Blind Signature Schemes based on ElGamal Signature for Electronic Voting: A Survey

Monira M. Khater
Computer Science Department
Faculty of Computer & Informatics, Benha University
Benha, Egypt

Ayman Al-Ahwal
Communication and Electronics
Pyramid-Institute for Engineering and Technology
Egypt

Mazen M. Selim
Computer Science Department
Faculty of Computer & Informatics, Benha University,
Benha, Egypt

Hala H. Zayed
Computer Science Department
Faculty of Computer & Informatics, Benha University,
Benha, Egypt

ABSTRACT
The Electronic Voting (E-Voting) became a truly crucial part in the democracy of our life in which the election data is recorded, stored and prepared fundamentally as computerized data. Important basic properties of E-Voting are eligibility, privacy, fairness, uniqueness, receipt-freeness and verifiability. In addition to properties of blind signature such as correctness, blindness, anonymity and unforgeability. Blind signature allows to obtain a signature from the signer who signs a message without reading the content of the message. This paper presented a survey on blind signature schemes based on ElGamal Signature. The aim of this paper is to compare the existing blind signature schemes based on modifications of their parameters such as blinding factor, blinded message, blind signature, and Signature pair that satisfy these basic properties.

Keywords
E-Voting, Blind signature, ElGamal signature, universally forgeable Attack

1. INTRODUCTION
Recently, the research on E-voting becomes a very important topic in the advance of democracy. E-voting is the voting process held over electronic media, which give voters the right to cast a secret ballot over the Internet. E-voting is more comfortable for the voters in that it allows voters to vote from any poll site in the country. It can increase the participation of disabled people [1, 2]. Although E-voting is more comfortable and easier for voters than the conventional voting, yet it additionally more vulnerable than the conventional voting due to the nature of digital processing of election data which can be easily spread, manipulated within the network, hence that may result in widespread fraud and corruption [3]. So it isn't an easy task to achieve secure E-voting system. There are so many properties that have been proposed to make the E-voting a secure process. Some of these properties that must be satisfied are shown as follow:

- **Eligibility:** Only eligible voters are permitted to cast their ballots.
- **Uniqueness:** No voter can cast his ballot more than once.
- **Privacy:** No person can access the information about the voters vote.
- **Receipt-freeness:** A voter should not have any information which can be utilized to demonstrate to a coercer that he voted to prevent vote purchasing or selling.
- **Fairness:** No partial result is available before the final result comes out.
- **Mobility:** there are no restrictions on the location from which voters can cast their ballots.
- **Anonymity:** Guarantee that no link between the voter's identity and the marked ballot [4 - 7].
- **Correctness:** Anyone can independently verify that all votes have been counted correctly by using the signer public key.
- **Blindness:** The content of the ballot should be blinded to the authority when he signs the ballot.
- **Unforgeability:** Only the Authority can give a valid signature for the associated ballot [8, 9].

Blind signature is one of the most popular cryptographic techniques in E-voting system (EVS) that guarantee the anonymity of the voters. Blind signature allows a document to be signed without revealing its contents. The impact is like putting a document and a sheet of carbon paper inside of the envelope [10]. If someone signs the outside of the envelope, he also signs the document on the inside of the envelope. When document is removed from the envelope, the signature remains attached to it [6] .The first electronic election scheme was proposed by David Chaum in (1982) based on the RSA algorithm [10,11].

In this paper a survey of blind signature schemes for E voting that is based on ElGamal Algorithm is carried out. Because of ElGamal signature is accepted to be a secure and efficient public-key cryptosystem, it has an important property that ensures if a message is signed multiple times; the corresponding signatures are different [12].

This paper is organized as follow: Section 2 briefly introduces ElGamal digital signature scheme. Section 3, explains an overview of Blind Signature Scheme. Section 4, briefly introduces the literature survey and security analysis. Discussion is shown on section 5. Finally section 6, presents the conclusion and future work.

2. ELGAMAL DIGITAL SIGNATURE SCHEME
A digital signature is an electronic signature that demonstrate the authenticity of an electronic document or message in digital communication and uses encryption techniques to give confirmation of original and unmodified documentation [11]. Two main properties are required in digital signature namely, authentication, data integrity. In the digital signature scheme, there are two participants, namely, the signer and the verifier. The signer uses his private key to sign a document and then

sends this signature to the verifier. The verifier receives the signature, then he uses a public key to verify the validity of the signature [11, 13].

ElGamal Algorithm is one of the digital signature schemes. It was invented by Taher ElGamal [14] in (1984). It is based on the difficulty of solving discrete logarithm problem (DLP). ElGamal signature scheme was discussed as in [13-15]. There were two participants, namely, the signer and the verifier and three phases, namely key generation, signing, and verification. In key generation phase, parameters of the signer are initialized. In signing phase, the signer uses his private key to sign a document and then sends this signature to the verifier. In verification phase, the verifier uses signer's public key to verify the validity of the signature, which can be summarized as in scheme (1).

