АЛГОРИТМЫ ГЕНЕРАЦИИ и ТЕСТИРОВАНИЯ СЛУЧАЙНЫХ и ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

ХНУРЭ, факультет **КИУ**, каф **ЭВМ**,
Тел. 70-21-354. Доц. Торба А.А.

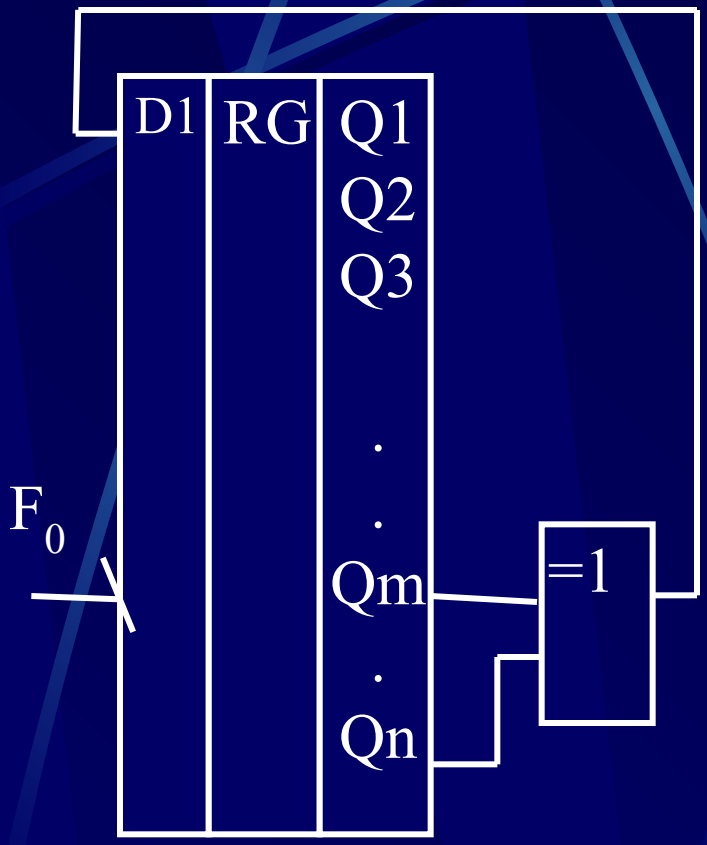
ОСНОВНЫЕ ТЕМЫ ЛЕКЦИИ

- **ОТЛИЧИЯ СЛУЧАЙНЫХ и ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ**
- **ВЫБОР ФИЗИЧЕСКИХ ДАТЧИКОВ ШУМА**
- **БАЗОВАЯ МОДЕЛЬ ГЕНЕРАТОРА СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ**
- **ВЫРАВНИВАНИЕ ВЕРОЯТНОСТЕЙ ГЕНЕРИРУЕМЫХ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ**
- **МЕТОДЫ ПОВЫШЕНИЯ БЫСТРОДЕЙСТВИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ**
- **МЕТОДЫ ТЕСТИРОВАНИЯ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ МЕТОДИКИ FIPS 140-1.**

