Pseudo-Voter Identity (PVID) Scheme for e-Voting Protocols

Orhan Cetinkaya
Institute of Applied Mathematics,
METU, Ankara, Turkey
e113754@metu.edu.tr

Ali Doganaksoy
Department of Mathematics,
METU, Ankara, Turkey
aldoks@metu.edu.tr

Abstract

Voter anonymity, also known as unlinkability, is the primary requirement to satisfy privacy in e-voting protocols. Up until now, e-voting protocols have tried to make communication channels anonymous in order to keep voter's identity hidden and many protocols have been proposed to construct anonymous communication channels. On the other hand, instead of making channel anonymous if we provide anonymous credentials to voter, we can easily hide voter's identity without any need of anonymous channels.

This paper introduces Pseudo-Voter Identity (PVID) scheme based on blind signature in order to achieve anonymity in e-voting protocols. Blind signature is applied on pseudo identities selected by voter. Therefore voter obtains blindly signed pseudo identities namely PVIDs and uses them throughout the entire communication with the authorities. By using PVID scheme, e-voting protocols do not need anonymous channels anymore.

This work aims at bringing unlinkable pseudo-voter identities based on blind signature bear on anonymous e-voting protocols.

1. Introduction

Electronic voting (e-voting) is a challenging topic in advanced cryptography. The challenge arises primarily from the need to achieve voter anonymity, in other words to remove voter's identity from his cast ballot, in order to ensure voter privacy. Therefore, e-voting has been intensively studied in the last decades.

In the literature, many e-voting protocols have been proposed fulfilling the anonymity requirement which means that voter can use the e-voting system without disclosing his identity. Most of the proposed protocols rely on anonymous channels to achieve the anonymity. However, anonymous channels add sizeable complexity to the protocol and their implementations need expensive operations and complex calculations.

Anonymity is the primary requirement of the e-voting protocols in order to satisfy voter privacy. A secure electronic voting protocol should not allow opportunities for fraud and should not sacrifice voter privacy which can be stated as unlinkability between any particular voter and his cast vote. Therefore, keeping voter identity hidden is the crucial problem of e-voting. Privacy is a vital requirement in e-voting protocols as nobody can know voter's cast vote. So it should be impossible to reveal and prove the relationship between voter and his vote. This is the principal requirement for both paper based voting and e-voting. Any proposed e-voting protocol should satisfy this requirement.

In usual e-voting protocols, voter generally uses his real identity while communicating with the authorities. Up until now, e-voting protocols have tried to make communication channels anonymous in order to keep voter's privacy hidden. Hence, many protocols have been proposed to construct anonymous communication channels. On the other hand, instead of making channel anonymous if we provide anonymous credentials to voter, we can easily achieve voter's privacy without any need of anonymous channels.

In this paper, we propose Pseudo-Voter Identity (PVID) scheme based on blind signature in order to achieve anonymity in e-voting protocols. E-voting protocols, which employ PVID scheme, do not need any anonymous channels anymore. In PVID scheme, voter prepares a list of blinded identities and then he obtains blind signature for each of them separately by interacting with the approval authority in one session. Later, voter extracts anonymous pseudo identities (PVIDs) which are unlinkable to voter's registration identity. Each PVID is selected by the voter and blindly signed by the approval authority. Thus, nobody knows the value of PVID except voter.

In existing e-voting protocols, voter generally uses his real identity while communicating with the authorities. On the other hand, in PVID scheme, voter

uses anonymous pseudo identities, which have no relation with the voter's real identity and are unlinkable to it. Voter can use them throughout the entire communication and he can easily hide his real identity. Hence, PVID scheme provides anonymity without requiring any complex cryptographic mechanisms and computational operations. It employs only blind signature.

Anonymous channels were introduced by Chaum [13]. Since then, many protocols and implementations have been proposed to construct anonymous channels such as mix-nets [5], [14], [15], [16], [18]. However, all these protocols and implementations need expensive operations and complex calculations. Moreover, anonymous channels are not easy to set up and add substantial complexity to the protocol. For example, in mix-nets, many mix servers are needed. The cast votes are forwarded via a sequence of mix servers. All incoming messages are rearranged before being forwarded to the next mix server and to the final destination. Depending on the number of mix servers and rearrangement computation, many encryption and decryption operations should be done. In order to satisfy anonymity, the basic assumption is at least one mix server is trustable; otherwise some additional work should be done. On the other hand, PVID scheme only needs blind signature and the cost of blind signature operations is relatively small and inexpensive in terms of calculations and computations.

