

A Smart Card Oriented Secure Electronic Voting Machine Built on NTRU

Safdar Shaheen¹, Muhammad Yousaf¹, and Mudassar Jalil²

¹Riphah Institute of Systems Engineering, Riphah International University, Pakistan

²Department of Mathematics, COMSAT Institute of Information Technology, Pakistan

Abstract: Free and fair elections are indispensable to quantify the sentiments of the populace for forming the government of representatives in democratic countries. Due to its procedural variation from country to country and complexity, to maneuverer, it is a challenging task. Since the Orthodox paper-based electoral systems are slow and error-prone, therefore, a secure and efficient electoral system always remained a key area of research. Although a lot of literature is available on this topic. However, due to reported anomalies and weaknesses in American and France election in 2016, it once again has become a pivotal subject of research. In this article, we proposed a new secure and efficient electronic voting scheme based on public key cryptosystem dubbed as Number Theory Research Unit (NTRU). Furthermore, an efficient and robust three factors authentication protocol based on a personalized memorable password, a smartcard, and bioHash is proposed to validate the legitimacy of a voter for casting a legal vote. NTRU based blind signatures are used to preserve the anonymity and privacy of vote and voters, whereas the proficiency of secure and efficient counting of votes is achieved through NTRU based homomorphic tally. Non-coercibility and individual verifiability are attained through Mark Pledge scheme. The proposed applied electronic voting scheme is, secure, transparent and efficient for large scale elections.

Keywords: EVM, blind signature, homomorphic tally, smart card, NTRU.

Received July 29, 2017; accepted June 19, 2018

<https://doi.org/10.34028/iajit/17/3/12>

1. Introduction

In current epoch, the applicability of electronic technology has become an indispensable part of our daily life and swelling day by day throughout the globe. A consensus is being built to utilize this technology for privacy, efficiency, and scalability of a democratic election. The USA was the pioneer country who used computer first time for casting votes in 1964 [10]. It was a turning point (major drift) towards electronic voting devices. Electronic voting is a process which uses electronic means (devices) for casting votes and counting results in place of ballot papers and boxes. Such votes are recorded, stored and processed in digital form on electronic devices called Electronic Voting Machines (EVM). Primarily there exist two families of an electronic voting system dubbed as online and offline. In online mechanism [1] votes are cast via internet infrastructure whereas, in an offline scenario [3] independent electronic polling booths are used. Amongst them, some schemes are built on cryptographic frameworks whereas others have non-cryptographic properties. Furthermore, some are receipt oriented [8, 20] while the others have receipt-free [13] characteristics. Although, an online voting mechanism is more portable and flexible than offline voting, it is less trustworthy than offline voting due to inbuilt infrastructural vulnerabilities. Many attacks such as: Denial of Service (DoS), Distributed

DDoS, and interception are major hurdles in ways of online voting. The residue trust in online voting has further been broken by reported anomalies and weaknesses in American and France election held in 2016. As the security is more important than flexibility, therefore, we have adopted offline voting scenario in the present paper. Subsequently, the most important decisions are linked with the outcomes of election and any loophole or flaw in an election can lead to indecisive or incorrect election results. Therefore, in the light of aforementioned facts, it is a common perception to design an efficient and secure EVM which is capable to address the following basic questions:

- Q1. How to verify the legitimacy of the voter?
- Q2. How to preserve the anonymity and privacy of vote and voter?
- Q3. How can voter check that vote is cast as intended?
- Q4. How to randomize the contesting candidates during each vote?
- Q5. How to attain a non-coercibility of a vote?
- Q6. How to count the votes securely and efficiently?

In the present paper, we proposed a new secure and efficient EVM based on the asymmetric cryptosystem called Number Theory Research Unit (NTRU). It has been designed in the light of questions mentioned above. To validate the legitimacy of a voter in this scheme, a lightweight authentication mechanism based

on three factors namely smartcard (something a voter have), personalized password (something a voter knows) and a bioHash fingerprint (something a voter is) is proposed. This scheme uses a hash function for authentication and therefore, computationally faster. The main reason for the adoption of a smartcard is its portability, low computational cost and secure storage capability properties. The anonymity and privacy of vote and voter are preserved using blind signature built on lattice-based post-quantum resistance public key cryptosystem, NTRU [2, 14, 25, 29]. Moreover, the secure and efficient counting of votes is accomplished through NTRU based homomorphic tally process. Additionally, the legendary Mark Pledge [17] scheme is used to attain individual verifiability and non-coercibility in the current paper. This new electronic voting scheme is secure, transparent and efficient for large scale elections.

