International Journal of Engineering & Technology, 4 (2) (2015) 327-341
www.sciencepubco.com/index.php/IJET

doi: 10.14419/ijet.v4i2.4441
Research paper

Secured Transparent Computerized Voting System performance measurements

Enas Elbarbary [1]*, Ghada Abdelhady [2], Hussam Elbehiery [2], Abdelhahim Zekry [3]

[1] *VACSERA, Department of Electrical Engineering, EGYPT*
[2] *Culture & Science City, Higher Institute of Computer Science & Information Systems, EGYPT*
[3] *Ain Shams University, Faculty of Engineering, EGYPT*
**Corresponding author E-mail: enas_elbarbary@yahoo.com*

Abstract

In this paper, a multipurpose Secured Transparent Computerized Voting System (STCVS) is proposed. STCVS introduces an improvement methodology to the regular election systems. It could handle electronic ballots with multiple scopes at the same time, e.g., presidential, parliamentary, local, amongst others. STCVS's design warrants well-secured identification and authentication processes for the voter via using voter's digital signatures, certificates. Also, it guarantees voting data protection via encryption. Tallying of the voting counts is achieved automatically; candidates recorded percentages are displayed as charts for the supervision trusted parties. STCVS eliminates counting errors, voting duplication, and vote attack raised in paper-based elections systems. Voting transparency is achieved through the election process steps to assure voting credibility. This is confirmed by a feedback e-mail that the voter receives after finalizing the voting process. In addition, the proposed system saves the huge budget required for authentication devices, Electronic Voting Machines (EVM) that consist similar voting systems. To evaluate the robustness and reliability of the proposed system, performance measurements were achieved by applying the Avalanche Effect (AE) tests. Results of these measurements show the degree of security and the performance of the proposed system.

Keywords: *Asymmetric Encryption; Certificates; Cryptanalysis; Cryptography; DS; Elgamal; EVM; Javascript; Mysql; PHP; SHA-1; STCVS.*

1. Introduction

The worldwide revolution in computer and telecommunication technologies and the underlying infrastructures makes the online voting or E-Voting (Electronic Voting) no longer a North American or Western phenomenon [1] [2].
This ballot casting technology was extended far beyond the United States, spreading throughout the entire world. E-Voting, along with its benefits and drawbacks, can now be extended from the developed countries of Europe to the developing countries of Asia and South America. Besides reliable E-Voting technologies, there is a necessity for international standards to govern the technology, the software reliability and accuracy, the processes and algorithms applied within the technology, and the evaluation of all hardware, software and protocols involved. Such standards will ultimately allow elections to progress around the world without the need for monitoring parties [3].
Remote E-voting [4], where the voter can vote from everywhere, guarantees both participation high rates in the elections and the user's satisfaction as it assures an easier voting process and saves the voting procedure's time. However, remote E-Voting system suffers from some security vulnerabilities that should be taken into consideration while designing such a system. Those vulnerabilities include harder user authentication, voting duplication, and vote attack.
In addition to authentication, a perfectly designed voting system should use data encryption to protect lawful users from wire-tapping and impersonation and apply data masking to assure granularity of data access [5]. This concept is applied to find the STCVS [6] performance measurements as will be introduced in this paper.
The proposed system covers the basic security services, i.e. the confidentiality, the integrity, the authentication, and the non-repudiation [7] [8] [9].

AE refers to a cryptography desirable property to evaluate cryptographic algorithms, typically block ciphers and cryptographic hash functions. AE testing covers both Linear and Differential Cryptanalysis. AE is used as a main measurement for the performance of the proposed voting system (STCVS).
STCVS is an approach for implementing computerized voting system in a secured, verifiable manner via the Internet [10] [11]. The reliability of the introduced voting system against attacks is an important aspect to be considered. To eliminate the risk of attacks, voting data is encrypted from the client-side and along all channels [12] [13] [14].
This is achieved by combining Elgamal cryptography algorithm, data masking, hash-based data structures, and Elgamal Digital Signature (Elgamal DS) algorithm. The main goal is to achieve voting data encryption and voters authentication. Furthermore, certificates are applied for the proposed system.
Voters can get verifying their own vote by receiving a feedback from the proposed computerized voting system. Feedback is an acknowledgement e-mail sent to the voter as being registered. It consists of the voting data, i.e. the candidates numbers selected by the voter.
Recent electronic voting systems require the presence of a huge number of electronic voting machines. This would definitely increase the voting system cost [15] [16] [17] [18] [19] [20]. Using special EVM costing huge budget is not required for the proposed system. Furthermore, the required budget for biometrics devices needed for some E-Voting systems [3] [21] is not needed here since authentication is achieved via digital signatures.
Finally, the proposed system (STCVS) ensures automatic real-time votes counting, so votes tallying is achieved easily.
This paper is organized such that section 2 represents the Suggested cryptographic algorithms for Encryption, and Authentication, as well as the performance measurements. Section 3 describes the proposed STCVS, while section 4 discusses the STCVS performance measurements. Finally, the paper is concluded in section 5.

2. Suggested cryptographic algorithms & performance measurements

The suggested cryptographic algorithms used to implement the proposed work include: Firstly, Elgamal Encryption scheme used to encrypt and decrypt the voting data, i.e. the selected candidates numbers [6]. Secondly, Elgamal DS scheme, certificates are used to sign and verify the public keys, and voters pass-codes, thus providing voters authentication. Finally, SHA-1 algorithm is used to get the hash function for the voters pass-codes to save it securely in the proposed STCVS database and to protect it from being hacked on the accessed voting channel. Furthermore, the performance measurements used to verify the degree of security for the proposed system, i.e. the data masking and the AE will be described.

2.1. Elgamal Digital Signature scheme

Digital signatures are essentially used as cryptographic tools that are highly extended today. Applications for digital signatures vary from digital certificates for secure e-commerce to legal signing of contracts to secure software updates. In addition, key establishment over insecure channels, they have also great importance for public-key cryptography [9].
DS purpose is to provide a means for a party to express its identity to a piece of information. The signing process is achieved by transforming the message, and some secret information used as identification for this party into a tag called a signature, similarly to a signature on a paper document [7] [8].
DS is a cryptographic primitive which is fundamental in authentication, authorization, and non-repudiation. They assure both integrity and authentication, in general, encryption alone provides neither [8] [22].
It is impossible to amend the message without access to the recipient's private key, so the message is authenticated both in terms of source and in terms of data integrity [7] [23].
Digital Signatures are used for both Voter ID (Pass-code), and Voter Public Key, where each one is almost (25 bits) length. Signing, i.e. digital signatures generation is achieved at "Server side" via (PHP) code. Both digital signatures are verified as authentication "Certificate Verification" on the "Client-side" via (JavaScript) code before allowing the voter to access the Voting Form webpage via the STCVS website as will be described in details in sub-section 3.3. Elgamal DS is the algorithm used for Certificate DS.
Elgamal signature scheme, which was published in 1985, is based on the difficulty of computing discrete logarithms, the algorithm phases are summarized in the following sections [7] [8] [9] [24]:

- Setup (Key Generation):

A large prime number (p), a primitive element (α) are chosen. Equation (1) illustrates the public key computation having the private key $d \in \{2, 3 \ldots p-2\}$ used as random integer:

$$\beta = \alpha^d \bmod p \quad (1)$$

Where: β = Public Key

- Signature Generation:

(β, K_E) are two public keys for each message. A random integer is used as ephemeral key $K_E \in \{0, 1, 2 \ldots p-2\}$ such that the greatest common divisor gcd (K_E, p-1) =1.
Equations (2), (3) summarize the steps to compute the signature parameters (r, s):

$$r = \alpha^{KE} \bmod p \quad (2)$$

$$s = (x - d.r)\,(K_E^{-1} - 1) \bmod (p - 1) \quad (3)$$

Where: X = Plain Text (Decrypted) Message
K_E^{-1} = Ephemeral Key Multiplicative Inverse
The signature consists of the pair (r, s). Both have roughly the same bit length as (p).

