Клеточные автоматы и их свойства применительно к генерации псевдослучайных последовательностей

Сухинин Борис

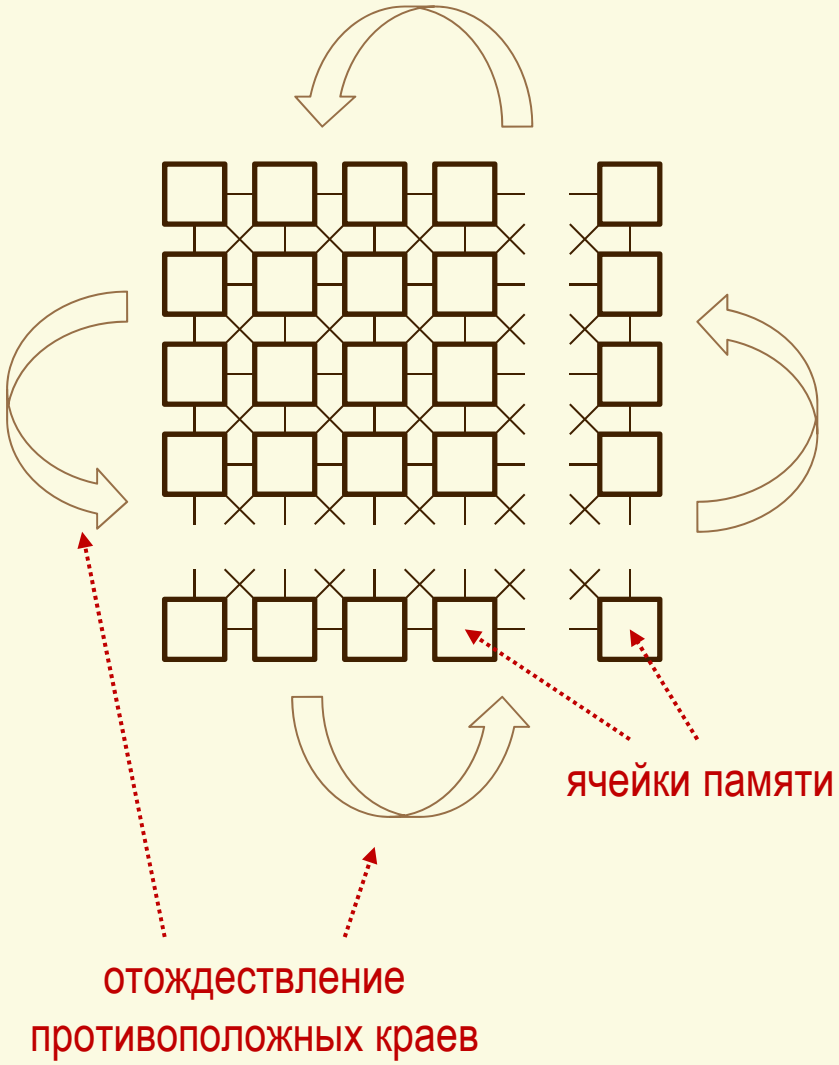
МГТУ им. Н.Э. Баумана

Классические клеточные автоматы (ККлА)

Однородные двумерные булевы клеточные автоматы

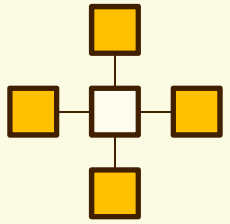
Классический клеточный автомат

- Внутреннее состояние – набор ячеек памяти
  - Принимают двоичные значения
  - Расположены в узлах двумерной решетки
  - Неразличимы по свойствам (противоположные края решетки отождествляются) → однородность

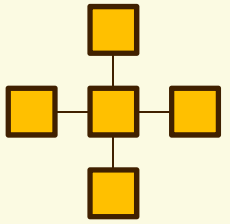


Классический клеточный автомат

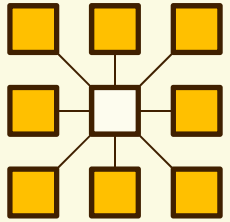
- Правила перехода
  - Значение всех ячеек изменяется синхронно и одновременно
  - Значение каждой ячейки определяется как булева функция – локальная функция связи
  - Локальная функция связи одинакова для всех ячеек
  - Аргументами функции являются значения непосредственно смежных ячеек и, возможно, данной ячейки → локальность
  - Рассматриваются функции от 4, 5, 8 и 9 аргументов



