ISSN 1392–124X (print), ISSN 2335–884X (online) INFORMATION TECHNOLOGY AND CONTROL, 2014, T. 43, Nr. 2

Provably Secure Proxy Multi-Signature Scheme Based On ECC

Namita Tiwari

Department of Mathematics, Motilal Nehru National Institute of Technology
Allahabad-211004, India
e-mail: namita.mnnit@gmail.com

Sahadeo Padhye

Department of Mathematics, Motilal Nehru National Institute of Technology
Allahabad-211004, India
e-mail: sahadeomathrsu@gmail.com

Debiao He

School of Mathematics and Statistics
Wuhan University, Hubei Province, 430072, P.R.China
e-mail: hedebiao@163.com

crossref http://dx.doi.org/10.5755/j01.itc.43.2.5377

Abstract. The elliptic curve cryptosystem (ECC) achieves the security level equivalent to that of digital signature algorithm (DSA), but has a lower computational cost and a smaller key size than the DSA. Till now so many proxy multi-signature schemes based on ECC without pairings have been proposed. To the best of our knowledge, none of them are provable secure. Having motivated, we first define a formal security model and then propose a provable secure proxy multi-signature scheme based on ECC without pairings. Our proposed scheme can play a crucial role in application to distributed systems, grid computing, mobile agent environment etc.

Keywords: Digital signature; Proxy multi-signature; Elliptic curve discrete-log problem; Bilinear pairings.

1. Introduction

Proxy signature (introduced by Mambo et al. [26] in 1996) allows an entity called original signer, to delegate its signing capability to another entity, called proxy signer. Since it is proposed, the proxy signature schemes have been suggested for use in many applications, particularly in distributed computing, where delegation of rights is quite common. According to the number of users in the original and proxy groups, the proxy signature primitives can be categorized in multi-proxy signature, proxy multi-signature and multi-proxy multi-signature schemes [39]. If a company releases a document that may involve the financial department, engineering department, and program office, etc. The document must be signed jointly by these entities, or signed by an authorized proxy signer. One solution to this problem is to use a proxy multi-signature (PMS) scheme in which a proxy signer can generate the signature for the document on behalf of several original signers. Reader may refer to [10, 21, 35] for the details about the proxy signature.

Related work: Yi et al. [40] firstly proposed two PMS schemes in 2000. Sun [30] analyzed that the schemes [40] do not resist the public key substitution attack. Consequently, Sun presented improved PMS schemes that can resist such forgery. Sun's improvement increases security but requires very complex operations (to derive the proxy public key) due to the presence of exponential operations. Equations of such complex operations could be modified at the same level of security because of the concept of elliptic curve introduced by Koblitz [18, 19] and Miller [25]. The ECC can achieve a security level equal to that of RSA and DSA but has a lower computational cost and smaller key size. Therefore, to improve the efficiency of Sun's schemes, Chen et al.

[4, 5] proposed the first PMS scheme based on ECC. Park et el. [27] pointed out that the scheme [4] is insecure and the scheme [5] can't resist the conspiracy attack from all original signers but they neither provided an improved version nor a new version. At the same time, Ji and Li [17] proposed a PMS scheme based on ECDLP. However, Cao et al. [7] presented an attack on the scheme [17] by original signer's forgery, and modified the scheme [17] by improving the key generation process. Yin et al. [41] pointed out that the scheme [7] still does not possess the properties of distinguishabil-ity, strong undeniability and presence of proxy misuse. Further they proposed a new PMS scheme with proxy revocation [23, 24] based on ECDLP. Accordingly, their scheme can resolve the proxy revocation and prevent proxy misuse due to use of a signature center. Recently, to resist the forgery attack on the scheme [4] and conspiracy attack on [5], two modified schemes have been proposed by Xue et al. [38].

