Олейников Р.В.
Харьковский национальный университет радиоэлектроники, Харьков, Украина

Анализ свойств перспективной схемы разворачивания ключей для блочных симметричных алгоритмов шифрования

Блочные симметричные алгоритмы шифрования являются одними из наиболее широко распространённых криптографических примитивов. Помимо обеспечения конфиденциальности, блочные алгоритмы используются в составе хэш-функций, генераторов псевдослучайных последовательностей и др.

Современные блочные алгоритмы имеют итеративную структуру: слабое криптографическое преобразование (цикловая функция) повторяется заданное количество раз для получения стойкого шифра. Для введения неопределенности криптоаналитика цикловая функция параметризуется раундовым ключом, который формируется из ключа шифрования.

Свойства схемы разворачивания ключей имеют важное значение для обеспечения стойкости шифра к различным криптоаналитическим атакам. В частности, известные атаки на AES [1] используют слабый лавинный эффект в схеме разворачивания.

Для перспективных алгоритмов предлагается использование новой схемы, обеспечивающей следующие свойства: нелинейная зависимость битов раундовых ключей от ключа шифрования; высокая вычислительная сложность получения ключа шифрования по одному или нескольким раундовым ключам; вычислительная сложность формирования всех раундовых ключей не превышает сложности зашифрования одного блока. Процедура генерации может быть описана следующим образом:

$$K_i = \sigma_{K_M} \circ \prod_{j=1}^{t} \theta \circ \pi \circ \gamma \circ \sigma_{K_M}, \qquad (1)$$

где σ_{K_M} – сложение с ключом шифрования; γ – блок нелинейного преобразования; π, θ – блоки линейного преобразования. Количество итераций t выбирается в зависимости от свойств распространения блоков линейного и нелинейного преобразований. В качестве входного значения функции генерации используется некоторая константа.

Как было показано в предыдущей работе [2], такая схема потенциально является небиективной, что может привести к уменьшению мощности множества раундовых ключей, и, соответственно, появлению эквивалентных ключей шифрования.

Соотношение (1) можно представить как некоторое случайное отображение $y = x \oplus \lambda(x)$. Условием появления коллизионного раундового ключа является выполнение $x \oplus \lambda(x) = x' \oplus \lambda(x')$ при $x \neq x'$, или $x \oplus x' = \lambda(x) \oplus \lambda(x')$. Нелинейность отображения λ обеспечивает возможность появления лишь случайных коллизий. Оценка математического ожидания количества коллизий для одного раундового ключа и для всей схемы разворачивания дают крайне малую вероятность появления эквивалентных ключей.

Таким образом, рассмотренная схема разворачивания ключей для блочных симметричных шифров обладает заявленными свойствами и обеспечивает защиту алгоритма от криптоаналитических атак.

Литература

1. Biryukov A. Related-key cryptoanalysis of the full AES-192 and AES-256 [Electronic resource] / A. Biryukov, D. Khovratovich. Mode of access: WWW.URL: https://cryptolux.org/mediawiki/uploads/1/1a/Aes-192-256.pdf – Last access: 2010. – Title from the screen.
2. Р. Олейников. Анализ свойств схемы разворачивания ключей алгоритма шифрования “Калина” / 12-ая Международная конференция “Безопасность информации в информационно-телекоммуникационных системах”. – К.: НИЦ “ТЕЗИС” НТУУ “КПИ”, 2009.