- Signature Verification

Equations (4), (5) illustrate how a parameter (t) is computed then used to check whether the computed signature is valid or invalid:

$$t = \beta^r . r^s \bmod p \quad (4)$$

$$t = \alpha^x \bmod p \quad (5)$$

If equation (5) is fulfilled, so a signature is valid, otherwise signature is invalid.

2.1.1. Elgamal Digital Signature scheme attacks

Elgamal Digital Signature scheme attacks are summarized as follows:
1) Reuse of Ephemeral Key
The attacker can generate a fake message, say, "Please transfer 1000 Euros into Oscar account". He could behave as the sender, could use random (K_E), and generate (s) by simply applying the scheme [9].
The same Ephemeral Key (K_E) should not be reused. This is eliminated using the proposed system (STCVS) by using randomly generated Ephemeral Key (K_E). Hence, this attack is not working for STCVS.
2) Existential Forgery Attack
The attacker can generate a signature that looks like a valid signature to the recipient, but cannot control the message. To overcome this attack, certificates as described in the following section should be used [9]. This is achieved for the proposed system (STCVS).

2.2. Certificates application for STCVS

Public Keys authentications are essential for all asymmetric protocols, e.g., by applying certificates. Otherwise man-in-the-middle attacks are possible. Certification is a means for a trusted third party (TTP) to bind the identity of a user to a public key.
MITM (Man in the Middle) attack works against all Public Key (PK) schemes. The attacker (Oscar) shares a session key with the sender (Alice) and another one with the recipient (Bob). However, Alice and Bob still think that they are talking to each other. Oscar has now full control over the communication between Alice and Bob.
The problem here is that the public keys are not authenticated, so, identification for the sender (Alice) for example, should be used. (ID_A) is used to indicate (A) is Alice's Public Key. (ID_A) is accompanied with (A), it could be e-mail, name, address, employee no… etc. It is an identifying information [8] [9].
Using standard digital signature, this attack could also run. Public key is sent over the channel, is replaced by Oscar, who puts his verification key. So, Oscar can replace the public key with his own one in every asymmetric protocol (Elgamal, RSA, EC, DH… etc.). This powerful, universal attack takes only "10 minutes". So, Certificates are used as countermeasures. The idea is to use a crypto "tool" that provides authentication, such as:
1) Using DS.
2) Using Message Authentication Codes (MAC).
The first method is the efficient one, since MAC is based on using symmetric cryptography. A need to protect asymmetric schemes without having the problems of key exchange should be considered. DS is the way to prevent MITM attack [8] [9].
For the proposed system (STCVS), digital signatures are computed and verified for both the public key, and the pass-code thus providing voter's authentication.
The problem here is that DS is based on PK, and attack works against any PK scheme. As DS is needed to repair other PK schemes, this conflict could be solved by using a Centrally Trusted Authority: Certificate Authority (CA) "As Key Distribution Center (KDC) for symmetric schemes" [7] [8] [9].
For the proposed system (STCVS), the Higher Committee of Elections, and the Human Rights Association represent the CA. The message to be signed "elector no." is too short (6 bits as plain text, so it is max. 50 bits as cipher text).
"Invalid Certificate. Unsecured Channel. Please use another device for voting" are the alert messages shown on the web browser when either the digital signature for the public key or the voter's pass-code is not verified, so voting procedure could not be achieved. Otherwise, "Valid Certificate" alert message is shown on the web browser and voting form is accessed for the voter to achieve his voting procedure by selecting the candidates' numbers.

2.3. Data masking

Data masking is applied to obscure specific data elements within data stores. The objective is to hide sensitive user's information, so it could not be accessed outside of the authorized environment. It replaces these data elements with a similar-looking fake data. Data masking is used to generate a realistic data set for development, testing and user training purposes. This is a one-way irreversible transformation similar to a one-way cipher.
Data masking does not apply encryption, thus no decryption key is used. Best ciphers can be cracked (may be in million years using recent technologies), while masked data cannot be unmasked. Resulting masked data set does not contain any references to the original data. That makes it absolutely useless for the attackers [5].

2.3.1. Avalanche Effect

AE refers to a cryptography desirable property to evaluate cryptographic algorithms, typically block ciphers and cryptographic hash functions. Good AE is obviously attained if when an input is changed slightly (for example, by flipping a single bit), the output changes significantly (e.g., half the output bits flip). In the case of well-designed cryptographic systems based on block ciphers, such a small change in either the key or the plaintext should cause a great change in the cipher text.
Data protection from attacker hacking is ensured by reaching intermediate probabilities for the AE. A null probability of change of output bits means that the hash output does not change when the input tested pattern has a single bit flipped. Similarity, a very high probability of change of output means that the bit is bound to reverse upon flipping one bit in the input [25].
The Strict Avalanche Criterion (SAC) is a generalization of the Avalanche Effect. It is fulfilled if, whenever a single input bit is complemented, each of the output bits is flipped with a "50%" probability. This concludes that the designed system has a good AE [25] [26] [27].
Avalanche characteristics studies are essential to ensure that a cipher is not vulnerable to statistical attacks. The strength of system avalanche characteristics may evaluate the randomness of the ciphertext [27] [28].
If a block cipher or cryptographic hash function does not reveal the desired AE, then it has poor randomization, hence a cryptanalyst can predict the input knowing only the output. This may lead to partially or completely break the algorithm [27].

