Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Voter Anonimity Methods

I Gusti Made Ardana*, Kuspriyanto and Tito Waluyo Purboyo
School of Electrical Engineering and Informatics
Institut Teknologi Bandung
Indonesia

Abstract— Voter privacy is the main thing that should be kept in the voting process either conventionally or electronically. Privacy in the context of voter protection against disturbances that appear on a ballot means that the voter's choice cannot be proven. To protect the privacy of voters using e-voting scheme can be done by eliminating the voter identity so that the voter identity anonymous. This is known as voter anonymity. Voter anonymity, also called unlinkability is a major parameter in e-voting. This method is applied to achieve anonymity in e-voting election. This method can be divided into two major parts, namely an integrated and non-integrated. The mix network and homomorphic encryption are methods that is integrated with e-voting system, while the blind signature is a separate method of e-voting. Pseudo-Voter Identity (PVID) is one application of a blind voter signature to achieve anonymity in e-voting. The advantages of these methods are the transparency of the flow of voter anonymity, the simplicity of the protocol and do not require complex calculations.

Keywords— E-voting; Voter Anonymity; Mix Network; Homomorphic Encription; Blind Signature.

I. INTRODUCTION

Secret voting schemes have been proposed by many researchers from both the theoretical and practical points of view. There are two types of the secret voting schemes approach: one is the voter sends the ballot in an encrypted form and the other is voter sends the ballot through an anonymous communication channel [1]. Democracy depends on the proper administration of popular elections. Voters should receive assurance that their intent was correctly captured and that all eligible votes were correctly tallied. The election system as a whole should ensure that voter coercion is unlikely, even when voters are willing to be influenced. These conflicting requirements present a significant challenge: how can voters receive enough assurance to trust the election result, but not so much that they can prove to a potential coercer how they voted? In [2], Adida et. all explore cryptographic techniques for implementing verifiable, secret-ballot elections. They present the power of cryptographic voting, in particular its ability to successfully achieve both verifiability and ballot secrecy, a combination that cannot be achieved by other means. They review a large portion of the literature on cryptographic voting. 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 [4]. 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 evoting 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 [4]. The objective of electronic voting schemes is to allow elections to take place securely over general-purpose and open computer networks. During the ballot collecting process, a set of eligible voters use the computer network to cast their ballots. After some time, the system stops accepting ballots. The counting process is initiated and, .nally, the tally is published [10].

The organization of the rest of this article is as follows. Section 2 introduces an overview of voter anonimity methods. A comparison of voter anonimity methods are given in Section 3. We give a conclusion in Section 4.

II. AN OVERVIEW OF VOTER ANONIMITY

Research on Anonymity technology began in the early 1980s, pioneered by David Chaum, with his paper entitled "Electronic Mail untraceable" and further research is growing rapidly since 2000 with two topics, data and communication. At publication Freehaven Anonymity Bibliography sub topics of study include Anonymous Communication, Traffic Analysis, provable shuffles, Anonymous Publication, Economics, Formal Methods, Pseudonymity and Miscellaneous. E-voting research in sub-topics including Shufless provable. Many anonymity systems

can be modeled in terms of unlinkability. Unlinkability is defined by Pfitzmann and Hansen [5] as follows: unlinkability of two or more items of interest (IOIs, e.g., subjects, messages, events, actions, ...) means that within the system (comprising these and possibly other items), from the attacker's perspective, these items of interest are no more and no less related after his observation than they are related concerning his a-priori knowledge.

Anonymity terminology begins with the determination of the entities of subject, object and action. The subject is also called the sender and the delivery action is called a message, and the message received by the recipient using the subject line of communication [5]. All three of these entities can be drawn as follows:

Fig. 1 Entity Setting [5]

From the background of the entity setting the figure 1, Pfitzmann and Hansen [5] defined anonymity as the state of being not identifiable within a set of subjects, the anonymity set. This definition, first proposed in year 2000, has been adopted in most of the anonymity literature.

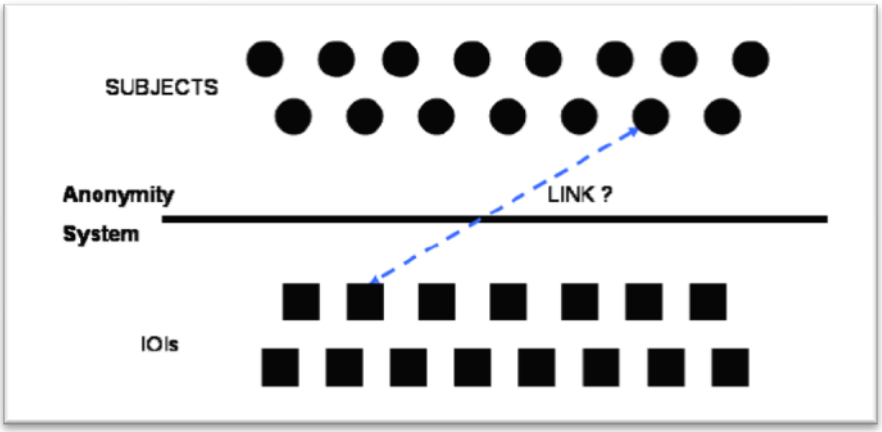

Fig. 2 Model for Anonymity Systems [3]

