A Generic Approach to Prevent Board Flooding Attacks in Coercion-Resistant Electronic Voting Schemes

Preliminary version

Rolf Haenni

Bern University of Applied Sciences, CH-2501 Biel, Switzerland
E-mail: rolf.haenni@bfh.ch
Phone: +41 32 321 6482 Fax: +41 32 321 6523

Reto E. Koenig

Bern University of Applied Sciences, CH-2501 Biel, Switzerland
E-mail: reto.koenig@bfh.ch
Phone: +41 32 321 6207 Fax: +41 32 321 6523

Abstract

This paper presents a generic approach to prevent board flooding attacks in remote electronic voting schemes providing coercion-resistance. A key property of these schemes is the possibility of casting invalid votes to the public bulletin board, which are indistinguishable from proper votes. Exactly this possibility is crucial for making these schemes coercion-resistant, but it also opens doors for flooding the bulletin board with an enormous amount of invalid votes, eventually spoiling the efficiency of the tallying process. To prevent such attacks, we present a generic enhancement for these schemes, in which we restrict the total amount of votes accepted by the public bulletin board. For this, voters receive a certain amount of posting tickets, each of which allowing its owner to post a single vote to the bulletin board. The list of all posting tickets is published along with the electoral register. Votes with no valid posting ticket are immediately rejected by the bulletin board. The maximum amount of postings accepted

by the bulletin board is thus bounded by the total number of issued posting tickets. This prevents a massive board flooding attack with a very large number of invalid votes and thus guarantees the efficiency of the tallying phase. Except with respect to forced vote abstention, our enhancement preserves all properties of the existing scheme in use. Although coercion by forced vote abstention cannot be ruled out entirely, such attacks are at least not scalable to a considerable portion of the electorate.

1 Introduction

One of the most challenging problems in remote electronic voting is the design of a system that prevents voters from selling their votes or from being coerced. The first scheme that is resistant against both the selling of votes and the coercion of voters has been proposed by Juels, Catalano, and Jakobsson in [1]. To achieve *coercion-resistance* (which implies mere *receipt-freeness*), the so-called "JCJ-scheme" uses an anonymous authentication mechanism to guarantee that the identities of the voters remain hidden during the whole voting and tallying process. The anonymous authentication mechanism requires that during the registration phase each voter receives a *secret credential* over an untappable channel. The knowledge of the secret credential allows the voter to post an encrypted vote anonymously to the public bulletin board, such that its inclusion in the final tally is guaranteed. It is also possible to post invalid votes based on *fake credentials*, but those will be filtered out later during the tallying phase. Since both types of board entries are indistinguishable, it is always possible to lie about the secret credential and to supply an adversary with a fake one. The adversary will then see the posted invalid vote on the public bulletin board, but at this early stage of the scheme, there is no way to tell whether a particular board entry will be included in the final tally or not. This is the principal mechanism that renders the JCJ-scheme coercion-resistant.

The JCJ-scheme is the point of departure of most advanced schemes for remote electronic voting today dealing with coercion-resistance. The scheme as presented in [1] has at least two major problems (further major and minor problems of the JCJ-scheme are discussed in [2, 3]). The first problem is the quadratic running time of the tallying process, where duplicate and invalid votes need to be eliminated. Detecting duplicate votes requires so-called

plaintext equivalence tests [4] for every pair of votes, and detecting invalid votes requires each vote to be checked against the public electoral register, thus making the scheme quite inefficient for large scale elections. The *Civitas system* [5], an implementation of the JCJ-scheme, weakens this problem by breaking up the electoral register into various independent blocks of a given fixed size. Several other improvements based on hash tables were proposed by Smith, Weber, and others [6, 7, 3, 8, 9], but they have been shown to be vulnerable to Pfitzmann's attack against anonymous channels [10, 11]. More recent developments in this direction offer parametrized coercion-resistance based on group signatures [11, 12], anonymity sets [13, 14], fake votes generated by the talliers [15], or similar techniques [16].

1.1 Contribution

In this paper, we address the second problem of the original JCJ-scheme, which results from the aforementioned possibility of posting invalid votes based on fake credentials to the public bulletin board. Exactly this possibility is crucial for making the scheme coercion-resistant, but it also opens doors for flooding the public bulletin board with an enormous amount of invalid votes. As invalid votes are indistinguishable from proper votes from the perspective of the bulletin board, there are no direct counter-measures against such types of attack, i.e., as long as the incoming votes are well-formed and comply with the scheme, the public bulletin board needs to treat them all in the exact same manner. A massive application-level flooding attack of that kind may therefore both jeopardize the availability of the public bulletin board and spoil the efficiency of the tallying process.

The above problem seems to be intrinsic to the chosen approach, but by accepting a slightly weakened, parameterizable degree of coercion-resistance, we can define a generic scheme enhancement for JCJ-based schemes, which solves the board flooding problem. The key idea is to equip the public bulletin board with a stronger filter on what is an acceptable vote. For this, voters receive some *posting tickets* (in addition to the secret credential) during the registration phase. Each posting ticket can be used to post a single (valid or invalid) vote to the bulletin board. Votes with no valid posting ticket are immediately rejected by the bulletin board. The maximum amount of entries on the bulletin board is thus bounded by the total number of issued posting tickets. This prevents massive application-level flooding attacks with a very large number of invalid votes. Although our solution does not generally

prevent denial-of-service attacks (for example on network protocol level), it guarantees the efficiency of the tallying phase.

In a similar recent approach, the maximal amount of board entries is controlled by issuing a limited number of so-called *dummy credentials* to the voters during their registration [17]. The role of the dummy credentials is thus similar to posting tickets, but the generic approach introduced in this paper has at least three important differences and benefits. First, it can be applied to any of the existing JCJ-based schemes, thus offering a generic (not a specific) solution to the board flooding problem. Second, checking the validity of posting tickets is more efficient and involves less parties than checking dummy credentials. Third, coercion-resistance is only weakened with respect to forced vote abstention, but not to other types of coercion.

1.2 Overview

The structure of this paper is as follows. In Section 2, we give an introduction to the original JCJ-scheme and some of its recent derivatives. In Section 3, we introduce the generic enhancement for making JCJ-based schemes resistant against board flooding attacks. We compare this approach with the existing scheme based on dummy credentials. As we will see, both approaches have a number of potential pitfalls. These pitfalls will be discussed in Section 4 and possible solutions will be presented. In Section 5, we conclude the paper.

2 Coercion-Resistant Electronic Voting

In free democratic elections, voters should have the possibility to cast their votes in full privacy and without any external pressure. A prerequisite to achieve this in remote electronic voting is to prevent the system from providing a receipt, which allows voters to prove to somebody else how (or that) they voted. The absence of such voting receipts disallows voters from selling their votes and protects them from being coerced. Many schemes offering *receipt-freeness* are known in the literature [18, 19, 20, 21, 22, 23], but most of them rely on unrealistic physical assumptions.

A more formal and even stronger notion of coercion has been proposed by Jules, Catalano, and Jakobsson in [1]. Their goal is to make remote electronic voting resistant against various forms of coercion. While privacy is defined in terms of an adversary that cannot interact with voters during

the election process, it is assumed that a coercive adversary may interact with voters at any time. Thus an election scheme is called *private*, if the adversary cannot guess somebody's vote (or the fact that there is no vote) better than an adversarial algorithm whose only input is the final tally, and the scheme is called *coercion-resistant*, if the adversary can be deceived into thinking that a coerced voter has behaved as instructed. Clearly, a scheme with this property prevents voters from selling their votes or from being coerced. According to [1], forcing a voter to vote for a particular candidate selection is only one of several types of coercive attacks. The following list describes other coercive attacks applicable to remote electronic voting, which a coercion-resistant system must address.

