УДК 004.056.53

О РАЗЛИЧНЫХ ВИДАХ КРИПТОАНАЛИЗА ПРИ ОЦЕНКЕ СТОЙКОСТИ КРИПТОГРАФИЧЕСКИХ ХЕШ-ФУНКЦИЙ И ПОТОЧНЫХ ШИФРОВ

Кирьянова А. П. (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательскийуниверситет ИТМО»)

Научный руководитель – кандидат технических наук, преподаватель Давыдов В. В. (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Введение. После создания криптографического алгоритма важным этапом является доказательство его стойкости: для криптографических хеш-функций необходимо обосновать стойкость к поискам прообразов и коллизий, а для поточных шифров – устойчивость к статистическим и аналитическим атакам. При оценке стойкости криптографических хеш-функций обычно анализируется функция сжатия, в поточных шифрах – генератор ключевого потока, для оценки криптостойкости которых можно использовать логический, дифференциальный, алгебраический, линейный криптоанализ и другие.

Основная часть. В работе рассмотрены различные виды криптоанализа, основные идеи и принцип работы для анализа стойкости поточных шифров и криптографических хеш-функций. Были показаны результаты успешного применения различных видов криптоанализа для нахождения коллизий криптографических хеш-функций SHA-1 [1], MD4 и MD5 [2], нахождение прообраза для неполнораундовых версий MD4 [3] и MD5 [4], криптоанализ поточных шифров HiTag2 и Crypto-1 [5], а также атака на генератор ключевого потока шифра A5/1 [6]. Изучены комбинации различных видов криптоанализа, включая комбинацию дифференциального и SAT-криптоанализа.

Выводы. Проанализированы криптографические хеш-функции SHA-1, MD4 и MD5, а также потоковые шифры A5/1, HiTag2 и Crypto-1, рассмотрена их стойкость к различным атакам и криптоанализу. Изучены различные виды криптоанализа, рассмотрены возможности их комбинирования для анализа стойкости криптографических хеш-функций и поточных шифров. Сделаны выводы о безопасности различных криптографических конструкций для защиты данных в современных реалиях.

Список использованных источников:

1. Stevens M. et al. The first collision for full SHA-1 // Advances in Cryptology–CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20–24, 2017, Proceedings, Part I 37. – Springer International Publishing, 2017. – С. 570-596.
2. Mironov I., Zhang L. Applications of SAT solvers to cryptanalysis of hash functions // Theory and Applications of Satisfiability Testing-SAT 2006: 9th International Conference, Seattle, WA, USA, August 12-15, 2006. Proceedings 9. – Springer Berlin Heidelberg, 2006. – С. 102-115.
3. Zaikin O. Inverting 43-step MD4 via Cube-and-Conquer. – 2022.
4. Заикин О. Обращение 29-шаговой функции сжатия MD5 при помощи алгоритмов решения проблемы булевой выполнимости // Прикладная дискретная математика. Приложение. – 2023. – №. 16. – С. 36-40.
5. Soos M., Nohl K., Castelluccia C. Extending SAT solvers to cryptographic problems // International Conference on Theory and Applications of Satisfiability Testing. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2009. – С. 244-257.
6. Посыпкин М. А. и др. Решение задач криптоанализа поточных шифров в распределенных вычислительных средах // Труды Института системного анализа Российской академии наук. – 2009. – Т. 46. – С. 119-137.

Кирьянова А. П. (автор)

Давыдов В. В. (научный руководитель)