Детерминированные генераторы псевдослучайных чисел, основанные на блочных шифрах и функциях хэширования: принципы синтеза и методы анализа

Григорий Маршалко

2 апреля 2013 г.

Случайность – основополагающее понятие в криптографии. Где взять?

- Физические датчики – последовательность равновероятных независимых случайных величин
- Программные датчики – детерминированные последовательности со случайным началом

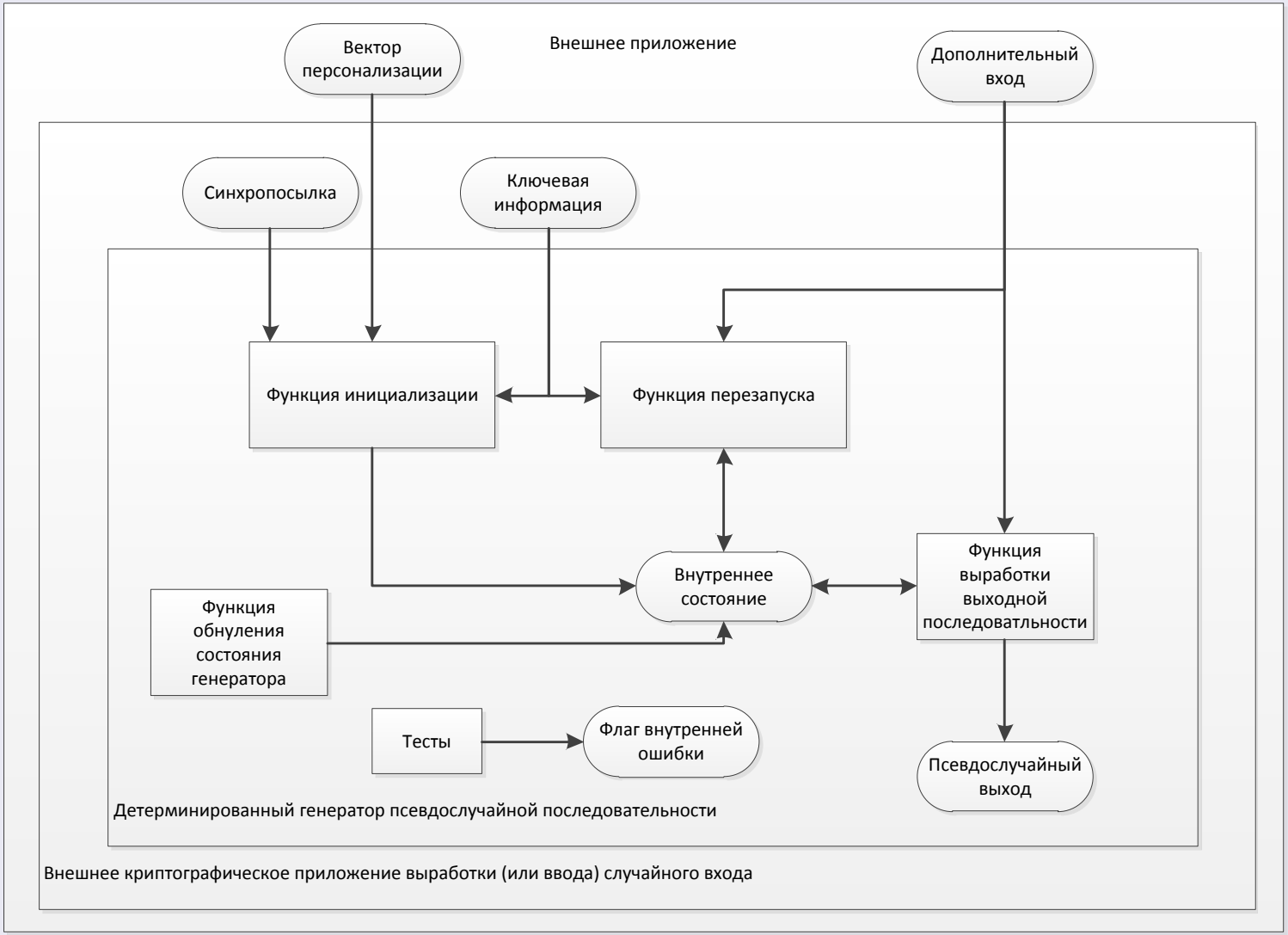
Типы программных датчиков

- специфические датчики (поточные шифры – скорость).
- датчики, основанные на теоретико-числовых задачах (сведение к трудно решаемой задаче – стойкость);
- датчики, основанные на стойких криптографических примитивах (блочном шифре, ключевой или бесключевой функции хэширования – разумный компромисс);

