International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12– No.19, February 2019 – www.ijais.org

Undeniable Organizational Signature Scheme without a Trusted Party

Fatty M. Salem
Department of Electronics, Communications, and Computers Engineering
Helwan University, Faculty of Engineering
1 Sherif St., Helwan, Cairo, Egypt

ABSTRACT
Organizational signature is a new kind of digital signature introduced to facilitate and guarantee legitimacy of transactions among organizations. It allows employee in the organization to sign messages through his affiliation not only through his personal identity. As non-repudiation is basic characteristic for digital signature, this paper presents an undeniable organizational signature scheme to guarantee undeniability of both the employee and organization. Moreover, in the proposed scheme, the collaboration between the employee and organization to generate the digital signature can be securely accomplished without need for a trusted third party. The proposed signature scheme is based on Elliptic Curve Cryptography (ECC) as ECC requires smaller keys and has a low computational cost in comparison of non-ECC cryptography to provide equivalent security. Moreover, the security of the proposed scheme has been proved.

Keywords
Digital signature; Organizational signature; Elliptic curve cryptography; Non-repudiation; Trusted third party.

1. INTRODUCTION
Digital signature is a security scheme for authenticating the signer and validating the integrity of the signed message or digital document. Digital signature is designed to solve the problem of tampering and impersonation in digital communications over open networks. There are some common properties of the existing digital signature schemes for communication applications as authentication, integrity, and non-repudiation.

Many ordinary digital signature algorithms have been early proposed to guarantee the abovementioned security services such as: the public key cryptosystem RSA [1], the digital signature algorithm [2], El-Gamal signature scheme [3], Rabin signature scheme [4], and Boneh-Lynn-Shacham signature scheme [5].

Furthermore, numerous schemes have been proposed based on digital signature with different properties according to the application needs [6]. Threshold signature schemes [7-12] have been proposed to enable any subset of t users of a total of n prospective users to produce a valid signature of the message. This system is known as (t, n)-threshold.

Group signature schemes [13-15] have been proposed to allow group's members to sign messages on behalf of the group, such that the resulting signature can be verified with respect to a single group public key without revealing the identity of the signer. These schemes need the collaboration of a manager or trusted third party. A similar scheme has been proposed and defined as ring signature scheme [16-18]; however, ring signature excludes the requirement of a group manager. Moreover, ring signature guarantees the anonymity of signers.

In blind signature schemes [19-21], a signer can sign a message for a user without knowing the contents of the message, while the user is kept anonymous with respect to all other users. This technique has been proposed to create an electronic version of money such that an e-coin could not be easily traced from the bank to the shop. Moreover, transactions executed by the same user cannot be linked together.

Multi-signature schemes [22-25] have been proposed to allow multiple signers to generate a single signature in a collaborative and simultaneous manner. The number of signers is not fixed and signers' identities are obvious from a given multi-signature. In some applications, the co-signers of the multi-signature may participate with different roles/positions. Therefore, they have different management liabilities and authorization capabilities.

Proxy signature schemes [26-29] have been proposed to enable a proxy signer to compute signatures on behalf of an original signer. Proxy signer is the delegator to afford partial signature to other users. Proxy signatures cannot offer anonymity; however, the authors in [30] have proposed a threshold proxy signature scheme in which all proxy signers remain anonymous. Furthermore, a secure ID-based blind and proxy blind signature scheme is proposed in [31] to satisfy the security features of both blind and proxy signature schemes.

In society oriented signature schemes [32-34], the verifier just knows that the signature is generated from some association and verifies its correctness with respect to a single identity and a fixed public key of the association. It is not necessary for the verifier to know the actual co-signers or even the number of cooperated signers to sign the message.

Attribute-based signature schemes [35-37] have been proposed to allow a signer to sign a message with a predicate that is satisfied by his attributes issued from an attribute authority. A valid signature can be generated without disclosing any further information about the signer. In [38], multiple attribute-based signature scheme has been proposed to meet with the requirement of distributed authentication techniques and to protect the consumers privacy.