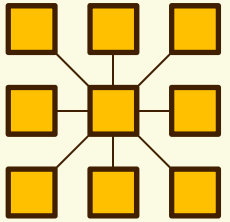
4 аргумента



5 аргументов



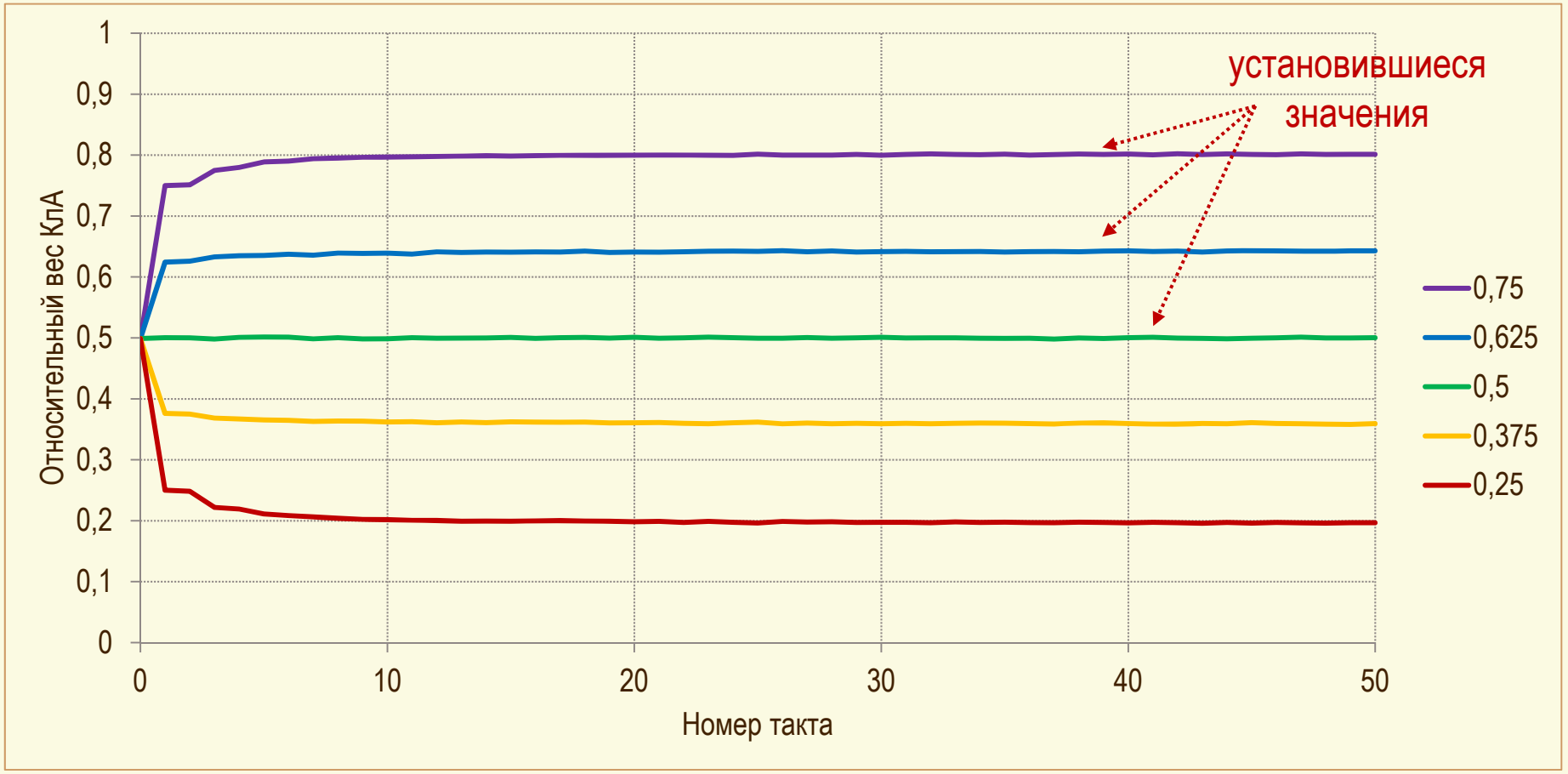
8 аргументов



9 аргументов

Локальная функция связи

- Нелинейная для обеспечения сложности преобразования
- Равновесная для обеспечения статистических свойств



