Towards secure online elections: Models, primitives and open issues

Article *in* Electronic Government an International Journal · January 2007

DOI: 10.1504/EG.2007.014161 · Source: DBLP

3 authors:

Emmanouil Magkos
Ionian University
55 PUBLICATIONS **600** CITATIONS
SEE PROFILE

Panayiotis Kotzanikolaou
University of Piraeus
81 PUBLICATIONS **1,166** CITATIONS
SEE PROFILE

Christos Douligeris
University of Piraeus
385 PUBLICATIONS **4,356** CITATIONS
SEE PROFILE

Towards Secure Online Elections – Models, Primitives and Open Issues

E. Magkos

Department of Informatics, Ionian University,

7 Plateia Tsirigoti, 49100, Corfu, Greece

E-mail: emagos@ionio.gr

P. Kotzanikolaou and C. Douligeris

Department of Informatics, University of Piraeus,

80, Karaoli & Dimitriou, 18534, Piraeus, Greece

Email: pkotzani@unipi.gr E-mail: cdoulig@unipi.gr

Abstract: Electronic voting may be a feasible option for several election environments, from closed-group elections to nation-wide elections. Especially with *online voting*, people will be able to cast their votes through a web browser, from their home or any other location where they can get Internet access. This paper reviews the generic cryptographic models that have been proposed in the academic literature for secure electronic voting and provides a comprehensive assessment, in terms of security and functionality, of recent cryptographic schemes that extend the generic models to support online elections. The paper also highlights several critical security and implementation issues that need to be addressed before online voting is adopted for critical elections.

Keywords: e-government; e-democracy; online elections; Internet voting; security; cryptography; implementation issues; organizational issues.

Reference to this paper should be made as follows: Magkos, E., Kotzanikolaou, P., and Douligeris, C. (XXXX) 'Towards Secure Online Elections – Models, Primitives and Open Issues', *Electronic Government*, Vol. X, No. X, pp.XXX–XXX.

Biographical notes: Emmanouil Magkos received his BSc in Computer Science from the University of Piraeus, Greece in 1997 and his Ph.D. degree in 2003 from the same university. Currently he is affiliated with the Department of Informatics, Ionian University, Corfu, Greece. His research interests include information security and cryptography, key management in wireless networks, secure distributed systems

Panayiotis Kotzanikolaou received his BSc in Computer Science from the University of Piraeus, Greece in 1998 and his Ph.D. in 2003 from the same university. Currently he is affiliated with the Greek Regulatory Authority for the Assurance of Information and Communication Security and Privacy. His research focuses on cryptography and security for mobile agents, distributed systems, intelligent networks, ad hoc networks and sensor networks.

Christos Douligeris received the Diploma in Electrical Engineering from the National Technical University of Athens in 1984 and the M.S., M.Phil. and Ph.D. degrees from Columbia University in 1985, 1987, 1990, respectively. Currently he is affiliated with the Department of Informatics, University of Piraeus in Greece. His research focuses on

performance evaluation of high speed networks, neurocomputing in networking, resource allocation in wireless networks and information management, risk assessment and evaluation for emergency response operations.

1 Introduction

With the advent of information and communication technologies, electronic voting (e-voting) may become a viable form of electronic democracy. The unique features of e-voting systems are likely to bring advantages to the public, and can be seen as a very important step towards the e-government process of transferring conventional political procedures onto electronic networks. E-voting systems have been recently approved and deployed in various jurisdictions, aiming at improving the voting experience and reducing the cost associated with printing paper ballots. In a simplistic view, each election involves four distinctive stages:

- **Registration**. At some time before the election, voters prove their identity and eligibility to vote. They are usually given a credential[1] to be used during the identification stage.

[1] A credential may be physical (*e.g.* an identity card) or electronic *e.g.* a PIN/password, a cryptographic key or any such credentials embedded in a tamper-resistant token.

- **Identification**. Just before casting their vote, voters present their credential. Only one vote can be associated with a given credential.
- **Voting**. Voters use the voting system to submit their vote.
- **Tallying**. After the voting period ends, all votes are counted and the election results are published.

Each of the above stages can take place by using physical or electronic procedures. As opposed to paper-based elections, e-voting systems use digital data to capture the voter selections. In *polling place* e-voting, both the voting clients and the physical environment are supervised by authorized entities. On the other hand, *online voting* (or Internet voting) refers to an election process whereby people can cast their votes through a web browser, from their home or any other location where they can get Internet access. Registration may be either physical or electronic, while the identification, voting and tallying stages are fully electronic (Burmester and Magkos (2003)).

The use of Internet technologies is expected to increase voter convenience and participation (Houston et al (2005)), allow voters to be more informed, and make access to the democratic process widely available. However, critics of online voting claim that the technology is not mature enough for protecting voter privacy, securely authenticating online voters, and for ensuring the integrity of the voting and tallying stages in a

universally verifiable way. Moreover, there is the fear that the digital divide will skew political power towards non-minorities (*e.g.* Rubin (2004); Kohno et al. (2004)).

In general, online voting systems are expected to satisfy the following security goals (Neumann (1993); Cranor and Cytron (1997); Benaloh and Tuinstra (1994)):

- *Democracy*: only eligible voters are able to cast a vote (eligibility), and no voter is able to cast more than one vote (double voting protection).
- *Accuracy*: votes cannot be altered, duplicated or eliminated from the final tally.
- *Privacy*: the unlinkability between a vote and the voter who cast it.
- Fairness: all votes remain secret while the voting period is not completed.
- *Verifiability*: any individual voter (atomic verifiability) or an external observer (universal verifiability) are able to verify that the tally is correct.
- *Robustness*: the system is secure despite any failure or a malicious behavior by a coalition of voters, authorities or outsiders.

- *Receipt-freeness*: no voter should be able to prove to others how he/she voted (even if he/she wants to).
- *Uncoercibility*: no party should be able to coerce a voter into revealing his/her vote[2].

Cryptography is naturally used to secure transactions in complex systems where the interests of the participating entities are in conflict. Not surprisingly, cryptography is one of the most significant tools for securing online voting protocols. While in traditional elections most ideal security goals such as *democracy*, *privacy*, *accuracy*, *fairness* and *verifiability*, are assured to a point given physical and administrative premises, this same task is quite difficult in online elections. For example, *receipt-freeness* and *verifiability* seem to be contradictory: when voting over the Internet, the very means that allow a voter to verify that his/her vote was counted properly (*e.g.* receipts[3], vote encrypting keys, user-selected randomness,

[2] Clearly, the notion of receipt freeness is stronger than uncoercibility, since uncoercible solutions such as *deniable encryption* (Canetti et al. (1997)) are not always receipt-free. For example, in (Hirt and Sako (2000)) it is shown that the protocol of (Benaloh and Tuinstra (1994)) is uncoercible but does not provide receipt-freeness. Furthermore, voters using deniable encryption can actually decide not to lie in order to sell their vote to a coercer. In (Delaune et al. (2005)) a rather stronger notion of receipt freeness is formalized: A coercer should fail not only in respect of *how* the voter has voted, but also in respect of *whether* the voter has voted.

