An Electronic Voting System Using GSM Mobile Technology

Yang Feng, Siaw-Lynn Ng and Scarlet Schwiderski-Grosche

Technical Report
RHUL–MA–2006–5
26 June 2006

Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX, England
http://www.rhul.ac.uk/mathematics/techreports

Abstract

Electronic voting systems have the potential to improve traditional voting procedures by providing added convenience and flexibility to the voter. Numerous electronic voting schemes have been proposed in the past, but most of them have failed to provide voter authentication in an efficient and transparent way. On the other hand, GSM (Global System for Mobile communications) is the most widely used mobile networking standard. There are more than one billion GSM users worldwide that represent a large user potential, not just for mobile telephony, but also for other mobile applications that exploit the mature GSM infrastructure. In this paper, an electronic voting scheme using GSM mobile technology is presented. By integrating an electronic voting scheme with the GSM infrastructure, we are able to exploit existing GSM authentication mechanisms and provide enhanced voter authentication and mobility while maintaining voter privacy.

1 Introduction

In democratic societies, voting is an important tool to collect and reflect people's opinions. Traditionally, voting is conducted in centralised or distributed places called voting booths. Voters go to voting booths and cast their votes under the supervision of authorised parties. The votes are then counted manually once the election has finished. With the rapid development of computer technology and cryptographic methods, electronic voting systems can be employed that replace the inefficient and most importantly error-prone human component. To increase the efficiency and accuracy of voting procedures, computerised voting systems were developed to help collecting and counting the votes. These include Lever Voting Machines, Punched Cards for Voting, Optical Mark-Sense Scanners and Direct Recording Electronic (DRE) voting systems [1].

For a variety of reasons, voters may be unable to attend voting booths physically, but need to vote remotely, for example, from home or while travelling abroad. Hence, there is great demand for remote voting procedures that are easy, transparent, and, most importantly, secure. Today, the most common way for remote voting is postal voting, where voters cast their votes by post. However, it lacks proper authentication and involves a time-consuming procedure. Internet voting was introduced to provide more flexibility. Because of the inherited security vulnerabilities of the Internet and computerised systems in general, Internet voting incurred a wide range of criticism. However, to date many pilot projects in different countries and

research groups have been carried out. The Secure Electronic Registration and Voting Experiment (SERVE), an Internet-based voting system built by Accenture and its subcontractors for the U.S. Department of Defense's Federal Voting Assistance Program (FVAP), is the most well-known of this kind. A thorough analysis of this system can be found in [9].

In this paper, we endeavour to improve mobility and address security problems of remote voting procedures and systems. We present an electronic voting scheme using GSM. With more than one billion users[1], the GSM authentication infrastructure is the most widely deployed authentication mechanism by far. We make use of this well-designed GSM authentication infrastructure to improve mobility and security of mobile voting procedures.

The cryptographic protocol of our GSM mobile voting scheme is based on the earlier work of Fujioka et al. [7]. In our proposed scheme, voters are authenticated by their GSM mobile operators, and the votes are sent using GSM wireless communication. Voters and their votes cannot be linked and votes remain secret until the final counting. The Fujioka et al. scheme [7] applies a public-key based signature scheme for every single voter. By employing the GSM authentication infrastructure instead, we avoid using a public-key based solution and employ a full-fledged scheme for every single voter. Hence the public-key infrastructure overhead is largely reduced.

This paper is structured as follows: in Section 2 we give a background relating to the proposed scheme, including the security features provided by GSM, and a brief description of the Fujioka et al. scheme [7]; Section 3 define the security criteria a voting system should fulfil. Section 4 introduces the proposed protocol, including a list of assumptions, a description of the role of each system component, and a detailed description of the proposed scheme. In Section 5, we present an analysis of the security properties of the proposed scheme and the extent to which the scheme satisfies the security requirements outlined in Section 3. Finally, a conclusion is given in Section 6.

