Modification of Double Voter Perceptible Okamoto Blind Signature Based Electronic Voting Protocol

Asagunla Temitope

Submitted to the
Institute of Graduate Studies and Research
in partial fulfillment of the requirements for the Degree of

Master of Science
in
Computer Engineering

Eastern Mediterranean University
February 2015
Gazimağusa, North Cyprus

Approval of the Institute of Graduate Studies and Research

Prof. Dr. Serhan Çiftçioğlu
Acting Director

I certify that this thesis satisfies the requirements as a thesis for the degree of Master of Science in Computer Engineering.

Prof. Dr. Işık Aybay
Chair, Department of Computer Engineering

We certify that we have read this thesis and that in our opinion it is fully adequate in scope and quality as a thesis for the degree of Master of Science in Computer Engineering.

Assoc. Prof. Dr. Alexander Chefranov
Supervisor

Examining Committee

1. Assoc. Prof. Dr. Alexander Chefranov

2. Asst. Prof. Dr. Gürcü Öz

3. Asst. Prof. Dr. Önsen Toygar

ABSTRACT

Three electronic voting protocols aiming double perceptibility were considered in this thesis. The most promising of them is double voter perceptible blind signature based electronic voting protocol proposed by Baseri et al. However, it is found that generally, the protocol might fail due to the selection of g_0 as generator of $\mathbb{Z}_{\mathrm{n_{CA}}}$ (where $\mathrm{n_{CA}}$ is a product of $\mathrm{p_{CA}}$ and $\mathrm{q_{CA}}$) by the certificate authority as such generator does not exist. Furthermore, $\mathrm{h}_1$and h_2 were chosen as generators of $\mathbb{Z}_\mathrm{p}$ and $\mathrm{g}_1, \mathrm{g}_2$ as generators of $\mathbb{Z}_\mathrm{q}$ (where p and q are two large prime publicly known) by the certificate authority; thus, the modular p equality checks performed in the protocol might fail because used in their exponents are congruent modulo q and not congruent modulo Euler's totient function of p. These failures are shown by providing numerical counter-examples.

We proposed the way of fixing these problems. Firstly, we modified one of these equalities such that g_0 can be selected randomly in $\mathbb{Z}_{\mathrm{n_{CA}}}$. Moreover, we included the public key of the certificate authority with random value ξ selected in $\mathbb{Z}_{\mathrm{n_{CA}}}$ in the message sent to the voting server by the voter; thus, identity of the voter is verified. Secondly, we selected $\mathrm{h}_1, \mathrm{h}_2, \mathrm{g}_1$and g_2 in $\mathbb{Z}_\mathrm{p}$ of order q. This way, we might have different values as exponent on both sides of the equality but shall be congruent modulus p. Thus, all equality checks become valid. Lastly, we removed d and r_0 from the message sent to the ballot-counting server by the voting server since these are not used in revealing the identity of a dishonest voter. The modifications made retained all security properties of the protocol including the double perceptibility feature.

Keywords: Electronic voting, double perceptibility, blind Signature, RSA crypto-system.

ÖZ

Bu tezde, çift algılanabilirliği amaçlayan üç elektronik oylama protokolü ele alınmıştır. Bunlar arasında en umut verici olanı Baseri ve diğ. tarafından önerilen çift seçmen algılayan kör imza tabanlı elektronik oylama protokolüdür. Ancak, $\mathbb{Z}_{\mathrm{n_{CA}}}$ ($\mathrm{n_{CA}}$ öğesinin $\mathrm{p_{CA}}$ ve $\mathrm{q_{CA}}$'nin birer ürünü olduğundan) üreticisi olarak $\mathrm{g_0}$ öğesinin sertifika yetkilisi tarafından seçilmesiyle, bu gibi bir üreticinin mevcut olmamasından dolayı protokolün başarısız olabileceği sonucuna varılmıştır. Buna ek olarak, sertifika yetkilisi tarafından $\mathrm{h_1}$ve $\mathrm{h_2}$, $\mathbb{Z}_{\mathrm{p}}$'nin üreticisi ve $\mathrm{g_1, g_2}$ ise $\mathbb{Z}_{\mathrm{q}}$'nin üreticisi olarak seçilmiştir (p ve q bilinen iki büyük asaldır). Buna bağlı olarak, örneklerinde eşleşik modulo q ve eşleşik olmayan modulo Euler'in totient fonksiyonu p kullanıldığından, protokoldeki modüler p eşitlik kontrolleri başarısız olabilir. Bu başarısızlıklar, sayısal karşı örnekler sağlayarak gösterilmiştir.

Bu çalışmada, belirtilen sorunların çözülmesine ilişkin yollar önerilmiştir. Öncelikle, g_0'nin $\mathbb{Z}_{\mathrm{n_{CA}}}$'de rastlantısal olarak seçilebilmesi için bu eşitliklerden biri değiştirilmiştir. Ayrıca, oylama sunucusuna seçmen tarafından gönderilen iletideki $\mathbb{Z}_{\mathrm{n_{CA}}}$ içerisinde ξ random değeri seçili olan sertifika yetkilisi ortak anahtarı eklenmiştir. Böylece seçmen kimliği doğrulanmıştır. Ardından, q sırasıyla $\mathbb{Z}_{\mathrm{p}}$ içerisinde $\mathrm{h_1, h_2, g_1}$ve $\mathrm{g_2}$ seçilmiştir. Bu şekilde, eşitliğin her iki tarafında eşleşik modulus p olan farklı değerler örnek olarak bulunabilir. Buna bağlı olarak tüm eşitlik kontrolleri geçerli hale getirilir. Son olarak, dürüst olmayan bir seçmenin kimliğini belirleyemediğinden d ve $\mathrm{r_0}$ değerleri, oylama sunucusu tarafından oy sayımı sunucusuna gönderilen iletiden çıkarılmıştır. Tüm değişiklikler, çift algılanabilirlik özelliği dahil protokolün güvenlik özelliklerini korur.

Anahtar Sözcükler: Elektronik oylama, çift algılanabilirlik, kör imza, RSA kripto sistemi.

Dedicated to My Family

For Their Love and Support.

ACKNOWLEDGEMENT

First, I want to thank Almighty God for his faithfulness and for guiding me through this chapter of my life.

I would love to extend great gratitude to my supervisor, Assoc. Prof. Dr. Alexander Chefranov for his immense support, knowledge sharing and fatherly guide given throughout the period of this research.

I would also want to thank my parents, siblings and fiancée for their love and encouragement during the hard times. I want appreciate the effort of Ede Cyril, Femi Olaifa, Oyedeji Ajiobola, Ibrahim Ahmed, Lavi Bahram and other colleagues in Computer Engineering Department for their sincere critics and contributions to this work. Abiola Ayopo Abiodun , Jack and Jerry Sambe, Erinfolami Oluwatobi, Aanu Olushola, Clement Ajani, Basir Adamu sulaimon, Rccg Shekinah Parish family in Famagusta, I appreciate you all.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

AS	Authentication Server
BCS	Ballot Counting Server
CA	Certificate Authority
GCD	Greatest Common Divisor
ID_V	Identifier of Voters
ID_{VS}	Identifier Voting Server
$(e_{AS,}\ n_{AS})$	RSA Public Key of AS
d_{AS}	RSA Private Key of AS
$(e_{AS,}\ n_{AS})$	RSA Public Key of AS
d_{CA}	RSA Private Key of CA
$(e_{CA,}\ n_{CA})$	RSA Public Key of CA
V	Voter
VS	Voting Server

Chapter 1

INTRODUCTION

1.1 General Overview

Seeking people opinion is essential to critical decision-making; In order to achieve this, a voting mechanism has to be designed. Voting as defined in [1] is an act of freely expressing one's choice among publicly available alternatives. In last years, there have been debates whether e- voting systems can replace the traditional voting system having found in most cases evidences of misbehaving of participating parties in the latter.

Traditional base voting mechanisms are losing confidence in the fairness of the election [2]. One such traditional voting mechanism is making a head counts to get the number of people in support or against an opinion. Whichever has the greater number of headcount (Against or in support) wins.

This type of mechanism is very porous, as the system is easily cheated since no proper documentation are made. People can vote more than once since there is no way to know who voted before.

Another example is a paper-based voting. In this case, people come on the day of voting to a polling booth, registered and authenticated to collect a ticket (ballot paper), and cast their vote at a poling cubicle. Lastly, voters can cast their vote in a glass box in the presences of some jurisdiction and signed that they have voted.

As soon as voting stage is over, the glass boxes sometimes called ballot boxes are opened publicly, ballot papers are counted and the result of the election is publish or announce. One major problem of this method of voting system is that it consumes time. The time for counting and the exactness of results needs improvement to fast track the announcement and enforcement of decisions. Another problem with such system is that it is prone to fraud; elections manipulation is possible with little or no trace [3].

To some extent, people are quite not convinced that security properties of such voting systems such as anonymity, confidentiality, authentication or verifiability could be attained by the paper base election [4]. Until this day, this kind of voting system is still widely used.

1.2 Electronic Voting System and Limitations

Electronic voting systems are beginning to gain more research interest due to the advancement of information security that tend to provide solutions to the security challenges faced by paper-based voting systems. Several studies have focused on this area, and different author have modeled various aspects of cryptographic techniques analytically with the aim of providing a robust electronic voting system. However, this has not in any way increase the popularity of such system in our society. Most of the proposed electronic voting system does not meet the safety standards they claimed to offer. This can be attributed to lack of proper theoretical testing of the underlying algorithm of the system.

Moreover, many of these cryptographic techniques being used could not provide an acceptable, user friendly e-voting system. This is attributed to factors like fairness (one voter one vote), privacy, authentication, forgery, verifiability, bribery and coercion, correctness, time consumption, computational cost, availability of internet, illiteracy of voters among others among others.

