International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 2, April 2018, pp. 1074~1083
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i2.pp1074-1083

New Blind Muti-signature Schemes based on ECDLP

Duc Nguyen Tan[1], Hai Nguyen Nam[2], Minh Nguyen Hieu[3], Hiep Nguyen Van[4], Lam Tran Thi[5]
[1,2]Posts and Telecommunications Institute of Technology, Vietnam
[3,4]Academy of Cryptography Techniques, Vietnam
[5]Le Quy Don Technical University, Vietnam

Article Info

Article history:

Received Sep 10, 2017
Revised Dec 23, 2017
Accepted Dec 29, 2017

Keyword:

Blind signature
EC-Schnorr signature
GOST R34.10-2012 standard
Multi-signature scheme
Random oracle model (ROM)

ABSTRACT

In various types of electronic transactions, including election systems and digital cash schemes, user anonymity and authentication are always required. Blind signatures are considered the most important solutions to meeting these requirements. Many studies have focused on blind signature schemes; however, most of the studied schemes are single blind signature schemes. Although blind multi-signature schemes are available, few studies have focused on these schemes. In this article, blind multi-signature schemes are proposed based on the Elliptic Curve Discrete Logarithm Problem (ECDLP). The proposed schemes are based on the GOST R34.10-2012 digital signature standard and the EC-Schnorr digital signature scheme, and they satisfy blind multi-signature security requirements and have better computational performance than previously proposed schemes. The proposed schemes can be applied in election systems and digital cash schemes.

Corresponding Author:

Minh Nguyen Hieu,
Faculty of Electronics & Telecommunications,
Academy of Cryptography Techniques,
141 Chien Thang, Tan Trieu, Thanh Tri, Ha Noi, Vietnam.
Email: hieuminhmta@gmail.com

1. INTRODUCTION

David Chaum first proposed the idea of blind signatures based on the RSA signature scheme in 1983 [1]. Subsequently, a number of research studies on blind signatures was completed to protect the anonymity of users and prevent fake online transactions.

In recent decades, elliptic curves have emerged as important factors in digital and crypto theory. The security level of cryptography systems is based on elliptic curve cryptography (ECC) and the difficulty of elliptic curve discrete logarithm problems (ECDLPs). The advantages of ECC cryptosystems compared with other public-key cryptography systems is that ECC ciphers provide security attributes comparable to traditional public-key cryptography systems despite their smaller key lengths. Reports have estimated that the 3248-bit length in the RSA cryptosystem has the same security level as the 256-bit length of the ECC cryptosystem. Thus, the installation of ECC consumes less system resources and energy and provides a higher level of security. Because of the advantage of small key length, ECC has been widely applied in many fields.

Digital signatures based on the difficulty of ECDLPs were first introduced in 1991 in the independent research of NealsKoblitz [2]. Since the 2000s, the USA, Russia, Japan, Korea and several European countries have investigated these problems and have developed standard system solutions, such as the standards by ISO, ANSI, IEEE, SECG, and FIPS. ECDLP is the predominant cryptosystem in Russia. In 2001, Russia produced the GOST R34.10-2001 digital signature standard based on ECDLP with a 256-bit key length. The newest Russia version of the digital signature is GOST R34.10-2012 [3], which has a key length between 256 bits and 512 bits.

Blind multi-signatures (BMSs) are signatures in which the signer does not know what they are signing, thus the term "blind". Such signatures are possible because the content of the message *M* has been "blinded" to become *M′* before the message is provided to the collective to sign. Thus, the signing collective signed *M′* and not *M*. Specifically the user U needs the collective S to sign message *M*; however, U does not provide S with *M* but rather blinds *M* to *M′* and then provides the blinded *M′* to S to sign. After receiving the signed *M′*, U unblinds the message to obtain the signature for *M*. Therefore, U has a signature for *M* without providing S with information on *M*. Blind multi-signatures have many practical applications, such as anonymous access control or anonymous multi-sided authorization. Figure 1 show the blind Multi-Signature Process.

