IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁂ Impact Factor 7.39 ⁂ Vol. 11, Issue 9, September 2022

DOI: 10.17148/IJARCCE.2022.11901

Adopting EVS as Solution to Nigeria Election using Novel Proxy, Oblivious and Blind Signature

Olalekan Ihinkalu[1*], Sunday E. Adewumi[2], Helen O. Edogbanya[3]

Department of Computer Science, Federal University Lokoja, Kogi State, Nigeria[1,2]

Mathematics Department, Federal University Lokoja, Kogi State, Nigeria[3]

*Correspondence should be addressed to Olalekan E. Ihinkalu; olalekan.ihinkalu@fulokoja.edu.ng

Abstract: Electioneering processes can be much more convenient by the introduction of Electronic Voting Systems (EVS). However, there are some lacunas associated with EVS, for instance, if a blank vote is signed into the server before voters cast their votes, it results into multi-voting. In addition to that, if users cast their votes before signing into the server, the information of the election could have leaked out from the server and the election would have been compromised. So, we introduced Blind signatures to help prevent leakage of the election information through the server. However, hackers may try to bring in a non-candidate signature for non-legal usage at that moment or in a later time. For these issues to be addressed, this research suggests a novel work, oblivious signature scheme with proxy signature to meet security requirements that includes; message verification, information protection, and personal privacy, in order to ensure that rigging is drastically reduced between voters, candidates and the system (the server). That is why, an EVS that uses a combination of blind signature, oblivious signature and proxy signature scheme is proposed and we have also implemented this scheme electronically to show that users can vote conveniently and securely.

Keywords: Blind signature, Oblivious signature, Proxy signature, Electronic Voting System (EVS), Privacy and Security.

I. INTRODUCTION

Computer has become popular in our current world. Today, computer science and technology has taken over almost all spheres of influence of the modern man [1]. Ranging from seat reservations in airlines, train reservations, hotel reservations, medical diagnosis, to modern farming patterns all uses technological approach to proffer solutions to issues in our day to day activities [2].

Voting of leaders into position of influence is one major area of decision making globally. Election is the basic way people make their choice known [3]. Most voting is done manually; this has reduced the willingness of people to participate in the voting process because it is characterized with a lot of manipulations [4]. This manual way of voting involves counting the votes of individuals to determine how many people voted for each aspirants contesting for a particular office and then the aspirant with the major number of votes is declared the winner [4].

Another disadvantage of manual system of voting is that multiple voting is not easily detectible. The manual voting system also takes a longer time for voters to cast their votes, sometimes they are left with no choice but to cast their votes under the scorching sun or in extreme cases under the rain. But with the use of EVS, you log into the system, and you are allowed to vote [5][6].

Another pitfall associated with the manual process of electioneering is during the counting of results. When voters cast their votes, the officials overseeing the election, will open up the ballot boxes to count the votes, the process of counting takes long time and not only that, so much energy is used and the accuracy and precision cannot and will never be guaranteed. Falsification of results is associated with this manual method of counting, especially when the number of voters are much in a polling unit, region, provinces, states or nation. All of these aforementioned, causes the delay in the announcement of election results [7], but with the introduction of EVS all of these issues can be addressed.

Manual system of voting has a lot of disadvantages but a lot of people are still unwilling to embrace EVS which is void of double counting of results, rigging, ballot snatching, but it assures efficiency, security and accuracy because they are not yet ready to conduct a free and fair election [8]. Voting System (VS) has been in existence since inception of man on the planet earth. It all began with the balloting and there is need for a transformation to a paperless sphere [9].

II. RELATED WORKS

A. Advent of Voting System (VS)

At the inception of voting, election is carried out manually, whereby people go to a nearby Polling Unit (PU) to register as an eligible person to vote, in the process they will be given a Permanent Voter's Card (PVC) which contains all information necessary to allow them cast their franchise during election process, and this has some lacuna associated with it, ranging from double voting, rigging, results manipulation, and costly to manage [10].

B. Advent of Electronic Voting System (EVS)

EVS has been practiced for over three decades now. The first idea of EVS was designed as decision telegraph which was invented in 1849 by De Brettes [11]. The first man who invented electronic recorder was Thomas Edison in 1869 [11]. Where the main recorder (central) obtains signal, then list the names of members eligible to be voted for in a matrix form, using two columns with headings "Yes" or "No". while in 1886, an automated VS was also invented still by Edison [12]. Between 1840 to 1909, in a state called Victoria in the country of Australia, election was first conducted in 1856 by a ballot system, candidates' names were listed out and the election was conducted and counted manually [13].

Internet Voting (IV) in the year 2000, was introduced, and everything was approached electronically (E), E-Education, E-Commerce, E-Banking, E-Government, with the advent of internet. EVS method of voting has become widely accepted ever since then in most developed countries till date, because it proffered solution to critical problems associated with manual VS. Just to mention few developed nations that have adopted the use of EVS, we have Estonia, Switzerland, Germany, India, and United Kingdom. The first ever election that was introduced at the parliament election in Brazil using IV was conducted [14], other nations since then have tested and used IV or EVS like the city of Cologne, Germany, Finland, United State and France and many more countries.

C. Voting System as at Today in Nigeria

In Nigeria currently, what is obtainable today is Bimodal Voter Accreditation System (BVAS), BVAS is an electronic device which is built in such a way that it can read Permanent Voter Cards (PVCs) and automatically verifies the voters – using voters' fingerprints mechanism – to prove that they are authorized to perform their civic right voting in a designated polling unit [15].

With the various technology improvements by Independent National Electoral Commission (INEC) the election umpire in Nigeria, the introduction of BVAS has curbed the challenges of ballot snatching, in that if your accredited number of voters is less than the result of those who voted at a Polling Unit (PU) such results will be cancelled, and also the result from each PU are sent electronically to the server right before the eyes of the voters.