Furthermore, it is a common criticism that electronic voting systems have a usability issue. It is often said that cryptographic e-voting systems are too complicated for the typical voter [4]. The issue of trust has also been raised, since most voters do not understand what happened behind the scene. This results in many proposed e-voting systems like the one in [5] not had been used in the real election [4].

In this regards, researchers kept relating existing or create new cryptographic techniques to design a potent and effective e-voting system with concerns for these security fundamentals.

1.3 Problem Statement

The author in [6] proposed an electronic voting protocol that provides double perceptibility of voter among other good features. However, Mateu et al. in [2] gave a fair criticism of the scheme. It is said that the failure of [6] was because of the publication of two elements g_1, g_2 of large prime order l chosen in $\mathbb{Z}_{n_{AS}}$ by CA; factoring of n_{AS} is possible by performing the greatest common divisor of $(g_1 - 1, n_{AS})$ [2].

Mateu et al however proposed an e-voting protocol based on [7] and [8] offline E-coin schemes. The two e-coin scheme does provide the double perceptibility of voter; nevertheless, the clarity of how to achieve it was not defined [6].

This thesis does a theoretical investigation of [9] that provides the double perceptibility of voter with other good security features, but fails due to wrong use of Okamoto blind signature scheme and also use of congruency of modular arithmetic. We provided solutions to these problems preserving the security features of the protocol. The rest of this thesis was structured as follows;

Firstly, in Chapter 2, a brief definition of some security properties to be satisfied by robust electronic voting systems were given; secondly, some standard cryptographic techniques that had been used by different authors to provide a secure e-voting platform were also alighted.

Secondly, in Chapter 3, we gave summary of Okamoto blind signature, which is the underlying foundation of [9]. Furthermore, we showed deficiencies in [9] by providing proof that the equality to be checked by the authorities might fail under the assumptions of the protocol. To support our claims, we provided numerical counter examples.

Finally, in Chapter 4, we proposed solutions to these problems and made modifications to part of the scheme without any effect on its security properties and in Chapter 5, we presented our conclusion and highlighted some future work.

Chapter 2

LITERATURE REVIEW

In this chapter, firstly, we gave a brief description of some standard security properties to be satisfied by an electronic voting system. Secondly, we highlighted some cryptographic techniques that could be used to achieve these security properties, giving the advantages of blind signature over others.

2.1 Brief Definition of Security Properties of E-Voting System

There are some standard securities Properties of voting to satisfy with an electronic voting system. These features include but no limited to the Privacy (Confidentiality), Fairness, Verifiability, Correctness (Accuracy), Robustness, Democracy, Receipt-Freeness. We regard the system as more secure if it can avoid forgery, bribery, and coercion [10].

2.1.1 Privacy

We define privacy as keeping secret of identity (identity is untraceable). In electronic voting or voting in general, it was assumed that no other participant/authority other than the voter should know the content of the casted ballot. In another form, the casted ballot should not be linked in any way to the voter who casted the vote [11].

In [12], to attain privacy, all ballot must be secret. Also, [13] wrote, “A secret ballot protocol is said to be private if the confidentiality of the voter is preserved”. Privacy is categorized into two in [11] :

a) Perfect Privacy: This is when no affiliation of participant e.g. authority, excluding the voter who is to cast his vote, can acquire details of the voter’s decision.

b) N-Privacy: This is when no N actors of the protocol, other than the voter, can obtain any details on the voter’s ballot.

In order to provide the feel of secret balloting in paper-based voting system, this property is highly required.

2.1.2 Exactness

Exactness or Correctness is clearly the most significant properties of any electronic voting system. In a summary, if all election process participants are truthful and behave as planned, thus the result of the process is to be the effective tally of the casted vote. The author in [12] called this completeness which means all valid votes are tallied accurately. The author in [14] gave another meaning as; an election is correctly counted if and only if the actual counted ballot matches the tallied ballot computed by the scheme.

Put differently, the result of a confidential balloting electronic voting protocol is accurate if the announced result is equal to the exact or real outcome of the election process. Though, its seems to be a straightforward explanation but factors like invalid vote, time frame for casting ballot among others could make such protocol violate this property.

2.1.3 Verifiability

As simple and straightforward as it is, a standard electronic voting protocol must be a process that is verifiable to prevent incorrect result and distrust [1]. However, paper-based voting does not provide such environment, but this would allow the voters to build trust in the system knowing that they could verify if their vote was part of the final tally [1].

There are majorly two types of verifiability, universal verifiability and individual verifiability:

a) Universal (Public) Verifiability: In this case, an active/quiet participant can be assured of the genuity or validity of distinct votes and the outcome of the election process. It is not an easy property to attain [15].

b) Individual Verifiability: This is type verifiability where every valid voter verifies that his or her vote was counted in the end of the election. This kind of verifiability is straightforward to achieve [15].

2.1.4 Fairness

In order to achieve this, no participant including authorities should have previous knowledge about a partial or total outcome of the election before the aggregating stage [8]. Any knowledge (partial or total) on the election outcome could have an effect on the decision of voters who are yet to cast their votes. The author in [16] wrote; A secret ticket election is fair when no active or passive participant can aqcuire tangible information on the aggregate outcome of the process before the announcement phase.

2.1.5 Robustness

Rajaskova in his paper in [17] defined robustness as the threshold of faulty behavior of n-combination of participant or authority can tolerate. No combination of active/ passive participator can halt the election process, and any not honest participant in such process is revealed. Another author in [3] wrote that the robustness assure that the electronic voting protocol can endure a definite number of false members.

2.1.6 Receipt Freeness

The concept of receipt-freeness in electronic voting is to prevent selling and buying of votes; this ensures voters cannot be used as an intermidiary or manipulated to cast votes. Author in [3] defined it as a process where voter must not be able to construct a receipt that can prove how he or she voted.

2.1.7 Democracy

The essence of voting is to determine the opinion of people. We can only achieve this if one and only one vote is counter to a voter. In order words, no voter should vote twice. The author in [12] defined democracy as a way of preventing multiple voting. Only eligible voter is allowed to cast ballot once, such that each voter has equal power to determine the outcome of the process.

2.1.8 Additional Properties

The security features highlighted above are of most importance when designing an electronic system, though they are not limited to these. We discuss some other properties here that could make the system more secure.

a) Transmission cost: This is the total cost of transmission due to the number of messages sent for all necessary computation and proofs [18].

b) Complexity of each round: This shows how efficient the scheme is during election times.

c) Pre-Election Processing: Electronic voting protocol is more reliable and secure, if a large amount of pre-computation could be carried our before the election time [16]. This is not the case for most e-voting protocols.

d) Flexibility: An electronic voting scheme is flexible if it is adaptable with respect to the number of participant or efficiency/ security tradeoff choice.

2.2 Cryptographic Techniques used in E-Voting

In order to achieve the security properties listed above, it is inevitable that we must employ the used of cryptographic techniques. Though there have been many arguments over the past years that cryptography cannot provide the necessary protection needed in electronic voting protocols [16]. We listed and discussed below some of the cryptographic techniques used in securing an electronic voting system.

a) Mixnet Encryption

b) Homomorphic Encryption

c) Secret Sharing

d) Interactive Zero Proof of Knowledge

e) Blind Signature

2.2.1 Mix-net Encryption

Chaum first introduced this encryption technique in his paper in [19], this method involve mixing of messages or votes by sending them through a chain of commands called Mixers. Each mixer scrambles the received votes before transfering to the next mixer; this ensures the anonymity of the voter [19].

However, there are different kinds of mix-net but the scope of this thesis does not cover such. Nevertheless, each mixer has a public key/ private key pairs. The ballot has to be preprocessed in advance using the mix server’s public key. Each casted ballot passes through the mix-net and decrypted by the sequent mix server’s private key before the counting stage. The method provides correctness, privacy, authentication, but the computational cost of large-scale election is high. The diagram below shows how a typical mix-net encryption.

2.2.2 Homomorphic Encryption

Homomorphism is an algebraic property that has also been employed providing necessary securities for an electronic voting protocol. It allows operations to be performed on groups of encrypted votes not decrypting them. It is a complicated mathematical procedure, but it does guarantee privacy, correctness, individual verifiability. Pascal Paillier and David Pointcheval gave a definition in [20] as; For a group of plain text M and ciphertext C, a process is Homomorphic if for any instance E of the encryption scheme, given $c_1 = E_{r1}\ (m_1)\ and\ c_{12} = E_{r2}\ (m_2)$ there exist an r such that $c_1 \otimes\ c_2\ = E_r\ (\ m_1\ \oplus\ m_2\ )$. Example of such encryption formed the basis in RSA and ElGamal protocols.

This encryption scheme has not gained much ground in securing e-voting system because of its computational overhead.

2.2.3 Secret Sharing

Secret sharing is an important cryptographic technique that could be used to provide need securities for an electronic voting system. It involves a secret key shared with a certain numbers of authorities in a way that no authority can construct the secret key without the consent of other [21]. A secret key for encrypting or decrypting a ballot is divided, and shared between N numbers of authority, such that any P out of N authorities can reconstruct the secret key but not less than P authorities can reconstruct the key.

It is possible that authorities can control the flow of election to manipulate the outcome. In such cases, a secret sharing algorithm is used such that no single authority can influence the election. The computational time and cost of having many authorities and the fact that authorities can be bribed to collapse the entire system are the main reason secret sharing has not gained much popularity with electronic voting.

2.2.4 Zero Prove of Knowledge

Zero knowledge prove demonstrates to a verifier that the validity of the statement is true without revealing anything information about statement except that the statement is true by the prover [22]. The author in [23] classified it into two as Interactive and Non Interactive. In interactive zero-knowledge prove, the protocol requires that the verifier make some input in the form of challenge questions. The response to such challenge will convince the verifier that the statement is true if and only if the statement is valid. It requires that both parties must be online.

