Cryptology ePrint Archive: Report 2011/317

Two Simple Code-Verification Voting Protocols

Helger Lipmaa

Abstract: Norwegian nationwide Internet voting will make use of a setting that we will call the code-verification voting. The concrete protocol that will be used in Norway was proposed by Scytl and improved by Gj{\o}steen. As we show, Gj{\o}steen's protocol has several undesirable properties. In particular, one of the online servers shares the secret key with the offline tallier. Even without considering that, the coalition of two online voting servers can breach voter privacy. We propose two new code-verification voting protocols. The first protocol separates the secret keys, and is as efficient as Gj{\o}steen's protocol. The second protocol provides voter privacy against the coalition of online voting servers but is somewhat less efficient. While the new protocols are more secure than the protocol that is going to be used in the Norwegian nationwide Internet voting, they are based on the same setting, so as to minimize the required infrastructural changes.

Category / Keywords: applications / Code-verification voting, Internet voting, malicious voter PC

Date: received 15 Jun 2011

Contact author: helger lipmaa at gmail com