

Blind Signature Scheme Based on MGES.

Demba Sow

LACGAA, Faculte des Sciences et Techniques,
Universit'e Cheikh Anta Diop de Dakar, S'en'egal'
demba1.sow@ucad.edu.sn

Abstract: This paper presents a Modified Generalized ElGamal Signature Scheme (briefly called MGES) and introduces a new Blind Signature Scheme based on the MGES scheme. The security of our modified and blind schemes is based on the discrete logarithm problem (DLP). We also show that our new blind signature scheme verifies all the properties of blind signature.

Keywords: Blind-signature, ElGamal, DLP.

I Introduction

Using one's right to vote is a way of exercising one's citizenship. It allows citizens to protect their freedom and make democracy work. Electronic voting consists of using computer and telecommunications technologies in the voting process. A device (computer, telephone) allows you to cast your vote and automatically count all the votes. The benefits thus sought are as follows: facilitating voting and, in so doing, increasing participation in elections while making their results immediately. The E-vote allows us to vote everywhere, anywhere. It permits to count the votes electronically, reduces the time, and simplifies the organization of the vote. Online electronic voting must provide very high levels of guarantees and confidence on:

- the integrity of the digital ballots at the time of its constitution, of its sending, and its storage (nonmanipulation), and in the final results of the ballot.
- the inviolability of the expression of the vote and the digital ballot during the electoral operations and after the counting (total respect for anonymity);
- the integrity of the electronic voting system itself through traceability and full transparency of all actions carried out before the launch of the ballot, during, and after until the counting.

In [9], some properties to make secure the Evote are presented. Some of these properties are Eligibility, Uniqueness, Privacy, Receipt-freeness, Fairness, Mobility, Anonymity, Correctness, Blindness and Unforgeability. Blind signing is one of the most widely used cryptographic techniques in electronic voting systems (EVS) to prove voter anonymity [9], [1], [12].

Contributions: In this article, our contributions are presented as follows:

1. We, first, propose a modified version of the Generalized ElGamal signature scheme that is more efficient and as safe as the Generalized ElGamal signature scheme.
2. Our second aim is to design a blind signature scheme based on a modified Generalized ElGamal signature scheme [15], [14]. This new blind signature scheme is efficient because its complexity is less, and uses only one factor instead of two or three like the schemes already proposed. It is also a safe scheme because it verifies the four properties of a blind signature scheme, namely correctness, blindness, unforgeability, and anonymity.

Outline: This paper is structured in seven sections.

- The Section 2 describes some previous works about modified ElGamal signature schemes and Blind signature schemes like.
- In Section 3, we present some preliminaries which help to understand the rest of the paper (definition of blind signature 3.1, participants ?? and requirements 3.2).
- Section 4 presents the Harn signature scheme 4.1 which is modified ElGamal signature scheme and reviews the Khater *et al.*'s blind signature scheme 4.2 which is based on the Harn signature scheme.
- In Section 5, we propose a new signature scheme based on the Generalized ElGamal signature scheme. this new scheme is briefly called MGES. We also, prove its security against no-message and an adaptively chosen message attacks under discrete logarithm problem assumptions 5.2.
- In Section 6, we show a new blind signature scheme based on the modified Generalized ElGamal signature scheme (MGES). We also, presented its security in 6.2.
- The last section 7 presents the conclusion of this article.

II Previous Works

Presented in August 1984 by Taher ElGamal [Elg85], (ElGamal), from which the algorithm takes its name, it offers an asymmetric encryption protocol and a digital signature designed from the Diffie-Hellman Key Exchange. In [1396], Pointcheval *et al.* presented that the original ElGamal signature scheme is not secure against no-message attack. In their paper, authors proposed a new modified signature scheme which is secure against no-message and an adaptively chosen message attacks. In 1994, Harn presented a new new digital signature scheme based on discrete logarithm [7]. In his signature scheme, no inverse is needed to calculate, thus, making the calculation process fast.

Sow *et al.*, in [15], proposed a new signature scheme based on ElGamal signature scheme. Authors presented many versions of signature in their paper.

