Mehran University Research Journal of Engineering and Technology
Vol. 40, No. 2, 314 - 322, April 2021
p-ISSN: 0254-7821, e-ISSN: 2413-7219
DOI: 10.22581/muet1982.2102.06

Novel Blind Signcryption Scheme for E-Voting System Based on Elliptic Curves

Abdul Waheed[1,2], Nizamud Din[3], Arif Iqbal Umar[1b], Riaz Ullah[1c], Noor Ul Amin[4]

RECEIVED ON 02.11.2018, ACCEPTED ON 15.09.2020

ABSTRACT

To make the electoral process more secure, comfortable, and universal, it is essential to use modern cryptographic techniques for ensuring the anonymity of information in the electronic voting system. In many emerging applications like electronic voting data anonymity as well as un-traceability are the most essential security properties. To ensure these properties we present here in this paper a more secure and comparatively efficient blind signcryption scheme using the Elliptic Curve Cryptosystem (ECC). The existing e-voting schemes are based on El-Gamal and the Rivest-Shamir-Adleman (RSA) cryptosystems which are not only expensive approaches but also lack the security features like unlinkability and forward secrecy. In our proposed scheme we use a low-cost elliptic curve cryptosystem with 160 bits key as compared to El-Gamal 2048 bits key and RSA 1024 bits key. In this scheme signer signs the message blindly without knowing the original contents then the voter forward signcrypted vote to polling server. The polling server is the actual voter data verifier or validator. The polling server checks the validity/authenticity of the voter and has the right to accept or reject the vote. Moreover, this scheme offers forward secrecy, unlinkability, and non-repudiation in addition to the basic security features like confidentiality, authenticity, integrity, and unforgeability. Overall performance evaluation proves that our scheme is comparatively more efficient in terms of computational and communicational costs. Furthermore, this scheme is suitable for the e-voting system due to its lower cost and extra security features.

Keywords: Anonymity, Secure Communication, Public Key Cryptosystem, ECC, Digital Blind Signature, E Voting System, Un-Traceability.

1. INTRODUCTION

E-voting is a confinement environment that aims to provide a secure and efficient voting mechanism within Internet of Things (IoT) services. However, this mechanism faces many security concerns like voter anonymity and fraud *etc*. In the literature, different e-voting schemes could be found [1-6] using different security mechanisms. These were threshold blind signature, simple blind signature, and anonymous communication based on discrete logarithmic protocols using varying operational complexities for a secure voting system.

A secure e-voting system should satisfy the following properties:

Anonymity: Voter privacy cannot be traced by the other system authorities.

[1] Department of Information Technology, Hazara University Mansehra, Mansehra 21120, Pakistan.
Email: [a]abdul@netlab.snu.ac.kr (Corresponding Author), [b]arifiqbalumar@yahoo.com, [c]riazktk_18@yahoo.com
[2] School of Electrical and Computer Engineering, Seoul National University, Seoul 08826, South Korea.
[3] Department of Computer Science, University of Chitral, Chitral 17200, Pakistan. Email: nizam@uoch.edu.pk
[4] Department of Telecommunication, Hazara University Mansehra, Mansehra 21120, Pakistan.
Email: naminhu@gmail.com

Perfectness: A valid voter will always be accepted by the administrator.
Robustness: An attacker or dishonest voter is not able to disturb the overall system.
Un-reusability: A voter cannot cast more than one votes.
Fairness: Fairness and transparency is ensured in every aspect throughout the system.
Public Verifiability: The results will be publically verifiable.
Individual Verifiability: Every voter can verify the vote individually.

This paper aims to introduce and develop a novel cryptosystem that satisfies the basic security requirement of e-voting with comparatively minimal operational cost. Therefore, the blind signature is the best security primitive used to achieve these goals.

2. BLIND SIGNCRYPTION BASED E-VOTING SYSTEMS

Many kinds of widely recognized e-voting systems have been proposed that used more complex algorithmic structures to achieve security features required for e-voting systems. We are using a blind signcryption approach in this paper. The approach is easily adaptable in such kind of environments. E-voting scenario is shown in Fig. 1.

