Chapter

TOWARDS SECURE AND PRACTICAL E-ELECTIONS IN THE NEW ERA

Mike Burmester; Emmanouil Magkos
Department of Computer Science, Florida State University, 214 Love Building, Tallahassee, Florida 32306, USA; Department of Informatics, University of Piraeus, 80 Karaoli & Dimitriou, Piraeus, 18534, Greece

Abstract: We overview the main e-voting schemes currently proposed in the literature and assess their security and practicality. We also analyze the security risks and discuss methods to minimize them.

Key words: E-voting, I-voting, security, cryptography, uncoercible protocols

1. INTRODUCTION

There is concern in many democracies about the declining rates in voter turnout and more generally, the (perceived) trend towards political apathy. To reverse this, and to promote political activity, political reform is needed. One of the measures considered is to simplify the election procedure by introducing electronic voting, and in particular Internet voting. It is expected that this will increase voter convenience and voter confidence in the accuracy of election results.

Electronic voting (e-voting) uses digital data to capture the voter selections. With Internet voting (I-voting) we also get remote connectivity via the Internet. A few Internet-based elections have already taken place[1], while pilot elections are scheduled in several countries. Broadly speaking, each election involves four distinct stages:

[1] Examples are: the Arizona Democratic party's election (legally binding), March 2000 [36]; the Military personnel Presidential election in the US and overseas (legally binding), 2000 [21]; the Alaska Republican party's election (non-binding), January 2000 [35]; the UK local and mayoral elections (non-binding), May 2002 [18].

- **Registration.** Prior to the election, voters prove their identity and eligibility. An electoral roll is created.
- **Validation.** During the election, voters are authenticated before casting their vote. Only one vote per voter is authorized.
- **Casting.** Voters cast their vote.
- **Tallying.** At the end of the voting period, all votes are counted.

Each of the above stages can take place by using *physical* or *electronic* procedures. In this paper we consider e-voting and focus on those types that involve at least one remote interaction via an open network such as the Internet. We distinguish two types of e-voting: polling place voting and Internet voting –see Fig. 1.

Polling place voting. In a polling place, both the voting clients (voting machines) and the physical environment are supervised by authorized entities. Depending on the type of polling place (precinct or kiosk [6]), validation may be either physical (e.g. by election officials) or electronic (with some kind of digital identification). Casting and tallying are electronic: the voting clients may be Direct Recording Electronic devices[2] (DRE's) or they may send their tallies electronically to a central site (e.g. by using a "secure" Internet connection, a dedicated line or even an ATM[3] network [28]).

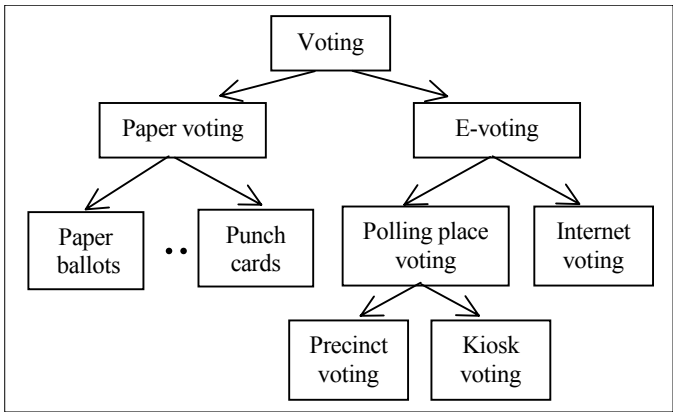

Figure 1. Different types of voting

[2] With such devices voters make their choices on a computer. Votes are locally tabulated and internally stored on a removable cartridge and/or hard drives.

[3] ATM networks have several highly desirable security features (privacy, well-equipped tamper-resistant terminals, national distribution etc). However there are reservations about their appropriateness for voting [32].

Internet voting. The vote is cast over the Internet and the voting client is unsupervised during voting (the voting client may be at home, at work, in a library, etc). Registration may be either physical (at the elections office) or electronic (with some form of digital identification). Validation, casting and tallying are electronic.

