AN EFFICIENT PROXY-MULTI SIGNATURE SCHEME BASED ON DLP

SWATI VERMA

Abstract: During electronic communication, proxy signature helps the signer to sign message on behalf of the original signer. This type of signature scheme is usedwhen the signatory is not available to sign this document. In this paper, wepropose a new proxy-multi signature scheme, based on discrete logarithm problem, where the proxy signer can signmessage on behalf of the group of original signer. Our scheme is suitable for e-commerce applications, such as mobile agent in e-commerce settings.

Keyword*:* Proxy signature, Proxy-multi signature, DLP, Security.

Introduction: The notion of proxy signature was first introduced by Mambo et al. in 1996 [7]-[8].Aproxy signature scheme is an important investigation in the field of digital signature which involves three entities: an original signer, a proxy signer and a verifier.It provides tools to the original signer to delegate his signing right to a particularsigner, known as proxy signer. Once the proxy signer signed the message on behalfof the original signer, the verifier, who knows the public keys of the original and proxy signers, verifies the validity of the proxy signature after receiving it [4]-[6].

In 2000, Yi et al. [10] proposed another type of proxy signature scheme calledProxy-multi signature schemes. In a proxy-multi signature scheme, a designatedproxy signer can generate the signature on behalf of a group of original signers.Proxy-multi signatures can play important role in the following scenario: A company releases a document that may involve the financial department, engineering department, and program office, etc [9]. The document must by signed jointly by theseentities, or signed by a proxy signer authorized by these entities. One solution tothe later case of this problem is to use a proxy multi-signature scheme.According to whether valid multi-signatures are generated only by the proxysigner, proxy multi-signatures can be classified into two types. One is a proxy-unprotected multi-signature, in which besides the proxy signer, only the cooperationof all members in the original group can create valid proxy signatures. The other isa proxy-protected multi-signature, in which only the proxy signer can create validproxy signatures.

Then some proxy multi-signature schemes were proposed [1,2,3]. In this paper,we propose a new proxy-multi signature scheme based on difficulty of solving discrete logarithm problem. The algorithm for a proxy signature is as follows:

2. Proxy Signature Algorithm

The proxy signer can sign some messages on behalf of the original signer. Afterreceiving the proxy signature the verifier which knows the public keys of the original and proxy signers verified the validity of the proxy signature. Generally, a proxysignature consists of four algorithms:

***Key Generation:** This probabilistic have two public and private key pairsfor the original signer.

***Proxy Generation:** The original signer and the proxy signer execute thisinteractive randomized algorithm to generate a proxy key pair (x_P, y_P) forproxy signer, such that only proxy signer knows the value of x_P, while y_P ispublic.

***Proxy Signature Generation:** The proxy signer runs this algorithm togenerate a proxy signature $\xi$for a message m by using the proxy private keyx_P.

* Proxy Signature Verification:A verifier runs this deterministic algorithmto check whether proxy signature $\xi$for a message m is valid with respect to a specific original signer and a proxy signer.

3. Classification of Proxy Signature: Proxy signature schemes are classified mainly into following categories.

- **Full Delegation :** In this category, original signer gives his private key to aproxy signer and the proxy signer signs the document using original signer'ssecret key. The drawback of this class of proxy signature is the absence of a distinguish ability between original signer and proxy signer.
- **Partial Delegation :** In this category of proxy signature, the original signerderives a proxy key from his secret key and gives to the proxy signer as adelegation of his signing right. In this case, the proxy signer can misuse thedelegation right, because partial delegation does not restrict the proxy signer'sto misuse this signing right.
- **Delegation by Warrant:** In this category, the original signer gives the proxysigner a warrant, which construct of a message part and public key. Then, theproxy signer can use the corresponding private key to sign. However, since itrequires consecutive execution, it cannot provide faster processing speed.
- **Unprotected Proxy Signature:** In the category of proxy-unprotected signaturescheme, the proxy signer generates proxy signatures with the proxy

signaturekey given by the original signer only. As a result, both the original signer andthe proxy signer can produce the same proxy signatures. When dispute occursbetween the original signer and the proxy signer, no one can identify the realsigner of the message.

- **Protected Proxy Signature:** In the category of proxy-protected signaturescheme, only the proxy signer can generate valid proxy signatures. In otherwords, anyone else, including the original signer, is unable to produce the sameproxy signatures.

