International Journal of Digital Information and Wireless Communications (IJDIWC) 2(4): 296-305
The Society of Digital Information and Wireless Communications, 2012 (ISSN: 2225X-658X)

A PRACTICAL PROXY SIGNATURE SCHEME

Sattar J Aboud and Sufian Yousef
Telecommunications Engineering Research Group
Anglia Ruskin University, UK
sattar_aboud@yahoo.com

ABSTRACT

A proxy signature scheme is a variation of the ordinary digital signature scheme which enables a proxy signer to generate signatures on behalf of an original signer. In this paper, we present two efficient types of proxy signature scheme. The first one is the proxy signature for warrant partial delegation combines an advantage of two well known warrant partial delegation schemes. This proposed proxy signature scheme is based on the difficulty of solving the discrete logarithm problem. The second proposed scheme is based on threshold delegation the proxy signer power to sign the message is share. We claim that the proposed proxy signature schemes meet the security requirements and more practical than the existing proxy signature schemes.

KEYWORDS

Proxy signature scheme, warrant partial delegation, proxy unprotected scheme, proxy protected scheme, threshold delegation.

1 INTRODUCTION

The idea of a proxy signature scheme was first presented by Mambo et al. [1] in 1996. Their proxy signature scheme allows an original signer to delegate his signing right to a proxy signer to sign the message on behalf of an original signer. Later, the verifier, which knows the public keys of original signer and a proxy signer can check a validity of a proxy signature issued by a proxy signer.

Till now we have the following types of delegations. In general, there are three different types of delegations: full delegation, partial delegation and delegation by warrant. In a full delegation proxy signature scheme, a proxy signer uses the same private key as an original signer and creates the proxy signature as an original signer does. The drawback of a full delegation comes from a difficulty of distinctive between an original signer and a proxy signer. In a partial delegation proxy signature scheme, the original signer derives the proxy key from his private key and passes it to the proxy signer in a secure channel. In the proxy signature scheme with delegation by warrant, an original signer provides the proxy signer a special message namely warrant. The warrant certifies that a proxy signer is legal and contains signer identity, delegation period and the types of a message on which proxy signer can sign.

Also, there are two types in the second one: protected and unprotected proxy signature schemes. In unprotected proxy signature scheme, a proxy signature is generated by both the proxy signer and an original signer. In this case, the verifier cannot distinguish the identity of a signer. In the protected proxy signature scheme, a proxy signature is generated by the proxy signature key of an original signer and also with a private key of a proxy signer.

Later, a verifier validates a proxy signature with the public keys of both an original signer and a proxy signer. Proxy signature scheme is useful in many uses such as e-payment systems and wireless networks [2, 3, 4, 5]. In this paper, we introduce an efficient type of delegation that is warrant partial delegation.

In delegation by warrant, the original signer signs a warrant which describes the relative rights and information of the original signer and proxy signer such that a signature verifier can use the warrant as a part of verification information. Usually, delegation by warrant incurs more computational cost than the other two. In this paper we propose efficient and solid proxy signature schemes

- One is a proxy unprotected type and the other is a proxy protected type.
- The proposed schemes are appropriate to schemes using a discrete logarithm assumption. Also, because the proposed proxy protected scheme needs a linear combination of two shared secrets, so it can be develop to a threshold proxy signature schemes without difficulty..

2 PRELIMINARIE

In this section we present some of the preliminaries required for proxy based signatures and threshold.

2.1 Security Requirements

A secure proxy signature scheme must satisfy the following requirements:

1. Identifiability: Any person can determine an identity of a corresponding proxy signer from a proxy signature.
2. unforgeability: Only the designated proxy signer can create the valid proxy signature on behalf of an original signer.
3. undeniability: Once the proxy signer generates the valid proxy signature on behalf of the original signer, cannot deny a signature creation against anyone else.
4. Verifiability: From a proxy signature, the verifier is convinced of an original signer agreement on the signed message.
5. Proxy signer deviation: The proxy signer cannot generate the valid signature not detected as the proxy signature.

2.2 Notations Used

Throughout this paper, we will use the following notations.

A : original signer entity A.

B : proxy signer entity B.