Нормативные документы

- ANSI X 9.17 (Revised) American National Standard for Financial Institution Key Management (Wholesale), American Bankers Association, 1985. 2001.
- FIPS PUB 186 Digital Signature Standerd, NIST, 1994, 2001.
- NIST SP 800-90A. Recommendation for random number generation using deterministic random bit generators. . January 2012.
- ISO/IEC 18031. Information technology. Security techniques. Random bit generation. 2012.
- AIS 20. Functionality classes and evaluation methodology for deterministic random number generators. 1999. (AIS 20. A proposal for: Functionality classes and evaluation methodology for deterministic random number generators. 2011)
- 'отраслевые', коммерческие стандарты (RSAREF,CryptoLib,...)

Высокоуровневая блок-схема программного датчика



Криптографически стойкие датчики

- Анализ свойств датчика без учета возможности восстановления секретного параметра
- Анализ свойств датчика с возможностью восстановления секретного параметра

Анализ без восстановления секретного параметра

- Статистические свойства выходной последовательности
  - Невозможность предугадывания последующих символов по предыдущим
  - Невозможность предугадывания предыдущих символов по последующим
  - Атаки с возможностью манипулирования входными данными (фиксация, зацикливание временных меток, синхропосылок, зависимости в векторе ключевой информации)
- Подход с позиции теории доказуемой стойкости (редукционистская стойкость)

Доказуемая (редукционистская) стойкость

- Редукция стойкости преобразования к стойкости используемого примитива
- Примитив заменяется (псевдо) случайным объектом (подстановкой или функцией)
- Рассматривается задача отличения выходной последовательности от случайной с помощью некоторого алгоритма
- Получаемая оценка зависит от "классической"(общей) задачи (парадокс дней рождения)

Доказуемая (редукционисткая) стойкость

Необходимо отличить выходную последовательность алгоритма Alg, от последовательности вырабатываемой случайным оракулом

$$Adv_{\Sigma,A} = Pr\left[Exp^{Alg}_{\Sigma,A} = 1\right] - Pr\left[Exp^{Rand}_{\Sigma,A} = 1\right].$$

- Σ – некоторый набор ограничений, определяемый видом решаемой задачи,
- Exp^{*}_{Σ} – результат некоторого вычислительного эксперимента A над последовательностью выработанной алгоритмом $*$.

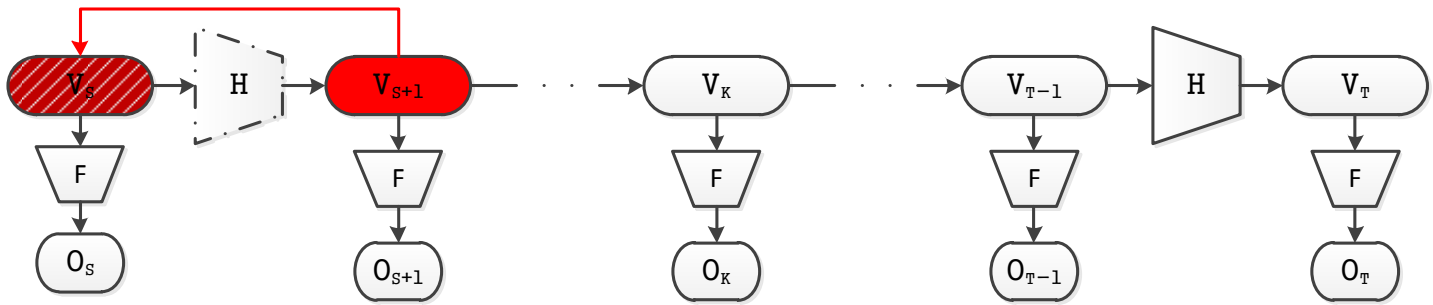
Результирующая характеристика

$$Adv_{\Sigma}(q) = max_{A}\left(Adv_{\Sigma,A}\right),$$

где максимум берется по всем алгоритмам временной сложности q.

