Why Public Registration Boards are Required in E-Voting Systems Based on Threshold Blind Signature Protocols

Reto E. Koenig
University of Fribourg
Department of Computer Science
CH-1700 Fribourg, Switzerland
reto.koenig@unifr.ch

Eric Dubuis, Rolf Haenni
Research Institute for Security in the Information Society
Bern University of Applied Sciences
Quellgasse 21, Postfach
CH-2501 Biel, Switzerland
{eric.dubuis,rolf.haenni}@bfh.ch

Abstract: In this paper we demonstrate that e-voting protocols based on threshold blind signatures from multiple authorities allow a coalition of m eligible voters to cast more than m votes. This property presents a serious violation of democracy of the voting process. We analyze the applicability of this violation and provide a generic solution using a public registration board and modified threshold signature schemes.

1 Introduction

Threshold blind signature schemes provide several highly desired properties in cryptography: privacy, security, robustness through redundancy, and avoidance of single points of failure. Many existing threshold blind signature schemes allow independent signature requests from multiple signers, i.e., no communication among the signers has to take place. Exactly this property applied in an e-voting protocol results in a severe violation of the democracy of the voting process. To the best of our knowledge, no protocol design based on threshold blind signature has ever been analyzed regarding this fact.

1.1 Related Work

One of the central technical challenges of designing an e-voting protocol is to simultaneously authenticate voters unequivocally while preserving the anonymity of their votes. One approach is to define the system based on *blind signatures* [Ch82], [Ch83]. The development of such systems is stimulated by the fact that blind signature schemes are simple to understand and implement, flexible to be adjusted to all sorts of settings, and suitable for large-scale elections.

Applying blind signatures to e-voting has first been proposed in [FOO92]. In the suggested protocol, known as FOO92, the voter first encrypts the vote and then requests a blind signature from the voting authority. The blind signature ensures that the content of the vote remains entirely disguised from the voting authority during the authorization process. The encrypted vote, together with the blind signature, is then sent over an anonymous channel to a public board. To open the votes for counting, the voter supplies the encryption key at the end of the voting period, again over an anonymous channel.

One of the major drawbacks of FOO92 is its potential for single points of failure, e.g. it allows the authority to introduce votes for voters who abstain from casting their votes. This and other drawbacks have been addressed in the literature, and hence, many variations of the FOO92 protocol exist today [CC96], [Ok97], [Ba94], [Oh99], [RRN01], [CC97], and [He97].

One aspect which is common for nowadays protocols, is the replication of entities having the property of single point of failure. This replication allows the distribution of power as only a certain number of instances is needed in order to keep the protocol from failing, see for example [Du99], [Ki02], [JZF03], [Ba0], [AFT07], [AW07], and [CCM08].

1.2 Contribution and Overview

In Section 2, we will briefly illustrate the above-mentioned class of protocols. We will demonstrating a generic e-voting protocol based on threshold blind signature, where entities with the property of single point of failure are replicated. We will then analyze the attack on the provided generic scheme where any coalition of m eligible voters can cast more than m votes. Our analysis will provide us with some qualitative and quantitative results.

In Section 3, we present a generic counter-measure against the above-mentioned attack, which is applicable to many existing e-voting schemes of that class. Section 4 gives a security analysis on the revisions made in Section 3, and Section 5 provides our conclusion.

2 E-Voting Protocol using Threshold Blind Signature Scheme

In the following we present a generic template e-voting protocol using threshold blind signatures. This protocol shall serve as the representative for various state-of-the-art e-voting protocols of this class. For the sake of readability, certain aspects of the protocol will be omitted whereas a more detailed view will follow in a proceeding section. Even though other protocols are different in detail, they carry the same threshold properties.