2 Background

In this section, we review the GSM security features, in particular the authentication function. We then briefly review the Fujioka et al. scheme [7].

2.1 Security Features in GSM

GSM is a digital wireless network standard widely used in European and Asian countries. It provides a common set of compatible services and capa-

[1] www.gsmworld.com

bilities to all GSM mobile users [10]. The services and security features to subscribers are listed in [6] as subscriber identity confidentiality, subscriber identity authentication, user data confidentiality on physical connections, connectionless user data confidentiality and signalling information element confidentiality. They are summarised as follows:

Subscriber identity confidentiality is the property that the subscriber's real identity remains secret by protecting her International Mobile Subscriber Identity(IMSI), which is an internal subscriber identity used only by the network, and using only temporary identities for visited networks.

Subscriber identity authentication is the property that ensures that the mobile subscriber who is accessing the network or using the service is the one claimed. This feature is to protect the network against unauthorised use.

Data confidentiality is the property that the user information and signalling data is not disclosed to unauthorised individuals, entities or processes. This feature is to ensure the privacy of the user information.

In our proposed GSM mobile voting scheme, communication between the mobile equipment and the GSM network uses standard GSM technology. Hence GSM security features apply. Among which, the subscriber identity authentication feature is particularly used in the protocol. The comprehensive descriptions of above security features can be found in [6, 10]. Here, we only describe the subscriber identity authentication feature in greater detail.

The subscriber identity authentication in GSM is based on a challenge-response protocol. A random challenge RAND is issued when a mobile subscriber tries to access a visited network. The Authentication Centre (AC) computes a response SRES from RAND using an algorithm A3 under the control of a subscriber authentication key K_i, where the key K_i is unique to the subscriber, and is stored in the Subscriber Identity Module (SIM) on the mobile equipment (ME), as well as the Home Location Register (HLR). The ME also computes a response SRES from RAND as well. Then the value SRES computed by the ME is signalled to the visited network, where it is compared with the value SRES computed by the AC. The access of the subscriber will be accepted or denied depending upon the result of comparing the two values. If the two values of SRES are the same, the mobile subscriber has been authenticated, and the connection is allowed to proceed. If the values are different, then access is denied. The process is illustrated in Figure 1.

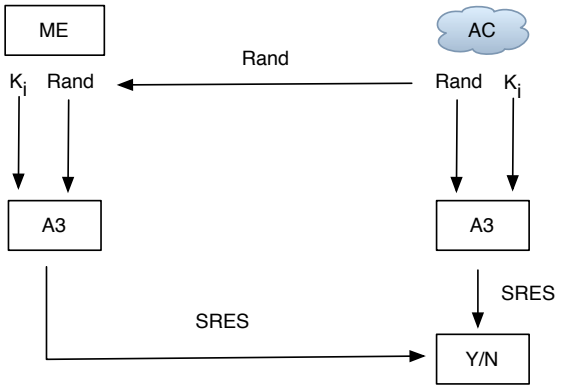

Figure 1: GSM Authentication

2.2 The Fujioka et al. Scheme

Since the idea of electronic voting was first proposed by Chaum [3], many electronic voting schemes, both theoretical and practical, have been proposed. According to the mechanism they use to achieve voter privacy, these voting schemes can be classified as homomorphic encryption schemes, mix-net schemes and blind signature schemes. Most of the homomorphic and mix-nets schemes require large amount of computation capabilities. In a mobile environment, the mobile device have limited computational abilities, so employing schemes with large computation is not practical. Therefore, we develop our GSM mobile voting scheme based on a blind signature voting scheme presented by Fujioka et al. in 1992. It is a prototype system based on blind signatures. It was intended as a practical secret voting scheme for large scale elections. There are voters, an administrator, and a counter participating in the scheme. The scheme assumes that voters and the counter communicate through an anonymous communication channel [2, 4], which is a communication channel that allows the communication entities to remain anonymous throughout the communication. The structure of the scheme was outlined in [7] as:

Preparation:	A voter fills in a ballot, blinds the ballot using the blind signature technique to get the administrator's signature, and sends it to the administrator.
Administration:	The administrator signs the message in which the voter's ballot is hidden, and returns the signature to the voter.
Voting:	The voter extracts the ballot with the administrator's signature, and sends it to the counter anonymously.
Collecting:	The counter publishes a list of received ballots.
Opening:	The voter opens her vote by sending her encryption key anonymously.
Counting:	The counter counts the votes and announces the result.

