Міністерство освіти і науки України
Вінницький національний технічний університет
Прикарпатський національний університет ім. Василя Стефаника
Інститут кібернетики імені В. М. Глушкова НАН України
Національний технічний університет України “КПІ"
Харківський національний технічний університет «ХПІ»
Новий університет Лісабона - Португалія
Азербайджанська державна нафтова академія
Об’єднаний інститут проблем інформатики НАН Білорусі
Гірничо-металургійна академія AGH - Польща
Інститут інженерів з електротехніки та електроніки (IEEE), Українська секція

Методи та засоби кодування, захисту й ущільнення інформації

Тези доповідей
Шостої Міжнародної
науково-практичної конференції
м. Вінниця, Україна
24 - 25 жовтня 2017 року

Методы и средства кодирования, защиты и сжатия информации

Тезисы докладов
Шестой Международной
научно-практической конференции
г. Винница, Украина
24 - 25 октября 2017 года

ВНТУ 2017

УДК 004+681.3+621.3
ББК 32
М54

Відповідальний редактор В. А. Лужецький

Матеріали статей опубліковані в авторській редакції

Методи та засоби кодування, захисту й ущільнення інформації. М54 Тези доповідей Шостої Міжнародної науково-практичної конференції м. Вінниця, 24-25 жовтня 2017 року : збірник наукових праць. – Вінниця: ВНТУ, 2017. – 170 с.

ISBN 978-966-641-709-4

Збірка містить матеріали доповідей Шостої Міжнародної науково-практичної конференції з сучасних проблем кодування, захисту й ущільнення інформації за чотирма основними напрямками: методи та засоби завадостійкого кодування; методи та засоби захисту інформації від несанкціонованого доступу; методи та засоби ущільнення інформації; методи та засоби перетворення форм інформації.

УДК 004+681.3+621.3
ББК32

ISBN 978-966-641-709-4

ЗМІСТ

СЕКЦІЯ 1. ***Методи та засоби завадостійкого кодування***

О ДЕКАДНОСТІ ФІБОНАЧІЄВИХ ЧИСЕЛ
Мальченков С., Борисенко О. 7

ОСОБЛИВОСТІ ОДИНИЧНОГО КОДУВАННЯ ІНФОРМАЦІЇ
Мартинюк Т., Тарасова О., Очкуров М., Павлов П 10

ШВИДКЕ ДЕКОДУВАННЯ ПАРАЛЕЛЬНИХ КОДІВ CRC
Семеренко В.П, Григорчук Б.О. 13

СЕКЦІЯ 2. ***Методи та засоби захисту інформації***

NUMERAL SYSTEMS WITH IRRATIONAL BASES FOR MISSION-CRITICAL APPLICATIONS.THE BASIC CONCEPTS AND SCIENTIFIC RESULTS
O. Stakhov 16

СИНТЕЗ И АНАЛИЗ УОЛША-ПОДОБНЫХ СИСТЕМ СЕКВЕНТНЫХ ФУНКЦИЙ
Белецкий А. Я. 21

HASH FUNCTIONS BASED ON ONE- AND MULTY-DIMENSIONAL CELLULAR AUTOMATA
O. Konstantynyuk, Yu. Tanasyuk, S. Ostapov 25

COMPARATIVE OVERVIEW OF BASIC CYBERVULNERABILITIES OF MOBILE APPLICATIONS FOR ANDROID OPERATING SYSTEM
Semenov S., Shypova T., Movchan O 29

ЗАХИСТ АКУСТИЧНОЇ ІНФОРМАЦІЇ МЕТОДОМ ПРОТИФАЗНОГО ПРИДУШЕННЯ
Цирульник С. М. , Бородай Я. О., Роптанов В. І 32

FACE SEARCHING BY IMAGE PARTITIONING, HISTOGRAM EQUALIZING AND FRAMES
R. A. Melnyk, S. O. Dakhnii 35

ФОРМУВАННЯ РЕКОМЕНДАЦІЙ ДЛЯ УСУНЕННЯ НАСЛІДКІВ МЕРЕЖЕВИХ АТАК
Суприган О.І., Гикава М.В 38

ПЕРЕВІРКА ДЕЛЕГОВАНИХ ОБЧИСЛЕНЬ ЗА ДОПОМОГОЮ ДОДАВАЛЬНОЇ МАШИНИ
Анісімов А.В., Новокшонов А.К. 42

SYSTEM OF THE SQL INJECTION PREVENTION
Voitovych O.P., Kupershtein L.M., Ostapenko A.V.Yuvkovetskyi O.S 45

MODELS OF PSEUDONONDETERMINISTIC CRYPTOGRAPHIC TRANSFORMATIONS
Baryshev Y.V 48

СПОСІБ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ГРАФІЧНИХ ДАНИХ НА ОСНОВІ СХЕМИ ВІДПОВІДНОСТІ БІТІВ ТА АНАЛІЗУ ВІЗУАЛЬНИХ ВЛАСТИВОСТЕЙ КОНТЕЙНЕРА
Радченко Є. О., Сулема Є. С. …… 51

СИСТЕМА МОНІТОРИНГУ ТА АУДИТУ БЕЗПЕКИ В ОС ANDROID
Войтович О.П., Гурський М.В.…… 54

ВИКОРИСТАННЯ ТРАНСФЕРНИХ ВУЗЛІВ РУХОМИХ МЕРЕЖ ДЛЯ АТАКИ НА КОМП'ЮТЕРНІ СИСТЕМИ НАЗЕМНИХ АБОНЕНТІВ МЕРЕЖІ
Журавська І. М.……. 58

КОНЦЕПТУАЛЬНІ НАПРЯМКИ КОМПЛЕКСНОГО ВИРІШЕННЯ ПРОБЛЕМИ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ В СКЛАДНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ
Вдовенко С. Г., Даник Ю. Г.…… 61

СПОСІБ ПЕРЕХОПЛЕННЯ КЕРУВАННЯ БЕЗПІЛОТНИМИ ЛІТАЮЧИМИ АПАРАТАМИ У МЕЖАХ КОНТРОЛЬОВАНОЇ ЗОНИ
Самойленко Д. М., Нечуєв Д. О.……. 65

ДОСЛІДЖЕННЯ БЕЗПЕКИ СИСТЕМИ РОЗУМНОГО БУДИНКУ
Войтович О.П., Вишньовський В.В., Савченко К.В…….. 67

РЕАЛІЗАЦІЯ БЕЗПЕЧНОГО ТРАНЗИТУ ПАРАМЕТРІВ HTTP ПРОТОКОЛУ
Самойленко Д. М., Сівко О.Е……..... 71

КОНЦЕПТУАЛЬНИЙ ПІДХІД ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СОЦІОТЕХНІЧНОЇ СИСТЕМИ
Дудатьєв А.В., Літушко О.А…….. 73

ДОСЛІДЖЕННЯ МЕТОДІВ АНАЛІЗУ СОЦІАЛЬНИХ МЕРЕЖ ЯК СЕРЕДОВИЩА ІНФОРМАЦІЙНИХ ВІЙН
Войтович О. П., Буда А. Г., Головенько В. О …….. 76

МАСШТАБИРОВАНИЕ ГИБКОЙ МЕТОДОЛОГИИ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С УЧЕТОМ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ
Семенов С. Г., Кассем Халифе, Змиевская В. Н…….. 81

СЕКЦІЯ 3. ***Методи та засоби ущільнення інформації***

ПОДІЛЬНІ КОДИ ТА ЇХ ЗАСТОСУВАННЯ
Анісімов А.В., Завадський І.О…… 84

АСПЕКТИ ОПТИМІЗАЦІЇ ШВИДКОСТІ ФРАКТАЛЬНОГО УЩІЛЬНЕННЯ ЗОБРАЖЕНЬ
Майданюк В.П., Ліщук О.О.…….. 89

ЗАСТОСУВАННЯ ОРТОГОНАЛЬНОГО ПЕРЕТВОРЕННЯ НА ОСНОВІ ТРІЙКОВИХ СИМЕТРИЧНИХ ФУНКЦІЙ ДЛЯ ЦИФРОВОЇ ОБРОБКИ ІНФОРМАЦІЇ 93
Ізмайлов А. ……..

МЕТОД ДВОХГРАДАЦІЙНОГО НЕРІВНОМІРНОГО ПОЗИЦІЙНОГО КОДУВАННЯ З ДИНАМІЧНИМ БАЗИСОМ ОСНОВ
Краснорyцький А.О., Бараннік Д.В…….. 97

СЖАТИЕ ДВОИЧНОЙ ИНФОРМАЦИИ НА ОСНОВЕ БИНОМИАЛЬНОЙ ЧИСЛОВОЙ ФУНКЦИИ
Борисенко А.А., Кулик И.А…… 102

CODING OF A RESOURCE BLOCK BY A SYSTEM WITH NON EQUILIBRIUM WEIGHTING COEFFICIENTS FOR LTE-BASED MOBILE COMMUNICATION TECHNOLOGIES
Barannik V., Okladnoy D., Podlesnyi S…… 105

ЭФФЕКТИВНОЕ КОДИРОВАНИЕ СЕГМЕНТИРОВАННЫХ ВИДЕОКАДРОВ ДЛЯ СНИЖЕНИЯ ИНФОРМАЦИОННОЙ ИНТЕНСИВНОСТИ ВИДЕОПОТОКА
Баранник В.В., Хіменко В.В., Тарасенко Д.А……. 109

СЕКЦІЯ 4. ***Методи та засоби перетворення форм інформації***

METHOD OF DETERMINING THE UNUSED COMBINATIONS IN THE ADC OF SUCCESSIVE APPROXIMATION WITH WEIGHT REDUNDANCY
Zakharchenko S., Zakharchenko M., Humeniuk R…….. 114

КАЛІБРУВАННЯ НЕЛІНІЙНОСТІ БІОМЕДИЧНИХ ОПТИЧНИХ СЕНСОРІВ В АЦ-СИСТЕМАХ
Гарнага В., Крупельницький Л., Стогнушко Є……... 118

РОЗРОБКА СПЕЦІАЛІЗОВАНОГО АУДІОПРИСТРОЮ З РОЗВИНЕНОЮ ФУНКЦІОНАЛЬНОЮ ТА КОМУТАЦІЙНОЮ СИСТЕМОЮ
Войтко В., Білоконь В., Рекута Ю., Яковенко О., Кокушкін В., Цукрук В……. 121

ПІДХОДИ ЩОДО ЗМЕНШЕННЯ ГЛІТЧІВ ТА ШУМІВ В АЦП ПОРОЗРЯДНОГО ВРІВНОВАЖЕННЯ З ВАГОВОЮ НАДЛИШКОВІСТЮ
Азаров О., Крупельницький Л., Медяний Р.………. 124

МЕТОД ТА АНАЛОГО-ЦИФРОВІ ЗАСОБИ ПАСИВНОГО АКУСТИЧНОГО СКАНУВАННЯ ВНУТРІШНІХ ОРГАНІВ ЛЮДИНИ
Крупельницький Л.В., Грабчак С.О., Фігас А.С……….. 128

МЕТОДИ АДИТИВНОГО ТА СУБТРАКТИВНО-АДИТИВНОГО АНАЛОГОВО-ЦИФРОВОГО ПЕРЕТВОРЕННЯ
Петришин М.Л………. 131

ЗАСТОСУВАННЯ ТЕОРІЇ МАСОВОГО ОБСЛУГОВУВАННЯ НА СТАДІЇ МОДЕЛЮВАННЯ БАГАТОПРОЦЕСОРНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ
Петришин Л.Б…….. 135

