The Biometric based Mobile ID and Its Application to Electronic Voting

Sung-hyun Yun[1] **and Heui-seok Lim**[2]
[1] Div. of Information & Communication Engineering, Baekseok University
Cheonan, Chungnam, Korea
[2] Dept. of Computer Science Education, Korea University
Seoul, Korea
[e-mail: shcrpt@gmail.com, limhseok@korea.ac.kr]
*Corresponding author: Sung-hyun Yun

Received April 9, 2012; revised September 18, 2012; revised November 10, 2012; accepted December 9, 2012; published January 29, 2013

Abstract

It requires a lot of costs and manpower to manage an election. The electronic voting scheme can make the election system economic and trustful. The widespread use of smart phones causes mobile voting to be a major issue. The smart phone can be used as a mobile voting platform since it can carry out many services in addition to basic telephone service. To make mobile voting practical and trustful, we analyzed two subjects of study. Firstly, the way to make a biometric based mobile ID, which has legal binding forces. In mobile voting, user identification is accomplished on line since the voter should be able to vote wherever they go. The digital ID conducts a similar role to the need for a resident card. The user's identity is bound to the resident card legally. To bind the user's identity to the smart phone, we use USIM. Biometric recognition is also needed to authenticate the user, since the user cannot prove him or her on line face-to-face. The proposed mobile ID can be reissued by means of introducing a random secret value. Secondly, the mobile voting scheme is proposed where candidates can accept election results without doubt. The goal of an election is to select a leader among two or more candidates. Existing electronic voting schemes mainly focus on the study of ballot verification accomplished by voters. These approaches are not safe against collusion attacks where candidates and the election administration center are able to collude to fabricate election results. Therefore, a new type of voting and counting method is needed where candidates can directly take part in voting and counting stages. The biometric based multi-signature scheme is used to make the undeniable multi-signed ballot. The ballot cannot be verified without the help of all candidates. If candidates accept election results without a doubt, the fairness of the election is satisfied.

Keywords: Mobile Voting, Undeniable Multi-Signature Scheme, Mobile ID, Biometric Signature, Electronic Voting Scheme

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No. 2012-0004515). The preliminary version of this paper was presented in ICONI 2011 (International Conference on Internet 2011)
http://dx.doi.org/10.3837/tiis.2013.01.011

1. Introduction

An election is an important social activity that represents public opinion in order to select the political leader in a democratic society. Many costs and manpower are required to manage large-scale elections, such as the general election for National Assembly or the President. The board of elections has to perform jobs such as announcement on voting day, administration of polling hours, security of voting place, production and transportation of ballot papers, etc. To make the election fair, the board of elections appoints returning officers by whom the voting and counting stages are monitored.

Electronic voting schemes can make the election system economic and trustful. These are classified as fully computerized voting (full e-voting) and partially computerized voting (partial e-voting). In full e-voting schemes, the stages of the entire election are computerized. On the other hand, partial steps of the election stages are computerized in partial e-voting schemes [8].

Currently, the wide spread use of smart phones makes mobile voting a major research issue. The smart phone can be used as a key component in a mobile voting platform because it can carry out many operations in addition to basic telephone service [1, 2]. To make mobile voting practical and trustful, we consider two subjects of study: how to make a biometric based mobile ID and a mobile voting scheme where all candidates assure the election results.

1.1 Biometric based Mobile ID

In mobile voting, user authentication is accomplished on line, since the voter can vote with a smart phone wherever he or she goes. User authentication means proving one's identity to others. In password based schemes, if the password is easy to remember, it is usually also easy to guess. If it is difficult to compromise, it is usually also difficult to remember. In token based schemes, tokens can be easily forgotten, lost, or stolen, and, as it happens with the credit cards, can be fraudulently duplicated [7]. In addition, both the password and token are not physically bound to the user's identity. Thus, proxy authentication is possible [13]. This means that a user can access another user's smart phone to cast a mobile vote.

As a result, biometry appears as a good solution. In a biometric recognition scheme, the user's identity is ensured by the result of matching a biometric template with the enrolled template. Since the biometric data comes from the user, only the biometric data can be physically bound to the smart phone as the user's identity. The increasing capabilities of biometric capture on smart phones such as signature, face, voice, fingerprint, etc. makes biometric recognition practical [3].

In cyber space, it is not possible to verify whether a logged in user is the actual person it claims to be. The mobile ID is digital data that represents user's identity. Especially, in mobile voting, the mobile ID should not be shared with other users. Thus, the mobile ID should be made with the user's biometric data. To authenticate the user, it must be available only if the user submits his/her own biometric data [13].

In mobile commerce, cryptographic keys are needed to sign and verify commercial documents. It's preferable to generate the private key from the biometric mobile ID. If the signer wants to sign a document, the signer (or key owner) must present his/her own biometric data to obtain the private key. This property of biometric key can be used to many applications such as electronic voting where a proxy user cannot be allowed to sign a document.

To be used in mobile voting, the mobile ID has to represent to which phone owner's identity it is legally bound to. It also should have a similar role as a resident card. It requires face-to-face user recognition to make the identity card have legal binding forces. The Universal Subscriber Identity Module (USIM) is unique and binds the phone owner's identity to the mobile phone. During USIM registration, the phone owner authenticates himself/herself to the registration center face-to-face with his resident card. Thus, USIM legally binds the user identity to the phone [1, 13].

In addition, the mobile ID should be reissued when the user's mobile ID is lost, disclosed, or stolen. If the user's biometric data is compromised, it cannot be used again since the biometric data is unique [6]. Thus, to make cancellable mobile ID, the user's random secret value is needed in addition.

1.2 Mobile Voting Scheme based on Undeniable Multi-Signed Ballot

For the mobile voting scheme to be practical, it's more appropriate to consider the requirements of full e-voting [8, 14]. These include universal verifiability, individual verifiability, receipt freeness, etc. Universal verifiability means all participants can verify whether election results are valid or not. If verification fails, all participants must vote again. This can be a burden in a large-scale election such as general election for National Assembly or the President.

Individual verifiability means that each voter can verify whether his vote was counted correctly to the election results. To do this, each voter gets the receipt of the vote. To protect vote selling and vote by coercion, participants of the election should not be able to judge who voted for whom based on the receipt [8, 14].

The goal of an election is to select a leader among two or more candidates. Thus, the most important requirement of an election is fairness, and candidates must agree on the election results. Existing electronic voting schemes mainly focus on the study of ballot verification accomplished by voters. It's not sufficient enough to guarantee voting results to candidates. It's possible to collude among candidates and administrators to fabricate election results.