In this journey, so many PMS schemes [2, 13, 20, 28, 37] have been proposed by using the elliptic curve bilinear pairings also. All of these schemes from pairings except [20] are proven secure in the random oracle model (ROM). Two more PMS schemes [22, 33] also exist in the literature having security proof in the standard model [36]. However, in 2010 Sun et al [33] demonstrated that the scheme [22] is insecure to some attacks. Consequently, they proposed a new scheme having security in standard model to defeat these weaknesses. Since the pairing over elliptic curve is regarded as one of the very expensive cryptography primitives. Such use of pairings make the scheme [33] less applicable in practical applications, even secure in standard model. So, the schemes without pairing and based on ECC are more applicable from the efficiency point of view. Recently, some proxy signature schemes without pairings have been proposed [16, 31, 32, 34]. One can also use the batch verification algorithm [14] and specified group of verifier [15]to reduce the proxy signature verification time to make the scheme more efficient. In this article we propose a new PMS scheme based on elliptic curve discrete log problem(ECDLP) without pairing which is provable secure in ROM. It is still an open problem to propose a new PMS scheme based on ECDLP without pairings, secure in standard model.

Our contribution: So many developments of proxy multi-signature scheme without pairings based on ECC have been proposed, as discussed above. They do not have well defined formal security model and proofs. To the best of our knowledge, none of them are proven to be secure even in ROM. ROM [1] is an effective method to measure the practical security of cryptography. In practice, random oracles are used to model cryptographic hash functions in schemes where strong randomness assumptions are required for the hash function's output. Such a proof generally shows that a system or a protocol is secure by showing that an attacker solves mathematical problem believed to be hard, in order to break the protocol. Major application of random oracles is shown in the work of Fiat and Shamir [11]. In this paper, we first define a security model and then propose a PMS scheme based on ECDLP. Our scheme is provable secure against adaptive chosen message attack in the ROM. The relative computation cost of a pairing is approximately more than ten times higher than the scalar multiplication over elliptic curve group [6] as discussed in the literature [8, 16] etc. In this sense, our proposed scheme is more efficient than the existing schemes [2, 13, 20, 28, 37] based on ECC from bilinear pairings.

Organization: The rest of this paper is organized as follows: In Section 2, we introduce the complexity assumption. In Section 3, we give a definition of proxy multi-signature scheme and then define a security model for it. In Section 4, we propose a new proxy multi-signature scheme. We prove its security in Section 5. Section 6 presents a comparative analysis with the existing schemes. Finally, Section 7 concludes the paper.

2. Preliminaries

2.1. Background of elliptic curve group

Let $E = F_q$ denotes an elliptic curve E over a prime finite field F_q defined by an equation $y^2 = (x^3 + ax + b) \bmod q, a, b \in F_q$, together with an extra point $\{\infty\}$ (called the point at infinity). If the discriminant $\Delta = (4a^3 + 27b^2) \bmod q \neq 0$, equivalently, the polynomial $x^3 + ax + b$ has distinct factors, then E/F_q is nonsingular, i.e it does not have any cusp or node singularity. We can define a binary operation (the point addition A"+") on the points of E/F_q using chord and tangent rule. The elliptic curve with this binary operation "+" forms an additive abelian group $(E/F_q, "+") = \{(x, y): x, y \in F_q, E(x, y) = 0\} \cup \{\infty\}$.

Let G be a cyclic additive subgroup of $(E/F_q, "+")$ with generator P of prime order n. Scalar multiplication tP over E/F_p mean t times addition of P, that can be calculated using double-and-add method. Reader may refer to [18, 19] for details about the elliptic curve.

2.2. Complexity assumption

Elliptic curve discrete logarithm problem (ECDLP): Given $Q \in_R Z_n^*$ and P the generator of G, to compute x s.t $Q = xP$ is called ECDLP and assumed to be intractable.

3. Proxy Multi-Signature Scheme

Let $\mathcal{P}$ be the proxy signer designated by the original signers $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_l$.

3.1. Definition of Proxy Multi-Signature Scheme

A proxy multi-signature scheme is specified by a polynomial-time algorithms with the following functionalities.

