Кафедра 42
Криптология и дискретная математика
Тел. 324-7334; факс. 323-9137; e-mail: kaf42@mail.ru.

Построение ДСЧ на основе измерения времени доступа к оперативной памяти

Агафьин С.С.

РусКрипто – 2015 г.

Использование датчиков случайных чисел

- Генерация криптографических ключей.
- Генерация случайных значений для протоколов электронной подписи и установления ключа обмена.
- Генерация случайных значений для протоколов установления защищенного соединения.
- Прочие задачи защиты информации (например, рандомизация адресов с помощью ASLR).

Модель нарушителя

- Нарушитель Н3 согласно «Методическим рекомендациям по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» от 21.02.2008г.
- Способен:
  - влиять на пользовательские процессы;
  - воздействовать на аппаратуру и сети энергоснабжения;
  - проводить статистический анализ последовательностей известными методами;

Сравнение существующих ДСЧ

Анализируемый ДСЧ	Критерий сравнения		
	Наличие полноценного обоснования случайности	Высокая скорость (≥1 Кбит/с)	Совместимость с большинством аппаратных конфигурация
Биологические ДСЧ (КриптоПро CSP, PGP, …)	+	–	+/–
Встроенные ДСЧ (Intel Secure Key, VIA Padlock)	+/–	+	–
Дополнительные устройства ДСЧ (PCI-платы и USB-токены)	+	+	–
ДСЧ на основе измерения отклика периферийного оборудования (CryptGenRandom, /dev/random)	–	+	–
ДСЧ на основе измерения погрешности счетчиков времени (Попов, Смышляев: РусКрипто'13)	+/–	+	+
ДСЧ на основе измерения времени доступа к памяти (Mueller: chronox.de)	–	+	+

Причины рассмотрения работы с оперативной памятью

- Простота контуров взаимодействия:
  - Встроенный контроллер памяти (исключен «северный мост» как отдельный чип);
  - Стабильное напряжение от блока питания;
  - Точные умножители.
- Наличие случайной составляющей:
  - В процессорах Intel и AMD используются технологии энергосбережения, что привело к исключению механизма полной стабилизации частоты;
  - Несовпадение частот процессора и памяти.

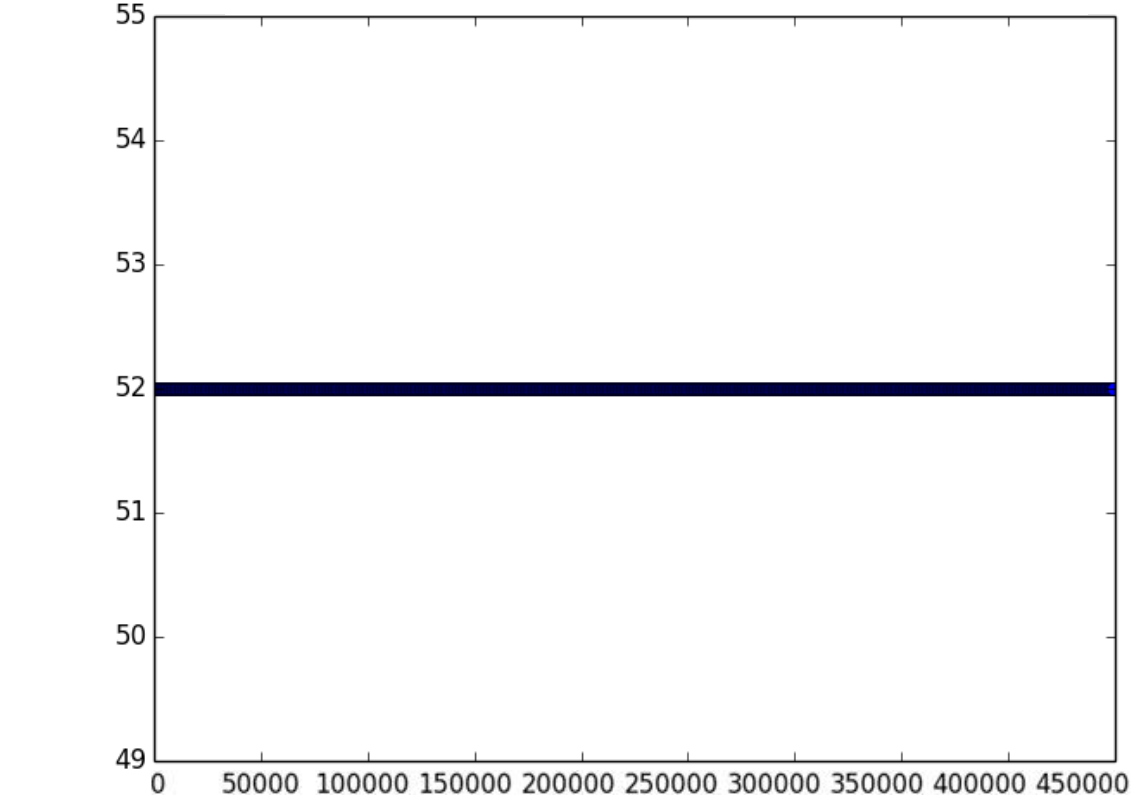
Предварительные условия для получения случайных данных

