ANONYMITY IN E-VOTING PROTOCOLS

Orhan Çetinkaya[1], Deniz Çetinkaya[2]
[1] *Institute of Applied Mathematics, Middle East Technical University, 06531 Ankara, Turkey*
e113754@metu.edu.tr
[2] *Computer Engineering (M.Sc.), Middle East Technical University, 06531 Ankara, Turkey*
e131263@ceng.metu.edu.tr

Abstract: Voter anonymity, also known as unlinkability, is the basic requirement in order to satisfy privacy in electronic voting (e-voting) protocols, which means that a particular vote is not linkable to any voter. In other words, the relationship between voter identity and the related cast vote should be private to that particular voter and it should not be revealed or proved in any way. Many e-voting protocols have been proposed from both theoretical and practical perspectives in the last decades. This paper focuses on the anonymity properties of some previously proposed e-voting protocols and classifies the e-voting protocols by their privacy preserving approaches as: (a) protocols based on anonymous channel, (b) protocols based on homomorphic encryption and (c) other protocols. Then, main features and characteristics of these approaches are pointed out and feasibility of performing practical and secure e-voting is discussed.

1. Introduction:

Electronic voting (e-voting) is a challenging topic in advanced cryptography. Chaum introduced the first cryptographic voting protocol in 1981 (Chaum, 1981) and many voting protocols have been proposed from both theoretical and practical perspectives since then. However, to the best of our knowledge, no complete solution has been found because of the importance of security requirements in voting systems such as privacy, accuracy, fairness and verifiability. For further reading on e-voting requirements we refer the interested readers to the recent work of (Cetinkaya, 2007).

One of the most important and desirable requirement is voter anonymity, which is also known as unlinkability. Voter anonymity is the basic requirement in order to satisfy privacy in e-voting protocols, which means that a particular vote is not linkable to any voter. In other words it is impossible to reveal and prove voter-vote relationship. Anonymity requirement makes electronic voting different than other electronic applications. It also makes fraud easier since addition, deletion, or modification of anonymous votes is harder to detect. Hence, various techniques have been proposed in order to satisfy anonymity and they are used in many proposed e-voting protocols in order to satisfy privacy.

The electronic voting protocols proposed so far could be classified by their privacy preserving approaches as: (a) protocols based on anonymous channel (Fujioka, 1992), (Park, 1993), (Baraani, 1994), (Sako, 1995), (Cranor, 1997), (Okamoto, 1997), (Magkos, 2002), (Aditya, 2004-1), (Juels, 2005), (Chaum, 2005); (b) protocols based on homomorphic encryption (Benaloh, 1994), (Sako, 1994), (Cramer, 1997), (Hirt, 2000), (Baudron, 2001), (Acquisti, 2004); and (c) other protocols (Mu, 1998), (He, 1998), (Riera, 1999), (Karro, 1999), (Ray, 2001), (Yang, 2004), (Hillery, 2005).

Many researchers classify the protocols described in (Fujioka, 1992), (Cranor, 1997), (Okamoto, 1997) and some others as blind signature based e-voting protocols. However voting protocols using blind signature still require the existence of anonymous channels or apply some cryptographic techniques. For example, in many papers (Fujioka, 1992) is said to be blind signature based. But voter sends his vote to the counter authority through an anonymous communication channel in that protocol. In other words, it is not appropriate to classify this kind of protocols as blind signature based since they require anonymous channels, homomorphic encryption or some other cryptographic techniques besides blind signature.

Each approach has pros and cons, but most of them have large computational complexity, which makes them unpractical. Therefore recent studies try to improve the efficiency of e-voting protocols (Groth, 2003), (Aditya, 2004-1), (Chaum, 2005).

An efficient and practical solution to assure anonymity will make secure e-voting applicable in real-life, since guaranteeing the voter anonymity is harder than other e-voting requirements.

This paper focuses on the anonymity properties of some previously proposed e-voting protocols and classifies them into three categories. Then, it describes the main features and characteristics of these approaches, provides a review of cryptographic voting protocols and discusses the feasibility of performing practical and secure e-voting.

