Cryptology ePrint Archive: Report 2011/027

Simple and Efficient Single Round Almost Perfectly Secure Message Transmission Tolerating Generalized Adversary

Ashish Choudhury and Kaoru Kurosawa and Arpita Patra

Abstract: Patra et al. gave a necessary and sufficient condition for the possibility of almost perfectly secure message transmission protocols tolerating general, non-threshold Q^2 adversary structure. However, their protocol requires at least three rounds and performs exponential (exponential in the size of the adversary structure) computation and communication. Moreover, they have left it as an open problem to design efficient protocol for almost perfectly secure message transmission, tolerating Q^2 adversary structure.

In this paper, we show the first single round almost perfectly secure message transmission protocol tolerating Q^2 adversary structure. The computation and communication complexities of the protocol are both polynomial} in the size of underlying linear secret sharing scheme (LSSS) and adversary structure. This solves the open problem raised by Patra et al..

When we restrict our general protocol to threshold adversary with n=2t+1, we obtain a single round, communication optimal almost secure message transmission protocol tolerating threshold adversary, which is much more computationally efficient and relatively simpler than the previous communication optimal protocol of Srinathan et al.

Category / Keywords: cryptographic protocols /

Date: received 12 Jan 2011

Contact author: partho_31 at yahoo co in, partho31@gmail com, kurosawa@mx ibaraki ac jp, arpitapatra_10@yahoo co in, arpitapatra10@gmail com, arpita@cs au dk

Available formats: PDF | BibTeX Citation

Version: 20110114:042137 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]