- Отключение всех ядер процессора, кроме одного.
- Отключение HyperThreading и управления энергопотреблением.
- Отключение поддержки аппаратной виртуализации.
- Запрет аппаратных прерываний (cli).
- **Отключение кэширования:**
  - Установка 31-го бита в CR0;
  - Нужен kernel-mode (ДСЧ в модуле ядра / драйвере).

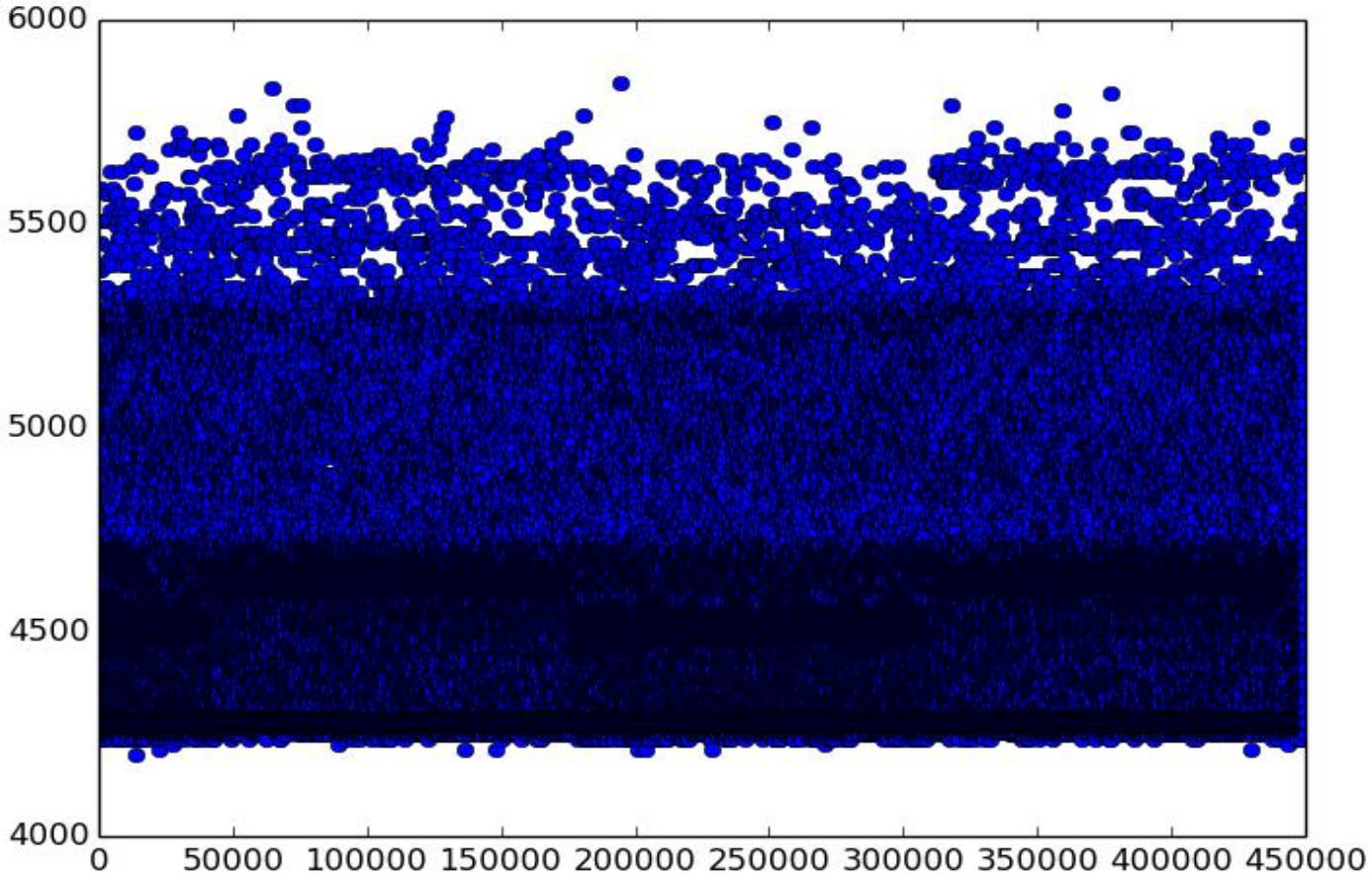
Алгоритм измерения времени доступа к оперативной памяти