Scheme 1. ElGamal scheme

key generation	1. Signer chooses large prime numbers $\boldsymbol{p}$ in Galois field $\boldsymbol{Z_p}$, $\boldsymbol{g}$ is the Primitive root $\boldsymbol{of\ p} \in \boldsymbol{Z_p}$ and $\boldsymbol{x} \in \boldsymbol{Z_p}$ randomly as his private key. 2. Compute $\boldsymbol{y = g^x\ mod\ p}$ as his public key. 3. Publish $\boldsymbol{p, g, y}$ in public, but keep the private key $\boldsymbol{x}$ in a secret.
Signing	1. Signer randomly chooses integer $\boldsymbol{k}$, $(\boldsymbol{k < p})$ $\in \boldsymbol{Z_p}$and $\boldsymbol{gcd\ (k, p-1) = 1}$ 2. Compute $\boldsymbol{r = g^k\ mod\ p}$ and $\boldsymbol{s = k^{-1}(m - xr)\ mod\ (p-1)}$ where $\boldsymbol{m}$ is the message and $(\boldsymbol{r}, \boldsymbol{s})$ is the final signature. 3. Send the final signature$(\boldsymbol{r, s})$, $\boldsymbol{m}$ to the verifier.
Verification	1. From the public key $(\boldsymbol{p, g, y})$,Verifier check $\boldsymbol{g^m \equiv y^r r^s\ mod\ p}$ to verify the validity of the signature $(\boldsymbol{r, s})$

3. BLIND SIGNATURE SCHEME

Blind signature scheme is an extension of the digital signature scheme which allows a requester to get a signature from a signer without revealing any information about the message it signed [13]. The blind signature scheme must achieve four requirements, namely, Correctness, Blindness, Unforgeability and Anonymity. Blind signature scheme has three participants, namely, the signer, the requester and the verifier. It has five phases (see Figure 1), it is described as follow [8, 11, and 16].

- **Initialization (Key generation):** All the system parameters of both requester and signer are initialized in this phase.
- **Blinding:** The requester blinds the message by selecting a blind factor and sends the blind message to the signer.
- **Signing:** Once the signer gets the blinded message, he use his private key to sign it and then sends back the blind signature to the requester.
- **Unblinding***:* Once the requester receives it, he uses his blind factor to recover the signer's digital signature from the blinded message and sends it to the verifier.
- **Verifying:** verifier can use the signer's public key to verify whether the signature is authentic or not.

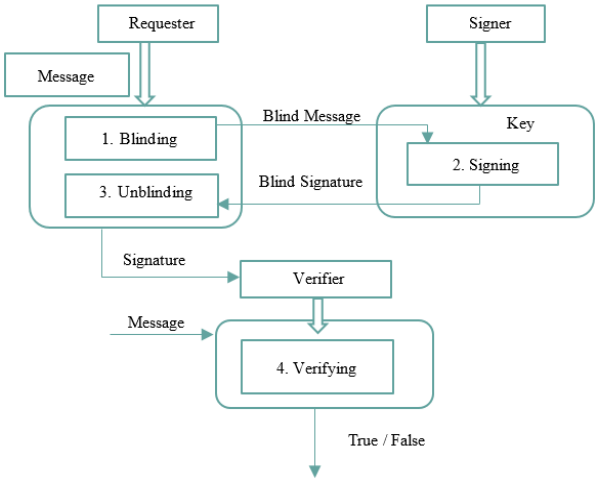

Fig 1: Flow of blind signature [11]

4. LITERATURE SURVEY

There are several studies have been carried out in the last few years that based on ElGamal digital signature scheme such as:

4.1 R. L. Shen, et al.'s Scheme

He presented a blind signature scheme based on the DLP and the modified ElGamal signature in [13].There are 18 modified ElGamal digital signature schemes shown by Dr. L. Harn [17]. (See table 1 in [17]), the modified ElGamal digital signature scheme No.15 was the basis for the proposed blind signature scheme.

The signature equation for the modified ElGamal signature represented as $ax = bk + c\ mod\ p - 1$, and the verification equation could be: $y^a = r^b g^c\ mod\ p$, where (a, b, c) are the three parameters from the set of values(m, r, s), each parameter (a, b, c)could be a mathematical combination of (m, r, s), with certain criteria for the combination between these parameters. The signature and verification equations that were the basis for R. L. Shen, et al.'s scheme were shown below.

Signature equation: $sx = k + (m + r)$, Verification equation: $y^s = r g^{r+h(m)}\ mod\ p$

In this scheme, there are three participants, namely, the requester, the signer, and the verifier; and five phases, namely, (1) initialization phase, 2) blinding phase, (3) signing phase, (4) unbinding phase and (5) verification phase were described as follow:

Initialization phase: The signer chooses a large prime p and g as a primitive root of p. Then randomly chooses a number x $(2 < x < (p-2))$ to computes $y = g^x\ mod\ p$. the signer publishes (y, g, p) as the public key, keeps x as the private key, and chooses a one-way hash function $h(.)$ such as SHA-1 or MD5.

Blinding phase: First, the requester sends a request to the signer for signing message m .

The signer choose random number k', such that $gcd\ (k', p-1) = 1$ and computes $r' = g^{k'}\ mod\ p$ then sends r' to the requester.