3. STCVS

3.1. STCVS methodology

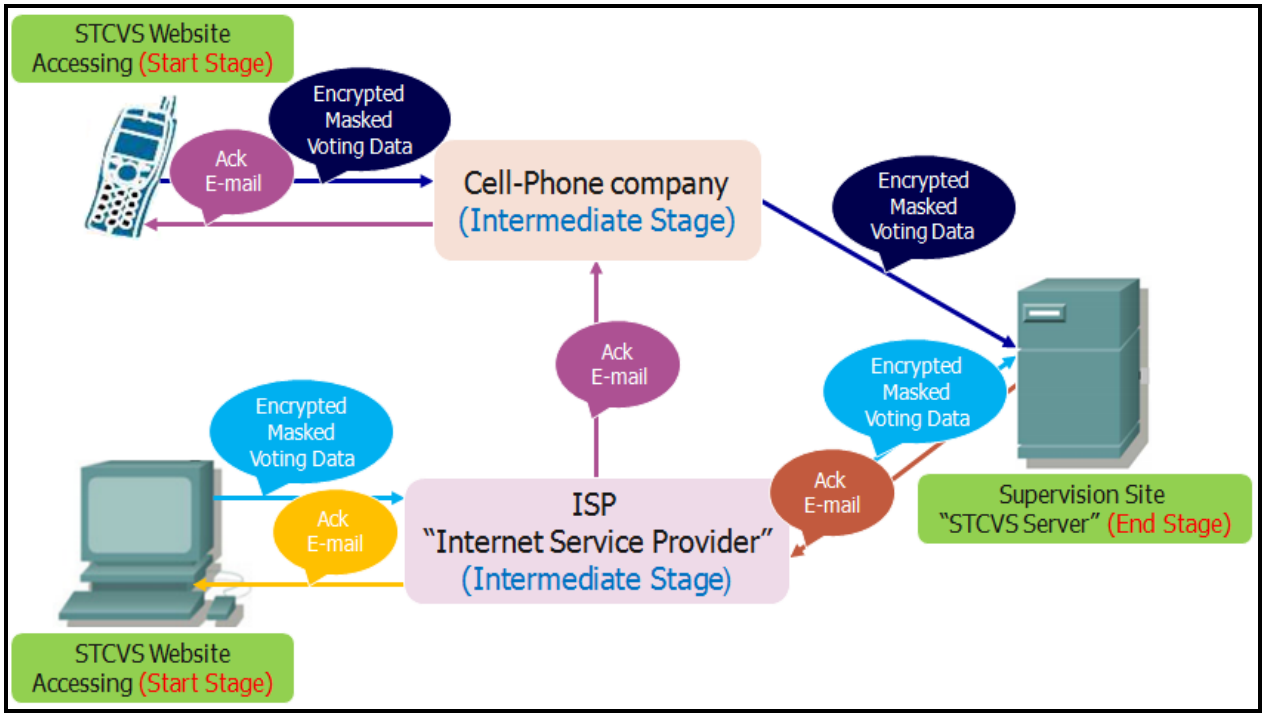

Fig. 1: STCVS Block Diagram

Fig. 1 illustrates the proposed technique to achieve a secured computerized voting procedure. In the "Start Stage", the user (Voter) would access the proposed Secured Transparent Computerized Voting System (STCVS) website using

a smart phone, laptop, PC, tablet or any computerized communication device. He would enter his login data, i.e. his full-name, pass-code as saved in the STCVS database.
Voter's authentication by verifying his login data to access the STCVS website should be successfully achieved. Furthermore, the digital signatures for his pass-code, public key (certificate verification) is a must to access the voting procedure, i.e. selecting the candidates numbers.
Voting Data (selected candidates numbers) would be masked using "LFSR", then encrypted using "Elgamal Asymmetric Encryption Protocol" (Public-Key). These procedures are used to prevent voting data attack while being sent from any computerized communication device to the next stages.
Encrypted masked voting data would be sent via either a cell-phone company or an Internet Service Provider (ISP) "Intermediate Stage", depending on the STCVS website access procedure, to the STCVS "Host" Server representing the (Supervision Site) "End Stage". The latter represents the supervision sites ("Higher Committee for Elections" and the "Human Rights Association" in the proposed system).
The accessed (cell-phone company or ISP) would only transmit the encrypted masked voting data as it is to the STCVS server. The latter would decrypt the voting data using "Elgamal Asymmetric Encryption Protocol" (Private-Key).
STCVS protects the Voting Data since the later would be sent Encrypted from the Client-Side where the user would achieve his voting and until the Host Server representing the Supervision Site. Encryption is achieved using an asymmetric cryptography algorithm (Elgamal) via Public-Keys. Decryption for the voting data is achieved by the Host Server using Private-Key. Each key (public / private) has approximately (20 – 25 bits).
The user gets a feedback (acknowledgement e-mail) from the STCVS website to his registered e-mail, also saved in the STCVS database. This e-mail consists of his voting data (decrypted selected candidates numbers).
Vote Attack could not be achieved since the voter pass-code is used once, it would be expired after each election. Thus, it could not be used by another voter or by the same voter for a next election. Also, voting duplication would not be allowed since the user could achieve voting once using the proposed system (STCVS).
Finally, the recorded percentages for the candidates numbers for each round are displayed as voting charts by accessing either of the "two" Supervision Sites accounts from the STCVS server. For security, correlation could be achieved easily between both voting charts for the "two" sites as a final verification before voting results official publishing.

3.2. STCVS database

STCVS uses MySQL database, which is an open source and free. As shown in Table 1, the STCVS database consists of "six" fields (Username – Password – Postalcode – Email – Address – Hasvoted). This table represents a snapshot from the STCVS database.

Table 1: STCVS Database

Uid	username	password	postalcode	email	address	hasvoted
1	Abdelhalim Zekry	1f4a04e5543d8760660bb080226040b987b88d47	12513	aaazekry@hotmail.com	Elharam	0
2	Enas Elbarbary	9653be2baea351aae7f81499705e784981ecb694	12511	enas_elbarbary@yahoo.com	Nasr City	1
3	Yassin Mahmoud	71abb7159f9649c5d2b327c910bd9f7d7d9f2324	12513	yassin_mahmoud@gmail.com	Elharam	1
4	Khaled Nader	cba5e9693c96ce3142a327d79f7bba9e2035df3a	12511	k_nader@yahoo.com	Nasr City	0
5	Rania Aly	a2fb50af0332fec4b5134abca7e446d1f58d5b79	12511	rania.aly@hotmail.com	Nasr City	1
6	Peter Meijer	d542e4604284d436f96dc2bed51cb797d1e17ddd	12511	pater_meijer@yahoo.com	Nasr City	1
7	Ingy Ashraf	719be3e0ae6dbd8820802d915ea44cfa27dfb220	12512	ingy.ashraf@yahoo.com	Maadi	0
8	Arigue Ashraf	abceb17294657a091deb8a8b3e5acdb74a91b594	12512	arigue.ashraf@yahoo.com	Maadi	0
9	Muhammad Khaled	1d92a3915dcddf4d9851aaa1ada15cf2d1492981	12512	m.khaled@gmail.com	Maadi	1
10	Lougy Ahmed	057a596588f2f336f95cf13026bb1b2afa8218dd	12512	lougy_ahmed@yahoo.com	Maadi	1

"User Identifier" (Uid) field represents simply an index for the voters stored in the database. "Username" field consists of the voters names stored in the STCVS database. "Password" field consists of the voters pass-codes, values shown in the above table are the (SHA-1') values for "ten" digits decimal number for each voter pass-code.

"Postalcode" field is related to the "Address" one. The proposed system is tested using "three" postal-codes (12511, 12512, 12513) for "three" different addresses (Nasr City, Maadi, Elharam). They represent "three" different voting rounds. STCVS was tested for "300" voters.
"E-mail" field consists of the voters registered e-mails to which the STCVS website will send the feedback e-mail (acknowledgement) as described in the next section.
"Hasvoted" field is (0/1) value, where "0" indicates that the voter has not yet vote, "1" indicates that the voter has already vote, this is used to prevent a voting duplication as will be discussed in the next section.

3.3. STCVS website

3.3.1. Voting Login

The voter would access the STCVS website using the URL: http://stcvs.no-ip.org, then login by entering his full-name, pass-code as shown in Fig. 2. Login data will be matched with that stored in the database; also a valid certificate will be verified for the voter by verifying the digital signatures for his pass-code, public key. So, voter authentication is verified.

