International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:6, No:8, 2012

A New Design Partially Blind Signature Scheme Based on Two Hard Mathematical Problems

Nedal Tahat

Abstract—Recently, many existing partially blind signature scheme based on a single hard problem such as factoring, discrete logarithm, residuosity or elliptic curve discrete logarithm problems. However sooner or later these systems will become broken and vulnerable, if the factoring or discrete logarithms problems are cracked. This paper proposes a secured partially blind signature scheme based on factoring (FAC) problem and elliptic curve discrete logarithms (ECDL) problem. As the proposed scheme is focused on factoring and ECDLP hard problems, it has a solid structure and will totally leave the intruder bemused because it is very unlikely to solve the two hard problems simultaneously. In order to assess the security level of the proposed scheme a performance analysis has been conducted. Results have proved that the proposed scheme effectively deals with the partial blindness, randomization, unlinkability and unforgeability properties. Apart from this we have also investigated the computation cost of the proposed scheme. The new proposed scheme is robust and it is difficult for the malevolent attacks to break our scheme. .

Keywords—Cryptography; Partially Blind Signature; Factoring; Elliptic Curve Discrete Logarithms.

I. Introduction

BLIND signature is a type of digital signature and was introduced by Chaum [1]. In this signature the content of a message is blinded before it is delivered, hence the name blind signature. These signatures are usually employed in privacy-related protocols, and is significantly used in a lot of applications such as electronic voting, electronic cash schemes of which ambiguity is one of the biggest challenges. The definitions of security and partial blind signature can be found in Juels [2] , Pointcheval [3], and Pointcheval and Stern [4], [5]. Abe and Fujisaki [6] were the pioneers of the concept of partial blind signatures. The partial blind signature provides a signer with common agreed information which is clearly evident in spite of the blinding process. This concept of the blind signature eradicates some drawbacks of the fully blind signatures where the signer will not have any control over the elements except those, which are bound by the public key. The partial blind signatures are very vital in designing proficient electronic cash systems, where the banks can have a single public key for different coin values. Furthermore, the size of the database would not increase infinitely over time, while storing the previously spent coins to detect double-spending. Fan and Lei [7] have proposed the partially blind based on quadratic residue problem in which there is no need for modular exponentiation and inverse computations to be performed by the signature requesters. Furthermore, it needs several modular additions and multiplications for receivers to get and verify a signature in their protocol. The blind signature schemes proposed in the literatures, Fan and Lei [7] minimizes the number of computations for the signature requesters or users by nearly 98 under a 1024-bit modulus, however it does not reduce the load of computation for the signer. Hence their scheme is principally appropriate for mobile signature requesters and smart-card users. Hwang [8] have stated that Fan and Lei [7] schemes was unable to meet the intractability property of a blind signature. Nevertheless Chien [9] have proposed a partially blind signature scheme based on RSA that is capable of minimizing the computation load. Moreover Maitland and Boyd [10] have first integrated these two blind signatures and proposed a practically secured restrictive partially blind signature scheme, which satisfies the partial blindness and restrictive blindness. Their scheme was based on the model proposed by Abe and Okamoto [11] and has employed Brand's restrictive blind signature scheme. Huang and Chang [12] have proposed a novel and competent, partially blind signature based on discrete logarithm and the Chinese remainder theorem. However later, Zhang and Chen [13] have proved that the scheme proposed by Huang and Chang is not secured, where any malevolent requester can confiscate the embedded public common information from the signer's signature and get a partially blind signature with special public information. As of now the question of designing a partially blind signature based on the elliptic curve discrete logarithm and factoring, is still open. In this paper, we have proposed a new blind signature based on the elliptic curve discrete logarithm and factoring problems. The reminder of the paper is organized as follows: the next section presents the basic concept and definition of partial blind signature (PBS) and introduces the notations that are used throughout the rest of the paper. In section III we have presented our new scheme. The section IV elucidates details of the security and performance evaluation and finally section V provides the conclusion of the paper.

N. Tahat is with the Department of Mathematics,Faculty of Sciences, The Hashemite University, Zarqa 13115, Jordan email: nedal@hu.edu.jo.

