\ t_q$*.**

3.2 Proxy Key Generation

To create a proxy key pair (x_p, y_p) for proxy signer, *n* real signer and the proxy signer execute the following procedure:

1. Each user U_i $(0 \le i \le n)$pick sar and om number $k \in Z_p^*$, compute $r_i = f^{k_i} modp$ (1)

2. Each user U_i discloses the value of r_i, $(0 \le i \le n)$. Then, each user checks whether all $r_i s$ are correct, i.e. $r^q \equiv 1 mod\ p$, for each $0 \le i \le n_i$.

3. Each original signer $O_j(0 \le j \le n)$

   computes $r_P = r_o r_1 \ldots r_n\ mod\ p$,

   $$s_j = k_j + x_j\,.h(m_w, r_P)\ modq \quad \ldots\ldots\ldots\ldots.(2)$$

   and sends the pair (r_j, s_j) to proxy signer *P*.

4. Upon receiving (r_j, s_j), *P* first compute $r_P = r_o r_1 \ldots r_n mod\ p$, and checks whether

   $$f^{s_j} \equiv y_j^{h(m_w, r_P)}.r_j modp, \ldots\ldots\ldots\ldots(3)$$

   If all validation pass, proxy signer calculates

   $$s_P = k_o + x_P.h(m_w, r_P)\ modq \quad \ldots\ldots\ldots.(4)$$

   and sets proxy key pair (x_P, y_P) by

   $$x_P = s_P + s_1 + s_2 + \ldots + s_n modq, \ and$$
   $$y_P = f^{x_P} modp \quad \ldots\ldots\ldots.(5)$$

The point is that only the proxy signer knows the proxy secret key x_P, but (r_P, x_P) needs to be generated by the *n* original signers and the proxy signer jointly.

3. 3 Proxy Signature Generation

To create a proxy signature on a text message *m* that conforms to the warrant m_w, the proxy signer performs the following:

firstly selects a and number $k \in Z_q^*$, then computes

$$r = f^{k} \, mod \; p \ldots \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(6)$$

$$and \qquad s = k + x_P . h(m, m_w, r) mod q \ldots\ldots(7)$$

The resulting proxy signature on message m is $\xi = (m_w, r_P, r, s)$.

3.4 *Proxy* Signature Verification

To verify the validity of ξ, a verifier operates as follows:

1. Check whether or not the message m follows to the warrant m_w.
2. Check whether each user $j(j \in 1, 2, ..., n)$ is specified as the original signer, and proxy signer is specified as the proxy signer in the warrant m_w.
3. Recovery of proxy public key y_P by computing

$$y_P = (y_1 y_2 \ldots y_n)^{h(m_w, r)} . r_P \; mod \; p \ldots\ldots\ldots(8)$$

4. Accept the proxy signature ξ if the following equation holds:

$$f^{s} \equiv y^{h(m, m_w, r)} . r \; modp \ldots\ldots\ldots\ldots\ldots\ldots\ldots(9)$$

4 Security Analysis

Proposition: Under the discrete logarithm assumption, our proxy-multi signature scheme is secure in the random oracle model. We claim that in our scheme even n users combine together, they cannot forge a valid proxy key pair (x_P, y_P) satisfying equation (8) and $y_P = f^{x_P} \; modp$.

If possible, there is an adversary A that can forge a valid proxy key pair in the scheme with multiple original signers, then from A we can construct a new adversary A^{j} that forges a valid proxy key pair in the basic proxy signature scheme. More specifically, A^{j} can be constructed as follows:

For a given public key pair (y_A, y_B), we first choose an index $i \in [1, n]$ and a random number $a \in Z_q^{*}$ at random and set $x_i = x_A + a \; mod \; q$, $y_i = y_A . f^{a} mod \; p$.

Then, for each index $1 \leq j \leq n$ and $j \; f = i$, we select random numbers $x_j \in Z_q^{*}$ such that $\Sigma x_j \; modq = -a$, and set $y_j = f^{x_j} mod \; p$. So we have

$$y_A . y_B = y_B y_1 \ldots y_n \; modp.$$

Finally, we feed on the adversary A by input $(y_B, y_1 \ldots y_n)$. Consequently, when A outputs a valid proxy key pair (x_P, y_P). In addition, any adversary (including the original signers) cannot forge valid proxy signatures in the name of the proxy signer. Therefore, the proposed proxy signature scheme with multiple original signers is unforgeable.

