Extension of Votopia to Mobile Voting

Hyunrok Lee, Duc Liem Vo and Kwangjo Kim

International Research center for Information Security(IRIS)

Information and Communications University (ICU), Korea

Abstract

The electronic voting becomes new challenging area in cryptographic application. A variety of schemes are designed and implemented based on cryptographic protocols. Initiated by ICU, one of best practices was *votopia*[1] which was successfully served into the Internet voting based on modified Ohkubo *et al.*'s scheme[2] under Public Key Infrastructure (PKI) and Java technology. *Votopia* was used to select the Most Valuable Player and Best Goal Keepers of 2002 FIFA World Cup Korea/Japan™ through the Internet where most voters can access and cast their ballots from any place and at any time. However, *votopia* assumed that the resources of the Internet voters only connected via wired environment. In this paper, we suggest how to extend *votopia* to mobile voting which has limited computing resources.

I. Introduction

The Internet voting has become in reality. There are many experiments and implementations done successfully over the Internet such as the election scheme proposed by the state of California[3], Caltech-MIT joint project[4], and most recently one so called *votopia*[1] for selecting the Most Valuable Player and Best Goal Keepers of 2002 FIFA World Cup Korea/Japan™. All voting schemes have successful served in the wired Internet environment where voters use desktop PC or notebook providing enough resource for quite heavy computation. But now, the Internet voting face a new requirement to enable voting to be performed on mobile devices such as PDA (Personal Digital Assistant) or mobile phone which has limited computing resources and low power supply.

The mobile voting has just begun. For example, CyberVote[5], VoteHere[6], eVoteSheffield[7] and Euro-Citi[8] try to serve mobile voting via mobile phone or PDA device. The Internet voting system as well as the mobile voting system must meet cryptographic requirements such as anonymity, privacy, completeness, fairness, verifiability, and receipt-freeness. Some mobile voting systems don't provide end-to-end security using only encrypted channels (i.e., SSL) and simple identification mechanism (i.e., PIN code). Others attempt to apply a cryptographic voting protocol satisfied with the requirements to their system. However, the most important point in the design of the mobile voting system is reduction of computation in a mobile device.

In this paper, we describe mobile voting requirements and extend the functionality of *votopia* to mobile voting, named as *mobile votopia*.

This paper is organized as follows: In Section II, we review cryptographic requirements of electronic voting system discussed in the open literature, an overview of the *votopia* Internet voting system, previous works, and Java mobile technology. Section III describes the requirements for extension of *votopia* to mobile voting and proposed design. Finally, concluding

remarks will be made in Section V.

II. Preliminaries

1. Cryptographic Requirements

Many extensive researches[10,11,12,13,14,15] on electronic voting have been conducted and an extensive list of cryptographic requirements for electronic voting is available. In general, we can classify the cryptographic requirements of electronic voting system into the two parts.

■ Basic Requirements

- ivacy: All votes should be secret.
- ɔmpleteness: All valid votes should be counted correctly.
- ɹundness: Anyone cannot disturb the voting.
- ɹreusability: All voters can vote only one.
- igibility: Anyone who is eligible can vote.
- ɹirness: Noting can affect the voting.

In general most electronic voting system as well as paper voting system must meet these basic requirements.

■ Extended Requirements

- alk-away: The voter need not to perform any action after voting.
- ɔbustness: The voting system should be successful regardless of partial failure of the system.
- ɹiversal verifiability: Anyone can verify the validity of the whole voting process.
- ɔceipt-freeness: Voter should not be able to prove his or her vote to a buyer. Voter does not have any receipt for the vote to prevent vote-selling.

The extended requirements are of great cryptographic interest, but are found to be very expensive for practical implementation. To the best of our knowledge, there is no relevant electronic voting system which satisfies with the basic and extended requirements together. Note that Safevote[9] listed a set of requirements in paper, electronic and Internet voting systems.