However, the non-interactive zero knowledge proof, the prover proves the statement regardless of the verifier being online or not. Both interactive and non-interactive zero knowledge proof had been applied to electronic voting, but the latter is considered faster than the former. The author [23] Presented an e-voting scheme with non-interactive zero knowledge proof where the voter is consider the prover and the election officials are consider the verifier. The encryption technique guarantee anonymity, authentication.

2.2.5 Blind Signature

Chaum first introduced the protocol in 1982 as a form of digital signature. It allows a person to get signature on a message without revealing any information about the message to the signer [19]. A typical example from a world of paper document is enclosing a message in a carbon-lined enclosure. The signer appends the signature on the outside of the enclosure without checking the content of the message. A carbon copy of that the signature is impressed on the message and a third party can verify the signature.

2.3 Some Existing E-voting Protocols

There are different schemes that have employed different cryptographic methods to achieve the security properties mentioned in Section 2.1. In this thesis, we only reviewed those that used blind signature to achieve their security properties.

Chaum in [19] uses blind signature to attain privacy; although the ballot-counting server knows the content of the ballot, but it cannot trace it back to the voter that casted the voter due to the blinding factor. Moreover, each voter ballot is assigned a unique identifier thereby making the voters to verify if their ballot were part of the final tally. The authors in [12] and [25] used similar techniques to achieved accuracy, verifiability, and authentication. However, these schemes do not negate the effect of bribery and coercion.

The authors in [26] proposed a protocol that could provide the needed shield against bribery and corruption. They employed private voting space and physical voting booths as done with traditional elections to provide anonymity. Thus allowing voters to vote freely instead of fearing the coercer whom they might have made promises to. Unfortunately, the cumbersome of physical presence of voters and high cost of voting machines made the protocol not applicable in real life.

Sako and Kilian in [27] proposed another scheme aimed to provide security against bribery and forging of ballot under two assumptions. First, the channel of communication is untappable. Second, the briber cannot force the voter to reveal his vote. Unfortunately, the voter can use the ticket obtained to show how he voted.

The authors in [1] also discussed the issue of end-to-end verifiability; they proposed a system that provides verifiability of casted vote without revealing the identity of the voters to the verifier excluding the voter itself. Unfortunately, a greedy voter can reveal his identity but this cannot affect the outcome of the election, since voter can only verify if his vote is counted when election is over.

In real practice, there has been usage of electronic voting schemes in many countries all over the world in small scale. The first know web voting protocol was called Midac used in 1995 by the French government [28]. The system was used to run a voting pool on the need to test on nuclear testing in the pacific region. The Australian government did the first real used in the democratic settings; in October 2001 electronic voting was used in vesting vote were over sixteen thousand parliamentarian participated in the election [28].

Estonia began the use of electronic voting in their 2005 local elections thus, became the first country to use electronic voting to have legally bind a general election and it was declared a huge success by the country [29]. Moreover it was also used in there parliamentary election in 2011 where over two million people casted their online.

Furthermore, India introduced electronic voting into their system in 1982; they further expanded the used in 2004 and 2009 when it was used in their parliamentary election. So far, they are the only one to have recorded the largest number of voter that participated in an election held with electronic voting [28].

Apart from Helios used mentioned in [5], the implementation details of practical real world electronic voting protocols that were discussed above are unknown to the public.

Chapter 3

ANALYSIS OF DOUBLE VOTER PERCEPTIBLE BLIND SIGNATURE BASE VOTING PROTOCOL

In this chapter, we gave a brief summary of Okamoto blind signature protocol. Furthermore, we analyzed and gave a review of the double voter perceptible blind signature based e-voting protocol proposed by Baseri et al in [9]. The scheme was found to have deficiencies, which we fixed in next chapter.

3.1 Okamoto Blind Signature Scheme

The scheme was introduced in [29] by Tatsuaki Okamoto in 1992. It was an extension of a signature scheme proposed in [29]. It assumed that a user wants to get message msg signed blindly by an authority; this way his identity is preserved. The parameters used in this scheme are as follows: Two large prime numbers p and q are chosen such that $q|p-1$, two random numbers h_1 and h_2 are also chosen in $\mathbb{Z}_P^*$ of order q such that to solve the discrete logarithm problem in group $\mathbb{G} = \langle h_1 \rangle \approx \langle h_2 \rangle$ with respect to bases h_1 and h_2 is difficult. The signer (authority) picks two privates keys x_1, x_2 and gets a public key y from a certificate authority [29].

$$y = h_1^{x_1} \, h_2^{x_2} \, mod \, p \tag{3.1}$$

The corresponding signature for the message msg is the tuple $(\varepsilon\,, \rho_1, \rho_1)$; the signature is valid if it satisfies (3.2), where $\mathcal{H}$ is a one-way hash function.

$$\varepsilon = \mathcal{H}(h_1^{\rho_1} h_2^{\rho_2} / y^{\varepsilon} || msg) \tag{3.2}$$

We illustrate the scheme with Figure 1 below. Authors in [30] proved the privacy of this blind signature scheme in a random oracle mode and the un-forgeability of the protocol.

$(p, q, h_1, h_2, x_1, x_2)$ **Authority**		$(y = h_1^{x_1} h_2^{x_2} mod\, p, msg, p, q, h_1, h_2)$ **User**
$u_1, u_2 \in \mathbb{Z}_q$ $a = h_1^{u_1} h_2^{u_2}\ mod\, p$		
	$\xrightarrow{a}$	$t_1, t_2, t_3, \in \mathbb{Z}_q$ $\alpha = a h_1^{t_1}\ h_2^{t_2} y^{-t_3} mod\, p$ $\varepsilon = \mathcal{H}(\alpha \|\ msg)$ $c = \varepsilon - t_3 mod\ q$
	$\xleftarrow{c}$	
$re_1\ = u_1 + cx_1\, mod\, p$ $re_2 = u_2 + cx_2\, mod\, p$	$\xrightarrow{re_1\ ,re_2}$	
		$h_1^{re_1} h_2^{re_2} \overset{?}{=} ay^c\ \ mod\, p$ $\rho_1 = re_1 + t_1\, mod\ q$ $\rho_2 = re_2 + t_2\, mod\ q$ $\varepsilon \overset{?}{=} H({h_1}^{\rho_1} {h_2}^{\rho_2}\ / y^{\varepsilon} \| msg)$ ↓
		$(\varepsilon, \rho_1, \rho_2)$ signature

Figure 1: Summary of Okamoto Blind Signature (Reproduced from [9]

3.2 Review of Double Voter Perceptible Blind Signature Base Electronic voting Protocol

The scheme was proposed to eradicate the weakness found in Rodriquez-Henriquez et al protocol [9]. The author claimed that the protocol provides anonymity, authenticity; eliminate the problem of double voting and forgery by a legitimate voter. The foundation of the scheme is based on Okamoto blind signature.

The following authorities participates in the voting process; Voter (V), Certificate Authority (CA), Authentication Server (AS), Voting Server (VS), and Ballot Counting Server (BSC). We divided the whole scheme into 4 stages:

a) Stage 0 (Preliminary Stage): The certificate authority publishes the parameter needed by other authorities participating in the protocol

b) Stage 1: The voter gets a voting ticket from the authentication server, whose parameters are blindly signed by the authentication server.

c) Stage 2: The voter casts his vote with the voting server based on the information received from the authentication server. The voting server checks for validity of casted ballot and send it to the ballot-counting server.

d) Stage 3: The ballot-counting server receives the valid ballot, checks for double voting and updates its database of received ballot. After voting has ended, the ballot-counting server published result.

We give a diagrammatic schema of the protocol with the following figures

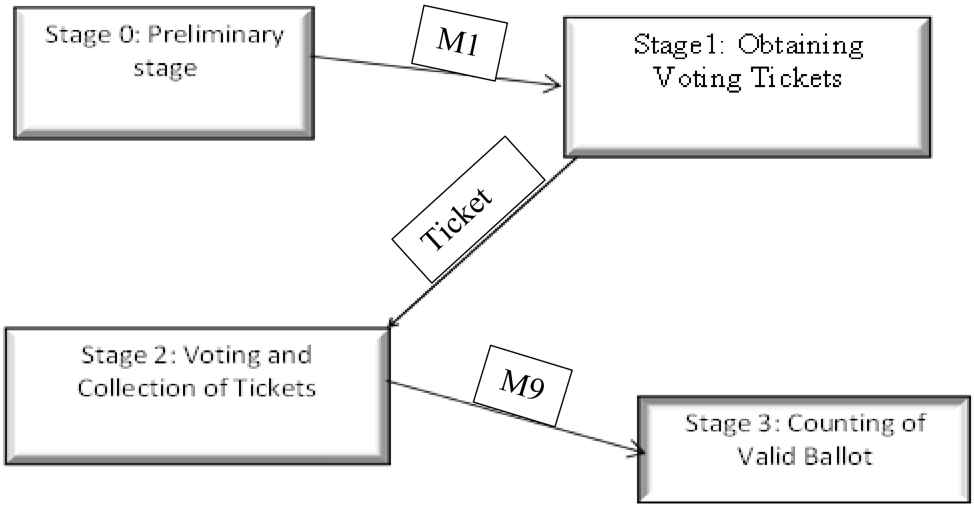
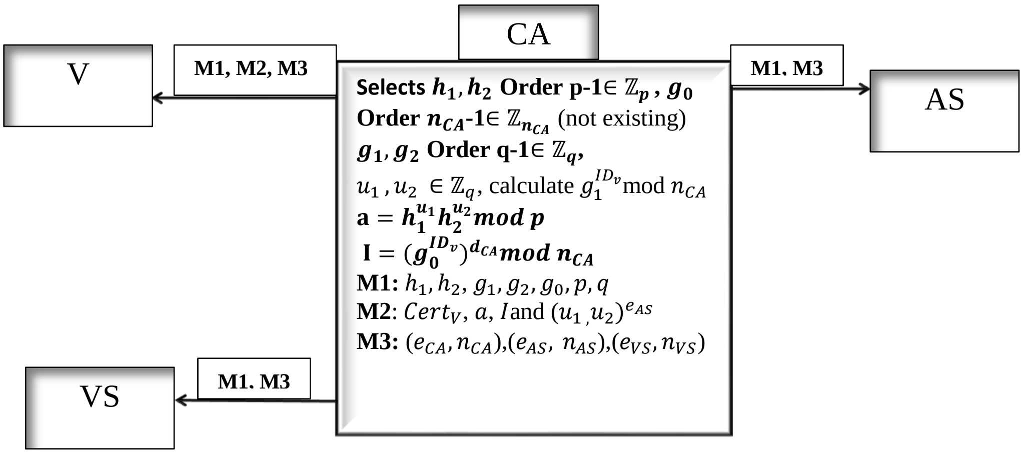

Stage 0: Preliminary stage
M1
Stage1: Obtaining Voting Tickets
Ticket
Stage 2: Voting and Collection of Tickets
M9
Stage 3: Counting of Valid Ballot

Figure 2: Scheme [9] in Stages

We elaborate further with the figures below on what happened in each stage of the protocol.