Figure 2 presents a simplified anonymity model. The goal of anonymity systems is to hide the relationship between subjects and IOIs. Hiding these links is the basic mechanism behind anonymous transactions. An observer of the system sees that a set of subjects are accessing the anonymity system. At the output of the system, they see IOIs which are hard to link to a particular subject. The set of subjects who might be linked to an IOI is called the anonymity set. The larger the anonymity set, the more anonymity a subject is enjoying.

The properties can only be attached to anonymity is defined as the attacker has established and marked. Anonymity properties are defined as follows:

a. Unlinkability, the attacker can not distinguish whether an item of Interests (IOIs) related or not, where IOIs is subject, message and action.
b. Undetectability, the attacker can not distinguish whether the Item of Interest (IOIs) or not, where IOIs is subject, message and action.
c. Unobservability, Item of Interest (IOIs) is undetectable to all subjects involved in it even for one another other subjects.
d. Untraceability, consisting of the receiver and the sender while the sender and the recipient can not be tracked by an attacker.

The concept of blind signature was introduced by Chaum [17] 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.

III. A COMPARISON OF VOTER ANONIMITY METHODS

Voter Anonymity or unlinkability is a primary parameter in e-voting, because this parameter is closely related to the privacy of voters [4]. Making voters as voter anonymity will negate the possibility of tracking the process and the voters choice.

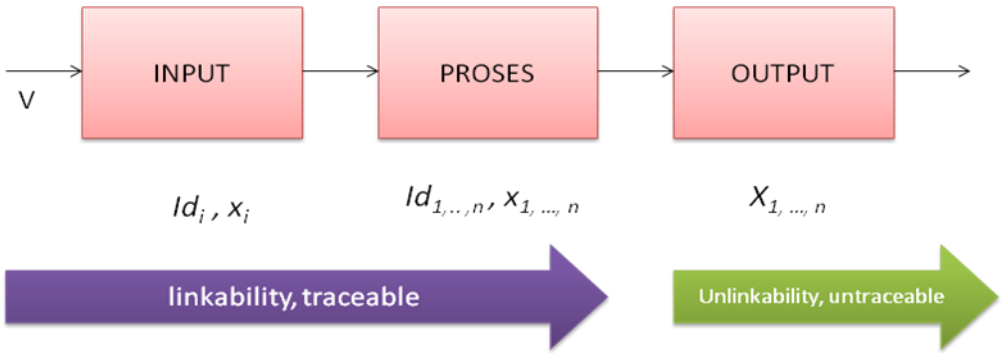

Fig. 3 e-Voting System

Voter Anonymity aims to remove the link between voter choice and a voice that can not be proven voice option. Voter anonymity method integrated with e-voting system requires a very complex computational process and anonymous channel for securing the computational results. Voter anonymity is the subject of trees in the expansion of e-voting [4]. Verifiable voting technology approach to voter anonymity using three methods namely network-based mix, homomorphic encryption and blind signature.

A. Mix Network

The mix network approach was proposed by David Chaum [17] for untraceable payment of interest and untraceable electronic mail. The principle used by mix network approach is to use one or more servers to perform data encryption, an anonymous channel for transmission media. Computational processes that occur in the mix network are very complex. In Figure 4, the basic process of data encryption by one server is provided.

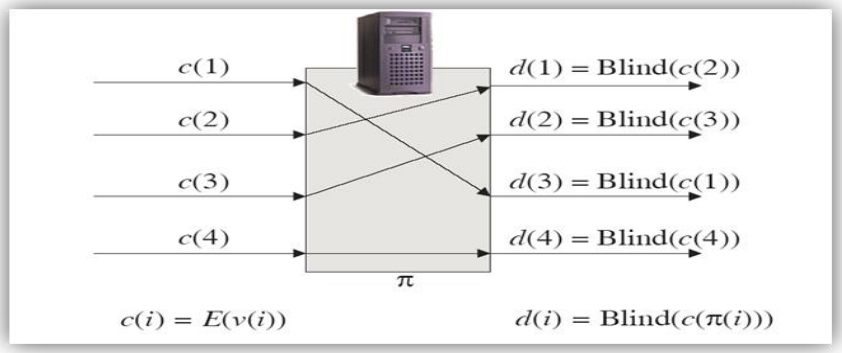

Fig. 4 Basic Scheme of Mix Network with One Server [14]

In the mix network, the encryption c(i) = E(v(i)) performed on c(1), c(2), ..., c(4) are intended to produce values that have been "blinded". Further, the decryption process use the equation d(i) = Blind (c(π(i))), where π is the number of mix network. In the process of voter anonymization on more complex e-voting which use 3 pieces of mix servers, cryptographic techniques are used in the process of encryption and permutation data.