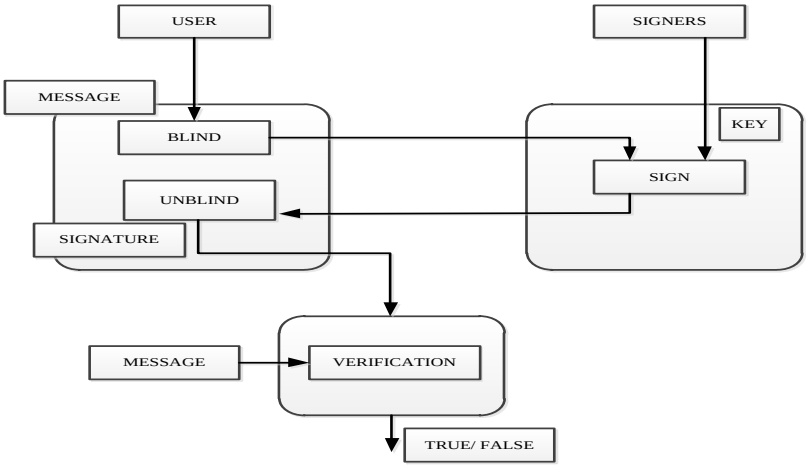

Figure 1. Blind Multi-Signature Process

In 1999, Popescu [4] presented blind multi-signatures based on elliptic curves. In 2005, Chow et al. proposed two blind signature schemes partially based on Bilinear Pairings [5]. In 2011, Moldovyan [6] presented a blind signature scheme based on the GOST R34.10-2001 signature standard. In 2012, Nguyen and Dang [7] provided enhanced security for voting protocols on the Internet using blind signatures; Swati Verma et al. also presented New Proxy Blind Multi Signature based on Integer Factorization and Discrete-Logarithm Problems [8]. In 2013, Panda et al. researched blind signing authorizations in electronic voting processes [9]. In 2014, Hua Sun et al. proposed New Certificateless Blind Ring Signature Scheme [10]. In 2016, Shilbayeh et al. proposed security schemes for electronic voting processes [11]. In 2017, Minh H et al. New Blind Signature Protocols based on a New Hard Problem [12]; Salome James et al. proposed Identity-Based Blind Signature Scheme with Message Recovery [13].

In the next section, details on the ECDLP will be presented, the blind multi-signature schemes based on digital signature standards will be proposed, security through the Random Oracle Model (ROM) will be demonstrated and a comparison between the proposed schemes and available schemes will be performed.

2. BACKGROUND

The following notations are used:

Z: set of all integers
p: prime number, *p*> 3
a, *b*: elliptic curve coefficients
m: points of the elliptic curve group order
q: subgroup order of group of points of the elliptic curve
O: zero point of the elliptic curve
P: elliptic curve point of order *q*
d: integer - a signature key
G: elliptic curve point - a verification key
An elliptic curve with the following form is studied in this work:

$$y^2 = x^3 + ax + b \bmod p. \quad (1)$$

where a and b are constants, the values of x, y, a, b are in the fields GF(p) and $4a^3 + 27b^2 \neq 0 \bmod p$.

In addition, $J(E)$ can be used to calculate E as follows:

$$J(E) = 1728\frac{4a^3}{4a^3 + 27b^2} \bmod p.$$

The constants a and b can be determined by $J(E)$ as follows:

$$a = 2k \pmod p; b = 3k \pmod p.$$

$$\text{where } k = \frac{J(E)}{1728 - J(E)} \bmod p; J(E) \neq 0; J(E) \neq 1728.$$

Definition 1 (BMS): A blind multi-signature scheme can be described by following five algorithms: setup, blind, sign, unblind, and verification.

A third trust party (TTP) is used, and the process is detailed as follows.

a. Setup: Create public arguments based on the GF(p) field and open the argument (p,q,G,P) to the public. Each user in the group can use their private key as identification and calculate the value of the public key.
b. Blind: Users chose two random arguments and combine them with the hash of message M to make the content of M blind. The first part of the signature value (r) is simultaneously blinded in this part and sent to the signing group.
c. Sign: Each user in the signing group calculates their own signature, and the TTP calculates the signature of the group and sends it back to the requesting user.
d. Unblind: The requesting user unblinds the signature. The result is the set (r,s), which is the blind multi-signature on message M.
e. Verify: the checking user verifies the signature, which is only accepted if the verification process is satisfied; otherwise, the signature is not accepted.

The digital signature parameters are:

a. p is a large prime number, which composes the field $GF(p)$ of EC.
b. EC is determined by the description in Part 2.
c. integer m is an elliptic curve EC points group order: $m = nq$, n belongs to Z, $n \geq 1$.
d. q is a prime number that indicates the number of EC point groups and is determined as follows: $2^{254} < q < 2^{256}$ or $2^{508} < q < 2^{512}$.
e. G is a point that does not coincide with the origin O of EC and has the coordinate (x_G, y_G), which satisfies the following condition: $q \times G \equiv O$
f. $H(M)$ is the value of the hash function with an l-bit length satisfies the following condition:

   If $2^{254} < q < 2^{256}$ then $l = 256$; If $2^{508} < q < 2^{512}$ then $l = 512$.

g. d is a private key of user ($0 < d < q$).

