Electronic Voting: An Electronic Voting Scheme using the Secure Payment card System

Voke Augoye

Technical Report
RHUL–MA–2013– 10
01 May 2013

Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX,
United Kingdom

www.ma.rhul.ac.uk/tech

Table of Contents

LIST OF FIGURES

EXECUTIVE SUMMARY

Voting is an essential part of any government. Voting in a general election is the way citizens of a nation express their opinion in selecting the best candidate to lead them. Electronic voting is the means of voting using electronic devices [1]. This concept of e-voting was introduced by Chaum in the early 1980s and since then there have been a lot of work done in this area.

Electronic voting requires a very high level of security, much higher than ecommerce. In this thesis we would discuss the security requirements of an electronic voting scheme. We would then discuss the Fujioka, Okamoto and Ohta's scheme (FOO scheme) and the GSM voting scheme and do a security analysis of these schemes against the security requirement of an e-voting scheme to show their limitations.

The financial institutions are one of the highest deplorer of cryptography, so in this thesis we would propose an electronic voting scheme using the secure payment card system. We would leverage on the authentication mechanism of the payment card system in providing an efficient and secure way of authenticating a voter to verify his eligibility and provide voter's mobility.

Finally, we do a security analysis of our scheme and show how we not only improve on the limitations of the FOO scheme and GSM mobile voting scheme but we also satisfy all the security requirements of an electronic voting scheme we discussed.

CHAPTER 1 INTRODUCTION

1.0 INTRODUCTION

Voting is an essential part of any government. Voting is the way citizens of a country express their opinion in a bid to elect the best candidate to lead the people or how the general public decides who the winner of a reality TV show should be. Voting has existed for several years and the process of voting has progressed over the years. Voting has migrated in some countries from hand ballot systems to more electronic means such as Internet voting which have been tried in pilot elections in Norway and even in actual elections like in Estonia [25] and in USA (party election in the state of Arizona in the year 2000) [1].

Electronic voting began in the early 1960's with the use of punch cards, in the 1970's optical mark sense ballot (which converts paper ballots to electronic forms) and its application in voting was being explored. In the late 1990's about 25% of voters in USA was making use of this optical mark sense voting technology [2]. The Direct Recording Electronic voting systems which has an interface that can be used in capturing votes directly has also been used in the USA after the discrepancies in the 2000 presidential elections. A lot of concerns have also been raised about the security of this DRE system, the trust placed on the underlying system and lack of audit trail which prevents it from satisfying the Verifiability property which we would talk about under security requirements [10] in section 2.2.

There have also been other concerns raised about electronic voting especially via a network such as an internet due to the inherent weaknesses of the internet and level of security of PCs as discussed in the report released by some security experts who analysed the Secure Electronic Registration and Voting Experiment (SERVE) [27] in which they said other schemes suffer from the same weaknesses. They also expressed the higher security requirements for electronic voting over E-commerce [27]and the difficulty in preventing impersonation (family member voting for another one i.e. brother voting for his sister) or someone looking over the shoulder of a voter to see how they voted since elections by remote voting are mainly unsupervised.

1.1 MY PERSONAL VOTING EXPERIENCE

In this section I talk about my experience in the Nigerian general election in 2011 from the registration phase to the tallying phase.

Registration phase: in this phase all citizens above eighteen chose a polling unit that is easily accessible to them to register. Each citizen presents their various credentials which includes a Birth certificate, passport photograph and a form of Identity (International passport, National ID card or Drivers license). The electoral officials take these documents and make copies of them. A computer is used to capture all the details (like date of birth, mother's maiden name, occupation etc.) of the citizens. There is also a device to capture the biometric details of eligible voters. In this case it was finger prints of voters that were captured. The electoral officials then feed in all the relevant details of the voters manually into a register, and then the voters sign against their names along with their thumb print.

Finally, a voter's card with some relevant details of the voters, along with an image of the voter is produced and given to each voter. This voter's card shows that you are an eligible voter that has been registered and it must be brought by each voter on the day of the election. With the image on the voter's card it would be difficult to impersonate a voter come Election Day.

ACCREDITATION: On the day of the election each voter goes to the polling centre which they did their registration if they intend to vote. It is not possible to register in one polling centre and vote in another. The accreditation process is similar to the authentication process in electronic voting where voting authorities ensure that only eligible and registered voters can take part in this exercise.

So on the Election Day each voter comes to the polling centre with their Voter's card and stand on a queue till they get accredited by the officials. The officials go through the register of registered voters, confirm the face on the voter's card matches with the voter and that on the register. If the voter is a legitimate one, the voter fills in some details in the register to acknowledge that he have been accredited. A tag with a number is then given to the voter this tag would be used in the voting phase. After all the voters have been registered, the officials now count how many voters have been accredited and announce the number to

the hearing of all parties (i.e. observers, party official and voters). Then they process progresses to the voting phase.

VOTING PHASE: In the voting phase every accredited voter stands on a queue and according to your number you know exactly what queue you should be on. The officials at this stage go through the accreditation register to confirm the tag number and details of the voter. If there are no discrepancies the voter signs and thumb prints against his details on another register called the voting register. The voters are now handed the blank ballot with the party name and symbol. The voter then proceeds to a secret ballot stand (Kiosk) to cast his vote. After choosing a candidate and thumb printing against the party which the candidate is the flag bearer, the voter then drops this ballot in a transparent ballot box. This type of secret ballot casting provides anonymity for the voter. After the last voter has voted the voting phase is ended and the election progresses to the next phase which I would call initial tallying.

INITIAL TALLYING: At this stage of the electoral process all the votes from the various ballots are collated and counted by the voting officials in the presence of voters, observers and party officials. The results are announced at the polling centre, the result sheet is completed and party officials sign to acknowledge satisfaction with the process and the results. This process of initial tallying and announcement at the polling centre was introduced because of the reported cases of ballot stuffing and theft of ballot boxes with votes when they are being transported from the various polling centres to central collating centre. These issues have led to a lot of electoral fraud over the years, hence the adoption of this process to introduce **transparency** and some level of **verifiability** to the electoral process.

At the completion of this stage the ballot boxes with the votes and result sheets are then transported to the central collating centre for the final collation, tallying and announcement of the result.

ANNOUNCEMENT: When all the ballots and result sheets have gotten the central collating centre, they are tallied, re-counted and verified. If everything checks out correctly the results are then announced to the general public and the head of the electoral commission announces the winner.

1.1.1 ISSUES WITH THIS VOTING PROCESS

This process still gives allowance for some electoral fraud, there might be inaccuracy in the tallying process, and some votes might be discredited if the voters do not thumb print correctly.

On the day of the election it was found out that a lot of registered voters did not find their names on the register for registered voters so they could not participate in the election. It appears that the register had been tampered with and some names were omitted. There were also reported cases of ballot boxes with votes missing hence they could not verify the accuracy of the results on the result sheet at the central collation centre.

Another issue with this electoral process was the low turnout of voters as compared to the number of registered voters; this issue could be attributed to the lack of mobility in the electoral process. For example a voter that works in location A decides to register in location B which happens to be his state of origin and intends to vote for a particular candidate in the elections in his community hence he registered at location B. Unfortunately, if the voter happens to be at work in location A during say the presidential election this would imply that the voter cannot exercise his franchise in an election that serious. Hence this issue of mobility is a very serious issue that has to be addressed to improve voter's participation in elections. In some countries they use the postal voting to address the voter's mobility issue but in this election which I participated in postal ballot was not an available option.

Addressing some of these election issues are part of my motivation for proposing an electronic voting scheme in this thesis.

1.2 MOTIVATION FOR THIS RESEARCH

An electronic voting system requires a higher level of security than an E-commerce system, the platform over which electronic voting is carried out goes a long way in determining the security requirements they can achieve and its practicability in actual elections. Traditional voting systems also has its shortcomings in terms of lack of Voter's mobility, flexibility,

Individual verifiability and accuracy of the tallying process due to human errors which can be addressed using an electronic voting over a secure platform. These issues have inspired this thesis in which I intend to propose an electronic voting scheme over a platform more secure than the GSM voting scheme [60] or a remote voting scheme over the internet like SENSUS [3].

1.3 OBJECTIVES OF THIS RESEARCH

1. Define the security requirements of an electronic voting scheme required for a large scale general election.
2. Analyse an electronic voting scheme against the security requirements.
3. Propose an electronic voting scheme using the Secure Payment Card system as the platform.

1.4 SCOPE OF THIS RESEARCH

Analyse the GSM electronic voting scheme which is based on the Fujioka, Okamoto and Ohta's scheme (FOO scheme) against the electronic voting security requirements then propose an electronic voting scheme using the secure payment card technology. Finally, analyse my proposed scheme against the E-voting security requirements then make recommendations for improvement of the limitations of my scheme.

1.5 STRUCTURE OF THE RESEARCH

In chapter two we do a general overview of electronic voting, we talk about the security requirements of an electronic voting scheme and schemes that provide verifiability and auditability in electronic voting. In chapter three we do a general overview and a brief

analysis of electronic voting scheme based on the 3 general models i.e. Blind signatures, Mix-nets and Homomorphic encryption models. In chapter four, we would talk about the secure payment card system and how smartcards are authenticated. We then define a few cryptographic primitives, do an overview of the schemes (FOO scheme and GSM voting scheme) which ours is based on, and then finally do a security analysis of the GSM voting scheme and its limitations.

In chapter five of this thesis our scheme which is an **electronic voting scheme based on a secure card payment technology** is proposed, an analysis of our scheme and how it satisfies the electronic voting security requirements talked about in chapter 2 is also done. In chapter six we discuss future works to be done and then conclusion.

CHAPTER 2 LITERATURE REVIEW

2.0 BACKGROUND

Over the years there has been a lot of election fraud and a steady decline in turnout of eligible voters this is part of the major drivers for the push for an electronic voting system which is believed would increase mobility and accuracy of the voting process. The wide spread deployment of the internet and use of computers is an extra reason why there has been a lot of call for the inclusion of an electronic voting system where voters can participate remotely via the internet.

There are typically three different places where electronic voting can be implemented. Two of these three are in a polling place which could either be in a precinct or a kiosk where the voter is supervised by election officials, while the third way is via the Internet which is known as Remote Internet voting where the voter is unsupervised [33]. Most of the electronic voting protocols are designed with the environment where they would be deployed and the type of voting in mind. Fig 1 below shows the different types of voting both traditional paper voting and electronic voting.

With the paper voting it could either be a paper ballot like the Australian ballot system in which the candidates name and party is printed on the ballot papers and voters can thumb print using an Ink on their preferred candidate before it is dropped in a ballot (transparent) box. This paper ballot is the type employed in the general elections in Nigeria in 2011 in which I participated. The punch card system is also based on this Australian ballot but in this case the votes are tallied using a punch card. In this thesis we would not talk much about the paper ballots and punch card voting technologies rather our focus would be on electronic means of voting either at polling places supervised by electoral officials or remotely via the internet which is unsupervised by officials.

There have been a lot of research and literature on practical e-voting systems [33] for the past 3 decades since the concept was first introduced by Chaum [4] in the early 1980s. Some of these schemes have high computational cost so they are not practical to deploy while

other schemes cannot really meet up with all the security properties required for an electronic voting scheme. In chapter 3 we would do an overview of existing literatures of electronic voting.

Although electronic voting has already been used in some real world elections i.e. in Estonia and pilot systems have been tried in other countries like Norway [25]. Even in year 2000 Arizona party elections used internet voting, the election was reported to have gone on smoothly without any security breach and there was massive participation especially amongst youth who are normally less interested in exercising their franchise [1]. Direct Recording Electronic (DRE) voting machines have also been used in USA for casting and tallying of votes.

However, there are a lot of issues related with the electronic voting especially remote internet voting. This has brought hindrances in the wide scale deployment of the existing e-voting scheme for large scale elections even with the success of the Arizona party elections and elections in Estonia.

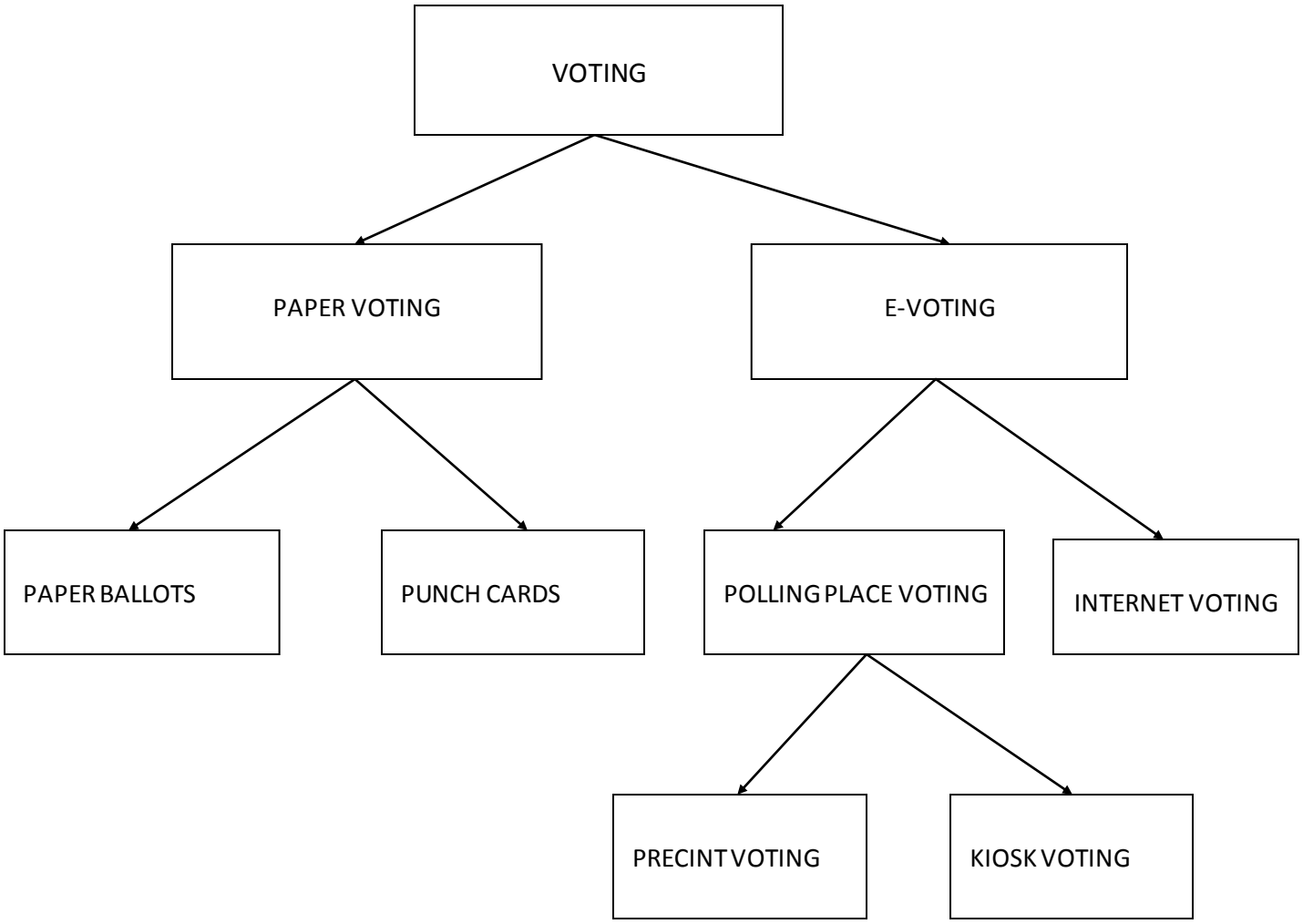

FIGURE 1: DIFFERENT TYPES OF VOTING (From [2])

2.1 ELECTRONIC VOTING

Voting has existed in communities for a long time and it's the process the populace use in expressing their political choices in a bid to elect their leaders.

