РАЗДЕЛЕНИЕ КЛЮЧЕВОГО ПРОСТРАНСТВА СИММЕТРИЧНЫХ ШИФРОВ НА ОСНОВЕ УСЕЧЕННОЙ ИНТЕРПОЛЯЦИОННОЙ ОЦЕНКИ ТЕСТОВОЙ ХАРАКТЕРИСТИКИ

С.Б. САЛОМАТИН, Д.М. БИЛЬДЮК

Надежность симметричных алгоритмов шифрования характеризуется безопасным временем, которое определяет устойчивость криптоалгоритма к использованию метода прямого перебора для отыскания ключа. Если длина ключа составляет n бит, то метод прямого перебора требует проведения порядка 2^n операций криптоанализа. Существуют методы дифференциального и линейного криптоанализа, позволяющие исключить из рассмотрения значительную часть вариантов ключа, что приводит к уменьшению вычислительной сложности криптоанализа по сравнению с прямым перебором. Однако данные методы не эффективны при анализе шифров типа AES.

Один из путей ускорения криптоанализа состоит в разделении множества ключевых комбинаций на классы по форме кривой усеченной интерполяционной оценки тестовой характеристики симметричного шифра.

Тестовая характеристика шифра представляла собой отклик шифра на воздействие импульсных информационных кодов, при заданной форме ключа.

Усеченная интерполяционная оценка выполнялась по методу Бен–Ор–Тивари с использованием алгоритма Берлекампа–Месси и исключением последнего этапа решения системы уравнений. Результат интерполяционных преобразований отображался в виде кривой визуализации.

Результаты моделирования. Исследовались шифры AES и ГОСТ 28147. Моделирование алгоритмов показало, что ключевое пространство криптосистем можно разделить на классы по следующим признакам: кривые визуализации параболического типа разного масштаба и отсутствие решения алгоритма Берлекампа–Месси.

Полученный результат позволяет использовать разделение ключевого пространства для ускорения процесса криптоанализа.