Therefore, a new type of voting and counting method is needed, where candidates can directly take part in voting and counting stages. The method should allow candidates to be confident in the voting results. The biometric based multi-signature scheme [19] is used to make an undeniable multi-signed ballot. The ballot cannot be verified without the help of all candidates. If candidates accept election results without a doubt, the fairness of the election is satisfied.

In this paper, a mobile voting scheme is proposed where candidates guarantee the fairness of the election. The proposed scheme provides how to create a mobile ID and pair of digital signature keys. The ballot of the voter is created based on the undeniable multi-signature scheme. During the counting stage, to verify the ballot, the multi-signature confirmation protocol is launched between the voter and candidates. Thus, the undeniable multi-signed ballot cannot be counted without the help of all candidates.

We assume that vote selling and vote by coercion are not possible. Under this assumption, we show that the proposed ballot registration, voting and counting procedures are applicable to mobile voting.

In section 2, we review existing electronic voting schemes. In section 3, we present how to create a mobile ID and pair of digital signature keys. In section 4, the mobile voting scheme is proposed. In section 5, we analyze and discuss the proposed scheme. In section 6, conclusion and future works are described.

2. Related Works

In section 2, we analyze the requirements of large-scale election and existing electronic voting schemes.

2.1 Requirements of Large-Scale Electronic Election [8, 17]

- Unreusability

  Registered voters can vote only once. It's not possible to vote multiple times with copied ballots.
- Anonymity (Untraceability)

  All participants cannot know who voted for whom. When counting results, participants cannot analogize correlation between the ballot and the voter. Untraceability means that the source address of packets carrying voter's ballot should not be traced during the transmission period.
- Lawfulness

  Only registered voters can participate in the electronic voting.
- Completeness

  All valid ballots must be counted to produce election results. The software implemented for the voting scheme has to be coded bug free and designed securely to prevent various attacks. The source code is also opened publicly to prohibit disputes among participants on whether the voting and counting stages are proceeded fairly.
- Individual Verifiability

  Each voter can identify whether his/her vote was counted correctly.
- Universal Verifiability

  All participants can identify whether the election results are correct.

2.2 Partially Computerized Voting [1, 8]

The partially computerized voting (partial e-voting) is introduced to improve the credibility and efficiency of the existing paper based voting. In a partial e-voting scheme, to protect vote selling and vote by coercion, user registration steps and voting activities are configured the same as those of paper based voting.

Though a paper based voting scheme demands a lot of costs, the voter can identify his/her own ballot. If disputes on the election results exist, ballot recounting is also possible. However, in paper based voting, balloting mistakes occur frequently and lower the credibility of the voting system. In a mechanical voting system, the voting machine is used to vote and count the ballot. It can save a lot of costs to manage the election. However, the voter has to trust the machine operates correctly. It can reduce balloting mistakes, but ballot recounting is not possible. The DRE voting machine is an electronic equivalent of a mechanical-lever machine. Many of the reasons for the increased adoption of DRE machines include accessibility and prevention of voter mistakes. DRE machines save precincts the costs associated with producing and securing paper ballots. As with a mechanical-lever machine, no physical record of a voter's intent exists. Unlike a mechanical-lever machine, however, the mechanism for recording a vote is hidden in the code for the machine, which vendors keep secret [8]. The voting software should be opened to the public and coded securely. Thus, studies on how to make secure voting schemes and procedures independent of e-voting software are needed.

2.3 Fully Computerized Voting [1, 12, 14, 15, 16, 17, 18]

In fully computerized voting (full e-voting), all election stages are proceeded on line. With wide spread use of smart phones and Wi-Fi, the need for mobile voting is increased. In Internet based mobile voting, returning officers cannot monitor voter's registration and voting activities. In paper based voting and partial e-voting, returning officers can monitor voting activities since the voting occurs at a designated place. Thus, vote selling and vote by coercion are not possible. The following assumption has to be satisfied to make full e-voting put to practical use.

Assumption 2.1: All participants cannot know who voted for whom, even if they can view voter's ballot and voting activities.

Technically, to satisfy assumption 2.1, the voter must prove to returning officers that only the voter alone can vote. The smart phone can be used to prove that the voter is voting alone by showing the voting place. In full e-voting, voters can participate in the election without time and space constraints. Due to such constraints, theoretical approaches are mainly studied rather than practical approaches. The study on how to protect double voting and voter's privacy was one such approach. Currently, studies on how to implement untraceable channel, individual ballot verification, and receipt-freeness are growing as major issues.

We can know who voted for whom by analyzing the IP address of the packet loaded with each voter's ballot. In electronic voting, the role of untraceable channel is the same as that of the ballot box in the current paper based voting system. It should be designed to forbid participants to trace the packet by shuffling and encrypting incoming packets at the relay server [12]. All voters should verify correctness of voting results from the encrypted ballot.

In addition, receipt-freeness is one of the important requirements to be satisfied to avoid vote selling. Receipt-freeness means that the voter cannot prove to others for whom he/she votes with the receipt.

3. Biometric based Mobile ID

To be used in mobile voting and commerce, the mobile ID should have properties similar to those of a resident card. In **Table 1**, we present the requirements that a mobile ID should have.

Table 1. Mobile ID Requirements

Requirements	Descriptions
Legal binding forces	To open and use the smart phone, the user has to register USIM. The user submits a resident card to the registration center to prove his/her identity. To accomplish legal binding forces, face-to-face user authentication is needed at least once. Thus, application of USIM is a good way to make the legal mobile ID.
Biometric recognition	It's not possible to verify whether the logged in user is real on the internet. To apply to mobile voting, the mobile ID should not be shared with other users. As a result, it's necessary to use the biometric data to authenticate the user.
Cancellable property	Since the user's biometric data is unique, if the data is compromised, then the corresponding biometric data cannot be used again. Thus, to make a biometric based mobile ID holding cancellation and regeneration properties, the mobile ID should be designed to contain the user's token that is randomly generated.

