Abstract

In this paper, we introduce a new efficient technique allowing to render an off-line e-cash system traceable without need to a trusted party. The main idea is the use of the publicly verifiable secret sharing technique in order to revoke the anonymity of double spending users. The anonymity of honest users is still provided. Security analysis shows that the proposed technique does not undermine the security requirements of a traceable off-line e-cash scheme, including anonymity. A concrete construction of a traceable off-line e-cash system based on a particular blind signature scheme combined with the proposed technique is also given.

Reference

- H. ABELSON, R. ANDERSON, S. BELLOVIN, J. BENALOH, M. BLAZE, W. DIFFIE, J.


**Index Terms**

Computer Science  
Security
Key words

E-cash
Threshold secret sharing

Blind signature