Selects h_1, h_2 Order p-1$\in \mathbb{Z}_p$ **,** g_0
Order n_{CA}-1$\in \mathbb{Z}_{n_{CA}}$ (not existing)
g_1, g_2 **Order q-1**$\in \mathbb{Z}_q$**,**
$u_1, u_2 \in \mathbb{Z}_q$, calculate $g_1^{ID_v}$mod n_{CA}
$\mathbf{a} = h_1^{u_1} h_2^{u_2} mod\ p$
$\mathbf{I} = (g_0^{ID_v})^{d_{CA}} mod\ n_{CA}$
M1: $h_1, h_2, g_1, g_2, g_0, p, q$
M2: $Cert_V$, a, $I$and $(u_1, u_2)^{e_{AS}}$
M3: (e_{CA}, n_{CA}),(e_{AS}, n_{AS}),(e_{VS}, n_{VS})

Figure 3: Preliminary Stage

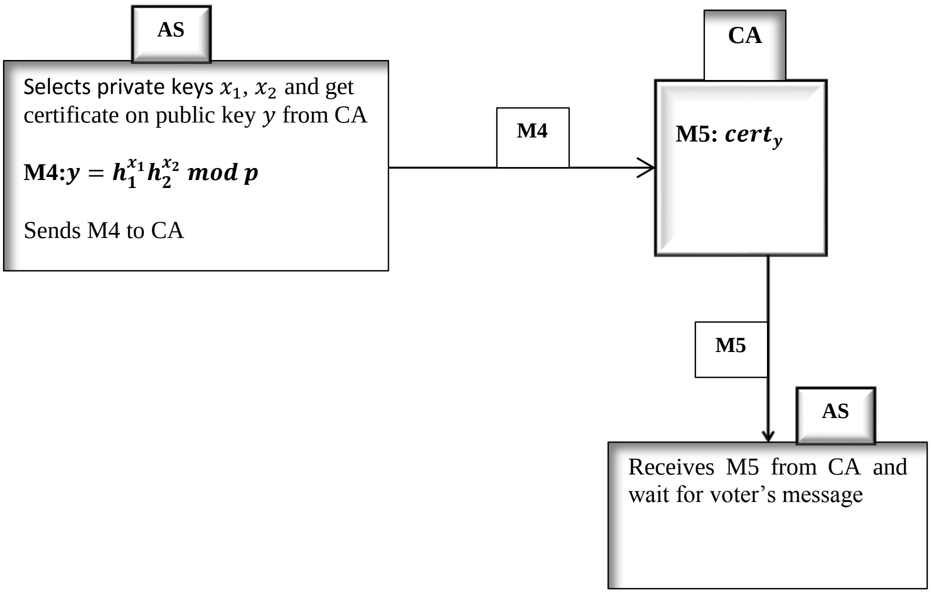

AS
Selects private keys x_1, x_2 and get certificate on public key y from CA
M4: $y = h_1^{x_1} h_2^{x_2}\ mod\ p$
Sends M4 to CA
M4
CA
M5: $cert_y$
M5
AS
Receives M5 from CA and wait for voter's message

Figure 4: Obtaining Voting Ticket (a)

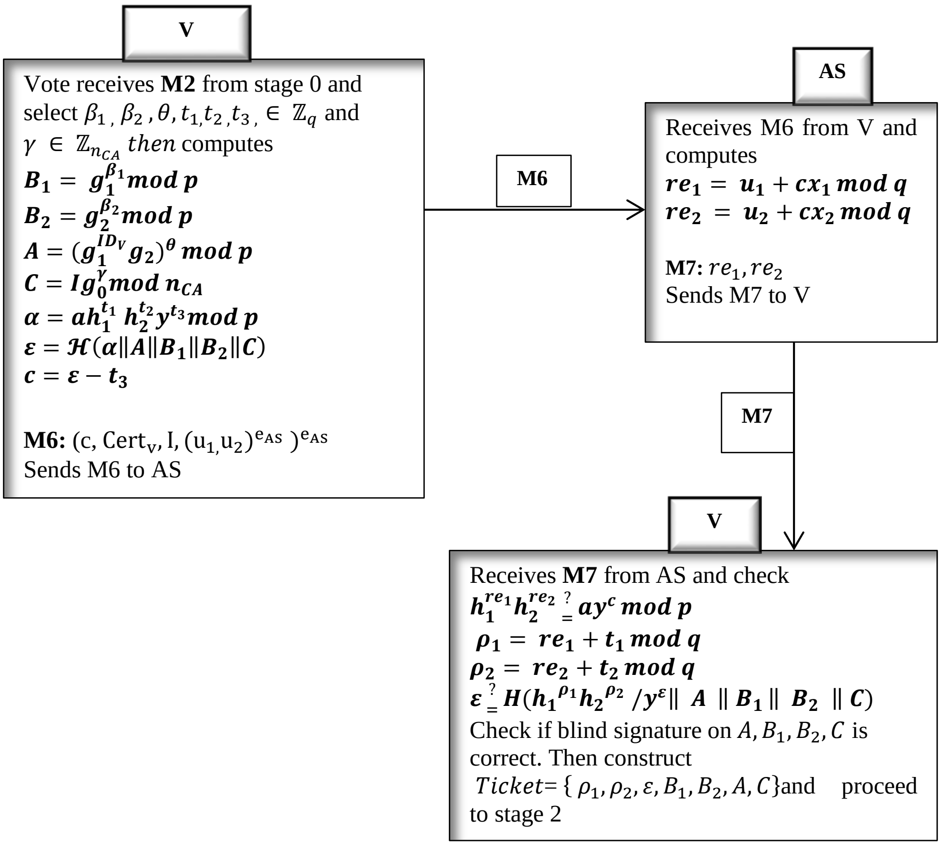

V
Vote receives **M2** from stage 0 and select $\beta_1, \beta_2, \theta, t_1, t_2, t_3, \in \mathbb{Z}_q$ and $\gamma \in \mathbb{Z}_{n_{CA}}$ $then$ computes
$B_1 = g_1^{\beta_1} mod\ p$
$B_2 = g_2^{\beta_2} mod\ p$
$A = (g_1^{ID_V} g_2)^{\theta}\ mod\ p$
$C = Ig_0^{\gamma} mod\ n_{CA}$
$\alpha = ah_1^{t_1}\ h_2^{t_2} y^{t_3} mod\ p$
$\varepsilon = \mathcal{H}(\alpha \| A \| B_1 \| B_2 \| C)$
$c = \varepsilon - t_3$
M6: (c, Cert$_V$, I, $(u_1, u_2)^{e_{AS}}$)$^{e_{AS}}$
Sends M6 to AS
M6
AS
Receives M6 from V and computes
$re_1 = u_1 + cx_1\ mod\ q$
$re_2 = u_2 + cx_2\ mod\ q$
M7: re_1, re_2
Sends M7 to V
M7
V
Receives **M7** from AS and check
$h_1^{re_1} h_2^{re_2} \overset{?}{=} ay^c\ mod\ p$
$\rho_1 = re_1 + t_1\ mod\ q$
$\rho_2 = re_2 + t_2\ mod\ q$
$\varepsilon \overset{?}{=} H(h_1^{\rho_1} h_2^{\rho_2} / y^{\varepsilon} \|\ A\ \| B_1 \|\ B_2\ \| C)$
Check if blind signature on A, B_1, B_2, C is correct. Then construct
$Ticket$= { $\rho_1, \rho_2, \varepsilon, B_1, B_2, A, C$}and proceed to stage 2

Figure 5: Obtaining Voting Ticket (b)

