Bingo Voting: Secure and Coercion-Free Voting Using a Trusted Random Number Generator

Jens-Matthias Bohli[1,⋆], Jörn Müller-Quade[2], and Stefan Röhrich[2]

[1] NEC Laboratories Europe, Network Research Division,
Kurfürsten-Anlage 36, 69115 Heidelberg, Germany
bohli@nw.neclab.eu
[2] Institut für Algorithmen und Kognitive Systeme / E.I.S.S.,
Universität Karlsruhe (TH), 76128 Karlsruhe, Germany
{muellerq,sr}@ira.uka.de

Abstract. It is debatable if current direct-recording electronic voting machines can sufficiently be trusted for a use in elections. Reports about malfunctions and possible ways of manipulation abound. Voting schemes have to fulfill seemingly contradictory requirements: On one hand the election process should be verifiable to prevent electoral fraud and on the other hand each vote should be deniable to avoid coercion and vote buying.

This work presents a new verifiable and coercion-free voting scheme *Bingo Voting*, which is based on a trusted random number generator. As a motivation for the new scheme two coercion/vote buying attacks on voting schemes are presented which show that it can be dangerous to let the voter contribute randomness to the voting scheme.

A proof-of-concept implementation of the scheme shows the practicality of the scheme: all costly computations can be moved to a non time critical pre-voting phase.

Keywords: Secure electronic voting, coercion-free, receipt-free.

1 Introduction

Elections have to meet a lot of requirements, e.g., the German constitution speaks about the selection of the members of German House of Representatives in general, direct, free, equal, and secret elections[1]. For security considerations of voting protocols, mainly the last three properties are of interest: An election should be free, i.e., nobody can be coerced to cast a certain vote, it should be equal, i.e., nobody can influence the result more than with her own vote, and it should be secret: no one is able to learn the votes of other people.

Traditional voting schemes using paper and ballot boxes cannot be trusted to guarantee all these security properties. Ballot stuffing, miscounting, and the manipulation or destruction of votes during tallying are possible. Current voting

⋆ Work done while the author was at Universität Karlsruhe (TH).

[1] Grundgesetz Art. 38(1): "Die Abgeordneten des Deutschen Bundestages werden in allgemeiner, unmittelbarer, freier, gleicher und geheimer Wahl gewählt."

A. Alkassar and M. Volkamer (Eds.): VOTE-ID 2007, LNCS 4896, pp. 111–124, 2007.

machines cannot be considered to be a secure solution as studies about machines used in practice [1,2] showed.

These problems led to an increasing interest in voting schemes which allow the voter to verify that her vote was counted. However, such a proof should be meaningful only for the direct recipient, because otherwise coercion and vote buying become substantially simplified. Such schemes are called coercion-free or receipt-free[2].

An additional important requirement for voting schemes is usability. A scheme must be convincing in a very direct way and one cannot expect all voters to use electronic devices apart from the voting machine. This makes the design of a voting scheme even more difficult, because many cryptographic techniques cannot be used to directly convince humans.

Our Contribution

In this work we propose a new voting scheme, called Bingo Voting due to the use of a random number generator, comparable to a bingo cage. The new scheme achieves:

- Ballot casting assurance and universal verifiability, i.e., the voter can check if her own vote is cast and counted as intended, and everyone is able to verify that all votes are correctly counted as recorded on a bulletin board without learning the content.
- Depending on the binding property of the commitments used the scheme offers either everlasting privacy or unconditional correctness.
- Coercion-freeness, i.e., even if the voter deviates from the protocol she does not gain any evidence which allows her to prove anything about the contents of her vote.

Security properties like anonymity or eligibility (i.e., one vote per eligible voter) are, in contrast to purely electronic voting schemes, easily obtained by traditional methods. The authorization is handled in front of the voting booth and an eligible voter may enter once to cast his vote. The voting machine reorders the votes and has to be trusted in order to guarantee anonymity.

The voting scheme offers a very high usability. Only very limited capabilities on the side of the voter are required. The voting process corresponds to the voting with today's voting machines: the voter has to press the button that is assigned to the intended candidate. To ensure the correctness of her vote, the voter only needs to check equality of two random numbers and check if her paper receipt has been posted to a bulletin board. The scheme remains secure if not all voters actually verify the process as long as the attacker cannot predict which voter actually will be verifying.

The security properties listed above are achieved relative to very realistic assumptions:

- A non interactive commitment scheme with some homomorphic properties is needed, e.g., Pedersen commitments [3]. If general zero-knowledge protocols

[2] The term receipt-free might be misleading as the voter indeed obtains a receipt.