Recently, a new variant digital signature scheme has been proposed for the organization's structures and liabilities; this scheme is called organizational signature scheme [40]. Organizational signature schemes [39-41] allow the organization to obtain the signature of any employee not as an individual but through his organization related signature. Due to this kind of signature, an organization can generate different signatures related to each position. However, a trusted third party is a must in these proposed organizational schemes to collect the private keys of both the employee and organization center to compute the organizational key pair. This may destroy the undeniability notion of both the

employee and organization. Hence, in this paper, a strong undeniable organizational signature scheme has been proposed to guarantee undeniability of both the employee and organization without need for trusted third party.

1.1. Our contribution

This paper claims the following contributions.

- It has been pointed out that the existing organizational signature schemes cannot provide undeniability of both the employee and organization.
- It has been pointed out that the trusted third party is a must in the existing organizational signature schemes.
- The main contribution of this paper is to design and analyze an undeniable organizational signature scheme for organization's structures and liabilities.
- The proposed scheme can provide unforgeability, undeniability, and linkability to employee's job without a need for a trusted third party.

1.2. Roadmap of the paper

The rest of the paper is organized as follows: The security issues of the organizational schemes are described in section 2. The existing concatenated organizational signature scheme is reviewed in section 3. In section 4, the proposed undeniable organizational signature scheme is introduced. The security of the proposed scheme is analyzed in section 6. Finally, our work is concluded in section 7.

2. SECURITY ISSUES OF ORGANIZATIONAL SIGNATURE

The security issues for a secure organization's structure are listed below:

Organizational Signature: Anyone can check that the signature was formed by means and collaboration of the organization.

Unforgeability: Only the original signer can collaborate with the organization to create a valid organizational signature related to his affiliation.

Organization Undeniability: The employee cannot create a valid organizational signature individually, but he has to collaborate with the organization to create a valid organizational signature.

Employee Undeniability: The organization cannot create a valid organizational signature of an existing employee on his job. However, if the employee left the job, the organization has to change the public parameter of the signature and revoke the previous employee and its signature.

No Trusted Party Existence: The collaboration between the employee and organization to agree on the secret and public keys can be accomplished without a need for a trusted third party.

Verifiability: Any receiver who has the related public parameters can check the validity of the received signature.

Linkability: The verifier can relate the signature to the job of the employee as the verifier has its public information.

3. THE EXISTING ORGANIZATIONAL SIGNATURE SCHEME

The authors in [41] have proposed three different schemes based on the scenarios of organizational signature [39]. In this section, the concatenated organizational signature scheme is recalled.

Initially, the organization generation center generates the elliptic curve parameters (G, n) where G is the elliptic curve base point and a generator of the elliptic curve with large prime order *n*. In addition, the organization generation center picks a random key $x_o \in [1, n-1]$, which will be the organization part of the private key used in signing messages. It then computes the public key $Y_o = x_o G$ and publishes G and Y_o. It is assumed that each employee has a personal key pair (x_p, Y_p). Then the following three phases are executed:

Key generation: In this phase, a trusted third party receives both the employee's and organization's part of the private key through a secure channel to compute the organizational key pair. The trusted third party:

- Selects random number $a \in [1, n-1]$.
- Computes the organization private key as $x = a(xp+xo)(mod\ q)$.
- Computes the pubic key as $Y = xG$.
- Publishes *Y* and securely sends *x* to the employee.

Signature generation: In this phase, the employee can independently generate a signature (s, r) for a message m as follows:

- He/she selects random number $k \in [1, n-1]$.
- He/she computes $s = a.(k + xh(m))(mod\ q)$.
- He/she computes $r = kG$.

Signature verification: Any entity can verify the validity of the signature as follows:

- He/she computes $V_1 = sG$.
- He/she computes $V_2 = r + h(m)Y$.
- He/she accepts if $V_1 = V_2$, O.W, discards.