In the just concluded election, in the Osun governorship election on 16th July, 2022 [15], there were no news of ballot boxes been snatched but what was rampant was vote buying and selling.

This is the latest way of administering election in Nigeria as at 2022, however it is still prone to other manual processes, but what we are introducing in this research is to eradicate completely the use of manual way of voting whereby everything is done electronically, and we will be using the scheme proposed by Chiou's [16] with an additional security method of blind signature [17, 18].

III. METHODOLOGY

A. System Process*:* Let's assume that the database (DB), contains the list of eligible voters, and the **BB** (Bulletin Board) is restricted to be read-only by every entity.

Step One: Set-up Phase Section: All parameters are generated by the algorithm. (See (Fig. 1,7)).

Step Two: The Proxy Phase Section

Step Two (i). A which is the original signer will delegate authority to the proxy signer which is **B**,

Step Two (ii). The Proxy Signer (**B**) then publish the public key on the Bulletin Board(**BB)**. (See (Fig. 2,8)).

Step Three: The Registration Phase Section

Step Three (i). The Proxy signer (**B**), who checks whether **R,** the voter**,** is legally registered and if the condition is fulfilled, a voting certificate is issued to **R** which is the Voter.

Step Three(ii). **B**, who is the Proxy signer then send all the certificates by publishing them on **BB** which is the bulletin Board.

Step Three(iii). The Voter**, R** checks through **BB**, the bulletin Board to see whether he/she was successfully registered. (See (Fig. 3,9)).

Step Four: The Circling Phase Section: **R,** The Voter selects his/her candidate and then receives signature on it from **B**, the Proxy signer. (See (Fig. 4,10)).

Step FIVE: The Voting Phase Section

DOI: 10.17148/IJARCCE.2022.11901

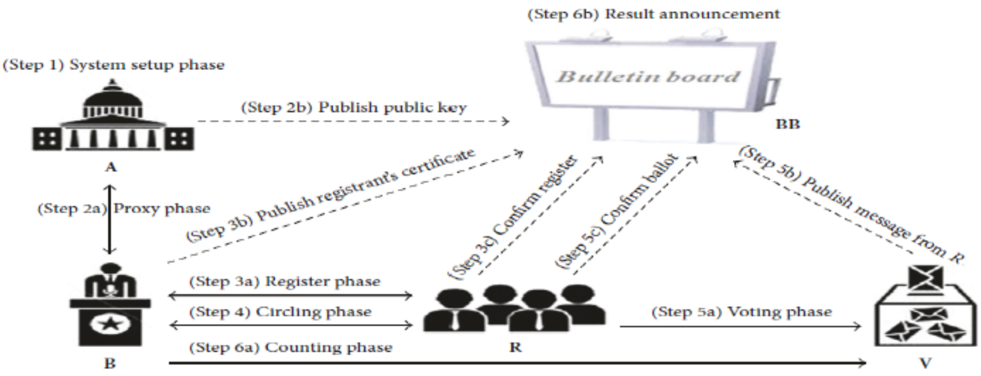

(Step 6b) Result announcement
Bulletin board
BB
(Step 1) System setup phase
(Step 2b) Publish public key
A
(Step 2a) Proxy phase
(Step 3b) Publish registrant's certificate
(Step 3c) Confirm register
(Step 5c) Confirm ballot
(Step 5b) Publish message from R
(Step 3a) Register phase
(Step 4) Circling phase
(Step 6a) Counting phase
(Step 5a) Voting phase
B
R
V

Fig. 1: System Actors and Phases

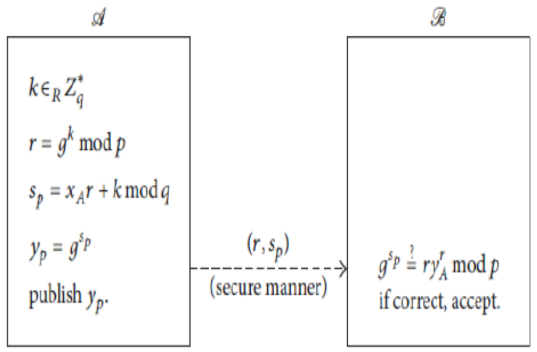


Fig. 2: Proxy Phase Segment

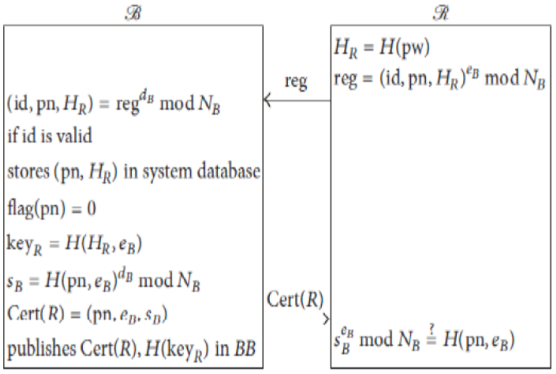

$\mathscr{B}$
$\mathscr{R}$
$H_R = H(\mathrm{pw})$
$\mathrm{reg} = (\mathrm{id}, \mathrm{pn}, H_R)^{e_B} \bmod N_B$
reg
$(\mathrm{id}, \mathrm{pn}, H_R) = \mathrm{reg}^{d_B} \bmod N_B$
if id is valid
stores (pn, H_R) in system database
$\mathrm{flag}(\mathrm{pn}) = 0$
$\mathrm{key}_R = H(H_R, e_B)$
$s_B = H(\mathrm{pn}, e_B)^{d_B} \bmod N_B$
$\mathrm{Cert}(R) = (\mathrm{pn}, e_B, s_B)$
publishes $\mathrm{Cert}(R)$, $H(\mathrm{key}_R)$ in BB
$\mathrm{Cert}(R)$
$s_B^{e_B} \bmod N_B \overset{?}{=} H(\mathrm{pn}, e_B)$