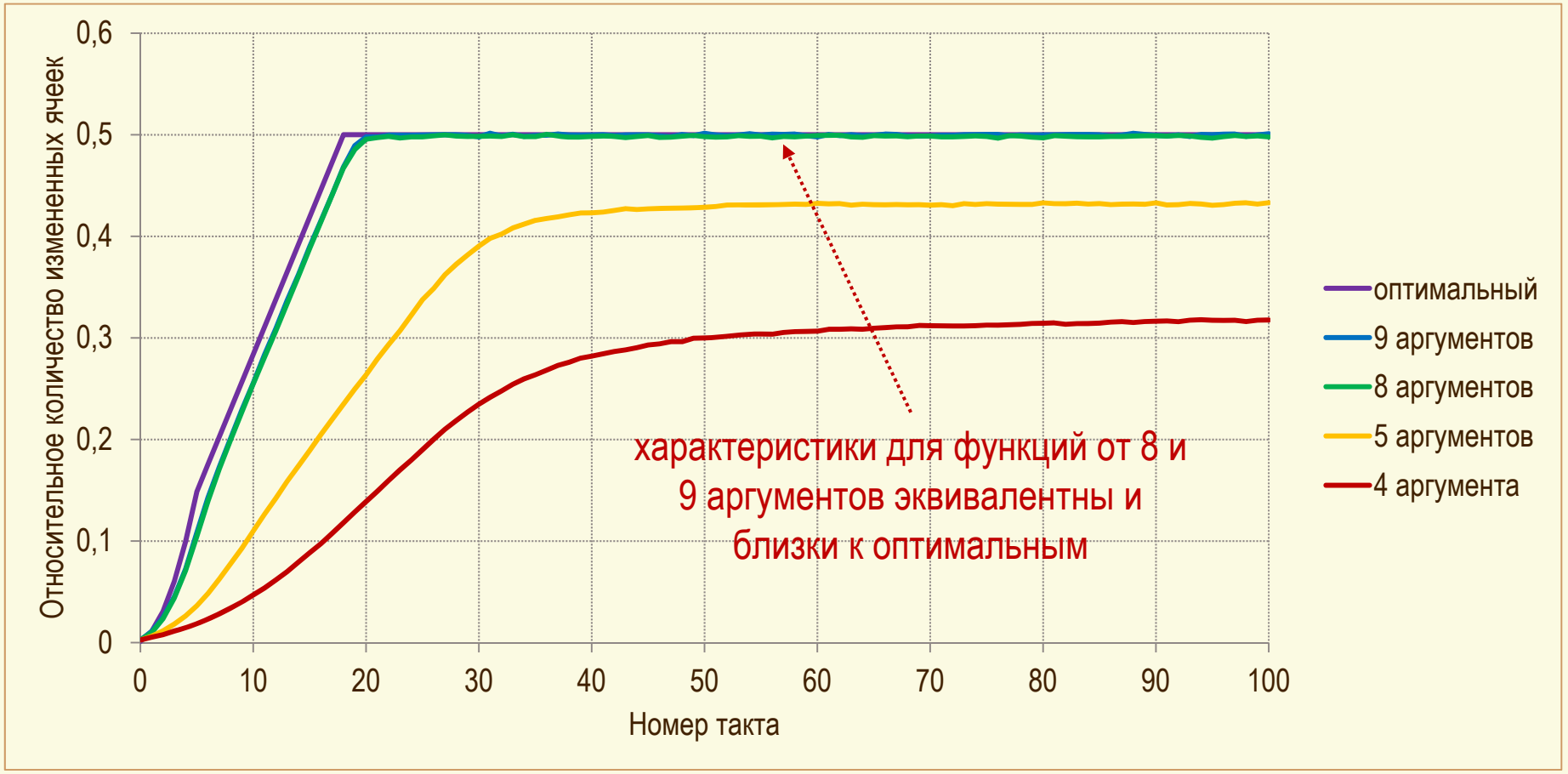
Лавинный эффект (ЛЭ)

- Введен по аналогии с Фейстелем
- Отражает изменения в заполнении решетки, вызванные сменой значения одной ячейки

- Лавинный эффект является оптимальным, если:
  - Изменения распространяются с максимально возможной скоростью
  - Изменяются значения ровно половины ячеек

