Zbiór zestawów algorytmów kryptograficznych typu B wg dokumentu RFC 6379 zabezpieczających protokoły IPSec nie jest odporny na kryptoanalizę kwantową.

Tytuł
Zbiór zestawów algorytmów kryptograficznych typu B wg dokumentu RFC 6379 zabezpieczających protokoły IPSec nie jest odporny na kryptoanalizę kwantową.

Typ publikacji
Artykuł

Rok
2020

Data dokładna
2020

Autorzy słownie

Autorzy
Borowski Mariusz

ISBN/ISSN
ISSN: 1230-3496, e-ISSN: 2449-7487

Informacje dodatkowe
Przegląd Telekomunikacyjny - Wiadomości Telekomunikacyjne, 2020, nr 7-8 + CD, strony 238--241, CD

DOI: 10.15199/59.2020.7-8.23
Referat wygłoszony na:

Krajowa Konferencja Radiokomunikacji, Radiofonii i Telewizji
(17-18.09.2020 ; Łódź, Polska)

Abstrakty:

PL

Dokument RFC 6379 definiuje zbiór czterech zestawów algorytmów kryptograficznych wraz z parametrami bezpieczeństwa do kryptograficznej ochrony korporacyjnych wirtualnych sieci prywatnych VPN. W związku wykorzystaniem asymetrycznego schematu uzgadniania kluczy sesji podatnego na atak z użyciem algorytmu Shora oraz kombinacji obniżonych parametrów bezpieczeństwa algorytmów symetrycznych, informacje zabezpieczane poprzez zdefiniowane tam mechanizmy kryptograficzne, wraz z rozwojem komputerów kwantowych, nie będą odporne na kryptoanalizę przy ich wykorzystaniu.

EN

RFC 6379 defines the collection consisted of four cryptographic algorithms sets with security parameters for protection of corporate virtual private VPNs. Due to the use of an asymmetric key agreement scheme vulnerable to an attack using the Shor algorithm and combination of reduced safety parameters of symmetric algorithms, information secured by the cryptographic mechanisms defined there, along with the development of quantum computers, will not be resistant to cryptanalysis using them.

Słowa kluczowe

PL

ECDH, IPsec, kryptoanaliza kwantowa, złożoność obliczeniowa
EN computational complexity, ECDH, IPsec, quantum, cryptanalysis

Powiązane publikacje

-

Adres url strony
http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-859b9fbe-820c-4a76-8fa3-2584ff9fb391