The rest of paper is arranged in the following ways. Section 2 briefly describes the literature review. Section 3 illustrates the foundational features essential to understand the proposed EVM. Our smartcard oriented secure and efficient EVM built on advanced public key cryptosystem NTRU is presented in section 4. Security analysis of proposed scheme is given in section 5. The conclusion and future work are presented in the last section.

2. Literature Review

Chaum [9] first time proposed an idea of EVM. This idea became a centre of attraction amongst the researcher community and later on, a race is started amongst them to construct an efficient and secure EVM. In a short span of time, many cryptographic and non- cryptographic [23, 24] articles were published regarding EVM. Since non-cryptographic voting schemes emphasis only on availability but not on security, therefore, they are not suitable for secure voting system and out of the scope of this paper. Chaum [7] proposed another paper which addresses anonymity of voter identity. But major drawback pointed out in this article was that a single voter can disrupt the whole voting process. Despite all, Chaum [7, 9] and Neff [23] ideas laid down a foundation of a new paradigm in electronic voting research. The concept of the blind signature was also first proposed by Chaum [6] to preserve anonymity and privacy of votes. Moreover, Wang *et al.* [28] proposed an efficient scheme based on the blind signature. Juels *et al.* [18] receipt-free voting scheme is considered one of the most efficient and practical schemes to date. Furthermore, some receipt oriented schemes [8, 20] were proposed. After that, the homomorphic encryption based voting schemes were proposed in [4, 30]. A smartcard based voting machine was proposed in [5]. Aforementioned EVMs do not address all the security requirements. Also, all these schemes are

based on Rivest, Shamir, and Adelman (RSA), Elliptic Curve Cryptography (ECC), EL-Gamal, Paillier and ID-based [22] public key cryptosystems which are less efficient than NTRU [2, 14, 25, 29]. We can observe that most of the schemes referred above focus on some specific properties. They are lacking to present a broad view of secure EVM which can address nearly all security requirements. The above mentioned smartcard scheme is also susceptible to password guessing and smart card loss attack. Also, it does not offer bioHash services. Resultantly, there is an utmost need to build a secure and efficient EVM which can solve aforementioned problems and satisfy more and more security and implementation requirements. Furthermore, it is proficient to address the questions mentioned in the introduction section.

3. Foundational Blocks

The building blocks which play a vital role in constructing our proposed EVM are given below:

3.1. Number Theory Research Unit (NTRU)

It is a lattice-based public key cryptosystem, first presented by Hoffstein *et al.* [14]. It is selected due to its simplicity, efficiency, small key size and high level of security. It operates on a truncated ring of a polynomial and uses in lightweight devices. It is said that quantum computers will break most of the conventional public key cryptosystems due to its tremendous speed [19] but NTRU will resist against quantum attacks.

3.2. Blind Signature

Blind signature [15, 27, 28] is used to protect the anonymity of voters i.e., to hide the linkage between voter and vote. It is a special variant of digital signature that preserves all properties of digital signature together with correctness, blindness, unforgeability, and untraceability.

3.3. Homomorphic Encryption

It is a form of encryption in which mathematical operations are performed on encrypted text to achieve the encrypted result [11, 12]. When this result is decrypted, it matches the result obtained by performing mathematical operations on plaintext. In voting schemes, homomorphic algorithms [4] are used for tallying of votes while preserving the confidentiality of individual votes. In our proposed scheme NTRU is used to fulfil this task.

3.4. Commitment/Opening Scheme

Commitment schemes enable an entity to commit a value without revealing it to others. The two main properties of these schemes are hiding and binding.

The commitment leaks no information about the value committed due to its hiding property. Whereas, binding property eliminates the possibility of modification in original commitment. To show the committed value, a secret opening value has to be revealed to others.

3.5. Security and Implementation Features

The security and implementation features along with their definitions necessary to build a secure, efficient and scalable EVM are given below.

- **Authentication:** The legitimacy of each voter is verified before casting vote through an authentication protocol. This mechanism discourages illegitimate voter to cast a bogus vote.
- **Authorization:** After authentication and legitimacy assurance of voter, an authorization token is granted to the voter to cast his vote.
- **Confidentiality:** The privacy protection of vote and voter is called confidentiality.
- **Integrity:** After casting a vote no one should be able to tamper or modify vote intentionally or unintentionally.
- **Accuracy:** Assurance that vote is recorded correctly in the voting process.
- **Eligibility:** Only the legitimate voter can cast a vote.
- **Anonymity:** No one can find a link between voter and casted vote.
- **Non-coercibility:** Voter should not be able to prove to whom he/she voted.
- **Verifiability:** Validation that votes are counted correctly in final tally is called verifiability and it has two type namely individual verifiability (verification by a voter that his/her vote is counted in the final tally) and universal verifiability (verification of votes by the third party).
- **Uniqueness:** No one can cast vote more than once.
- **Fairness:** No participant can gain any knowledge about the tally before the counting stage.