The requester chooses the set of values(a, b, c) are relatively prime to $(p-1)$ and computes $r = r'^a\ y^b g^c\ mod\ p$ and

$h\,(m)$ generated by the hash function $h\,(.)$. Next he blinds the value $h\,(m)$ with the blind equation $m' = a^{-1}\,(\mathrm{c} + h\,(m) + \mathrm{r}) - r'\,mod\,(p-1)$,then he sends the value m' to the signer.

Signing phase: After the signer receives the value m', he computes $\mathrm{s}' = x^{-1}\left(k' + \left(m' + r'\right)\right)\,mod(\,p-1)$. Then he sends the value s' to the requester.

Unblinding phase: The requester computes $s = a\,s' + b\,mod\,(p-1)$, after receiving s' from the signer, to obtain the message-signature(m, r, s). Then he send the message-signature pair (m, r, s) to the verifier.

Verifying phase: When the verifier receives the message-signature pair(m, r, s), he use the one-way hash function $h\,(.)$ and the public key (y, g, p) to verify the legitimacy of the signature by checking, $v_1 = y^s\,mod\,p$

$$v_2 = r g^{r+h(m)}\,mod\,p$$

If $v_1 = v_2$, then the verification passes; else the verification fails.

4.1.1 Security Analysis

In this section we show that R. L. Shen, et al.'s scheme in [13]satisfied all the requirements of blind scheme namely, Correctness, Blindness, Unforgeability, and Anonymity.

- **Correctness:** The following steps confirm the verification equation $y^s = r\,g^{\,h\,(m)+r}\,mod\,p$

$$g^{\,xs} \equiv g^k g^{r+h(m)}\,mod\,p$$

$$xs \equiv k + r + h(m) mod\,p-1$$

$$x\left(a\,s' + b\right) \equiv a\,k' + bx + c + r + h(m) mod\,p - 1$$

$$xas' \equiv a\,k' + c + r + h(m)\,mod\,p-1$$

$$a\left(x\,s' - k'\right) \equiv c + h(m) + r\,mod\,p-1$$

Multiplied simultaneously by a^{-1}

$$\left(xs' - k'\right) \equiv a^{-1}(c + h(m) + r) mod\,p-1$$

Subtracted simultaneously by r'

$$x\,s' - k' - r' \equiv a^{-1}(c + h(m) + r) - r'\,mod\,p-1$$

$$x\,s' - k' - r' \equiv m'\,mod\,p-1$$

$$s'x \equiv k' + m' + r'\,mod\,p-1.$$

- **Blindness:** The signer cannot obtain the message m from blinded equation $m' = a^{-1}\,(\mathrm{c} + h\,(m) + \mathrm{r}) - r'\,mod\,p-1$, because the signer has three unknown parameters, namely, $a, c\ and\ r$, so the signature scheme is blind.
- **Unforgeability:** No one can forge a valid signature pair (r, s) on the message m to pass the verification, because it is very difficult to solve the discrete logarithm problem.
- **Anonymity:** If the signer wants to trace the blind signature, he keeps the set of values(m', r', s'). When the requester publishes the message-signature pair (m, r, s) in public, the signer unable to obtain any information from the set of values that he keeps. Because the signer does not know the values including $a, b, c\ and\ r$, he cannot link the relation between the message-signature pair and the blind signature.

4.2 Dameri et al.'s Scheme

He proposed blind signature scheme based on modified ElGamal signature in [18]. He pointed that this scheme is not only increases the security but also decreases the complexity of calculation in blind signature.

In this scheme, there are three participants, namely, the requester, the signer, and the verifier; and five phases, namely, (1) initialization phase, 2) blinding phase, (3) signing phase, (4) unbinding phase and (5) verification phase were described as follow:

Initialization Phase: The signer chooses large prime number p and the Primitive root $g \in Z_p *$. He chooses $x \in Z_p *$ as the private key where $x < p$, and compute $y = g^x\,mod\,p$ then publish p, g, y in public.

Blinding phase: Requester blinds message m by choosing blinding factor $h \in z_p$ randomly.

$m' = m + h\,mod\,(p-1)$, then he sends m' to the signer.

Signing phase: After the signer receives m', he chooses a random number $k(k \in Z_{p-1} *)$ to calculate $s' = \left(m' - (x + k)\right)r\,mod\,(p-1)$ and $r = g^k\,(mod\,p)$, then he sends (s', r) to the requester.

Unblinding phase: the requester receives blind signature s' from the signer and computes $s = s' - rh\,mod\,p-1$.Then he sends message m and signature pair (s, r) to verifier.