2.1. GOST R 34-10-2012 Standard [3]

a. Setup: Calculate the public key point as follows: P = d × G.
   The signing party choses a random number k that satisfies (0< k < q) and calculates C = k × G.
b. Sign: Calculate the hash value of message M. Determine the first part of signature r as follows: $r = x_C \bmod q$, where x_C is the abscissa of point C. If r = 0, then another value of k needs to be chosen. Calculate $e = H(M) \bmod q$. Calculate the second part of the signatureas $s = (rd + ke) \bmod q$. If s = 0, then choose another value of k.
   The output of the algorithm is the set (r,s), which is set as the digital signature on message M.

c. Verify: Calculate $C' = (se^{-1} \bmod q) \times G - (re^{-1} \bmod q) \times P$; $r' = x_{C'} \bmod q$. Compare r' with r. If $r' = r$, then the digital signature is accepted; otherwise, the digital signature is not accepted.

2.2. EC-Schnorr scheme [14]

a. Setup: Calculate the public key point: $P = d \times G$. The signing party choses a random number k that satisfies $(0<k<q)$ and calculates $C = k \times G$.

b. Sign: Calculate the first part of the signature. Determine the first part of signature as $r = H(M, x_C) \bmod q$. Where x_C is the abscissa of point C. If $r = 0$, then another value of k is chosen. Calculate $s = (k - rd) \bmod q$. If $s = 0$, then the process is started again.

The output of the algorithm is the set (r,s), which is used as the digital signature on message M.

c. Verify: Calculate $C' = s \times G + r \times P$ and $r' = H(M, x_{C'})$. Compare r' with r. If $r' = r$, then the digital signature is accepted; otherwise, the digital signature is not accepted.

2.3. Blind Multi-signature

Assume that user U asks the entire group S who has the authority to include n signers to sign document M; however, this user does not want this authorized group to know the content of M. First, this user blinds the document M, which becomes document M'. Then, M' is sent to the authorized signing group. This group signs M' and sends it back to the requesting user. Then, the user unblinds M' to M and checks the received signature. If the signature is valid, then the user has a valid signature on document M.

2.4. Random Oracle Model

In 1993, Bellare and Rogaway [15] generalized a model that allowed for the security of different coding schemes. A blind digital signature scheme is considered safe when its characteristics of blindness and anti-forgery can be ensured in a random predictive model.

Definition 3: (Blindness). With all polynomial time algorithms of attacker A acting as the signer, the probability of success of the experiment below is a negligibly small function.

There are two trusted users U_0, U_1, which join the blind multi-signature signature scheme with A on the message M_{1-b}, M_b, and the output the signature s_{1-b}, s_b corresponding to $b \in \{0,1\}$ is randomly selected. $(M_{1-b}, M_b, s_{1-b}, s_b)$ is then sent to A, and the output is $b' \in \{0,1\}$. For all A, U_0, U_1, when any constant prime number p is large enough, the probability of success of the experiment is negligible: $|\Pr[b = b'] - \frac{1}{2}| < \frac{1}{p^c}$.

Definition 4: (Assumed ECDLP Problem) Taking a set of points P that have a field Z_p and elementary G so $d \times G \in P$, where d is a random number chosen in the field Z_q^*, the assumed ECDLP of P is the calculated value of d. (ε, t) - is assumed in the point P group if it can solve within time t the difficult ECDLP of group P with the smallest probability ε.

3. PROPOSED BLIND MULTISIGNATURE SCHEMES

3.1. BMS based on the GOST R34-10-2012 standard

a. Setup: For each signer with the authority to sign S, calculate the value of the public key and send it to the TTP to calculate the public key value: $P_i = d_i \times G$ and $P = P_1 + P_2 + ... + P_n = \sum_{i=1}^{n} d_i \times G$.

Each signer with the authority to sign selects the random numbers $k_i (k_i \in Z_q)$ and calculates C_i, which is sent to the TTP to calculate $\bar{C}$ with $C_i = k_i \times G$, where i = 1,2,... n and $\bar{C} = \sum_{i=1}^{n} C_i = \sum_{i=1}^{n} k_i \times G$. S sends $\bar{C}$ to U.

b. Blind: U selects two random numbers, $\alpha, \beta \in \{1,2,...,q\text{-}1\}$, and the following variants are calculated.