2. Overview of Votopia

In this Section, we introduce briefly the system design and implementation of *votopia*. It is quite natural assumption that all the voters can trust the admin server completely, and anybody can post, but nobody can erase or overwrite the data once written in the bulletin board. We use some cryptographic primitives such as ElGamal cryptosystem, Schnorr digital signature, and Schnorr blind signature. This ensures that the overall security of *votopia* is based on the difficulty of solving discrete logarithm only.

Votopia has three main stages: registration, voting and counting as most voting systems do. Before initiating these stages, the system parameter including key pairs of each servers except a voter should be generated and distributed by PKI and Java cryptographic library. In order to implement *votopia* efficiently, software products made by Korean security industries have been chosen and their functions have been extended to meet the objectives of *votopia* such as CA server, Java cryptolibrary, and firewall. And we implemented admin server and bulletin board under Unix system using Apache as a web server, Tomcat as a servlet container and JavaServer Page™ (JSP) implementation. The main part of admin server and bulletin board have been developed by using JSP, JDK1.2, and Java cryptolibrary. Oracle DB is used by admin server to manage a large number of informations of all voters and candidates. Bulletin board also uses an independent DB to handle ballots. All clients must get the voting signed applet which is downloadable program code executed in a web browser of a voter supporting Java. This contains necessary information to support the actual candidate selections. The key size of ElGamal cryptosystem and Schnorr digital signature are fixed to 512-bit for fast computation to a client side.

3. Previous Works

1) CyberVote

After European industry initiated to allow the Internet voting in highly secure and verifiable way by using PC, PDA or mobile phones. It will be tested during some trial elections in Germany, in France and in Sweden. The system is based on Cramer et al.'s scheme[17] that aims at guaranteeing universal verifiability without using vote receipts and accuracy of the final tally by multiple-talliers combines the use of PKI for eligible voters registration, system modules (talliers and scrutineers) certification, result time stamping and digital signature, with the use of homomorphic functions and zero knowledge proof to guarantee universal verifiability of the results and voters' privacy. But, the system, especially mobile voters, has communication overhead and computational complexity for proofs of knowledge and validity. So, the system provide no efficiency in voter's point of view.

2) VoteHere

The system was designed by US company based on Cramer et al.'s scheme. VoteHere guarantees accuracy through multi-authority tabulator, but do not provide an efficiency in mobile devices by the same reason of CyberVote.

3) Euro-Citi

An European research project started in September 2000. The system will be tested during some trial elections in Greece, England and Spain. The Euro-citi platform is organized to permit system user access either from their home PC or from public places, kiosks, or from GSM terminals. For providing mobile voting, the system just use WAP(Wireless Application Protocol), WTLS(Wireless Transport Layer Security) and PIN(Personal Identification Number) code.

4) eVoteSheffield

The eVoteSheffield use mobile SMS (Short Message Service) voting with PIN code. The detailed concept of system did not define yet.

4. Java Mobile Technology

For implementing mobile voting, Java is an important technology due to the platform-independent characteristics. Sun Microsystems has introduced Java 2 Micro Edition[16] (J2ME) is suitable to mobile and handheld devices. J2ME, a highly optimized Java Runtime Environment, is categorized into two different configurations by the size of the virtual machine. For supporting the devices that have limited memory (less than 512KB) and unstable network connection, *CLDC*(Connected Limited Device Configuration) was designed. This configuration provides the virtual function named KVM that has limited function. In order to support more powerful mobile devices that have over 2MB memory and stable network, *CDC*(Connected Device Configuration) was designed. In this configuration, fully functional JVM is provided. Running above each configuration are "Profiles" which provide functions to applications. At current status, MIDP(Mobile Information Device Profile) v1.0 on CLDC, Personal Profile on CDC and *MIDlet* that equally supports the role of applet are available.

