MESSAGE RECOVERY USING PROXY MULTI-SIGNATURE SCHEME WITH VERIFIABLE SELF-CERTIFIED PUBLIC KEY

MANOJ KUMAR CHANDE[1]

Department of Mathematics, Shri Shankaracharya Institute of Professional Management and Technology, Raipur, Chhattisgarh, India

ABSTRACT

In a proxy multi-signature scheme (PMSS), more than one actual signers cooperate each other to transfer their signing authority to a particular person named as proxy(delegated) signer. In this paper a PMSS is proposed, incorporate functionality of message recovery and verifiable self-certified public keys (SCPK). In our scheme, the delegated signer generates an authentic and valid proxy multi-signature (PMS) for plural actual signers. The verifier can verify signature and simultaneously recover message from the signature. One of the advantages of proposed scheme is that problem of non-repudiation is eliminated by the use of verifiable SCPK. All the three tasks of public key validation, proxy signature validation , and recovery of message are performed in one stroke. The security of our PMSS rests upon discrete log problem (DLP). The discussion regarding security of our scheme demonstrate that how the active attacks fail against security of our PMSS. This scheme is applicable for short messages only.

KEYWORDS: Discrete Logarithm Problem (DLP), Proxy Signature, Multi-signature, Message Recovery, Self- certified Key.

Digitalized signatures are an important tool and plays a very crucial role in security of modern electronic transactions. The signatures popular in digital world are RSA [1] and ElGamal [2]. Digital signature provides confidentiality, data integrity, and authentication. In commonly used signature the signatory apply his secret key to create signature for the desired message, and validation of signature can be done by the verifier using public key of actual signer. A certification authority (CA) issues these public keys to each signer to make sure that the public keys used are authentic. To manage these public key certificates is quite cumbersome and costly because of storage, communication, computation costs increases with the number of participants. The genuineness of public keys is questioned till, Girault [3], gave the notion of SCPK. In this approach every user is able to determine his secret key, while the CA, is responsible for generation of public keys. This reduces the computation and communication efforts. Petersen et al. [4], shows that this approach of Girault [3], still has a problem with non-repudiability. Later Kim, Park and Won (KPW) [5], gave the solution of this problem in form of verifiable SCPK.

The digitalized signatures can be classified mainly in two categories: First the signatures with the appendix [2], [6] and second is signatures which allows recovery of message [7-10]. The signature schemes which allows to recover message restricts an adversary to obtain message through the appendix. The actual message remains safe and unaltered until the recipient decrypts it, so in this way these schemes provide confidentiality of message along with authenticity, integrity, and non-repudiability. The message is being sent along with the signature and recovered by the designated verifier. The hashing of message is not required and need not be sent along with the signature, which brings down the requirement of computation, storage space, and communication bandwidth.

Mambo, Usuda and Okamoto (MUO) [11], gave the first construction of proxy/delegated signature. Who will sign the routine/important documents, if actual signer is not available or busy with the assignments of higher priority. The proxy signature helps in such situation and it is one of the important variants of digital signature. The fundamental proxy signature, enables an actual signer to pass on his signing power to some another entity, who is known as proxy signer. After this transfer of authority the delegated signer is capable of to signing in place of actual signer. This scheme attracts researchers community, since then different new constructions of proxy signatures and its variants, in combination with various special signatures [12-23], come into existence.

In practice there exists different variants or extensions of inital proxy signatures depending on how many actual signer and proxy signer involved: like proxy-multi, multi-proxy and multi-proxy multi-signatures. Suppose that, if two or more actual signers looking to pass on their signing authority to a specific signer, then how it is possible. To achieve this goal PMS schemes were firstly proposed by Yi, Bai and Xiao [24]. They presents two types of PMS schemes, first one is of MUO [11], type and second is of KPW [25], type. In a PMSS, for more than one actual signers, an authorized delegated signer can generate the valid signature. Sun [26], showed that schemes given by Yi et al. [24], are not secure against the