Variant 1	Variant 2
$h = H(M);$	$h = H(M);$
$e = h \bmod q;$	$e = h \bmod q;$
$\bar{e} = \alpha e \bmod q;$	$\bar{e} = \beta e \bmod q;$
$C = \beta \times \bar{C} + \alpha \times G;$	$C = (\alpha^{-1} \bmod q) \times \bar{C} + P + G;$
$r = x_C \bmod q;$	$r = x_C \bmod q;$
$\bar{r} = (r\beta^{-1}\alpha) \bmod q.$	$\bar{r} = \alpha\beta(r+e) \bmod q.$

U sends $\bar{r}$ and $\bar{e}$ to the group with the authority to sign S.

c. Sign blind: Each signer calculates s_i, sends it to the TTP to calculate $\bar{s}$, and then sends $\bar{s}$ to the user as follows: $s_i = k_i\bar{e} + d_i\bar{r} \bmod q;\ \bar{s} = \sum_{i=1}^{n} s_i \bmod q.$

d. Unblind: The user calculates s. A pair (r, s) is the blind multi-signature of a signer collective for message M.

Variant 1	Variant 2
$s = (\beta\alpha^{-1}\bar{s} + \alpha e) \bmod q.$	$s = (\beta^{-1}\alpha^{-1}\bar{s} + e) \bmod q.$

e. Verify: Calculate the following: $C' = (se^{-1} \bmod q) \times G - (re^{-1} \bmod q) \times P$ and $r' = x_{C'} \bmod q.$ Compare r' and r. If $r' = r,$ then the signature will be accepted.

Proof:

V

$$s_i \times G = [(k_i\bar{e} + d_i\bar{r}) \bmod q] \times G;$$
$$C_i = k_i \times G = (s_i\bar{e}^{-1} \bmod q) \times G - (d_i\overline{re}^{-1} \bmod q) \times G;$$
$$\bar{C} = \sum_{i=1}^{m} C_i = \bar{e}^{-1} \sum_{i=1}^{m} (s_i \bmod q) \times G - \overline{re}^{-1} \sum_{i=1}^{m} (d_i \bmod q) \times G;$$
$$\bar{C} = (\overline{se}^{-1} \bmod q) \times G - (\overline{re}^{-1} \bmod q) \times P;$$
$$\bar{r} = (r\beta^{-1}\alpha) \bmod q \text{®} r = \bar{r}\beta\alpha^{-1} \bmod q;$$
$$C' = (se^{-1} \bmod q) \times G - (re^{-1} \bmod q) \times P;$$
$$C' = [(\alpha e + \beta\bar{s}\alpha^{-1})e^{-1} \bmod q] \times G - [(\bar{r}\beta\alpha^{-1}e^{-1}) \bmod q] \times P;$$
$$C' = \beta[(\overline{se}^{-1} \bmod q) \times G - (\overline{re}^{-1} \bmod q) \times P] + (\alpha \bmod q) \times G;$$
$$C' = \beta \times \bar{C} + \alpha \times G;$$
$$r' = r.$$

V

$$s_i \times G = [(k_i\bar{e} + d_i\bar{r}) \bmod q] \times G;$$
$$C_i = k_i \times G = (s_i\bar{e}^{-1} \bmod q) \times G - (d_i\overline{re}^{-1} \bmod q) \times G;$$
$$\bar{C} = \sum_{i=1}^{n} C_i = \bar{e}^{-1} \sum_{i=1}^{n} (s_i \bmod q) \times G - \overline{re}^{-1} \sum_{i=1}^{n} (d_i \bmod q) \times G;$$
$$\bar{C} = (\overline{se}^{-1} \bmod q) \times G - (\overline{re}^{-1} \bmod q) \times P;$$
$$\bar{r} = \alpha\beta(r+e) \bmod q \text{®} r = (\alpha^{-1}\beta^{-1}\bar{r} - e) \bmod q;$$
$$C' = (se^{-1} \bmod q) \times G - (re^{-1} \bmod q) \times P;$$
$$C' = [(\alpha^{-1}\beta^{-1}\bar{s} + e)e^{-1} \bmod q] \times G - [(\alpha^{-1}\beta^{-1}\bar{r} - e)e^{-1} \bmod q] \times P;$$
$$C' = [(\alpha^{-1}\beta^{-1}\bar{s}e^{-1} + 1) \bmod q] \times G - [(\alpha^{-1}\beta^{-1}\bar{r}e^{-1} - 1) \bmod q] \times P];$$
$$C' = \alpha^{-1} \bmod q \times \bar{C} + P + G \equiv C;$$
$$r' = r.$$