V : verifier entity V.

p : large prime number.

g : generator Z_p^*.

$h(.)$: secure one-way hush function.

Id_A : identity of original signer

Id_B : identity of proxy signer

m_w : a warrant.

$WI(b)$: represents a computing cost to achieve $b-bit$ modular inversion.

$WH(b)$: denotes a computing cost to find hash function with b–bit long input

2.3 Definitions Used

This paper presents two new types of delegation, called delegation with warrant and threshold delegation.

Definition 1. (Partial delegation with warrant). In partial delegation with warrant, the new secret b is calculated from the secret s of entity A and the warrant and b is provided to entity B in a

secure manner. From security point view s must not be calculated from b and the warrant. Partial delegation with warrant also combines a benefit of a partial delegation and the delegation by warrant. Thus this delegation has rapid processing and is suitable for limiting messages to be signed. Also, since a proxy for partial delegation with warrant can identify its valid time, the proposed scheme is not required an extra proxy revocation protocol.

Now in a group-oriented association it is preferred that a proxy signer strength to sign documents is shared. The entity A, for example, has teach the secretary entity B to reply instead of her accordingly. However, assume a secretary entity B is not follow given information provided by entity A. It means that an entity B is not sign the message which requires to be answered rapidly or he sign what entity A has teach to hold back. Therefore, for security reasons, it may be an organization rules that messages be signed by i proxy signers rather than one entity.

Definition 2. (threshold delegation)
In threshold delegation, n proxy signers are provided shares for example $t \le n$ are required to create the proxy signature rather than the original signer but less than t. This is entitled (t,n) threshold delegation that is in a (t,n) threshold proxy signature scheme.

- t out of n proxy signers should help to issue a proxy signature
- any $t-1$ corrupt proxy signers cannot forge a signature.

3. RELATED WORK

Mambo et al. in 1996 [1] developed a systematic approach to proxy or delegated signatures. Neuman in 1993 [6] introduced the scheme for delegation by warrant, which was further extended by Kim et al. in 1997 [7] to partial delegation by warrant. Okamoto et al. in1999 [8] proposes a proxy-unprotected signature scheme. They analyze the security of their scheme by using the reduction among functions. Yi et al, in 2000 [9], proposed proxy multi-signature scheme which allows a group of original signers to delegate its signing power to a single proxy signer.

Hwang et al, in 2001 [10], introduced a new proxy multi-signature scheme. In 2001, Lee et al. [11] proposed a proxy-protected signature scheme. Unfortunately, its security proof is incorrect by Wang 2004 [5]. In 2002, Lin et al. [12] present a multi proxy signature scheme for partial delegation with cheater identification, they claim that their scheme required less computational overhead compare with other schemes.

Zhou et al. in 2005 [13] propose two efficient proxy protected signature schemes. They claim that their schemes are more efficient than other schemes. Unfortunately, their schemes insecure. In 2006, Qin Wang and Zhenfu Cao [14] present an attack on the aggregate-signature based proxy signature scheme, they give arguments for partial delegation with warrant proxy signature schemes. They construct a new proxy signature scheme and prove that it is secure against existentially forgery on adaptively chosen-message attacks and adaptively chosen-warrant attacks under the random oracle model.

Moreover, Liu et al. in 2007 [15] point out that Zhou et al. schemes vulnerable to the un-delegated proxy signature attack In 2005 Sunder Lal and Amit Awasthi [16] introduce a new multi-proxy signature scheme for partial

delegation with warrant, which requires less computational overhead in comparison to Lin et al, and also fulfill the requirement of partial delegation with warrant simultaneously.

In 2008, Sunitha and Amberker [17] proposed a proxy signature schemes for controlled delegation. They find that the scheme can be used to control delegation of financial power to a proxy signer. They use the digital signature algorithm in their scheme. Shao in 2009 [18] propose proxy-protected signature scheme.

In 2010,, Liu and Huang [19] proposed a variant of threshold proxy signature scheme in which all proxy signers remain anonymous. The authors claimed their construction satisfies unforgeability, proxy signer deviation, identifability, undeniability and variability. However, this scheme does not provide the proxy signer deviation and identifability requirements. In 2011, Constantin Popescu [20] introduced a secure proxy signature scheme with delegation by warrant, the scheme is based on the difficulty of solving the discrete logarithm problem.