2.1 Threshold Blind Signature

To avoid an entity to become a single point of failure, the entity is replicated N times where it is assumed that at least t replicates work in the sense of the protocol. The threshold t must be greater than 1 and smaller than N. To maximize the robustness and

reliability of the protocol, the choice of t should make it unlikely that t or more replicates of an entity collude, or that $N - t$ replicates fail. For e-voting protocols, $\frac{2}{3}N \leq t \leq \frac{3}{4}N$ is often mentioned as a reasonable choice in multi-party computation [Hi01].

Concrete Examples of Blind Signature Schemes

RSA Based Blind Signature. A *blind signature*, as introduced by Chaum [Ch82], is a form of digital signature, where the signer A is not supposed to see the real message to be signed, nor can the signer trace back the signature to the voter V (i.e., an unknown signature to an unknown message for a known requester). In order to achieve this goal, the data x to be signed is disguised before it is given to the signer using a blinding function. This function usually involves a public key e of the signer and a random number r:

1. $V \to A: x' = \text{blind}_e(x, r)$.

After the signer has signed the blinded data x' with the private key d, the resulting blind signature s' can be transformed to an ordinary digital signature s using a corresponding unblinding function:

2. $A \to V: s' = \text{sign}_d(x')$,
3. $A: s = \text{unblind}(s', r)$.

In the classical RSA scheme, the blinding and unblinding functions consist of multiplying x with the blinding factor r^e and s' with the unblinding factor r^{-1}, respectively.

Schnorr Based Blind Signature. Blind signature schemes based on discrete logarithm were first introduced by Schnorr [Sc90]. In this scheme, the blinding and unblinding function consists of a typical Σ communication scheme:

1. $A \to V: r' = g^k \bmod p$, where $k \in_R Z_q$, $e = g^{-c} \bmod p$, and g, p, q are setup parameters.
2. $V \to A: x' = \varepsilon - \beta$ where $\varepsilon = H(x, r)$, $r = r'^{g^\alpha e^\beta} \bmod p$, and $\alpha, \beta \in_R Z_q$.
3. $A \to V: s'_i = k + x'c \bmod q$.

The resulting blind signature (r, s') for the blinded data x' can be transformed to a signature (r, s) for the data x by applying the corresponding unblinding function $s = s' + \alpha \bmod q$.

Threshold Blind Signatures

A *threshold blind signature* scheme is a combination of a threshold signature scheme with blind signatures such that the data to be signed is not revealed to the signers, nor can the signers trace back the signature to the corresponding voter.

A threshold blind signature scheme can be defined as (t, N)-*threshold signature* scheme. This scheme lets N parties sign some common data, such that the outcome is a valid signature, if at least t parties have contributed to the signature [Bo03]. We can simply realize such a scheme by having each party sign the data x individually and then counting the number of valid signatures, in order to decide if the threshold has been reached. In the following we will use a generic description of blind signatures which can be adapted to any blind signature scheme: If $\mathbf{s} = (s_1, \dots, s_k)$ with $t \leq k \leq N$ denotes the individual signatures and $\mathbf{e} = (e_1, \dots, e_N)$ the public keys of the signers, we denote the corresponding verification function by

$$\text{verify}_{\mathbf{e},t}(\mathbf{s}, x) \in \{true, false\}.$$

2.2 The Protocol

The common e-voting protocol for such systems involves five entity types (voter, administration, the registration authority, the key authority, voting board), and consists of five consecutive phases:

Phase 1: Initialization. The administration initiates the voting process by distributing the empty ballot, and the set of identities of legitimate voters together with their public keys to all necessary entities.

The key authorities create the public-key / secret-key pair for a randomized asymmetric cryptography used during the voting process. In order to dissolve power, the key generation process is done in a distributed way, by using a threshold scheme such as [Ge03] of which its description is beyond the scope of this paper.

Phase 2: Voter Preparation. The voter fills in the empty ballot and randomly encrypts the resulting vote by the public key provided by the key authorities. The resulting message is called the vote. At the end of this phase, the voter is ready to start the registration process.