4. UNDENIABLE ORGANIZATIONAL SIGNATURE SCHEME

In this section, the proposed undeniable organizational signature scheme is introduced. The scheme consists of three algorithms: Key Generation, Signature Generation, and Signature Verification. These algorithms are described as follows:

4.1 Key Generation

Key generation is the initial phase of the proposed scheme in which the employee and organization collaborate to establish the public key. It is obvious that the key generation phase is done only once. First, the organization generates an identifier for each employee ID_E when the employee is joining the organization. Then, the employee and organization cooperate to compute the public key as shown in Fig. 1 and detailed in the following steps:

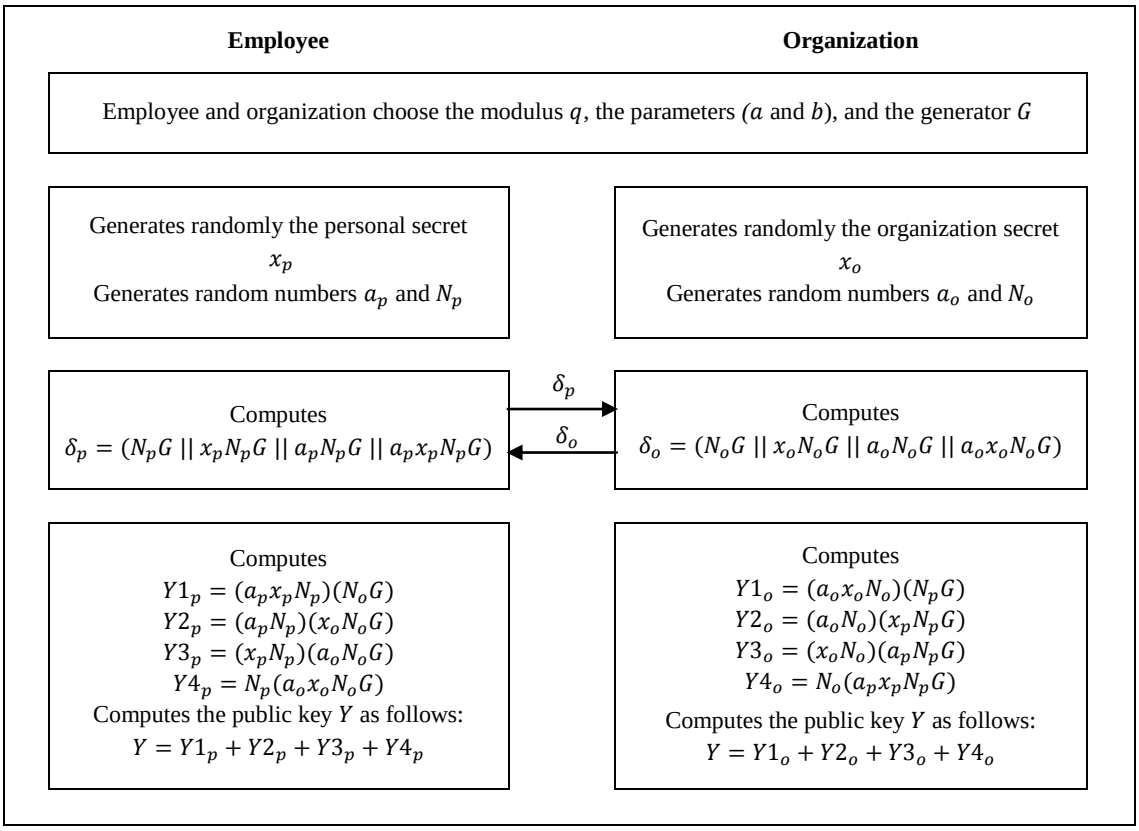

Fig 1: The key generation algorithm

The employee and organization choose the modulus q, the elliptic curve parameters (a and b), and the generator G (with a large prime order n).

The employee generates randomly its personal secret x_p, and generates two random numbers a_p and N_p. Then, the employee computes $\delta_p = (N_pG \,||\, x_pN_pG \,||\, a_pN_pG \,||\, a_px_pN_pG)$, and sends δ_p to the organization.

