

Cryptographic protocol: security analysis based on trusted freshness

Ling, Dong, editor

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20409957&lokasi=lokal>

Abstrak

This book mainly discusses how to analyze and design cryptographic protocols based on the idea of system engineering and that of the trusted freshness component. A novel freshness principle based on the trusted freshness component is presented; this principle is the basis for an efficient and easy method for analyzing the security of cryptographic protocols. The reasoning results of the new approach, when compared with the security conditions, can either establish the correctness of a cryptographic protocol when the protocol is in fact correct, or identify the absence of the security properties, which leads the structure to construct attacks directly. Furthermore, based on the freshness principle, a belief multiset formalism is presented. This formalism's efficiency, rigorousness, and the possibility of its automation are also presented.