[3] Current machines in polling place e-voting do not produce paper receipts but require voters to trust them on correctly recording their vote and including it in the final tally. A new kind of encrypted receipts for polling place elections, which cannot be transferred to a coercer, was recently proposed in (Chaum (2004)) and it is based on visual cryptography.

etc), may also allow a dishonest third party to force the voter to reveal his/her vote. Another controversial pair of security properties are *privacy* and *eligibility*: it seems difficult in online elections to unequivocally identify and check the credentials of a voter, while at the same time protecting the privacy of his/her vote.

In the following sections we review the proposed generic cryptographic models and describe how these models were extended by recent cryptographic schemes to improve their security and functionality. Furthermore we refer to implementation and organizational issues and review a list of important and open issues that still need to be addressed before online voting is adopted for national elections.

2 Cryptographic models

Since the first cryptographic protocols for electronic elections was published (Chaum (1981); Demillo et al. (1982); Benaloh (1987)), several solutions have been described in academia to deal with the security problems in online voting. In this section we review the generic models and assess their suitability in terms of the following criteria: universal verifiability, support for write-in ballots, efficient voting, efficient tallying and large-scale support.

2.1 The Mix-net model

Mix networks (mix-nets), introduced in (Chaum (1981)), usually consist of a set of servers (mixes) which accept a batch of input messages and output the batch in randomly permuted (mixed) order so that the input and output messages are unlinkable (see Figure 1). Although originally proposed for anonymous e-mail communication between distrusting entities, mix-nets in online elections aim at hiding the origin of a ballot: tallying officials permute and randomize the encrypted ballots so that the link between the identity of the voter and the vote is broken. Depending on the mixing mechanism, mix-nets can be classified into *re-encryption* mix-nets and *decryption* mix-nets.

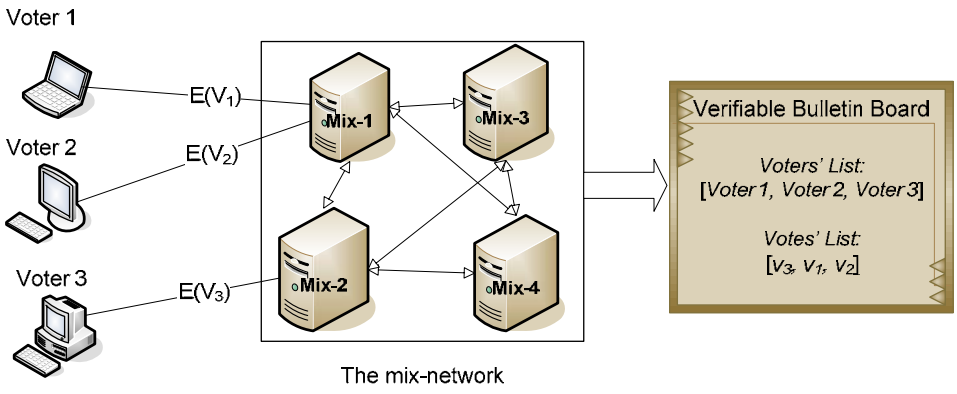

Figure 1. Voting with a mix-net (the general case)

Re-encryption mix-net. This type of mix-net (*e.g.* Ogata et al. (1997); Jakobsson (1999); Golle et al. (2004); Nguyen et al. (2004)) usually relies on a public key cryptosystem, which allows re-encryption of the input messages with a random number. Most re-encryption mix-nets use randomized public-key encryption schemes such as the ElGamal (ElGamal (1985)) or the Paillier (Paillier (1999)) cryptosystems, where the size of the ciphertexts can be independent of the number of the involved mix servers. In a typical implementation, individual votes are encrypted with the public key of the mix-net, while the decryption key is shared among the mix servers. Then the list of encrypted votes is sequentially re-encrypted and shuffled in each mix server.

The transformations are secret and verifiable, even if a number of mix servers are malicious. The final list of encrypted votes is decrypted by a number of honest mix servers, using *threshold decryption*[4] techniques (Desmedt (1994)). A few cryptographic schemes (*e.g.* Hirt and Sako (2000); Neff (2001); Juels et al. (2002); Jakobsson et al. (2002); Acquisti (2004); Aditya et al. (2004)) employ re-encryption mix-nets to protect voter privacy, since this model adds flexibility by separating the mixing

[4] Threshold cryptosystems (Desmedt (1994)) have been proposed to establish robustness in distributed protocols. In one setting, a set of M voting authorities in a (t, M) threshold public-key encryption system share a private key, and there is only one public key corresponding to the shared private key. The voter posts the ballot encrypted with the

and the decryption phases. A typical re-encryption mix-net for voting is shown in Figure 2.

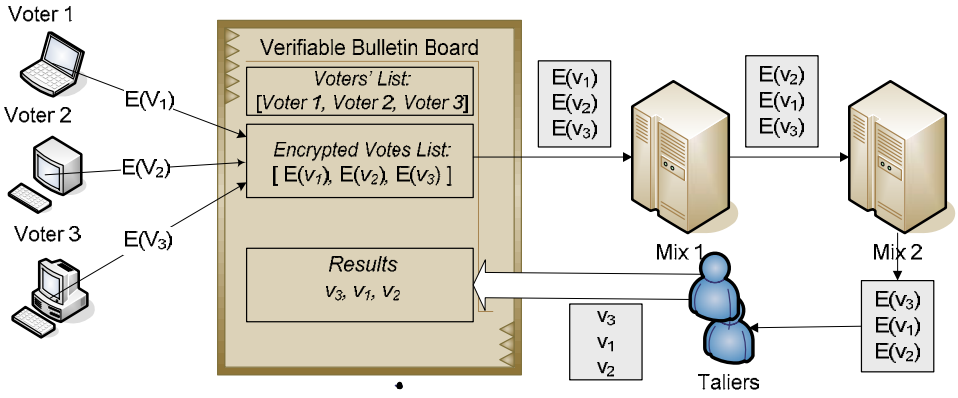

Figure 2. A typical re-encryption mix-net

Shuffle decryption mix-net. This type of mix-net (*e.g.* Chaum (1981); Abe (1998); Furukawa (2004)) accepts as input a collection of ciphertexts and outputs the corresponding list of plaintexts in a randomly permuted order[5]. A number of independent mixers sequentially perform the shuffling and decryption of encrypted votes in a way that the final votes cannot be linked to the original set of encrypted votes, while at the same time the verifiability of the correct output is established. Shuffle decryption is considered as more efficient than re-encryption shuffles.

public key of the authorities. Any subset of *t* honest and functioning authorities are able to combine their key shares and decrypt the final tally.

[5] In the original proposal (Chaum (1981)) the ballot is successively encrypted with the public key of each of the mix servers it will traverse, in reverse order. Each server then decrypts, shuffles and forwards to the next server.

However in case of failure of one of the mix servers, systems based on shuffle decryption usually need more computation to recover (Furukawa (2004)).

The mix-net model (both re-encryption and shuffle decryption techniques) satisfies voter privacy, verifiability, and robustness. In the optimum scenario, voter privacy is assured if at least one mix server behaves honestly and does not reveal the relation between its input and output links. To satisfy the verifiability criterion, the servers must prove or at least provide strong evidence (*e.g.* Jakobsson et al. (2002)) that their shuffles were correctly constructed; otherwise a malicious server could insert fake votes to the final tally. These proofs are constructed using *zero-knowledge*[6] techniques (Goldreich et al. (1991)), so that no information is provided about the secret shuffle, besides that the shuffle was correct. In universally verifiable mix-nets (*e.g.* Abe (1998)), an independent observer is able to verify that the output of each mix was correctly computed from the input. Alternatively, the servers may establish verifiability among them and then validate the generated list (*e.g.* Jakobsson (1999)).