The remainder of the paper is organized as follows. In the next section some cryptographic primitives such as anonymous channels, homomorphic encryption, blind signatures and threshold cryptography are summarized. In Section 3 and Section 4 the main features and characteristics of e-voting protocols based on anonymous channel and based on homomorphic encryption are described respectively. Then it is explained how the e-voting protocols using neither anonymous channels nor homomorphic encryption assure anonymity in Section 5. Finally, conclusions are drawn and future work is suggested.

2. Cryptographic Primitives:

E-voting protocols employ some cryptographic primitives to achieve e-voting requirements. Some of the well known primitives are listed below.

2.1. Anonymous Channels:

Assumption of an efficient verifiable anonymous channel is done by many e-voting protocols. Various techniques have been proposed in order to achieve anonymous communication. The most common solution is mix-networks, which were originally introduced by Chaum in 1981 (Chaum, 1981). Hence using anonymous communication channels in e-voting protocols is generally called as mix voting.

Main idea of mix networks (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. However, the details of mixing protocol implementation change depending on configurations and arrangements of mix-nets. The first mix-nets are decryption mix-nets (Chaum, 1981) where messages are wrapped in several layers of encryption and then are routed through mix servers each of which peels off a layer of encryption and then forwards them in random order to the next one. In decryption mix-nets, decryption in each mix server is repeated until all layers are removed. One of the well-known implementation of decryption mix-nets is Onion routing (Camenisch, 2005).

Later re-encryption mix-nets were introduced (Park, 1993), where the incoming messages are not decrypted but they are re-encrypted in each mix server. In re-encryption mix-nets, decryption occurs after shuffling is 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. Therefore they are extended to be verifiable. In verifiable mix-nets, a mix server additionally has to prove in zero knowledge that it decrypted/re-encrypted and shuffled the inputs correctly. There are several approaches to achieve verifiable mix-nets; the main difficulty in these approaches is efficiency of proof techniques.

An alternative anonymous channel solution to mix-nets is a system referred as “crowds” (Reiter, 1998), where a group of participants want to protect each other’s privacy. When one of them wants to send a message somewhere, he instead sends it to one of the members of the group. This member either sends it to its destination, or passes it on to another group member. It provides anonymity; however it may not be practical for e-voting, since it requires group members, i.e. voters, to be available for each other during the voting process.

2.2. Homomorphic Encryption:

A cryptosystem is homomorphic when $E(s_1) \circ E(s_2) = E(s_1 \Diamond s_2)$, where E is a public encryption function, s is a secret message, and $\circ$ and $\Diamond$ are some binary operators. Note that the binary operators may be equal. Thus, it is possible to compute the combination of the individual messages without having to retrieve the individual messages themselves. Thereby, the individual messages can remain confidential. Two popular examples of homomorphic cryptosystems in the literature are ElGamal and Paillier cryptosystems (Adida, 2006).

2.3. Blind Signature:

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 concept of blind signature was introduced by Chaum (Chaum, 1982) as a method to digitally authenticate a message without knowing the content of the message.

2.4. Zero-Knowledge Proofs:

In cryptographic protocols it is often needed to prove some statement to someone without revealing any extra information. This is accomplished by zero-knowledge proofs. Zero-knowledge proofs are used mostly by authentication systems where one party wants to prove its identity to a second party via some secret information but does not want the second party to learn anything about this secret. Zero knowledge proof protocols are two-party protocols between a prover and a verifier. They allow the prover to convince the verifier that he knows a secret, but without giving any information about the secret. After the execution of the protocol the verifier has gained zero knowledge concerning the secret.

2.5. Threshold Cryptosystem:

A *(t, n)* threshold cryptography is a system to distribute secret keys or operations of a cryptosystem between *n* parties in order to remove single point of failure. The required trust in the cryptographic service is distributed among the group of authorities.
The goal is to allow any subset of more than *t* parties to jointly reconstruct a secret and perform the computation while preserving security even in the presence of an active adversary which can corrupt up to *t* (a threshold) parties.

2.6. Bulletin Boards:

Chaum (Chaum, 1981) introduced the concept of bulletin board, a public broadcast channel with memory where a party may write information that any party may read. Since then, bulletin boards have been often used in e-voting protocols. All communications with the bulletin board are public and therefore can be monitored. Generally, data already written to a bulletin board cannot be altered or deleted anymore, but it can be read or appended.