Fig. 3: Registration Phase Segment

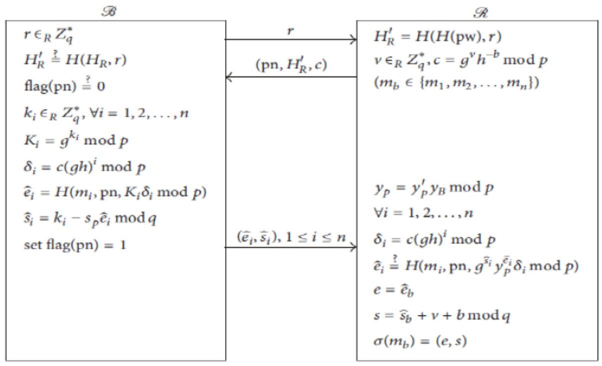

$\mathscr{B}$
$\mathscr{R}$
$r \in_R Z_q^*$
$H'_R \overset{?}{=} H(H_R, r)$
$\mathrm{flag}(\mathrm{pn}) \overset{?}{=} 0$
$k_i \in_R Z_q^*, \forall i = 1, 2, \ldots, n$
$K_i = g^{k_i} \bmod p$
$\delta_i = c(gh)^i \bmod p$
$\hat{e}_i = H(m_i, \mathrm{pn}, K_i \delta_i \bmod p)$
$\hat{s}_i = k_i - s_p \hat{e}_i \bmod q$
set $\mathrm{flag}(\mathrm{pn}) = 1$
r
(pn, H'_R, c)
$(\hat{e}_i, \hat{s}_i), 1 \le i \le n$
$H'_R = H(H(\mathrm{pw}), r)$
$v \in_R Z_q^*, c = g^v h^{-b} \bmod p$
$(m_b \in \{m_1, m_2, \ldots, m_n\})$
$y_p = y'_p y_B \bmod p$
$\forall i = 1, 2, \ldots, n$
$\delta_i = c(gh)^i \bmod p$
$\hat{e}_i \overset{?}{=} H(m_i, \mathrm{pn}, g^{\hat{s}_i} y_p^{\hat{e}_i} \delta_i \bmod p)$
$e = \hat{e}_b$
$s = \hat{s}_b + v + b \bmod q$
$\sigma(m_b) = (e, s)$

Fig. 4: Circling Phase Segment

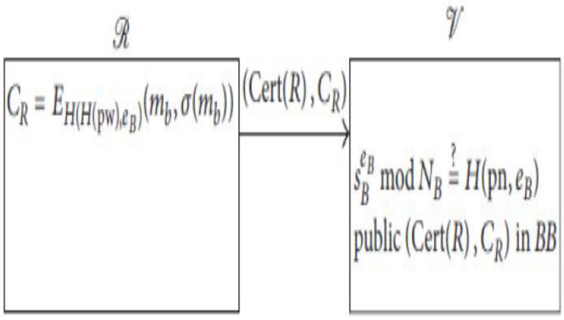

$\mathscr{R}$
$\mathscr{V}$
$C_R = E_{H(H(\mathrm{pw}), e_B)}(m_b, \sigma(m_b))$
$(\mathrm{Cert}(R), C_R)$
$s_B^{e_B} \bmod N_B \overset{?}{=} H(\mathrm{pn}, e_B)$
public $(\mathrm{Cert}(R), C_R)$ in BB

Fig. 5: Voting Phase Segment

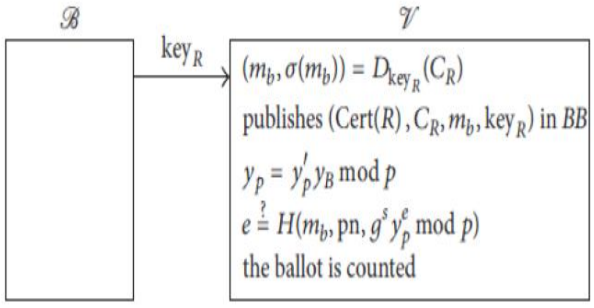

$\mathscr{B}$
$\mathscr{V}$
key_R
$(m_b, \sigma(m_b)) = D_{\mathrm{key}_R}(C_R)$
publishes $(\mathrm{Cert}(R), C_R, m_b, \mathrm{key}_R)$ in BB
$y_p = y'_p y_B \bmod p$
$e \overset{?}{=} H(m_b, \mathrm{pn}, g^s y_p^e \bmod p)$
the ballot is counted

Fig. 6: Counting Phase Segment

Step Five (i). R which is the Voter, then casts his vote by sends it to **V**, which is the voting center which is represented as **V**.

Step Five (ii). The Voting center, **V** instantly publishes the message of the vote casted by the Voter, **R** on the Bulletin Board**, BB**.
Step Five (iii). **R**, the voter, confirms the ballot received by **V**, the Vote center else R, the Voter can re-send his/her ballot. (See (Fig. 5,11)).
Step Six: Counting Phase Section
Step Six(i). When the stipulated time for voting is over, **B**, the Proxy Signer forwards the key that converts encrypted message or coded message back to plain text to the Vote Center, **V**, and then **V**, the vote center verifies and counts all votes.
Step Six(ii). The vote center, **V** publishes results of the votes to the Bulletin Board **BB**, where every voter, **R** can verify and count all the votes. (See (Fig. 6,12)).