- *Setup*: Given a security parameter k, this algorithm outputs the system parameters.
- *Extract*: It takes as input the security parameter k and outputs the secret-public key pairs (sk_i, pk_i), $\forall i = 1, 2, \dots, l$ for original signers, and (sk_p, pk_p) for the proxy signer.
- *DelGen*: Given the system's parameter, the original signer's private key sk_i and the warrant m_ω to be signed, this algorithm outputs the delegation $W_{\mathcal{A}_i \to \mathcal{P}}$.
- *DelVerif* : This algorithm takes $pk_i W_{\mathcal{A}_i \to \mathcal{P}}$ as input and verifies whether it is a valid delegation came from $\mathcal{A}_i$.
- *PKGen*: The proxy key generation algorithm takes $W_{\mathcal{A}_i \to \mathcal{P}} \forall i = 1, 2, \dots, l$ and some other secret information (for example, the secret key of the executor) as inputs, and outputs a proxy signing key sk_{pr} for proxy signature.
- *PMSign*: The proxy signing algorithm takes a proxy signing key sk_{pr} and a message $m \in \{0,1\}^*$ as inputs, and outputs a proxy signature $(m;\ s)$.
- *PMVerif* : The proxy verification algorithm takes pk_i , $\forall i = 1, 2, \dots, l, p$, and a proxy signature (m, s) as inputs, and outputs 0 or 1. In the later case, (m, s) is a valid proxy multi-signature on m by the proxy signer on behalf of the original signers.

3.2. Security Model of Proxy Multi-Signature Scheme

We consider an adversary $\mathcal{T}$ which is assumed to be a probabilistic polynomial time algorithm which takes as input the global scheme parameters and a random tape. Existential unforgeability under adaptively chosen-message attack [12] for a signature scheme (KeyGen, Sign, and Verif) is defined using the following game between a challenger C and an adversary $\mathcal{T}$.

For PMS scheme, we define an experiment $Exp_{\mathcal{T}}^{PMS}$ of adversary $\mathcal{T}$ and security parameter k as follows.

- *Setup*: The challenger C runs algorithm KeyGen to obtain a public key pk and private key sk. The adversary $\mathcal{T}$ is given pk.
- *Queries*: Proceeding adaptively, $\mathcal{T}$ requests signatures with pk on at most q_s messages of his choice $m_1, \dots, m_{q_s} \in \{0,1\}^*$. The challenger responds to each query with a signature $s_j = Sign(sk, m_j)$.
- *Output*: Eventually, $\mathcal{T}$ outputs a pair $(m,\ s)$ and wins the game, i.e $Exp_{\mathcal{T}}^{PMS}$ returns yes, if
  (a) m is not any of the $m_1, \dots, m_{q_s}$ and
  (b) Verif(pk, m, s) = valid. Otherwise returns no.

Definition-A PMS scheme is said to be existential proxy signature unforgeable under adaptively chosen message attack (PS-EUF-ACMA), if for any polynomial-time adversary $\mathcal{T}$, $\Pr[Exp_{\mathcal{T}}^{PMS}(k) = yes]$ is negligible.

4. Proposed Scheme

In this section, we present a secure PMS scheme based on ECDLP.

- *Setup*: This algorithm takes a security parameter k, and returns system parameters $\Omega = \{F_q, E/F_q, G, P, H_1, H_2\}$ as defined in Section 2.1.
  $H_1: \{0,1\}^* \times G \to Z_q^*$ and
  $H_2: \{0,1\}^* \times G \to Z_n^*$ are two
  cryptographic secure hash functions.
- *Extract*: Each signer picks at random $sk_i \in Z_q^*$ and computes $pk_i = sk_i P$. Thus (sk_i, pk_i) , $i \in \{1, 2, \dots, l, p\}$ is private and public key pair.
- *DelGen*: This algorithm takes $\mathcal{A}_i$'s secret key sk_i and a message warrant m_w as inputs, and outputs the delegation $W_{\mathcal{A}_i \to \mathcal{P}}$, $i \in \{1, 2, \dots, l\}$ as follows:
  1) Generates randomly $a_i \in Z_q^*$, computes $K_i = a_i P$.
  2) Computes $h_i = H_1(m_w, K_i)$ and $\sigma_i = (h_i sk_i + a_i) \bmod n$.
  Each $\mathcal{A}_i$ sends delegation $W_{\mathcal{A}_i \to \mathcal{P}} = \{pk_i, m_w, K - i, \sigma_i\}$ to proxy signer $\mathcal{P}$.
- *DelVerif* : To verify the delegation $W_{\mathcal{A}_i \to \mathcal{P}} (\forall i = 1, 2, \dots, l)$ and message warrant m_w, proxy signer $\mathcal{P}$ first computes $h_i = H_1(m_w, K_i)$, then checks whether $\sigma_i P = h_i pk_i + K_i$. Accepts if it is equal, otherwise rejects.
- *PKGen*: If $\mathcal{P}$ accepts each delegation $W_{\mathcal{A}_i \to \mathcal{P}}$, he computes the proxy signing key sk_{pr} as:
  chooses $b \in Z_n^*$ and computes $R = bP$, $h_2 = H_2(m, R)$, $sk_{pr} = \sum_1^l \sigma_i + sk_p h_2$.
- *PMSign*: Takes system parameters, the proxy signing key sk_{pr} and a message m as inputs, returns a signature of the message m. The proxy signer $\mathcal{P}$ does as follows.
  1) checks whether the equation $gcd(b + h_2, n) = 1$, continues if it does, otherwise returns to PKGen.
  2) computes $s = (b + h_2)^{-1} sk_{pr} \bmod n$.
  The resulting signature is $(pk_i, K_i, m_w, m, R, s, (i = 1, 2, \dots, l, p))$.
- *PMVerif*: To check whether the signature $(pk_i, K_i, m_w, m, R, s,\ (i = 1, 2, \dots, l, p))$ is a valid proxy multi-signature on message m under warrant m_w, the verifier $\mathcal{V}$ first checks if the proxy signer and the message confirm to m_w, then computes $h_i = H_1(m_w, K_i)$, $h_2 = H_2(m, R)$, finally verify whether the following equation holds.

