The ISC Int'l Journal of Information Security

ISeCure

July 2009, Volume 1, Number 2 (pp. 125–131)

http://www.isecure-journal.org

An Efficient Blind Signature Scheme Based on the Elliptic Curve Discrete Logarithm Problem

Morteza Nikooghadam [a], Ali Zakerolhosseini [a,*]

[a] *Department of Electrical and Computer Engineering, Shahid Beheshti University, Tehran, Iran*

ARTICLE INFO.

Article history:
Received: 14 November 2008
Revised: 12 July 2009
Accepted: 18 July 2009
Published Online: 25 July 2009

Keywords:
Blind signature, Elliptic Curves Cryptosystems, Untraceability, Blindness

ABSTRACT

Elliptic Curve Cryptosystems (ECC) have recently received significant attention by researchers due to their high performance such as low computational cost and small key size. In this paper a novel untraceable blind signature scheme is presented. Since the security of proposed method is based on difficulty of solving discrete logarithm over an elliptic curve, performance of the proposed scheme is quite commendable in comparison with the previous work in terms of security and time complexity.

1 Introduction

The notion of blind signatures was introduced by Chaum in 1982 [1]. There are two properties which any blind signature scheme must satisfy: Blindness and Untraceability [1–3]. *Blindness* means the content of a message should be blind to the signer. *Untraceability* is satisfied if, whenever a blind signature is revealed to the public, the signer will be unable to know who the owner of the signature is. The principle behind the blind signature can be illustrated by a simple example. Assume we put a carbon paper along with a letter inside an envelope. Then any signature on the envelope will also appear on the letter inside [4].

In this paper, a novel blind signature scheme based on the Elliptic Curve Discrete Logarithm Problem (ECDLP) is presented that is more efficient than other schemes presented based on the DLP. Since ECDLP is significantly more difficult than the integer factorization problem or the discrete logarithm problem [5], to satisfy the security requirements, the Elliptic Curve Cryptosystems (ECC) need a smaller key size compared to other cryptosystems [6]. Obviously, this means ECC has the advantages of higher speed, lower power consumption, and code size reduction.

The remainder of the paper is organized as follows: Section 2 investigates the related work. Section 3 briefly reviews some background information. In Section 4, the proposed blind signature scheme is presented. Section 5 analyzes the security of the proposed scheme. The performance of this scheme is examined in Section 6. Finally, conclusions are presented in Section 7.

2 Related Work

Nowadays, the blind signatures are widely adopted for building the infrastructures of many advanced communication services, such as anonymous electronic voting or electronic cash systems [3, 7, 8]. To guarantee the quality of these cryptographic services, several blind signature schemes are proposed in the literature. In 1995, Camenisch *et al.* [9] proposed a novel blind signature scheme based on the Discrete Logarithm Problem (DLP). Later, Harn [2] claimed that the blind signature in [9] is traceable by the signer. However, Horster *et al.* [10] illustrated that the signer cannot trace back to the owner of the signature. In-

* Corresponding author.
Email addresses: m_nikooghadam@sbu.ac.ir (M. Nikooghadam), a-zaker@sbu.ac.ir (A. Zakerolhosseini).
ISSN: 2008-2045