3. E-voting Protocols based on Anonymous Channel:

Using anonymous channels in e-voting is as old as e-voting, since the first cryptographic e-voting protocol employed anonymous channels (Chaum, 1981). The protocols that use homomorphic encryption were introduced later (Cohen, 1985).
Many e-voting protocols assume that there exists an efficient verifiable anonymous channel. E-voting protocols based on anonymous channel are very popular in practice due to their support for any type of voting. However the implementation of verifiable anonymous channels has large computational complexity. In addition, various types of attacks have emerged over the years and most of the proposed anonymous channel implementations are shown to be not secure (Pfitzmann, 1994).

Efficient and secure anonymous channels will make many e-voting protocols assuming the existence of anonymous communication channels applicable.

As a general approach, it is accepted that a vote cannot be linked to a particular voter by tracing the network packets in anonymous channel. In e-voting protocols based on anonymous channel, voter casts his vote over an anonymous channel, i.e. the vote cast by the voter is anonymized.

(Fujioka, 1992), (Baraani, 1994), (Okamoto, 1997), (Cranor, 1997), (Magkos, 2002) and (Juels, 2005) assume voter access to an anonymous channel at some point during the voting process. (Juang, 2002) uses also anonymous channels, but assumes that it is provided by an untraceable e-mail system.

(Park, 1993), (Sako, 1995), (Aditya, 2004-1), (Chaum, 2005) use mix-nets and (Joaqim, 2003) uses Anonymizer servers in order to achieve anonymous communication.

E-voting protocols based on anonymous channel are easy to understand since they mimic the traditional paper based voting systems. Voter encrypts and sends his cast vote to the authorities through an anonymous channel. The authorities decrypt the collected votes and count each vote separately. Voters do not need to prove the validity of the ballots; hence the computational cost for voter is reasonably less compared with the e-voting protocols based on homomorphic encryption. However, mix servers suffer from computational cost for proving that their mixing is correct.

4. E-voting Protocols based on Homomorphic Encryption:

E-voting protocols based on homomorphic encryption have more security properties than other protocols, but their communication complexity is quite high. In addition, these protocols do not support any type of voting. They are best suitable for yes-no or 1-out-of-L voting; however they can be extended for other types.

Homomorphic voting protocols are efficient when the number of candidates or choices is small. However, homomorphic voting has a drawback where each vote must be verified 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 verification of vote validity is so high that homomorphic voting becomes less efficient than mix voting (Aditya, 2004-2).

(Benaloh, 1994), (Sako, 1994), (Cramer, 1997), (Hirt, 2000), (Baudron, 2001), (Acquisti, 2004) use homomorphic encryption and propose secure e-voting protocols.

In e-voting protocols based on homomorphic encryption, 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. In these protocols voting results are obtained easily so ballot tabulations are more efficient.

5. Other E-voting Protocols:

There are some e-voting protocols in the literature which use neither anonymous channels nor homomorphic encryption in order to assure anonymity. Nevertheless they use other cryptographic primitives.

In (Riera, 1999), a large scale voting scheme based on the concurrent operation of multiple electronic electoral colleges is proposed with no need for independent anonymous channels. In this protocol, anonymity of ballots is assured by shuffling of ballot boxes by a set of mobile agents acting on behalf of a central voting authority.

(Hillery, 2005) analyses the privacy and the voting problem in the framework of quantum theory. Quantum information is used to ensure privacy.

(Karro, 1999) uses neither blind signatures nor anonymous communication channels, but uses a secure form of communication for all transactions.

(Mu, 1997), (He, 1998), (Ray, 2001), (Yang, 2004) use voting tickets or tokens in order to assure anonymous voting. These protocols make the voter anonymous before the voting stage which sacrifices receipt-freeness and

uncoercibility. They also make fraud easier since addition, deletion, or modification of anonymous votes/voters is harder to detect.
E-voting protocols claiming that they assure privacy without anonymous channels or homomorphic encryption generally rely on computational assumptions or trusted authorities.