The rest of this paper is organized as follows. After we described the related work in section 3. we will describe in section 4 the Mambo et al. scheme for partial delegation. In section 5 the proposed proxy signature scheme is described.

However, in subsections 5.1 and 5.2 we will explain and suggest an efficient and solid proxy signature schemes for warrant partial delegation. The first one is the proxy unprotected scheme and the second one is proxy protected scheme. In subsections 3.3 and 5.4 we discuss the performance analysis and security analysis of the proposed scheme which is extensively appropriate to scheme under a discrete logarithm assumption. Lastly, this paper is concluded in section 6.

4 MAMBO et al. SCHEME

It is supposed that the original signer entity A invites the proxy signer entity B to perform signing on behalf of him, and the verifier entity V verifies the validity of generated signatures. Also, suppose that p is a large prime number and g is a generator for Z_p^*. Select a random integer value e as a public key where $e = g^u \bmod p$, and $u \in Z_{p-1}$.

4.1 Description of the Scheme

The steps of the scheme are as follows:

Generation: The original singer entity A should do the following:

1. select an integer $i \in Z_{p-1}$
2. compute $t_1 = g^i \bmod p$
3. find $b = u_A + i * t_1 \bmod p - 1$
4. pass (b, t_1) to a proxy signer entity B in a secure channel.

Signing: Entity B should do the following:

1. verifies $g^b \equiv e_A * t_1^i \bmod p$.
2. signs the message m_p on behalf of entity A
3. employs b as a substitute to u_A
4. implements an ordinary signing process.
5. the generated proxy signature on m_p is $(m_p, s_b, (m_p)t_1)$

Verification: Entity V should do the following:

1. find $e^- = e_A * t_1^i \bmod p$ as the new public key

2. a verification of proxy signature is implemented by the same verifying process as in an original signature scheme.

5 PROPOSED PROXY SIGNATURE SCHEMES

we will explain and suggest an efficient and solid two proxy signature schemes for warrant partial delegation. The first one with two types the first type is the proxy unprotected scheme and the second type is proxy protected scheme. The second scheme is also with two types. The first type is a proxy sharing unprotected and the second type is a proxy protected sharing.

5.1 Proposed Schemes Using Discrete Logarithm Assumption

There are two types which are as follows

5.1.1 Proxy Unprotected Scheme

The steps of the first type are as follows:
Generation: The original signer entity A should do the following:

1. selects an arbitrary integer value $i \in Z_{p-1}$
2. finds $t_1 = g^i \bmod p$.
3. concatenates $(m_w \| t_1)$
4. computes $j = h(m_w, t_1)$ such that an information on a delegation must be described in the warrant m_w for example its valid period.
5. finds $b = j * u_A + i \bmod p-1$.
6. passes (m_w, b, t_1) to the proxy signer in the secure channel.

Signing: entity B must do the following:

1. checks $j = h(m_w, t_1)$
2. verifies $g^b \equiv e_A^j * t_1 \bmod p$ (1)
3. for signing message m_p uses b instead of u_A and implements an ordinary signing process. Thus the proxy signature on m_p is $(m_p, s_b(m_p), t_1, m_w)$ such that $s_b(m_p)$ indicates the signing message m_p by secret key b.

Verification: A verification of a proxy signature is performed by the same checking process as in an original signature scheme except for an additional calculation:

1. compute $j = h(m_w, t_1)$
2. compute $e' = e_A^j * t_1 \bmod p$.
3. A computed component e' handled as a new public key clearly showing the participation of entity A.
4. A scheme has the following type similar to the congruence (1)
5. $g^b = e^{h(t)} * t_1 \bmod p$ (2)

5.1. 2 Proxy Protected Scheme

The steps of the second type are as follows:
1. **Generation** and **modification**: After checking a validity of (m_w, b, t_1) where m_w must be created from an original signer Id_A, proxy signature Id_B and other data on the delegation, a proxy signer entity B computes a substitute proxy (b_p, t_1):

$$b_p = b + u_B * h(m_w, t_1) \bmod p-1 \quad (3)$$

2. **Signing**: To signing the message m_p, entity B uses b_p as a substitute to u_A and performs an ordinary signing process. Thus, a proxy signature on m_p is $(m_p, s_{b_p}(m_p) t_1, m_w)$.

