УДК 658.012.011.56:681.3.06
Я.І. Кінах – кандидат технічних. наук, доцент
Тернопільський національний технічний університет імені Івана, Україна

ВИКОРИСТАННЯ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ ДЛЯ ОБҐРУНТУВАННЯ РІВНЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

I.I. Kinakh – Ph.D, Assoc. Prof.

PARALLEL COMPUTING FOR GROUND LEVEL CRYPTOGRAPHIC PROTECTION OF INFORMATION IN COMPUTER NETWORKS

Актуальною науково – технічною задачею є обґрунтування та дослідження рівня криптографічного захисту інформації в комп'ютерних мережах. При цьому особливої значимості набуває задача ефективного захисту від можливої атаки криптоаналітиків на основі паралельних комп'ютенрих алгоритмів.

За оцінками фахівців, протягом найближчого десятиліття основною телекомунікаційною послугою в Україні планується бездротове з'єднання. Тому здійснювати криптоаналіз задіявши все обладнання діючих станцій недоцільно, оскільки за нинішніх умов спроба вдосконалити обслуговування звичайного базового виклику трудомісткіша, ніж надання нових послуг тим користувачам, які їх потребують. Для розв'язку цієї задачі доцільно доповнювати діючі станції мультисервісними вузлами, розрахованими на невелику кількість користувачів, це дозволить залучати більше інформаційних ресурсів для обґрунтування рівня захисту мереж [1].

Реалізація методу сумісного базового використання комп'ютерних мереж для виконання алгоритму загального решета числового поля в повній мірі може бути здійснена на основі концепції розвитку мобільного зв'язку [2]. Концепція призводить до базової тришарової архітектурі паралельного крипто аналізу. Пропонується реалізація методу сумісного паралельного використання базових ресурсів комп'ютерних мереж. Аналіз задач криптоаналізу показує, що для реалізації паралельних обчислень згідно алгоритму загального решета числового поля його функції в повній мірі забезпечують реалізацію криптоаналітичного алгоритму.

Транспортний рівень здійснює управління підзадачами алгоритму загального решета числового поля та виконанням сервісної логіки, забезпечуючи обробку викликів та надання даних та програмного забезпечення на всіх етапах виконання криптоаналітичного алгоритму [3]. До пристроїв цього рівня належать так званий софтсвіч або контролер медіа-шлюзів – MGC та сервер прикладних програм AS. Для реалізації криптоаналізу ці пристрої взаємодіють з пристроями рівнів інформації та сигналізації. Взаємодія між шлюзом та контролером здійснюється через протокол Megaco (H.248) або MGCP, це дозволить проводити ефективний криптоаналіз не змінюючи структури наявної мережі.

Література

[1] Anderson R., Bond M., Clulow J., Skorobogatov, S. Cryptographic processors – a survey (англ.) // Proceedings of the IEEE : журнал. — 2006. — Vol. 94, fasc. 2. —P. 357—369. — ISSN 0018-9219. — DOI:10.1109/JPROC.2005.862423.

[2] Barenghi, A.; Bertoni, G.; Parrinello, E.; Pelosi, G. Low Voltage Fault Attacks on the RSA Cryptosystem (англ.) // Workshop on Fault Diagnosis and Tolerance in Cryptography : сборник. — 2009. — P. 23—31. — ISBN 978-1-4244-4972-9. — DOI:10.1109/FDTC.2009.30.