Furthermore, the notation used in our proposed scheme along with their description is organized in Table 1.

Table 1. Notations used in the paper along with their description.

Notation	Description
V_i	Voter; $i=1$ to n
$BioH^{V_i}$	Biohashing of voter's biometric template
NIC^{V_i}	Personal Identification Number of Voter
$Passwd$	Passphrase provided by a voter
$h(.)$	Collusion resistance hash function
$\chi(.)$	bioHash Extraction function
$Pub_{NTRU}^{V_i}$	Public Key of voter generated by NTRU
$Pr v_{NTRU}^{V_i}$	Private Key of voter generated by NTRU
σ^{V_i}	Signature of voter
SP^{V_i}	Double hash of secret password of voter
VID^{V_i}	Voting Identity of voter
$L_{Token}^{V_i}$	Locality Token is a unique identifier assigned to each Electronic Polling Booth (EPB)
EL_{id}	Election Identity
PRV^{V_i}	Private Parameter: Encrypted private key with AES and having a key $Passwd$
RS^{SCIC}	Random Secret of SCIS
RN_i^{SCIC}	Random Number generated by SCIC
MK^{SCIC}	Master Key of SCIC
$E_{Token}^{V_i}$	Eligibility Token for casting a vote
$CData^{V_i}$	A parameter for validating eligibility token and random secret
TAG^{V_i}	A parameter for validating legitimacy for a voter
K_{pub}^{EC}	A public key of Election Commission generated through NTRU
VC	Verification Token
C_i	Encrypted votes with the public key of EC
H_i	Hashed value of encrypted vote
VS^{V_i}	Verification string for a voter
β	Small random polynomial for commitment and opening commitment
h	A public key generated by NTRU
(f, f_p)	Private keys generated by NTRU
$Commit(.)$	Commitment function
$OpeningCommit(.)$	Commitment opening function
\oplus	Xoring
\parallel	Concatenation

4. NTRU based proposed EVM

4.1. Role and Responsibilities of Key Components

Before depicting the functionality of proposed scheme, it is necessary to understand the role and responsibilities of key components mentioned below.

- **Election Commission (EC):** EC is responsible to endorse policies, procedures, a rule of laws and hiring experts for conducting a free and fair election.
- **Public Verification Server (PVS):** PVS is used for publishing, confirmation, and validation of public data relevant to the election.
- **Election Management Cell (EMC):** EMC is responsible for conducting the election according to the policy endorsed by EC.
- **Voter:** A legitimate entity authorized to cast vote.
- **Voter Registration and Credential Verification Cell (VR&CVC):** Voters are got register through

VR&CVC. This cell is liable to verify the voter identity through submitted credentials including National Identity Card (NIC) number and imprinted biometric fingerprints. The reason for conducting biometric verification is that it is a reliable and quantifiable way to identify a voter. On successful verification, Voter Registration and Credential Verification Cell (VR&CVC) extracts $BioH^V_i$ from biometric figure prints. The main reason for choosing biohashing [16, 21] is to overcome the false rejection problem. Afterward, a voter generates the parameters shown in Figure 1. (cf. subsection 4.2.1.) from steps 3-7. Then these parameters are sent to VR&CVC for further usability. VR&CVC takes a voter identity from received data, extracts a locality token (cf. Table 1), and election identity stored against National Identity of a voter in a database. These parameters are digitally signed with the private key of VR&CVC and sent to SCIC.

- *Smartcard Issuance Cell (SCIC)*: It burns these parameters on a Voter Smartcard (VSC) and issues it to the associated voter.
- *Electronic Polling Booth (EPB)*: The tasks of authentication, verification, authorization and vote casting are accomplished through the EPB.
- *Signing Authority (SA)*: SA validates a voter and signs on his/her vote blindly on the behalf of power delegated to his/her by EC for legalization.
- *Verifying Authority (VA)*: VA verifies the sign of SA on a vote and sends it to Electronic Ballot Box (EBB).
- *Blockchain Server (BCS)*: A public ledger uses to store, read and validate the electronic data in the form of blocks is called Blockchain. Its key characteristics are integrity, transparency, and verifiability. In our proposed scheme manages such kind of activities.
- *Third Party (TP)*: TP is responsible for verifying the legitimacy, accuracy, and authenticity of votes.

4.2. Operational Procedure

The step by step operational mechanism of our proposed scheme is given as under:

4.2.1. Registration and VSC Issuance

Voter V_i physically approaches to $VR\&CVC_i$ for registration. He performs the following steps by using a system located in $VR\&CVC_i$ premises.