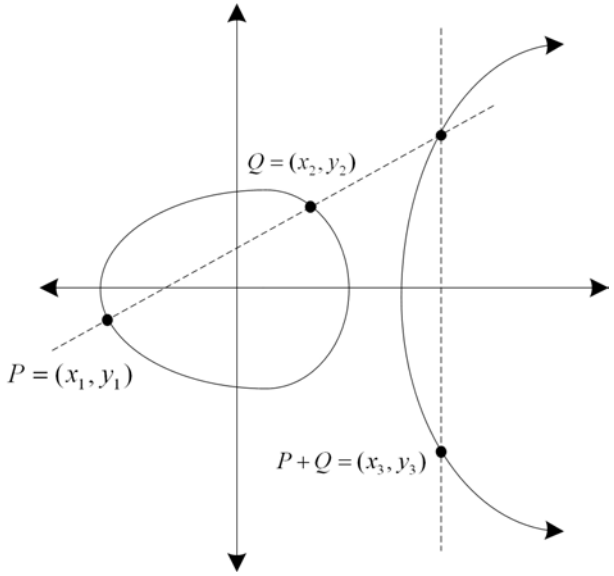

Figure 1. Addition on Elliptic Curves

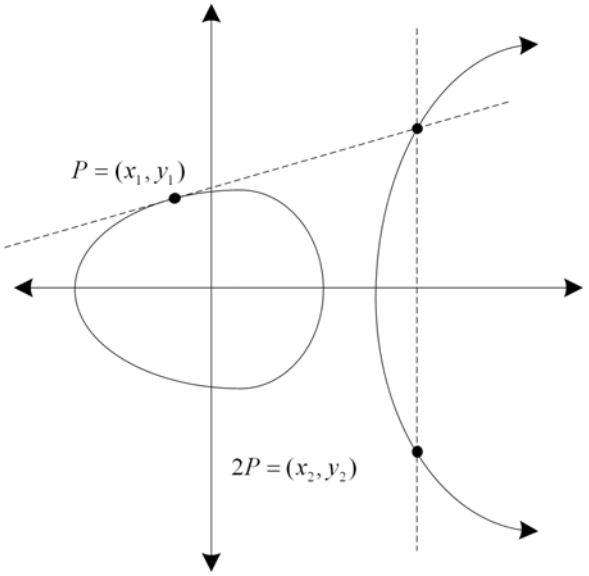

Figure 2. Doubling a Point

spired by cryptanalysis techniques in [2], Lee *et al.* [3] illustrated that the Camenisch *et al.*'s scheme does not satisfy the untraceability. To overcome this weakness, they proposed a new blind signature scheme based on the DLP. Finally, in 2005, Wu and Wang [7] proved the untraceability of the Camenisch *et al.*'s scheme. They also claimed that Lee *et al.*'s scheme is untraceable; but their proof of its untraceability is wrong. They corrected the proof of Lee *et al.* untraceability and concluded that Camenisch *et al.*'s scheme is still more efficient than Lee *et al.* Later, Jena *et al.* [8, 11] proposed two novel blind signature schemes; nevertheless there was no reasonable proof for correctness of their schemes. Since their work, especially [11], includes many mistakes (not only in the proposed scheme but even in the expression), it is uncommon to refer to them in the blind signature context. Recently Fan *et al.* [12] devised an attack on [3] and [7] schemes such that a signature requester, by performing only one round of protocol, can obtain more than one valid signature. They conclude that, a secure and novel blind signature scheme is urgently required in this field. The proposed scheme in this paper is the first work based on elliptic curve cryptosystems, which we hope fills the gap.

3 Mathematical Background of the Elliptic Curve Cryptosystems

Utilizing elliptic curves in cryptography was first suggested by Miller [13] and Koblitz [14]. Let $\mathbf{GF}(2^m)$ be a finite field of 2^m elements, where m is an integer. An elliptic curve over $\mathbf{GF}(2^m)$ is defined as [15]:

$$y^2 + xy = x^3 + a_1x^2 + a_2 \quad (1)$$
$$\text{with } a_1, a_2 \in \mathbf{GF}(2^m), a_2 \neq 0$$

An elliptic curve over $\mathbf{GF}(2^m)$ consists of all points (x, y) where $x, y \in \mathbf{GF}(2^m)$ such that it satisfies Equation (1) together with the point at infinity $\mathbf{O}$. The addition of two points and doubling a point on this elliptic curve in a geometrical space, are illustrated in figures 1 and 2, respectively.

Considering an elliptic curve C on $\mathbf{GF}(2^m)$, the addition of points follows specific rules indicated below [15]:

(1) $\mathbf{O} + \mathbf{O} = \mathbf{O}$
(2) $\mathbf{P} + \mathbf{O} = \mathbf{P}$ for all values of $\mathbf{P} = (x, y) \in C$. Namely, C has $\mathbf{O}$ as its identity element.
(3) $\mathbf{P} + \mathbf{Q} = \mathbf{O}$ for all values of $\mathbf{P} = (x, y) \in C$ and $\mathbf{Q} = (x, -x - y) \in C$. In other words, the inverse of (x, y) is simply $(x, -x - y)$.
(4) Adding two distinct points:
For all $\mathbf{P} = (x_1, y_1) \in C$ and $\mathbf{Q} = (x_2, y_2) \in C$ with $x_1 \neq x_2$, $\mathbf{P} + \mathbf{Q} = (x_3, y_3)$ is defined as:

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$$
$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1 \quad \text{where } \lambda = \frac{y_2 + y_1}{x_2 + x_1}$$

(5) Doubling a point:
For any $\mathbf{P} = (x_1, y_1) \in C$ with $y_1 \neq 0$, $2\mathbf{P} = (x_2, y_2)$ is defined as:

$$x_2 = \lambda^2 + \lambda + a$$
$$y_2 = \lambda(x_1 + x_2) + x_2 + y_1 \quad \text{where } \lambda = x_1 + \frac{x_1}{y_1}$$

The *scalar multiplication* is a fundamental operation in ECCs. The operation is simply the addition

of a point $\mathbf{P}$ to itself for k times (k is an m-bit long scalar) [15, 16]:

$$\mathbf{Q} = k\mathbf{P} = \underbrace{\mathbf{P} + \mathbf{P} + \cdots + \mathbf{P}}_{k} \tag{2}$$

Regarding the algorithm in [17] for the calculation of scalar multiplication, it does not require k to be less than n (i.e. $1 \leq k \leq n-1$) where n is the order of $\mathbf{P}$. Even if $k > n$, the value of k is replaced by $k \pmod{n}$ at the initial stage of the algorithm.

Let $\mathbf{P}$ and $\mathbf{Q}$ be two points on an elliptic curve, whose order is a prime number n. Consider the equation $\mathbf{Q} = k\mathbf{P}$. Given the points $\mathbf{P}$ and $\mathbf{Q}$, determining the value of k is computationally infeasible. This is called the *Elliptic Curve Discrete Logarithm Problem* (ECDLP) [16].

4 The Proposed Scheme

In the proposed blind signature scheme there are two kinds of participants: a **signer**, and a group of users called, **requesters**. A user requests signatures from the signer, and the signer computes and issues blind signatures to the user. The proposed scheme consists of five steps: (1) initialization, (2) request, (3) signature generation, (4) extraction, and (5) verification. The signer publishes the necessary information in the initialization step. To obtain the signature of a message, the user submits a blinded version of the message to the signer in the *request phase*. In the *signature generation phase*, the signer signs the blinded message, and sends the result back to the user. Afterwards, the user extracts the signature in the *extraction phase*. During the *verification phase*, the validity of the declared signature is verified. The details of these phases are described below.

(1) **Initialization:** The signer determines a field size q which defines the underlying finite field F_q, where either $q = p$ in case that p is an odd prime, or $q = 2^m$ when q is a prime power. Regarding the proposed scheme, $q = 2^m$ is chosen as the underlying finite field in all calculations and also to the equations. The elements of $\mathbf{GF}(2^m)$ are represented by bit strings of length m. Therefore, elements of $\mathbf{GF}(2^m)$ can be represented by non-negative integers $0, 1, 2, \ldots, 2^m - 1$.

The signer specifies an appropriate elliptic curve (E) by selecting two parameters a_1 and a_2 of the elliptic curve of Equation 1 over F_q. Then, the base point $\mathbf{G}$ is determined, that is a finite point on elliptic curve having the largest order n such that $n\mathbf{G} = \mathbf{O}$, where $\mathbf{O}$ indicates the point at infinity. He makes the values $E(F_q)$, $\mathbf{G}$ and n public. Moreover, the signer selects a random integer d that should be an element of $\mathbf{GF}(2^m)$ as the private key and computes $\mathbf{Q} = d\mathbf{G}$. The point Q is declared as a public key. Note that as it is mentioned previously, it is not necessary for d to be in $\{1, 2, \ldots, n-1\}$.

(2) **Request:** For each user request, the signer selects a random integer $k \in \mathbf{GF}(2^m)$. It then keeps the value of k secret and computes the point $\mathbf{R} = k\mathbf{G}$. The signer then sends back the point R to the user. Afterwards, the requester randomly selects three blinding factors a, b and c all of which are $\mathbf{GF}(2^m)$ elements. As demonstrated previously, we emphasize that it is not required for the elements to be in $\{1, 2, \ldots, n-1\}$. Finally, the requester computes the point $\mathbf{F}$ having coordinates (x_0, y_0) as follows (the underlying finite field is $\mathbf{GF}(2^m)$):

$$\begin{aligned} \mathbf{F} &= b^{-1}\mathbf{R} + ab^{-1}\mathbf{Q} + c\mathbf{G} \\ &= b^{-1}(k\mathbf{G}) + ab^{-1}(d\mathbf{G}) + c\mathbf{G} \\ &= (b^{-1}k + ab^{-1}d + c)\mathbf{G} \end{aligned} \tag{3}$$