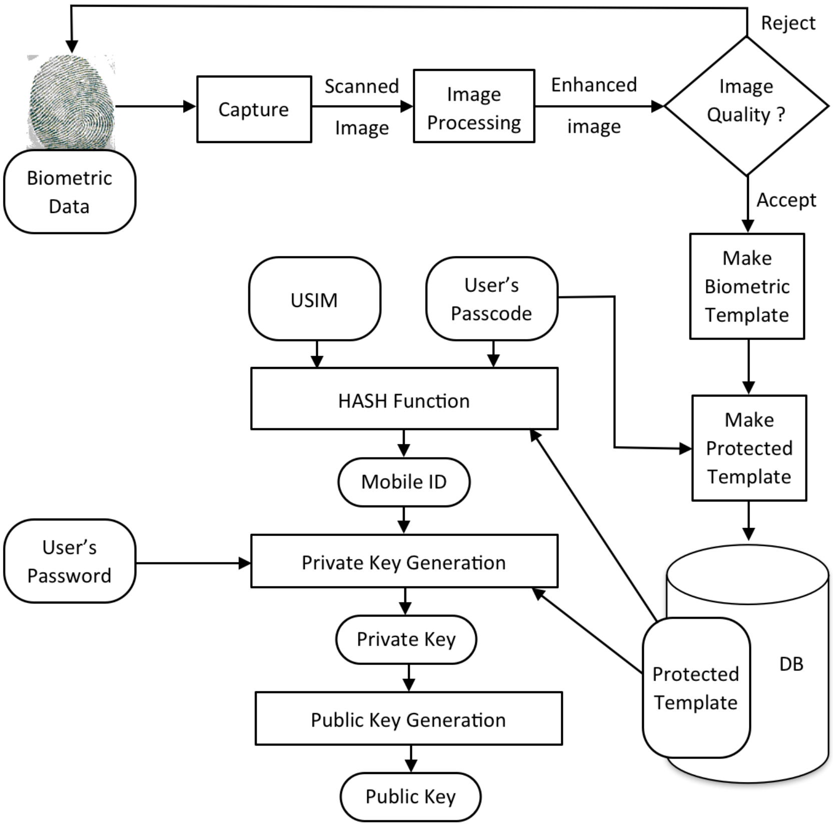

Fig. 1. USIM based Biometric Key Generation

According to the ETSI TS 102.221 standard, a USIM is a smart card that stores the subscriber's identity (IMSI) and computes the AKA authentication algorithm [4, 5]. To activate the phone, the smart phone user should register the USIM card and insert it into the phone. The registration procedure is formal and legally binding. So, the USIM card can be used to represent the phone user's identity.

Fig. 1 shows how to make a mobile ID and related cryptographic keys. The generation steps for mobile ID and pair of digital signature keys are as follows. The proposed scheme satisfies the requirements of **Table 1**.

Assumption 3.1: There exists a trustful Mobile ID Authentication Center (MC). The roles of MC are similar to CA (Certification Authority) of PKI system. These are registration, cancellation, and reissuance of the Mobile ID. The pair of public and private keys is as follows.

Step 1: We assume that a user has a smart phone with a built-in fingerprint scanner. The user's biometric data captured by the fingerprint scanner is converted to the digital image. The noise on the captured image should be reduced through image processing. If quality of the image is acceptable, the fingerprint's end points, bifurcation points and degree of each point are extracted to make the biometric template. Otherwise, the user should restart the step 1.

Step 2: The user's biometric template is enrolled to the DB. In terms of security and privacy, the biometric data should not be stored to the DB in its original form. Because, the biometric data is unique, if the biometric data is disclosed, it cannot be reused any more. It violates the user's privacy. Thus, the original biometric template is transformed to the protected template by using the user's passcode, the random secret value as like [6]. Even if the protected template is disclosed, it's possible that the user can revoke the protected template and make a new protected template by changing the passcode only.

Step 3: The user's mobile ID, the private key, and the public key are generated as follows.

$$\mathrm{ID_U} = \mathrm{H}(\mathrm{USIM_U}, \mathrm{PC_U}, \mathrm{BIO_U}) \in \mathrm{Z}_{p-1}$$

$$\mathrm{sk_U} = \mathrm{H}(\mathrm{ID_U}, \mathrm{PW_U}, \mathrm{BIO_U}) \in \mathrm{Z}_{p-1}, \quad \mathrm{pk_U} \equiv g^{\mathrm{sk_U}} \bmod p$$

Step 4: The user signs the mobile ID with his/her own private key and encrypts it with the MC's public key. The user sends them to the MC.

Step 5: The MC decrypts the encrypted mobile ID with the MC's private key and verifies the signature on it. If the user's signature is valid, the MC signs the mobile ID. Otherwise, the mobile ID is discarded. The MC registers the mobile ID and sends the signed copy to the user.

Step 6: The user verifies the MC's signature on the mobile ID and stores it to the smart phone.

$$\mathrm{sk_{MC}} \in \mathrm{Z}_{p-1}, \quad \mathrm{pk_{MC}} \equiv g^{\mathrm{sk_{MC}}} \bmod p$$

Table 2. Mobile ID Parameters

Terms	Descriptions
$\mathrm{ID_U}$	The user's mobile ID
H	Hash function
$\mathrm{USIM_U}$	The user's USIM
$\mathrm{BIO_U}$	The user's protected template
$\mathrm{PC_U}$	The user's passcode
$\mathrm{PW_U}$	The user's password

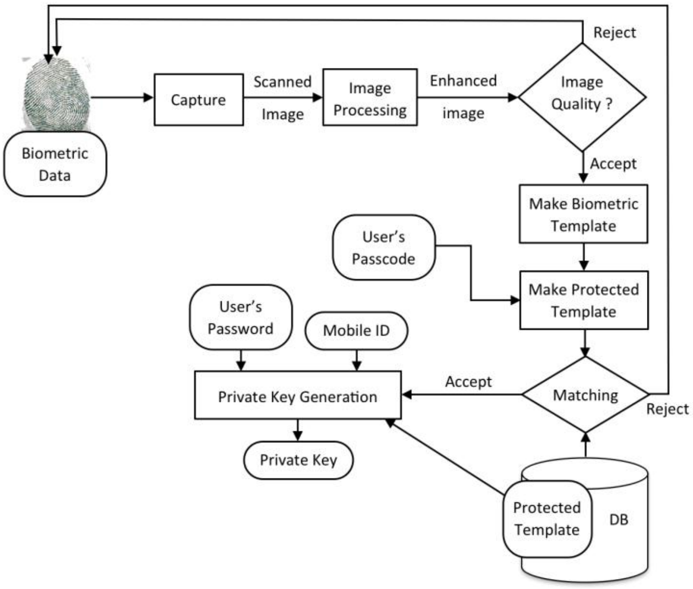

Fig. 2. Private Key Generation with Biometric Recognition

Fig. 2 shows how the signer (the voter) obtains the private key. The private key is needed to sign a document. For security reasons, it's preferable not to store the secret key to the mobile phone even if it's encrypted. In addition, to prove the signer's real identity on line, the signer should authenticate himself/herself through the biometric recognition.