The blind signature notion is, first, proposed by Chaum in 1983 in [4]. In a blind signature scheme, the signer uses his private key to sign a blind message, and everyone can verify the legitimacy signature with the signer's public key. A blind signature allows the security of electronic votes. Many blind signature schemes, based on the ElGamal signature scheme, have been proposed by authors [10]. Among these, some blind signature schemes: Shen *et al.* [16], Dameri *et al.* [2], Biswa *et al.* [3], Hamid *et al.* [8], and Chanchal *et al.* [5].

In 2018, Khater *et al.* [11] proposed a new blind signature scheme based on Harn's signature scheme [7] proposed in 1994. In their paper, the authors first, showed a forgery attack on Mohsen *et al.*'s blind signature scheme [17], then, presented their new blind signature scheme.

III Blind Signature Scheme

3.1 Definition

The authors David Chaum (in [4]) and Shen *et al.* (in [16]) defined a blind signature made on a document that was masked before being signed so that the signer could not know the meaning of the message. Generally, one uses a blind signature when the document author and the signer are different.

A Blind Signature scheme allows a user U to obtain a blind signature of the message m in a message space M , issued by a signer S .

Definition 3.1 (Blind Signature scheme [4]) *A blind signature scheme is a Probabilistic Polynomial Time (PPT) algorithm, which consists of three protocols organised as follows:*

Key Generation: $\text{KeyGen}(1^k)$ is a probabilistic algorithm that uses as input the security parameter k , and it returns a key pair (pk, sk) .

Blind signature: $\text{BlindSign}(U(m, pk), S(sk))$ is a protocol run by user U and signer S . U uses as input the message $m \in M$ and the public key pk , and S gets the private key sk as input. After running the protocol, we obtain an output σ , which corresponds to the signature of m , or \perp if the protocol ended unsuccessfully.

This protocol can often be decomposed into four algorithms: $\text{Commit}(sk) \rightarrow r; \text{Blind}(pk, r, m) \rightarrow (r', m'); \text{Sign}(sk, m') \rightarrow \sigma'; \text{Unblind}(pk, r', \sigma') \rightarrow \sigma$. Commit and Sign are executed by S , the two other by U .

Verification: $\text{VerifyBlindSign}_{pk}(m, \sigma)$ is a deterministic protocol that given a message $m \in M$, a signature σ and a public key pk , it returns 1 if σ is a valid signature on m regarding pk , otherwise it returns 0.

3.2 Requirements

A blind signature must verify must satisfy three security properties: *Correctness, unforgeability and blindness.*

- *Correctness:* By executing all the algorithms regularly we will always obtain a valid signature that can be verified by anyone given the public key, the message and the signature. For a message space M this can be formalised as follows¹.

$$\forall m \in M, \forall (sk, pk) \in [\text{KeyGen}()],$$

$$\forall \sigma \in [\text{BlindSign}(U(pk, m), A(sk))], \text{VerifyBlindSign}_{pk}(m, \sigma) = 1.$$

- *EUF-CMA:* A blind signature scheme BS is *Existentially Unforgeable under Chosen Message Attacks* if for an honest signer S and for any polynomial time adversary U^* , the probability such that

¹ $[\text{Alg}()]$ refer to the set of all values that can be outputted by Alg.

$\text{Adv}_{\text{BS}, \mathcal{U}^*}^{uf}(\mathcal{R}) = \Pr[\text{Exp}_{\text{BS}, \mathcal{U}^*}^{uf}(\mathcal{R}) = 1]$ is negligible². $\text{Exp}_{\text{BS}, \mathcal{U}^*}^{uf}(\mathcal{R})$ defined in Experiment 1 is the experiment that the adversary \mathcal{U}^* must be able to win in order to break the property. For that it must be able to generate $q_s + 1$ valid signature after at most q_s complete interactions with the honest signer S .