Verifying phase: The verifier use the signer's public key to verify the legitimacy of the signer's signature by checking whether $g^{rm} = g^s (yr)^r\,mod\,p$

4.2.1 Security Analysis

Mala, Hamid, et al [19], pointed out that Dameri et al.'s scheme is universally forgeable, everyone can forge a valid signature on an arbitrary message without knowing the signer's private key, Assume an attacker has eavesdropped a valid message/signature m and (s, r) . He can make a valid signature on message m', by following these steps:

Compute $k' = m' - m\,mod\,(p-1)$, and

$r' = r g^{k'} = g^{k+k'}\,mod\,p$,then compute s' as below:

$$s' = s * \left(\frac{r'}{r}\right) = \left(m - (k + x)\right)r'$$

$$= \left(\left(m + k'\right) - \left(k + k' + x\right)\right)r'$$

$$= \left(m' - \left(k + k' + x\right)\right)r'\,mod\,p-1$$

Finally, $\left(s', r'\right)$ are verified as a valid signature for message m', since the verification equation is satisfied as blow:

$$s' = \left(m' - \left(k + k' + x\right)\right)r'\,mod\,p-1$$

$$r'm' = s' + \left(k + k' + x\right)r' mod\,p-1$$

$$g^{r'm'} = g^{s'} g^{(k+k'+x)r'} mod\,p-1$$

$$g^{r'm'} = g^{s'}(g^x g^{k+k'})^{r'}$$

$$g^{r'm'} = g^{s'}(yr')^{r'}\,mod\,p$$

So, Dameri et al.'s scheme is unsecure.

4.3 Biswa Bhusan Biswal, et al.'s Scheme

He proposed blind signature scheme based on DLP and the modified ElGamal signature in [20], this scheme was less complexity and faster than other schemes by reducing the number of mathematical operations. (See table 1 in [17]), the modified ElGamal digital signature scheme No.7 was the basis for Biswa Bhusan Biswal, et al.'s scheme.

In this scheme, there were three participants, namely, the requester, the signer, and the verifier; and five phases, namely, (1) initialization phase, 2) blinding phase, (3) signing phase, (4) unbinding phase and (5) verification phase. This scheme was described as follow:-

Initialization phase: The signer randomly selects large primes p_1 & p_2 such that $n = p_1\, p_2$,$p = 2n + 1$ and p is prime. Then he selects private keys x , k & public keys $y = g^x mod\ p$, and $r' = g^k mod\ p$, where g is a primitive root of p. Then he sends public key set (p, g, y, n, r') to the requester.

Blinding phase: He selects private keys a, b & c randomly and computes

i. $r = h(r'\, g^a y^b \bmod p, m)$, where $h(.)$ is a cryptographic hash function (preferably SHA-512).

ii. $m' = r + b \bmod n$

iii. $z = g^c \bmod p$, then he sends the blinded message m' to the signer.

Signing phase: After receiving m' from requester, the signer computes $s' = (k + m'x) \bmod n$ and sends s' to requester.

Unblinding phase: After receiving s', the requester computes $s = s' + a + c \bmod n$, then he sends (r, s, z) as the Blind signature on message m, to the verifier.

Verification phase: Given(m, r, s, z), the legitimacy of the signature (r, s) for the message m is verified by examining the verification equation:

$$h(g^s y^{-r}\, z^{-1} mod\ p, m) mod\ n = r\ mod\ n$$

4.3.1 Security Analysis

In this section we show that the security of this scheme was based on both the strength of the hash function and the difficulty of computing the discrete logarithm problem. So this scheme satisfied all the requirements of blind signature scheme namely, Correctness, Blindness, Unforgeability, and Anonymity [20].

- **Correctness:** The proof of equality is as follows:-

$$h(g^s y^{-r}\, z^{-1} mod\ p, m) mod\ n$$

$$= h(g^{s'+a+c}\, y^{-r}\, z^{-1} mod\ p, m) mod\ n$$

$$= h(g^{k+m'x}\, g^a g^c y^{-r}\, z^{-1} mod\ p, m) mod\ n$$

$$= h(g^{k+(r+b)x}\, g^a g^c y^{-r}\, z^{-1} mod\ p, m) mod\ n$$

$$= h(g^k\, g^{rx} g^{bx} g^a g^c y^{-r}\, z^{-1} mod\ p, m) mod\ n$$

$$= h(r' y^r y^b g^a z\, y^{-r}\, z^{-1} mod\ p, m) mod\ n$$

$$= h(r' y^b g^a mod\ p, m) mod\ n$$

$$= r\ mod\ n$$

- **Blindness:** Random parameters a , b and c, were ambiguous to the signer, they used to blind the message m as $m' = r + b\ mod\ n$, and $r = h(r'\, g^a y^b\ mod\ p, m)$. The signer cannot obtain $h(m)$, from m' , so the signature scheme was blind.
- **Unforgeability:** Its strength is based on the difficulty of solving the DLP, given $y\ and\ g$, it is impossible to compute x (private key) from $y = g^x\ mod\ p$ and infeasibility of inverting the hash function to get the message from it. For passing verification equation: $h(g^s y^{-r}\, z^{-1} mod\ p, m)\ mod\ n = r\ mod\ n$, successfully an Attacker had to randomly choose any two values from (s, r, z) , and computed the third one.It was infeasible to find the third one, due to the hash function and the difficulty of solving DLP.
- **Anonymity:** In this scheme , it is impossible for the signer to trace the blind signature , which was demonstrated as follows: For each blinded message that was sent to the signer , he could keep a record of the values : (m', s') , and when the requester revealed (s, r, z, m) to receiver in public , he could calculate a value , b' from $m' - r\ mod\ n$. But from s, s' , he could calculate $s - s' = a' + c' mod\ n$. From z, he couldn't calculate c' due to the difficulty of discrete logarithm problem. So, since $c'$was unknown, a' couldn't be calculated, so he couldn't trace the message by using $r = h(r'\, g^a y^b\ mod\ p, m)$.