[6] These are prover-verifier interactive protocols, where the prover proves a statement to the verifier and the verifier learns nothing from the prover that he could not learn by himself, apart from the fact that the prover knows the proof (Goldreich et al. (1991)). Zero-knowledge proofs have been extensively used in online voting schemes, for example to establish correctness of shuffles in mix-nets (Hirt and Sako (2000)), to prove the validity of a vote in homomorphic elections (Cramer et al. (1997)), to prove

Mixnet elections require fewer interactions by the voters and have inherent support for "write in" ballots. A disadvantage of mix-nets is that in their fully robust form they may need complex protocols for generating and maintaining shared private keys, as well as for mixing and proving correctness of the shuffles. Mix-nets can be efficient if: (a) the computation required by a voter is independent of the number of mix servers; (b) the complexity involved at the server-side processing can be tolerable; and (c) the verifiability checks can be kept substantially low. Recent results, have improved the efficiency and practicality of mix-nets (*e.g.* Furukawa (2004); Nguyen et al. (2004)).

2.2 The homomorphic model

According to this model, introduced in (Cramer et al. (1997)) and extended in (Baudron et al. (2001)), each voter signs and publishes an encryption of his/her vote. Encrypted votes are then "added" into the final tally, to form an encryption of the "sum" of the submitted votes. The model is based on the algebraic *homomorphic* properties of several probabilistic public key cryptosystems. These cryptosystems encrypt a

---

correctness of decrypting the votes without revealing the secret decryption key (Neff (2001)).

message M by raising a base g to the power M modulo a large prime number, and then randomizing the result. With homomorphic encryption there is an operation $\oplus$ defined on the message space and an operation $\otimes$ defined on the cipher space, such that the "product" of the encryptions of any two votes is the encryption of the "sum" of the votes, *i.e.*:

$$E_{M_1} \otimes E_{M_2} = E(M_1 \oplus M_2)$$

This property allows either to tally votes as aggregates or to combine shares of votes (see for example Benaloh (1987); Schoenmakers (1999)), without decrypting single votes. However, each vote must belong to a well-determined set of possible votes such as {+1, -1} for {"yes", "no"} votes. Moreover, each voter must provide a universally verifiable proof that his/her vote belongs to the predefined set of votes, otherwise, it would be easy for a malicious voter to manipulate the final tally.

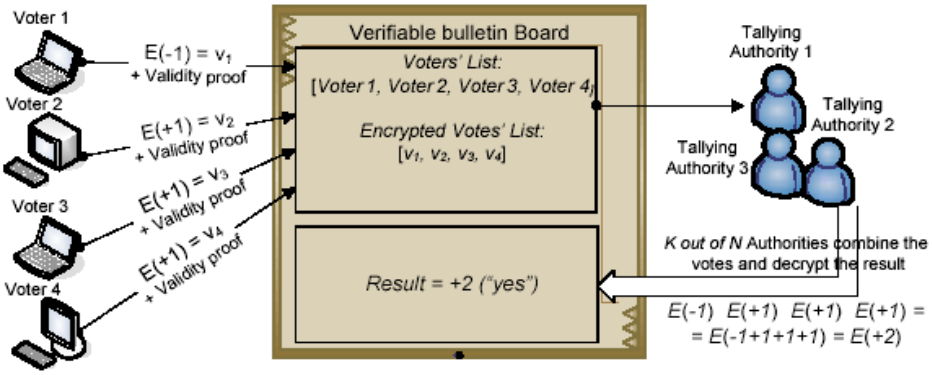

Figure 3. The homomorphic model (Cramer et al. (1997))

After the voting period has closed, a threshold of election authorities cooperatively decrypt the final tally. The results are published on a *bulletin board*[7] and the accuracy of the voting stage is verified. Depending on the level of trust given to them, the authorities may also provide a publicly verifiable proof that the decryption was correct. In this way individual voters and/or external observers can be assured that all the votes were counted correctly. An example of the homomorphic voting model is shown in Figure 3.

While the original model provides a general framework that allows usage of any probabilistic encryption scheme, only few probabilistic encryption schemes can scale well in large elections with multiple candidates. For example, in (Cramer et al. (1997)) a variant of the ElGamal encryption scheme required an exhaustive search over all possible election results by the authorities for the computation of the final tally. Recent proposals have been based on additively homomorphic public key cryptosystems with trapdoor decryption of discrete logarithms (Paillier (1999); Baudron et al. (2001); Damgard et al. (2003)), in order to allow handling of very large tallies.

[7] The notion of a bulletin board was introduced in (Benaloh (1987)) as a basic primitive that allows authenticated communication between each pair of processes in a system. All

The homomorphic model satisfies the accuracy, privacy, fairness, robustness and universal verifiability properties. It also inherently supports prevention of double voting, since the voters do not need to be anonymous. It works well in elections where ballots have only questions of a *K-out-of-L* type, which precludes write-in ballots. Another unattractive feature is that voters may need to run special-purpose code on their computer, for constructing the zero-knowledge proof of validity for their vote.

2.3 The verifiable secret sharing model

This model (Benaloh (1987)) uses a *homomorphic secret sharing* scheme. With such schemes there is an operation $\oplus$ defined on the share space, such that the "sum" of the shares of any two secrets x_1, x_2 is a share of the secret $x_1 \oplus x_2$. In the voting scheme proposed in Benaloh (1987) each voter shares his/her vote among *n* voting authorities. The shares are encrypted with the public key of the receiving authority, authenticated, and posted on a bulletin board. At the end of the voting period each authority adds all the received shares to get an encrypted share of the tally.

---

communication supported by the bulletin board is public and authenticated. A practical implementation of the primitive was proposed in the Rampart project (Reiter (1995)).

Finally the authorities combine their shares to get the encrypted tally. Thus no single vote is ever decrypted. For robustness, a (t, N) homomorphic threshold scheme is used: then only t out of N authorities need to combine their (true) shares. Late schemes employ this model in a universally verifiable way, both in the sharing and tallying phases (Cramer et al. (1996); Schoenmakers (1999)).

The verifiable secret sharing model achieves voter privacy, robustness and universal verifiability. Protection from double voting is analogous to the homomorphic model. In order to prevent voters from disrupting the election by sending false shares to authorities, voters similarly need to construct zero knowledge proofs of validity for their votes. Compared with the homomorphic model, verifiable secret sharing moves computation and communication burden from talliers to voters. This method requires communication between a voter and all servers, while the talliers do not need to run a shared-key generation protocol for a threshold decryption scheme. As a result, it can be considered as more suitable for small-scale elections, where voters may be talliers as well.

2.4 The «blind» signature model

Election protocols of this category, introduced in (Fujioka et al. (1992)), enable voters to get their vote validated from an election authority, while preserving the secrecy of their vote. Blind signatures (Chaum (1982)) are the electronic equivalent of signing carbon-paper-lined envelopes: a user seals a slip of a paper inside such an envelope, and later gets it signed on the outside. When the envelope is opened, the slip will bear the carbon image of the signature. When used in an online voting protocol, a voter encrypts, then blinds the vote, and presents it to a validating authority for validation. After the authority validates the vote, the voter un-blinds the encrypted vote and gets a validated vote that cannot longer be correlated to the original blinded message. The voter then uses an *anonymous channel*[8] to submit the validated vote to the tallying authorities, as shown in Figure 4.