Phase 3: Registration. The purpose of the registration phase is to authorize legitimate voters to cast their votes. For this, the voter requests a signature for the blinded vote from at least $t \leq N$ registration authorities. The blinding of the vote has to be generated for each replicated registration authority separately, as each replicate uses its own private key for signing. The voter sends the blinded vote to each registration authority where it will be signed and returned if and only if the following two conditions hold: The voter is allowed to vote, and the voter has not previously requested another signature during the voting process. Upon reception, the voter obtains the signatures for the vote by unblinding. If at least t signatures have been received then the voter is ready to start the vote casting process.

Phase 4: Vote Casting. The voter sends the vote together with the authorities' signatures anonymously to the public voting board. The board accepts the vote if and only if there are at least t valid signatures associated to it.

Phase 5: Counting. The last phase of the e-voting protocol involves the opening of the votes to make them available for counting. For this, the key authorities publicly decrypt the cast votes using the secret part of the key pair. The votes are now ready to be counted by everyone.[1]

2.3 Violation of Democracy

We will now demonstrate the attack on democracy by exploiting the properties of the described threshold blind signature protocols.[2]

Definition 1 (Democracy). A system is democratic if authorized voters can vote (*eligibility*), and if eligible voters can vote only once (*uniqueness*).

Let us first analyze Phase 3 in more detail where the voter has to address a signing request to at least t replicates of the registration authority. The voter generates a blinded message for each signer, whereas each blinded message consists of the same vote. Each signer will sign the received message and returns it to the voter. The vote will be declared valid if at least t different and valid signatures for the vote are provided.

This protocol implicitly violates democracy and therefore can be used as an attack on the e-voting system. As only t signatures are needed in order to render a vote valid, $N - t$ signatures can be used for another vote. One voter cannot get more than one valid vote, but a group of voters can. The following example shall demonstrate a possible attack:

- available registration authorities: $N = 4$
- authority signature threshold: $t = 3$

A *fair* voter V_i generates four blinded messages (one blinded message w'_{ji} per authority A_j, $1 \leq j \leq 4$) containing the same vote w_i:

	A_1	A_2	A_3	A_4
V_i	w'_{1i}	w'_{2i}	w'_{3i}	w'_{4i}

Each authority signs the blinded message and returns the signature s_{ji}' to the voter. To cast the vote w_i, the voter sends it together with three out of four unblinded signatures s_{ji} anonymously to the voting board. The voter discards the remaining signature.

[1] This phase can be adapted in manifold ways, such as re-encryption to gain receipt freeness or homomorphic counting instead of individual decryption. Since these adoptions distract from the intended focus of this paper and, hence, will not be followed any further.

[2] Many to our colleague Emmanuel Benoist for pointing this out.

A *malicious voter group* consisting of three colluding voters V_k, V_l, V_m, where $k, l, m \in \{1, \dots, N\}$ and $k \neq l \neq m$ can generate an additional vote w_x resulting in four independent votes:

	A_1	A_2	A_3	A_4
V_k	w'_{1k}	w'_{2k}	w'_{3k}	w'_{4x}
V_l	w'_{1l}	w'_{2l}	w'_{3x}	w'_{4l}
V_m	w'_{1m}	w'_{2x}	w'_{3m}	w'_{4m}

The following holds true:

- w_k is rendered valid by the signatures s_{1k}, s_{2k}, s_{3k} of authorities A_1, A_2, and A_3;
- w_l is rendered valid by the signatures s_{1l}, s_{2l}, s_{4l} of authorities A_1, A_2, and A_4;
- w_m is rendered valid by the signatures s_{1m}, s_{3m}, s_{4m} of authorities A_1, A_3, and A_4; and
- w_x is rendered valid by the signatures s_{2x}, s_{3x}, s_{4x} of authorities A_2, A_3, and A_4.