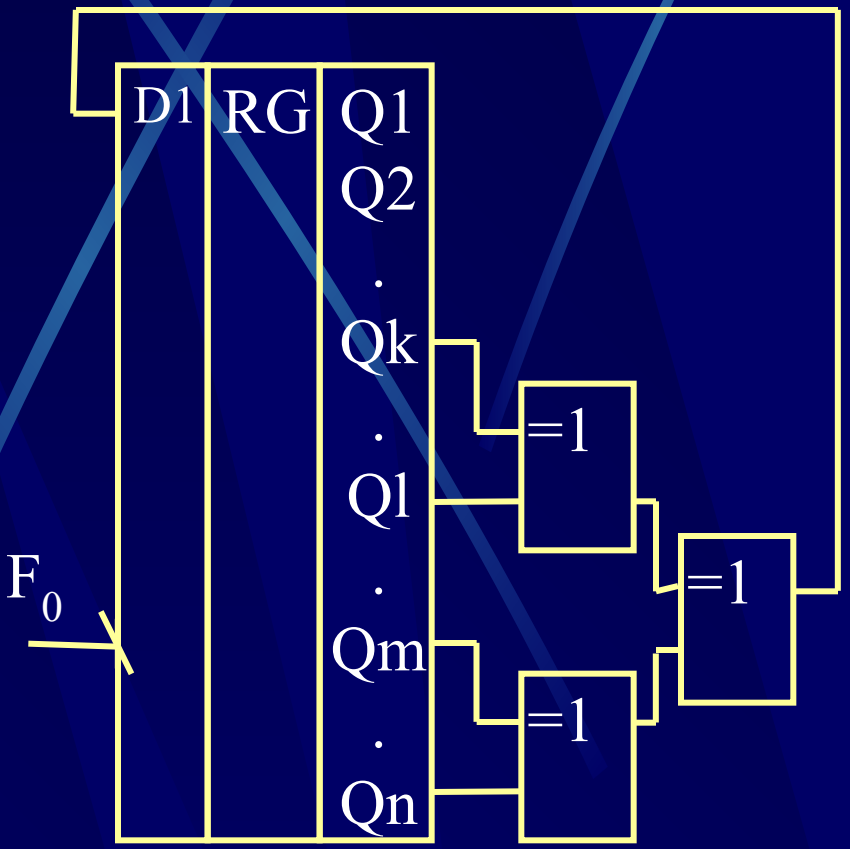
РЕАЛИЗАЦИЯ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

- С помощью **цифровых логических схем** можно необычайно просто генерировать последовательности бит с **хорошими стохастическими свойствами**, т.е. последовательности, которые будут обладать такими же **вероятностными** и **корреляционными** свойствами, какими обладает идеальная машина для подбрасывания монеты.
- Поскольку эти последовательности генерируются стандартными элементами **детерминированной логики**, получающиеся двоичные последовательности на самом деле являются **предсказуемыми** и повторяемыми (**детерминированными**), хотя любой фрагмент такой последовательности во всех отношениях выглядит, как **случайное чередование «0» и «1».**

- Наиболее известным (и самым простым) генератором **ПСП** является регистр сдвига с обратной связью



Последовательный регистр с одним отводом



Последовательный регистр с тремя отводами

- Последовательный регистр **RG** длиной **«n»** осуществляет **сдвиг хранимого кода** после каждого тактового импульса с частотой ***Fo***. Входной сигнал первого триггера регистра – **D1** формируется с помощью вентиля **ИСКЛЮЧАЮЩЕЕ ИЛИ** (сумматора по модулю 2), на входы которого поступают сигналы от **m-того** и последнего (**n-того**) разрядов регистра.
- Такая схема проходит через множество состояний, которые после **К** тактов начинают **повторяться**, т.е. последовательность состояний является **циклической** с **периодом К.**

- Максимальное число возможных состояний **n-разрядного** регистра равно $K=2^n$, т.е. числу **n-битовых** двоичных комбинаций. Однако состояние **«все нули»** для этой схемы является **тупиковым**, поскольку на выходе схемы **ИСКЛЮЧАЮЩЕЕ ИЛИ** постоянно **появляются нули**, которые поступают на вход схемы и **зацикливаются**.
- Если для формирования входного сигнала использовать элемент **«ИСКЛЮЧАЮЩЕЕ ИЛИ» с инверсией**, то **«тупиковой»** будет комбинация – **«все единицы».**
- Таким образом, **последовательность максимальной длины**, которую может сформировать данная схема, содержит 2^n-1 бит.

- При использовании **33-х** разрядного регистра, работающего **на частоте 1 МГц**, **время цикла** будет около **2-х часов**. Время цикла **100 разрядного** регистра, работающего на частоте **10 МГц**, будет в **миллион раз больше, чем возраст Вселенной**.
- Генераторы **ПСП** на сдвигающих регистрах можно использовать для **шифрования сообщений и данных**, поскольку идентичный генератор **ПСП** на приемном конце дает **ключ к шифру**.
- **ПСП** широко используются в кодах, **обнаруживающих и исправляющих ошибки**, так как они позволяют видоизменить блоки данных таким образом, что **правильные кодовые сообщения** будут находиться друг от друга на **максимально возможном «расстоянии Хэмминга»** (измеряется числом позиций с разными данными).