МЕТОД ЗМЕНЬШЕННЯ ГЛІТЧІВ У ЦАП ІЗ ВАГОВОЮ НАДЛИШКОВІСТЮ
Азаров О.Д., Муращенко О.Г …….. 139

ДЖЕРЕЛА СТАБІЛЬНОГО СТРУМУ ДЛЯ БАГАТОРОЗРЯДНИХ АЦП І ЦАП
Азаров О.Д., Обертюх М.Р. …… 143

ВИКОРИСТАННЯ БЕЗДРОТОВИХ МЕРЕЖ У СИСТЕМАХ ОПРАЦЮВАННЯ БІОМЕДИЧНИХ СИГНАЛІВ
Азаров О.Д., Крупельницький Л.В., Богомолов С.В., Гончарук В.І., Тищенко В.М. 146

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ТЕПЛОВИХ СЕНСОРІВ ПОТОКУ ЗАГАЛЬНОГО ТА БІОМЕДИЧНОГО ПРИЗНАЧЕННЯ
Голяка Р., Вуйцик В., Павлов С., Карнакова Г. Ж., Куленко С ……. 151

АНАЛІЗ СУЧАСНИХ МЕТОДІВ І ОПТИЧНИХ СИСТЕМ ДЛЯ ДІАГНОСТУВАННЯ ПАТОЛОГІЙ МОЛОЧНОЇ ЗАЛОЗИ
Радченко К.О …….. 155

МНОГОУРОВНЕВАЯ СИСТЕМА ЗАЩИТЫ И УПРАВЛЕНИЯ МЕДИЦИНСКИМ ДИАГНОСТИЧЕСКИМ ОБОРУДОВАНИЕМ (МДО)
Злепко С. М.,. Чернышова Т. А, Кривоносов В. Е., Азархов О. Ю.,
Ярославский Я. И., Барановский Д. М ……. 157

ОСНОВНІ ПЕРЕВАГИ ЗАСТОСУВАННЯ ВИСОКОРОЗРЯДНИХ ЦАП З ВАГОВОЮ НАДЛИШКОВІСТЮ У СИСТЕМАХ ПРЯМОГО ЦИФРОВОГО СИНТЕЗУ
Азаров О.Д., Крупельницький Л.В., Генеральницький Є. С ……... 160

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ВІДДАЛЕНОГО ВИДІЛЕННЯ ЦІЛОЇ І ДРОБОВОЇ ЧАСТИН ЧИСЕЛ У КОДАХ ЗОЛОТОЇ ПРОПОРЦІЇ
Азаров О.Д., Черняк О.І., Залізецький В.В ……... 163

ОСОБЕННОСТИ ПРИМЕНЕНИЯ СЕНСОРОВ НА ОСНОВЕ ВОЛОКОННО-ОПТИЧЕСКИХ БРЭГГОВСКИХ РЕШЕТОК ДЛЯ ИЗМЕРЕНИЯ ТЕМПЕРАТУРЫ
Вуйцик В., Павлов С., Шедреева И …….. 167

СЕКЦІЯ 1.
Методи та засоби завадостійкого кодування

О декадності фібоначієвих чисел

Олексій Борисенко, Сергій Мальченков
кафедра електроенергетики,
Сумський державний університет
Суми, Україна
malchenkovs@gmail.com

About Decades Fibonachi Numbers

Oleksii Borisenko, Serhii Malchenkov
Department of Electronic and Computer Technology
Sumy State University
Sumy, Ukraine,
malchenkovs@gmail.com

***Анотація* — У даній роботі пропонуються один із способів підвищення швидкодії системи при зберіганні належної надійності системи шляхом використання фібоначчієвого-десяткових модульних лічильників. Розкривається декадність Фібоначчієвих чисел, їх зведення до зручного використання у двійковій логіці, та об'єднання у модульну структуру, що підвищує технологічність, завадостійкість, швидкодію усієї системи, та призводить до зменшення апаратурних затрат у подальшому зрощуванні розрядності.**

***Abstract* — In this paper, propose one of the ways to improve the performance system while maintaining the system's due reliability is by using Fibonacci-decade counters. The decade of the Fibonacci numbers, their reduction to convenient using in binary logic, and merging into a modular structure that increases the technological capacity, noise immunity, and the speed of the whole system, is revealed, and leads to a decrease in hardware in the further incorporation of the bit.**

Ключові слова — швидкодія, завадостійкість, модульна система, фібоначчі-декадний лічильник, числа Фібоначчі

Keywords — performance, noise immunity, modular system, Fibonacci decade counter, Fibonacci numbers

I. Вступ

Починаючи з 60-70хх років минулого століття була поставлена задача побудови повноцінного комп'ютерного пристрою на основі фібоначчієвих кодів – комп'ютер Фібоначчі. Нажаль, дана задача не була вирішена і на деякий час ця проблема була відкладена. Але сучасні тенденції, щодо розвитку інформаційних технологій, призводять до постановки задач вдосконалення процесів транспортування, обробки і відображення інформації у найбільш короткий час з максимально можливою надійністю. Так як двійкові коди заполонили усі системи і алгоритми роботи існуючих пристроїв та систем, починаючи з К. Шеннона та Дж. фон Неймана [6], це робить недоцільним вирішення поставлених задач через принципово інший код з більшим алфавітом, хоча такі наміри і є (наприклад, троїчні коди). Натомість тому виступають завадостійкі коди, які не потребують надмірності, в противагу двійковим. До них відносяться біноміальні, факториальні і фібоначчієві коди. Біноміальні і факторіальні коди мають свої переваги, але все ж для більшості задач не дотягують за необхідним показником швидкодії, і підходять для вирішення задач більш вузької направленості. [1,2] Фібоначчієві коди є найбільш швидкодіючими для застосування у лічильних пристроях з існуючих завадостійких кодів.

Ціль даних тез викласти ідею використання Фібоначчієвих чисел у проблемах завадостійкості та швидкодії вимірювальних систем, так і електронних систем в цілому

II. Теоретичний базис Фібоначчієвих чисел

Числами Фібоначчі називають послідовність, члени якої, починаючи з третього, дорівнюють сумі двох попередніх, при перших двох членах послідовності, що дорівнюють одиниці:

$F_n=F_{n-2}+F_{n-1}$, при $F_1=F_2=1$ (1)

Завдяки числам Фібоначчі можна отримати код для побудови лічильника з необхідними параметрами.

Перевагами лічильників Фібоначчі виступає як можливість позбавитися від переносів між розрядами, так і однорідна структура, технологічність. З цього випливає, що для задач

вимірювальної техніки будувати лічильники ефективніше з кодів, що надають підвищену швидкодію при необхідному рівні надійності. (табл. 1).

Табл. 1. – Послідовність фібоначієвих чисел для ряду – 1, 2, 3, 5, 8.

№	Фибоначчиєві числа				
	8	5	3	2	1
0	0	0	0	0	0
1	0	0	0	0	1
2	0	0	0	1	0
3	0	0	1	0	0
4	0	0	1	0	1
5	0	1	0	0	0
6	0	1	0	0	1
7	0	1	0	1	0
8	1	0	0	0	0
9	1	0	0	0	1

Розберемо таблицю 1: 0-9 – це десяткові відповідники фібоначчієвих чисел; F_n=1, 2, 3, 5, 8 – ваги розрядів, представленні фібоначчієвою послідовністю, де кожний наступний член, починаючи з третього, дорівнює сумі двох попередніх. Для зручності побудови чисел першу одиницю послідовності не використовується. При розрядності n=5 виходить максимально 13 дозволених комбінацій. Щоб отримати декадний лічильник потрібно лише використовувати десять перших комбінацій. Самі ж фібоччієві числа у мінімальній формі представлення мають цікаву властивість: вони не мають поруч стоячих одиниць. Це дуже зручно, так як при їх появі лічильник зможе виявити помилку.

При задачах, зокрема, вимірювання фізичних величин постає питання лічби. Доволі часто у вимірювальній техніці використовуються декадні лічильники. Це зумовлено потрібністю у перетворенні інформації у вигляд, зрозумілий для сприйняття оператора (людини). Для зручності і ефективності такого процесу використовують декадні лічильники, тобто лічильники з коефіцієнтом перерахунку 10. Такі лічильники є зручними для задач подальшого оброблення, транспортування і відображення інформації в першу чергу тому, що наш світ звик до десяткової системи лічби і усі пристрої відображення інформації, що направленні на вивід зрозумілої людині інформації у кінцевому випадку прив'язуються до них. З іншого боку, декадний лічильник дозволяє швидко нарощувати розрядність лічильника без розв'язку проектувальних задач.

III. Модульна система представлення лічильників Фібоначі у мінімальній формі

Почнемо з прикладу. Візьмемо звичайний 4-х розрядний двійковий лічильник, то отримаємо 16 дозволених комбінацій і жодної забороненої. Завадостійкість такого коду сходить до нуля (при розрахунку П=1-n/M, де n – кількість дозволених кодових комбінацій, M – загальна кількості кодових комбінацій). Для того, щоб отримати декадний лічильник, з цих кодових комбінацій беремо 10, останні 6 становляться забороненими. Завадостійкість такого коду збільшується з нуля до 37,5 %.

Візьмемо лічильник Фібоначчі у мінімальній формі представлення [3]. Він має 13 дозволених кодових комбінацій та 19 заборонених. Завадостійкість такого коду вже складає 40,6 %. Візьмемо декаду 10 кодових комбінацій, 22 – будуть заборонені. Завадостійкість збільшується на 28,15 % і складає 68,75 %. Беремо до уваги те, що даний лічильник може виявляти помилку при появі двох поруч стоячих одиниць, то завадостійкість ще збільшується. Такі лічильники можна ставити один за одним, збільшуючи розрядність не ускладняючи схему, що призводить до універсальності пристрою.

Якщо говорити про лічильник Фібоначчі [3], то стає питання його удосконалення. П'яти розрядний лічильник Фібоначчі представлений у мінімальній формі при тринадцяти кодових комбінацій створює додаткові задачі при його використані та перетворені з вимірювальних пристроях у чистому вигляді. Ця проблема розв'язується шляхом приведення даного лічильника у декадну форму. Коефіцієнт переліку даного лічильника складає десять, що гармонійно сходиться з десятковою системою лічби, яка використовується у повсякденні і є зручною, як для відображення інформації, так і її транспортування. Тому що відпадає необхідність її перетворення. При використані декади Фібоначчі код Фібоначчі зручно перетворювати у двійковий, та навпаки, не переходячи до десяткового еквіваленту.

Декада Фібоначчі підводить до теорії фібоначчієво-десяткових чисел, які мають властивості фібоначієвих чисел представлених у мінімальній формі [4].

У табл. 2 приведено співвідношення фібоначчієво-десяткових і двійково-десяткових чисел.

