Генератор случайных чисел на основе мультипликативной свёртки

Антонов Николай Андреевич

Аспирант 1 курса

Институт ВМиИТ(ВМК) КФУ, Казань, Россия

E-mail: nikoljaany@mail.ru

Научный руководитель *— Ишмухаметов Шамиль Талгатович*

Современные алгоритмические генераторы случайных чисел характеризуются компромиссом между степенью их соответствия источнику выборки из равномерного распределения, скоростью производства псевдослучайных последовательностей и криптографической стойкостью к атакам. Ниже представлен новый алгоритмический генератор случайных чисел, который в высокой степени удовлетворяет всем трём вышеуказанным характеристикам одновременно. Главной особенностью генератора является «мультипликативная свёртка» – нелинейное преобразование, успешно осуществляемое обыкновенным регистром сдвига с линейной обратной связью, если он удовлетворяет некоторым условиям.

Алгоритм получения выходного бита. Рассмотрим регистр сдвига длиной $p-1$ ячеек, где p – простое число вида $4t+3$ (t – натуральное число). Пусть механизм линейной обратной связи задан примитивным над полем $GF(2)$ многочленом $P(x)$, а регистр находится в произвольном ненулевом состоянии s. Будем считать, что ячейки регистра последовательно пронумерованы числами от 1 до $p-1$. Результат одного такта работы генератора получается по следующим правилам:

1. Рассмотреть ячейки регистра, содержащие нулевой бит, перемножить их порядковые номера и взять остаток от деления на p. (Получим некоторое натуральное число $n : 0 < n < p$)

2. Рассмотреть ячейки регистра, содержащие единичный бит, перемножить их порядковые номера и взять остаток от деления на p. (Получим некоторое натуральное число $e : 0 < e < p$)

3. Сформировать выходной бит, выполнив операцию XOR над битами, взятыми из ячеек под номерами n и e.

4. При помощи многочлена $P(x)$ вычислить бит обратной связи и осуществить сдвиг - так же, как вычисляется линейная обратная связь и осуществляется сдвиг обыкновенного регистра.

Действия, указанные в пунктах 1-3, образуют «мультипликативную свёртку» битов регистра, в результате которой получается единственный бит выходной последовательности.

Оценка сложности. Прямое выполнение алгоритма имеет сложность $O(p(log(p)))$. Выполнение $O(p)$ предварительных вычислений с использованием $O(p)$ памяти для хранения результатов позволяет снизить временную сложность до линейной, уравнивая такт генератора с тактом обыкновенного регистра сдвига.

Статистические свойства. Выходные последовательности генератора проходят статистические тесты $NIST$ (пройдены все тесты пакета, размер выборки 10 Мегабайтов), $Diehard$ (пройдены все тесты пакета, размер выборки 1 Гигабайт), $DieHarder$ (пройдено 30/32 тестов пакета, размер выборки 4 Гигабайта). Эмпирически подтверждается, что побитовая сумма двух произвольных выходных последовательностей генератора сохраняет статистические свойства выборки из равномерного распределения.

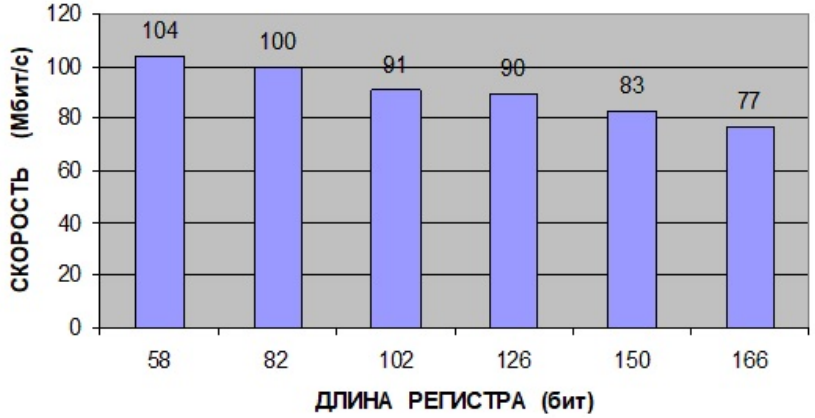
Криптографические свойства. Нелинейность мультипликативной свёртки делает бессмысленным поиск начального состояния регистра посредством алгоритма Берлекэмпа-Месси. Наличие в генераторе единственного регистра сдвига исключает возможность проведения корреляционных атак. Эмпирическая оценка периода генератора совпадает с максимальным периодом обыкновенного регистра сдвига и равна $2^n - 1$, где n – длина регистра. Выходные последовательности генератора имеют крайне низкую степень автокорреляции (график автокорреляции выходной последовательности длиной 1000 бит, сгенерированной при $p = 83$ и случайно выбранном начальном состоянии, представлен ниже).

Скорость производства псевдослучайной последовательности. Программная реализация генератора выполнена на языке C++/2020 и поддерживает скорость выработки псевдослучайных битов, пригодную для потокового шифрования на максимальных скоростях стандарта $4G$ (80 – 100 Мбит/с).

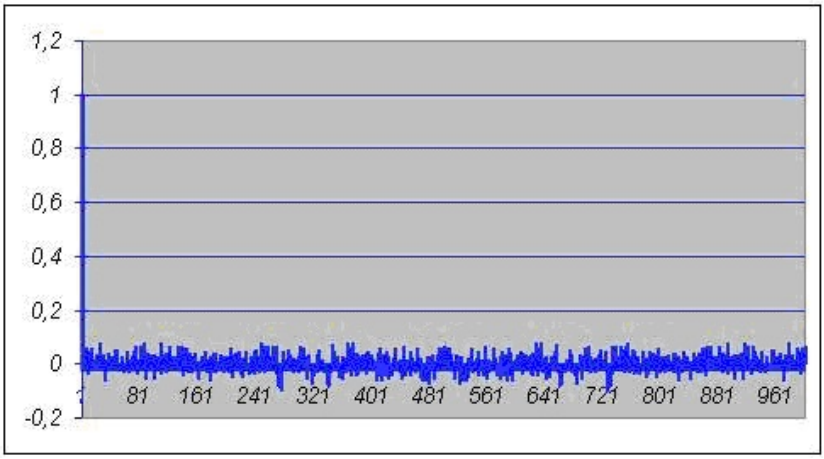
Литература

1. Antonov N.A. Improving the random number generator with multiplicative convolution transform // Journal of Advanced Research in Dynamical and Control Systems, Volume 11, Issue 8, Pages 2827–2833, Scopus, 2019.

Иллюстрации



Скорость работы генератора в зависимости от длины регистра.



Автокорреляция фрагмента последовательности длиной 1000 бит.