v. 2.0

Криптография

Лекция 6. Случайные числа в криптографии.

Дмитрий Яхонтов *“Кочерга”, 2019*

Для чего нужны случайные числа

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

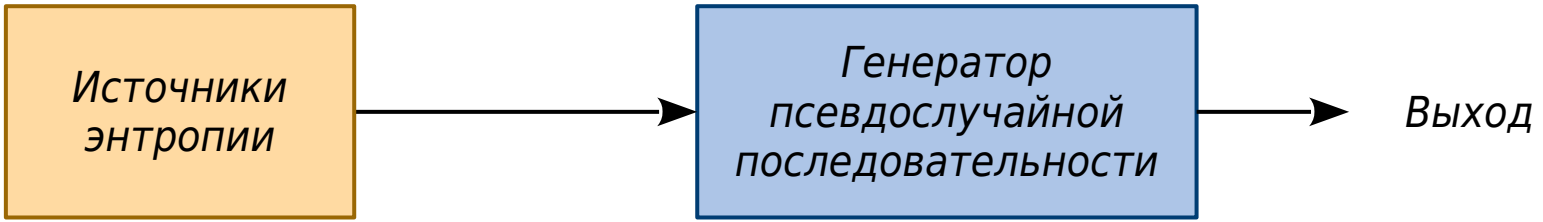
Требования к генератору случайных чисел

- 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

Источник энтропии обеспечивает недетерминированность (истинную случайность)

- На основе односторонних функций
- На основе алгоритмов шифрования

ГПСП обеспечивает скорость, статистические свойства и криптографическую стойкость

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

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

выход — младший бит состояния X_n

- M = p*q, где p и q — большие простые числа
- p, q = 3 mod 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

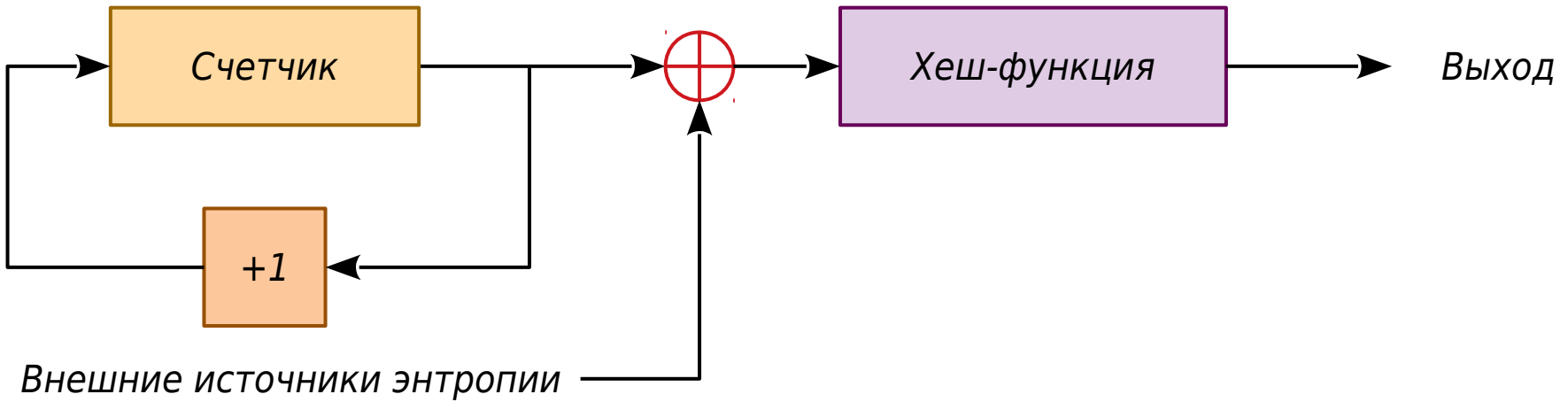
Генератор на основе дискретного логарифма

$$\mathbf{X_{n+1}} = \mathbf{g}^{\mathbf{X_n}} \bmod \mathbf{p}$$

$$\text{выход} — \begin{cases} 0, & \text{если } X_n < p/2 \\ 1, & \text{если } X_n \geq p/2 \end{cases}$$