$\text{Exp}_{\text{BS}, \mathcal{U}^*}^{uf}(\mathcal{R})$

1. $\text{params} \leftarrow \text{Setup}(1^K)$
2. $(\text{pk}, \text{sk}) \leftarrow \text{KeyGen}(\text{params})$
3. For $i = 1, \dots, q_s$, $\text{BlindSign}(A(\cdot, \text{pk}), S(\text{sk}))$
4. $((m_1, \sigma_1), \dots, (m_{q_s+1}, \sigma_{q_s+1})) \leftarrow A(\text{pk})$
5. If $\exists i \neq j, m_i = m_j$ or if $\exists i$,
 $\text{VerifyBlindSign}(\text{pk}, m_i, \sigma_i) = 0$;
 Return 0
6. Else Return 1

Experiment 1: Unforgeability Experiment of a Blind Signature.

- **Blindness:** The content of the ballot should no be linkable to any execution of the blind signature algorithms. A Blind signature scheme BS is blind if for all polynomial time adversaries S^* with access to two user instances, there is a negligible function $\epsilon(\cdot)$ such that $\text{Adv}_{\text{BS}, S^*}^{bl}(\mathcal{R}) =$

$$|1/2 - \Pr[\text{Exp}_{\text{BS}, S^*}^{bl}(\mathcal{K}) = 1]| < \epsilon(\mathcal{K}) \text{ for some}$$

$\mathcal{K} \in \mathbb{N}$.

$\text{Exp}_{\text{BS}, S^*}^{bl}(\mathcal{R})$

1. $\text{params} \leftarrow \text{Setup}(1^K)$
2. $(\text{pk}, m_0, m_1) \leftarrow A(\text{params})$
3. $b \leftarrow \{^S \quad 0, 1\}$
4. $\sigma_b \leftarrow \text{BlindSign}(U(\text{pk}, m_b), A)$
5. $\sigma_{1-b} \leftarrow \text{BlindSign}(A, U(\text{pk}, m_b))$
6. $b^* \leftarrow A((m_0, \sigma_0), (m_1, \sigma_1))$
7. Return $b^* = b$

Experiment 2: Blindness Experiment of a Blind Signature.

If any of these three properties does not hold, we will consider that the given blind signature has major weaknesses and thus is not secure to use. In the rest of this paper we will use the message space of binary strings $M = \{0, 1\}^*$.

IV Review Khater *et al.*'s Blind Signature Scheme.

4.1 Harn signature scheme

In 1994, Harn has proposed a new signature scheme based on the discrete logarithm problem [7]. Here, we present key generation, signature and verification algorithms.

Key generation algorithm.

1. Choose a group $G = \mathbb{Z}_p$ of order a large prime number p , and a generator $g \in G$.
2. Select a random number $x \in \mathbb{Z}_p$ and compute $y = g^x \text{ mod } p$.

Then public key is (g, y, p) and the private key is (x, p) .

Signature algorithm. To sign a message m with the private key (x, p) , do the following:

1. Select randomly a number $k \in \mathbb{Z}_p^*$.
2. Compute $r = g^k \text{ mod } p$ and $s = x(h(m)+r) - k \text{ mod } (p-1)$, where h is a hash function. The signature of the message m is (r, s) .

² A function f is negligible, if for every polynomial $P, \exists k \in \mathbb{N}$, $|f(n)| < \frac{1}{P(n)} \forall n > k$.

Verification algorithm. To verify a signature (r,s) of the message m , do the following:

1. Check the following equation is correct: $rg^s \equiv y^{h(m)+r} \pmod p$.

The signature (r,s) is valid, otherwise invalid.

4.2 Blind Signature Based on Harn Signature Scheme

Blind signature based on Harn signature scheme is proposed by Khater *et al.* in [11]. In this subsection, we show its initialization, blinding, unblinding and verification phases.

Initialization phase.

1. Signer: choose un Galois group $G = \mathbb{Z}_p$ with a large prime number p , and un primitive root $g \in G$. He selects a random number $x \in \mathbb{Z}_p$, computes $y = g^x \pmod p$ and chooses a hash function h . He publish the public key (g,y,p) and keep the private key (x,p) .

