
# О подходах к построению ДСЧ в программных СКЗИ

Попов Владимир Олегович
Смышляев Станислав Витальевич

# Описание проблематики

• В СКЗИ датчики случайных чисел используются для выработки ключей и криптографических параметров (синхропосылки, UKM, seed и др.). Для обеспечения необходимой производительности совместно используются ДСЧ и ПДСЧ.

**Общие требования к ДСЧ:**

- Близость выходной последовательности к последовательности независимых равномерно распределенных случайных величин (в определенном смысле).
- В частности: невозможность по отрезку выходной последовательности предсказывать предшествующий или последующий отрезок.

# Требования к ДСЧ в СКЗИ

**Дополнительные требования к ДСЧ:**

При использовании ДСЧ для использования в программных СКЗИ возникают дополнительные специфические требования.

- Обязана присутствовать возможность гибкой настройки ДСЧ для порождения различных типов величин.
- Для одних типов задач должна обеспечивать максимальная производительность (например, при порождении синхропосылок), для других типов – наилучшие свойства выходной последовательности (например, при порождении ключевого материала).
- При всех вариантах использования обязана обеспечиваться непредсказываемость выходных символов даже в случае сбоев аппаратных компонент.
- Возможность параллельной работы ДСЧ в независимых сессиях с сохранением обеспечения требуемых свойств.

# ПДСЧ на основе случайного автомата

- Предлагаемая схема реализована по схеме случайного автомата со случайным выбором начального состояния автомата при его начальной инициализации и случайной функцией перехода.

- Аналог: конструкция Барака-Халеви.
  - refresh(s, x) = G(s $\oplus$ extract(x)).
  - output(s)|next(s) = G(s).

- Для случайного выбора начального состояния автомата используется физический датчик случайных чисел (ФДСЧ) ПАК защиты от НСД (при его наличии в составе СКЗИ) или биологический датчик случайных чисел (БиоДСЧ), основанный на случайном распределении времени между моментами отжатий оператором клавиш клавиатуры или между моментами изменений движения мыши.

- Для определения случайной функции перехода используются также источники времени событий, наступающих в процессе работы СКЗИ.

# ПДСЧ на основе случайного автомата

- ПДСЧ работает следующим образом: случайной последовательностью, вырабатываемой физическим ДСЧ, инициализируется случайное начальное состояние автомата, автомат вырабатывает от инициального состояния последовательность с использованием последовательности случайных переходов.

- В основе ПДСЧ находится конечный автомат A, который строится на базе алгебраической структуры с трудно решаемой задачей (логарифмирование в мультипликативной группе конечного поля, группе точек эллиптической кривой и т. п.).

# ПДСЧ на основе случайного автомата

Конструкция основана на следующих элементах.

- S – множество всех возможных состояний (например, группа точек эллиптической кривой над конечным полем);
- R – конечное множество;
- F(s,r) – функция, трудно обратимая по r при фиксированном s и трудно обратимая по s при фиксированном r;
- H(s) – трудно обратимая функция.

Общая структура ПДСЧ:

- $s(1) = s_0$
- $r(i) \in R$, $s(i+1) = F(s(i), r(i))$, i=1,2,...
- out(i) = h(s(i)), i=2,3,...