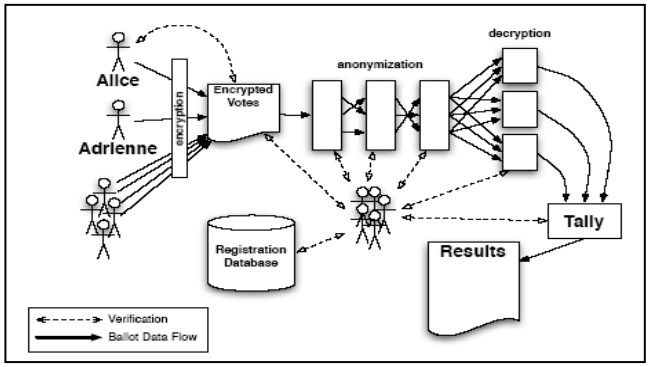

Fig. 5. Cryptographic Voting at a High Level [15]

B. Homomorphic Encryption

The encryption algorithm E( ) is homomorphic if given E(x) and E(y), one can obtain E(x⊥y) without decrypting x and y for some operation ⊥. Homomorphic encryption is a technique in cryptography that uses two algebra methods to encrypt the plaintext.

1. RSA Multiplicative Homomophirsm, where $c_i = E(m_i) = m^e_i \bmod N$

$$c_1 = m^e_1 \quad mod\ N$$
$$c_2 = m^e_2 \quad mod\ N$$
$$c_1 . c_2 = m^e_1 . m^e_2 \quad mod\ N = (m_1 . m_2)^e \quad mod\ N$$

2. Paillier additive homomorphic property [14].
   1. For encryption of message m Є Z_N:
   2. Choose x Є $_R$ Z^*_N

   Create encryption $E(m) = g^m x^N \bmod N^2$, then the property paillier additive homomorphic is:

$$E(m_1) = g^{m1} x_1^N \quad mod\ N^2$$
$$E(m_2) = g^{m2} x_2^N \quad mod\ N^2$$
$$E(m_1).E(m_2) = g^{m1+m2} (x_1 x_2)^N \quad mod\ N^2 = E(m_1 + m_2)$$

3. Approach to e-voting with homomorphic encryption [16]

   Election officer will create a public key for compute homomorphic encryption for each candidate with $C_{pi} = E_{pk}$ [0], for each polling station [C_{p1}, C_{p2}, ... , C_{pn}]. At the time of the election, all choice made as a random choice, and filled one by one by the voters for each election counters, we do now after the election is over, the officer will perform the decryption to count the votes [16].

Encryption with Public key : $C=E_{pk}[M]$,
Someone will compute : $C'=E_{pk}[M+1]$,
Example :
Public key : $N=pq$, g , *private key* p,q
$E_{pk}[M] = g^m r^N \ [mod\ N^2]$
$C=E_{pk}[M] => C'=C.g.(r')^N,\ N^2$

C. Blind Signature

Pseudo-Voter Identity (PVID) is one method that uses blind signatures in the implementation of the procedure as in Figure 6.

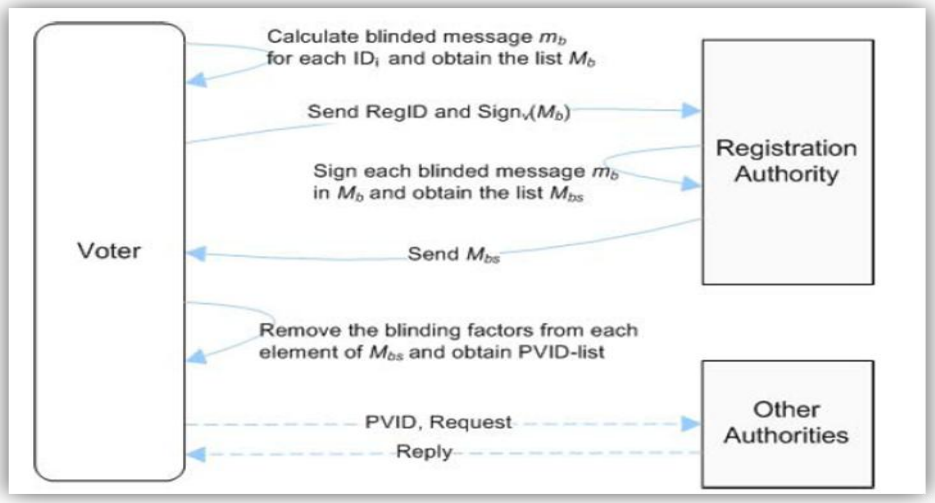

Fig. 6 Basic Scheme of Pseudo-Voter Identity [4]