Blinding phase.

1. Requester: sends a request to the signer for signing his message m .
2. Signer: chooses random number k to compute $r' = g^k \pmod p$, then sends r' to the requester.
3. Requester: randomly chooses two random numbers (a,b) to compute $r = r'^a g^b \pmod p$. Then use hash function h to compute his blinded message $m' = a^{-1}(h(m)+r)-r' \pmod{(p-1)}$ and Requester sends m' to the signer.

Signing phase. Signer computes the blind signature $s' = x(m'+r')+k \pmod{(p-1)}$ and sends s' to the requester.

Unblinding phase. Requester extracts the signature as follows: $s = as' + b \pmod{(p-1)}$ and sends the message m and the signature (r,s) to the verifier.

Verification phase. Verifier checks the signature as follows: $g^s = ry^{h(m)+r} \pmod p$.

Security Analysis The Khater *et al.*'s blind signature scheme satisfies all the properties of blind signature namely Correctness, Blindness, Unforgeability, and Anonymity [11]. The security of their scheme is based on both the strength of the hash function and hardness of the DLP in \mathbb{Z}_p^* .

V The Modified Generalized ElGamal Scheme (MGES)

In this section, we present a modified version of the Generalized ElGamal signature algorithm proposed by Sow *et al.* in [15]. Generalized ElGamal Signature Scheme proposed in [15] by Sow *et al.* is modified version of the ElGamal Signature Scheme [Elg85]. Here, we propose a modified version of the Generalized ElGamal Signature Scheme (briefly called MGES).

5.1 Algorithms

In this subsection, we present key generation, signature and verification algorithms or the Modified Generalized ElGamal Signature Scheme.

Key generation algorithm. To create a pair of public and private key, we do the following:

1. Select a cyclic group $G = \mathbb{Z}_p^*$ with a large prime p and with order $d = \#G$ such that $G = \langle g \rangle$.
2. Select two random integers λ and δ sufficiently large such that $2 < \delta < d$ and λ of size half the size of d i.e., $\log_2(\lambda) = \frac{\log_2(d)}{2}$. Compute δd .
3. Compute with Euclidean division algorithm, the pair $(\alpha, \beta) \in \mathbb{Z}_d^2$ such that $\delta d = \alpha \lambda + \beta$ where $\beta = \delta d \pmod \lambda$. Note that the size of β is smaller or equal to the size of λ , i.e., $\log_2(\beta) \leq \log_2(\lambda)$.
4. Compute $u = g^\alpha$ and $v = g^\beta$ in G . Note that we necessarily have $u \neq 1$, it should still be ensured that $v \neq 1$.

Then public key is (u,v,G) and the private key is (λ, G) .

Signature algorithm. To sign a message $m \in$

$\{0,1\}^*$ with the private key (λ, G) , do the following: 1. Select a random integer $2 < k < d = \#g$ such that k and d are co-prime.

2. Compute $r = u^k \bmod p$ and $s = \lambda(h(m)+r) + k \bmod (p-1)$.

The signature is (r,s) .

Verification algorithm. To verify a signature (r,s) of the message m , check that:

$$us^{v(h(m)+r)} = r \pmod p$$

Correctness.

$$\begin{aligned} V_1 &= us^{v(h(m)+r)} \pmod p \\ &= g^{\alpha(\lambda(h(m)+r)+k)} g^{\beta(h(m)+r)} \pmod p \\ &= g^{(\alpha\lambda+\beta)(h(m)+r)} g^{\alpha k} \pmod p \\ &= g^{\delta(h(m)+r)} u^k \pmod p \\ &= r \pmod p \\ &= V_2. \end{aligned}$$

5.2 Security analysis

In 2011, Sow *et al.* have proposed a new variant of ElGamal encryption and signature scheme (called Generalized ElGamal) [15]. In their paper, authors have showed the security and performance analysis of the Generalized ElGamal signature scheme. The Generalized ElGamal signature scheme is secure against no-message and an adaptively chosen message attacks.

