

Криптография

Лекция 6. Случайные числа в криптографии.

Дмитрий Яхонтов

“Кочерга”, 2018

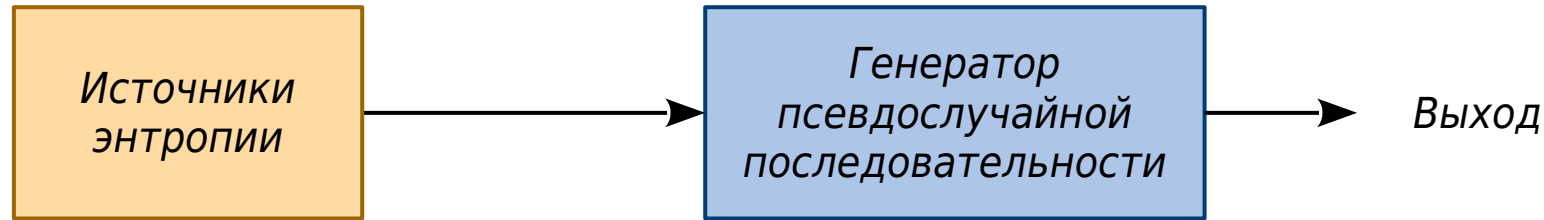
Для чего нужны случайные числа

- Генерация ключей
- Соль
- Одноразовые случайные значения (*nonce*)
- Протоколы “запрос-ответ” (*challenge-response*)
- Безопасное удаление данных

Требования к генератору случайных чисел

- Статистические
 - примерно равное число нулей и единиц
 - распределение длин серий 0000... и 1111...
 - отсутствие автокорреляций
 - спектральные тесты
- Непредсказуемость
 - не должно быть простого способа, зная N бит последовательности, предсказать $(N+1)$ -й с вероятностью больше 50%
- Нереверсируемость
 - не должно быть простого способа, зная состояние генератора, вычислить последовательность в предыдущие моменты времени

Общая структура ГСЧ



- Программные
- Аппаратные
- На основе односторонних функций
- На основе алгоритмов шифрования

Источник энтропии обеспечивает недетерминированность (истинную случайность)

ГПСЧ обеспечивает скорость, статистические свойства и криптографическую стойкость

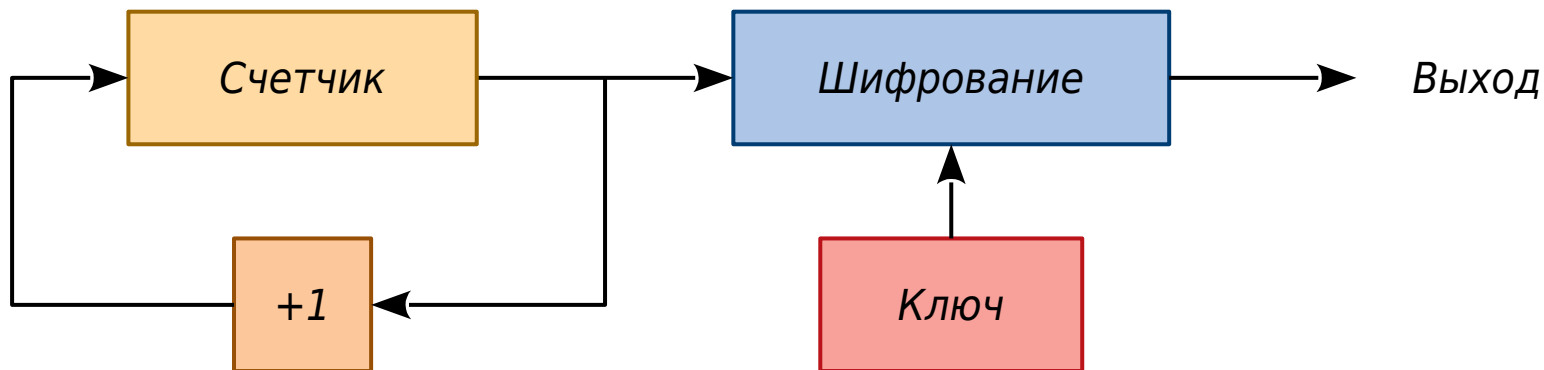
Генератор Блум–Блюма–Шуба (Blum–Blum–Shub)

$$X_{n+1} = (X_n)^2 \bmod M$$

выход — младший бит состояния X_n

- $M = p \cdot q$, где p и q — большие простые числа
- $p, q \equiv 3 \pmod{4}$ (гарантирует отсутствие запрещенных состояний)
- наибольший общий делитель $(p-1, q-1)$ должен быть малым
(увеличивает период генератора)
- начальное состояние X_0 должно быть взаимно-простым с M