1. Each ID_i, containing information Electoral Data, Authority and a random number, ID_i = (Election Data, Authority Data, Random Number).
2. Voters will generate a random number r, and check your m_b contained in each ID_i, thus gaining M_b

$$M_b = (r^e[ID_i] \bmod n \quad where \quad gcd\ (r,n) = 1$$
$$M_b = \{m_{b1}, m_{b2}, \ldots, m_{bk}\}$$

3. Then voters will sign M_b, resulting $Sign_v$, then voters encrypt RegID and $Sign_v$ (M_b) using the public key of Registration Authority. M_b values have been "blinded" by the value of the random number r.
4. Registration Authority will then decrypt messages that have been received and verify the message. When Voter Reg ID and the ID list M_b are identic and don't use selecting yet, the Registration Authority will sign the message m_b to produce the IDs Sign, M_{bs}

$$M_{bs} = m_b^d \bmod n$$
$$M_{bs} = \{m_{bs1}, m_{bs2}, \ldots, m_{bsk}\}$$

5. Voters decrypt the received message and get ID list M_{bs}, and voters easily receive $PVID_s$, real ID_s and obtain $PVID_i$ for each ID_i that will be used to communicate with other Election Authority.

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

IV. CONCLUSIONS

In this paper, three methods of voter anonimity are explained. These methods are mix network, homomorphic encription and blind signature. 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. 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. Mixnet-based voting is more difficult to operate than homomorphic-based voting, because the re-encryption and shuffle processes must be executed on a trusted computing base, keeping the details of the shuffle secret from all others. However, mixnets present two important advantages: the complete set of ballots is preserved for election auditing, and freeform ballots, including write-ins, are supported. As a result, mixnet-based voting schemes offer the most promise in real-world, democratic election implementation, even if they are operationally more complex. As a future work, we are planning to develop a voter anonimity methods based on the methods described in this paper. We will implement a prototype in order to be ready to use in the e-voting protocols.

REFERENCES

[1] A. Fujioka, T. Okamoto, 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] B. Adida, "Advances in Cryptographic Voting System," PhD. Thesis, Massachusetts Institute of Technology, 2006.

[3] C. Diaz, "Final Anonymity and Privacy in Electronic Services," PhD. Thesis, Katholieke Universiteit Leuven, December 2005.

[4] O. Centinkaya, "Pseudo-Voter Identity (PVID) Scheme for e-Voting Protocols," Proceedings of The Second International Conference on Availability, Reliability and Security (ARES) 2007, IEEE Intl. Conference, Vienna, Angkara, Turkey, p. 1190 – 119610-13 April 2007.

[5] A. Pfitzmann, M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management," Version v0.34 August 10, 2010.

[6] A. Serjantov, G. Danezis, "Towards an information theoretic metric for anonymity," Proceedings of the 2nd international conference on Privacy enhancing technologies (PET'02), p. 41-53, 2002.

[7] Y. Deng, J. Pang, P. Wu, "Measuring anonymity with relative entropy," Proceedings of the 4th international conference on Formal aspects in security and trust (FAST'06), p. 65-79, 2006.

[8] C. Diaz, "Anonymity Metrics Revisited," Dagstuhl Seminar on Anonymous Communication and Its Applications, October 2005.

[9] A. Serjantov, "On the anonymity of Anonymity System," PhD. Thesis, University of Cambridge, March 2004

[10] C. Díaz, S. Seys, J. Claessens, B. Preneel, "Towards measuring anonymity," Proceeding PET'02 (Proceedings of the 2nd international conference on Privacy enhancing technologies), p. 54-68, 2002.

[11] A. Riera, J. Borrell, "Practical Approach to Anonymity in Large Scale Electronic Voting Schemes," In Network and Distributed System Security Symposium (NDSS 99), p. 69-82, 1999.
[12] C. E. Shannon, "A Mathematical Theory of Communication," The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948.
[13] L. Sweeneyk, "k-anonymity: a model for protecting privacy," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Volume 10, Issue 5, p. 557 – 570, October 2002.
[14] R.L. Rivest, "Voting Homomorphic Encryption, "Lecture Note 15, George Washington University, 2002.
[15] Ecaterina Velica, http://students.info.uaic.ro.
[16] D. Boneh, J. Mitchell, Electronic Voting, Stanford University, 2004.
[17] D. Chaum, "Blind signatures for untraceable payments", In Advances in Cryptology, CRYPTO'82, NY, USA, pp. 199-203, 1982.