Step 1: The user's biometric data is captured and converted to the digital image. The scanned image is enhanced through noise reduction processing. If quality of the image is acceptable, the biometric template is generated. Otherwise, the user should restart the step 1.

Step 2: The captured biometric template is transformed by using the user's passcode. Even if the same user scans his/her own biometric data multiple times, scanned images almost always are not identical. Thus, matching function is used to compare the transformed template with the protected template in DB. It calculates similarity score and authenticates the user according to the threshold value [6]. If the matching fails, the user should go to the step 1 and restart the procedure.

Step 3: The mobile ID, the protected template, and the user's password are hashed to produce the private key.

4. Proposed Mobile Voting Scheme

In section 4, we propose the voting scheme based on the mobile ID. The proposed scheme consists of preparation, registration, voting, and counting stages.

There are the election administration center (EAC), PKI based CAs, voters, candidates, and vote mixing servers (VMS) in the mobile voting system. EAC has the responsibility for election related works and ballot counting. The CA issues public key certificates to voters, candidates, and the EAC. Voters use the voting app of the smart phone to participate in the election. VMS makes the untraceable channels where the voters' ballots cannot be traced [12].

4.1 Preparation Stage

EAC makes an ID of each candidate. Each voter makes a mobile ID and pair of signature keys. CA issues public key certificates to participants of the election.

Assumption 4.1 : There exists a trustful EAC responsible for voter registration, ballot authentication, and ballot counting.

Assumption 4.2 : There exists a vote mixing server, VMS, between the EAC and voters [12].

Assumption 4.3 : Vote selling and vote by coercion for designated candidate are not possible.

Mobile voting is accomplished on line. This means the EAC cannot confirm the real identity of the voter. Thus, during the voting stage, someone can watch and record the voting activities of the voter. In this case, vote selling and vote by coercion are possible. Thus, to make mobile voting practical, even if someone watches over the voter's voting activities, the ballot of the voter should not be verified.

This requirement is beyond the scope of this paper. In this paper, we propose the voting scheme providing fairness of election ensured by candidates under assumption 4.3. The undeniable multi-signature scheme is applied to satisfy voting fairness.

Table 3. Definition of Voting Components

Components	**Definition**
Candidates	$C = \{C_1, C_2, \ldots\ldots, C_k\}$
Candidates ID	$P = \{P_1, P_2, \ldots\ldots, P_k\}$
Voters	$U = \{U_1, U_2, \ldots\ldots, U_n\}$
Election Administration Center	EAC
Vote Mixing Server	VMS
Ballots	$B = \{B_1, B_2, \ldots\ldots, B_n\}$
Blind ballots	$H = \{H_1, H_2, \ldots\ldots, H_n\}$

Table 4. Pair of Signature Keys

Item	**Signature Keys**	
Candidates	Private Key	$skc_i \in Z_{p-1}$
	Public Key	$pkc_i \equiv g^{skc_i} \bmod p$
Voters	Private Key	$sku_i \in Z_{p-1}$
	Public Key	$pku_i \equiv g^{sku_i} \bmod p$
EAC	Private Key	$skvc_i \in Z_{p-1}$
	Public Key	$pkvc_i \equiv g^{skvc_i} \bmod p$

Assumption 4.4 : There are a number of k candidates and n voters. It is assumed that cryptographically secure galois field GF(p) and generator g exist.

Step 1: Voters, candidates, and the EAC generate digital signature keys, as shown in Table 4. The keys are generated through step 2 of the key generation protocol (**Fig. 1**) defined in section 3.

Step 2: The EAC announces lists of candidates and voters (C, U) to the public board.

Step 3: The EAC requests creation of the PK, the common public key, to the first candidate C_1.

Step 4: The first candidate C_1 computes PK_1 as follows. C_1 sends PK_1 to the second candidate C_2.

$$PK_1 = pkc_1 \equiv g^{skc_1} \bmod p$$

Step 5: The intermediate candidate C_i receives PK_{i-1} from the previous candidate C_{i-1}.

$$PK_{i-1} \equiv PK_{i-2}^{skc_{i-1}} \bmod p, \quad 2 \le i \le k$$

Step 6: The candidate C_i computes PK_i as follows.

$$PK_i \equiv PK_{i-1}^{skc_i} \equiv g^{\prod_{j=1}^{i} skc_j} \bmod p$$

Step 7: The candidate C_i sends PK_i to the next candidate C_{i+1}. The step 5, step 6 and step 7 are repeated until the last candidate C_k computes the PK as follows. Then, the C_k announces the common public key PK.

$$PK \equiv PK_{k-1}^{skc_k} \equiv g^{\prod_{j=1}^{k} skc_j} \bmod p$$

4.2 Undeniable Multi-Signed Ballot Generation

The ballot registration stage consists of generation and registration of the blinded ballot and extraction of the signed ballot. Fig. 3 shows the overall steps of how undeniable multi-signed ballot is generated.