In [1396], Pointcheval *et al.* showed that the original ElGamal signature scheme is not secure against an adaptively chosen message attack. Hence, the authors proposed a modification of the ElGamal signature scheme and proved its security against an adaptively chosen message attack. Like their security proof in [1396], we show that our modified ElGamal signature scheme (MGES) is secure against an adaptively chosen message attack.

We first recall some lemmas and definitions used in the security proofs of our scheme (see [1396] for comments and proofs).

Lemma 5.1 *Let A be a Probabilistic Polynomial Time Turing machine, given only the public data as input. If A can find, with non-negligible probability, a valid signature $(m, \sigma_1, h, \sigma_2)$, then, with non-negligible probability, a replay of this machine, with the same random tape and a different oracle, outputs two valid signatures $(m, \sigma_1, h, \sigma_2)$ and $(m, \sigma_1, h', \sigma_2')$ such that $h \neq h'$.*

Lemma 5.2 *Let $A \subset X \times Y$, such that $\Pr[A(x,y)] \geq \epsilon$, then there exists $\Omega \subset X$ such that*

- $\Pr[x \in \Omega] \geq \epsilon/2$
- whenever $a \in \Omega$, $\Pr[A(a,y)] \geq \epsilon/2$

Definition 5.3 *Let α be a fixed real. An α -hard prime number p is such that the factorization of $p-1$ yields $p-1 = QR$ with Q prime and $R \leq |p|^\alpha$.*

Lemma 5.4 *For α -hard prime numbers, the signer can be simulated with an indistinguishable distribution.*

5.2.1 Security against a no-message attack

We first present the security of our scheme against no-message attacks. To prove the above theorem, we focus on the one in [1396]. We are just going to show that from our signature scheme, we can find the same equations (1 and 2) in the proof of the Theorem 10 in [1396] which serve as a discussion on the proof. The rest of the proof is similar to the proof of Theorem 10 in [1396].

Theorem 5.5 *Consider a no-message attack in the random oracle model against schemes using α -hard prime moduli. Probabilities are taken over random tapes, random oracles and public keys. If an existential forgery of this scheme has*

non-negligible probability of success, then the discrete logarithm problem with α -hard prime moduli can be solved in polynomial time.

Proof 5.6 By the Lemma 5.1, one obtains two valid signatures (m, r, h, s) and (m, r, h', s') such that $u^s v^{h+r} \bmod p = r \bmod p$ and $u^{s'} v^{h'+r} \bmod p = r \bmod p$. Thus, we have: $u^s v^{h+r} \bmod p = r \bmod p \Rightarrow g^{as+\beta(h+r)} \bmod p = r \bmod p$ and $u^{s'} v^{h'+r} \bmod p = r \bmod p \Rightarrow g^{as'+\beta(h'+r)} \bmod p = r \bmod p$. Hence, $g^{as+\beta(h+r)} \bmod p = g^{as'+\beta(h'+r)} \bmod p$.

Since, $u^{s'} v^{s(h'+r)} \bmod p = r^{s'} \bmod p$ and, then $\frac{u^{s'} v^{s(h'+r)}}{v^{s'(h+r)-s(h'+r)}} \bmod p = \frac{r^{s'}}{r^s} \bmod p \Rightarrow g^{\beta[(hs'-h's)+r(s'-s)]} \bmod p = r^{s'-s} \bmod p$. Since, $\mathbb{Z}_p^* = \langle g \rangle$, then there exists a such that $g^a \bmod p = r \bmod p$. Thus, we obtain $\beta[(hs'-h's) + r(s'-s)] = a(s'-s) \bmod (p-1) \Rightarrow \beta(hs'-h's) = (a-\beta r)(s'-s) \bmod (p-1)$ and $\beta(h'-h) = a(s-s') \bmod (p-1)$. Since $\gcd(\beta, p-1) = 1$, then there exists $x \in \mathbb{Z}_p$

such that $\frac{1}{\beta} \bmod (p-1) = x$. Pose $t = xa$
 $\bmod (p-1)$ and $\theta = (a-\beta r) \bmod (p-1)$, then we get the same equations in [1396]:

$$hs' - h's = x\theta(s' - s) \bmod (p-1) \quad (1) \quad h' - h = t(s - s') \bmod (p-1) \quad (2)$$

Using the Lemma 5.2 and the discussions in the proof of the Theorem 10 in [1396], we prove that our signature scheme is secure against no-message attacks.