Табл. 2. – Перетворення фібоначчієво-десяткових чисел у двійково-десяткові числа

№	5	4	3	2	1	4	3	2	1
	8	5	3	2	1	8	4	2	1
	a_5	a_4	a_3	a_2	a_1	a_4	a_3	a_2	a_1
0	0	0	0	0	0	**0**	**0**	**0**	**0**
1	0	0	0	0	1	**0**	**0**	**0**	**1**
2	0	0	0	1	0	**0**	**0**	**1**	**0**
3	0	0	1	0	0	**0**	**0**	**1**	**1**
4	0	0	1	0	1	**0**	**1**	**0**	**0**
5	0	1	0	0	0	**0**	**1**	**0**	**1**
6	0	1	0	0	1	**0**	**1**	**1**	**0**
7	0	1	0	1	0	**0**	**1**	**1**	**1**
8	1	0	0	0	0	**1**	**0**	**0**	**0**
9	1	0	0	0	1	**1**	**0**	**0**	**1**

У даній таблиці 2 у першому стовпці перелічені десяткові еквіваленти фібоначчієво-десятковим числам. З другого до шостого стовпця приведені порозрядно фібоначчієво-десяткові числа, де a_5 – це старший розряд кодового числа і a_1 – молодший розряд кодового числа. З сьомого до десятого стовпця вказано двійково-десяткові еквіваленти фібоначчі-десяткових чисел. З такого співвідношення випливає те, що немає необхідності переходу від фібоначчієвої форми представлення числа у десятковий, а потім переходити від десяткового до двійкового, як це може бути при використанні завадостійких кодів у повному вигляді або кодів з надмірністю (наприклад, циклічні коди).

З цього випливає модульна структура фібоначчі-десяткових лічильників. Зі збільшенням коефіцієнту переліку збільшується і розрядність лічильника. При п'яти розрядах максимальна кількість кодових комбінацій 13, при 6-ти – 21, при 7-ми – 34 і т.д. Якщо ж взяти фібоначчієво-десятковий лічильник, що має десять кодових комбінацій, то якщо поставити два таких лічильника послідовно, то тоді отримаємо коефіцієнт переліку 100, три – 1000, чотири - 10000 і так далі. Це призводить до універсальності і технологічності кінцевого пристрою і спрощує задачу проектування і подальшого транспортування, обробки та відображення інформації. При зрощуванні коефіцієнта перерахунку стає задача звичайного нарощування кількості модулів у лічильному пристрої, а не його розрядність. Використовуючи фібоначчі-десяткові лічильники спрощується етапи перетворення і зберігання проміжних результатів. Якщо порівнювати один модуль – лічильник з лічильником Фібоначчі, то швидкодія принципово не зміниться. А ось якщо виходити на модульність, то при збільшені модулів пристрою швидкодія системи, в порівнянні зі збільшенням розрядів [5], буде лише зрощуватись, як і завадостійкість усієї системи.

IV. Висновки.

З розвитком інформаційних систем постало питання збільшення швидкості її транспортування, обробки і відображенні при належному рівні її достовірності та при мінімальних апаратурних затратах. Як варіант, рішення такої глобальної задачі пропонується роботою фібоначчі-декадних лічильників, побудованих за модульним принципом. З одного боку, він задіє усі властивості фібоначчієвої системи числення, не потребує знаходження десяткового еквіваленту при перетворені коду, і, з іншого, завдяки модульному принципу з легкістю нарощується розрядність без розв'язування складних проектувальних задач.

Література

1. Петров В. В. Методы и модели построения компонентов цифровых устройств на основе матричных биномиальных чисел: Дис. канд. техн. наук: 05.13.05 / В. В. Петров. – Сумы., 2012. – 207 с.

2. Горячев, А. Е., Метод генерации перестановок на основе факториальных чисел с использованием дополняющего массива [Текст] / А. Е. Горячев, С. А. Дегтяр // Висник Сумского державного ниверситета. Серия технических наук. - 2012. - Выпуск 4. - С. 86-93.

3. Пат. на корисну модель 89153 Україна, МПК (2014) H03K 23/00. Лічильник імпульсів / О. А. Борисенко, С. М. Маценко; заявн. Сумський державний університет. – № u201313302; заявл. 15.11.2013; опубл. 10.04.2014; Бюл. №7. – С. 1–5.

4. Борисенко О.А., Стахов О.П,, Маценко С.М., Пристрій для дешифрування кодів Фібоначі: Матеріали статей П'ятої Міжнародної науково-практичної конференції "Інформаційні технології та комп'ютерна інженерія", м. Івано-Франківськ, 2015. – 230 с.

5. Борисенко А.А, Маценко С.М., Мальченков С.М., Ямник О.И. О помехоустойчивости фибоначчиевых чисел: журнал «Системы обработки информации», Харьков, 2015. – 4(129).

6. Стахов А. П. Микропроцессоры Фибоначчи – как одна из базисных инноваций будущего технологического уклада, изменяющих уровень информационной безопасности систем. «Междисциплинарные исследования в науке и образовании» №1, г. Киев, 2012. – 59 с.

References

[1] Petrov, VV, Methods and models for constructing components of digital devices based on matrix binomial numbers: Dis. Cand. tech. Sciences: 05.13.05 / VV Petrov. - Sumy., 2012. - 207 p.

[2] Goryachev, AE, Method of generation of permutations on the basis of factorial numbers with the use of a complementing array [Text] / AE Goryachev, SA Degtyar // Visnik of the Sumy State University. A series of technical sciences. - 2012. - Issue 4. - P. 86-93.

[3] Stalemate. to utility model 89153 Ukraine, IPC (2014) H03K 23/00. Pulse counter / O. A. Borisenko, S. M. Matsenko; an application Sumy State University. - № u201313302; stated. 15.11.2013; has published 04/10/2014; Bull No. 7 - P. 1-5.

[4] Borisenko OA, Stakhov O.P., Matsenko S.M., Device for decoding codes Fibonacci: Articles of the Fifth International Scientific and Practical Conference "Information Technologies and Computer Engineering", Ivano-Frankivsk city, 2015. - 230 p.

[5] Borisenko A.A., Matsenko S.M., Malchenkov S.M., Yamnik O.I. On Noise Immunity of Fibonacci Numbers: Journal of Information Processing Systems, Kharkov, 2015. - 4 (129).

[6] Stakhov AP Fibonacci microprocessors - as one of the basic innovations of the future technological order that change the level of information security of systems. "Interdisciplinary Research in Science and Education" № 1, Kyiv, 2012. - 59 p.

Особливості одиничного кодування інформації

Тетяна Мартинюк
кафедра обчислювальної техніки
Вінницький національний технічний університет
Вінниця, Україна
martyniuk.t.b@gmail.com

Микола Очкуров
кафедра обчислювальної техніки
Вінницький національний технічний університет
Вінниця, Україна
ochkurovma.50@ukr.net

Ольга Тарасова
кафедра обчислювальної техніки
Вінницький національний технічний університет
Вінниця, Україна
Tarasovaolga016@gmail.com

Петро Павлов
кафедра обчислювальної техніки
Вінницький національний технічний університет
Вінниця, Україна
batman-peter@ukr.net

Features of the unit coding of information

Tetiana Martyniuk
Department of Computer Technique
Vinnytsia National Technical University
Vinnytsia, Ukraine,
martyniuk.t.b@gmail.com

Mykola Ochkurov
Department of Computer Technique
Vinnytsia National Technical University
Vinnytsia, Ukraine,
ochkurovma.50@ukr.net

Olha Tarasova
Department of Computer Technique
Vinnytsia National Technical University
Vinnytsia, Ukraine,
Tarasovaolga016@gmail.com

Peter Pavlov
Department of Computer Technique
Vinnytsia National Technical University
Vinnytsia, Ukraine,
batman-peter@ukr.net

***Анотація*—В роботі розглянуто особливості двох різновидів одиничного коду: одиничний нормальний та одиничний позиційний коди. Наведено результати дослідження основних властивостей одиничних кодів за принципами алгебраїчної теорії кодування. Проведено порівняльний аналіз одиничних кодів і коду Хеммінга. Визначено місце одиничних кодів у класифікаційній схемі відомих кодів. Показано, що одиничні коди класифікуються як окрема група кодів зі специфічними властивостями.**

***Abstract*—In the work the features of two varieties of unit code are considered: single normal and unit position codes. The results of the study of the basic properties of unit codes based on the principles of the theory of coding algebra are given. A comparative analysis of unit codes and Hamming code are conducted. place of unit codes in the classification scheme of known codes. Unit codes are classified as a separate group of codes with specific properties.**

Ключові слов—одиничне кодування; класифікаційна схема кодування.

Keywords—unit coding; classification scheme of coding.

I. Вступ

Поряд із широко відомими способами представлення числової інформації, а саме, двійковою, трійковою і десятковою системами числення, у процесі комп'ютерної обробки числової інформації знайшли застосування і нетрадиційні методи кодування, а саме, кодування в знакологарифмічній системі, у системі залишкових класів [1].

Серед нетрадиційних методів кодування займають своє місце одиничні коди, що орієнтовані на реалізацію з використанням оптоелектронної елементної бази [2-4]. Область застосування цих кодів охоплює не тільки арифметичну і логічну обробку і представлення числової інформації, але й асоціативну обробку, а також попередню обробку й аналіз зображень [5].

II. Одиничні коди та їх характеристики

За специфікою формування ваги розрядів від двійкових кодів відрізняються одиничні коди [2, 3, 6]. У загальному випадку одиничним називається код, в якому кожне двійкове слово (вектор) визначається місцем розташування певного

маркувального коду, а саме місцем розташування одиничного маркера (1) [3].

Відомо, що для обробки і подання десяткової інформації використовуються два види одиничного коду [2]: одиничний нормальний та одиничний позиційний код. Одиничний код може бути одиничним нормальним одноканальним або одиничним позиційним (багатоканальним), призначеним для передачі одиничними імпульсами по провідниках лінії зв'язку.

Кожне слово $C_i(i=\overline{1,m})$ одиничного позиційного коду формується за таким правилом [7]:

$$C_i = \alpha \sum_{j=1}^{i} \varphi_j, j = \overline{1,n} \quad (1)$$

де α – одиничний маркер, α = 1; φ_j – вага j-го розряду слова коду, φ_j = 1.

Слова $C_i(i=\overline{1,m})$ одиничного нормального коду формуються за таким правилом [7]:

$$C_i = \alpha \sum_{j=1}^{n} \alpha_{ij} \varphi_j = \sum_{j=1}^{i} \alpha_{ij}^{1} \varphi_j + \sum_{j=i+1}^{n} \alpha_{ij}^{0} \varphi_j, \quad (2)$$

де $\alpha_{ij} \in \{0;1\}, \alpha_{ij}^{1} = 1, \alpha_{ij}^{0} = 0, \varphi_j = 1$.

Відповідно до приведених виразів (1) та (2) матриця кодування D_{10p}^{10} [3, 7] для одиничного позиційного коду матиме такий вигляд (3)

$$D_{10p}^{10} = \begin{bmatrix} 1000000000 \\ 0100000000 \\ 0010000000 \\ 0001000000 \\ 0000100000 \\ 0000010000 \\ 0000001000 \\ 0000000100 \\ 0000000010 \\ 0000000001 \end{bmatrix}, \quad (3)$$

а матриця кодування D_{10n}^{10} для одиничного нормального коду матиме такий вигляд (4)

$$D_{10n}^{10} = \begin{bmatrix} 1000000000 \\ 0100000000 \\ 0110000000 \\ 0111000000 \\ 0111100000 \\ 0111110000 \\ 0111111000 \\ 0111111100 \\ 0111111110 \\ 0111111111 \end{bmatrix}. \quad (4)$$

Поширення одиничного способу кодування на представлення цифр дозволило вирішити одну з важливих проблем – досягти незалежності представлення для нуля та одиниці [2, 3]. Аналіз результатів одиничних кодів дає можливість визначити такі їх основні переваги:

- Збереження всіх основних арифметичних і логічних переваг позиційних систем числення (простота правил виконання арифметичних і логічних операцій, способу порівняння за величиною ознаки переповнення розрядної сітки).
- Можливість округлення чисел і представлення дробових і від'ємних чисел, ітераційність чи однорідність цифрових структур, що реалізують арифметику в порівнянні з іншими способами введення кодової надмірності в ЕОМ (система залишкових класів, контроль за модулем і т. п.) [2, 3, 6, 7].
- Відсутність необхідності в декодуванні (дешифруванні) значень одиничних позиційних кодів для представлення керуючої й адресної інформації [5, 6].