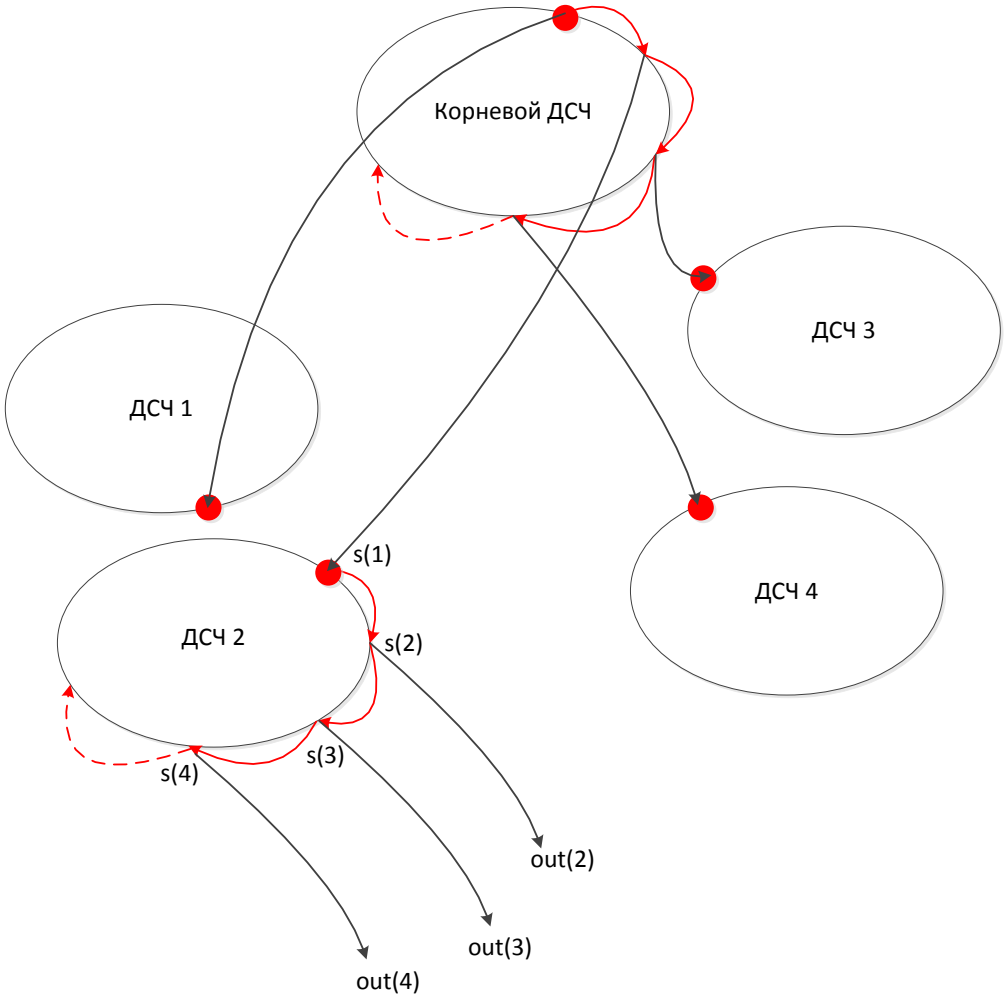
# ПДСЧ на основе случайного автомата

Общая структура ПДСЧ:

- $s(1) = s_0$
- $r(i) \in R$, $s(i+1) = F(s(i), r(i))$, $i=1,2,...$
- $out(i) = h(s(i))$, $i=2,3,...$

Частный случай:
S – группа точек эллиптической кривой простого порядка q,
$F(s,r) = s + (r+x(s) \bmod \sqrt{q})G$, где G – порождающий элемент S.

# ПДСЧ на основе случайного автомата



# Свойства ПДСЧ

- Каждое изменение состояния зависит от дополнительного входа. Выбор источника данных, подаваемых на данный вход, позволяет контролировать баланс между производительностью ПДСЧ, возможностью его использования в том или ином классе систем и гарантиями качества его выходной последовательности.

- Даже в случае вырожденной последовательности r(i) обеспечивается период не менее $\sqrt{q}$, трудность нахождения по отрезку выходной последовательности предшествующих или последующих символов, пренебрежимо малая вероятность совпадений выходных значений.

- Начальное состояние ДСЧ для каждой сессии вырабатывается с помощью корневого ДСЧ. Инициализация корневого ДСЧ происходит с помощью наилучшего доступного в конкретной системе источника энтропии.

