An Efficient Organizational Signature Schemes based on the Elliptic Curve Cryptography

Shereen M. Mahgoub
Engineer
Arab Radio and TV Union,
Cairo, Egypt

Ali M. Allam
Assistant Professor
Communication Engineering
Department, Helwan University

Ihab Abdel-Wahab Ali
Professor
Communication Engineering
Department, Helwan University

ABSTRACT

We introduce the notation of organizational signature. This is a new variant of digital signature, which allows the organization to obtain the signature of any employee not as an individual but through his affiliation. Due to this signature, an organization, e.g. company, can create different signatures related to each position. Elliptic curves discrete logarithm problem (ECDLP) has a low computational cost and small key size, comparing with the factorization problem of RSA. In this paper, we introduce the notion of organizational signature schemes; show a construction of organizational signature schemes based on Elliptic Curve Cryptography (ECC) in the standard model.

Keywords

Elliptic curve cryptography; organizational signature; public key cryptography; discrete logarithm problem

1. INTRODUCTION

Digital Signature is the cornerstone for all the electronic transaction in our today 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 organization 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 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 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 is 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 for organization work.

Koblitz [6] and Miller [7] have independently proposed using the group of points on an elliptic curve defined over a finite field in discrete logarithm cryptosystems. Today, elliptic curves are widely used in public key cryptosystems. Elliptic curve cryptography (ECC) makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field. Typically, elliptic curves are defined over either the integers modulo a prime number $GF(p)$ or over binary polynomials $GF(2^m)$. The digital signature algorithm (DSA) was proposed in August 1991 by the U.S. National Institute of Standards and Technology (NIST) and became a U.S. Federal Information Processing Standard (FIPS 186) in 1993. It was the first digital signature scheme to be accepted as legal binding by a government.

Most digital signature schemes are based on the public key system of RSA and El-Gamal. The security of RSA-type signature scheme [8] is based on factoring; the El-Gamal-type signature scheme [9] is based on the discrete logarithm problem over the finite field $GF(p)$. However, the length of the RSA signature is too long and the verification of the El-Gamal signature requires too much computations. ECC can be viewed as elliptic curve analogues of the older discrete logarithm (DL) cryptosystems in which the subgroup of $\mathbb{Z}_p$is replaced by the group of points on an elliptic curve over a finite field. The mathematical basis for the security of elliptic curve cryptosystems [10] is the computational intractability of the elliptic curve discrete logarithm problem (ECDLP). The primary reason for the attractiveness of ECC over systems such as RSA and DSA is that the best algorithm known for solving the underlying mathematical problem namely, the ECDLP takes fully exponential time. In contrast, sub-exponential time algorithms are known for underlying mathematical problems on which RSA and DSA are based, namely the integer factorization problem and the discrete logarithm problems. This means that the algorithms for solving the ECDLP become infeasible much more rapidly as the problem size increases more than those algorithms for the IFP and DLP. For this reason, ECC offers security equivalent to RSA and DSA while using far smaller key sizes.

Our contributions are to propose a new digital signature scheme with new properties fit for organization 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 digital signature algorithm [11] model based on elliptic curve 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 algebraic properties of ECC. Section 3 discusses the model of organizational signature and its security properties. Our proposed schemes presents 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.
- $\mathbb{F}_p$: The underlying finite field of order p.
- E: Elliptic curve defined on finite field $\mathbb{F}_p$ with large order.
- G: A point in $E(\mathbb{F}_p)$ with order n, where n is a large prime number.
- $H(\cdot)$: 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 $x_i \in [1, n-1]$and $Y_i = x_i \cdot G$, i is either personal p,or affiliation a, or organizational o.
- ||: Concatenation operation between two bit strings.

2.2 Elliptic Curve over $\mathbb{F}_p$

In this section, we recall the additive operation on points belonging to an elliptic curve $(\mathbb{F}_p)$. For more details, we refer the reader to [12, 13].

Let $p \geq 3$ be a prime number. Let $a, b \in \mathbb{F}_p$ be such that $4a^3 + 27b^2 \neq 0$ in $\mathbb{F}_p$. An elliptic curve E over $\mathbb{F}_p$ defined by the parameters a and b is the set of all solutions $(x, y) \forall x, y \in \mathbb{F}_p$, to the equation $y^2 = x^3 + ax + b$, together with an extra point $\mathcal{O}$, the point at infinity. The set of points $E(\mathbb{F}_p)$ forms an Abelian group with the following addition rules [14]:

1. Identity: $P + \mathcal{O} = \mathcal{O} + P, \forall P \in E(\mathbb{F}_p)$.
2. Negative: if $P(x, y) \in E(\mathbb{F}_p)$ then $(x, y) + (x, -y) = \mathcal{O}$. The point $(x, -y)$ is denoted as $-P$ called negative of P.
3. Point addition: Let $P(x_1, y_1), Q(x_2, y_2) \in E(\mathbb{F}_p)$,then $P + Q = R \in E(\mathbb{F}_p)$ with co-ordinate (x_3, y_3) is given by $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$ where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$.
4. Point doubling: Let $P(x_1, y_1) \in E(\mathbb{F}_p)$, where $P \neq -P$, then $2P = (x_3, y_3)$ where, $x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$ and $y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 (x_1 - x_3) - y_1$.