I-voting requires a much greater level of security than e-commerce. While checking the eligibility of voters, and that no voter casts more than one vote, is no more difficult than meeting the security requirements of an e-commerce application, *ensuring this* and meeting other requirements such as privacy, a universally verifiable audit trail and uncoercibility, has been difficult to achieve in a practical and affordable way.

In this paper we assess e-voting from various security and practicality aspects, analyse security risks and discuss methods to minimize them. We also discuss cryptographic models and protocols that have been proposed to establish security in large-scale I-voting protocols.

2. AN ASSESSMENT OF E-VOTING

To design an e-voting system that can be used for large-scale elections, it is important to identify a set of publicly acceptable and technologically neutral criteria. A system should be [14, 28, 45]:

- **Secure**[4]. That is,
  - *Democratic.* Only eligible voters can cast votes, and no voter can cast more than one vote.
  - *Accurate.* No vote can be altered, duplicated or eliminated without being detected.
  - *Private.* All votes remain secret while the voting takes place, and each individual vote cannot be linked to the voter who cast it. For uncoercibility, no voter should be able to prove the value of his/her vote to another party.
  - *Universally verifiable.* Any observer can be convinced that the election is accurate and that the published tally is correctly computed from votes that were correctly cast[5].

[4] The cryptographic security of electronic elections is also discussed in Section 3.

[5] *Atomic* verifiability is a weaker version, in which voters can only check their own votes and correct mistakes without sacrificing privacy. Atomic verifiability is useful in small-scale elections, where the cost of achieving universal verifiability outweighs its benefit.

  - *Robust.* All security requirements are fully satisfied, despite failure and/or malicious behaviour by any (reasonably sized) coalition of parties (voters, authorities, outsiders).
- **Practical.** That is, convenient, compatible with a variety of standard platforms and technologies, and accessible to the disabled. It should support a variety of ballot formats, its performance not drastically affected by the size of the election, and be tested extensively so that officials and the public have confidence in it.

2.1 Advantages

E-voting. Traditional voting systems are not perfect. In the US 2000 elections, a large number of residual votes (under votes, spoiled votes, uncounted votes, etc) were cast [7]. E-voting promises to ameliorate this error rate substantially. It also promises to improve accessibility for disabled voters. Furthermore, election results will be calculated quickly and efficiently, with less chance of human error, and long-term costs will be reduced by eliminating the expense of printing ballots.

I-voting. Uniform Internet access will soon be a fact of life for most developed countries. I-voting is very likely to increase voter convenience and therefore the potential voter turnout. Computers and equipment in public facilities can be made available to the voting public during an election period. I-voting could also play a very important role in small-scale elections.

2.2 Disadvantages

While current paper-based voting systems carry a potential for small-scale vote fraud, the potential of fraud with e-voting is considerable because of automation and network connectivity [6, 11, 28, 44].

E-voting. E-data is likely to be more easily altered or destroyed than physical ballots. In addition, all kinds of e-voting systems are susceptible to a certain extent to *insider attacks* and *Denial of Service* (DOS) attacks.

It is widely known that current e-voting systems have poor audit trails. Even worse, although there are strong cryptographic algorithms we do not have systems (e.g. platforms, operational systems) with adequate security into which the cryptography can be embedded [43].

I-voting. This type of voting will only become democratically acceptable when most eligible voters have easy access to the Internet. I-voting systems

may also introduce high costs in terms of buying and up-keeping voting servers, standardized databases and routing systems. From a security point of view, I-voting is more susceptible to coercion attacks. Voters may also be required to secure their own machines before they vote, to guarantee accuracy for the election results. Testing and certification of I-voting systems may be difficult, as such systems will likely rely on third-party (secret-source) components, such as operating systems and browsers.