СВОЙСТВА ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ МАКСИМАЛЬНОЙ ДЛИНЫ

- В **полном цикле** число **«1»** на единицу больше, чем число **«0».** Добавочная **«1»** появляется за счет исключения состояния **«все нули».** При большом количестве разрядов регистра вероятности **«0»** и **«1»** практически равны (**17-ти разрядный** регистр будет вырабатывать 65536 **«1»** и 65535 **«0»** за один цикл);
- В **одном цикле** половина серий из последовательных **«1»** имеет **длину 1**, одна четвертая серий – **длину 2**, одна восьмая – **длину 3** и т.д. Таким же свойством обладают и серии из **«0»** с учетом пропущенного **«0».** Это говорит о том, что вероятности **«0»** и **«1»** не зависят от исхода предыдущего опыта, т.е. **вероятность появления «0» или «1» в следующем бите не зависит от значения предыдущего бита**;

- Если последовательность полного цикла сравнить с этой же последовательностью, но циклически **сдвинутой на любое число битов** (не равное нулю или длине К), то **число несовпадений** будет на **единицу** больше, чем **число совпадений**. Научно выражаясь, **автокорреляционная функция** этой последовательности представляет собой дельта-**функцию Кронекера** при нулевой задержке и равна величине **1/К** при любой другой задержке.

ОСНОВНЫЕ ОТЛИЧИЯ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ ОТ СЛУЧАЙНЫХ

- Псевдослучайные числа являются **детерминированными**, то есть предсказуемыми. Зная **алгоритм формирования** и **начальное значение**, можно предсказать **все** последующие числа наперед.
- В **новом эксперименте** всегда можно повторить **предыдущий эксперимент**.
- Псевдослучайные последовательности являются **периодическими**, через известные промежутки времени они будут **точно повторяться.**

- Предельные характеристики стойкости криптографических систем достигаются в случае, если для формирования ключей, параметров и синхромаркеров используется генератор случайных последовательностей на основе **ФИЗИЧЕСКИХ ДАТЧИКОВ ШУМА** с наилучшими параметрами:

- **равновероятности,**
- **независимости** и
- **некоррелированности** на сколь угодно длинном интервале.

- Простейшие **физические датчики**, реализованные на основе случайных механических перемещений:
  - подбрасывание монеты,
  - бросание «игральных костей»,
  - наблюдения броуновского движения и др.

обладают недостаточным быстродействием и требуют для своей реализации оптические устройства ввода результатов опытов в ЭВМ.