- In a *randomization attack*, voters are forced to vote for a random selection of candidates. The goal of this attack is to nullify with high probability the choice of the group of voters under attack, for example by selecting them from an area with a well-predictable election outcome. Note that for the success of this attack, the attacker (and perhaps even the voters) does not need to learn the actual candidate selection.

- In a *forced-abstention attack*, voters are forced to abstain from participating in the election, either by not casting a vote at all or by casting an invalid vote. With respect to its goal and effectiveness, this type of attack is closely related to a randomization attack, however much easier to achieve. By simply observing the public bulletin board in a scheme prone to this kind of attack, no direct interaction with the coerced voter is needed.

- In a *simulation attack*, voters are forced to hand over the legitimation to vote, for example by handing out the private voting credentials to the coercer, which can then impersonate (simulate) the coerced voters and hence vote on their behalf.

The JCJ-scheme is the first remote electronic voting scheme that offers full coercion-resistance under minimal assumptions. While many other schemes assume the existence of an untappable channel during the voting phase to offer mere receipt-freeness, an untappable channel is only required during the registration phase of the JCJ-scheme. Since credentials can be re-used in many subsequent voting events, this minimal assumption seems realistic

as credentials can be distributed easily when citizens appear in person at the administration offices to register as new community members.

2.1 Original JCJ-Scheme

In the following paragraphs, we describe each phase of the original JCJ-scheme. All cryptographic building blocks are based on a multiplicative cyclic group G_q of order q, for which the decisional Diffie-Hellman assumption is believed to hold. Apart from standard ElGamal encryption and decryption [24], we also need a threshold cryptosystem [25, 26], plaintext equivalence tests [4], non-interactive zero-knowledge proofs of knowledge [27, 28], verifiable re-encryption mix-nets [19, 29, 30, 31], an anonymous channel [32], and an append-only public bulletin board [33, 34, 35].

For a given referendum or election, a finite set $\mathcal{C} \subseteq G_q$ of available choices is publicly known, and we write $c \in \mathcal{C}$ for the voter's actual choice (a single option or candidate, a set of options or candidates, an ordered set of options or candidates, etc.). A general overview of the scheme is shown in Figure 1.

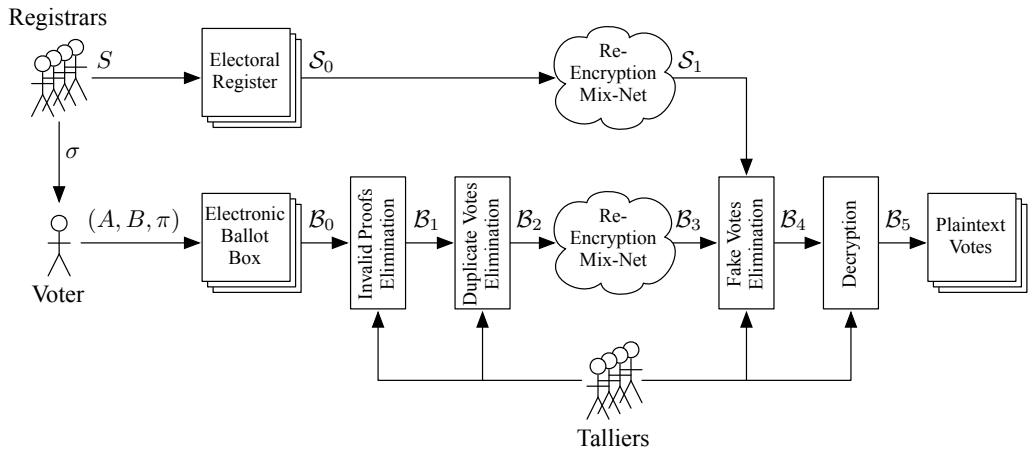

Figure 1: Overview of the original JCJ-scheme: the first filter eliminates votes with invalid proofs, the second filter eliminates duplicate votes, and the third filter eliminates fake votes by checking them against the electoral register.

Registration The *registrars* jointly establish a random credential $\sigma \in G_q$ and deliver it to the voter via an untappable channel. Additionally, they

jointly compute the ElGamal encryption $S = Enc_y(\sigma, r_S)$, where y represents the talliers' common public key and r_S is a secret randomization. Finally, the registrars add S to the voter's entry in the *electoral register*, which resides on the public bulletin board. Assuming a majority of trustworthy registrars, only the voter will know σ and no one will know r_S. At the end of the registration phase, the complete electoral register is digitally signed by the registrars. $\mathcal{S}_0$ denotes the set of all encrypted credentials in the electoral register, and $n = |\mathcal{S}_0|$ is the size of the electorate.

Vote Casting The voter chooses $c \in \mathcal{C}$ from the set of available choices and computes ElGamal encryptions $A = Enc_y(\sigma, r_A)$ and $B = Enc_y(c, r_B)$. To cast the vote, A and B must be accompanied by a conjunctive composition $\pi = \pi_A \wedge \pi_B$ of two non-interactive zero-knowledge proofs,

$$\pi_A = ZKP\{(\sigma, r_A) : A = Enc_y(\sigma, r_A)\},$$
$$\pi_B = ZKP\{(r_B) : \bigvee_{c \in \mathcal{C}} B = Enc_y(c, r_B)\},$$

one to prove knowledge of σ and one to prove $c \in \mathcal{C}$.[1] If the voter desires to fake a vote, σ can be replaced by any other value in G_q, a so-called *fake credential*. The resulting *ballot* (A, B, π) is posted to the *electronic ballot box* $\mathcal{B}_0$, which resides on the public bulletin board. $N = |\mathcal{B}_0|$ denotes the number of ballots in the electronic ballot box at the end of the vote casting phase.

Tallying Five consecutive steps are necessary to detect and eliminate invalid ballots and to derive the election result from the remaining encrypted votes (see Figure 1). The main actors in the tallying phase are the *talliers*, which share the private decryption key x and jointly perform corresponding computations.

1. The proofs π are verified for all ballots $(A, B, \pi) \in \mathcal{B}_0$. Ballots for which the proof does not hold are excluded from further processing. The remaining reduced ballots (A, B) form a new set $\mathcal{B}_1$.

[1] The first proof π_A prevents attackers from casting unauthorized votes by re-encrypting entries from the electoral register (recall that r_S is not known to anyone). Since each authorized vote on the bulletin board will be decrypted during the tallying phase, π_B is needed to prevent coercers from forcing voters to select $c \notin \mathcal{C}$ according to some prescribed pattern, thus obtaining a receipt [36].

2. If two ballots contain the same plaintext credential, one of them is excluded from further processing according to some policy. This is the case if the plaintext equivalence test $PET(A, A')$ returns *true* for two distinct ballots $(A, B) \in \mathcal{B}_1$ and $(A', B') \in \mathcal{B}_1$. The remaining ballots form a new set $\mathcal{B}_2$.

3. The sets $\mathcal{B}_2$ and $\mathcal{S}_0$ are mixed in two separate verifiable re-encryption mix-nets. These mix-nets produce two new sets $\mathcal{B}_3$ and $\mathcal{S}_1$.

4. Ballots not containing a valid credential are excluded from further processing. This is the case for a ballot $(A, B) \in \mathcal{B}_3$, if $PET(A, S) = \mathit{false}$ holds for every $S \in \mathcal{S}_1$. The remaining encrypted votes B form a new set $\mathcal{B}_4$.

5. The encrypted votes $B \in \mathcal{B}_4$ are jointly decrypted. This yields a new set $\mathcal{B}_5$, which contains the plaintext votes ready to be counted.