Note that b^{-1} indicates the inversion in the finite field, which is one of the required operations in elliptic curve digital signature algorithm [17]. An efficient execution procedure of this operation is presented in [17]. If $\mathbf{F}$ is equal to $\mathbf{O}$, the requester has to reselect the blinding factors a, b and c, and then recalculate $\mathbf{F}$ from Equation (3) above.

Assuming $r = x_0 \pmod{n}$, the requester determines the blinded message, $\hat{m}$, from the original message, m, on $\mathbf{GF}(2^m)$ as $\hat{m} = br(m) + a$, and transmits $\hat{m}$ to the signer.

(3) **Signature generation:** The signer computes the blind signature $\hat{s}$ as, $\hat{s} = d(\hat{m}) + k$ on $\mathbf{GF}(2^m)$ and forwards it to the requester.

(4) **Extraction:** After receiving $\hat{s}$ the requester computes $s = b^{-1}(\hat{s}) + c$ on $\mathbf{GF}(2^m)$. Finally, the requester declares the tuple $(s, \mathbf{F})$ as the signature of the message m.

(5) **Verification:** The validity of the signature $(s, \mathbf{F})$ for a message m is verified by examining the correctness of the equation $s\mathbf{G} = rm\mathbf{Q} + \mathbf{F}$ on $\mathbf{GF}(2^m)$ using Equation (4).

