РусКрипто

XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Об особенностях квантовых генераторов случайных чисел

А.П. Науменко, И.М. Арбеков, В.А. Кирюхин, А.А. Щербаченко

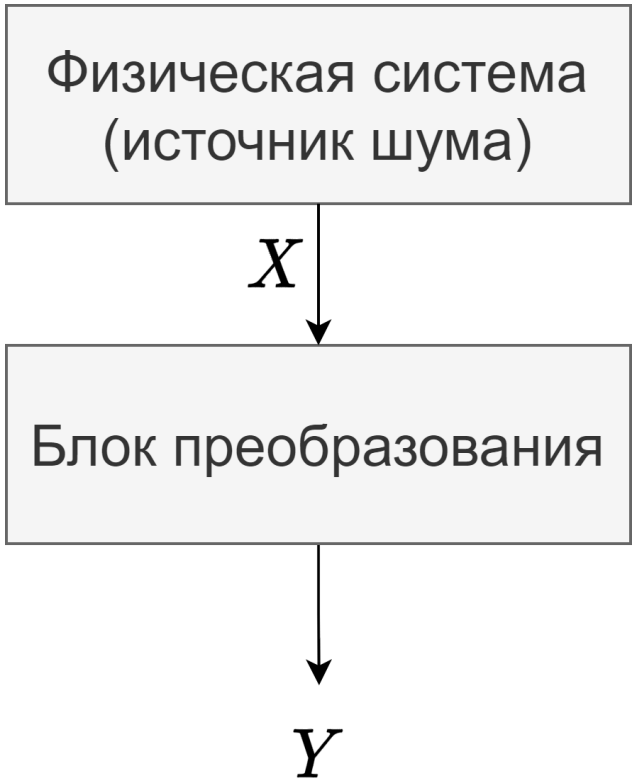
ООО «СФБ Лаб», АО «ИнфоТеКС»

РусКрипто’2025
20 марта 2025

Anton.Naumenko@infotecs.ru

СФБ ЛАБ

Структура



X– исходная последовательность

Y – выходная случайная последовательность

ФГСЧ

Физическая система

СФБ ЛАБ

- Шумовой диод в режиме пробоя
- Суммарный (интегральный) джиттер кольца инверторов
- Эффект метастабильности транзистора
- Тепловые шумы
- и др.

Исходная последовательность случайна, вероятностные распределения неизвестны

СФБ ЛАБ

- Случайность X оценивается мин-энтропией H_{min} на бит, согласно методике [1]
- Методика состоит из 10 тестов в том числе несколько тестов на угадывание последующего бита последовательности по некоторой предистории
- Оценка H_{min} – минимальная оценка по всем тестам

[1] NIST SP 800-90B
Recommendation for the Entropy Sources Used for Random Bit Generation
2018

Блок преобразования

Блок преобразования – сжатие (хэширование) случайно выбранной функцией g из класса G

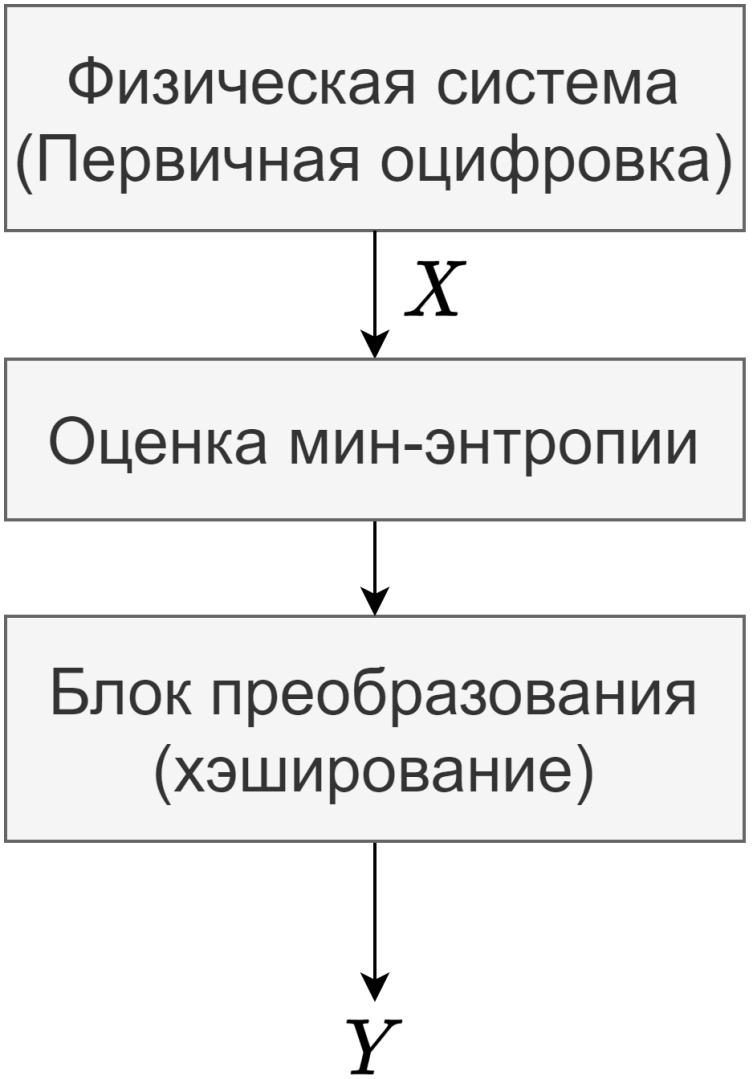
$$g : X \rightarrow Y$$

$$g : \{0,1\}^L \rightarrow \{0,1\}^N$$

Функция применяется к q блокам:

$$g(X_1) = Y_1, \ldots, g(X_q) = Y_q$$

Структура ФГСЧ



Выходная последовательность

СФБ ЛАБ

Leftover hash lemma (LHL)

