Cryptology ePrint Archive: Report 2011/166

Selections: Internet Voting with Over-the-Shoulder Coercion-Resistance

Jeremy Clark and Urs Hengartner

Abstract: We present Selections, a new cryptographic voting protocol that is end-to-end verifiable and suitable for Internet voting. After a one-time in-person registration, voters can cast ballots in an arbitrary number of elections. We say a system provides over-the-shoulder coercion-resistance if a voter can undetectably avoid complying with an adversary that is present during the vote casting process. Our system is the first in the literature to offer this property without the voter having to anticipate coercion and precompute values. Instead, a voter can employ a panic password. We prove that Selections is coercion-resistant against a non-adaptive adversary.

Category / Keywords: cryptographic protocols / election schemes

Publication Info: Full version of paper appearing at Financial Cryptography 2011.

Date: received 1 Apr 2011, last revised 17 Nov 2011

Contact author: j5clark at cs uwaterloo ca