Cryptology ePrint Archive: Report 2011/325

New Receipt-Free E-Voting Scheme and Self-Proving Mix Net as New Paradigm

Aram Jivanyan and Gurgen Khachatryan

Abstract: The contribution of this paper is twofold. First we present a new simple electronic voting scheme having standard re-encryption mix net back-end, which allows to cast a ballot and verify its correctness in a new way. Then we extend the proposed scheme to represent a new very efficient mix network construction. We called our mix network to be self-proving mix, because it is shown how mix process correctness can be verified without demanding from mix party a special proof. Our proposed mix network allows to reveal all the cheating occurred during a mix process at verification of decryption parties work.

Category / Keywords: cryptographic protocols / election schemes , self-proving mix net, receipt-freeness

Date: received 16 Jun 2011

Contact author: jivanyan at gmail com