B. EVS description [16]

1. Set-up phase Segment

1.1. Two large primes, p, q such that $q|(p-1)$ are picked, e.g., $p = 11, q = 5$. They are published on BB.
1.2. Two numbers $g, h \in Z_p^* = \{1, ., p-1\}$ such that $\mathrm{Ord}_p g = \mathrm{Ord}_p h = q$ are selected, e.g., $h = 5, g = 9$. They are published.
1.3. The creator [A], selects randomly its secret key, $x_A \in Z_q^*$, and calculates its public key, $y_A = g^{x_A} \bmod p$, e.g., $x_A = 2, y_A = 4$, and y_A is published.
1.4. The proxy creator, [B], selects randomly its secret key, $x_B \in Z_q^*$, and calculates its public key, $y_B = g^{x_B} \bmod p$, e.g., $x_B = 4, y_B = 5$, and y_B is published.
1.5. [B] chooses two secret large primes, $p_B \neq q_B$, e.g., $p_B = 11,\ q_B = 5$, they are not equal
1.6. [B] computes $N_B = p_B \cdot q_B,\ \ N_B = 55$.
1.7. [B] computes Euler's totient function, $\varphi(N_B) = (p_B - 1)(q_B - 1)$, $\varphi(N_B) = 40$.
1.8. [B] selects, e_B such that $\gcd\left(e_B,\ \varphi(N_B)\right) = 1$, $e_B = 3$. RSA public key of B, (e_B, N_B), is published.
1.9. [B] calculates $d_B = e_B^{-1} \bmod \varphi(N_B)$, e.g., $d_B = 27$, which may be calculated using Extended Euclidean Algorithm [5]. B's RSA secret private key is (d_B, N_B) = (27,40).

2. Proxy phase Segment

2.1. Creator, [A], randomly chooses $k \in Z_q^*$ and computes $r_A = g^k \bmod p, s_A = x_A \cdot r_A + k \bmod q$, and $y_p' = g^{s_A} \bmod p$, i.e, $k = 3, r_A = 3, s_A = 4, y_p' = 3$.
2.2. [A], RSA encrypts the pair, (r_A, s_A) , using [B]'s public key, (e_B, N_B), forwards the encrypted pair to [B], and publishes y_p'.
2.3. Proxy creator,[B], decrypts (r_A, s_A) using its private key, (d_B, N_B), and checks whether $g^{s_A} = r_A \cdot y_A^{r_A} \bmod p$ holds, e.g., $g^{s_A} \bmod p = 5, r_A \cdot y_A^{r_A} \bmod p = 5$. If they are equal, [B] accepts the proxy, and then calculates $s_p = s_A + x_B$ as proxy signature, e.g., $s_p = 4 + 4 \bmod 5 = 3$.
2.4. [B] generates RSA signature, $s_{A,B} = H(g^{s_A} \bmod p)^{d_B} \bmod N_B$, and forwards it to [A].
2.5. [A] checks whether $s_{A,B}^{e_B} = H\left(y_p'\right) \bmod N_B$ holds, if so, [A] approves the further work.

3. Register phase Segment

3.1. R, who is the voter, chooses pseudo name (pn), and also password (pw), calculates $H_R = H(pw)$, encrypts $(id, pn, H(pw))$ utilizing (e_B, N_B), sends results to [B], the proxy signer.
3.2. Proxy creator, [B] decrypts $(id, pn, H(pw))$ utilizing (d_B, N_B), and confirms whether the voter [R] is eligible. If so, [B], the proxy signer saves (pn, H_R) to the system **DB,** which is the database, sets $\mathrm{flag}(pn) = 0$, calculates $\mathrm{key}_R = H(H_R, e_B)$, $s_B = H(pn, e_B))^{d_B} \bmod N_B$, will return $\mathrm{Cert}(R)$ to the voter [R], and then publishes $\mathrm{Cert}(R)$ to, the bulletin board **(BB)**, so that $\mathrm{Cert}(R) = (pn, e_B, s_B)$.
3.3. The Voter [R], verifies RSA signature, to see if $s_B^{e_B} = H(pn, e_B) \bmod N_B$ is equal. If so, the voter [R] can vote.

4. Circling phase Segment

4.1. [B], the Proxy creator sends random number, $r \in Z_q^*$, to [R], the voter after accepting a login request from R.
4.2. Voter [R] computes $H_R^{'} = H(H(pw), r)$, picks a random number, $v \in Z_q^*$, calculates $c = g^v h^{-b} \bmod p, m_b \in \{m_1, .., m_n\}$, where $\{m_1, .., m_n\}$ is a list of n candidates available for R from the bulletin board, BB, and b is the number of the candidate of [R]'s choice, which is hidden in c using random v, and forwards $(pn, H_R^{'}, c)$ to B.
4.3. The Proxy creator [B] checks whether $H_R^{'} = H(H_R, r)$ is equal. If so, [B] the proxy signature examines whether $\mathrm{flag}(pn) = 0$ holds. If it holds, [B] chooses $k_i \in Z_q^*$ randomly, mathematically solves $K_i = g^{k_i} \bmod p, \delta_i =$

$c(g\cdot h)^i \bmod p, \widehat{e_i} = H(m_i, pn, K_i\delta_i \bmod p)$, and $\widehat{s_i} = k_i - s_p\widehat{e_i} \bmod q, i = 1,..,n$, returns $(\widehat{e_i}, \widehat{s_i}), i = 1,..,n$, to R (these are blindly signed by proxy all candidates including the one selected by [R], and sets $\text{flag}(pn) = 1$.

