УДК 004.056.55

ОЦЕНКА КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ ШИФРА КУЗНЕЧИК ПРИ АТАКАХ МЕТОДОМ НЕВОЗМОЖНЫХ ДИФФЕРЕНЦИАЛОВ

Ниткин И.С.
Научный руководитель – к.т.н. Таранов С.В.
Университет ИТМО

В ходе работы дана оценка криптографической стойкости блочного симметричного шифра Кузнечик при атаках методом невозможных дифференциалов. Набор шагов, необходимый для проведения указанной оценки систематизирован в виде расширенной методики оценки криптографической стойкости шифра Кузнечик при атаках методом невозможных дифференциалов.

ГОСТ 34.12-2018 «Информационная технология. Криптографическая защита информации. Блочные шифры», который утверждает в качестве одного из вариантов стандарта блочный симметричный шифр Кузнечик. С 1 января 2022 года реализация алгоритмов ГОСТ 34.12-2018 обязательна для прохождения процедуры сертификации ФСБ России.
В открытых источниках отсутствуют публикации об оценке криптографической стойкости шифра Кузнечик при атаках методом невозможных дифференциалов. Однако, атаки методом невозможных дифференциалов реализуемы в отношении отдельных сокращенных версий шифров и, в перспективе развития вычислительной техники, достижимы для полных версий шифров.
Автором была представлена методика оценки криптографической стойкости шифра Кузнечик при атаках методом невозможных дифференциалов. По результатам исследований, была установлена оценка криптографической стойкости при атаках методом невозможных дифференциалов на уровне полного перебора значений ключа шифрования.
Представленная методика предусматривает разработку упрощенной версий шифра Кузнечик, в отношении которой проводятся исследования. При построении невозможных дифференциалов рассматриваются дифференциальные последовательности в обобщенном до полубайтовых структур дифференциалов виде. Сделан вывод, что применение подобного подхода не позволяет построение невозможных дифференциалов как для упрощенной, так и для полной версии шифра Кузнечик.

Настоящая работа является продолжением исследований автора по оценке криптографической стойкости шифра Кузнечик.
С целью уточнения оценки криптографической стойкости шифра Кузнечик при атаках методом невозможных дифференциалов проводится углубленное исследование упрощенной версии шифра Кузнечик.
Упрощенная версия шифра Кузнечик имеет сокращенный, относительно полной версии размер блока и ключа шифрования, уменьшенное количество раундов шифрования. При этом преобразования упрощенной версии имеют структуру, соответствующую преобразованиям полной версии шифра Кузнечик.
В рамках настоящего исследования построение невозможных дифференциальных последовательностей упрощенной версии шифра Кузнечик производится для дифференциалов в общем виде, необобщенном до дифференциальных полубайтовых структур.
По результатам, предлагаются два алгоритма построения невозможных дифференциалов: алгоритм на основе способа «промах посередине» и алгоритм на основе перебора всех возможных значений входных дифференциалов для четырех раундов шифрования.
На основе полученных невозможных дифференциалов разработан алгоритм проведения атаки методом невозможных дифференциалов в отношении упрощенной версии шифра Кузнечик.

Проведена оценка вычислительной сложности указанной атаки, оценка необходимого объема памяти, для реализации атаки по указанному алгоритму.
На основе полученных сведений дана оценка криптографической стойкости упрощенной версии шифра Кузнечик при атаках методом невозможных дифференциалов.
Полученные результаты обобщены для оценки криптографической стойкости полной версии шифра Кузнечик.

Таким образом, по результатам исследования получена обновленная оценка криптографической стойкости шифра Кузнечик при атаках методом невозможных дифференциалов.
Проделанный набор шагов систематизирован в виде расширенной методики оценки криптографической стойкости шифра Кузнечик при атаках методом невозможных дифференциалов.
Указанная методика может быть обобщена для оценки криптографической стойкости блочных симметричных шифров.

Ниткин И.С. (автор) Подпись

Таранов С.В. (научный руководитель) Подпись