# Источники энтропии в компьютерных системах

**Вносимая человеком/внешней средой энтропия**

- Моменты нажатия клавиш на клавиатуре
- Изменения направления движения мыши при хаотическом движении и моменты этих изменений
- Фотографирование хаотической системы (пример: Lavarand)
- Координаты касаний тачскрина высокого разрешения при требовании попаданий в круги, появляющиеся на экране в случайном месте

**Проблемы:**

- Трудности в обосновании
- Низкая скорость работы
- Требование присутствия человека около системы
- Неуместность использования во вспомогательных системах

# Источники энтропии в компьютерных системах

**Накопление энтропии процессов в КС (Linux RNG, Windows RNG)**

- События с клавиатуры и мыши (без специального сбора данных специфическими действиями пользователя)
- Операции чтения/записи информации с жесткого диска (Linux RNG, Windows RNG)
- Прерывания (Linux RNG, Windows RNG)

**Проблемы (Gutterman, Pinkas, Reinman, Dorrendorf):**

- Легкость построения DoS-атак (в Linux 2.6.26 ряд контрмер).
- Трудность корректного использования в среде с несколькими пользователями.
- Возможность навязывания накапливаемых данных для пула (после работ Гуттермана и Доррендорфа – ряд средств противодействия).
- При доступе к пулу – потенциальная возможность предсказывания будущих выходных значений (NIST Special Publication 800-90A, Rev 1: общая проблема, если нет гарантий нового случайного входа перед порождением каждого выходного значения).

# Предлагаемый метод

**Предположения о системе**

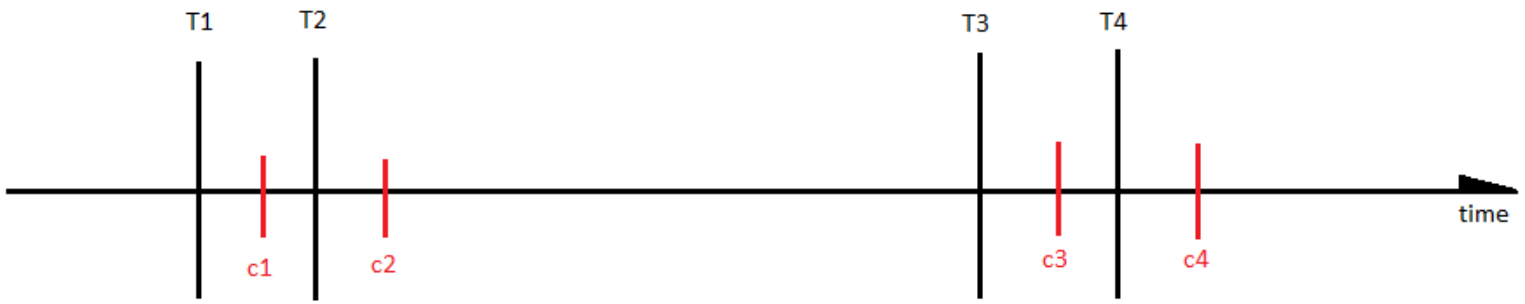
Далее будем предполагать, что выполняются следующие требования.

- Требуется независимость физических источников, на которых базируются счетчики CR и CT.
- Требуется, чтобы за время одного изменения значения CT было возможно провести не менее W циклов с последовательным измерением CT, CR, CT, CR.
- Требуется, чтобы за время одного цикла с последовательным измерением CT, CR, CT, CR значение CR менялось не менее V раз.
- Величины V и W выбираются исходя из требований к быстродействию, некоррелированности соседних выходных случайных величин, энтропии, дисперсии.