[8] The logic of mix networks has been implemented in various systems to provide for anonymous web browsing (*e.g.* the onion routing system (Goldschlag et al. (1999)) and for anonymous electronic mail (*e.g.* the Mixminion system (Danezis et al. (2003)). Besides mix networks, proxy-based systems such as the Anonymizer and the Lucent Personalized Web Assistant (Lucent, 2001) have been implemented. Other systems combine several characteristics of both mix-nets and proxy-based systems, such as the CROWDS (Reiter and Rubin (1998)) and the Hordes (Shields and Levine (2000)) systems. Admittedly though, anonymous channels are still considered quite difficult to implement in practice (Danezis (2004)).

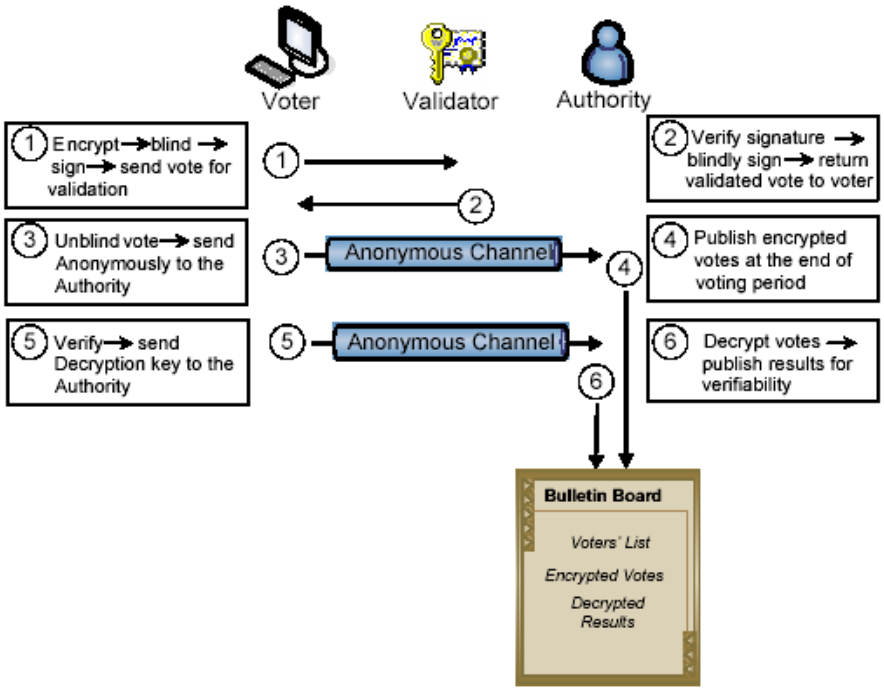

Figure 4. The blind signature model (Fujioka et al. (1992))

Protocols within this model are simple, easily manageable, computationally efficient and naturally support "write-in" ballots. A problem with early schemes (Fujioka et al. (1992); Cranor and Cytron (1997); Herschberg (1997)) was the ability of a malicious server to impersonate absentee voters in the final tally, thus violating the democracy criterion. In the original model (Fujioka et al. (1992)) two-phase voting was supported to achieve fairness: voters submitted their encrypted vote and then waited until the end of the election to submit their vote-opening keys. In (Cranor and Cytron (1997); Herschberg (1997)) the protocol of

(Fujioka et al. (1992)) was changed to allow voters to vote and walk away, however in both protocols there is the risk that a malicious authority learns intermediate results, therefore violating the fairness property. In subsequent proposals (Ohkubo et al. (1999); Durette (1999); Joaquim et al. (2003); Lebre et al. (2004)) the power of administration is distributed among multiple authorities so that a) no election administrator is able to impersonate legitimate voters in the final tally, and b) the results are becoming available only at the end of the election. To establish robustness in the election process, threshold techniques were also proposed (Ohkubo et al. (1999); Joaquim et al. (2003); Lebre et al. (2004)). For example, in Ohkubo et al. (1999), a (t, N) threshold cryptosystem assured that as long as N-t+1 counters are honest, the results will only be available at the end of the election. Figure 5 summarizes the basic cryptographic models for online voting and their core properties.

Properties / Models	Universal verifiability	Write-in ballots	Efficient voting	Efficient tallying	Large-scale support
Homomorphic Model	√	X	X	√	√
Verifiable Secret Sharing	√	X	X	√	X
Mix-net Model	√	√	√	X	X
Blind Signature Model	X	√	√	√	√

Figure 5. The basic cryptographic models and their core properties

2.5 Hybrid schemes

Recent proposals combine two or more election models in order to satisfy most of the security requirements and integrate the best of each model into a single online election protocol. The scheme of (Hirt and Sako (2000)) combines the homomorphic model with mix-net shuffles to allow universally verifiable elections with receipt-free ballots. In (Baudron et al. (2001)), the blind signature model was proposed to establish voter anonymity in receipt-free homomorphic elections. In (Kiayias and Yung (2004)) another hybrid scheme was presented, based on the homomorphic

and the mix-net models, providing support for a variety of ballots (write-in and *1-out-of-L* voter choices) in universally verifiable elections. In another proposal (Acquisti (2004)) a set of mix authorities issue shares of credentials to each voter; Later, the voter combines his/her vote with the credentials using the homomorphic property of the encryption scheme. The hybrid scheme in Acquisti (2004) satisfies universal verifiability and receipt-freeness without untappability assumptions about the communication channel between the voters and the authorities.

Hybrid schemes are by default complex systems. A challenge for the research community is the design of hybrid systems that efficiently and effectively balance the requirement for secure and practical online elections. Figure 6 summarizes the security properties of recent cryptographic schemes for online elections.

	Security *						Practicality *			Crypto Models		Cryptographic Primitives							
	Universal verifiability	Fairness	Receipt-Freeness	Democracy – Accuracy	Privacy	Robustness	Large-scale	Write-in Ballots	Multile Candidates	Hommomorphic	Verifiable Secret Sharing	Mix-net	Blind Signature	Bulletin Board	Untappable Channels	Anonymous Channels	Threshold Crypto	ZKP (Voter)	ZKP (Authority)
Crypto Schemes																			
ADITYA *et al*, 2004	v	v	v	v	v		v	v	v			v		v	v		v		v
ACQUISTI, 2004	v	v	v	v	v	v	v		v	v		v		v			v		v
BALDRON *et al*, 2001	v	v	v	v	v	v	v		v	v			v	v			v	v	v
CRAMMER *et al*, 1996	v	v		v	v	v	v				v			v			v	v	
CRAMMER *et al*, 1997	v	v		v	v	v	v			v				v			v	v	
CRANOR and CYTRON, 1997					v			v	v				v			v			
DAMGARD et al, 2003	v	v		v	v	v	v		v	v				v			v	v	
DURETTE, 1999		v		v	v		v	v	v				v			v			
HERSCHBERG, 1997		v			v			v	v				v			v			
HIRT and SAKO, 2000	v	v	v	v	v	v			v	v		v		v	v		v		v
JUELS *et al*, 2002	v	v	v	v	v	v			v			v		v		v	v	v	v
KATZ *et al*, 2001	v	v		v	v	v				v				v			v		v
KIAYIAS and YUNG, 2004	v	v		v	v	v	v	v	v	v		v		v	v		v	v	v
LEBRE *et al*, 2004		v		v	v	v	v	v	v				v			v	v		
LEE and KIM, 2002	v	v	v	v	v	v	v		v	v				v	v		v	v	
MAGKOS *et al*, 2001	v	v	v	v	v	v	v			v				v	v		v	v	
NEFF, 2001	v	v		v	v	v	v	v	v			v		v			v		v
OHKUBO *et al*, 1999		v		v	v	v	v	v	v				v	v		v	v		
SCHOENMAKERS, 1997	v	v		v	v						v			v				v	
TING and HUNG, 2004	v	v		v	v	v			v		v	v		v			v	v	