3.2. BMS based on the EC-Schnorr signature scheme

a. Setup: For each signer with the authority to sign S, calculate the value of the public key and send it to the TTP to calculate the public key value: $P_i = d_i \times G$, where i = 1, 2,…,n and $P = P_1 + P_2 + ... + P_n = \sum_{i=1}^{n} d_i \times G.$

Each signer with signing authority selects the random numbers $k_i (k_i \in Z_q)$, calculates C_i and then sends it to the TTP to calculate $\overline{C}$ as follows: $C_i = k_i \times G$, where i = 1, 2,…,n and $\overline{C} = \sum_{i=1}^{n} C_i = \sum_{i=1}^{n} k_i \times G.$ The authorized signers then send $\overline{C}$ to U.

b. Blind: U selects two random numbers $\alpha, \beta \in \{1,2,...,q\text{-}1\}$, and the variants are calculated:

Variant 1	Variant 2
$C = \overline{C} + \alpha \times G + \beta \times P;$	$C = \alpha \times \overline{C} + \beta \times G;$
$r = H(M, x_C) \bmod q;$	$r = H(M, x_C) \bmod q;$
$\overline{r} = (r - \beta) \bmod q.$	$\overline{r} = \alpha^{-1}(r - \beta) \bmod q.$

The users then sends $\overline{r}$ to each of the signers.

c. Sign blind: Each signer calculates s_i, sends it to TTP to calculate $\overline{s}$ and then sends $\overline{s}$ to the user as follows: $s_i = k_i - d_i \overline{r} \bmod q; \overline{s} = \sum_{i=1}^{n} s_i \bmod q.$

d. Unblind: The following variants are calculated.

Variant 1	Variant 2
$s = (\overline{s} + \alpha) \bmod q.$	$s = \alpha \overline{s} \bmod q.$

The pair (r, s) is the blind multi-signature of the signer collective on message M.

e. Verify: Calculate $C' = s \times G - r \times P; r' = H(M, x_{C'})$. If r′ = r, then the signature will be accepted.

Proof:

V

$$C' = s \times G - r \times P;$$
$$C' = (\overline{s} + \alpha) \times G + (\overline{r} + \beta) \times P;$$
$$C' = (\alpha \times G + \beta \times P + \sum_{i=1}^{n} (k_i - \overline{r} x_i) \times G + \overline{r} \sum_{i=1}^{n} x_i \times G);$$
$$C' = \overline{C} + \alpha \times G + \beta \times P;$$
$$C' \equiv C;$$
$$r' = H(M, x_{C'}) = H(M, x_C) = r.$$

V

$$C' = s \times G + r \times P;$$
$$C' = \alpha \overline{s} \times G + (\overline{r} \alpha + \beta) \times P;$$
$$C' = \alpha \sum_{i=1}^{n} (k_i - x_i \overline{r}) \times G + \alpha \overline{r} \sum_{i=1}^{n} x_i \times G + \beta \times P;$$
$$C' = \alpha \times \overline{C} + \beta \times G;$$
$$r' = H(M, x_{C'}) = H(M, x_C) = r.$$

4. ANALYSIS OF THE PROPOSED BMS SECURITY

4.1. Security Analysis

A security blind multi-signature scheme is determined by the following two characteristics: blindness and unforgeability.

Theorem 1. (Blindness) The proposed blind multi-signature schemes are blind.

Proof [16], [17]: Definition 3 is used for the proof.

First, the signature pair $(M,r,s)\in\{(M_0,r_0,s_0),(M_1,r_1,s_1)\}$ is considered one of the two signature sets for A (A acts as the signatory), and $(\bar{e},\bar{r},\bar{s})$ is the data stored in the release scheme of A. Two random parameters α, β occur and link $(\bar{e},\bar{r},\bar{s})$ to (*M*,*r*,*s*).

r always has a relation that is constant, regardless of the blinding factors α, β. Therefore, $(M,r,s)\in\{(M_0,r_0,s_0),(M_1,r_1,s_1)\}$ are selected with the stored data in the scheme A. In $(\bar{r},\bar{s})$, the (α,β) pair always occurs and is satisfied. The largest probability of choosing the right $(b'=b)$ in the release signature set $(M,r,s)\in\{(M_0,r_0,s_0),(M_1,r_1,s_1)\}$ is $\frac{1}{2}$. In addition, $\Pr[b'=b]=\frac{1}{2}$, therefore $|\Pr[b'=b]-\frac{1}{2}|<\frac{1}{p^c}$ satisfies definition 3 and the schemes are unconditionally blind.