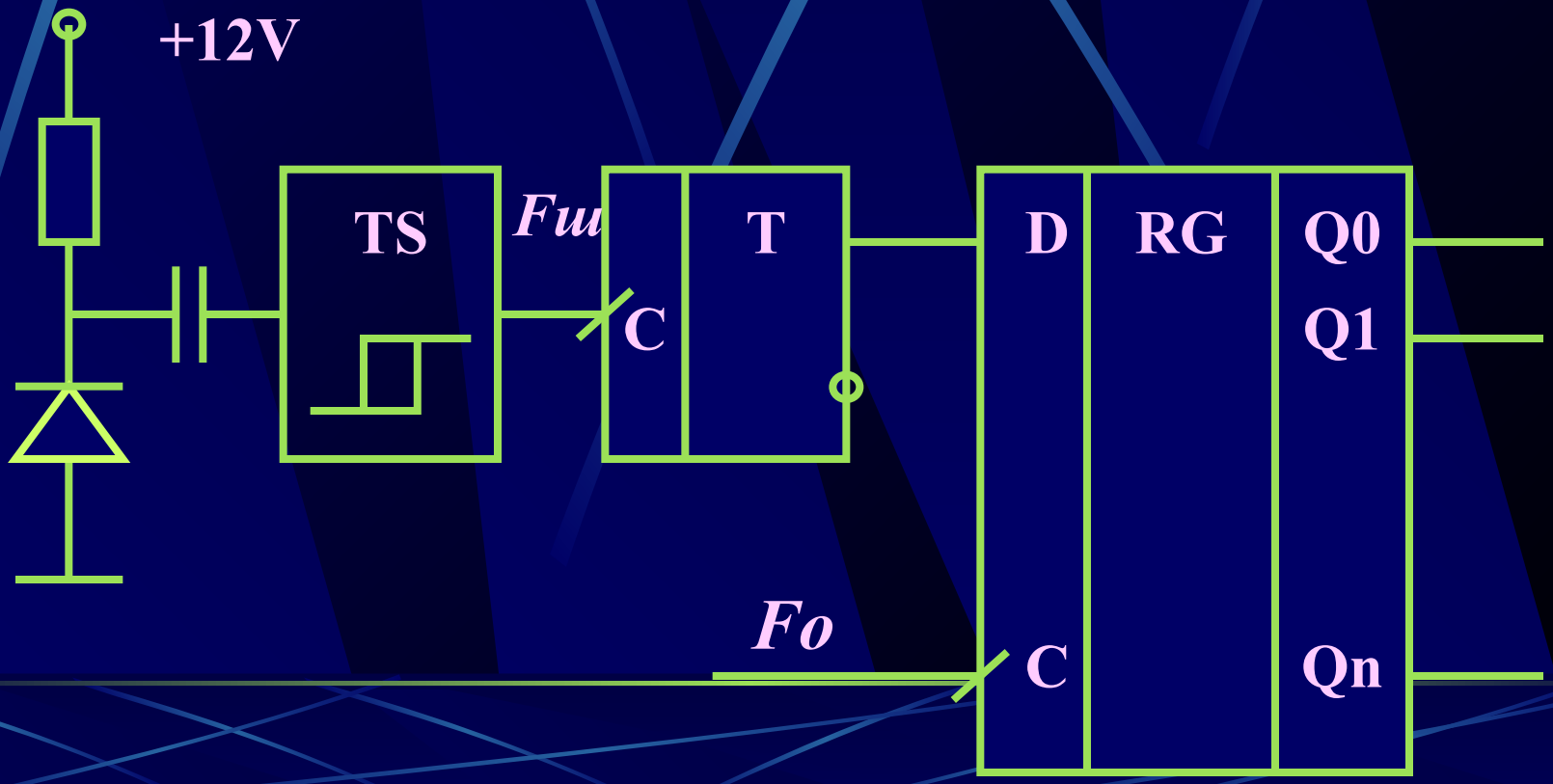
Основные датчики шума

- Резисторы
- P-n-переходы
- **Диоды с Зенеров-ским пробоем**
- Электр. лампы
- Газоразрядные лампы
- ФЭУ
- Счетчики радиоактивности