* The symbol v may indicate either unconditional or conditional fulfilment of a property *e.g.* under physical or logical assumptions

Figure 6. Properties of recent cryptographic schemes for online elections

2.6 Level of trust in the cryptographic setting

In a few cryptographic elections the power of the voting authorities is distributed by using *threshold cryptography* (Desmedt (1994)), to achieve a minimal level of robustness. In practice this approach should involve parties having no reason to collude (*e.g.* opposing political parties or interest groups). In other schemes, a coalition of two authorities may undermine one or more security properties (*e.g.* Cranor and Cytron (1997)). In the least secure systems, a single authority is usually trusted for privacy and democracy. Other protocols, which assume that all voters, or a majority of voters behave honestly (*e.g.* Chaum (1981)) cannot be of practical use for large-scale elections.

2.7 Implementations of the cryptographic models

While several cryptographic protocols have been proposed in the literature, only few of them have been implemented during R&D project development or by commercial systems. The «blind signature» model has been implemented in several projects, mainly due to its simplicity and flexibility. The first implementations were the Sensus system (Cranor and Cytron (1997)) and the EVOX (Herschberg (1997)) system. The EVOX

system was improved by EVOX Multiple Administrators (Durette (1999)) which in turn was succeeded by the REVS system (Joaquim et al. (2003)) in an effort to eliminate single entities from disrupting the election. Improved implementations of the REVS system (Lebre et al. (2004)) increase the robustness of REVS. This is achieved with a scheme that prevents specific denial of service attacks against protocol participants from colluding malicious servers.

The EU (Cybervote) and the E-Vote (EU-IST (2004)) projects led to the implementation and use in pilot elections (in Germany, France, Portugal and Greece among others) of a system based on the homomorphic model, and specifically on its extension with the Paillier cryptosystem (Damgard et al. (2003)). Recent E-Vote pilot projects in Portugal involved the testing of mobility platforms. An internet vote platform in simulation format was implemented, for voters living abroad. Another pilot project involved a system that produces paper trail for the voter, since such systems increase the confidence of the system[9]. In order to attain political and social consensus necessary to project's success, both experiences were supervised by the National Commission on Elections and by the National Commission for Data Protection.

[9] Concerns about implementations that do not produce paper trail have been raised in many countries, including the United States.

Finally, a re-encryption mix-net (Neff (2001)) has been implemented by the commercial system VoteHere (VoteHere). Recent improvements of this system allow voters to track the status of their own ballot over a Web site and verify their vote, using encrypted identification codes. As mix-nets are becoming more efficient, it is expected that they will play their role in online voting systems.

3 Scalability and Flexibility Issues for Cryptographic Protocols

Any online election system destined for wide-scale elections must have inherent support for large sets of voters and candidates. Moreover, it may be a requirement that the system be able to handle a variety of ballot question formats and/or write-in ballots. On the other hand, there is a broad category of cryptographic protocols that aim at elections held among a relatively small set of voters, for example boardroom meetings within an organization. Such protocols are of special interest, they introduce new privacy requirements and will be studied separately.

3.1 Large groups of voters and multiple candidates

For technical reasons, early voting schemes employed the Boolean {“yes”, “no”} model in a single candidate setting. As this was not flexible, most schemes were modified over time to support *1-out-of-L* or *K-out-of-L* selections (see for example Cramer et al. (1997); Baudron et al. (2001)). The candidates may be people names or any arbitrary set of propositions among which a choice has to be made. Running an election with large tallies and multiple candidates may affect the overall efficiency of the election protocol, especially during the voting and tallying stages. For example, in Cramer et al. (1997) the authorities needed an exhaustive search of $\Omega(\sqrt{M}^{L-1})$ exponentiations to decrypt the final tally, where M is the number of voters and L is the number of candidates in a *1-out-of-L* setting. This may be acceptable in small size elections with boolean decisions (L=2) but it is not practical in national multi-candidate elections. Recent proposals (*e.g.*, Baudron et al. (2001); Damgard et al. (2003); Kiayias and Yung (2004)) turn the complexity of decrypting the tally logarithmic or linear to the number of candidates. This is done by employing trapdoor discrete logarithm schemes, such as the Paillier cryptosystem (Paillier (1999)).

3.2 Write-in ballots

Another challenge in cryptographic election schemes is the format of the submitted ballots. With write-in ballots a voter is able to insert a freely chosen message. This right is provided in a few legislations and jurisdictions. Among the cryptographic models described earlier, the homomorphic model and the verifiable secret sharing model are not suitable for supporting write-in ballots. Schemes of the above category are rather suitable for *1-out-of-L* or *K-out-of-L* choices. On the other hand, elections based on mix-nets and blind signatures have inherent support for write-in ballots (Neff (2001)). Of special interest is the design of receipt-free protocols that also allow for write-in ballots (Acquisti (2004)), which seems contradictory: a voter can always commit to an arbitrary random-like value, supplied a priori by the coercer. Thus, when write-in ballots are allowed, the protocol may become exposed to: a) randomization attacks aiming to force the voter to vote in a certain way, and b) forced abstention attacks aiming to ensure that a vote will not be counted (Juels et al. (2002)). It seems that receipt-freeness can only be achieved if there is some fixed encoding format for the write-in ballots.

3.3 Small-scale elections

Cryptographic small-scale elections were originally proposed in Chaum (1981). In boardroom elections (*e.g.* Katz et al. (2001); Ting and Hung (2004)) the sets of voters and voting authorities need not be disjoint: each player may be both a voter and a tallier. Such elections may also introduce stronger privacy requirements: for example, the election must not disclose the vote counts of any individual candidate but only determine the winner (Ting and Hung (2004)). Among the models described earlier, the homomorphic model and the verifiable secret sharing model can naturally support small-scale elections, since encrypted votes are accumulated in the final tally and atomic votes are never decrypted. There are constructions that are exclusively fitted in boardroom elections where the outcome can be described with only one bit of information. These constructions are self-adjudicated and can be cast in the framework of secure *multiparty computation* techniques (Goldreich et al. (1986)). These constructions require interaction among voters. As a result, if any voter stops following the voting protocol the election may be disrupted. In a different approach, a failure of a single voter still disrupts the election, but the failure can be traced (Chaum (1988)). In general, protocols that require interaction among voters are not considered suitable for large-scale elections.