This is possible as the different registration authorities operate independently from each other and, hence, no synchronization takes place amongst them. Even though the attack is not possible on an exponential scale, it is still significant. The quantitative impact of the attack is proportional to the number of colluding voters.

Due to the nature of threshold there always exists a subset of size $N - t$ authorities not needed in order to get sufficient signatures for a valid vote. Let V_c be the size of a malicious colluding voter group. Hence, the maximum number of additional votes v_+ that can be rendered valid by the malicious voter group, is:

$$v_+ = \left\lfloor \frac{N - t}{t} V_c \right\rfloor$$

For the threshold values N, t such that $\frac{2}{3}N \leq t \leq \frac{3}{4}N$ (see Section 2.1), v_+ is in the range of:

$$\frac{V_c}{3} \leq v_+ \leq \frac{V_c}{2}$$

The violation of democracy shown above is present in all protocols based on threshold blind signature where the blinding procedure results in a different message for every individual signer. Therefore, a common registration board must be used as knowledge base for synchronization amongst the registration authorities.

3 E-Voting Protocol Using a Public Registration Board

A public board is a broadcast channel with memory. Data can be broadcast by anyone. By using a guard,[3] the accepted data can be restricted to authorized participants only. Once published, the data can be read by everyone but cannot be altered anymore. The concept of the public board has been introduced by Benaloh et al. [CF85] and [Be87] and brings verifiability to e-voting schemes.

To prevent the violation of democracy, we introduce a public registration board. We assume that the guard of the board guarantees the following properties:

- Only eligible voters can append an entry (using the public key for identification).
- Each eligible voter can append only once.
- Only eligible registration authorities can append signatures (using the public key for identification).
- Each eligible registration authority can append only one signature per eligible voter entry.

3.1 Revised Voting Protocol

By introducing a public board for the registration process, the voter no longer communicates to the registration authorities. Instead, the blinded hash of the encrypted vote is broadcast to the public registration board. In addition, the registration authorities no longer communicate to the voters. Instead, the registration authorities read the public registration board entries and broadcast the signed voter entries back to it. Therefore, the initial Phase 3 of the generic protocol in Section 2.3 needs the following revision:

Phase 3: Registration. The purpose of the registration phase is to authorize legitimate voters to cast only their votes. For this, the voter requests a signature for the blinded hash of the encrypted vote from at least $t \leq N$ registration authorities. The voter does so by broadcasting the blinded hash of the encrypted vote along with the public voter key to the public registration board. The registration board will accept the message if and only if the following two conditions hold: The voter is allowed to vote, and the voter has not yet requested another signature during the voting process. These conditions also prevent the public registration board from being flooded. Each registration authority will sign one blinded hash per voter and broadcasts this signature back to the public registration board. Then, the voter can obtain the signatures for the hash by unblinding them. If at least t signatures have been added to the public registration board then the voter is ready to start the vote casting process.

The following revision of the Phase 4 prevents the board from being flooded:

[3] A guard is a predicate on a candidate entry and on the board's state. The predicate must evaluate to true for the entry being added to the board. If the predicate evaluates to true then we call the candidate entry to be *valid*, and it is added. Otherwise, if the predicate evaluates to false then the candidate entry is discarded.

Phase 4: Vote Casting. The voter sends the encrypted vote, the vote hash, and the authorities' signatures anonymously to the voting board. The board accepts the vote if and only if there are at least t valid signatures associated to the vote hash.

3.2 Public Registration Board Collective

The public registration board presented at the beginning of Section 3 may suffer from some catastrophic failure that prohibits it from fulfilling its duty. It may no longer be able to service its regular clients, or it may be victim of a denial of service attack, with the same effect that prevents regular clients to communicate successfully with the board.

In [HL09], a scheme for a collective of public boards is presented being based on N *peers* of identical public boards. As long as a threshold set of t out of N public boards function correctly, the integrity of the entries on the boards can be guaranteed by the collective. Each peer accepts and stores the same information as outlined in the beginning of Section 3. In order to write information onto the board, voters and authorities send their messages to one peer of their choice. The peer in turn will then form a threshold set t of peers to guarantee (in terms of a receipt) the publishing of the message.