5 Efficiency

Now, we discuss the efficiency of proposed scheme as below:

Firstly, note that the procedure of proxy key pair generation needs to be executed only once for a sufficiently long period. Secondly, to generate a proxy signature, only one modular exponentiation is needed. Thirdly, to improve the concert equations (8) and (9) can be checked together as a single equation. That is, a verifier only needs to check the following equation:

$$\boldsymbol{f^{s} . (y_1 y_2 \ldots y_n)^{-h_1 h_2} . r_P \equiv r \; modp,} \qquad \ldots\ldots\ldots\ldots\ldots(10)$$

where $h_1 = h(m_w, r_P)$ and $h_2 = h(m, m_w, r)$. So all phases can be carried out in modular exponentiations $7E$, where E is modular multiplication by means of an exponent array and a proxy signature can be generated and verified by total $6M$. Where M modular multiplication.

6 Conclusion

In this paper, we proposed a new efficient proxy-multi signature scheme based on discrete logarithm problem having different form of public key with more efficiency and security. This proxy- multi signature can be also used for suitable type of blockchain structure. Our scheme satisfies all the security properties of a proxy-multi signature.

REFERENCES

[1] H. Chine, Extending RSA cryptosystems to proxy multi-signature scheme allowing parallel individual signing operation; Journal. Chin Inst Engineering, vol. 29, no.3, pp.527-532, (2006).

[2] J. Z. Dai, X. H. Yang and J. X. Dong, Designated-Receiver Proxy Signature Scheme for Electronic Commerce; Proceeding of IEEE International Conference on Systems and Cybernetics,Vol.1,pp.384-387, (2003).

[3] M. Gasser, A. Goldstein, C. Kaufman and B. Lampson, The digital distributed system security architecture. Proceedings of NCSC, pp. 305-319, (1989).

[4] C. L. Hsu, T. S. Wu, and W. H. He; New proxy-multi signature scheme. Applied Mathematics and Computation, Vol. 62, pp.1201-1206, (2005).

[5] S. J. Hwang and C.C. Chen, A new proxy multi-signature scheme. International Workshop on Cryptology and Network Security, Taiwan, ROC, pp. 199-204, (2001).

[6] S. Kim, S. Park and D. Won, Proxy signatures. Revisited. In: ICICS97. LNCS 1334. Springer-Verlag, 223-232, (1997).

[7] B. Lee, H. Kim and K. Kim, Secure mobile agent using strong non-designated proxy signature. Information security and private (ACISP01), LNCS 2119, Springer-Verlag, PP.474-486, (2001).

[8] B. Lee, H. Kim and K. Kim, Strong proxy signature and its applications. In: Proceeding of the 2001 symposium on cryptography and information security (SCIS01), vol. 2(2), 603-608, (2001).

[9] Y. Liu, H. Wen and C. Lin, Proxy-protected signature secure against the undelegated proxy signature attack. Computation Electron Eng Vol. 33, No.3, pp.177-185, (2007).

[10] R. Lu and Z. Cao, Designated verifier proxy signature scheme with message recovery. Applied Math Computing, Vol.169, No.2, 1237-1246, (2005).

[11] M. Mambo, K. Usuda and E. Okamoto, Proxy signatures for delegating sign operation. Proceeding of the 3rd ACM conference on computer and communications security (CCS96), ACM press, pp. 48-57, (1996).

[12] M. Mambo, K. Usuda and E. Okamoto, Proxy signatures: delegation of the power to sign messages. IEICE Trans Fundamental, E79-A(9), pp. 1338-1354, (1996).

[13] T. Okamoto, Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes; In Proc. CRYPTO 92, pp 31-53. Lecture Notes in Computer Science; No. 740, Springer-Verlag, (1993).

[14] H. U. Park and I. Y. Lee, A digital nominative proxy signature scheme for mobile communications. Information and Communications Security (ICICS01), LNCS 2229, pp. 451-455. Springer-Verlag, (2001).

[15] C. P. Schnorr, Efficient Signature Generation by Smart Cards; Journal of Cryptology, Vol. 4, No.3, pp. 161-174, (1991).

[16] K. Shum and V. K. Wei; A strong proxy signature scheme with proxy signer privacy

protection. In: Proceedings of IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE02), (2002).

[17] H. M. Sun; On proxy-multi signature schemes, International Computer Symposium, Taiwan, ROC, pp. 65-72, (2000).

[18] L. Yi, G. Bai and G. Xiao, A new type of proxy signature scheme. Electron Lett, 36(6), 527-528,(2000).

[19] T. ElGamal, "A public key cryptosystem and signature scheme based on the discrete logarithms." *IEEE Transactions on Information Theory*, 31, 469–472, (1985).