Cryptology ePrint Archive: Report 2013/077

UC-Secure Multi-Session OT Using Tamper-Proof Hardware

Kaoru Kurosawa and Ro Nojima and Le Trieu Phong

Abstract: In this paper, we show the first UC-secure {\it multi-session} OT protocol using tamper-proof hardware tokens. The sender and the receiver exchange tokens only at the beginning. Then these tokens are reused in arbitrarily many sessions of OT. The proposed scheme is UC-secure against static adversaries if the DDH assumption holds and a unique signature scheme exists. There exist a unique signature schemes under the Many DH assumption or under the DDHE assumption (in the standard model).

Category / Keywords: tamper-proof hardware token, UC-security, multi-session OT

Date: received 15 Feb 2013, last revised 23 Apr 2013

Contact author: kurosawa at mx ibaraki ac jp

Available formats: PDF | BibTeX Citation

Note: The random oracle is removed.

Version: 20130424:025104 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]