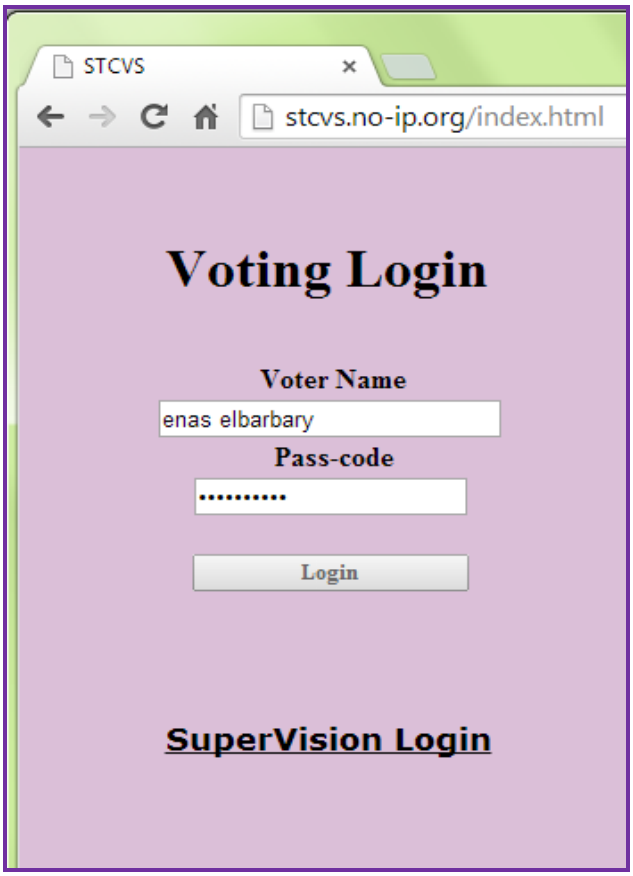

Fig. 2: STCVS Login Webpage

In case that the login data matching is achieved, and that the digital signatures for the public key and the voter's pass-code are verified, i.e. valid certificate is verified, a message box "Valid Certificate" will be displayed.
If the digital signature for either the public key or the voter's pass-code is not verified, voting procedure could not be achieved. Two error message boxes will be displayed consecutively "Invalid Certificate", "Unsecured Channel. Please use another device for voting".
According to each voter's postal-code stored in the database, a voting webpage as shown in Fig. 3 will be displayed where candidates numbers belonging to the voter's round could be selected [6].

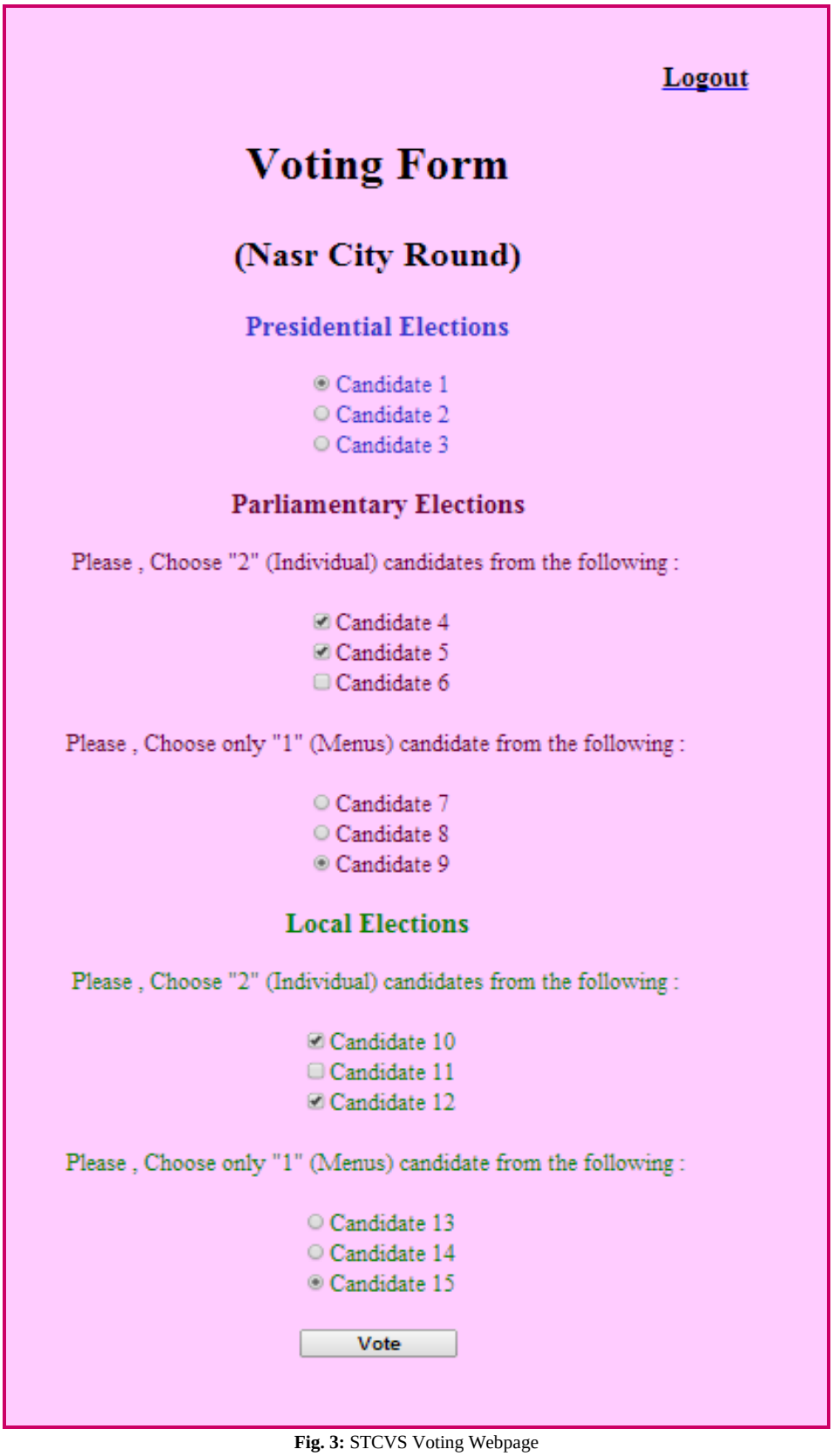

Fig. 3: STCVS Voting Webpage

A message box as shown in Fig. 4 will then be displayed as a confirmation that the voting procedure was achieved successfully. It consists of the voting data, i.e. the candidates numbers that the voter selected. Finally, it confirms that a feedback e-mail (acknowledgement) was sent from the STCVS website to the voter's e-mail registered in the STCVS database.

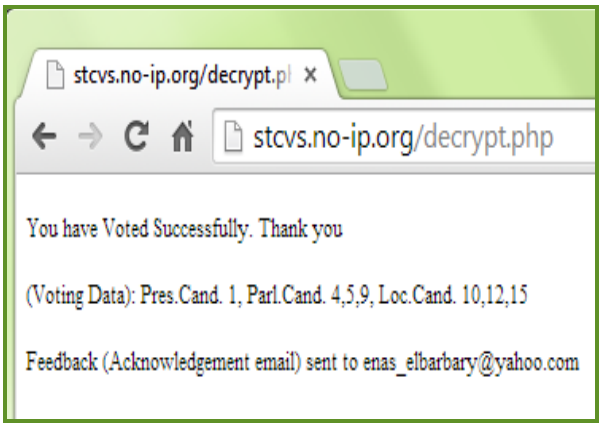

Fig. 4: STCVS Feedback E-mail (Acknowledgement)

Error message boxes are shown as alerts in case of any incorrect choice procedure, so that the voter can correct it to complete his voting procedure. These error messages are either concerning login or voting procedure as follows:

- Login error messages:

Login error message boxes are displayed in the following cases:

1) If the voter enters his full-name incorrectly, i.e. not as stored in the STCVS database. An error message box "That Voter does not exist in our Database" will be displayed. Voting login webpage shown in Fig. 2 will be displayed again to allow the voter a next login trial to achieve his voting procedure.
2) If the voter enters his pass-code incorrectly, i.e. not as stored in the STCVS database. An error message box "Incorrect Pass-code. Please try again" will be displayed indicating that this pass-code is not matched with that stored in the database. Voting login web page shown in Fig. 2 will be displayed again to allow the voter a next login trial to achieve his voting procedure.
3) If the voter tries to press the login button in the Voting login webpage shown in Fig. 2 without entering the login data. An error message box "Please Login to Vote" will be displayed indicating he has not yet login to vote.
4) If the voter has already achieved a successful voting procedure, then he tried to login again to vote, duplication will not be allowed. So, an error message box "You have already Voted" will be displayed indicating that he has already achieved his voting procedure.