4 Open problems and other issues for real elections

4.1 Receipt-free and uncoercible protocols

Receipt-freeness will probably be the last security property that will be supported by real-life systems for online elections. In cryptographic research, most proposals for receipt-freeness involve some ad hoc physical assumptions and procedural constraints, for example *untappable channels* (Okamoto (1997); Hirt and Sako (2000); Aditya et al. (2004)), or physical *voting booths* (Benaloh and Tuinstra (1994)). An untappable channel may require a physically separated and closed communication medium, *e.g.* a leased line inaccessible from outsiders. In large-scale online elections, implementing such channels without introducing extra inconveniences for voters seems impossible. In Hirt and Sako (2000) it was claimed that one-way untappable channels between voters and authorities is a minimal physical assumption for receipt-free elections. Other schemes assumed the existence of tamper-resistant smartcards (Magkos et al. (2001)) or randomizers (Lee and Kim (2002)) to refrain voters from creating a receipt for their ballot. Current research focuses in designing receipt-free but also flexible systems with minimal or no physical constraints (Baudron et al. (2001); Juels et al. (2002); Acquisti (2004); Groth and Salomonsen

(2004)). Furthermore, recent receipt-free schemes (Baudron et al. (2001); Juels et al. (2002); Lee and Kim (2002); Acquisti (2004)) use a specific class of zero-knowledge proofs, namely *designated verifier* proofs (Jakobsson et al. (1996)) and *divertible zero-knowledge* proofs (Burmester and Desmedt (1991)), in order to prove in a non-transferable way: a) the correctness of re-encrypting and/or b) the validity of an encrypted vote. These proofs relax the need for physical assumptions about the voter-authority communication channel.

Most receipt-free protocols are oriented towards the homomorphic model since encrypted votes are accumulated and individual votes are never decrypted. However, there have also been presented receipt-free protocols that belong to the mix-net model (Aditya et al. (2004)) and the blind signature model (Okamoto (1997)).

4.2 Public Key Infrastructures

Most online voting schemes assume either implicitly or explicitly, the existence of a Public Key Infrastructure (PKI). It is assumed that voters are registered prior to the election and that cryptographic keys are in place without always specifying the details of key management. Ideally, in a network with an established PKI, all participating entities would obtain

authentic certificates regarding their public keys (for encryption and/or signature) in order to be able to establish secret and authenticated communications throughout the election stages. In practice however, setting up a PKI for online large-scale elections seems a difficult task. Existing methods for secure integration of public key verification systems into web browsers still face challenges such as trust and certificate revocation issues. As a result, until a PKI is in place, solutions based on usernames and passwords will introduce substantial security risks.

4.3 External attacks

Two kinds of attacks against online voting systems can be considered: external attacks and internal attacks. External attacks may corrupt some of the protocol's properties but do not explicitly target the voting protocol and its vulnerabilities, nor the protocol entities. For example, attacks against operating systems, buffer overflows, worms, Trojans and key-loggers, as well as network oriented attacks such as Distributed Denial of Service, SYN flooding, packet sniffing and spoofing attacks. Social engineering may also be considered as an external attack, where voters may be deceived into connecting to a spoofed election site and expose their vote to an attacker; in this attack, also known as a *Man In the Middle* (MIM) attack, the attacker may also collect whatever credentials the voter

has and cast a (new) vote on behalf of the victim. Another kind of external attack that cannot be dealt by any online election protocol is the case where a coercer watches the voter as he/she submits a vote over the Internet. This attack is possible in any system that uses personal computers to vote over the Internet and it is beyond the scope of cryptographic research. However, if a voter uses the voting protocol to get or construct a receipt of his vote, then this is considered as an internal attack. The goal of receipt-free voting protocols is to prevent such a massive coercion scenario, where receipts could be massively sent through the Internet to a coercer, thus disrupting the election results.

4.4 Implementation issues

The majority of voting systems that have been used so far for pilot online elections (*e.g.* refer to (Prosser et al. (2005)) for a list and references) may be considered as the electronic equivalent of submitting absentee ballots. In this setting two processes are usually involved, one for checking the identity of the voters (*e.g.* using a PIN-based approach) and the other for tallying the "anonymous" votes. Such systems cannot guarantee voter privacy against a malicious election server or a coalition between the election processes (Kohno et al. (2004)). Furthermore, the majority of commercial e-voting platforms received much criticism concerning

security and privacy issues (e.g. a report on the e-voting system used for national voting in Ireland can be found in (Commission (2006)). In practice, the commercial vendor of the voting platform is usually trusted on most of the core security properties for the election. This is a major weakness, considering the fact that most commercial systems are based on closed code and their functionality has minimal transparency (Rubin (2004); Kohno et al. (2004)). Critics often argue that a line-by-line independent review on the voting software (which is embedded in the voting machines or distributed for remote e-voting) is needed to exclude the possibility that malicious code is embedded in the system. Furthermore, real systems need to be supported by complementary mechanisms (e.g. tamper-resistant modules) to prevent or detect possible tampering with the software. Moreover, cryptographic protection is often neglected or not well documented.

It is believed that present or future real-life systems must meet several security-related requirements before they can be used for national elections or other elections with strict security requirements:

- *Open source software*. Open code can be examined for flaws by independent outsiders and may prevent embedding of malicious code.

- *Testing Transparency*. Testing should be transparent for the voters who should be aware of the testing process.
- *Standardization*. Hardware and/or software implementation should be based on well-defined standards.
- *Legal framework*. Attempts to bypass or manipulate the system, either from the providers of hardware and software or from any other party, and non-complience with security standards should be under severe legal penalties.

A very important issue, although not directly related to security and thus not considered in this paper, is the design and usability challenges (Fairweather, (2005)) for any practical online voting system. Furthermore, new trends for establishing a number of alternative channels for remote voting (e.g. telephone, SMS text message, interactive TV e.t.c.) amplify the need for designing lightweight applications and interoperable services. A risk analysis methodology for different e-voting channels was proposed in (Nevo and Kim, (2006)). Implementing security and cryptography for such alternative voting channels must also take into account the efficiency and bandwidth requirements often posed by handheld-like devices.

4.5 Managerial implications

Running an e-voting system (whether polling place, kiosk or Internet) for large scale elections requires the completion of numerous administrative activities (Xenakis and Macintosh, (2005)). Especially for remote Internet voting, of specific interest are the electronic management of voter registration, as well as the management and dissemination of voting credentials (such as tamper-resistant smartcards). Furthermore, provisions for the maintenance and the availability of election databases and telecommunication facilities should be explicitly documented. In addition, procedures for the safe storage of submitted votes, for reporting election results and maintaining audit trails need to be documented as well. Finally, procedures for the provision, installation and examination of the authorized software and hardware for the election server(s) must be documented and agreed upon long before the election day. The roles and responsibilities of the participants (voters, election personnel, commercial suppliers, software testers e.c.t). need to be clearly and unambiguously defined. Communication channels, both internal between the authorities and e-voting suppliers, as well as external between the electorate and the local authorities should be established during a necessary period before the election day.

5. Is secure online voting feasible?

In the cryptographic research there has never been an online election scheme which satisfies completely all the ideal security and functionality requirements. Evidently there is a tradeoff between security and efficiency and the research community is on a quest for balancing this tradeoff. In addition, a few schemes attempt to satisfy contradicting security requirements such as verifiability & receipt freeness, and privacy & democracy. It seems that a perfect online voting scheme for generic use may be a paradox. However, as described in the previous sections, current cryptographic research has come up with satisfactory solutions for specific voting applications. Secure small-scale voting schemes seem to be more feasible, especially in the case of boardroom elections. Also the case of {“yes”, “no”} online voting seems to deal less practical problems. Admittedly though, there is still a lot of work required from cryptographic research.