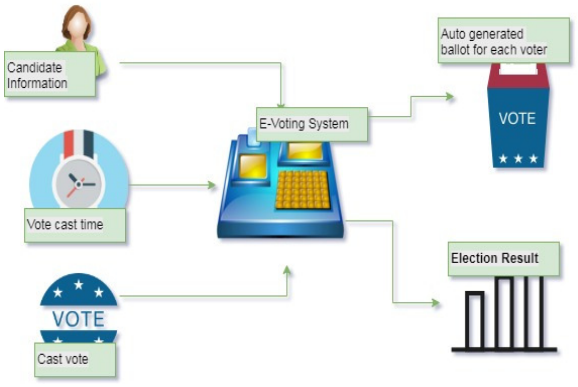

Fig. 1: E-Voting Scheme Scenario

Chaum [1] had given an idea of a blind signature for the first time. In his proposed scheme, the signature is generated outside the documents and the carbon copy is placed inside secret documents to make the same copy of signature inside without signer knowing about internal documents/contents (the signer is not allowed to see the contents of documents). Signed documents are encrypted and forwarded to servers/verifier for necessary action and maintaining the records. To operate blind signature with encryption at a time is referred to as digital blind signcryption which is a flavor of signcryption.

Signcryption was introduced by Zhang [7] for the first time. This cryptographic primitive combines signature and encryption logically in a single step to reduce operational cost. Blind signcryption is used to ensure anonymous communications in electronic voting. Anonymous communication is gaining importance in various fields and applications such as online transactions and mobile phone voting [8]. Blind signcryption ensures confidentiality with anonymous communication at once due to which it is applicable in a democratic environment which allows freedom of thought and opinion [8]. We also suggest here that the advanced version of blind signcryption will be applicable for a specified citizen's portal system as well. Moreover, the goal of this study is to introduce efficient blind signcryption for e-voting with comparatively lower cost and high security with smaller key size and efficiency.

Our scheme ensures the following properties;

(i) **Confidentiality:** For an attacker, it is infeasible to recover messages from signcrypted text without knowing the private key of receivers.
(ii) **Integrity:** The receiver ensures that the received messages are not altered on the way.
(iii) **Authenticity:** Having this property, the receiver ensures that the received message is sent by an authentic sender.
(iv) **Non-repudiation:** After digitally signing the message, the sender cannot deny his/her signature at a later stage.
(v) **Un-forgeability:** This property ensures that an attacker cannot generate a valid signature without the private key of the sender or signature generator.
(vi) **Blindness:** No one can read the message contents except the receiver.

(vii) **Un-traceability:** Having this property neither signer traces to voters nor makes links to previous messages of voters.

3. RELATED WORK

Chaum *et al.* [9] introduced the idea of a blind signature that ensured sender anonymity and presented an untraceable online payment scheme.
Brands [10] also presented a resistive scheme for double-spending anonymous communication and payment system after the identification of the same problem. This is an electronic cash scheme with some conditions and restrictions.

Nikooghadam and Zakerolhosseini [11] proposed an elliptic curve-based blind signature which was more efficient compared with Discrete Logarithm Problem (DLP) based schemes. Chakraborty and Mehta [12] proposed an ECC based signature scheme. This scheme introduced a duel encryption mechanism on the requestor side. A signer can decrypt outer encryption and the internal encryption use to hide the contents from the signer.

Awasthi and Lal [13] introduced DLP based blind signcryption for the first time. This scheme faced high operational costs and a lack of public verifiability. Xiuying and Dake [14] presented a DLP based blind signcryption scheme with public verifiability (*i.e.*, in case of any dispute third party can verify and dissolve the issues). Howover, this scheme was impractical for resource constraint environments due to its comparatively high cost. In reference [15] and [16] ECC based blind signcryption schemes have been presented. Those schemes used complex structures due to which could not get much attraction from the research community.

In the modern era, e-voting has got more attention from the research community. It is the objective to introduce a more mature and implementable e-voting system that will be trustworthy, free from faults, robust and inexpensive. Furthermore, the system can preserve the rights of citizens of the regions or countries where it is supposed to be used. Our new proposed scheme ensures election mechanism integrity, reduces the risks in threat circumstances and removes all the flaws found in traditional and manual systems.
The remaining sections of this paper are organized as follows: description and methodology is reflected in section 4, section 5 presents scheme participants, section 6 presents proposed scheme. Detailed security and cost comparison is presented in section 7, and section 8 concludes the paper.