II. Preliminaries

A. The Model of Partially Blind Signature Scheme

In partially blind signature scheme there are two types of participants, a signer and a signature requester. The following are the processes of the two participants of the scheme:

- Suppose a requester would request a partially blind signature from the signer, then the requester will notify the signer.
- After that, the requester provides the blinded data/message and the common information and sends them to the signer. At this stage, the signer will decide on this common information.

- If the signer agrees on this common information, then he/she signs the blinded data with this common information embedded on the signature
- For the partial blindness property, the requester derives the signature from the signed data, but he/she cannot remove or change the embedded common information. So the agreed common information should be genuinely shared among the requester, the signer and the verifiers.

A secure FDRS must satisfy the following properties:

1) Partial blindness: It allows a user to acquire a signature on a message without revealing anything about the message to the signer. Blindness property ensures that no one can derive a link between a view and valid blind signature except the signature requester. A view of the signer is defined to be the set of all messages that the signer has received and generated when issuing the signature. Based on this blindness property, blind signatures have been widely used in untraceable electronic cash systems.
2) Randomization: The signer will inject one or more randomizing factors into the blinded message so that the attackers cannot predict the exact content of the message signed by the signer. In a secure randomized signature scheme, a user cannot remove the signer's randomizing factor.
3) Unlinkability: In a secure blind signature scheme, it is computationally infeasible for the signer to link a signature shown for verification to the instance of the signing protocol that has produced that signature. This property is usually referred to as the unlinkability property.
4) Unforgeability: It means that only the signer can generate the valid signatures.

B. Elliptic Curve

Elliptic curve cryptosystem have attracted much attention in recent years because of the relatively small size of keys they require. An elliptic over $GF(p)$ is the set of points (x,y) with $x,y \in GF(p)$ satisfying the equation

$$y^2 = x^3 + ax + b \tag{1}$$

Where $a,b \in K$ and $4a^3 + 27b^2 \neq 0$. The set $E(K)$ consists of all points $(x,y), x,y \in K$ which satisfy the defining (1) together with a special point O called the point at infinity. Let G be a point on the elliptic curve defined in (1) and if n the smallest positive integer is satisfying the equation $nG = O$, then we say that G has an order n and is called the base point. Refer [14], [15], [16], [17] for complete discussion on elliptic curves specifically on how two elliptic points are added and multiplication between a constant and an elliptic point. The hard problems of ECDL and FAC are the following

- ECDL: Let G and C be two elliptic curve points on (1). Then find a positive integer d such that $dG = C$.
- FAC: Is the problem to find the prime divisor p and q for a positive integer $n = pq$, where p and q are positive distinct large primes.

III. The new scheme

This section explains about our proposed PBS scheme based on the elliptic curve discrete logarithm problems. The scheme can be divided into five phases: initialization, key generation, requesting, signing and extraction and Signature verification. The signer publishes the necessary information in the initialization. In the requesting phase, a requester submits the blinded data and the common information to the signer. In the signing phase, the signer signs the blinded data with this common information imposed on it and then sends the result back to the requester. Finally, the requester extracts the signature from the signed data in the extraction phase. The details of the proposed partially blind signature scheme are described as follows.

A. Initialization

Let p be a large prime number and $p-1$ have two prime factors $\bar{p}$ and $\bar{q}$, $n = \bar{p}\bar{q}$, so that $n/(p-1)$. $a,b \in GF(p)$ which confirm the elliptic curve. The root points of Elliptic curve construct a circulating subgroup. G is a generating element for the subgroup and its rank equals to n. $h(.)$ is a secure hash function. The public parameters are p,n,G and the secret parameter are $\bar{p}$ and $\bar{q}$.

B. Key Generation

Selects a random integer $x \in [1,n-1]$ and computes

$$y = xG$$

Next select at random an integer $e \in \mathbb{Z}^*_{\varphi(n)}$ and calculate an integer d satisfying the congruence

$$ed \equiv 1 (\mathrm{mod} \varphi(n))$$

Finally, publishes (e,y) as a pair of public key whereas kept (d,x) as a pair of secret key of the scheme.

