International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 10 – No.4, January 2016 – www.ijais.org

An Organizational Signature Schemes based on ElGamal Signature

Ali M. Allam
Assistant Professor
Department of Electronic, Communication and Computer Engineering, Faculty of Engineering, Helwan University, PO box 11792, Cairo, Egypt.
Department of Applied Natural Sciences, UCC, Qassim University, Unaizah, 51911, PO box 4394, Saudi Arabia

ABSTRACT
We introduce the notation of organizational signature. This new scheme has a valuable property that assures, that if a message is signed in an organization transaction, the corresponding signature will be differentiated between the personal signature of the employee and his affiliation signature. This adds to the binding between the employee and his affiliation. Due to this signature, an organization, e.g. company, can create different signatures related to each position. In this paper, we introduce the notion of organizational signature scheme; show a construction of organizational signature schemes based on the ElGamal signature on the standard model.

Keywords
Organizational signature; public key cryptography; discrete logarithm problem

1. INTRODUCTION
Digital Signature is the cornerstone for all the electronic transaction in our today's world. Due to the dependency of the world trade on digital signatures, many additional properties are needed. The notion of organizational signature proposed in [1]. In this notion, it allows the organization to obtain the signature of its employee's not as individual but through his affiliation. This additional property can be provided in three different scenarios according to organizational needs. **First**, concatenated organizational signature combines the personal private key and the affiliation private key to get the new organizational private key that will be used to sign the organization's message and computes the corresponding public key so the verifier can make verification. The advantage of this scenario is that it is the most flexible scenario as we have one key used by the signer resulting in lower complexity and more flexibility for verifier. **Second**, encapsulated organizational signature is a scheme in which a signer signs the message first using the personal private key then the organization signs the signed message using the affiliation private key, so the verifier will use the affiliation public key then the personal public key to verify. The advantage of this scenario, which is the most secure scenario, as the organization center can verify the personal signature before it re-sign the signed message. In addition, the message cannot be sent without the organization's affiliation signature. Therefore, it will be more trustable for the verifier as he will be sure that this signature came from a position-holder in this organization. However, the organization makes verification before resign resulting in more efforts & complexity. **Finally**, appended organizational signature in which the message is signed twice independently by the signer and the organization. The signer signs the original message first using his personal key, then, after verifying the personal signature; the organization signs the original and not the signed message using the affiliation key. In addition, appends the affiliation signature to the personal one. Correspondingly, the verifier makes two independent verifications and accepts the message only when both verifications succeed.

There are many digital signature schemes with different properties in the literature according to needs. However, none of them fulfills the needs of organizational signature.

In [2], the notion of group signatures introduced by Chaum and van Heyst. A group member can generate a signature, which exposes nothing about the signer's identity except that he is a member of the group. On the other hand, group manager can detect the signer's identity. This cannot satisfy the needs of signing by the affiliation in an organization, because in the organization transactions, the signer's identity must be known for all verifier beside his affiliation in the organization.
Undeniable signature suggested by Chaum and van Antwerpen in [3]. In this notion, the signature can only be verified with the signer's consent. However, if a signature is only verifiable with the aid of a signer, a dishonest signer may refuse to authenticate a genuine document. Undeniable signatures solve this problem by adding a new component called the disavowal protocol in addition to the normal components of signature and verification.
Threshold signature [4] necessitates that allows any subset of k players out of l to generate a signature, but that cancels the creation of a legal signature if less than k players contribute in the scheme.
In proxy signature [5] allows a delegator to give partial signing rights to other parties called proxy signers. Proxy signatures do not offer Anonymity. In organizational transaction, the employee must have full signing rights.

Therefore, no digital signature notations can fulfill the needs of organizational work.

In 1984, T. ElGamal announced a public-key scheme based on discrete logarithms, closely related to the Diffie-Hellman technique [6, 7]. The ElGamal encryption scheme is designed to enable encryption by a user's public key with decryption by the user's private key. The ElGamal signature scheme involves the use of the private key for encryption and the public key for decryption. The ElGamal cryptosystem is used in some form in a number of standards, including the digital signature standard (DSS) and the S/MIME email standard.