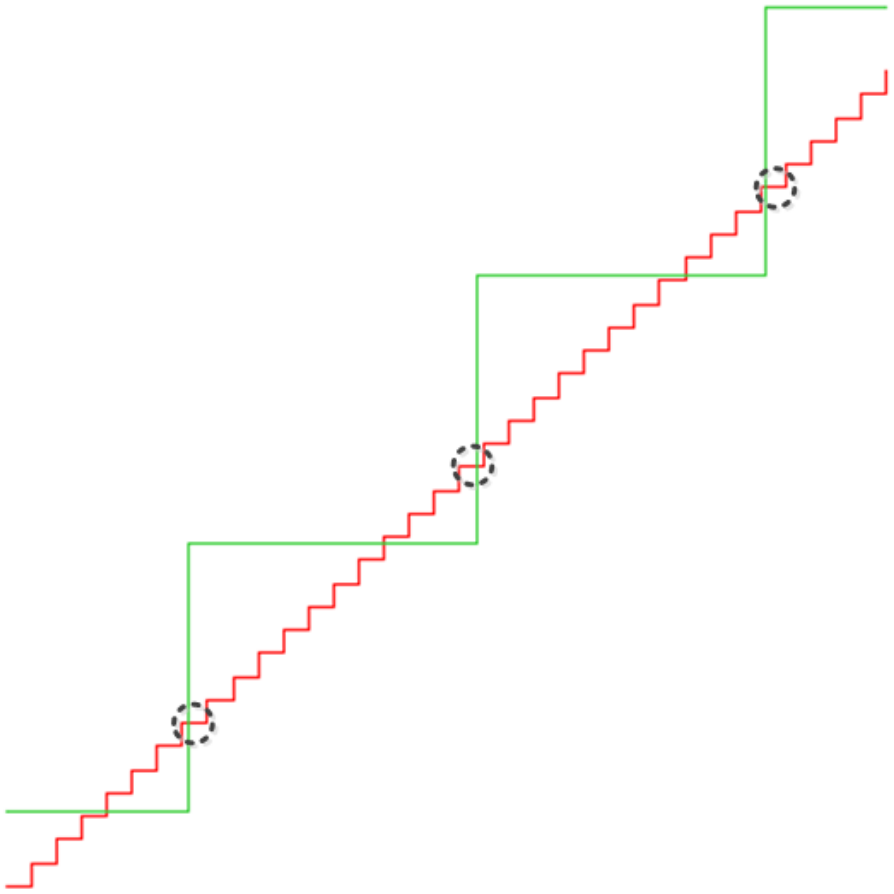
# Схема работы ДСЧ

- Рассмотрим эксперимент, в течение которого поочередно снимаются следующие значения:
  T1, значение CT; c1, значение CR; T2, значение CT; c2, значение CR.

- В случае если T2>T1, то естественно считать, что значение c1 с наилучшей возможной точностью соответствует значению CR в момент изменения значения CT. Назовем схему, в которой описанный эксперимент проводится до выполнения условия T2>T1, ловушкой.



