Thesis Title	Untraceable Electronic Off-line Cash Payment System
Thesis Credits	12
Candidate	Miss Suphawan Boonchuaidee
Supervisor	Dr. Prasert Kuntamanon
Degree of Study	Master of Science
Department	Information Technology
Academic Year	1999

Abstract

This thesis presents two novel untraceable electronic off-line cash payment protocols which are suitable for off-line payment system such as smart card. The proposed protocols solve double spending problem which is a serious problem of untraceable electronic off-line cash system. Both protocols have different properties. The first protocol provides a mechanism to solve double spending problem by identifying illegal cardholder at the end of process. The second protocol provides a mechanism to prevent double spending problem.

The proposed protocols have better properties than existing ones by comparing in terms of exchanged transactions, total transaction data, and required data storage. Data security in both protocols is also maintained by employing digital signature of Modified DSA (Digital Signature Algorithm) and blind signature of Blind Modified DSA.

Keywords : Untraceable Electronic Off-line Cash/ Digital Signature/ Blind Signature/ Double Spending