Критерии выбора

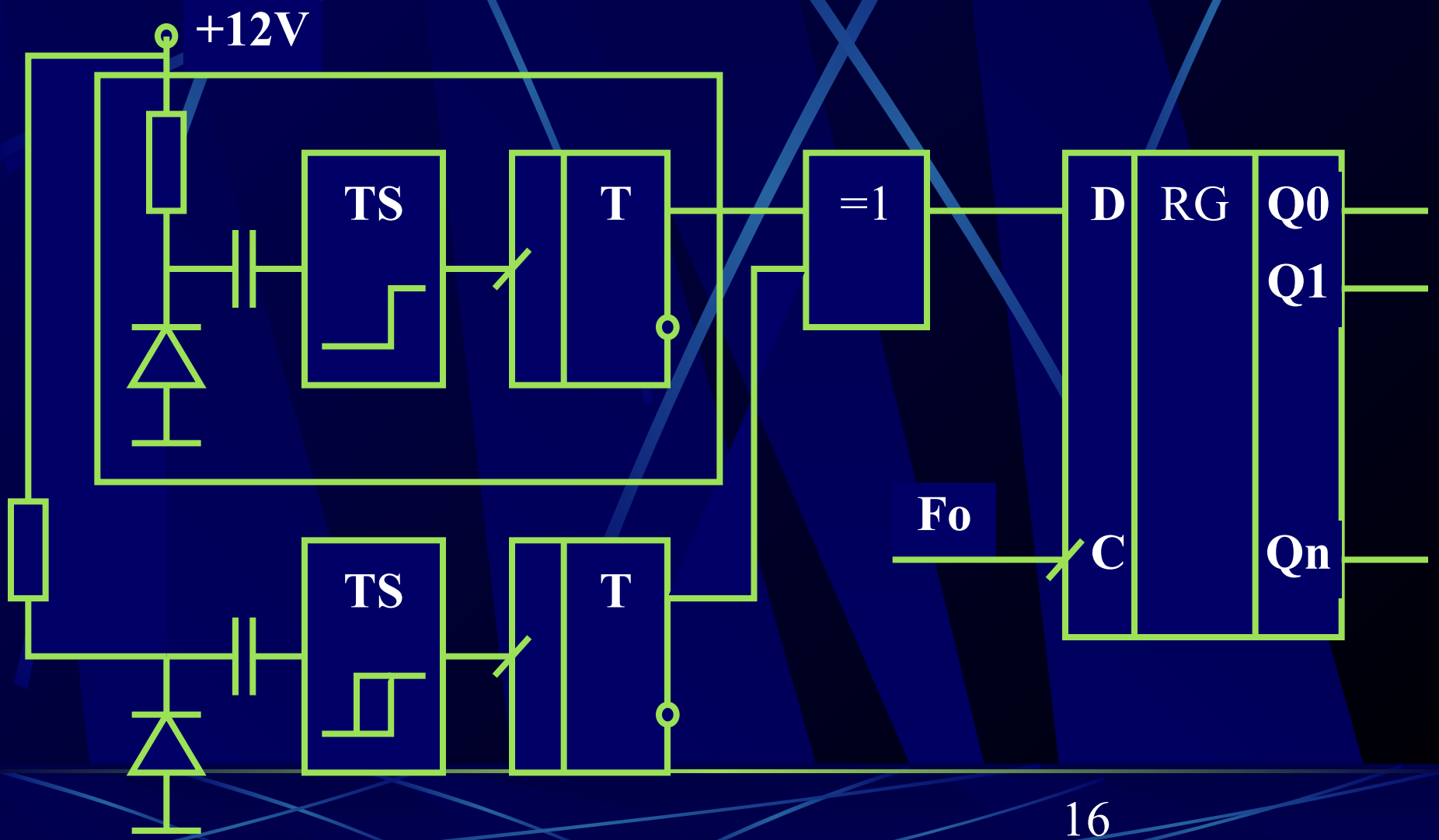
- полоса частот случайного сигнала;
- выходное напряжение (амплитуда шума);
- потребляемая мощность;
- напряжение питания;
- массогабаритные парамет-ры;
- надежность работы при изменении условий эксплуатации;
- экономические показатели (стоимость).

- На рис. приведена базовая схема генератора случайных последовательностей на основе физического датчика – диода с **Зенеровским пробоем**.



- Повышение эксплуатационной **надежности** канала формирования случайных битов достигается **горячим резервированием**, то есть параллельной работой нескольких каналов.
- Выходные равновероятные случайные логические сигналы всех каналов объединяются схемой **«ИСКЛЮЧАЮЩЕЕ ИЛИ»** (схемой суммирования по модулю 2) и считываются в сдвигающий регистр с частотой *Fo*

- Горячее резервирование генераторов случайных последовательностей



УКРАЇНА

(19) **(UA)**

(11) **59670 А**

(51) 7 **G06F7/58, G07C15/00**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Деклараційний патент
на винахід

видано відповідно до Закону України "Про охорону прав на винаходи і корисні моделі"

Голова Державного Департаменту інтелектуальної власності М. Паладій

(21) 2002119010
(22) 12.11.2002
(24) 15.09.2003
(46) 15.09.2003. Бюл.№ 9

(72) Торба Олександр Олексійович, Горбенко Іван Дмитрович, Єлаков Сергій Генадійович, Степченко Олексій Зотович, Бобух Всеволод Анатолійович, Торба Ганна Олександрівна
(73) ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ, АКЦІОНЕРНЕ ТОВАРИСТВО "ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ"

(54) ГЕНЕРАТОР РІВНОМІРНО РОЗПОДІЛЕНИХ ВИПАДКОВИХ ЧИСЕЛ

УКРАЇНА

(19) **(UA)**

(11) **61439 А**

(51) 7 **G06F7/58, G07C15/00**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Деклараційний патент
на винахід

видано відповідно до Закону України "Про охорону прав на винаходи і корисні моделі"

