# Coercion-Resistant Cryptographic Voting: Implementing Free and Secret Electronic Elections

*Extended Abstract*

**Stefan G. Weber**
sweber@tk.informatik.tu-darmstadt.de

## 1 Introduction

Using information technology and computers to conduct elections is known as *electronic voting* or shortly *e-voting*. In this setting, technology helps to organize the voting process and speeds up the computation of the results. A special case of this is *remote electronic voting over the Internet*, also named *online voting* and *Internet voting*. It enables voters to cast their votes over the Internet, from arbitrary computers, and thus offers convenience and does not require geographical proximity on an election day. Thus, it has the potential to allure those groups of voters that regularly abstain from general elections.

Along with the introduction of e-government services, many countries prepare electronic voting projects for future elections. Even more companies develop solutions for non-political elections. The challenging task is to design election systems that allow the voters casting their votes secretly, freely and securely in non-supervised environments, while establishing auditing mechanism to detect manipulations of the results.
Two further threats have to be addressed to guarantee democratic elections: vote buying and coercion against voters. It still is an open question how to realize legally binding e-enabled general elections, that overcome those threats.

In this context, we explore countermeasures against these threats. A cryptographic voting protocol is developed, evaluated and prototy-pically implemented that offers mechanisms to protect voters against coercion and thwarts vote buying. Beside this, the proposed solution is verifiable, robust, practical and has a linear work factor. Building on concepts by Smith [Smi05], it improves on a previous voting protocol by Juels et. al. [JCJ05], which exhibits a quadratic runtime.

## 2 Coercion-Resistant Elections

A lot of former cryptographic research dealing with vote buying and coercion has been focussing on *receipt freeness*, meaning that a voter may not be able to create a *receipt*, i.e. any information that can be used to convince a third person that she voted in a specific manner.

Receipt-free voting schemes thwart vote buying and protect voters against being forced to cast a vote for a certain candidate, as the vote buyer or coercer cannot determine the voters' behaviour. However, receipt freeness fails to protect an election system against several attacks: a voter can additionally be forced to abstain from voting, to cast a random vote or to give away secret keys she possesses, to allow a coercer voting on her behalf. A voting scheme that also protects against these attacks is called ***coercion-resistant*** [JCJ05].

In this work [Web08], we present a voting protocol[1] that achieves the coercion resistance property. The key idea is to enable a voter to deceive a coercer about her true behaviour in an election by using an indirect authentication and authorization mechanism: an *anonymous credential* is registered to each voter, that hse has to include to a vote she wants to be valid and counted. Additionally, the voter is enabled to use and give away fake credentials to a coercer, to satisfy the coercer's demands. As a coercer cannot distinguish between fake and valid credentials and thus votes, no basis for coercion and vote buying is given.

# 3 Building Blocks of the Voting Protocol

The proposed voting protocol is composed of advanced cryptographic primitives:

- *Zero knowledge proofs* assure the correctness of protocol steps involving secret keys and secret data,
- *Threshold cryptosystems* distribute the cryptographic operations among several servers to distribute trust and to achieve robustness,
- *Mixnets* anonymize incoming votes.

Those primitives allow satisfying seemingly contradictory requirements: the voting scheme guarantees verifiability and correctness of the processing of the votes while maintaining a high level of privacy for the voters. Chapter 2 of this work describes these primitives in detail.

# 4 The Coercion-Resistant Voting Protocol

The coercion-resistant voting protocol is presented in Chapter 3 of this work. It is shortly sketched in the following and illustrated in Figure 1.

In order to vote, voters submit their ballots to a bulletin board server. Each ballot contains non-deterministic encryptions of their vote and their credential together with a non-interactive zero knowledge validity proof, assuring that it contains a valid candidate.

In order to compute the result of the election, a set of servers cooperatively processes those ballots by

1. excluding ballots with invalid proofs,
2. eliminating ballots containing duplicate credentials via a blind hashtable lookup on encrypted credentials,

[1] A previous description can be found in [Web06], further details are given in [WAB07].

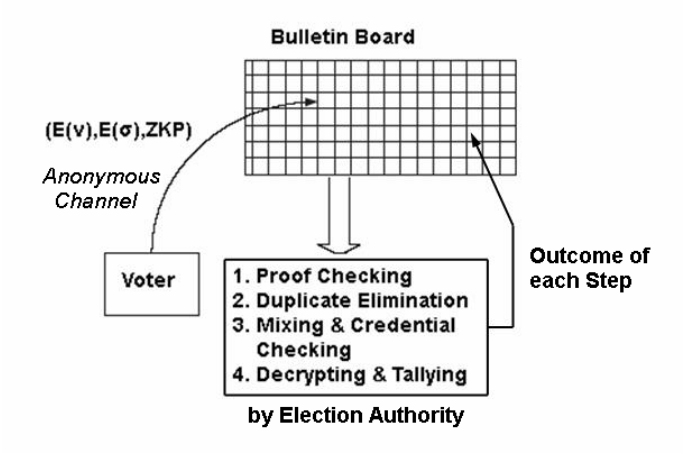


Figure 1: The coercion-resistant voting protocol

3. mixing the ballots as well as the encrypted credentials from a registration list and checking the ballots' credentials via a blind hashtable lookup against this mixed reference list, thus authorizing valid votes,

4. and finally decrypting and tallying all authorized votes.

The election result and all intermediate steps are published on a public readable bulletin board server to allow for external verification and to prove correctness of the result.

In Chapter 4 of this work, the protocol is evaluated in detail. This analysis shows that the protocol is coercion-resistant, correct, universal verifiable, robust, practical and has runtime linear in the number of cast votes. Additionally, in Chapter 5, several extensions and variants are developed and discussed. It is shown how to integrate *homomorphic encryption* mechanisms into the scheme, in order to combine encrypted votes to produce the final election result without decrypting single votes.

# 5 Implementation

As a proof-of-concept, a prototype of the voting scheme is implemented in Java (based on JCE/JCA). It is described in Chapter 6 of this work. It realizes the proposed cryptographic concepts and demonstrates their feasibility. Furthermore, the implementation offers a basic library to develop further voting protocols.

# References

[JCJ05] Ari Juels, Dario Catalano, and Markus Jakobsson, *Coercion-Resistant Electronic Elections*, ACM Workshop On Privacy In The Electronic Society 2005 (WPES'05), November 2005, pp. 61-70.

[Smi05] Warren D. Smith, *New Cryptographic Election Protocol with Best-Known Theoretical Properties*, Workshop on Frontiers in Electronic Elections (FEE'05), September 2005.

[Web06] Stefan G. Weber *A Coercion-Resistant Cryptographic Voting Protocol - Evaluation and Prototype Implementation*, Diploma Thesis, TU Darmstadt, July 2006.

[WAB07] Stefan G. Weber, Roberto Araujo, and Johannes Buchmann, *On Coercion-Resistant Electronic Elections with Linear Work*, Workshop on Dependability and Security in e-Government (DeSeGov 2007) at Int. Conference on Availability, Reliability and Security (ARES'07), April 2007, pp. 908-916.

[Web08] Stefan G. Weber *Coercion-Resistant Cryptographic Voting: Implementing Free and Secret Electronic Elections*, VDM Verlag Dr. Müller, March 2008.