In [2] the author expressed the fact that elections are very critical for the normal functioning of a society and it serves as a means where the society can express their opinions there by granting power to selected officials and also helps in building trust in the government and their support for democracy.

The traditional process of election normally depends on the trust worthiness of the election officials. This has lead to a lot of electoral fraud in elections but at the same time in some elections the election officials are actually trust worthy mainly due to segregation of duty which helps to check collusion or election officials being monitored by representatives of the various parties to ensure the electoral process is free and fair.

Voting has evolved over the years from the purely manual process to more electronic means. The use of electronic devices in voting is known as electronic voting [1]. According to [2] electronic voting should be able to ensure that the authenticity of the cast ballot can be verified and the transaction should be untraceable.

Some voting systems still use a hybrid system which is a combination of a manual process and an electronic process like the voting system used in Estonia where a voter that has already cast a vote remotely can go the polling centre and cast a paper vote which overrides the remote cast vote because priority is given to paper votes [25].

The concept of electronic voting was proposed by Chaum [4] since then there have been a lot of work done in this area some schemes proposed so far have been practical while others have been theoretical and cannot be implemented because of the computational cost amongst other issues.

Concerns have been expressed in the steady reduction of participants in election and the call for online voting to improve participation [2]. Due to the rapid growth in the use of computers and advances in cryptography there is a serious push for e-voting since a lot of people already have access to the internet [3]

Electronic voting gives elections the much desired mobility which can improve election participation. Absentee ballot systems have been present for a while this gives voters that are out of their local precinct the ability to participate in elections. The idea behind absentee ballots is what electronic voting is based on loosely speaking.

A lot of concerns have been raised over the years about the risks of using electronic voting systems considering all the possible threats they face [9,10] such as privacy issues, double voting etc.

The electronic voting system must be sufficiently robust to be resistant to different kinds of attack and it must not be too complex so that voters can understand how to use these systems and also have confidence in the system that their votes are counted because the integrity of a voting system is paramount to the integrity of any democratic system [10]

Neumann says the Direct Recording Electronic (DRE) voting machines gives no assurance that ballots cast are properly tallied and processed since it has no guaranteed audit [7]. The same concern was expressed in the CALTECH MIT voting project [8] about the need for an effective and efficient audit trail; they proposed a system using audio which they called Voters Verified Audio Audit Transcript Trail (VVAATT). They also compared their system with the Voters Verified Paper Audit Trail (VVPAT) introduced by Rebecca Mercuri in 1992 [9]. Both systems have their short comings but they both provide a means through which a voter can verify that they have chosen the correct candidate during the electoral process and an audit trail which can be used to verify that there were no discrepancies in large case of electoral fraud.

Peter G. Neumann also expresses concerns about the errors which occur during elections mainly due to operators rather than the programmers and if these errors can occur so frequently, how can we be sure intentional electoral frauds do not occur [7]. All these concerns give rise to one of the requirements for an electronic voting scheme which is **Verifiability** which we would talk more about under security requirements for electronic voting in section 2.2.

2.2 E-VOTING SECURITY REQUIREMENTS

According to [5] the way elections are conducted have the biggest impact on any society and citizens can lose trust in the system if there are any discrepancies or foul play in the electoral process, so security is very important for an e-voting system.

Electoral fraud is by default a threat to electronic voting [11] so security is very important to prevent the realisation of this threat. Electronic voting is quite different from E-commerce so requires a much higher level of security than E-commerce for example anonymity which is a strong requirement for electronic voting might not be required in an E-commerce system.

The sensitivity of the electronic voting scheme also goes a long way in determining the security requirements they need to meet, for example an electronic voting scheme needed to choose a student union president in a university or the winner of a talent show (American idols, Big Brother Africa) would not be the same as the security requirements for an e-voting scheme required for a large scale general election in a country. In this thesis my focus is on the security requirements for a large scale general election.

A lot of the proposed electronic voting schemes do not meet up with all the requirements expected for an e-voting scheme and in most cases these requirements tend to be contradictory for example individual verifiability and receipt freeness seems quite difficult to meet at the same time. This contradictory requirements is known as the electronic voting problem as discussed in [2] [28].

Below are the security requirements electronic voting protocols try to meet:

- **Privacy**: this is the security property which requires that a voter's identity should not be linked to a vote cast for example if a Voter Alice casts a vote XYZ, it should be impossible for an unauthorised 3rd party to link the vote XYZ to Alice. This means that the system shouldn't be able to reveal how the voter voted as defined in [13]. This property hence requires the voter's identity to remain anonymous [14]. This voter's privacy should be guaranteed even after the conclusion of the elections [28].

- **Democracy**: Any electronic voting protocol or system should be able to ensure that only eligible voters are allowed to vote and the protocol should also prevent the eligible voters from voting more than ones [15], this property is defined in [13] as Eligibility and in [16] as Un-reusability (i.e. a Voter cannot vote twice)

- **Receipt-freeness**: this is the property that ensures that a voter does not get any information that he could use to prove to a coercer that he voted in a certain way [13]. This property helps to prevent vote selling by eligible voters which would be the adversary in this instance. According to [17] this is the property that allows the electronic voting meet the security of the secret-ballot election offered by a traditional voting booth.

- **Verifiability**: this is the ability for anyone i.e. voters, public or external auditors, to verify or audit an election to ensure votes have been counted correctly [3] [30]. This type of verifiability is usually known as **public or universal verifiability** [12] which is a much stronger form of verifiability because verification is not limited to the particular voter that cast the vote, anyone including a passive party can observe and be convinced that the election is fair [29]. In [16] verifiability is defined as the ability to prevent falsification of voting results by anyone. According to [28] universal verifiability and accuracy can be seen as the same requirement because when you satisfy the accuracy requirement you also satisfy universal verifiability.

- **Individual Verifiability**: this ensures that there are mechanisms in place to enable a voter to verify that his vote has been counted [30] and can file a sound complaint if that is not the case without revealing the contents of the ballot. [2]. This property of an electronic voting system that voters can check that their votes have been counted and tabulated correctly is also talked about in [28] and termed Individual vote checks.

- **Robustness**: this property ensures that even if different parties collude the system should still recover from any faulty behaviour [29]. This property also means that votes cannot be included my fraudulent authorities for voters that abstain and that the systems should be resilient to any external attack such as a denial of service attack [2].

- **Fairness**: If voters already have an idea of how votes have gone before they cast their votes it may influence their decision. So this property ensures that all candidates are given a fair chance by preventing the release of any partial tally such that even counting officials have no clue about results [28] and voter's decisions are not influenced [30].

- **Accuracy**: this property requires that all valid votes should be counted correctly, invalid votes cannot be added and valid votes cannot be modified, removed or invalidated from the finally tally and if this happens it can be easily detected [28] [30] this property is defined in [16] as Correctness.

- **Uncoercibility**: this property ensures that any coercer cannot force a voter to get the value of his vote, or make the voter to cast votes in a particular way or for a particular candidate[28] [31]. Even authorities should not be able to derive the value of the vote.

Plenty proposed e-voting schemes make strong assumptions in terms of the physical conditions i.e. existence of a one way anonymous channel from authorities to voters [35] or an untappable channel [34]; based on trusted authorities [15] or the presence of a voting booth supervised by electoral officials [34]. These assumptions may determine the security requirements that may be necessary in these electronic voting schemes.

2.2.1 CONTRADICTORY SECURITY PROPERTIES OF AN E-VOTING SCHEME

It is very difficult to satisfy all the security properties of an electronic voting scheme at the same time since quite a number of them are contradictory.

Privacy requires that a voter cannot be linked with the vote he casts (Ballot), while **Verifiability** requires that an observer should be able to verify the legitimacy of the voters and the integrity of the vote cast. Achieving both properties is especially difficult because it is hard to audit an election to ensure that every vote cast was by an eligible voter without compromising the privacy of the voter and his vote.

In the same light, **Individual verifiability** requires that voters can check that their votes were included in the final tally and they have not been tampered with and this property is usually achieved by giving the voter a receipt at the end of the election to confirm this. However this receipt can now be used by coercers to ensure voters voted in a certain way or by fraudulent voters in selling votes which is contradictory to the **Receipt-freeness/Uncoeribility** property in which voters should get no proof of how they voted that they could show to a third party.

Although **Efficiency** is not a security property of an electronic voting scheme but achieving the other security properties i.e. accuracy, robustness, Universal Verifiability require the use of cryptography that have high computational demands which seriously affects the efficiency of an electronic voting scheme [2].

2.3 VERIFICATION AND AUDITABILITY

The electronic voting schemes talked about in this section focus on the verifiability property of an e-voting scheme.

Depending on the electronic voting scheme and the assumptions made the need for voter's verification might be one of the most important security property of an electronic voting scheme.

Traditional voting scheme, some electronic voting schemes in use like those in the USA, and a lot of other e-voting schemes proposed, voter's place their trust on the electoral officials, electronic voting machines, voting procedures & processes, trusted parties, certifying bodies, that the machines do what they say they do and the protocols meet up with their objectives hence their votes would be included in the final tally [18]. With the high rate of electoral fraud explicit trust cannot be placed on machine and authorities, this is the rationale behind schemes that try to provide voter's verifiability and auditability [24].

In 2004, ACM also recommended that voters should have a physical record they could check to ensure that their vote has been added to the final tally [36]. Chaum provides a

voting scheme that ensures that a voter can confirm that their vote has been included in the final tally in his paper ''A Practical Voter-Verifiable Election Scheme '' [18].

Chaum's scheme [18] maintains ballot secrecy and provides high degree of transparency using high number of cryptographic techniques and primitives from the cryptographic toolkit.

A scheme known has prêt a voter has also been proposed, these schemes aim to achieve assurance from the fact the election is auditable rather than placing trust on the system components or electoral officials [20]. The philosophy behind these schemes is end-to-end voter verifiable election where voters can verify that their votes are included in the final tally and auditors can audit every step of the voting process to detect any electoral fraud [20].

Chaum's visual cryptographic scheme [19] has inspired the prêt a voter approach and several work have been done based on this approach [21] [22] [23]. This prêt a voter schemes, a receipt is given to the voter which they can use in verifying their vote, this schemes still maintains the receipt-freeness security property because the receipts given are encrypted hence cannot be used in vote selling or buying by a coercer.

There are still other schemes which gives a code to the voter rather than an encrypted receipt as seen in [23] and compatible with the US Opscan voting system [20].

The scratch and vote scheme proposed by Ronald .L. Rivest using paper based ballots also aims at minimising trust by providing a scheme in which voters can participate in the audit process on election day before they cast their own votes and can also verify their vote has counted [24]

In [5], a scheme was proposed which provides voters with incoercible voter's verifiable receipts to satisfy the verifiability property of an e-voting scheme, they authors claim the scheme is an improvement on older schemes based on mix-nets [19] which do not scale well and can only give voters a fixed level anonymity which their scheme improves on to give voters who do not trust the system ability to control their degree of anonymity beyond the level the system provides by default.

2.4 REAL WORLD APPLICATION OF ELECTRONIC VOTING

Electronic voting has been used in quite a number of practical elections over the last decade both a pilot projects and large scale elections. In the USA electronic voting using the DRE voting machines and optical mark sense voting have been used in elections in some states.

In the US a scheme was proposed for remote voting called SERVE which allows voters to cast their votes via the internet. The idea behind this voting system was one which overseas voters and military personnel could cast their votes. This SERVE system was meant to be deployed in the 2004 primaries in their general elections in the US. Voters require a web browser such as internet explorer with certain features enabled to partake in the voting process and voters would need to have registered in their home district before they can vote remotely from any location [27]. After careful examination of SERVE by a group of security experts in 2004 the system was found to be insecure and not suitable for large scale elections considering the current state of the internet and security of computers [27]. According to [26] SERVE has some vulnerabilities like the lack of individual audit log system; online vote counting server storing both the votes and identity of voters etc.

In Estonia remote voting was used in 2005 and every citizen around the world had the opportunity to use this, it was used for their local election and parliamentary elections in 2007 [26]. Voters who have participated in remote voting via the internet in Estonia have been on the steady increase over the years from 0.9% in 2005, to 3.4 % in 2007 and in 2009 it was 9% of all the eligible voters [25].

According to [25] Norway intended to run a nationwide electronic voting in 2017 after a pilot system in 2011.

In 2003, electronic voting via the internet was also conducted in WU Vienna, this test election was done in parallel with Austrian student union election [1].

Despite all the advantages that can be gained from electronic voting such as increased participation of voters and mobility especially in remote voting the uptake of electronic voting has been slow round the world because of the difficulty in meeting with all the

required security properties, the inherent security weakness of the internet and lack of trust for e-voting system by voters. This is part of the motivation for this project.