4.4. Voter [R] computes $y_p = y'_p \cdot y_B \bmod p$, and, for every $i = 1,..,n$, R calculates $\delta_i = c(g\cdot h)^i \bmod p$ and checks whether $\widehat{e_i} = H(m_i, pn, g^{\widehat{s_i}} y_p^{\widehat{e_i}} \delta_i \bmod p)$ is correct. Thus, Voter [R] checks correctness of the candidates list including [R]'s choice blindly signed by [B]. If it is correct, [R] computes $s = \widehat{s_b} + v + b \bmod q$, and sets $e = \widehat{e_b}$. The final oblivious signature of [R] is $\sigma(m_b) = (e, s)$.

5. Voting phase Segment

5.1. The Voter [R] computes $H(H(pw), e_B)$ and uses the result as symmetric key to encrypt $(m_b, \sigma(m_b))$, which produces a cipher text, C_R, then sends $(\text{Cert}(R),\ C_R)$ to the voting center [V**]**.

5.2. Voting center [V] first checks whether $s_B^{e_B} = H(pn, e_B) \bmod N_B$ are equivalent. If yes, the Vote center[V] publishes [R]'s ballot, $(\text{Cert}(R),\ C_R)$, to [BB] the bulletin board.

5.3. Every voter, [R], can check whether his/her ballot is received by [V] via the bulletin board, [BB]. If it is not published, then [R] resends the ballot to [V].

6. Counting phase Segment

6.1. Proxy creator [B] forwards to the voting center, [V], $\text{key}_R = H(H_R, e_B)$

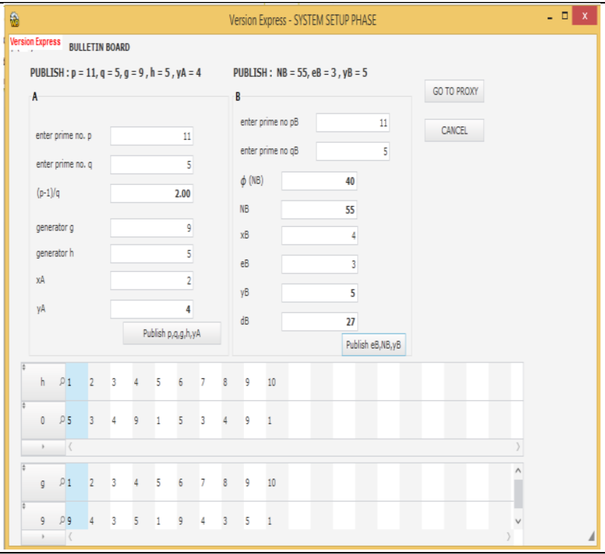
6.2. [V] , the Voting center decrypts C_R by the use of symmetric key, key_R, and publishes $(\text{Cert}(R),\ C_R,\ m_b,\ \text{key}_R)$ to [BB], which is the bulletin board, and computes $y_p = y'_p \cdot y_B \bmod p$, and checks whether $e = H\big(m_b, pn, g^s y_p^e \bmod p\big)$ result is equal. If the result is yes, the signature will be accepted, and the ballot result is counted.

6.3. The Voting center [V], publishes the result of the election. Everyone can count and verify the ballots results through [BB], the bulletin board.

End of the EVS [16] description.

IV. EXPECTED RESULT

This section shows the deployment of the application of an anonymous EVS with proxy signer implemented on a computer system. The system assumes that any signer who places request to get his/her public key will be receiving the public key immediately. The system steps are slated as follows for the implemented and for the tested system:



PUBLISH : p = 11, q = 5, g = 9 , h = 5 , yA = 4

PUBLISH : NB = 55, eB = 3 , yB = 5

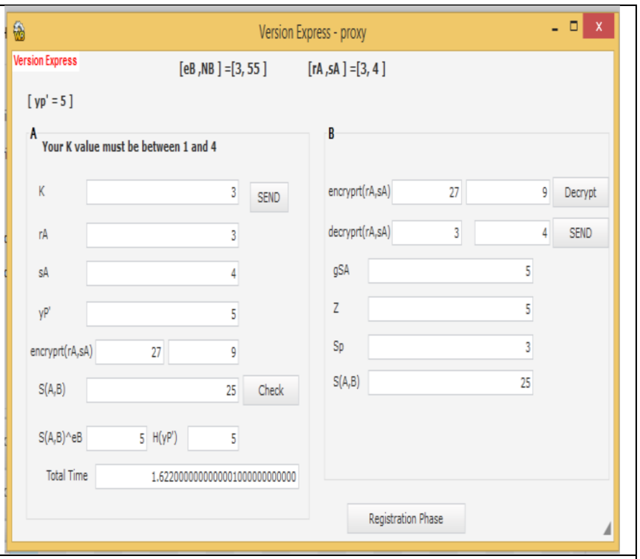
enter prime no. p	11
enter prime no. q	5
(p-1)/q	2.00
generator g	9
generator h	5
xA	2
yA	4

enter prime no pB	11
enter prime no qB	5
ϕ (NB)	40
NB	55
xB	4
eB	3
yB	5
dB	27

h	1	2	3	4	5	6	7	8	9	10
0	5	3	4	9	1	5	3	4	9	1

g	1	2	3	4	5	6	7	8	9	10
9	9	4	3	5	1	9	4	3	5	1

Fig. 7: System Set-up Phase Segment



[eB ,NB] =[3, 55]

[rA ,sA] =[3, 4]

[yp' = 5]