From the schema description,

Based on the GOST R34-10-2012 standard	Variant 1	$\bar{e}=\alpha e \bmod q;\bar{r}=(r\beta^{-1}\alpha)\bmod q;$ $s=(\beta\alpha^{-1}\bar{s}+\alpha e)\bmod q;$ $\rightarrow \alpha=\bar{e}e^{-1};\beta=(s-\bar{e})\bar{e}e^{-1}\bar{s}^{-1};$ $\bar{r}=(r\beta^{-1}\alpha)\bmod q;$ $\rightarrow r=\bar{r}(s-\bar{e})\bar{s}^{-1}\bmod q.$
	Variant 2	$\bar{e}=\beta e \bmod p;\bar{r}=\beta\alpha(r+e)\bmod q;$ $s=(\beta^{-1}\alpha^{-1}\bar{s}+e)\bmod q;\beta=\bar{e}e^{-1};$ $\alpha=(s-e)^{-1}\bar{e}^{-1}e\bar{s};$ $\bar{r}=\beta\alpha(r+e)\bmod q;r=\bar{r}(s-e)\bar{s}^{-1}-e.$
Based on the EC-Schnorr signature scheme	Variant 1	$\bar{r}=(r-\beta)\bmod q;s=(\bar{s}+\alpha)\bmod q;$ $\alpha=s-\bar{s};\beta=(r-\bar{r});$ $C=\bar{C}+\alpha\times G+\beta\times P;$ $\rightarrow C=\bar{C}+(s-\bar{s})\times G+(r-\bar{r})\times P;$ $r=H(M,x_C).$
	Variant 2	$\bar{r}=\alpha^{-1}(r-\beta)\bmod q;s=\alpha\bar{s}\bmod q;$ $\alpha=s\bar{s}^{-1};\beta=r-\bar{r}s\bar{s}^{-1};$ $C=\alpha\times\bar{C}+\beta\times G;$ $C=s\bar{s}^{-1}\times\bar{C}+(r-\bar{r}s\bar{s}^{-1})\times G\bmod p;$ $r=h(M,x_C)\bmod q.$

Theorem 2. [16] The proposed blind multi-signature schemes are $(\varepsilon,t,q_h,q_e,q_s)$ in the ROM assuming that (ε',t') - DLP holds in Z_p, where: $\varepsilon'=(1-\frac{q_h(q_e+q_s)}{q})(1-\frac{1}{q})\frac{1}{q_h}\varepsilon;\ t'=t+O(q_e+q_s)E$ and (q_h,q_e,q_s) are the number of extract queries, sign queries and hashing queries, respectively; and *E* is the time for a scalar calculation operation.

Proof: Assuming that a forger A exists, algorithm B is constructed, and it employs A to solve a discrete logarithm problem. B is considered a nucleus group *G* in *GF*(*p*) with the element *G* and a prime *q*, and point *Q* is on the elliptic curve. B is asked to find $x\in Z_q$ such that $Q=x\times G$. B can be solved as follows: B chooses the hash function value $h=H\in\{0,1\}^*\rightarrow Z_q$ and then sends the public parameters (*p*, *G*, *Q*, *e*) to A and B selects two random parameters (*k*′,*d*′) to calculate the following

Based on the GOST R34-10-2012 standard	Variant 1	$C^* = k' \times Q + d' \times G.$
	Variant 2	$C^* = k'^{-1} \times Q + G + P.$
Based on the EC-Schnorr signature scheme	Variant 1	$C^* = Q + d' \times G + k' \times P'.$
	Variant 2	$C^* = k' \times Q + d' \times G.$

d' is defined as the private key (secret) of the signer, k' is a value that is randomly selected and (k', d', C^*) are the outputs.

A queries the signing Oracle for message M and the identity d'. B checks whether d' has been previously queried for the ROM. If yes, then sets are retrieved from the table, and these values are used to sign message M according to the signing phase that was described in the scheme. The signature $(M, \overline{r'}, \overline{s'})$ is output. If d' has not been queried by the extraction Oracle, then B executes the simulation of the extraction Oracle and uses the corresponding secret key to sign message M.