Organization: The remaining parts of this paper an organized as follows. Insection 2, 3 and 4, we elaborate proxy signature algorithm, classification and security properties of the proxy signature scheme, respectively. Next,we proposed our proxy-multi signature scheme in section 5. In section 6 and 7, weanalyze the security and efficient of our proposed scheme, respectively. Finally, in section 8,we give our concluding remarks.

Security Requirements of Proxy Signature Scheme: The security requirements for any proxy signature are first studied in [5]-[6], andlater those were improved in [7]-[8]. According to them, a secure proxy signaturescheme is expected to satisfy the following five requirements:

Verifiability: The verifier is convinced that the original signer has given consentto the proxy signer to sign a message.

Strong unforgeability: Nobody else other than the designated proxy signercan create a valid proxy signature on behalf of the original signer.

Strong identifiability: Anyone can determine the identity of the proxy signerof the corresponding proxy signature.

Strong undeniability: Once a proxy signer creates a valid proxy signature onbehalf of an original signer, he cannot repudiate the signature creation againstanyone else.

Prevention of misuse: The proxy signer cannot use the proxy key for thepurposes other than generating a valid proxy signature. In case of misuse, theresponsibility of the proxy signer should be determined explicitly.

Preliminaries

Discrete Logarithm (DL) assumption:

Let $G_q = \langle g \rangle$ be a cyclic multiplicative group generated by g of order q. Then, on inputs $(g, g^x) \in G_q^2$, where $x \in Z_q$ is a random number, there is no probabilisticpolynomial-time algorithm that outputs the value of x with non-negligible probability.The DL assumption is widely believed to be true for many cyclic groups, such asthe multiplicative subgroup $G_q = \langle g \rangle$ of the finite field Z_p, where p is a large primeand q is a prime factor of p-1.

Proposed Proxy-Multi Signature Scheme: In this section, we propose a new proxy protected signature scheme, which is basedon discrete logarithm problem [15] having different form of public key and with high security. 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, a large prime factor 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.*

5.1 Key Generation

For the convenience of describing our work, we define the parameters as follows:

* U_j : the original signer
* P: the proxy signer
* U_i : all users
* p, q : two large prime number with $q/(p-1)$
* g: generator of order q in Z_p^*
* h() : a secure one-way hash function
* m_w : warrant
* G_q =<g>: discrete logarithm assumption holds in G_q.

5.2 Proxy Key Generation

To generate a proxy key pair (x_p, y_p) for proxy signer, n original signers and the proxy signer execute the following protocol:

Each user $U_i (0 \le i \le n)$ picks a random number $k \in Z_p^*$, compute $r_i = g^{k_i} \bmod p$ (1)

Each user U_i reveals the value of $r_i (0 \le i \le n)$. Then, each user checkswhether all $r_i s$ are correct, i.e. $r_i^q = 1 \bmod p$, for each $0 \le i \le n$.

Each original signer $O_i (0 \le i \le n)$ computes $r_p = r_{0,} \ldots\ldots r_n \bmod p$.

$s_j = k_j + x_j . h(m_w, r_p) \bmod q$ (2)and sends the pair (r_j, s_j) to proxy signer P.

Upon receiving (r_j, s_j), P first compute $r_p = r_0, r_1 \ldots\ldots\ldots r_n \bmod p$, and checks whether

$$g^{s_j} = y_j^{h(m_w, r_p)} . r_j \bmod p, \quad (3)$$

If all validation passes, proxy signer calculates

$$s_p = k_0 + x_p . h(m_w, r_p) \bmod q \quad (4)$$

and sets proxy key pair (x_p, y_p) by

$$x_p = S_p + S_1 + S_2 + \ldots\ldots S_n \bmod q, \; y_p = g^{x_p} \bmod p \quad (5)$$

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 signerjointly.

5.3 Proxy Signature Generation

To generate a proxy signature on a message m that conforms to the warrant m_w, the proxy signer performs the following: first selects a random number $k \in Z_q^*$ computes

$$r = g^k \bmod p \quad (6)$$

and $S = k + x_p . h(m, m_w, r) \bmod q \quad (7)$

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

5.4 Proxy Signature Verification

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

Check whether the message m conforms to the warrant mw. If not, stop. Otherwise, continue.

