

**Генератори  
на  
случайни последователности  
в  
паралелна изпълнителна среда**



# **Генератори на случайни последователности в паралелна изпълнителна среда**

---

Милен Луканчевски

Русенски университет "Ангел Кънчев"

УДК 004.272 + 004.421.5 + 519.688

## **Генератори на случайни последователности в паралелна изпълнителна среда**

© Автор **д-р инж. Милен Луканчевски, 2013**

Рецензенти: **проф. д.т.н Райчо Иларионов, ТУ-Габрово**  
**доц. д-р Лидия Георгиева, РУ “А. Кънчев”**

Компютърна обработка: **д-р инж. Милен Луканчевски**

Националност на автора: **българска**

Език на изданието: **български**

Тип (жанр): **научен, монография**

Поредност: **първо**

ISBN 978-619-7071-26-9

Формат 64 x 90/16

Издателски център на Русенския университет “А. Кънчев”, 2013.

На лицевата корица: Елементи от екрана на паралелната развойна среда *xTIMEcomposer Studio* на фирмата *XMOS*.

На задната корица: Част от опитната постановка, използвана за изследване и експериментиране с предложените реализации на генератори на случайни последователности.

Изследването и изданието са финансирани от автора и от ръководеното от него научно развойно направление “*Компютърни телекомуникационни системи*”.

***На мислещите компютърни специалисти,  
призвани да преодолеят третата сингулярност***



# ПРЕДИСЛОВИЕ

Главните направления на развитие на компютърните архитектури на съвременния етап включват постепенен преход от последователния фоннойманов към паралелния изчислителен модел, както и изследването на възможностите за използване принципите на квантовата механика за съхранение, обработка и пренос на информацията.

Предпоказва работите и при двете направления са физическите ограничения на класическия последователен изчислителен модел. Но докато при първото направление тези ограничения се преодоляват на макрониво, то при второто направление стремежът е да се използва скрития на квантово ниво потенциал за паралелна обработка.

От началото на 90-те години в катедра "Компютърни системи и технологии" на Русенския университет "А. Кънчев" се работи в областта на паралелните компютърни системи, което в голяма степен е стимулирано от резултатите в дисертационния труд на автора. Изследванията се основават на паралелния изчислителен модел *CSP* на Чарлз Хоар. Като елементна база са използвани скаларни микропроцесори с общо предназначение.

От 2009 година, както в изследователската, така и в учебната работа, авторът експериментира с новата *SMT/TLP* архитектура *XS1* на фирмата *XMOS*.

Като резултат от осмислянето на получените резултати и на основното противоречие в областта на компютърните архитектури и системи, авторът започва да развива от 2012 година тематика за изследване на квантовите явления чрез моделирането им в паралелна изпълнителна среда.

Възприет за водещ методологичен принцип е съвместното разглеждане на двете главни направления на развитие на компютърните архитектури: на макрониво и на квантово ниво. Акцентира се върху изоморфизма на изображението на структурата на изследвания обект или явление в модел с глобален структурен паралелизъм. Оттук произтича и избора на изпълнителната среда с глобален структурен паралелизъм *XCORE/XC*, базирана на *SMT/TLP* архитектура *XS1*.

Като инициатор и ръководител на тези изследвания, авторът

се счита длъжен да представя в монографична форма най-съществените резултати от всеки отделен, логически завършен техен етап.

Предмет на тази монография са основните резултати от първия етап от изследванията, посветен на генераторите на случайни последователности в паралелната изпълнителна среда *XCORE/XC*.

Едновременно излиза от печат и другата монография, в която се обобщават резултатите от втория етап на изследванията - структурното моделиране на ключовите квантови явления поляризация, суперпозиция, квантова телепортация и сплитане [9].

По въпроси, свързани със съдържанието на работата, може да се обръщате на електронната поща [mil@ieee.org](mailto:mil@ieee.org) на автора.

+++

Използвам случая да благодаря на своите студенти, участвали в работите. Най-вече на маг. инж. Бисер Николов за неговия младежки плам и отдаденост на професията.

Възможността за провеждане на изследванията се дължат на подкрепата, която срещам от научно-изследователското направление "Компютърни телекомуникационни системи" към катедра "Компютърни системи и технологии" на Русенския университет "А. Кънчев".