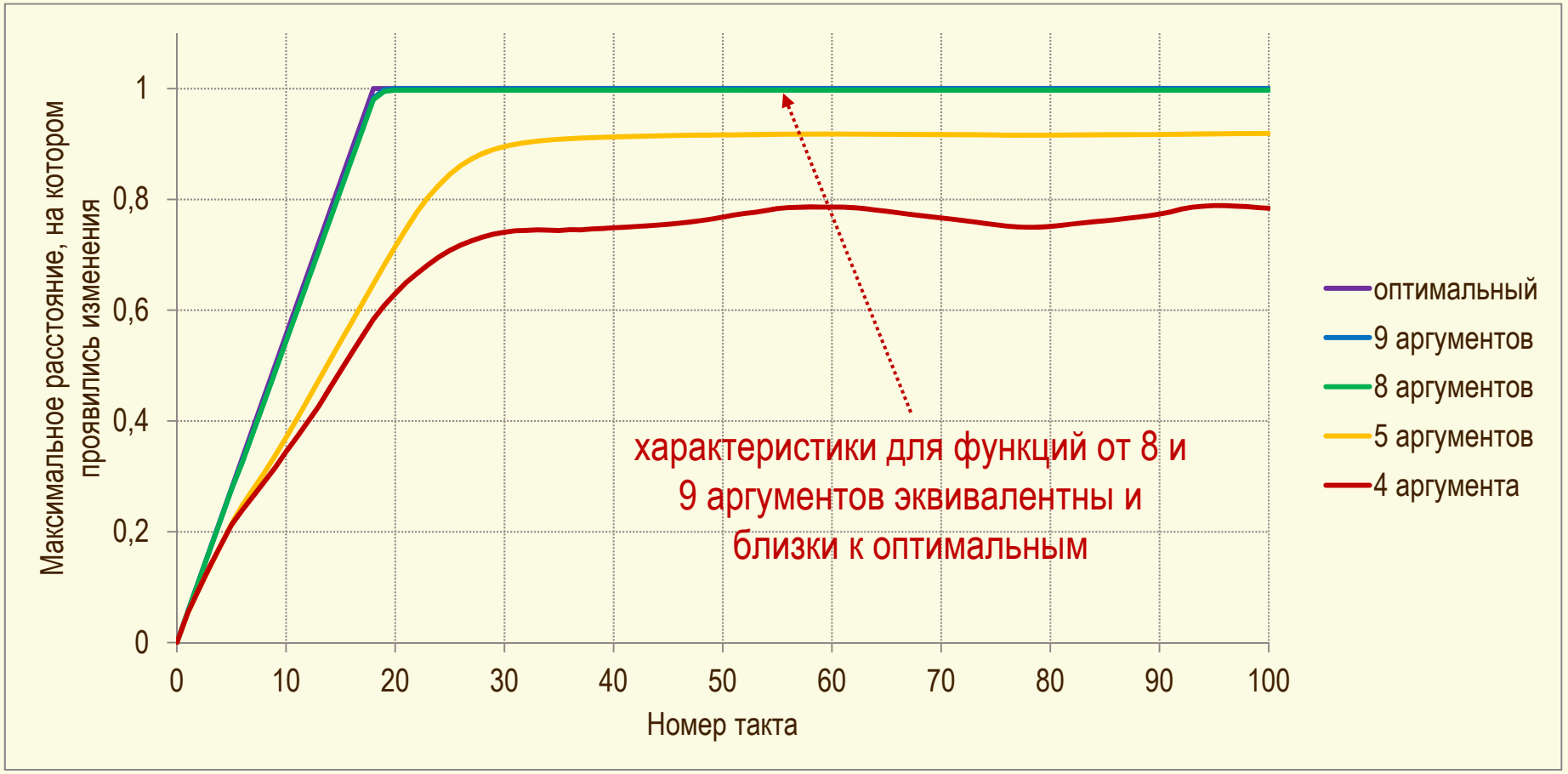
Интегральная характеристика ЛЭ

- Показывает временную зависимость количества изменившихся ячеек



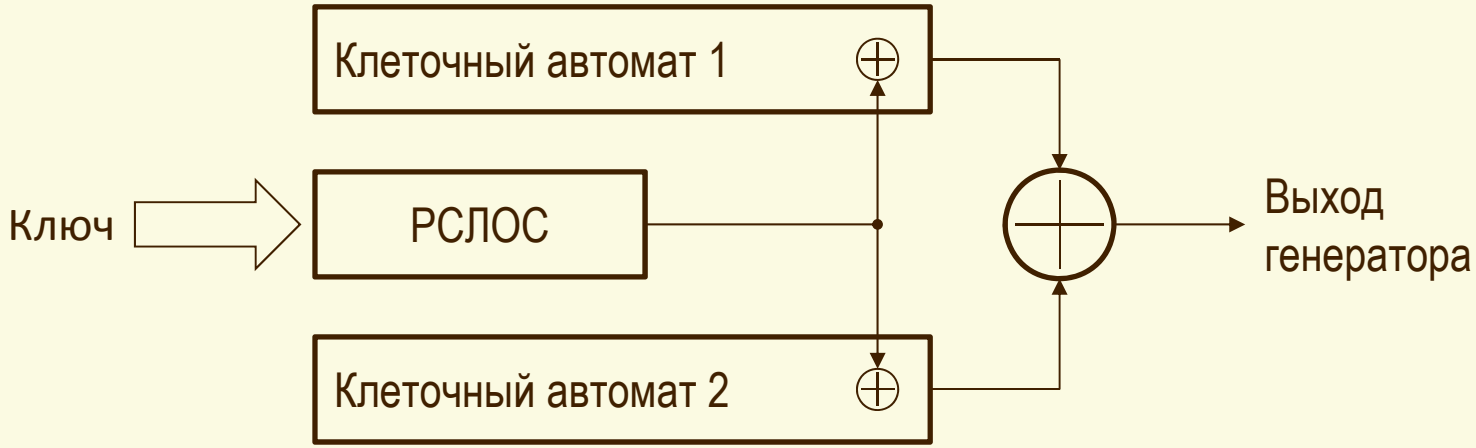
Пространственная характеристика ЛЭ

- Показывает временную зависимость максимального расстояния, на котором проявились изменения