$$s(R + h_2P) = \sum_{1}^{l}(h_i pk_i + K_i) + h_2 pk_p.$$

If the equality holds, Verifier $\mathcal{V}$ accepts the signature, otherwise rejects it.

Correctness: Since $R = bP$ and $s = (b + h_2)^{-1}\, sk_{pr} \bmod n$, we have

$$s(R + h_2P) = (b + h_2)^{-1} sk_{pr}(b + h_2)P$$
$$= sk_{pr}P = \sum_{1}^{l}(h_i pk_i + K_i) + h_2 pk_p.$$

5. Security Analysis

Assume there is an adversary $\mathcal{T}$ who can break our PMS scheme say $\sum$ .We will construct a polynomialtime algorithm $\mathcal{F}$ that, by simulating the challenger and interacting with $\mathcal{T}$, solves the ECDLP.

Theorem 1. *If an attacker $\mathcal{T}$ can break $\sum$ with at most q_{H_2} H_2-queries and q_s signature queries within time bound t and non negligible probability ε under adaptively chosen message attack against $\sum$, then there exist an algorithm to solve the ECDLP with nonnegligible probability.*

Proof. Suppose an attacker $\mathcal{T}$ can break $\sum$ through adaptively chosen message attack, then $Pr[Exp_{\mathcal{T}}^{PMS}(k) = yes]$ is non negligible. Our aim is now to show that using the ability of $\mathcal{T}$, one can construct an algorithm $\mathcal{F}$, for solving the ECDLP.

For this purpose, $\mathcal{F}$ sets $\{F_q, E/F_q, G, P, H\_1, H\_2\}$ as system parameters and answers $\mathcal{T}$'s queries as described in Section 3.2.

We prove by contradiction that the scheme is secure. The Algorithm $\mathcal{F}$ simulates the challenger and interacts with forger $\mathcal{T}$ as follows.

- *Setup*: Algorithm $\mathcal{F}$ starts to obtain public key pk and private key sk. The adversary $\mathcal{T}$ is given pk.
- *PMSign-query:* $\mathcal{T}$ is allowed to query the signature oracle for m under the delegation $W_{\mathcal{A}_i \to \mathcal{P}} = \{pk_i, m_w, K_i, \sigma_i, i = 1, 2, \ldots, l\}$.
  There exist a simulator S that simulates the oracle and generates the signature (m, R, s) which satisfies the equation
  $$s(R + h_2P) = \sum_{1}^{l}(h_1 pk_i + K_i) + h_2 pk_p.$$
- *Output*: If $\mathcal{T}$ can forge a valid signature on message m with the probability $Pr[Exp_{\mathcal{T}}^{PMS}(k) = yes] = \varepsilon \geq 10(q_{H_2} + 1)(q_{H_2} + q_s)/2^k$ where m has not been queried to the signature oracle, then a replay of $\mathcal{F}$ with the same random tape but different choice of H_2 will output two valid signatures $(pk_i, m_w, K_i, m, R, s, h_2)$ and $(pk_i, m_w, K_i, m, R, \acute{s}, \acute{h_2})$.