При представленні інформації з використання одиничного кодування виникає необхідність у застосуванні багатозначних елементів, які можна розглядати як елементарні автомати з пам'яттю і без пам'яті, що працюють у k-значному структурному алфавіті.

При конкретних принципах зображення інформації та при обліку особливостей фізичної реалізації багатозначних елементів можуть виникати додаткові можливості для спрощення багатозначних комбінаційних схем [3, 6].

III. Порівняльний аналіз одиничних кодів

У роботах [7, 8] зроблено аналіз і класифікацію двох різновидів одиничного коду.

При порівняльному аналізі з іншими способами двійкового кодування було враховано такі кодові ознаки, як лінійність, циклічність, надлишковість,

подільність, систематичність, еквівалентність, рівномірність та рівнозваженість.

Розглянуті одиничні коди за наведеними базовими ознаками класифікаційної схеми можна подати як у таблиці 1.

TABLE I. ПОРІВНЯЛЬНИЙ АНАЛІЗ ОДИНИЧНИХ КОДІВ

Характеристики	Одиничний позиційний код	Одиничний нормальний код
Блокова довжиа n	Всі позиції інформаційні	Всі позиції інформаційні
Вага w слова	$w(C_i) = 1$, $w(C_i) = const$	$w(C_i) \neq const$; $w(C_1) = 1$, $w(C_2) = 2, \dots, w(C_n) = n$
Кодова попарна відстань d	d = 2; d = const	$d_{min}=1$
Кількість m слів коду	m = n	m = n
Перевірочна матриця	Відсутня. Код нелінійний	Відсутня. Код нелінійний
Контролездатність (теоретична)	Виявляє одиночні помилки	Не виявляє навіть одиночні помилки
Контролездатність (за модифікованою перевірочною матрицею)	Тільки виявляє помилки (від одиночної до u помилок)	Виявляє і виправляє помилки за умови, що це випадання внутрішніх одиниць у словах коду
Циклічна перестановка	Виконується	Не виконується
Еквідістантність	Існує (d = 2)	Не існує (d = 1)
Надлишковість	Існує $K_{над} = const$	Існує $K_{над} \neq const$
Подільність	Не існує	Не існує
Систематичність	Не існує	Не існує
Рівномірність	Існує (n = 10)	Існує (n = 10)
Рівнозваженість	Існує	Існує

При цьому було використано такі характеристики кодів з алгебраїчної теорії кодування, як матриця кодування, блокова довжина, перевірочна матриця, синдром, кодова попарна відстань, вага слова, суміжний клас і лідер [7,8], що дозволяють не тільки класифікувати, але й визначити його завадостійкість та контролездатність [9, 10].

Проведений аналіз одиничних кодів показав також, що вони представляють собою нелінійні коди, але для них існує можливість складання відповідних модифікованих перевірочних матриць. Отже, надлишковість розрядів в обох одиничних кодах у порівнянні з двійково-десятковим кодом приводить до підвищення рівня реальної контролездатності у порівнянні з теоретичною. Крім того, ці коди мають просте синхронне декодування (за аналогією з кодами Хеммінга) [7, 8].

IV. ВИСНОВКИ

1. Необхідно відзначити, що одиничні коди є специфічними кодами і їх використання не зможе замінити такі універсальні коди, як двійковий і десятковий.

2. Така унікальна властивість одиничних кодів, як просторове розподілення при зображенні числової інформації, значно поширює область їх застосування за рахунок можливості ефективної реалізації асоціативної обробки числової інформації, наприклад, масових інформаційно-логічних операцій (пошук максимуму, мінімуму, пошук у заданому інтервалі, пошук найближчого числа та інші).

3. Базові логічно-часові операції (порівняння і зсув) дозволяють ефективно виконувати у асоціативному процесорі на масиві лічильників таку складну операцію, як сортування масиву чисел.

4. Таким чином, відомі властивості одиничних кодів мають свою сферу застосування, що не обмежується арифметично-логічною обробкою числової інформації, де ці коди не конкурують із двійковим і десятковим кодуванням.

ЛІТЕРАТУРА REFERENCES

[1] Николайчук Я. М. Теорія джерел інформації / Я. М.Николайчук. – Тернопіль: ТзОВ «Терно-граф», 2010. – 536 с. – ISBN 978-966-654-233-8.

[2] Мартинюк Т. Б. Особливості логіко-часового зображення числової інформації / Т. Б. Мартинюк, О. М. Тарасова, М. М. Аль-Хіярі // Вісник Вінницького політехнічного інституту. – 2000. – №1. – С. 72-76. – ISSN 1997-9266.

[3] Кожемяко В. П. Оптоэлектронная схемотехника: Учебное пособие / В. П. Кожемяко, О. Г. Натрошвили, Т. Б. Мартынюк, Л.Ш.Имнаишвили. - К.: УМК ВО, 1988.- 276 с.

[4] Kozhemiako V., Martyniuk T., Kozhemiako O. “Vector-matrix conversions for parallel information processing in logic-time base”. In Selected Papers from the International Conference on Optoelectronic Information Technologies. Proceedings of SPIE, Vol. 4425 (2001). pp. 106-108.

[5] Мартынюк Т. Б. Организация ассоциативного процессора с поразрядно-последовательной обработкой информации / Т.Б.Мартынюк // Электронное моделирование. – 1996. – Т. 18, №13. – С. 28-31.

[6] Мартинюк Т. Б. Функційна повнота логічно-часового принципу зображення інформації / Т. Б. Мартинюк, М. М. Аль-Хіярі, С.А.Василецький // Вісник Вінницького політехнічного інституту. – 2000. №2. – С. 48-52. – ISSN 1997-9266.

[7] Мартинюк Т. Б. Аналіз можливостей одиничного кодування числової інформації / Т. Б. Мартинюк, Мохамед Салем Нассер, В.В.Власійчук, О.М.Наконечний // Оптико-електронні інформаційно-енергетичні технології. – 2006. - №2(10). – С. 39-44. – ISSN 1681-7893.

[8] Кожем’яко В. П. Класифікація одиничних кодів / В. П. Кожем’яко, Т.Б. Мартинюк, В. В. Дмитрук, В.В.Власійчук // Оптико-електронні інформаційно-енергетичні технології. – 2006. - №1(11). – С. 36-42. – ISSN 1681-7893.

[9] Дадаев Ю. Г. Теория арифметических кодов / Ю. Г.Дадаев.– М.: Радио и связь, 1981.– 272 с.

[10] Берлекэмп Э. Алгебраическая теория кодирования: пер. с анг. / Э.Берлекэмп.– М.: Мир, 1971.– 480 с.

Швидке декодування паралельних кодів CRC

Василь Семеренко, Богдан Григорчук
кафедра обчислювальної техніки,
Вінницький національний технічний університет
Вінниця, Україна
vpsemerenko@ukr.net

Fast decoding of parallel CRC codes

Vasyl Semerenko, Bogdan Grygorchuk
Department of Computer Technique
Vinnytsia National Technical University
Vinnytsia, Ukraine,
vpsemerenko@ukr.net

Анотація—Запропоновано новий спосіб швидкого декодування кодів CRC (Cyclic Redundancy Code) в каналах з паралельним надходженням вхідних даних. Використання теорії паралельних ЛПС (лінійних послідовнісних схем) та математичного представлення симетрії часу дозволяє вдвічі прискорити CRC-контроль. Такий спосіб контролю може бути використано в системах зберігання та архівації даних.

Abstract—A new method for fast decoding of CRC (Cyclic Redundancy Code) in channels with parallel input data is proposed. The use of the theory of linear finite state machine (LFSM) and the mathematical representation of time symmetry makes it possible to double the speed of the check with the help of CRC. This check method can be used in data storage and archiving systems.

Ключові слова—коди CRC; контрольна сума; паралельні обчислення; лінійна послідовнісна схема; декодування

Keywords—CRC codes; checksum; parallel processing; linear finite state machine; decoding

I. Вступ

Виявлення помилок за допомогою контролю CRC найчастіше використовується в різноманітних системах передачі даних, зокрема в обчислювальних мережах стандарту Ethernet [1]. CRC також є ефективним для забезпечення цілісності даних, які зберігаються на різноманітних пристроях збереження даних, зокрема на магнітних дисках та дискових масивах.

В останні роки CRC стали успішно застосовувати і в ПЛІС для безперервного контролю цілісності даних в конфігураційній пам'яті [2]. Однак, цей метод апаратного контролю віднімає значну частину ресурсів ПЛІС. Наприклад, в сімействі ПЛІС Cyclone зменшується максимальна частота на 9%, збільшується використання провідників на 21% та збільшується час трасування на 9%. Тому актуальною є задача зменшення використання ресурсів обчислювальних пристроїв, зокрема часу, при збереженні засобів контролю даних.

II. Теоретичний базис паралельних кодів CRC

CRC має дві розшифровки його абревіатури і, відповідно, дві інтерпретації [3]. Найчастіше CRC розглядають як *Cyclic Redundancy Check* – циклічний надлишковий контроль, тобто контрольну суму. В цьому випадку CRC є ущільненим представленням заданої вхідної послідовності I довільної довжини (близький аналог в криптографії – хеш-функція). Зміна значення контрольної суми з великою ймовірністю свідчить про наявність помилок в послідовності I.

Інтерпретація CRC як *Cyclic Redundancy Code* – циклічного надлишкового коду, дозволяє перевіряти правильність даних за відомими правилами завадостійкого кодування.

В сучасних багатоканальних системах передачі даних реалізована паралельна передача даних: біти одного байту або слова (2, 4, 8 байт) поступають одночасно. Кожний байт або слово можна інтерпретувати як один ρ-бітовий символ (ρ=8,16,32,64), тоді для передачі w біт знадобиться m символів ($m = w/\rho$). Такий спосіб передавання даних називається символьно-паралельним [4].

Послідовність із m символів будемо розглядати як кодове слово коду CRC, яке формується кодером на стороні передавача та декодується декодером на стороні приймача. Передачу даних можна розглядати або як передачу по послідовному каналу символів, або як передачу бітів даних по ρ паралельним каналам. В першому випадку знадобляться математичні перетворення в недвійкових полях Галуа $GF(2^\rho)$, а в другому випадку – математичні перетворення в двійкових полях Галуа $GF(2)$.

В цій роботі розглядається лише другий випадок, більш простий для програмно-апаратної реалізації. Такий спосіб інтерпретації даних означатиме, що код CRC складається із ρ кодових

слів z_i ($i = 1 \dots \rho$), об'єднаних в кодову матрицю:

$$Z_{(\rho)} = \begin{bmatrix} z_1 \\ z_2 \\ \dots \\ z_\rho \end{bmatrix} = \begin{bmatrix} z_{11} & z_{12} & \dots & z_{1n} \\ z_{21} & z_{22} & \dots & z_{2n} \\ \dots & \dots & \dots & \dots \\ z_{\rho 1} & z_{\rho 2} & \dots & z_{\rho n} \end{bmatrix}, GF(2). \quad (1)$$

Коди CPC є різновидом циклічних кодів, тому для їх опису часто використовують традиційні способи представлення циклічних кодів (матричне, поліноміальне, алгебраїчне). Найчастіше циклічний код задається породжувальним поліномом:

$$g(x) = g_0 + g_1 x + \dots + g_{r-1} x^{r-1} + x^r, \quad GF(2) \quad (2)$$

З позицій теорії циклічного кодування коди CPC належать або до циклічних кодів Хемінга, або до кодів Абрамсона [3]. Будемо використовувати коди Хемінга, які мають найбільшу довжину. Таким чином, породжувальний поліном (2) має задовольняти двом вимогам:

– поліном має бути примітивним;

– степінь поліному має бути $r \geq log_2 m$.