Recent test-beds and critics on commercial e-voting systems have shown that current systems fail on establishing assurances for some very basic security features such as voter privacy and verifiability. This becomes even harder, considering the requirements for low complexity and user simplicity. Moreover, one has to have in mind that cryptography is not a

panacea for secure online voting. Real-life systems will face much the same threats as other Internet applications.

We believe that transition to remote online voting cannot be a one-off step. Considering the implications of external attacks such as malware and network protocols attacks against users with low security awareness, there may still be a long way until setting up a remote Internet voting channel (e.g. using a PC at home), where the most vulnerable part will be the voter's computing environment. Intermediate steps such as voting via Internet-connected kiosks, already implemented in several pilots (e.g. in 2003 UK local elections (Electoral Commission (2003)), may be a viable option for the near future. The final step of this transition, *i.e.* remote online voting from PCs and other personal devices, will require further security research before it becomes a viable reality. Until then, cryptographic and security research needs to evolve in parallel with research on the various organizational issues that surround the electoral reform. Furthermore, analysis and lessons learned from e-voting pilots already conducted in a number of places will provide us with valuable experience.

References

Abe, M. 1998. Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-centers. In Proceedings of the Advances in Cryptology – EUROCRYPT 98, LNCSVol. 1403. Springer-Verlag, 437–447.

Acquisti, A. 2004. Receipt-Free Homomorphic Elections And Write-In Ballots. Tech. Rep. 2004/105, CMU-ISRI-04-116, Carnegie Mellon.

Aditya, R., Lee, B., Boyd, C., And Dawson, E. 2004. An Efficient Mixnetbased Voting Scheme Providing Receipt-Freeness. In Proceedings of the 1st Trustbus 2004, LNCS Vol. 3184. Springer-Verlag, 152–161.

Anonymizer. Available at: http:/www.anonymizer.com.

Baudron, O., Fouque, P., Pointcheval, D., Poupard, G., And Stern, J. 2001. Practical Multi-Candidate Election System. In *Proc. of the 20th ACM Symposium on Principles of Distributed Computing*. ACM Press, 274–283.

Benaloh, J. 1987. Verifiable Secret Ballot Elections. Ph.D. Thesis, Yale University.

Benaloh, J. And Tuinstra, D. 1994. Receipt-Free Secret-Ballot Elections. In Procceedings of the 26th Annual ACM Symposium on Theory of Computing. ACM Press, 544–553.

Burmester, M. And Desmedt, Y. 1991. All Languages In Np Have Divertible Zero-Knowledge Proofs And Arguments Under Cryptographic Assumptions. In Proceedings of the Advances in Cryptology – EUROCRYPT'90. LNCS, vol. 473. Springer-Verlag, 1–10.

Burmester, M. And Magkos, E. 2003. Towards Secure And Practical E-Elections In The New Era. In Advances in Information Security – Secure Electronic Voting. Kluwer Academic Publishers, 63–76.

Canetti, R., Dwork, C., Naor, M., And Ostrovsky, R. 1997. Deniable Encryption. In Proceedings of the Advances in Cryptology – CRYPTO'97. LNCS, vol. 1294. Springer-Verlag, 90–104.

Chaum, D. 1981. Untraceable Electronic Mail, Return Addresses, And Digital Pseudonyms. Commun. ACM 24, 2, 84–88.

Chaum, D. 1982. Blind Signatures For Untraceable Payments. In Proceedings of the Advances in Cryptology – CRYPTO'82. Plenum Press, 199–203.

Chaum, D. 1988. Elections With Unconditionally Secret Ballots And Disruption Equivalent to Breaking RSA. In Proceedings of the Advances in Cryptology – EUROCRYPT'88. LNCS, vol. 330. Springer-Verlag, 177–182.

Chaum, D. 2004. Secret-Ballot Receipts: True Voter-Verifiable Elections. In Security and Privacy. IEEE , 2, 1), 38–47.

Commission On Electronic Voting, 2006. Second Report on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System. Available: http://www.cev.ie/htm/report/download second.htm

Cramer, R., Franklin, M., Schoenmakers, B., And Yung, M. 1996. Multi-Authority Secret-Ballot Elections with Linear Work. In Proceedings of the Advances in Cryptology – EUROCRYPT'96. LNCS, vol. 1070. Springer-Verlag, 72–83.

Cramer, R., Gennaro, R., And Schoenmakers, B. 1997. A Secure And Optimally Efficient Multi-Authority Election Scheme. European Trans. On Telecommunications 8, 5, 481–490.

Cranor, L. And Cytron, R. 1997. Sensus: A Security-Conscious Electronic Polling System For The Internet. In Proceedings of the International Conference on System Sciences. Wailea, Hawaii.

Cybervote. The Cybervote Project. Available: Http://Www.Eucybervote.Org/

Damgard, I., Jurik, M., And Nielsen, J. 2003. A Generalization Of Paillier's Public-Key System With Applications To Electronic Voting. International Journal Of Information Security To Appear.

Danezis, G. 2004. Better Anonymous Communications. Ph.D. thesis, University of Cambridge.

Danezis, G., Dingledine, R., And Mathewson, N. 2003. Mixminion: Design of A Type Iii Anonymous Remailer Protocol. In Proceedings of the IEEE Symposium on Security and Privacy. IEEE.

Delaune, S., Kremer, S., And Ryan, M. 2005. Receipt-Freeness: Formal Definition and Fault Attacks (Extended Abstract). In Proceedings of the Frontiers in Electronic Elections Workshop (FEE'05). IEEE, Milan, Italy.

Demillo, R., Lynch, N., And Merritt, M. 1982. Cryptographic Protocols. In Proceedings of he 14th Annual ACM Symposium on Theory of Computing. ACM, 383–400.

Desmedt, Y. 1994. Threshold Cryptography. European Transactions on Telecommunications 5, 4, 449–457.

Durette, B. W. 1999. Multiple Administrators for Electronic Voting. M.S. thesis, Massachusetts Institute of Technology.

ElGamal, T. 1985. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Trans. on Information Theory 30, 4, 469–472.

Electoral Commission. 2003. Technical Report on the May 2003 Pilots. Available at: http://www.electoralcommission.org.uk/files/dms/Copyofcoverandreport-final_11369-8944__E__N__S__W__.pdf

EU-IST. 2004. E-Vote: An Internet Based Electronic Voting System, Legal And Regulatory Issues On E-Voting And Data Protection in Europe. EU-IST-200-29518 (D.3.4.).

Fairweather, B. 2005. Interfaces for Electronic Voting: Focus Group Evidence. In Electronic Government - an International Journal, Vol. 2, No.4, pp. 369-383.

Fujioka, A., Okamoto, T., And Ohta, K. 1992. A Practical Secret Voting Scheme for Large Scale Elections. In Proceedings of the Advances in Cryptology – AUSCRYPT '92. LNCS, vol. 718. Springer-Verlag, 244–251.

Furukawa, J. 2004. Efficient, Verifiable Shuffle Decryption and its Requirement of Unlinkability. In Proceedings of the Public Key Cryptography (PKC'04). LNCS, vol. 2947. Springer-Verlag, 319–332.

Goldreich, O., Micali, S., And Widgerson, A. 1991. Proofs That Yield Nothing But Their Validity, or All Languages in NP Have Zero-Knowledge Proof Systems. Journ. of the ACM 38, 691–729.