Рецензентите на представената работа - проф. д.т.н. Райчо Иларионов и доц. д-р Лидия Георгиева поеха с желание отговорността да помогнат за повишаване на нейното ниво чрез своите бележки, коментари и препоръки.

Благодаря на майка си - моят най-верен приятел, вдъхновител и ориентир!

Милен Луканчевски,  
*IEEE Computer Society,*  
*IEEE Communications Society & ACM Member*

Русе, октомври 2013 г.



# СЪДЪРЖАНИЕ

<b>ПРЕДИСЛОВИЕ</b>	<b>7</b>
<b>СПИСЪК НА СЪКРАЩЕНИЯТА</b>	<b>12</b>
<b>ВЪВЕДЕНИЕ</b>	<b>14</b>
<b>1. ФОРМУЛИРОВКА НА ПРОБЛЕМА</b>	<b>21</b>
1.1. ОСНОВНИ МЕТОДИ ЗА ГЕНЕРАЦИЯ НА СЛУЧАЙНИ ПОСЛЕДОВАТЕЛНОСТИ	22
1.2. ПАРАЛЕЛНА SMT/TLR АРХИТЕКТУРА XS1	31
1.3. РАЗВОЕН КИТ ХК-1	37
1.4. ЦЕЛ И ЗАДАЧИ НА ИЗСЛЕДВАНЕТО	40
<b>2. РЕАЛИЗАЦИЯ И ИЗСЛЕДВАНЕ НА ГРУПА ГЕНЕРАТОРИ НА СЛУЧАЙНИ ПОСЛЕДОВАТЕЛНОСТИ В ПАРАЛЕЛНА ИЗПЪЛНИТЕЛНА СРЕДА</b>	<b>41</b>
2.1. ГЕНЕРАТОРИ С ИЗМЕСТВАЩИ РЕГИСТРИ С ЛИНЕЙНА ОБРАТНА ВРЪЗКА	42
2.2. ГЕНЕРАТОРИ, БАЗИРАНИ НА ПРИМИТИВНА ФУНКЦИЯ НА ИЗПЪЛНИТЕЛНАТА СРЕДА	51
2.3. ГЕНЕРАТОРИ, БАЗИРАНИ НА ЕНТРОПИЕН ИЗТОЧНИК ОТ ИЗПЪЛНИТЕЛНАТА СРЕДА	54
2.4. ГЕНЕРАТОРИ, БАЗИРАНИ НА ВГРАДЕНИЯ В АЛТЕРНАТИВНАТА КОМАНДА НЕДЕТЕРМИНИЗЪМ	58
2.5. ТЕХНИКА ЗА ВГРАЖДАНЕ НА НЕДЕТЕРМИНИЗЪМ В ОПЕРАТОРА <i>SELECT</i>	62
2.6. ВАРИАНТ НА МОНОБИТНИЯ ТЕСТ ЗА ПРОВЕРКА НА ГЕНЕРИРАНАТА ПОСЛЕДОВАТЕЛНОСТ В РЕАЛНО ВРЕМЕ	69
<b>3. ЕКСПЕРИМЕНТАЛНА ОЦЕНКА НА ПРЕДЛОЖЕНИТЕ РЕШЕНИЯ</b>	<b>75</b>
<b>ИЗВОДИ</b>	<b>81</b>
<b>ЛИТЕРАТУРА</b>	<b>83</b>
<b>ПРИЛОЖЕНИЯ</b>	<b>87</b>
ПРИЛОЖЕНИЕ П1: ПРОЕКТ I-T001	88
ПРИЛОЖЕНИЕ П2: ПРОЕКТ I-T002	96
ПРИЛОЖЕНИЕ П3: ПРОЕКТ I-T003	105
ПРИЛОЖЕНИЕ П4: ПРОЕКТ I-T004	115
ПРИЛОЖЕНИЕ П5: ПРОЕКТ I-T005	126