1. Инициализация счетчика (k:=0).
2. Ожидание конвейера (CPUID).
3. Замер времени (RDTSC).
4. Запоминание времени в RDI:
    1. mov edi, edx
    2. shl rdi, 32
    3. mov eax, edi
5. Замер времени с сериализацией (RDTSCP).
6. Занесение разности (5) и (3) в массив.
7. if (++k < MAX_LIMIT) goto (2).
8. Завершение алгоритма.

Измерение времени исполнения инструкций (с кэш-памятью)

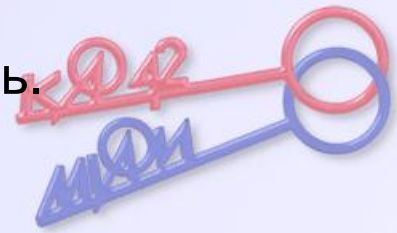


Измерение времени исполнения инструкций (без кэш-памяти)



Исключение периодичности

- Представим полученную последовательность как цифровой сигнал.
- Пусть:
  - N – число измерений,
  - $\{x_k\}$ – множество измерений,
  - $\{X_n\} = \text{ДПФ}(\{x_k\})$ – результат дискретного преобразования Фурье,
  - ${I^p}_k = \begin{cases} 1, \text{если } |X_n| \geq p, \\ 0, \text{если } |X_n| < p. \end{cases}$, где $p \in \mathbb{R}$, – индикатор того, что амплитуда превышает p,
  - $C_p = \sum_k {I^p}_k$, – число гармоник с высокой амплитудой,
  - $\theta_p = \frac{C_p - C_{1.05p}}{N}$ – доля гармоник, чья амплитуда попадает в 5% интервал,
- $\theta_p = f(p).\ f(0) = 0, f(\max(|X_n|) = 1 \Rightarrow \exists p' : \max(f) = \theta_{p'}$
- ${X'}_i = \begin{cases} 0, , \text{если} |X_i| > p' \text{ и } i = 0, \\ X_{i-1}, \text{если} |X_i| > p' \text{ и } i > 0, \\ X_i, \text{если } |X_i| < p'. \end{cases}$
- $x' = FT^{-1}(\{X'_n\})$ – истинно случайная последовательность.