Adversary A outputs the forged signature $s_1^* = (e, \overline{r'}, \overline{s_1'})$ for the message M with the secret key d'. B retains $(e, \overline{r'})$ and in return asks A to re-sign the message to obtain $s_2^* = (e, \overline{r'}, \overline{s_2'})$.

Based on the GOST R 34-10-2012 standard

	We have: $C^* = (se^{-1} \bmod q) \times G - (re^{-1} \bmod q) \times P;$
	with $P = d \times G.$
Variant 1	$k' \times Q + d' \times G = (s_j^* e^{-1} \bmod q) \times G - (re^{-1} \bmod q) \times P;$
	$k'x \times G + d' \times G = (s_j^* e^{-1} \bmod q) \times G - (re^{-1} \bmod q) d' \times G;$
	$s_j^* = e(k'x + d') + rd'.$
	We have: $C^* = (se^{-1} \bmod q) \times G - (re^{-1} \bmod q) \times P;$
	with: $P = d' \times G.$
Variant 2	$k'^{-1} \times Q + G + P = (se^{-1} \bmod q) \times G - (re^{-1} \bmod q) \times P;$
	$xk'^{-1} + d' + 1 = s_j^* h^{-1} - rh^{-1} d';$
	$s_j^* = h(xk'^{-1} + d' + 1) + rd'.$

Based on the EC-Schnorr signature scheme

	We have : $C^* = s \times G + r \times P.$
Variant 1	$Q + k'd' \times G + d' \times G = s_j^* \times G + r \times P;$
	$x \times G + k'd' \times G + d' \times G = s_j^* \times G + rd' \times G;$
	$s_j^* = x + d'k' - rd' + d'.$
	We have: $C^* = s \times G + r \times P.$
Variant 2	$k' \times Q + d' \times G = s \times G + r \times P;$
	$xk' + d' = s_j^* + rd';$
	$s_j^* = xk' + d' - rd'.$

The output is the linear equation x, which solves the discrete logarithm problems.

4.2. Probability Analysis

A probability analysis is performed, and the results indicate that the right hash function value is $1 - \frac{q_h}{q}$ and is completed in $(q_e + q_s)$ iterations. Thus, $(1 - \frac{q_h}{q})^{q_e + q_s} \geq 1 - \frac{q_h(q_e + q_s)}{q}$. B can determine a strict point to reselect the hash function value with a probability of $\frac{1}{q_h}$. In the ROM, the ideal probability value

that does not equate to signature s is $\frac{1}{q}$. ε' was obtained with a successful probability as $\varepsilon' = (1-\frac{q_h(q_e+q_s)}{q})(1-\frac{1}{q})\frac{1}{q_h}\varepsilon$. The time complexity of algorithm B based on the exponentiation function performed in the extract and sign phase is equal to $t' = t + O(q_e + q_s)E$.

4.3. Performance Analysis

The efficiency of two proposed BMS models with two other schemes [6, 18] is determined with the assumption that these schemes must be calculated with the same security parameters used for Z_p and include "*n"* member signers.

Notations:

T_h time cost of a hash operation in Z_p.

T_s time cost of a scalar multiplication in Z_p.

T_{inv} time cost of an inverse operation in Z_p.

T_m time cost of a modular multiplication in Z_p.

T_+ time cost of a extra points in Z_p.

The computational costs for the two signed regression schemes is as follows: According to [4], $T_h \approx T_m; T_s \approx 29T_m; T_{inv} \approx 240T_m; T_+ \approx 0,12T_m$.

Table 1. Performance comparison of the different schemes

	BMS based on the GOST R34.10-2012 standard		BMS based on the EC-Schnorr signature scheme		[6]	[4]
	Variant 1	Variant 2	Variant 1	Variant 2		
Setup	$59nT_m$	$59nT_m$	$59nT_m$	$59nT_m$	$59nT_m$	$59nT_m$
Blind	$302T_m$	$245T_m$	$58T_m$	$245T_m$	$332T_m$	$245T_m$
Blind sign	$2nT_m$	$2nT_m$	nT_m	nT_m	$2nT_m$	$2nT_m$
Unblind	$243T_m$	$482T_m$	Negligible	T_m	$483T_m$	T_m
Verify	$482T_m$	$482T_m$	$58T_m$	$58T_m$	$482T_m$	$88T_m$
Total	$1027T_m$ $+61nT_m$	$1169T_m$ $+61nT_m$	$116T_m$ $+60nT_m$	$304T_m$ $+60nT_m$	$1197T_m$ $+61nT_m$	$334T_m$ $+61nT_m$

The following results are based on the comparison Table 1. We realized that the time cost of the proposed blind multi-signature scheme based on the GOST R34.10-2012 standard according to Variant 1 and 2 has a higher computational complexity than the proposed blind digital signature scheme based on the EC-Schnorr digital signature scheme.

