Zabezpieczenia protokołu uzgadniania kluczy sesji przed kryptoanalizą przy wykorzystaniu komputerów kwantowych

Tytuł
Zabezpieczenia protokołu uzgadniania kluczy sesji przed kryptoanalizą przy wykorzystaniu komputerów kwantowych

Typ publikacji
Artykuł

Rok
2019

Data dokładna
2019

Autorzy słownie

Autorzy
Borowski Mariusz Gocałek Jarosław Wicik Robert

ISBN/ISSN
ISSN: 1230-3496, e-ISSN: 2449-7497

Informacje dodatkowe

Przegląd Telekomunikacyjny-Wiadomości Telekomunikacyjne nr 7/2019
DOI: 10.15199/59.2019.7.14
Streszczenie: W celu zapewnienia elastyczności działania systemów telekomunikacyjnych, w których wymagana jest ochrona informacji, wykorzystywane są mechanizmy oparte na kryptografii z kluczem publicznym, m. in. protokoły uzgadniania kluczy sesji do szyfrowania transmisji danych. W związku z zagrożeniem bezpieczeństwa tych protokołów, wynikającym z rozwoju komputerów kwantowych, zaproponowano ich wzmocnienie poprzez zastosowanie tajnych kluczy różnicujących.
Abstract: In order to ensure flexibility in operation of telecommunication systems with information protection, mechanisms based on public key cryptography are used. Due to the security risk of the key agreement protocols by quantum computers, it was proposed to strengthen it by exclusion keys usage.
Słowa kluczowe: ECMQV, komputer kwantowy, kryptografia klucza publicznego, krzywe eliptyczne.
Keywords: ECMQV, elliptic curve, public key cryptography, quantum computer

Powiązane publikacje

-

Adres url strony

https://sigma-not.pl/publikacja-121120-zabezpieczenia-protoko%C5%82u-uzgadniania-kluczy-sesji-przed-kryptoanaliza-przy-wykorzystaniu-komputer%C3%B3w-kwantowych-przeglad-telekomunikacyjny-2019-7.html