Для опису паралельних кодів найбільш придатним математичним апаратом є теорія лінійних послідовнісних схем (ЛПС) [5].

Традиційна ЛПС з одним входом і одним виходом є кінцевим автоматом лінійного типу (лінійним автоматом), який над полем Галуа $GF(2)$ описується функцією станів (переходів)

$$S(t+1) = A \times S(t) + B \times U(t), \quad GF(2) \quad (3)$$

і функцією виходів

$$Y(t) = C \times S(t) + D \times U(t), \quad GF(2),$$

де t – дискретний час; A, B, C, D – характеристичні матриці ЛПС; $S(t)$ – слово стану; $U(t)$ – вхідне слово; $Y(t)$ – вихідне слово.

В подальшому виходами ЛПС будемо вважати значення її відповідних станів, тому для такої ЛПС достатньо використати лише функцію станів (переходів) ЛПС (3). Апаратною реалізацією такої ЛПС є звичайний регістр зсуву з лінійними оберненими зв'язками.

Розрізняють два типи паралельних кодів CRC: складені та інтегровані [6]. В подальшому будемо говорити лише про інтегровані коди CRC.

Вхідні дані паралельного коду CRC поступають по паралельних каналах, тому необхідно використати багатовходову ЛПС. Для опису структури входів ЛПС використовується характеристична матриця B, тому у випадку ρ-входової ($\rho = 1 \div r$) паралельної ЛПС над двійковим полем Галуа має бути така одинична ($r \times r$)-матриця B:

$$B_{(\rho)} = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Матриця A визначає внутрішню структуру ЛПС. Багатовходова ЛПС має таку ж внутрішню структуру, що і традиційна одновходова ЛПС, тому матриця A залишиться без змін. Серед різних типів ЛПС найбільш поширеною є рекурсивна ЛПС типу 1 з матрицею

$$A = \begin{bmatrix} 0 & 0 & 0 & \dots & g_0 \\ 1 & 0 & 0 & \dots & g_1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 1 & \dots & g_{r-2} \\ 0 & 0 & 0 & 1 & g_{r-1} \end{bmatrix}. \quad (4)$$

Елементи останнього стовпця матриці A із (4) представляють собою коефіцієнти породжувального поліному (2).

Таким чином, теоретичною основою паралельних кодів CRC при декодуванні кодової матриці (1) може бути паралельна ЛПС, функціонування якої описується функцією станів (переходів)

$$S(t+1) = A \times S(t) + B_{(\rho)} \times Z_{(\rho)}(t), \quad GF(2) \quad (5)$$

III. Декодування паралельного коду CRC

Традиційний спосіб перевірки даних полягає у формування для них контрольної суми Σ_f, наприклад, CRC-суми і порівнянні її з наперед обчисленої (еталонною) контрольною сумою Σ_v: їх рівність вважається доказом відсутності спотворень у даних. Контрольні суми, як правило, обчислюються послідовно, що потребує багато часу. Якщо дані поступають також послідовно, тоді затримка з обчисленням суми Σ_f буде практично відсутньою. Якщо ж дані можна отримати швидше, наприклад, використовуючи додаткові канали зв'язку, тоді бажано обчислити швидше і контрольні дані.

Будемо вважати, що дані поступають посимвольно, тобто всі можливості по прискоренню обчислень за рахунок використання паралельної обробки даних вже використані. Окрім традиційного каналу зв'язку, по якому дані передаються від початку набору даних, є також можливість зчитувати дані з кінця набору даних. В результаті дані будуть передані вдвічі швидше. Чи можна в даному випадку прискорити вдвічі процес обчислення контрольної суми Σ_f ?

Рекурсивне обчислення CRC-суми (як і CRC-коду) здійснюється згідно формули (5), тобто в

порядку надходження t-го вектора $Z_{(\rho)}(t)$. Іншими словами, рекурсивні обчислення традиційно здійснюються при зміні часу від "теперішнього" в "майбутнє".

Відомо, що фундаментальні закони класичної та квантової динаміки обернені в часі, з чого випливає математична еквівалентність "минулого" і "майбутнього" [7]. Для динамічних систем з одним ступенем свободи, прикладом яких може служити ЛПС, рекурсивні обчислення можуть здійснюватись також і при зміні часу від "теперішнього" в "минуле".

Таким чином, якщо дані можна одночасно передавати в двох напрямках: від початку набору даних (файлу) та з кінця набору даних (файлу), тоді можна одночасно використати дві ЛПС для обчислення CRC-суми. Перша ЛПС з матрицею A (назвемо її прямою) визначає перехід із початкового нульового стану $S(0)$ в наступні такти часу $t > 0$ згідно формули (5). Друга ЛПС з матрицею A_{inv} (назвемо її оберненою) визначає перехід із кінцевого стану $S(n)$ в попередні такти часу $t < n$ згідно формули:

$$S(t) = A_{inv} \times (S(t+1) + B_{(\rho)} \times Z_{(\rho)}(t)), \quad GF(2).$$

Правила переходу між матрицями A і A_{inv} наведено в [6].

В такт часу $t = n/2$ пряма ЛПС перейде в стан $S_f(n/2)$. В цей же такт часу обернена ЛПС перейде в стан $S_v(n/2)$. При відсутності помилок в наборі даних (файлі) зазначені стани мають бути однаковими:

$$S_f(n/2) = S_v(n/2) \quad \text{при непарному } n,$$
$$S_f(n/2) = S_v(n+1/2) \quad \text{при парному } n.$$

Відзначимо, що тут проявляється невелика відмінність між двома інтерпретаціями CRC. Якщо розглядати CRC як контрольну суму, тоді кінцевий стан $S(n)$ і є еталонною CRC-сумою, як правило, ненульовою.

Якщо ж розглядати CRC як циклічний код, тоді довжина послідовності I дорівнює $(m+r)$, а кінцевий стан $S(n)$ є синдромом помилки коду (обов'язково нульовим, оскільки помилок перед початком передачі даних ще немає). В цьому випадку роль CRC відіграє ненульове r-розрядне контрольне слово коду.

Отже, при наявності одночасного доступу до початку та кінця масиву даних, який контролюється, перевірка коректності даних буде виконана вдвічі швидше. Це правило є справедливим не тільки при бітовій передачі даних [8], але також і при символьній передачі даних.

IV. Висновки

Основним методом прискорення обчислень є використання паралельної обробки даних. При використанні контролю даних на основі CRC ефективним є паралелізм по протилежним осям часу. В роботі показано як можна вдвічі прискорити обчислення CRC лише на основі тих даних, що вже використовуються в системах передачі даних. Якщо будуть відомі еталонні проміжні контрольні суми, тоді можна ще в декілька разів прискорити обчислення CRC.

Такий спосіб контролю може бути використано в системах зберігання та архівації даних при умові одночасного доступу до початку та кінця масиву даних.

Література References

[1]. В. Столлингс, Компьютерные системы передачи даннях. Изд. 6-е, пер. с англ., М., Издательский дом «Вильямс», 928 с., 2002.

[2]. Д. Иоффе, "Обнаружение и исправление ошибок с использованием CRC в устройствах FPGA фирмы Altera," *Компоненты и технологии*, no. 8, 2006.

[3]. В. П. Семеренко, "Теория и практика CRC кодов: новые результаты на основе автоматных моделей," *Східно-Європейський журнал передових технологій*, том. 4, випуск 9 (76), с. 38–48, 2015.

[4]. V.P. Semerenko, "The Theory of Parallel CRC Codes Based on Automaton Models," *Eastern-European Journal of Enterprise Technologies*, vol. 6, issue 9 (84), pp. 45–55, 2016.

[5]. А. Гилл, *Линейные последовательностные машины*. Пер. с англ., М., Наука, 288 с., 1974.

[6]. В. П. Семеренко, *Теорія циклічних кодів на основі автоматних моделей*. Монографія, Вінниця, ВНТУ, 444 с., 2015.

[7]. И. Пригожин, И. Стенгерс, *Время, хаос, квант*. Пер. с англ., М., издат. группа Прогресс, 272 с., 1994.

[8]. В. П. Семеренко, Б. О. Григорчук, "Швидке декодування кодів CRC на основі симетрії часу," Науково-технічна конференція Вінницького національного технічного університету (ВНТУ), 15-16 березеня 2017, Вінниця, 2017.

СЕКЦІЯ 2.
Методи та засоби захисту інформації

Numeral Systems with Irrational Bases for Mission-Critical Applications. The Basic Concepts and Scientific Results

Oleksiy Stakhov
Computer Firm FibTech (Fibonacci Technology), Ontario, Canada
goldenmuseum@rogers.com

Системи числення з ірраціональними основами для критично важливих застосувань. Головні концепції та наукові результати

Олексій Стахов
Компютерна фірма FibTech (Fibonacci Technology), Онтаріо, Канада
goldenmuseum@rogers.com

Abstract— This speech is of an overview nature. Its main goal is to substantiate the basic concepts and scientific results of a new direction in the theory of coding-the numeral system with irrational bases, and their application in mission-critical systems. This scientific direction began to develop in the Taganrog Radiotechnical Institute after the defense of the doctoral dissertation of the author of this speech (1972), and then successfully continued to develop in the Vinnytsya Polytechnic Institute at the Department of Computer Technology. Nowadays this scientific direction is developing in Canada (computer firm FibTech (Fibonacci Technology)) and at Sumy University.

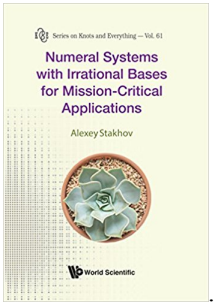
Анотація—Ця доповідь має оглядовий характер. Її основна мета – обгрунтувати головні концепції та наукові результати нового напрямку в теорії кодування – системи числення з ірраціональними основами, та їх застосування в критично-важливих системах. Цей науковий напрямок почав розвиаатися в Таганрогському радіотехнічному інституті після захисту докторської дисертації автора цієї доповіді (1972), потім успішно продовжив розвиватися в Вінницькому політехнічному інституті на кафедрі обчислювальної техніки. Зараз цей науковий напрямок розвивається в Канаді (компьютерна фірма FibTech (Fibonacci Technology) та в Сумському університеті.

Keywords*—mission-**critical systems; Bergman's system; Fibonacci p-codes; codes of the golden p-proportions, ternary mirror-symmetrical arithmetc.***

Ключові слова—критично-важливі системи; система Бергмана; р-коди Фібоначчі; коди золотої р-пропорції, трійкова зеркально-симетрична арифметика

INTRODUCTION

In 2017 the International Publishing House "World Scientific" has published new book of the author "Numeral Systems with Irrational Bases for Mission-Critical Applications".