[1]Corresponding author

attack mounted by replacement of public key and also gives an improved version. Sun [26], scheme involves exponential operations, therefore computationally it is, little more complex. Afterwards several other proxy multi-signatures [27-32], are given by researchers. Most of them were unable to satisfy the desired security requirement. The PMSS is very useful in many practical situations, for an instance a public welfare project initiated by government, that may involve the finance ministry, public works department, municipal corporation, and local administration authorities, etc. The relevant documents must be signed jointly by all these contributors. A project in-charge can be appointed to supervise this project, so that the smooth functioning is possible. He will work as a proxy of all the concerning departments and sign all the related documents.

The natural question arises that, is it possible to generate PMS using merits of message recovery and verifiable SCPK ? Our paper incorporates these merits and propose a new PMSS. The organization of rest of the paper is as follows: a new PMSS is being proposed in next section; its security analysis is given in Section III and we concludes our proposed scheme in the last Section.

OUR SIGNATURE SCHEME

Our PMSS scheme has these phases: (A) System Initialization, (B) Registration of users, (C) Proxy Delegation, (D) PMS Generation and (E) PMS Verification and Message Recovery.

System Initialization

The system authority (SA), chooses p and q, prime values and holds $q \mid p-1$. The SA also selects a generator element g with order q, a one way hash function (OWHF) $h(\cdot)$. The pair (γ, β) of the private and public keys of SA, where $\gamma \in Z_q^*$, and $\beta = g^{\gamma} \bmod p$. Ultimately SA keeps γ secret and makes p, q, g and $h(\cdot)$ public.

Registration of Users

Each original signer U_i, $(i = 1,2,3,...t)$ selects their ID_i and an integer $a_i \in Z_q^*$ respecively. All U_i compute

$$v_i = g^{h(a_i \| ID_i)} \bmod p \qquad (1)$$

then each U_i, transmit (v_i, ID_i), to system authority. After this, SA selects $b_i \in Z_q^*$ and computes

$$y_i = v_i \cdot h(ID_i)^{-1} \bmod p \qquad (2)$$

$$w_i = b_i + \gamma \cdot h(y_i \| ID_i) \bmod q \qquad (3)$$

then transmit (y_i, w_i) to actual signer U_i, thereafter U_i calculate his secret key

$$x_i = w_i + h(a_i \| ID_i) \bmod q \qquad (4)$$

and checks the validity of public key y_i as

$$Y_i = g^{x_i} = \beta^{h(y_i \| ID_i)} \cdot h(ID_i) \cdot y_i \bmod p \qquad (5)$$

if this holds , then signer U_i, consider (x_i, y_i) as his secret and public key. This equation also authenticate y_i corresponding to x_i. Next each U_i chooses an integer value $c_i \in Z_q^*$ and calculate

$$d_i = g^{c_i} \bmod p \qquad (6)$$

and generates pair (e_i, δ_i) as

$$e_i = h(d_i) \bmod p \qquad (7)$$

$$\delta_i = c_i - x_i \cdot e_i \bmod p \qquad (8)$$

Finally the verifiable SCPK of the signer U_i is $(e_i, \delta_i, y_i, ID_i)$. Through the following verification equation these SCPK can be verified

$$e_i = h\left[\left(g^{\delta_i} \cdot Y_i\right)^{e_i}\right] \bmod p \qquad (9)$$

Proxy Delegation

Each U_i selects and calculates

$$r_i = g^{k_i} \bmod p \qquad (10)$$

and transmit to rest of the $(t-1)$ original signatory, then each U_i, compute

$$r = \prod_{i=1}^{t} r_i \bmod p \qquad (11)$$

$$s_i = x_i \cdot h(m_w \| r) + k_i \bmod q \qquad (12)$$

Now (m_w, r_i, s_i), is the partial signature of each U_i , send to U_P computes r same as calculated in equation (10) and verifies these values as

$$g^{s_i} = r_i \cdot Y_i^{h(m_w \| r)} \bmod p \qquad (13)$$

It is valid for all $i = 1,2,3..t$, then proxy signer calculates his proxy key as

$$X_P = \sum_{i=1}^{t} s_i + x_P \cdot h(m_w \| r) \bmod q \qquad (14)$$

and corresponding public key is $Y_P = g^{X_P} \bmod p$.