III. Our Design

1. Requirements for Mobile Votopia

While preserving the overall architecture of *votopia*, we must consider the following requirements to serve mobile devices as a voting client:

1) Cryptographic Requirement

At least mobile voting must satisfy the cryptographic requirements which was offered by *votopia* previously.

2) Computational Requirement

To overcome limitation of computational power of mobile devices, most computational work such as key generation for clients should be performed at server side. Only useful information is sent to users. The binary code sent to user must be optimized too. In addition, server side should have a recognizing

mechanism which kind of clients is connecting to server.

3) Device Requirements

Mobile devices used in *votopia* must support TCP/IP protocol stack (regardless of communication media) and Java virtual machine for achieving platform independence.

4) User Interface Requirement

Small screen size is a characteristic of most mobile devices, so that heavy graphical user interface should be changed into simpler user interface. Only is valuable information displayed on clients screen.

2. Design

In this session, we proposed our design and main protocol step for mobile voting based on *votopia*. For convenience, our notations are follow:

■ Notation

AS: Admin Server, *CT*: Counting Server

WS: Web Server, *B()*: Blinding function

UB(): Unblinding function

BB: Bulletin board and ballot box

V_i: Voter i, v_i : vote value by V_i

C_i: V_i's Certification

RA: Registration Authority

■ **Registration Stage**

(R1) V_i access *AS* via *WS* to download a registration form and certificate manger *MIDlet*. In order to solve low computational limitation of mobile devices to eliminating key generation, the certificate manager can download and manage various certificate such as simplified certificate for *votopia*, official X.509v3 certificate which is issued from CA companies for Internet banking. V_i can retrieve official certificate and encrypted private key from stored-data in his computer. And also *AS* can issue C_i by using V_i's registration information through *CA*.

(R2) After downloading or issuing certificate C_i, V_i keeps his encrypted private key and certificate in safe storage such as flash ROM installed in his device. *CA* can keep C_i in *DB* instead of V_i if V_i does not want keep.

(R3) All informations that related in voting are passed through secure channel like using SSL. Especially, the registration information of V_i is encrypted with *AS*'s public key and is sent to *AS*. The *AS* checks V_i has the right to vote after decrypting the information. If V_i doesn't have the right, *AS* gives an error message. Otherwise *AS* gives V_i the right to download voting *MIDlet*.

■ **Voting Stage**

(V1) After downloading voting *MIDlet* to enter voting stage, V_i provides authentication data (ID, password and certificate). *AS* checks whether the voter has already voted or not. If V_i had already voted, *AS* rejects the authorization. Otherwise, *AS* gives V_i the right to download the voting *MIDlet*.

(V2) Using voting *MIDlet*, V_i selects vote v_i of his choice and encypts v_i with *CT*'s public key of the ElGamal encyption as $x_i=E_{CT}(v_i)$. V_i blinds x_i as e_i = B(x_i, r_i), where r_i is a randomly chosen blinding factor. Vi signs e_i as s_i = $S_i(e_i)$ and sends (ID_i, e_i., s_i) to *AS*.

(V3) *AS* verifies the signature s_i of message e_i. If s_i is valid, then *AS* signs e_i as d_i = $S_A(e_i.)$ and sends d_i to V_i. At the end of the voting stage, *AS* announces the number of voters receiving *AS*'s signature, and publishes the final list as (ID_i, e_i., s_i).

(V4) V_i retrieves the desired signature y_i of ballot x_i by y_i = $UB(d_i, r_i)$. V_i checks whether y_i is *AS*'s signature for x_i. If this check fails, V_i claims it by showing that (x_i, y_i) is invalid.

(V5) V_i sends (x_i, y_i) to *BB* via anonymous channel.

■ **Counting Stage**

(C1) *CT* verifies the signature y_i of x_i. If the verification fails, *CT* claims that y_i is not a valid signature of x_i and exclude the vote from further steps of the counting stage.

(C2) *CT* decrypts ballot x_i and retrieves vote v_i as v_i = $D_{CT}(x_i)$. *CT* store the voting results

to *DB*.