Check whether each user $j (j \in 1,2 \ldots\ldots n)$ is specified as the original signer,and proxy signer is specified as the proxy signer in the warrant m_w.

Recover the proxy public key y_p by computing

$$y_p = (y_1, y_2 \ldots . y_n)^{h(m_w, r)} . r_p \bmod p \quad (8)$$

Accept the proxy signature ξ if the following equation holds: $g^s = y_p^{h(m, m_w, r)} . r \bmod p \quad (9)$

Security Analyses:

Proposition 6.1 *Under the discrete logarithm assumption, our proxy-multi signature scheme is secure in the random oracle model.*

Proof: we claim that in our scheme even n users combine together, they cannot forge avalid proxy key pair (x_P y_P) satisfying equation (8) and $y_p = g^{x_p} \bmod p$.

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 Ao that forges a valid proxy key pair in the basic proxy signature scheme. More specifically,Ao 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 randomnumber $a \in Z_q^*$ and set $x_i = x_A + a \bmod q, \; y_i = y_A . g^a \bmod p.$ Then, for each index$1 \le j \le n and j \ne i$,we select random numbers $x_j \in Z_q^*$ such that $\sum x_j \bmod q = -a \;\; and \;\; set \;\; y_j = g^{x_j} \bmod p.$ So we have $y_A y_B = y_B y_1 \ldots y_n \bmod p.$ Finally, we feed on the adversary A by input $(y_B y_1 \ldots y_n)$. Consequently, when Aoutputs a valid proxy key pair (x_P, y_P). In addition, any adversary (including theoriginal signers) cannot forge valid proxy signatures in the name of the proxy signer.Therefore, the proposed proxy signature scheme with multiple original signers isunforgeable.

7. Efficiency

Now, we discuss the efficiency of proposed scheme as follow: 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 enhance the perform equations (8) and (9) can be checked together as a single equation. That is, a verifieronly needs to check the following equation:

$$g^s . (y_1 . y_2 \ldots . y_n)^{-h_1 h_2} . r_P \equiv r \bmod p,$$

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

8. Conclusion

In this paper, we proposed a new proxy-multi signature scheme based on discretelogarithm problem with more efficiency. Our scheme satisfies the security properties of a proxy signature with random oracle model.Our scheme is suitable for e-commerce applications, such as mobile agent in e-commerce settings.

References :

1. Chien H., Extending RSA cryptosystems to proxy multi-signature schemeallowing parallel individual signing operation. J Chin Inst Eng 29(3), 527-532,(2006).
2. C.L. Hsu, T.S. Wu, and W.H. He., New proxy multisignature scheme. AppliedMathematics and Computation, vol. 62, pp.12011206, (2005).
3. S.J. Hwang, C.C. Chen, A new proxy multi-signature scheme. InternationalWorkshop on Cryptology and Network Security, Taiwan, ROC, pp.199-204, (2001).
4. Kim S., Park S. and Won D., Proxy signatures. revisited. In: ICICS97. LNCS1334. Springer-Verlag, 223-232, (1997).
5. Lee B., Kim H. and Kim K., Secure mobile agent using strong non-designatedproxy signature. In: Information security and private (ACISP01), LNCS 2119,Springer-Verlag, 474-486, (2001).
6. Lee B., Kim H., and Kim K., Strong proxy signature and its applications. In:Proceeding of the 2001 symposium on cryptography and information security(SCIS01), vol. 2(2), 603-608, (2001).
7. Mambo M., Usuda K. and Okamoto E., Proxy signatures for delegating signoperation. In: Proceeding of the 3rd ACM conference on computer and communications security (CCS96), ACM press, 48-57, (1996).
8. Mambo M., Usuda K. and Okamoto E., Proxy signatures: delegation of thepower to sign messages. IEICE Trans Fundam, E79-A(9), 1338-1354, (1996).
9. Schnorr C.P., Efficient Signature Generation by Smart Cards; Journal of Cryptology, Vol. 4, No.3, pp. 161-174, (1991).
10. Yi L., Bai G. and Xiao G., A new type of proxy signature scheme. ElectronLett, 36(6), 527-528, (2000).

***

Swati Verma/Research Scholar
School of Studies in MathematicsPt. Ravishankar Shukla University Raipur(C.G.)
swativerma15@gmail.com.