In this scheme, digital signature, blind signature and bit-commitment mechanisms were used. As these mechanisms are also the primitive cryptographic elements in our proposed scheme, a brief description of these mechanisms is given as follows:

Digital signature [11] is an essential cryptographic primitive for authentication, authorisation, and non-repudiation. It binds a message and a secret known only to the signer in a way that the public can verify that the message has been signed by the signer without knowing the secret. In a public-key encryption based digital signature scheme, the secret is the private key, and the information that is used by the public to verify the signature is called the public key.

Blind signature [11] is a signature scheme with special functionality, where the signer has no knowledge of the message she signs and the signature. Hence, the signed message cannot be associated with the sender. A blind signature protocol usually includes three steps: blinding, signing and unblinding. For example, sender A wants to get a blind signature from signer B upon message m. Functions g and h are blinding and unblinding functions that are only known to A, and $S_B(x)$ represents the normal digital signature of B on x. First, sender A blinds the message m with the blinding function g, namely $g(m)$, and sends it to signer B. Signer B signs $g(m)$ with B's signature, as $S_B(g(m))$, and sends it back to sender A. Finally, A unblinds it with the unblinding function h, as $h(S_B(g(m)))$, where $h(S_B(g(m)))=S_B(m)$. In the end, sender A obtains signer B's signature upon message m, without signer B knowing the message m and the signature on m, so the signer cannot link the signed message m to the sender A.

Bit-commitment [11, 12] is the basic component of many cryptographic

protocols. In a bit-commitment scheme, the sender A sends an encrypted message m to the receiver B in such a way that when later on A sends B the key to decrypt the message, B can be confident that it is the right key to the message m and the decrypted message B gets is the same message m that A committed to with B.

3 Security Requirements for Voting Schemes

In accordance with [1, 5, 7, 8], we describe a set of voting security criteria. However, depending on different democratic requirements in different countries, and the different scales of electronic voting systems, security goals can vary. General security requirements include democracy, privacy, accuracy, fairness, verifiability and recoverability.

Democracy: All and only the authorised voters can vote, and each eligible voter can vote no more than once. Voters can also choose not to vote. To achieve democracy, voters need to be properly registered and authenticated, and then there should be a convenient way for them to cast their votes, for example, availability of different language choices, special aid for disabled voters, and proper ways for absentee voting and early voting.

Privacy: All votes remain secret while voting takes place and each individual vote cannot be linked by any individual or authority to the voter who casts it. This is important even if the voter herself does not care about it. In a small-scale voting system, such as a private company or an organisation, the privacy issue is paramount.

Accuracy: The voting result accurately reflects voters' choices. In this case, no vote can be altered, duplicated or eliminated without being detected.

Fairness: No partial result is available before the final result comes out.

Verifiability: There are two notions of verifiability. The weaker one is individual verifiability, where any voter can check that her own vote has been considered in the tally. The stronger one is universal verifiability, which ensures that any party including observers can be convinced that the election is fair and the published tally has been correctly computed from the correctly cast ballots.

Recoverability: If any failure, mistake or cheating is detected, there should be proper methods and procedures and information available to help recover the voting system. Recounts may take place.

4 The GSM Mobile Voting Scheme

In this section, we introduce our GSM mobile voting scheme. In this scheme, GSM is used for the voting system to introduce voter mobility and provide voter authentication. The proposed scheme is based on the electronic voting scheme proposed by Fujioka et al. [7], as described in Section 2.2.