C. Requesting

Suppose requester A wants to obtain a signature on message $h(m)$. Firstly, he must notify the signer and then:

- A signer selects an integer $r \in [1,n-1]$ and compute

$$\bar{R} = rG = (x_1, x_2)$$

  where $\bar{u} = x_1 (\mathrm{mod}\, n)$ and then send $\bar{R}$ to the requester A.
- After receiving $\bar{R}$ prepares the common information a, according to a pre-defined format. Then the value a is a common input of both the requester A and the signer.
- The requester A also randomly select two blinding factors $\alpha, \beta \in [1,n-1]$ and computes

$$\begin{aligned} R &= \alpha\bar{R} + \beta G = (y_1, y_2), \text{ where } u \equiv y_1 (\mathrm{mod}\, n) \\ \sigma &\equiv \alpha^{-1} h(m) \bar{u} u^{-2} (\mathrm{mod}\, n) \end{aligned}$$

  and then send (σ, a) to the signer.

D. Signing and Extraction

The signer signs blindly the message $h(m)$ as follows:

- The signer computes and sends
$$\bar{s} \equiv (\sigma x a^2 + r\bar{u}) (\mathrm{mod}\, n)$$
to the requester A
- The requester A computes and sends
$$s \equiv (\bar{s}u^2(\bar{u})^{-1}\alpha + \beta u^2)((\bar{s})^e)^{-1} (\mathrm{mod}\, n)$$
to the signer
- The signer computes and sends $\bar{\mu} \equiv s^d (\mathrm{mod}\, n)$ to the requester A.
- The requester A computes $\mu \equiv \bar{\mu}\bar{s} (\mathrm{mod}\, n)$.Then the signature is given by (a, R, μ) .

E. Signature Verification

Calculates

$$\begin{aligned} w_1 &= \mu^e G (\mathrm{mod}\, n) \\ w_2 &= (h(m)a^2 y + u^2 R) (\mathrm{mod}\, n) \end{aligned}$$

The following theorem shows that if a signature (a, R, μ) of a message m is produced by the proposed partially blind signature scheme, then it satisfies $w_1 = w_2$.

Theorem 3.1. *(a, R, μ) is a signature of the message m produced by a proposed new partially blind signature scheme, then $w_1 = w_2$ and the protocol above is a blind scheme.*

Proof. Note that

$$\begin{aligned} w_1 &= \mu^e (\mathrm{mod}\, n) \\ &= (\bar{\mu}\bar{s})^e (\mathrm{mod}\, n) G \\ &= s^{ed} (\bar{s})^e (\mathrm{mod}\, n) G \\ &= s(\bar{s})^e G \\ &= (\bar{s}u^2(\bar{u})^{-1}\alpha + \beta u^2)((\bar{s})^e)^{-1}(\bar{s})^e G \\ &= ((\sigma x a^2 + r\bar{u})u^2(\bar{u})^{-1}\alpha + \beta u^2))G \\ &= (((\alpha^{-1}h(m)\bar{u}u^{-2})xa^2 + r\bar{u})u^2(\bar{u})^{-1}\alpha + \beta u^2))G \\ &= (a^2 h(m)xG + ru^2\alpha G + \beta u^2 G) \\ &= (a^2 h(m)y + u^2(\alpha\bar{R} + \beta G) \\ &= (h(m)a^2 y + u^2 R) (\mathrm{mod}\, n) \\ &= w_2 \end{aligned}$$

Which means that (a, R, μ) is a valid signature of m. So, our proposed protocol provides a partially blind signature scheme.

IV. Security and efficiency performance

A. Security

We discuss some security properties of our new partially blind signature scheme. A secure partially blind signature schemes should satisfy the following requirements [12]:

1) *Partial* blindness: The partial blindness property of all signature issued by the signer must contain a clear common information a according to the predefined format negotiated and agreed by all the requester and the signer and the requester will not be able to change or remove the embedded information a while keeping the verification of signature successful. In the proposed scheme, the signature-requester has to submit the blinded data σ to the signer, and then the signer computes and sends $\bar{s} \equiv (\sigma x a^2 + r\bar{u}) (\mathrm{mod}\, n)$ to the signature-requester. If the signature-requester can successfully change or remove this common information a from the corresponding signature (a, R, μ), then he or she computes $\bar{s} \equiv (\sigma x a^2 + r\bar{u}) (\mathrm{mod}\, n)$. However, it is difficult to derive the secret key x. Also the signature-requester has to submit the blinded data s to the signer then the signer computes and sends $\bar{\mu}$ to the signature-requester. The signature-requester cannot change or remove $\bar{\mu} \equiv s^d (\mathrm{mod} n)$ because it is difficult to solve FAC problem. Hence, in the proposed scheme, the signature-requester cannot change or remove the a and $\bar{\mu}$ from the corresponding signature (a, R, μ), of message m to forge the unblind part of the signature.