# Схема работы ДСЧ

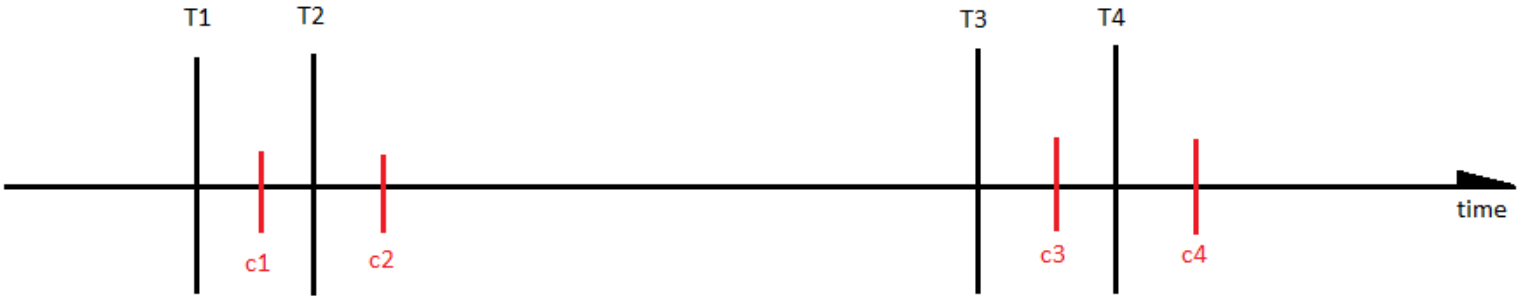


# Схема работы ДСЧ

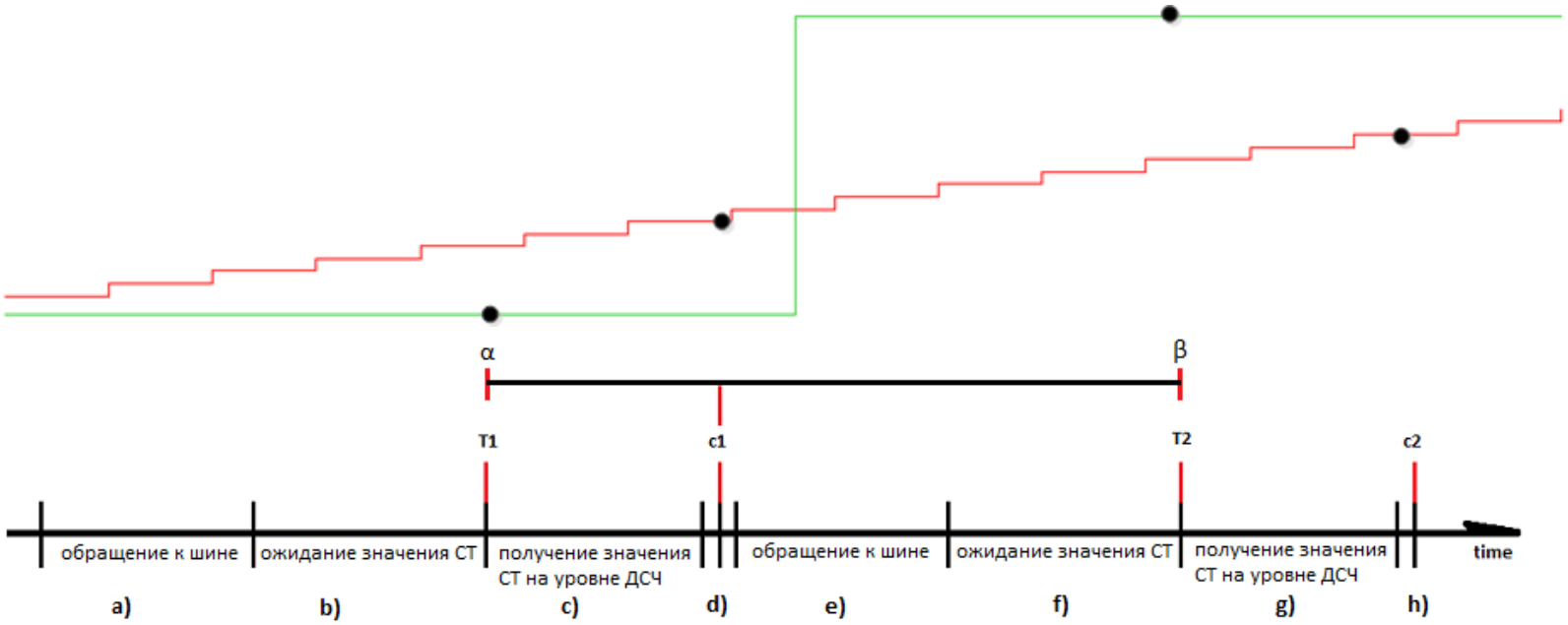
- Будем рассматривать последовательные пары ловушек (считается, что во второй из двух наблюдаются T3,c3,T4,c4), между которыми производятся вызовы процедуры ожидания, и соответствующие восьмерки s(i)=(T1(i),c1(i),T2(i),c2(i),T3(i),c3(i),T4(i),c4(i)), i=1,2,…

- Эти восьмерки образуют обозреваемую, нормируемую и преобразуемую для порождения очередного элемента выходной последовательности датчика последовательность.

- Восьмёрки s(i) преобразуются в скалярные величины g(i) некоторой детерминированной функцией после чего значения g(i), i=1,2,…,n, некоторым образом преобразуются в битовый выходной набор ДСЧ f(i), i=1,2,…,m(n).