The organization generates randomly its secret key x_o, and generates two random numbers a_o and N_o. Then, the organization computes $\delta_o = (N_oG \,||\, x_oN_oG \,||\, a_oN_oG \,||\, a_ox_oN_oG)$, and sends δ_o to the employee.

The employee computes the following:

$$Y1_p = (a_px_pN_p)(N_oG)$$
$$Y2_p = (a_pN_p)(x_oN_oG)$$
$$Y3_p = (x_pN_p)(a_oN_oG)$$
$$Y4_p = N_p(a_ox_oN_oG)$$

The organization computes the following:

$$Y1_o = (a_ox_oN_o)(N_pG)$$
$$Y2_o = (a_oN_o)(x_pN_pG)$$
$$Y3_o = (x_oN_o)(a_pN_pG)$$
$$Y4_o = N_o(a_px_pN_pG)$$

Finally, the employee can compute the public key as $Y = Y1_p + Y2_p + Y3_p + Y4_p$, and also the organization can compute the public key as $Y = Y1_o + Y2_o + Y3_o + Y4_o$. The employee and organization compute equal values where the public key $Y = xG$ and the final private key $x = N_pN_o(a_p + a_o)(x_p + x_o)modq$. At the end of this phase, the public parameters (a, b, q, G) and the public key Y is publicly published.

4.2 Signature Generation

The employee and organization collaborate to generate the signature of a message m. Let $h(M)$ be the hash function of M, where $M = (ID_E||Aff||m)$, ID_E is the employee's identifier, and Aff is the affiliation of the employee. This phase runs each time the employee sends $M = (ID_E||Aff||m)$ to any destination. The signature generation algorithm is shown in Fig. 2 and detailed as follows:

The employee picks a random number k_p such that $k_p \in [1, n-1]$. Then, the employee computes $\xi_p = ((a_pN_ph(M))||(k_pN_pG))$, and sends ξ_p to the organization.

The organization picks a random number k_o such that $k_o \in [1, n-1]$. Then, the organization computes $\xi_o = ((a_oN_oh(M))||(k_oN_oG))$, and sends ξ_o to the employee.

The employee computes $t_p = (k_pN_p + a_px_pN_ph(M))(mod\ q)$ and $u_p = N_p(k_oN_oG)$, then sends $(t_p||u_p)$ to the organization.

The organization computes $t_o = (k_oN_o + a_ox_oN_oh(M))(mod\ q)$ and $u_o = N_o(k_pN_pG)$, then sends $(t_o||u_o)$ to the employee.