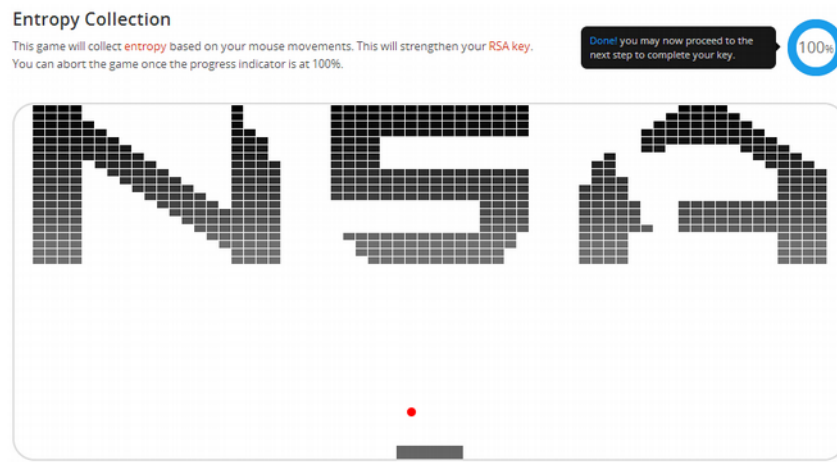
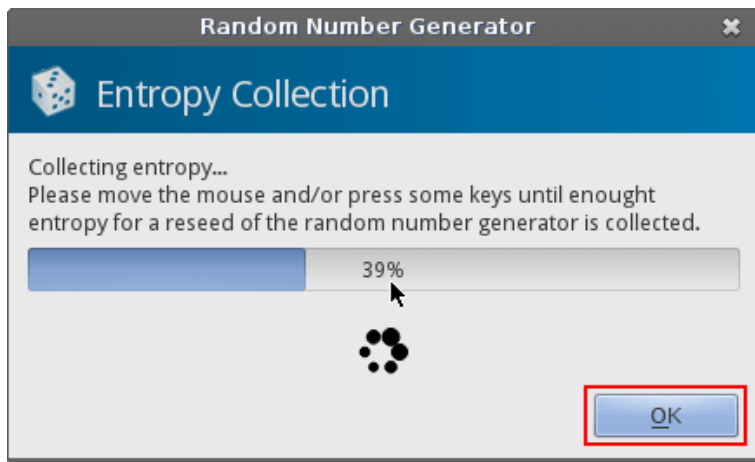
Генератор на основе блочного шифра



- Безопасность зависит от стойкости шифра и секретности ключа
- Для n -битного шифра максимальный период генератора — 2^n

Программные источники энтропии

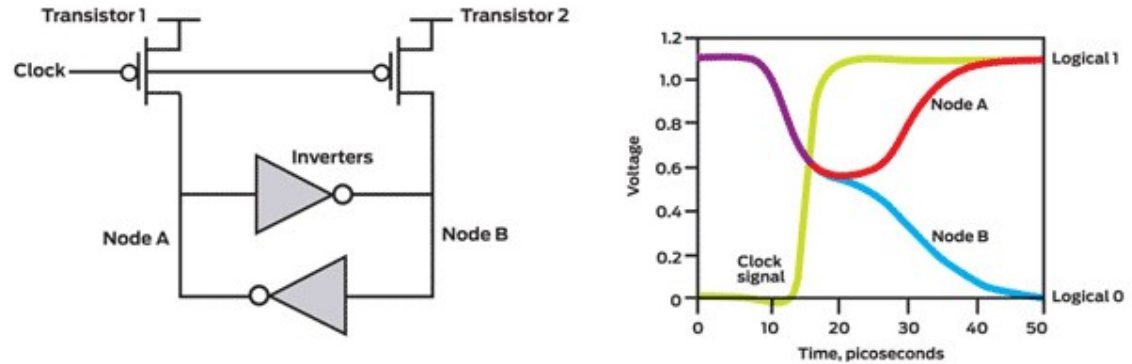
- Действия пользователя (клавиатура, мышь)