(C3) After the period of voting is over, *CT* publishes the voting results by using *BB*.

V. Comparison

In this Section, we briefly compare *mobile votopia(MV)* with others. The comparison is performed in points of providing cryptographic requirements(CR), communication overhead(CO) and computational complexity(CC), which is summarized in Table 1. Especially, we consider that compare CO and CC in viewpoints of capability of mobile device, not in server side. Also CR is most important factor among all other factors.

	[5]	[6]	[7]	[8]	*MV*
CR	O	O	X	△	O
CO	H	H	L	L	M
CC	H	H	L	L	M

Table 2 Comparison of Mobile Voting

IV. Concluding Remarks

Along with development of mobile technology as well as information technology, mobile voting will come true soon. Mobile voting enables voters to cast a vote in any where at any time, makes them to vote more conveniently. It is unsuitable to apply *votopia* protocol directly because most mobile devices still are limited in computing resources. So, in this paper, we deal with requirements to extend the functionality of *votopia* to mobile voting system using PKI and propose new protocol.

In order to implement extended *votopia*, further works like binary code optimization that can be downloaded into mobile devices and minor change of server side must be executed.

References

[1] Kwanjo Kim, *Result of the 1st Worldwide Internet Voting System,* appear in Proc. of CISC2002, Seoul, Korea.

[2] M.Ohkubo, F.Miura, M.Abe, A.Fujioka and T.Okamoto, *An Improvement on a Practical Secret Voting Scheme*, Information Security'99, LNCS Vol.1729, pp.225-234, Springer-Verlag, 1999.

[3] The BELL Newsletter on Internet Voting, The Bell,Vol.1 No.4, Safevote Inc., Aug.2000.

[4] CALTECH-MIT/Voting Technology Project, Dec,2000, *http://www.vote.caltech.edu/*

[5] *http://www.eucybervote.org/*

[6] *http://votehere.com/*

[7] *http://evotesheffield.com/*

[8] *http://www.euro-citi.org/*

[9] *Internet Voting Requirements*, The Bell, Vol.1 No.7, p.3, Safevote Inc., Nov. 2000, http://www.thebell.net/papers/vite-reg.pdf

[10] J.C.Benaloh and D.Tuinstra, *Receipt-free secret ballot elections*, Proc. of 26th ACM STOC, pp.544-553, 1994.

[11] A.Fujioka, T.Okamoto and K.Ohta, *A Practical Secret Voting Scheme for Large Scale Election*, Advances in Cryptology-Auscrypt'92, LNCS Vol.718, pp.248-259, Springer-Verlag, 1993.

[12] B.Lee and K.Kim, *Receipt-free electronic voting through collaboration of voter and honest verifier*, Proceeding of JW-ISC2000, pp.101-108, Jan.25-26, 2000, Okinawa, Japan.

[13] M.Maichels and P.Horster, *Some remarks on a receipt-free and universally verifiable mix-type voting scheme*, Advances in Cryptology-Asiacrypt'96, LNCS Vol.1163, pp.125-132, Springer-Verlag, 1996.

[14] V. Niemi and A.Renvall, *How to prevent buying of voters in computer elections*, Advances in Cryptology-Asiacrypt'94, LNCS Vol.917, pp.164-170, Springer-Verlag, 1994.

[15] B.Schoenmakers, *A simple publicly verifiable secret sharing scheme and its application to electronic voting*, Advances in Cryptology-Crypto'99, LNCS Vol.1666, pp.148-164, Springer-Verlag, 1999.

[16] Sun Microsystems Java2ME Homepage, *http://java.sun.com/j2me/*

[17] R. Cramer, R.Gennaro and B.Schoenmakers, *A Secure and Optimally Efficient Multi-Authority Election Scheme*, European Transaction on Telecommunications, Vol.8, No.5, pp.481-490, Sep-Oct, 1997.