The time cost of the proposed scheme based on the GOST R34.10-2012 standard has lower computational efficiency than another scheme [6], and the proposed scheme based on the EC-Schnorr scheme has lower computational efficiency than the other scheme [6], [4].

When comparing the performance on a per-standard digital signature scheme, the performance of the proposed blind multi-signature has better computational efficiency.

5. CONCLUSION

In this paper, we presented options for building blind multi-signature signature schemes based on the GOST R34.10-2012 digital signature standard and the EC-Schnorr digital signature scheme. The blind multi-signature signature schemes were developed that inherits the security and the properties of digital signature standards in practice. The proofs of the proposed schemes were full blindness and unforgeability in the ROM. The results show that the proposed blind multi-signature signature schemes are safe and present high performance; therefore, they can be applied in practice.

REFERENCES

[1] Chaum D, "Blind signatures for untraceable payments", Advances in Cryptology, Crypto'82, Plenum (1983) 199-203

[2] N. Koblitz (1987), "Elliptic curve cryptosystems", *Mathematics of Computation*, Vol.48, pp.203-209.

[3] GOST R 34.10-2012, "Digital Signature Algorithm draft-dolmatov-gost34102012-00, V. Dolmatov, Ed, (2013).

[4] Popescu C, "Blind Signature and BMS Using Elliptic Curve"s. Studia univ. "babes¸–bolyai", Informatica. (1999) 43-49

[5] S. S. Chow et al. (2005), "Two Improved Partially Blind Signature Schemes from Bilinear Pairings", *Information Security and Privacy*, 3547, pp. 316–328.

[6] Moldovyan, N.A., "Blind Signature Protocols from Digital Signature Standards", *International Journal of Network Security* (2011) 22-30

[7] T. A. T. Nguyen and T. K. Dang (2013), "Enhanced security in internet voting protocol using blind signature and dynamic ballots", *Electronic Commerce Research*, 13.

[8] Swati Verma, Birendra Kumar Sharmal (2012), "New Proxy Blind Multi Signature based on Integer Factorization and Discrete-Logarithm Problems", http://journal.portalgaruda.org/index.php/EEI, Vol.1, pp 185~190.

[9] S. Panda et al. (2013), "An Application of time stamped proxy blind signature in e-voting", *International Journal on Computer Science and Engineering*, 5 (6), pp. 547–552.

[10] Hua Sun, Yanqiang Ge (2014), "New Certificateless Blind Ring Signature Scheme", *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, Vol.12, No.1, pp 778-783

[11] Shilbayeh, N.F., Al-Saidi, R.A., Alsswey, A.H., "Evaluation and Analysis of the Secure E-Voting Authentication Preparation Scheme", *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, (2016) 560-568.

[12] Minh, H., Hai, N., Moldovyan, N., Giang, T., "New Blind Signature Protocols Based on a New Hard Problem", *The International Arab Journal of Information Technology*, Vol. 14, No.3, May 2017.

[13] Salome James, T. Gowri, G.V. Ramesh Babu, P. Vasudeva Reddy (2017), "Identity-Based Blind Signature Scheme with Message Recovery", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 7, No. 5, pp2674-2682.

[14] Darrel Hankerson, Alfred Meneze, Scott Vanstone (2004), Guide to EllipticCurve Cryptography, Springer, NewYork, USA.

[15] Bellare, M., Rogaway, P., *"Random oracles are practical: a paradigm for designing efficient protocols"*, Proceedings of the 1st ACM conference on Computer and communications security. (1993) 62–73

[16] Liu, J.K., Baek, J, Zhou, J., Yang, Y., Wong, J.W., "Efficient online/offline identity-based signature for wireless sensor network", *International Journal of Information Security*, (2010) 287-296

[17] Chun-I Fan, Wei-Zhe Sun, Vincent Shi-Ming Huang (2010), "Provably secure randomized blind signature scheme based on bilinear pairing".

[18] D. Schroder (2010), On the Complexity of Blind Signatures, Technischen Universitat Darmstadt genehmigte.