4. METHODOLOGY DESCRIPTION

Fig. 2 depicts the proposed electronic voting scenario. The system operates in presence of the internet where authorized voters cast vote from any place using electronic devices. Polling servers count overall votes at the end and ensure voters anonymity. Our system generally is comprised of three participants that are signer/Polling station, voter, and Polling server. Further, we structured the proposed algorithm in four phases to generate keys, establish sessions between two parties, blind signcryption, and unsigncryption.

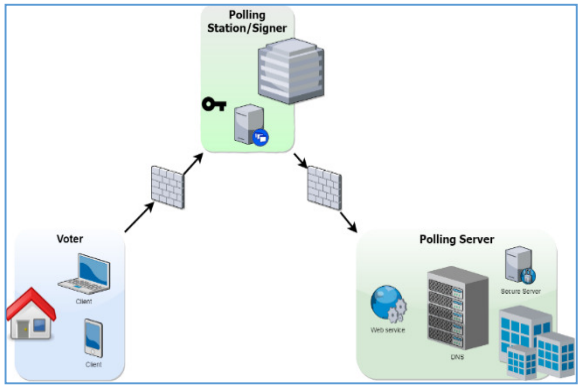

Fig. 2: Proposed Electronic Voting Scenario

5. SCHEME PARTICIPANTS

Proposed scheme participant details are as under:

Signer/Polling Station: At polling station, the signer blindly sign the message for a voter without knowing about the contents of the message.

Voter: Voter communicates the polling server anonymously. He/she forwards signcrypted vote/data to the polling server.

Polling Server: Polling server is an actual voter's data verifier that obtains voter signcrypted message and verifies after unsigncryption. It checks validity. If vote is authentic then it adds the vote to the voter list and maintains the record, otherwise rejects the vote. Fig. 3 shows the above three phases of the scheme participants. The symbols/parameters used throughout this manuscript are described in Table 1.

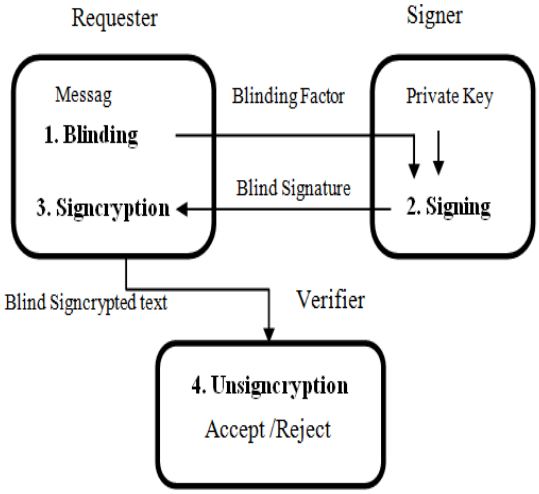

Fig. 3: Data Flow Mechanism in Blind Signcryption

Table 1: Symbols or Parameters Description

SYMBOLS/PARAMETERS	DESCRIPTION
$E(F_p)$	Points on ECC Curve
G	Basepoint on E
$E_k(.)/D_k(.)$	Enc/ Dec operation
Pri_k	Private key
Pub_k	Public key
d_{sign}	Signer's Private key
P_{sign}	Signer's Public Key
d_{req}	Requester's Private key
P_{req}	Requester's Public Key
d_{ver}	Ballot paper verifier's /Polling Server Private key
P_{ver}	Ballot paper verifier's /Polling Server Public Key
k	Secret parameter
h	Hashed value
m/c	Message/Ciphertext
r	Blind factor
$\mathcal{Z}$, $\bar{s}$	Blindly Signed factors
$(c, r, s, R, \mathcal{Z})$	Requester parameters forward to polling server after the blind signer
$\|\|$	Concatenation symbol
Q	Point Multiplication on the curve
$M-Exp$	Modular Exponentiation operation
Mul	Multiplication operation

6. PROPOSED SCHEME PHASES

In this section, we discuss the scheme details and its working principles.

Setup phase: This phase defines security parameters using the elliptic curve cryptosystem.