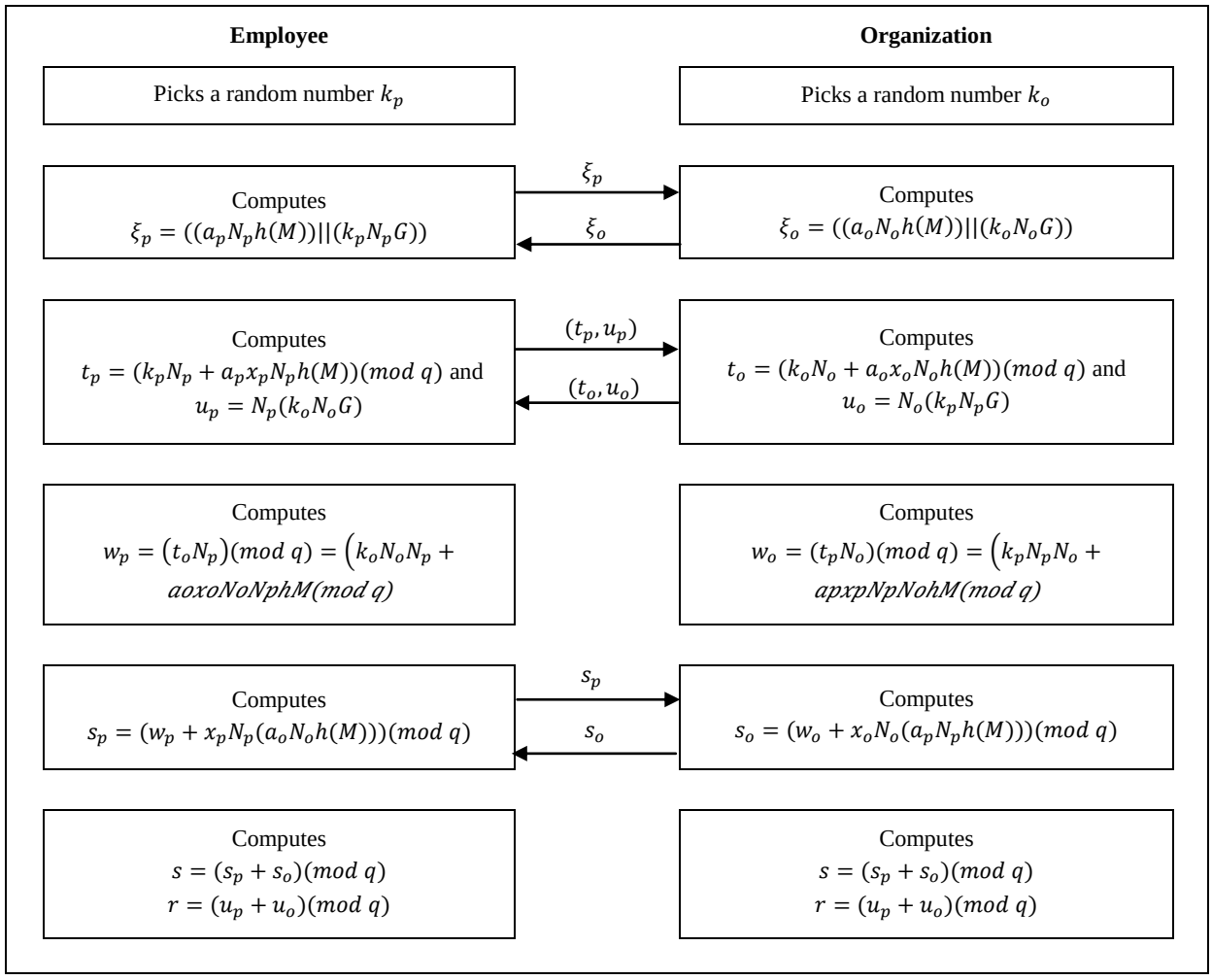

Fig 2: The signature generation algorithm

The employee computes $w_p = (t_o N_p) mod\ q = \left(k_o N_o N_p + a_o x_o N_o N_p h(M)\right)(mod\ q)$ and $s_p = (w_p + x_p N_p(a_o N_o h(M)))(mod\ q)$, then sends s_p to the organization. It is obvious that $s_p = \left(k_o N_o N_p + a_o x_o N_o N_p h(M) + x_p N_p\left(a_o N_o h(M)\right)\right)(mod\ q)$.

The organization computes $w_o = (t_p N_o)(mod\ q) = \left(k_p N_p N_o + a_p x_p N_p N_o h(M)\right)(mod\ q)$ and $s_o = (w_o + x_o N_o(a_p N_p h(M)))(mod\ q)$, then the organization sends s_o to the employee. It is obvious that $s_o = \left(k_p N_p N_o + apxpNpNohM + xoNoapNphM(mod\ q)\right.$.

Finally, the employee and the organization can compute the signature (r, s) of the message M as $r = (u_p + u_o)(mod\ q)$ and $s = (s_p + s_o)(mod\ q)$. The final organizational signature sent to the receiver is $(M||r||\ s)$. It is obvious that $s = \left(k + xh(M)\right)(mod\ q)$ and $r = kG$, where $x = N_p N_o(a_p + a_o)(x_p + x_o)(mod\ q)$ and $k = N_p N_o\left(k_p + k_o\right)(mod\ q)$.

4.3 Signature Verification

The receiver can verify the validity of the signature as follows:

- Computes $V_1 = sG$.
- Computes $V_2 = r + h(M)Y$.
- If $V_1 = V_2$, accepts the message, else rejects.

