Cryptology ePrint Archive: Report 2011/517

Verifiability, Privacy, and Coercion-Resistance: New Insights from a Case Study

Ralf Kuesters and Tomasz Truderung and Andreas Vogt

Abstract: In this paper, we present new insights into central properties of voting systems, namely verifiability, privacy, and coercion-resistance. We demonstrate that the combination of the two forms of verifiability considered in the literature---individual and universal verifiability---are, unlike commonly believed, insufficient to guarantee overall verifiability. We also demonstrate that the relationship between coercion-resistance and privacy is more subtle than suggested in the literature.

Our findings are partly based on a case study of prominent voting systems, ThreeBallot and VAV, for which, among others, we show that, unlike commonly believed, they do not provide any reasonable level of verifiability, even though they satisfy individual and universal verifiability. Also, we show that the original variants of ThreeBallot and VAV provide a better level of coercion-resistance than of privacy.

Category / Keywords: cryptographic protocols / voting; verifiability; coercion-resistance; privacy; protocol analysis

Date: received 20 Sep 2011

Contact author: vogt at uni-trier de