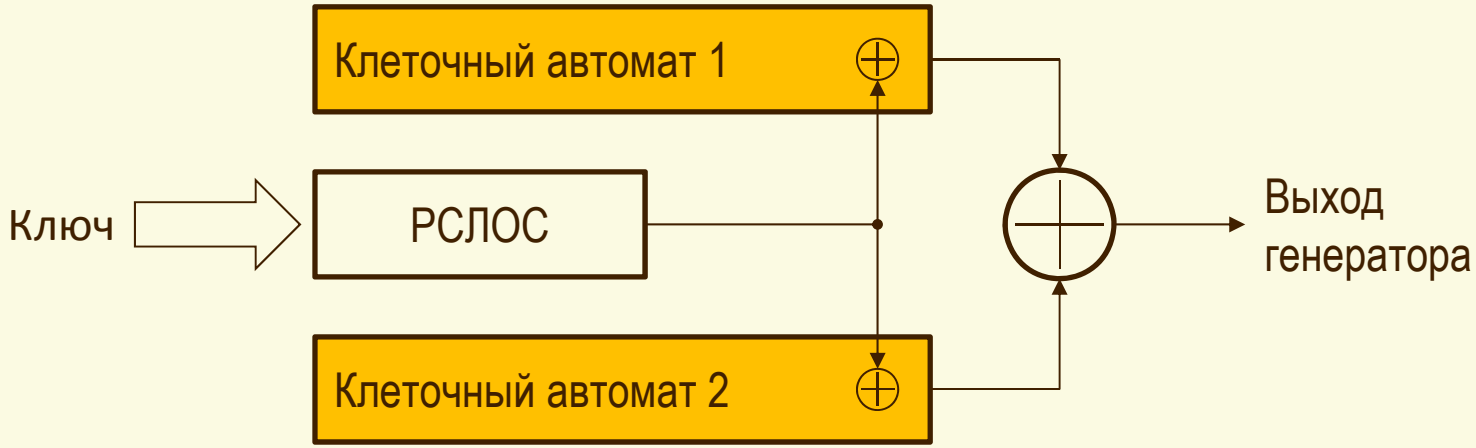
Структура генератора

- Компоненты:
  - 2 клеточных автомата
  - регистр сдвига с линейной обратной связью (РСЛОС)
- Выходная последовательность (гамма) формируется сложением по модулю 2 выходных последовательностей клеточных автоматов



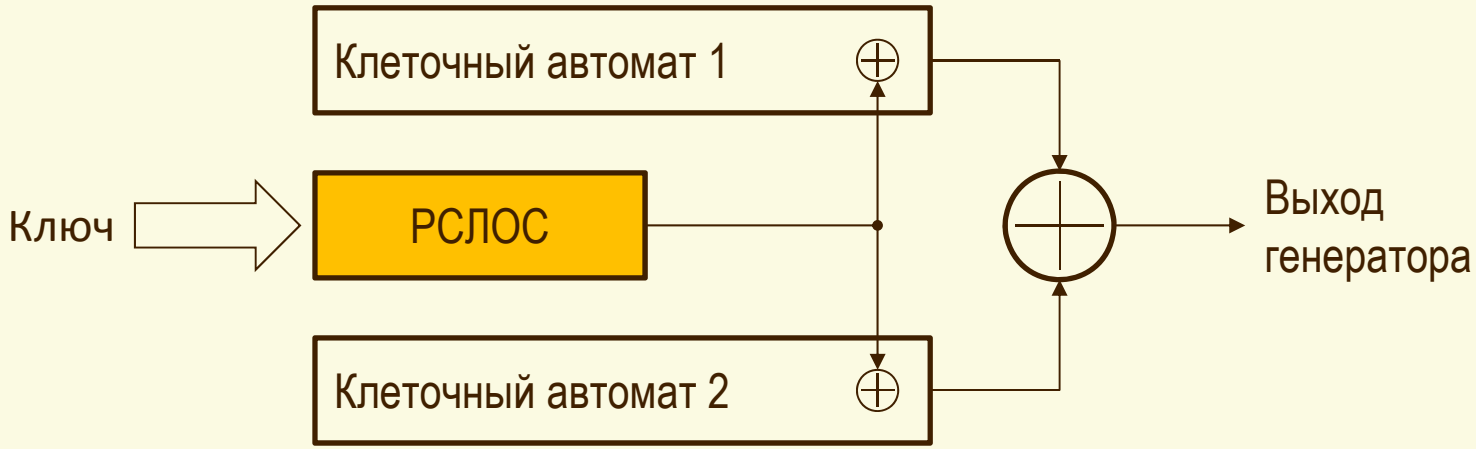
Структура генератора

- Клеточные автоматы вырабатывают псевдослучайную последовательность
  - Размеры решетки 37×11 ячеек (простые числа – для исключения возникновения пространственных периодов)
  - Локальная функция связи от 8 аргументов
  - Выход – значения ячеек подрешетки 32×8 (256 бит)