We start by introducing the different components of the scheme, followed by stating a list of assumptions on which the protocol is based. Then the proposed voting scheme is described in detail.

4.1 The Components

- **Voting Device (ME)**: In electronic voting schemes, voters need to use dedicated voting devices to cast their votes electronically, for instance, Internet connected computers or DRE machines. In our scheme, the voting device corresponds to the GSM mobile equipment (ME), which consists of a GSM SIM card and a GSM card reader, for example, a GSM phone, a GSM enabled PDA, or a laptop with a GSM card reader. The device needs to provide a platform to run the voting application, which consists of the candidate information, the key storage and generation functions.

- **Authentication Centre (AC)**: AC is an entity within the GSM network. As described in Section 2.1, AC generates the authentication parameters and authenticates the mobile equipment. Apart from authenticating the mobile equipment, AC is also an important information distribution server in the proposed scheme. AC needs to be trusted to transfer the messages as required, as discussed in Section 4.2.

- **Verification Server (VS)**: VS belongs to the voting authority, who organises the voting event. It verifies the legitimacy of the voter and issues a voting token to the voter. VS also publishes a list of voter information.

- **Collecting and Counting Server (CS)**: CS is the server that collects and counts the votes to give the final result. CS's action need to be audited by all candidate parties.

4.2 Assumptions

Our system is based on a number of assumptions that are listed in this section.

1. We assume that the proposed GSM mobile voting scheme is part of a voting system, and that voters can choose to vote through different methods, for example, the voting booth, postal or GSM. If voters want to vote through GSM, they have to be registered GSM subscribers. This means that the voters have already registered their real names and addresses with their mobile operators by presenting their eligible credentials at the time of subscription.

2. We assume that the GSM mobile operator is trusted to authenticate the mobile users for the purpose of voting and send the correct information to VS and CS. We will discuss this in more details in Section 5.

3. We assume that there are means of authenticating a user to access in the voting application on the mobile phone, for instance, password protection. This will prevent unauthorised use of the voting application.

4. We also assume the integrity of the voting application on the ME is maintained throughout the voting event. To achieve this, a Trusted Platform Module[2] may be employed on the ME to provide a secure platform for running the application and enhancing end-user security. We will also discuss this further in Section 6.

4.3 Overview

In this section, we outline our GSM mobile voting scheme. It is divided into three phases: the pre-voting phase, the voting phase and the post-voting phase.

The Pre-voting Phase: In this phase, the voter installs the application, fills in the ballot, and obtains a voting token from VS without revealing the vote. In this paper, we consider the ballot an electronic equivalent of a paper ballot, which is an electronic form with the voter's choice of the candidates. We also define the voting token as the encrypted ballot signed by VS.

- The voter fills in the ballot, encrypts the ballot, blinds it using the blinding technique of a blind signature scheme, and sends it to AC using GSM wireless communication.

[2]https://www.trustedcomputinggroup.org/

- AC authenticates the voter, signs the encrypted ballot and forwards the encrypted ballot along with the signature to VS.
- VS checks the signature of AC and the eligibility of the voter, signs the encrypted ballot with its private key, and sends the signed encrypted ballot back to the voter.
- The voter checks the signature and retrieves (unblind) the VS-signed ballot from the message using the retrieving (unblinding) technique of the blind signature scheme.

The Voting Phase: In this phase, the voter sends the voting token and the encrypted version of the key to CS, where the key is the one used to encrypt the ballot.

- The voter sends the voting token to AC, along with the decryption key of the ballot encrypted with CS's public key to avoid AC decrypting the ballot and compromising the privacy of the voter.
- AC encrypts the key again with a randomly generated symmetric key, which is the same for all voters through the same AC in one particular voting event.
- Upon receiving the encrypted key and the voting token, CS checks if the voting token is valid and allocates a serial number to the voter and sends a confirmation along with the number back to the voter.