6. Discussion:

In this paper, the electronic voting protocols proposed so far are classified by their privacy preserving approaches as: (a) protocols based on anonymous channel, (b) protocols based on homomorphic encryption and (c) other protocols.
In anonymous channel based e-voting protocols voters do not need to prove the validity of the ballots; where it is required in homomorphic encryption based e-voting protocols. Hence the computational cost for voter is relatively more in homomorphic encryption based e-voting protocols compared with others. However, mix servers also suffer from computational cost for proving that their mixing is correct, in order to make the system trustworthy.
Anonymous channel based e-voting protocols support wide variety of voting types, even write-in ballots, where the others are just suitable for the selected voting types such as yes-no or 1-out-of-L voting.
In homomorphic encryption based e-voting protocols voting results are obtained easily so ballot tabulations are more efficient. However anonymous channel based e-voting protocols become more popular since they are relatively easy to implement.
E-voting protocols claiming that they assure privacy without anonymous channels or homomorphic encryption are also not very popular since they generally rely on computational assumptions or trusted authorities.
In the future, an alternative for anonymous channels or homomorphic encryption should be proposed in order to achieve practical secure e-voting protocols. More efficient cryptographic techniques should be used in order to make e-voting protocols practical. Besides, robustness of the cryptographic primitives should be improved.

7. References:

Acquisti A., "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.

Adida B., *Advances in Cryptographic Voting Systems*, PhD Thesis, MIT, USA, 2006.

Aditya R., Lee B., Boyd C., Dawson E., "An Efficient Mixnet-based Voting Scheme Providing Receipt-Freeness", *First Int. Conf. on Trust and Privacy in Digital Business,* Zaragoza, Spain, 2004, pp. 152-161. (Aditya, 2004-1)

Aditya R., Lee B., Boyd C., Dawson E., "Implementation Issues In Secure E-Voting Schemes", *Asia-Pacific Industrial Engineering and Management Systems Conference,* Goldcoast, Australia, 2004. (Aditya, 2004-2)

Baraani-Dastjerdi A., Pieprzyk J., Safavi-Naini R.. "A Practical Electronic Voting Protocol Using Threshold Schemes", *Technical Report TR-94-13,* Department of Computer Science, The University of Wollongong, Wollongong, Australia, 1994.

Baudron O., Fouque P.A., Pointcheval D., Poupard G., Stern J., "Practical Multi-Candidate Election System", *Proc. of the 20th ACM Symposium on Principles of Distributed Computing (PODC '01),* Newport, RI, USA, 2001, pp. 274-283.

Benaloh J., Tuinstra D., "Receipt-free secret-ballot elections", *Proc. of the 26th ACM Symposium on Theory of Computing,* Montreal, Canada, 1994, pp. 544-553.

Camenisch J., Lysyanskaya A., "A Formal Treatment of Onion Routing", *In Advances in Cryptology, CRYPTO'05,* 2005, pp. 169-187.

Cetinkaya, O., Cetinkaya, D., "Towards Secure E-Elections in Turkey: Requirements and Principles", *DeSeGov'07*, Vienna, Austria, 2007.

Chaum D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *Communications of the ACM vol. 24-2*, 1981, pp. 84-88.

Chaum D., "Blind Signatures for Untraceable Payments", *CRYPTO '82,* 1982, pp. 199-203.

Chaum D., Ryan P. Y. A., Schneider S., "A Practical, Voter-Verifiable Election Scheme", *ESORICS'05*, Milan, Italy, 2005, pp. 118-139.

Cohen J. D., Fischer M. J., "A Robust and Verifiable Cryptographically Secure Election Scheme (Extended Abstract)", *In the Proc. of 26th Annual Symposium on Foundations of Computer Science,* Portland, OR, USA, 1985, pp. 372-382.

Cramer R., Gennaro R., Schoenmakers B., "A Secure and Optimally Efficient Multi-Authority Election Scheme", *EUROCRYPT'97,* Konstanz, Germany, 1997, pp. 103-118.

Cranor L., Cytron, R., "Sensus: A Security-Conscious Electronic Polling System for the Internet", *Proc. of the Thirtieth Annual Hawaii Int. Conf. on System Sciences,* Wailea, Hawaii, 1997.

