

Симметрик блокли шифрлаш алгоритмларининг чизиқли криптотаҳлили

Ўзбекистон миллий Университети

Жўраев Г.У, Шермухаммедов Ж.А
shermuhammedov.j.a@mail.ru

Маълумки блокли шифрлаш алгоритмларини криптотаҳлил қилишнинг турли методлари мавжуд. Буларга мисол қилиб, дифференциал, интеграл чизиқли криптотаҳлилларни келтиришимиз мумкин.

Чизиқли криптотаҳлил – шифрни очиш методи бўлиб, унинг ишлашини тавсифлашда чизиқли яқинлашишлардан фойдаланилади. Чизиқли криптотаҳлил Япон криптологи Мицуру Мацуи томонидан яратилган бўлиб, криптотаҳлилнинг ушбу усули дастлаб DES ва FEAL алгоритмларини очишга қаратилган. Оқибатда чизиқли криптотаҳлил бошқа алгоритмларига қўлланилган. У дифференциал криптотаҳлил сингари шифрларни очиш усуллари орасида энг кўп тарқалган усул ҳисобланади. Унинг ёрдамида симметрик блокли шифрларга ҳужумлар ишлаб чиқилган.

Чизиқли криптотаҳлил икки қадамда амалга оширилади:

- 1–қадам. Очiq матн, шифрограмма ва калит орасида чизиқли муносабатларни ўрнатиш ҳисобланади;
- 2–қадамда эса “Очiq матн – шифрограмма” жуфтлигини олинган муносабатлар билан бирга ишлатиш орқали калит битлари ҳосил қилинади. Ушбу ишда DES симметрик блокли шифрлаш алгоритми учун чизиқли яқинлашишлар куриш ҳамда ушбу шифрлаш алгоритмини чизиқли таҳлил қилишга доир масалалар ўрганилган.

Адабиётлар

1. M. Matsui, "Linear Cryptanalysis Method for DES Cipher", Advances in Cryptology EUROCRYPT '93, Springer-Verlag, pp. 386-397, 1994.
2. K. Nyberg, "Linear Approximations of Block Ciphers", Advances in Cryptology EUROCRYPT '94, Springer-Verlag, pp. 439-444, 1995.