УДК 004.912
Піх В.В.
(Тернопільський національний технічний університет імені Івана Пулюя)

ОЦІНКА ЕФЕКТИВНОСТІ АЛГОРИТМІВ БЛОКОВО-СИМЕТРИЧНОГО ШИФРУВАННЯ НА ОСНОВІ ВИКОРИСТАННЯ МІНІ-ВЕРСІЙ

UDC 004.912
Pikh V.V.

EVALUATION OF EFFICIENCY OF BLOCK-SYMMETRIC ENCRYPTION ALGORITHMS BASED ON THE USE OF MINI-VERSIONS

Блоково-симетричні шифри (БСШ) опрацьовують інформацію блоками певної довжини, при цьому для шифрування і розшифрування застосовується один і той же криптографічний ключ. Разом з високою швидкістю перетворень і простотою практичної реалізації симетричні криптоалгоритми дозволяють забезпечувати високу стійкість до різних методів криптографічного аналізу. Під ефективністю проектування БСШ розуміється комплексна оцінка алгоритму БСШ, що відображає обґрунтованість і оптимальність вибраних конструкцій для вирішення завдання проектування БСШ, тобто мінімізації апаратних “витрат”, необхідних для забезпечення стійкості алгоритму до атак криптоаналізу [1–3]. Отже, алгоритм може вважатися ефективним, якщо рівень захисту від відомих криптоаналітичних атак може бути досягнутий ціною істотно менших апаратних витрат.

Отримані результати в ході дослідження спрощених версій БСШ для оцінки доказової безпеки повномасштабних моделей шифрів до атак диференціального і лінійного криптоаналізу на основі збільшення розміру входу в шифр підтверджують можливість їх використання. Адекватність результатів оцінки властивостей спрощеної моделі БСШ залежить від вибору коефіцієнта масштабування, який визначає властивості своїх прототипів повних шифрів. Вибір значення коефіцієнта повинен бути пропорційний максимальному ресурсу обчислювальних засобів, що використовуються для проведення досліджень. Для кожного блокового симетричного шифру (з числа відомих ітеративних БСШ) існує цілком визначене число циклів, після якого шифр набуває властивостей випадкової підстановки. Подальше нарощування числа циклів не впливає на підсумкові диференціальні і лінійні властивості шифру. Разом з тим, для збереження всіх властивостей прототипів в спрощених моделях необхідною умовою їх адекватності є використання mini-S-box з основними показниками ефективності нелінійних вузлів замін (збалансованість, нелінійність, автокореляція) на рівні даних показників повномасштабних шифрів.

Література.

1. Oliynykov R. V. Results of Ukrainian national public cryptographic competition / R. V. Oliynykov, I. O. Gorbenko, V. A. Dolgov, V. B. Ruzhentsev // Tatra Mt. Math. Publ. 47. – 2010. – pp. 99–113.
2. 2. Горбенко, И. Д. Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / И.Д. Горбенко, В.И. Долгов, И.В. Лисицкая, Р.В. Олейников // Прикладная радиоэлектроника. – 2010. – Т. 9. № 3. – С. 212-320.
3. Лисицкая И. В. Эксперементальные данные по определению динамических показателей прихода блочных симметричных шифров к состоянию случайности / И.В. Лисицкая, К.Е. Лисицкий, М.Ю. Родинко, И.А. Головко, И.И. Жариков, М.А. Корниенко, М.В. Кулеба// Радіоелектроніка, інформатика, управління. – 2017. – № 1. – С. 129 – 141.