Up to now, several election protocols based on blind signature have been proposed [1], [2], [3], [19], [20]. All these protocols employ blind signature on voter's vote or part of it. On the other hand, we employ blind signature on voter's identity. The idea behind blind signature based protocols is that the voter prepares a ballot stating for whom he wishes to vote. He then interacts with an authentication authority who issues a blind signature on the ballot. Informally, this means that the voter obtains the authority's digital signature on the ballot, without the authority learning any information about the content of the ballot. Finally, all voters send their ballots to another authority that is responsible for counting votes. In order to preserve the privacy of voters, this must be done through an anonymous channel. After all ballots have been collected, votes can be counted directly. In the proposed work, blind signature scheme is applied on voter's pseudo identities and so, voter obtains blindly signed pseudo identities, and uses them throughout the entire communication with the authorities.

In order to satisfy anonymity requirement in the e-voting protocols, homomorphic encryption is employed as an alternative to anonymous channels [6], [7], [8], [9]. In homomorphic encryption based e-voting protocols, a combination of encrypted votes yields accumulation of votes. The voting result is then obtained from the accumulation of votes, while no individual ballot is opened and the corresponding individual vote remains secret. However, e-voting protocols based on homomorphic encryption have quite high communication complexity. Moreover, these protocols are generally suitable for yes-no or 1-out-of-L voting types. Homomorphic encryption based e-voting protocols are efficient when the number of candidates or choices is small. However, they have a drawback where each vote must be checked to be valid, since without validation, correctness of the tallying cannot be guaranteed. When the number of candidates or choices is large, computational and communicational cost for the proof and vote validation is so high that homomorphic voting becomes less efficient.

The proposed scheme uses neither anonymous channels nor homomorphic encryption in order to achieve anonymity. It only employs blind signature and provides a practical way of assuring anonymity in e-voting protocols.

The remainder of the paper is organized as follows. The next section provides overview of the cryptographic mechanisms used in PVID scheme. In Section 3, the PVID scheme is introduced. Then, it is illustrated that how to apply the PVID scheme to Fujioka *et al.* e-voting protocol as a case study. Next, some security requirements are discussed. Finally, conclusions are drawn and future work is suggested.

2. Background

2.1. Anonymous Channels in E-Voting Protocols

In the literature, many e-voting protocol proposals construct their protocols based on an efficient verifiable anonymous channel assumption. Therefore, several techniques have been proposed in order to achieve anonymous communication. The most common solution is mix-nets which were originally introduced by Chaum [5].

The main idea of mix-nets is to permute and shuffle the messages in order to hide the relation between the message and its sender. A mix-net generally consists of a set of mix servers. The details of mixing protocol implementation change depending upon the configurations of mix-nets. The first mix-nets were decryption mix-nets [5] where messages are wrapped in several layers of encryption and then route through mix servers each of which remove the outer layer of encryption and then forward them in random order to the next one. In decryption mix-nets, decryption in

each mix server is repeated until all layers are removed. "Onion routing" is an implementation of decryption mix-nets [14], [15]. Later re-encryption mix-nets were introduced [16], where the incoming messages are re-encrypted in each mix server instead of decrypting them. In re-encryption mix-nets, decryption occurs after shuffling has been completed.

The major drawback of the decryption and re-encryption mix-nets is that one server may compromise and cheat by removing or replacing any number of items. Hence, mix-nets are extended to be verifiable [18]. In verifiable mix-nets, a mix server additionally has to prove in zero knowledge that decryption/re-encryption and shuffling of the inputs are done correctly. There are several approaches to achieve verifiable mix-nets; the main difficulty in these approaches is efficiency of proof techniques.

2.2. Cryptographic Mechanisms

RSA is used as a public key cryptosystem. A random number generator is used to feed PVID with a random number. Blind signature scheme is used to obtain Registration Authority's signature. Threshold cryptography is employed in order to prevent Registration Authority corruption. Blind signature scheme and threshold cryptography are explained in detail.