# СПИСЪК НА ФИГУРИТЕ И ТАБЛИЦИТЕ

Фиг. В1. Графика на развитието на производителността.....	15
Фиг. В2. Графика на изменението на тактовата честота на процесорите.....	17
Фиг. 1.1. Класификация на основните видове <i>RNG</i> .....	23
Фиг. 1.3. <i>LFSR</i> генератор – конфигурация Галоа.....	25
Фиг. 1.2. <i>LFSR</i> генератор – конфигурация Фибоначи.....	25
Фиг. 1.4. Блокова схема на физически генератор ( <i>RRNG</i> ).....	26
Фиг. 1.5. Принципна схема на физически източник на шум.....	27
Фиг. 1.6. Схема на кръгов осцилатор.....	28
Фиг. 1.7. Графика на ентропията при $n = 2$ .....	29
Фиг. 1.8. Структура на <i>CSP</i> машина.....	31
Фиг. 1.9. Двучовково еднопосочно взаимодействие.....	32
Фиг. 1.10. Връзка между абстрактната и реалната страна на <i>CSP</i> .....	34
Фиг. 1.11. Процесори от фамилия <i>XS1</i> .....	35
Фиг. 1.12. Ресурси на ядрото <i>XCORE</i> .....	36
Фиг. 1.13. Физическо разположение на основните компоненти на компютърния възел.....	37
Фиг. 1.14. Блокова схема на компютърния възел.....	38
Фиг. 2.1. Схема на връзките в паралелната система.....	42
Фиг. 2.2. Управление на светодиодната индикация.....	46
Фиг. 2.3. Част от осцилограмата на изходния сигнал на порт <i>oportRngBit</i> при <i>RNG LFSR</i> -Фибоначи.....	48
Фиг. 2.4. Част от осцилограмата на изходния сигнал на порт <i>oportRngBit</i> при <i>RNG LFSR</i> -Галоа.....	48
Фиг. 2.5. Схематично представяне на реализацията на Алгоритъм-М.....	49
Фиг. 2.6. Диаграма на използваните апаратни ресурси.....	50
Фиг. 2.7. Част от осцилограмата на изходния сигнал на порт <i>oportRngBit</i> при <i>RNG</i> с примитивна функция на средата.....	52
Фиг. 2.8. Схема на генератора, използващ кръговите осцилатори на средата.....	55
Фиг.2.9. Осцилограмата на изходния сигнал на порт <i>oportRngBit</i> при <i>RRNG</i> в момента на разпакетиране.....	57
Фиг. 2.10. Граф на участва от паралелната система с вграден недетерминизъм.....	59
Фиг. 2.11. Част от осцилограмата на изходния сигнал на порт	

<b>oportRngBit за изследването на вградения недетерминизъм</b>	<b>61</b>
<b>Фиг. 2.12. Диаграма на състоянията при детерминиран избор</b>	<b>63</b>
<b>Фиг. 2.13. Диаграма на състоянията при недетерминиран избор</b>	<b>63</b>
<b>Фиг. 2.14. Паралелна система с недетерминизъм – два източника</b>	<b>64</b>
<b>Фиг. 2.15. Изходна последователност при система с два източника</b>	<b>65</b>
<b>Фиг. 2.16. Паралелна система с недетерминизъм – три източника</b>	<b>66</b>
<b>Фиг. 2.17. Изходна последователност при система с три източника</b>	<b>66</b>
<b>Фиг. 2.18. Включване на недетерминизъм при обработката на събитията</b>	<b>67</b>
<b>Фиг. 2.19. Параметри на изчисляваната статистика</b>	<b>70</b>
<b>Фиг. 2.20. Таблица на разпределението <math>\chi^2</math> при степен на свобода 1</b>	<b>73</b>
<b>Фиг. 2.21. Формиране на контролната плъзгаща се статистика в реално време</b>	<b>74</b>
<b>Фиг. 3.1. Схема на опитната постановка</b>	<b>75</b>
<b>Фиг. 3.2. Снимка на опитната постановка</b>	<b>76</b>
<b>Фиг. 3.3. Виртуален панел за управление на осцилоскопа</b>	<b>76</b>
<b>Фиг. 3.4. Разположение на точките на прекъсване за целите на настройката</b>	<b>77</b>
<b>Фиг. 3.5. Първоначален достъп до статистиката чрез дебъгера на средата XDE</b>	<b>78</b>
<b>Фиг. 3.6. Следващ достъп до статистиката чрез дебъгера на средата XDE</b>	<b>79</b>
<b>Фиг. 3.7. Обобщени резултати от измерванията</b>	<b>79</b>
<b>Фиг. 3.8. Графично представяне на резултатите от измерванията</b>	<b>79</b>