4.4 Hamid Mala, et al.'s Scheme

He proposed blind scheme based on the DLP and the modified ElGamal signature in [19]. In [17] , (See table 1), the modified ElGamal digital signature scheme No.7 was the basis for Hamid Mala, et al's scheme. It is variation of Nyberg-Rueppel Signature Scheme [21] [22]. In this scheme, there were three participants, namely, the requester, the signer, and the verifier; and five phases, namely, (1) initialization phase, 2) blinding phase, (3) signing phase, (4) unbinding phase and (5) verification phase were described as follow:

Initialization phase: The signer chooses $\boldsymbol{x \in Z_p^*}$, randomly as his private key and compute $\boldsymbol{y = g^x\ mod\ p}$ as the public key, where g is a Primitive root of $\boldsymbol{Z_p^*}$

Blinding phase: The requester sends a request message to the signer.

Then the signer chooses $k \in Z_p^*$ randomly to compute $r' = g^k\ modp$ and sends r' to the requester.

The requester chooses $a\ and\ b$ at random and computes blinding factor: $r = r'^a g^b\ modp = g^{ak+b}\ modp$ .Then requester blinds the hash of message m, by computing: $m' = a^{-1} rh(m) mod\ p - 1$where $h(.) : \{0,1\}^* \in Z_p^*$ is a cryptographic hash function. Then he sends m' to the signer.

Signing phase: The signer computes the signature of the blinded message as: $s' = m'x + k\ mod\ p - 1$ Then he sends the result back to the requester.

Unblinding phase: the requester extracts the signature of message m from the signature of the blinded message, by computing: $s = as' + b\ modp - 1$ .Then he declares the pair (r, s) as the signature of message m.

Verification phase: Given(m, r, s), the legitimacy of the signature (r, s) for the message m is verified by examining the verification equation: $g^s = r\, y^{r\, h(m)} modp$.

4.4.1 Security Analysis

In this section we show that Hamid Mala, et al.'s scheme in [19] satisfied all the requirements of blind signature scheme namely, Correctness, Blindness, Unforgeability, and Anonymity.

- **Correctness:** We prove the correctness of the verification equation is as follows:

$$\begin{aligned} g^s &= g^{as'+b} mod p \\ &= g^{a(xm'+k)+b} \ mod p \\ &= g^{a(xa^{-1}rh(m)+k)+b} \\ &= g^{xrh(m)} g^{ak} g^b \\ &= y^{rh(m)} r'^a g^b \\ &= r\, y^{rh(m)} \end{aligned}$$

- **Blindness:** From blinded message $m' = a^{-1} r\, h(m) \ mod p - 1$. Random integers$(a, r)$ both unknown to the signer, so the signer cannot know the content of message.
- **Unforgeability:** Based on the difficulty of computing the discrete logarithm problem over a large finite field Z_p^*, so this scheme is unforgeable.
- **Anonymity:** Suppose the malicious signer has kept a set record $\{k'_i, r', m'_i, s'_i\}$for all the blinded messages. When requester reveals $\{m_j, r_j, s_j\}$ in public. The signer unable to own any information from the set of values that he keeps. Because the signer does not know the values including a *and* b .He cannot link the relationship between the message-signature pair and the blind signature.so the scheme signature satisfies anonymity.

4.5 Chanchal Chandra, et al.'s Scheme

He proposed blind scheme based on DLP and the modified ElGamal signature in [15], this scheme had less computational overhead and short signature length.

In this scheme, there were three participants, namely, the requester, the signer, and the verifier; and five phases, namely, (1) initialization phase, 2) blinding phase, (3) signing phase, (4) unbinding phase and (5) verification phase were described as follow:

Initialization phase: Signer chooses big prime number $p \in Z_p^*$, q is a prime factor of $(p-1)$, and $g \in Z_q^*$ as primitive root of q. He choose his private key $x_a \in Z_q^*$and publish $y_a = g^{x_a} \pmod p$ in public. Requester chooses his private key $x_b \in Z_q^*$ and publishes his public key $y_b = g^{x_b} \pmod p$ in public.

Blinding Phase: Signer select two numbers k, β randomly in Z_q^* to compute $r' = g^k \ (mod\ p)$, $r = (k + r' x_a) \ (mod\ p)$, and $v = g^{-r\beta} \ (mod\ p)$ then send v to requester.

Requester chooses random numbers (α, c) as blind factors and use the one-way hash function $h(.)$ to computes $z = g^c \ (mod\ p)$ and blind message $m' = h\left(m, (z^{c^{-1}x_b})\left(y_b^{\ r\, x_b^{-1}}\right) vzg^{-\alpha}\right) mod\ p)$, then requester sends blind message m' to signer.

Signing Phase: Signer calculate blind signature $s' = (m' + \beta)r \ \ (mod\ p)$, then sends (r, s') to the requester.