2) *Randomization*: In the proposed scheme, the signer randomizes the blinded data using the random factor r before signing it in the signing phase. In the requesting phase, the signer selects an integer r and sends $\bar{R} = rG$ to the recipient. Then, the recipient sends σ to the signer and the signer returns $\bar{s} \equiv (\sigma x a^2 + r\bar{u}) (\mathrm{mod}\, n)$ to the signature-requester. If the signature-requester tries to remove r from $\bar{s}$, then he has to derive x from $y = xG$. However, it is difficult to determine x because that the derivation is ECDLP. Hence, in the proposed scheme, the signature-requester cannot remove the random r from the corresponding signature (a, R, μ).

3) *Unlinkability*: For every instance, the signer can record the transmitted messages (σ_i, s_i) between the signature-requester and the signer during the instance i of the protocol. The pair (σ_i, s_i) is usually referred to as the view of the signer to the instance of the protocol. Thus, we have the following theorem:

Theorem 4.1. Giving a signature (a, R, μ) produced by the proposed scheme, the signer can derive $(\acute{\alpha}_i, \acute{\beta}_i)$ for every (σ_i, s_i) such that

$$\begin{aligned} \sigma_i &\equiv \acute{\alpha}_i^{-1} h(m)\, \bar{u}\, (u)^{-2} (\mathrm{mod}\, n) \\ s_i &\equiv (\bar{s}u^2(\bar{u})^{-1}\acute{\alpha}_i + \acute{\beta}_i u^2)((\bar{s})^e)^{-1} (\mathrm{mod}\, n) \end{aligned}$$

Proof. If $\sigma_i \equiv \acute{\alpha}_i^{-1} h(m)\, \bar{u}\, (u)^{-2} (\mathrm{mod}\, n)$, we have that

$$\begin{aligned} \sigma_i \acute{\alpha}_i &\equiv h(m)\, \bar{u}\, (u)^{-2} (\mathrm{mod}\, n) \\ \acute{\alpha}_i &\equiv \sigma_i^{-1} h(m)\, \bar{u}\, (u)^{-2} (\mathrm{mod}\, n) \end{aligned}$$

If $s_i \equiv (\bar{s}u^2(\bar{u})^{-1}\acute{\alpha}_i + \acute{\beta}_i u^2)((\bar{s})^e)^{-1} (\mathrm{mod}\, n)$ then we have

$$\begin{aligned} s_i(\bar{s})^e &\equiv (\bar{s}u^2(\bar{u})^{-1}\acute{\alpha}_i + \acute{\beta}_i u^2) (\mathrm{mod}\, n) \\ \acute{\beta}_i u^2 &\equiv (s_i(\bar{s})^e - \bar{s}u^2(\bar{u})^{-1}\acute{\alpha}_i) (\mathrm{mod}\, n) \\ \acute{\beta}_i &\equiv (s_i(\bar{s})^e - \bar{s}u^2(\bar{u})^{-1}\acute{\alpha}_i) u^{-2} (\mathrm{mod}\, n) \end{aligned}$$

According to the above derivations, the signer can derive $\acute{\alpha}_i, \acute{\beta}_i$ for every record (σ_i, s_i). Hence, giving a signature (a, R, μ) produced by the proposed scheme, the signer can always

derive the two blinding factors $\acute{\alpha}_i, \acute{\beta}_i$ for every transmitted record (σ_i, s_i). This implies that the signer is unable to find the link between the signature and its corresponding signing process instance. So, our scheme can achieve the unlinkability property.

4) *Unforgability*: The adversary (Adv) may try to derive some forged signatures by using different ways. We have proved that all the attacks fail on our scheme.

Attack 1: Adv tries to derive the signature (a,R,μ) for a given message, m by letting two integer fixed and finding the other one. In this case, Adv randomly select (R,a) or (R,μ) or (μ,a) and finds μ or a or R respectively such that $w_1 = w_2$. For example, fixed the values (R,a) and tries to figure out the value of μ to satisfying $w_1 = w_2$ and vise-versa. Adv starts by computing $\gamma = (h(m)a^2y + u^2R)$ and solve $\mu^e(modn)G$ for μ. He can only find μ if both FAC and ECDL are breakable. Say that ECDL problem is breakable, then Adv knows μ but still cannot figure the value of μ since he learns nothing about d. In this case too, the breakable of FAC problem does not help the Adv at all. The rests of two cases go similarly.

