A Secure and Efficient Off-line Electronic Transaction Protocol

Constantin Popescu

Department of Mathematics and Computer Science, University of Oradea
Oradea 410087, Romania
cpopescu@uoradea.ro

Abstract: In this paper we propose a secure and efficient off-line electronic transaction protocol based on an ID-based public key encryption system and group signature schemes, which is constructed from bilinear pairings. The anonymity of the customer is revocable by a trustee in case of dispute. Because the amount of communication in the payment protocol is about 1280 bits, our off-line electronic transaction protocol can be used in the wireless networks with the limited bandwidth or the limited-storage environment such as smart card.

Keywords: Cryptography, protocol, electronic cash system, bilinear pairings, group signatures.