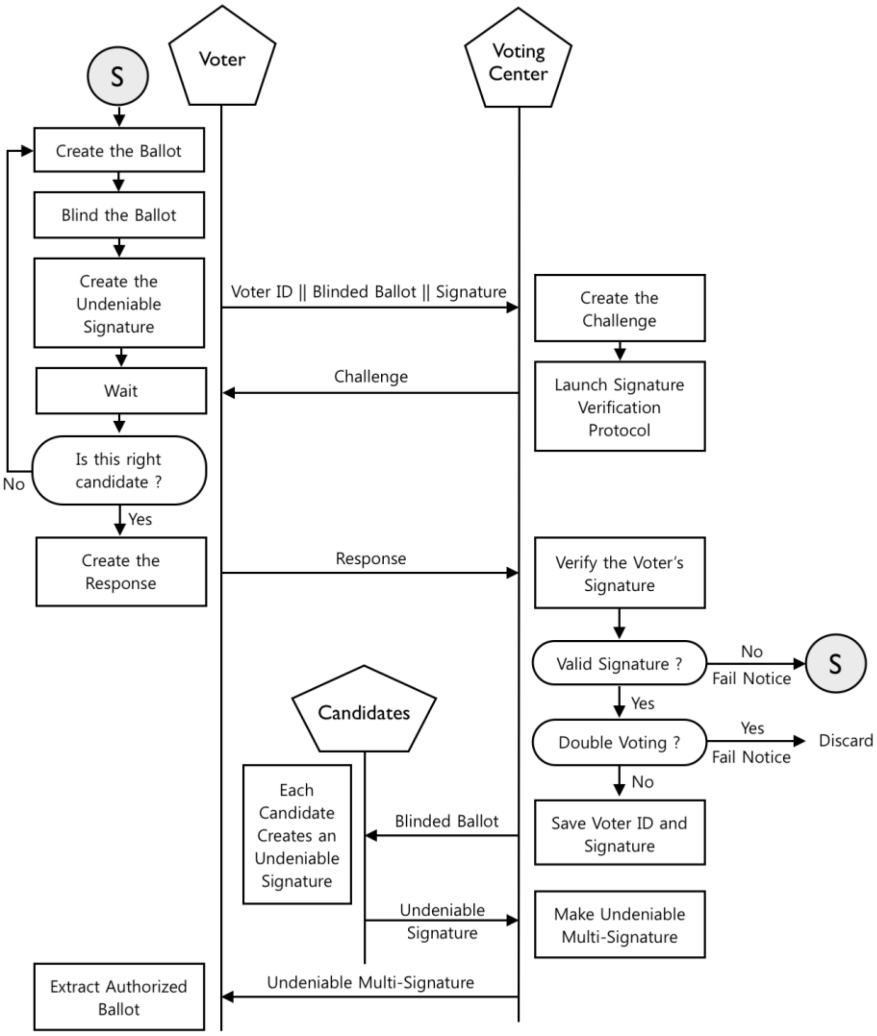
Voter
Voting Center
S
Create the Ballot
Blind the Ballot
Create the Undeniable Signature
Wait
Is this right candidate ?
No
Yes
Create the Response
Voter ID || Blinded Ballot || Signature
Challenge
Response
Create the Challenge
Launch Signature Verification Protocol
Verify the Voter's Signature
Valid Signature ?
No
Fail Notice
S
Yes
Double Voting ?
Yes
Fail Notice
Discard
No
Save Voter ID and Signature
Make Undeniable Multi-Signature
Candidates
Each Candidate Creates an Undeniable Signature
Blinded Ballot
Undeniable Signature
Undeniable Multi-Signature
Extract Authorized Ballot

Fig. 3. Undeniable Multi-Signed Ballot Generation

4.2.1 Blinded Ballot Generation

Step 1: The voter U_V generates the random number ps_V and sets it as the pseudo ID. Then, U_V selects the candidate C_j. The voter U_V generates the ballot B_V by using C_j's pseudo ID P_j with U_V's pseudo ID ps_V.

$$B_v \equiv (P_j \times ps_v)^{ps_v} \bmod p,\ 1 \le j \le k,\ \ 1 \le v \le n$$

Step 2: The voter U_V generates the blinding factor bf_V and blinds the ballot B_V as follows.

$$H_v \equiv {B_v}^{bf_v} \bmod p,\ \ bf_v \times {bf_v}^{-1} \equiv 1 \bmod p-1$$

Step 3: The voter U_V chooses the random number ku_V and keeps it secret. The ku_V should be selected relatively prime to p-1.

Step 4: The voter U_V generates the undeniable signature (SU_V, RU_V) on the blinded ballot H_V. The private key sku_V is generated from the steps in **Fig. 2**.

$$RU_v \equiv {H_v}^{ku_v} \bmod p,\ ku_v\ \in\ Z_{p-1},\ ku_v \times SU_v \equiv sku_v \times RU_v - ku_v \times H_v \bmod p-1$$

Step 5: The voter U_V sends the mobile ID, blinded ballot, and the undeniable signature (SU_V, RU_V) to the EAC.

4.2.2 Registration of the Voter

The EAC verifies the voter U_V's signature as follows.

Step 1: The EAC selects (a, b) at random and generates the challenge ch_V as follows.

$$ch_v \equiv (RU_v)^{a\cdot(H_v+SU_v)} \times {pku_v}^{RU_v\cdot b} \bmod p$$

Step 2: The EAC sends the ch_V to the voter U_V.

Step 3: The voter U_V generates the response rsp_V as follows and sends it to the EAC. The private key sku_V is generated from **Fig. 2**.

$$rsp_v \equiv {ch_v}^{sku_v^{-1}}\ \bmod p$$

Step 4: The EAC makes the following equation. If this equation holds, ther voter's signature is verified as valid. If signature verification fails, the voter's registration is cancelled and the EAC sends failure notification to the voter U_V. Then, the voter should restart the registration stage.

$$rsp_v \equiv (H_v)^{RU_v\cdot a} \times g^{RU_v\cdot b} \bmod p$$

Step 5: The EAC checks the voter's ID so as to know whether the voter has already registered. In case that same voter attempts to register twice, the EAC cancels corresponding registration process and sends failure notification to the voter U_V.

Step 6: The EAC records the voter's mobile ID, blinded ballot, and the signature.

4.2.3 Registration of the Blinded Ballot

Step 1: The EAC sends the voter U_V's blinded ballot H_V to all candidates.

Step 2: The EAC requests creation of the value R to the first candidate C_1. R is used to make an undeniable multi-signature.

Step 3: The first candidate C_1 selects the random number k_1 and creates R_1 as follows. C_1 sends R_1 to the next candidate C_2. The k_1 should be selected relatively prime to p-1 and kept secret.

$$R_1 \equiv {H_v}^{k_1} \bmod p$$

Step 4: The intermediate candidate C_i receives R_{i-1} from the previous candidate C_{i-1}.

$$R_{i-1} \equiv {R_{i-2}}^{k_{i-1}} \bmod p,\ \ 2 \leq i \leq k$$

Step 5: The candidate C_i computes R_i as follows.

$$R_i \equiv {R_{i-1}}^{k_i} \equiv {H_v}^{\prod_{j=1}^{i} k_j} \bmod p$$

Step 6: The candidate C_i sends R_i to the next candidate C_{i+1}. If the C_i is the last candidate, the value R is computed as follows and sends it to the EAC and all candidates.

$$R \equiv {R_{k-1}}^{k_k} \equiv {H_v}^{\prod_{j=1}^{k} k_j} \bmod p$$

Step 7: The candidate C_i computes undeniable signature s_i on the ballot and sends it to the EAC.

$$k_i \times s_i \equiv skc_i \times R - k_i \times H_v \ \bmod p-1,\ \ 1 \leq i \leq k$$

Step 8: The EAC makes the undeniable multi-signature S as follows.

$$S \equiv \prod_{j=1}^{k} (H_v + s_j) \ \bmod p$$

Step 9: The EAC sends the undeniable multi-signature (S, R) to the voter.