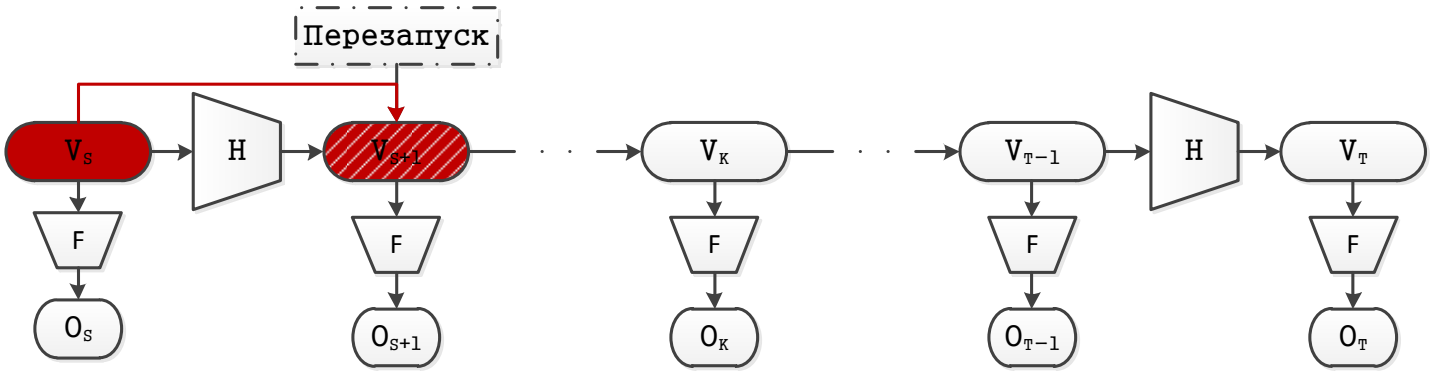
Анализ с восстановлением секретного параметра

- Требование к невозможности чтения назад



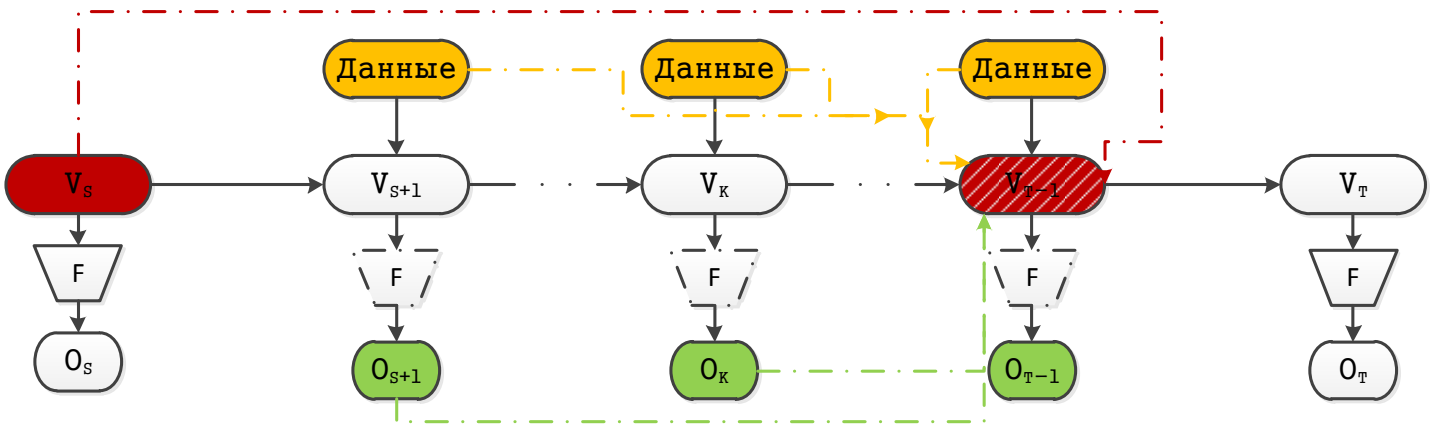
Анализ с восстановлением секретного параметра

