УДК 004.056.55

Применимость статистических тестов к эволюционным методам декомпозиции экземпляров задачи о булевой выполнимости для криптоанализа генераторов ключевого потока

Автор: Павленко А. Л. (Университет ИТМО, г. Санкт-Петербург)
Научный руководитель: Ульянцев В. И. (Университет ИТМО, г. Санкт-Петербург)

Введение. Генераторы ключевого потока, и, в частности, потоковые шифры, рассматриваемые в данной работе, используются для безопасной передачи данных по незащищенным каналам связи. В момент начала передачи данных инициализируется некоторый *секретный ключ*, который используется для шифрования и расшифровки информации, и передается по защищенному каналу связи.

Эволюционные методы, рассматриваемые в данной работе, позволяют оценить стойкость различных шифров к дешифровке методами из класса guess-and-determine, посредством их декомпозиции.

Целью работы является адаптация и реализация методов применения статистических тестов для криптоанализа генераторов ключевого потока, а также проведение экспериментов, подтверждающие целесообразность их использования в эволюционных методах декомпозиции экземпляров SAT задачи.

Базовые положения исследования. Для исследования криптографических функций в данной работе применяются эволюционные алгоритмы. В предыдущей работе [1] описан процесс перехода от криптографической функции к SAT-задаче и последующий способ ее декомпозиции. В данной работе для оценивания декомпозиционных (*guessed bit*) множеств используется метод из класса Guess-and-Determine: Inversive Backdoor Sets (IBS) [2]. Задача криптоанализа декомпозируется соответствующим множеством, и с помощью метода Монте-Карло [3] формируется множество подзадач размером N. Особенностью IBS является то, что для вычисления каждой подзадачи выделяется определенный временной ресурс T. Если SAT-решатель за отведенный лимит времени T находит разрешающее множество значений переменных, то соответствующая подзадача k является решенной $\xi_k = 1$, иначе $\xi_k = 0$. Когда для каждой подзадачи определено значение переменной ξ_k, то для нее можно подсчитать значение оценочной функции Φ для рассматриваемого guessed bit множества B по следующей формуле, выведенной в статье [2]:

$$\Phi = 2^{|B|} \cdot T \cdot \frac{3N}{\sum_{k=0}^{N} \xi_k}, \quad (1)$$

где $|B|$ – мощность декомпозиционного множества, то есть число переменных в нем. Точность вычисляемого оценочного значения Φ зависит от использованного объема выборки N. Но при увеличении объема выборки N растет и время, которое затрачивается на подсчет значения оценочной функции для рассматриваемого декомпозионного множества B. А значит уменьшается число *guessed bit* множеств, которые будут рассмотренны за выделенный лимит времени. Статистические тесты позволяют увеличить их число, не снижая точности получаемых оценок. Основная идея заключается в том, чтобы заранее отсеивать заведомо плохие декомпозиционные множества. Для этого выборка объема N делится на несколько небольших выборок объема N_b. Затем для каждого *guessed bit*

множества на текущей итерации вычисляется первое приближение оценочного значения на выборке объемом N_b. С помощью статистических тестов, используя эти приближения, отсеиваются заведомо плохие декомпозиционные множества, *p-value* которых меньше заданного (в нашем случае 0.05) по сравнению с лучшим найденым на текущий момент декомпозиционным множеством. Для оставшихся *guessed bit* множеств выборка N продолжает наращиваться с шагом N_b до некоторого N_{max}. После каждого увеличения выборки также происходит отсеивание заведомо плохих декомпозиционных множеств с помощью статистических тестов.

Основные результаты:

- Были адаптированы и реализованы следующие непараметрические статистические тесты для эволюционных методов декомпозиции экземпляров SAT задачи для криптоанализа генераторов ключевого потока: U-критерий Манна-Уитни [4] и тест Барнарда [5].
- Были получены экспериментальные данные, подтверждающие успешное применение статистических тестов к эволюционным методам декомпозиции экземпляров задачи о булевой выполнимости для криптоанализа генераторов ключевого потока.

Литература

[1] Павленко А.Л., Ульянцев В.И.: Эволюционные алгоритмы для криптоанализа генераторов ключевого потока с использованием программных средств решения задачи выполнимости. Сборник тезисов докладов конгресса молодых ученых. Электронное издание (2018)

[2] Semenov A., Zaikin O., Otpuschennikov I., Kochemazov S., Ignatiev, A.: On Cryptographic Attacks Using Backdoors for SAT. In: Proc. of AAAI 2018. pp. 6641–6648 (2018)

[3] Metropolis N., Ulam S.: The Monte Carlo Method. J. Amer. Statistical Assoc. 44(247), 335–341 (1949)

[4] Henry B. M., Donald R. W.: On a Test of Whether one of Two Random Variables is Stochastically Larger than the Other. Annals of Mathematical Statistics 18, 1, pp. 50–60 (1947)

[5] George A. B.: A New Test for 2 × 2 Tables. Nature 156 (1945), 177. https://doi.org/10.1038/156177a0 (1945)