0.1. *Журавлев В.А.* Генератор псевдослучайных чисел с внешним источником энтропии, генерирующий последовательности, нормальные по Борелю

В моделировании и криптографии нужны генераторы случайных чисел, порождающие последовательности бит, которые одновременно выдерживают наборы статистических тестов и остаются непредсказуемыми. Цель этой работы - построить генератор псевдослучайных чисел с внешним источником энтропии, у которого выходная последовательность будет асимптотически нормальна по Борелю и в котором будет поддерживаться инкрементальный режим.

Основой предлагаемого генератора псевдослучайных чисел являются *двуликие процессы* - такие процессы, у которых для слов длины $\leq l$ частоты равны 2^{-l} [1].

Архитектура генератора следующая: X - сумма слоев нескольких двуликих процессов разного порядка по модулю 2 [2] (нормализующая последовательность); Y - последовательность, получаемая из внешнего источника, с помощью криптографической хэш-функции (энтропийная последовательность; данная последовательность проходит тесты NIST [3], [4]); $Z = X \oplus Y$ - итоговая последовательность, которая называется схема с добавленной энтропией. Доказано, что если X и Y независимы друг от друга, то для любого фиксированного k сохраняется k?распределенность, а значит, асимптотическая нормальность по Борелю. Реализация использует скользящую XOR?сумму: $O(1)$ операций на бит на слой и $O(\sum m_i)$ памяти; Y делает reseed при поступлении новых порций энтропии без пересчета X.

Пройдены статистические тесты: NIST (при $\alpha = 0{,}01$); TestU01 (SmallCrush/Crush/BigCrush) - без подозрений; PractRand - без аномалий до 8 ГБ. Проверка подпоследовательностей длины k не показала систематических отклонений до 2^{40} бит.

Основные результаты работы:

1. Реализован генератор псевдослучайных чисел, сохраняющий k-распределенность при сумме по модулю 2 двух независимых последователей.
2. Нормализирующая последовательность X основана на нескольких двуликих процессах, сложенных по модулю 2, с поддержкой инкрементального режима - добавления новых слоев двуликих процессов в процессе работы генератора.
3. Добавление последовательности Y, на основе внешнего источника энтропии (аппаратного генератора случайных чисел, например на основе шумов датчиков) без пересчета предыдущей последовательности

Итоговая схема проста для реализации: $Z = X \oplus Y$. Также она эффективна с точки зрения статистических свойств. Ограничение: нормальность по Борелю - необходимое, но не достаточное свойство для криптографической стойкости.

Научный руководитель — д.т.н. Рябко Б.Я.

Список литературы

[1] Ryabko B. Low-Entropy Stochastic Processes for Generating k-Distributed and Normal Sequences, and the Relationship of These Processes with Random Number Generators. // Mathematics. 2019. Vol. 7. N. 9. P. 838.

[2] Ryabko B. A Pseudo-Random Generator Whose Output is a Normal Sequence. // International Journal of Foundations of Computer Science. 2021. Vol. 32. N. 8. P. 981–989.

[3] NIST SP 800-22 Rev. 1. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographics Applications. / Gaithersburg, MD: NIST, 2010. 131 p.

[4] NIST SP 800-90B. Recommendation for the Entropy Sources Used for Random Bit Generation. / Gaithersburg, MD: NIST, 2018. 84 p.