Then we have

$$s(R + h_2P) = \sum_{1}^{l}(h_i pk_i + K_i) + h_2 pk_p, \quad (1)$$

$$\acute{s}\left(R + \acute{h_2}P\right) = \sum_{1}^{l}(h_i pk_i + K_i) + \acute{h_2} pk_p, \quad (2)$$

subtracting equation (2) to (1), we have

$$\left[(s - \acute{s})b + \left(sh_2 - \acute{s}\acute{h_2}\right)\right]P = \left(h_2 - \acute{h_2}\right)sk_pP.$$

Let $u = (s - \acute{s})b + \left(sh_2 - \acute{s}\acute{h_2}\right) \bmod n$ and $v = \left(h_2 - \acute{h_2}\right)^{-1} \bmod n$. Then $sk_p = uv \bmod n$.

According to Lemma 4 in [9], the ECDLP can be solved with probability $\acute{\varepsilon} \geq 1/9$ and time $\acute{t} \leq 23_{q_{H_2}} t/\varepsilon$.

6. Comparative Analysis

In this section, we discuss the security of the schemes [4, 5, 7, 17, 38, 41] in Table 1 and compare the efficiency of our scheme with the schemes [2, 13,20, 28, 37] in Table 2. Since the running time of one pairing operation is $20.04\, ms$, ECC-based scalar multiplication is $2.21\, ms$, pairing-based scalar multiplication is $6.38\, ms$ and Map-to-point hash function is $3.04\, ms$ [16]. These operation times for various cryptographic operations have been obtained using MIRACAL [29]. The hardware platform is a PIV 3 GHZ processor with 512 M bytes memory and the Windows XP operating system. For the pairing-based scheme, to achieve the 1024-bit RSA level security, Tate pairing defined over the supersingular elliptic curve $E/F_q : y^2 = x^3 + x$ with embedding degree 2 has been used, where u is a 160-bit Solinas prime $u = 2^{159} + 2^{17} + 1$ and q a 512-bit prime satisfying $q + 1 = 12ur$. For the ECC-based schemes, to achieve the same security level, the parameter secp160r1 [3], recommended by the Certicom Corporation has been employed, where $u = 2^{160} - 2^{31} - 1$. We use these running time calculations to present the computational cost comparison in Table 2.

Table 1. Security analysis of the schemes without pairings

Scheme	Security	Security in ROM
[4]	insecure against forgery attack	No
[5]	insecure against conspiracy attack	No
[17]	insecure against forgery attack	No
[7]	insecure against distinguishability, undeniability, proxy misuse	No
[41]	secure	No
[38]	secure	No
Our	secure	yes

Table 2. Efficiency comparison with the schemes from pairings

Scheme	Computational cost	Running time (ms.)	Security Model
[20]	$3M_P + 4H_M + 5O_P$	131.5	No
[13]	$9M_P + 4H_M + 6O_P$	189.82	ROM
[37]	$12M_P + 13H_M + 6O_P$	236.32	ROM
[2]	$7M_P + 9H_M + 7O_P$	212.30	ROM
[28]	$5M_P + 7H_M + 7O_P$	193.46	ROM
Our	$9M_E$	19.89	ROM

In the table M_E, M_P, H_M, O_P stand for one ECC based scalar multiplication, pairing based scalar multiplication, Map-to-point hash function and pairing operation, respectively.

Remarks:

1. Since the schemes [4, 5, 7, 17, 38, 41] do not provide any formal security proof, we do not feel to compare the efficiency of our proposed scheme with them.

2. Our scheme has the running time only 15.12% of [20], 10.47% of [13], 8.41% of [37], 9.36% of [2] and 10.28% of [28].

Open Problem:

ECDLP based schemes are fully exponential time and have the same security level as RSA and DSA, but smaller key size. On the other hand, pairing is regarded as an expensive cryptography primitive. Therefore, we think that schemes based on ECDLP without pairing would be more appealing in terms of efficiency. We propose first PMS scheme without pairing and secure in ROM. But it is still an open problem to propose a new PMS scheme based on ECDLP without pairings, secure in standard model.

