Michał Glet
Wojskowa Akademia Techniczna

Kryptoanaliza strukturalna sieci SAN

Referat wprowadza czytelnika w świat kryptoanalizy strukturalnej czyli takiej, która bazuje jedynie na metodzie konstrukcji prymitywu kryptograficznego, a nie na jego specyfice wynikającej z implementacji. Dzięki kryptoanalizie strukturalnej możliwe jest na przykład określenie minimalnych wymagań na liczbę rund przy stosowania konkretnych metod projektowania.

W chwili obecnej w świecie kryptologii istnieją dwa główne nurty tworzenia szyfrów blokowych. Pierwszym z nich jest budowanie szyfrów w oparciu o sieci Feistela. W podejściu drugim buduje się prymitywy bazujące na sieciach permutacyjno-podstawieniowych (a w chwili obecnej permutacyjno-afinicznych).

Referat odwołuje się do publikacji Alexa Biryukova i Adi Shamira *Structural Cryptoanalysis of SASAS*, analizuje przedstawioną metodę ataków strukturalnych na szyfry zbudowane z wykorzystaniem sieci SAN (np. AES) oraz prezentuje wyniki implementacji otrzymane przez autora.