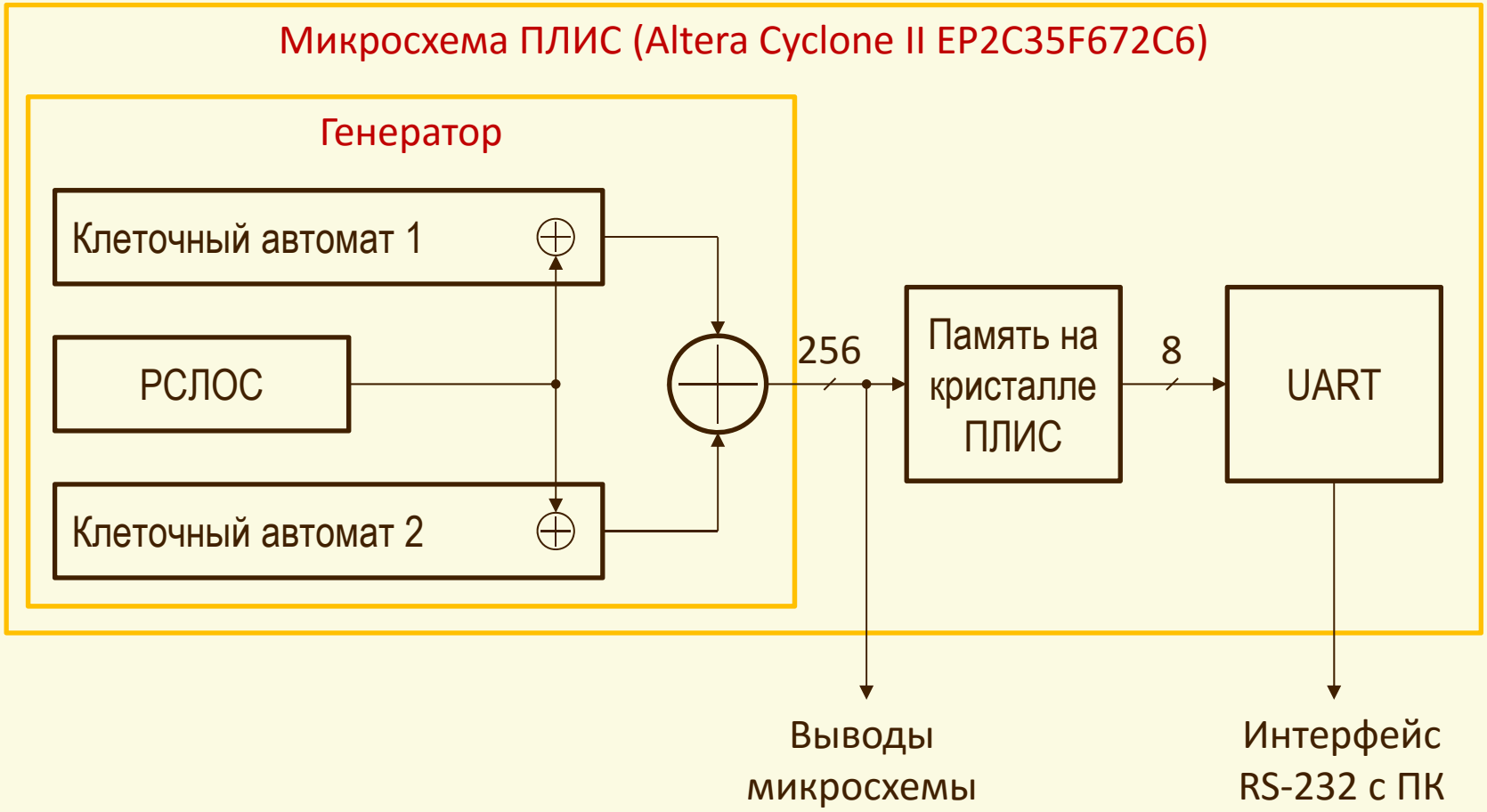


Структура генератора

- Регистр сдвига с линейной обратной связью обеспечивает период выходной последовательности
  - Длина регистра – 63 бита (может быть изменена)
  - Выход регистра прибавляется по модулю 2 к значению одной из ячеек (фиксированной) каждого клеточного автомата
  - Начальное значение является ключом выработки гаммы



Аппаратная реализация



Достоинства и недостатки

Достоинства

- Хорошие статистические свойства – тесты NIST не выявляют отклонений
- Высокая скорость аппаратной реализации – 256 бит/такт (23,8 Гбит/с на частоте 100 МГц)

Недостатки

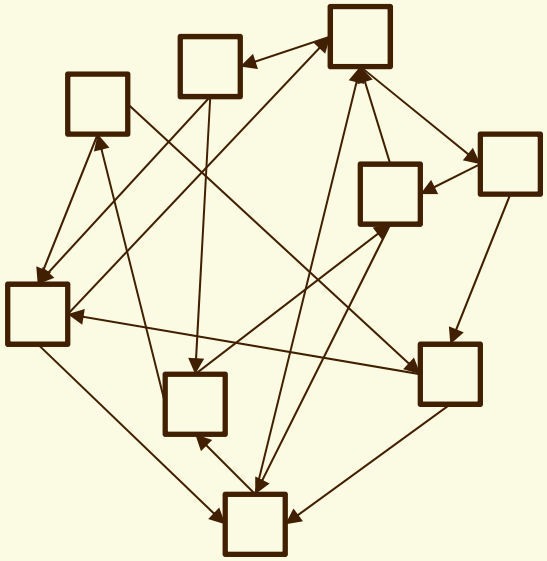
- Большая ресурсоемкость аппаратной реализации: около 22000 LE на Altera Cyclone II

Неоднородные клеточные автоматы (НКлА)