5. SECURITY ANALYSIS

In this section, the proposed scheme will be analyzed, and the security issues discussed in section 2 will be verified. In the proposed undeniable organizational signature scheme, two kinds of attacks are considered:

Attack1. An adversary intends to deduce the final secret key x from the known public key Y and the parameters (G, n, and q). The proposed scheme is resilient against this kind of attack.

Proof. The adversary cannot derive the secret key from the known public key and parameters since it needs to solve the Elliptic Curve Discrete Logarithm Problem (ECDLP) which is widely-believed to be a very hard computation problem.

Attack2. An adversary attempts to forge the organizational signature to impersonate the employee and/or the organization. Our proposed scheme is resilient against this kind of attack.

Proof. If the adversary wants to create a valid signature, he needs to know the value of the employee's private key x_p

and/or the organization's private key x_o; this is not possible in our scheme. The private key is not possible due to ECDLP to recover from the public known information (shown in Attack 1).

Security issues of organizational structure are guaranteed in the proposed scheme by the following theorems:

Theorem 1. (Organizational signature) It is clear that the creation of the signature depends on the organization.

Proof. As the signature includes the organization secret key for each message the employee intends to sign, $s = \big(k + xh(M)\big)(mod\ q)$, where $x = N_p N_o(a_p + a_o)(x_p + x_o)(mod\ q)$; hence, it must be done by the organization.

Theorem 2. (Unforgeability) Only the original signer can collaborate with the organization to create a valid organizational signature related to his affiliation.

Proof. As the signature depends on the employee secret key x_p to compute $s = \big(k + xh(M)\big)(mod\ q)$, where $x = N_p N_o(a_p + a_o)(x_p + x_o)(mod\ q)$; hence, no other party (hasn't the employee secret key) can collaborate with the organization to create a valid signature.

Theorem 3. (Organization Undeniability) The proposed scheme provides organization non-repudiation for any signature.

Proof. The organization can't deny the signature as the creation of the signature relies on the organization secret key x_o.

Theorem 4. (Employee Undeniability) The proposed scheme provides employee non-repudiation for any signature.

Proof. The employee cannot deny the signature as the creation of the signature relies on the employee secret key x_p.

Theorem 5. (No Trusted Party Existence) The proposed scheme doesn't need the existence of a trusted third party to agree on the secret key and public parameters or to complete the creation of the digital signature.

Proof. The organization generates the random numbers (a_o, N_o) and the employee generates the random numbers (a_p, N_p) to agree on the private key $x = N_p N_o(a_p + a_o)(x_p + x_o)(mod\ q)$ and the public key $Y = xG$ without revealing the secret keys (x_o, x_p) to each other due to the elliptic curve discrete logarithm problem and the computational Diffie-Hellman problem. Moreover, the creation of the signature depends only on the organization's and employee's parameters; hence, there is no need for trusted third party in the key generation phase.

Theorem 6. (Verifiability) Any receiver who has the related public parameters can verify the validity of the proposed signature in our scheme.

Proof. As the receiver holds the public parameters (G, q) and the public key $Y = xG$; hence, when it receives the signature $s = \big(k + xh(M)\big)(mod\ q)$ and $r = kG$, it can verify the signature by comparing $V_1 = sG$ with $V_2 = r + h(M)Y$.

Theorem 7. (Linkability) The proposed signature scheme provides the linkable property.

Proof. As the signed message $M = (ID_E||Aff||m)$ includes the affiliation of the employee, and the signature of the message M cannot be created before checking the contents of the message M by the organization; hence, the signature can be linked to its affiliation in the organization.

6. CONCLUSION

In this paper, an undeniable organizational signature scheme has been proposed to solve the security issues for organization's structures. In addition, the proposed scheme extends the security issues to prevent both the employee and organization to deny the signed message. The proposed scheme can solve these security issues without need for trusted third party. The security of the proposed scheme is proved based on the hardness of elliptic curve discrete logarithm problem and the computational Diffie-Hellman problem. To the best of our knowledge, this paper presents the first undeniable organizational signature scheme which considers all security issues of organization's structure.