Assume that $\mathcal{P} \geq 2^{224}$ be a large prime number and a and b are two values specified by F_p over ECC. An elliptic curve $E(F_{\mathcal{P}})$ over finite field F_p is defined as: $E(F_{\mathcal{P}}) : y^2 = x^3 + ax + b$

$4a^3 + 27b^2 \neq 0$

G is a base point on E of order $n \geq 2^{224}$; hash function is denoted by h; message is denoted by m and encryption/decryption is denoted by $E_k(.)/D_k(.)$ where k is a secret key and c is the ciphertext.

Key Generation Phase: Each voter chooses his/her private key Pri_k and computes Pub_k. Then, obtains a certificate from a concern certificate authority. The procedure is summarized below:

- Polling station/signer selects a randomly private key Pri_k where Pri_k equal to $d_{sign} \in \{1, \ldots, n-1\}$ and computes public key Pub_k as $P_{sign} = d_{sign} . \mathbb{G}$
- Requester/voter selects a randomly private key Pri_k where private key equal to $d_{req} \in \{1, \ldots, n-1\}$ and computes public key Pub_k as $P_{req} = d_{req} . \mathbb{G}$
- Verifier selects a randomly private key Pri_k where private key equals to $d_{ver} \in \{1, \ldots, n-1\}$ and computes public key Pub_k as $P_{ver} = d_{ver} . \mathbb{G}$

Novel Blind Signcryption for E-Voting System

The requester/voter wants to anonymously communicate a message m to polling server/verifier over a noisy channel in an authenticated and confidential way.

The following steps are required to generate the blind signcrypted text.

Voter /Requester: Selects integers randomly as

$\beta_{\in_R}\{1 \dots n-1\}$
Computes $\mathcal{R} = \beta.\mathbb{G}$
Computes $r = h(m \parallel \mathcal{R} \oplus T)$
Forwards r to signer/voter

Signer/Polling Station

Selects randomly an integer $\gamma_{\in_R}\{1 \dots n-1\}$
Computes $\mathcal{Z} = \gamma.\mathbb{G}$
Generates
$\bar{s} = (d_{sign} + r.\gamma) \bmod n$
Sends $(\mathcal{Z}, \bar{s})$ to requester/voter

Requester/Voter

Selects randomly integers $\alpha, \in_R \{1, \dots \dots n-1\}$
Computes $k_e = h(\alpha.P_{ver})$
Computes $c = E_{k_e}(m||\bar{s})$
Computes $s = \left(\alpha/_{r+\beta+\bar{s}}\right) \bmod n$
Sends$(c, r, s, R, \mathcal{Z})$ to verifier/Polling server

Unsigncryption

Polling Server/Verifier obtains message from blind signcrypted text and checks the validity. If verified then accept and add to voters record, otherwise reject.
Computes $u = d_{ver}.s \bmod n$
Computes $k_e = h\left(u.(P_{sign} + r.(\mathcal{Z} + \mathbb{G}) + \mathcal{R})\right)$
Computes $m||\bar{s} = D_{k_e}(c)$
Computes $r' = h(m \parallel \mathcal{R} \oplus T)$
If $r' = r$ mean m is original and accept it, else reject.

Theorem-1:
The above blind signcryption/unsigncryption is correct if the sender and receiver/verifier confirms the following:

$$u.\left(P_{sign} + r(\mathcal{R} + \mathbb{G}) + \mathcal{R}\right) = \alpha.P_{ver}$$

Proof:

$u.\left(P_{sign} + r(R + \mathbb{G}) + \mathcal{R}\right)$
$= u.\left(P_{sign} + r.\gamma.G + r\mathbb{G} + \mathcal{R}\right)$
$= d_{ver}.s.\left(P_{sign} + r.\gamma.\mathbb{G} + r.G + \mathcal{R}\right)$
$= \alpha/r + \beta + \bar{s}\left(d_{ver}.\left(d_{sign}.G + r.\gamma.\mathbb{G} + r\mathbb{G} + \beta.\mathbb{G}\right)\right)$
$= \alpha.P_{ver}/r + \beta + \bar{s}\left(d_{sign} + r.\gamma + r + \beta\right)$
$= \alpha.P_{ver}/(r + \beta + d_{sign} + r.\gamma)\,(d_s + r.\gamma + r + \beta)$
$= \alpha.P_{ver}$

This proof shows the scheme is correct.