4.2.4 Extraction of Authorized Ballot

Step 1: The voter extracts the authorized ballot from the blinded ballot.

$$S_A(B_v) \equiv R^{S\times bf^{-1}\times(R^k)^{-1}} \equiv {H_v}^{bf^{-1}\times(R^k)^{-1}\times\prod_{j=1}^{k} k_j\times(H_v+s_j)} \equiv {B_v}^{\prod_{j=1}^{k} skc_j} \bmod p$$

4.3 Voting

Step 1: The voter generates the challenge ch on the authorized ballot $S_A(B_V)$ as follows. (a, b) is selected at random. PK is the common public key to be used by all candidates.

$$\mathrm{ch} \equiv \mathrm{S_A}(\mathrm{B_v})^{\mathrm{a}} \times \mathrm{PK}^{\mathrm{b}} \bmod \mathrm{p}$$

Step 2: The voter sends the ballot to the EAC together with the challenge through VMS [12].

Step 3: The EAC sends ($S_A(B_V)$, ch) to the first candidate C_1.

Step 4: The first candidate C_1 computes the response rsp_1 as follows and sends it to the second candidate C_2.

$$\mathrm{S_A}(\mathrm{B_v})^{\mathrm{skc}_1^{-1}} \bmod \mathrm{p}, \;\; \mathrm{rsp}_1 \equiv \mathrm{ch}^{\mathrm{skc}_1^{-1}} \bmod \mathrm{p}$$

Step 5: The candidate C_i receives the following responses from the C_{i-1}.

$$\mathrm{S_A}(\mathrm{B_v})^{\prod_{j=1}^{i-1}\mathrm{skc}_j^{-1}} \bmod \mathrm{p}, \;\; \mathrm{rsp}_{i-1} \equiv \mathrm{ch}^{\prod_{j=1}^{i-1}\mathrm{skc}_j^{-1}} \bmod \mathrm{p}, \;\; 2 \le \mathrm{i} \le \mathrm{k}$$

Step 5: The candidate C_i generates the response as follows. The private key skc_i is only obtained by submitting the C_i's biometric data and password from **Fig. 2**.

$$\left(\mathrm{S_A}(\mathrm{B_v})^{\prod_{j=1}^{i-1}\mathrm{skc}_j^{-1}}\right)^{\mathrm{skc}_i^{-1}} \equiv \mathrm{B_v}^{\prod_{j=i+1}^{k}\mathrm{skc}_j} \bmod \mathrm{p}$$

$$\mathrm{rsp}_i \equiv \left(\mathrm{ch}^{\prod_{j=1}^{i-1}\mathrm{skc}_j^{-1}}\right)^{\mathrm{skc}_i^{-1}} \equiv \mathrm{B_v}^{\mathrm{a}\times\prod_{j=i+1}^{k}\mathrm{skc}_j} \times \mathrm{g}^{\mathrm{b}\times\prod_{j=i+1}^{k}\mathrm{skc}_j} \bmod \mathrm{p}$$

Step 6: The candidate C_i sends the response to the next candidate C_{i+1}. If the C_i is the last candidate, the C_k generates the response rsp_k as follows. The rsp_k contains responses of all candidates on the voter's challenge, ch.

$$\mathrm{S_A}(\mathrm{B_v})^{\prod_{j=1}^{k}\mathrm{skc}_j^{-1}} \equiv \mathrm{B_v}^{\prod_{j=1}^{k}\mathrm{skc}_j\times\mathrm{skc}_j^{-1}} \equiv \mathrm{B_v} \bmod \mathrm{p}$$

$$\mathrm{rsp}_k \equiv \mathrm{ch}^{\prod_{j=1}^{k}\mathrm{skc}_j^{-1}} \equiv \mathrm{B_v}^{\mathrm{a}} \times \mathrm{g}^{\mathrm{b}} \bmod \mathrm{p}$$

Step 7: The EAC announces the signature, the ballot, and the response as follows.

$$(\mathrm{S_A}(\mathrm{B_v}), \mathrm{B_v}, \mathrm{rsp}_k)$$

4.4 Counting Stage

Step 1: The voter verifies the response rsp_k. If the response is not valid, disavowal protocol is launched to discriminate whether the signature is modified or some candidates have cheated. If the response is valid, the voter sends pseudo ID ps_V to the EAC through VMS [12].

Step 2: The EAC opens the ballot by using the ps_V. If P_j is in the candidates list P, the EAC adds the ballot to the count of the corresponding candidate. Otherwise, the ballot is discarded.

$$\frac{{B_v}^{{ps_v}^{-1}}}{ps_v} \equiv \frac{\left(P_j \times ps_v\right)}{ps_v} \equiv P_j \text{ mod p}, \quad 1 \le j \le k$$

Step 3: The EAC announces the counting results to the public as follows.

$$(ps_v, P_j, S_A(B_v), B_v)$$

5. Security Analysis and Discussion

In this section, we analyze the security of the proposed scheme and discuss voting fairness assured by candidates.

5.1 Security Analysis

(1) Undeniability

If the ballot is not verified as valid, the voter can launch disavowal protocol so as to discriminate whether the signature is modified or some candidates have cheated. Therefore, candidates cannot collude with other candidates or the EAC.

(Proof) In the voting stage, the first challenge and the response are generated as follows.

$$\text{ch1} \equiv S_A(B_v)^a \times PK^b \text{ mod p}, \quad \text{rsp1}_k \equiv \text{ch1}^{\prod_{j=1}^{k} \text{skc}_j^{-1}} \equiv {B_v}^a \times g^b \text{ mod p}$$

If the verification of the ballot fails, the following disavowal protocol is launched.

Step 1: The voter generates the second challenge ch2 on the authorized ballot $S_A(B_V)$. (c, d) are selected at random. The voter sends the ballot to the EAC together with challenge ch2 through the VMS.

$$\text{ch2} \equiv S_A(B_v)^c \times PK^d \text{ mod p}$$

Step 2: The EAC sends ($S_A(B_V)$, ch2) to the first candidate C_1.