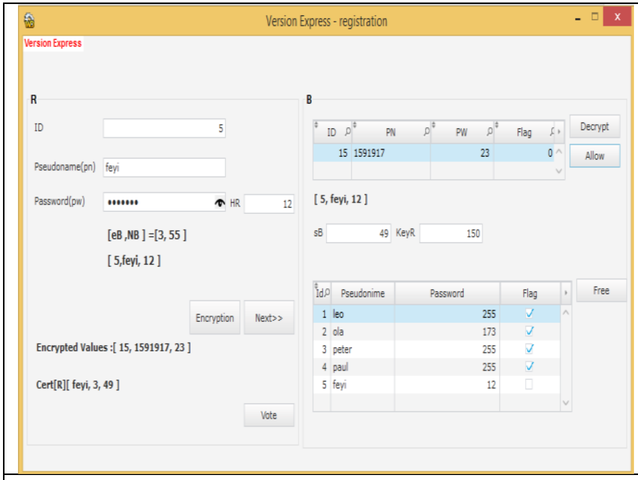
Your K value must be between 1 and 4

K	3	
rA	3	
sA	4	
yP'	5	
encryprt(rA,sA)	27	9
S(A,B)	25	
S(A,B)^eB	5	
H(yP')	5	
Total Time	1.6220000000000001000000000000	

encryprt(rA,sA)	27	9
decryprt(rA,sA)	3	4
gSA	5	
Z	5	
Sp	3	
S(A,B)	25	

Fig. 8: Proxy Phase Segment

DOI: 10.17148/IJARCCE.2022.11901



ID: 5

Pseudoname(pn): feyi

Password(pw): ••••••• HR: 12

[eB ,NB] =[3, 55]

[5,feyi, 12]

Encrypted Values :[15, 1591917, 23]

Cert[R][feyi, 3, 49]

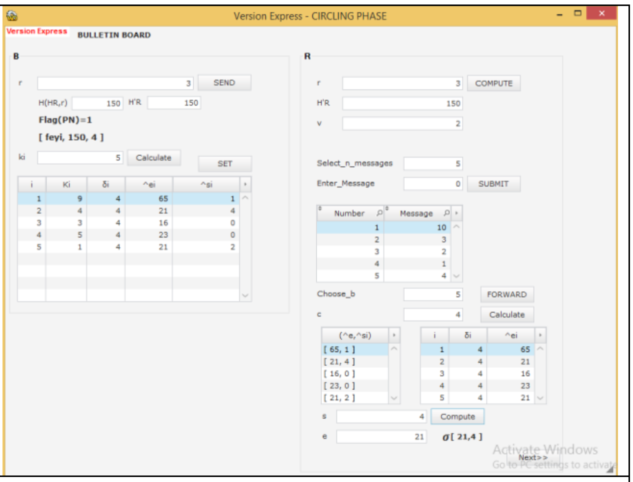
ID	PN	PW	Flag
15	1591917	23	0

[5, feyi, 12]

sB: 49 KeyR: 150

Id	Pseudonime	Password	Flag
1	leo	255	✓
2	ola	173	✓
3	peter	255	✓
4	paul	255	✓
5	feyi	12	□

Fig. 9: Registration Phase Segment



r: 3

H(HR,r): 150 H'R: 150

Flag(PN)=1

[feyi, 150, 4]

ki: 5

i	Ki	δi	^ei	^si
1	9	4	65	1
2	4	4	21	4
3	3	4	16	0
4	5	4	23	0
5	1	4	21	2

r: 3

H'R: 150

v: 2

Select_n_messages: 5

Enter_Message: 0

Number	Message
1	10
2	3
3	2
4	1
5	4

Choose_b: 5

c: 4

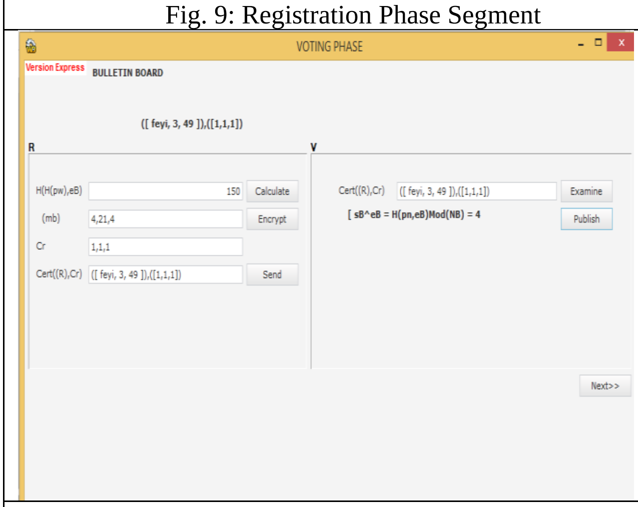
(^e,^si)
[65, 1]
[21, 4]
[16, 0]
[23, 0]
[21, 2]

i	δi	^ei
1	4	65
2	4	21
3	4	16
4	4	23
5	4	21

s: 4

e: 21 σ[21,4]

Fig. 10: Circling Phase Segment



([feyi, 3, 49]),([1,1,1])

H(H(pw),eB): 150

(mb): 4,21,4

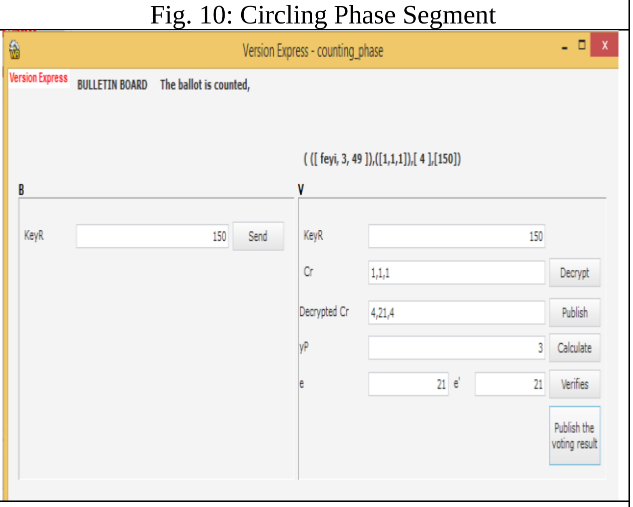
Cr: 1,1,1

Cert((R),Cr): ([feyi, 3, 49]),([1,1,1])