- Voting error messages:

Voting error message boxes are displayed in the following cases:

1) If the voter has any missed field in the Voting form shown in Fig. 3. An error message box "Please, fill all the required fields to vote" will be displayed.
2) If the voter while using the Voting form shown in Fig. 3, has selected another number rather than "two" for (Parliamentary candidates [Individual]). An error message box "Please, choose [2] candidates from {Parliamentary Elections} checkboxes" will be displayed.

The same is achieved regarding the (Local candidates [Individual]).

3.3.2. Supervision Login

Supervision Login webpage shown in Fig. 5 is accessed from the Voting login webpage shown in Fig. 2 by pressing the "SuperVision Login" hyperlink.

The supervisor will enter his name, password to login. Login data should be verified to allow a supervisor login; passwords are verified as (SHA-1') values for "twenty" letters password length, otherwise access will be denied as described in the previous section for the voting login.

The supervisors represent the ("Higher Committee for Elections" and the "Human Rights Association" in the proposed work). So, "two" supervisors accounts could be accessed from the webpage shown in Fig. 5.

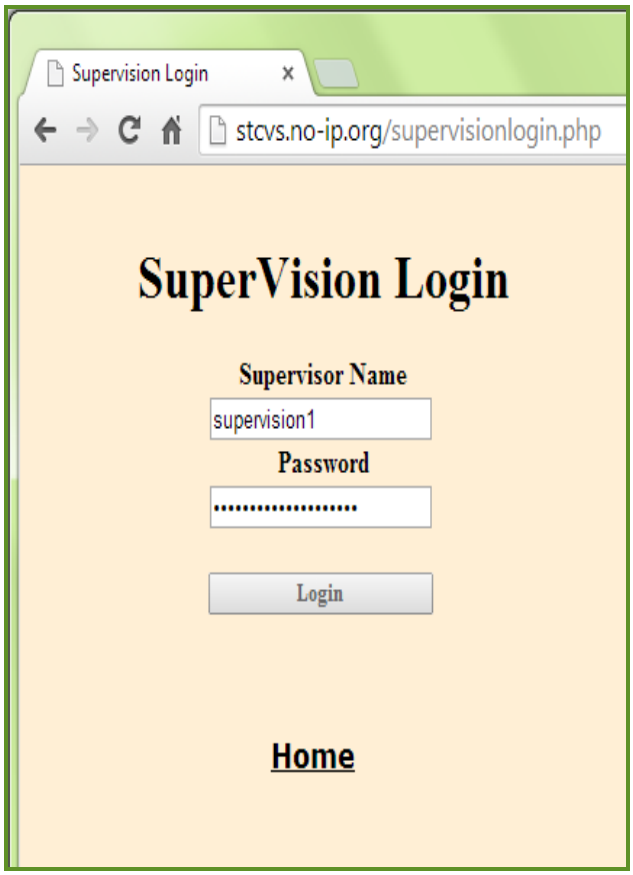

Fig. 5: STCVS SuperVision Login Webpage

Each of the "two" supervision sites has a table in the STCVS database in which voter selected candidates numbers (voting data) will be recorded as shown in Table 2 which represents a snapshot from the STCVS database. "Vote_id" represents only a serial number for the voting action. "Voter_id" represents the "Uid" described in the STCVS database in Table 1.

Table 2: STCVS Records

vote_id	voter_id	1	2	3	4	5	6	7
271	11	1	4	5	8	10	12	13
272	12	2	4	6	7	10	11	15
273	13	2	28	29	31	34	36	39
274	14	1	4	5	8	11	12	15
275	8	1	16	18	19	23	24	26
276	18	1	29	30	32	35	36	39
277	19	3	29	30	32	35	36	38
278	22	1	28	29	32	35	36	39
279	20	1	4	5	7	10	11	13
280	10	1	16	17	9	23	24	25

The fields (1 to 7) consist of the "seven" candidates numbers that the voter has to select from the Voting form described in Fig. 3. So, the voting data will be saved in the supervisors' database tables. According to these last fields, voting percentages will be recorded. If the supervisor login is succeeded, the supervisor will then be able to get the voting percentage for each candidate by the charts shown in Fig. 6. This is available for the presidential elections, also for each round separately regarding the (Parliamentary / Local) elections. Hence, our aim to protect the voting data will be achieved since it will be available only with the supervision site ("Higher Committee for Elections" and the "Human

Rights Association"). They are trusted to be the owner of the Host Server for the proposed system (STCVS). The later posses the code, and the keys' generation, will decrypt the voting data and send the confirmation (feedback e-mail) to the voter. Furthermore, the supervision sites will be responsible for any updates in the system like the database, the candidates numbers updating.

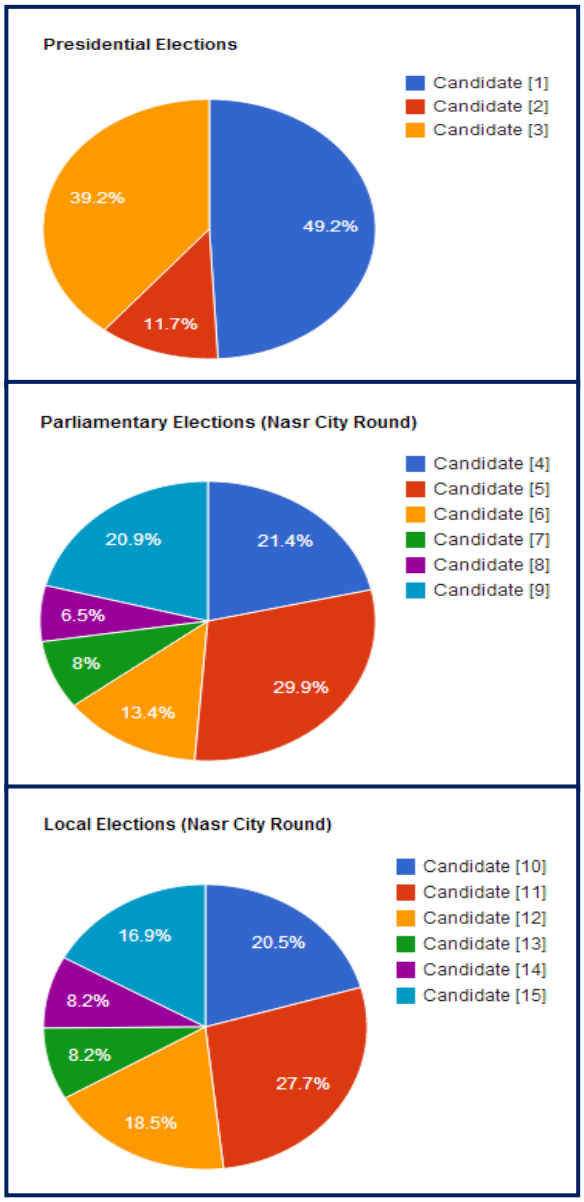

Fig. 6: Presidential / Parliamentary / Local Elections Charts

3.4. STCVS platform

The proposed system (STCVS) has been tested on a laptop with the specifications shown in Table 3. Code is written in Hypertext Preprocessor (PHP), JavaScript.