- Требование к невозможности чтения назад
- Требование к невозможности чтения вперед



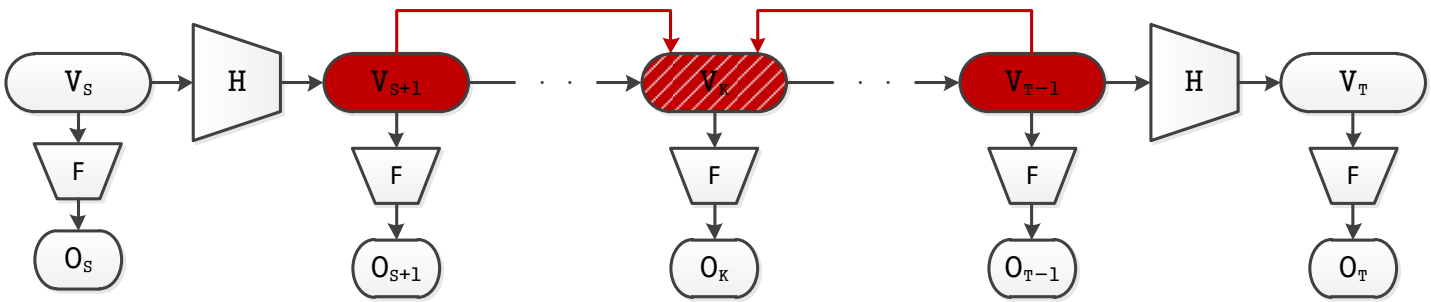
Анализ с восстановлением секретного параметра

- Требование к невозможности чтения назад
- Требование к невозможности чтения вперед
- Атака итеративного угадывания



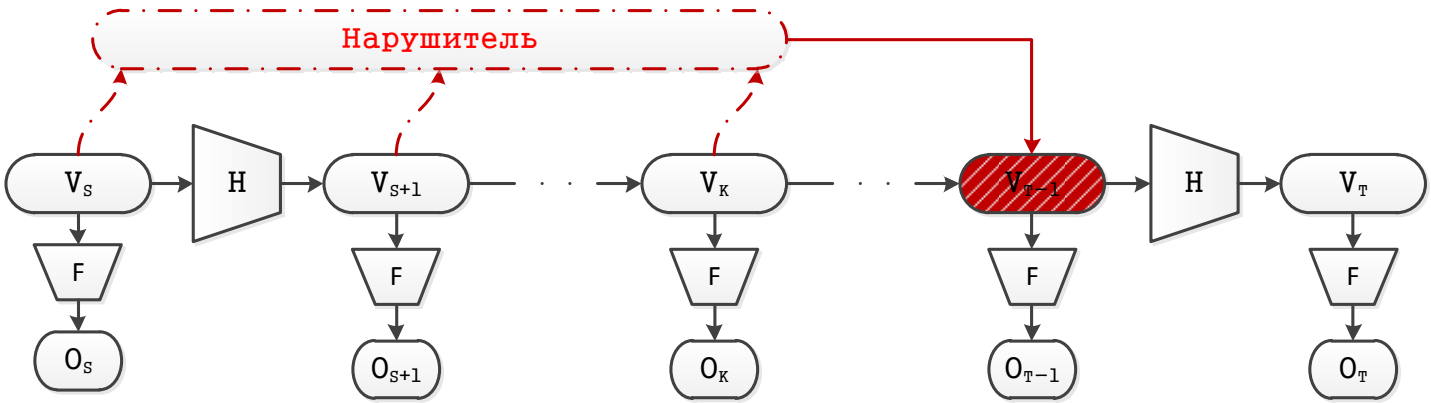
Анализ с восстановлением секретного параметра

- Требование к невозможности чтения назад
- Требование к невозможности чтения вперед
- Атака итеративного угадывания
- Атака встречи посередине