Definition 1 [15]**. Elliptic Curve DISCRETE Logarithm Problem (ECDLP)** Given an elliptic curve E over a finite field $\mathbb{F}_p$, a point $P(x, y) \in E(\mathbb{F}_p)$ of order n, and a point Q, find the integer $l \in [0, n-1]$ such that $Q = l \cdot P$, the integer l is called discrete logarithm of Q to base P.

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 has 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:** any one 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 mean 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 [1]. 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 $x_a \in [1, n-1]$, which will be the affiliation private key. It computes the public key as $Y_a = x_a G$ and publishes 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 private key in a secure manner to a trust third party to compute the organizational key pair.

The trusted third party

- Selects random number $a \in [1, n-1]$.
- Computes $x_o = a \cdot (x_p + x_a)\ (mod\ p)$, which will be the organization private key.
- Computes the organization pubic key as $Y_o = x_o G$.
- 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, s, R) for message m.

- Selects random number $k \in [1, n-1]$.
- Computes $s = (k + x_o \cdot H(m))(mod\ p)$.
- Computes $R = kG$.

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

- Computes $V_1 = sG$.
- Computes $V_2 = R + H(m) \cdot Y_o$.
- 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 $k \in [1, n-1]$.
- Computes $s_p = \left(k + x_p \cdot H(m)\right) (mod\ p)$.
- Computes $R = kG$.
- Sends (m, s_p, R) to the organization key generation center.

The organization key generation center check the validity of employee signature by

- Computes $V_1 = s_p G$.
- Computes $V_2 = R + H(m) \cdot Y_p$.
- Accepts if $V_1 = V_2$, else reject.

Organization signature generation. In this phase, the organization key generation center generates a signature $(m, s_o, s_p, \acute{R})$ for message m.

- Selects random number $\acute{k} \in [1, n-1]$.
- Computes $s_o = \left(\acute{k} + x_a \cdot H(m \parallel s_p)\right) (mod\ p)$.
- Computes $\acute{R} = \acute{k}G$.

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

- Computes $V_3 = s_o G$.
- Computes $V_4 = \acute{R} + H(m \cdot s_p) \cdot Y_a$.

Accepts if $V_3 = V_4$, 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 $k \in [1, n-1]$.
- Computes $s_p = \left(k + x_p \cdot H(m)\right) (mod\ p)$.
- Computes $R = kG$.
- Sends (m, s_p, R) to the organization key generation center.

The organization key generation center check the validity of employee signature by

- Computes $V_1 = s_p G$.
- Computes $V_2 = R + H(m) \cdot Y_p$.
- Accepts if $V_1 = V_2$, else reject.

Organization signature generation. In this phase, the organization key generation center generates a signature $(m, s_a, \acute{R})$ for message m.

- Selects random number $\acute{k} \in [1, n-1]$.
- Computes $s_a = \left(\acute{k} + x_a \cdot H(m)\right) (mod\ p)$.
- Computes $\acute{R} = \acute{k}G$.

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

- Computes $V_3 = s_a G$.
- Computes $V_4 = \acute{R} + H(m) \cdot Y_a$.

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 depend on the difficulty of breach the one-way hash function and the elliptic curve discrete logarithm problem (ECDLP).

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, $s_p = \left(k + x_p \cdot H(m)\right)$, 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 include the affiliation private key for each affiliation, $s_a = \left(\acute{k} + x_a \cdot H(m)\right)$, 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 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 $s = \left(k + x_o \cdot H(m)\right)$ 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 in the organization 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 efficient organizational signature schemes based on ECC 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 elliptic curve discrete logarithm problem (ECDLP). The desirability of ECC will growth relative to other public-key cryptosystems as computing power improvements potency a general increase in the key size. The benefits of this higher-strength per-bit include higher speeds, lower power consumption, bandwidth savings, storage efficiencies, and smaller certificates. Therefore, these schemes can be designed for low computational power devices with small memory size.

7. REFERENCES

[1] Ihab A. Ali, Shereen M. Mahgoub, and Ali M. Allam, "A New direction in Digital Signature Systems: Organizational signature" International Journal of Computer Information Systems, Vol. 3, No. 4, 2011.

[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] N. Koblitz. "Elliptic curve cryptosystems." Mathematics of Computation, vol. 48, no. 177, pp. 203-209, 1987.

[7] V. Miller. "Uses of elliptic curves in Cryptography." Advances in Cryptology-CRYPTO 85, Proceedings, Lecture Notes in Computer Science, No 218, pp. 417-426, Springer-Verlag, 1985.

[8] R. Y. Y. Cao and C. Fu, "An efficient implementation of RSA digital signature algorithm," Intelligent Computation Technology and Automation (ICICTA), 2008.

[9] 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.

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

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

[12] 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.

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

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

[15] 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.