Накопление случайности в генераторах псевдослучайных чисел.

Чайко Владимир Иванович, студент бакалавриата
Сибирский государственный индустриальный университет
(г. Новокузнецк).

В статье автор рассказывает о накоплении случайности в генераторах псевдослучайных чисел и приводит результаты экспериментов, подтверждающих факт возможности накопления случайностей.

Ключевые слова: *ГПСЧ, накопление случайности, псевдослучайное число, XOR.*

Случайными числами называют последовательность чисел, которая составлена из чисел определенного диапазона, между которыми нет никакой статистической и математической зависимости, и подчиняется какому-либо закону распределения. При идеальной генерации случайных чисел вероятность «выпадения» у всех чисел диапазона одинакова и определяется по формуле вероятности:

$$P(A) = \frac{m}{n}$$

где: m — количество способов, которыми может выпасть конкретное число из диапазона, n — всего чисел в диапазоне.

В вычислительной технике случайностей нет и генерировать случайные числа она не может. Однако компьютеры могут создавать числа, которые выглядят случайными, но таковыми не являются. Такие числа называются псевдослучайными, а их генераторы — генераторами псевдослучайных чисел (ГПСЧ). Простыми примерами ГПСЧ могут служить метод «середины квадрата» [1] и линейный конгруэнтный метод [2].

Больше всего в случайных числах нуждается криптография — наука о шифровании (защиты информации). Любой алгоритм шифрования использует ключ — псевдослучайное секретное число, позволяющее

зашифровать и расшифровать данные. Случайность таких чисел должна быть очень высока, а их размер, на сегодняшний день, не менее 128 бит. [3] Почти все ГПСЧ не могут быть использованы в области криптографии из-за малой случайности. При этом о возможности накопления этими генераторами случайности до необходимого уровня в какой-либо литературе и научных работах не говорится (автор таких книг и научных работ не нашел).

«Неслучайность» (Q) при генерации мыслится мной как разница вероятностей появления наиболее вероятного и наименее вероятного числа:

$$Q = P(A)_{max} - P(A)_{min} = \Delta P(A) = \frac{n_{max}}{m} - \frac{n_{min}}{m} = \frac{\Delta n}{m}$$

где: Q — неслучайность ГПСЧ, $P(A)_{max}$ — вероятность наиболее вероятного числа, $P(A)_{min}$ — вероятность наименее вероятного числа, n_{max} — количество появлений наиболее вероятного числа, n_{min} — количество появлений наименее вероятного числа, m — количество генерируемых чисел всего. Чем меньше Q, тем более случайные генерируются числа. Таким образом, случайность генератора чисел (S) вычисляется по формуле:

$$S = 1 - Q$$

Кроме случайности, у ГПСЧ, есть еще один параметр — энтропия. Несмотря на взаимосвязь случайности и энтропии, вторая никак не влияет на первую, поэтому в данной работе рассматриваться не будет. [4] [5]

В 1917 году Гилберт Вернам изобрел невзламываемый шифр (шифр Вернама). Реализуется он при помощи логической функции $\oplus$ («сложение по модулю 2», «исключающее или», XOR). Дело в том, что в результате применения $\oplus$ к тексту и ключу (случайному числу) побитно, получается абсолютно случайная последовательность неподдающаяся какому-либо анализу и взлому. [5] Можно сказать, что при помощи $\oplus$ сообщение «наделяется» той хаотичностью и случайностью, которой обладает ее ключ. Именно таким образом можно «накапливать» случайность в генераторах псевдослучайных чисел, приближая случайность создаваемых им чисел к идеальной. Формулой это можно выразить так:

$$n_1 \oplus n_2 = n_3$$

где: n_1– 1 псевдослучайное число, n_2 – 2 псевдослучайное число, n_3– 3 псевдослучайное число, более случайное, чем n_1 и n_2. Приведем пример: генератор псевдослучайных чисел сгенерировал псевдослучайное число n_1. Случайность этого числа можно увеличить, сгенерировав псевдослучайное число n_2 и применив к ним $\oplus$ побитно. Для дальнейшего накопления случайности необходимо и дальше генерировать псевдослучайные числа с последующим сложением их по модулю 2:

$$n_1 \oplus n_2 \oplus \ldots \oplus n_m = n_{m+1}$$

Для доказательства теоремы был проведен следующий эксперимент: 4 различных ГПСЧ по 9 раз генерировали 1 миллион псевдослучайных чисел от 0 до 9. Первый миллион чисел генерировался без сложения по модулю два с другими псевдослучайными числами. Второй миллион чисел генерировался с 1 сложением по модулю 2 с другим псевдослучайным числом, созданным этим же генератором. Последующие генерации производились с увеличением числа сложений по модулю 2 в 2 раза. Далее были вычислены по каждому миллиону чисел $P(A)_{max}$, $P(A)_{min}$ и Q. Для проведения эксперимента были выбраны следующие ГПСЧ: «rand» [6], «random_int» [7], «random_bytes» [8], и «openssl_random_pseudo_bytes» [9]. Результаты эксперимента представлены в таблицах 1 и 2.