Unblinding Phase: Requester computes digital signature $s = (s' - c - a)\ (mod\ q)$, then send the message m, blind message m' and signature pair $(r, s)$to the verifier.

Verification Phase: From the public (p, g, y_b), verifier computes $t'' = h\left(m, y_b . g^{r(1+m')} . g^s\right) mod\ p$

Check if $t'' = m'$ so accepts.

4.5.1 Security Analysis

In this section we show that the strength of this scheme was based on difficulty of solving DLP in addition to complex hash function. It satisfied all the requirements of blind signature scheme namely, Correctness, Blindness, Unforgeability, and Anonymity.

- **Correctness:** Prove verification of the proposed scheme as follow.

$$m' = h\left(m, (z^{c^{-1}x_b})\left(y_b^{\ r\, x_b^{-1}}\right) vzg^{-\alpha}\right) mod\ p$$

$$m' = h\left(m, (g^{c\, c^{-1} x_b})\left(g^{x_b\ r\, x_b^{-1}}\right) vzg^{-\alpha}\right) mod\ p$$

$$m' = h(m, (g^{x_b})(g^{\ r}) vzg^{-\alpha}) \ mod\ p$$

$$m' = h(m, (g^{x_b})(g^{\ r}) g^{-r\beta} g^c g^{-\alpha}) \ mod\ p$$

$$m' = h(m, (g^{x_b})(g^{\ r}) g^{-r\beta} g^{s'-s-\alpha} g^{-\alpha} \ mod\ p$$

$$m' = h(m, (g^{x_b})(g^{\ r}) g^{-r\beta} g^{(m'+\beta)r-s-\alpha} g^{-\alpha} \ mod\ p$$

$$m' = h(m, (g^{x_b})(g^{\ r}) . g^{(rm')-s-\alpha} g^{-\alpha} \ mod\ p$$

$$m' = h(m, (g^{x_b})\left(g^{\ r\,(m'+1)}\right) . g^{s+\alpha} g^{-\alpha} \ mod\ p$$

$$m' = h(m, (g^{x_b})\left(g^{\ r\,(m'+1)}\right) . g^s mod\ p$$

$$\therefore \ m' = t''$$

- **Blindness:** From the blinded equation $m' = h\left(m, (z^{c^{-1}x_b})\left(y_b^{\ r\, x_b^{-1}}\right) vzg^{-\alpha}\right) mod\ p$, there are three ambiguous parameters, namely a, c and x_b, the signer unable to get message m from m', *so* this scheme is blind.
- **Unforgeability:** Its security is based on DLP and IFP, so it is impossible to attack to obtain private keys. It is resistant against forgery attack such as existential and selective forgery.
- **Anonymity:** Signer cannot link the relationship between the message m -signature pair(r, s) and the blind signature s', because the signer does not know the values including a, b, c *and* x_b, although he keeps the set of values(m', s') and the requester put (m, r, s) in public.

5. DISCUSSION

As stated at the section 4 of this paper, we presented R. L. Shen, et al.'s [13], Dameri et al.'s [18], Biswa Bhusan Biswal, et al.'s [20], Hamid Mala et al.'s [19], and Chanchal Chandra et al.'s [15] schemes. Based on modifications of parameters such as blinding factor, blinded message, blind signature and Signature pair for comparison between those schemes as shown in table 1 and table 2, the Correctness property was satisfied in R. L. Shen, et al. [13], Dameri et al. [18], Biswa Bhusan Biswal, et al. [20], Hamid Mala, et al. [19], and Chanchal Chandra, et al. [15] schemes.

Blindness property was satisfied in R. L. Shen, et al, Dameri et al, Biswa Bhusan Biswal, et al, Hamid Mala, et al, and Chanchal Chandra, et al. schemes.

Unforgeability property was satisfied in R. L. Shen, et al, Biswa Bhusan Biswal, et al, Hamid Mala, et al, and Chanchal Chandra, et al. schemes but wasn't satisfied in Dameri et al.'s scheme.

Finally Anonymity property was satisfied in R. L. Shen, et al, Dameri et al, Biswa Bhusan Biswal, et al, Hamid Mala, et al, and Chanchal Chandra, et al Schemes. The scheme becomes also more secure when the blind factor has a higher value as shown in table 3.

In addition to we compared the existing schemes from computational complexity, the R. L. Shen, et al.'s scheme has numbers of operations (6 modular multiplication, 7 modular exponentiation, 2 modular multiplication inverse and 2 hashing) operations in all phases.

The Dameri et al.'s scheme has numbers of operations (4 modular multiplication, 5 modular exponentiation, 0 modular multiplication inverse and 0 hashing) operations.

The Biswa Bhusan Biswal, et al.'s Scheme has numbers of operations (7 modular multiplication, 7 modular exponentiation, 1 modular multiplication inverse and 2 hashing) operations.

Hamid Mala, et al.'s scheme has numbers of operations (7 modular multiplication, 6 modular exponentiation, 1 modular multiplication inverse and 2 hashing) operations.

Chanchal Chandra, et al.'s Scheme has numbers of operations (10 modular multiplication, 9 modular exponentiation, 2 modular multiplication inverse and 2 hashing) operations.