7. RESULTS AND ANALYSIS

In this section of the paper, we present the proposed scheme analysis.
This section has been further divided into two sub sections; Fist one discusses the security analysis of the e-voting model. The second one presents the cost analysis of the proposed scheme and compares it with the existing ones.

7.1 Security Analysis

This scheme is based upon the elliptic curve discrete logarithm problem and we claim that the proposed scheme is secure against various attacks. Here we compare several security attributes with the existing state of the art schemes to check and validate the proposed scheme security.

Definitions:

Elliptic Curve Discrete Logarithm Problem (ECDLP): Let us assume two points P and Q given on elliptic curve E_P such that k is an integer value and compute $Q = k.P$ which is equivalent to the computation of ECDLP.

Confidentiality: Our scheme is secure against various attacks to ensure the confidentiality of message contents, if an attacker gets the secret key d_{sign}, he/she cannot solve ECDLP which is a hard problem.

Case-1: Let us assume that attacker computes k_e using the following equations (1) and (2), but to compute d_{ver} is infeasible (i.e., equal to solve ECDP a hard problem) for an attacker.

$$P_{ver} = d_{ver}\mathbb{G} \quad (1)$$
$$u = d_{ver}.s \quad (2)$$
$$k_e = h\left(u.\left(P_{sign} + r.(\mathcal{Z} + \mathbb{G}) + \mathcal{R}\right)\right) \quad (3)$$

Case-2: Let us assume that the attacker computes k_e using equations (5) and (6) but to

compute β is infeasible (i.e., equivalent to solve ECDP a hard problem) for an attacker.

$$\mathcal{R} = \beta.\mathbb{G} \quad (4)$$
$$\alpha = s.(r + \bar{s} + \beta) \bmod n \quad (5)$$
$$k_e = \quad h\,(\alpha.P_{ver}) \quad (6)$$

Integrity: The integrity property ensures that message does not alter during communication on the noisy channel. Our proposed scheme verifies the voting server. Voter computes $r = h(m \parallel \mathcal{R} \oplus T)$ and forwards to the polling station to sign contents blindly and generates $\bar{s}$. After polling station/signer signature returns to the voter to generate his/ her own signature s and then forwards to polling server for validation. If the attacker changes the message contents during communication from $c \rightarrow \bar{c}$, means this will make to change the value of $m \rightarrow \bar{m}$ as well on the server-side. Thus values r, s will also be changed to $\bar{r}, \bar{s}$ which is infeasible due to the hash function random oracle properties such that $h(m \parallel \mathcal{R} \oplus T) = h(\bar{m} \parallel \mathcal{R} \oplus T)$.

For a valid signature attacker's needs β, d_{sign}, and m to compute from equations (4) and (7) respectively that are also equivalent to solve ECDP a hard problem.

$$P_{sign} = d_{sign}.\mathbb{G} \quad (7)$$

Un-Forgeability: Un-forgeability means nobody can forge values of signature (c, r, s) during communication over a noisy channel, neither attacker nor receiver of the message.

In our e-voting scheme, to generate a valid signature attacker's needs β, d_{sign} and m to compute from equations (4) and (7) respectively that are equivalent to solve ECDP a hard problem.

Authentication: Authenticity ensures the received message/sender is legitimate or not. Our proposed e-voting scheme provides authenticity at two levels; first provides signer/polling station authenticity and second to authenticate casted vote received to polling server.

Here we can discuss that polling server after receiving data verifies the signature using the public key of polling station/signer using the public key P_{sign} associated with a signature key (private key d_{sign}). If verified it means signature generated by the legitimate signer else anybody changed it on the way or somewhere else which will not be acceptable by the verifier/polling server. Computing d_{sign} from equation (7) is already discussed previously that is equivalent to solve ECDP a hard problem.

Public Verifiability: In case of dispute third party can verify message contents after the provision of signature parameters to judge without knowing any secrets about the message. The proposed scheme ensures public verifiability. In case of any dispute the polling server forwards $(m, \bar{s}, \mathcal{Z})$ to judge for issue settlement and verify the original signer.