I-voting is more vulnerable to attacks than polling place voting:

- *At the voting client.* Worm-like viruses or Trojan horses may alter the vote before any encryption or authentication is applied to the data. An attacker may (remotely) exploit security holes at the operating system or at the web browser level [44].
- *At the communication level.* During a spoofing attack, an attacker could feed a voter with a seemingly legitimate web page. This may be enough to change the voter's vote. Communication may also be threatened by other network-based attacks (e.g. TCP SYN spoofing, IP fragmentation, etc).
- *At the election server.* Attacks at this level are similar to attacks at the voting client. Denial of Service (DOS) attacks are also possible. The *bottleneck* problem is similar to a DOS attack except that the jam is caused by an overwhelming number of legitimate contacts occurring simultaneously.

2.3 Security Precautions

There are several issues, both technical and policy related, that must be resolved before e-voting is publicly acceptable. Strong cryptographic methods must be employed to establish auditability and thus public confidence in e-voting systems, and voters need to be educated regarding the very nature of cryptographic assurances. Observe that if the voting clients and the physical environment are carefully supervised, such as with polling place voting, then e-voting may be feasible [6, 11, 28] even with an Internet connection[6] between clients and election servers. However for large-scale I-voting, additional precautions should be taken.

I-voting will become fully electronic (from registration to tallying) only when a secure and uniform Public Key Infrastructure for digital signatures becomes available. Accuracy and privacy over the Internet should be protected with strong digital signatures and encryption techniques. Browsers

[6] With tools such as *encrypting firewalls* and VPN (Virtual Private Networks) technologies, secure and authenticated channels can be built over the Internet.

that allow both the encryption and digital signing at the browser level should be designed. Furthermore, technologies such as Secure Socket Layer (SSL) and digital certificates should be adopted to deal with spoofing attacks.

Strong recount and auditing procedures, anti-virus systems at the host side, firewalls and Intrusion Detection Systems (IDS) at the server side should be employed. Furthermore, the use of redundancy and failover procedures (e.g. power backup systems) in election servers, as well as in communication traffic (e.g. high bandwidth connections), and strong analysis techniques such as thorough testing and high-assurance methods should be supported.

Finally, a robust security policy must be carefully designed to deal with all possible attacks and threats. New laws need to be enacted to protect the right to cast a secret vote and to criminalize behaviours such as coercion of the voter, hacking voting systems or individual votes, jamming a voting system or preventing access to the system, etc.

3. CRYPTOGRAPHIC MODELS AND PROTOCOLS

Currently four election models are used: the mix-net model [10], the blind signatures model [23], the Benaloh's model [3], and the homomorphic encryption model [13]. We briefly describe these.

The mix-net model. Chaum [10] was the first to introduce the concept of a *mix-net*, which is a cryptographic alternative to an anonymous channel. A mix net is composed of several linked servers called *mixes*. Each mix takes a batch of messages (e.g. encrypted votes), randomises it and then outputs a batch of permuted messages such that the input and output messages are unlinkable. In the original proposal, a vote is first encrypted with the public key of each mix (in reverse order). It is then decrypted, shuffled and forwarded to the next mix. This type of mix-net is referred to as a *decryption net*. Another type is the *re-encryption net* [29], in which all votes are encrypted with the public key of the first mix, and then randomised re-encryption takes place at each layer in a verifiable way.

A useful property of mix-nets, especially in large-scale elections, is their universal verifiability. Mix-nets are also quite efficient (provided there are not too many mixes). Several methods to improve mix-nets in both terms of correctness and efficiency have been proposed in the literature (e.g. [30, 37]) No election system based on mixes has been implemented so far.

The blind signatures model. The concept of blind signatures[7] was introduced by Chaum [9] as a method to digitally authenticate a message without knowing the contents of the message. A distinguishing feature of blind signatures is their unlinkability: the signer cannot derive the correspondence between the signing process and the signature, which is later made public. This method, originally conceived for e-cash applications, was used by Fujioka et al [23] to solve the problem of validating votes without sacrificing privacy: each voter encrypts his/her vote and then gets the encryption blindly signed by a *validator*. The voter un-blinds the signature and sends the encryption and the signature to a voting authority (this could be the validator) via an *anonymous channel* (Section 3.1), for privacy. At the end of the voting period the authority posts all encrypted votes and their blind signatures on a *bulletin board* (Section 3.1). Each voter checks that his/her encrypted vote is on the board and then sends the decryption key to the authority, also anonymously. The authority decrypts the votes and posts the tally on the board.