7. Conclusion

In this paper, we first defined a security model of PMS scheme, then proposed a PMS scheme based on ECDLP. It provides theoretical foundations for the provable security of PMS schemes based on ECDLP. Our scheme is secure against adaptive chosen message attack in the ROM.

Acknowledgments

The authors are grateful to the Editor and anonymous reviewers for their valuable comments and suggestions for improving an earlier version of the paper.

References

[1] **M. Bellare, P. Rogaway**. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. First ACM Conference on Computer and Communications Security, ACM, November 1993, pp. 1-21.

[2] **F. Cao, Z. Cao**. A secure identity-based proxy multi-signature scheme. Information Science, 2009, Vol. 179, No. 3, 292-302.

[3] The Certicom Corporation, SEC 2: Recommended Elliptic Curve Domain Parameters, <www.secg.org/collateral/sec2final.pdf>.

[4] **T. S. Chen, Y. E. Chung, G. S. Huang**. Efficient proxy multi-signature schemes based on the elliptic curve cryptosystem. *Computer and Security*, 2003, Vol. 22, No. 6, 527-534.

[5] **T. S. Chen, Y. E. Chung, K. H. Huang**. A traceable proxy multi-signature scheme based on the elliptic curve cryptosystem. *Applied Mathematics and Computation*, 2004, Vol. 159, No. 1, 137-145.

[6] **L. Chen, Z. Cheng, N. P. Smart.** Identity-based key agreement protocols from pairings. *International Journal of Information Security*, 2007, Vol. 6, No. 4, 213-241.

[7] **T. J. Cao, D. D. Lin, R. Xue**. Security analysis of some proxy multi-signature schemes based on elliptic curve cryptosystem. Mini-Micro System, 2006, Vol. 27, No. 5, 798-801.

[8] **X. Cao, W. Kou, X. Du**. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. *Information Sciences*, 2010, Vol. 180, No. 15, 2895-2903.

[9] **P. David, S. Jacques**. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 2000, Vol.13, No. 3, 361-396.

[10] **M. Das, A. Saxena, D. B. Pathak**. Algorithms and approaches of proxy signature: a survey. *International Journal of Network Security*, 2009, Vol. 9, No. 3, 264-284.

[11] **A. Fiat, A. Shamir**. How to prove yourself: practical solutions to identification and signature problems. *Advances in Cryptology, CRYPTO'86, Lecture Notes in Computer Science(LNCS)*, 1986, Issue 263, pp. 186-194.

[12] **S. Goldwasser, S. Micali, R. Rivest**. A digital signature scheme secure against adaptive chosen message attacks. SIAM Journal of Computing, 1988, Vol. 17, No. 2, 281-308.

[13] **C. X. Gu, H. Pan, Y. F. Zhu.** A new ID based proxy multi signature scheme from bilinear pairings. *Wuhan University Journal of Natural Sciences*, 2006, Vol. 11, No. 1, 193-197.

[14] **S. F. Tzeng, C. C. Lee, M. S. Hwang.** A batch verification for multiple proxy signature. *Parallel Processing Letters*, 2011, Vol. 21, No. 1, 77-84.

[15] **M. S. Hwang, C. C. Lee, S. F. Tzeng.** A new proxy signature scheme for a specified group of verifiers. *Information Sciences*, 2013, Vol. 227, 102-115.

[16] **D. He, J. Chen, J. Hu.** An ID-based proxy signature schemes without bilinear pairings. *Annals of Telecommunications*, December 2011, Vol. 66, No. 11-12, 657-662.

[17] **J. H. Ji, D. X. Li.** A New Proxy Multi-Signature scheme. *Journal of Computer Research and Development*, 2004, Vol. 41, No. 4, 715-719.

[18] **N. Koblitz**. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 1987, Vol. 48, 203-209.

[19] **N. Koblitz**. A Course in Number Theory and Cryptography. *New York, Springer-Verlag*, Second edition, 1994.

