Cryptology ePrint Archive: Report 2011/305

A new attack on Jakobsson Hybrid Mix-Net

Seyyed Amir Mortazavi

Abstract: The Jakobsson hybrid Mix-net proposed by Jakobsson and Juels, is a very practical and efficient scheme for long input messages. But this hybrid Mix-net does not have public verifiable property. In this paper a new attack to the Jakobsson hybrid Mix-net is introduced. This attack breaks the robustness of the hybrid Mix-net scheme, given that the corrupted first mix server and one of the senders collude with each other.

Category / Keywords: cryptographic protocols / Mix-net, Hybrid Mix-net, Anonymity

Date: received 3 Jun 2011

Contact author: sa mortezavi at gmail com

Available formats: PDF | BibTeX Citation

Version: 20110609:114507 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]