УДК 004.056.55

Обзор и сравнение легковесных модификаций шифра AES для сети маломощных устройств

Березовская О.И. (Университет ИТМО)
Научный руководитель – к.т.н., доцент Таранов С.В.
(Университет ИТМО)

Аннотация. В современных реалиях развитие умного города и киберфизических систем невозможно без обеспечения достаточного уровня защиты информации. В условиях ограниченных ресурсов, когда объем памяти, вычислительную мощность и запас заряда батареи/аккумулятора устройства нельзя увеличить без увеличения его стоимости, необходимо соблюдать баланс между криптостойкостью алгоритма шифрования и налагаемыми им требованиями. В рамках исследования было произведено сравнение легковесных модификаций симметричного блочного шифра AES для выявления наиболее сбалансированного решения.

Введение. Симметричные блочные шифры считаются наиболее энергоэффективными и наименее требовательными к аппаратной составляющей по сравнению с поточными или асимметричными. Криптосистема AES используется в таких протоколах беспроводной связи, как Bluetooth Low Energy, ZigBee, Thread и Z-Wave. Существует множество облегченных модификаций этого алгоритма, однако отсутствует их сравнительный анализ - не только со стандартным алгоритмом, но и между собой.

Основная часть. С точки зрения криптографии, конфузия и диффузия являются двумя свойствами, затрудняющими криптоанализ. Конфузия - метод, отвечающий за усложнение зависимости ключа и выходных данных, диффузия - распределяет избыточность в статистике открытого текста по всей структуре выходных данных.
В ходе работы был предложен набор критериев оценки алгоритмов шифрования на основе статистических тестов NIST. Он может быть расширен для сравнения не только криптостойкости, но и накладных расходов реализации шифра, таких как потребление памяти и временных ресурсов. Различные легковесные модификации AES были подвержены тестированию и сравнению в соответствии с этими критериями, в результате чего был сделан вывод о достоинствах и недостатках их уровней, отвечающих за конфузию и диффузию.

Выводы. Результаты исследования будут полезны при разработке легковесной модификации шифра AES с учетом оценки существующих решений. В качестве следующего этапа исследований планируется реализация новой модификации, ее сравнение со стандартом и аналогами при помощи того же набора критериев.

Березовская О.И. (автор) Подпись

Таранов С.В. (научный руководитель) Подпись