7. ACKNOWLEDGMENTS

We would like to acknowledge with much appreciation our colleague Associate Professor Maged Hamada Ibrahim from Helwan University who provided invaluable guidance that greatly assisted the research.

8. REFERENCES

[1] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21 (2), 1978, pp. 120-126.

[2] ANSI X9.30:1-1997, Public Key Cryptography for the Financial Services Industry: Part 1: The Digital Signature Algorithm (DSA), (Revision of X9.30:1-1995), American Bankers Association, Washington, DC, 1997. Available from the ANSI Catalog, 1997.

[3] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithm problem. IEEE Trans. Info. Theory, IT-31, 1985, pp. 469-472.

[4] Rabin MO. Digitalized signatures and public-key functions as intractable as factorization, Technical Report 212, MIT Laboratory for Computer Science, 1979.

[5] Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing. In Proceedings of Asiacrypt, 2001.

[6] Singh S, Iqbal MD, Jaiswal A. Survey on techniques developed using digital signature: public key cryptography. International Journal of Computer Applications, 117(16), 2015, pp.1-4

[7] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Robust and efficient sharing of RSA functions. Advances in Cryptology – CRYPTO '96, Springer-Verlag LNCS 1109, 1996, pp.157–172.

[8] Nguyen HL. Partially interactive threshold RSA signatures. Cryptography and Coding, Institute of Mathematics and its application, IMA. Unpublished, 2005.

[9] Ibrahim MH, Ali IA, Ibrahim, II El-Sawy AH. Fast fully distributed and threshold RSA function sharing. In

proceedings of Information Systems: New Generation Conference), Las Vegas, Nevada, USA, 2004, pp. 11-15.

[10] Ibrahim MH, Ali IA, Ibrahim, II El-Sawy AH. Reducing the risk of the honest dealer assumption in robust threshold RSA function sharing. In proceedings of the 1st International Computer Engineering Conference on New Technologies for the Information Society (ICENCO 2004), Cairo, Egypt, 2004.

[11] Ibrahim MH, Ali IA, Ibrahim, II El-Sawy AH. Fully distributed and robust threshold RSA function sharing efficient for small number of players. In the Proceedings of the Information Systems: New Generations (ISNG'04), 2004, pp. 7-12.

[12] Ibrahim MH, Ali IA, Ibrahim, II El-Sawy AH. Robust threshold elliptic curve digital signature. In proceedings of the IEEE 46th symposium on Circuits and Systems, Cairo, Egypt, 2003.

[13] Chaum D, Heyst EV. Group signatures. In Advances in Cryptology - EUROCRYPT' 91, LNCS 950, Springer-Verlag, 1992, pp. 257-265.

[14] Gu K, Yin B. Efficient Group Signature Scheme without Pairings. IACR Cryptology ePrint Archive 2018: 879 (2018).

[15] Ibrahim MH. Resisting traitors in linkable democratic group signatures. International Journal of Network Security (IJNS), 9(1), 2009, pp. 51-60.

[16] Chow SSM, Wei VK, Liu JK, Yuen TH. Ring signatures without random oracles. In Proc. ACM Symposium on Information, Computer and Communications Security (ASIACCS), ACH, 2006, pp. 297-302.

[17] Naor M. Deniable ring authentication. In Advances in Cryptology | Crypto 2002, volume 2442 of Lecture Notes in Computer Science, Springer, 2002, pp. 481- 498.

[18] M lina L, Hajny J, Dzurenda P, Ricci S. Lightweight Ring Signatures for Decentralized Privacy-preserving Transactions. 15th International Conference on Security and Cryptography, 2018, pp. 692-697.

[19] Chaum D. Blind signature systems. Advances in Cryptology, Crypto'83, 1983, pp.153-156.

[20] James S, Gayathri N, Reddy PV. Pairing Free Identity-Based Blind Signature Scheme with Message Recovery. Cryptography 2018, 2, 29.