- *Step 1*: V_i submits his/her *Credentials* V_i including NIC^{V_i} and imprinted biometric finger prints ($Biometric^{V_i}$) through feature extraction device to $VR\&CVC_i$. At the time of registration for getting NIC^{V_i} at the age of eighteen, voter's biometric fingerprints had already been registered in CVC.

- *Step 2*: The $VR\&CVC_i$ scrutinized voter's credentials and conducts biometric verification against template already stored in its database. The voter is informed about verification status accordingly. On successful validation, bioHash ($BioH^{V_i}$) is extracted from biometric template through bioHash extraction function $\chi(\cdot)$ and stored in its database.
- *Step 3*: After that V_i generates his/her public and private keys $Pub_{NTRU}^{V_i}, Prv_{NTRU}^{V_i}$ using advanced public key cryptosystem, NTRU.
- *Step 4*: Then, V_i self-signs his/her public key using his/her own private key as $\sigma^{V_i} = Sign_{Prv}^{V_i}(Pub_{NTRU}^{V_i})$.
- *Step 5*: After this V_i compute the double hash of unique secret password through collusion free hash function $h(\cdot)$ as $SP^{V_i} = h(h(Passwd))$.
- *Step 6*: By using $Passwd$ as a key, V_i encrypts his/her private key through symmetric key algorithm AES as $PRV^{V_i} = \xi_{Passwd}^{AES}(Prv_{NTRU}^{V_i})$.
- *Step 7*: Finally, V_i submits parameters $\langle NIC^{V_i}, Pub_{NTRU}^{V_i}, \sigma^{V_i}, PRV^{V_i}, SP^{V_i} \rangle$ to $VR\&CVC_i$ for getting VSC.
- *Step 8*: Afterward, $VR\&CVC_i$ assigns Voting Identity (VID^{V_i}), Locality token ($L_{Token}^{V_i}$), Election Identity (EL_{ID}) and BioHash ($BioH^{V_i}$) to voter and sent these parameters along with other received parameters (cf. Step 7) to SCIC, digitally signed with its private key ($Prv^{VR\&CVC}$).
- *Step 9*: From this step to onward, VSC burning procedure is started. Initially, SCIC verifies the signature of $VR\&CVC_i$ on parameters and generates a Random Secret (RS) by hashing its master key and a random number generated through a Pseudo Random Number Generator (PRNG) algorithm as $RS^{SCIC} = h(MK^{SCIC} || RN_i^{SCIC})$.
- *Step 10*: Then SCIC computes the eligibility token of a voter as $E_{Token}^{V_i} = h(VID^{V_i} || SP^{V_i} || BioH^{V_i} || L_{Token}^{V_i})$.
- *Step 11*: After that $CData^{V_i}$ and TAG^{V_i} are figured out for origin authentication and integrity validation of parameters.
- *Step 12*: Finally, VSC is sent to voter via $VR\&CVC_i$ after burning the following parameters $\langle VID^{V_i}, SP^{V_i}, Pub_{NTRU}^{V_i}, \sigma^{V_i}, PRV^{V_i}, CData^{V_i}, TAG^{V_i} \rangle$

Above-mentioned steps are demonstrated in Figure 1.

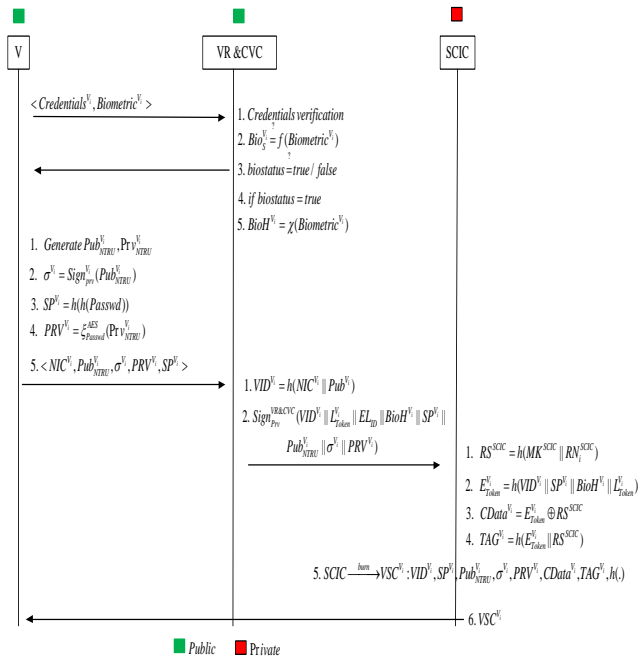


Figure 1. Voter’s registration and VSC issuance procedure.