Fujioka A., Okamoto T., Ohta K., "A Practical Secret Voting Scheme for Large Scale Elections", *In Advances in Cryptology Auscrypt'92,* Gold Coast , Australia, 1992, pp. 244-251.

Groth J., "A Verifiable Secret Shuffle of Homomorphic Encryptions", *Proc. of the 6th Int. Workshop on Theory and Practice in Public Key Cryptography,* Miami, FL, 2003, pp. 145-160.

He Q., Su Z., "A New Practical Secure e-Voting Scheme", *IFIP/SEC'98,* Austrian Computer Society, 1998, pp. 196-205.

Hillery M., Ziman M., Buzek V., Bielikova M., "Towards quantum-based privacy and voting", *Physics Letters A 349, Elsevier,* 2005, pp. 75-81.

Hirt M., Sako K., "Efficient Receipt-Free Voting Based on Homomorphic Encryption", *EUROCRYPT'00*, Bruges, Belgium, 2000, pp. 539-556.

Joaquim R., Zuquete A., Ferreira P., "REVS - A Robust Electronic Voting System", *Proc. of IADIS Int. Conf. on e-Society,* Lisbon, Portugal, 2003, pp. 95-103.

Juang W. S., Lei C. L., Liaw H. T., "A Verifiable Multi-authority Secret Election Allowing Abstention From Voting", *The Computer Journal vol. 45-6,* Oxford University Press, UK, 2002, pp. 672-682.

Juels A., Catalano D., Jakobsson M., "Coercion-Resistant Electronic Elections", *Proc. of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES 2005),* Alexandria, VA, USA, 2005, pp. 61-70.

Karro J., Wang J., "Towards a Practical, Secure, and Very Large Scale Online Election", *In the Proc. of the 15th Annual Computer Security Applications Conference (ACSAC'99),* Los Alamitos, CA, USA, 1999.

Magkos E., Chrissikopoulos V., "Equitably Fair Internet Voting", *In Journal of Internet Technology vol. 3-3,* Special Issue on Network Security, 2002, pp. 187-193.

Mu Y., Varadharajan V., "Anonymous Secure E-Voting Over a Network", *Proc. of the 14th Annual Computer Security Applications Conference,* Scottsdale, AZ, USA, 1998, pp. 293-299.

Okamoto T., "Receipt-free electronic voting schemes for large scale elections", *In the Proc. of Security Protocols Workshop,* Paris, France, 1997, pages 25-35.

Park C., Itoh K., Kurosawa K., “Efficient Anonymous Channel and All/Nothing Election Scheme”, *EUROCRYPT'93,* Lofthus, Norway, 1993, pp. 248-259.

Pfitzmann B., “Breaking Efficient Anonymous Channel”, *EUROCRYPT’04,* Perugia, Italy, 1994, pp. 332-340.

Ray I., Ray I., Narasimhamurthi N., “An anonymous electronic voting protocol for voting over the internet”, *In the Proc. of the Third Int. Workshop on Advanced Issues of E-Commerce and Web-based Information Systems,* San Juan, CA, USA, 2001.

Reiter, M. K., Rubin, A. D., “Crowds: Anonymity for Web Transactions”, *ACM Transactions on Information and System Security* 1(1), 1998, pp. 66-92.

Riera A., Borrell J., “Practical Approach to Anonymity in Large Scale Electronic Voting Schemes”, *In the Proc. of the Network and Distributed System Security Symposium,* San Diego, CA, USA, 1999.

Sako K., Kilian J., “Secure Voting Using Partially Compatible Homomorphisms”, *In Advances in Cryptology CRYPTO'94,* Santa Barbara, CA, USA, 1994, pp. 411-424.

Sako K., Kilian J., “Receipt-Free Mix-Type Voting Scheme: A Practical Solution to the Implementation of A Voting Booth”, *EUROCRYPT’95,* Malo, France, 1995, pp. 393-403.

Yang C. C., Lin C. Y., Yang H. W., “Improved Anonymous Secure e-Voting over a Network”, *Int. Journal of Information & Security vol. 15-2,* 2004, pp.181-194.