The third-party verification operations are as following;

Judge (Third verifier)

Verify $(m, \bar{s}, \mathcal{Z}, P_{ver})$

(1) Verifies sender public key P_{sign} with certificate
(2) Computes $r = h(m \parallel \mathcal{R} \oplus T)$
(3) Computes $y = (\bar{s}.\mathbb{G} - r.\mathcal{Z})$
(4) If $y = P_{sign}$ means sign generated by legitimate one with the public key P_{sign}.

Theorem-2

If hold the following means correctness of the above-discussed procedure proved.

$$\bar{s}.\mathbb{G} - r.\mathcal{Z} = P_{sign}$$

Proof:

$$\begin{aligned} &\bar{s}.\mathbb{G} - r.\mathcal{Z} \\ &= (d_s + r.\gamma)\mathbb{G} - r\mathcal{Z} \\ &= d_s.\mathbb{G} + r.\gamma\mathbb{G} - r\mathcal{Z} \\ &= d_s.\mathbb{G} + r.\gamma\mathbb{G} - r\gamma\mathbb{G} \\ &= d_s.\mathbb{G} \\ &= P_{sign} \end{aligned}$$

So, verification is correct.

Non-Repudiation: In case of dispute (polling station and polling server) the third party can verify message contents after the provision of signature parameters to judge without knowing any secrets about the message.

This scheme ensures public verifiability in case of any dispute the polling server forwards parameters $(m, \bar{s}, \mathcal{Z})$ to judge for issue settlement. The judge verifies the original signer or content signed by a legitimate one or someone else.

Our proposed scheme provides third-party verification without disclosing any secret parameters. For dispute settlement, the recipient sends $(m, \bar{s}, \mathcal{Z})$ to judge, to check either the signer signed the original message (m) or not.

Judge Verify $(m, \bar{s}, Z, P_{ver})$
Verifies sender public key P_{sign} having a certificate
Computes $r = h(m \parallel \mathcal{R} \oplus T)$
Computes $y = (\bar{s}.\mathbb{G} - r.\mathcal{Z})$
If $y = P_{sign}$ means sign is generated by legitimate one with the public key P_{sign}.

Un-traceability: Un-traceability ensures that there will be no way for the message's receiver to trace the message's sender. The voter used the random number as a private key α, β for computing parameters (c_i, r_i, $\mathcal{R}_i$, s_i, Z_i) and send to the polling station and thus the verifier or polling station has no way to check the validity of the sender.

Unlinkability: Unlinkability means no way to link previous messages with a sender of the massage. For example, voter sends $r = h(m \parallel \mathcal{R})$ for a sign to a polling station and signer maintains the record list L_i $(r_1, r_2, \ldots, r_i)$. Later on, the signer/polling station cannot link r_i generated from m_i because of such pair (m_i, r_i) generated by anybody else either polling server or polling station.

Forward Secrecy: Attacker unable to get private keys d_{req} and d_{sign} of any correspondent after losing long term communication as well as not be able to get previous messages.
Our e-voting scheme provides forward secrecy if losses any private key. The attacker cannot recover it from previous signcrypted text $(c, r, s, \mathcal{R}, \mathcal{Z})$. Moreover, if an attacker tries to compute α, he/she has to first compute β from equation (4)which is infeasible (*i.e.*, equivalent to solve ECDP a hard problem).

All the security properties compared with existing schemes are reflected in Table 2.

7.2 Cost Analysis

Total operations are taken by an algorithm and extra bits appended with a message for security purposes using an insecure communication network referred to as the cost of that scheme. Cost depends on the processing time calculated on every node and appended extra bits with messages known as overhead bits discussed in the following two sub-sections.

7.2.1 Computational Cost

To calculate operational cost we mostly count the number of costly operations used in that scheme. These operations are exponentiations $(M - Exp)$ and scalar multiplication (Mul) and remaining operations consider negligible. As per the security controller, Infineon's (SLE66CUX640P) [17] processing time unit for per Mul is 83 ms and for the unit, $M - Exp$ is counted 220 ms. Here we measure propose e-voting scheme operational cost and compare with already existing schemes found in the literature. The proposed scheme algorithmic complexity reflected in Table 3 and total computational cost comparison with other schemes reflected in Fig. 4.