Several election schemes based on blind signatures have been proposed (e.g. [38, 40]). There are also several systems that have been piloted in small-scale elections[8]. An advantage of blind signature election schemes is that their communication and computation overhead is fairly small even when the number of voters is large. Furthermore, these schemes can easily be managed and realize elections with multiple candidates. However, they only offer *atomic verifiability*[5] and require that every eligible voter should not abstain after the registration phase, or else a corrupted validator can add extra votes on behalf of abstaining voters [14]. This is an impractical assumption. To get robustness, the power of the validator can be distributed by using *threshold cryptography* [17]. An implementation is given in [19].

Benaloh's model. This model 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 by Benaloh [3] 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.

[7] Blind signatures are the 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.

[8] The SENSUS system [14] was the first to be implemented. The Davenport et al system [16] was used to conduct student governmental elections. The EVOX system [25] was used at MIT for undergraduate association elections.

At the end of the voting period each authority adds all the received shares to get a share of the sum of the tally. Finally the authorities combine their shares to get the tally. For robustness, a (t,n) homomorphic threshold scheme is used: then only t authorities need to combine their (true) shares. Results are universally verifiable.

Schemes of this type (e.g. [46]), although structurally quite simple, have a high communication cost: each voter must cast his/her vote over n communication channels.

The homomorphic encryption model. This election model, proposed by Cramer et al [13], uses the special properties of homomorphic encryption algorithms to establish universal verifiability in large-scale elections, while retaining privacy for individual votes. With homomorphic encryptions, 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 v_1, v_2: $E(v_1) \otimes E(v_2)$, is the encryption $E(v_1 \oplus v_2)$ of the "sum" of the votes.

In [13], a variant of the ElGamal encryption scheme [20] is used. For this scheme the votes are *+1* or *-1* (*yes*/*no*). We shall briefly describe it. Let $p, q,$ be large primes such that q is a factor of $p-1,$ and let $g \in Z_p$ be an element of order q. The secret encryption key is $x \in Z_q$ and the public encryption key is $y = g^x \bmod p.$ The encryption of a vote $v \in \{-1, +1\}$ is given by: (z,w) where $z = g^k \bmod p,$ and $w = y^k g^v \bmod p,$ where k is a random number in Z_q. (z,w) is decrypted by taking $w / z^x \bmod p,$ and by comparing the result with $g^{-1} \bmod p$ and $g^{+1} \bmod p.$

Each voter encrypts his/her vote with the public encryption key of a voting authority and then publishes the encryption on a bulletin board, together with a proof of correctness: that the encryption contains a valid vote –we shall discuss such proofs in Section 3.1.

At the end of the voting period the authorities "multiply" all the received encryptions to get an encryption of the tally –see Fig. 2. The authorities then jointly decrypt this. The final tally can be checked for accuracy by all parties. So we have universal verifiability. For robustness the encryption procedure is distributed among n authorities using threshold cryptography [17] (Section 3.1).