There are two versions of the collective: The first one having a *synchronized history*, all peers maintain the same order among the accepted messages. The second version supports the concept of an *unsynchronized history* which satisfies our requirements. To read all messages previously published, however, clients need to consult $N - t + 1$ peers.

3.3 Revised Threshold Blind Signature Schemes

The revision of Phase 3 requires a property which is not present in the normal schemes as defined in Section 2.1. It requires that each signing party (registration authority) is given the *same* blinded data x' such that the very same data is signed by all parties. Therefore, a new assumption has to be introduced: The blinding and the unblinding function,

$$x' = \text{blind}_{\mathbf{e}}(x, r),$$
$$\mathbf{s} = \text{unblind}_{\mathbf{e}}(\mathbf{s}', r),$$

depend on the public keys $\mathbf{e}$ of all signing parties.

RSA Based Threshold Blind Signature

To realize such a scheme based on RSA, we use a common blinding factor $r^{e_1 \cdots e_N}$ and individual unblinding factors $r^{-(e_1 \cdots e_{i-1} e_{i+1} \cdots e_N)}$ to obtain classical RSA signatures $s_i = x^{d_i}$. Note that if m_i denotes the modulus for the public key e_i, then $m_1 \cdots m_N$ will

be an appropriate modulus for $r^{e_1 \cdots e_N}$. The individual modulus m_i can then be used by the i-th signer to sign the common blinded data x' and by the recipient of the blind signatures to do the unblinding.

Schnorr Based Threshold Blind Signature

To realize such a scheme based on Schnorr, we can use the threshold blind signature scheme introduced by Jinho Kim et al. [KKL02]. The original scheme describes the following message flow for the message signing procedure:[4]

1. $V \rightarrow A_i: \omega_i = \prod_{k=1,k\neq i}^{t} \frac{k}{k-i}$
2. $A_i \rightarrow V: e_i = g^{t_i} h^{u_i} \bmod p$ where $t, u \in_R Z_q$ and g, h, p setup parameters
3. $V \rightarrow A_i: x' = \varepsilon - \delta$ where $\varepsilon = H(x, \hat{e})$, $\hat{e} = e g^{\beta} h^{\gamma} y^{\delta} \bmod p$, $e = \prod_{i=1}^{t} e_i$ and $\beta, \gamma, \delta \in_R Z_q$
4. $A_i \rightarrow V: (R_i, S_i)$ where $R_i = t_i - x' r_i \omega_i \bmod q$, $S_i = u_i - x' s_i \omega_i \bmod q$ with r_i, s_i public key of A_i.

However, even this protocol is still prone to the attack, if used without public registration board, and hence the message flow has to be adapted[5] in order to gain democracy using this protocol:

1. $A_i \Rightarrow board: (e_i, id_V)$ for each eligible voter
2. $V \Rightarrow board: (\omega_i, x', id_{A_i})$ for at least t authorities
3. $A_i \Rightarrow board: (R_i, S_i, id_V)$

Each authority calculates the commitment for each eligible voter in advance and places them on the public board next to the voter id. Any voter can then start the blinding and signature process. The voter is allowed to present one and only one blinded data x' on the public registration board.

4 Security Analysis

The question whether the attack presented in Section 2 is still possible, can be denied rather intuitively. Every voter can send only one message (a commitment to the voters vote) to be signed to the public registration board. Every registration authority provably signs the very same message per voter. Therefore, no threshold attack can be executed any more, and democracy is established under such circumstances.

We now have to prove that the revision does not introduces other security issues for the whole e-voting process.

[4] For the sake of readability, the protocol steps presented are stripped down to the signing process. Please refer to the original paper for a more detailed view of the complete protocol.
[5] ⇒ indicates that each message has to be signed by the sender.