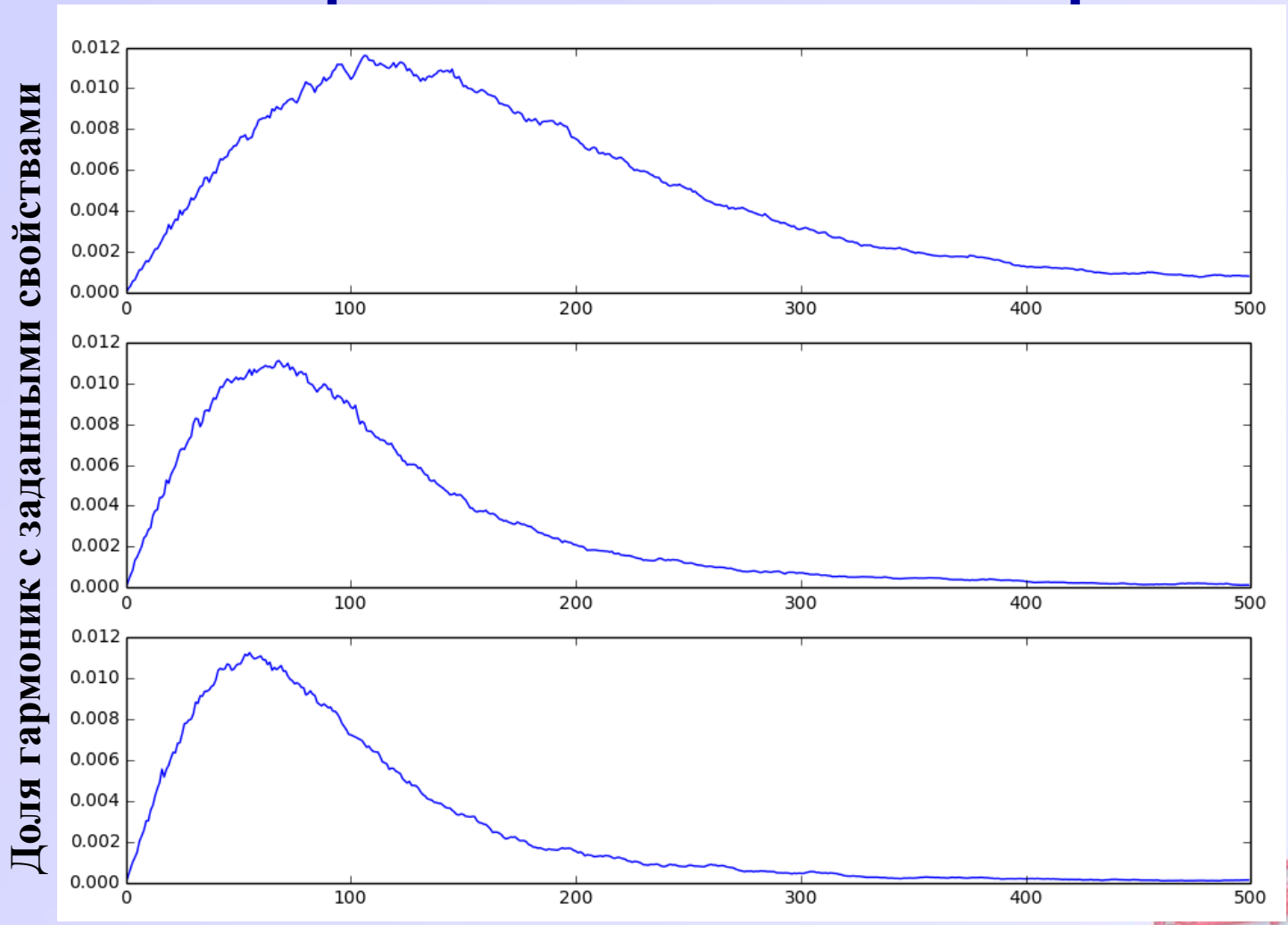


Тестовые стенды

Номер стенда	Конфигурация
1	AMD Athlon FX-4200 (Bulldozer), DDR3-1866
2	AMD Athlon X2, DDR3-2400
3	Intel Core i7 (Sandy Bridge), DDR3-1866
4	Intel Core i5 (Haswell), DDR3-2400

