УДК 519.7 DOI 10.17223/2226308X/9/19

ОЦЕНКИ СТОЙКОСТИ ШИФРОВ СЕМЕЙСТВА TRIVIUM К КРИПТОАНАЛИЗУ НА ОСНОВЕ АЛГОРИТМОВ РЕШЕНИЯ ПРОБЛЕМЫ БУЛЕВОЙ ВЫПОЛНИМОСТИ[1]

О. С. Заикин, И. В. Отпущенников, А. А. Семёнов

Представлены результаты криптоанализа трёх поточных шифров семейства Trivium (Bivium, Trivium toy, Bivium toy). Криптоанализ осуществляется за счёт сведения обращения соответствующих дискретных функций к задаче о булевой выполнимости (SAT). Криптоанализ неослабленного шифра Bivium toy удалось осуществить на персональном компьютере. Задачи криптоанализа шифров Bivium и Trivium toy оказались более сложными, в связи с чем исследованы их ослабленные варианты. Соответствующие SAT-задачи были решены на вычислительном кластере и проекте добровольных распределённых вычислений SAT@home. При этом использована предложенная ранее техника распараллеливания по данным, согласно которой из множества переменных пропозициональной кодировки рассматриваемой задачи специальным образом выбирается некоторое подмножество, по которому исходная задача разбивается на независимые подзадачи.

Ключевые слова: *поточный шифр, шифр Trivium, шифр Bivium, криптоанализ, задача о булевой выполнимости.*

В [1] предложен поточный шифр Trivium, который состоит из трёх сдвиговых регистров специального вида. Первый из них включает 93 ячейки, второй — 84, третий — 111 ячеек (суммарная длина состояний регистров Trivium равна 288 битам). Trivium принимал участие в конкурсе eSTREAM и стал одним из победителей в «аппаратной» категории. С исследовательскими целями параллельно с Trivium его автор ввёл в рассмотрение шифр Bivium, в котором используются только два первых регистра Trivium.

В работе [2] выполнен скрупулёзный анализ возможных слабостей Trivium и Bivium. Как результат, описана атака, основанная на алгоритме восстановления внутренних состояний регистров, эксплуатирующем особенности уравнений шифрования рассматриваемых шифров. Сложность этой атаки для Bivium оказалась существенно меньше сложности полного перебора ключевого пространства. Несмотря на это, данная атака, к сожалению, плохо подходит для практической реализации из-за очень больших констант в оценке эффективности лежащего в её основе алгоритма. В работе [3] впервые было предложено использовать для криптоанализа Bivium SAT-подход. В [4 – 7] предложены последовательно улучшающиеся оценки времени SAT-криптоанализа Bivium. В [7] описана техника распараллеливания SAT, основанная на стохастическом оценивании времени обработки декомпозиционных множеств. Данная техника в применении к Bivium дала рекордную на настоящий момент оценку времени его криптоанализа.

В [8] введены в рассмотрение т. н. «игрушечные» версии шифров Trivium и Bivium — соответственно Trivium toy и Bivium toy. Авторы [8] позиционировали эти шифры как объекты для применения к ним новых методов криптоанализа, которые, возможно, будут полезны в дальнейшем при исследовании «полновесных» шифров.

[1]Работа частично поддержана РФФИ (гранты №14-07-00403-а, 15-07-07891-а и 16-07-00155-а) и советом по грантам Президента РФ (стипендия №СП-1184.2015.5).

В работе представлены результаты SAT-криптоанализа шифров Bivium, Bivium toy и Trivium toy. На примере криптоанализа Bivium продемонстрирована техника распараллеливания SAT, кратко описанная в [7]. Результаты криптоанализа Bivium toy и Trivium toy являются полностью новыми. Для сведения к SAT задач криптоанализа перечисленных шифров использован программный комплекс Transalg [9, 10]. Декомпозиционные представления получаемых SAT-задач обрабатывались посредством параллельного SAT-решателя PD-SAT [6].

Шифр Trivium toy получен из шифра Trivium уменьшением длины каждого регистра в 3 раза. Соответственно первый его регистр состоит из 31 ячейки, второй — из 28, третий — из 37 ячеек. Шифр Bivium toy, в свою очередь, получен из шифра Trivium toy отбрасыванием третьего регистра (по аналогии с построением Bivium на основе Trivium). Таким образом, задача криптоанализа (восстановления состояний регистров) Trivium toy заключается в нахождении 96 бит, а для Bivium toy — 59 бит.

Криптоанализ Bivium toy оказался очень простым — для его успешной реализации не потребовалось даже распараллеливать соответствующую SAT-задачу. Всего с помощью обычных (последовательных) SAT-решателей решено 10 задач криптоанализа Bivium toy в описанной постановке. Лучшие результаты при этом показал SAT-решатель rokk (один из призёров конкурса SAT Competition 2014): среднее время его работы на одном ядре процессора AMD Opteron 6276 составило около 2 мин.

Криптоанализ шифра Bivium кратко описан в [7]. Последние результаты в этом направлении заключаются в следующем. Для данного шифра удаётся осуществлять вариант «guess-and-determine»-атаки [11], в которой предполагаются известными значения 9 бит в последних ячейках второго регистра Bivium. Таким образом, требуется восстановить 168 неизвестных бит заполнения регистров Bivium (их суммарная длина равна 177 бит). При этом анализируются 200 бит ключевого потока. На решение данной задачи техникой, описанной в [7], уходит в среднем две недели работы проекта добровольных вычислений SAT@home.