Anonymity: The introduction of the public registration board seems to raise an anonymity issue. But this is not the case as the only information that can be learned through the public registration board is the fact that some voter initiated the e-voting process. But nothing can be learned of the vote itself nor its containing data. Furthermore, it is not possible to trace the voter's vote. This results in the inability to know if a voter really finished the e-voting process by casting the vote.

Democracy: In the revised protocol the registration authorities do not sign the blinded encrypted vote any more but its blinded hash-value. The consequence of this refinement comes into operation only during the vote casting process. As a blindly signed message is a valid message, the public voting board accepts it as being authorized. As a consequence of this, the voting board could be tainted by receiving signed messages from the public registration board. These votes, however, would be invalid and would not affect the final tally. On the other hand, this is a serious issue, and it can be addressed by letting the voting board to accept only the following tuple: Encrypted vote, and the signatures of the hash-value of the encrypted vote.

Persistence: The use of the public registration board implies the permanent storage of the signatures. Hence, the voter does not need to keep them anymore. The only information the voter needs to keep at a safe place is the blinding factor.

Privacy: If all involved registration authorities collude against a single voter, the voter's privacy is still warranted by the blinding factor the voter has chosen, since finding the correct blinding factor is considered hard [Be01], [KKL02].

5 Conclusion

In this paper we demonstrated that any blind signature protocol with threshold bears an intrinsic weakness on democracy and unforgeability of votes, if no public registration board is in use. The public registration board acts as a point of synchronization, where each voter has to give the commitment to only one single blinded message, ready to be signed by all signing authorities. Therefore, a public board not only serves as a means for individual and universal verifiability. The public registration board is an imperative instrument of communication to multiple authorities within a threshold system. Furthermore, we showed that the special requirement, the provably signing the same data, by multiple signers within the threshold signature scheme based on RSA or on Schnorr can be achieved by a refinement of the blinding / unblinding process.

References

[AFT07] R. Anane, R. Freeland, and G. Theodoropoulos. E-voting requirements and implementation. In CEC'07, 9th IEEE Conference on E-Commerce Technology, pages 382–392, Tokyo, Japan, 2007.

[AW07] A. Aeby and M. Wiget. On-Line Meinungsumfragen. Diploma thesis, Bern University of Applied Sciences, Biel, Switzerland, 2007.

[Ba94] A. Baraani-Dastjerdi, J. Pieprzyk, and R. Safavi-Naini. A practical electronic voting protocol using threshold schemes. Technical report, University of Wollongong, Department of Computer Science, Wollongong, Australia, 1994.

[Be87] Josh Daniel Cohen Benaloh. Verifiable secret-ballot elections. PhD thesis, New Haven, CT, USA, 1987.

[Ba05] F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi, and A. Vaccarelli. SEAS, a secure e-voting protocol: Design and implementation. Computers & Security, 24(8):642–652, 2005.

[Be01] M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko. The one-more-RSA-inversion problems and the security of Chaum's blind signature scheme. 2001.

[Bo03] A. Boldyreva. Threshold signatures, multi-signatures and blind signatures based on the Gap-Diffie-Hellman-group signature scheme. In Y. Desmedt, editor, PKC'03, 6th International Workshop on Theory and Practice in Public Key Cryptography, LNCS 2567, pages 31–46, Miami, USA, 2003.

[CC96] L. F. Cranor and R. K. Cytron. Design and implementation of a practical security-conscious electronic polling system. Technical Report WUCS-96-02, Washington University, 1996.

[CC97] L. F. Cranor and R. K. Cytron. Sensus: A security-conscious electronic polling system for the internet. In HICSS-30, 30th Hawaii International Conference on System Sciences, volume 03, pages 561–570, Maui, USA, 1997.