4.2.2. Legitimacy Validation of Voter

On Election Day, voter goes to the Polling Station (PS) for casting his/her vote. He uses EPB located in PS premises to get validated. The step by step procedure for the authentication of a voter is given below:

- **Step 1:** Initially, a voter inserts his/her VSC into card reading device attached to the EPB. Then he/she enters a unique secret password (*Passwd*) using User Graphic Interface (GUI) of EPB. Finally, he/she imprints biometric fingerprints through biometric extraction device attached to the EPB.
- **Step 2:** Three factors authentication is performed in this step. The detail is given below one by one.

First Factor Authentication (FFA): EPB extracts a VID^V from VSC and compares it to already stored VID^V in EPB database.

Second Factor Authentication (SFA): After successful verification of FFA, EPB computes a double hash of *Passwd* entered by a voter to get a new hash SP_N^{EPB} and compares it with old SP^V stored on VSC.

Third Factor Authentication (TFA): On the true result of SFA, a biometric extraction procedure is performed on imprinted biometric fingerprints and a new bioHash $BioH_N^{EPB}$ is calculated and compared to the old bioHash stored in EPB database against voter’s identity VID^V . If the comparison is true then EPB computes an

eligibility token E_{Token}^{EPB} by performing hashing operation $h(.)$ on parameters VID^V , SP_N^{EPB} , $BioH_N^{EPB}$ currently computed and L_{Token}^{EPB} token already stored in EPB’s local record as its identity. This step restricts the voter to cast vote in his/her own locality EPB.

- **Step 3:** For origin authentication and integrity validation of parameters, a random seed RS^{EPB} is computed by performing a XOR operation \oplus between E_{Token}^{EPB} calculated in step 2 and $CData^{Vi}$ already saved on VSC. This process is depicted in Figure 2.

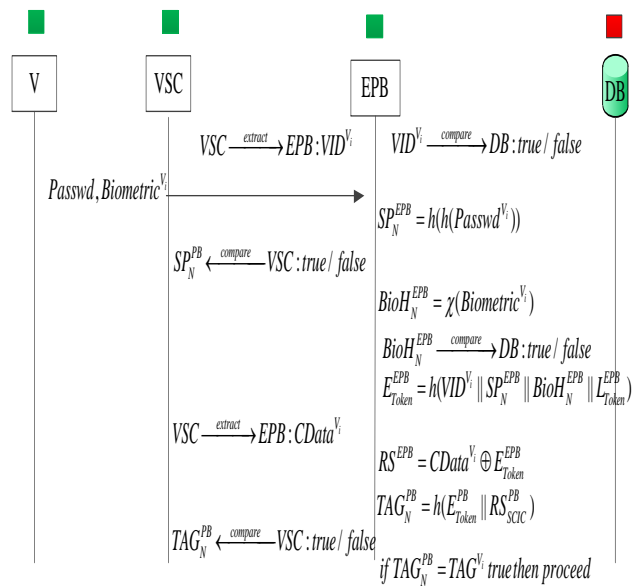


Figure 2. Validation and verification procedure.

- **Step 4:** Finally, a new TAG^V is computed by performing $h(.)$ on the concatenated result of E_{Token}^{EPB} and $CData^{Vi}$ i.e., $E_{Token}^{EPB} || RS_{KG}^{EPB}$.
- **Step 5:** If new TAG^V and old TAG stored on VSC are same then VSC is genuine, parameters on VSC are correct and generated by SCIC and voter is legitimate (on the basis of VSC, password and biometric fingerprints).

He/she is an authentic voter and authorized to cast vote. Therefore, a fresh ballot paper with permuted contesting candidates is displayed on EPB’s screen.

4.2.3. Preparing Vote for Casting

A voter prepares his/her ballot paper by selecting his/her favourite candidate. On candidate selection, a verification code will be displayed at the bottom of a ballot paper and in VC column (encircled with red colour). The verification code displayed at the bottom of ballot paper will be equal to the VC against a selected candidate. This procedure is shown in Figure 3.




Ballot Number: 135947			
Candidate	Symbol Assigned	Vote for	VC
A		<input type="checkbox"/>	8FD3
B		<input type="checkbox"/>	72T9
C		<input checked="" type="checkbox"/>	PZ8R
Verification Code: PZ8R			

Figure 3. Pictorial presentation of a ballot paper.

This verification code is calculated by using the following formula taken from Mark pledge 3 [17].

$$VC_i = \begin{cases} \theta_i = (b'.r - r + \theta_i) / b' & \text{if } b' = 1 \\ 2r - \theta_i = (b'.r - r + \theta_i) / b' & \text{if } b' = -1 \end{cases} \quad (1)$$

randomly generates θ_i and r ; $i = 1, \dots, n$

Calculate VC_i for each candidate, pledge value for Yes candidate

For YES vote the value of “ b' ” is one, whereas for NO vote it has value equal to minus one. The verification code is denoted by θ whereas a random number by “ r ”.