2.2.1. Blind Signatures. The concept of blind signature was introduced by Chaum [13] as a method to digitally authenticate a message without knowing the contents of the message. A distinguishing feature of blind signatures is their unlinkability: The signer cannot drive any association between the signing process and the signature, which is later made public. In other words, blind signatures are the equivalent of signing carbon paper lined envelopes. Writing a signature on the outside of such envelope leaves a carbon copy of the signature on a slip of paper within the envelope. When the envelope is opened, the slip will show the carbon image of the signature.

The blind signature scheme, based on RSA, briefly, is as follows. Suppose Alice has a message m that she wishes to have signed by Bob. Alice does not want Bob to learn anything about m. Let (e, n) and (d, n) be Bob's public and private keys respectively.

- Alice generates a random number r such that $gcd(r,n)=1$, and calculates $x = (r^e\, m) \bmod n$ and then sends x to Bob. The value x is "*blinded*" by the random value r; hence Bob cannot derive any useful information from it.
- Bob signs x as $t = x^d \bmod n$, and then sends t to Alice.
- Alice reads t. Since $t = x^d \bmod n = (r^e m)^d \bmod n = r^{ed} m^d \bmod n = r m^d \bmod n$, she obtains the true signature s of m by computing $s = r^{-1} t \bmod n = m^d \bmod n$. This is the sign of m.

2.2.2. Threshold cryptography. The (t, n)-threshold cryptography [11], [12] is used to distribute highly sensitive secret information (i.e. a secret key) and computation (i.e., decryption or signing operations) between n participants in order to remove single point of failure so that only when more than t participants come together, the secret can be reconstructed and the computation can be performed. The required trust in the cryptographic service is distributed among the group of authorities in such a way that:

- Any $t-1$ or fewer participants cannot figure out the secret and perform operation;
- Only t or more participants can reconstruct the secret information and perform operation.

Threshold cryptography can be used to distribute signature operations among several participants. In order to sign a message m more than t participants execute an interactive signature generation protocol by using their secret shared keys and obtain the signature of m that can be verified by anybody using the public key. One of the key features of threshold cryptography is robustness since even t corrupt participants cannot learn any information about the secret key or cannot forge a valid signature.

3. Pseudo-Voter Identity (PVID) Scheme

Prior to explaining the PVID scheme, we briefly depict the definitions of anonymity, anonymous, pseudonymity, pseudonym, pseudonymous.

Anonymity: "Anonymity ensures that a subject may use a resource or service without disclosing its user identity." [10].

Anonymous: A subject can be said to be anonymous towards another subject in a particular transaction if his identity in that transaction is concealed from that other subject. Anonymity of any subject is thus always considered and specified with respect to one or more specific other subjects in the transaction. [17]

Pseudonymity: "Pseudonymity ensures that a subject may use a resource or service without disclosing its identity, but can still be accountable for that use. The subject can be accountable by directly being related to a reference (alias), or by providing an alias that will be used for processing purposes, such as an account number." [10].

Pseudonym: A pseudonym is an identifier with a local meaning. A user may choose or create his

pseudonym; or, organizations issuing certificates or credentials may create pseudonyms for users. [17]

Pseudonymous: A transaction carried out under a pseudonym is a pseudonymous transaction. The use of pseudonyms assumes that it is not trivial, for at least some participants in the system or for outsiders, to derive a real identity from the pseudonym. According to the definition of anonymity, the user in a pseudonymous transaction is anonymous towards the party or parties that cannot map the pseudonym used to the user's real identity. [17]

We proceed by stating the definitions used in the proposed scheme: Pseudo-Voter, Pseudo-Voter Identity, and Pseudo-Voter Identity List.

Pseudo-Voter is a voter who has anonymous credentials to access to the voting system. It can be called as anonymous voter instead of pseudo-voter; however, this may cause some misunderstandings since voter selects his identity. So, we prefer to use "*Pseudo*".

Pseudo-Voter Identity (PVID) is an identity used by Pseudo-Voter. More precisely, PVID is an anonymous pseudo identity which is unlinkable to voter's registration identity. In other words, PVID is an unlinkable pseudonym that nobody can map it to the voter's registration identity. PVID is selected by the voter and blindly signed by Registration Authority. Thus, nobody knows the value of PVID except voter. When voter employs PVID scheme, he obtains anonymous pseudo credentials, so we call him as pseudo-voter instead of voter. He is a real voter but the identity used is pseudo.