В неослабленном варианте шифр Trivium toy оказался весьма стойким к SAT-криптоанализу. Это лишний раз подчёркивает, насколько удачны идеи, на которых он построен. Мы рассматривали задачу восстановления состояния регистров Trivium toy на основе 100 известных бит ключевого потока. На текущем этапе за приемлемое время удаётся осуществлять лишь вариант «guess-and-determine»-атаки, в которой известными предполагаются биты восстанавливаемого состояния, находящиеся в первых 16 ячейках второго регистра. Таким образом, в данной постановке необходимо найти оставшиеся 80 из 96 бит начального заполнения регистров. Решено 5 таких задач. Для решения каждой использовался решатель PD-SAT, обрабатывающий декомпозиционное семейство, построенное по 31 переменным, кодирующим первый регистр Trivium toy. Все эти задачи успешно решены на вычислительном кластере ИНЦ СО РАН «Академик В. М. Матросов». В среднем на каждую задачу потребовалось около суток работы двадцати 16-ядерных процессоров AMD Opteron 6276 (т. е. 320 процессорных ядер).

ЛИТЕРАТУРА

1. *Canniere C. D.* Trivium: A stream cipher construction inspired by block cipher design principles // LNCS. 2006. V. 4176. P. 171–186.
2. *Maximov A. and Biryukov A.* Two trivial attacks on Trivium // SAC'07. LNCS. 2007. V. 4876. P. 36–55.

3. *Mcdonald C., Charnes C., and Pieprzyk J.* Attacking Bivium with MiniSat. Technical Report 2007/040. ECRYPT Stream Cipher Project, 2007.
4. *Eibach T., Pilz E., and Volkel G.* Attacking Bivium using SAT solvers // LNCS. 2008. V. 4996. P. 63–76.
5. *Soos M., Nohl K., and Castelluccia C.* Extending SAT solvers to cryptographic problems // LNCS. 2009. V. 5584. P. 244–257.
6. *Заикин О. С., Семенов А. А.* Применение метода Монте-Карло к прогнозированию времени параллельного решения проблемы булевой выполнимости // Вычислительные методы и программирование: новые вычислительные технологии. 2014. Т. 15. № 1. С. 22–35.
7. *Semenov A. A. and Zaikin O. S.* Using Monte Carlo method for searching partitionings of hard variants of Boolean satisfiability problem // LNCS. 2015. V. 9251. P. 222–230.
8. *Lechtaler A. C., Cipriano M., Garcia E., et al.* Model design for a reduced variant of a Trivium type stream cipher // J. Computer Science & Technology. 2014. V. 14. No. 1. P. 55–58.
9. *Отпущенников И. В., Семенов А. А.* Технология трансляции комбинаторных проблем в булевы уравнения // Прикладная дискретная математика. 2011. № 1. С. 96–115.
10. *Otpuschennikov I. V., Semenov A. A., and Kochemazov S. E.* Transalg: a tool for translating procedural descriptions of discrete functions to SAT // Proc. 5th Intern. Workshop on Computer Science and Engineering: Information Processing and Control Engineering (WCSE 2015-IPCE). 2015. P. 289–294.
11. *Bard G. V.* Algebraic Cryptanalysis. Springer, 2009.

УДК 519.1 DOI 10.17223/2226308X/9/20

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ЭКСПОНЕНТОВ РАУНДОВЫХ ПЕРЕМЕШИВАЮЩИХ МАТРИЦ ОБОБЩЁННЫХ СЕТЕЙ ФЕЙСТЕЛЯ

А. М. Коренева, В. Н. Мартышин

Исследованы перемешивающие свойства раундовых функций обобщённых сетей Фейстеля, построенных на основе регистров сдвига длины 4 над множеством двоичных 32-мерных векторов. Рассмотрены регистровые функции с различным числом обратных связей регистра. Приведены результаты экспериментального исследования, направленного на выбор параметров регистровых функций, при которых реализуется наиболее быстрое перемешивание входных данных.

Ключевые слова: *обобщённая сеть Фейстеля, раунд шифрования, перемешивающая матрица, экспонент матрицы.*

Введение

Обозначим через $R(n, r, k)$ класс регистров сдвига длины n над множеством V_r двоичных r-мерных векторов с k обратными связями, $n, r > 1$, $k \geqslant 1$. Класс $R(n, r, k)$ обобщает класс $R(2, r, 1)$, относящийся к оригинальным сетям Фейстеля.

Увеличение длины базового регистра способствует увеличению производительности шифрования и вместе с тем числа раундов, достаточного для перемешивания входных данных. Свойства обобщённых сетей Фейстеля (ОСФ) исследовались как в зарубежных [1 – 4], так и в отечественных работах [5 – 7]. На основе ОСФ построены алгоритмы CAST-256, MARS, SMS4, CLEFIA, Piccolo, HIGHT и др. В [3] исследованы классы сетей $R(n, r, n/2)$, n — чётное (эти сети названы обобщёнными сетями Фейстеля 2-го типа). Отмечено, что вычислительная реализация таких сетей допускает распараллеливание и количество раундов, необходимых для перемешивания входных