Advertising information on the book is posted at the site of "World Scientific" (http://www.worldscientific.com/worldscibooks/10.1142/10671) and the site of Amazon.com (https://www.amazon.com/Numeral-Irrational-Mission-Critical-Applications-Everything/dp/981322861X)

Abstract of the book

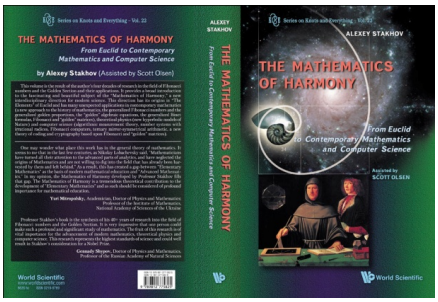
This volume is the result of the author's many-years of research in this field. These results were presented in the author's two books, Introduction to the Algorithmic Measurement Theory(Moscow, Soviet Radio, 1977), and Codes of the Golden Proportion (Moscow, Radio and Communications, 1984), which had not been translated into English and are therefore not known to English-speaking audience. This volume

sets forth new informational and arithmetical fundamentals of computer and measurement systems based on Fibonacci p-codes and codes of the golden p-proportions, and also on Bergman's system and "golden" ternary mirror-symmetrical arithmetic. The book presents some new historical hypotheses concerning the origin of the Egyptian calendar and the Babylonian numeral system with base 60 (dodecahedral hypothesis), as well as about the origin of the Mayan's calendar and their numeral system with base 20 (icosahedral hypothesis). The book is intended for the college and university level. The book will also be of interest to all researchers, who use the golden ratio and Fibonacci numbers in their subject areas, and to all readers who are interested to the history of mathematics. Readership: Researchers in mathematics and computer science.

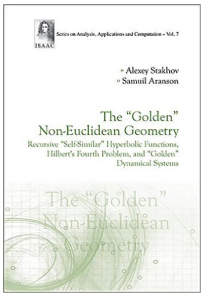
The main goal of this speech is to substantiate the basic concepts and scientific results of a new direction in the coding theory - the numeral system with irrational bases, and their application in mission-critical systems.

In addition to this book, the Publishing House "World Scientific" published two fundamental author's books:

1. Alexey Stakhov. Assisted by Scott Olsen. "The Mathematics of Harmony. From Euclid to Contemporary Mathematics and Computer Science", World Scientific, 2009
http://www.worldscientific.com/worldscibooks/10.1142/6635



2. Alexey Stakhov, Samuil Aranson. Assisted by Scott Olsen. The "Golden" Non-Euclidean Geometry: Hilbert's Fourth Problem, "Golden" Dynamical Systems, and the Fine-Structure Constant, World Scientific, 2016.
http://www.worldscientific.com/worldscibooks/10.1142/9603



All these three books are author's contribution to the development not only of world science, but also of Ukrainian science, in particular, of Ukrainian mathematics, computer science and digital metrology.

The author dedicates the last book "Numeral Systems with Irrational Bases for Mission-Critical Applications" to the 45th anniversary of the Computer Technology Department, Vinnytsia National Technical University.

BASIC CONCEPTS AND THE MAIN SCIENTIFIC RESULTS:

1. Mission-critical applications. At the present time the computer science and digital metrology are passing to new stage of their development, to the stage of designing computing and measuring systems for **mission-critical applications.** In the Wikipedia article "Mission critical" we read:

*"**Mission critical** refers to any factor of a system (components, equipment, Personnel, process, procedure, software, etc.) that is essential to business operation or to an organization. Failure or disruption of **mission critical** factors will result in serious impact on business operations or upon an organization, and even can cause social turmoil and catastrophes. Therefore, it is extremely critical to the organization's "mission" (to avoid Mission Critical Failures).*

***Mission critical system** is a system whose failure may result in the failure of some goal-directed activity. Mission essential equipment and mission critical application are also known as mission-critical system. Examples of mission critical systems are: an online banking system, railway / aircraft operating and control systems, electric power systems, and many other computer systems that will adversely affect business and society seriously if downed. A good example of a mission critical system is a navigational system for a spacecraft."*

This puts forward new requirements for ensuring informational reliability of such systems. The most important requirement is to prevent the occurrence of "false signals" at the output of the mission-critical systems that can lead to technological disasters.

2. "**Philosophy" of error detection for the error-correcting codes (ECC)**. Modern methods of providing informational reliability of mission-critical systems (in particular, the use of error-correcting codes) do not always provide the required informational reliability of the mission-critical systems. In particular, the theory of ECC mainly is focused on the detection and correction of the errors of low multiplicity (for example, single-bit and double-bit errors) as the most probable. *With regard to the errors of high multiplicity, the theory of ECC simply ignores them because of their low probability; this follows from the model of "symmetrical channel".* Such "philosophy" of error detection is absolutely unacceptable for the case of the mission-critical systems, because these undetectable errors can be the source of "false signals" at the output of mission-

critical systems what can lead to enormous social and technological disasters.

3. Paradox of Hamming code. The main paradox of Hamming code and its analogs (for example, Hsiao code) consists of the fact that the Hamming and Hsiao codes perceive many-bit errors of the odd multiplicity (3,5,7,9,…) as single-bit errors, and for these cases they begin "false correction" by adding new errors to the erroneous code word. That is, for this case the Hamming and Hsiao codes are turned out into **anti-ECC**, because they are "ruining" the Hamming and Hsiao code words. This "paradoxical" property of the Hamming and Hsiao codes is well known to experts in the field of ECC, but many consumers do not always know about this. For such cases, the main arguments for customers consist in the fact that the errors of large multiplicity are unlikely, but *such arguments are unacceptable for mission-critical applications.*

4. Row hammer effect is a new phenomenon in the field of electronic memory. The main reason of this phenomenon is microminiaturization of electronic memory, which leads to mutual electrical interaction between nearby memory rows. This interaction is altering the contents of nearby memory rows that were not addressed in the original memory access. No effective methods of fighting against *row hammer effect* have been proposed until now. Possibly, the only reasonable proposal is to introduce restrictions on microminiaturization of electronic memory. But then the question arises how we have to design nano-electronic memory?

5. "Trojan horse" of the binary system. The prominent American scientist, physicist and mathematician John von Neumann (1903–1957), together with his colleagues from the Prinstone Institute Goldstein and Berks after careful analysis of the strengths and weaknesses of the first electronic computer ENIAC gave *strong preference to the binary system as a universal way of coding of data in electronic computers*. However, this proposal contains in itself a great danger for the case of mission-critical systems. The classical binary code has zero code redundancy what excludes a possibility detecting any errors in computer structures. This danger was called "Trojan horse" of binary system by the Russian academician Yaroslav Khetagurov. Because of the "Trojan Horse" phenomenon, humanity becomes a hostage to the binary system for the case of mission-critical applications. *From here, it follows the conclusion that the binary system is unacceptable for designing computational and measuring systems for mission-critical applications.*

5. Bergman's system, introduced in 1957 by the American 12-year-old wunderkind George Bergman, is an unprecedented case in the history of mathematics. The mathematical discovery of the young American mathematician returns mathematics to the Babylonian positional numeral system, that is, to the initial period in the development of mathematics, when the numeral systems and rules of performing basic arithmetic operations stood at the center of mathematics. But the most important is the fact that the famous irrational number $\Phi = \frac{1+\sqrt{5}}{2}$ (the *golden ratio*) is the base of *Bergman's system* what puts forward the irrational numbers on the first position among the numbers. *It can be argued that the Bergman's system is the greatest modern mathematical discovery in the field of numeral systems, which changes our ideas about numeral systems and alters both the number theory and computer science.*

6.The "golden" number theory and new properties of natural numbers is the first important consequence, following from Bergman's system. For many mathematicians in the field of number theory, it is a great surprise that new properties of natural numbers (*Z*-property, *D*-property, *F*-code, *L*-code) were discovered in the 21st century, that is, 2.5 millennia after the writing of Euclid's *Elements*, in which systematic studying the properties of natural numbers started. *Bergman's system* is the source for the *"golden" number theory* what once again emphasizes a fundamental nature of the mathematical discovery of George Bergman.

7. Ternary mirror-symmetrical numeral system and new ternary mirror-symmetrical arithmetic are the main applied scientific results, following from *Bergman's system*. These results alter our ideas about ternary numeral system. The *property of mirror symmetry* is the main checking property, which allows detecting errors in all arithmetical operations.

8. Fibonacci *p*-codes and Fibonacci arithmetic based on the basic micro-operations. The new computer arithmetic consists in the sequential execution of the so-called "basic micro-operations." The errors are detected by built-in error-detection device simultaneously with the execution of the micro-operations in the moment of errors occurrence what ensures the high information reliability of the arithmetic device for mission-critical applications.

9. Codes of the golden *p*-proportions, "golden" resistive divisors and self-correcting ADC and DAC. The codes of the golden *p*-proportions with the base Φ_p (the positive root of the algebraic equation $x^{p+1} - x^p - 1 = 0, p = 0.1, 2, 3, \ldots$) are a wide generalization of the *binary system* (p=0) and *Bergman's system* (p=1). The "golden" resistive divisors, based on the golden *p*-proportions Φ_p, have unique electrical properties, which allow to design self-correcting analog-to-digital and digital-to-analog converters. Metrological parameters of such ADCs and DACs remain unchanged in the process of temperature changing and elements aging, what is important for mission-critical applications.

10.The final concept. The above theory of numeral systems with irrational bases are a new direction in the field of coding theory, intended for increasing informational reliability and noise-immunity of specialized computing and measuring systems. This direction does not set itself the task of replacing the classical binary system in those cases where the use of the binary system does not threaten an appearance of

technological disasters and where informational reliability and noise immunity can be ensured by traditional methods. The main task of this direction is preventing or significantly reducing the probability of "false signals" at the output of information systems that can lead to social or technological disasters. This scientific direction is at the initial stage of its development and can lead to new technical solutions in the field of computer science and digital metrology.

11. **The main conclusion** of author's book **"Numeral Systems with Irrational Bases for Mission-Critical Applications**" is the fact that the mission-critical applications are that major area of computer science and digital metrology, where numeral systems with irrational bases (Fibonacci codes and codes of the golden proportion) get their natural applications and can realize all their basic advantages.

References

[1] Kharkevich, A.A. (1963) Fighting against noises. Moscow: State Publishing House of Physical and Mathematical Literature (Russian).

[2] Florence, Jessie MacWilliams, Sloane, Neil James Alexander. (1978) The Theory of Error-correcting Codes. North-Holland Publishing Company.

[3] Mission critical. From Wikipedia, the free encyclopedia https://en.wikipedia.org/wiki/Mission_critical

[4] Hamming code. From Wikipedia, the free encyclopedia https://en.wikipedia.org/wiki/Hamming_code

[5] Hsiao M.Y. (1970) A class of optimal minimum odd-weight-column SEC-DED codes. IBM J. Res. Develop. Vol. 14.

[6] Petrov K.A. Investigation of the characteristics of noise-immune codes used in submicron static RAMs (Russian) http://gigabaza.ru/doc/194118.html

[7] Row hammer. From Wikipedia, the free encyclopedia https://en.wikipedia.org/wiki/Row_hammer

[8] Bashmakova, J.G., Youshkevich, A.P. (1951) An origin of the numeral systems. Encyclopedia of Elementary Arithmetics. Book 1. Arithmetic. Moscow-Leningrad: Gostekhizdat (Russian).