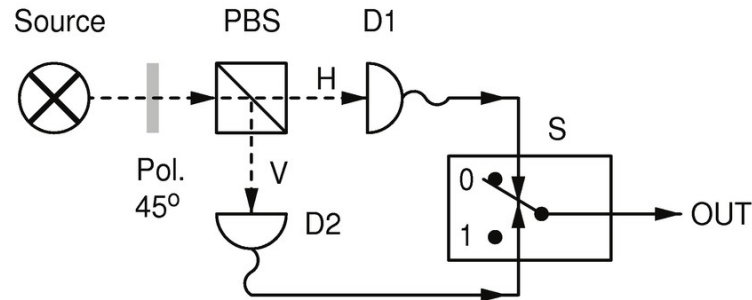
- Внешние события (сеть, дисковые операции)
- Асинхронные таймеры
- “Гонки” в многопоточных программах

Аппаратные источники энтропии

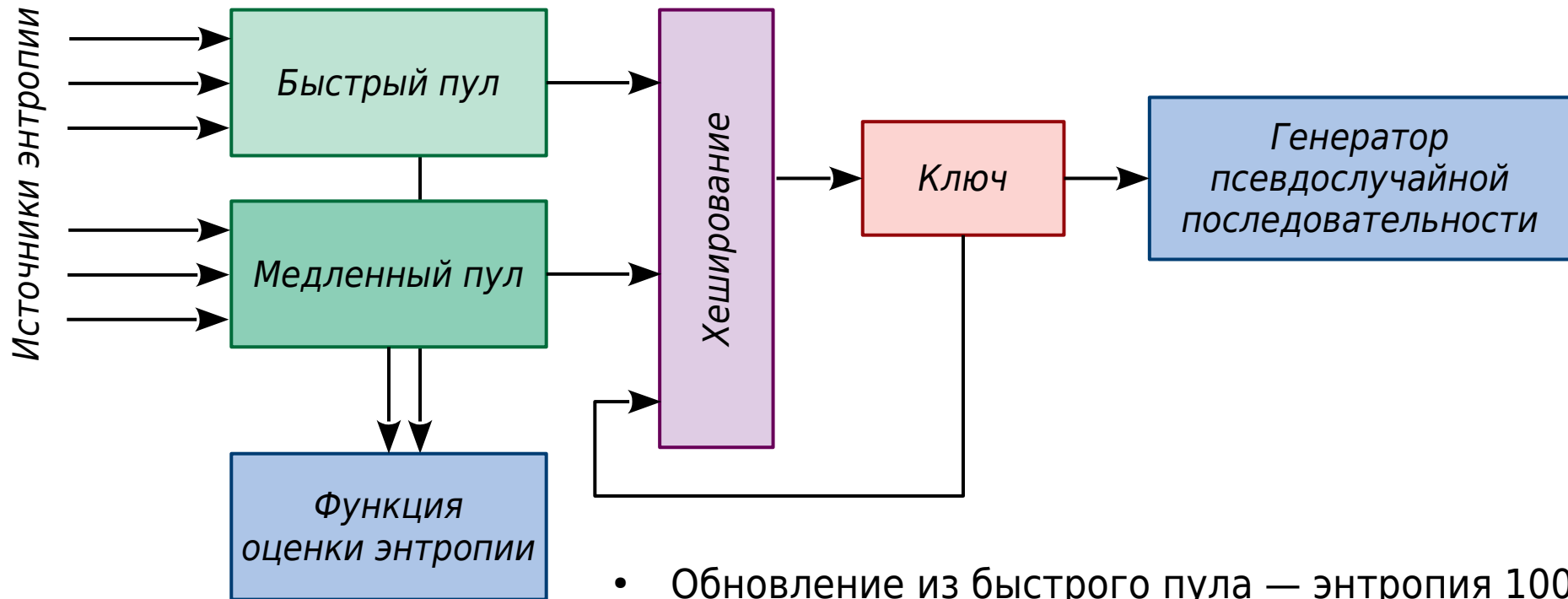
- Оцифровка теплового шума
- Генератор на метастабильных состояниях