Step 3: The first candidate C_1 computes the response rsp2_1 as follows and sends it to the second candidate C_2.

$$S_A(B_v)^{\text{skc}_1^{-1}} \text{ mod p}, \quad \text{rsp2}_1 \equiv \text{ch2}^{\text{skc}_1^{-1}} \text{ mod p}$$

Step 4: The intermediate candidate C_i receives following responses from the C_{i-1}.

$$S_A(B_v)^{\prod_{j=1}^{i-1} \text{skc}_j^{-1}} \text{ mod p}, \quad \text{rsp2}_{i-1} \equiv \text{ch2}^{\prod_{j=1}^{i-1} \text{skc}_j^{-1}} \text{ mod p}$$

Step 5: The candidate C_i generates responses as follows.

$$(\mathrm{S_A}(\mathrm{B_v})^{\prod_{j=1}^{i-1}\mathrm{skc}_j^{-1}})^{\mathrm{skc}_i^{-1}} \equiv \mathrm{B_v}^{\prod_{j=i+1}^{k}\mathrm{skc}_j} \bmod p$$

$$\mathrm{rsp2}_i \equiv (\mathrm{ch2}^{\prod_{j=1}^{i-1}\mathrm{skc}_j^{-1}})^{\mathrm{skc}_i^{-1}} \equiv \mathrm{B_v}^{c\times\prod_{j=i+1}^{k}\mathrm{skc}_j} \times g^{d\times\prod_{j=i+1}^{k}\mathrm{skc}_j} \bmod p$$

Step 6: The candidate C_i sends responses to the next candidate C_{i+1}. If the C_i is the last candidate, the C_k generates the response $\mathrm{rsp2}_k$ as follows. The $\mathrm{rsp2}_k$ contains responses of all candidates on the ch2.

$$\mathrm{S_A}(\mathrm{B_v})^{\prod_{j=1}^{k}\mathrm{skc}_j^{-1}} \equiv \mathrm{B_v}^{\prod_{j=1}^{k}\mathrm{skc}_j\times\mathrm{skc}_j^{-1}} \equiv \mathrm{B_v} \bmod p$$

$$\mathrm{rsp2}_k \equiv \mathrm{ch2}^{\prod_{j=1}^{k}\mathrm{skc}_j^{-1}} \equiv \mathrm{B_v}^{c} \times g^{d} \bmod p$$

Step 7: The voter computes the following discrimination equations. If the multi-signature is modified, R_1 does not equal to R_2. Otherwise, it means that some candidates have cheated on the valid multi-signature.

$$R_1 \equiv \left(\mathrm{rsp1}_k \cdot g^{-b}\right)^{c} \pmod p\,,\quad R_2 \equiv \left(\mathrm{rsp2}_k \cdot g^{-d}\right)^{a} \pmod p \qquad \text{Q.E.D}$$

(2) Unreusability

The authorized voter cannot vote more than once using the registered ballot.

(Proof) During the registration stage, the EAC checks each voter's ID to prevent multiple registrations. Therefore, a dishonest voter who wants to vote more than once should solve the following equations to make an authorized ballot.

$$\mathrm{S_A}(\mathrm{B_v}) \equiv \mathrm{B_v}^{X} \bmod p\,,\quad X \equiv \prod_{j=1}^{k}\mathrm{skc}_j \bmod p$$

$$X \equiv \log_{\mathrm{B_v}}\mathrm{S_A}(\mathrm{B_v}) \bmod p \qquad (5.1)$$

To solve the equation 5.1, the dishonest voter must solve the discrete logarithms over large prime number p. It's proven that solving discrete logarithms over GF(p) is computationally infeasible [9, 10]. Therefore, the authorized voter cannot vote more than once. Q.E.D.

(3) Privacy

The privacy of each voter is based on the security of the blind protocol and assumption 4.2. If these requirements are fulfilled, then participants cannot determine who voted for whom.

(Proof) In the registration stage, the voter generates the ballot with the voter's pseudo ID. Then, the voter blinds the ballot with the blinding factor. The voter sends blinded ballot to the EAC via VMS. The EAC makes an undeniable multi-signature on the blinded ballot with the help of all candidates. The voter extracts the registered ballot from the multi-signed blinded ballot. The dishonest participants who want to know who voted for whom must find the blinding factor bf as follows.

$$\mathrm{H_v} \equiv \mathrm{B_v}^{\mathrm{bf_v}} \bmod \mathrm{p}\,,\ \ \mathrm{bf_v} \equiv \log_{\mathrm{B_v}} \mathrm{H_v} \bmod \mathrm{p} \quad (5.2)$$

To find the blinding factor $\mathrm{bf_V}$, the dishonest participants must solve equation 5.2. It's proven that solving discrete logarithms over GF(p) is computationally infeasible. We also assume the existence of untraceable network in assumption 4.2. Therefore, dishonest users cannot trace the ballot in order to know who voted for whom. Q.E.D.

(4) Eligibility

Only legally registered voters can vote.

(Proof) In the proposed scheme, the mobile ID is issued to the voter with legally accepted procedures. A pair of digital signature keys are generated based on the mobile ID. The public key is authenticated by PKI based CA. During the registration stage, the voter submits the mobile ID, blinded ballot, and the signature signed with the voter's private key. The EAC determines voter's eligibility by launching signature confirmation protocol. Therefore, an unregistered voter who wants to vote must make a verifiable digital signature. This is only possible if the unregistered voter colludes with the EAC. However, this contradicts assumption 4.1. Q.E.D.

5.2 Discussion

In an election, the most important requirement is that candidates should accept the results of the election. Candidates who represent the party should manage the party's policy and interests. It appears to be a good solution to make voting and counting methods by which candidates can be assured of election fairness on their own.

Existing full e-voting schemes are mainly focused on verification of the ballot by the voter and not by candidates. In the proposed mobile voting scheme, candidates make the ballot by using an undeniable multi-signature scheme. Thus, the voter's ballot cannot be opened without the help of all candidates during the counting stage.

The ordinary digital multi-signature has a self-verification property. Meanwhile, the undeniable signature scheme has a property that the signature on the document cannot be verified without help of the signer [11]. Therefore, even if the undeniable signature is open to the public, participants cannot verify whether this signature is valid or not. Due to this property, the undeniable signature scheme can be used to make receipt of the ballot in an electronic voting scheme. To verify the receipt of the ballot, the signer's consent to signature verification is essential. Candidates make the undeniable multi-signature on the voter's ballot sequentially. Challenge response protocol between the voter and candidates are needed to verify multi-signature. Thus, candidates as well as voters can participate in the voting and counting stages.

