Cryptology ePrint Archive: Report 2011/594

Receipt Freeness of Prêt à Voter Provably Secure

Dalia Khader and Peter Y.A. Ryan

Abstract: Prêt à Voter is an end-to-end verifiable voting scheme that is also receipt free. Formal method analysis was used to prove that Prêt à Voter is receipt free. In this paper we use one of the latest versions of Prêt à Voter[XCH+10] to prove receipt freeness of the scheme using computational methods. We use provable security game models for the first time to prove a paper based voting scheme receipt free. In this paper we propose a game model that defines receipt freeness. We show that in order to simulate the game we require IND-CCA2 encryption scheme to create the ballots. The usual schemes used in constructing Prêt à Voter are either exponential ElGamal or Paillier because of their homomorphic properties that are needed for tallying, however both are IND-CPA secure. We propose a new verifiable shuffle ``D-shuffle'' to be used together with an IND-CPA encryption schemes that guarantees that the outputs of the shuffle are IND-CCA2 secure ciphertexts and they are used for constructing the ballots. The idea is based on Naor-Yung transformation[NY95]. We prove that if there exist an adversary that breaks receipt freeness then there exist an adversary that breaks the IND-CCA2 security of Naor-Yung encryption scheme. We further show that the ``D-Shuffle'' provides us with the option of having multiple authorities creating the ballots such that no single authority can break voter's privacy.

Category / Keywords: Provable security, E-Voting, Receipt Freeness

Publication Info: Submitted

Date: received 3 Nov 2011, last revised 20 Jan 2012

Contact author: daliakhader at googlemail com