There are three main models which most electronic voting schemes are based on the Mix-net models, the Homomorphic encryption models and the blind signature models. We explore this 3 models and schemes based on them in the next chapter.

CHAPTER 3 OVERVIEW OF ELECTRONIC VOTING SCHEMES

3.0 INTRODUCTION

In this chapter we do taxonomy to group the main e-voting schemes discussed in literature into 3 main models which is the mix-net models [4]; the Blind signature model [55]; the Homomorphic encryption model [17]. Then we do a general discussion and analysis on schemes that have been proposed over the years based on these models.

3.1 MIX-NET AND HOW IT WORKS

A mix-net is a cryptographic alternative to an anonymous channel [44]. In a mix-net used for election for example, messages which is the vote are sent from several senders to several receivers which would be the talliers via a third party (mix server) and an observer cannot tell the relationship between a particular sender and the receiver meaning that the relationship between a vote cast and the particular voter cannot be observed externally hence protecting the privacy of the voter. Below are the notations and a brief run of protocol to show how this is achieved:

We assume a PKI already exists so the taller and the mix server already have a private and public key pair.

V= voter

T=Tallier

M= Mix Server

ID_t= tallier's Identifier

PK_t= Talliers public key

PK_m= Public key of a mix server (third party).

R= Random number

The Voters prepares his ballot appends a random string to the ballot (Message) and encrypts this with the public key of the tallier who is the intended recipient[1]. The voter now appends another random string R1 to the message alongside the identifier of the tallier, this identifier enables the mix-server know who the message is intended for. The voter now encrypts this message with the public key of the Mix-server this is as described in message 1 of the protocol run.

1. $V \longrightarrow M: PK_m(R1, PK_t(R0, Message), ID_t)$

In message 2 of the protocol run the mix server decrypts the message with his private key, sees the identifier (ID_t) of the recipient which is the tallier, discards the random number R1 then forwards the new message to the Tallier.

2. $M \longrightarrow T: (PK_t(Ro, Message), ID_t)$

3.1.1 OVERVIEW OF E-VOTING SCHEMES BASED ON MIX-NETS

In 1981 Chaum introduced mix-nets [4] and each layer of a sent message from a sender i.e. Alice to a receiver i.e. Bob is decrypted by each mix-server along the way from sender to receiver and at the end an external observer cannot observe the relationship between any sender in particular and recipient. This message is first encrypted with the public key of each of the mixes [37]. This type of mix-net proposed by Chaum is a **decryption type mix-net** with simple RSA mixes.

These types of mix introduced by Chaum are not very resilient to failure on like the **re-encryption mixes** [38] which has greater resilience according to [5]. The scheme introduced by Markus Jakobsson [38] eliminates the use of zero-knowledge proof making it more efficient than previous schemes based on mix-nets [39] and also eliminates the issue of encryption of the same plaintext resulting into similar cipher text that could be detected as seen in [39] according to the author.

[1] http://en.wikipedia.org/wiki/Mix_network

There are also user centric mix-nets [40] which allow users manage their privacy requirements. In this mix-net [40] proposed by Alessandro Acquisti resilience is increased due to the collaboration in the exchange of ballot between the voters and third parties [5], although this protocol was generic but it can be applied to an e-voting scheme. At the end of the exchange of messages nobody observing can tell the relation between any particular voter and votes cast. In this scheme [40] a third party (electoral official) verifies the identity of the voter to ascertain his eligibility. The third party acts as go between the voter and the tallier, the tallier trusts the third party and believes that the eligibility of the voter and validity of the vote has been verified although the tallier and the third party (election officials) cannot link the transactions back to a specific voter [40]. After registration all the voters are given a unique token, they all simultaneously submit this unique token to the third party who now issues out another new unique token in such a way that it cannot tell which voter got which token. In this approach of mix-net the user has to pay more attention to the process and although you can achieve the anonymity and privacy property but it is not very practical because of the increased user involvement and cost by possibly sending larger amount of messages [40].

In [41] the authors proposed a scheme which improved on the chaum's mixnet [4]. According to [41] their scheme improves on the message expansion issue Chaum's mix-net scheme had because in Chaum's scheme [4] the number of MIXes increases in relation to the length of the message making it less efficient than their scheme in which the length of the message is irrelevant to the number of mixes used. In the second scheme proposed in [41], they claim they improve on chaum's scheme which provides very little level of correctness (i.e. a mix-net should ensure that an output corresponds to the input) and doesn't satisfy the fairness property meaning that if one vote is disrupted the outcome of the election can be learnt before the final tally is announced [2].

Further analysis was done on the scheme proposed in [41] and according to [42] the scheme can be attacked and secrecy of votes in the election scheme can be compromised. They proposed a countermeasure but they however did not guarantee that modifications to the protocol would make the channels or corresponding election protocol secure.

Abstractly a mix-net should achieve these 3 goals: A mix-net should ensure that the output corresponds to the input (the correctness property); an observer should not be able to link an input element to a given output element this property is known as privacy; a mix-net should be robust i.e. provide a proof that it has operated correctly which can be verified by all parties [37].

The scheme proposed in [37] aims at making mix-net robust by revealing a relation between the input and output which is selected pseudo-randomly by each mix-server as evidence of correctness in its operation. The process used in this scheme is known as "Randomised Partial Checking" [37].

According to [37] privacy is not dependent on a single server being honest like traditional mix-net schemes [4] rather it's a global property since every server reveals a portion of the relation between the input/output and even with corrupt mix-servers there is no way of connecting an input with a particular output.

In 2001 Neff [43] proposed an efficient verifiable mixing technique that can be used to achieve universally verifiable elections. Voter's credentials are mixed before the election commences rather than mixing encrypted votes (cipher texts) after the vote collection centre has received the ballots.

In [18] Chaum proposed a scheme for electronic voting where voters get encrypted receipts to verify their votes and the tellers ensure there is no link between the encrypted version and decrypted ballot receipts by performing anonymizing mixes.

Ryan and Schneider later proposed another scheme [45] which uses re-encryption mixes in the anonymizing tabulation phase instead of decryption mixes this has an advantage over the RSA decryption mix used in his earlier schemes by Chaum [4] [18] because its more tolerant to failure of any of the mix tellers and enables full independent rerun of the mixes and audit if necessary

Mayasuki Abe in [44] proposed a robust e-voting scheme based on mix-net that is universally verifiable where the amount of mix-servers does not determine the amount of work done by the verifier i.e. the work done by a verifier is not dependent on the number of mix-servers.

There have also been other literatures based on mix-nets [46] and other literatures attacking mix-nets to compromise the privacy of votes and robustness of the electronic voting system like the attacks shown in [48] which attacked the scheme proposed in [47]

3.2 WHAT IS HOMORMORPHIC ENCRYPTION

Homormorphic encryption is a form of encryption which allows specific type of encryptions to be carried on a ciphertext and obtain an encrypted result which is the ciphertext of the result of operations performed on the plaintext[2] which is the vote in an electronic voting scheme. For example one party could add two encrypted numbers and then another party i.e. voting authority that is in charge of vote tallying could decrypt the results without either of the parties being able to find the value of the individual numbers.

With homomorphic encryption there is an operation $\oplus$ defined on the message space and an operation × defined on the cipher space such that the product of the encryptions of any two votes V1, V2: Enc(V1) X Enc(V2), is the encryption Enc(V1 $\oplus$ V2) is the sum of the votes [5].

3.2.1 OVERVIEW OF E-VOTING SCHEMES BASED ON HOMOMORPHIC ENCRYPTION

In [17] Benaloh and Tuinstra proposed a scheme based on homomorphic property of a probabilistic encryption method (i.e El-Gamal) that provides the first verifiable secret-ballot election protocol that prevents vote selling and coercion. They assumed the existence of a voting booth which should help prevent coercion and the fact that voters are not given a receipt would prevent vote selling. They also proposed two protocols in this scheme one is a single authority voting protocol which does not achieve the secrecy of votes and the second

[2] http://en.wikipedia.org/wiki/Homomorphic_encryption

one which achieves vote secrecy, is a multi-authority scheme [17]. Both protocols use homomorphic encryption.

Martin hirt and Kazue sako [49] shows that the claims by Benaloh and Tuinstra that their scheme is the first receipt free scheme [17] is actually not the case because it doesn't achieve receipt-freeness. They proposed a practical receipt free-voting scheme based on homormorphic encryption with additional assumptions about the properties of the encryption function such as the decryption must be verifiable, the encryption must be infeasible to decrypt if the authorities are less than a certain number etc [49]. This scheme proposed by them also takes advantage of efficiency of the protocol proposed by Cramer, Gennaro and Schoenmaker in [50].

Cramer, Gennaro and Schoenmaker [50] proposed a scheme based on homomorphic encryption and its special properties to guarantee privacy, Universal verifiability, and robustness. This scheme uses a variant of El-gamal encryption and it is part of the security of the scheme because of the computational difficulty in solving the discrete logarithm problem in El-gamal. According to the authors their multi-authority scheme reduces the task of the voters to the bare minimum [50].

The scheme [50] achieves universal verifiability i.e. any observer can verify the final tally due to the homomorphic property of the encryption method used. The scheme also achieves privacy of votes and robustness (i.e. failure of authorities can be tolerated) by the use of threshold decryption techniques whereby the final tallying process is shared among several authorities [2].

According to [50] the communication complexity both for the individual voters and authorities is minimal making performance of the scheme optimal. However if the number of the candidates is large then it would have a relatively high computational complexity for this scheme based on El-gamal [2]. Furthermore, another downside of the scheme and other schemes based on homomorphic encryption is the limitation of the votes to YES/NO value which reduces flexibility [2] and hence makes it not very practical for large scale elections with multiple candidates or choices.

In [51] the authors proposed a new electronic voting scheme based on multiplicative homomorphormism where the votes are recovered by decrypting the product of the votes on like the other schemes [49] [17] that are based on additive homomorphomism where decryption is done on the sum of the votes. According to the authors this scheme is more efficient than previous schemes based on additive homomorphomism and also strong privacy and universal verifiability are obtained in this scheme [51].

When a multiplicative homomorphic algorithm is used to encrypt votes and a single decryption is performed on the product of the votes before factorization to recover the vote, the privacy of votes is maintained since in this scheme these actions are performed on a single vote [51]. According to [51] their scheme with multiplicative homomorphic voting maintains privacy and universal verifiability while improving efficiency.

In [53] Groth investigated four types of e-voting schemes namely: Borda Vote which is a preference vote where the best candidate receives L votes and the second L-1 votes etc; Approval vote which is any number of L candidates; Limited vote (N out of L candidates where N is the number of votes the voter can cast); Divisible vote where a huge number of vote is distributed among the candidates. They also presented some efficient non-interactive zero-knowledge (NIKZ) arguments based on homomorphic integer commitment. According to the authors [53] homomorphic threshold voting improves the efficiency of both Borda and Approval voting. In [54] the authors presented a scheme that achieves receipt freeness for the Groth's e-voting scheme since the Groth's scheme does not achieve receipt-freeness due to the ability of a voter to construct a receipt (which can be used for vote selling) by exploiting the randomness she chooses in encryption or commitment.

A lot of other schemes have been proposed based on homomorphic encryption, further details about them could be found in [6] [67] [68].

However concerns have been raised over schemes based on homomorphic encryption. In [51] it was expressed that mixing votes are said to be more efficient than homomorphic voting in elections where there are multiple choices and candidates because homomorphic voting requires each vote to be verified if not the validity of the tallying stage cannot be guaranteed hence it is restricted to YES/NO voting a similar view was also expressed in [2].

In [52] the authors compared two schemes using homormorphic encryption and mix-networks in other to achieve preferential voting. The authors [52] expressed that as the number of candidates L increases then the preferential voting system is inherently larger than the 1-out-of L (where 1 candidate is chosen out of M candidates) voting system. Hence voting system using mix-networks which we discussed in section 3.1 are more efficient because the number of candidates do not adversely affect the computational complexity on like voting systems with a form of homomorphic encryption which tend to be inefficient or not practical [52].

3.3 BLIND SIGNATURES

The concept of blind signature was introduced by Chaum in his paper "Blind Signatures for Untraceable Payment" [55] as a form of digital signature in which the message is authenticated without knowing the content of the message [5]. The signer of the message cannot derive the correspondence between signing process and the signature which is later publicly available hence making this type of signature unlinkable[3].

In electronic voting, the voter obtains a token which is a blindly signed token that only the voter knows, then the voter sends this token along with his vote to the appropriate electoral official [35].

A lot of schemes have been proposed for electronic voting using the blind signature scheme, we would consider some of these schemes in the next section.

3.3.1 OVERVIEW OF E-VOTING SCHEMES BASED ON BLIND SIGNATURES

Since Chaum introduced the concept of blind signature [55] a lot of electronic voting schemes have been proposed based on this blind signature. Fujioka A., Okamoto T., Ohta K.,

[3] http://en.wikipedia.org/wiki/Blind_signature

proposed an electronic voting scheme (FOO Scheme) based on blind signature for a practical large scale election that ensures privacy of the voters and realizes voting fairness [16]. We would talk more on this FOO scheme in a section 4.3.1 because our proposed scheme in this thesis is based on this scheme.

Other schemes have been proposed that are related to the work proposed in [16], Lorrie Faith Cranor and Cytron R.K. proposed a scheme called SENSUS [3] which is a Security-Conscious electronic polling system for the internet suitable for small scale elections but with minor modifications it can be used in large scale elections according to the authors [3]. This SENSUS also uses blind signature for security in providing privacy of voters. Both the SENSUS [3] and Fujioka's scheme [16] assume there is an anonymous communication between voters and election authorities. Both schemes also consist of a Voter, Registrar, Validator (administrator) and Tallier (counter). SENSUS has an extra central facility called a Pollster who acts as a voter's agent and performs all functions on behalf of the voters such as cryptographic functions and transfer of data functions [3] [15].

The SENSUS protocol [3] runs as follows: Voter prepares a ballot encrypts it with a secret key and blinds it. Voter signs ballot and sends to the validator. Validator verifies that the signature belongs to a registered and eligible voter that has not voted yet. Validator signs valid ballot and returns to the voter. Encrypted ballot signed by the validator is revealed to voter when the voter removes the blinding the encryption layer. The voter then sends the signed encrypted ballot to the tallier. The tallier checks the validity of the signature on the encrypted ballot and places the valid ballots on a list to be published after all voters vote. The tallier then signs the encrypted ballot and returns it to the voter as a receipt, who in turn sends the tallier the ballot decryption key upon receiving the receipt. The tallier uses the key to decrypt the ballot and adds the vote to the final tally [3].