Pseudo-Voter Identity List (PVID-list) is a list of PVIDs used to interact with the e-voting authorities. PVID-list is employed so as to prevent the e-voting authorities' corruption and to strengthen the accuracy and fairness in the e-voting protocols.

Voter has a registration identity (RegID) which can be any widely used identity such as social security number. On the election day, voter uses his RegID to authenticate himself to the system. To the best of our knowledge, in almost all blind signature based e-voting protocols, voter tries to obtain blindly signed ballot and/or his cast or part of them. In PVID scheme, voter only obtains a list of blindly signed anonymous pseudo identities and uses them instead of real RegID while interacting with the authorities.

We employ a Registration Authority to issue blind signature on voter's PVID-list after checking voter's eligibility. We assume that Registration Authority is trusted. Otherwise, it can blindly sign ineligible people's PVID-lists without being detected. The trustiness can be achieved by using threshold cryptography. Hence, threshold cryptography is applied to distribute the authority over *n* participants. In order to sign any request at least *t* participants should come together. In this case, *t* over *n* participants should be corrupted to issue fake PVIDs.

Mainly, any voting process can be divided into 3 stages: "voter authentication & authorization", "vote casting" and "counting". By using PVID scheme, we clearly distinguish the authentication and authorization stage from voting stage. As soon as obtaining PVID-list, voter can vote at any time by providing PVIDs to the voting authorities. The voting authorities only check Registration Authority's signature on the PVIDs. From now on, voter becomes anonymous voter without need of anonymous channel as PVID scheme provides anonymity. Voter uses the voting system twice by using RegID and PVIDs respectively. RegID is used in order to communicate with Registration Authority for authentication purposes and PVIDs are used for communicating with the remaining authorities.

The proposed Pseudo-Voter Identity (PVID) scheme is shown in Figure 1.

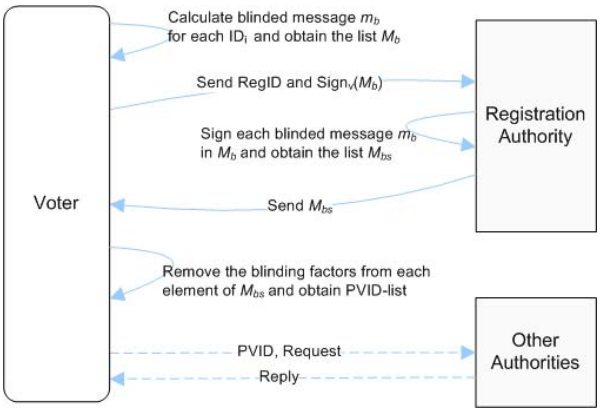

Figure 1. Overview of PVID scheme.

We formally define PVID scheme by using the following notation.

$Sign_v(m)$: message *m* is signed by the voter.

(e, n), (d, n): Registration Authority's public and private keys.

ID-list = $\{ID_1, ID_2 \ldots ID_k\}$ where ID_i is i^{th} identity chosen by the voter.

PVID-list = $\{PVID_1, PVID_2 \ldots PVID_k\}$ where $PVID_i$ is i^{th} PVID which is blindly signed identity by Registration Authority.

PVID-list is a list of blindly signed identities and it is required to be random and unique for each voter. Hence, each ID contains a big random number in addition to the election data which uniquely specify the election. Election data can be some pre-determined keywords such as election name, election date, election id …etc. Voting authorities can simply check PVID by applying Registration Authority's public key.

The number of PVIDs used in the e-voting protocol varies regarding to the protocol details. For instance, some protocols have more than one authority such as ballot distributor, key generator, counter, verifier … etc. We employ different PVIDs instead of a single PVID for each authority in order to prevent any corrupted authority to impersonate the voter. Hence, each ID contains authority data which specify the purpose of the PVID and can be authority name, authority's public key …etc.

If the e-voting protocol has just a single authority, ID-list and PVID-list become single element lists. Each e-voting protocol should have at least one authority; otherwise, voter could not cast his vote. So, the number of elements in PVID-list is at least one.

Each ID contains the election data, authority data (the details about the usage purpose) and a big random number, so it is constructed as following.