Attack 2: It is assumed that Adv is able to solve ECDL problem. In this case, Adv knows x and can generate or calculate the numbers $\bar{s}$ and s. Unfortunately, he or she does cannot compute $\bar{\mu} \equiv s^d (\mathrm{mod}\, n)$ because difficult solve FAC problem and then cannot compute $\mu \equiv \bar{\mu}\bar{s} (\mathrm{mod}\, n)$and fails to produce the signature (a,R,μ).

Attack 3: It is assumed that Adv is able to solve the FAC problem. That means, he knows the prime factorization of n. However, he or she cannot compute $\bar{s}$ since no information is available for x, hence cannot compute s because it is dependent on $\bar{s}$, then he or she cannot compute $\mu \equiv \bar{\mu}\bar{s} (\mathrm{mod}\, n)$. Thus fails to produce the signature (a,R,μ).

Attack 4: Adv may also try collecting t valid signatures (a_j, R_j, μ_j) on message m_j where $j = 1,2,,t$ and attempts to find secret keys. In this case, intruder has t equations given as follows:

$$\begin{aligned} \mu_1^e &\equiv xh(m_1)a_1^2 + u_1^2(\alpha_1 r_1 + \beta_1) \\ \mu_2^e &\equiv xh(m_2)a_2^2 + u_2^2(\alpha_2 r_2 + \beta_2) \\ &\vdots \\ \mu_t^e &\equiv xh(m_t)a_t^2 + u_t^2(\alpha_t r_t + \beta_t) \end{aligned}$$

In the above t equations, there are $t+1$ variables i.e. x and r_j which are not known by the Adv. Hence, x stays hard to detect because intruder can generate infinite solutions of the above system of equations but cannot figure out which one is correct. In addition, Adv wishes to obtain secret keys (x,d) using all information that available from system. In this case,Adv needs to solve $y = xG$ and $d \equiv e^{-1}(mod\, \varphi(n))$ which are clearly infeasible the difficulty of solving ECDL and FAC problems.

B. Efficiency Performance

The performance of our scheme is described in terms of number of keys computational complexity and communication costs. The following notations are used to analyze the computationally complexity. T_{mul} defines the time complexity for executing the modular multiplication; T_{exp} means the time for one exponentiation computation; T_{inv} denotes the time for one inverse computation; T_{ec-add} means the time complexity for executing the addition of two elliptic curve points; T_{ec-mul} means the time complexity for executing the multiplication on elliptic curve points; T_{sr} means the time complexity for executing the modular square computation; T_h denotes the time for executing the adopted one-way hash function in one's scheme. The number of secret keys (SK) and public keys (PK) of the scheme are respectively given by $SK = 2$ and $PK = 2$. The computational complexity for the key generation, performed by signer, by requester and verification is given in Table 1 and the last column converts various operation units to T_{mul} where $T_{exp} \approx 240T_{mul}$ and $T_{ec-mul} \approx 29T_{mul}$ are given by Koblitz, Menezes and Vanstone [16]. Assuming

TABLE I
THE COMPLEXITY IN UNIT T_{mul} OF THE PROPOSED SCHEME

Efficiency Terms	Time Complexity	Complexity in T_{mul}
Computation for key generation	$T_{ec-mul} + T_{mul}$	$29T_{mul} + 2T_{sr}$
Computation for signer	$T_{ec-mul} + 3T_{mul} + T_{exp} + T_{sr}$	$272T_{mul} + T_{sr}$
Computation for requester	$2T_{ec-mul} + 11T_{mul} + T_{exp} + T_{sr}$	$59T_{mul} + 3T_{sr}$
Computation for verification	$T_exp + 3T_{ec-mul} + T_{mul} + 2T_{sr} + T_h$	$328T_{mul} + 2T_{sr} + T_h$