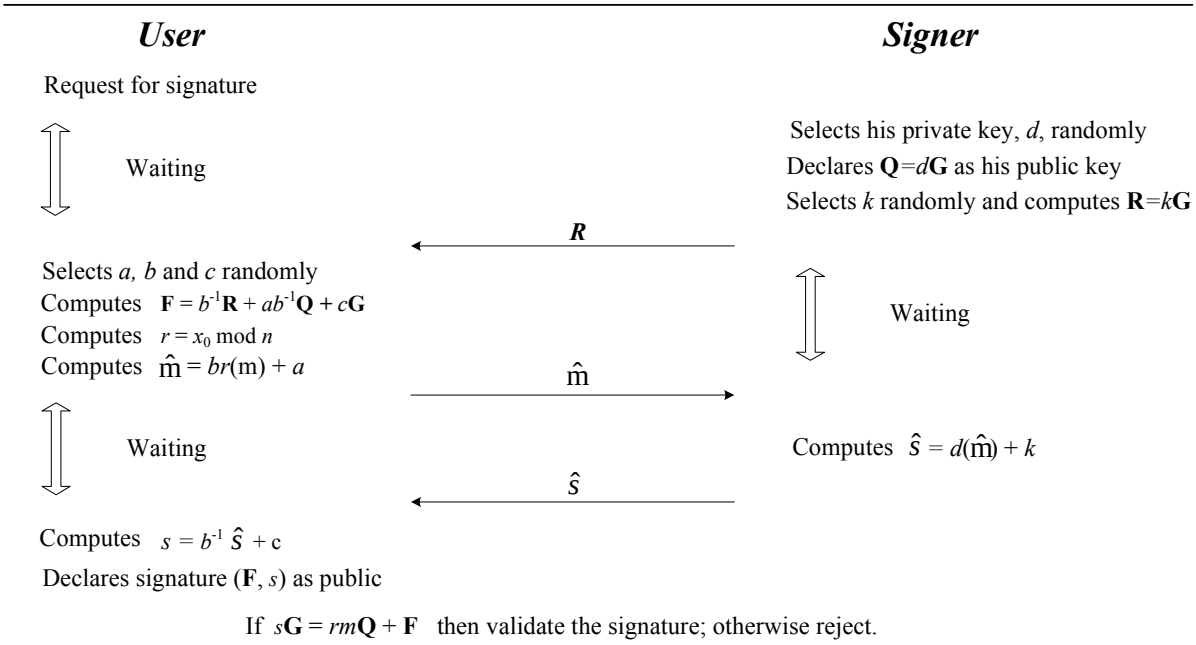

Figure 3. The Proposed Blind Signature Scheme

$$\begin{aligned} s\mathbf{G} &= \left(b^{-1}(\hat{s})+c\right)\mathbf{G} \\ &= \left(b^{-1}\left(d\left(\hat{m}\right)+k\right)+c\right)\mathbf{G} \\ &= \left(b^{-1}\left(d\left(brm+a\right)+k\right)+c\right)\mathbf{G} \\ &= (drm+b^{-1}da+b^{-1}k+c)\mathbf{G} \\ &= (drm)\mathbf{G}+(b^{-1}da+b^{-1}k+c)\mathbf{G} \\ &= rm(d\mathbf{G})+(b^{-1}(k\mathbf{G})+ab^{-1}(d\mathbf{G})+c\mathbf{G}) \\ &= rm\mathbf{Q}+(b^{-1}\mathbf{R}+ab^{-1}\mathbf{Q}+c\mathbf{G}) \\ &= rm\mathbf{Q}+\mathbf{F} \end{aligned} \tag{4}$$

The various phases of the proposed scheme are summarized in Figure 3.

5 The Security of the Proposed Scheme

The security of the proposed method is based on the difficulty of solving the discrete logarithm problem over an elliptic curve, and the security resulted from such problems is still sufficient under reasonable computational complexity [5, 18]. No one can forge a valid signature pair $(s, \mathbf{F})$ on the message m in order to satisfy $s\mathbf{G} = rm\mathbf{Q}+\mathbf{F}$ for the verification. The unforgeability proof demonstrated below is similar to proxy blind signature proof presented in [19].

Proof of Security: Assume a forged signature for an altered message m^* is $(s^*, \mathbf{F}^*)$. The attacker must choose s^* and $\mathbf{F}^*$ in order to satisfy Equation (5) for the verification, where r^* is the x-coordinate of $\mathbf{F}^*$.

$$s^*\mathbf{G} = r^*m^*\mathbf{Q}+\mathbf{F}^* \tag{5}$$

If the attacker chooses the point $\mathbf{F}^*$ in Equation (5) first, and then tries to calculate s^*, as r^*, m^*, $\mathbf{F}^*$ and $\mathbf{Q}$ are all available to the forger, then, the forger has the value of the point $s^*\mathbf{G}$. However, to obtain s^*, he is faced with an instance of the ECDLP and this makes determining s^* value infeasible.

On the other hand, if the attacker chooses s^* and tries to calculate $\mathbf{F}^*$, he must solve Equation (6), which is another form of Equation (5). There is no feasible solution to this equation. Since $\mathbf{F}^*$ is unknown, its x-coordinate r^* is unknown as well, resulting in the $r^*m^*\mathbf{Q}$ point to be unavailable to the forger. Therefore, the left-hand side of Equation (6) cannot be computed and stays unknown.

$$s^*\mathbf{G}-r^*m^*\mathbf{Q} = \mathbf{F}^* \tag{6}$$

From the above discussion, determining the value of $\mathbf{F}^*$ is not feasible. ■

In addition, our scheme prevents the signer from tracing the blind signature, which is demonstrated as follows. The outline is similar to *untraceability* proof of blind signature schemes presented in [7].

Proof of Untraceability: The signer will keep a set of records $(k, \mathbf{R}, \hat{m}, \hat{s})$ for each blind signature requested. When the message m and its signature $(s, \mathbf{F})$ are revealed to the public, the signer searches through

Table 1. Definition of Given Notations

Notation	Definition
T_{MUL}	Time complexity for the execution of a multiplication
T_{EXP}	Time complexity for the execution of a exponentiation
T_{ADD}	Time complexity for the execution of an addition
T_{EC_MUL}	Time complexity for the execution of a multiplication in an elliptic curve point
T_{EC_ADD}	Time complexity for the execution of an addition of two points in an elliptic curve
T_{inv}	Time complexity for the execution of a inversion

all sets of records. By employing these records and the revealed message-signature pair $(m, s, \mathbf{F})$, the signer tries to check the correctness of Equation (7) in order to trace the blind signature.

$$\mathbf{F} = b^{-1}\mathbf{R} + ab^{-1}\mathbf{Q} + c\mathbf{G} \tag{7}$$

For this purpose, the signer needs to have the blinding factors (a, b, c) in addition to the values of points $\mathbf{F}$, $\mathbf{R}$, $\mathbf{G}$ and $\mathbf{Q}$. However, he only has the following information for calculation.

