A Proxy to Proxy Blind Multi-Signature Scheme based on DLP

Subhashree Naik
M tech, Scholar
Centurion University
Of Technology, Bhubaneswar

Manoj Kumar Behera
Assistant Professor
Centurion University
Of Technology, Bhubaneswar

Sumanjit Das
Assistant Professor
Centurion University
Of Technology, Bhubaneswar

ABSTRACT

Proxy blind multi-signature , it combines the properties of proxy-signature , blind signature and multi-signature ,which has been applied in different application .In this paper, we showed a new proxy to proxy blind multi-signature based on difficulty of solving the discrete logarithm problem (DLP) which fulfill the absence of single proxy signer in Dongre's[9] scheme by delegating his signing capabilities to a designated proxy signer . Moreover, we are taking this existing scheme into a new level or in next grade in order to sign the document on behalf of group of original signers.

Keywords

Proxy, Blind, Multi-signature, DLP

1. INTRODUCTION

To prevent the forgery of message between senders and receivers, a digital signature technology is required. Now a day different types of digital signatures are introduced like blind signature, proxy signature, multi signature etc.The blind signature scheme was first designed by Chaum [2] in 1982. It allows a signer to sign on a message without revealing the content of the message .This type of signature protects the applicant of signing or participants of different applications in electronic voting and electronic payment system. Membo.et.al in 1996[3] first propounded the concept of proxy signature, that notion allows a designated person called proxy signer, signs message on behalf of an original signer and the original signer delegates his signing power to his proxy signer .Proxy blind signature, is the combination of blind signature and proxy signature was first proposed by Lin and Jan [4] in 2000. First multi-signature scheme was proposed by Itakura and Nakamura [5] in year 1983. Harn L[6] proposed a multi digital signature scheme which allows two or more users to generate signature collaboratively and simultaneously . Finally the concept of proxy blind multi signature is the extension of proxy blind signature , was first introduced by Lu ,Cao ,Zhou in 2005 [7] . But according to Lu et al's [7], Sun et al [8] the scheme is not secure against original Signer's forgery attack, a dishonest original signers can forge a proxy secret key and generate a valid proxy multi-signature. So to overcome this problem, Sangeet Dongre [9] proposed a scheme that solves the forgery attack by using trusted third party called certificate authority which certifies public keys. But in some real situation, we need to inherit the technology in some extent. Here, a new scheme proxy to proxy blind multi-signature is proposed based on DLP. When the single proxy signer is absent then a signature scheme can be created in which after accepting delegation from the original signer's group, a proxy signer can also delegate the signing capabilities to other proxy signer in the next grade in order to sign the document on behalf of group of original signers. This scheme shows the improved in term using different parameters and communication overhead and also satisfies all the security properties.

2. A PROXY TO PROXY BLIND MULTI-SIGNATURE SCHEME BASED ON DLP

In this section, a new proxy to proxy blind multi-signature based on DLP scheme is proposed .This scheme involves different cryptographic primitive entities : A trusted third party called certificate authority CA ,group of original signers O_i ,two proxy signers P_1 ,P_2 and a requester R of the signature. Here, in absence of first proxy signer P_1 , second proxy signer P_2 signs a blinded message m on behalf of first proxy signer and all original signers.

2.1 System Initialization

CA selects p and q as a large prime number such that q | p-1.

g : an element of Z_p^* with order q.

mw_o : is the warrant which keeps information about the original signers and proxy signers ,message type ,delegation limit by authority and valid delegation period.

$h(.)$: Public cryptographically strong hash functions.

| | : Concatenation of the strings.

Then CA generates a secret key $\alpha \in_R Z_q^*$ and computes

$\equiv g^{\alpha}$(mod p) as public key.

Keeping α as a secret and CA broadcasts p , q , g, β, h(.)

2.2 Registration Phase

Here , all the signers has registered with the certificate authority CA by sending their identities ID_i , ID_{p1}, ID_{p2} .