3. **Verification**: A verifier entity V performs the same verifying process as in an original signature scheme except for an additional calculation:

$$j = h(m_w, t_1)$$

$$e_p^{'} = (e_A * e_B)^j * t_1 \bmod p$$

The calculated key $e_p^{'}$ is processed as the new public key clearly showing an participation of entity A.

5.2 Proposed Scheme Using Threshold Proxy Signature

Assume that the original signer entity A needs to delegate the group to sign a document in such a way that a proxy signature can be generated by the set of t proxy singers from the designated group G of n proxy signers but a subset with $t-1$ proxy signers cannot.

Here, we illustrate the efficient (t,n) threshold proxy signature scheme by using a scheme that we proposed in section 5.1 and Ceredo Schnorr type threshold digital signature scheme [21]. For expediency, we suppose that $G = (P_i \mid 1 \le i \le n)$. The public parameters are the same as those of section 4 except that $p-1$ has large prime factor q and selects $g \in z_p$ with the order of q.

5.2.1 Generation Random Number

Assume that the dealer with an arbitrary secret D selects the random polynomial where $f(x) = D + a_1 x + ... + a_{t-1} x^{t-1}$ passes $u_i = f(i)$ to P_i privately for $i = 1,...,n$ and transmits $d = g^D \bmod p$ and $g^{a_1},...,g^{a_{t-1}} \bmod p$ This process is generated by the following protocol:

1. Every proxy signer P_i selects $y_i \in Z_q$ arbitrarily and transmits $d_i = g^{y_i} \bmod p$ to each proxy signers.
2. To deliver y_i every P_i arbitrarily chooses a polynomial f_i of degree $t-1$ in Z_q where $f_i(0) = y_i$ that is: $f_i(x = y_i + a_{i,1}x + a_{i,2}x^2 ... + a_{i,t-1}x^{t-1}$ with $a_{i,1},...,a_{i,t-1} \in Z_q$ and passes $f_i(j) \bmod q$ to P_j in a secure way $(\forall j \ne i)$. P_i also transmits a value $g^{a_{i,1}},...,g^{a_{i,t-1}} \bmod p$.
3. From delivered $f_j(i)(\forall j \ne i), P_i$ verifies if for every $j(j \ne i),$ by

$$g^{f_j(i)} \equiv d_j \bullet (g^{a_{j,1}})^{i^l} ... (g^{a_{j,t-1}})^{i^{t-1}} \bmod p$$

4. Assume $L \equiv (P_j \mid P_j)$ is not noticed to be dishonest in step 3. Every P_i finds share $u = \sum_{j \in L} f_j(i)$ privately and finds

$$d = \prod_{j \in L} d_j, g^{a_1} = \prod_{j \in L} g^{a_{j,1}}, ..., g^{a_{t-1}} = \prod_{j \in L} g^{a_{j,t-1}}$$

5.2.2 Proxy Unprotected Sharing

This scheme contains four phases which are as follows:

1. Proxy Generation

The original signer entity A should do the following:

1. selects arbitrarily $i \in Z_q$.
2. obtains $t_1 = g^i \bmod p$.
3. finds $(m_w \| t_1)$,
4. computes $j = h(m_w, t_1)$.
5. calculates $b = j \bullet u_A + i \bmod q$.

