INTRODUCTION TO SECURE ELECTRONIC VOTING REQUIREMENTS

Pance Ribarski pance@ii.edu.mk
Ljupcho Antovski anto@ii.edu.mk
Faculty of Natural Sciences and Mathematics
Institute of Informatics
Skopje, Macedonia

ABSTRACT

Voting takes great part in the human society. The act of choosing a representative in a vote-like process has always been a delicate and fragile. Electronic voting is being introduced not so long ago [12]. We can see the progress of e-voting just by looking the goals that researchers set their selves [1, 3, 7, 21, 22]. Accomplishment of these goals went in two directions: using blind signatures [1, 2, 3, 4, 5, 12, 24], or using homomorphic crypto-system [6, 9, 10, 20, 26]. The notion of mixnets is also intertwining with e-voting systems to ensure an anonymous communication channel. This research will try to unite these concepts and to review the various techniques brought by researchers in the past 20 years or so.

I. INTRODUCTION TO E-VOTING

Voting takes great part in the human society. The act of choosing a representative among many has always been a delicate and fragile process. The prize of being chosen often deduced electives into fraudulent actions, trying to swing the election process on their side.

Electronic voting is being introduced not so long ago [12]. The aim of e-voting is to overcome the cons of traditional voting: expensive, slow results, hard to organize, fraudulent and generally hard to verify the results. On the other hand, e-voting should be: working on inexpensive everyday hardware, fast results, easy to employ, easy to verify etc.

Section 2 will discuss the e-voting goals set to achieve a complete system for secure and verifiable e-voting. Section 3 will cover the blind signatures introduced by Chaum [12] and later followed by many [1, 2, 3, 4, 5, 13, 24] others. Section 4 is about the two types of mixnets as implementation of anonymous communication channel [27, 29]. In Section 5 another way of conducting e-voting is presented: homomorphic cryptosystem [6, 9, 20, 26]. At last, in Section 6 we conclude this short review of e-voting principles, techniques and history.

II. E-VOTING GOALS

E-voting has advanced a lot through the years. We can see the progress just by looking the goals that researchers set their selves [1, 3, 7, 21, 22]. The first goals were set to privacy and verifiability. Privacy for the voter and their vote, that is inability to trace a vote to a voter. Further more, the voter is eligible to vote only if they exist in the electoral rolls, and can vote only once. Verifiability is divided into individual and universal: individual meaning that voter can verify their vote was accounted for; universal meaning that the final result is the real sum of the correct votes. The "fastness" of e-voting came to another goal – fairness. This goal ensures that no intermediate results can influence the future voters. The voting process has always been a place for attracting violence, boycotting elections where a loose situation is predicted, etc. The goal robustness for e-voting systems means that result is correct and counted from all valid votes, successfully obscuring boycott or fraud. Recently researchers introduced new goals trying to disallow coercion. This led to receipt-freeness and coercion resistance, the first meaning that voter doesn't take home a proof of the vote; leading to the second – a voter can not cooperate with a coercer to prove their vote. Closely tied problem is also the problem of authentication [16].

The sum of the goals that every good e-voting system should posses is:

- privacy
- eligibility
- individual verifiability
- universal verifiability
- fairness
- robustness
- receipt-freeness
- coercion resistance

Some researchers found results that sometimes combination of these goals is simply not possible. At least not possible with non-standard assumptions like secure channels or high-interactivity between voters [23]. The authors show that these goals can be met only if stronger assumptions are introduces, which is sometimes impossible in pure electronic or internet manners.

III. BLIND SIGNATURES

One of the first e-voting category which employed cryptographic primitives was an algorithm with blind signatures. Introduced by David Chaum [12] in 1982, was followed by many researchers in the years to come [1, 24, 4, 3, 5, 2]. This technique essentially uses three roles: administrator - A, counter - C and a voter – V. The following functions are necessary for the computations:

- private administrator function g and public inverse function g' such that g'(g(x))=x; g' should not have knowledge of g

- private voter function f and private inverse function f' such that f'(g(f(x)))=g(x); f(x) and g should not have knowledge of x

The voting protocol is conducted in the following phases:

- V creates a message x with filled ballot and random number, blinds it with f(x); V sends f(x) along with credentials to A
- A checks credentials for V; if credentials are ok A blindly signs f(x) and gets g(f(x)); A sends back g(f(x)) V
- V receives blindly signed message; unblinds with f'(g(f(x)))=g(x) getting the A's signature on the message x; sends g(x) to C through anonymous channel (later on anonymous channels)
- C gets the ballot with g'(g(x))=x