5.2.2 Security against an adaptively chosen message attack

Our signature scheme is also a modified version of the ElGamal signature scheme just like the modified Pointcheval *et al.*'s scheme [1396]. The security of the two modified schemes is based on the discrete logarithm problem. Like Pointcheval *et al.*'s signature scheme, our modified ElGamal signature scheme is secure against an adaptively chosen message attack in the random oracle model.

Theorem 5.7 Consider an adaptively chosen message attack in the random oracle model against schemes using α -hard prime moduli. Probabilities are taken over random tapes, random oracles and public keys. If an existential forgery of this scheme has non-negligible probability of success, then the discrete logarithm problem with α -hard prime moduli can be solved in polynomial time.

Proof 5.8 For all the signature simulations (r_i, h_i, s_i) of the messages m_i , the simulator S requesting $h(m_i)$ is supposed to have h_i . It is therefore easy to see that request collisions occur with negligible probability, thus the attacker is unable to distinguish the legitimate signature from the simulator. Hence, like Theorem 5.5, discrete logarithms can be solved from the collision of the simulator and the attacker.

VI Blind Signature Based on MGES Scheme

Here, we propose a blind signature scheme based on this modified version of the Generalized ElGamal scheme.

6.1 Algorithms

Key generation process. We will use the same key generation process as in MGES 5. Hence, we have a public key (u, v, p) and a private key (λ, p) .

Blinding phase.

1. Signer: randomly chooses a number k , computes $r' = u^k \bmod p$ and sends r' to the requester.
2. Requester: computes $r = r'^w \bmod p$. Randomly chooses a number w and a hash function h , computes $m' = w^{-1}(h(m)+r)-r' \bmod (p-1)$ and sends m' to the signer.

Signing phase. Signer computes the blind signature $s' = \lambda(m'+r')+k \bmod (p-1)$ and sends s' to the requester.

Unblinding phase. Requester extracts the signature as follows: $s = ws' \bmod (p-1)$ and sends the message m and the signature (r, s) to the verifier.

Verification phase. Verifier checks the signature as follows: $u^s v^{h(m)+r} \bmod p = r \bmod p$.

6.2 Security Analysis

The security of the new blind signature based on MGES scheme is based on both the strength of the hash function and hardness of the Discrete Logarithm

Problem in \mathbb{Z}_p^* .

Our scheme also satisfies all the properties of blind signature namely Correctness, Blindness, Unforgeability, and Anonymity.

- *Correctness.* The verification equation is checking as follows:

$$\begin{aligned} u^v &= u^{ws'h(m)+r} \pmod p \\ &= g^{\alpha w(\lambda(m+r)+k)g\beta(h(m)+r)} \pmod p \\ &= g^{\alpha w[\lambda(w^{-1}(h(m)+r)-r'+r')+k]g\beta(h(m)+r)} \\ &= g^{\alpha w k_g(\alpha\lambda+\beta)(h(m)+r)} \pmod p \\ &= u w k g d(h(m)+r) \pmod p \\ &= r \pmod p. \end{aligned}$$

