Современные технологии проектирования блочных симметричных шифров

УДК 004.056.55 Александр Кузнецов[1], Бахытжан Ахметов[2], Анар Ташимова[2]

[1] Харьковский национальный университет имени В.Н. Каразина, kuznetsov@karazin.ua

[2] Казахский национальный исследовательский технический университет имени К.И. Сатпаева, bakhytzhan.akhmetov.54@mail.ru

Основным и наиболее эффективным механизмом криптографической защиты информации являются методы блочного симметричного криптографического преобразования. Наряду с высокой скоростью и простотой практической реализации симметричные криптоалгоритмы позволяют обеспечить высокую стойкость к различным методам криптографического анализа.

Известные на сегодняшний день результаты в области проектирования, разработки, исследования, стандартизации, введения в действие и непосредственного использования моделей, методов и вычислительных алгоритмов блочного симметричного криптопреобразования составляют научно-методологическую и проектно-технологическую основу современных стандартизированных на международном и национальных уровнях алгоритмов и режимов симметричного шифрования. Например, принятый в конце 2001 года Национальным институтом стандартов и технологий (NIST) США Федеральный Стандарт Обработки Информации FIPS-197 определяет спецификацию нового алгоритма блочного симметричного шифрования Advanced Encryption Standard (AES), также известного как Rijndael. Необходимость в принятии нового стандарта США была вызвана небольшой длиной ключа существующего стандарта DES (56 бит), что теоретически позволяло применить метод грубой силы (полный перебор ключей) против этого алгоритма. Кроме того, архитектура DES была ориентирована на аппаратную реализацию, и программная реализация алгоритма на платформах с ограниченными ресурсами не давала достаточного быстродействия. Новый алгоритм был выбран в результате открытого криптографического конкурса, в ходе которого на протяжении пяти лет (1997-2001) проводились всесторонние масштабные исследования в области проектирования современных блочных криптоалгоритмов, разработки методики статистического тестирования, имплементации основных криптопримитивов в программном и аппаратном виде на различных вычислительных платформах, обоснования критериев и показателей эффективности, разработки моделей безопасности, угроз и злоумышленников и многое другое. Накопленные в ходе проведения конкурса AES теоретические и практические результаты существенно расширили используемый научно-методологический аппарат в области проектирования, разработки и внедрения симметричных криптоалгоритмов, а спецификация шифра FIPS-197 фактически установила новый мировой стандарт шифрования 21 века. На сегодняшний день алгоритм AES стандартизирован на международном уровне в ISO/IEC 18033-3 и является одним из самых

распространённых в мире алгоритмов симметричного шифрования, который поддерживают многие производители современных вычислительных систем. Тем не менее, многочисленные исследования за прошедшие 15 лет со дня его утверждения выявили ряд существенных недостатков, в частности:

- развитие методов алгебраического криптоанализа и их практическая реализация в виде эффективных вычислительных алгоритмов позволили получить существенный прогресс в решении разреженных и структурированных алгебраических уравнений, связывающих открытый и закрытый текст с битами секретного ключа симметричных шифров. Алгоритм шифрования AES с чрезвычайно простой алгебраической структурой применяемых нелинейных узлов замен наиболее подвержен подобным атакам, его криптоанализ рассматривается как наиболее вероятное применение разработанных методов решения разреженных и структурированных алгебраических уравнений;

- ключевое расписание шифра AES уязвимо к современным атакам на связанных ключах. В частности, в известных работах предложена первая криптоаналитическая атака на основе связанных ключей на полнораундовые шифры AES-192 и AES-256 (варианты FIPS-197 с длиной ключа 192 и 256 бит). Такая атака эффективнее полного перебора мастер-ключей, т.е. можно с уверенностью утверждать о реальном снижении стойкости стандартизированного на международном уровне криптоалгоритма;

- развитие квантовых вычислительных систем и методов квантового криптоанализа вынуждает пересматривать основные параметры современных криптоалгоритмов. Для симметричных шифров применение квантовых методов криптоанализа чревато снижением стойкости, которое эквивалентно снижению длинны секретного ключа (размера блока банных) в 2 раза. В этом смысле, алгоритм AES нуждается в модернизации или подлежит замене на т.н. пост-квантовые криптоалгоритмы, эффективно функционирующие и в условиях применения квантовых методов криптоанализа.

За разработку и исследования перспективных методов криптографической защиты на постсоветском пространстве традиционно отвечают специальные службы соответствующих стран, большая часть работ в данной области оставалась до недавнего времени закрытой для публичного ознакомления. Однако в последние годы национальными правительствами и ответственными органами постсоветских стран перенимается передовой опыт проведения открытых конкурсов криптографических алгоритмов и публичного обсуждения полученных результатов исследований. В качестве примера можно привести проведенный в конце прошлого десятилетия в Украине открытый конкурс симметричных блочных шифров. На основе результатов проведенного конкурса в конце 2014 года в Украине был принят новый стандарт блочного криптопреобразования ДСТУ 7624:2014, в котором устранена большая часть недостатков и уязвимостей алгоритма AES. В Российской Федерации и в Республике Беларусь также приняты новые стандарты шифрования ГОСТ Р 34.12-2015 и СТБ 34.101.31-2011, которые учитывают передовой опыт разработки и исследования криптографических систем.