$$(s, \mathbf{F}, m, \mathbf{Q}, \mathbf{G}, d, k, \mathbf{R}, \hat{m}, \hat{s})$$

And there are only two equations including the blinding factors:

$$\hat{m} = br(m) + a$$
$$s = b^{-1}(\hat{s}) + c$$

It is considered that Equation (7) could not reveal any information about the blind factors since finding each of the blinding factors in this equation leads to solving ECDLP and this is infeasible. Obviously, finding three unknown factors from the two equations above is impossible; hence there is no way for the signer to trace the blind signature by checking the correctness of Equation (7). Therefore our scheme is untraceable even if the signer has recorded information on the entire requested blind signature. Therefore, the privacy of the user is correctly protected and the signer is not able to derive the link between a signature and the corresponding instance of signing protocol which produced that signature. ■

Furthermore, we use a and b in order to blind message as $\hat{m} = br(m) + a$ in the request phase, since the signer can never find a and b, hence blindness property is correctly achieved.

6 The Performance of the Proposed Scheme

As mentioned previously, Wu and Wang [7] declared that the blind signature scheme proposed by Camenisch *et al.* has a superior performance compared to other schemes based on the DLP. Therefore, we shall compare the proposed scheme to that of Camenisch *et al.* for the purpose of performance evaluation.

Table 1 defines the notations used in this paper. The time complexity of various operation units in terms of time complexity of a modular multiplication is illustrated in Table 2 as extracted from [18, 20]. The values in the first column of Table 2 are in $\mathbf{GF}(2^m)$ with 160-bit m, while the operations in the second column are in $\mathbf{GF}(q)$ with a 1024-bit prime q.

The time complexities of the proposed scheme and that of Camenisch *et al.* are illustrated in Table 3. The required computational cost for both schemes has been estimated by accumulating execution times of all the required operations. Later, based on the information in Table 2, all the estimated times have been exhibited in terms of required execution time for a modular multiplication, that is called the rough estimation. By comparing the results, the performance of

Table 2. Unit Conversion of Various Operations in Terms of T_{MUL}

Time Complexity of an Operation Unit	Time Complexity in Terms of Multiplication
T_{EXP}	$240 \cdot T_{MUL}$
T_{EC_MUL}	$29 \cdot T_{MUL}$
T_{EC_ADD}	$0.12 \cdot T_{MUL}$
T_{ADD}	Negligible
T_{INV}	$0.073 \cdot T_{MUL}$

Table 3. Required Time Complexity in Unit of T_{MUL}

	Required Computation Cost	
	Time complexity	**Rough Estimation**
Camenisch *et al.* scheme [7, 9]	$10 \cdot T_{MUL} + 7 \cdot T_{EXP} + 2 \cdot T_{INV} + 2 \cdot T_{ADD}$	$1696 \cdot T_{MUL}$
Proposed scheme	$6 \cdot T_{MUL} + 7 \cdot T_{EC\_MUL} + 3 \cdot T_{EC\_ADD} + T_{INV} + 3 \cdot T_{ADD}$	$203.57T_{MUL}$

our scheme exceeds the performance of Camenisch *et al.* method significantly [7, 9], in terms of time complexity.

7 Conclusion

In this paper, an efficient untraceable blind signature scheme is presented. The security of the proposed method is obtained by utilizing the elliptic curve discrete logarithm problem. The time complexity of the proposed scheme is compared to a well known scheme and the results indicated that the time complexity of the proposed scheme is significantly reduced. Therefore, the proposed scheme is suitable for applications where the computational resources of requesters are limited, e.g. mobile clients and smart cards.

References

[1] David Chaum. Blind Signatures for Untraceable Payments. In *Advances in Cryptology—CRYPTO '82*, pages 199–203, Santa. Barbara, California, 1982. Plemum.

[2] Lein Harn. Cryptanalysis of the Blind Signatures Based on the Discrete Logarithm Problem. *Electronic Letters*, 31(14):1136, 1995.

[3] Cheng-Chi Lee, Min-Shiang Hwang, and Wei-Pang Yang. A New Blind Signature Based on the Discrete Logarithm Problem for Untraceability. *Applied Mathematics and Computation*, 164(3): 837–841, 2005.