ID_i = *(Election Data, Authority Data, Random Number)*

Now, voter has an ID-list that he wishes to have signed each ID_i in the list by Registration Authority. Voter does not want Registration Authority to learn anything about ID_i.

i.) Voter generates a random number r and calculates blinded message m_b for each ID_i, and obtains a list of blinded IDs which is M_b:

$$m_b = (r^e[ID_i]) \bmod n \quad \text{where} \quad \gcd(r,n) = 1$$
$$M_b = \{m_{b_1}, m_{b_2}, ..., m_{b_k}\}$$

Voter signs the list M_b and obtains $\text{Sign}_v(M_b)$. Then, he encrypts his RegID and the $\text{Sign}_v(M_b)$ with Registration Authority's public key and sends it to Registration Authority. The value m_b is *"blinded"* by the random value r; hence Registration Authority cannot derive any useful information from it.

ii.) Registration Authority decrypts the received message and checks voter's signature and obtains the voter's RegID and the blinded ID list M_b. Registration Authority verifies voter's eligibility. If voter is eligible and has not made any request yet, Registration Authority signs each blinded message m_b in the list M_b and calculate m_{bs}. Subsequently, Registration Authority obtains a list of blindly signed IDs which is M_{bs}:

$$m_{bs} = m_b{}^d \bmod n$$
$$M_{bs} = \{m_{bs_1}, m_{bs_2}, ..., m_{bs_k}\}$$

Then Registration Authority encrypts the list M_{bs} with the voter's public key and sends it to the voter.

iii.) Voter decrypts the received message and obtains the blindly signed ID list M_{bs}. Voter can easily obtain PVIDs, the true sign of *IDs,* by removing the blinding factor r from each m_{bs}. Voter carries out the following operations for each m_{bs} in the list M_{bs} in order to obtain $PVID_i$ for each ID_i.

$$m_{bs} = m_b{}^d \bmod n = (r^e[ID_i])^d \bmod n$$
$$m_{bs} = r^{ed}[ID_i]^d \bmod n = r[ID_i]^d \bmod n$$
$$PVID_i = r^{-1} m_{bs} \bmod n = [ID_i]^d \bmod n$$

$PVID_i$ is the sign of voter's selected ID_i. Later voter populates PVID-list with PVIDs.

When voter uses his PVID, the authority only checks signature on the PVID. To prevent timing attacks, voter can keep PVID for a while then use it to cast his vote at any time during the election period. The voter, after waiting for a random amount of time, sends his vote to the counting authority.

In any e-voting protocol, authorities can be grouped as registration, voting and counting authorities. An anonymous channel should be used in between voter and counting authorities in e-voting protocols which rely on anonymous channel. Therefore voter could not communicate directly with counting authorities. On the other hand, in PVID scheme, voter is able to communicate directly with the counting authorities without any hesitation, since the PVIDs are unlinkable pseudo identities and voter himself is pseudo-voter.

PVID scheme is highly flexible and is applicable for both voting pool type elections and wide area network based elections. If the election takes place in an uncontrolled and unsupervised environments e.g., in the Internet, nothing could prevent coercibility and vote selling. In order to overcome this problem, recasting of votes eliminates coercibility problem in the uncontrolled environments since nobody can know whether the current vote will be the final one.

Due to the fact that PVID is not voter's real identity and counting authorities can keep PVIDs, PVID scheme allows vote recasting. Counting authorities store voter's vote with the associated PVID during the election period. It does not violate voter privacy as voter uses PVID. When voting authorities allow vote recasting then if someone coerces voter, voter casts by that way. Later, he can change his vote, by recasting a new one and overwriting the old one. Same logic can be applied to vote selling. So, practically there is no point to coerce voter or to buy vote from voter. PVID scheme makes vote selling more difficult, because the

buyer now has to lock the seller until the end of the election to prevent the seller from changing his vote.

PVID scheme is successfully applied in a recently proposed e-voting protocol [4]. However, we will apply PVID scheme to one of the extensively studied milestone protocol [1] in order to demonstrate how PVID scheme can easily be replaced with anonymous channels.

3.1. Case Study: Applying PVID Scheme to Fujioka et al. Protocol

Fujioka *et al*. proposed an e-voting protocol which uses blind signature scheme and anonymous communication channel [1]. Prior to applying PVID scheme to the protocol, we give a short description about the protocol; more details can be found in the original work [1]. In the proposed protocol, voter prepares a ballot x_i as following. He selects his vote v_i and applies bit commitment scheme for v_i by encrypting it with randomly chosen bit commitment secret key k_i. Then, voter blinds x_i with a random number r_i and obtains blinded ballot e_i. Voter then signs e_i and sends <ID, e_i, $\text{Sign}_v(e_i)$> to Administrator.