Разложение в ряд Фурье

Доля гармоник в рассматриваемом интервале

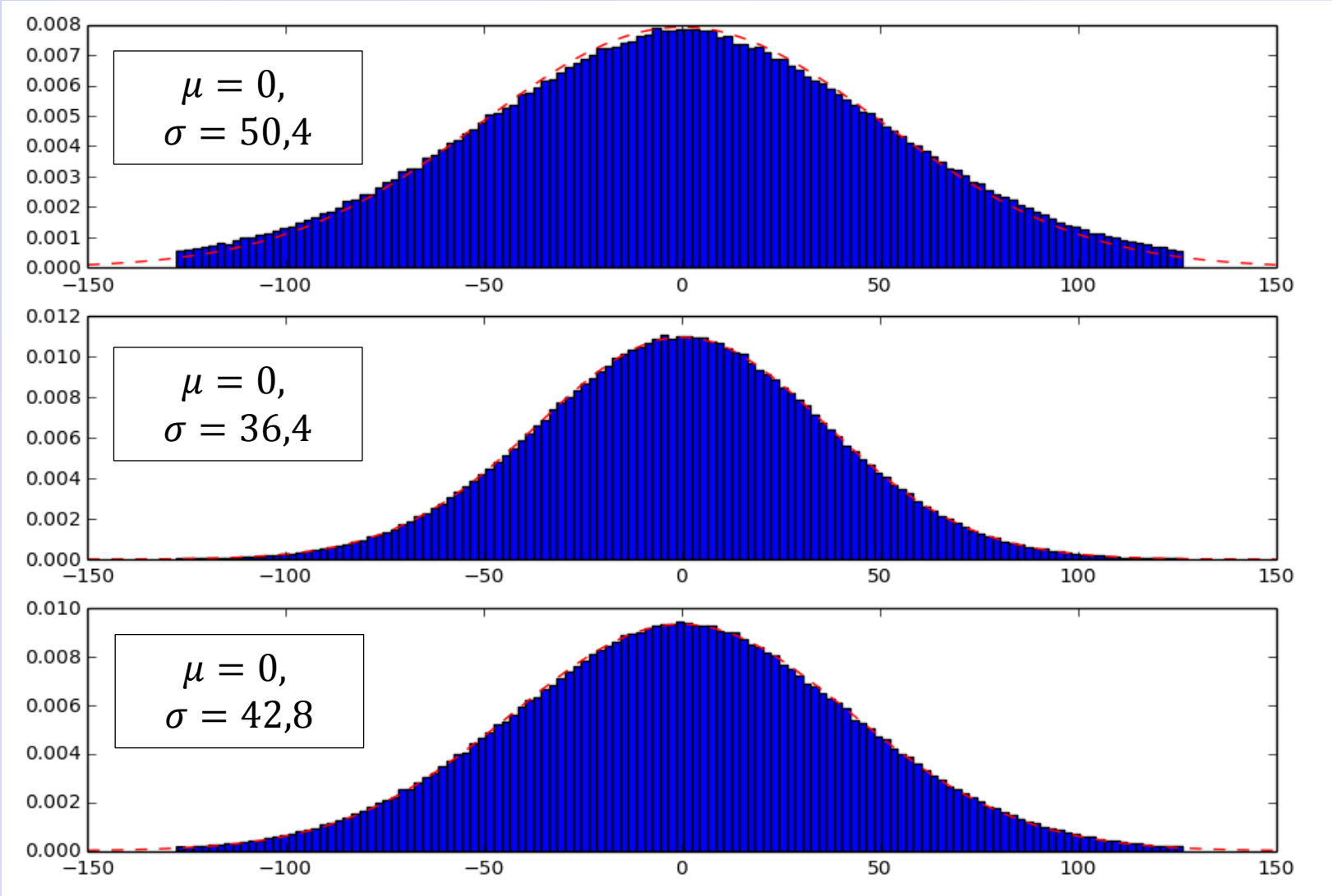


Пороговое значение амплитуды, 10^4

Результаты фильтрации

Номера стенда	Пороговое значение p'	Доля фильтруемых гармоник
1	106334	20.4%
3	68198	18.2%
4	55410	19.8%

Распределение элементов в последовательности



Оценка производительности свойств

Номер стенда	Среднее отклонение σ	Энтропия элементов последовательности (бит / 1 элемент)	Время генерации (сек.)	Производи-тельность (Кбит / сек.)
1	50,4	5,3	13,50	43,13
3	36,4	5,0	14,10	38,96
4	42,8	5,2	13,80	41,39

Пройдены все тесты из набора NIST SP800-22.

Надежность реализации предлагаемого ДСЧ

- Отсутствует зависимость между статистическими характеристиками выходной последовательности и следующими величинами:
  - средним значением напряжения процессора (в штатном диапазоне);
  - средним значением температуры процессора (в штатном диапазоне);
  - сопротивлением и энергопотреблением устройств, подключенных параллельно к ЭВМ.

Спасибо за внимание!

sagafyin@gmail.com