1) Each original signer $O_i(1 \leq i \leq n)$ selects $v_i \in Z_q^*$ and computes

$u_i = g^{h(v_i||ID_i)} mod\ p$……………………………................. .(1)

Similarly, proxy signers select $v_{p1}, v_{p2} \in Z_q^*$ and compute

$u_{p1} = g^{h(v_{p1}||ID_{p1})} mod\ p$…………………………...............(2)

$u_{p2} = g^{h(v_{p2}||ID_{p2})} mod\ p$……………………......................(3)

And each sends $(u_{i,}u_{p1}u_{p2},)$ to CA

2) CA selects a time variant $t_i, t_{p1}, t_{p2} \in Z_q^*$ and compute for each original signers,

$Y_i = u_i g^{t_i} - h(ID_i)\ mod\ p$……………………………..........(4)

$w_i = t_i + \alpha\left(Y_i + h(ID_i)\right)\ mod\ q$ ……………………………...(5)

And send $(Y_{i,}w_i)$ to O_i

For first proxy signer,

$Y_{p1} = u_{p1} g^{t_{p1}} - h\left(ID_{p1}\right)\ mod\ p$………...............................(6)

$w_{p1} = t_{p1} + \alpha\left(Y_{p1} + h\left(ID_{p1}\right)\right)\ mod\ q$ ……………………..(7)

And send $(Y_{p1,}w_{p1})$ to P_1

For second proxy signer,

$Y_{p2} = u_{p2} g^{t_{p2}} - h\left(ID_{p2}\right)\ mod\ p$……………………...........(8)

$w_{p2} = t_{p2} + \alpha\left(Y_{p2} + h\left(ID_{p2}\right)\right)\ mod\ q$ …...........................(9)

And send $(Y_{p2,}w_{p2})$ to P_2

3) Now each signers can compute secret key and public key

For original signers, secret key and public key will be

$x_i = w_i + h(v_i||ID_i) mod\ q$ …………………………..(10)

$y_i = g^{x_i}$ mod p ……………………………………………...(11)

$= (Y_i + h(ID_i))\beta^{(Y_i + h(ID_i))}\ mod\ p$

If it holds, then accepts it otherwise reject it.

For first proxy signer,

$x_{p1} = w_{p1} + h(v_{p1}||ID_{p1}) mod\ q$ … ……………………..(12)

$y_{p1} = g^{x_{p1}}$ mod p ………………………………………....(13)

$= \left(Y_{p1} + h\left(ID_{p1}\right)\right)\beta^{\left(Y_{p1} + h\left(ID_{p1}\right)\right)}\ mod$ p

If it holds, then accepts it otherwise reject it.

For second proxy signer,

$x_{p2} = w_{p2} + h(v_{p2}||ID_{p2}) mod\ q$…………………………(14)

$y_{p2} = g^{x_{p2}}\ mod\ p$……………………….........................(15)

$= (Y_{p2} + h(ID_{p2}))\beta^{\left(Y_{p2} + h\left(ID_{p2}\right)\right)}\ mod\ p$

If it holds, then accepts it otherwise reject it.

2.3 Proxy key pair generation

In this phase, all the original signers will provide their signing capability to a single proxy signer.

1) Each original signer chooses $k_i \in Z_q^*$ and computes

$r_i = g^{k_i}\ mod\ p$ ………………………………………………(16)

And broadcasts r_i

$r_o = r_1 r_2 \ldots \ldots r_n\ mod\ p$……………………………………...(17)

$s_i = x_i + k_i h(mw_o||r_o) mod\ \ q$ …………………………….(18)

Then each original signer broadcasts (r_o, mw_o) and sends s_i to the first proxy signer through a insecure channel.

2) Here the first proxy signer checks

$g^{s_i} = y_i r_i^{h(mw_o||r_o)} mod\ p$ ……………;.........................(19)

If it holds then computes the signing secret key

$x_1' = \sum_{i=1}^{n} s_i + x_{p1}\ mod\ q$ ………………………………... (20)

And public key

$y_1' = g^{x_1'}\ mod\ p$…………………………………………….(21)

$$y_1' = \prod_{i=1}^{n} y_i y_{p1} r_o^{h(mw_o||r_o)}\ mod\ p$$

2.4 Proxy to Proxy Key pair generation

Here, the first proxy signer sends his signing capability to the second proxy signer.