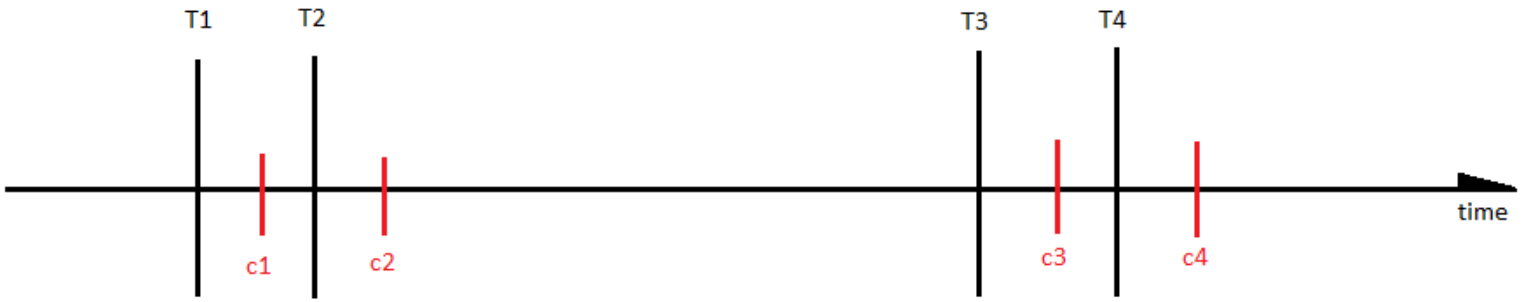


# Схема работы ДСЧ



# Схема работы ДСЧ

- Будем для получения последовательности g(i) использовать детерминированные функции вида a(i) - b(i)*k(i), где a(i) = c3(i)-c1(i), b(i) = T4(i)-T2(i), k(i) – некоторая зависящая только от s(1),s(2),…,s(i) величина.