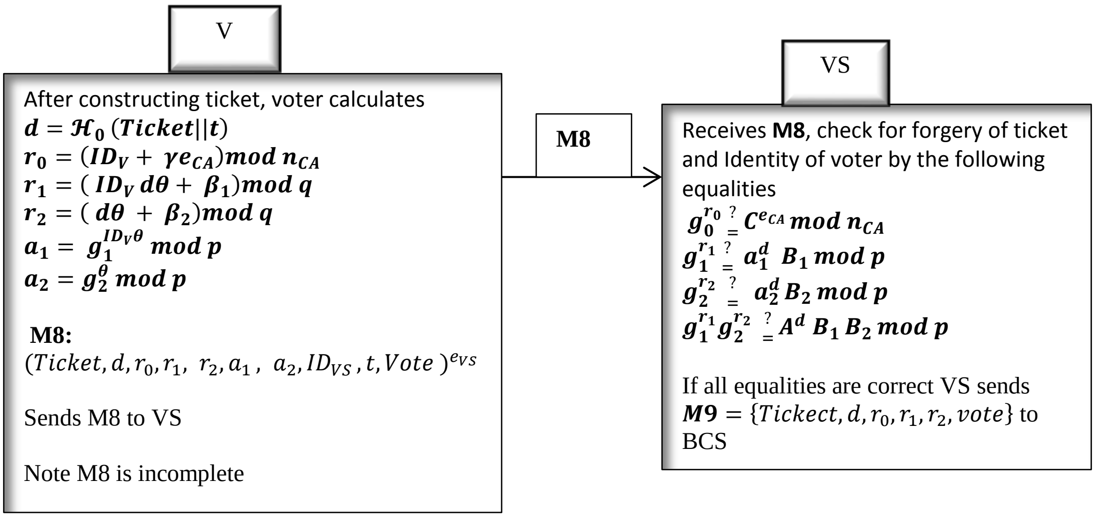

V
After constructing ticket, voter calculates
$d = \mathcal{H}_0\,(Ticket||t)$
$r_0 = (ID_V + \gamma e_{CA}) mod\, n_{CA}$
$r_1 = (\, ID_V\, d\theta + \beta_1) mod\, q$
$r_2 = (\, d\theta\, + \beta_2) mod\, q$
$a_1 = g_1^{ID_V\theta}\, mod\, p$
$a_2 = g_2^{\theta}\, mod\, p$
M8:
$(Ticket, d, r_0, r_1,\, r_2, a_1,\, a_2, ID_{VS}, t, Vote\,)^{e_{VS}}$
Sends M8 to VS
Note M8 is incomplete
M8
VS
Receives M8, check for forgery of ticket and Identity of voter by the following equalities
$g_0^{r_0} \overset{?}{=} C^{e_{CA}}\, mod\, n_{CA}$
$g_1^{r_1} \overset{?}{=} a_1^d\; B_1\, mod\, p$
$g_2^{r_2} \overset{?}{=} a_2^d\, B_2\, mod\, p$
$g_1^{r_1} g_2^{r_2} \overset{?}{=} A^d\, B_1\, B_2\, mod\, p$
If all equalities are correct VS sends $M9 = \{Tickect, d, r_0, r_1, r_2, vote\}$ to BCS

Figure 6: Voting and Collection of Ticket

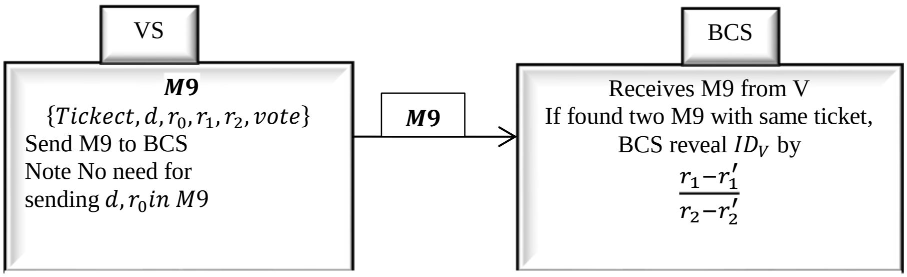

VS
$M9$
$\{Tickect, d, r_0, r_1, r_2, vote\}$
Send M9 to BCS
Note No need for sending $d, r_0 in\ M9$
$M9$
BCS
Receives M9 from V
If found two M9 with same ticket, BCS reveal ID_V by
$\frac{r_1 - r_1'}{r_2 - r_2'}$

Figure 7: Counting of Valid Ballot

We give a more detailed explanation of the protocol in stages below.

3.2.1 Stage 0: Preliminary Stage

Aside giving certificates to participating authorities, the CA also publishes h_1 and h_2 as distinct generators of $\mathbb{Z}_p$, g_0 as generator of $\mathbb{Z}_{n_{CA}}$ (note that such a does not exist) [32], because $n_{CA} = p_{CA} \times q_{CA}$, where p_{CA} and q_{CA} are two large secret prime numbers such that $(q_{CA}|p_{CA} - 1)$ and g_1, g_2 as generators of $\mathbb{Z}_q$; p and q are considered as two large prime numbers such that $q|p - 1$ publicly know.

The CA also publishes the RSA public keys of itself (e_{CA}, n_{CA}), of AS (e_{AS}, n_{AS}) and of VS (e_{VS}, n_{VS}) whereas d_{CA}, d_{AS}, d_{VS} are private keys of CA, AS and VS respectively. Voters are to acquire certificate from the CA.

The CA also places $g_1^{ID_v}$ mod n_{CA} in the voter's certificate, where ID_V is the voter's identifier chosen by CA in $\mathbb{Z}_q$ (we assume ID_V is present in the certificate obtained by voter from CA but not explicitly said in [9]). CA also chooses $u_1, u_2 \in \mathbb{Z}_q$ and computes

$$\mathrm{a} = h_1^{u_1} h_2^{u_2} mod\, p, \tag{3.3}$$

$$\mathrm{I} = (g_0^{ID_v})^{d_{CA}} mod\, n_{CA} \ . \tag{3.4}$$

Finally, CA sends $Cert_V, a, I$and $(u_{1\,,}u_2)^{e_{AS}}$ to the voter as M2 as shown in Figure 3.

3.2.2 Stage 1: Obtaining Voting Tickets

The authentication server chooses $x_1,\ x_2$ as private keys and gets certificate on corresponding public key y of the Okamoto Blind signature [30] from the CA as shown in Figure 4 , where

$$y = h_1^{x_1} h_2^{x_2}\ mod\, p. \tag{3.5}$$

However, in [30], h_1, h_2 are selected as having order of q, not as generators of $\mathbb{Z}_p$ as made in this scheme (See Section 3.1).

For a voter to be legitimate, he should take a ticket from AS (note, in this protocol voter constructs the ticket but he gets Okamoto blind signature from the AS). The process of taking the ticket is described below.

a) Voter selects $\beta_{1\,,}\,\beta_2 \in \mathbb{Z}_q$ and $\theta \in \mathbb{Z}_q$ and computes

$$B_1 = g_1^{\beta_1} mod\, p, \tag{3.6}$$

$$B_2 = g_2^{\beta_2} mod\, p, \tag{3.7}$$

$$A = (g_1^{ID_V} g_2)^{\theta}\ \ mod\, p. \tag{3.8}$$

Moreover, the voter selects a random value $\gamma \in \mathbb{Z}_{n_{CA}}$ and $t_{1,}t_{2\,,}t_{3\,,} \in_R \mathbb{Z}_q$ to compute the following using (3.3)-(3.8)

$$C = Ig_0^{\gamma} mod\ n_{CA}, \tag{3.9}$$

$$\alpha = ah_1^{t_1}\ h_2^{t_2} y^{t_3} mod\ p, \tag{3.10}$$

$$\varepsilon = \mathcal{H}(\alpha \| A \| B_1 \| B_2 \| C), \tag{3.11}$$

$$c = \varepsilon - t_3. \tag{3.12}$$

Where $\mathcal{H}$ is a one-way hash function. Finally, the voter sends $(\mathrm{c}, \mathrm{Cert_v}, \mathrm{I}, (\mathrm{u_{1,}u_2})^{\mathrm{e_{AS}}}\ )^{\mathrm{e_{AS}}}$ to the AS as M6 as shown in Figure 5. This is to obtain a blind signature from AS to preserve the voter's privacy.

b) AS receives (c, $Cert_v\ , I, (u_{1,}u_2)^{e_{AS}}\ )^{e_{AS}}$, and at first decrypts the message using its private key and check the validity of I given by (3.4): since CA publish g_0, ID_v is present in $Cert_v$ and lastly AS knows the public key e_{CA} of CA, it can easily confirm I. If I is valid, AS decrypt $(u_{1,}u_2)^{e_{AS}}$, extract $u_{1,}u_2$ and send to the voter re_1 and re_2 as M7 shown in Figure 5. re_1 and re_2 are computed as follows

$$re_1 = \ u_1 + cx_1\ mod\ q, \tag{3.13}$$

$$re_2 \ = \ u_2 + cx_2\ mod\ q. \tag{3.14}$$

c) The voter receives re_1 and re_2, and checks equality below.

$$h_1^{re_1} h_2^{re_2} \overset{?}{=} ay^c\ mod\ p. \tag{3.15}$$

Equality (3.15) is checked by the voter to make sure that the message (c, $Cert_v\ , I, (u_{1,}u_2)^{e_{AS}}\ )^{e_{AS}}$ was received without any alteration since only AS can get c (see (3.12)) generated by the voter and $u_{1,}u_2$ generated by CA, and used in (3.3) for calculating a, and x_1, x_2 generated by AS and used in (3.5) for computing y. Note that equality (3.15) might fail according to protocol [9] inputs because of the choice of h_1 and h_2; they are chosen as generators of $\mathbb{Z}_p$.

Statement 1: Equality (3.15) might fail in the conditions of the protocol [9].

Proof: Substituting (3.3), (3.5), (3.13) and (3.14) in (3.15), and collecting like terms we obtain;

$$h_1^{(u_1+cx_1)modq} h_2^{(u_2+cx_2)modq} = h_1^{u_1} h_2^{u_2} (h_1^{x_1} h_2^{x_2})^c \quad mod\, p$$
$$= \; h_1^{u_1+cx_1} h_2^{u_2+cx_2} mod\, p$$

(3.16)

Exponentiations in the left hand and right hand sides of the expression above may produce the same result modulo p if their powers are congruent modulo Euler's totient function $\varphi(p) = p - 1$ but in (3.15) they are congruent modulo q. Hence, they may have different values as shown in the constructed below numerical example.