In general, the complete transition from $\mathcal{B}_0$ to $\mathcal{B}_5$ runs in $\mathcal{O}(N^2 + N \cdot n)$ time.[2] This implies $\mathcal{O}(n^2)$ for $N \leq n$ and $\mathcal{O}(N^2)$ for $N \geq n$. The quadratic growth rate in both cases makes the scheme not only impractical in a large-scale setting, but also vulnerable against massive board flooding attacks (where N may be orders of magnitudes larger than n).

2.2 Linear-Time Schemes

The problem of the inefficient tallying procedure of the original JCJ protocol has been widely discussed and addressed in the recent literature. Various promising protocol improvements with a linear-time tallying procedure have been proposed. In this section, we provide a short summary of these approaches. Some of them include a security parameter β to trade off efficiency against coercion-resistance. Each of them is a possible candidate for the proposed enhancement in Section 3 (except for the first one, which has been broken).

[2] This is the asymptotic running time in terms of number of plaintext equivalence tests. The number of mix servers and the size of the resulting proof π_B (which depends on $|\mathcal{C}|$) are not taken into account. For a more detailed running time analysis, we refer to [14].

Scheme by Smith and Weber [3, 8, 9] Instead of applying PET(A, A') pairwise on all elements of $\mathcal{B}_1$ for removing duplicates, both Smith and Weber suggest computing and decrypting $A^z = Enc_y(\sigma, r_A)^z = Enc_y(\sigma^z, z{\cdot}r_A)$, where $z \in \mathbb{Z}_q$ is a random *blinding value* shared among the talliers. The resulting blinded value σ^z is stored in a hash table for collision detection in linear time. Clearly, if $\sigma^z = \sigma'^z$ holds for another credential σ', then σ and σ' must be the same. Both authors propose using the same procedure for eliminating fake votes. In that case, however, based on the fact that the same exponent z is used across multiple times, the coercer gets an attack strategy to identify whether a vote with known σ makes it into the final tally [5, 10, 11]. Note that this attack does not apply to the above method of removing duplicates.

Scheme by Clark and Hengartner [13, 37] Although this scheme, called SELECTIONS, is based on JCJ, it has a slightly different setting. The public credential S is not an encryption of the voter's credential σ, but an encryption of g^σ, i.e., $S = Enc_y(g^\sigma, r_S)$. For every election, the public credentials are transformed into $T_S = S^\alpha = \mathrm{Enc}_y(\hat{g}^\sigma, r_S{\cdot}\alpha)$, where $\hat{g} = g^\alpha$ is jointly generated and published by the some trustworthy authorities, such that α is not revealed. This mechanism prevents information leakage across elections. When casting a vote, the voter sends a commitment $A = \hat{g}^\sigma$, the encrypted vote $B = Enc_y(c, r_B)$, and a re-encryption of the public credential $C = ReEnc_y(T_S, r_C)$ to the public bulletin board. Additionally, an *anonymity set* $\mathcal{T}$ containing T_S and $\beta - 1$ randomly chosen public credentials different from T_S is selected. Then the voter constructs a NIZKP $\pi = \pi_A \wedge \pi_B \wedge \pi_C$, where

$$\pi_A = ZKP\{(\sigma) : A = \hat{g}^\sigma\}$$

proves knowledge of σ, π_B proves $c \in \mathcal{C}$ (as before), and

$$\pi_C = ZKP\{(r_C) : \bigvee_{T \in \mathcal{T}} C = ReEnc_y(T, r_C)\}$$

proves that C is a re-encryption of one of the β public credentials in the anonymity set $\mathcal{T}$. The ballot (A, B, C, π) is posted to the electronic ballot box. After excluding ballots with an invalid proof, detecting and eliminating duplicate votes is based on the simple fact that votes with the same credential will have the same commitment $A = \hat{g}^\sigma$. In that case, only one vote is kept

for further processing. The remaining ballots (A, B, C) are mixed, where A is treated as an encryption with randomness 0. Finally, the talliers perform a single plaintext equivalence test for each ballot. If $PET(A, C)$ returns *true*, B is decrypted and counted. The complete tallying procedure runs in $\mathcal{O}(\beta N)$ time.

Scheme by Spycher et al. [15] The registration step is conducted according to the original JCJ-scheme. In addition to values A and B, the voter computes $C = Enc_y(i, r_C)$, where i is the index of the voter's entry in the electoral register. In the extended proof $\pi = \pi_A \wedge \pi_B \wedge \pi_C$, π_A and π_B are as in the original scheme and

$$\pi_C = ZKP\{(i, r_C) : C = Enc_y(i, r_C)\}$$

proves knowledge of i. The resulting ballot (A, B, C, π) is posted to the electronic ballot box. After excluding ballots with an invalid proof, the talliers generate a random number (β in the average) of additional fake votes for each index i. After removing duplicate votes as in Smith's and Weber's scheme, the resulting list of ballots (A, B, C) is mixed in a first re-encryption mixnet. Next, the talliers jointly decrypt C into i and establish a new set of ballots (A, B, S) by retrieving S from the electoral register at index i. This set is mixed in a second re-encryption mixnet. Finally, the talliers perform a single plaintext equivalence test for each ballot. If $PET(A, S)$ returns *true*, B is decrypted and counted. The complete tallying procedure runs in $\mathcal{O}(N + \beta n)$ time. In [16], an improved version of this protocol shifts the additional workload resulting from the security parameter β to the setup phase and thus offers an $\mathcal{O}(N)$ time tallying procedure.

Scheme by Schläpfer et al. [14, 38] The registration step is identical to the original JCJ-scheme. Additionally to computing values A and B along with a conjunctive proof $\pi = \pi_A \wedge \pi_B$, a subset $I \subseteq \{1, \ldots, n\}$ of size β is chosen at random and added to the ballot. This is the ballot's anonymity set, which must include the voter's own index i. After excluding ballots with an invalid proof, duplicate votes are removed as in Smith's and Weber's scheme. For every remaining ballot (A, B, I, π), the talliers create β new ballots (A, B, S) by retrieving S from the electoral register at every index $i \in I$. The resulting list of ballots is mixed in re-encryption mix-net. Finally, the talliers perform a single plaintext equivalence test for each ballot. If

$PET(A, S)$ returns *true*, B is decrypted and counted. The complete tallying procedure runs in $\mathcal{O}(\beta N)$ time.

Scheme by Araújo et al. [11, 12, 39] This approach is based on group signatures. At registration, voters obtain their credential, but there are no corresponding public values and therefore no public electoral register. Duplicate votes are identified by the simple fact that respective ballots contain identical values. After mixing, the talliers use their private keys to identify the valid votes. Notably, all information on their validity is included in the ballot, but can only be assessed by a sufficiently large group of talliers. An inherent weakness of this approach is the fact that a majority of colluding registrars could compute valid (but illegitimate) credentials unnoticed. The complete tallying procedure runs in $\mathcal{O}(N)$ time.

3 Preventing Board Flooding Attacks

A common property of all JCJ-based schemes introduced in the previous section is that efficiency of their tallying procedures is determined by N, the total number of ballots sent to the electronic ballot box. Since N has no upper limit, all schemes are prone to application-level board flooding attacks, where an enormous amount of ballots reaches the ballot box, thus spoiling the efficiency of the tallying process. In this section, we describe a generic, linear-time enhancement for any of the JCJ-based schemes introduced above to become resistant against such attacks. This enhancement guarantees a hard upper limit for N, thus ensuring efficient tallying. At the end of this section, we discuss a recent approach [17], which integrates a similar mechanism into the original JCJ-scheme.

