УДК 004.056.53

О КРИПТОАНАЛИЗЕ БЛОЧНЫХ И ПОТОЧНЫХ ШИФРОВ

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

Научный руководитель – доктор технических наук, профессор Беззатеев С. В.
(Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Введение. Шифрование является частью криптографической защиты в информационных системах. Оно используется для обеспечения конфиденциальности сообщений, для аутентификации источника информации, другими словами, служит защитой различной информации в Интернете от несанкционированного доступа, а также от активного или пассивного прослушивания. Одним из важных шагов при создании шифра, как и любого другого криптографического алгоритма, является формальная оценка его безопасности и проверка на различные уязвимости.

Основная часть. В работе рассмотрены блочные шифры ГОСТ 34.12, AES, Camellia, SM4 и LEA, являющиеся современными стандартами шифрования разных стран, а также некоторые поточные шифры (Salsa20, HC-256, SNOW) и легковесные блочные шифры (PUFFIN-2, Fantomas, PRESENT). Была проанализирована структура этих шифров, описаны их достоинства, недостатки, уязвимости и применение, а также различные атаки как на конкретные алгоритмы, так и на шифры в целом [1, 2]. Были показаны результаты успешного применения дифференциального [3], линейного [4] и алгебраического [5] криптоанализа различных шифров, атака SWEET32 для нахождения открытого текста Blowfish и Triple DES [6], атака с использованием машинного обучения [7], а также атака линейных различителей с нулевой корреляцией [8].

Выводы. Рассмотрены подходы к построению блочных и поточных шифров, рассмотрено их место в современном мире обеспечения безопасности информации. Проанализированы как конкретные, так и общие атаки на конструкции шифрования. Исследована возможность улучшения современной методики формальной оценки безопасности шифров.

Список использованных источников:

1. Schneier B. Applied cryptography: protocols, algorithms, and source code in C. – john wiley & sons, 2007.
2. Hatzivasilis G. et al. A review of lightweight block ciphers //Journal of cryptographic Engineering. – 2018. – Т. 8. – С. 141-184.
3. Ferguson N. Impossible differentials in Twofish //Counterpane Systems. October. – 1999. – Т. 19.
4. Biham E., Dunkelman O., Keller N. Linear cryptanalysis of reduced round serpent //International Workshop on Fast Software Encryption. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2001. – С. 16-27.
5. Courtois N. T., Bard G. V. Algebraic cryptanalysis of the data encryption standard //Cryptography and Coding: 11th IMA International Conference, Cirencester, UK, December 18-20, 2007. Proceedings 11. – Springer Berlin Heidelberg, 2007. – С. 152-169.
6. Bhargavan K., Leurent G. Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN //Opgeroepen op Augustus. – 2016. – Т. 21. – С. 2018.
7. Gohr A. Improving attacks on round-reduced speck32/64 using deep learning //Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part II 39. – Springer International Publishing, 2019. – С. 150-179.

8. Bogdanov A. et al. Integral and multidimensional linear distinguishers with correlation zero //Advances in Cryptology–ASIACRYPT 2012: 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings 18. – Springer Berlin Heidelberg, 2012. – С. 244-261.