PMS Generation

To produce PMS, the delegated signer first choose $k \in Z_q^*$ and calculates

$$A = [m \| h(m)] \cdot g^{-k \cdot h(m)} \bmod p \qquad (15)$$

$$B = [m \| h(m)] \cdot g^{-k \cdot A} \bmod p \qquad (16)$$

$$S = k \cdot A - X_P \cdot h(B) \qquad (17)$$

Ultimately, the PMS for the message m, is (m_w, r, A, B, S).

PMS Verification and Message Recovery

As the verifier receives the signature for verification (m_w, r, A, B, S), he recovers the message m as

$$m \| h(m) = B \cdot g^{S} \cdot r^{h(B)} \cdot \left[\left\{ \prod_{i=1}^{t} Y_i \right\} \cdot Y_P \right]^{h(B) \cdot h(m_w \| r)} \qquad (18)$$

further the verifier checks whether

$$\left[A \cdot m^{-1}\right]^{A} = \left[B \cdot m^{-1}\right]^{h(m)} \qquad (19)$$

or not. The above two equations (18) and (19) are to be verified the signature is valid one. The message is recovered as follows

$$m \| h(m) = B \cdot g^{k \cdot A} \qquad \{By\ (16)\}$$

$$= B \cdot g^{S + X_P \cdot h(B)} \qquad \{By\ (17)\}$$

$$= B \cdot g^{S} \cdot g^{\left[\sum_{i=1}^{t} [s_i + X_P \cdot h(m_w \| r)]\right] h(B)} \qquad \{By\ (14)\}$$

$$= B \cdot g^{S} \cdot \left[\prod_{i=1}^{t} \{r_i \cdot Y_i\}^{h(m_w \| r)} \cdot Y_P^{h(m_w \| r)} \right]^{h(B)} \qquad \{By\ (5), (10)\}$$

$$= B \cdot g^{S} \cdot r^{h(B)} \cdot \left[\left\{ \prod_{i=1}^{t} Y_i \right\} \cdot Y_P \right]^{h(B) \cdot h(m_w \| r)}$$

In case verification fails, then check authenticity of the public key through equation (9).

SECURITY ANALYSIS

The security analysis of the proposed proxy multi-signature is in two parts (A) Attack Analysis and (B) Security Properties.

Attack Analysis

In this subsection we explain that how the proposed scheme is secure against forgery attack, public key substitution attack, and re-registration attack.

Forgery Attack

In the proxy signature generation phase, the equation (15), (16) and (17), similar to the Nyberg and Ruppel signature scheme [7]. So an adversary encounters the difficulty of solving DLP to forge a valid PMS, without knowing the secret key of the designated proxy signer.

Public Key Substitution Attack

Let a registered signatory mount a public key substitution attack by modifying his public key y_i to y'_i. He can choose randomly other parameters and message m' of his choice and then try to find y'_i, from the equation (18), but it is infeasible due to DLP.

Re-registration Attack

Suppose the adversary attempt to re-register one of the identity information, which is already registered by the original signer U_i or the proxy signer U_P. The adversary hope that SA will create another valid SCPK, which will help him to participate as the actual signer or the delegated signer. In this way the adversary masquerade as the genuine signer in the subsequent proxy signature without being identified. This attack can be restricted by keeping record of identity information registered and SA should check every time whenever he is going to generate new self-certified key for any member.

Security Property

Distinguishability

The message warrant m_w is included in proxy signature. On the other hand, Y_P, the proxy public key of the proxy signer, includes public key's of original signer as well as proxy signer. So in this way the delegated signature can be easily distinguish from the ordinary signature.

Prevention of Misuse

The message warrant m_w, includes information regarding identity of original as well as of proxy signer.