3.1 Generic Approach

To protect the electronic ballot box against application-level flooding attacks, it needs to be equipped with a stronger filter on what is an acceptable ballot. By introducing *posting tickets*, which are distributed by the registrars to the voters during the registration phase, ballots not accompanied by a valid posting ticket can be filtered out right from the beginning. To realize this filter, we use a combination of Schnorr's identification scheme [40] and an

exponentiation mix-net [41, 42], an idea similar to the anonymous authentication technique proposed in [43, 44]. During the mixing, a random exponent α is applied to a given list of public keys. If x and $y = g^x$ form an input key pair, then x and $\hat{y} = y^\alpha = \hat{g}^x$ form an output key pair with respect to a fresh generator $\hat{g} = g^\alpha$ ($\hat{g}$ is published along with the mix-net data without revealing α). In our generic approach, pairs (x, y) are used as private and public posting tickets. By applying the Schnorr protocol to prove knowledge of x with respect to $\hat{y}$ and $\hat{g}$, the voter is authenticated anonymously as a holder of a valid posting ticket. This allows the electronic ballot box to reject ballots with invalid proofs. In the following, we introduce the required generic enhancement of the registration and vote casting phase (the tallying phase remains untouched). An overview of an enhanced scheme is given in Figure 2.

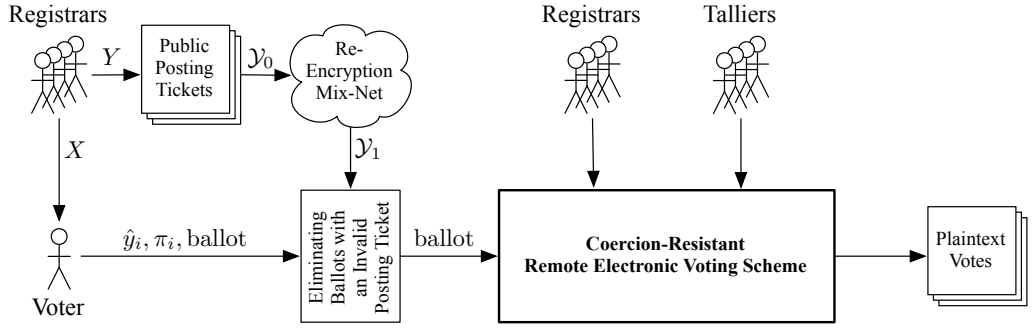

Figure 2: Overview of the generic protocol enhancement: the ballot sent to the electronic ballot box is accompanied by a Schnorr identification proof for an anonymized public posting ticket. Ballots with an invalid proof are filtered out from the beginning, i.e., they will be discarded and thus never reach the JCJ-based scheme in use.

Registration In addition to the registration requirements of the JCJ-based scheme in use, the registrars jointly establish a set of private posting tickets $X = \{x_i \in \mathbb{Z}_q : 1 \leq i \leq d\}$ and the set $Y = \{y_i \in G_q : 1 \leq i \leq d\}$ of corresponding public posting tickets $y_i = g^{x_i}$, where d might be different for every voter (see Section 4). X is delivered to the voter via an untappable channel and Y is added to the set $\mathcal{Y}_0$ of all public posting tickets for all voters, which resides on the public bulletin board. At the end of the registration phase, the complete set $\mathcal{Y}_0$ is digitally signed by the registrars. The total

number of issued posting tickets, $D = |\mathcal{Y}_0|$, represents the maximum amount of ballots allowed on the electronic ballot box. At the end of the registration phase, $\mathcal{Y}_0$ is mixed in an exponentiation mix-net and the fresh generator $\hat{g}$ is published. $\mathcal{Y}_1$ denotes the output of the mix-net.

Vote Casting To cast a vote using a private posting ticket x_i, the ballot of the JCJ-based scheme in use is enhanced by $\hat{y}_i = \hat{g}^{x_i}$ and a Schnorr proof $\pi_i = ZKP\{(x_i) : y_i = \hat{g}_i^x\}$ of knowing the x_i. The resulting enhanced ballot is accepted by the electronic ballot box, if the verification of the enhanced proof succeeds and if $\hat{y}_i \in \mathcal{Y}_1 \setminus \mathcal{Z}$, where $\mathcal{Z}$ denotes the set of public posting tickets already appearing in the electronic ballot box. Finally, all $N \leq D$ accepted ballots are passed without the enhancement to the tallying phase of the JCJ-based scheme in use.

3.2 Integrated Approach

By applying the generic approach introduced above to any of the existing JCJ-based schemes, we restrict the maximum number of ballots in the tallying phase to D, which implies that N is $\mathcal{O}(n)$ if D is constant. If applied to the original JCJ-scheme, we still obtain $\mathcal{O}(n^2)$ for the tallying phase. In a recent protocol addressing the board flooding problem [17], the idea of the generic approach and the original JCJ-scheme are integrated more tightly, resulting in a linear-time tallying phase. In this *integrated approach*, a set of so-called *dummy credentials* is distributed to the voters during the registration phase (together with the proper secret credential). Ballots not containing a proper or a dummy credential can then be rejected by the electronic ballot box during vote casting. Dummy credentials are used to produce fake votes. In other words, a voter can post several ballots to the electronic ballot box, but only the one containing the proper credential will make it to the final tally. This way, the credentials themselves bear the additional property provided by the posting tickets in the generic approach. An overview of this scheme is given in Figure 3.

Registration Let $\{\tau_i \in G_q : 1 \leq i \leq d\}$ be the set of dummy credentials for a given voter. They are generated jointly by the registrars together with the secret credential σ and distributed over an untappable channel. As in the generic approach, the number of dummy credentials d might be different

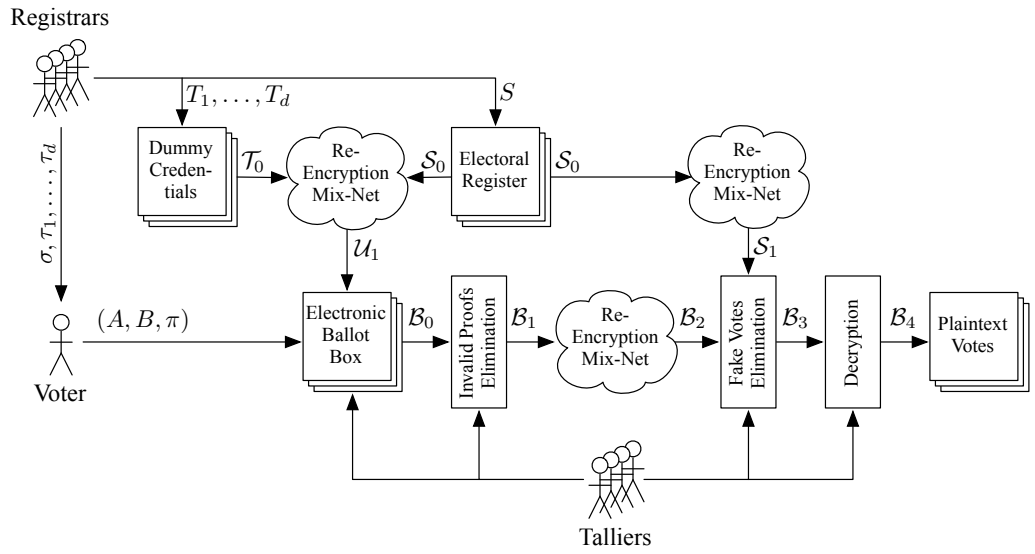

Figure 3: Overview of the integrated approach: ballots not containing a proper or dummy credential are rejected by the electronic ballot box with the help of the talliers.

for every voter. Corresponding encryptions $T_i = \mathrm{Enc}_y(\tau_i, r_{T_i})$ are published on the public bulletin board. The set of all dummy credentials published on the board is denoted by $\mathcal{T}_0$ and its size by $D = |\mathcal{T}_0|$. If the set of proper credentials is denoted by $\mathcal{S}_0$, as in our description of the original JCJ-scheme, then $\mathcal{U}_0 = \mathcal{S}_0 \cup \mathcal{T}_0$ represents the complete set of available credentials. The size of this set, $U = |\mathcal{U}_0| = n + D$, represents the maximum number of ballots in the electronic ballot box. By applying a verifiable re-encryption mix-net to $\mathcal{U}_0$ at the end of the registration phase, we obtain a new set $\mathcal{U}_1$.