Let p=*11*, q=*5*, $h_1 = 2,\ h_2 = 6,\ u_1 = 2,\ u_2 = 4,\ c = 6, x_1 = 3, x_2 = 4.$ Then according to (3.3),

$$a = h_1^{u_1} h_2^{u_2} modp = 2^2 6^4 mod 11 = 3.$$

From (3.5),

$$y = h_1^{x_1} h_2^{x_2} modp = 2^3 6^4 mod 11 = 6.$$

From (3.13) and (3.14),

$$re_1 = (u_1 + cx_1) modq = (2 + 6 \cdot 3) mod\ 5 = 0,$$

$$re_2 = (u_2 + cx_2) modq = (4 + 6 \cdot 4) mod\ 5 = 3.$$

Left hand side of (3.15) then becomes

$$h_1^{re_1} h_2^{re_2} modp = 2^0 \ \times 6^3 mod 11 = 1 \times 7\ mod 11 = 7.$$

Right hand side of (3.15) also becomes

$$ay^c modp = 3 \cdot 6^6 mod 11 = 15 mod 11 = 4.$$

Which is not equal to the left hand side, hence generally (3.15) is not true and that proves the statement. Note that $u_2 + cx_2 = 28$ which has different values modulo

$q = 5$ and modulo $\varphi(p) = p - 1 = 10$. If h_1, h_2 would be not generators of $\mathbb{Z}_p$, but have order q, as supposed in [30], then equality (3.15) would be true.

Once the correctness of (3.15) is checked, the voter compute ρ_1 and ρ_2 as:

$$\rho_1 = re_1 + t_1 \, mod \, q, \tag{3.17}$$

$$\rho_2 = re_2 + t_2 \, mod \, q. \tag{3.18}$$

The voter then verifies the blind signature of AS on A, B_1, B_2, C by checking the correctness of the equality below.

$$\varepsilon \overset{?}{=} H({h_1}^{\rho_1} {h_2}^{\rho_2} / y^{\varepsilon} \| \; A \; \| B_1 \| \; B_2 \; \| C) \tag{3.19}$$

Note that (3.19) might also fail for the protocol [9] inputs.

Statement 2: Equality (3.19) might fail in the conditions of the protocol [9].

Proof: From(3.11), (3.19), it follows that we need proving:

$${h_1}^{\rho_1} {h_2}^{\rho_2} y^{-\varepsilon} = \alpha \tag{3.20}$$

Subtituting (3.10), (3.17), and (3.18) into (3.20) we have

$$\frac{({h_1}^{re_1 mod\, q} {h_2}^{re_2 mod\, q}) \, ({h_1}^{t_1 mod\, q} \, {h_2}^{t_2 mod\, q})}{y^{\varepsilon}} = a h_1^{t_1} \, h_2^{t_2} y^{t_3} mod \, p \tag{3.21}$$

We again subtitutes (3.12), (3.13) and (3.14) into (3.21) and collect like terms

$$\frac{{h_1}^{u_1 mod\, q} {h_2}^{u_2 mod\, q} \, {h_1}^{cx_1 \, mod\, q} {h_2}^{cx_2 mod\, q} \; {h_1}^{t_1 mod\, q} {h_2}^{t_2 mod\, q}}{y^{t_3 + c}} = a h_1^{t_1} \, h_2^{t_2} y^{t_3} mod \, p \tag{3.22}$$

It is clear that again as in the case of (3.15), the problem of (3.19)-(3.22) is in the use of modulo q operation in the exponent instead of modulo $(p - 1)$. Also, sign of t_3 in (3.10) shall be negative or sign of ε shall be positive in (3.19) as it follows from the comparison of the sides of (3.22). We build a numerical counter-example for (3.19) using settings of the proof of the Statement 1.

So, $p=11$, $q=5$, $h_1 = 2, h_2 = 6, u_1 = 2, u_2 = 4, c = 6, x_1 = 3, x_2 = 4$, $a = 3$, $y = 6, re_1 = 0, re_2 = 3$. Let $t_1 = t_2 = t_3 = 1$.

From (3.17), (3.18),

$$\rho_1 = (\ re_1 + t_1\ ) mod\ q = (0 + 1) mod 5 = 1,$$

$$\rho_2 = (\ re_2 + t_2\ ) mod\ q = (3 + 1) mod 5 = 4.$$

From (3.12),

$$\varepsilon = c + t_3 = 6 + 1 = 7.$$

Then left hand side of (3.20) becomes

$h_1{}^{\rho_1} h_2{}^{\rho_2}\ y^{-\varepsilon} modp = 2^1 \cdot 6^4 \cdot 6^{-7} mod 11 = 2^1 \cdot 6^4 \cdot 2^7 mod 11 = 2^8 \cdot 6^4 mod 11 = 3 \cdot 9 mod 11 = 5.$

The right hand side of (3.20) also becomes

$$\alpha = a h_1^{t_1}\ h_2^{t_2} y^{t_3} mod\ p = 3 \cdot 2^1 \cdot 6^1 \cdot 6^1 mod\ 11 = 7.$$

Thus, the right hand side is not equal to the left hand side. If we use in (3.10) negated t_3, then the right hand side of (3.20) becomes

$\alpha = a h_1^{t_1}\ h_2^{t_2} y^{-t_3} mod\ p = 3 \cdot 2^1 \cdot 6^1 \cdot 6^{-1} mod\ 11 = 3 \cdot 2 \cdot 6 \cdot 2 mod\ 11 = 6,$ that is also not equal to the left hand side of(3.20). Hence, the statement is proved.

Finally if (3.19) holds, As construct the voter's ticket as;

$$Ticket = \{\ \rho_1, \rho_2, \varepsilon, B_1, B_2, A, C\} \tag{3.23}$$

As opposed to the AS constructing the voter's ticket, this should be done by the voter, since the parameters of the ticket are calculated by the voter but the voter got blind signature on theses parameters from the AS.

3.2.3 Stage 2: Voting and Collection of Tickets

a) After constrcting the ticket, the voter computes:

$$d = \mathcal{H}_0\,(Ticket||t) \tag{3.24}$$

$$r_0 = (ID_V + \gamma e_{CA}) mod\; n_{CA} \tag{3.25}$$

$$r_1 = (\,ID_V\, d\theta + \beta_1) mod\; q \tag{3.26}$$

$$r_2 = (\,d\theta\; + \beta_2) mod\; q \tag{3.27}$$

$$a_1 = g_1^{ID_V\theta}\; mod\; p \tag{3.28}$$

$$a_2 = g_2^{\theta}\; mod\; p \tag{3.29}$$

Where $\mathcal{H}_0$ is a public one way hash function.

The voter sends $(Ticket, d, r_0,\ r_1,\ r_2,\ a_1\,,\ a_2, ID_{VS}\,, t, Vote\,)^{evs}$ as message M8 to the VS, where ID_{VS} is the identity of the voting server.

Note that VS does not have any information on the CA, hence the message $(Ticket, d, r_0,\ r_1,\ r_2,\ a_1\,,\ a_2, ID_{VS}\,, t, Vote\,)^{evs}$ is incomplete since it does not define a particular CA: we might have many CAs participating in the voting process.

b) The voting server receives $(Ticket, d, r_0,\ r_1,\ r_2,\ a_1\,, a_2, ID_{VS}\,, t, Vote\,)^{e_{vs}}$, decrypts it and computes the value of d, it also check that the time stamp t has not expires, validates the legality of the voter by checking the signature of the Ticket and using (3.30) VS verifies the correct use of ID_V . Also, it checks r_1, r_2 (necessary to counter double voting) in (3.31)-(3.33).

$$g_0^{r_0} \overset{?}{=} C^{e_{CA}}\, mod\; n_{CA} \tag{3.30}$$

$$g_1^{r_1} \overset{?}{=} a_1^d\; B_1\, mod\; p \tag{3.31}$$

$$g_2^{r_2} \overset{?}{=} a_2^d B_2\, mod\; p \tag{3.32}$$

$$g_1^{r_1} g_2^{r_2} \overset{?}{=} A^d\; B_1\, B_2\, mod\; p \tag{3.33}$$

Note again that equalities (3.31)-(3.33) uses exponentiation and, hence, the powers must be congruent modulo Euler's totient function which is not used here just as in (3.15),(3.19). Also, used in (3.30) g_0 expected to be a generator for $\mathbb{Z}_{n_{CA}}$ (see Section 3.2.1) does not exist.

Equalities (3.31)-(3.33) checks correctness of r_1, r_2 by the VS, but it is not necessary since they are inside a message encrypted by the public key of VS and having its identifier inside: if this identifier is correct, the message is authentic. Verification of (3.30) is necessary to be sure that the voter is actually certified by CA.

Statement 3: Equality (3.30) might fail under assumptions of protocol [9].

Proof: we substitute (3.25) into the left hand side and (3.4), (3.9) into the right hand side of (3.30) and obtain

$$g_0^{(ID_V+\gamma e_{CA}) mod n_{CA}} \overset{?}{=} g_0^{(ID_V.d_{CA}).e_{CA}} . g_0^{\gamma.e_{CA}} mod n_{CA}, \tag{3.34}$$

From (3.34)

$$g_0^{(ID_V+\gamma e_{CA}) mod n_{CA}} \overset{?}{=} g_0^{ID_V+\gamma e_{CA}} mod\ n_{CA.} \tag{3.35}$$

Where $e_{CA}.d_{CA}\ mod\ \varphi(n_{CA}) = 1$. It follows that (3.30) might fail even if g_0 be any number in $\mathbb{Z}_{n_{CA}}$ because, the exponents are congruent modulo n_{CA}, not the Euler's totient function $\varphi(n_{CA}) = (p_{CA} - 1)(q_{CA} - 1)$. We build a counter example to show the failure of (3.30).

Let $p_{CA} = 7, q_{CA} = 3, n_{CA} = 21, e_{CA} = 5, d_{CA} = 5, g_0 = 2 \in \mathbb{Z}_{n_{CA}}$.

From Section (3.2.1), let $ID_V = 2 \in \mathbb{Z}_q$ and $\gamma = 5 \in \mathbb{Z}_{n_{CA}}$.