SENSUS doesn't prevent vote selling because a voter can prove he voted in a certain way, SENSUS also satisfies individual verifiability but not universal verifiability where any interested party can verify that all votes were counted [3].

Other schemes have also been proposed based on blind signature in the past 3 decades. In 1998 Yi Mu and Vijay Varadharajan proposed two secure electronic voting schemes [56] to conduct elections over a network such as an internet based on El-gamal digital signature.

This scheme proposed meets the security requirements of an electronic voting system, it ensures privacy is maintained and it prevents double voting [56]. The scheme uses a blind signature between the Voter and Authentication Server (AS) this way the AS does not have any information on voting tickets and other parameters to be used in future voting process [56]. In 2003 the authors of [57] showed that the scheme proposed in [56] has some security flaws and that double voting which the authors believed their scheme [56] prevents is actually not the case because some voters can double vote without being detected. They now proposed a modification of the protocol used in the scheme in [56] which also comprises of three phases: The voting ticket obtaining phase, voting and ticket collecting phase, and the ticket counting phase [57]. Their scheme prevents the double voting flaw and also meets other security requirements like anonymity of voters, verifiability, correctness etc. [57]. However, in [58] the authors show that the improvement on the scheme proposed [56] by the authors of [57] allows authorities to break the anonymity requirements of an e-voting scheme hence compromising Voter's privacy because the authorities can identify the owners of the cast tickets. They now proposed a new scheme to solve this issue [58].

Another scheme was proposed in [59] that is based on the initial scheme proposed in [56], the authors looked at all the works done in [57] and [58] and according to them there is a high probability that voters would have difficulties signing voting contents. In their scheme [59] they replaced El-gamal digital signature which was used in all the previous schemes [56] [57] [58] with Digital Signature Algorithm (DSA) and RSA to generate blind signatures, this they believe would solve the aforementioned issue.

Another scheme based on the FOO scheme [16] was proposed in [60] also based on blind signatures and it uses the already existing GSM infrastructure, taking advantage of the authentication method in GSM to propose an electronic voting scheme which gives efficient, transparent and mobile authentication of voters without compromising their privacy.

In 2008 the authors of [61] proposed an electronic voting protocol based on a dual-randomized blind signature where voters get multiple receipts as a mean to provide individual verifiability while preventing coercion of or vote selling by voters because the coercer cannot tell which of the receipt is the actual vote. According to the authors their

multi-receipt concept is not theoretically perfect but it is suitable for a practical election, especially in cases where vote selling and buying in the elections are minimal. In 2010 another scheme proposed in [62] also used blind signature for authentication and XOR operations to generate votes in their multi-authority electronic voting protocol that they say is suitable for large scale elections and in 2011 another blind signature scheme with its electronic voting protocol based on elliptic curve was also designed more details about this scheme could be found in [63].

In this thesis the proposed scheme would be based on blind signature but the exact details on the type of blind signature i.e RSA blind signature or a special variant of El-gamal would be left out.

CHAPTER 4 BUILDING BLOCKS FOR OUR PROPOSED PROTOCOL

4.0 INTRODUCTION

In this thesis we are going to propose an e-voting scheme based on the secure payment card technology, in this chapter we introduce the payment card system, the various entities of the payment card technology and the means by which a smartcard is authenticated. We would then talk about the various cryptographic primitives used in the design of the FOO scheme, the GSM voting scheme and in the protocol for our proposed electronic voting scheme based on the payment card system technology. Then we move further to discuss two schemes which our scheme would be based on and their limitations.

4.1 SECURE PAYMENT CARD SYSTEM

The payment card system has been in use for quite some time and the financial sector organisatons have been the first to deploy cryptography massively after the military to provide security for information i.e. financial transactions. The card has progressed from the magnetic stripe cards to the EMV standard of cards over the years which have improved the security of the system. We assume that the smartcard in use in our proposed scheme meets the EMV specification. In our scheme we would leverage on the already existing payment card system infrastructure and the security it provides. We would also make use of the Dynamic data authentication and the online card/issuer authentication.

4.1.1 ENTITIES OF THE PAYMENT CARD SYSTEM

The payment card system is made up of four entities namely: Issuing bank, Acquirer Bank, Merchant and the Client [64] [65].

The issuing bank is the bank that the client has a relationship with i.e. an account and they issue the customer with a smart card to enable them make payment for goods and services.

The acquirer bank is the bank which has a relationship with the merchant, it enables the merchant accept card payment transactions from the client through Point of Sale (POS) machines and ATM machines.

The client is in possession of the smartcard which was issued by the card issuing bank. This smart card could either be a debit or credit card, it is tied to every customer and is used by the customer to make payment for goods and services.

The merchant is the entity selling a service or product to the client. The merchant is in control of the POS and ATM machines and has a relationship with the acquirer bank.

There is also a **Payment Card Operator** or **Scheme Operator** that do not actually issue out cards but they handle clearing and settlement between the acquirer bank and the issuing bank which enables the client and the merchant to transact [64] [65]. Figure 3 shows a diagram of a payment card system with all the entities.

4.1.2 CARD AUTHENTICATION IN PAYMENT CARD SYSTEM.

Our proposed scheme is in chapter 5 is based on the payment card system so we would make use of the card authentication mechanism already present in this system. There are basically three types of card authentication in a payment card system. The Static Data Authentication, Dynamic Data Authentication (DDA) and Combined Data Authentication (CDA). In our scheme we would focus on the Dynamic Data Authentication (DDA) but further details about SDA and CDA can be found in [64] [65].

Dynamic data authentication assumes there is already an existing PKI in place where the Scheme operator i.e. VISA acts as the Certification Authority (CA) and issues certificate to the Card Issuing Bank. The Issuer also has a Public and Private Key pair, the card has a Private and public key pair and the Scheme operator has a Private and Public key pair. The public key of the Scheme operator is stored on all the terminals controlled by the merchant. The scheme operator signs the Issuing bank's certificate which is stored on the smart card.

The Issuing bank signs the certificate of the smart card. During a transaction the terminal tries to authenticate the card to ensure that it is a valid card and alive in the transaction. So the terminal sends a randomly generated data to the card to sign. The card signs this data and returns it to the terminal, the terminal can verify this data was signed by a legitimate card because the public key of the scheme operator who is the Certificate authority is on d terminal, so with this it can verify the Card issuing bank's certificate which is on the card and can then verify the signature on the data since the card issuing bank has signed the certificate of the card [64] [65]. This process of authentication is shown in figure 2.

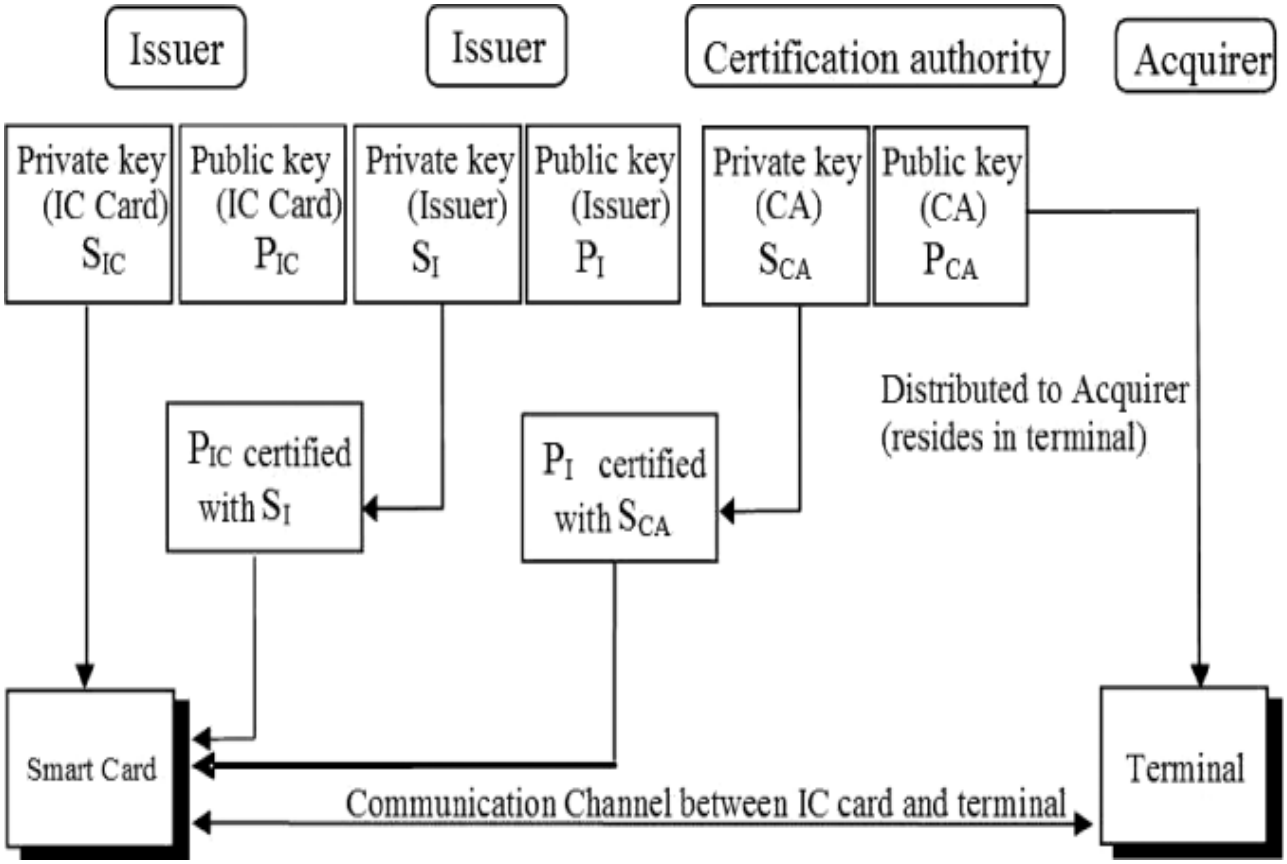

FIGURE 2 DYNAMIC DATA AUTHENTICATION. **(From [65])**

4.1.3 CARD/ISSUER AUTHENTICATION.

This is a stronger form of authentication and it would be used in the electronic voting scheme proposed in chapter 5 to authenticate the voter (smartcard) to the issuing bank which would serve as the registration and authentication centre, more on this to come in chapter 5. In this type of authentication which is done online real time, the card issuing bank authenticates the smartcard to make sure it is a legitimate card that it issued. In this card/issuer authentication the smart card and the issuing bank share a symmetric key. The terminal generates data and sends to the card. The card then computes a MAC over this data and sends back to the terminal, which then sends it to the issuing bank. The issuing bank computes a MAC over the same data and if it corresponds to the MAC value received from the smart card via the terminal then the MAC has been verified and the card is authenticated [64] [65].

4.2 HIGH LEVEL PRIMITIVES

Electronic voting is a very sensitive process that requires a very high level of security. Cryptography can be used to build in security into an electronic voting scheme. The following cryptographic primitives were used in the voting schemes we would analyse later on in this chapter and also in the design of the protocol of our proposed scheme.

4.2.1 DIGITAL SIGNATURE.

A digital signature is a cryptographic primitive that is used to provide an assurance that the message has not been altered (Integrity) and it comes from a particular signer (Data Orign Authentication). A digital signature also provides non-repudiation service which means that a signer cannot deny signing a message, and a recipient of a signed message can always present it to a third party in cases of misunderstanding to prove the origin of the message. A digital signature has a signature key which is a secret parameter known only to the signer this is what guarantees the non-repudiation service [64]. It also has a verification key which the recipient can use to verify the legitimacy of the signature. In the scheme proposed in

chapter 5 there would be extensive use of digital signature to guarantee the integrity and origin of messages.

4.2.2 THRESHOLD CRYPTOGRAPHY

In a threshold cryptosystem there is one public key which is used to encrypt the message and the private decryption key is shared between various parties (*n)* in such a way that there should be at the least a threshold of parties (t) before the message can be decrypted hence the system is called a (t,n) threshold public key encryption system [2]. In an electronic voting context the voter encrypts a vote using a Public encryption key and all the electoral authorities which should not be less than the threshold t have to corporate to decrypt this vote. If the authorities are less than ***t*** then it is infeasible to decrypt the message to get the value of the vote hence assuring privacy of the votes and accuracy of the tally [2].Threshold cryptography adds **robustness** to a voting scheme hence we apply it in the scheme proposed in this thesis.

4.2.3 BIT COMMITMENT

In electronic voting a bit commitment is a cryptographic primitive in which a voter encrypts his vote and send it to an authority in such a way that when the voter sends the authority the decryption key the authority has the assurance that the message which the voter committed to the authority should be the same as the decrypted message (Vote) [60].