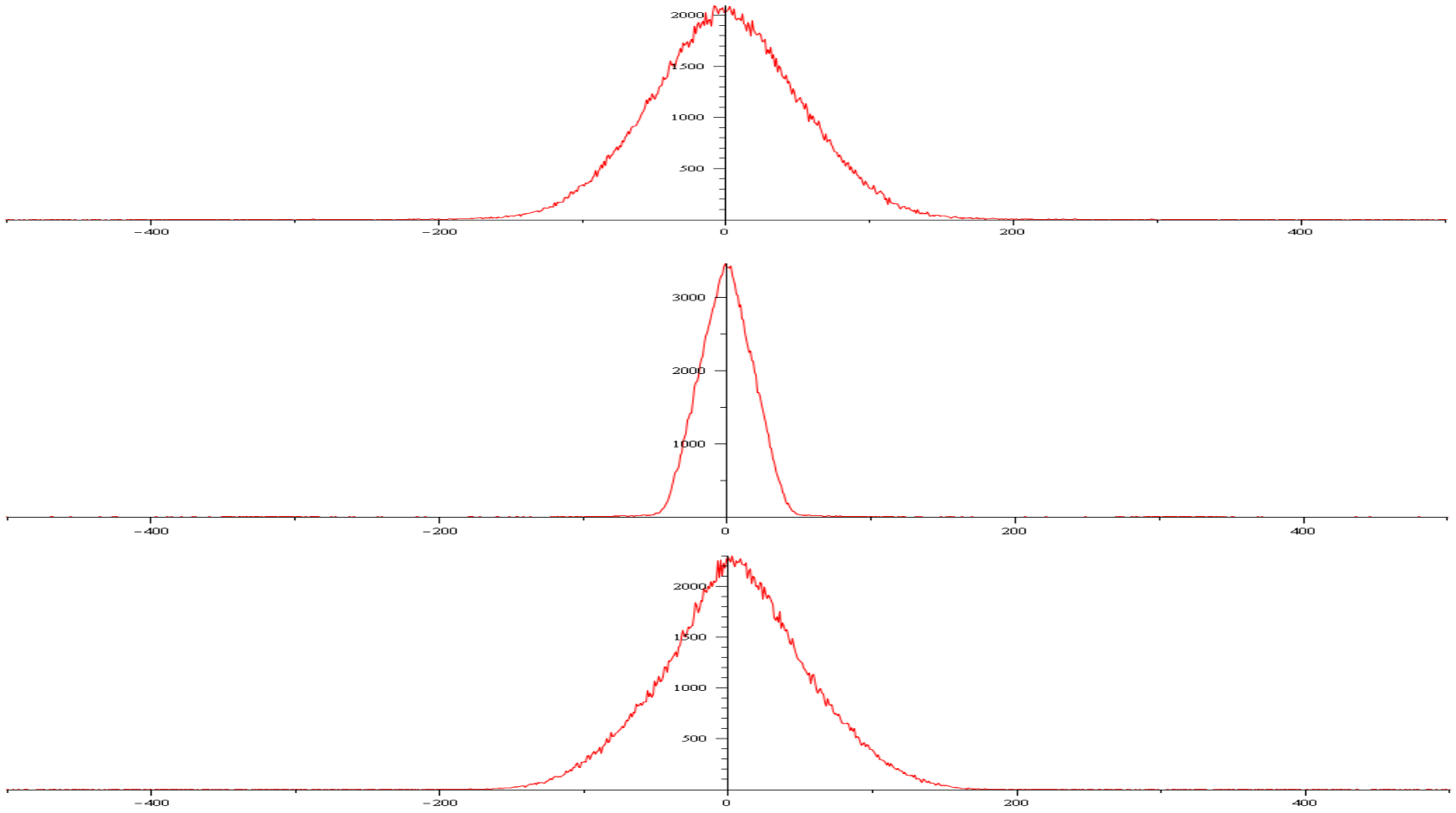


# Экспериментальные данные: методика исследований

1. Распределение. Для определения свойств распределения случайных величин g(i) вычислялись их моменты до пятого включительно, вычислялась выборочная энтропия по младшим 8 битам. Полученные данные свидетельствуют о симметричности распределений относительно оси Oy и об убывании плотности вероятности с удалением от нуля, а также о достаточности значений дисперсии и энтропии для построения датчика.

2. Независимость. Для проверки того, что случайные величины g(i) независимы в совокупности, производились следующие процедуры. Для пар (g(i),g(i+q)), отстоящих на расстояние q=1,2,...9 проводились следующие проверки. Числовая ось делилась на равномощные подмножества, соответствующие выделению нескольких битов в двоичной записи g(i) и g(i+q), затем проверялась гипотеза о независимости событий, соответствующих попаданию g(i) и g(i+q) из одной пары в определенную пару подмножеств. Проверка данной гипотезы производилась с помощью хи-квадрат критерия с уровнем значимости 0.05. Результаты экспериментов подтверждают независимость случайных величин g(i).

3. Однородность. На каждой из систем эксперименты проводились как без нагрузки, так и под существенной нагрузкой. Влияния нагрузки на эффективность работы датчика, или на свойства порождаемых случайных величин замечено не было.



# Экспериментальные данные: результаты

Платформы: x86, x64, ARM, SPARC, с ОС семейств Windows NT, UNIX, Linux, Solaris, MacOS, iOS.

Приведенные утверждения и полученные в результате экспериментов данные о независимости и выборочные оценки энтропии случайных величин g(i) позволяют сделать заключение о наличии неустранимой нестабильности, связанной со свойствами функционирования вычислительной системы.

При этом неопределенность g(i) складывается из нестабильности времени запроса и ожидания ответа на запрос при вычислении значения CT и нестабильности времени изменения значения CT относительно CR с точки зрения наблюдателя при отделенных друг от друга экспериментах. Таким образом, энтропия g(i) всегда не меньше энтропии времени запроса и ожидания ответа на запрос при вычислении значения CT, что подтверждается и экспериментами.

Другими словами, при проведении экспериментов в соответствии с описанной моделью происходит накопление энтропии, происходящей из неустранимых источников неопределенности в вычислительной системе.


# СПАСИБО ЗА ВНИМАНИЕ!

**КРИПТО-ПРО – ключевое слово в защите информации**

http://www.cryptopro.ru
vpopov@cryptopro.ru
svs@cryptopro.ru

Тел./факс:
+7 (495) 780-48-20
+7 (495) 660-23-30