Неоднородные булевы клеточные автоматы

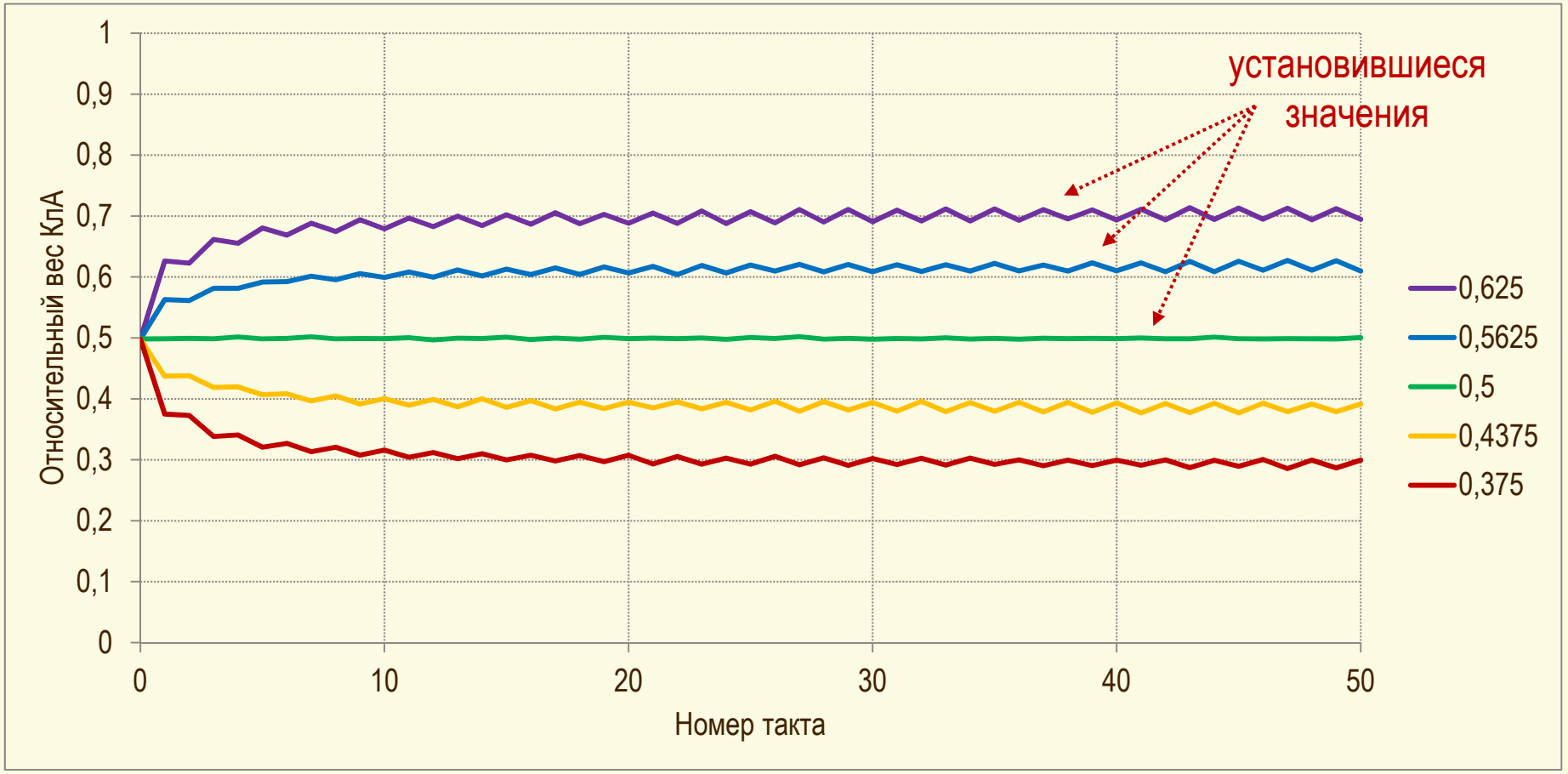
Отличия от классических клеточных автоматов

- Внутреннее состояние
  - Набор ячеек является неупорядоченным → представление в виде решетки неприменимо
- Правила перехода
  - Аргументы функции связи выбираются случайно из всего множества ячеек, но являются фиксированными для конкретного автомата