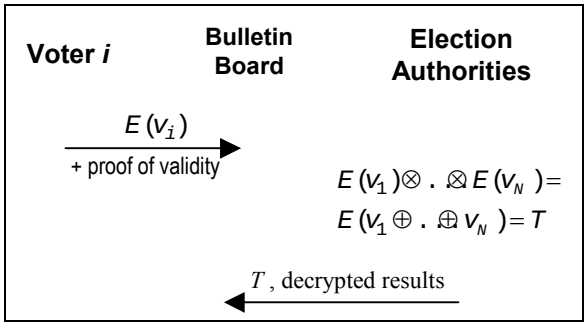

Figure 2. The flow diagram of a basic homomorphic encryption voting system

An election system based on the Cramer et al scheme [13] has been implemented (the VoteHere system [1]) and piloted on a limited basis. A drawback of such schemes is their reduced flexibility, as the votes are essentially limited to yes/no values. In addition, the Cramer et al scheme which uses ElGamal encryption has a relatively high computational complexity, if the number of candidates is large. Indeed, since there is no known trapdoor for the discrete logarithm, the only way to get the decrypted tally T from the decryption $g^T = w/z^x \bmod p$, is by exhaustive search. If ℓ is the number of voters and r the number of candidates, the complexity (number of multiplications) of an exhaustive search is exponential in the number of candidates $(\Omega(\ell^{(r-1)/2}))$

Alternative homomorphic encryption voting schemes have been proposed for which the computational complexity is either *linear* [2], or even *logarithmic* [15]. These schemes are based on the Pallier cryptosystem [39].

3.1 High-Level Primitives

Bulletin boards. These are public broadcast channels that enable voters to communicate with the voting authority(ies) in public. By using digital signatures, the communication is authenticated. A practical implementation of a bulletin board was proposed in the Rampart toolkit project [41]. Public key verification can be integrated into a web browser environment by using an established Public Key Infrastructure.

Anonymous channels. These assure the anonymity of voters. Besides mix-nets, which we discussed earlier, proxy-based systems such as the Anonymizer [12] and the LPWA system [33] have been proposed. A different approach which combines several characteristics of both mix-nets and proxy-based systems is the CROWDS system [42].

Threshold cryptography. Threshold cryptosystems [17] distribute the functionality of cryptographic protocols to establish robustness. In the election paradigm, the tallying process can be shared among *n* voting authorities by using a (t,n)threshold public-key encryption system. In this case there is only one public encryption key, while each of the *n* authorities has a share of the private decryption key. Each voter posts his/her vote encrypted with the public key of the authorities. The final tally is decrypted by the voting authorities jointly. Privacy of the votes and accuracy of the tally are assured provided at least a threshold of *t* authorities are not faulty (or corrupted). Threshold cryptosystems can be further enhanced to deal with dynamic attacks by using *proactive* mechanisms [26] and *strong forward security* [5].

Zero-knowledge proofs. These are prover-verifier interactive protocols, in which a Prover proves to a Verifier the correctness of a statement in such a way that the Verifier learns nothing from the Prover that he could not learn by himself, apart from the fact that the statement is correct [24]. Zero-knowledge proofs have been used extensively in e-voting schemes. For example, to prove correctness of permutations in mix-nets (e.g. [27]), to prove the validity of encrypted votes in homomorphic elections (e.g. [13]), to prove correctness of encryptions in uncoercible protocols [34], and to prove correctness of blind signatures [45]. Interactive zero-knowledge proofs are *non-transferable*. However, it is possible to transform such proofs into non-interactive proofs that *are* transferable (universally verifiable), by using the Fiat-Shamir heuristic [22].

3.2 Uncoercibility

The notions of receipt-freeness and uncoercibility were introduced to deal with vote-selling and coercion in e-voting systems [4]. These notions are similar in many respects, however there are subtle differences. With receipt-freeness the voter is the adversary: the voter should not be able to convince a third party of the value of the vote, even if the voter wants to (e.g. for reward). With uncoercibility, the adversary is a coercer: the coercer should not be able to extract the value of the vote from the voter, even if the voter is forced to (e.g. threatened). In fact receipt-freeness is stronger than uncoercibility, in the sense that there are e-systems that are uncoercible but not receipt-free (e.g. *deniable encryptions* [8]). This is because, although a voter can succeed in fooling a coercer (uncoercibility), the voter is also able to sell the vote by pre-committing to the random choices made during its encryption [27]. For simplicity, we shall assume that uncoercibility extends

to receipt-freeness. In particular, that voters can also be self-coercers, i.e. information sellers.

Most of the solutions for uncoercibility presented so far in the literature involve two basic premises: the existence of *voting booths* (e.g. [4, 38]) and the existence of *untappable channels* (e.g. [27]). However solutions based on these premises affect the mobility of the system and can be quite cumbersome to implement, particularly with large-scale I-voting [34].