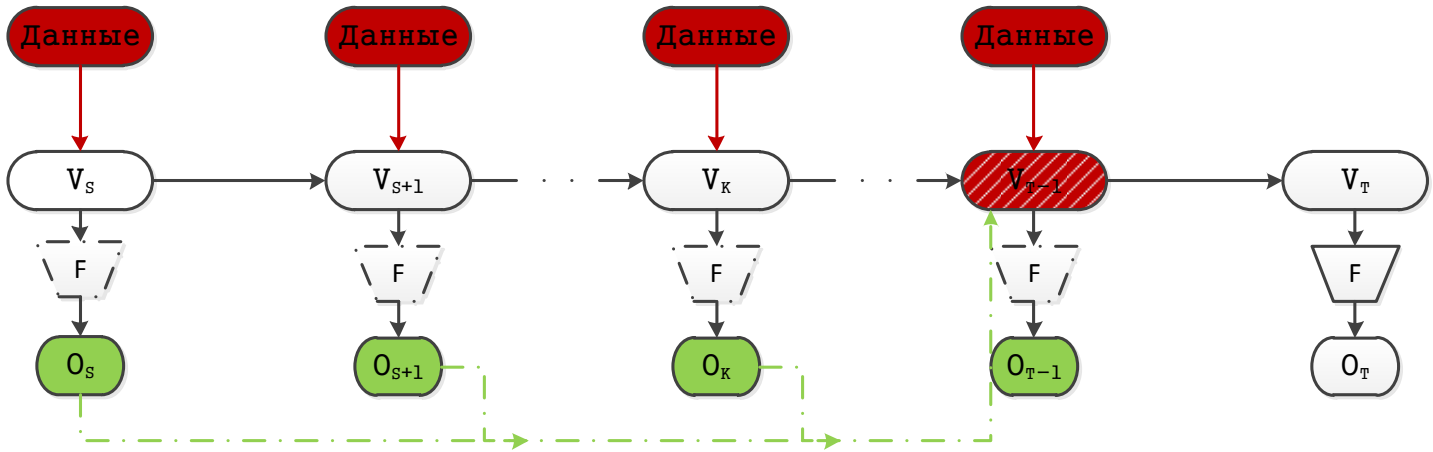
Анализ с восстановлением секретного параметра

- Требование к невозможности чтения назад
- Требование к невозможности чтения вперед
- Атака итеративного угадывания
- Атака встречи посередине
- Атаки на основе побочного излучения



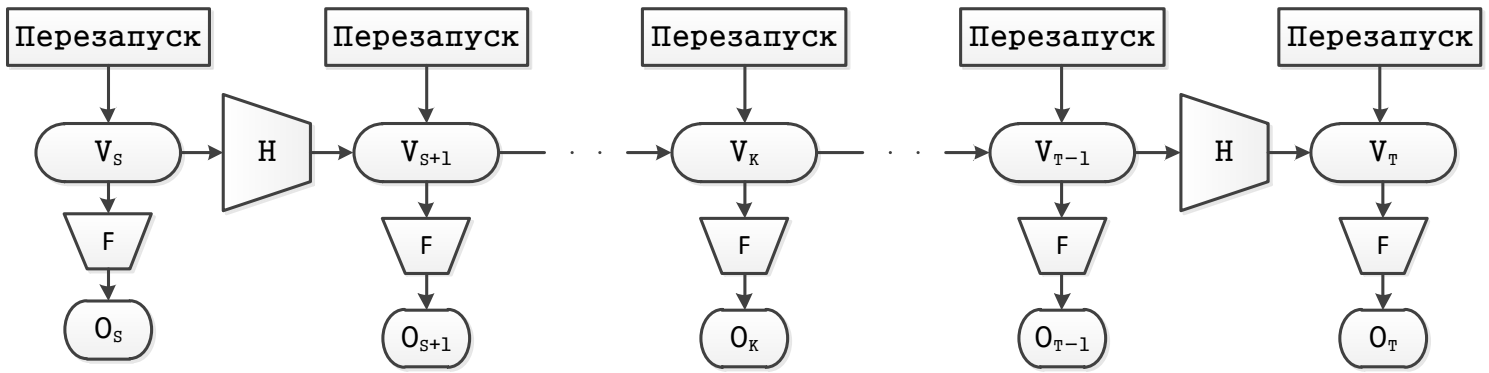
Анализ с восстановлением секретного параметра