2. Proxy Sharing

To share the proxy b in the threshold scheme with threshold t entity A should do the following:

1. chooses integer $b_j \in Zq, j = 1,...,t-1$

2. issues the result $B_j = g^{b_j}, j = 1,...,t-1$.
3. finds a proxy share b_i as follows:
   - $f^{'}(x) = b + b_1 x + b_2 x^2 + ...b_{t-1} x^{t-1}$
   - $b_i = f^{-}(i)$

3. Proxy Share Distribution

The original signer entity A should do the following:

1. passes to every proxy signer p_i(for $i = 1,...,n$) a proxy share b_i in a secure way
2. transmits (m_w, t_1)

4. Proxy Share Verification

To check the proxy share b_i a proxy signer p_i should do the following:

1. compute $j = h(m_w, t_1)$
2. check if $g^{b_i} \equiv (e_A^j t_1) \bullet \prod_{j=1}^{t-1} B_j^{i^j} \bmod p$

5.2.3 Proxy Signature Broadcasting without Exposing Shares

Assume that m_p is the document and $L \subseteq G$ publish the proxy signature. For expediency, suppose $L = (P_i \mid 1 \le i \le t)$. Thus, the rest of the steps of the protocol are as follows:

1. L implements the protocol for generation random number and obtain the public key $d = (g^y \bmod p), g^{a_1}, ..., g^{a_{t-1}} \bmod p$ and the private key of P_i, u_i such that $u_i = f(i) = y + a_1 i + ... + a_{-1} i^{t-1}$
2. Every proxy signer P_i do the following:
   1. finds $j = h(d, m_p)$
   2. computes $d_i = u_i + b_i \bullet j \bmod q$
   3. discloses d_i
3. Each proxy signer P_i checks the following:
   - $g^{d_l} = (d \prod_{j=1}^{t-1} (g^{a_j})^{l^j} \bullet$
     $((e_A^j t_1) \prod_{j=1}^{t-1} (g^{b_j})^{l^j})^{h(d, m_p)} \bmod p$ for $\forall l$.
4. Every $P_i \in L$ finds t satisfying:
   $t = y + b \bullet j = f(0) + f^{-}(0) j \bmod q$
   by using Langrage equation to d_i. A proxy signature is (m_p, t, j, t_1, m_w)
5. The validity of a signature (m_p, t, j, t_1, m_w) is checked by:
   - $d^{-} = g^t (e_A^{h(m_w, t_1)} t_1)^{-j} \bmod p$
   - $j \equiv h(d^{-}, m_p)$

In addition, by replacing an above proxy sharing with the following proxy protected sharing, we can clearly extend an unprotected threshold proxy signature scheme into a proxy protected threshold signature scheme.

5.2.4 Proxy Protected Sharing

There are five phases in this scheme which are as follows:

1. Group Key Generation

The G implement protocol for generating random number and get a public key of a group G

$e_G (= g^{u_G} \bmod p), g^{c_1, ..., g^{c_{t-1}}} \bmod p$

and private key of P_i, u_G, i (such that $u_G, i = f^{=}(i) = u_G + c_1 i + ... + c_{t-1} i^{t-1}$.

2. Proxy Generation

Entity A should do the following:

1. selects $i \in Z_q$.
2. finds $t_1 = g^i \bmod p$.
3. concatenates $(m_w \| t_1)$.
4. finds $j = h(m_w, t_1)$ where m_w contains original singer id ,proxy signer id.
5. finds $b = j \bullet u_A + i \bmod q$.

3. Proxy Sharing

To share the proxy b in the threshold scheme with threshold t entity A should do the following:

1. selects integer $b_j \in Z_q, j = 1,...,t-1$
2. issues a value $B_j = g^{b_j}, j = 1,...,t-1$.
3. finds a proxy share b_i such that:
$b_i = f^{-}(i) = b + b_1 i + ... + b_{t-1} i^{t-1}$

4. Proxy share delivery

An entity A should do the following:

1. passes to every P_i the proxy signature b_i in the secure way.
2. transmits (m_w, t_1).

5. Verification of the Proxy

The verification of (m_w, b_i, t_1) are as follows:

- The P_i computes another proxy $(b_{p,i}, t_1)$ as follows:
$b_{p,i} = b_i + u_{G,i} \bullet h(m_w, t_1) \bmod q$
- utilizes $b_{p,i}$ as an option to b_i

5.3 Performance Analysis

When we select the digital signature standard scheme [22] in generating the proxy signature and on checking, a computing time is lesser in a proxy signature for warrant partial delegation than that by the warrant.