Голова Державного Департаменту інтелектуальної власності М. Паладій

(21) 2003021014
(22) 05.02.2003
(24) 17.11.2003
(46) 17.11.2003. Бюл.№ 11

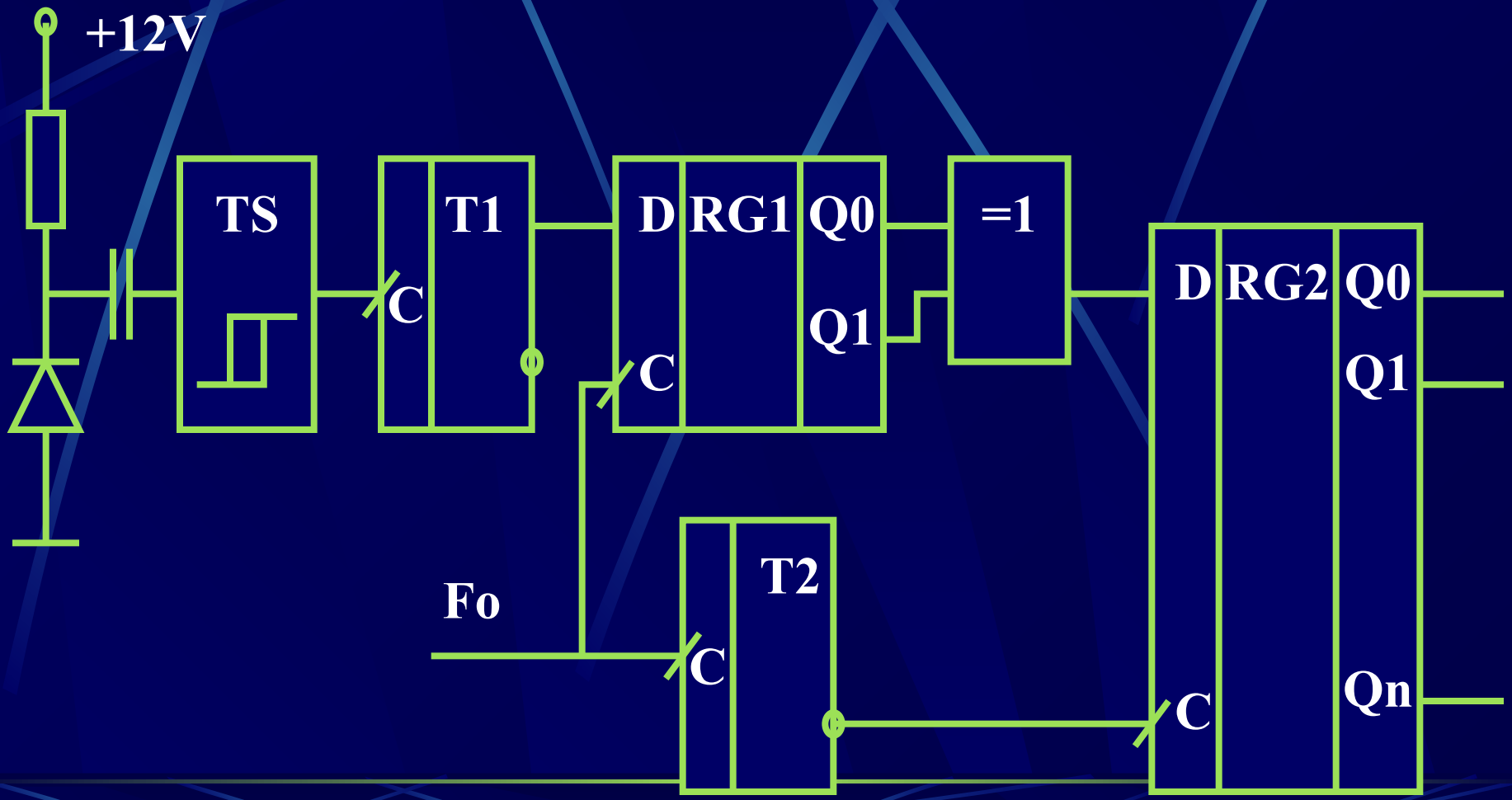
(72) Торба Алєксандр Алєксєєвіч, Єлаков Сергій Генадійович, Степченко Олексій Зотович, Бобух Всеволод Анатолійович, Торба Ганна Олександрівна
(73) ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ, АКЦІОНЕРНЕ ТОВАРИСТВО "ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ"