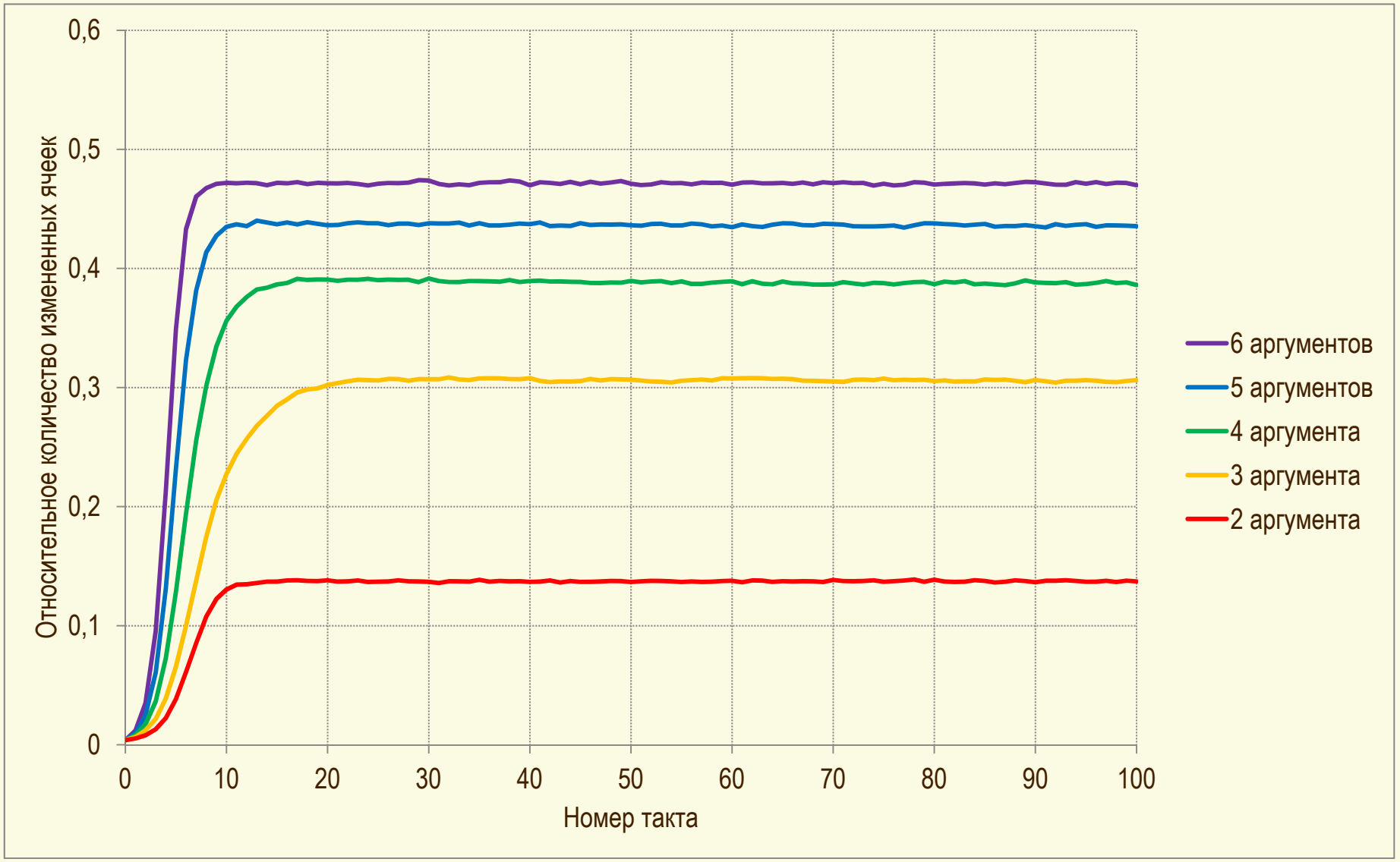


Локальная функция связи

- Нелинейная для обеспечения сложности преобразования
- Равновесная для обеспечения статистических свойств

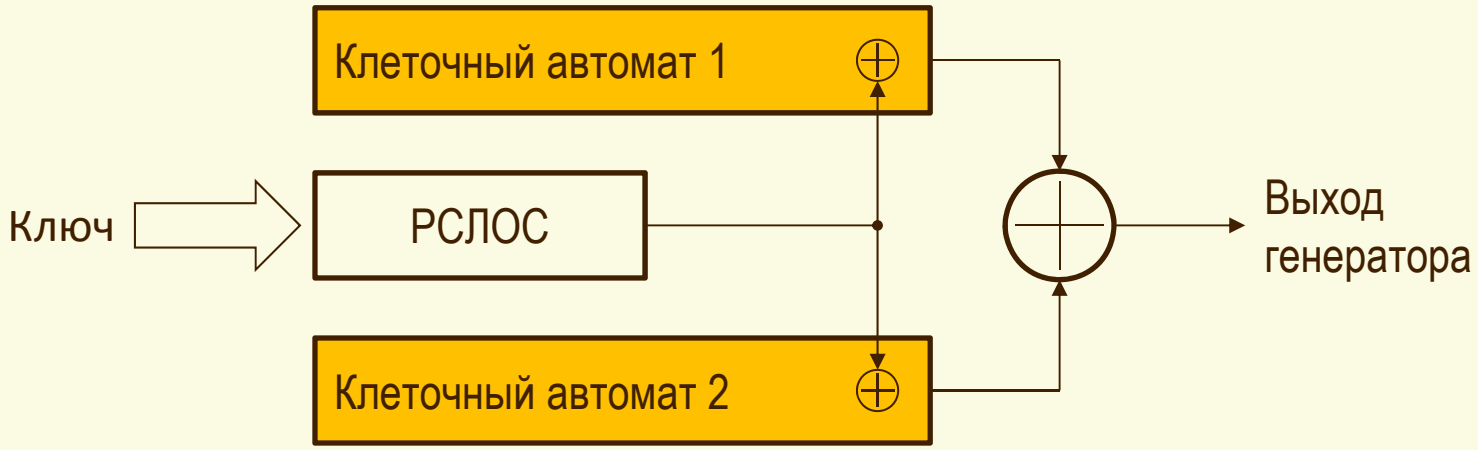


Интегральная характеристика лавинного эффекта



Структура генератора

- Клеточные автоматы вырабатывают псевдослучайную последовательность
  - Набор из 257 ячеек
  - Локальная функция связи от 4 аргументов
  - Выход – значения всех ячеек, кроме одной (256 бит)
- Остальные параметры генератора и аппаратная реализация не отличаются от классических клеточных автоматов



Достоинства

- Хорошие статистические свойства – тесты NIST не выявляют отклонений
- Высокая скорость аппаратной реализации – 256 бит/такт (23,8 Гбит/с на частоте 100 МГц)
- Низкая ресурсоемкость – около 1000 LE на Altera Cyclone II
- Для сравнения: Helion AES FPGA Core (Fast Encryptor)
  - Altera Cyclone III
  - 906 LE, 10 M9K
  - 2024 Мбит/с (128 bit, ECB)

Дальнейшие исследования

- Возможность реализации на GPU → массовое применение алгоритма