The Post-voting Phase: In this phase, AC sends its decryption key to CS to retrieve the key, which is used to open the ballot. CS then counts the votes.

4.4 The GSM Voting Protocol

In this section, we describe the GSM mobile voting scheme in detail. We start by introducing the notations used in this paper, which are based on the terms defined in [7], followed by a description of the scheme.

V_i: Voter i
ID_i: Voter V_i's identification
v_i: Vote of voter V_i
$E_k(m)$: The symmetric key encryption of message m using key k
$P_k(m)$: The public key encryption of message m using public key k
$S_A(m)$: A's signature scheme on message m
$B(v, k)$: Bit-commitment scheme for message v using key k
$g(m, r)$: Blinding technique for message m and random number r
$h(s, r)$: Retrieving (unblinding) technique of blind signature from message s and random number r

The protocol is illustrated in Figure 2.

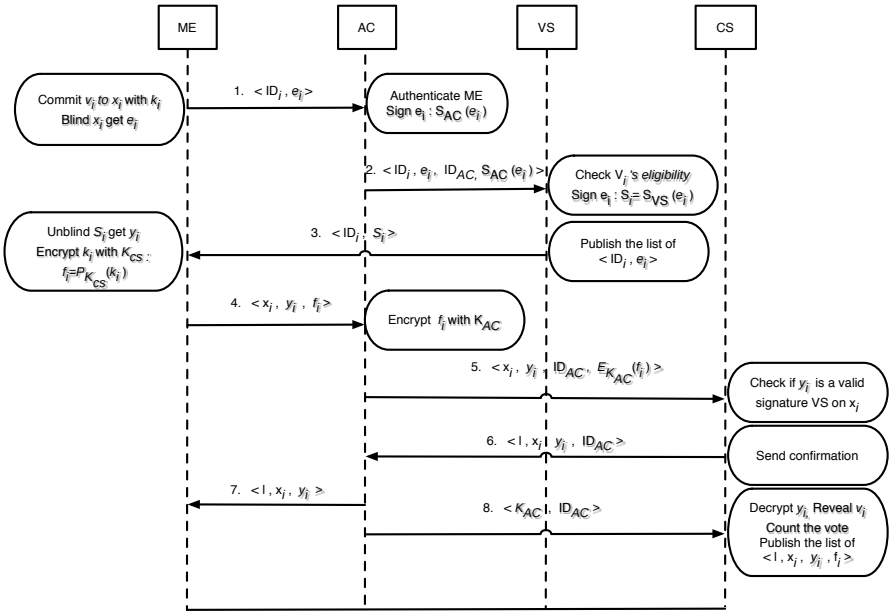

Figure 2: The GSM mobile voting scheme

4.4.1 The Pre-voting Phase

In this phase, voter V_i fills in a ballot and obtains a voting token from VS without revealing the vote v_i.

Initially, voter V_i fills in a ballot generated by the application on the mobile voting device ME. The ME completes the ballot by committing it to x_i as $x_i = B(v_i, k_i)$ using a randomly chosen key k_i, and blinds x_i by computing $e_i = g(x_i, r_i)$. Here, r_i is a randomly chosen blinding factor. Both k_i and r_i are generated by the ME within the application. Then V_i sends $< ID_i, e_i >$ to AC through GSM, shown in message 1 of Figure 2.

Upon receiving the message from voter V_i, AC authenticates the ME and checks the Home Location Register (HLR), where the subscriber's information is stored, verifying that the voter is who she claims to be. Then AC applies its signature and forwards it to VS along with its ID as $< ID_i, e_i, ID_{AC}, S_{AC}(e_i) >$, shown in message 2.