[4] David Chaum. Security without Identification: Transaction Systems to Make Big Brother Obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985. ISSN 0001-0782.

[5] Scott A. Vanstone. Elliptic Curve Cryptosystem—The Answer to Strong, Fast Public-Key Cryptography for Securing Constrained Environments. *Information Security Technical Report*, 2(2):78–87, 1997.

[6] William Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 2006.

[7] Wu Ting and Jin-Rong Wang. Comment: A New Blind Signature Based on the Discrete Logarithm Problem for Untraceability. *Applied Mathematics and Computation*, 170(2): 999–1005, 2005.

[8] Debasish Jena, Sanjay Kumar Jena, and Banshidhar Majhi. A Novel Blind Signature Scheme Based on Nyberg-Rueppel Signature Scheme and Applying in Off-Line Digital Cash. In *Proceedings of the 10th International Conference on Information Technology (ICIT'07)*, pages 19–22, Rourkela, India, 2007. IEEE Computer Society.

[9] Jan L. Camenisch, Jean-Marc Piveteau, and Markus A. Stadler. Blind Signatures Based on the Discrete Logarithm Problem. In *Advances in Cryptology—EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 428–432, Perugia, Italy, 1994. Springer.

[10] Patrick Horster, Markus Michels, and Holger Petersen. Comment: Cryptanalysis of the Blind Signatures Based on the Discrete Logarithm Problem. *Electronic Letters*, 31(21):1827, 1995.

[11] Debasish Jena, Sanjay Kumar Jena, and Banshidhar Majhi. A Novel Untraceable Blind Signature Based on Elliptic Curve Discrete Logarithm Problem. *IJCSNS International Journal of Computer Science and Network Security*, 7(6): 269–275, 2007.

[12] Chun-I Fan, D. J. Guan, Chih-I Wang, and Dai-Rui Lin. Cryptanalysis of Lee-Hwang-Yang Blind Signature Scheme. *Computer Standards & Interfaces*, 31(2):319–320, 2009.

[13] Victor S. Miller. Use of Elliptic Curves in Cryptography. In *Advances in Cryptology—CRYPTO '85*, volume 218 of *Lecture Notes in Computer Sciences*, pages 417–426, Santa. Barbara, California, 1986. Springer.

[14] Neal Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, pages 203–209, 1987.

[15] Don Johnson, Alfred J. Menezes, and Scott A. Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, 1(1):36–63, 2001.

[16] Darrel R. Hankerson, Scott A. Vanstone, and Alfred J. Menezes. *Guide to Elliptic Curve Cryptography*. Springer, 2004.

[17] ANSI X9.62: "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", 1998.

[18] Yu-Fang Chung, Kuo-Hsuan Huang, Feipei Lai, and Tzer-Shyong Chen. ID-based Digital Signature Scheme on the Elliptic Curve Cryptosystem. *Computer Standards & Interfaces*, 29(6): 601–604, 2007.

[19] Zuowen Tan, Zhuojun Liu, and Chunming Tang. Digital Proxy Blind Signature Schemes Based on DLP and ECDLP. *MM Research Preprints*, 21 (7):212–217, 2002.

[20] Neal Koblitz, Alfred J. Menezes, and Scott A. Vanstone. The State of Elliptic Curve Cryptography. *Designs, Codes and Cryptography*, 19(2–3):173–193, 2000.

Morteza Nikooghadam received the BSc degree from university of Sadjad, Iran, in 2006, MSc from the Shahid Beheshti University, Iran, in 2008, and currently he is a PhD student in computer architecture in the department of Electrical and Computer Engineering at Shahid Beheshti University, Iran. His research focuses on design of Reconfigurable Architectures for operations on the Galois Field $GF(2^m)$ under Supervisory of Dr. Ali Zakerolhosseini. His current research interests are Data Security, Cryptography and Sensor Network Security.

Ali Zakerolhoseini received the BSc degree from university of Coventry, UK, in 1985, MSc from the Bradford University, UK, in 1987, and PhD degree in Fast transforms from the University of Kent, UK, in 1998. He is currently been an assistant professor in the department of Electrical and Computer Engineering at Shahid Beheshti University, Iran. His research focuses on Reconfigurable device and multi classifiers. His current research interests are Data Security, Cryptography and Reconfigurable computing.