УДК 004.056.55

Білодід А. А.
Кирилащук Т. Г.

ЗАНАДТО БАГАТО КРИПТОВАЛЮТИ

Вінницький національний технічний університет

Анотація

У тезах проводиться критичний перегляд параметрів безпеки сучасних симетричних криптографічних примітивів, зокрема AES, BLAKE2, ChaCha та SHA-3. На основі аналізу двадцятирічного прогресу в галузі криптоаналізу обґрунтовується гіпотеза про надмірність поточної кількості раундів у загальноприйнятих стандартах. Досліджується розрив між теоретичними «академічними» атаками та реальною фізичною стійкістю алгоритмів. Запропоновано концепцію раціонального вибору кількості раундів, що базується на оцінці ризиків та обчислювальних витрат. Результати демонструють, що суттєве скорочення ітерацій обробки даних дозволяє досягти значного приросту продуктивності (до 2.5 разів) без реального зниження рівня захищеності інформації від практичних загроз.

Ключові слова: криптоаналіз, симетричне шифрування, AES, ChaCha, запас міцності, обчислювальна складність, інформаційна безпека.

Abstract

The theses provide a critical review of the security parameters of modern symmetric cryptographic primitives, including AES, BLAKE2, ChaCha, and SHA-3. Based on an analysis of twenty years of progress in cryptanalysis, the hypothesis of the redundancy of the current number of rounds in generally accepted standards is substantiated. The gap between theoretical "academic" attacks and the actual physical resistance of algorithms is investigated. The concept of a rational choice of the number of rounds based on risk assessment and computational costs is proposed. The results demonstrate that a significant reduction in data processing iterations allows for a substantial increase in performance (up to 2.5 times) without a real decrease in the level of information security against practical threats.

Keywords: cryptanalysis, symmetric encryption, AES, ChaCha, safety margin, computational complexity, information security.

Вступ

Швидкість симетричних примітивів є обернено пропорційною кількості їхніх раундів. Більшість сучасних алгоритмів було спроектовано з надзвичайно консервативним запасом міцності, щоб витримати десятиліття майбутніх досліджень. Однак сьогодні, коли природа симетричних функцій добре вивчена, стає зрозумілим, що багато систем витрачають надмірну енергію та час на виконання «зайвих» раундів, які не додають фактичної безпеки. У роботі аналізується можливість ревізії цих стандартів для створення швидших та ефективніших систем захисту, особливо в умовах масового впровадження пристроїв інтернет-речей (IoT).

Результати дослідження

У сучасному криптоаналізі склалася парадоксальна ситуація, коли алгоритм вважається «академічно зламаним», якщо знайдено спосіб розкрити його структуру хоча б на частку відсотка швидше за метод повного перебору, проте детальний аналіз Жана-Філіпа Омассона доводить, що такі результати часто не мають жодного стосунку до реальної практичної безпеки. Наприклад, теоретичні атаки на сім раундів алгоритму AES зі складністю 2^{146} операцій або об’ємом даних у 2^{100} байтів є фізично нездійсненними, оскільки необхідні для цього енергетичні та технічні ресурси перевищують можливості планети, що перетворює такі дослідження на суто інтелектуальні вправи. Аналіз конкретних примітивів свідчить про те, що за двадцять років спостережень найкращі атаки на AES-128

не подолали межу в сім раундів із десяти, тому пропоноване скорочення до дев'яти раундів дозволило б отримати приріст продуктивності до 25% без реального ризику для конфіденційності. Аналогічна ситуація спостерігається з алгоритмом ChaCha20, який при двадцяти стандартних раундах залишається вразливим лише на рівні семи раундів із фантастичною складністю 2^{235}, що робить перехід на вісім раундів (ChaCha8) стратегічно виправданим кроком для збільшення швидкості роботи у 2.5 рази. Найбільш консервативним виявився стандарт SHA-3, де при двадцяти чотирьох раундах практичні колізії знайдено лише для п'яти-шести раундів, а отже, скорочення ітерацій до десяти забезпечило б безпеку, що вдвічі перевищує теоретичну межу зламу, одночасно прискорюючи обробку даних у 2.4 рази. Важливим аспектом результатів є впровадження поняття «Crypto-Waste» або крипто-відходів, що описує ситуацію, коли колосальні обчислювальні потужність та електроенергія витрачаються на захист від подій, імовірність яких близька до нуля. Оскільки безпека будь-якої системи визначається її найслабшою ланкою, якою майже ніколи не є раундова функція шифру, а зазвичай стають помилки в реалізації програмного забезпечення, вразливості протоколів або людський фактор, підтримка надмірної кількості раундів стає економічно та технічно недоцільною. Навіть врахування квантової загрози та алгоритму Гровера не змінює цих висновків, оскільки стійкість до квантового перебору корелює з довжиною ключа, а не з ітераційною складністю внутрішніх перетворень, що підтверджує можливість безпечної оптимізації сучасних криптографічних стандартів.

Висновки

Дослідження підтверджує, що сучасна криптографія страждає від надмірного консерватизму. Запропонований перегляд кількості раундів для AES (9-11 раундів), ChaCha (8 раундів) та SHA-3 (10 раундів) дозволить досягти оптимального балансу між швидкістю та стійкістю. Це сприятиме поширенню шифрування в пристроях із обмеженими ресурсами та енергоефективних центрах обробки даних, значно знижуючи енергоспоживання цифрової інфраструктури без зниження реального рівня захищеності інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Aumasson J.-P. Too Much Crypto // Cryptology ePrint Archive, Report 2019/1492. – 2019. – 18 p.
2. Bernstein D. J. The Salsa20 family of stream ciphers // New Stream Cipher Designs. – Berlin: Springer, 2008. – P. 84–97.
3. Daemen J., Rijmen V. The Design of Rijndael: AES - The Advanced Encryption Standard. – Berlin: Springer-Verlag, 2002. – 238 p.
4. NIST. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions // FIPS PUB 202. – 2015. – 37 p.
5. Stallings W. Cryptography and Network Security: Principles and Practice. – 7th ed. – Boston: Pearson Education, 2017. – 766 p.

Білодід Анастасія Анатоліївна – студентка групи 2БС-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: bilodidnastia@gmail.com

Науковий керівник: ***Кирилащук Тетяна Геннадіївна*** – асистент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: kgt0998@gmail.com

Bilodid Anastasiia – student of group 2BS-24B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: bilodidnastia@gmail.com

Scientific Supervisor: ***Kyrylashchuk Tatyana*** – assistant of the Information Security Department, Vinnytsia National Technical University, Vinnytsia, e-mail: kgt0998@gmail.com