Message warrant m_w, also includes message type or message for which the actual signer delegates his authority to the proxy signer, validity period of delegation, etc. So, in way the misuse of proxy key duo can be prevented in our scheme.

Strong Unforgeability

Suppose original signers or an adversary is looking to counterfeit the signature. To sign the message X_P, none of them is able to find the proxy signers, proxy secret key X_P, from equation (14). Without the unknown secret X_P, it is not possible to forge the signature.

Strong Undeniability

In the process of signature verification and recovery of message the public key, identity of all original and proxy signers is used, so none of the signer deny his participation/agreement after having the signature.

Verifiablity

The verifier or recipient of proxy multi-signature, can be convinced that all the original signers were agreed to the message signed. It is due to the proxy public key involves the public keys of original signers. How the signature is verified and message is recovered is already shown.

CONCLUSION

We eliminate the problem of non-repudiation, by using verifiable SCPK. Our scheme has an advantage that of every signer's public key can simultaneously validated through proxy signature verification process. This will avoid the public key substitution attack, active attacks, and forgery attacks. At the same time of signature verification the message is also recovered this will reduce the load on the resources for computation and storage involved. It is shown in the security analysis that the proposed scheme satisfies all the basic security properties.

The proposed signature is secure cryptographically as shown in security analysis and applicable for large messages.

REFERENCES

R. L. Rivest, A. Shamir, and L. Adelman, “A method for obtaining digital signature and public key cryptosystem”, Communications of ACM, vol. 21, no. 2, pp. 120-126, 1978.

T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Transactions on Information Theory vol. 30, no. 4, pp. 469-472, 1985.

M. Girault , “Self-Certified Public Keys”, In Advances in Cryptology-Eurocrypt' 91; Springer; Berlin, Germany, pp. 491-497, 1991.

H. Petersen, P. Horster, ” Self-certified Keys Concepts and Applications”, In Proceedings of the 3rdConference on Communications and Multimedia Security, Chapman & Hall, 1997.

S. Kim, S. Oh, S. Park, and D. Won, “ Verifiable Self-certified Public Key”, In Proceedings of INRIA Workshop on Coding and Cryptography (WCC'99), pp. 139-148, 1999.

C. P. Schnorr, “ Efficient Signature Generation for Smart Cards”, Journal of Cryptology, vol. 4, no. 3, pp. 161-174, 1991.

K. Nyberg, A. R. Rueppel, “Message Recovery for Signature Schemes Based on The Discrete Logarithm Problem”, In Advances in Cryptology-Eurocrypt' 94, LNCS, vol. 950, pp. 175-190, 1994.

Y. F. Chang, C. C. Chang, and H. F. Huang, “Digital Signature with Message Recovery Using Self-certified Public Keys Without Trustworthy System Authority”, Applied Mathematics and Computation, vol. 161, no. 1**,** pp. 211-227, 2005.

Z. Shao, “Cryptanalysis and Improvement of Practical Convertible Authenticated Encryption Schemes Using Self-certified Public Keys”, Informatica, vol. 17, no. 4, pp. 577-586, 2006.

N. Tiwari, S. Padhye, “New Proxy Signature Scheme with Message Recovery using Verifiable Self-certified Public Keys”, In 2nd International Conference on Computer and Communication Technology (ICCCT) 2011, Allahabad, India, 15-17 September, pp. 539-544, 2011.

M. Mambo, K. Usuda, and E. Okamoto, “Proxy Signatures: Delegation of The Power to Sign Message”, IEICE Transactions on Fundamentals of Electronic Communications and Computer Science, E79-A(9), pp. 1338-1354, 1996.

A. Boldyreva, A. Palacio, and B. Warinschi, "Secure Proxy Signature Schemes for Delegation of Signing Rights", J. Cryptol., 25, 57-115, 2012.

F. Cao, and Z. F. Cao, "A Secure Identity-based Multi-proxy Signature Scheme", Computers and Electrical Engineering, vol. 35, no. 1, pp. 86-95, 2009.