Thus, a warrant delegation needs $2956 + 2WI(512)$ computing time, whereas a proposed warrant partial delegation want $2158 + WI(9512) + 2WH(|m_w|)$ $(2160 + WI(512) + 2WH(|m_w|)$ computing time with and without addition the value for the proxy unprotected signature scheme and that for the proxy protected signature scheme respectively. Numbers indicate a computing cost to achieve modular multiplication in 512 bits modulus, $WI(b)$ represents a computing cost to achieve $b-bit$ modular inversion, and $WH(b)$ denotes a computing cost to calculate the hash function with $b-bit$ long input.

When we compare the partial delegation with the proposed warrant partial delegation. The proposed scheme requires $641 + WH(|m_w|)(642 + WH(m_w|))$ of computing time in the proxy generation step, $642 + WI(512)(642 + WI(512))$ in signature generation $875 + WH(|m_w|)(876 + WH(m|m_w|))$ in a signature verification step.

But, partial delegation needs $641(642)$ of computing time in a proxy generation step, $642 + WI(512)(642 + WI(512))$ in a signature generation step, $875(906)$ in a signature verification step, and an extra 1282 of commuting time for proxy revocation algorithm.

Observe that as in [1], the subsequent congruence can be employed as a substitute to a congruence (3) $b_p = b + u_B * e_B \bmod p - 1$ and this requires $(906 + WH(|m_w|))$ of computing time in a signature verification step.

However, from a point of computational benefit, a warrant partial delegation decrease an amount of computing time compare with a delegation by warrant, and from the point of business, the proposed scheme needs no additional proxy revocation algorithm in a partial delegation, the proxy signature scheme [23] is calculated in the same manner.

5.4 Security Analysis

In this paper, we will discuss the following attacks:

Framing attack: In such attack, a hacker forges the proxy secret key and then creates valid proxy signatures such

that a verifier considers that these proxy signatures were signed by a proxy signer entity B on behalf of an original signer entity A. If the proxy signature is presented, entity A cannot repudiate that since is an original signer of a proxy signer entity B. The result is that entity A and entity B will be framed. To achieve this attack, hacker wants to forge entity B proxy key pair (x_p, d_p). As forward-secure signatures are used by proxy signer it is computationally hard to forge a proxy private key. Knowing a proxy public key d_p hacker cannot create a proxy private key given as it is hard to factorize. Thus the proposed scheme resists the above attacks. By this we can state that just a designated proxy signer can generate the valid proxy signature on behalf of an original signer. Thus a requirement of unforgeability, of the secure proxy signature is satisfied.

Forgery by original signer: The proxy private key is dependent on both a proxy information sent by an original signer and a private key of a proxy signer. So, an original signer cannot make a proxy private key. Also, cannot obtain a proxy private key from a proxy public key as it is hard to factorize. Thus an original signer is unable to sign like a proxy signer. So, forgery by an original signer is computationally impossible.

Impersonating attack: Suppose that entity B is not designated as the proxy signer by an original signer entity A. While entity B can create the proxy key pair (x_p, d_p) and sign the message on behalf of entity A, a verifier after receiving signatures, first validates using the verification formula if a signature is from the valid proxy signer or from the revoked proxy signer. During this test a verification fails and a verifier considers him as the revoked signer. Thus entity B cannot become a proxy signer unless he is designated by an original signer entity A.

6 CONCLUSION

We suggested two new kind of proxy signature. The first one is a warrant partial delegation, for which has the computational gain compared with an original proxy signature by warrant and has also the construction benefit over a proxy signature for partial delegation. The second one is the proxy for threshold delegation In the upcoming highly group oriented society, it is desired to delegate the power to sign messages to a group of n proxy signer. We illustrated the requirements related to a proposed thoughts and demonstrated that the proxy signature scheme for warrant partial delegation and a (t, n) threshold proxy signature scheme without exposing proxy shares.

Furthermore, a proposed scheme could be extended to a elliptic curve proxy signature scheme easily.

