Секция «Дискретная математика и математическая кибернетика»

О глубине аппаратной реализации блочного шифра Кузнечик

Курганов Евгений Александрович

Аспирант

Московский государственный университет имени М.В.Ломоносова,
Механико-математический факультет, Кафедра математической теории
интеллектуальных систем, Москва, Россия

E-mail: kuev@yandex.ru

Блочный шифр Кузнечик является частью нового стандарта блочного шифрования в РФ ГОСТ 34.12-2015 [2]. В работе исследуется вопрос оптимизации аппаратной (схемной) реализации данного алгоритма по глубине. Под глубиной понимается длина максимального простого пути схемы. Рассматривается базис из элементов конъюнкции, дизъюнкции, отрицания и задержки. При этом отрицание игнорируется при вычислении глубины (вычисление проводится по тем же правилам, что и в [1]).

По своей структуре новый шифр — это SP-сеть, которая состоит из 9 одинаковых раундов и еще одного дополнительного сложения с раундовым ключом. Один раунд данной сети имеет следующую структуру:

1) побитовое сложение (XOR) с раундовым ключом K_i;
2) нелинейное преобразование блоком подстановок S;
3) линейное преобразование L.

Предложен универсальный способ реализации S-блока размера 8 на 8 бит на основе СДНФ [3] с глубиной 10. Также показано, что линейное преобразование алгоритма Кузнечик может быть реализовано несколькими способами: при помощи линейного регистра сдвига с обратной связью, при помощи умножения матрицы на вектор в поле Галуа $GF(2^8)$ и при помощи умножения матрицы на вектор в поле $GF(2)$. При этом оптимальным по глубине является последний способ.

Далее приводится сравнение глубины алгоритма Кузнечик с другими распространенными алгоритмами блочного шифрования: Магма [2], AES [4], DES [5], 3DES [5].

Источники и литература

1) Болотов А. А., Галатенко А. В., Гринчук М. И., Золотых А. А., Иванович Л. Методы оптимизации глубины реализации хэш-функций // Интеллектуальные системы. 2013. No 17:1-4. С. 224–228
2) ГОСТ. Криптографическая защита информации. Блочные шифры. Государственный стандарт РФ, 2015.
3) Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. Москва; Наука, 1966.
4) NIST, FIPS PUB 197, 2001.
5) NIST, FIPS PUB 46-3, 1999.

Слова благодарности

Автор выражает благодарность своему научному руководителю старшему научному сотруднику Галатенко А. В. за постановку задачи и внимание к работе.