C. Hsu, and T. Wu, "New Nonrepudiable Threshold Proxy Signature Scheme with Known Signers", Journal of Systems and Software", 2001, vol. 58, no. (2,1), pp. 119-124, 2001.

M. S. Hwang, C. C. Lee, and S. J. Hwang, "Cryptanalysis of The Hwang-Shi Proxy Signature Scheme", Fundamenta Informaticae, vol. 53, no. 2, pp. 131-134, 2002.

M. S. Hwang, C. C. Lee, S. F. Tzeng, "A New Proxy Signature Scheme for A Specified Group of Verifiers", Information Sciences, vol. 227, pp.102-115, 2013.

B. Lee, H. Kim, and K. Kim, "Strong Proxy Signature and Its Applications", In: SCIS, pp. 603-608, 2001.

C. C. Lee, T. Y. Chen, S. C. Lin, M. S. Hwang, "A New Proxy Electronic Voting Scheme Based on Proxy Signatures", Lecture Notes in Electrical Engineering, vol. 164, PP. 3-12, 2012.

C. C. Lee, T. C. Lin, S. F. Tzeng, M. S. Hwang, " Generalization of Proxy Signature Based on Factorization", International Journal of Innovative Computing, Information and Control, vol. 7, no. 3, pp. 1039-1054, 2011.

X. Li, K. Chen, and L. Sun, "Certificateless Signature and Proxy Signature Schemes from Bilinear Pairings", Lithuanian Mathematical Journal, vol. 45, no.1, pp. 76-83, 2005.

J. L. Lu, M. S. Hwang, C. J. Huang, "A New Proxy Signature Scheme with Revocation", Applied Mathematics and Computation, 2005, vol. 161, no. 3, pp. 799-806, 2005.

S. F. Tzeng, C. C. Lee, and M.S. Hwang, "A Batch Verification for Multiple Proxy Signature", Parallel Processing Letters, vol. 21, no. 1, pp. 77-84, 2011.

Y. Yu, Y. Sun, and B. Yang, "Multi-proxy Signature Without Random Oracles", Chinese Journal of Electronics, vol. 17, no. 3, pp. 475-480, 2008.

L. Yi, G. Bai, G. Xiao, "Proxy Multi-signature Scheme: A New Type of Proxy Signature Scheme", Electronics Letters, vol. 36, no. 6 , pp. 527-528, 2000.

Kim, S.; Park, S.; Won, D. Proxy Signature Revisited. ICICS'97, Int. Conf, Information and Communication Security, LNCS 1997, 1334, 223-232.

H. M. Sun, "On Proxy Multisignature Schemes", In: Proceedings of the International Computer Symposium, pp. 65-72, 2000.

J. Ji, D. Li, and M. Wang, "New Proxy Multi-signature, Multi-proxy Signature and Multi-proxy Multi-signature Schemes from Bilinear Pairings", Chinese Journal of Computers, vol. 27, no. 10, pp. 1429-1435, 2004.

J. Ji, and D. Li, "A New Proxy Multi-signature Scheme", Journal of Computer Research and Development, vol. 41, no. 4, pp. 715-719, 2004.

C. Hsu, T. Wu, and W. He, "New Proxy Multi-signature Scheme. Applied Mathematics and Computation, vol. 162, pp. 1201-1206, 2005.

F. Cao, Z. Cao, "Security Model of Proxy-multi Signature Schemes", LNCS 2006, 4301, pp. 144-152, 2006.

R. Lu, Z. Cao, and J. Shao, "On Security of Two Nonrepudiable Threshold Multi-proxy Multi-signature Schemes with Shared Verification", International Journal of Network Security, vol. 4, no. 3, pp. 248-253, 2007.

Wang, F.; Chang, C. C.; Lin, C.; Chang, S. C., "Secure and Efficient Identity-based Proxy Multi-signature Using Cubic Residues", International Journal of Network Security, vol. 18, no. 1, pp. 90-98, 2016.