Vote Casting The ballot is constructed as in the original JCJ-scheme. To fake a vote, one that will appear on the public bulletin board but not in the final tally, a dummy credentials τ_i is taken in place of σ. In either case, the resulting ballot (A, B, π) is sent to the electronic ballot box $\mathcal{B}_0$. It is accepted if $PET(A, U) = \mathit{true}$ holds for some $U \in \mathcal{U}_1$ and if no other such match for U has been found before. To perform these tests in linear time, we can safely apply Smith's and Weber's technique here, because the votes have not yet been mixed. Note that this step requires the help of the talliers already during the vote casting phase, which is a true disadvantage compared

to the generic approach. Another consequence is the fact that the electronic ballot box does not accept and therefore will not hold any duplicate votes.

Tallying Four consecutive steps are necessary to single out the valid votes from the list of ballots in the electronic ballot box (see Figure 3):

1. The proofs π are verified for all ballots $(A, B, \pi) \in \mathcal{B}_0$. Ballots for which the proof does not hold are excluded from further processing. The remaining reduced ballots (A, B) form a new set $\mathcal{B}_1$.

2. The sets $\mathcal{B}_1$ and $\mathcal{S}_0$ are mixed in two separate verifiable re-encryption mix-nets. These mix-nets produce two new sets $\mathcal{B}_2$ and $\mathcal{S}_1$.

3. Ballots containing a dummy credential are excluded from further processing. This is the case for a ballot $(A, B) \in \mathcal{B}_2$, if $PET(A, S) = \mathit{false}$ holds for every $S \in \mathcal{S}_1$. We can again safely apply Smith's and Weber's technique to perform this step in linear time.[3] The remaining encrypted votes B form a new set $\mathcal{B}_3$.

4. The encrypted votes $B \in \mathcal{B}_3$ are jointly decrypted. This yields a new set $\mathcal{B}_4$, which contains the plaintext votes ready to be counted.

Let $N = |\mathcal{B}_0|$ denotes the number of ballots in the initial electronic ballot box. Clearly, the tallying procedure runs in $\mathcal{O}(N)$ time, where $n+|\mathcal{T}_0|$ defines an upper limit for N. If the average number of dummy credentials per voter is constant, which implies that N is $\mathcal{O}(n)$, we finally obtain $\mathcal{O}(n)$ for the tallying phase.

4 Analysis of Privacy and Coercion-Resistance

In this section, we analyze privacy and coercion-resistance with respect to the approaches presented in this paper. We use the same adversary model as introduced by Jules et al. [1], where it is assumed that the adversary may corrupt a minority of registrars, but such that the set of corrupted registrars is known to the voter. The adversary may also corrupt a minority of talliers and arbitrarily many voters in a static, active manner. By corrupting a tallier, the adversary learns the corresponding share of the private key x and all

[3]The attack described in [10] does not apply here, because voters cannot freely choose related plaintext credentials.

secret randomizations (see [45] for a detailed description of such an adversary). Furthermore, we assume that the adversary is polynomially bounded and thus incapable of breaking cryptographic primitives. By requiring an untappable channel during registration and an anonymous channel during vote casting, we assume that the adversary learns nothing about the voter's private communications over these channels. This implies that during vote casting, every voter has access to the anonymous channel for silently casting at least one vote. Finally, with respect to the pressure exercised on voters under coercion, we assume that the adversary has limited resources such as time or money.

By applying this adversary model to the different schemes discussed in this paper, we will now analyze their compliance with the notions of privacy and coercion-resistance as introduced in Section 2. We exclude arguments concerning the registration phase from our analysis, because they can be adopted from the original paper.

4.1 Coercion-Resistance in JCJ-Based Schemes?

What makes the original JCJ-scheme coercion-resistant is the fact, that any ballot sent to the electronic ballot box is accepted, if it is well-formed and complies with the scheme. This enables the voter to deceive the adversary with a randomly chosen fake credential (see Subsection 2.1), for example by using it for casting a vote that complies with the demands or by handing it over to the adversary in a simulation attack. Votes accompanied with such fake credentials are discarded during the tallying phase, but the two mix-nets involved in the tallying phase guarantee that no voter can prove to a third party whether a particular ballot has been discarded before tallying or not. This property finally prevents voters from selling their votes or from being coerced. Note that this conclusion holds for all four types of coercive attacks considered in [1]. For a more formal and more profound discussion of coercion-resistance in the JCJ-scheme, we refer to the original paper.

Three of the linear-time schemes presented in Subsection 2.2 offer an adjustable security parameter β to trade off coercion-resistance against efficient tallying, where β is the size of some anonymity set. To quantify coercion-resistance as a function of β, we consider the game-theoretic definition given in [46], where the level of coercion-resistance a protocol provides is defined in terms of the *adversarial uncertainty*, i.e., the probability $\delta \in [0, 1]$ that the adversary is able to distinguish whether a coerced voter is following the

instructions or running a counter-strategy.

In all three schemes offering a security parameter β [13, 14, 15], maximal coercion-resistance of degree $\delta = 0$ is achieved by selecting $\beta = n$, but then the tallying procedure falls back to a quadratic running time. On the other extreme, selecting $\beta = 1$ (respectively $\beta = 0$, depending on the scheme) implies efficient linear-time tallying, but then coercion-resistance is ruled out entirely by $\delta = 1$. As tallying remains efficient as long as β remains constant, a reasonable level of coercion-resistance $0 < \delta \ll 1$ can be achieved by selecting β appropriately (see [16] for a discussion on the relationship between β and δ in those schemes).[4] The scheme by Araújo et al. [11, 12] offers efficient tallying and full coercion-resistance of degree $\delta = 0$ simultaneously, but it allows ballot stuffing by a sufficiently large group of signing authorities and is therefore excluded from further analysis.

4.2 Coercion-Resistance in the Generic Approach

In the generic approach, the voter can submit a limited amount of ballots to the electronic ballot box, depending on the number of posting tickets received during registration. As a consequence, if the voter can be forced to expend all posting tickets with invalid votes or to hand them over to the adversary, then the possibility of submitting a final valid vote is denied. This restriction enables forced-abstention attacks, but does not generally affect coercion-resistance of the existing scheme in use.

To run a forced-abstention attack of the above type, the adversary may offer a certain amount of money for each posting ticket received from the voter or spent by the voter on an invalid vote. From an economical perspective, this means that restricting the number of posting tickets makes them valuable. If $\mu = {}^{D}/_{n}$ denotes the average number of posting tickets per voter, where $D = |\mathcal{Y}_0|$ is the total number of posting tickets and n the number of voters, then increasing μ decreases the value of each issued posting ticket, and vice versa. Therefore, μ plays the role of an additional security parameter, independent of β in some JCJ-based schemes, influencing δ. In the following, we provide answers to some questions on how to choose μ and on how to generally deal with posting tickets.

[4] In all three schemes, coercion-resistance is only reduced with respect to forced vote abstention.

How many posting tickets are needed?

To answer this question, suppose first that each voter receives the same number $d \geq 1$ of posting tickets. Then the adversary can simply force the voter to release all d posting tickets and check their validity by observing if corresponding ballots are accepted by the electronic ballot box. However, for the same reasons as in the original JCJ-scheme, releasing the secret voting credential σ cannot be enforced, i.e., the voter is still protected from being coerced, except for forced vote abstention.