From (3.4),

$$\mathrm{I} = (g_0^{ID_v})^{d_{CA}} mod\ n_{CA} = 2^{2\times5} mod\ 21 = 16,$$

Also from (3.9) and (3.25),

$$C = Ig_0^{\gamma} mod\ n_{CA} = 16 \times 2^5 mod\ 21 = 8,$$

$$r_0 = (ID_V + \gamma e_{CA}) mod\, n_{CA} = (2 + 5 \times 5) mod\, 21 = 6.$$

Left and right hand side of (3.30) becomes

$$g_0^{r_0} modn_{CA} = 2^6\, mod\, 21 = 1,$$

$$C^{e_{CA}} modn_{CA} = 8^5\, mod\, 21 = 8,$$

which is not equal left hand side. Hence Statement 3 is proved.

Statement 4: Equalities (3.31)-(3.33) might fail under assumptions of the protocol [9].

Proof: Substitute (3.26) into the left hand side, and (3.6), (3.24), (3.28) into the right hand side of (3.31):

$$g_1^{(ID_V d\theta + \beta_1) mod\, q} \overset{?}{=} g_1^{(ID_V \theta) d} g_1^{\beta_1} mod\, p, \tag{3.36}$$

From (3.36),

$$g_1^{(ID_V d\theta + \beta_1) mod\, q} \overset{?}{=} g_1^{(ID_V d\theta + \beta_1)} mod\, p. \tag{3.37}$$

The problem in (3.37) is same as that in (3.35), the exponents are congruent modulo q, not the Euler’s totient function. Equalities (3.32), (3.33) are similar to (3.31). Let’s build a counter-example showing failure of (3.31)-(3.33). Let $p = 23, q = 11$. From Section (3.2.1), let $ID_V = 2 \in Z_q$. From Section 3.2.2a, let $\theta = 2 \in Z_{q,}\beta_1 = 1 \in Z_q, \beta_2 = 3 \in Z_q$. Let according to (3.24), $d = 5$. Let, according to Section 3.2.1, $g_1 = 7,\ g_2 = 10$ as two generators of Z_q.

In addition to (3.26), (3.27),

$$r_1 = (ID_V d\theta + \beta_1) modq = (2 \cdot 5 \cdot 2 + 1) mod 11 = 10,$$

$$r_2 = (d\theta + \beta_2) modq = (5 \cdot 2 + 3) mod 11 = 2$$

Therefore, the left hand side of (3.31) and (3.32) respectively becomes

$$g_1^{r_1} mod p = 7^{10} mod 23 = 13,$$

$$g_2^{r_2} mod p = 10^2 mod 23 = 8.$$

Then according to (3.28), (3.29), (3.6),(3.7),

$$a_1 = g_1^{ID_V \theta} \ mod\ p = 7^{2 \cdot 2} \ mod 23 = 9 \ ,$$

$$a_2 = g_2^{\theta} \ mod\ p = 10^2 \ mod\ 23 = 8,$$

$$B_1 = g_1^{\beta_1} mod\ p = 7^1 mod 23 = 7,$$

$$B_2 = g_2^{\beta_2} mod\ p = 10^3 mod\ 23 = 11.$$

The right hand side of (3.31) is

$$a_1^d \ B_1 \, mod\ p = 9^5 \cdot 7 mod\ 23 = 10,$$

and it is not equal to the left hand side of (3.31).

The right hand side of (3.32) is

$$a_2^d B_2 \, mod\ p = 8^5 \cdot 11 mod\ 23 = 15,$$

and also not equal to the left hand side of (3.32). Thus, Statement 3 is proved for both equalities.

From (3.8),

$$\text{A} = (g_1^{ID_V} g_2)^{\theta} mod\ p = (7^2 \cdot 10)^2 mod 23 = 3 \ ,$$

Therefore, we calculate the hand side of (3.33) as

$$g_1^{r_1} g_2^{r_2} = 7^{10} \cdot 10^2 mod 23 = 12,$$

and the right hand side of (3.33) becomes

$$A^d \ B_1 \, B_2 \, mod\ p = 3 \cdot 7 \cdot 11 mod 23 = 1 \ ,$$

which is not equal to the left hand side of the equality. Thus, Statement 4 is fully proved.

After checking for the correctness of the equations above, VS ensures the validation of ballot $\{Tickect, d, r_0, r_1, r_2, vote\}$ and sends it to the ballot counting server [9].

3.2.4 Stage 3: Counting of Valid Ballot

All voting servers can store ballot in ballot boxes; once a ballot box is full, VS send them to the BSC over a network. BSC can check for double voting in case a voter votes with two different voting servers. If the BSC finds two ballots with the same tickets (i.e. $\{Ticket, d, r_0, r_1, r_2\}$ and $\{Ticket, d', r_0', r_1', r_2'\}$ by using the relationship between these entities, it can reveal the identity of the voter by computing:

$$ID_V = \frac{r_1 - r_1'}{r_2 - r_2'} = \frac{dID_V\theta - d'ID_V\theta}{d\theta - d'\theta} \tag{3.38}$$

This double perceptibility feature supported by (3.38) is very important since it gives credibility in terms of fairness (i.e. one voter, one vote).

Finally, the BSC can tally the valid votes and publish the tuple $\{C, vote\}$ in the bulletin board to give assurance to any voter that his vote was part of the final tally.

Note that, $vote$ should be included in the message sent by the VS to BCS since ballot-counting server needed to publish it. Furthermore, including d, r_0 in the message is not necessary since BCS does not use them in checking double voting.

Chapter 4

MODIFIED PROTOCOL

In Chapter 3, we showed that our claims are correct by provding proofs and numerial counter examples to show that indeed [9] has some deficiencies [33]. In this chapter we provided modifications to the protocol . This modifications does not in any way jeopadize the security features of the protocol but tends to solve the deficiencies found in the scheme.

We first provided correct assumptions to the selections of some parameters used in the protocol. Secondly , we provided proofs to show that our assupmtions are correct and made modification the equations to be verified by the voting server. Moreover, we made adjustment to the messaget sent to the voting server by the voter.

4.1 Proposal 1 (related with Statements 1, 2, and 4)

In order for the problems related to statements 1, 2 and 4 to be resolved, the Certificate authority should select $h_1, h_2, g_1, g_2 \in \mathbb{Z}_p$ of order q. In such the exponents on both sides of the equations shall be congruent modular q in general.

Proof: We have seen that the problems were related with the use of congruency modulo q in exponents whereas exponentiations were performed modulo p. If the base of the exponentiation is of order q, such exponentiations are equal, and all the equalities (3.15), (3.19), (3.31)-(3.33) mentioned in the Statements 1, 2 & 4 will be identical for the correct protocol inputs.

Actually, if (4.1) holds

$$b^q mod p = 1, \tag{4.1}$$

$$b^s mod p = b^{kq+r} mod p = (b^q)^k b^r mod p = b^r mod p, \tag{4.2}$$

where $k = s\ div\ q, r = s\ mod q$. Thus the Proposal 1 proof is completed.

4.2 Proposal 2 (related with statement 3)

We stated in Section 3.2.1 that g_0 selected by CA and expected to be a generator for $\mathbb{Z}_{n_{CA}}$ does not exist (see [32]). In order to solve this problem and validate (3.30), we select $g_0 \in \mathbb{Z}_{n_{CA}}$ and two random values $\xi, \delta \in \mathbb{Z}_{n_{CA}}$; Therefore, instead of (3.9) in Section 3.2.2a, we define C by (4.3); and instead of (3.25), we define r_0 by (4.4):

$$C = I^{\delta} mod\ n_{CA}, \tag{4.3}$$

$$r_0 = g_0^{ID_V \xi \delta}\ mod\ n_{CA}. \tag{4.4}$$

The voter in Stage 2a (Section 3.2.3) sends the following message extended by CA information $(Ticket, d, r_0,\ r_1,\ r_2,\ a_1,\ a_2, ID_{VS}, t, Vote, e_{CA}, \xi\ )^{evs}$ to the voting server.

The voting server can then check the correct use of ID_V with (4.5) instead of (3.30):

$$r_0 \overset{?}{=} C^{e_{CA}\xi}\ mod\ n_{CA} \tag{4.5}$$

Proof: We need to prove that (4.5) will validate ID_V instead of (3.30).

Since $I = (g_0^{ID_v})^{d_{CA}} mod\ n_{CA}$, (see (3.4)), we substitute I into (4.3) to obtain

$$C = g_0^{ID_V d_{CA} \delta}\ mod\ n_{CA}, \tag{4.6}$$

From (4.3), (4.4), (4.5), we get

$$C^{e_{CA}\xi}\ mod\ n_{CA} = g_0^{ID_V d_{CA} \delta e_{CA} \xi}\ mod\ n_{CA} = g_0^{ID_V \delta \xi}\ mod\ n_{CA} = r_0, \tag{4.7}$$

where we used $e_{CA} \cdot d_{CA} = 1 mod\ \varphi(n_{CA})$, and, hence, (4.5) is proved.

The voting server can verify all the equations necessary in this section and again, after all the necessary checks, the voting server sends the ballot $\{Ticket, r_1, r_2, vote\}$ to the BCS for the final phase. Finally, the BSC can check for double voting using (3.38).

4.3 Security Properties Achieved By Modified Protocol

In this section, we discussed the important security properties achieved by the modified protocol as mentioned in Chapter 2.

It is worth to mention that, the modification made to the protocol preserves the security properties achieved by the initial scheme. We rely solely on the proof of these security properties given in [9]. Moreover, since we only made the protocol work by fixing the problems, the properties retain.

1) **Privacy or Confidentiality**: As mentioned in Section 2.1.1 in chapter two, this is a very important property any electronic scheme should have. The Baseri scheme achieved this with Okamoto blind signature protocol.

   There is no link between the casted vote and the information available to the AS on the voter. Therefore, it is impossible to link any voter to a particular voter with the cooperation of the AS and VS.