Based on the comparison performed, the Dameri et al.'s scheme has less numbers of operations (4 modular multiplication, 5 modular exponentiation, 0 modular multiplication inverse and 0 hashing) operations. From these analysis, we find that Dameri et al.'s scheme has less operations than the other existing schemes as shown in Table 4. But it wasn't secure, it suffered from universally forgeable Attack.

Table 1. Comparison between Different Modifications of ElGamal

Signature in (Key Generation, Blinding, and Signing Phases)

Algorithm	Key generation	Requester /Blinding	Signer/Signing
ElGamal [14]	$y = g^x \bmod p$	----------	$s = k^{-1}(m - xr) \bmod (p-1)$
R. L. Shen [13]	$y = g^x \bmod p$ $r' = g^{k'} \bmod p,$ $r = r'^a y^b g^c \bmod p$	$m' = a^{-1}(c + h(m) + r) - r' \bmod p - 1$	$s' = x^{-1}\left(k' + (m' + r')\right) \bmod (p-1)$
Dameri [18]	$y = g^x \bmod p$ $r = g^k \bmod (p)$	$m' = m + h \bmod (p-1)$	$s' = \left(m' - (x + k)\right) r \bmod (p-1)$
Biswa Bhusan Biswal [20]	$n = p_1 p_2$ $p = 2n + 1$ $y = g^x \bmod p$ $r' = g^k \bmod p$ $z = g^c \bmod p$	$r = h(r' g^a y^b \bmod p, m)$ $m' = r + b \bmod n$	$s' = (k + m'x) \bmod n$
Hamid Mala [19]	$y = g^x \bmod p$ $r' = g^k \bmod p$ $r = r'^a g^b \bmod p$	$m' = a^{-1} rh(m) \bmod (p-1)$	$s' = k + m'x \bmod (p-1)$
Chanchal Chandra [15]	$y_a = g^{x_a} \bmod p$ $y_b = g^{x_b} \bmod p$ $r' = g^k \pmod p$ $r = (k + r'x_a) \pmod p$ $v = g^{-r\beta} \pmod p$ $z = g^c \pmod p$	$m' = h\left(m, (z^{c^{-1}x_b})\left(y_b^{r\,x_b^{-1}}\right)\right.$ $\left.vzg^{-\alpha}\right) \bmod p$	$s' = (m' + \beta)r \pmod p$

Table 2.Comparison between Different Modifications of ElGamal Signature in

(Unblinding and Verification Phases)

Algorithm	Requester/ Unblinding	Verifier/Verifying
ElGamal [14]	----------	$g^m \equiv y^r r^s \bmod p$
R. L. Shen [13]	$s = a s' + b \bmod (p-1)$	$y^s = r g^{r+h(m)} \bmod p$
Dameri [18]	$s = s' - rh \bmod (p-1)$	$g^{rm} = g^s (yr)^r \bmod p$
Biswa Bhusan Biswal [20]	$s = s' + a + c \bmod n$	$r = h(g^s y^{-r} z^{-1} \bmod p, m) \bmod n$
Hamid Mala [19]	$s = a s' + b \bmod (p-1)$	$g^s = r\, y^{rh(m)} \bmod p$
Chanchal Chandra [15]	$s = (s' - c - \alpha) \pmod q$	$m' = h(m, y_b . g^{r(1+m')} . g^s) \bmod p$

Table 3.Security Analysis on Blind Signature Schemes Based On Modified ElGamal Signature

Algorithm	R. L. Shen [13]	Dameri [18]	Biswa Bhusan Biswal [20]	Hamid Mala [19]	Chanchal Chandra [15]
Correctness	Yes	Yes	Yes	Yes	Yes
Blindness	Yes	Yes	Yes	Yes	Yes
Unforgeability	Yes	No	Yes	Yes	Yes
Anonymity	Yes	Yes	Yes	Yes	Yes
Blind factors	3	1	3	2	3
Weakness	------	Universally Forgeable Attack	------	------	------
Review security status	Secure	Unsecure	Secure	Secure	Secure

Table 4. Comparative Study of Computational Complexities

Type of Computation	R. L. Shen [13]	Dameri [18]	Biswa Bhusan Biswal [20]	Hamid Mala [19]	Chanchal Chandra [15]
Multiplication	6	4	7	7	10
Exponentiation	7	5	7	6	9
Inverse	2	0	1	1	2
Hash	2	0	2	2	2

6. CONCLUSIONS AND FUTURE WORK

In this paper, a survey of existing blind signature schemes based on ElGamal Signature is presented. Its security was based on the difficulty of computing the discrete logarithm problem. Schemes were compared in terms of requirements of blind signature namely, Correctness, blindness, anonymity and unforgeability. These requirements were either satisfied or dissatisfied in the schemes mentioned on this paper. Schemes such as Dameri, et al.'s [18] scheme was unsecure, it suffered from universally forgeable Attack. But R. L. Shen, et al. [13], Biswa Bhusan Biswal, et al. [20], Hamid Mala, et al. [19], and Chanchal Chandra, et al. [15] satisfied all requirements of blind signature. In addition to we compared the existing schemes from computational complexity. Except Dameri, et al.'s scheme, Hamid Mala, et al.'s scheme has less computation complexity and more secure than the existing schemes so it would be appropriately efficient in applications like EVS to achieve voter anonymity, in other words to remove voter's identity from his cast ballot, in order to ensure voter privacy.