# СПИСЪК НА СЪКРАЩЕНИЯТА

CSP - Communicating Sequential Processes (Взаимодействащи последователни процеси)

CRC – Cyclic Redundancy Check (Цикличен контролен код, Полиномиален контролен код)

DLP – Data Level Parallelism (Паралелизъм на ниво данни)

DSP – Digital Signal Processor/Digital Signal Processing (Процесор за цифрова обработка на сигналите/Цифрова обработка на сигналите, ЦОС)

ILP - Instruction Level Parallelism (Паралелизъм на ниво инструкции, локален паралелизъм, базиран на конвейеризацията на инструкциите)

JTAG – Joint Test Action Group (Стандартен интерфейс за връзка между инструменталната и целевата машина)

LCG – Linear Congruential Generator (Линеен конгруентен генератор)

LFSR – Linear Feedback Shift Register (Изместващ регистър с линейна обратна връзка)

MAC – Multiply And Accumulate (сложен оператор от вида „Умножи и натрупай“, популярен при DSP)

MLCG – Multiplicative Linear Congruential Generator (Мултипликативен линеен конгруентен генератор)

MPP – Massively-Parallel Processor (Масово-паралелен процесор)

MTP - Multithreading Parallelism (многонишков паралелизъм, паралелизъм на ниво нишки)

OCCAM – ОККАМ (Език за паралелно програмиране, базиран на CSP)

OSI – Open Systems Interconnection (Теоретичен модел, описващ принципния начин на комуникация и строежа на компютърните мрежи)

OTP – Once-Time Programmable Memory (Постоянна памет, ROM)

PHY - Physical Layer (Физическото ниво от OSI модела)

PRNG – Pseudo-Random Number Generator (Генератор на псевдослучайни числа)

RISC – Reduced Instruction Set Computer (Компютър с опростена система инструкции)

RNG – Random Number Generator (Генератор на случайни числа)

RRNG – Real Random Number Generator (Генератор на действително-случайни последователности)

SMT - Simultaneous Multithreading (Едновременно многонишково изпълнение; общоприето название на апаратната технология, позволяваща едновременното изпълнение на няколко нишки; фирмата Intel използва обозначението Hyperthreading)

SPI – Serial Peripheral Interface Bus (Сериен периферен интерфейс)

SRAM – Static Random-Access Memory (Статична памет с произволен достъп)

STL - Standard Template Library (Стандартна библиотека от шаблони на C++)

TLP – Task Level Parallelism (Паралелизъм на ниво задачи)

TRNG – True Random Number Generator (Генератор на действително-случайни последователности)

UVLSI – Ultra Very Large Scale Integration (СГИС, Свърхголеми интегрални схеми)

USB – Universal Serial Bus (Универсална серийна шина)

VLWI – Very Large Instruction Word (RISC архитектура с много голяма дължина на инструкцията; един от методите за явен ILP)

VLSI – Very Large Scale Integration (ГИС, Големи интегрални схеми)

XC – XMOS C (паралелна версия на езика C за архитектурата XS1 на фирмата XMOS, разширение на езика C с паралелни конструкции, повечето от които се поддържат директно на апаратно ниво)

XCORE - паралелно ядро от фамилията XS1 на фирмата XMOS с глобален структурен паралелизъм; физическа реализация на CSP-машина с апаратна поддръжка на паралелизма

XCORE/XC - паралелна платформа на фирмата XMOS, базирана на паралелната архитектура XCORE и на езика за паралелно програмиране XC

XDE – XMOS Development Environment (Название на развойната среда на фирмата XMOS до версия 11; от версия 12 е част от окупнената развойна среда *xTIMEcomposer Studio* на фирмата XMOS)

XOR – Exclusive Or (Изключващо ИЛИ)

XS1 - Фамилия паралелна архитектура от типа XCORE на фирмата XMOS