1) First proxy signer selects $k_{p1} \in Z_q^*$ and computes

$r_{p1} = g^{k_{p1}}\, mod\, p$ ……………………………………………(22)

$s_{p1} = x_1' + k_{p1} h(mw_o||r_{p1}) mod\;\; q$ ……...........................(23)

Then first proxy signer broadcasts (r_{p1}, mw_o) and send s_{p1} to the second proxy signer through a insecure channel.

2) Here the second proxy signer checks

$g^{s_{p1}} = y_1' r_{p1}^{h(mw_o||r_{p1})} mod\, p$ ……………………………….(24)

If it holds then computes the signing secret key

$x_2' = s_{p1} + x_{p2}\; mod\; q$ ……………………………………(25)

And public key

$y_2' = g^{x_2'}\, mod\, p$ ……………………………………………..(26)

$y_2' = y_1' y_{p2} r_{p1}^{h(mw_o||r_{p1})} mod\, p$

2.5 Proxy to Proxy Blind Multi-Signature Generation

In this phase, the requester or receiver randomly chooses blind factor, makes the message blinded and sends to the second proxy signer .Then the second proxy will give signature on blinded message on behalf of first proxy signer.

1) The second proxy signer randomly selects $k_{p2} \in Z_q^*$ and computes

$r_{p2} = g^{k_{p2}}\;\, mod\, p$ ……………………………………………..(27)

And then sends r_{p2} to the receiver *R.*

2) The requester R selects two random numbers that $a, b \in Z_q^*$ and computes

$r = r_{p2}^a . g^b . y'^{ab}_2\;\; mod\, p$ ……………………………………(28)

$e = h(r||m)$ …………………………………………………....(29)

$e^* = a^{-1}e - b\;\; mod\, p$ …………………………………......(30)

And sends e^* to the proxy signer p_2.

3) After receiving e^* , P_2 computes

$s' = -e^* x'_2 + k_{p2}$ ……………………...……………………..(31)

And sends it to user R.

4) With receiving s’ , R computes

$s = s'a + b\;\; mod\; q$ …………………...…………………..….(32)

2.6 Signature Verification

Any person can verify the validity of the signature (mw_o, r_{p1}, m, e, s) by checking

$e = h\big(g^s (y_2')^e ||m\big)\;\; mod\, p$ ……………………………….(33)

Where $y_2' = y_1' y_{p2} r_{p1}^{h(mw_o||r_{p1})} mod\, p$

If it is correct, the verifier will accept that it is a valid proxy to proxy blind multi-signature, otherwise rejects it.

3. SECURITY ANALYSIS

In this section, the proposed scheme has analyzed all the security properties and satisfies all the properties of the proxy blind multi signature.

3.1 Distinguish ability:

The proxy to proxy blind multi signature (mw_o, r_{p1}, m, e, s) holds the warrant mw_o and the proxy public key

$y_2' = y_1' y_{p2} r_{p1}^{h(mw_o||r_{p1})} mod\, p$ Where

$y_1' = \prod_{i=1}^{n} y_i y_{p1} r_o^{h(mw_o||r_o)}\;\; mod\, p$ includes all the original signer’s public key Y_i and public keys of first Y_{P1} and second Y_{P2} proxy signer. Likewise any verifier can easily distinguish the proxy to proxy blind multi-signature from the normal signature.

3.2 Non-repudiation:

Here, neither first nor second proxy signer can get the secret key of original signer nor the original signer can get the secret keys of proxy signers. And also the first proxy signer cannot get the secret key of other proxy signer party. During the verification of this notion, the verifier can confirm that the signature of the message have public keys of all the original signers and the two proxy signers. So, any party cannot sign in place of other party.

3.3 Prevention of Misuse:

The proposed notion can prevent proxy key pair misuse, because the warrant mw_o includes the entire original signer O_i ‘s, proxy signers P_1 ,P_2 ‘s identities information ID_i , ID_{p1}, ID_{p2} and message type to be signed by the proxy signer, delegation period etc.

3.4 Identifiability

On the one hand, the warrant mw_o includes the entire original signer O_i ‘s, proxy signers P_1 ,P_2 ‘s identities information ID_i, ID_{p1}, ID_{p2} . On the other hand, the proxy public key

$y_2' = y_1' y_{p2} r_{p1}^{h(mw_o||r_{p1})} mod\, p$ Where $y_1' = \prod_{i=1}^{n} y_i y_{p1} r_o^{h(mw_o||r_o)}$ mod p includes all the original signer’s public key Y_i and public keys of first Y_{P1} and second Y_{P2} proxy signer. Hence, anyone can determine the identity of the corresponding proxy signer from a proxy signatur.