Cert((R),Cr): ([feyi, 3, 49]),([1,1,1])

[sB^eB = H(pn,eB)Mod(NB) = 4

Fig. 11: Voting Phase Segment



The ballot is counted,

(([feyi, 3, 49]),([1,1,1]),[4],[150])

KeyR: 150

KeyR: 150

Cr: 1,1,1

Decrypted Cr: 4,21,4

yP: 3

e: 21 e': 21

Fig. 12: Counting Phase Segment

Step one (1): On the main page the implemented system and the tested system (Fig. 7,13(a)) respectively, users can log-on to select their role and to enter a pseudo-name (Fig. 7, 13(b)) respectively. The original signer initiates the process and then wait for **B**, the proxy signers (Fig. 7, 13(c)) respectively.

Step two (2): Proxy signer executes Step one (1) and makes a choice of a detected original signer to request a delegation (Fig. 8, 13(d)) respectively.

Step three (3): Then the original signer chooses the proxy signer on the available list to begin the process delegation (Fig. 8, 13(e)) respectively.

Step four (4): **A** check for the correctness of the delegation is made, **B** sets the voting parameters (Fig. 8, 13(f)) respectively, and waits for verifier (Fig. 8, 13(g)) respectively.

Step five (5): The verifier executes Step one (1) and awaits the proxy signer to send him/her the event of the voting (Fig. 9, 13(h)).

Step six (6): The proxy signer selects a verifier to send the event of voting (Fig. 9, 13 (i)) respectively, and starts holding the event (Fig. 10, 13(j)) respectively.

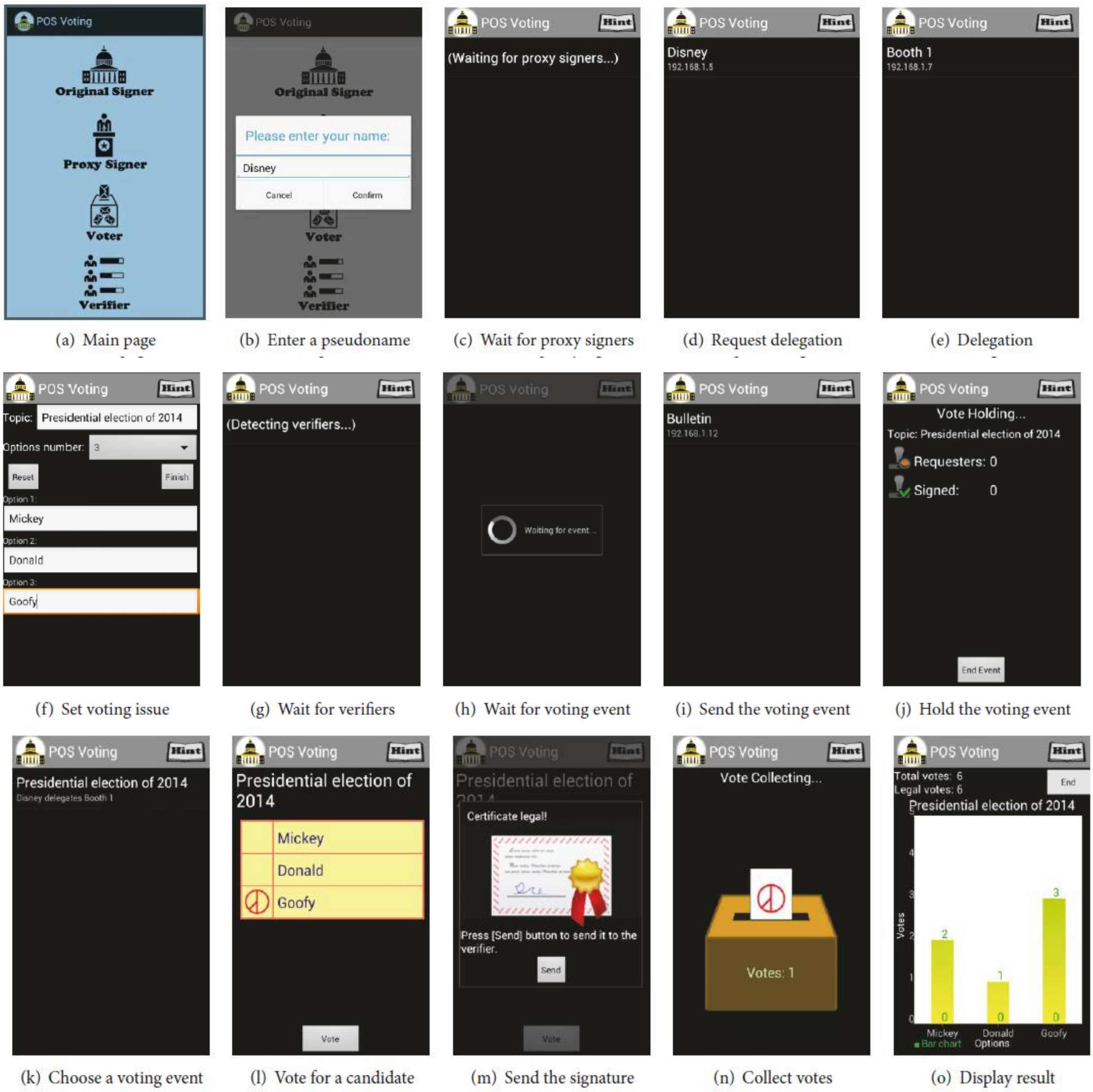
Step seven (7): The receiver chooses the "Voter" on the index page and selects a detected event of voting (Fig. 10, 13(k)) respectively.