To avoid the use of untappable channels the voting scheme in [34] uses a probabilistic homomorphic encryption, with randomness chosen jointly by the voter and a tamper-resistant token. That is, the voter first encrypts his/her vote and then the token randomises the encryption without affecting the encrypted vote –see Fig. 3. The voter must be convinced that the token has not altered the vote during its randomisation. For this purpose a zero-knowledge proof is used: the token proves correctness to the voter in a non-transferable way (the proof must be non-transferable to prevent vote selling) [34]. Finally the token and the voter jointly prove (in zero-knowledge) that the encryption is indeed an encryption of a valid vote [34].

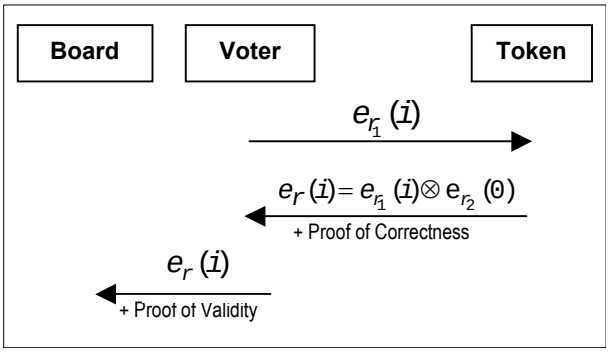

Figure 3. An uncoercible election based on tokens

Even in a vote-selling scenario, where the voter may conspire with a coercer, they will not succeed without the randomness of the token. Observe that in schemes with tamper-resistant tokens (e.g. smartcards), the tokens should incorporate strong identification mechanisms (e.g. biometric technologies).

A similar approach is used in [2], only this time the randomness for the encrypted vote is jointly chosen by the voter and *self-scrambling anonymizers*. These are trusted external entities. As previously, the anonymizers must prove correctness of their encryption in a non-transferable way. In this case a *designated-verifier* proof [31] is used. However, this approach (as well as the one in [27]) requires an untappable channel between the voter and the anonymizers.

I-voting will never gain social acceptance if the voters can construct a receipt for their vote. Policy makers and security experts often neglect uncoercibility, the main argument being that if voters can use a computer to vote via the Internet, then there is no way to prevent a coercer from watching them while they vote. The goal of I-voting protocols however should not be to prevent such attacks, but to prevent a voter from getting, or being able to construct, a receipt. In a *massive coercion* attack such receipts could easily be sent via the Internet to a coercer.

4. CONCLUSION

Due to our increased reliance on the Internet, it is inevitable that ultimately e-voting, and especially I-voting will replace traditional voting. However this will only happen when security issues such as privacy, voter identification and uncoercibility are first addressed.

In the cryptographic literature on e-voting only few protocols offer provable security. Furthermore, the demands placed on voters are usually impractical for large-scale environments. There is an urgent need for more research on secure and efficient cryptographic techniques to support electronic elections.

A well-designed e-voting system should produce an audit trail that is even stronger than that of conventional systems (including paper-based systems). Future of e-voting systems will exploit current technologies and tools including *smartcards*, *biometrics* (e.g. voice, fingerprint, retinal recognition –for identification), as well as *mobile* voting clients (e.g. hand-held organizers, cell phones, etc). Research is needed to determine to what extent such technologies are viable for e-voting.

REFERENCES

[1] Adler, J., Dai, W., Green, R., and Neff, A. “Computational Details of the VoteHere Homomorphic Election System”. November 2000, http://www.votehere.net/ada_compliant

[2] Baudron, O., Fouque, P., Pointcheval, D., Poupard, G., and Stern, J. “Practical Multi-Candidate Election System”. In *20th ACM Symposium on Principles of Distributed Computing*, ACM, pp. 274-283, 2001.

[3] Benaloh, J. “Verifiable Secret-Ballot Elections”. PhD Thesis, Yale University, 1987.