As a counter-measure against forced-abstention attacks, the registrars have to issue a random number of posting tickets to each voter. Suppose that a given voter receives $d \in \{1, \ldots, d_{max}\}$ posting tickets, where d_{max} denotes a fixed upper limit for all voters. If the scheme guarantees that d is not known to the adversary, then the voter can lie about it, for example by releasing only $d-1$ posting tickets to the adversary. Obviously, this argument works for every voter possessing $d > 1$ posting tickets and thus completely rules out coercion in those cases. Unfortunately, this is not true for voters possessing exactly $d = 1$ posting ticket. Under coercion, such (unfortunate) voters could only give away a single posting ticket, which means that they would be unable to cast the final vote. In other words, $d = 1$ makes voters prone to coercion by forced vote abstention. Note that this problem does not disappear by increasing the lower limit of d to some value $d_{min} < d_{max}$ or by decreasing it to 0. Another problem exists for voters in possession of $d = d_{max}$ posting tickets. They can prove the release of all posting tickets to a potential adversary paying for vote abstention.

As an answer to the above problems, we suggest that d is selected according to some non-uniform probability distribution over $\mathbb{N}_1 = \{1, \ldots, \infty\}$. The most natural choice—the one with maximum entry among all real-valued distributions with specified mean and variance—is a normal distribution $\mathcal{N}(\mu, \sigma^2)$ with reasonable mean $\mu > 0$ and variance $\sigma^2 > 0$. Since normal distributions are defined by continuous probability density functions $f : \mathbb{R} \to [0, 1]$ or corresponding cumulative density functions $F : \mathbb{R} \to [0, 1]$, they need to be applied in some discretized manner over $\mathbb{N}_1$. For this, let

$$f'(x) = c^{-1} \cdot f(x) \cdot H(x)$$

be the truncated distribution over $\mathbb{R}^+$, where $H(X)$ is the heavyside step

function and

$$c = \int_0^\infty f(x)dx = 1 - F(0)$$

the normalization constant. Then we can discretize f' into $f^* : \mathbb{N}_1 \to [0, 1]$ by

$$f^*(x) = \int_{x-1}^{x} f'(x)dx = \frac{F(x) - F(x-1)}{1 - F(0)} = \frac{\Phi(\frac{x-\mu}{\sigma}) - \Phi(\frac{x-\mu-1}{\sigma})}{\Phi(\frac{\mu}{\sigma})},$$

where Φ denotes the cumulative distribution function of the standard normal distribution $\mathcal{N}(0, 1)$, and interpret $f^*(d)$ as the probability of obtaining exactly d posting tickets from the registrars.

How does a given normal distribution affect coercion-resistance?

The advantage of using a distribution f^* with no upper limit is that no voter can prove the release of all posting tickets. The challenge then is to adjust the available parameters μ and σ^2 such that only very few voters receive the minimal number of posting tickets, but without ruling it out entirely.

Assuming that d is unknown to the adversary, the voter's best counter-strategy against forced vote abstention is to release only $d-1$ posting tickets, thus saving one for the final vote. As mentioned above, this strategy does not work for voters possessing a single posting ticket only. Therefore, the adversarial uncertainty δ depends on the voter under coercion. If d_i denotes the number of posting tickets of voter i, then

$$\delta_i = \begin{cases} 1, \text{ if } d_i = 1, \\ 0, \text{ if } d_i > 1. \end{cases}$$

denotes the adversarial uncertainty with respect to a single voter, and

$$\delta = \frac{1}{n} \sum_{i=1}^{n} \delta_i = f^*(1) = 1 - \frac{\Phi(\frac{\mu-1}{\sigma})}{\Phi(\frac{\mu}{\sigma})}$$

is the *average adversarial uncertainty* over the entire electorate. Some exemplary values for δ are shown in Table 1. To minimize δ, we can either choose

a large mean or a small variance. Note that making the mean too large will harm the efficiency of the tallying phase, and making the variance too small will lead to almost the same number of posting tickets for every voter. In the extreme case when σ^2 tends toward 0, which implies that δ tends toward 0, it even seems that coercion is completely ruled out, but then exactly the same number of posting tickets is issued to all voters, which corresponds to the first unpleasant scenario discussed in our analysis. The problem is that δ reflects coercibility with respect to a single voter only, which is not a characteristic measure for statistical attacks on groups of voters. To deal with such attacks, it seems that a large variance is desirable, but we do not introduce a measure dealing with statistical attacks in this paper. Therefore, forced vote abstention cannot entirely been ruled out by minimizing δ, but a careful selection of the security parameters μ and σ^2 can make it unbearable for the vast majority of voters (without spoiling the tallying procedure).

	$\sigma^2 = 1$	$\sigma^2 = 2$	$\sigma^2 = 3$	$\sigma^2 = 4$	$\sigma^2 = 5$	$\sigma^2 = 10$
$\mu = 1$	0.4057	0.3423	0.3038	0.2769	0.2567	0.1988
$\mu = 3$	0.0214	0.0628	0.0861	0.0984	0.1051	0.1112
$\mu = 5$	$3.1{\cdot}10^{-5}$	0.0021	0.0085	0.0166	0.0245	0.0488
$\mu = 10$	≈ 0	$9.7{\cdot}10^{-11}$	$9.8{\cdot}10^{-8}$	$3.1{\cdot}10^{-6}$	$2.5{\cdot}10^{-5}$	0.0014
$\mu = 20$	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0	$8.1{\cdot}10^{-10}$

Table 1: The adversarial uncertainty δ for some exemplary security parameters μ and σ^2.

How do registrars generate random numbers of posting tickets?

The naïve approach for the registrars to generate a random number of posting tickets for a given voter is to jointly apply F to determine d. The problem of this simple approach is that then d is not a secret of the voter alone, i.e., the voter cannot lie about it toward an adversary colluding with one of the registrars. As a solution to this problem, we suggest to split up the group of registrars into r sub-groups. Each of these sub-groups is then responsible for secretly generating an average of d/r posting tickets, but without informing the other groups about the exact number. To do so, we decompose the normal distribution $\mathcal{N}(\mu, \sigma^2)$ into a sum of r normal distributions $\mathcal{N}(\mu/r, \sigma^2/r^2)$. Each sub-group generates its own subset of posting tickets

and communicates them separately to the voter over the untappable channel. Coercion-resistance is maintained, if at least one sub-group remains honest. This constraint guarantees that d remains secret. Note that a single dishonest registrar constitutes a single point of failure of the corresponding sub-group. As this affects the robustness of the registration process, the number of registrars and the size of the sub-groups have to be chosen carefully.

How should the public board store the encrypted posting tickets?

In the original JCJ-scheme, the list of encrypted credentials $\mathcal{S}_0$ is published in the electoral register together with the plaintext identities of the voters. This list resides on the public bulletin board and can be inspected and verified by everybody. Doing the same with the posting tickets y_i by linking $Y = \{y_1, \ldots, y_d\}$ publicly with the voter's identity allows the adversary to derive the secret number d from Y. As a simple solution to this problem, we suggest that Y is published anonymously in $\mathcal{Y}_0$ without any links to the voters. Since $\mathcal{Y}_0$ does not serve as an electoral register, it does not necessarily need to be treated in exactly the same way as $\mathcal{S}_0$.

How can the voter hide the number of posting tickets?