In paper based voting, all voters vote at the designated voting place under surveillance of returning officers. Therefore, vote selling is not possible. In mobile voting, a voter has to vote regardless of places with his/her smart phone. Thus, vote selling or vote by coercion is possible.

In this paper, we focus on to solve fairness problem of mobile e-voting. Collusion among two or more candidates or the EAC could compromise election results. Therefore, we think that if candidates agree and could not repudiate on the election results, the fairness of the election is guaranteed. So we use biometric based undeniable multi-signature to solve this problem.

In biometric recognition process, image scanning and enhancement process requires high computation. Not all the mobile phones have high computation capability. Today's smart phones (iPhone, Android phones) are capable of high computation, but other old mobile phones are not. Our method is available with high computation mobile devices such as current smart phones. The increasing capabilities of biometric capture on smart phones such as signature, face, voice, fingerprint, etc. makes biometric recognition practical [3].

6. Conclusion

The electronic voting scheme can save a lot of costs to manage elections and boost the participation of voters. The voter can vote anytime and anywehere with the mobile voting scheme. In this paper, the mobile voting scheme is proposed and the requirements of mobile voting are analyzed.

The proposed scheme consists of mobile ID and digital signature key generation, blinded ballot creation, and verification based on undeniable multi-signature scheme. The mobile ID should have legal binding forces, cannot be lent to other users, and is possible to cancel, reissue, and register it again. The USIM, the biometric data, and the password of the user are applied to make the mobile ID to satisfy its requirements.

The voter creates a pseudo ID so as not to know who voted for whom. Then, the voter selects the candidate to vote for and makes the blinded ballot with the pseudo ID. Candidates make multi-signature on the blinded ballot sequentially. The voter extracts the authorized ballot from the blinded ballot. To verify and open the ballot, multi-signature confirmation protocol is launched. The ballot cannot be verified without help of all candidates. Thus, candidates guarantee the fairness of the election.

In future works, we plan to study how to solve vote-selling problem in the proposed scheme. The validity of the proposed undeniable ballot is only verified with challenge-response protocol, the signature confirmation protocol. The undeniable signature on the ballot itself, even if it is open to the public board with pseudonym, without help of all candidates it can not be verified. We think that to avoid vote selling in full e-voting, firstly the voter prove to the returning officers that he/she alone vote. This can be achieved by showing the voting place using mobile phone. Secondly, the voter could not prove to the third party that to whom he/she vote. This property can be satisfied if the third party cannot analogize the voter's intent from the voting results.

References

[1] J. Tepandi, I. Tšahhirov and S. Vassiljev, "Wireless PKI Security and Mobile Voting," *IEEE Computer*, vol. 43, no. 6, pp. 54-60, June, 2010. Article (CrossRef Link).

[2] R. Want, "iPhone: Smarter Than the Average Phone," IEEE Pervasive Computing, vol. 9, no. 3, pp. 6-9, July, 2010. Article (CrossRef Link).

[3] C. Vivaracho-Pascual and J. Pascual-Gaspar, "On the Use of Mobile Phones and Biometrics for Accessing Restricted Web Services," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 42, no. 2, pp. 213-222, Mar. 2012. Article (CrossRef Link).

[4] The 3GPP Project, "Characteristics of the USIM Application," *3GPP TS 31.02, http://www.3gpp.org/ftp/Specs/html-info/31102.htm.*

[5] P. Urien, "Convergent identity: Seamless OPENID services for 3G dongles using SSL enabled USIM smart cards," *IEEE CCNC*, pp. 830–831, Jan. 2011. Article (CrossRef Link).

[6] N. K. Ratha, J. H. Connell and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614-634, 2001. Article

(CrossRef Link).

[7] E. Maler and D. Reed, "The Venn of Identity: Options and Issues in Federated Identity Management," *IEEE Security & Privacy*, vol. 6, no. 2, pp. 16-23, March, 2008. Article (CrossRef Link).

[8] D. Evans and N. Paul, "Election Security: Perception and reality," *IEEE Security & Privacy*, vol. 2, no. 1, pp. 24-31, Jan. 2004. Article (CrossRef Link).

[9] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, Nov. 1976. Article (CrossRef Link).

[10] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469-472, Jul. 1985. Article (CrossRef Link).

[11] D. Chaum and H. Antwerpen, "Undeniable Signatures," *Advances in Cryptology*, CRYPTO'89, LNCS 435, Springer, pp. 212-216, 1990. Article (CrossRef Link).

[12] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, Vol. 24, No. 2, pp. 84-90, Feb. 1981. Article (CrossRef Link).

[13] S. H. Yun, "The USIM based Biometric Multi-Signature for Mobile Content Authentication," ICONI 2011, pp. 137-141, 2011.

[14] B. C. Lee, K. J. Kim, "Receipt-Free Electronic Voting Scheme with a Tamper-Resistant Randomizer," *ICISC 2002*, LNCS 2587, Springer, pp. 389- 406, 2003. Article (CrossRef Link).

[15] A. Baraani-Dastjerdi, J. Pieprzyk and R. Safavi-Naini, "A Secure Voting Protocol Using Threshold Schemes," In *Proc. of COMPSAC'95*, pp. 143-148, 1995.

[16] P. Horster, M. Michels and H. Petersen, "Blind Multisignature Schemes and Their Relevance for Electronic Voting," In *Proc. of COMPSAC'95*, pp. 149-155, 1995.

[17] A. Fujioka, T. Okamoto and K. Ohta, "A practical secret voting scheme for large scale elections," Advances in Cryptology, AUSCRYPT'92, LNCS 718, Springer, pp. 244-251, 1993. Article (CrossRef Link).

[18] C. Boyd, "A New Multiple Key Cipher and an Improved Voting Scheme," Advances in Cryptology, EUROCRYPT'89, LNCS 434, Springer, pp. 617-625, 1990. Article (CrossRef Link).

[19] S. H. Yun, H. S. Lim, Y. S. Jeong, S. Y. Jung and J. K. Chang, "The Biometric Based Convertible Undeniable Multi-Signature Scheme to Ensure Multi-Author Copyrights and Profits," *Wireless Personal Communications*, Springer, vol. 60, no. 3, pp. 405-418, Oct. 2011. Article (CrossRef Link).

[20] A. Juels and M. Sudan, "A Fuzzy Vault Scheme," *Designs, Codes and Cryptography*, Kluwer, vol. 38, no. 2, pp. 237-257, Feb. 2006. Article (CrossRef Link).

[21] ITU-T X.1088, (2008). A Framework for biometric digital key generation, ITU-T.