[4] Benaloh, J., and Tuinstra, D. “Receipt-Free Secret-Ballot Elections”. In *26th Annual ACM Symposium on Theory of Computing*, ACM, pp. 544-553, 1994.

[5] Burmester, M., Chrissikopoulos, V., Kotzanikolaou, P., and Magkos, E. “Strong Forward Security”. In *IFIP-SEC '01*, Kluwer Academic Publishers, pp. 109-119, 2001.

[6] California Internet Voting Task Force. *A Report on the Feasibility of Internet Voting*, Jan 2000. http://www.ss.ca.gov/executive/ivote/

[7] CALTEC/MIT. *Voting Technology Project*, 2001. http://www.vote.caltech.edu/reports/index.html

[8] Canetti, R., Dwork, C., Naor, M., and Ostrovsky, R. "Deniable Encryption". In *CRYPTO '97*, LNCS 1294, Springer-Verlag, pp. 90-104, 1997.

[9] Chaum, D. "Blind Signatures for Untraceable Payments". In *CRYPTO '82*, Plenum Press, pp. 199-203, 1982.

[10] Chaum, D. "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms". In *Communications of the ACM*, 24(2), pp. 84-88, 1981.

[11] Coleman, S. "Elections in the 21st Century: From Paper Ballot to E-Voting". Report by the Independent Commission on Alternative Voting Methods, London, Electoral Reform Society, February 2002.

[12] Community ConneXion, Inc., http://www.anonymizer.com

[13] Cramer, R., Gennaro, R., and Schoenmakers, B. "A Secure and Optimally Efficient Multi-Authority Election Scheme". In *EUROCRYPT '97*, LNCS 1233, Springer-Verlag, pp. 103-118, 1997.

[14] Cranor, L., and Cytron, R. "Sensus: A Security-Conscious Electronic Polling System for the Internet". In *Hawaii International Conference on System Sciences*, Wailea, Hawaii, 1997.

[15] Damgard, I., and Juric, M. "A Generalization, a Simplification and Some Applications of Pallier's Probabilistic Public-Key System". In *Public Key Cryptography '01*, LNCS 1992, Springer-Verlag, pp. 119-136, 2001.

[16] Davenport, B., Newberger, A., and Woodard, J. "Creating a Secure Digital Voting Protocol for Campus Elections". Princeton University, 1996. http://www.princeton.edu/

[17] Desmedt, Y. "Threshold Cryptography". In *European Transactions on Telecommunications*, 5(4), pp. 449-457, 1994.

[18] DTLR News Release. "May Elections to Trial Online Voting", 2002. http://www.press.dtlr.gov.uk/pns/DisplayPN.cgi?pi_id=2002_0033

[19] Durette, B. W. "Multiple Administrators for Electronic Voting". Bachelor's Thesis, Massachusetts Institute of Technology, May 1999.

[20] ElGamal, T. "A Public-key Cryptosystem and a Signature Scheme Based on Discrete Logarithms". In *IEEE Transactions on Information Theory*, 31(4), pp. 469-472, 1985.

[21] Federal Voting Assistance Program. *Voting Over the Internet Project*. www.fvap.ncr.gov/voireport.pdf.

[22] Fiat, A., and Shamir, A. "How to Prove yourself: Practical Solutions to Identification and Signature Problems". In *CRYPTO '86*, LNCS 263, Springer-Verlag, pp. 186-194, 1987.

[23] Fujioka, A., Okamoto, T., and Ohta, K. "A Practical Secret Voting Scheme for Large Scale Elections". In *AUSCRYPT '92*, LNCS 718, Springer-Verlag, pp. 244-251, 1993.

[24] Goldwasser, S., Micali S., and Rackoff, C. "The Knowledge Complexity of Interactive Proof Systems". In *SIAM Journal on Computing*, 18(1), pp. 186-208, 1989.