Table 3: Used Laptop Specifications

System	Specifications
Model	TOSHIBA Satellite P200
Processor	Genuine Intel(R) CPU 1.87 GHz
Installed Memory (RAM)	2.00 GB
HDD	500 GB
System Type	32-bit operating system

4. STCVS performance measurements

This section will present the proposed system performance measurements have been discussed in section 2. They include the input data masking using LFSR to protect the voting data and the Avalanche Effect results comparison for randomness testing using (LFSR/NLFSR) for data masking and finally without using data masking. AE is also tested for public key to test the system randomness as a design.

4.1. Plain text masking (LFSR)

LFSR are used to increase the randomness and hence to enhance the proposed system (STCVS) Avalanche Effect results as will be discussed in sub-section 4.2.1. It is used also for increasing the system security by applying data masking to protect the input data (voting data).
Table 4 presents the results of applying NLFSR, LFSR on (6 bits) input data (plain text) length. By flipping only one bit over the input data length as required for Avalanche Effect test, it is found that actually by applying masking (NLFSR / LFSR), a greater number of bits is flipped over the input data length. By using NLFSR, number of flipped bits over the input data length is found to be (2 or 3 or 4 or 5). Using LFSR, it is (3 or 4 or 5).

Table 4: Input Data Masking Effect

	Initial Data Value		
	43 / 101011 Input Data Without Masking (Decimal / Binary)	9 / 001001 Input Data Masked (NLFSR) (Decimal / Binary)	31 / 011111 Input Data Masked (LFSR) (Decimal / Binary)
Input Data after Bit No."1" Change	42 / 101010	50 / 110010	42 / 101010
Input Data after Bit No."2" Change	41 / 101001	36 / 100100	1 / 000001
Input Data after Bit No."3" Change	47 / 101111	5 / 000101	34 / 100010
Input Data after Bit No."4" Change	35 / 100011	27 / 011011	17 / 010001
Input Data after Bit No."5" Change	59 / 111011	34 / 100010	2 / 000010
Input Data after Bit No."6" Change	11 / 001011	49 / 110001	37 / 100101

Input data masking effect could also be analyzed by column charts as shown in Fig. 7. The charts show the number of input data changed bits due to one-bit change in an input data pattern consisting of (6 bits). Tests were achieved using LFSR/NLFSR for input data masking.

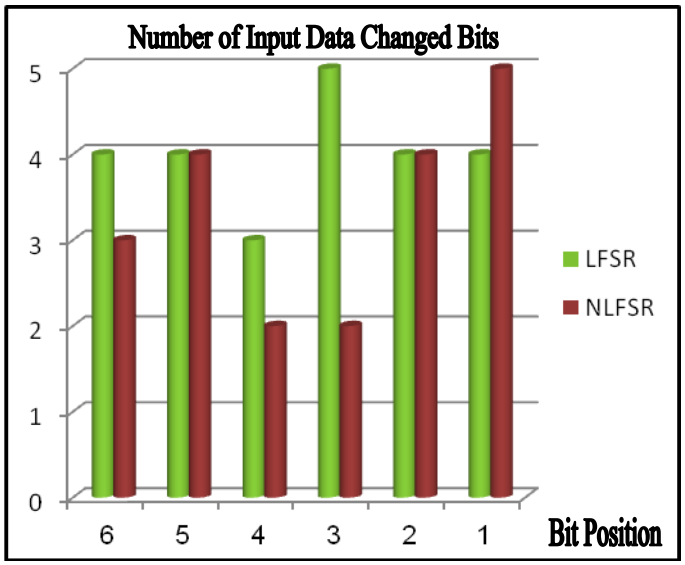

Fig. 7: Input Data Masking Effect Analysis

From the above results, clearly applying LFSR gives a higher number of flipped bits over the input data length than using NLFSR. This would enhance the Avalanche Effect results as will be discussed in sub-section 4.2.1.
For the input data tested pattern, the following functions were used for LFSR/NLFSR respectively:
LFSR applied function = Z_0 xor Z_2 xor Z_5.
NLFSR applied function = Z_0 xor Z_2 xor $Z_1.Z_5$ xor Z_4 xor $Z_0.Z_2.Z_3$.
Where Z_0 to Z_5 represents the "6" bits for input data, Z_0: LSB, Z_5: MSB.

4.2. Avalanche Effect results

AE was tested for the proposed system (STCVS) on both input data, public key as will be discussed in the following sub-sections.
To illustrate the reached AE results for input data, public key, different highlighting colors were used for the AE results' ranges. Green highlighting is used for AE range: (40-60%), yellow highlighting is used for AE ranges: (30-40% or 60-70%) and red highlighting is used for AE range: (<30% or >70%). This will be shown in Tables 5, 6.

4.2.1. Input data test

This test is based on flipping one bit over the input data length while keeping all other parameters fixed, and record the percentage of change in the output (cipher-text). The effect on output (cipher-text) would be due to "one-bit bit change in input data". Cipher-texts here are (21 bits).
Table 5 presents the Avalanche Effect percentage for testing (6 bits) input data length, tests are achieved without using masking, using NLFSR, LFSR for input data masking.
As shown in this table, by using NLFSR, (40-60%) percentage, which is the closest range to the ideal (50%) AE value is reached for (3) flipped bits only over the input data length. Using LFSR, this percentage is reached for (5) flipped bits over the input data length. So, using LFSR ensures better Avalanche Effect results.

Table 5: Input Data Avalanche Effect

Input Data Changed Bit No.	Avalanche Effect Percentage		
	Input Data Without Masking	Input Data Masked (NLFSR)	Input Data Masked (LFSR)
Bit No."1"	13/21 ~ 62%	11/21 ~ 52.4%	12/21 ~ 57.15%
Bit No."2"	11/21 ~ 52.4%	9/21 ~ 42.85%	8/21 ~ 38.1%
Bit No."3"	11/21 ~ 52.4%	14/21 ~ 66.67%	12/21 ~ 57.15%
Bit No."4"	12/21 ~ 57.15%	9/21 ~ 42.85%	10/21 ~ 47.62%
Bit No."5"	7/21 ~ 33.34%	8/21 ~ 38.1%	10/21 ~ 47.62%
Bit No."6"	11/21 ~ 52.4%	13/21 ~ 62%	9/21 ~ 42.85%

Input data AE could also be analyzed by column charts as shown in Fig. 8. The charts show the AE percentages due to one-bit change in an input data pattern consisting of (6 bits). Tests were achieved using LFSR/NLFSR for input data masking, and also without applying data masking.