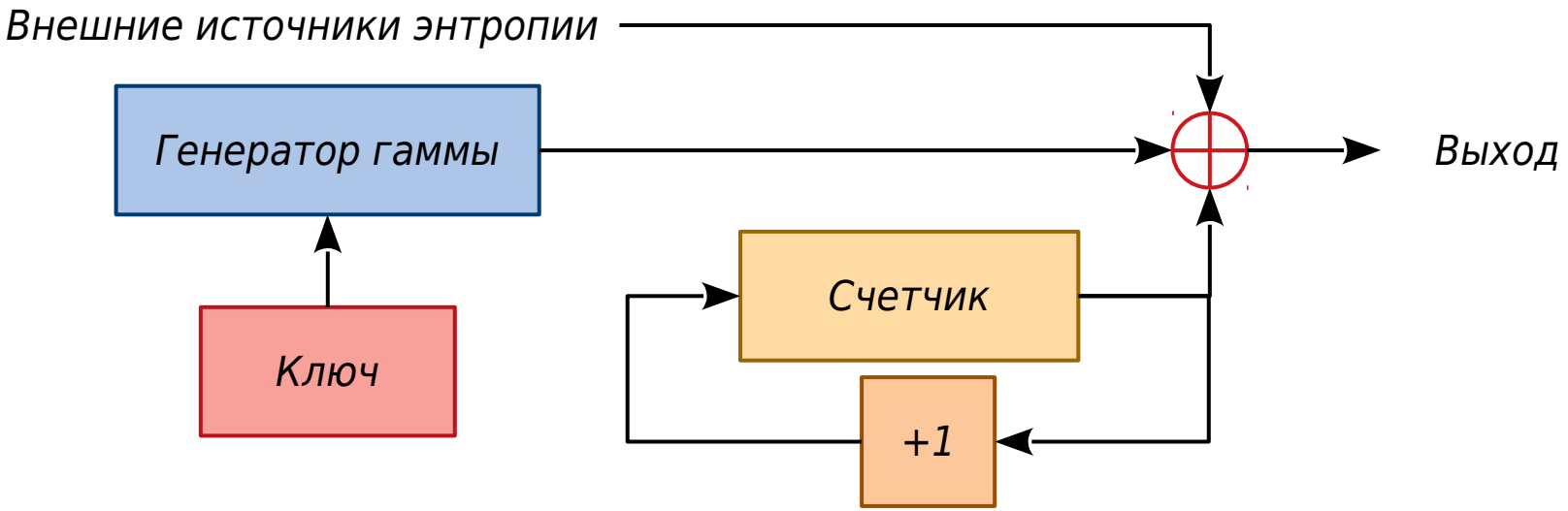
- **p** — большое простое число
- **g** — произвольное число, меньше p
- существуют модификации генератора на эллиптических кривых, например, Dual_EC_DRBG по стандарту NIST SP 800-90A
  (содержит backdoor!)

Генератор на основе хеш-функции



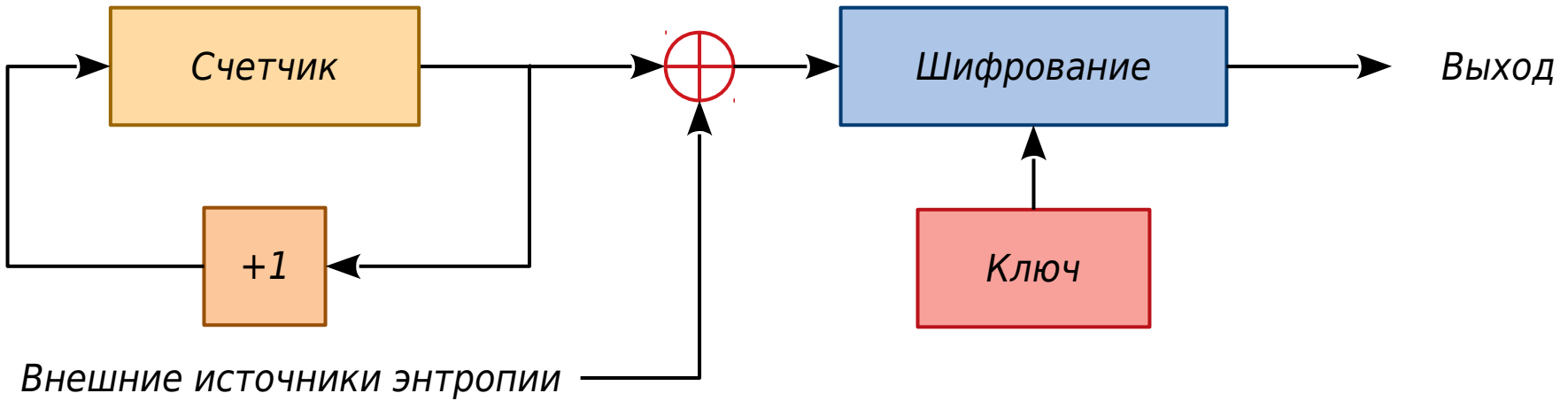
- Начальное состояние счетчика должно быть секретным
- Обычно применяется с другими ГПСЧ / источниками энтропии для обеспечения статистических свойств последовательности