- Квантовые источники

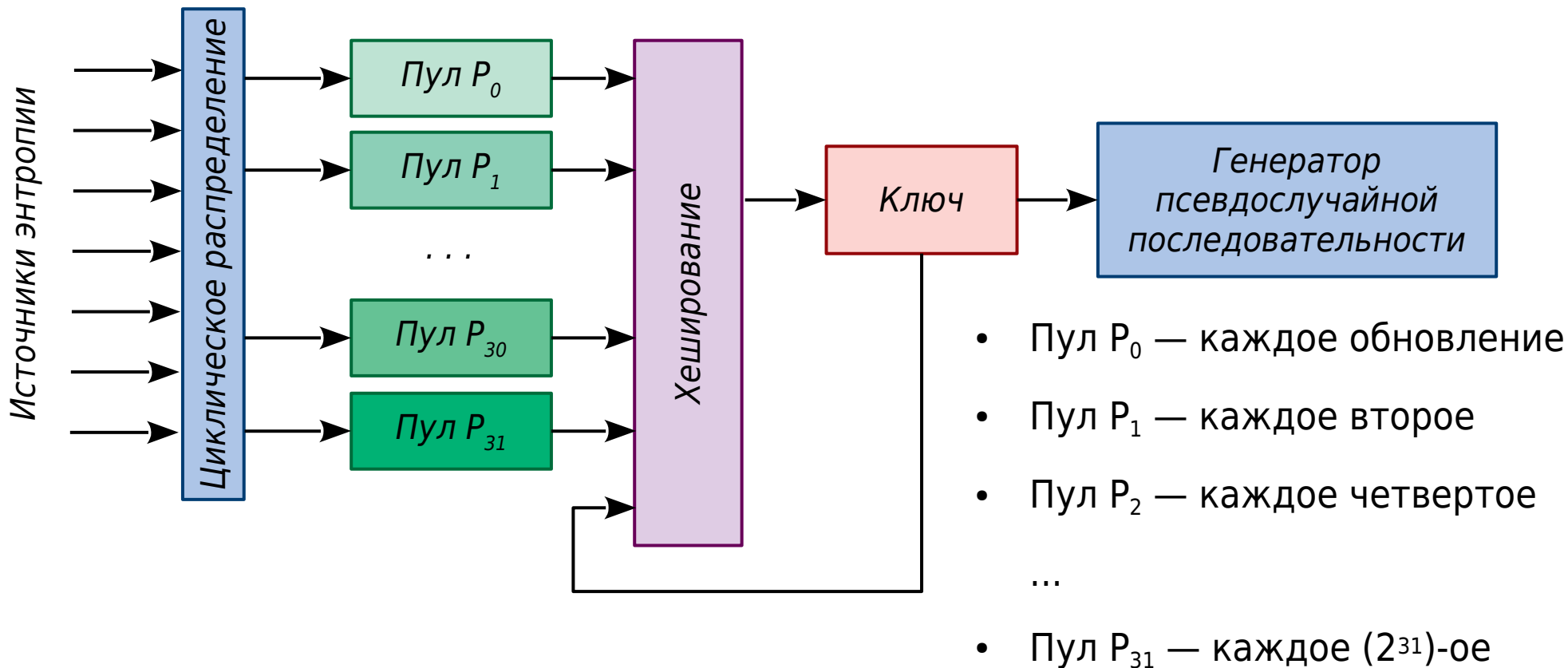


Алгоритм Yarrow



- Обновление из быстрого пула — энтропия 100 бит
- Обновление из медленного пула — энтропия 160 бит

Алгоритм Fortuna



Чем грозит слабая случайность

- 2008 г, RFID Mifare Crypto-1

Анализ схемотехники чипа показал, что в нём используется некриптостойкий ГСЧ с константным начальным состоянием. Единственный источник энтропии — время с момента включения. Можно избавиться от случайности в протоколе “запрос-ответ” и повторно использовать однажды перехваченные ответы.

- 2010 г, Sony PlayStation 3

Консоль позволяет запускать только ПО, подписанное цифровой подписью Sony (алгоритм ECDSA). Для всех цифровых подписей использовалось одно и то же “случайное” К. По двум подписям удалось восстановить закрытый ключ.

- 2013 г, аппаратный ГСЧ процессоров Intel

Показана теоретическая возможность создания backdoor'а в аппаратном ГСЧ. Модифицировав процесс легирования микросхемы, можно добиться константного ключа шифрования. Выход генератора проходит все тесты на случайность.

Ссылки

- Обратная связь:

✉ android.ruberoi@gmail.com

🔗 [@android_ruberoi](https://lesswrongru.slack.com)

- Анонсы:

📘 facebook.com/kocherga.club

👤 vk.com/kocherga_club

👤 vk.com/kocherga_prog

- Материалы лекций:

🐙 github.com/notOcelot/Kocherga_crypto

- Видео:

📺 youtube.com/channel/UCeLSDFOndI4eKFutg3oowHg