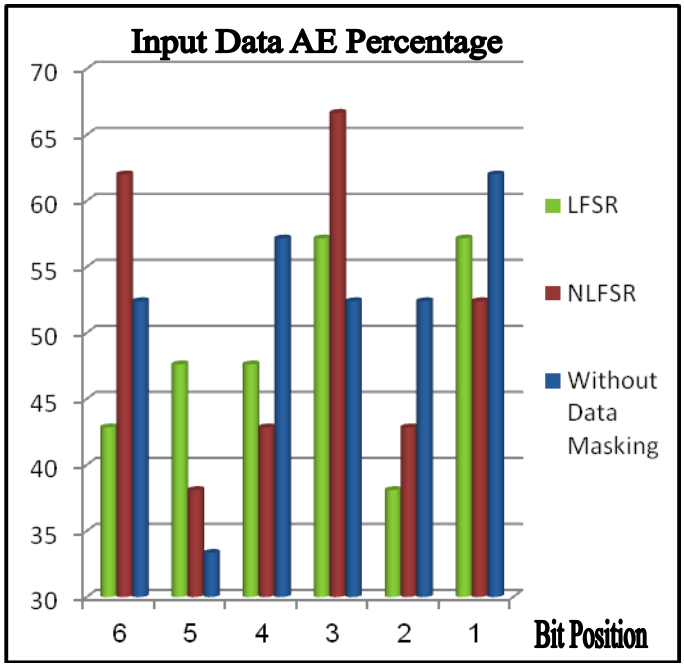

Fig. 8: Input Data Avalanche Effect Analysis

4.2.2. Public key test

This test is based on flipping one bit over the public-key length while keeping all other parameters fixed, and record the percentage of change in the output (cipher-text). The effect on output (cipher-text) would be due to "one-bit change in public key", tested public-key lengths are (23 bits). Corresponding cipher-texts lengths are also (23 bits).
Table 6 shows the Avalanche Effect percentage for this test. From these results, (40-60%) percentage which is the closest range to the ideal (50%) AE value is reached for (15) flipped bits over the (23) public-key length. Furthermore, the average AE percentage over the public-key length is (48.58%) which is so close to the ideal (50%) AE value.

Table 6: Public Key Avalanche Effect

Public Key Changed Bit No.	Avalanche Effect Percentage
Bit No."1"	13/23 ~ 56.52%
Bit No."2"	12/23 ~ 52.17%
Bit No."3"	14/23 ~ 60.87%
Bit No."4"	10/23 ~ 43.48%
Bit No."5"	11/23 ~ 47.83%
Bit No."6"	13/23 ~ 56.52%
Bit No."7"	6/23 ~ 26.1%
Bit No."8"	9/23 ~ 39.13%
Bit No."9"	13/23 ~ 56.52%
Bit No."10"	8/23 ~ 34.78%
Bit No."11"	15/23 ~ 65.21%
Bit No."12"	9/23 ~ 39.13%
Bit No."13"	12/23 ~ 52.17%
Bit No."14"	10/23 ~ 43.48%
Bit No."15"	11/23 ~ 47.83%
Bit No."16"	11/23 ~ 47.83%
Bit No."17"	11/23 ~ 47.83%
Bit No."18"	12/23 ~ 52.17%
Bit No."19"	14/23 ~ 60.87%
Bit No."20"	13/23 ~ 56.52%
Bit No."21"	9/23 ~ 39.13%
Bit No."22"	11/23 ~ 47.83%
Bit No."23"	10/23 ~ 43.48%
Average	48.58%

Public-key AE could also be analyzed by column charts as shown in Fig. 9. The charts show the AE percentages due to one-bit change in a public-key pattern consisting of (23 bits).

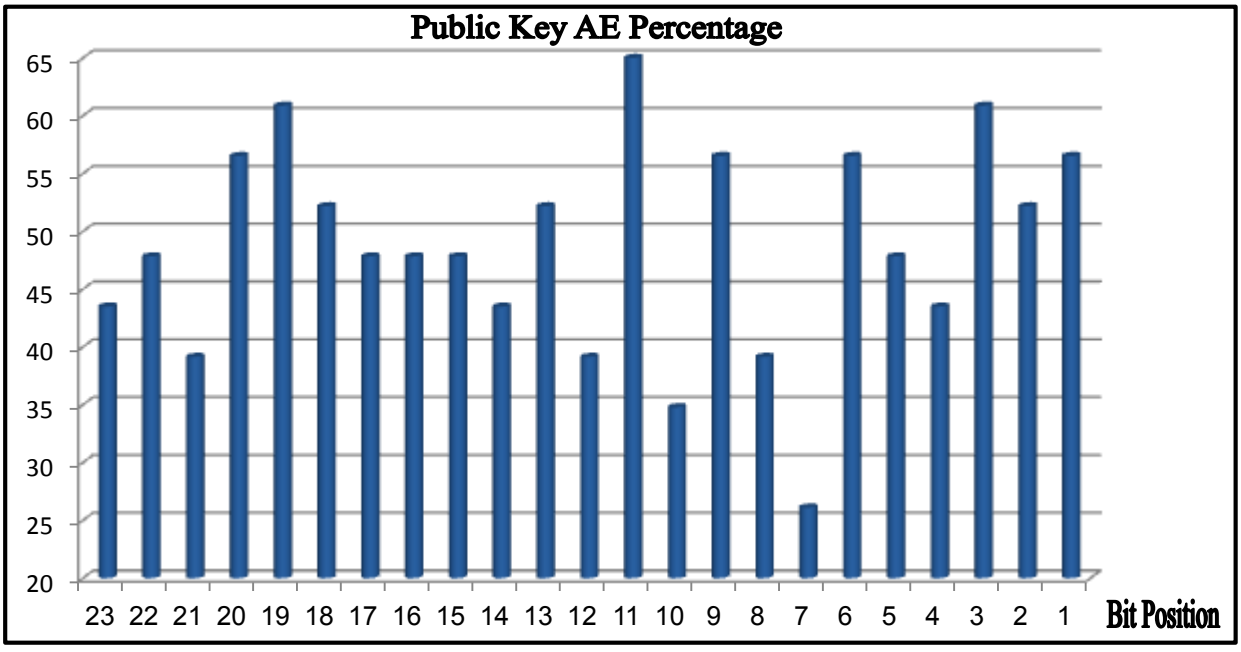

Fig. 9: Public Key Avalanche Effect Analysis

4.3. STCVS runtime

Tests were achieved using (300) registered voters for the proposed system (STCVS) database. The runtimes taken for voting, displaying the voting charts are as follows:

- Runtime / Vote ≈ (1) min.
- Runtime / Voting Charts displaying ≈ (30) sec.

The system was tested at real-time as a pilot using a laptop to simulate the Host Server. Public, private keys used for tests were (20 – 25) bits in length.

5. Conclusion

In this paper, STCVS has been proposed as an improvement methodology for conventional voting systems. STCVS could be accessed from everywhere, using a smart phone, laptop, PC, tablet or any computerized communication device. This is achieved by accessing the STCVS proposed website http://stcvs.no-ip.org to follow the voting process.

The proposed system maintains a real-time recording for the voting procedure to an allocated STCVS's database that could be accessed only by the supervision parties. While achieving voting transparency, the proposed system is capable of denying access to any illegal voter/s who is not registered in the proposed system database, or who enters an incorrect voting pass-code. Furthermore, STCVS prevents multiple votes by the same voter.

Moreover, the proposed voting system offers a simple to use website to assure voter's convenience. The voter gets a feedback (acknowledgement e-mail) consisting of his selected voting data.

The security of the proposed system is provided through the use of encryption/decryption and signing/verification mechanisms based on Elgamal public-key cryptography.

The experimented work describes the proposed STCVS results discussion and analysis as introduced in section 4. This section represents the proposed system performance measurements. It includes the input data masking using (LFSR/NLFSR) to protect the voting data. Furthermore, the AE results comparison for randomness testing while using (LFSR/NLFSR) for data masking. AE results without using data masking are also recorded. AE is also tested for public key to evaluate the system randomness as a design purpose. Finally, required processing time for voting/tallying is recorded.