Генератор на основе потокового шифра



- Ключ (начальное состояние генератора) должен быть секретным и уникальным для каждого экземпляра генератора
- Максимальный период определяется размером внутреннего состояния генератора и может быть увеличен добавлением внешних счетчиков

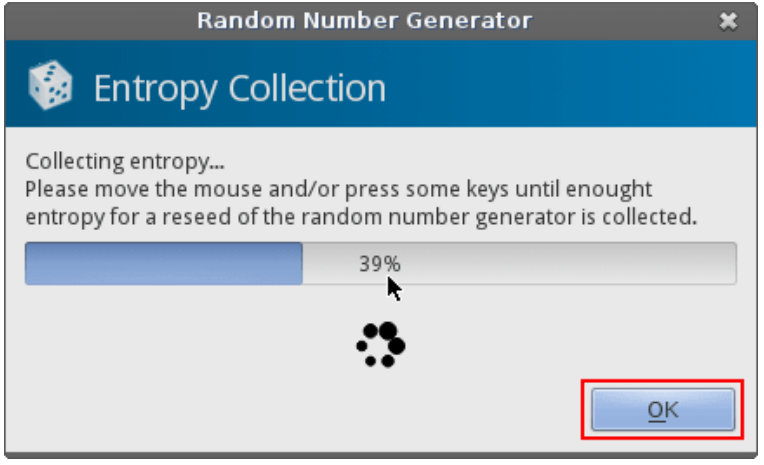
Генератор на основе блочного шифра

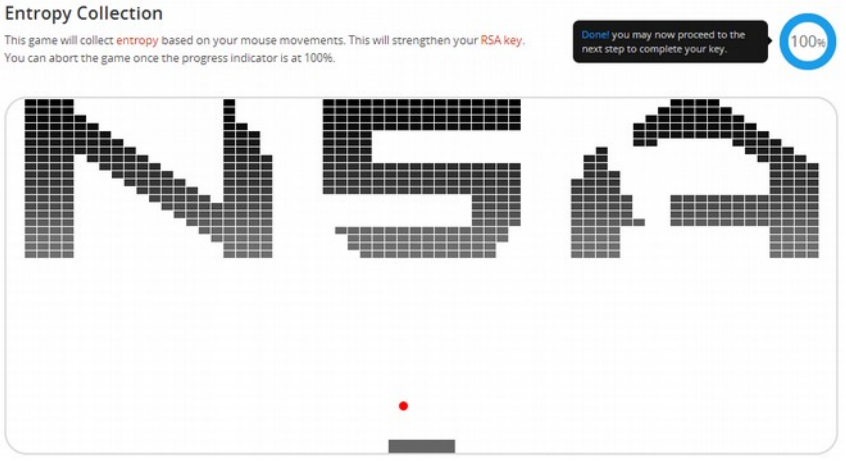


- Ключ должен быть секретным и уникальным для каждого экземпляра генератора
- Максимальный период генератора ограничен размером блока

Программные источники энтропии

- Действия пользователя (клавиатура, мышь)