Goldreich, O., Micali, S., And Wigderson, A. 1986. Proofs That Yield Nothing But Their Validity and a Methodology of Cryptographic Protocol Design. In Proceedings of the 27th Annual Symposium on Foundations of Computer Science, IEEE, Ed. 174–187.

Goldschlag, D., Reed, M., And Syverson, P. 1999. Onion Routing For Anonymous And Private Communications. Commun. of the ACM 42, 2, 39–41.

Golle, P., Jakobsson, M., Juels, A., And Syverson, P. 2004. Universal Re-encryption for Mixnets. In Proceedings of the RSA Conference Cryptographers Track '04, T. Okamoto, Ed. LNCS, vol. 2964. Springer-Verlag, 163–178.

Groth, J. And Salomonsen, G. 2004. Strong Privacy Protection in Electronic Voting. BRICS Report Series - RS-04-13-2004, BRICS.

Herschberg, M. 1997. Secure Electronic Voting Using the World Wide Web. M.S. Thesis, MIT.

Hirt, M. And Sako, K. 2000. Efficient Receipt-Free Voting Based on Homomorphic Encryption. In Proceedings of the Advances in Cryptology – EUROCRYPT'00. LNCS, vol. 1807. Springer-Verlag, 539–556.

Houston, A., Yao, Y., Okoli, C. And Watson, E. 2005. Will Remote Electronic Voting Systems Increase Participation? In Electronic Government - an International Journal, Vol. 2, No.3, pp. 353-368.

Jakobsson, M. 1999. Flash Mixing. In Proceeding of the PODC'99. IEEE, 83–89.

Jakobsson, M., Juels, A., And Rivest, R. 2002. Making Mix Nets Robust for Electronic Voting by Randomized Partial Checking. In Proceedings of the 11th USENIX Security Symposium. IEEE, 339–353.

Jakobsson, M., Sako, K., And Impagliazzo, R. 1996. Designated Verifier Proofs And Their Applications. In Proceedings Of The Advances in Cryptology – EUROCRYPT'96. LNCS, vol. 1070. Springer-Verlag, 143–154.

Joaquim, R., Zuquette, A., And Ferreira, P. 2003. REVS - A Robust Electronic Voting Systems. In Proceedings of the IADIS'03 International Conference of e- Society. 95–103.

Juels, A., Catalano, D., And Jakobsson, M. 2002. Coercion-Resistant Electronic Elections. Cryptology ePrint Archive 165.

Katz, J., Myers, S., And Ostrovskyo, R. 2001. Cryptographic Counters And Applications To Electronic Voting. In Proceedings of the Advances in Cryptology – EUROCRYPT'01. LNCS, vol. 2045. Springer-Verlag, 78–92.

Kiayias, A. And Yung, M. 2004. The Vector-Ballot E-Voting Approach. In Proceedings of the Financial Cryptography – FC'04. LNCS, vol. 3110. Springer-Verlag, 72–89.

Kohno, T., Stubblefield, A., Rubin, A. D., And Wallach, D. S. 2004. Analysis Of An Electronic Voting System. In Proceedings of the IEEE Symposium on Security and Privacy. IEEE.

Lebre, R., Joaquim, R., Zquete, A., And Ferreira, P. 2004. Internet Voting: Improving Resistance to Malicious Servers in REVS. In Proceedings of the International Conference on Applied Computing – IADIS'04.

Lee, B. And Kim, K. 2002. Receipt-Free Electronic Voting Scheme with a Tamper-Resistant Randomizer. In Proceedings of the ICISC'02. LNCS, vol. 2587. Springer-Verlag, 389–406.

Lucent. 2001. Lucent personalized web assistant. http://www.belllabs.com/projects/lpwa.

Magkos, E., Burmester, M., And Chrissikopoulos, V. 2001. Receipt-Freeness in Large-Scale Elections Without Untappable Channels. In Proceedings of the 1st IFIP Conference on E-Commerce, E-business and E-Government. Kluwer Academic Publishers, 683–693.

Neff, A. 2001. A Verifiable Secret Shuffle and Its Application to E-Voting. In Proceedings of the 8th Computer and Communications Security Conference. ACM, Philadelphia, USA.

Neumann, P. G. 1993. Security Criteria for Electronic Voting. In Proceedings of the 6th National Computer Security Conference. IEEE.

Nevo, S., And Kim, H. 2006. How to Compare and Analyse Risks of Internet Voting Versus Other Modes of Voting. In Electronic Government - an International Journal, Vol. 3, No.1, pp. 105-112, 2006.

Nguyen, L., Safavi-Naini, R., And Kurosawa, K. 2004. Verifiable Shuffles: A Formal Model and a Paillier-Based Efficient Construction with Provable Security. In Proceedings of the ACNS04. LNCS, vol. 3089. Springer-Verlag, 236–247.

Ogata , W., Kurosawa, K., Sako, K., And Takatani, K. 1997. Fault Tolerant Anonymous Channel. In Proceedings of the 1st International Conference on Information and Communications Security – ICICS. LNCS, vol. 1334. Springer-Verlag, 440–234.

Ohkubo, M., Miura, F., Abe, M., Fujioka, A., And Okamoto, T. 1999. An Improvement on a Practical Secret Voting Scheme. In Proceedings of the Information Security Conference – IS'99. LNCS, vol. 1729. Springer-Verlag, 225–234.

Okamoto, T. 1997. Receipt-Free Electronic Voting Schemes for Large Scale Elections. In Proceedings of the 5th Security Protocols Workshop. LNCS, vol. 1163. Springer-Verlag, 125–132.

Paillier, P. 1999. Public Key Cryptosystems Based On Discrete Logarithms Residues. In Proceedings of the Advances in Cryptology – EUROCRYPT'99. LNCS, vol. 1592. Springer-Verlag.

Prosser, A., Krimmer, R., Kofler, R., And Unger, M. K. 2005. The Role of Election Commission In Electronic Voting. In Proceedings of the 38th International Conference on System Sciences. Waikoloa, Big Island, Hawaii.

Reiter, M. 1995. The Rampart Toolkit for Building High-Integrity Services. In Proceedings of the International Conference on Theory and Practice in Distributed Systems. LNCS, vol. 938. Springer-Verlag, 99–110.

Reiter, M. K. And Rubin, A. D. 1998. Crowds: Anonymity for Web Transactions. ACM Trans. on Information and Systems Security 1, 1, 66–92.

Rubin, A. 2004. Security Considerations for Remote Electronic Voting Over the Internet. Tech. rep., AT&T Labs. Available at: http://avirubin.com/evoting.security.html.

Schoenmakers, B. 1999. A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting. In Proceedings of the Advances in Cryptology – CRYPTO'99. Vol. 1666.

Shields, C. And Levine, B. N. 2000. A Protocol for Anonymous Communication over the Internet. In Proceedings of the 7th ACM Conf. on Computer and Communication Security, Jajodia, Ed. ACM, Athens, Greece, 33–42.

Ting, P. And Hung, P. 2004. A Small-Scale Voting Protocol Hiding Vote-Counts of all Candidates. Cryptology ePrint Archive 355.

VoteHere. The VoteHere System. Available at: http://www.votehere.net

Xenakis, A., And Macintosh, A. 2005. E-electoral Administration: Organizational Lessons Learned From the Deployment of E-Voting in the UK. Proceedings of the 2005 National Conference On Digital Government Research, pp. 191 – 197.