Table 2: Security Analysis Comparison

Schemes	Confidentiality	Integrity	Authenticity	Un-Forge ability	Direct Public Verification	Non-Repudiation	Forward Secrecy	Un-Traceability	Un-Linkability
Riaz *et al* [14]	√	√	√	√	-	√	-	√	√
Xiuying *et al* [13]	√	√	√	√	√	-	√	√	-
Awasthi *et al* [12]	√	√	√	√	-	√	√	√	√
Scheme Proposed	√	√	√	√	√	√	√	√	√

Table. 3: Comparative Computational Cost			
Schemes		M-Exp	Mul
Ullah *et al.* [15]	Requester	-	3
	Signer	-	1
	Verifier	-	2
Xiuying *et al.* [14]	Requester	7	-
	Signer	2	-
	Verifier	2	-
Awasthi *et al.* [13]	Requester	4	-
	Signer	1	-
	Verifier	2	-
Scheme Proposed	Requester Voter	-	2
	Signer/Polling Station	-	1
	Verifier/Polling Server	-	2

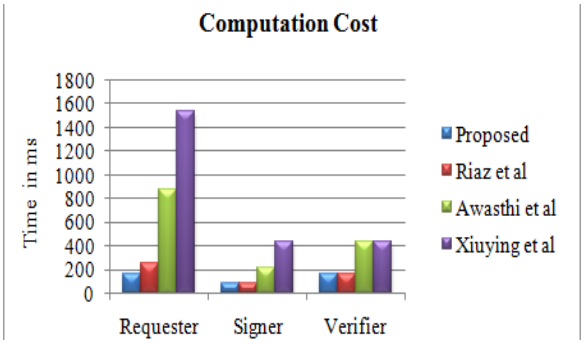

Fig. 4: Computational Time comparison on each node

7.2.2 Communication Overhead

The section reflects the communication cost comparison. For this purpose, we calculate total appended extra bits attached to the messages. It depends on the selection of parameters sent by the sender node to the receivers. According to NIST recommendation.

(For 2014 and onward) unit cost for basic parameters in bits are; our proposed e-voting scheme communicate $|r = 224bits|$, $|s = 224bits|$, $|R = 224bits|$ and $|Z = 224bits|$. The total communication overhead comparison shows in Fig. 5.

8. CONCLUSION

We present in this paper a secure and comparatively efficient blind signcryption scheme based e-voting scheme using elliptic curve cryptosystem. This scheme offers some extra properties like forwarding secrecy, unlink-ability, and non-repudiation with basic ones. We compared this scheme with existing schemes found in literature and proved that our proposed scheme has greater advantages over others based on operational and communicational cost. Furthermore, it is also best suited for a scarce environment like mobile commerce transactions or any country citizen's portal.

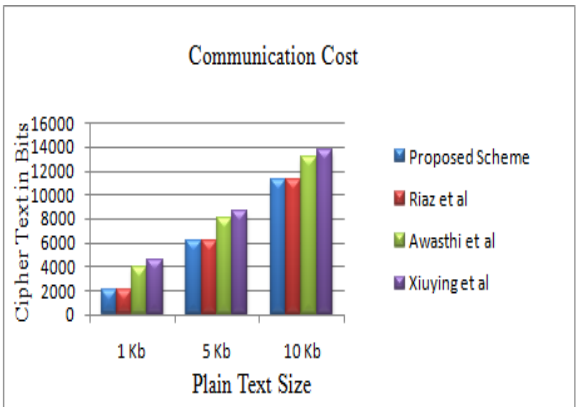

Fig. 5: Communication Cost Comparison using different size of messages

ACKNOWLEDGMENT

Authors acknowledge the Department of Information Technology, Hazara University Mansehra, Pakistan, for motivating and supporting the successful completion of this research work.