7. REFERENCES

[1] Subariah Ibrahim, Mazleena Salleh and Maznah Kamat, "Electronic Voting System: Preliminary Study," Jurnal Teknologi Maklumat, vol. 12, pp. 31- 40, 2000.

[2] Al-Ameen, Abdalla, and Samani A. Talab, "The technical feasibility and security of e-voting," Int. Arab J. Inf. Technol, vol. 10, no. 4, pp. 397-404, 2013.

[3] Kouta, Reham Mohamed, Essam-Eldean F. Elfakharany, and Wafaa Boghdady Mohamed, "Proposed Secured

Remote E-Voting Model based on Blind Signature," GJCST-E, vol. 13, no. 13, p. 2, 2013.

[4] Kalaichelvi, V., and R. M. Chandrasekaran, "Design and Analysis of Secured Electronic Voting Protocol," Asian Journal of Infor-mation Technology, vol. 11, no. 2, pp. 50-55, 2012.

[5] Cetinkaya, Orhan, and Deniz Cetinkaya, "Verification and validation issues in electronic voting," The Electronic Journal of e-Government, vol. 5, no. 2, pp. 117-119, 2007.

[6] Oo, Htet Ne, and Aye Moe Aung, "Implementation and Analysis of Secure Electronic Voting System," International Journal of Technology Enhancements and Emerging Engineer-ing Research, vol. 2, no. 3, pp. 158-159, 2013.

[7] Chin-Ling Chen, Yu-Yi Chen, Jinn-Ke Jan, Chih-Cheng Chen, 陳金鈴, "A Secure Anonymous E-Voting System based on Discrete Logarithm Problem," An International Journal of Applied Mathematics & Information Sciences, vol. 5, pp. 2571-2578, 2014.

[8] Singh, Nitu, and Sumanjit Das, "Cryptanalysis of Blind Signature Schemes," International Journal of Computer Applications, vol. 71, no.19, 2013.

[9] Singh, Nitu, and Sumanjit Das, "A Novel Proficient Blind Signature Scheme using ECC," in ." IJCA Proceedings on International Conference on Emergent Trends in Computing and Communication (ETCC-2014), 2014.

[10] Chaum, David, "Blind signatures for untraceable payments," in Advances in cryptology, Springer US, 1983.

[11] Thu, Aye Aye, and Khin Than Mya, "Implementation of an Efficient Blind Signature Scheme," International Journal of Innovation, Management and Technology, vol. 5, no. 6, p. 2, 2014.

[12] Aliabadian, Amir, and Ali Delavari Ghara, "New Blind Digital Signature Based On Modified Elgamal Signature in Electronic Voting," International Journal of Engineering and Advanced Technology , vol. 1, no. 6, pp. 144-147, 2012.

[13] Shen, Victor RL, Yu Fang Chung, Tzer Shyong Chen, and Yu An Lin, "A blind signature based on discrete logarithm problem," International journal of innovative computing information and control, vol. 7, no. 9, pp. 5403-5416, 2011.

[14] ElGamal, Taher, "A public key cryptosystem and a signature scheme based on discrete logarithms," in Workshop on the Theory and Application of Cryptographic Techniques, Springer Berlin Heidelberg, 1984.

[15] Chandra, Chanchal, "Design of Blind Signature Protocol Based upon DLP. Diss.," in NATIONAL INSTI-TUTE OF TECHNOLOGY, ROURKELA, 2013.

[16] Baral, Sumati, "An Efficient Blind Digital Signature Protocol Based on Elliptic Curve," INTERNATIONAL JOURNAL OF TECHNOLOGY ENHANCEMENTS AND EMERGING ENGINEERING RESEARCH, vol. 2, no. 9, p. 2, 2014.

[17] L. Harn and Y. Xu, "Design of generalized ElGamal type digital signature schemes based on discrete logarithm," Electronics Letters, vol. 30, no. 24, pp. 2025-2026, 1994.

[18] Dameri, A., and R. Boostani, "Processing a New Blind Signature Based on ElGamal," BIOINFO Security Informatics, vol. 2, no. 2, pp. 66-68, 2012.

[19] Mala, Hamid, and Nafiseh Nezhadansari, "New blind signature schemes based on the (elliptic curve) discrete logarithm problem," in Computer and Knowledge Engineering (ICCKE), 2013 3th International conference on. IEEE, Isfahan, Iran, 2013.

[20] Biswal, Biswa Bhusan, "A Novel Blind Signature Scheme Based On Discrete Logarithm Problem With Un-traceability," in National Institute of Technology, Rourkela, 2012.

[21] Nyberg, Kaisa, and Rainer A. Rueppel, "A new signature scheme based on the DSA giving message recovery," in Proceedings of the 1st ACM conference on Computer and communications security, 1993.

[22] Nyberg, Kaisa, and Rainer A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm problem," Springer Berlin Heidelberg, pp. 182-193,1994.