[CCM08] M. R. Clarkson, S. Chong, and A. C. Myers. Civitas: Toward a secure voting system. In SP'08, 29th IEEE Symposium on Security and Privacy, pages 354–368, Oakland, USA, 2008.

[CF85] Josh D. Cohen and Michael J. Fischer. A robust and verifiable cryptographically secure election scheme. In SFCS '85: Proceedings of the 26th Annual Symposium on Foundations of Computer Science, pages 372–382,Washington, DC, USA, 1985. IEEE Computer Society.

[Ch82] D. Chaum. Blind signatures for untraceable payments. In CRYPTO'82, 2nd International Cryptology Conference, pages 199–203, Santa Barbara, USA, 1982.

[Ch83] D. Chaum. Blind signature system. In CRYPTO'83, 3rd International Cryptology Conference, pages 153–156, Santa Barbara, USA, 1983.

[Du99] B. W. DuRette. Multiple administrators for electronic voting. Bachelor thesis, Massachusetts Institute of Technology, Boston, USA, 1999.

[FOO92] A. Fujioka, T. Okamoto, and K. Ohta. A practical secret voting scheme for large scale elections. In J. Seberry and Y. Zheng, editors, ASIACRYPT'92, Workshop on the Theory and Application of Cryptographic Techniques, LNCS 718, pages 244–251, Gold Coast, Australia, 1992.

[Ge03] Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin. Revisiting the distributed key generation for discrete-log based cryptosystems, 2003.

[He97] M. A. Herschberg. Secure electronic voting using the world wide web. Master's thesis, Massachusetts Institute of Technology, Boston, USA, 1997.

[Hi01] M. Hirt. Multi-Party Computation: Efficient Protocols, General Adversaries, and Voting. PhD thesis, ETH Zürich, Switzerland, 2001.

[HL09] James Heather and David Lundin. The append-only web bulletin board. In Pierpaolo Degano, Joshua Guttman, and Fabio Martinelli, editors, Formal Aspects in Security and Trust, LNCS 5491, pages 242–256, 2009. [JZF03] R. Joaquim, A. Zuquete, and P. Ferreira. REVS – a robust electronic voting system. In IADIS International Conference e-Society 2003, pages 95–103, Lisbon, Portugal, 2003.

[JZF03] R. Joaquim, A. Zuquete, and P. Ferreira. REVS – a robust electronic voting system. In IADIS International Conference e-Society 2003, pages 95–103, Lisbon, Portugal, 2003.

[Ki02] K. Kim. Killer application of PKI to internet voting. In IWAP'02, 2nd International Workshop for Asia Public Key Infrastructures, Taipei, Taiwan, 2002.

[KKL02] J. Kim, K. Kim, and C. Lee. An efficient and provably secure threshold blind signature. In K. Kim, editor, ICISC'01, 4th International Conference on Information Security and Cryptology, LNCS 2288, pages 318–327, Seoul, South Korea, 2002.

[Ok97] T. Okamoto. Receipt-free electronic voting schemes for large scale elections. In B. Christianson, B. Crispo, T. M. A. Lomas, and M. Roe, editors, 5th International Security Protocols Workshop, LNCS 1361, pages 25–35, Paris, France, 1997.

[Oh99] M. Ohkubo, F. Miura, M. Abe, A. Fujioka, and T. Okamoto. An improvement on a practical secret voting scheme. In M. Mambo and Y. Zheng, editors, ISW'99, 2nd International Workshop on Information Security, LNCS 1729, pages 225–234, Kuala Lumpur, Malaysia, 1999.

[RRN01] I. Ray, I. Ray, and N. Narasimhamurthi. An anonymous electronic voting protocol for voting over the internet. In WECWIS'01, 3rd International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems, pages 188–191, San Jose, USA, 2001.

[Sc90] Claus-Peter Schnorr. Efficient identification and signatures for smart cards. In CRYPTO '89: Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology, pages 239–252, London, UK, 1990. Springer-Verlag.