4.2.4. Getting Stamp on Vote by SA for Legalization

The key components involved in this protocol are a Voter (V), Signing Authority (SA) and Verifying Authority (VA). V gets encrypted ballot paper together with VS^{Vi} through the following procedure.

By using NTRU cryptosystem and choosing a small blind polynomial “ b ”, V encrypts the vote with EC’s public key to obscure its originality as

$$C_i = \xi_{Pub}^{NTRU} (V_i, b, h, p, q); i = 1 \text{ to } \# \text{ of candidates } V_i = \{1 \text{ or } 0\} \quad (2)$$

Then he computes verification string (VS^{Vi}) by making hash of θ_i (cf. Equation (1)) and C_i (cf. Equation (2)) as

$$VS^{Vi} = h(\theta_i \parallel C_i); i = 1 \text{ to } \# \text{ of candidates} \quad (3)$$

where θ_i is verification code and C_i is encrypted vote

A voter then saves VS^{Vi} , θ_i , and C_i on his/her VSC.

Finally, the following steps are performed in EPB.

- Step 1: V signs C_i and VID^{Vi} with his/her private key.
- Step 2: Then he sends signed parameters to the SA.
- Step 3: SA verifies the signature of the voter on a vote by applying V’s public key and validates VID^{Vi} of voter.
- Step 4: After verification, SA blindly signs the encrypted vote with his/her private key and returns the result back to V.
- Step 5: V validates the signature of SA on an encrypted vote, verifies its integrity (Equation (3)) and forwards it to VA for tallying process.
- Step 6: VA verifies the signature of SA on vote and verification string and sends them to the

Electronic Ballot Box (EBB) for tallying votes and further verification. This process is illustrated in Figure 4.

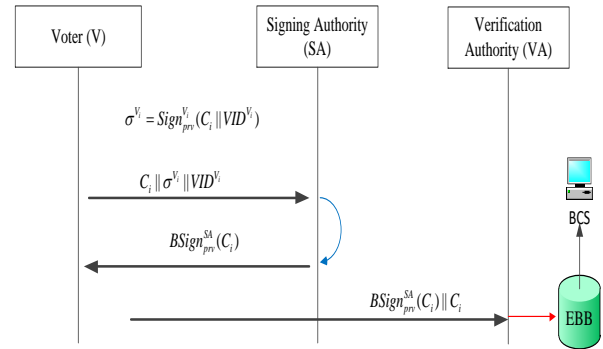


Figure 4. Blind signature and verification process.

At the end of election time, EBB shuffles encrypted votes and sends them to Blockchain Server (BCS). BCS using blockchain methodology makes tampered resistant chain of blocks [26]. Each BCS uses NTRU based homomorphic encryption for tallying process and forwards it to EC for publishing on PVS. After verifying received data thoroughly and tallying, the data is published on PVS. Now anyone can verify votes displayed on PVS in tampered proof format.

EC computes a Verification String (VS) for Third Party (TP) by using the following steps and displays VS and H_i on PVS.

$$Commit(m_i, r, h, p, q; \beta) = \xi_{Pub_{TP}}^{NTRU} (m_i, r, h, p, q; \beta) \oplus \beta = VS_i^{TP} \oplus \beta = VS \quad (4)$$

$m_i = (C_i \parallel H_i)$ and $H_i = h(C_i)$

After the announcement of the election result, a string β is sent to PVS for Third Party Verification. TP verifies the strings C_i by using the Algorithm 1 named Opening Commit described below:

```

Algorithm 1: OpeningCommit (VS, f, f_p, \beta)
{
  VS \oplus \beta = VS_i^{TP}
  D_{PVT_{TP}}^{NTRU} (VS_i^{TP}, f, f_p) = m_i
  #where m_i = (C_i \parallel H_i) and H_i = h(C_i)
  #Again compute
  h(C_i) = h_i
  if (h_i = H_i)
    C_i is accepted as genuine
  else
    rejected
}
    
```

5. Security Analysis of Proposed scheme

Our proposed scheme fulfils key security requirements essential for secure and efficient EVM. To validate the legitimacy of a voter, a lightweight authentication mechanism is built on three factors (cf. step 2; section 4.2.2). Since the computation in this mechanism is accomplished through a collusion-resistant hash function, therefore, it is computationally faster. In the case of VSC stolen or loss, a memorable password and biometric hashing will disallow the illegitimate voter

to cast his/her vote. In addition, a password guessing attack is avoided by using double hashing technique. Impersonation attack on parameters in VSC is not feasible due to integrity protection mechanism provided in the authentication protocol. This VSC is portable, have a secure storage capability and low computational cost.