3.5 Strong Un-deniability

Since the proxy public key contains the public keys of both original signers and proxy signers. So both the signer cannot deny their behavior.

3.6 Strong Un-forgeability

Schemes	Proxy Key Generation	Signing Phase	Verification	Total
Lu et al.[7]	$7n\,T_{exp} + 3n\,T_{hash} + 8n\,T_{mul}$	$(n+3)\,T_{exp} + (n+1)T_{hash} + (n^2 - n+3)\,T_{mul}$	$(n+2)T_{exp} + (n+1)T_{hash} + (n^2 - n+1)\,T_{mul}$	$(9n+5\,)\,T_{exp} + (5n+2\,)\,T_{hash} + (2n^2+6n+4)\,T_{mul}$
Sangeet Dongre [9]	$(2n\ +1)T_{exp} +2nT_{hash} + (n^2+n)\,T_{mul}$	$4T_{exp} + 2T_{hash} + 6T_{mul}$	$3T_{exp} + 2T_{hash} +(n+2)\,T_{mul}$	$(2n+8\,)\,T_{exp} + (2n+4)\,T_{hash} + (n^2+2n+8)\,T_{mul}$
Our scheme	$(2n+1)T_{exp} + 2nT_{hash} +(n^2+n)\ T_{mul}$	$4T_{exp} + 2T_{hash} + 6T_{mul}$	$3T_{exp} + 2T_{hash} + 3T_{mul}$	$(2n+8)T_{exp} + (2n+4)T_{hash} + (n^2+n+9)\,T_{mul}$

Table 1.Comparison of computational cost with different schemes

Here ,if any other party want to forge or obtain the delegation information ,then he cannot able to get the proxy to proxy signature key x_2' since it contains proxy signer's secret key x_p and its proxy signing secret key x_1' which is obtained by combining secret keys of all signers that the adversary does not know. So he cannot able to generate proxy to proxy signature secret key .Therefore, this scheme has strong unforgeability.

3.7 Secret key Dependencies:

The signature extraction of proxy to proxy blind multi-signature $s = s'a + b \ mod\, q$ depends on s' and s' contains proxy to proxy secret key x_2' which is impossible to create without the secret keys of all original signers and first proxy signer. Hence, the second proxy signer directly depends on the secret keys of first proxy signer.

3.8 Verifiability:

The proposed scheme satisfies verifiability property. The validness of the signature is verified as –

$$h\left(g^{s}(y_2')^{e}||m\right) = h\left(g^{s'a+b}(y_2')^{e}||m\right)$$

$$= h\left(g^{(-e^{*}x'_2+k_{p2})a+b}(y_2')^{e}||m\right)$$

$$= h\left(g^{(-e^{*}x'_2)a}g^{ak_{p2}\cdot}g^{b}(y_2')^{e}||m\right)$$

$$= h\left({y_2'}^{(-e^{*}a)}{r_{p2}}^{a\cdot}g^{b}(y_2')^{e}||m\right)$$

$$= h\left({r_{p2}}^{a\cdot}g^{b}{y_2'}^{(-e^{*}a)}(y_2')^{e}||m\right)$$

$$= h\left({r_{p2}}^{a\cdot}g^{b}{y_2'}^{-(e-ab)}(y_2')^{e}||m\right)$$

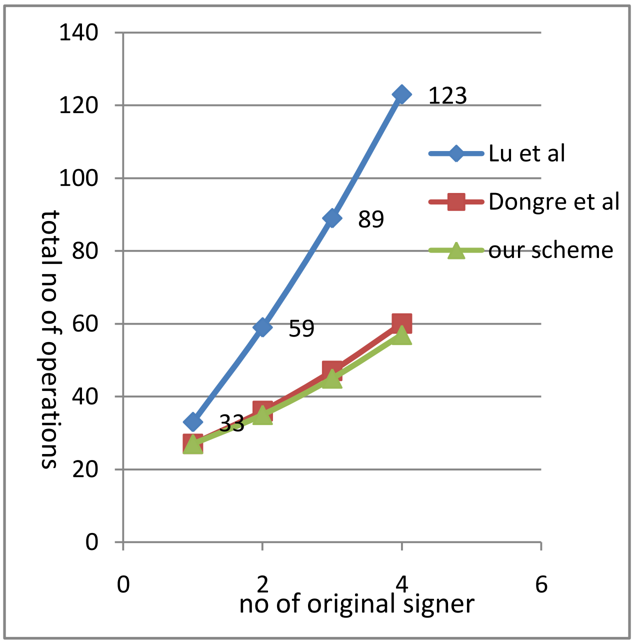
$$= h\left({r_{p2}}^{a\cdot}g^{b}\ (y_2')^{ab}||m\right)$$