Administrator verifies that the signature belongs to a registered voter who has not yet voted. If the ballot signature $\text{Sign}_v(e_i)$ is valid, Administrator extracts e_i by applying voter's public key. Then Administrator obtains $\text{Sign}_a(e_i)$ by signing the ballot e_i and returns it to voter. Voter removes the blinding factor r_i to retrieve an encrypted ballot y_i signed by Administrator. The voter then sends the resultant signed encrypted ballot y_i and x_i to Counter through an anonymous channel.

Counter checks the signature on the encrypted ballot. If the check succeeds, Counter places <x_i, y_i> on a list that is published after all voters vote and is accessible by voters. Afterwards voter checks that his ballot is listed on the list and then sends Counter the bit commitment decryption key necessary to open his ballot through an anonymous channel.

After the voting is completed, counter decrypts the ballots with the keys sent by voters and adds the votes to the election tally. Then Counter publishes the signed encrypted ballots, encrypted ballots, the decryption keys and votes as a list of <y_i, x_i, k_i, v_i> so that voters may independently verify the election results.

The protocol needs anonymous communication channel while sending votes and keys. When we apply PVID scheme to the protocol, voter does not need to obtain blindly signed vote since he is a pseudo-voter, and so he does not have to communicate with Administrator.

Firstly, the voter obtains a PVID-list by employing PVID scheme. Later he selects his vote v_i and applies bit commitment scheme for v_i by encrypting it with a randomly chosen bit commitment secret key k_i and so he obtains a ballot x_i. Instead of using anonymous channel, voter sends Counter the ballot x_i associated with his PVID. Counter checks the PVID. If it is valid, then Counter publishes <x_i> on a list. Voter verifies his ballot and then sends Counter his bit commitment decryption key along with his PVID. Counter counts the votes and announces the results <x_i, k_i, v_i>.

When we apply PVID scheme to the protocol, we obtain a slightly modified protocol which keeps fulfilling all security properties mentioned in the original proposal. Furthermore, voter can change his vote during the election period by recasting. Counter only counts the latest submission.

4. Discussion

Anonymity in PVID scheme relies on unlinkability between voter's pseudo identity and real identity. In order to prove any relation between them, the random number used to create blinded message should be known. Otherwise, adversary should break RSA cryptosystem since PVID scheme uses blind signature based on RSA public key cryptosystem, which is infeasible. The random number is generated by voter and nobody knows it.

In this study, we do not propose an e-voting protocol. However, any e-voting protocol which employs PVID scheme can easily fulfill some of the e-voting requirements in advance without requiring any extra work or with some small effort, such as privacy, uniqueness, eligibility and uncoercibility.

Privacy (A particular voter and his cast vote are unlinkable.): Registration Authority issues a blind signature on voter's blinded ID after checking voter's eligibility. Registration Authority is a trusted authority. The trustiness is achieved by the help of threshold cryptography. Since the blind signature scheme is used, any particular RegID is not linkable to any PVID and any particular PVID is not linkable to any RegID. Voter uses his PVID in voting process, and does not use his RegID. Revealing the RegID is equivalent to breaking RSA.

Eligibility (Only eligible and authorized voters can vote.): Registration Authority issues a blind signature on voter's blinded IDs after verifying voter's eligibility. Only eligible voters' blinded IDs are blindly signed by Registration Authority. Ineligible people's blinded IDs cannot be signed without being detected since threshold cryptography is applied to distribute the authority over n parties. In order to sign any request

at least *t* parties should assemble. In this case, *t* over *n* parties should be corrupted to issue a fake PVID.

Uniqueness (Only one vote for each voter is counted.): Each encrypted vote cast to the counting authorities is attached with a unique PVID. Even if recasting is allowed in PVID scheme, in the counting stage only one vote, possibly the last vote depending on the election policy, is counted.

Uncoercibility (Voter cannot be coerced to cast his vote in a particular way.): When the voting authorities allow vote recasting then if someone coerces voter, voter casts by that way. Afterwards, he can change his vote by recasting new one and overwriting the old one. Similarly, same logic can be applied to vote selling. So, practically it is not possible to coerce the voter or to buy vote from the voter, since nobody can know whether the current vote will be the final one or not. Hence, there is always a trade-off between uncoercibility and vote recasting.