[21] Hu X, Wang J, Yang Y. Secure ID-based blind signature scheme without random oracle. NCIS '11 Proceedings of the 2011 International Conference on Network Computing and Information Security, IEEE, 2011.

[22] Itakura K, Nakamura K. A public-key cryptosystem suitable for digital multisignature. NEC Research and Development, Vol. 71, October 1983, pp. 1-8.

[23] Lin C, Wu T, Hwang J. ID-based structured multisignature schemes. Advances in Network and Distributed Systems Security, Kluwer Academic Publishers (IFIP Conference Proceedings 206), Boston, 2001, pp. 45-59.

[24] Dung LH, Minh NH. New digital multisignature scheme with distinguished signing responsibilities. Int. J. Compt. Sci. Network Security, 10(1), 2010, pp. 51-57.

[25] Islam SK, Farash, Biswas GP, Khan MK, Obaidat MS. A pairing-free certificateless digital multisignature scheme using elliptic curve cryptography. International Journal of Computer Mathematics, 94(1), 2017, pp. 39-55.

[26] Mambo M, Usuda K, Okamoto E. Proxy Signatures: Delegation of the power to sign messages. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Volume E79-A, Number 9, 1996, pp. 1338-1353.

[27] Verma GK, Singh BB. Short certificate-based proxy signature scheme from pairings. Transactions on Emerging Telecommunications Technologies, 2017(1):3214.

[28] Liu Y, Wen H, Lin C. Proxy-protected signature secure against the un-delegated proxy signature attack. Computers and Electrical Engineering, 33(3), 2007, pp. 177-185.

[29] Popsecu C. A secure proxy signature scheme with delegation by Wwarrant. Studies in Informatics and Control, 20 (4), 2011, pp. 373-380.

[30] Liu, Huang S. Identity-based threshold proxy signature from bilinear pairings. Informatica, Inst. Math & Science, 21(1), 2010, pp. 41-56.

[31] Sarde P, Banerjee A. A secure ID-based blind and proxy blind signature scheme from bilinear pairings. Journal of Applied Security Research, 12(2), 2017, pp. 276-286.

[32] Saeednia S. An identity-based society oriented signature scheme with anonymous signers. Information Processing Letters, 83, 2002, pp. 295-299.

[33] Shao Z. Cryptanalysis of an identity-based society oriented signature scheme with anonymous signers. Information Processing Letters, 86, 2003, pp. 295-298.

[34] Huang H. A novel identity-based society oriented signature scheme with anonymous signers. Applied Mathematical Sciences, 1(32), 2007, pp. 1551-1562.

[35] Maji HK, Prabhakaran M, Rosulek M. Attribute-based signatures. Topics in Cryptology–CT-RSA 2011; Kiayias, A., Ed.; Springer: Berlin/Heidelberg, Germany, 2011 pp. 376–392.

[36] Li J., Au, MH, Susilo W, Xie D, Ren K. Attribute-based Signature and its applications. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS '10), Beijing, China, 13–16 April 2010; ACM: New York, NY, USA, 2010, pp. 60–69.

[37] Li BH, Huang YY, Zhao YL. Fully adaptive attribute-based group signature in standard model. Journal of the

Chinese Institute of Engineering, 38(1), 2015, pp. 200-2007.

[38] Maji HK, Prabhakaran M, Rosulek M. Attribute-based signatures: Achieving attribute-privacy and collusion-resistance. IACR Cryptol. ePrint Arch. 2008.

[39] Ali IA, Mahgoub SM, Allam AM. A new direction in digital signature systems: organizational signature. International Journal of Computer Information Systems, 3(4), 2011, pp. 90–116.

[40] Allam AM, Ali IA, Mahgoub SM. A provably secure certificateless organizational signature schemes. International Journal Communication Systems, 2015. DOI: 10.1002/dac.3038.

[41] Mahgoub SM, Allam AM, Ali IA. An efficient organizational signature schemes based on the elliptic curve cryptography. International Journal of Applied Information Systems, 7(11), 2014, pp. 7-10.