REFERENCES

1. Chaum D, "Blind Signatures for Untraceable Payments". In: Chaum D., Rivest R.L., Sherman A.T. (Eds.) *Advances in Cryptology*, pp. 199 203, Springer, Boston, M.A., 1983.
2. Khan K. M., Arshad, J., Khan M. M, "Investigating performance constraints for blockchain based secure e-voting system", *Future Generation Computer Systems*, Vol. 105, pp. 13-26, 2020.
3. Kalaiyarasi G., Balaji K., Narmadha T., Naveen V., "E-Voting System In Smart Phone Using Mobile Application", *Proceedings of the 6th International IEEE Conference on Advanced*

Computing and Communication Systems (ICACCS), pp. 1466-1469, Coimbatore, India, 6-7 March 2020.

4. Nadar T., Rawal M., Patel J., Shah A., Revathi A. S. A., "Novel Approach to Implement Decentralized Voting System Using Blockchain", *Proceedings of the International Conference on Wireless Communication*, Springer, Singapore, pp. 471-479, 2020.
5. Dipti P., Sakhapara A., Badgujar A., Adepu D., Andrade M., "Secure Online Voting System Using Biometric and Blockch Pain," In *Data Management, Analytics and Innovation*, Springer, Singapore, pp. 93-110, 2020.
6. Shahram N., Shaikh A.Z., Naqvi S., "A Novel Hybrid Biometric Electronic Voting System: Integrating Finger Print and Face Recognition", *Mehran University Research Journal of Engineering and Technology*, Vol. 37, No. 1, pp. 59-68, January 2018.
7. Zheng Y., "Digital signcryption or how to achieve cost (signature & encryption) ≪ cost (signature) + cost (encryption)", In: *Kaliski (Eds.) Advances in Cryptology-(CRYPTO' 97)*, Lecture Notes in Computer Science, Vol. 1294, Springer, Berlin, Heidelberg, pp. 165-179, Springer-Verlag, 1997.
8. Mohib Ullah, Nizamuddin, Umar. A. I., Amin N, Amin S., "An Efficient Mobile Phone Voting System based on Blind Signcryption", P*roceedings of the 4th International Conference on Computer and Emerging Technologies (ICCET)*, Shah Abdul Latif University, Khairpur Mirs, Pakistan, 2-22 March 2014.
9. Chaum D., Fiat A., Naor M., "Untraceable electronic cash", In *Goldwasser S. (Eds.) Advances in Cryptology (Crypto'88),* Lecture Notes in Computer Science, Vol. 403, pp. 319-327, Springer, New York, N.Y., 1990.
10. Brands S.A., "Untraceable Off-line Cash in Wallets with Observer", In *Stinson D.R. (Eds.): Advances in Cryptology (Crypto '93)*, Lecture Notes in Computer Science, Vol. 773, pp. 302-318, Springer, Berlin, Heidelberg, 1994.
11. Nikooghadam M., Zakerolhosseini A., "An efficient Blind Signature Scheme Based on the Elliptic Curve Discrete Logarithm Problem", *The ISC International Journal of Information Security*, Vol. 1, No. 2, 125-131, 2009.
12. Chakraborty K., Mehta J., "A stamped blind signature scheme based on elliptic curve discrete logarithm problem", *International Journal of Network Security*, Vol. 14, No. 6, pp. 316-319, 2012.
13. Awasthi A. K. Lal S., "An Efficient Scheme for Sensitive Message Transmission Using Blind Signcryption", *Proceedings of the International Conference on Communication,* Kumabakonam India, December 2004.
14. Xiuying Y., Dake H., "A new efficient blind Signcryption Scheme", *Wuhan University Journal of Natural Sciences*, Vol. 13, No.6, pp. 662-664, 2008.
15. Ullah R., Nizamud Din, Umar. A. I., Amin N, "Blind Signcryption Scheme Based on Elliptic Curves", *Proceedings of the Conference on Information Assurance and Cyber Security (CIACS),* pp. 51-54, Rawalpindi, Pakistan, 2014.
16. Batina, L., S. B. O¨rs, B. Preneel, Vandewalle, J., L. Batina, "Hardware architectures for public-key cryptography", *Integration, the VLSI Journal*, Vol. 34, No. 1–2, pp. 1–64, 2003.
17. Certicom Research. Standards for efficient cryptography, SEC1: elliptic curve cryptography, Standards for efficient cryptography group (SECG), September 20, 2000. Available at: https://www.secg.org/SEC1-Ver-1.0.pdf [Last accessed on 10th January 2018].