ГЕНЕРАЦИЯ КРИПТОГРАФИЧЕСКИ СТОЙКОЙ ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ ДЛЯ АЛГОРИТМА ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТРОЙКИ РАБОЧЕЙ ЧАСТОТЫ В СИСТЕМАХ ЗАЩИТЫ КАНАЛА СВЯЗИ С БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТОМ

Мойсюк-Дранько Я.А.

Национальный детский технопарк г. Минск, Республика Беларусь

Дубовик И.А. – канд. техн. наук

Аннотация. В работе рассматривается проблема обеспечения защищённости радиоканала беспилотных летательных аппаратов посредством алгоритма псевдослучайной перестройки рабочей частоты (ППРЧ). Проведён сравнительный анализ генераторов псевдослучайных последовательностей: линейного конгруэнтного генератора, Mersenne Twister, XorShift и перемешанного конгруэнтного генератора (PCG) — по критериям периода, скорости генерации, прохождения статистических тестов BigCrush и наличия структурных паттернов в выходной последовательности. Замер вычислительной эффективности произведён на микроконтроллере ESP32-S3. Описан механизм формирования затравки генератора на пульте радиоуправления и её передачи на полётный контроллер посредством синхронизационного пакета. Показано, что PCG обеспечивает наилучшее сочетание статистической стойкости, периода генерации и вычислительной эффективности для применения в бортовых системах реального времени.

Современные беспилотные летательные аппараты функционируют в условиях интенсивного радиоэлектронного противодействия, что требует применения методов защиты радиоканала управления. Одним из ключевых является псевдослучайная перестройка рабочей частоты (ППРЧ, FHSS), при которой несущая частота изменяется по псевдослучайному закону, известному лишь легитимным участникам связи [1]. Качество алгоритма ППРЧ непосредственно определяется свойствами генератора псевдослучайной последовательности (ГПСП): он должен обеспечивать максимальный период, равномерное распределение, непредсказуемость выходных значений без знания внутреннего состояния и низкую вычислительную сложность.

Линейный конгруэнтный генератор (LCG) вычисляет последовательность по рекуррентному соотношению:

$$X_{n+1} = (a \cdot X_n + c)\ mod\ m \quad (1),$$

Алгоритм отличается простотой и высокой скоростью, однако имеет критический недостаток: младшие биты выходной последовательности обладают существенно меньшим периодом, а внутреннее состояние тривиально восстанавливается по нескольким наблюдаемым значениям [2], что делает LCG непригодным для криптографических применений.

Генератор Mersenne Twister (MT19937) основан на линейном регистре сдвига с обратной связью и обеспечивает период $2^{19937}-1$ [3]. Он проходит большинство стандартных статистических тестов, однако знание 624 последовательных 32-битных выходов позволяет полностью восстановить внутреннее состояние и предсказать всю дальнейшую последовательность [4]. Это является неприемлемым для задач защиты радиоканала.

Генератор XorShift основан на последовательном применении операций XOR и побитового сдвига к внутреннему состоянию:

$$X_{n+1} = X_n \oplus (X_n \ll a) \oplus (X_n \gg b) \quad (2),$$

где a и b — константы сдвига, подобранные для обеспечения максимального периода.

Генератор отличается исключительной простотой реализации и высокой скоростью работы, так как использует только операции, нативные для большинства процессорных архитектур. Тем не менее базовый XorShift не проходит ряд тестов пакета BigCrush, а его выходная последовательность уязвима к линейному криптоанализу [5]. Расширенные варианты — XorShift128+ и XorShift1024* — частично устраняют статистические недостатки, однако не решают проблему криптографической стойкости.

Перемешанный конгруэнтный генератор (PCG) устраняет указанные недостатки. Внутреннее состояние обновляется по схеме LCG, к которой затем применяются операции «перемешивания» (permutations/mixing) для маскировки линейных закономерностей [6]. Выходное значение формируется функцией пермутации PCG-XSH-RR, которая применяет операции XOR-сдвига и циклического сдвига для маскировки линейных закономерностей внутреннего состояния:

Для оценки вычислительной эффективности рассматриваемых алгоритмов был разработан тестовая программа, реализующая последовательную генерацию 10^6 псевдослучайных чисел для каждого из генераторов. Замер времени выполнения производился на микроконтроллере ESP32-S3 с тактовой частотой 240 МГц, представляющем типичную аппаратную платформу для бортовых систем управления БЛА. Результаты измерений подтвердили, что PCG и XorShift демонстрируют сопоставимую скорость генерации, существенно превосходя Mersenne Twister ввиду значительно меньшего размера внутреннего состояния и отсутствия операций с большими массивами данных. Исход сравнения приведён в таблице 1.

Таблица 1 – Сравнение генераторов псевдослучайных последовательностей

Характеристика	LCG	Mersenne Twister	XorShift	PCG
Период	2^{64}	2^{19937}-1	2^{64}-1	2^{64}
Скорость генерации (чисел/секунду)	7.949.125	2.977.431	7.951.021	4.467.077
Прохождение тестов BigCrush	нет	частично	частично	да
Обнаружение паттерна	да	нет	да	нет

В алгоритме ППРЧ текущая частота на k интервале определяется как:

$$f_k = f_{min} + (PCG(S_k) \bmod N) \cdot \Delta f \quad (3),$$

где N — число рабочих частот, $f_{\min}$ — минимальная частота сетки, Δf — шаг.