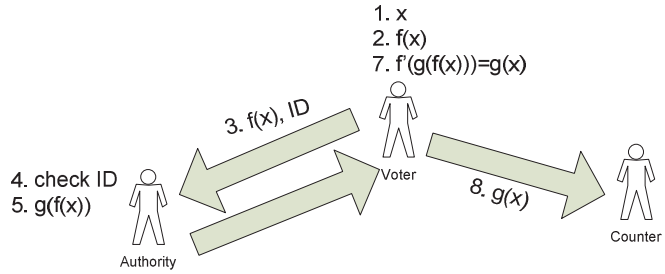

Figure 1: Blind Signatures scheme

Usually the cryptosystem used by blind signatures is RSA [4]. ElGamal cryptosystem is also found in some solutions[2]. The number of calculations included in the process makes it feasible for large-scale elections. The first solution by Okamoto [24] was using blind signatures with RSA cryptosystem, and even satisfied the receipt-freeness goal. Later was showed [4] that this breaks the coercibility goal. With inclusion of physical assumption of untappable channel and other modifications the goals were satisfied[4]. Another solution was made to fix [24] with the coercibility flaw [5]. They solved the problem employing a secret ballot technique found in Pret a Voter solution [25]. Also [5] is using the assumption of untappable channel implementing mixnets.

IV. MIXNETS

In many e-voting scenarios there is an assumption of anonymous or untappable channel. We know that in reality, at least with the current network implementation, there is little to nothing anonymous in the communication between peers. The anonymous property is needed if we want to satisfy the e-voting goals stated above. One of the ways to get an anonymous channel is to implement mixnets. Firstly described by Chaum in 1981 [27], mixnets are a cryptographic way to achieve anonimicity, or to create anonymous channels. If one participant wants to send a message M anonymously to a participant with an address A, they are sealing the message M with the receiving participant's public key K_a. Then they seal the sealed data with the mix server's public key K_1 creating a data package of K_1(R_1, K_a(R_0, M), A). Here R_0 and R_1 are random strings. The mix server decrypts the data with their private key, getting K_a(R_0, M) and A. With a cascade of these mix servers we can create group of mix-servers, of which if only one is honest then the permutation links will be kept secure. The prepared message for such a cascade consisted of n servers would be:

$$K_n(R_n, K_{n-1}(R_{n-1},...., K_2(R_2, K_1(R_1, K_a(R_0, M), A))....)))$$

This category is also known as decryption mixnets. Every server is decrypting his own part of the message, and the last server finally gives K_a(R_0, M) to A. There is a flaw with this concept; when one server fails, the decryption of the whole cascade will fail. Pfitzmann and Pfitzmann found an attack to this category of mixnets [28]. The attacked would use two sequential messages, the second one chosen with relationship with the first one. Because the two messages correlate in the plaintext form, they will correlate in the output answers from the mix – targeting the output of the first message. Another undesirable property with the decryption mixnets is the length of the ciphertext – it is proportional with the number of mix servers. If we want to add more mix server to the cascade, it will eventually result in a very large ciphertext.

Another category of mixnets is being started in 1993 by Park et al. [29], called re-encryption mixnets. In this cascade, every server is rerandomizing the ciphertexts with new randomization values which are algebraically combined with the previous randomization, in spite of the concatenation in the decryption mixnets. Every input is encrypted with a scheme which has homomorphic properties, such as ElGamal. Each mix server shuffles the ciphertexts and rerandomizes them. This influences the robustness of the system – failure of one mix server will not disrupt the process.

V. HOMOMORPHIC CRYPTOSYSTEM

Another way of conducting e-voting presented by researchers is the by using so called homomorphic cryptosystems. These cryptosystems are based on the following algebraic property:

$$E(M_1 * M_2) = E(M_1) * E(M_2) \text{ and}$$
$$E(k * m) = E(M)^k$$

Some cryptosystems that satisfies this property are ElGamal, Naccache-Stern, Okamoto-Uchiyama, Paillier etc. ElGamal is found in many solutions [26, 20, 6, 9]. This cryptosystem is useful when "0/1" type of voting is used – ElGamal can manage only small numbers. But if the type of voting is multi-candidate then the encoding size of the tally would be O(m x |n|), where m is the number of candidates,

and |n| is the size of the number of voters [10]. In these cases other cryptosystem is being used – favorably Paillier.