2) **Receipt-Freeness**: Though most of the computation is done at the voters end, it is clear that this protocol provides receipts in form of ticket but voters cannot use it to prove how he voted until the result of election is published by BSC.

3) **Unforgeability of Tickets**: let us assumed that an opponent want to forge the ticket $\{Ticket, r_1, r_2, vote\}$, it must satisfy (4.5) since the identity of the voter cannot be forged, therefore it is not possible forge the ticket.

4) **Perceptibility of double voter**: This property is important to achieve fairness and democracy. If we have a dis-honest voter who wants to cheat by voting twice with same ticket such that $\{Ticket, r_1', r_2', vote'\}$, $\{Ticket, r_1, r_2, vote\}$, the BCS can reveal the identity of such voter using (3.38) and such vote is discarded.

5) **Exactness**: Since no dishonest voter or attacker can fool the protocol we can be assured that correctness can be achieved with no consideration on invalid ballot and illegitimate voters.

Chapter 5

CONCLUSION AND FUTURE WORK

5.1 Conclusion

Thus far, we have investigated an electronic voting scheme proposed by [9] . The scheme uses Okamoto blind signature to provide security properties mentioned in Chapter 4, most especially double voting perceptibility and privacy. However, it failed due to the following reasons;

1) Selection of h_1, h_2 as generators of $\mathbb{Z}_p$ and g_1, g_2 as generators of $\mathbb{Z}_q$ by the certificate authority.
2) Selection of g_0 as generator of $\mathbb{Z}_{n_{CA}}$ which for any $n_{CA} = (p_{CA} \times q_{CA})$ does not exist.
3) Wrong use of inverse modulus used in the calculation of α made by the Voter.

Generally, because of these selections the equality to be checked by the authorities does not validate at some point, which we have shown with numerical counter examples.

We fixed these problems firstly by modifying one of the equalities such that g_0 can be selected randomly in $\mathbb{Z}_{\mathrm{n_{CA}}}$. Moreover, we included the public key of the certificate authority with random value ξ selected in $\mathbb{Z}_{\mathrm{n_{CA}}}$ in the message sent to the voting server by the voter; thus, identity of the voter is verified. Secondly, we selected $\mathrm{h_1, h_2, g_1}$ and $\mathrm{g_2}$ in $\mathbb{Z}_{\mathrm{p}}$ of order q. This way, we might have different values as exponent on both sides of the equality but shall be congruent modulus p. Thus, all equality checks become valid. Lastly, we removed d and r_0 from the message sent to the ballot-counting server by the voting server since these are not used in revealing the identity of a dishonest voter. The modifications made retained all security properties of the protocol including the double perceptibility feature.

5.2 Future Work

Since most of the computations were done on the voter's side, this might discourage the use of the system if implemented. A revised version of the protocol to have less computation on the voter's side will be encouraged. Furthermore, implementation of the modified protocol to use it in small-scale election be given a consideration.

REFERENCES

[1] 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.

[2] V. Mateu, F. Sebe & 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.

[3] B. Lee et al , "Providing Receipt-Freeness in Mixnet-based Voting Protocols," in *6th International Conference on Information Security and Cryptology (ICISC),*LNCS vol. 2971,pp.245–258, Seoul, Korea, 27-28 November 2003.

[4] 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.

[5] B. Adida, "Helios: Web-based Open-Audit Voting," in *17th USENIX Security Symposium,* San Jose, CA, pp. 335-348, July 28- August 1 ,2008.

[6] Y. Baseri, M. S. Amir & A. R. Maryam, "Double Perceptible Blind Signature Based Electronic Voting Protocol," *The ISC Int'l Journal of Information*

Security, vol. 3, no. 1, pp. 1-8, 2011.

[7] S. Brands, "Untraceable Off-Line Cash in Wallet with Observers," in *Advances in Cryptology — CRYPTO’ 93: 13th Annual International Cryptology Conference,*LNCS, vol 773, pp.302-318, Santa Barbara, California, USA, 22–26 August 1993.

[8] J. Liu, P. Tsang & D.S Wong, "Recoverable and Untraceable-Cash," in *Second European PKI Workshop,*LNCS, vol 3545, pp.206–214, Kent, England, 30 June - 1 July 2005.

[9] Y. Baseri, M. Pourpouneh & J. Mohajeri, "Double Voter Perceptible Blind Signature Based Electronic Voting Protocol," http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.215.3814, citeseerx.ist.psu.edu, 2009.

[10] Z.-Y. Wu, "An Electronic Voting Mechanism for Fighting Bribery and Coercion," *Journal of Networks and Computer Applications,* vol. 40, pp. 139-150, 2014.

[11] H. Jonker, S. Mauw & J. Pang, "Privacy and Verifiability in Voting Systems:Methods, Developments and Trends," *Journal of Computer Science Review,* vol. 10, pp. 1-30, 2013.

[12] A. Fujioka, T. Okamoto & K. Ohta, "A Practical Secret Voting Scheme for Large Scale Elections," in *Advances in Cryptology - AUSCRYPT'92,*LNCS, vol 718, pp.244-251, Queensland, Australia, 13–16 December 1992.

[13] J. Wen-Sheng, L. Chin-Laung & Y. Pei-Ling , "A Verifiable Multi-Authorities Secret Elections Allowing Abstaining from Voting," in *Proceedings on Cryptology and Information Security at International Computer Symposium,*pp.1-21, Tainan, Taiwan, December 1998.

[14] D. Josh, B. Cohen & Y. Moti, "Distributing the Power of a Government to Enhance the Privacy of Voters," in *PODC '86: Proceedings of the Fifth Annual ACM Symposium on Principles of Distributed Computing,*pp.52–62, Calgary, AB, Canada, 11-13 August1986.

[15] L. Fouard, M. Duclos & P. Lafourcade, "Survey on Electronic Voting Schemes,2007[Online].Available"*http://*wwwverimag.imag.fr/~duclos/paper/e-vote.pdf, [Accessed 02 10 2014].

[16] S. Davtyan et al, "Intergrity of Electronic Voting Systems: Fallacious Use of Cryptography," in *Symposium On Applied Computing,* Riva del Garda (Trento), Italy, March 26-30 2012.

[17] Z. Rjaskova, "Electronic Voting Schemes: PhD Thesis Comenius University Bratislava,"2002. [Online]. Available: http://people.ksp.sk/~zuzka/elevote.pdf.

[Accessed 22 09 2014].

[18] K. Kwangjo, "Experimental Design of Worldwide Internet Voting System UsingPKI,"2001.[Online].Available:http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.6.1111. [Accessed 6 08 2014].

[19] D. L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," in *Communication of the ACM,*pp. 84-90, New York, NY, USA, Febuary 1981.

[20] P. Pascal & P. David, "Efficient Public-Key Crypto-Systems Provably Secure Against Active Adversaries," in *ASIACRYPT '99: Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security,* LNCS,vol 1716, pp.165–179, Singapore, 14-18 November 1999.

[21] D. L. Chaum, "Secret-Ballot Receipts: True Voter-Verification Elections," *IEEE Security and Privacy,* vol. 2, no. 1, pp.38-47, Feb 2004.

[22] K. MacNamara & I. Iedemska, "A Survey of Electronic Voting Schemes," 14 December2012.[Online].Available:http://www.cs.ucsb.edu/~koc/ns/projects/12Reports/MacNamaraIedemska.pdf. [Accessed 26 11 2014].

[23] M. Abdul Based & S.F Mjølsnes, "A Non-Interactive Zero Knowledge Proof

Protocol in an Internet Voting Scheme," in *Norwegian Information Security Conference (NISK)*, Trondheim, Norway, pp.148-160, 24-25 November 2009.

[24] B. Kharchineh & M. Ettelaee, "A New Electronic Voting Protocol Using A New Blind Signature Scheme," in *Second International Conference on Future Networks*, pp 190-194, Sanya, Hainan , 22-24 January 2010.

[25] I. C. Lin, M. S. Hwang & C. C. Chang, "Security Enhancement for Anonymous Secure E-Voting Over a Network," *Computer Standards and Interfaces*, vol. 25, no. 2, pp. 131-139, May 2003.

[26] J. Benaloh & D. Tuinstra, "Receipt-Free Secret-Ballot Elections," in *STOC '94: 26th Annual ACM Symposium on the Theory of Computing*, Montréal, pp.544-553, Québec, Canada, , 23-25 May 1994.

[27] K. Sako & J. Killian, "Receipt-Free Mix-Type Voting Scheme-A Practical Implementation of a Voting Booth," in *Advances in Cryptology- CRYPTO'95: The 15th Annual Crypto Conference*, LNCS, vol 1361 pp.393–403, Santa Barbara, California, USA, 27-31 August 1995.

[28] R. McCallum, "Participating in Political and Public life," *Alternative Law Journal: An Australian Referred Law Journal* , vol. 36, no. 2, 2011.

[29] A. Broache, "Estonia Pulls off Nationwide Net Voting," CNET News.

[30] T. Okamoto, "Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes," in *CRYPTO' 92: Advances in Cryptography,*LNCS, vol 740, pp.31-53, Santa Barbara, California, USA, 16-20 August 1992.

[31] D. Juels, M. Luby & R. Ostrovsky, "Security of Blind Digital Signature," in *CRYPTO '97 Proceedings of International Conference on the Theory and Applications of Cryptograhy and Information Security: Advances in Cryptography*, LNCS vol 1291, pp. 150-164, Santa Barbara, California, USA, 1997.

[32] Euler, "E271 -- Theoremata Arithmetica Nova Methodo Demonstrata," *Novi Commentarii Academiae Scientiarum Petropolitanae*, vol. 8, pp. 74-104, 1763.

[33] A. G. Chefranov & A. S. Temitope, "Modification of Double Voter Perceptible Blind Signature Based Electronic Voting Protocol," *Journal of Network and Computer Applications,* Ms. Ref. No.: JNCA-D-15-00136.