[9] Von Neumann architecture. From Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/Von_Neumann_architecture

[10] Khetagurov J.A. (2009). Ensuring the national security of real-time systems. ВС / NW, №2 (15): 11.1 (Russian)
http://network-journal.mpei.ac.ru/cgi-bin/main.pl?l=ru&n=15&pa=11&ar=1

[11] Kautz, W. (1966) Error-correcting codes and their implementation in digital systems. In the book "Methods of introducing redundancy for computing systems" Transl. from English. Moscow: Soviet Radio (Russian).

[12] Tolstyakov, V.S. Nomokonov, V.N. Kartsovsky, M.G. and others. (1972) Detection and correction of errors in discrete devices. Edited by V.S. Tolstyakov. Moscow: Soviet Radio, (Russian).

[13] Bergman, George (1957). "A Number System with an Irrational Base". Mathematics Magazine. 31 (2). doi:10.2307/3029218. JSTOR 3029218, https://en.wikipedia.org/wiki/Golden_ratio_base

[14] Golden ratio base. From Wikipedia, the free encyclopaedia https://en.wikipedia.org/wiki/Golden_ratio_base

[15] Phi Number System. From WolframMathWorld http://mathworld.wolfram.com/PhiNumberSystem.html1957, No 31.

[16] Knuth, Donald E. (1997) The Art of Computer Programming. Volume 1. Fundamental Algorithms (Third edition). Massachusetts: Addison-Wesley.

[17] Stakhov, A.P. (2009) The Mathematics of Harmony. From Euclid to Contemporary Mathematics and Computer Science. Assisted by Scott Olsen. International Publisher "World Scientific" (New Jersey, London, Singapore, Beijing, Shanghai, Hong Kong, Taipei, Chennai).

[18] Stakhov, AP. (2002) Brousentsov's ternary principle, Bergman's number system and ternary mirror-symmetrical arithmetic. The Computer Journal Vol. 45, No. 2.

[19] Stakhov, A.P. (2015) The "Golden" Number Theory and New Properties of Natural Numbers. British Journal of Mathematics & Computer Science Vol.11, No 6.

[20] Stakhov, A.P. (2016) The importance of the Golden Number for Mathematics and Computer Science: Exploration of the Bergman's system and the Stakhov's Ternary Mirror-symmetrical System (Numeral Systems with Irrational Bases). British Journal of Mathematics & Computer Science Vol. 18, No 3.

[21] Pospelov, D.A. (1970) Arithmetic Foundations of Computers. Moscow: High School, (Russian).

[22] Polya, George. (1962), (1965) Mathematical Discovery. On understanding, learning and teaching problem solving. New York – London: Volume I; Volume II.

[23] Stakhov, AP. (1977) Introduction into algorithmic measurement theory. Moscow: Soviet Radio (Russian).

[24] Stakhov, A.P. (1984) Codes of the Golden Proportion. Moscow: Radio and Communication (Russian).

[25] Stakhov, Alexey. (1972) Synthesis of optimal algorithms for analog-to-digital conversion. Doctoral thesis, Kiev Institute of Civil Aviation Engineers (Russian)

[26] Vorobyov, N.N. (1961) Fibonacci Numbers. Moscow: Publishing house "Nauka," (Russian).

[27] Hoggatt, V.E. (1969) Fibonacci and Lucas Numbers. Palo Alto, CA: Houghton-Mifflin.

[28] Koshy, Thomas. (2017) Fibonacci and Lucas Numbers with Applications, 2-nd edition. John Wiley & Sons, Inc.

[29] Stakhov, A.P. (1974) Redundant binary positional numeral systems. In the book "Homogenous digital computer and integrated structures." Taganrog Radio University, No 2 (Russian).

[30] Stakhov, A.P. (1975) A use of natural redundancy of the Fibonacci number systems for computer systems control. Automation and Computer Systems, No 6 (Russian).

[31] Reduction method of p-Fibonacci code to the minimal form and device for its realization. Patent certificate of USA No 4187500.

[32] Device for reduction of p-Fibonacci codes to the minimal form. Patent certificate of USA No 4290051.

[33] Reduction method of p-Fibonacci code to the minimal form and device for its realization. Patent certificate of England No 1543302.

[34] Device for reduction of p-Fibonacci codes to the minimal form. Patent certificate of England No 2050011.

[35] Reduction method of p-Fibonacci code to the minimal form and device for its realization. Patent certificate of Germany No 2732008.

[36] Device for reduction of p-Fibonacci codes to the minimal form. Patent certificate of Germany No 2921053.

[37] Reduction method of p-Fibonacci code to the minimal form and device for its realization. Patent certificate of Japan No 1118407.

[38] Reduction method of p-Fibonacci code to the minimal form and device for its realization. Patent certificates of France No 7722036, No 2359460.

[39] Device for reduction of p-Fibonacci codes to the minimal form. Patent certificates of France No 7917216, No 2460367.

[40] Reduction method of p-Fibonacci code to the minimal form and device for its realization. Patent certificate of Canada No 1134510.

[41] Device for reduction of p-Fibonacci codes to the minimal form. Patent certificate of Canada N1132263.

[42] Reduction method of p-Fibonacci code to the minimal form and device for its realization. Patent certificate of Poland No 108086.

[43] Reduction method of p-Fibonacci code to the minimal form and device for its realization. Patent certificate of DDR No 150514.

[44] Stakhov, A.P. (2016) Fibonacci p-codes and Codes of the Golden p-proportions: New Informational and Arithmetical Foundations of Computer Science and Digital Metrology for Mission-Critical Applications. British Journal of Mathematics & Computer Science Vol.17, No 1.

[45] Luzhetsky, V.A., Stakhov, A.P., Wachowski, V.G. (1989) Noise-immune Fibonacci computers. The brochure "Noise-immune codes. Fibonacci Computer." Moscow: Knowledge. A series "New life, science and technology" (Russian).

[46] Ancient Egyptian mathematics. From Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/Ancient_Egyptian_mathematics#Multiplication_and_division

[47] Stakhov, A.P. (1978) Fibonacci and "Golden" Ratio Codes. In the book "Fault-tolerant Systems and Diagnostic FTSD-78," Gdansk.

[48] Stakhov, A.P. (1980) The golden mean in the digital technology. Automation and Computer Systems No 1 (Russian).

[49] Stakhov, A.P. (1984) Codes of the Golden Proportion. Moscow: Radio and Communication (Russian).

[50] Stakhov, A.P. (1978) Digital Metrology on the basis of the Fibonacci codes and Golden Proportion Codes. In the book "Contemporary Problems of Metrology." Moscow Machine-building Institute (Russian).

[51] Stakhov, A.P., Azarov, A.D. Moiseev. V.I., Martsenyuk, V.P., Stejskal, V.Y. (1986) The 17-bit Self-correcting ADC. Devices and Control Systems, №1.

[52] Stakhov, A.P., Azarov, A.D. Moiseev. V.I., Stejskal, V.Y. (1989) Analog-to-digital Converters on the Basis of Redundant Numeral Systems. The brochure "Noise-immune codes. Fibonacci Computer." Moscow: Knowledge. A series "New life, science and technology" (Russian).

[53] Licomendes, P. and Newcomb, R. (1984) Multilevel Fibonacci Conversion and Addition, The Fibonacci Quarterly, Vol. 22, No 3.

[54] Ligomenides, P. and Newcomb, R. (1981) Equivalence of some Binary, Ternary, and Quaternary Fibonacci Computers. Proceeding of the Eleventh International Symposium on Multiple-Valued Logic, Norman, Oklahoma.

[55] Ligomenides, P. and Newcomb, R. (1981) Complement Representations in the Fibonacci Computer. Proceedings of the Fifth Symposium ob Computer Arithmetic, Ann Arbor, Michigan.

[56] Newcomb, R. (1974) Fibonacci Numbers as a Computer Base. Conference Proceedings of the Second Inter-American Conference on Systems and Informatics, Mexico City.

[57] Hoang, V.D. (1979) A Class of Arithmetic Burst-Error-Correcting Codes for the Fibonacci Computer. PhD thesis, University Maryland.

Acknowledgements

This book is a result of author's research in the field of the Golden Section, Fibonacci numbers and their applications in computer science and digital metrology during an approximately 50 year period. The author has met many remarkable people who had evaluated and supported author's scientific direction. About 50 years ago the author had read the remarkable brochure *Fibonacci Numbers* written by the famous Soviet mathematician **Nikolay Vorobyov**. This brochure was the first mathematical work on Fibonacci numbers published in the second half of the 20th century. This brochure determined author's scientific interests in Fibonacci numbers. In 1974 the author met with Professor Vorobyov in Leningrad (now St. Petersburg) and discussed with him author's scientific achievements in this area. He gave the author as a keepsake his brochure *Fibonacci Numbers* with the following inscription: *"To highly respected Alexey Stakhov with Fibonacci's greetings."*

The author's expresses great thanks to his teacher, the outstanding Ukrainian scientist, Professor **Alexander Volkov**; under his scientific leadership the author defended PhD dissertation (1966) and then DrSci dissertation (1972). These dissertations were the first step in author's research, which led the author to the conceptions of Mathematics of Harmony and Fibonacci computers, based on the Golden Section and Fibonacci numbers,.

During stormy scientific life, the author met many fine people, who could understand and evaluated author's enthusiasm and appreciate his scientific direction. With deep gratitude, the author recollects a meeting with the famous Austrian mathematician **Alexander Ajgner** in the Austrian city Graz in 1976. The meeting with Professor Aigner was the beginning of the international recognition of author's scientific direction. Another remarkable person, who had a great influence on author's research was the Ukrainian mathematician academician **Yury Mitropolsky**. His influence on author's research, pertinent to the history of mathematics and other topics, such as the application of "Harmony Mathematics" in contemporary mathematics, computer science and mathematical education, is inestimable contribution. Thanks to the support of Yury Mitropolski, the author had published many important articles in various Ukrainian academic journals.

Author's arrival to Canada in 2004 became the beginning of new stage in author's scientific research. Within 13 years, the author has published 50 fundamental articles in different international English-language journals. The publication of 3 fundamental books *The Mathematics of Harmony* (World Scientific, 2009) and *The "Golden" Non-Euclidean Geometry* (World Scientific, 2016) and *Numeral Systems with Irrational Bases for Mission-Critical Applications* (World Scientific, 2017) is the main author's scientific achievements of the Canadian period of author's scientific creativity. These books were published thanks to the support of the famous American mathematician Prof. **Louis Kauffman**, editor of the Series on Knots and Everything (World Scientific) and Prof. **M.S. Wong**, the famous Canadian mathematician (York University) and editor of the Series on Analysis, Application and Computation. The present book has been published by the initiative of Prof. **Louis Kauffman.** A huge help in editing of the above first two author's books was rendered by the American philosopher Prof. **Scott Olsen**, one of the leading American experts in the field of the golden section. The author expresses deep gratitude to these scientists for supporting the publications of the mentioned above author's books.

Lastly, this book would never have been written without self-denying support of my wife Antonina, who always created the perfect conditions for scientific work in any countries, where the author worked. She had been sailing together with the author for more than 50 years on the "Golden" journey to different countries and continents (Europe, Africa (Libya and Mozambique), America (Canada)). In addition, the author would like to express his special thanks to his daughter Anna Sluchenkova for her critical remarks, and her invaluable help in the English translation and editing of the book, and, especially, for her work in preparing illustrations, and coordination and final preparation of camera-ready manuscript. Without her support this book was never been published.

OLEKSIY STAKHOV.