By checking the signature of AC, VS is confident that AC has already authenticated the voter. It then verifies the eligibility of V_i to vote by checking the database to see if the voter has voted before, and adds V_i's information to the database as $< ID_i, e_i >$. Most importantly in this phase, VS issues a voting token to the eligible voter without revealing the vote v_i, so after verifying the eligibility of the voter, VS signs the committed and blinded vote e_i with its own signature and sends it back to the voter V_i as $s_i = S_{VS}(e_i)$ with ID_i, which is $< ID_i, s_i >$, shown in message 3.

Upon receiving the message from VS, the voter V_i unblinds s_i to obtain the signature $y_i = h(s_i, r_i)$. If y_i is a valid signature of VS upon x_i, the voter can use it as a voting token to cast her vote in the Voting Phase. Otherwise, voter V_i reports to the voting authority, in provision of the evidence of $< x_i, y_i >$.

At the end of the Pre-voting phase, VS announces the number of voters who registered and have been given a voting token, and publishes the entry $< ID_i, e_i >$.

4.4.2 The Voting Phase

After VS publishes the entries of the registered voters, voters can check the list, and claim any errors during the registration by providing the evidence $< x_i, y_i >$. Now voters can cast their votes with the verified token anytime they want before the voting deadline. In [7], the scheme assumes that voters cast their votes through an anonymous channel to protect voters' privacy. In the proposed scheme, we achieve the privacy of voters by making use of GSM's AC.

V_i encrypts k_i with the CS's public key k_{CS} as $f_i = P_{k_{CS}}(k_i)$, and sends $< x_i, y_i, f_i >$ to AC, shown in message 4. By encrypting k_i with k_{CS}, AC cannot observe the voter V_i's vote, and only CS can reveal k_i by decrypting f_i with its private key.

Upon receiving the message, AC encrypts f_i with the key k_{AC}, which

is generated by AC, and is the same for all voters who votes through this AC. AC will only send k_{AC} to CS when the voting phase finishes, then CS can open the key to decrypt the votes. By doing this, there is no partial result revealed to any party before the voting phase finishes. AC sends $< x_i, y_i, ID_{AC}, E_{k_{AC}}(f_i) >$ to CS, shown in message 5.

After receiving the message, CS checks if y_i is a valid VS's signature on x_i. If it is, CS assigns a serial reference number l for each voter, and publishes the entry $< l, x_i, y_i >$. Otherwise vote is denied. Then CS sends $< l, x_i, y_i, ID_{AC} >$ back to AC, and AC forwards $< l, x_i, y_i >$ back to voter V_i for confirmation, shown in message 6, 7. Upon receiving the corresponding reference number l, voters can check the published entries on the bulletin board, and report any errors.

After the voting phase starts, the registered voters will get a reminder generated by the application to ask the voter if she wants to cast the vote, and the voter can choose to vote now, later and not at all. If voter V_i decides not to vote, the application generates an empty vote, sends it to AC and CS, and CS publishes it in the list. This empty vote can be pre-loaded, blinded, signed and cast in the same way as the normal vote is. Hence, the number of the entry published by VS in the Pre-voting Phase should be the same as the entry published by CS in the Voting Phase. As a result, even if some voters choose not to vote, CS cannot forge the vote.

4.4.3 The Post-voting Phase

After the voting phase, the ACs from different networks and regions send the corresponding k_{AC} to CS, shown in message 8. CS reveals f_i using k_{AC}, and decrypts f_i to get k_i using CS's private key. CS can decrypt all the votes with k_i, count them and add f_i to the corresponding entry of the list published in the Voting Phase.

To help understand the protocol, the different status of the votes and the keys are as shown in Figure 3.

5 Security Analysis

In this section, we discuss how and to what extent the protocol fulfils the security requirements listed in Section 3.