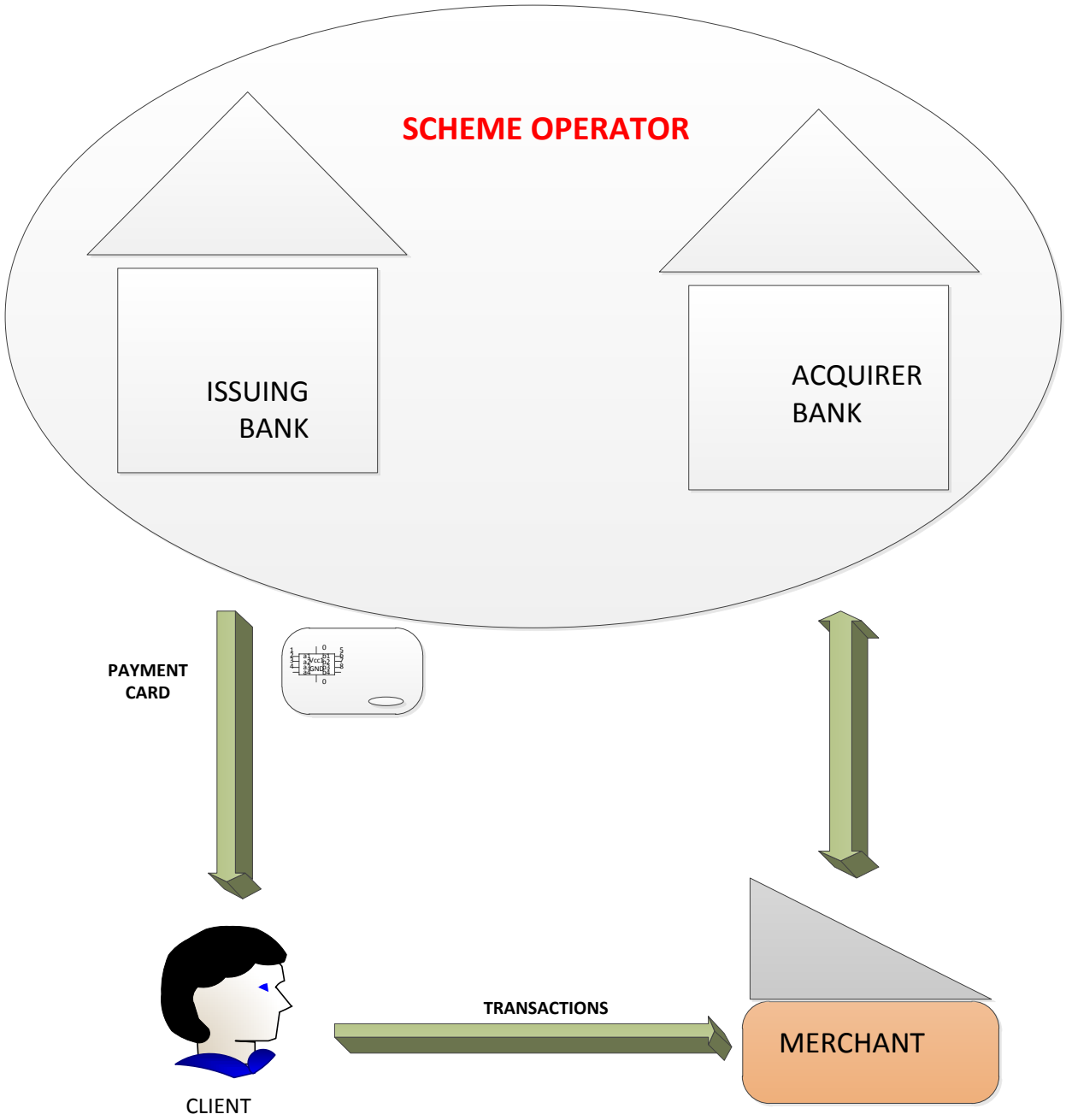

FIGURE 3 PAYMENT CARD SYSTEMS

4.2.4 BULLETIN BOARDS

In an electronic voting system a bulletin board can be used between voters and authorities to communicate. Any information posted in a bulletin board cannot be changed by another party except the party that posted it. In the proposed electronic voting scheme the electoral authorities post the final tally on the bulletin board which the voters and observers can check to have an assurance about the legitimacy of the election results.

4.3 OVERVIEW OF TWO VOTING SCHEME AND THEIR SECURITY

In this section we do a brief description of the FOO scheme [16] and the Electronic voting scheme using the GSM infrastructure [60]. We also show the limitations of the FOO scheme, then move on to do a security analysis of the GSM mobile voting scheme and show what security it offers and which security properties of an e-voting scheme it fails to meet. Our proposed scheme is an adaptation of both schemes with some improvement on the security these schemes offer.

4.3.1 FOO SCHEME

In [16] the authors proposed an electronic voting scheme based on blind signatures. The main entities of this scheme are the voters, an administrator and a counter who is responsible for vote tallying. The voter and the counter communicate through an anonymous channel, this counter can be a public board and the anonymous channel allows the communicating party to remain anonymous throughout the communication.

In this scheme [16] different cryptographic primitives were used such as digital signature as explained in section 4.2.1, blind signatures and bit commitment. Below is an outline of all the stages and processes involved in this scheme [16]:

Preparation Phase: The voter fills the ballot, using the blind signature technique, the voter blinds the message and sends to the administrator to get the administrator's signature.

Administration Phase: the administrator signs the message in which the voter's ballot is hidden and returns the signature to the voter.

Voting Phase: On receiving the ballots signed by the administrator, the voter sends it to the counter anonymously.

Collecting phase: The counter publishes a list of received ballots, this list could be published on a bulletin board for example.

Opening Phase: The voter opens his vote by sending his encryption key anonymously.

Counting phase: The counter counts the vote and announces the result.

4.3.2 LIMITATIONS OF THE FOO SCHEME

This scheme requires voters to participate at all stages of the election. The too much involvement by voter's requirement is not practical [66] especially the fact that the scheme expects voters who did not vote in the first instance to monitor the election to ensure votes were not added for them. This implies that if a voter abstains from voting a malicious authority can stuff the ballot by adding votes for voters, this violates the accuracy property of an electronic voting scheme [33].

4.4 AN ELECTRONIC VOTING SYSTEM USING GSM MOBILE ARCHITECTURE

In this section we do an overview of the GSM mobile voting scheme proposed in [60].

In [60] the scheme proposed aimed at providing a better means of authentication of voters and mobility of voters using the GSM technology. The scheme is based on the FOO scheme as discussed in section 4.3.1. The four main components of the scheme are the Voting

device which is the mobile equipment (ME), the Authentication Centre (AC), the Voting Server (VS), and the Collecting & Counting Server (CS). The Mobile Equipment in this scheme runs the voting application, key storage and generation functions [60]. The authentication centre in this scheme authenticates the voter and it is also responsible for information distribution. The Voting server issues voting token to voters after they have verified their eligibility, it is part of the voting authority that organizes the elections [60]. Finally, the Collection and Counting server is responsible for the final tallying and publishing of the votes/result.

The GSM mobile voting scheme is made up of three phases, the Pre-voting phase, the Voting phase and Post-voting phase. Below is a quick overview of the run of the protocol used in this scheme more in depth details can be found in [60].

PRE-VOTING PHASE [60]: the voter fills out a ballot by committing it using a key, encrypts the ballot then blinds it using a blind signature scheme before sending it to the authentication centre (AC). The AC then authenticates the voter, signs the ballot and sends it to the Voting Server (VS) along with its identity (i.e. $ID_{AC)}$. The VS then verifies the signature of the AC, checks the eligibility of the voter and if they have not voted already before it signs the committed and blinded ballot. The VS then sends this back to the voter which serves as the voting token (encrypted ballot signed by VS is the voting token). When the voter receives the message from VS, it unblinds it to retrieve the signed ballot by the Voting server.

VOTING PHASE [60]: The voter encrypts his key using the public key of the Counting Server (CS) and sends this to AC along with the voting token which in this protocol is the Vote. AC encrypts the Key again and sends the encrypted key with the Voting token to CS. If the voting token is valid CS generates and allocates a serial number to the voter which he sends to AC. AC then sends this serial number to the Voter along with a confirmation of the Voting exercise. The Counting server also publishes the Serial number, the completed ballot and VS's signature on the completed ballot. In cases where voters decide not to vote the voting application sends a blank ballot to the counting server on behalf of the voter

POST VOTING PHASE [60]: The Authentication Centre send sends his decryption key to the counting server to retrieve the voter's key with which he can then open the ballot. This process is done after the voting phase has been completed.

4.4.1 SECURITY ANALYSIS OF THE GSM MOBILE VOTING SCHEME

In this section we talk about how the GSM voting scheme [60] satisfies the security requirements of an electronic voting scheme.

PRIVACY: In this scheme privacy is maintained by the use of blind signature to blind the ballot so even if the Authentication centre and the Voting server collude they cannot tell the relationship between the Voter and the Vote cast. Also the voter does not communicate directly with the counting server hence CS cannot tell which voter cast which vote.

FAIRNESS: The votes are collected and counted by CS to give the final result at the end of the voting exercise when the Authentication server sends his key (which it used in encrypting the voter's decryption key which was encrypted with CS's public key) to the counting server hence TS cannot release any partial result before voting is completed making the GSM voting scheme satisfy the fairness property.

DEMOCRACY: The GSM voting scheme also satisfies this property of democracy because the Authentication centre first authenticates the voter as a legitimate voter, the Voting server also checks that the voter is eligible to vote and has not voted before signing the committed and blinded ballot (voting token) which the voter uses to vote hence preventing double voting.

VERIFIABILITY: The scheme also satisfies the weaker version of verifiability which is *Individual Verifiability* and the stronger version *Universal Verifiability.* At the end of the election the counting server publishes a list of entries on the bulletin board which includes the serial number given to each voter after voting, the committed ballot and the signature of the voting server over the committed ballot. With this serial number the voter can verify his vote has counted which satisfies the *Individual Verifiability* property. Since the Voting Server's signature is computed over the Voter's ballot and published on the bulletin board,

this enables an observer to be able to verify the signature and have an assurance that it is a legitimate signature over the ballot. The ability of an observer to verify this voting server's signature means the protocol satisfies the *Universal Verifiablity* property.

ACCURACY: If we assume that the voter monitors the list of published information after all the phases of the election and the voting application sends a blank ballot on behalf of a voter who did not vote then the scheme would satisfy the accuracy property meaning that the neither the Authentication server nor the Counting server can impersonate a voter, alter, duplicate or replace votes.

4.4.2 LIMITATIONS OF THE GSM VOTING SCHEME

In this section we talk about the limitations of the GSM voting scheme and how some security properties are violated.

First of all, instead of filling a blank ballot in the pre-voting phase since this phase is just to authenticate the voter, check his eligibility and give the voter a voting token, the ballot which the voter completes is actually the Voter's choice of candidate (the vote) and this leads to all sorts of security issues not because the voting token is the vote but for the main fact that the pre-voting phase takes place at a completely separate time from the voting phase.

RECEIPT-FREENESS: The voting token is an encrypted ballot signed by the voting server. When the voter blinds the completed ballot, he sends it through the Authentication centre to the voting server. The voting server signs this and sends back to the voter. The voter then unblinds this to retrieve the signed ballot by the Voting server. At this stage a voter can prove to a coercer what his choice of candidate is by showing him the ballot he filled, this he does by decrypting the signed ballot. The coercer can also have further assurance that this vote is legitimate since he can verify the Voting serve's signature on the ballot. Hence fraudulent voters can always sell their vote making this scheme violate the receipt-freeness property.

UNCOERIBILITY: This scheme also violates the property of uncoercibility due to the insecure platform and unsupervised process used in the GSM voting scheme. A coercer can always gather voters and coerce them to vote for a particular candidate while he watches them as they vote to gain confirmation.

FAIRNESS: This property ensures that late voters would not be influenced to vote in a certain way because of the release of partial results before the end of the final tally. If we assume that a coercer has access to large amount of voters while they are voting, and there are large amount of fraudulent voters who intend to sell their votes then the coercer can have a rough idea about how a sizeable amount of voters have voted before the final tally is announced and this would defeat the fairness property which the GSM voting scheme initially satisfies.

This is possible because at the end of the pre-voting phase a voter has access to the unblinded ballot and VS's signature to confirm the legitimacy of the vote with which the coercer can be convinced about the vote. For example if a coercer bought votes from 500 voters and it requires 600 votes to win an election. If there are 400 voters left to vote, the coercer can easily convince 100 voters to sell their vote by presenting proof of the partial results to the voters.

Accuracy: The voting application in the GSM voting scheme sends a blank ballot on behalf of the Voter if he doesn't vote. The voters are also meant to check the published list of entries to verify if their votes have been counted correctly without duplication. According to the authors of the protocol the fact that the voting application on the mobile phone sends a blank ballot on behalf of the voter stops the Counting server from adding votes for voters that abstain. In a practical scenario it would be difficult for voters to monitor each phase of the election especially voters that did not vote to check for any foul play by the voting authorities. Also, for voters that abstained we cannot always guarantee that the voting application would send a blank ballot because the voter's phone could be switched off, or out of network coverage area. It is not clear what percentage of eligible voters are likely to face this issue but the fact that this is a possibility means that there is room for the Authentication centre or the counting server to forge votes for voters that have abstained

just before voting closes. Hence under these conditions the GSM voting scheme might not satisfy the accuracy property as discussed in section 2.2

Finally the fact that the pre-voting and voting phase are done at different times and the voter has to check the published list at every stage to ensure his vote counts at the end violates the property of voting once and leaving called the **walk away** property in [2].

The scheme proposed in chapter 5 addresses most of the limitations of the GSM voting scheme [60].

4.5 CHAPTER CONCLUSION

In this chapter we talked about the secure payment card system and how the terminals use DDA to authenticate the smartcard. We then defined a few cryptographic primitives which would be used in the design of our scheme in chapter 5.

We did an overview of the FOO scheme and its limitation. Finally we discussed the GSM mobile voting scheme, did an analysis of this scheme against the security requirements of an e-voitng scheme and then showed the limitations of the scheme.

CHAPTER 5 THE SECURE PAYMENT CARD VOTING SCHEME

In this section, we introduce an electronic voting scheme using the secure payment card system as the platform. We use the secure payment card system to provide a means of authentication and voter's mobility to the voting process while providing a higher level of security than was provided in the GSM voting scheme [60]. Our proposed scheme is based on the FOO scheme and the protocol used in the GSM voting scheme discussed in section 4.3.1 and section 4.4.1 respectively.

In the following sections in this chapter we would introduce the core entities of our voting scheme; we then state a list of assumptions we make that enables the design of the protocol used. Then we do an overview of the voting scheme in very high level and go into the details of the protocol. Finally we do a security analysis of the scheme against the security properties we discussed in section 2.2 and the limitations of the scheme.

5.1 THE CORE ENTITIES SECURE PAYMENT CARD VOTING SCHEME

- **Smart Card (SC)**: this smart card contains all the information and data of the voter relevant to the voting process such as Unique Identifier of the voter (UID), cryptographic keys, random number generators and algorithms needed to carry out all the computations on behalf of the voter. The smart card is the representative of the voter and it is unique for every voter. The smart card is tamper resistant making any unauthorized retrieval of any secret information from the card that could be used to clone the card infeasible without damaging the card.