In the proposed scheme, a Random Secret (RS) of SCIC is generated and embedded on VSC by including its master key. The parameters stored on VSC cannot be impersonated without knowing the master key. Hence, it also protects the integrity of VSC's parameters. Since the voter becomes capable to cast his vote after integrity check of all necessary parameters stored on VSC. Therefore, it is not practicable for a fraudulent voter to cast a bogus vote.

To restrict voter to cast vote in his/her own locality/ward, a locality token is extracted from the database of local EPB. Eligibility token is created and compared to the eligibility token stored on VSC for locality assurance. This action compels the voter to cast his/her vote in the registered locality only. Also, he/she cannot cast his/her vote more than once.

The anonymity and privacy of vote and voter are preserved using blind signature scheme built on NTRU. The individual verifiability in proposed scheme is attained by using MarkPledge3 [17] scheme. Third Party (TP) may conduct verification by using Commit and Opening protocol having binding and hiding properties. Likewise, the secure and efficient counting of votes is done through NTRU based homomorphic tally process.

Our registration process provides liberty to the voter to set his memorable password and generates key pairs using NTRU. This process shifts the control of secret parameters towards voter. In this scheme, votes are displayed in encrypted form in public domain. Therefore, they can be verified in encrypted form but a voter cannot tell anyone about the candidate to whom the vote is cast. This feature adds the non-coercibility property in our proposed scheme.

The online voting schemes are vulnerable to many attacks due to its worldwide connectivity. So, we adopted an offline voting scenario to avoid possible attacks such as Dos, replay and impersonation attacks.

6. Conclusions

In the present paper, a new secure and efficient scheme is proposed based on post-quantum cryptosystem NTRU. The legitimacy of a voter is validated through a lightweight authentication mechanism based on three factors namely smartcard, personalized Password, and bioHash fingerprints. This scheme has been designed in the light of questions mentioned in the introduction section and fulfils key security requirements essential for secure and efficient EVM. The security and efficiency of the counting process is obtained through

NTRU based homomorphic tally process. This new electronic voting scheme is secure, transparent and efficient for large scale elections. As a future work, we will prepare a test bed for proposed paper and publish results in an upcoming paper.

References

- [1] Agarwal H. and Pandey G., "Online Voting System for India Based on AADHAAR ID," in *Proceedings of 11th International Conference on ICT and Knowledge Engineering*, Bangkok, pp. 1-4, 2013.
- [2] Alsaïdi N. and Yassein H., "BITRU: Binary Version of the NTRU Public Key Cryptosystem via Binary Algebra," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 11, pp. 1-6, 2016.
- [3] Arooj A. and Riaz M., "Electronic Voting with Biometric Verification Offline and Hybrid Evms Solution," in *Proceedings of 6th International Conference on Innovative Computing Technology*, Dublin, pp. 332-337, 2016.
- [4] Balasubramanian K. and Jayanthi M., "A Homomorphic Crypto System for Electronic Election Schemes," *Circuits and Systems*, vol. 7, no. 10, pp. 3193-3203, 2016.
- [5] Canard S. and Sibert H., "Votinbox-A Voting System Based on Smart Cards," France Telecom, Research and Development, 42 rue des Coutures, BP 6243, F-14066 Caen Cedex 4, France, 2008.
- [6] Chaum D., "Blind Signatures for Untraceable Payments," in *Proceedings of Advances in Cryptology*, Springer, pp. 199-203, 1983.
- [7] Chaum D., "Elections with Unconditionally-Secret Ballots and Disruption Equivalent To Breaking RSA," in *Proceedings of Workshop on the Theory and Application of Cryptographic Techniques*, Switzerland, pp. 177-182, 1988.
- [8] Chaum D., "Secret-Ballot Receipts: True Voter-Verifiable Elections," *Security and Privacy*, vol. 2, no. 1, pp. 38-47, 2004.
- [9] Chaum D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84-90, 1981.
- [10] Gallegos C. and Shin D., "A Novel Device for Secure Home E-Voting," in *Proceedings of the Conference on Research in Adaptive and Convergent Systems*, Prague Czech Republic, pp. 321-323, 2015.
- [11] Gong L., Lia S., Mao Q., Wang D., and Dou J., "A Homomorphic Encryption Scheme with Adaptive Chosen Ciphertext Security but Without Random Oracle," *Theoretical Computer Science*, vol. 609, pp. 253-261, 2016.
- [12] Hariss K., Noura H., and Samhat A., "Fully Enhanced Homomorphic Encryption Algorithm