Our contributions are proposing a new digital signature scheme with new properties fit for organizing work. In the

new notion, a signature holder can designate the signature to an organization with his affiliation. We present three schemes that fit into the digital signature algorithm [11] model based on ElGamal cryptosystem. We provide security properties proofs for our schemes.

The rest of this paper is organized as follows; the notations used in the paper presents in section 2, with the definition of DLP. Section 3 discusses the model of organizational signature and its security properties. Our proposed schemes present in section 4. Section 5 gives the security analysis of our schemes, and finally the conclusion.

2. PRELIMINARIES

2.1 Notations

Common notations used in this paper as follows.

- p: Prime number, presents the order of underlying finite filed.
- $H(\cdot)$: A secure one-way hash function. The hash value is an element of $\mathbb{Z}_p^*$.
- (x_i, y_i): The private/public key pair of i, where $x_i, y_i \in [1, p-1]$. i is either personal p,or affiliation a, or organizational o.

2.2 Discrete Logarithm Problem (DLP)

The basic problem of the presented schemes is the Discrete Logarithm problem. It describes that it is hard to compute the exponent given a power in a known multiplicative group. An instance of a DL Problem consists of the following:

- A multiplicative group $(G, .)$,
- A generator g of G and
- An element $x \in G$.

The question now is to find the unique integer a, $0 \leq a \leq n-1$ such that $g^a = x$. the a in this question can be seen as the $log_a x$, thus the search for the required exponent for g to retrieve x.

3. ORGANIZATIONAL SIGNATURE

3.1 Model of organizational signature

The schemes consist of singing key generation, organizational signature generation, and organizational signature verification [1].

The participant involve in these schemes are:

- An organization key-generation center**,** it is responsible for generating the affiliation key and uses this key to sign the message with the signer if needed and verify the personal part. Therefore, it must have a database containing all organization affiliation keys and all revoked signer key.
- A signer, who occupies the position now and he has only his personal key.
- A verifier, who verifies the organizational signature and decides to accept or reject.

3.2 Security properties

The security properties for a secure organizational signature scheme are as follows

- **Transferability:** the transfer of the position in organization from one employee to another with the ability to get signature related to each employee and can transfer the signature to the new employee and revoke the previous signature.
- **Organizational Signature:** anyone can check that the signature was formed by the organization.
- **Unforgeability:** only the original signer can create a valid organizational signature related to his affiliation.
- **Distinguishability:** Valid personal signatures are distinguishable from valid affiliation signatures in polynomial time or size computation.
- **Undeniability:** Once a personal signer creates a valid organizational signature related to his position, he can't deny his signature as the signature depends on his personal key that only known by him.
- **Linkability:** the affiliation part must be linkable, as any one must be able to relate the signature to the different position in the organization. The personal part must be unlinkable as it depends on the secret of the person. The verifier can relate the signature to the position as it has its public information, but it is not important to link the signature to specific signer as the verifier trust the organization.
- **Verifiability:** verifiability means that any verifier who hold the related public parameters can check whether organizational signature is valid and can be confirmed that the signature is generated according to the signature of the original signer if the signature is valid.

4. PROPOSED SCHEMES

In this section, we will introduce three different schemes based on the scenarios of organizational signature presented in the introduction. We assume that each signer has a personal key pair (x_p, y_p), and all the suggested schemes have a common initialization phase.

Initialization phase: the organization generation center selects random number $x_a \in [1, p-1]$, which will be the affiliation private key. It computes the public key as $y_a = g^{x_a} \ mod \ p$ and publish g, y_a. and secure one-way hash function $H(\cdot)$.

4.1 Concatenated Organizational Signature Scheme

Organization key pair generation. In this phase, both of the organization center and the employee send the affiliation and personal's private key in a secure manner to a trusted third party to compute the organizational key pair.

The trusted third party

- Selects random number $a \in [1, p-1]$.
- Computes $x_o = a \cdot (x_p + x_a) \ (mod \ p)$, which will be the organization private key.
- Computes the organization pubic key as $y_o = g^{x_o} \ mod \ p$
- Publishes y_o, and sends x_o in secure manner to the employee (signer).

Organization signature generation. In this phase, the employee generates a signature (m, α, β) for message m.