- Требование к невозможности чтения назад
- Требование к невозможности чтения вперед
- Атака итеративного угадывания
- Атака встречи посередине
- Атаки на основе побочного излучения
- Атаки с возможностью манипулирования входными данными (фиксация, зацикливание временных меток, синхропосылок, зависимости в векторе ключевой информации



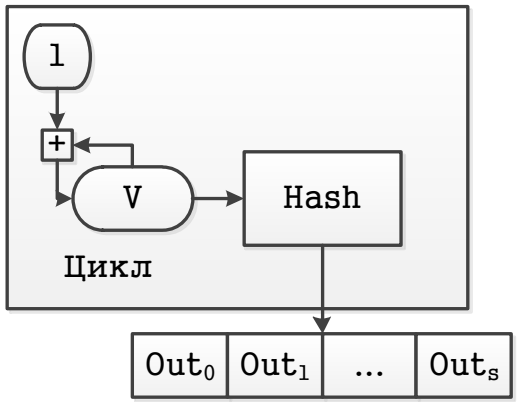
Анализ с восстановлением секретного параметра

- Требование к невозможности чтения назад
- Требование к невозможности чтения вперед
- Атака итеративного угадывания
- Атака встречи посередине
- Атаки на основе побочного излучения
- Атаки с возможностью манипулирования входными данными (фиксация, зацикливание временных меток, синхропосылок, зависимости в векторе ключевой информации



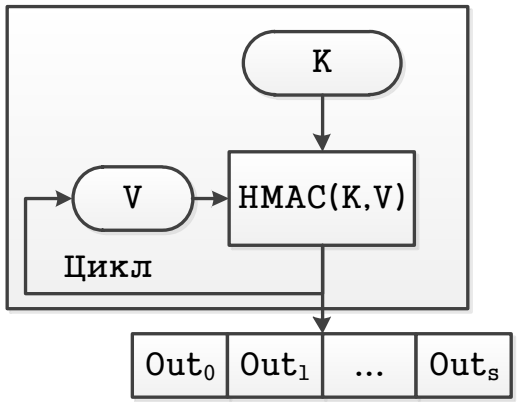
Конструкции датчиков

- На функциях хэширования
  - HASH_DRBG (NIST,ISO,FIPS)



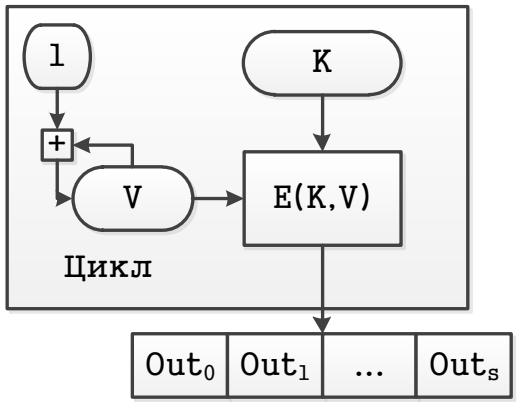
Конструкции датчиков

- На функциях хэширования
  - HASH_DRBG (NIST,ISO,FIPS)
  - HMAC_DRBG (NIST,ISO)



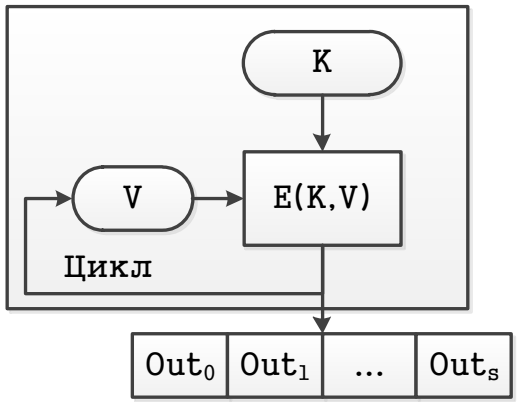
Конструкции датчиков

- На функциях хэширования
  - HASH_DRBG (NIST,ISO,FIPS)
  - HMAC_DRBG (NIST,ISO)
- На блочных шифрах
  - CTR_DRBG (NIST,ISO)



