УДК 681.3.06
Р. Козак
(Тернопільський національний технічний університет імені Івана Пулюя)

КЕРОВАНІ ОПЕРАЦІЇ ПІДСТАНОВКИ БЛОКОВИХ ШИФРІВ

Криптографічні перетворення інформації за своєю структури та послідовністю реалізації в блокових шифрах можна представити у вигляді сукупності елементарних або базових криптографічних примітивів.

Криптографічними примітивами, традиційно використовуваними при створенні симетричних криптосистем, є:

- підстановки;
- перестановки;
- арифметичні й алгебраїчні операції;

а також деякі інші допоміжні операції.

Особливо часто застосовують операцію підстановки, що має найбільш загальний характер. Дана операція є тим криптографічним примітивом, на якому ґрунтується стійкість більшості блокових шифрів.

При оцінці якості будь-яких криптографічних примітивів варто враховувати сукупність наступних трьох основних параметрів, що визначають стійкість шифрів до різних методів криптоаналізу:

- ступеня нелінійності;
- ступеня поширення змін (помилок);
- рівня кореляційної іммунності.

Аналізуючи загалом перераховані властивості для підстановочних примітивів, варто мати на увазі, що S-блоки призначені забезпечити задану в межах кожного S-блоку ступінь нелінійності та ступінь поширення (розповсюдження) помилок. Разом з тим, досить проблематичним є досягнення високих показників одночасно за усіма трьома параметрами у відношенні всього перетворюваного блоку даних з використанням серії S-блоків малого розміру.

З іншого боку, ефективно реалізовані програмно та нескладні при апаратній реалізації математичні операції (XOR і додавання за модулем 2^n) мають високу кореляційну іммунність для всього перетворюваного блоку даних, але мають невисокий ступінь нелінійності й поширення змін.

Тому, очевидною є перспектива створення спеціальних криптографічних примітивів, що поєднують і оптимізують позитивні властивості використовуваних у блокових шифрах підстановочних перетворень.

Іншим важливим напрямком вдосконалення криптографічних примітивів є підвищення їхнього ступеня невизначеності за рахунок збільшення розмірів блоку перетворюваних даних і введення додаткових параметрів, що визначають результати перетворень і модифікацій, які збільшують їх кількість. Зокрема, зазначена ідея може бути реалізована у вигляді спеціальних операцій, додатково керованих деякими псевдовипадковими векторами, що залежать від перетворюваних даних і ключів шифру, – керованих перетворень.

За своїм змістом і суттю керовані операції підстановки є спеціально проектованими операціями криптографічної орієнтації, виконуваними над двома й більше двійковими векторами. Будуються такі операції за певним правилом, що дозволяє розробляти операції для перетворення двійкових векторів довільного розміру.

Практика створення сучасних блокових шифрів показує, що використання керованих перетворень є перспективним напрямком проектування нових криптографічних примітивів. Однак пропоновані нові криптографічні примітиви не розглядаються як ідеальні конструкції, що є повною альтернативою іншим методам криптографічних перетворень.