УДК 519.7

А.В. ГОДОВ, К.В. АНТОНОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ОБ АЛГЕБРАИЧЕСКОМ КРИПТОАНАЛИЗЕ TRIVIUM-ПОДОБНЫХ АЛГОРИТМОВ ПОТОЧНОГО ШИФРОВАНИЯ

Задача восстановления секретного ключа алгоритма поточного шифрования может быть эффективно сведена к задаче смешанного целочисленного линейного программирования (ЦЛП). В работе предлагается комбинация методов ЦЛП и атак из класса «угадывай и определяй», а именно техники вероятностных лазеек. При помощи указанного подхода производится оценка стойкости Trivium-подобных алгоритмов поточного шифрования в сценарии атаки по подобранным значениям векторов инициализации.

Одной из NP-трудных задач является задача смешанного целочисленного линейного программирования (ЦЛП) – задача оптимизации вещественнозначной линейной функции при условии целочисленности некоторых её аргументов и выполнимости ряда линейных ограничений. Для решения ЦЛП существует множество программных средств (решателей), таких как Gurobi [1], CPLEX [2], SCIP [3].

Описываемые в работе атаки на основе решателей задачи ЦЛП принадлежат к классу «угадывай и определяй». Конкретно, к подходу на основе ЦЛП адаптированы атаки IBS [4], которые используют понятие вероятностных лазеек. Говоря неформально, вероятностной лазейкой в алгебраической задаче называется набор переменных, подстановка значений которых упрощает задачу так, что её можно эффективно решить с ненулевой вероятностью. В работе впервые предлагается применить комбинированный подход в криптоанализе: атаки на основе вероятностных лазеек с применением методов ЦЛП.

Объектом криптоанализа являются Trivium-подобные алгоритмы поточного шифрования, редуцированные по числу шагов инициализации: Trivium [5] и Bivium-A [6]. Схема Trivium построена на основе регистров сдвига, зашифрование происходит путём наложения на открытый текст гаммы, получаемой из секретного ключа и несекретного вектора инициализации. Рассматриваем несколько сценариев атаки:

1) восстановление неизвестного состояния регистров, гамма считается известной;

2) восстановление ключа по известному фрагменту гаммы, значение вектора инициализации известно, но выбирается случайно равновероятно;

3) восстановление ключа по подобранным значениям векторов инициализации: у криптоаналитика имеется возможность получить фрагменты гаммы для искомого секретного ключа и любых выбранных значений векторов инициализации.

В экспериментах использовался решатель SCIP [3]. Поиск оптимальной по трудоёмкости атаки проводился при помощи модифицированного алгоритма 1+1 на вычислительном кластере МИФИ [7]. Для Bivium-A были построены атаки на полную версию алгоритма (708 шагов), у Trivium же в спецификации 1152 шага, и атаки построены на редуцированные версии. Трудоёмкости построенных атак приведены в табл. 1 и 2.

Таблица 1. Трудоёмкость атак на Bivium-A

Сценарий атаки	Вероятность успеха атаки	Трудоёмкость атаки, с.
2	0,05	2^{74}
1	0,57	2^{8}
1	1	2^{29}

Таблица 2. Трудоёмкость атак на Trivium

Сценарий атаки	Число шагов инициализации	Вероятность успеха атаки	Трудоёмкость атаки, с.
1	64	1	2^{74}
1	80	1	2^{77}
1	96	1	2^{80}
3	128	1	2^{74}

Список литературы

1. Gurobi Optimizer. Режим доступа: https://www.gurobi.com/documentation/
2. IBM ILOG CPLEX. https://www.ibm.com/products/ilog-cplex-optimization-studio/
3. SCIP. https://www.scipopt.org/
4. Семёнов А.А. Атаки из класса «угадывай и определяй» и автоматические способы их построения. Прикладная дискретная математика, 2018, с. 81–86.
5. De Cannière C., Preneel B. TRIVIUM Specifications, 2005.
6. Borghoff J., Knudsen L.R., Stolpe M. Bivium as a Mixed-Integer Linear Programming Problem. Cryptography and Coding, 2009, p. 135–152.
7. Вычислительный кластер НИЯУ МИФИ. https://it.mephi.ru/hpc/