- *Blindness.* To extract the message m from the blind message $m' = w^{-1}(h(m)+r)-r' \pmod p$, a signer must solve the discrete logarithm problem given r' and $r = r'^w \pmod p$; he, also, cannot obtain m from its hash $h(m)$. Thus, a signer cannot extract a clear message from the blind message. The signer cannot link a signature (r,s) of a message m to a user. He has no information about the parameters m , r , and s .
- *Unforgeability.* To forge a valid signature (r,s) on his message m , an attacker twice must solve the discrete logarithm problem given g , $u = g^\alpha$ and $v = g^\beta$ to obtain the private key λ from α and β . If the attacker solves the DLP problem and obtains α and β , he will get the random value δ in the equation $\delta d = \alpha\lambda + \beta$ to obtain the private key λ . It is a very difficult problem. Thus, no one can forge a valid signature (r,s) of message m to pass the verification.
- *Anonymity.* Consider that a malicious signer has kept all the signatures of the messages blind and that a requester publishes the signature (r_i, s_i) of a message m_i . Then this signer cannot derive any information from the values it retains because the values he receives are blind and do not know the w factor. Thus, he cannot link the blind signature and the message-signature pair. Our signature scheme, therefore, satisfies anonymity.

VII Conclusion

We have successfully proposed a modified version of the Generalized ElGamal signature scheme (called MGES) which is more efficient and as safe as the Generalized ElGamal signature scheme. We also designed a new blind signature scheme based on the modified Generalized ElGamal signature scheme (MGES). Our blind signature scheme verifies the four properties of a blind signature scheme, namely correctness, blindness, unforgeability, and anonymity.

References

1. Amir Aliabadian and Ali Delavari Ghara. New blind digital signature based on modified elgamal signature in electronic voting. International Journal of Engineering and Advanced Technology, 1(6):144–147, 2012.
2. Dameri A. and Boostani R. Processing a new blind signature based on elgamal. BIOINFO Security Informatics, 2(2):66–68, 2012.
3. Biswa Bhusan Biswal and Sukanta Kumar Mangal. A novel blind signature scheme based on discrete logarithm problem with un-traceability. National Institute of Technology, Rourkela, 2012.
4. David Chaum. Blind signatures for untraceable payments. In Advances in cryptology, pages 199–203. Springer, 1983.
5. Chanchal Chandra. Design of blind signature protocol based upon dlp. diss. National Institute of Technology, Rourkela, 2013.
6. T. Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In CRYPTO, IT-31(4), volume 4, pages 469–472, 1985.
7. Lein Harn. New digital signature scheme based on discrete logarithm. Electronics letters, 30(5):396–398, 1994.
8. Mala Hamid and Nafiseh Nezhadansari. New blind signature schemes based on the (elliptic curve) discrete logarithm problem. 2013.
9. Subariah Ibrahim, Mazleena Salleh, and Maznah Kamat. Electronic voting system: Preliminary study. Jurnal Teknologi Maklumat, 12:31–40, 2000.
10. Monira M. Khater, Ayman Al-Ahwal, Mazen M. Selim, and Hala H. Zayed. Blind signature schemes based on elgamal signature for electronic voting: A survey. International Journal of Computer Applications, 180(30):21–28, Apr 2018.
11. Monira M Khater, Ayman Al-Ahwal, Mazen M Selim, and Hala H Zayed. New blind signature schemes based on elgamal signature for secure electronic voting. International Journal of Computer Applications, 9:917–921, March 2018.
12. Reham Mohamed Kouta, Essam-Eldean F. Elfakharany, and Wafaa Boghdady Mohamed. Proposed secured remote e-voting model based on blind signature. Global journal of computer science and technology, 13, 2013.

13. David Pointcheval and Jacques Stern. Security proofs for signature schemes. In International conference on the theory and applications of cryptographic techniques, pages 387–398. Springer, 1996.
14. Demba Sow and Mamadou Ghouraisiou Camara. Provable security of the generalized elgamal signature scheme. *Journal of Mathematics Research*, 11(6):77–83, December 2019.
15. Demba Sow and Djiby Sow. A new variant of el gamal's encryption and signatures schemes. *JP Journal of Algebra, Number Theory and Applications*, 20(1):21–39, 2011.
16. Tzer Shyong Chen Shen Victor RL, Yu Fang Chung and Yu An Lin. A blind signature based on discrete logarithm problem. *International Journal of Innovative Computing*, 7(9):5403–5416, September 2011.
17. Ali Zaghian and Mohsen Mansouri. A new blind signature scheme based on improved elgamal signature scheme. 2012.