Качество выходной последовательности оценивается как

$$\frac{1}{2}\sum_{G} P(g) \sum_{Y_1,\ldots,Y_q} \left| \Pr(Y_1, \ldots, Y_q) - \frac{1}{2^{qN}} \right| \leq \frac{1}{2} q \sqrt{2^{-LH_{min}+N}} \leq \varepsilon$$

q – число сжимаемых блоков
ε – заданный уровень качества Y
H_{min} – мин-энтропия на бит
L и N – битовая длина входа и выхода g

Выбор ε – уровня качества Y

Для выбора конкретного значения ε можно использовать результаты следующей работы

А.С Логачев, В.О. Миронкин
О влиянии вероятностных характеристик дискретных источников, формирующих криптографические ключи, на практическую секретность ключа
2024

КГСЧ

Физическая система

- Слабое лазерное излучение. Фотодетектирование во временных окнах [1]
- Лазерное излучение. Разность токов фотодетекторов на выходах светоделителя после смешения с вакуумным состоянием на входе (гомодинное детектирование) [2]
- и др.

[1] К.А. Балыгин, С.П. Кулик, С.Н. Молотков - Письма в ЖЭТФ 2024

Реализация квантового генератора случайных чисел: экстракция доказуемо случайных битовых последовательностей из коррелированных марковских цепочек

[2] M. Herrero-Collantes, J. Carlos Garcia-Escartin - RMP 2017

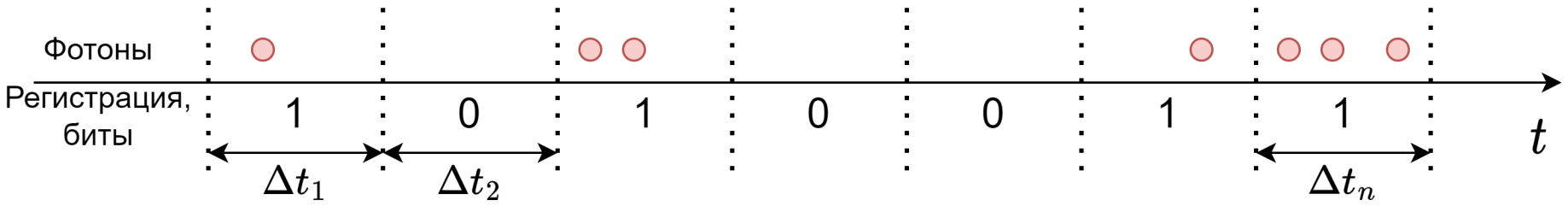
Quantum Random Number Generators

Достоинства КГСЧ

СФБ ЛАБ

1. Высокая скорость выработки случайных битов
2. Удается уточнить вероятностную модель исходной последовательности

Фотодетектирование во временных окнах



- Фотоны в интервале Δt_i, $i \in [1, n]$ регистрируются фотодетектором
- Бит 0 – отсутствие регистрации
- Бит 1 – наличие

Фотодетектирование во временных окнах

Распределение числа фотонов при **отсутствии** флуктуаций интенсивности оптического поля лазера

$$\Pr\left(\xi\left(\Delta t_i\right)=k\right)=\frac{\mu^k}{k!}e^{-\mu}$$

Совместное распределение

$$\Pr\left(\xi\left(\Delta t_1\right)=k_1,\ldots,\xi\left(\Delta t_n\right)=k_n\right)=\prod_{i=1}^{n}\Pr\left(\xi\left(\Delta t_i\right)=k_i\right)$$

Отсюда следует **независимость** битов исходной последовательности с распределением

$$P(0)=e^{-\mu},P(1)=1-e^{-\mu}$$

Л. Мандель, Э. Вольф, 2000
Оптическая когерентность и квантовая оптика

Исходная последовательность – независимая

Независимость X проверяется критериями согласия

Проект Технической спецификации ТК26
Информационная технология. Криптографическая защита информации. Временная методика проверки соответствия образца физического генератора случайных чисел его теоретико-вероятностной модели

Блок преобразования

1. Применяется арифметическое кодирование (нумерация) В.Ф. Бабкина для последовательных блоков X
2. Экстракция двоичных битов выходной последовательности производится из двоичного разложения номеров блоков

В результате образуется выходная двоичная последовательность Y длины ℓ.