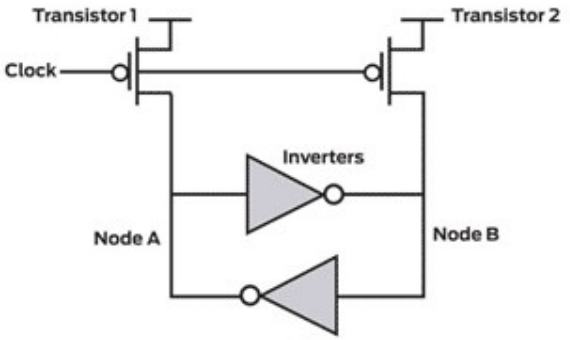


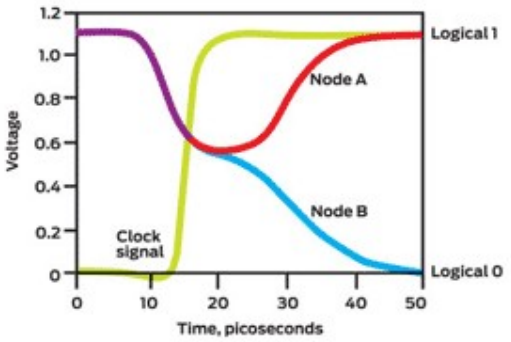


- Внешние события (сеть, дисковые операции)
- Асинхронные таймеры
- “Гонки” в многопоточных программах