$$= h(r||m)$$

$$= e$$

3.9 Proxy Unlinkability

The proxy unlinkability holds if only if there is no conjunction between (r_{p2}, e^{*}, s') and $(mw_{o,}m, e, s, r_{p1})$ .In this scheme , it is obvious from equation (27) to (32) that the value r_{p2} is only included in equation (28) and connected to e through equation (29) .Similarly , e^{*} and s' are also be associated .For this one must be able to compute 'r ' which is masked with two random numbers. They fail again due to the random numbers. So , the proposed scheme provides proxy unlinkability.



Graph 1. Comparison of computational cost with different schemes

4. EFFICIENCY

This is the new scheme which is more efficient as compared to the scheme of Lu et al's [7] which was newly proposed in literature and also effective from Dongre's [9] scheme. The detailed costs in each phase are analogized in Table 1.Also in Graph 1, the comparison results are tried to be shown by means of graphs. This graph is generated by taking the different values of *n*. Here proxy to proxy key pair generation phase is a particular of our scheme, thus not be involved in the comparison. In this table,T_{mul}, T_{exp} , T_{hash} denote the once running of multiplication operation ,modulo exponential and hash operations. The modulo-additions are omitted due to its high performance. Also note that all the minus exponential operations can be transformed to positive exponential operations without losing almost any efficiency.

5. CONCLUSION

In this paper, we represent a proxy to proxy blind multi-signature scheme based on DLP. This proposed scheme satisfies all the securities requirement and also does not require any secure channel for communication .Therefore, this scheme is useful in many real situation ,such as e-cash and e-commerce . The future work can design more effectively scheme with low computation that provably secure in the standard model .We can be also designed a new scheme in which each original signer delegates a proxy signer when some original signer are available to provide signature.

6. REFERENCES

[1] Behrouz A.Forouzan.2007.Cryptography and Network Security Tata McGraw Hill.

[2] David Chaum. 1982. Blind Signatures for Untraceable Payments. In CRYPTO, pages 199-203.

[3] Masahiro Mambo, keisuke Usuda, and Eiji Okamoto. 1996. Proxy Signatures for Delegating Signing Operation. In CCS '96: Proceedings of the 3rd ACM conference on Computer and communications security, pages 48-57, New York, NY, USA.

[4] W.D. Lin, and J.K. Jan. 2000. A security personal learning tools using a proxy blind signature scheme, Proc. of Int'1 Conf. on Chinese Language Computing, pp.273-277.

[5] K. Itakura and K. Nakamura. A Public Key Cryptosystem Suitable for Digital Multi-signatures. NEC Research and Development, (71):1-8, 1983.

[6] Harn L,Xu Y. 1994. Design of Generalized ElGamal Type Digital Signature Schemes Based on the Discrete Logarithm .Electronics Letters, 30(24):2025-2026.

[7] Rongxing Lu, Zhenfu Cao, and Yuan Zhou. 2005. Proxy Blind Multi-signature Scheme without a Secure Channel. Applied Mathematics and Computation, 164(1):179-187.

[8] Ying Sun, Chunxiang Xu, Qi Xia, and Yong Yu . 2009. Analysis and Improvement of a Proxy Blind Multi-signature Scheme without a Secure Channel. In IAS, pages 661-664. IEEE Computer Society.

[9] Sangeet Dongre and Sujata Mohanty. 2010 .A Secure and efficient Proxy Blind Multi-signature Scheme based on DLP. In Fifth International Conference on Industrial and information Systems, NIT Suratkal, Karnataka, India.