7 REFERENCES

1. Mambo M., Usuda K., and Okamoto E.: Proxy Signatures: Delegation of the power to sign Foundational, Volume E79-A, Number 9, PP. 1338-1354 (1996).
2. Chaum D., Fiat A., Naor M.: Untraceable Electronic Cash, Proceeding of the Crypto'88, pp. 319-327 (1990).
3. Oros H., Popescu C.: A Secure and Efficient Off-line Electronic Payment System for Wireless Networks, International Journal of

Computers, Communications and Control, volume 5(4), pp. 551-557 (2010).
4. Popescu C.: A Secure and Efficient Off-line Electronic Transaction Protocol, Studies in Informatics and Control, volume 19(1), pp. 27-34 (2010).
5. Wang G.: Designated-verifier Proxy Signatures for e-Commerce, Proceeding of IEEE 2004 International Conference on Multimedia and Expo (ICME 2004), pp. 1731-1734 (2004).
6. Neuman B C.: Proxy-based authorization and accounting for distributed systems, Proc. 13th International conference on Distributed Computing systems, pp 283 – 291 (1993).
7. Kim S, Park S, Won D.: Proxy Signatures, Revisited, ICICS'97, LNCS – 1334, Springer –verlag, pp 223 – 232 (1997).
8. Okamoto T., Tada M., Okamoto E." Extended Proxy Signatures for Smart Cards, Proceeding. of Information Security Workshop (ISW'99), LNCS 1729, Springer-verlag, pp. 247-58 (1999).
9. Yi L, Bai G, and Xiao G.: A new type of proxy signature scheme, Electron Letter, 36(6), 527–8 (2000).
10. Hwang S., Chen C.: A new proxy multi-signature scheme, International workshop on cryptology and network security, Tamkang University Taipei, Taiwan, pp 26–28 (2001).
11. Lee, B., Kim H., Kim K..: Secure Mobile Agent using Strong Non-designated Proxy Signature, Proceeding of the Australasian Conference on Information Security and Privacy, LNCS 2119, pp. 474-486 (2001).
12. Lin C., Wu T., Hwang J.: Multi proxy signature scheme for partial delegation with cheater identification, Institute of Information Management, NCTU (2002).
13. Zhou Y, Cao Z, and Lu R.: Provably secure proxy-protected signature schemes based on factoring, Application Math Computer164(1), pp. 83–98 (2005).
14. Wang Q., CAO Z.: An Identity-based Strong Designated Verifier Proxy Signature Scheme, Wuhan University Journal of Natural Sciences, vol. 11(6), pp. 1633-1635 (2006).
15. Liu, Y., Wen H., and Lin C.: Proxy-Protected Signature Secure Against the Un-delegated Proxy Signature Attack, Computers and Electrical Engineering, Volume 33(3), pp. 177-185 (2007).
16. Sunder Lal, Awasthi A.: A scheme for obtaining a warrant message from the digital proxy signatures, Cryptology e-print Archive Report 2005/073, (2005).
17. Sunitha and Amberker: Proxy Signature Schemes for Controlled Delegation, Journal of Information Assurance and Security, 159-174 (2008).
18. Shao Z.: Provably secure proxy-protected signature schemes based on RSA, Computer Electronic Engineering, 35, pp. 497-505 (2009).
19. Liu and S. Huang: Identity-Based Threshold Proxy Signature from Bilinear Pairings, Informatica, Inst. Math & Science, Volume. 21, Number. 1, pp. 41-56, IOS press (2010).
20. Constantin Popescu: A Secure Proxy Signature Scheme with Delegation by Warrant, SIC: Volume 20, issue 4, pp. 373-380 (2011).
21. Cerecedo M, Matsumoto T, and Imai H.: Efficient and Secure Multiparty Generation of Digital Signatures based on Discrete Logarithms, IEICE Transactions Fundamental, Volume E76-A, Number A, pp. 532-545 (1993).
22. Lu R, Dong X, & Cao Z.: Designing efficient proxy signature schemes for mobile communication, In Science in China, F, 51(2), pp. 183–95 (2008).
23. B. Umaprasada Rao and P. Vasudeva Reddy: ID-Based Directed Multi-Proxy Signature Scheme from Bilinear Pairings, International Journal of Computer Science and Security (IJCSS), Volume 5, Issue 1, pp. 107-117 (2011.