Two-channel Cryptography

Atefeh Mashatan
Combinatorics and Optimization, University of Waterloo
amashata@uwaterloo.ca

Abstract

In two-channel cryptography, two channels, with different properties in terms of security and cost, are accessible for communication. In general, the more properties one channel has, the more expensive it is to provide, or use, such a channel. The goal of two-channel cryptography is to try to achieve a certain cryptographic goal, such as message authentication, entity authentication, and data confidentiality, by means of the two channels while optimizing the cost.

Applications of two-channel cryptography include pairing of devices in Wireless Personal Area Networks (WPAN), authentication in ad hoc networks, and a disaster case, where a trusted infrastructure has been compromised.