Step eight (8): The Voter selects a candidate of his/her choice and clicks on the button captioned "Vote" (Fig. 11, 13(l)) respectively, to send blinded casted vote to **B**, the proxy signer. He/she then receives proxy oblivious signature and sends the withdrawn signature to the verifier by pressing the button captioned "Send". See (Fig. 11, 13(m)) respectively.

Step nine (9): Votes keeps coming to The verifier (Fig. 12, 13(n)) respectively, until the time stipulate for the election to end and this is done by the proxy signer who clicks on the button captioned "End Event". See (Fig. 12, 13(j)) respectively.

Step ten (10): At the end of the voting, the verifier quickly verifies all votes collected and automatically projects the result (Fig. 12, 13(o)) respectively.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 9, September 2022
DOI: 10.17148/IJARCCE.2022.11901



(a) Main page (b) Enter a pseudoname (c) Wait for proxy signers (d) Request delegation (e) Delegation

(f) Set voting issue (g) Wait for verifiers (h) Wait for voting event (i) Send the voting event (j) Hold the voting event

(k) Choose a voting event (l) Vote for a candidate (m) Send the signature (n) Collect votes (o) Display result

Fig. 13: Implemented EVS using Proxy, Oblivious and Blind Signature

V. CONCLUSION

This work proposes the combine advantages of using an oblivious signature and proxy signature combined with blind signature to make election process more robust that satisfies the security requirements which gives us an advantage of ambiguity, unforgeability, undeniability, unlinkability, distinguishability, verifiability and completeness in electioneering.These schemes perform well in terms usability and complexity. Finally, it is implemented on computer system to prove its ability and the results are amazing.

REFERENCES

[1] PWC. 2015 Information Security Breaches Survey; Technical Report; PWC: London, UK, 2015.
[2] M. Morris, Mano (1993). Computer System Architecture (4th edition). Prentice Hall of India.
[3] R. Joaquin, P. Ferreira & C. Riberio, "EVIV: An End-to-End Verifiable Internet Voting System," Journal of Computer and Security, vol. 32, pp. 170-191, 2013.
[4] V. Mateu, F. Sebe, and M. Valls, "Constructing Credential-Based E-Voting Systems from Offline E-Coin Protocols," Journal of Network and Computer Applications, vol. 42, pp. 39-44, 2014.

DOI: 10.17148/IJARCCE.2022.11901

[5] D. DeSilver. U.S. voter turnout trails most developed countries. *Fact Tank Blog*, Pew Research Center. August 2, 2016.

[6]B.C. Burden et al. Election laws, mobilization, and turnout: The unanticipated consequences of election reform. *American Journal of Political Science*. September 9, 2013. doi: 10.1111/ajps.12063.

[7] V. Mateu, F. Sebe, and M. Valls, "Constructing Credential-Based E-Voting Systems from Offline E-Coin Protocols," Journal of Network and Computer Applications, vol. 42, pp. 39-44, 2014.

[8] J. Ben-Nun et al, "A New Implementation of a Dual (Paper and Cryptographic) Voting System," in 5th International Conference on Electronics Voting (EVOTE 2012), pp.315-329, Lochau/Bregenz, Austria, 2012.

[9] M. Mesbahuddin Sarker, Tajim Md. Niamat Ullah Akhund (2016). The Roadmap to the Electronic Voting System Development: A Literature Review. International Journal of Advanced Engineering, Management and Science (ISSN: 2454-1311),2(5), 492-497.

[10] P. Atiya, H. Sobia, and S. Saoud "Scope and Limitation Of Electronic Voting System"Ijcsmc, Vol. 2, Issue. 5, May 2013, Pg.123 – 128.

[11] T. A. Edison (2008): "Improvement in Electrographic Vote-Recorder," U.S. Patent 90,646, June 1, 1869 [http://edison.rutgers.edu/patents/00090646.PDF], accessed February 4, 2008.

[12] "Vote Recorder (2008):" The Edison Papers [http://edison.rutgers.edu/vote.htm], accessed February 4, 2008.

[13] M. Bellis (1889): "The History of Voting Machines," inventors.about.com, Nov. 13, 2000

[14] L. F. Cranor (2003): "In Search of the Perfect Voting Technology: No Easy Answers," in Secure Electronic Voting, D. Gritzalis, ed., 2003 International Journal of Advanced Engineering, Management and Science (IJAEMS) [Vol-2, Issue-5, May- 2016] Infogain Publication (Infogainpublication.com) ISSN: 2454-1311

[15] "Election in Nigeria". [Online]. Available:https://en.wikipedia.org/wiki/Elections_in_Nigeria [Accessed 25 07 2022].

[16] Chiou et al, "Design and Implementation of a Mobile Voting System Using a Novel Oblivious and Proxy Signature", Security and Communication Networks vol.2017, article Id 30752210, 16 pages, 2017

[17] Y. Baseri et al., "Double Voter Perceptible Blind Signature Based Electronic Voting Protocol" The ISC Int'l Journal of Information Security (ISeCurei), Vol-3 Issues 1, January 2011], pg. 1-8. http://www.isecure-journal.org

[18] O. Ihinkalu, A. G Chefranov. "Analysis, Design and Implementation of a Voting System Using a Novel Oblivious and Proxy Signature", EMU Institutional Repository, Vol. 7, 2019, pages 1-9. http://irep.emu.edu.tr:8080/jspui/bitstream/11129/5005/1/Ebenezerolalekan.pdf