The use of homomorphic cryptosystems is usually implemented in some threshold variation. This is done to keep the fairness goal – the inability to have results before hand, thus influencing voters. In this threshold variation, the cryptosystem allows decryption only if k out of m parties join together.

Another important part of this category of e-voting systems is zero-knowledge proofs. Because the counting phase skips individual decoding, the voter may "cheat" and enter invalid parameter. In a "0/1" type of voting, he may enter 5, or even -5, thus invalidating the total count. Therefore, the voter passes a constructed zero-knowledge proof for validity. This proof only states that a valid parameter has been encoded, not giving information about what the parameter was.

The physical assumptions for untappable channels appear in homomorphic system too. They are needed to prove the receipt-freeness and incoercibility goals.

VI. Conclusion

We see that pretty much research effort is put towards the topic of electronic voting. Because the traditional voting is complex, expensive and time-consuming, this work on e-voting systems is more than welcomed. This review is only the beginning of a much bigger research – creation of a fully verifiable, distributive and secure e-voting system. The goals set in Section 2 are the ultimate goal set that every e-voting systems used in practice should satisfy. The techniques reviewed should help in the process of choosing effective and secure parts for overall practical implementation of an e-voting system.

References

[1] A. Fujioka, T. Okamoto, K. Ohta, A Practical Secret Voting Scheme for Large Scale Elections

[2] Y. Baseri, M. Pourpouneh, J. Mohajeri, Double Voter Perceptible Blind Signature Based Electronic Voting Protocol

[3] I. Ray, I. Ray, N. Narasimhamurthi, An Anonymous Electronic Voting Protocol for Voting Over The Internet

[4] T. Okamoto, Receipt-Free Electronic Voting Schemes for Large Scale Elections

[5] Z. Xia, S. Scheider, A New Receipt-Free E-Voting Scheme Based on Blind Signature

[6] D. Sandler, K. Derr, D. S. Wallach, VoteBox: a tamper-evident, verifiable electronic voting system

[7] I. Damgard, J. Groth, G. Salomonsen, The Theory and Implementation of an Electronic Voting System

[8] J. Groth, Non-interactive Zero-Knowledge Arguments for Voting

[9] B. Adida, Helios: Web-based Open-Audit Voting

[10] O. Baudron, P. A. Fouque, D. Pointcheval, G. Poupard, J. Stern, Practical Multi-Candidate Election System

[11] J. Katz, S. Myers, R. Ostrovsky, Cryptographic Counters and Applications to Electronic Voting

[12] D. Chaum, Blind signatures for untraceable payments

[13] Lj. Antovski, P. Ribarski, Mobile Voting: Overview of The Road From Paper to Mobile

[14] D. Chaum, Security without identification: transaction systems to make big brother obsolete

[15] R. L. Rivest, The ThreeBalot Voting System

[16] P. Ribarski, Lj. Antovski, Introducing Strong Authentication for E-Government Services in Macedonia

[17] P. Y. A. Ryan, Pret a Voter with Paillier Encryption

[18] D. Chaum, Secret-Ballot Receipts: True Voter-Verifiable Elections

[19] Z. Xia, S. A. Scheider, J. Heather, Analysis, Improvement and Simplification of Pret a Voter with Paillier Encryption

[20] I. Damgard, On Electronic Voting Schemes

[21] Stephanie Delaune, Steve Kremer, Mark Ryan, Coercion-Resistance and Receipt-Freeness in Electronic Voting

[22] Stephanie Delaune, Steve Kremer, Mark Ryan, Verifying Properties of Electronic Voting Protocols

[23] Benoit Chevallier-Mames, Pierre-Alain Fouque, David Pointcheval, Julien Stern, Jacques Traore, On Some Incompatible Properties of Voting Schemes

[24] Tatsuaki Okamoto, An Electronic Voting System

[25] David Chaum, Peter Y A Ryan, Steve Schneider, A Practical, Voter-Verifiable Election Scheme

[26] R. Cramer, R. Gennaro, B. Schoenmaker, A Secure and Optimally Efficient Multi-Authority Election Scheme

[27] D. Chaum, Unraceable Electronic Mail, Return Addresses, and Digital Pseudonyms

[28] B. Pfitzmann, A. Pfitzmann, How to break the direct rsa-implementation of mixes

[29] Choonsik Park, Kazutomo Itoh, Kaoru Kurosawa, Efficient anonymous channel and all/nothing election scheme