- of MORE Approach for Real World Applications,” *Journal of Information Security and Applications*, vol. 34, pp. 233-242, 2017.
- [13] Hirt M. and Sako K., “Efficient Receipt-Free Voting Based on Homomorphic Encryption,” in *Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques*, Belgium, pp. 539-556, 2000.
- [14] Hoffstein J., Pipher J., and Silverman J., “NTRU: A Ring-based Public Key Cryptosystem,” in *Proceedings of International Algorithmic Number Theory Symposium*, Portland, pp. 267-288, 1998.
- [15] Hwang M., Lee C., and Lai Y., “An Untraceable Blind Signature Scheme,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 86, no. 7, pp. 1902-1906, 2003.
- [16] Jin A., Ling D., and Goh A., “Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenised Random Number,” *Pattern Recognition*, vol. 37, no. 11, pp. 2245-2255, 2004.
- [17] Joaquim R. and Ribeiro C., “An Efficient and Highly Sound Voter Verification Technique and its Implementation,” in *Proceedings of International Conference on E-Voting and Identity*, Tallinn, pp. 104-121, 2011.
- [18] Juels A., Catalano D., and Jakobsson M., *Towards Trustworthy Elections*, Springer, 2005.
- [19] Kawachi A. and Koshihara T., *Quantum Computation and Information*, Springer, 2006.
- [20] Lee Y., Park S., Mambo M., Kim S., and Won D., “Towards Trustworthy E-Voting Using Paper Receipts,” *Computer Standards and Interfaces*, vol. 32, no. 5, pp. 305-311, 2010.
- [21] Lumini A. and Nanni L., “An Improved Biohashing for Human Authentication,” *Pattern Recognition*, vol. 40, no. 3, pp. 1057-1065, 2007.
- [22] Ming Y. and Wang Y., “Identity Based Broadcast Encryption with Group of Prime Order,” *The International Arab Journal of Information Technology*, vol. 13, no. 5, pp. 513-541, 2016.
- [23] Neff C., *Practical High Certainty Intent Verification For Encrypted Votes*, Citeseer, 2004.
- [24] Randell B. and Ryan P., “Voting Technologies and Trust,” *IEEE Security and Privacy*, vol. 4, no. 5, pp. 50-56, 2006.
- [25] Sadiq A., Hussein N., and Khoja S., “Proposal for Two Enhanced NTRU,” *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 5, pp. 48-51, 2014.
- [26] Shaheen S., Yousaf M., and Jalil M., “Temper Proof Data Distribution for Universal Verifiability and Accuracy in Electoral Process Using Blockchain,” in *Proceedings of the 13th International Conference on Emerging Technologies*, Islamabad, pp. 1-6, 2017.
- [27] Tian H., Zhang F., and Wei B., “A lattice-based Partially Blind Signature,” *Security and Communication Networks*, vol. 9, no. 12, pp. 1820-1828, 2016.
- [28] Wang L., Guo J., and Luo M., “A more Effective Voting Scheme Based on Blind Signature,” in *Proceedings of the International Conference on Computational Intelligence and Security*, Guangzhou, pp. 1507-1510, 2006.
- [29] Yao J., Dong Z., and Li X., “A Novel Group Signature Scheme Based on NTRU,” in *Proceedings of the 7th International Conference on Computational Intelligence and Security*, Hainan, pp. 861-864, 2011.
- [30] Zhang P., Yu J., and Liu H., “Homomorphic Signature Scheme and its Application in The Electronic Voting,” *Journal of Shenzhen University Science and Engineering*, vol. 28, pp. 489-494 2011.



Safdar Shaheen received his MS degree in Information Security from Sichuan University, China. He is currently working towards the PhD degree from Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan. He has published and presented five papers at various national/international conferences. His research interests include authentication, privacy, cryptology, multicast security, blockchain and secure electronic voting machine.



Muhammad Yousaf is working as Associate Professor in Faculty of Computing, Riphah International University (RIU), Islamabad, Pakistan. He is also serving as Academic Advisor in Riphah Institute of Systems Engineering (RISE), Islamabad. He completed his PhD in Computer Engineering in 2013 from Center for Advanced Studies in Engineering (CASE), Islamabad. His research interests include network security, network forensics, traffic analysis, mobility management, and bandwidth aggregation.



Mudassar Jalil earned his PhD degree from COMSATS Institute of Information Technology, Islamabad, Pakistan. During PhD research, he visited Heidelberg Graduate School of Mathematical and Computational Methods for the Sciences, University of Heidelberg, Germany as an ERASMUS exchange student. He has 14 international publications in well recognized journals. His research area is Fluid Mechanics and Cryptography.