Cryptographic protection of classified information in military radio communication faced with threats from quantum computers

Vol. 11442

https://doi.org/10.1117/12.2565467

Book Series: „Proceedings of SPIE”

Abstract: Classified information protection is regulated by dedicated acts and related laws that require use of necessary physical, personal, information and communication technologies, electromagnetic and cryptographic security measures. Equipment and tools for cryptographic protection of classified information should be examined and assessed by the designated government services. Certificates issued by these services authorize the use of cryptographic devices to protect classified information, but this is not a sufficient condition. Each ICT system intended for processing classified information is subject to accreditation. All this makes the process of reaching the right level of protection for this type of information long and expensive – especially if this protection should be effectively provided in the battlefield. Additional specific requirements are put on information protection measures for radio communication, especially military, where radio transmission is characterized by uncertainty of establishing and maintaining connections, bit rates are lower than in cable or fiber optic connections, most often there is no full duplex. All this has an impact on the methods of cryptographic synchronization and implementation of cryptographic functions. A different approach to information protection is required by classic narrowband radio communications, a different one in time-division multi-access mode, and another one in broadband packet data transmission. Systems designed for the protection of classified information in radio communications implement appropriate operating modes of operation for cryptographic algorithms and protocols. Latest threats from quantum computers pose new challenges to the cryptographic protection, especially in systems using public key cryptography, because there are algorithms that can be used to attack public-key schemes with polynomial complexity.

Keywords: classified information protection, cryptography, cryptanalysis, quantum computers

Powiązane publikacje

Society of Photo-Optical Instrumentation Engineers (SPIE).

Adres url strony

https://www.spiedigitallibrary.org/conference-proceedings-of-spie/11442/114420Q/Cryptographic-protection-of-classified-information-in-military-radio-communication-faced/10.1117/12.2565467.full?SSO=1

Plik


PDF