[25] Herschberg, M. "Secure Electronic Voting Using the World Wide Web". Master's Thesis, MIT, June 1997. http://theory.lcs.mit.edu/~cis/theses/herschberg-masters.pdf

[26] Herzberg, A., Jakobsson, M., Jarecki, S., Krawczyk H. and Yung, M. "Proactive Public-key and Signature Schemes". In *4th ACM Annual Conference on Computer and Communications Security*, ACM, pp. 100-110, 1997.

[27] Hirt, M., and Sako, K. "Efficient Receipt-Free Voting Based on Homomorphic Encryption". In *EUROCRYPT 2000*, LNCS 1807, Springer-Verlag, pp 539-556, 2000.

[28] Internet Policy Institute. *Report of the National Workshop on Internet Voting*, March 2001. www.internetpolicy.org.

[29] Jakobsson, M. "Flash Mixing". In *18th ACM Symposium on Principles of Distributed Computing PODC '99*, ACM, pp. 83-89, 1999.

[30] Jakobsson, M., Juels, A., and Rivest, R. L. "Making Mix Nets Robust for Electronic Voting by Randomized Partial Checking", 2002. http://theory.lcs.mit.edu/~rivest

[31] Jakobsson, M., Sako, K., and Impagliazzo, R. "Designated Verifier Proofs and their Applications". In *EUROCRYPT '96*, LNCS 1070, Springer-Verlag, pp. 143-154, 1996.

[32] Jefferson, D. "ATM Network Voting: A non-Starter". The Risks Digest, 21(15), 2000. http://catless.ncl.ac.uk/Risks/21.15.html#subj2

[33] The Lucent Personalized Web Assistant, http://lpwa.com

[34] Magkos, E., Burmester, M., and Chrissikopoulos V. "Receipt-Freeness in Large-scale Elections without Untappable Channels". In *1st IFIP Conference on E-Commerce/E-business/E-Government*, Kluwer Academic Publishers, pp. 683-693, 2001.

[35] May, P. "Alaskan Voters are Pioneers". Mercury News, Jan 25, 2000. http://www.mercurycenter.com/svtech/news/indepth/docs/vote012600.htm

[36] Mohen, J., and Glidden, J. "The Case for Internet Voting". In *Communications of the ACM*, 44(1), 2001.

[37] Neff, A. "A verifiable Secret Shuffle and its Application to E-voting". In *8th ACM conference on Computer and Communications Security*, Philadelphia, 2001. http://www.votehere.net

[38] Okamoto, T. "Receipt-Free Electronic Voting Schemes for Large Scale Elections". In *5th Security Protocols Workshop '97*, LNCS 1163, Springer-Verlag, pp. 125-132, 1997.

[39] Pallier, P. "Public-Key Cryptosystems Based on Discrete Logarithm Residues". In *EUROCRYPT '99*, LNCS 1592, Springer-Verlag, pp. 223-238, 1999.

[40] Petersen, H., Horster, P., and Michels, M. "Blind Multisignature Schemes and their Relevance to Electronic Voting". In 11th Annual Computer Security Applications Conference, IEEE Press, pp. 149-155, 1995.

[41] Reiter, M."The Rampart Toolkit for Building High-Integrity Services". In *Theory and Practice in Distributed Systems*, LNCS 938, Springer-Verlag, pp. 99-110, 1995.

[42] Reiter M., and Rubin A. "Crowds, Anonymity for Web Transactions", DIMACS Technical Report 97-15, April 1997. http://www.research.att.com/projects/crowds/

[43] Rivest, R. "Electronic Voting". In *Financial Cryptography '01*. http://theory.lcs.mit.edu/~rivest/Rivest-ElectronicVoting-ppt.pdf

[44] Rubin, A. "Security Considerations for Remote E-Voting over the Internet", AT&T Labs-Research, June 2001. http://avirubin.com/e-voting.security.html

[45] Schneier, B., *Applied Cryptography - Protocols, Algorithms and Source Code in C*. 2nd Edition, 1996.

[46] Schoenmakers, B. "A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting". In *CRYPTO '99*, LNCS 1666, Springer-Verlag, pp. 148-164, 1999.