Для обнаружения паттернов возникаемых у отражает результат визуального и автокорреляционного анализа выходной последовательности: для каждого генератора строилась двумерная диаграмма рассеяния пар последовательных значений (X_n, X_{n+1}), на которой структурные закономерности проявляются в виде выраженных линий или плоскостей — так называемая гиперплоскостная структура, характерная для генераторов с линейным внутренним преобразованием. У LCG и XorShift такие паттерны были визуально обнаружены, что соответствует теореме Марсальи. PCG и Mersenne Twister паттернов в двумерной проекции не обнаружили, однако MT уязвим к восстановлению состояния, тогда как PCG устойчив как к визуальному, так и к алгебраическому анализу.

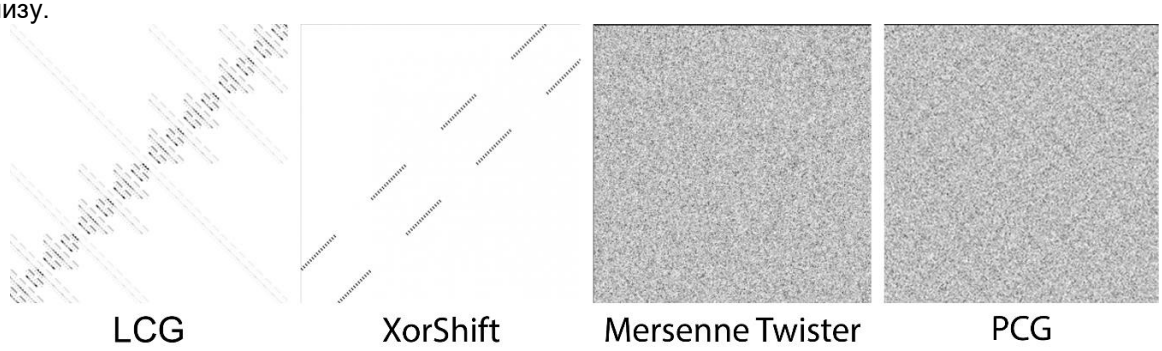

Рисунок 1 – Диаграммы обнаружения паттернов генераторов псевдослучайных чисел

На пульте радиоуправления начальное значение генератора (seed, затравка) формируется путём объединения секретного ключа K, прошитого в оба устройства на этапе производства, с текущей временной меткой T и одноразовым числом N_{once}, генерируемым при каждом включении:

$$S_0 = H(K \mid T \mid N_{once}) \quad (4),$$

где H — криптографическая хэш-функция. Сформированная затравка передаётся на полётный контроллер в составе синхронизационного пакета по защищённому каналу до начала сеанса связи, после чего оба устройства независимо инициализируют генератор PCG одним и тем же значением S_0 и воспроизводят идентичную псевдослучайную последовательность частот. Поскольку состояние генератора детерминировано начальным значением, пульт и полётный контроллер в каждый момент времени переходят на одну и ту же частоту синхронно, не обмениваясь дополнительными данными в ходе полёта; перехват синхронизационного пакета без знания ключа K не позволяет противнику восстановить затравку ввиду односторонности хэш-функции.

Таким образом, XorShift превосходит LCG по качеству выходной последовательности и сопоставим с ним по скорости, однако уязвим к алгебраическим атакам ввиду линейной структуры преобразования. PCG превосходит все рассмотренные алгоритмы по совокупности криптографических и вычислительных характеристик, что делает его оптимальным выбором в качестве ядра генератора ПСП для систем ППРЧ беспилотных летательных аппаратов.

Список использованных источников

1. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. — 2-е изд. — М. : Вильямс, 2007. — 1104 с.

2. Кнут, Д. Э. Искусство программирования. Т. 2 : Получисленные алгоритмы / Д. Э. Кнут. — 3-е изд. — М. : Вильямс, 2007. — 832 с.

3. Matsumoto, M. Mersenne Twister: A 623-dimensionally equidistributed uniform pseudo-random number generator / M. Matsumoto, T. Nishimura // ACM Transactions on Modeling and Computer Simulation. — 1998. — Vol. 8, № 1. — P. 3–30.

4. Шахтарин, Б. И. Генераторы псевдослучайных сигналов / Б. И. Шахтарин, В. А. Ковригин. — М. : Горячая линия–Телеком, 2010. — 192 с.

5. Marsaglia, G. Xorshift RNGs / G. Marsaglia // Journal of Statistical Software. — 2003. — Vol. 8, № 14. — P. 1–6.

6. O'Neill, M. E. PCG: A Family of Simple Fast Space-Efficient Statistically Good Algorithms for Random Number Generation / M. E. O'Neill // Harvey Mudd College Technical Report. — 2014. — HMC-CS-2014-0905. — 65 p.