Таблица 1. **Результаты экспериментов на ГПСЧ rand и random _ int**

XOR	**ГПСЧ rand**			**ГПСЧ random_int**		
	$P(A)_{max}$	**$P(A)_{min}$**	**Q**	**$P(A)_{max}$**	**$P(A)_{min}$**	**Q**
0	0,100557	0,09927	0,001287	0,100659	0,099493	0,001166
1	0,099836	0,039736	0,0601	0,100229	0,039834	0,060395
2	0,07629	0,051983	0,024307	0,076284	0,051853	0,024431
4	0,067772	0,057911	0,009861	0,067595	0,057815	0,00978
8	0,063374	0,061632	0,001742	0,062879	0,061376	0,001503
16	0,06273	0,062291	0,000439	0,062827	0,062031	0,000796
32	0,062743	0,062134	0,000609	0,062877	0,062028	0,000849
64	0,062916	0,062189	0,000727	0,062853	0,062064	0,000789
128	0,062851	0,062288	0,000563	0,062453	0,061976	0,000477

Таблица 2. **Результаты экспериментов с ГПСЧ random_bytes и openssl_random_pseudo_bytes**

XOR	ГПСЧ random_bytes			ГПСЧ openssl_random_pseudo_bytes		
	$P(A)_{max}$	$P(A)_{min}$	Q	$P(A)_{max}$	$P(A)_{min}$	Q
0	0,003947	0,003793	0,000154	0,00394	0,003824	0,000116
1	0,003983	0,003846	0,000137	0,004008	0,003904	0,000104
2	0,004011	0,003778	0,000233	0,003943	0,003769	0,000174
4	0,004021	0,003835	0,000186	0,004012	0,003837	0,000175
8	0,00404	0,003863	0,000177	0,003997	0,003778	0,000219
16	0,003994	0,0038	0,000194	0,003985	0,003758	0,000227
32	0,004051	0,003823	0,000228	0,004003	0,003846	0,000157
64	0,003957	0,00384	0,000117	0,00402	0,003826	0,000194
128	0,004014	0,003769	0,000245	0,004052	0,003796	0,000256

Выводы:

1. Накапливать случайность ГПСЧ возможно путем сложения по модулю 2 с другими случайными числами.

2. Максимально возможная случайность (S) любого ГПСЧ $0{,}9999 \leq S < 1$ ($0 < Q < 0{,}0001$).

3. Если ГПСЧ имеет случайность (S) в диапазоне $0{,}9999 \leq S < 1$ ($0 < Q < 0{,}0001$), то дальнейшее существенное накопление случайности на нем невозможно.

4. У некоторых ГПСЧ при первом сложении по модулю 2 случайность генерируемых чисел может уменьшиться, но она возрастает при дальнейшем накоплении при помощи $\oplus$.

5. ГПСЧ с низкой случайностью можно использовать в криптографии при условии накопления ими случайности.

Литература:

1. Von, Neumann. Various techniques used in connection with random digits. / Neumann Von, John.. — Текст: непосредственный // National Bureau of Standards Applied Mathematics Series.. — 1951. — № 12. — С. 36–38.
2. Маккафри, Д. Тесты — Упрощенная генерация случайных чисел. / Д. Маккафри. — Текст: электронный // Microsoft.: [сайт]. — URL: https://docs.microsoft.com/ru-ru/archive/msdn-magazine/2016/august/test-run-lightweight-random-number-generation (дата обращения: 04.02.2022).
3. A. Biryukov, D. Khovratovich. Related-key Cryptanalysis of the Full AES-192 and AES-256. / A. Biryukov, D. Khovratovich. — Текст: электронный // impic.org: [электронный документ]. — URL: http://www.impic.org/papers/Aes-192–256.pdf (дата обращения: 04.02.2022).
4. Shannon, C. E. A Mathematical Theory of Communication / C. E. Shannon. — Текст: непосредственный // Bell System Technical Journal. — 1948. — № 27. — С. 379–423.
5. Shannon, C. E. Communication Theory of Secrecy Systems / C. E. Shannon. — Текст: непосредственный // Bell System Technical Journal. — 1949. — № 28. — С. 656–715.
6. rand. — Текст: электронный // php.net: [сайт]. — URL: https://www.php.net/manual/ru/function.rand.php (дата обращения: 07.02.2022).
7. random_int. — Текст: электронный // php.net: [сайт]. — URL: https://www.php.net/manual/ru/function.random-int.php (дата обращения: 07.02.2022).
8. random_bytes. — Текст: электронный // php.net: [сайт]. — URL: https://www.php.net/manual/ru/function.random-bytes.php (дата обращения: 07.02.2022).

9. openssl_random_pseudo_bytes. — Текст: электронный // php.net: [сайт]. — URL: https://www.php.net/manual/ru/function.openssl-random-pseudo-bytes.php (дата обращения: 07.02.2022).