During registration, the voter receives d posting tickets over an untappable channel. To omit vote-abstention attacks, the voter has to be able to hide d from the attacker. Therefore, the voter is required to manage each posting ticket independently, so that disclosing one posting ticket does not infer the existence of another. In practice, especially if d is large, it is difficult for the voter to realize such a management in a usable way. As a possible approach, we suggest a cryptographic component similar to an encrypted password vault, but with the additional property that the extraction of a single secret does not disclose any information about the remaining secrets and that the exact number of secrets always remains hidden. An approach for a system with these properties based on polynomial interpolation is currently under investigation [47, 48].

4.3 Coercion-Resistance in the Integrated Approach

By issuing dummy credentials instead of posting tickets, the integrated approach limits the number of ballots the voter can submit to the electronic

ballot box in a similar way as in the generic approach. If $\mu = {}^{D}/_{n}$ denotes the average number of dummy credentials per voter and $D = |\mathcal{T}_0|$ the total number of dummy credentials, then μ plays the role of a security parameter influencing δ as in the generic approach. This raises the same questions on how to choose μ and on how to generally deal with dummy credentials. All conclusions from the previous subsection can be adopted, except those concerning the impact of a successful coercion attack.

Consider the attack from the generic approach, where voters possessing a single posting ticket can be forced to abstain from voting. In the integrated approach, the same attack enables the adversary to get into possession of both the single dummy credential and the secret credential, simply by forcing the voter to release two credentials. Their validity can then be checked by sending respective ballots to the electronic ballot box and by observing if they get accepted. Therefore, voters in possession of only $d = 1$ dummy credential are exposed to all four types of coercive attacks. However, using a normal distribution with appropriate parameters for picking d limits the scalability of this attack in the same way as in the generic approach.

5 Conclusion

This paper is a new contribution to making the original JCJ-scheme—applicable under the assumption of unrealistic computing power only—more efficient and thus more practicable. The goal of our approach is different than in other existing improvements of the JCJ-scheme. Instead of focusing on a linear-time tallying procedure, we propose a generic mechanism for limiting the maximum number of ballots in the electronic ballot box. This is an important counter-measure to prevent application-level flooding attacks, where the electronic ballot box is filled up with an enormous amount of invalid votes. Our solution has some negative consequences with respect to perfect coercion-resistance, but by allowing a trade-off between the obtained level of coercion-resistance and the maximal amount of ballots in the electronic ballot box, it is possible to minimize this effect to a small subset of voters.

In our approach, voters receive a random amount of posting tickets at registration. These tickets can be used for sending ballots to the electronic ballot box. The limited total number of issued posting tickets defines an upper bound for the ballot box size. This idea is similar to the integrated approach presented recently in [17], but the new approach presented in this

paper has at least three major advantages:

- The approach is generic, meaning that it is applicable to any of the existing linear-time JCJ-based schemes (even to the integrated approach itself).
- For checking the incoming ballots, no third parties need to cooperate with the electronic ballot box.
- Coercion-resistance is only affected with respect to forced vote abstention.

An open question is the residual statistical vulnerability of our solution. For this, we need to extent our definition of adversarial uncertainty from a single voter under attack to a group of voters under attack. As a general countermeasure against such statistical attacks, we may consider the possibility of obtaining additional posting tickets during the vote casting phase, for example by exchanging them between voters. On the more practical side, we need to provide solutions for the creation and management of posting tickets, which adds some non-negligible organizational complexity to the overall scheme.

Acknowledgments.

We thank the anonymous reviewers for their thorough reviews and highly appreciate the comments and suggestions. We would also like to thank our colleagues Oliver Spycher and Stephan Fischli for their constructive inputs and critical comments, which significantly contributed to improving the quality of this paper. This research has been supported by the *Hasler Foundation* (project No. 09037).

References

[1] A. Juels, D. Catalano, M. Jakobsson, Coercion-resistant electronic elections, in: V. Atluri, S. De Capitani di Vimercati, R. Dingledine (Eds.), WPES'05, 4th ACM Workshop on Privacy in the Electronic Society, Alexandria, USA, 2005, pp. 61–70.

[2] B. Meng, A critical review of receipt-freeness and coercion-resistance, Information Technology Journal 8 (7) (2009) 934–964.

[3] W. D. Smith, New cryptographic voting scheme with best-known theoretical properties, in: FEE'05, Workshop on Frontiers in Electronic Elections, Milan, Italy, 2005.

[4] M. Jakobsson, A. Juels, Mix and match: Secure function evaluation via ciphertexts, in: T. Okamoto (Ed.), ASIACRYPT'00, 6th International Conference on the Theory and Application of Cryptographic Techniques, LNCS 1976, Kyoto, Japan, 2000, pp. 162–177.

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

[6] G. Meister, D. Hühnlein, J. Eichholz, R. Araújo, eVoting with the European citizen card, in: A. Brömme, C. Busch, D. Hühnlein (Eds.), BIOSIG'08, Special Interest Group on Biometrics and Electronic Signatures, no. P-137 in Lecture Notes in Informatics, Gesellschaft für Informatik E.V., Darmstadt, Germany, 2008, pp. 67–78.

[7] J. Schweisgut, Coercion-resistant electronic elections with observer, in: R. Krimmer (Ed.), EVOTE'06, 2nd International Workshop on Electronic Voting, no. P-86 in Lecture Notes in Informatics, Gesellschaft für Informatik E.V., Bregenz, Austria, 2006, pp. 171–177.

[8] G. Weber, R. Araújo, J. Buchmann, On coercion-resistant electronic elections with linear work, in: ARES'07, 2nd International Conference on Availability, Reliability and Security, Vienna, Austria, 2007, pp. 908–916.

[9] S. Weber, Coercion-Resistant Cryptographic Voting: Implementing Free and Secret Electronic Elections, VDM Verlag, Saarbrücken, Germany, 2008.

[10] B. Pfitzmann, Breaking an efficient anonymous channel, in: A. De Santis (Ed.), EUROCRYPT'94, 13th International Conference on the Theory and Applications of Cryptographic Techniques, Vol. 950 of LNCS 950, Perugia, Italy, 1994, pp. 332–340.

[11] R. Araújo, S. Foulle, J. Traoré, A practical and secure coercion-resistant scheme for remote elections, in: D. Chaum, M. Kutylowski, R. L. Rivest,

P. Y. A. Ryan (Eds.), FEE'07, Workshop on Frontiers in Electronic Elections, Schloss Dagstuhl, Germany, 2007, pp. 330–342.

[12] R. Araújo, R. R. N. Ben Rajeb, J. Traoré, S. Youssfi, Towards practical and secure coercion-resistant electronic elections, in: S. H. Heng, R. N. Wright, B. M. Goi (Eds.), CANS'10, 9th International Conference on Cryptology And Network Security, LNCS 6467, Kuala Lumpur, Malaysia, 2010, pp. 278–297.

[13] J. Clark, U. Hengartner, Selections: Internet voting with over-the-shoulder coercion-resistance, in: G. Danezis (Ed.), FC'11, 15th International Conference on Financial Cryptography, LNCS 7035, St. Lucia, 2011, pp. 47–61.

[14] M. Schläpfer, R. Haenni, R. E. Koenig, O. Spycher, Efficient vote authorization in coercion-resistant internet voting, in: VoteID'11, 3rd International Conference on E-Voting and Identity, LNCS 7187, Tallinn, Estonia, 2011, pp. 71–88.

[15] O. Spycher, R. E. Koenig, R. Haenni, M. Schläpfer, A new approach towards coercion-resistant remote e-voting in linear time, in: G. Danezis (Ed.), FC'11, 15th International Conference on Financial Cryptography, LNCS 7035, St. Lucia, 2011, pp. 182–189.