В.Ф. Бабкин
Метод универсального кодирования источника независимых сообщений неэкспоненциальной трудоемкости
1971

Выходная последовательность

В предположении независимости исходной последовательности доказывается равновероятность выходной последовательности

$$P(Y) = 2^{-\ell},$$

вариационное расстояние $\varepsilon = 0$.

И.М. Арбеков, С.Н. Молотков
Об экстракции квантовой случайности
2021

Исходная последовательность – цепь Маркова

Случайность X проверяется критериями согласия на соответствие математической модели однородной цепи Маркова порядка r

Г.И. Ивченко, Ю.И. Медведев
Введение в математическую статистику
2010

Блок преобразования

1. Исходная последовательность распараллеливается на 2^r подпоследовательностей.
2. Применяется арифметическое кодирование (нумерация) В.Ф. Бабкина для отдельных блоков подпоследовательностей
3. Экстракция двоичных битов выходной последовательности производится из двоичного разложения номеров блоков

В результате образуется выходная двоичная последовательность Y длины ℓ.

В.Ф. Бабкин
Метод универсального кодирования источника независимых сообщений неэкспоненциальной трудоемкости
1971

Выходная последовательность

В предположении марковости исходной последовательности доказывается равновероятность выходной последовательности

$$P(Y) = 2^{-\ell},$$

вариационное расстояние $\varepsilon = 0$.

H. Zhou
Randomness and Noise in Information Systems
2012

И.М. Арбеков, С.Н. Молотков
Методические заметки. Квантовые генераторы случайных чисел, экстракция доказуемо случайных битовых последовательностей из траекторий цепей Маркова
2024

Пример КГСЧ на марковских цепочках

- Скорость образца КГСЧ на основе эффекта фотодетектирования $\approx$ 150 Мбит/с.
- Порядок цепи Маркова – $8 \div 9$.
- Распараллеливание происходит на 2^{10} подпоследовательностей.

К.А. Балыгин, С.П. Кулик, С.Н. Молотков - Письма в ЖЭТФ 2024
Реализация квантового генератора случайных чисел: экстракция доказуемо случайных битовых последовательностей из коррелированных марковских цепочек

Криптографическая защита ФГСЧ (КГСЧ) от сбоев в физической системе

Сбои в физической системе

Сбои в физической системе приводят к:

- уменьшению H_{min}
- потеря независимости, марковости

Сбои в физической системе

Сбои в физической системе приводят к:

- уменьшению H_{min}
- потеря независимости, марковости

Невозможно обеспечить малое вариационное расстояние!

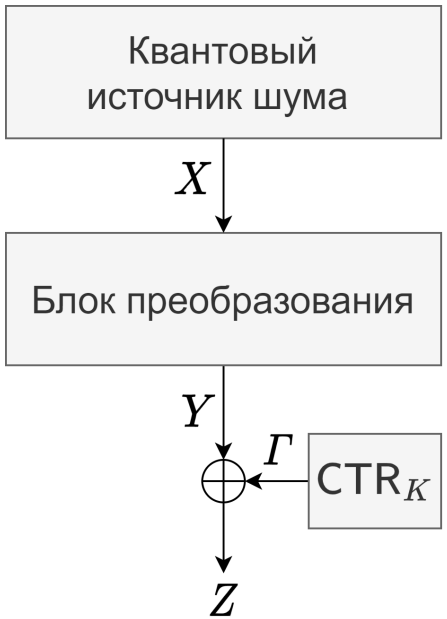
Защита при сбоях

Используем криптоалгоритмы с секретным ключом:

- шифрование выхода
- наложение гаммы
- каскад хэш-функций
- и др.

КГСЧ

Защита для КГСЧ, основанном на марковском процессе – блочный шифр с секретным ключом в режиме гаммирования.



Штатная работа – выход Z случайный и равновероятный.
Сбой – выход Z *вычислительно* неотличим от случайного.

Заключение

- Марковская цепь конечного порядка – адекватная мат. модель исходной последовательности КГСЧ

Заключение

- Марковская цепь конечного порядка – адекватная мат. модель исходной последовательности КГСЧ
- КГСЧ в условиях марковости обеспечивает идеальную (равновероятную) выходную последовательность

Заключение

- Марковская цепь конечного порядка – адекватная мат. модель исходной последовательности КГСЧ
- КГСЧ в условиях марковости обеспечивает идеальную (равновероятную) выходную последовательность
- Гаммирование выходной последовательности даёт КГСЧ защиту от сбоев

Заключение

СФБ ЛАБ

- Марковская цепь конечного порядка – адекватная мат. модель исходной последовательности КГСЧ
- КГСЧ в условиях марковости обеспечивает идеальную (равновероятную) выходную последовательность
- Гаммирование выходной последовательности даёт КГСЧ защиту от сбоев
- КГСЧ позволяет достичь больших скоростей, что необходимо при построении систем КРК

Благодарю за внимание!

А.П. Науменко, И.М. Арбеков,
В.А. Кирюхин, А.А. Щербаченко

ООО «СФБ Лаб», АО «ИнфоТеКС»

РусКрипто’2025
20 марта 2025

Anton.Naumenko@infotecs.ru

СФБ ЛАБ