- Selects random number $k \in [1, p-1]$.
- Computes $\alpha = g^k \bmod p$.
- Computes k^{-1} the inverse of $k \bmod (p-1)$.
- Computes $\beta = k^{-1}.[H(m) - x_o.\alpha] \bmod (p-1)$.

Signature verification. Any person can verifies the validity of the signature by the following steps.

- Computes $V_1 = g^{H(m)} \bmod p$.
- Computes $V_2 = {y_o}^{\alpha}.\alpha^{\beta} \bmod p$.
- Accepts if $V_1 = V_2$, else reject.

4.2 Encapsulated organizational signature scheme

Registration. Here the employee must authenticate himself first to the organization key generation center (signer).

For a message m, the employee

- Selects random number $k \in [1, p-1]$.
- Computes $\alpha = g^k \bmod p$.
- Computes k^{-1} the inverse of $k \bmod (p-1)$.
- Computes $\beta = k^{-1}.[H(m) - x_p.\alpha] \bmod (p-1)$.
- Sends (m, α, β) to the organization key generation center.

The organization key generation center checks the validity of employee signatures by

- Computes $V_1 = g^{H(m)} \bmod p$.
- Computes $V_2 = {y_p}^{\alpha}.\alpha^{\beta} \bmod p$.
- Accepts if $V_1 = V_2$, else reject.

Organization signature generation. In this phase, the organization key generation center generates a signature $(m, \alpha, \sigma, \beta)$ for message m.

- Computes $\sigma = k^{-1}.[H(\beta) - x_a.\alpha] \bmod (p-1)$.
- Sends $(m, \alpha, \sigma, \beta)$ to the organization client.

Signature verification. The client organization can verify the validity of the signature by the following steps.

- Computes $V_1 = g^{H(\beta)} \bmod p$.
- Computes $V_2 = {y_o}^{\alpha}.\alpha^{\sigma} \bmod p$.
- Computes $V_3 = g^{H(m)} \bmod p$.
- Computes $V_4 = {y_p}^{\alpha}.\alpha^{\beta} \bmod p$.
- Accepts if $V_1 = V_2$ & $V_3 = V_4$, else reject.

4.3 Appended organizational signature scheme

Registration. Here the employee must authenticate himself first to the organization key generation center (signer).

For a message$m$, the employee

- Selects random number $k \in [1, p-1]$.
- Computes $\alpha = g^k \bmod p$.
- Computes k^{-1} the inverse of $k \bmod (p-1)$.
- Computes $\beta = k^{-1}.[H(m) - x_p.\alpha] \bmod (p-1)$.
- Sends (m, α, β) to the organization key generation center.

The organization key generation center checks the validity of employee signatures by

- Computes $V_1 = g^{H(m)} \bmod p$.
- Computes $V_2 = {y_p}^{\alpha}.\alpha^{\beta} \bmod p$.
- Accepts if $V_1 = V_2$, else reject.

Organization signature generation. In this phase, the organization key generation center generates a signature (m, γ, σ) for message m.

- Selects random number $k \in [1, p-1]$.
- Computes $\gamma = g^k \bmod p$.
- Computes k^{-1} the inverse of $k \bmod (p-1)$.
- Computes $\sigma = k^{-1}.[H(m) - x_a.\alpha] \bmod (p-1)$.
- Sends $(m, \alpha, \beta, \gamma, \sigma)$ to the organization client.

Signature verification. The organization client can verifies the validity of the signature by the following steps.

- Computes $V_1 = g^{H(m)} \bmod p$.
- Computes $V_2 = {y_p}^{\alpha}.\alpha^{\beta} \bmod p$.
- Accepts if $V_1 = V_2$, else reject.
- Computes $V_3 = g^{H(m)} \bmod p$.
- Computes $V_4 = {y_a}^{\gamma}.\gamma^{\sigma} \bmod p$.
- Accepts if $V_3 = V_4$, else reject.

5. SECURITY ANALYSIS

Let us discuss the security of the proposed scheme. The security of the proposed schemes depends on the difficulty of breaking the one-way hash function and the discrete logarithm problem (DLP).