5. Conclusion

In order to satisfy anonymity requirement in e-voting protocols, PVID scheme provides PVIDs which are anonymous pseudo identities and blindly signed by Registration Authority. The proposed PVID scheme is applicable to virtually any e-voting protocols that use anonymous channels. By using PVID scheme, practical and adequate e-voting protocols, satisfying all fundamental requirements can be proposed as well.

As a future work, we are planning to implement a prototype in order to be ready to use in the e-voting protocols. Based on this work, we will also illustrate that the PVID scheme performance is reasonably much more efficient compared with the existing anonymous channel implementations.

6. References

[1] A. Fujioka, T. Okamoto, and K. Ohta, "A practical secret voting scheme for large scale elections," *In Advances in Cryptology Auscrypt'92*, Gold Coast , Australia, pp. 244-251, 1992.

[2] L. Cranor, and R. Cytron: "Sensus: A security-conscious electronic polling system for the Internet," *Hawaii International Conference on System Sciences,* Wailea, Hawaii, 1997.

[3] O. Cetinkaya, and Ali Doganaksoy, "A practical privacy preserving e-voting protocol using dynamic ballots," *2nd National Cryptology Symposium,* Ankara, Turkey, 2006.

[4] O. Cetinkaya, and A. Doganaksoy, "A practical verifiable e-voting protocol for large scale elections over a network," *ARES'07,* Vienna, Austria, 2007.

[5] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of ACM*, Vol. 24, pp. 84-88, 1981.

[6] J. Benaloh, and D. Tuinstra, "Receipt-free secret-ballot elections," *Proc. of the 26th ACM Symp. on the Theory of Computing*, 544-553, 1994.

[7] R. Cramer, R. Gennaro, and B. Schoenmakers, "A secure and optimally efficient multi-authority election scheme," *EUROCRYPT'97*, Konstanz, Germany, pp. 103-118, 1997.

[8] A. Acquisti, "Receipt-free homomorphic elections and write-in voter verified ballots," *ISRI Technical Report CMU-ISRI-04-116,* School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, USA, 2004.

[9] M. Hirt, and K. Sako, "Efficient receipt-free voting based on homomorphic encryption", *EUROCRYPT'00*, Bruges, Belgium, pp. 539-556, 2000.

[10] ISO/IEC 15408-2, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements, http://www.iso.org, 2005.

[11] A. Shamir, "How to share a secret", *Comm. ACM*, 22(11):612613, 1979.

[12] Y. Desmedt, and Y. Frankel, "Threshold cryptosystems", *In Advances in Cryptology, CRYPTO'89*, Santa Barbara, CA, USA, pp. 307-315, 1990.

[13] D. Chaum, "Blind signatures for untraceable payments", *In Advances in Cryptology, CRYPTO'82*, NY, USA, pp. 199-203, 1982.

[14] D. Goldschlag, M. Reed, and P. Syverson, "Onion Routing for Anonymous and Private Communications", *Communications of the ACM*, Vol. 42, No. 2, pp. 39–41, 1999.

[15] J. Camenisch, and A. Lysyanskaya, "A formal treatment of onion routing", *In Advances in Cryptology, CRYPTO'05*, pp. 169-187, 2005.

[16] C. Park, K. Itoh, and K. Kurosawa, "Efficient anonymous channel and all/nothing election scheme", *In Advances in Cryptology EUROCRYPT'93*, Lofthus, Norway, pp. 248-259, 1993.

[17] E. V. Herreweghen, "Unidentifiability and accountability in electronic transactions", *PhD thesis*, Katholieke Universiteit Leuven, 2004.

[18] M. Abe, "Universally verifiable mix-net with verification work independent of the number of mix-servers", *In Advances in Cryptology EUROCRYPT'98*, volume 1403, pp. 437–447, 1998.

[19] W. S. Juang, C. L. Lei, and H. T. Liaw, "A verifiable multi-authority secret election allowing abstention from voting", *Computer Journal*, 45(6), pp. 672-682, 2002.

[20] H. T. Liaw, "A secure electronic voting protocol for general elections", *Journal of Computers & Security*, Vol.23 (pp.107-119), 2003.