the time complexity for T_h and T_{inv} are negligible, we found that, the performed by signer $272T_{mul}$ time complexity and the performed by the requester $40T_{mul}$ time complexity. In Chien, Jan and Tseng paper [9] RSA-Based partially blind signature with low computations, the computational complexity for the signer and the requester are $83T_{mul}$ and $728T_{mul}$ respectively. When we compare our scheme with the scheme Chien and Tseng is very clear to conclude that our scheme is more efficient than Chien scheme. In addition, our scheme is based on two hard problems which offer a longer security than Chien and Tseng scheme [9]. The efficiency performance reveals that our modular multiplication and multiplication on elliptic curve points operations dominates our scheme. However this operation does not interrupt the process of the scheme since it can always speeded up, also there is no exponentiation computation performed by the requester. Therfore, the proposed method can provide more efficient services for both the signer and the signature requester.

V. CONCLUSION

In this paper, we had presented a new partially blind signature scheme based on ECDL and FAC problems and its security is analysed in detail. The scheme based on two

hard problems provides longer and higher level security than scheme that based on a single hard problem. Moreover, the presented scheme had satisfied all the security requirements of partially blind signature, so it has obvious superiority over normal partially blind signature based on only one hard mathematical problem. The proposed scheme requires only minimal operation both in signing and verifying logarithms and thus makes it very efficient. We had tested the proposed scheme against some possible attacks have also been considered and proved that the scheme is secured from those attacks.

REFERENCES

[1] D. Chaum, "Blind signature for untraceable payments," *Advances in Cryptology, Proceedings of CRYPTO '82*, pp. 199–203, 2000.
[2] A. Juels, M. Luby, and R. Ostrovsky, "Security of blind signatures," *Advances in Cryptology - Crypto 1997, LNCS 1294. Springer-Verlag*, pp. 150–164., 1997.
[3] D. Pointcheval, "Strengthened security for blind signatures," *Advances in Cryptology -Eurocrypt 1998, LNCS 1403. Springer-Verlag,*, pp. 391–403, 1998.
[4] D. Pointcheval and J. Stern, "Provably secure blind signature schemes," *Advances in Cryptology - Asiacrypt 1996, LNCS 1163. Springer- Verlag*, pp. 252–265, 1996.
[5] D. Pointchval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptography*, vol. 13 (3), pp. 361–396, 2000.
[6] M. Abe and E. Fujisaki, "How to date blind signatures," *Lecture Notes in Computer Science, 1163.Springer-Verlag*, pp. 244–251, 1996.
[7] C. I. Fan and C. Lei, "Low-computation partially blind signatures for electronic cash," *IEICE Transaction on Fundamentals*, vol. E81-A, pp. 199–203, 1998.
[8] M. S. Hwang, C. C. Lee, and Y. Lai, "Traceability on low computation partially blind signatures for electronic cash," *IEICE Transaction on Fundamentals*, vol. 85, pp. 1181–1182, 2002.
[9] H. Chien, H. Y. Jan, and Y. M. Tseng, "Rsa-based partially blind signature with low computation," in *8th International Conference On Parallel and Distribute Systemes*, 2001, pp. 385–389.
[10] G. Maitland and C. Boyd, "A provably secure restrictive partially blind signature scheme," *PKC 2002, LNCS 2274. Springer-Verlag,*, pp. 99–114, 2002.
[11] T. Abe, M. Okamoto, "Provably secure partially blind signatures," *Advances In Cryptology-Crypto,LNCS 1880.Springer-Verlag*, vol. 5, pp. 271–286, 2000.
[12] H. Chien, H. Y. Jan, and Y. M. Tseng, "A new design of efficient partially blind signature scheme," *Journal of Systems and Software*, vol. 73, pp. 397–403, 2004.
[13] F. Zhang and X. Chen, "Cryptanalysis of huangchang partially blind signature scheme," *The Journal of Systems and Software*, vol. 76, pp. 76: 323–325, 2005.
[14] D. A. Johnson, D. A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm," *International Journal of Information Security*, vol. 1(1), pp. 36–63, 2001.
[15] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48(177), pp. 203–209, 1987.
[16] N. Koblizt, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Design, Code Cryptography*, vol. 19(2-3), pp. 173–193, 2000.
[17] V. Miller, "Uses of elliptic curve in cryptography," *Advances in Cryptology-Proceeding of CRYPTO'85. LNCS 218, Springer-Verlag*, pp. 417–426, 1986.