Testing was achieved for input data. It was clear that applying LFSR gives the higher number of flipped bits over the input data length than using NLFSR. This enhances the Avalanche Effect results as described.

For better performance and more reliability, integrating biometrics with the proposed system would be suggested for more security. Biometrics is used in computer science as a form of authentication and access control. Voter fingerprint authentication, voter iris recognition could be integrated with the proposed system. This would surely increase the system cost since additional hardware, and software would be needed.

More security for such an elections system could be increased by increasing the private key size. This also necessities more advanced system specifications with definitely higher cost to support such larger key size.

A more realistic performance test with a larger network setup and a larger number of voters could be performed. This would provide a more realistic election system. Furthermore, it necessities more advanced system specifications with definitely higher cost to support such as larger database.

Finally, to improve the performance of the proposed system (STCVS) in respect to vote selling/coercion, though the proposed system design focuses on security and anonymity of the voting process. Therefore, to enhance the system design, ways of mitigating this issue have to be examined.

References

[1] Drew Springall, Travis Finkenauer, Zakir Durumeric and J. Alex Halderman, University of Michigan, Ann Arbor, MI, U.S.A., Jason Kitcat, Harri Hursti and Margaret MacAlpine, Open Rights Group, U.K., "Security Analysis of the Estonian Internet Voting System", (2014).

[2] Ahmed Hassan and Xiaowen Zhang, "Design and Build A Secure E-voting Infrastructure", Department of Computer Science, College of Staten Island, CUNY, USA, (2013). http://dx.doi.org/10.1109/LISAT.2013.6578240.

[3] Mohammed Khasawneh, Mohammad Malkawi, Omar Al-Jarrah, Thaier S. Hayajneh, and Munzer S. Ebaid, "A Biometric-Secure e-Voting System for Election Processes", *Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08)*, IEEE, Amman, Jordan, (2008). http://dx.doi.org/10.1109/ISMA.2008.4648818.

[4] Maina M. Olembo, Patrick Schmidt and Melanie Volkamer, "Introducing Verifiability in the POLYAS Remote Electronic Voting System", *Sixth International Conference on Availability, Reliability and Security*, Vienna, (2011), pp:127-134, available online: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6045924.

[5] Vitaly Dubravin, "Is Data Masking better than Encryption", available online: http://droidcafe.wordpress.com/2011/11/11/isdata-masking-better-than-encryption/, (2011).

[6] Enas Elbarbary, Ghada Abdelhady, Hussam Elbehiery, and Abdelhahim Zekry, "Secured Transparent Computerized Voting System accessible everywhere", *Journal of American Science*, (2014), available online: http://www.jofamericanscience.org/journals/am-sci/am1001/024_22810am100114_151_157.pdf.

[7] William Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition, Pearson Education Inc., (2006).

[8] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography, Massachusetts Institute of Technology, Cambridge, USA, (1996). http://dx.doi.org/10.1201/9781439821916.

[9] Christof Paar, and Jan Pelzl, Understanding Cryptography A Textbook for Students and Practitioners, Springer-Verlag, Berlin, Heidelberg, Germany, (2010).

[10] David Chaum, "Secret-Ballot Receipts: True Voter-Verifiable Elections", *IEEE Security and Privacy*, (2004). http://dx.doi.org/10.1109/MSECP.2004.1264852.

[11] Rui Joaquim, André Zúquete, and Paulo Ferreira, "REVS – A Robust Electronic Voting System", *IADIS International Journal of WWW/Internet*, Vol.1, No.2, (2003), pp.47-63.

[12] Jared Karro, and Jie Wang, "Towards a Practical, Secure, and Very Large Scale Online Election", *Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99)*, USA, (1999). http://dx.doi.org/10.1109/CSAC.1999.816024.

[13] Lorrie Faith Cranor, and Ron K. Cytron, "Sensus: A Security-Conscious Electronic Polling System for the Internet", *Proceedings of the Hawaii International Conference on System Sciences*, USA, (1997), available online: http://lorrie.cranor.org/pubs/hicss/hicss.html

[14] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta, "A practical Secret Voting Scheme for Large Scale Elections", *Advances in Cryptology - AUSCRYPT '92, Computer Science*, Japan, Vol.718, (1993), pp.244-251.

[15] Arthur M. Keller, Alan Dechert, Karl Auerbach, David Mertz, Amy Pearl, and Joseph Lorenzo Hall, "A PC-Based Open-Source Voting Machine with an Accessible Voter-Verifiable Paper Ballot", *USENIX '05, FREENIX track*, California, (2005), available online: http://infolab.stanford.edu/pub/keller/2005/electronic-voting-machine.html.

[16] Angel Tchorbadjiiski, "Liquid Democracy Diploma Thesis", RWTH AACHEN University, Germany, (2012).

[17] Berry Schoenmakers, "Fully Auditable Electronic Secret-Ballot Elections", XOOTIC Magazine, (2000).

[18] Manzur Murshed, Tishna Sabrina, Anindya Iqbal, and Mortuza Ali, "Verifiable and Privacy Preserving Electronic Voting with Untrusted Machines", *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Melbourne, VIC, (2013), pp: 798 - 804, available online: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6680917.

[19] Yirendra Kumar Yadav, Saumya Batham, Mradul Jain, and Shivani Sharma, "An Approach to Electronic Voting System using UIDAI", *International Conference on Electronics and Communication Systems (ICECS)*, Coimbatore, (2014), pp:1-4, available online: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6892510.

[20] Sahibzada Muhammad Ali, Chaudhary Arshad Mehmood, Ahsan Khawja, Rahat Nasim, et al. "Micro-Controller Based Smart Electronic Voting Machine System", *Electro/Information Technology (EIT), IEEE International Conference*, Milwaukee, WI, (2014), pp:438 - 442, available online: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6871804.

[21] Baisa L. Gunjal, and Suresh N. Mali, "Secure E-voting System with Biometric and Wavelet based Watermarking Technique in YCgCB Color Space", *IET International Conference on Information Science and Control Engineering (ICISCE)*, (2012), available online: http://digital-library.theiet.org/content/conferences/10.1049/cp.2012.2284.

[22] "Public Key Encryption and Digital Signature: How do they work", CGI Group Inc., (2004).

[23] Taher Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *IEEE Transactions on Information Theory*, Vol. IT-31, No.4, (1985). http://dx.doi.org/10.1109/TIT.1985.1057074.

[24] Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman, An Introduction to Mathematical Cryptography, Springer Science and Business Media, LLC, USA, (2008).

[25] Siddharth Agarwal, Abhinav Rungta, R.Padmavathy, Mayank Shankar and Nipun Rajan, "An Improved Fast and Secure Hash Algorithm", *Journal of Information Processing Systems*, Vol.8, No.1, (2012).

[26] Nabil H. Shaker, Hanady H. Issa, Khaled A. Shehata and Somaia N. Hashem, "Design of F8 Encryption Algorithm Based on Customized Kasumi Block Cipher", *International Journal of Computer and Communication Engineering*, Vol.2, No.4, (2013).

[27] Howard M. Heys and Stafford E. Tavares, "Avalanche Characteristics of Substitution-Permutation Encryption Networks", *IEEE Transactions on Computers*, Vol.44, No.9, (1995). http://dx.doi.org/10.1109/12.464391.

[28] Ashwak ALabaichi, Ramlan Mahmod and Faudziah Ahmad, "Analysis of Some Security Criteriafor S-boxes in Blowfish Algorithm", *International Journal of Digital Content Technology and its Applications (JDCTA)*, Vol.7, No.12, (2013).