- **Democracy** *Only the authorised voters can vote.* First, voters are authenticated through GSM, which assures that voters are who they claim to be. Further assurance can be provided by using a PIN to protect

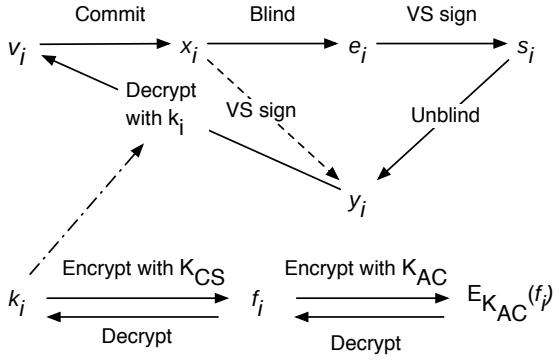

Figure 3: Vote Flow

the ME or by using randomly chosen identity-based questions. Therefore, the authentication of the voter is as good as GSM can provide. Second, the eligibility of voters is checked by VS. This prevents voters from voting more than once. *All the voters can vote.* The whole voting procedure can be performed remotely using a personal voting device. Hence, it provides an alternative method for people who cannot go to the voting booth. It is suitable for voters who travel abroad and voters who have disabilities. Also, the voting application runs on a mobile device, which can be written with different language choices, making the voting application accessible to all voters.

- **Privacy** *All votes remain secret while the voting takes place and each individual vote cannot be linked to the voter who casts it.* The proposed scheme is divided into three phases, and they are separated in time. In the pre-voting phase, a blind signature is applied to the vote in a way that e_i is not linkable with y_i, and e_i is signed without revealing the vote v_i. In the voting phase, the communication between voters and CS achieves anonymity with the help of AC. The voter V_i sends k_i encrypted with CS's public key k_{CS} to AC, so the AC is not able to reveal k_i to get the value of the vote v_i. While AC is able to link e_i, y_i to ID_i, it has no knowledge of v_i and is not able to link v_i to ID_i. Also, CS has no direct communication with voter V_i, so CS cannot tell which voter casts the vote. Hence, for all the components of the voting system, if their knowledge of ID_i cannot be linked with the vote v_i, the privacy of the voter is protected. To clarify this, the knowledge of each server and the public can be illustrated in the following table:

	AC	VS	CS	Public
Pre-voting	ID_i, e_i	ID_i, e_i, s_i		ID_i, e_i
Voting	l, ID_i, x_i, y_i, f_i		l, x_i, y_i	l, x_i, y_i
Post-voting	ID_i, l_i, x_i, y_i		l, x_i, y_i, f_i, v_i	l, x_i, y_i, f_i

- **Accuracy** *No vote can be altered, duplicated or eliminated without being detected.* At the end of the pre-voting phase, the entry $< ID_i, e_i >$ is published, and at the end of the voting phase the entry $< l, x_i, y_i, f_i >$ is published. Therefore, if any vote is altered, duplicated or eliminated, it can be detected by the voters. If a voter decides not to vote after she receives the voting token, the application will send the empty vote to CS. Hence, AC cannot impersonate a voter.

- **Fairness** *No partial result can be known before the final result comes out.* The voter v_i's commitment key k_i is sent to CS in the form of $E_{k_{AC}}(f_i)$, where $f_i = P_{k_{CS}}(k_i)$. CS can decrypt f_i to get k_i, but CS has no knowledge of k_{AC}. The k_{AC} is sent to CS after all voters have cast their votes or after the voting deadline. Hence, there is no partial result revealed before the final result.

- **Verifiability** Individual verifiability is satisfied since the appearance of $< l, x_i, y_i, f_i >$ assures voter V_i that her vote has been taken into account. Any observer can verify that the votes taken into account are legitimate, by verifying the signature y_i on x_i.

- **Recoverability** *If any failure, mistake or cheating is detected, there should be proper methods and procedures and information available to help recover the voting system.* The proposed scheme is divided into three phases, and they are separated in time. After each phase, voters check the published list of entries. If errors are detected, the voters can provide their copy of $< x_i, y_i, f_i >$ to recover their votes. In the case of anomalies in the published list, AC has enough information to check that votes are legitimate.

