Cryptology ePrint Archive: Report 2011/045

Private Identification, Authentication and Key Agreement Protocol with Security Mode Setup

Farshid Farhat, Somayeh Salimi, Ahmad Salahi

Abstract: Identification, authentication and key agreement protocol of UMTS networks with security mode setup has some weaknesses in the case of mutual freshness of key agreement, DoS-attack resistance, and efficient bandwidth consumption. In this article we consider UMTS AKA and some other proposed schemes. Then we explain the known weaknesses of the previous frameworks suggested for the UMTS AKA protocol. After that we propose a new protocol called private identification, authentication, and key agreement protocol (PIAKAP), for UMTS mobile network. Our suggested protocol combines identification and AKA stages of UMTS AKA protocol while eliminates disadvantages of related works and brings some new features to improve the UMTS AKA mechanism. These features consist of reducing the interactive rounds of the UMTS AKA with security mode setup and user privacy establishment.

Category / Keywords: applications /

Date: received 25 Jan 2011

Contact author: farhat at ee sharif edu

Available formats: PDF | BibTeX Citation

Version: 20110125:145605 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]