(54) ГЕНЕРАТОР РІВНОМІРНО РОЗПОДІЛЕНИХ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

ВЫРАВНИВАНИЕ ВЕРОЯТНОСТЕЙ ГЕНЕРИРУЕМЫХ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

- Этот алгоритм позволяет значительно уменьшить разность вероятностей генерируемых случайных битов.
- Для этого из двух последовательных случайных битов формируется их логическая функция **«ИСКЛЮЧАЮЩЕЕ ИЛИ».**
- Вероятность единичного формируемого бита **на входе** регистра RG1 обозначим **P(1),** а вероятность нулевого – **P(0) = P(1) + Δ.**

- Схема **выравнивания** вероятностей **«Дельта-квадрат»**



Все комбинации битов на выходе промежуточного регистра **RG1** и вероятности этих комбинаций (с учетом полной **статистической независимости** генерируемых соседних случайных битов) приведены в таблице:

Q1	Q2	Вероятности
0	0	[P(1) + Δ] * [P(1) + Δ]
0	1	[P(1) + Δ] * P(1)
1	0	P(1) * [P(1) + Δ]
1	1	P(1) * P(1)

- На выходе схемы **«ИСКЛЮЧАЮШЕЕ ИЛИ»** формируется **логический нуль** при комбинациях, соответствующих **первой** и **последней** строкам таблицы:

$$P(0)' = [\, P(1) + \Delta \,] * [\, P(1) + \Delta \,] + P(1) * P(1).$$

- **Логической единице** на выходе схемы **«ИСКЛЮЧАЮЩЕЕ ИЛИ»** будут соответствовать **две средние строки** в таблице:

$$P(1)' = [\, P(1) + \Delta \,] * P(1) + P(1) * [\, P(1) + \Delta \,].$$

- **Разность вероятностей** на выходе схемы «ИСКЛЮЧАЮЩЕЕ ИЛИ» **Δ'** равна:

$$\Delta' = P(0)' - P(1)' = \Delta^2.$$

МЕТОДЫ ПОВЫШЕНИЯ БЫСТРОДЕЙСТВИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

- Объединение двух или более независимых случайных процессов логическим элементом **«ИСКЛЮЧАЮЩЕЕ ИЛИ».**
- Записывать в **параллельный регистр RG2** результат выполнения операций **«ИСКЛЮ-ЧАЮЩЕЕ ИЛИ»** над сигналами с **первой** и **второй** половины **сдвигающего регистра RG1** с **перестановкой** выходных сигналов

МЕТОДЫ ТЕСТИРОВАНИЯ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ МЕТОДИКИ FIPS 140-1.

- Генераторы случайных битовых последовательностей, реализованные на **физических** источниках случайности, подвергнуты влиянию **внешних факторов**, а также **сбоям.**
- Поэтому такие устройства периодически необходимо **тестировать**, например, с помощью **статистических тестов.**

В американском федеральном стандарте **FIPS 140-1** используются четыре статистических теста на случайность:

- **монобитный тест,**
- **блочный тест,**
- **тест серий** и
- **тест длин серий.**

В этих тестах для удовлетворительных значений статистических параметров задаются **границы.**

Если какой-нибудь из тестов **не пройден**, то считается, что генератор (или последовательность) **не прошел тестирование**.

- Алгоритм тестирования **FIPS 140-1** может быть реализован **на программном уровне после ввода** последовательности s – 20000 случайных бит в **ПЭВМ.**
- Но в некоторых случаях тестирование случайных последовательностей необходимо производить **в аппаратном модуле** генерации случайных чисел (ГСЧ) **до ввода в ПЭВМ**.
- Для этих целей обычно применяют **одно-кристальные микро-ЭВМ** (ОМЭВМ) – **микроконтроллеры** (МК).

Вопросы для экспресс-контроля

- Назовите основные отличия **случайных** последовательностей от **псевдослучайных**.
- Назовите **методы генерации** псевдослучайных последовательностей.
- Назовите основные **источники физического шума** для генерации случайных последовательностей.
- Перечислите **основные тесты** американского стандарта тестирования случайных последовательностей **FIPS 140-1.**
- Назовите **методы выравнивания** вероятностей случайных битовых последовательностей.

Доклад окончен

- Спасибо за внимание