In this section, we have shown that the GSM mobile voting system fulfils the standard set of voting security criteria outlined in Section 3.

However, in our GSM mobile voting scheme, the AC authenticates the voters in the pre-voting phase, and encrypts the public key encrypted key which is needed to open final votes. Hence the voters must trust AC not to reveal the link between ID_i, e_i, and y_i, while CS and VS must trust AC to authenticate the voters. The trust between GSM mobile operator and mobile user is based on the formally established agreement between them,

which defines the trust and the liabilities. The trust between the mobile operator and the voting servers, namely VS and CS can also be agreed and formally established before the voting events take place. However, trust is not the most manageable solution, and when there are different ACs from different mobile operators involved in the voting system, it will be more difficult to manage the trust upon them. The elimination of this trust on AC will be one of the subjects of future work.

6 Conclusion and Future Work

We proposed a GSM mobile voting scheme, where the GSM authentication infrastructure is used to provide voter authentication and improve voter mobility. Authentication is always a difficult requirement to fulfil for remote voting schemes, most of which apply a public-key based signature scheme for voter authentication. In our scheme, by using the existing GSM authentication infrastructure, the public-key overhead is largely reduced. Our scheme also enhances the security and provides more mobility and convenience to voters. Where the voters' privacy is protected by applying a blind signature scheme. In this paper, we presented the basic structure and protocol of our GSM based mobile voting system.

However, further work is needed to address the importance we place in the trust on the AC, and we are therefore investigating options for enhancing and extending the GSM mobile voting scheme. In future work, we will discuss end-user device (ME) and application security. We will also address how the voters obtain the voting application and solutions to provide the integrity of the voting application running on the ME. The Trusted Platform Module and smart card solutions will be considered.

References

[1] M. Burmester and E. Magkos. Towards secure and practical e-elections in the new era. In D. Gritzalis, editor, *Secure Electronic Voting*, pages 63–72. Kluwer Academic Publishers, 2003.

[2] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, February 1981.

[3] D. Chaum. Blind signatures for untraceable payments. In D. Chaum, R. Rivest, and A. Sherman, editors, *Advances in Cryptology—Crypto '82*, pages 199–203, New York, 1983. Plenum Press.

[4] D. Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1(1):65–75, 1988.

[5] L. F. Cranor and R. K. Cytron. Sensus: A security-conscious electronic polling system for the internet. In *Proceedings of IEEE 30th Hawai'i International Conference on System Sciences (HICSS-30)*, pages 561–570, January 1997.

[6] ETS 300 506. *Security aspects (GSM 02.09 version 4.5.1), Digital cellular telecommunications system (phase 2)*, 2000.

[7] A. Fujioka, T. Okamoto, and K. Ohta. A practical secret voting scheme for large scale elections. In J. Seberry and Y. Zheng, editors, *Advances in Cryptology—Auscrypt'92*, volume 718 of *Lecture Notes in Computer Science*, pages pp. 244–251, Gold Coast, Queensland, Austrailia, 13-16 December 1992. Springer-Verlag.

[8] M. Hirt and K. Sako. Efficient receipt-free voting based on homomorphic encryption. In B. Preneel, editor, *Advances in Cryptology—EUROCRYPT '00*, volume 1807 of *Lecture Notes in Computer Science*, pages 539–556. Springer-Verlag, May 2000.

[9] D. Jefferson, A. D. Rubin, B. Simons, and D. Wagner. *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*, 2004.

[10] Y. Lin and I. Chlamtac. *Wireless and Mobile Network Architectures*. Wiley, 2000.

[11] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Inc., 1996.

[12] M. Naor. Bit commitment using pseudo-randomness (extended abstract). In G. Brassard, editor, *CRYPTO '89: Proceedings on Advances in cryptology*, pages 128–136. Springer-Verlag New York, Inc., 1989.