[20] **X. Li, K. Chen, S. Li**. Multi-proxy signature and proxy multi-signature schemes from bilinear pairings. PDCAT 2004, Springer-Verlag Berlin Heidelberg, LNCS, 2004, Vol. 3320, pp. 591-595.

[21] **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*, 2011, Vol. 7, No. 3, 1039-1054.

[22] **Z. Liu, Y. Hu, H. Ma**. Secure proxy multi-signature scheme in the standard model. Springer-Verlag Berlin Heidelberg, LNCS, 2008, Vol. 5324, 127-140.

[23] **E. 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, 799-806.

[24] **W. Y. Liu, F. Tong, B. W. Wang, Y. D. Wang.** A new proxy blind signature scheme with proxy revocation. *Journal of Electronics and Information Technology*, 2008, Vol. 30, No. 10, 2468-2471.

[25] **V. S. Miller**. Uses of Elliptic Curves in Cryptography. In: *Advances in Cryptology-Crypto'85, Proceedings, LNCS*, New York, Springer-Verlag, 1985, Vol. 218, pp. 417-426.

[26] **M. Mambo, K. Usuda, E. Okamoto**. Proxy signatures: delegation of the power to sign messages. *IEICE Transaction Functional E79-A*, 1996, Vol. 9, 1338-1353.

[27] **J. H. Park, B. G. Kang, S. W. Park**. Cryptanalysis of some group-oriented proxy signature schemes. Lecture Notes in Computer Science, Springer-Verlag Berlin, Heidelberg, 2006, Vol. 3786, 10-24.

[28] **Z. Shao.** Improvement of identity-based proxy multisignature scheme. Journal of System Software, 2009, Vol. 82, No. 5, 795-800.

[29] **Shamus Software** Ltd., Miracle library <http://www.shamus.ie/index.php?page=home>.

[30] **H. M. Sun**. On proxy multisignature Schemes. In: *Proceedings of the International Computer Symposium*, 2000, pp. 65-72.

[31] **S. Padhye, N. Tiwari.** Improved proxy signature scheme without bilinear pairings. Quality, Reliability, Security and Robustness in Heterogeneous Networks. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, 2013, Vol. 115, 682-688.

[32] **S. Padhye, N. Tiwari.** ECDLP-based certificateless proxy signature scheme with message recovery. *Transactions on Emerging Telecommunications Technologies*, 2012, doi: 10.1002/ett.2608.

[33] **Y. Sun, C. Xu, Y. Yu, B. Yang**. Improvement of a proxy multi-signature scheme without random oracles. *Computer Communications*, 2011, Vol. 34, No. 3, 257-263.

[34] **Z. Tan**. Efficient pairing-free provably secure identity based proxy blind signature scheme. *Security and Communication Networks*, 2013, Vol. 6, 593-601.

[35] **N. Tiwari, S. Padhye**. Analysis on the generalization of proxy signature. *Security and Communication Networks*, 2013, Vol. 6, 549-556.

[36] **R. Waters**. Efficient identity based encryption without random oracles. In: *Proceedings of the Eurocrypt 2005, LNCS*, 2005, Vol. 3494, pp.114-127.

[37] **Q. Wang, Z. Cao**. Identity based proxy multi-signature. *Journal of System Software*, 2007, Vol. 80, 1023-1029.

[38] **Q. Xue, F. Li, Z. Cao**. Two improved proxy multi-signature schemes based on the elliptic curve cryptosystem, Availabe at http://www.paper.edu/cn/index.php/default/enreleasepaper/content/41559, 2010.

[39] **X. Li, K. Chen**. ID-based multi-proxy signature, proxy multisignature and multi-proxy multi-signature schemes from bilinear pairings. *Applied Mathematics and Computation*, 2005, Vol. 169, 437-450.

[40] **L. Yi, G. Bai, G. Xiao**. Proxy multisignature scheme: a new type of proxy signature scheme. *Electronics Letters*, 2000, Vol. 36, No. 6, 527-528.

[41] **X. Yin, F. Y. S. Ou**. Proxy multi-signature scheme with proxy revocation. *Computational Intelligence and Software Engineering (CISE 2009)*, 2009, pp. 1-4., DOI:10.1109/CISE.2009.5364200.

Received October 2013.