- **Registration Authority RA (Issuing Bank)**: the issuing bank is in charge of registering the voters, issuing them with a unique smart card and authentication of the card during the election. The registration authority also has an electronic registered of all registered voters. In this scheme we refer to the issuing bank as the **Registration**

Authority (RA)

- **Terminal**: the merchant controls the terminals which host the voting application. These merchants are under the control of the acquirer bank. In this scheme we assume the terminal, merchant and acquirer bank are all one and the same and we would simply just refer to them as the **Terminal**. The voting applications are installed on the terminals (i.e. the ATM machines, POS machines connected to a PC) and voters can communicate with the applications and other authorities via this terminal.

- **Voting Server VS (Scheme operator)**: in the payment card systems, this would be organisations like VISA and Master card that handle settlement and reconciliation between the acquirer bank and the issuing bank. In this scheme they act as the Voting Server and they organize the electoral process. They also act as the Certification Authority (CA), so they issue out certificates to all the Registration Authorities and their public key is installed on all the terminals. The voting server is also responsible for providing a voting ticket for the Voter.

- **Tallying Server (TS)**: they are responsible for collecting, collating, tallying, counting and publishing the final results of the election. This scheme is designed in such a way that information published by the tallying server can be audited in case of any discrepancies along the way.

5.2 PROTOCOL ASSUMPTIONS

Below are the assumptions which this scheme is based on that enable us in achieving our security objectives.

1. We assume that the proposed voting scheme is part of a voting system and voters have been registered with their correct credentials by the Registration Authority RA and issued a unique smart card.
2. We assume that the integrity of the voting application on the terminals is guaranteed and it infeasible that a malware has been installed on these devices that could change a voters choice to one of their choosing.
3. We assume there is an existing PKI and the public key of each Voting server is installed on every terminal that would be used in the voting exercise.
4. We assume that an image of every voter is on the smart card and this can be verified on Election Day by electoral officials to prevent impersonation and every voter has a PIN number which initiates the authentication process.
5. We also assume that every terminal is monitored by electoral officials to give the secret ballot property which is achieved in traditional elections by the use of a voting booth, so every voter can vote with some level of privacy without interference or someone looking over their shoulders to see how they voted.
6. We assume there are multiple tallying servers N and we require T tallying servers out of N to decrypt the votes. In this scheme we assume that T is 70% of the total number of TS i.e. if there are 10 TS we need just 7 out of this 10 to decrypt the votes.
7. We assume the terminal is under the control of the merchant and the network between the acquirer bank and the merchant is a closed network that is infeasible for an external party to eavesdrop on their communication.

5.2.1 OVERVIEW OF THE SECURE PAYMENT CARD VOTING SCHEME

In this section we do a high level overview of the voting scheme. We divide the process into four different phases: Registration Phase, The authentication Phase, The voting Phase, and The Tallying Phase. For simplicity we broke down the scheme into the Authentication phase and voting phase but in the actual protocol flow the authentication phase flows into the voting phase on like the GSM voting protocol were authentication is done in the pre-voting

phase and voting takes place at a different time as discussed in section 4.4. We also want highlight that Voter and smartcard are used interchangeably but they both mean the same thing in the run of protocol where the smartcard represents the voter

REGISTRATION PHASE: in this phase the following actions are carried out:

1. Voter goes to the Registration Authority (RA) with his legitimate credentials and RA verifies the credentials to check if the voter is eligible.
2. RA records the voter's information in the electronic voters register.
3. RA issues a unique smart card to the voter before the day of the election.

AUTHENTICATION PHASE: the following activities are carried out in this phase:

4. The voter inserts his card into the terminal which could either be an ATM machine or a POS machine connected to a PC that hosts the voting application.
5. The terminal authenticates the card using the Dynamic Data Authentication DDA [64] [65] as discussed in section 4.1.2.
6. If the card is valid, the Voter then selects the voting application using the interface provided by the terminal.
7. When the terminal realizes the transaction is Voting, it initiates an online authentication of the card which is done by the Registration Authority (RA).
8. RA sends messages to the terminal after verification of the smart card to allow the voter proceed. If the card fails the verification the process is denied and the card is ejected automatically from the terminal.

VOTING PHASE: in this phase the following activities occur:

9. The voter fills a ballot.
10. The voter encrypts the ballot
11. The voter blinds the ballot using a blind signature technique like RSA blind signature or Elgamal blind signature scheme but in this thesis we do not go into the exact cryptographic primitive used for this purpose.
12. The voter then sends this message to the Registration Authority

13. The Registration Authority which has already authenticated the card signs the message and sends it to the Voting Server.
14. The Voting Server verifies the signature of RA, this gives it assurance that the voter has been authenticated by RA.
15. The Voting Server checks the Voter's register which has details of all votes cast to see if the Voter has voted before. If yes, the vote is discarded and the process is ended, this prevents double voting.
16. If the voter hasn't voted VS signs the message and sends back to the voter VIA the registration Authority and the terminal.
17. VS adds the voter's identity and the blinded committed ballot to the electronic voters register with this VS can tell which voter has voted and uses it to prevent double voting.
18. The voter which is the Smartcard unblinds this message to retrieve the signed encrypted ballot by VS this is the **Voting token**.
19. Before the voter casts his vote the applications prompts the voter to proceed with his choice or make another choice, this option is included in this scheme to give the voter an opportunity to chose another candidate just in case they haven't made up their mind as at when filling the ballot or they made a mistake by selecting the wrong candidate in the original ballot filled making this scheme a bit flexible.
20. The voter then sends the voting token to the tallying server or an encrypted ballot along the voting token in situations where the voter makes a different choice.
21. The voter encrypts his decryption key with the public key of the Tallying server and sends to the Registration Authority, he does this to prevent RA from decrypting the message to see how he voted.
22. The Registration Authority then encrypts the encrypted key with his own Key and sends this along with the voting token to the Tallying server.
23. When TS receives the voting token and the encrypted key, TS verifies the authenticity of the voting token.
24. TS allocates a unique number to the voter.
25. TS sends this unique number along with a confirmation that a vote has been received to the voter via RA.

26. RA has details of the voter like phone numbers, email address etc with which it forwards this confirmation to the voter.
27. TS publishes this unique number, the committed ballot, the voter's key encrypted using TS's public key and the voting token which is the encrypted ballot signed by VS.

TALLYING/ANNOUNCEMENT PHASE:

28. RA sends his decryption key to TS
29. The tallying server decrypts the encrypted key to reveal a cipher text which is the voters decryption key encrypted with TS's public key
30. TS use threshold cryptography to decrypt the cipher text to obtain the voter's decryption key.
31. TS opens the ballot using the voter's decryption key.
32. The tallying server counts the vote and announces the result.

5.3 THE SECURE PAYMENT CARD VOTING PROTOCOL

In this section we take a more detailed look at the voting protocol used in this e-voting scheme using the secure payment card technology. First we define the notations used in this protocol, and then we give the full protocol run with explanation of every message.

5.3.1 NOTATIONS OF THE PROTOCOL

SC:	Smartcard/Voter
||:	Concatenation
ID_X:	Entity X identifier
v_i:	Vote/Ballot
$E_K(m)$:	Encryption of message m using key K
$MAC_K(M)$:	Message Auth Code on Message M using key K

R_X: Random data from entity X

$Sig_X[m]$: X's Signature on message m

$B(v_i,r_i)$: Blinding technique for message v_i using a random blind factor r_i

$U(s,r_i)$: Unblinding technique of message s using a random factor r_i

$PK_X(M)$: encryption of message M using X's public key

$Commit(v_i,k)$: Bit commitment scheme for message v_i using key k.

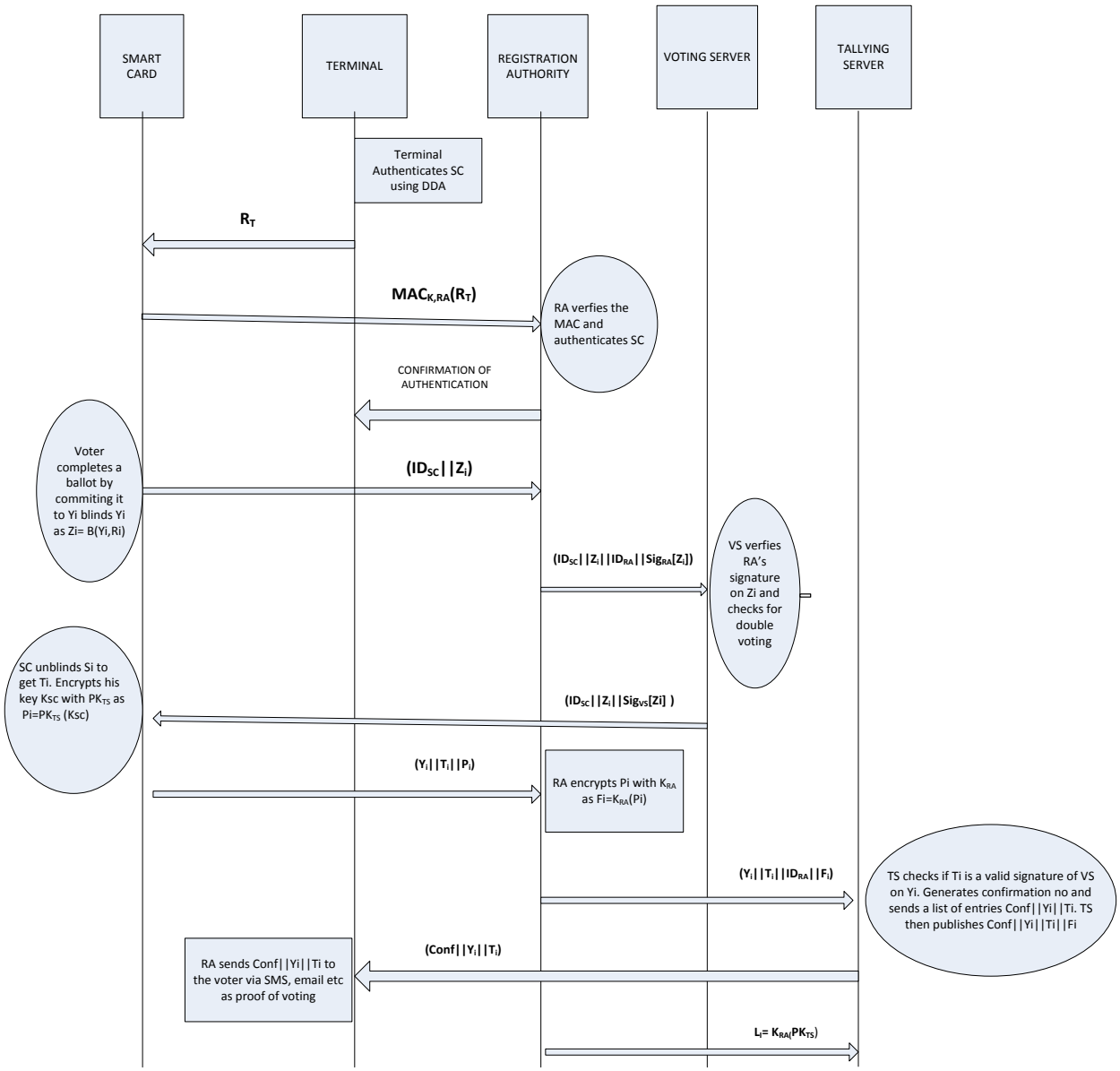

FIGURE 4 SECURE PAYMENT CARD VOTING SCHEME

5.3.2 THE PROTOCOL MESSAGES

This protocol is divided into three phases the Authentication phase, Voting phase and Tallying phase the flow of messages between the various entities as shown in figure 4 is explained below.

THE AUTHENTICATION PHASE

1. **T → SC: R_T**
2. **SC → RA: $MAC_{K,RA}(R_T)$**

After the terminal (T) has authenticated the card using DDA, in message (M) 1 the terminal generates a random data R_T and sends to the card (SC). In M2 SC computes a MAC over the random data R_T and sends to RA. RA and SC share a symmetric key K with which RA can verify the MAC and SC is authenticated.

THE VOTING PHASE: The voter fills in a ballot which appears on the interface provided by the terminal. The SC completes the ballot by committing it to **$Y_i = Commit(v_i, k_{sc})$,** where k_{sc} is a randomly generated key by the smartcard. The SC Blinds Y_i using the blinding function of a blind signature scheme with a randomly chosen blind factor r_i i.e. **$Z_i = (Y_i, r_i)$**

3. **SC → RA: $(ID_{SC} || Z_i)$**
4. **RA → VS: $(ID_{SC} || Z_i || ID_{RA} || Sig_{RA}[Z_i])$**
5. **VS → SC: $(ID_{SC} || Z_i || S_i)$**

In M3, SC sends message Z_i which is a committed and blinded ballot to RA along with his Identity ID_{SC}, RA checks the electronic voting register to make sure SC is eligible to vote. RA then signs the committed and blinded ballot Z_i. RA does not know the link between the voter's identity ID_{SC} and the Vote V_i because of the blind signature applied to the ballot by SC this helps to preserve the privacy of the vote.

In M4, RA sends VS the committed and blinded ballot Z_i along with his signature on Zi as **$(Sig_{RA}[Z_i])$** and both identifiers for the SC and RA (i.e. ID_{SC} and ID_{RA}). VS verifies RA's signature on Z_i i.e. **$(SIG_{RA}[Z_i])$** with which VS gains assurance that RA has authenticated SC. RA then

checks the voter's register to see if the voter has voted before this check is to prevent SC from voting twice.

VS signs the committed and blinded ballot Zi as $\mathbf{S_i = Sig_{VS}[Zi]}$ and in M5 VS sends the voter's Identifier ID_{SC}, Z_i, and S_i to SC.

On receipt of message 5, SC unblinds S_i with the same blinding factor r_i as $\mathbf{T_i = U(S_i, r_i)}$ to retrieve VS's signature on the encrypted ballot Y_i which SC can now use as the Voting token T_i. VS then updates the Voter's register with $\{ID_{Sc}, Z_i, S_i\}$ this enables it know the identities of all the voters that have voted.

SC then encrypts his key K_{sc} with the public encryption key of the tallying server as $\mathbf{P_i = PK_{TS}(K_{SC})}$. With this RA cannot decrypt the message using K_{SC} to recover the vote V_i hence preserving the privacy of the vote.