[16] O. Spycher, R. E. Koenig, R. Haenni, M. Schläpfer, Achieving meaningful efficiency in coercion-resistant, verifiable internet voting, in: M. Kripp (Ed.), EVOTE'12, 5th International Workshop on Electronic Voting, no. P-205 in Lecture Notes in Informatics, Gesellschaft für Informatik E.V., Bregenz, Austria, 2012, pp. 113–126.

[17] R. E. Koenig, R. Haenni, S. Fischli, Preventing board flooding attacks in coercion-resistant electronic voting schemes, in: J. Camenisch, S. Fischer-Hübner, Y. Murayama, A. Portmann, C. Rieder (Eds.), SEC'11, 26th IFIP International Information Security Conference, Vol. 354, Lucerne, Switzerland, 2011, pp. 116–127.

[18] J. Benaloh, D. Tuinstra, Receipt-free secret-ballot elections, in: STOC'94, 26th Annual ACM Symposium on Theory of Computing, Montréal, Canada, 1994, pp. 544–553.

[19] K. Sako, J. Kilian., Receipt-free mix-type voting scheme: A practical solution to the implementation of a voting booth, in: L. C. Guillou, J. J. Quisquater (Eds.), EUROCRYPT'95, 14th International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 921, Saint-Malo, France, 1995, pp. 393–403.

[20] T. Okamoto, Receipt-free electronic voting schemes for large scale elections, in: B. Christianson, B. Crispo, T. M. A. Lomas, M. Roe (Eds.), 5th International Security Protocols Workshop, LNCS 1361, Paris, France, 1997, pp. 25–35.

[21] M. Hirt, K. Sako, Efficient receipt-free voting based on homomorphic encryption, in: G. Goos, J. Hartmanis, J. van Leeuwen (Eds.), EUROCRYPT'00, 19th International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 1807, Bruges, Belgium, 2000, pp. 539–556.

[22] B. Lee, K. Kim, Receipt-free electronic voting scheme with a tamper-resistant randomizer, in: P. J. Lee, C. H. Lim (Eds.), ICISC'02, 5th International Conference on Information Security and Cryptology, LNCS 2587, Seoul, South Korea, 2002, pp. 389–406.

[23] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, S. Yoo, Providing receipt-freeness in mixnet-based voting protocols, in: G. Goos, J. Hartmanis, J. van Leeuwen (Eds.), ICISC'03, 6th International Conference on Information Security and Cryptology, LNCS 2971, Seoul, South Korea, 2003, pp. 245–258.

[24] T. El Gamal, A public key cryptosystem and a signature scheme based on discrete logarithms, in: G. R. Blakley, D. Chaum (Eds.), CRYPTO'84, Advances in Cryptology, LNCS 196, Springer, Santa Barbara, USA, 1984, pp. 10–18.

[25] Y. Desmedt, Y. Frankel, Threshold cryptosystems, in: G. Brassard (Ed.), CRYPTO'89, 9th Annual International Cryptology Conference on Advances in Cryptology, LNCS 435, Santa Barbara, USA, 1989, pp. 307–315.

[26] T. P. Pedersen, A threshold cryptosystem without a trusted party, in: D. W. Davies (Ed.), EUROCRYPT'91, 10th Workshop on the Theory

and Application of Cryptographic Techniques, Vol. 547 of LNCS 547, Brigthon, U.K., 1991, pp. 522–526.

[27] M. Bellare, O. Goldreich, On defining proofs of knowledge, in: E. F. Brickell (Ed.), CRYPTO'92, 12th Annual International Cryptology Conference on Advances in Cryptology, LNCS 740, Santa Barbara, USA, 1992, pp. 390–420.

[28] A. Fiat, A. Shamir, How to prove yourself: Practical solutions to identification and signature problems, in: A. M. Odlyzko (Ed.), CRYPTO'86, 6th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 1986, pp. 186–194.

[29] J. Groth, A verifiable secret shuffle of homomorphic encryptions, Journal of Cryptology 23 (4) (2010) 546–579.

[30] D. Wikström, A commitment-consistent proof of a shuffle, in: C. Boyd, J. González Nieto (Eds.), ACISP'09, 14th Australasian Conference on Information Security and Privacy, LNCS 5594, Brisbane, Australia, 2009, pp. 407–421.

[31] B. Terelius, D. Wikström, Proofs of restricted shuffles, in: D. J. Bernstein, T. Lange (Eds.), AFRICACRYPT'10, 3rd International Conference on Cryptology in Africa, LNCS 6055, Stellenbosch, South Africa, 2010, pp. 100–113.

[32] D. Chaum, Untraceable electronic mail, return addresses and digital pseudonyms, Communications of the ACM 24 (2) (1981) 84–88.

[33] J. Heather, D. Lundin, The append-only web bulletin board, in: P. Degano, J. Guttman, F. Martinelli (Eds.), FAST'08, 5th International Workshop on Formal Aspects in Security and Trust, LNCS 5491, Malaga, Spain, 2008, pp. 242–256.

[34] R. A. Peters, A secure bulletin board, Master's thesis, Department of Mathematics and Computing Science, Technische Universiteit Eindhoven, The Netherlands (2005).

[35] J. Beuchat, Append-only web bulletin board, Project report, Bern University of Applied Sciences, Biel, Switzerland (2011).

[36] R. Di Cosmo, On privacy and anonymity in electronic and non electronic voting: the ballot-as-signature attack, Hyper Articles en Ligne hal-00142440 (2).

[37] J. Clark, Democracy enhancing technologies: Toward deployable and incoercible E2E elections, Ph.D. thesis, University of Waterloo, Canada (2011).

[38] D. Berger, R. Linder, Sicheres und effizientes E-Voting, Bachelor thesis, Bern University of Applied Sciences, Biel, Switzerland (2012).

[39] R. Araújo, On remote and voter-verifiable voting, Ph.D. thesis, Department of Computer Science, Darmstadt University of Technology, Darmstadt, Germany (2008).

[40] C. P. Schnorr, Efficient signature generation by smart cards, Journal of Cryptology 4 (3) (1991) 161–174.

[41] C. A. Neff, A verifiable secret shuffle and its application to e-voting, in: P. Samarati (Ed.), CCS'01, 8th ACM Conference on Computer and Communications Security, Philadelphia, USA, 2001, pp. 116–125.

[42] D. Wikström, A sender verifiable mix-net and a new proof of a shuffle, in: B. K. Roy (Ed.), ASIACRYPT'05, 11th International Conference on the Theory and Application of Cryptographic Techniques, LNCS 3788, Chennai, India, 2005, pp. 273–292.

[43] R. Haenni, O. Spycher, Secure internet voting on limited devices with anonymized DSA public keys, in: H. Shacham, V. Teague (Eds.), EVT/WOTE'11, Electronic Voting Technology Workshop/Workshop on Trustworthy Elections, San Francisco, USA, 2011.

[44] O. Spycher, R. Haenni, A novel protocol to allow revocation of votes in a hybrid voting system, in: ISSA'10, 9th Annual Conference on Information Security – South Africa, Sandton, South Africa, 2010.

[45] R. Cramer, I. Damgård, J. B. Nielsen, Multiparty computation, an introduction, Lecture notes, Department of Computer Science, University of Aarhus, Denmark (2009).

[46] R. Küsters, T. Truderung, A. Vogt, A game-based definition of coercion-resistance and its applications, in: A. Myers, M. Backes (Eds.), CSF'10, 23nd IEEE Computer Security Foundations Symposium, Edinburgh, U.K., 2010, pp. 122–136.

[47] R. E. Koenig, R. Haenni, How to store some secrets, IACR Cryptology ePrint Archive 2012/375.

[48] J. T. Liechti, L. Bernath, KryptonIT – Password Tresor, Bachelor thesis, Bern University of Applied Sciences, Biel, Switzerland (2012).