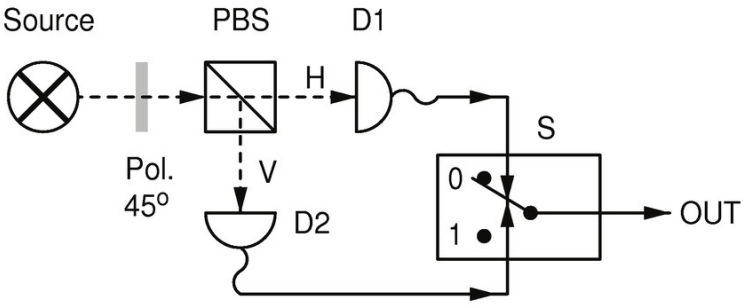
Аппаратные источники энтропии

- Оцифровка теплового шума
- Генератор на метастабильных состояниях

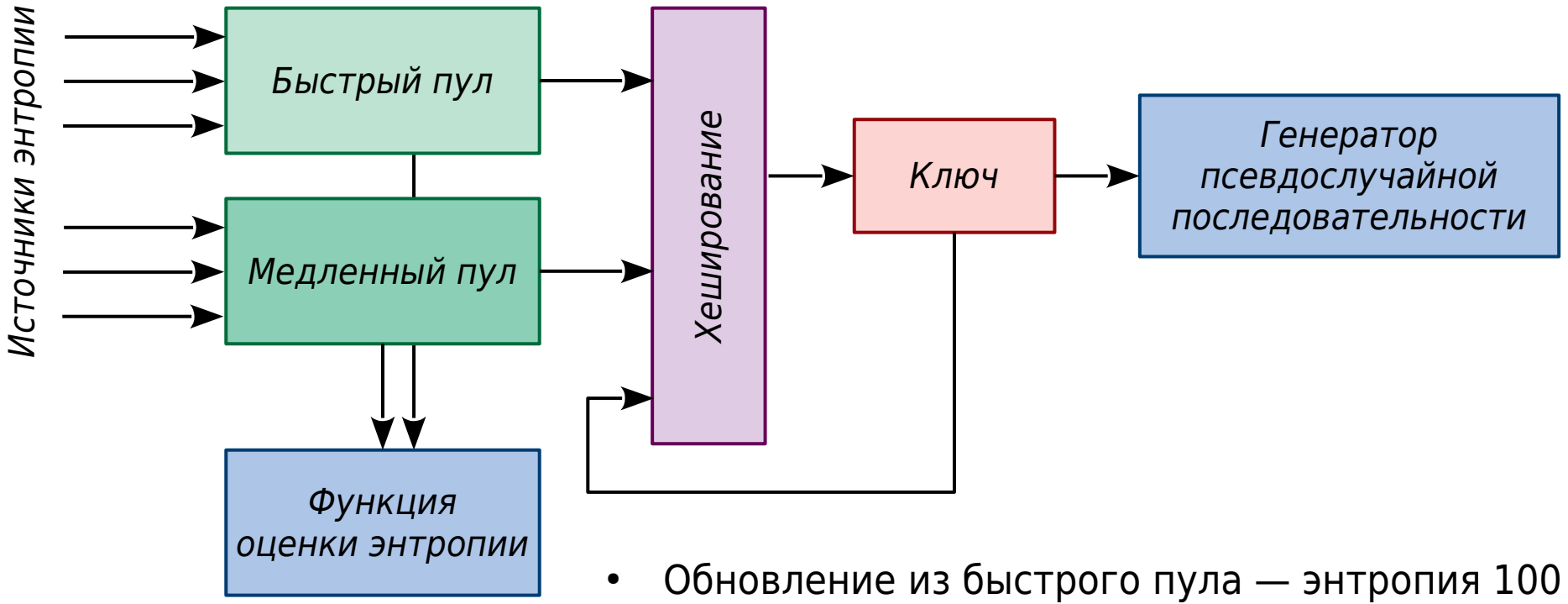




- Квантовые источники

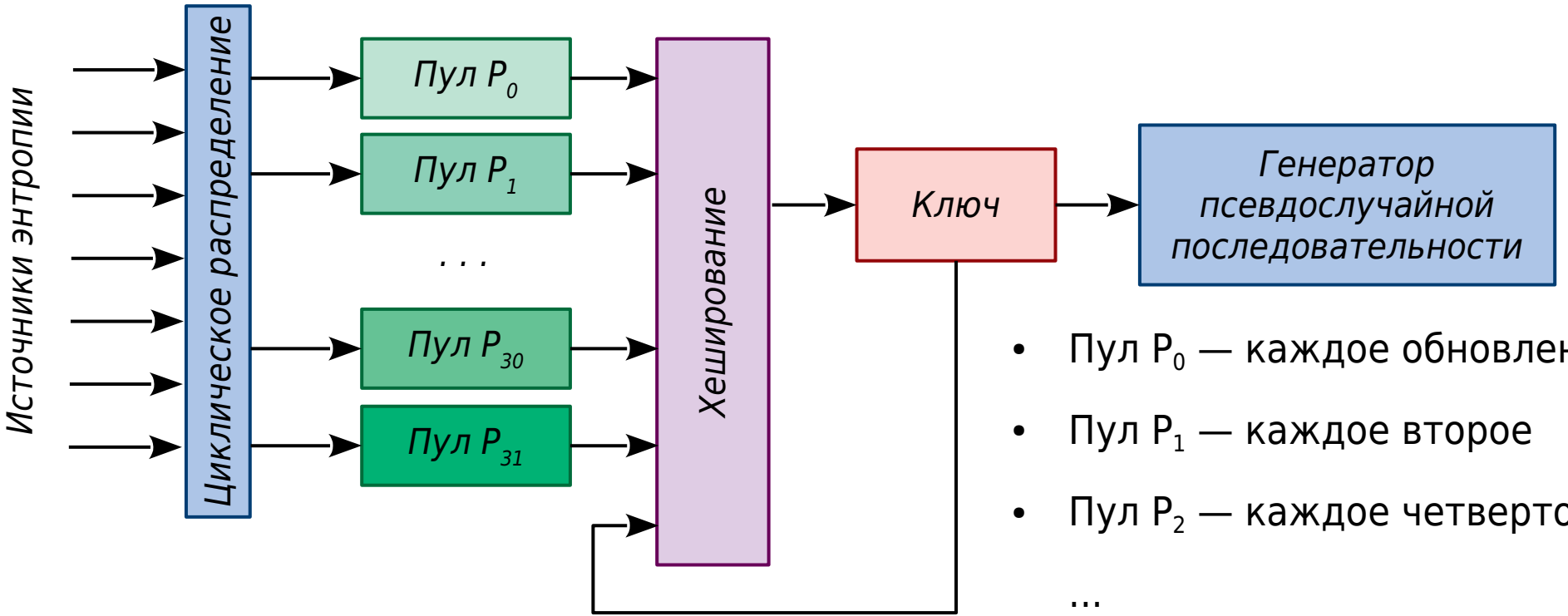


Алгоритм Yarrow



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

Алгоритм Fortuna



- Пул P_0 — каждое обновление
- Пул P_1 — каждое второе
- Пул P_2 — каждое четвертое

  ...
- Пул P_{31} — каждое (2^{31})-ое

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” K. 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.ruberoid@gmail.com
  - @androidruberoid
- Анонсы:
  - facebook.com/kocherga.club
  - vk.com/kocherga_club
  - vk.com/kocherga_prog
- Материалы лекций:
  - github.com/notOcelot/Kocherga_crypto
- Видео:
  - youtube.com/channel/UCeLSDFOndl4eKFutg3oowHg