6. **SC → RA: $(Y_i || T_i || P_i)$**
7. **RA → TS: $(Y_i || T_i || ID_{RA} || F_i)$**

In message 6 SC sends the committed ballot Yi, the Voting token Ti which is the vote cast by the voter and Pi (Voter's key encrypted with TS's public key) to RA. RA then encrypts Pi as $\mathbf{F_i = K_{RA}(P_i)}$.

In M7 RA then sends $(Y_i || T_i || ID_{RA} || F_i)$ to the Tallying Server TS. TS confirms if T_i is a valid signature of VS on the encrypted ballot Y_i.

Note that SC does not communicate directly with TS, TS can only confirm that Ti is a valid voting token and trust that the other authorities VS, RA have correctly authenticated the voter hence TS does not have any link between the voter's identity ID_{SC} and the Vote V_i, so the voter's anonymity cannot be compromised by TS.

8. **TS → RA: $(Conf || Y_i || T_i)$**

In M8 TS sends $(Conf || Y_i || T_i)$ to RA after TS generates a unique number (Conf) which is a confirmation that the voter has voted successfully. RA which has all the details of the voter then sends $(Conf || Y_i || T_i)$ VIA email, mobile phone number etc. to the voter as a

confirmation that their vote has been received by TS. TS then publishes (Conf||Y_i||T_i||F_i) on the bulletin board.

TALLYING PHASE:

9. RA →TS: L_i

At the end of the voting phase, in M9 RA sends TS his key encrypted with TS's public key as $\mathbf{L_I = K_{RA}(PK_{TS})}$, TS decrypts the message L_i to obtain K_{RA}. TS then use K_{RA} to decrypt F_i which it received in M7 in the voting phase to get P_i. TS with threshold cryptography which requires t-out-of-N authorities present now use their private key to decrypt P_i to obtain K_{SC}. When TS gets K_{SC} they can now open all the votes and count them. TS can be sure that K_{SC} is a valid key and V_i is a valid vote since they were committed by SC at the beginning of the voting phase.

5.3.3 SECURITY ANALYSIS OF THE SECURE PAYMENT CARD VOTING SCHEME

In this section we would analyse the secure payment card voting scheme against the security properties we discussed in section 2.2 and show how our protocol satisfies those properties.

INDIVIDUAL VERIFIABILITY: at the end of the voting phase the voter is sent (Conf||Y_i||T_i) by the Registration Authority with which the voter has assurance his vote has counted. The voter can also compare this list of entries with the list of entries (Conf||Y_i||T_i||F_i) published on the bulletin board by TS as a means of gaining further assurance that his vote has been included in the final tally. Hence this scheme satisfies the individual verifiability property

UNIVERSAL VERIFIABILITY: as seen in the GSM voting scheme [60], in the secure payment card voting scheme any observer can check the entries published on the bulletin board by TS and verify that T_i is a valid signature of VS on Y_i hence satisfying the universal verifiability property as discussed in section 2.2.

DEMOCRACY: this property ensures that only eligible voters can vote and they cannot vote more than ones. In this scheme the SC is authenticated by RA if SC can compute a legitimate MAC over the random data generated by the terminal. RA has an electronic register of all eligible voters which it confirms from to see if the voter has been registered. If the voter cannot compute the correct MAC and is not on the register then the voter is denied from continuing with the voting process. In the voting phase the VS updates the voter's register with a list of entries $\{ID_{SC},Z_i,S_i\}$, with this entries VS can verify if a voter has voted before and can prevent double voting. Hence this protocol satisfies the democracy property.

UNCOERCIBILITY: in this scheme the voter goes to a precinct which has a terminal to vote, this precincts are monitored by electoral officials, so on like the GSM voting scheme [60] which is unsupervised, a coercer cannot watch a voter when he votes in the secure payment card voting scheme, meaning that the coercer has no way of telling how the voter voted hence the scheme satisfies the uncoerciblity property of an e-voting scheme section 2.2.

FAIRNESS: This property ensures that there is no partial release of results that could influence voter's decision. In our scheme the voter encrypts his key using the public encryption key of the tallying server as $\mathbf{P_i=PK_{TS}(K_{SC})}$ and sends this in M6 to RA i.e. SC→RA: $(Y_i||T_i||P_i)$. RA the encrypts Pi with his own key as $F_i=K_{RA}(P_i)$ and forwards RA→TS: $(Y_i||T_i||ID_{RA}||F_i)$ which is M7 in the run of protocol. At the end of the voting phase when all the voters have voted RA sends his key to TS so that TS can obtain the voter's key K_{SC} with which TS can then open the votes. This scheme satisfies the fairness property because TS can only reveal the votes after all votes have been cast because that's when TS gets the voter's key, so even if TS is fraudulent he cannot compromise the election.

RECEIPT-FREENESS: this is the property that ensures that voters do not get any information at the end of the election to prove to a coercer he voted in a certain way [13]. In this

scheme when the voter finishes voting the terminal only tells the voter that his voting was successful, the voter does not get any receipt to show how he voted. Although, RA sends the voter a list of entries (Conf$||Y_i||T_i$) but Yi and Ti which represent the committed ballot (which is the encrypted ballot) and the voting token (which is VS's signature on the encrypted ballot) respectively are not in any format that a coercer can make sense out of it. The secret parameters (i.e. encryption key) used in carrying the cryptographic computations on the ballot are stored in the tamper resistant smart. So it is infeasible for a coercer to retrieve these secret parameters from the smart card and decrypt the ballot to see how he voted. Hence even if the voter is fraudulent he cannot convince a coercer he voted in a certain way, so our scheme satisfies the receipt-freeness property.

PRIVACY: this property ensures that a voter's identity is not linked to a vote he cast. In this scheme the voter never sends his key in the clear, he sends his key K_{SC} encrypted with TS's public key to RA, so RA cannot decrypt Y_i which is the committed ballot to tell the link between the voter's identity ID_{SC} and the vote V_i hence RA cannot compromise the voter's privacy at this stage.

Also, in M8 of the protocol, RA sends ($Y_i||T_i||ID_{RA}||F_i$) to TS, TS does not communicate directly with SC, meaning TS does not know which voter cast which vote. In this scheme, VS only signs a committed and blinded ballot Z_i from SC, so VS cannot tell what V_i is since SC blinds the committed ballot Y_i hence privacy of the scheme is protected because all the authorities cannot tell the relationship between ID_{sc} and V_i.

ACCURACY: in this scheme all computations are done by SC on behalf of the voter which stores all the secret parameters. If a fraudulent RA generates Z_i and tries to impersonate an abstaining voter by sending M4-($ID_{SC}||Z_i||ID_{RA}||Sig_{RA}[Z_i]$) to VS. When VS receives M4, signs Z_i as ($SIG_{VS}[Z_i]$), VS sends M5 ($ID_{SC}||Z_i||S_i$) directly to the voter, which by this time should have inserted his smartcard SC in the terminal. Since we assumed the network between the merchant and the acquirer bank is a closed network then RA cannot intercept

M5 and would be unable to generate T_i on his own. Without Ti which is the voting token RA cannot send M7 ($Y_i||T_i||ID_{RA}||F_i$) to TS hence RA cannot forge, duplicate or replace a vote.

Furthermore, TS cannot forge a vote for a voter because it would require the signing key of VS to be able to construct a valid voting token T_i which is part of the entries published on the bulletin board and in this scheme any observer can verify from the bulletin board if T_i is a valid signature of VS over Y_i, hence our scheme satisfies the accuracy property because even a fraudulent TS and RA cannot forge, replace or duplicate votes.

ROBUSTNESS: in this scheme the voters go to a precinct which has a terminal to vote, these precincts are monitored by electoral officials. The terminals only accept a smartcard at a time, in the tallying phase TS uses threshold cryptography to decrypt P_i to obtain the voter's key with which TS can open all the votes. So even if one out of the t-authorities is legitimate and voters conspire they cannot disrupt the election and its outcome hence our scheme is robust (as discussed in section 2.2).

WALK AWAY PROPERTY [2]: this property ensures that a voter votes once and leaves. Our scheme satisfies this property because voting is a one off process where the voter inserts his smartcard into the terminal and completes the authentication and voting phase before ejecting his smartcard and leaving on like in the GSM mobile voting protocol [60] where the different phases are done at different times and the voter has to be involved in all various phases.

5.3.4 LIMITATIONS OF THE SECURE PAYMENT CARD VOTING SCHEME

At the end of the voting phase RA has knowledge of all these entries <Conf,ID_{SC},Z_i,Y_i,T_i,P_i>,VS has knowledge of <ID_{SC},Z_i,S_i> and TS knows <Conf,Y_i,T_i,F_i,L_i> in the tallying phase. Knowledge of all this entries means that if RA and TS collude they can reveal the link between ID_{SC} and V_i which would compromise the voter's privacy.

Also, if RA decides to send $P_i=PK_{TS}(K_{SC})$ to TS before the election closes then if all t TS are corrupt, then they could decrypt P_i using threshold cryptography get the voter's key. With the voter's key K_{SC} they can then open the votes and release a partial result which would violate the fairness property of an electronic voting.

Our scheme relies on the trust we place on each of these authorities not to collude with one another, if this trust is broken it could lead to a compromise of the privacy and fairness property of our scheme.

5.4 CHAPTER CONCLUSION

In this chapter we talked about an electronic voting scheme using the secure payment card technology. We did an overview of the scheme, we then went on to give a more detailed view of the protocol and the messages exchanged between the various entities. After which we analyzed the scheme and showed how we satisfy the security properties of an e-voting scheme. Finally we discussed the limitations of the scheme.

In the next chapter we would discuss future works that need to be done on our scheme and then give a final conclusion.

CHAPTER 6 FUTURE WORKS AND CONCLUSION

6.0 FUTURE WORKS

Firstly, in this thesis we used high level cryptographic primitives like digital signatures, encryption algorithms, public key cryptography, blind signature schemes, bit-commitments and threshold cryptography however in actual implementation the exact type of cryptographic primitive used goes a long way in determining the efficiency and security requirements of the scheme our scheme can satisfy. Hence in future works more details should be given about the exact primitives and how they enhance the overall security and practicability of the scheme.

In the secure payment card voting scheme we proposed in this thesis we saw that the trust place on the various authorities especially the trust placed on the Registration Authority (RA) could lead to RA colluding with TS to reveal the identity of the voter there breaching the privacy requirement. We also discussed in section 5.3.4 the risk our scheme stands if RA decides to release the voter's secret key to TS before the voting phase finishes.

However, our trust assumptions addresses these risks since we assumed RA is trusted, so further work has to be done to investigate and propose ways of reducing the trust placed on the authorities especially on the registration authority RA.

Furthermore, a formal analysis on the protocol has to be done to investigate how feasible it is that our protocol works and actually satisfies the objectives of the voting scheme.

We also need to investigate how long it would take each voter to complete the voting process and if it is an acceptable time in a real world election with large amount of voters.

Finally, further works need to be done in designing and incorporating extra protocols into the existing one to cater for elections where voters need to vote for multiple candidates at various levels of the government (for example a voter needs to vote for candidate X for presidency, Y for senate and Z for governor of a state etc.) at a go without having to vote individually for every candidate at separate times.

6.1 CONCLUSION

In this thesis we did an overview of the existing literature on electronic voting. We discussed the security requirements of electronic voting and highlighted the contradiction in some of these requirements. We then looked at two voting schemes the FOO scheme [16] and the GSM mobile voting scheme [60] which is based on the previous. We did an analysis of both schemes and showed their limitations. We especially showed that the GSM voting scheme under certain conditions do not satisfy the security properties which they claimed to have satisfied.

We then went further to propose an electronic voting scheme based on the secure payment card technology. We showed how our scheme uses the Dynamic Data Authentication and card/issuer authentication of the payment card system to authenticate a voter's smartcard SC and this authentication enhances voter's mobility since voter's can now vote any where provided there is an available terminal that is part of the that is part of the voting system.

We then analyzed our scheme (which although uses a similar protocol with the GSM mobile voting scheme [60]) and showed how we satisfied the security requirements of electronic voting.

Finally we discussed limitations of our proposed scheme and suggested further works that should be done to address them.

BIBLIOGRAPHY

1. Baldersheim, H. & Kersting, N. (Ed). "Electronic voting and democracy: a comparative analysis". Palgrave Macmillan, New York. 2004

2. Gritzalis, D. "*Secure Electronic Voting*". Boston, Mass: Kluwer Academic, 2003.

3. L. Cranor and R. Cytron. Sensus: A security-conscious electronic polling system for the Internet. In Proceedings of the Hawaii International Conference on System Sciences. Wailea, Hawaii, 1997.

4. Chaum,D. "Untraceable Electronic Mail, Return Address and Digital Pseudonyms", Communications of the ACM, Vo1.24, No.2, February 1981, pp.84-88

5. Thomas E. Carroll, Daniel Grosu. "A secure and anonymous voter-controlled election scheme". Journal of network and computer applications [1084-8045] Carroll yr: 2009 vol:32 iss:3 pg:599. 2009

6. Keshk, A.E.; Abdul-Kader, H.M.; , "Development of remotely secure e-voting system," Information and Communications Technology, 2007. ICICT 2007. ITI 5th International Conference on, vol., no., pp.235-243, 16-18 Dec. 2007 doi: 10.1109/ITICT.2007.4475655
   URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4475655&isnumber=4475588

7. Neumann ,P.G. "Risks in Computerized Elections (Inside Risks)". Comm. ACM 33, 11, p. 170, November 1990.

8. Cohen, S. "Auditing technology for electronic voting machines". Undergraduate thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 2005.

9. Mercuri, R. "Physical Verifiability of Computer Systems," 5th International Computer Virus and Security Conference, March, 1992.

10. Kohno, T.; Stubblefield, A.; Rubin, A.D.; Wallach, D.S.; , "Analysis of an electronic voting system," Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on , vol., no., pp. 27-40, 9-12 May 2004 doi: 10.1109/SECPRI.2004.1301313\

    URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1301313&isnumber=28916

11. Aditya, Riza, Boyd, Colin, Dawson, Edward, & Lee, Byoungcheon (2004) "Implementation Issues in Secure E-Voting Schemes". In Kozan, E (Ed.) Proceedings of Abstracts and Papers (On CD-Rom) of the Fifth Asia-Pacific Industrial Engineering and Management Systems (APIEMS) Conference 2004 and the Seventh Asia-Pacific Division Meeting of the International Foundation of Production Research, 12-15 December 2004, Gold Coast, Australia.
This file was downloaded from: http://eprints.qut.edu.au/25538/

12. Schoenmakers, B. "A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting". In Advances in Cryptology—CRYPTO '99, Vol. 1666 of Lecture Notes in Computer Science, Springer-Verlag, 1999. pp. 148-164.