Theorem 1. (Transferability) *The organization can easily transfer the signature from one employee to another.*

Proof. As the person private of the employee $x_p$is a part of the signature, $\beta = k^{-1}.[H(m) - x_p.\alpha] \bmod (p-1)$ so if the employee leaves his position the new signature will depend on the new employee private key so it is easy to transfer the affiliation from employee to another by changing the personal part.

Theorem 2. (Organizational signature) *It is clear that the signature depends on the affiliation of the employee.*

Proof. As the signature includes the affiliation private key for each affiliation, $\sigma = k^{-1}.[H(m) - x_a.\alpha] \bmod (p-1)$, so it must be done by the organization.

Theorem 3. (Distinguishability) Anyone *can easily distinguish the organizational signature from the normal signature.*

Proof: Affiliation private key is different from the employee's private key and organization key created by trusted third party are different from each other, any organizational signature is distinguishable from original employee's signature.

The organizational signature $x_o = a \cdot (x_p + x_a)\ (mod\ p)$, contains the x_o organization private key that computed from both affiliation and personal private keys.

Theorem 4. (Undeniability) *The proposed schemes provide a non-repudiation for any signature.*

Proof. Neither the organization, nor the employee can deny his signature part of the organization's signature as each of them uses his own private x_p for the employee and x_a for the affiliation within the organization.

Theorem 5. (Linkability) *The proposed schemes provide signature linkable property.*

Proof. We can link the signature to the organization due to its public key y_o as in concatenated signature or due to the affiliation public key y_a as in appended and encapsulated signature and no need to relate or link the signature to the person as the organization is responsible for verifying the personal part.

6. CONCLUSION

In this paper, an organizational signature scheme based on ElGamal signature was proposed. It satisfies the security properties of organizational signature scheme. The security of the proposed schemes depend on the difficulty of breach the one-way hash function and the discrete logarithm problem (DLP).

7. REFERENCES

[1] Allam, A. M., Ali, I. A., and Mahgoub, S. M., "A provably secure certificateless organizational signature schemes," International Journal Communication System, 2015. DOI: 10.1002/dac.3038.

[2] Chaum, and van Heyst, "Group signatures," Advances in Cryptology — EUROCRYPT ’91, Lecture Notes in Computer Science 547, pp. 257–265, 1991.

[3] David Chaum, and Hans van Antwerpen, "Undeniable Signatures," Crypto'89, LNCS 435, Springer-Verlag, pp. 212-216, Berlin 1990.

[4] Wang, Kerui, Qiuliang Xu, and Guoyan Zhang. "A Secure Threshold Signature Scheme from Lattices." Computational Intelligence and Security (CIS), 2013 9th International Conference on. IEEE, Dec. 2013.

[5] Limin Sha. "Analysis of an ID-based proxy signature scheme without trusted PKG and a proxy blind multi-signature scheme." Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2014 15th IEEE/ACIS International Conference on. IEEE, July 2014.

[6] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, vol.IT-31, pp. 469-472, 1985.

[7] Diffie, W.; Hellman, M.E., "New directions in cryptography," in Information Theory, IEEE Transactions on , vol.22, no.6, pp.644-654, Nov 1976.

[8] Hung-Zih Liao, and Yuan-Yuan Shen, "On the Elliptic Curve Digital Signature Algorithm," Tunghai Science Vol.8, pp. 109-126, July 2006.

[9] F. Vercauteren, "Elliptic Curve Discrete Logarithm Problem", [Online], Kotholieke Universiteit Leuven, 2005,Available:http://homes.esat.kuleuven.be/~fvercaut/talks/ECDL.pdf.

[10] J. Kar, "Proxy Blind Multi-signature Scheme using ECC for handheld devices," Available at “International Association for Cryptology Research”, http://eprint.iacr.org/2011/043.pdf, 2011.

[11] A. Menezes, P. C Van Oorschot and S. A Vanstone Handbook of applied cryptography. CRC Press, 1997.

[12] B. Yu, "Establishment of elliptic curve cryptosystem," IEEE International Conference on Information Theory and Information Security (ICITIS), pp. 1165–1167, December 2010.

[13] S. K. Nayak, B. Majhi, and S. Mohanty, ”An ECDLP based untraceable blind signature scheme,” Second IEEE International Conference on Circuits, Power and Computing Technologies (ICCPCT), pp. 829 - 834, 20-21 March 2013.