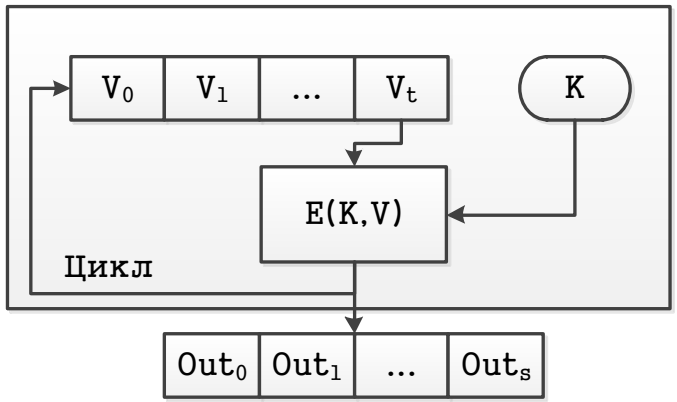
Конструкции датчиков

- На функциях хэширования
  - HASH_DRBG (NIST,ISO,FIPS)
  - HMAC_DRBG (NIST,ISO)
- На блочных шифрах
  - CTR_DRBG (NIST,ISO)
  - OFB_DRBG (ISO,ANSI)



Конструкции датчиков

- На функциях хэширования
  - HASH_DRBG (NIST,ISO,FIPS)
  - HMAC_DRBG (NIST,ISO)
- На блочных шифрах
  - CTR_DRBG (NIST,ISO)
  - OFB_DRBG (ISO,ANSI)
  - Регистровые (Cryptolib)



Сравнение рекомендаций NIST и ISO (CTR_DRBG)

	число интервалов	длина интервала	вероятность коллизии
NIST			
64	2^7	2^{32}	1
128	2^{12}	2^{48}	0.001951219
ISO			
64	2^{13}	2^{16}	0.007782062
128	2^{28}	2^{32}	0.001951219

Для хэш-функций аналогичные вероятности пренебрежимо малы (длина хэш-кода)!

на блочных шифрах

- Модель примитива - случайная подстановка

на хэш-функциях

- Модель примитива - случайная функция

на блочных шифрах

- Модель примитива - случайная подстановка
- Стойкость используемого шифра

на хэш-функциях

- Модель примитива - случайная функция
- Стойкость используемой (ключевой) хэш-функции

на блочных шифрах

- Модель примитива - случайная подстановка
- Стойкость используемого шифра
- Размер блока используемого шифра (ГОСТ 28147-89)

на хэш-функциях

- Модель примитива - случайная функция
- Стойкость используемой (ключевой) хэш-функции
- Длина хэш-кода

на блочных шифрах

- Модель примитива - случайная подстановка
- Стойкость используемого шифра
- Размер блока используемого шифра (ГОСТ 28147-89)
- Парадокс дней рождений на интервале перезапуска

на хэш-функциях

- Модель примитива - случайная функция
- Стойкость используемой (ключевой) хэш-функции
- Длина хэш-кода
- Характеристики случайного отображения на интервале перезапуска

на блочных шифрах

- Модель примитива - случайная подстановка
- Стойкость используемого шифра
- Размер блока используемого шифра (ГОСТ 28147-89)
- Парадокс дней рождений на интервале перезапуска
- Распараллеливание (CTR_DRBG)

на хэш-функциях

- Модель примитива - случайная функция
- Стойкость используемой (ключевой) хэш-функции
- Длина хэш-кода
- Характеристики случайного отображения на интервале перезапуска
- Распараллеливание (Hash_DRBG)

на блочных шифрах

- Модель примитива - случайная подстановка
- Стойкость используемого шифра
- Размер блока используемого шифра (ГОСТ 28147-89)
- Парадокс дней рождений на интервале перезапуска
- Распараллеливание (CTR_DRBG)
- Скорость

на хэш-функциях

- Модель примитива - случайная функция
- Стойкость используемой (ключевой) хэш-функции
- Длина хэш-кода
- Характеристики случайного отображения на интервале перезапуска
- Распараллеливание (Hash_DRBG)
- Скорость (HMAC_DRBG – медленный)

Спасибо за внимание!