13. Delaune, S., Kremer, S. and Ryan, M. D. (2006) "Verifying Properties of Electronic Voting Protocols", In Proceedings of IIAVoSS Workshop On Trustworthy Elections (WOTE'06), Cambridge, UK, pp. 45-52.

14. Jinn-Ke Jan; Yu-Yi Chen; Yi Lin; , "The design of protocol for e-voting on the Internet," Security Technology, 2001 IEEE 35th International Carnahan Conference on , vol., no., pp.180-189, Oct 2001 doi: 10.1109/.2001.962831
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=962831&isnumber=20784

15. Karro, J.; Wang, J.; , "Towards a practical, secure, and very large scale online election," Computer Security Applications Conference, 1999. (ACSAC '99) Proceedings. 15th Annual , vol., no., pp.161-169, 1999 doi: 10.1109/CSAC.1999.816024
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=816024&isnumber=17686

16. Fujioka, A., Okamoto, T., and Ohta, K. "A practical secret voting scheme for large scale elections". In Advances in Cyptology - AUSCRYPT '92 (Berlin, 1993), J. Seberry and Y. Zheng, Eds., vol. 718 of Lecture Notes in Computer Science, Springer-Verlag, pp. 244–251.

17. Benaloh, J. and Tuinstra, D. "Receipt-free secret-ballot elections," Proceedings of the 26th ACM Symposium on the Theory of Computing, 544-553, 1994.

18. David Chaum, Peter Y.A. Ryan, and Steve Schneider." A Practical Voter-Verifiable Election Scheme". S. De Capitani di Vimercati et al. (Eds.): ESORICS 2005, LNCS 3679, pp. 118–139, 2005._c Springer-Verlag Berlin Heidelberg 2005

19. Chaum, D.; , "Secret-ballot receipts: True voter-verifiable elections," Security & Privacy, IEEE , vol.2, no.1, pp. 38- 47, Jan.-Feb. 2004 doi: 10.1109/MSECP.2004.1264852
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1264852&isnumb

er=28290

20. Ryan, P.Y.A.; Bismark, D.; Heather, J.; Schneider, S.; Zhe Xia; , "PrÊt À Voter: a Voter-Verifiable Voting System," Information Forensics and Security, IEEE Transactions on , vol.4, no.4, pp.662-673, Dec. 2009 doi: 10.1109/TIFS.2009.2033233
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5272310&isnumber=5312765

21. Zhe Xia, Steve A. Schneider, James Heather, and Jacques Traor. "Analysis, improvement and simplification of Prêt à voter with Paillier encryption". In Proceedings of the conference on Electronic voting technology (EVT'08). USENIX Association, Berkeley, CA, USA, , Article 13 , 15 pages.2008

22. Peter Y. A. Ryan. "A variant of the Chaum voter-verifiable scheme". In Proceedings of the 2005 workshop on Issues in the theory of security (WITS '05). ACM, New York, NY, USA, 81-88. DOI=10.1145/1045405.1045414
http://doi.acm.org/10.1145/1045405.1045414

23. D. Chaum, R. Carback, J. Clark, A. Essex, S. Popoveniuc, R. L. Rivest, P. Y. A. Ryan, E. Shen, and A. T. Sherman, "Scantegrity II: End-to-end verifiability for optical scan election systems using invisible ink confirmation codes,". In Proc. 3rd USENIX/ACCURATE Electron. Voting Technol. Workshop (EVT'08), San Jose, CA, 2008.

24. Ben Adida and Ronald L. Rivest. 2006." Scratch & vote: self-contained paper-based cryptographic voting". In Proceedings of the 5th ACM workshop on Privacy in electronic society (WPES '06). ACM, New York, NY, USA, 29-40

25. Chowdhury, M.J. "Comparison of e-voting schemes: Estonian and Norwegian solutions". 2010.
URL: http://courses.cs.ut.ee/2010/security-seminar-fall/uploads/Main/chowdhury-final.pdf

26. Ahto Buldas., Triinu Mägi. "Practical Security Analysis of E-voting Systems". In Proceeding IWSEC'07 Proceedings of the Security 2nd international conference on Advances in information and computer security, Springer-Verlag Berlin Heidelberg 2007. Pages 320-335.

27. Jefferson, D., Rubin, A.D., Simons, B., Wagner, D. " A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)". January 2004.

28. Cetinkaya, O.; , "Analysis of Security Requirements for Cryptographic Voting Protocols (Extended Abstract)," *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on* , vol., no., pp.1451-1456, 4-7 March 2008
doi: 10.1109/ARES.2008.167

URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4529515&isnumber=4529303

29. Ronald Cramer., Matthew Franklin., Berry Schoenmakers., Moti Yung. "Multi-Authority Secret Ballot Elections with Linear Work". In Advances in Cryptology EUROCRYPT'96, Vol. 1070 of Lecture Notes in Computer Science, Springer-Verlag, 1996. pp. 72-83

30. Anane, R.; Freeland, R.; Theodoropoulos, G.; , "e-Voting Requirements and Implementation," *E-Commerce Technology and the 4th IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services, 2007. CEC/EEE 2007. The 9th IEEE International Conference on* , vol., no., pp.382-392, 23-26 July 2007 doi: 10.1109/CEC-EEE.2007.42
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4285237&isnumber=4285176

31. M. Burmester, and E. Magkos, "Towards secure and practical e-elections in the new era", Information Security - Secure Electronic Voting, Kluwer Academic Publishers, 2003 pp. 63-76.

32. California Internet Voting Task Force. "A Report on the Feasibility of Internet Voting", January, 2000. Available at:
http://www.sos.ca.gov/elections/ivote/final_report.pdf

33. Cetinkaya, Orhan; Doganaksoy, Ali; , "A Practical Verifiable e-Voting Protocol for Large Scale Elections over a Network," Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on , vol., no., pp.432-442, 10-13 April 2007. doi: 10.1109/ARES.2007.15
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4159833&isnumber=4159774

34. Tatsuaki Okamoto, "Receipt-Free Electronic Voting Schemes for Large Scale Elections", Proceedings of the 5th International Workshop on Security Protocols, p.25-35, April 07-09, 1997

35. Bo Meng; , "An Internet Voting Protocol with Receipt-Free and Coercion-Resistant," Computer and Information Technology, 2007. CIT 2007. 7th IEEE International Conference on , vol., no., pp.721-726, 16-19 Oct. 2007
doi: 10.1109/CIT.2007.23
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4385170&isnumber=4385041

36. ACM. ACM statement on voting systems. Communication ACM. 2004

37. M. Jakobsson, A. Juels, and Ronald L. Rivest. “Making mix nets robust for electronic voting by randomized partial checking”. In the proceeding of USENIX ’02, 2002: 339–353.

38. M. Jakobsson. “Flash mixing”. In Proceedings of the 18th ACM symposium on principles of distributed computing (PODC ’99). New York: ACM; 1999. p. 83–9.

39. M. Jakobsson, “A Practical Mix,” Eurocrypt 1998, pp. 448-461.

40. Acquisti A. “A user-centric MIX-net protocol to protect privacy”. In Proceedings of the workshop on privacy in digital environments: empowering users, November 2002.

41. Choonsik Park, Kazutomo Itoh, Kaoru Kurosawa. “ All/Nothing Election Scheme and Anonymous Channel”. EUROCRYPT ’93, Pre-proceedings, Lofthus, May 1993, T97-T112.

42. Birgit Pfitzmann. “Breaking an Efficient Anonymous Channel”. Eurocrypt 1994, LNCS 950, Springer-Verlag, Berlin 1995, 332-340

43. Neff A.” A verifiable secret shuffle and its application to e-voting”. In Proceedings of the ACM conference on computer and communications security; 2001. p. 116–25.

44. Masayuki Abe. “Universally verifiable mix-net with verification work independent of the number of mix-servers”. In the proceedings of EUROCRYPT 1998. Springer-Verlag, LNCS 1403, 1998: 437–447.

45. Ryan P Y A, Schneider S A. “Prêt a voter with re-encryption mixes”. ESORICS 2006. Lecture notes in computer science, vol.4189. Berlin: Springer; 2006. p. 313–26.

46. Vora P., “David Chaum’s Voter verification using encrypted paper receipts” .In DIMACS workshop on electronic voting—theory and practice. NewJersey: RutgersUniversity; May26–27, 2004.

47. Philippe Golle , Sheng Zhong , Dan Boneh , Markus Jakobsson , Ari Juels. “Optimistic Mixing for Exit-Polls”. Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, p.451-465, December 01-05, 2002.

48. Douglas Wikstrom. Five practical attacks for “optimistic mixing for exit-polls”. In Mitsuru Matsui and Robert J. Zuccherato, editors, Selected Areas in Cryptography, volume 3006 of Lecture Notes in Computer Science, pages 160–175. Springer, 2004

49. Martin Hirt and Kazue Sako. Efficient Receipt-Free Voting Based on Homomorphic Encryption. B. Preneel (Ed.): EUROCRYPT 2000, LNCS 1807, pp. 539-556, 2000. Springer-Verlag Berlin Heidelberg 2000

50. Ronald Cramer., Rosario Gennaro., Berry Schoenmakers. A Secure and Optimally Efficient Multi-Authority Election Scheme. In Advances in Cryptology. EUROCRYPT'97, Vol. 1233 of Lecture Notes in Computer Science, Springer-Verlag, 1997. pp. 103-118.

51. Aditya, Riza, Boyd, Colin, Dawson, Edward, Lee, Byoungcheon, & Peng, Kun. "Multiplicative Homomorphic E-Voting". In Canteaut, A & Viswanathan, K (Eds.) Progress in Cryptology - INDOCRYPT 2004. 5th International Conference on Cryptology in India.P. 20-22 December 2004, Chennai, India.

52. R. Aditya, C. Boyd, E. P. Dawson, and K. Viswanathan. "Secure e-voting for preferential elections". In proceedings of EGOV 03 Conference, pages 246–249, Berlin, 2003. Springer-Verlag. Lecture Notes in Computer Science Volume 2738.

53. J. Groth, "Non-interactive zero-knowledge arguments for voting," in Proceedings of International Conference on Applied Cryptography and Network Security, LNCS 3531, 2005, pp. 467-482, http://www.daimi.au.dk/~jg/ACNS05VoteProofFull.pdf.

54. Wei Han, Ke-fEI Chen, Dong Zheng. "Receipt-Freeness for Groth's e-Voting Schemes". JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 25, 517-530 (2009) 517

55. Chaum D. "Blind signatures for untraceable payments". In CRYPTO '82. New York: Plenum Press; 1982. p. 199–203.

56. Yi Mu; Varadharajan, V.; , "Anonymous secure e-voting over a network,". Computer Security Applications Conference, 1998, Proceedings., 14th Annual , vol., no., pp.293-299, 7-11 Dec 1998 doi: 10.1109/CSAC.1998.738649
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=738649&isnumber=15949

57. Lin, M. Hwang, C. Chang. "Security enhancement for anonymous secure e-voting over a network", Computer Standard and Interfaces 25 (2) (2003) 131–139.

58. S. Hwang, H. Wen, T. Hwang. "On the security enhancement for anonymous secure e-voting over computer network". Computer Standard & Interfaces 27 (2) (2005) 163–168.

59. F. Rodríguez-Henríquez, Daniel Ortiz-Arroyo, Claudia García-Zamora. "Yet another improvement over the Mu–Varadharajan e-voting protocol". Computer Standards & Interfaces 29 (2007) 471–480

60. Yang Feng, Siaw-Lynn Ng and Scarlet Schwiderski-Grosche. “An Electronic Voting System Using GSM Mobile Technology”. Technical Report. RHUL-MA-2006-5. (Department of Mathematics, Royal Holloway, University of London, 2006),http://www.ma.rhul.ac.uk/tech.

61. Chun-I Fan, Wei-Zhe Sun. ”An efficient multi-receipt mechanism for uncoercible anonymous electronic voting”. Mathematical and Computer Modelling, Volume 48, Issues 9–10, November 2008, Pages 1611-1627, ISSN 0895-7177, 10.1016/j.mcm.2008.05.039. (http://www.sciencedirect.com/science/article/pii/S0895717708001787）

62. Mohanty, Sujata; Majhi, Banshidhar; , "A Secure Multi Authority Electronic Voting Protocol Based on Blind Signature," Advances in Computer Engineering (ACE), 2010 International Conference on , vol., no., pp.271-273, 20-21 June 2010 doi: 10.1109/ACE.2010.82 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5532828&isnumber=5532798

63. Han Ran; Wu Zheng Peng; , "A protocol of electronic voting and blind digital signature based on elliptic curve," Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp.489-491, 27-29 May 2011 doi: 10.1109/ICCSN.2011.6014316 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6014316&isnumber=6013532

64. Martin, K. M. *“Everyday cryptography: Fundamental principles and applications”*. Oxford: Oxford University Press. 2012

65. Mayes, K. E., & Markantonakis, K., *”Smart cards, tokens, security and applications”*. New York: Springer. 2008

66. B. W. DuRette. "Multiple administrators for electronic voting". B.Sc thesis, MIT, 1999. http://theory.lcs.mit.edu/~cis/theses/DuRette-bachelors.pdf

67. Han Wei; Zheng Dong; Chen Ke-fei; , "A Receipt-Free Punch-Hole Ballot Electronic Voting Scheme," Signal-Image Technologies and Internet-Based System, 2007. SITIS '07. Third International IEEE Conference on, vol., no., pp.355-360, 16-18 Dec. 2007 doi: 10.1109/SITIS.2007.15 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4618796&isnumber=4618741

68. Kun Peng; Feng Bao; , "Efficient Proof of Validity of Votes in Homomorphic E-Voting," Network and System Security (NSS), 2010 4th International Conference on ,

vol., no., pp.17-23, 1-3 Sept. 2010 doi: 10.1109/NSS.2010.25
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5636135&isnumber=5635482