Синтез и анализ Уолша-подобных систем секвентных функций

Анатолий Белецкий
кафедра электроники
Национальный авиационный университет,
Киев, Украина,
abelnau@ukr.net

Synthesis of Walsh-like systems of sequential functions

Beletsky A. Ya.
Department of Electronics
National Aviation University,
Kiev, Ukraine,
abelnau@ukr.net

I. Введение

Теория и техника спектрального анализа сигналов ориентирована в основном на сигналы синусоидальных функций. Наряду с ними широкое применение в различных приложениях находят функции (волны) несинусоидальных форм. Типичным примером несинусоидальных волн являются функции Уолша [1], отличительная особенность которых состоит в том, что в пространстве оригиналов на двоично степенном интервале определения от 0 до $N = 2^n$, где n – натуральное число, функции Уолша принимают кусочно-постоянные значения $+1$ или -1, заменой которых соответственно числами 0 и 1 переводят системы в пространство изображений.

Спектральный анализ дискретных сигналов в большинстве случаев строится на основе базисов *дискретных экспоненциальных функций*, образуемых временной дискретизацией комплексно-значных гармонических сигналов. Известно, что к базисам быстрого преобразования Фурье (БПФ), предъявляются ряд требований, важнейшие из которых состоят в том, что, во-первых, формы базисных функций преобразования должны быть максимально близкими к формам анализируемых сигналов.

И, во-вторых, базисы должны поддерживать такое быстродействие процессоров БПФ, которое обеспечивает обработку сигналов в реальном времени.

Таким образом, выбор систем базисных функций определяется требованиями удобства вычислений и, в конечном счёте, трудоёмкостью алгоритмов реализации искомого преобразования. Исходя из этих соображений, применение вещественных базисов систем функций Уолша и их расширения — *Уолша-подобных систем секвентных функций*, представляется актуальным и перспективным для цифровой (спектральной) обработки сигналов.

II. Постановка задачи исследования

Данная работа посвящена построению в пространстве изображений систем дискретных Уолша-подобных (0,1)-секвентных функций (базисов), в которых число нулей и единиц в каждой половине интервала определения совсем не обязательно является одинаковым, как это имеет место в классических системах функций Уолша (за исключением функции, левая половина которой заполнена исключительно нулями, а правая — единицами). Обсуждаются области применения систем секвентных функций.

III. Изложение основного материала

Сформируем полное множество $\mathbf{\Omega}$ секвентных функций $\boldsymbol{s}_i \in \mathbf{\Omega}$ восьмого порядка, выбранного в качестве примера, включая в состав $\mathbf{\Omega}$ нулевую секвенту $\boldsymbol{s}_0$ и все те секвенты (байты), которые начинаются с нуля, а в оставшихся младших семи разрядах размещаются четыре единицы и три нуля. Количество ненулевых секвент восьмого порядка равно 35, так как определяется числом сочетаний из 7 по 3 и, следовательно, полный набор элементов $\mathbf{\Omega}$, включая нулевой, содержит 36 секвент $\boldsymbol{s}_i$, $i = \overline{0, 35}$, (табл. 1).

Таблица 1. Совокупность секвентных функций восьмого порядка

№ $\boldsymbol{s}_i$	Номер разряда функции								№ $\boldsymbol{s}_i$	Номер разряда функции							
	7	6	5	4	3	2	1	0		7	6	5	4	3	2	1	0
0	0	0	0	0	0	0	0	0	18	0	1	0	1	1	0	0	1
1	0	1	1	1	1	0	0	0	19	0	0	1	1	1	0	0	1
2	0	1	1	1	0	1	0	0	20	0	1	1	0	0	1	0	1
3	0	1	1	0	1	1	0	0	21	0	1	0	1	0	1	0	1
4	0	1	0	1	1	1	0	0	22	0	0	1	1	0	1	0	1
5	0	0	1	1	1	1	0	0	23	0	1	0	0	1	1	0	1
6	0	1	1	1	0	0	1	0	24	0	0	1	0	1	1	0	1
7	0	1	1	0	1	0	1	0	25	0	0	0	1	1	1	0	1
8	0	1	0	1	1	0	1	0	26	0	1	1	0	0	0	1	1
9	0	0	1	1	1	0	1	0	27	0	1	0	1	0	0	1	1
10	0	1	1	0	0	1	1	0	28	0	0	1	1	0	0	1	1
11	0	1	0	1	0	1	1	0	29	0	1	0	0	1	0	1	1
12	0	0	1	1	0	1	1	0	30	0	0	1	0	1	0	1	1
13	0	1	0	0	1	1	1	0	31	0	0	0	1	1	0	1	1
14	0	0	1	0	1	1	1	0	32	0	1	0	0	0	1	1	1
15	0	0	0	1	1	1	1	0	33	0	0	1	0	0	1	1	1
16	0	1	1	1	0	0	0	1	34	0	0	0	1	0	1	1	1
17	0	1	1	0	1	0	0	1	35	0	0	0	0	1	1	1	1

Каждая ненулевая секвента, обозначим ее $\hat{\boldsymbol{s}}_k$, $k=\overline{1,35}$, отстоит от секвенты $\boldsymbol{s}_0$ на расстоянии Хэмминга $d=N/2$ и для принятого порядка $N=8$ это расстояние равно четырем. Назовем $\hat{\boldsymbol{s}}_k$ *образующей секвентой* множества $\boldsymbol{\Omega}_k$. В состав каждого множества $\boldsymbol{\Omega}_k$ кроме пары $\boldsymbol{s}_0$ и $\hat{\boldsymbol{s}}_k$ входят все те секвенты $\boldsymbol{s}_i$ из табл. 1, которые отстоят от $\hat{\boldsymbol{s}}_k$ на расстоянии $d(\hat{\boldsymbol{s}}_k,\boldsymbol{s}_i)=4$. Неполный набор множеств $\boldsymbol{\Omega}_k$ с выделенными затенением элементами $\boldsymbol{s}_i\in\boldsymbol{\Omega}_k$ представлен в табл. 2.

Обратим внимание на такие особенности табл. 2. Во-первых, будучи дополненной отсутствующими образующими секвентами $\hat{\boldsymbol{s}}_k$, табл. 2 становится симметричной относительно главной диагонали. Во-вторых, каждый столбец таблицы кроме образующей секвенты $\hat{\boldsymbol{s}}_k$ (светлого диагонального элемента, выделенного жирной рамкой) включает 18 секвент $\boldsymbol{s}_i$, отстоящих от образующего элемента $\hat{\boldsymbol{s}}_k$ на расстоянии Хэмминга, равном четырем. Нулевая секвента $\boldsymbol{s}_0$ для компактности из табл. 2 исключена. И, наконец, в-третьих, полная совокупность столбцов табл. 2 (множеств $\boldsymbol{\Omega}_k$) разбито на 10 непересекающихся подмножеств $\boldsymbol{\Omega}^{[l]}$, $l=\overline{1,10}$, причем $l-$е подмножество включает подряд стоящие столбцы, содержащие одинаковое число n_l секвент, расположенных сверху (или слева), образующей секвенты $\hat{\boldsymbol{s}}_k$. Например, подмножество $\boldsymbol{\Omega}^{[1]}$ порождается секвентами $\hat{\boldsymbol{s}}_k$, $k=\overline{1,5}$, при этом $n_1=1$ (единственная секвента, которая находится над (слева) $\hat{\boldsymbol{s}}_k$, является нулевая секвента $\boldsymbol{s}_0$); второе подмножество $\boldsymbol{\Omega}^{[2]}$ формируют секвенты $\hat{\boldsymbol{s}}_k$, $k=\overline{6,9}$, для которых $n_2=4$ и т. д.

Как показали результаты анализа, все 35 множеств $\boldsymbol{\Omega}_k$, каждое из которых содержит 20 секвент $\boldsymbol{s}_i$, образуют по шесть полных групп $\boldsymbol{G}_{k,j}$, $j=\overline{1,6}$, в состав которых входят по восемь эквидистантных секвент $\boldsymbol{s}_i$ и в их числе — нулевая $\boldsymbol{s}_0$ и образующая секвента $\hat{\boldsymbol{s}}_k$.

Введем для совокупностей (множеств) этих шестерок групп восьмого порядка обозначение $\boldsymbol{SF}_k$ (***Sequence Full***), полагая $\boldsymbol{SF}_k=\bigcup_{j=1}^{6}\boldsymbol{G}_{k,j}$. В табл. 3 показаны выделенные затенением секвенты $\boldsymbol{s}_i$, которые входят в полные группы $\boldsymbol{G}_{k,j}$, $k=\overline{1,5}$, $j=\overline{1,6}$, множеств $\boldsymbol{SF}_k$ подмножества $\boldsymbol{\Omega}^{[1]}$.

30 групп $\boldsymbol{G}_{k,j}$, $k=\overline{1,5}$, $j=\overline{1,6}$, табл. 3 составляют *полный набор* групп секвентных эквидистантных байт-функций. Это означает, в частности, что группа функций, образуемая какой угодно секвентой $\hat{\boldsymbol{s}}_m$, $6\le m\le 35$, поглощается одной из групп $\boldsymbol{G}_{k,j}$ подмножества $\boldsymbol{\Omega}^{[1]}$.

В приложениях зачастую интересными могут оказаться не сами по себе полные системы (группы) эквидистантных секвентных функций $\boldsymbol{G}_{k,j}$, а их некоторые упорядочения, такие, например, как системы функций Уолша, образующие симметричные базисы, используемые для спектрального представления сигналов или решения других задач обработки дискретных сигналов.

Таблица 2. Компоненты множеств $\boldsymbol{\Omega}_k$

№ s_i	№ k множеств $\boldsymbol{\Omega}_k$ и образующих секвент $\hat{\boldsymbol{s}}_k$															
	1	2	3	4	5	6	7	8	29	30	31	32	33	34	35	
	$\boldsymbol{\Omega}^{[1]}$					$\boldsymbol{\Omega}^{[2]}$			$\boldsymbol{\Omega}^{[9]}$			$\boldsymbol{\Omega}^{[10]}$				
1									■	■	■					
2							■	■				■	■	■		
3						■		■	■	■		■	■		■	
4						■	■		■		■	■		■	■	
5						■	■	■		■	■		■	■	■	
6			■	■	■				■	■	■	■	■	■		
7		■		■	■						■	■	■		■	
8		■	■		■					■		■		■	■	
9		■	■	■					■				■	■	■	
10	■			■	■			■	■	■				■	■	
11	■		■		■		■		■		■		■		■	
12	■		■	■			■	■		■	■	■			■	
13	■	■			■	■				■	■		■	■		
14	■	■		■		■		■	■		■	■		■		
15	■	■	■			■	■		■	■		■	■			
16			■	■	■		■	■	■	■	■	■	■	■	■	
17		■			■	■					■	■	■	■	■	
18		■	■		■	■	■			■		■		■	■	
19		■	■	■		■	■	■	■				■	■	■	
20	■			■	■	■	■		■	■				■	■	
21	■		■		■	■		■	■		■		■		■	
22	■		■	■		■				■	■	■			■	
23	■	■			■		■	■		■	■		■	■		
24	■	■		■			■		■		■	■		■		
25	■	■	■					■	■	■		■	■			
26	■	■	■					■			■			■	■	
27	■	■		■			■			■			■			
28	■	■			■		■	■	■			■				
29	■		■	■		■							■	■		
30	■		■		■	■		■				■		■		
31	■			■	■	■	■					■	■			
32		■	■	■		■	■	■		■	■					
33		■	■		■	■	■		■		■					
34		■		■	■	■		■	■	■						
35			■	■	■		■	■								

Таблица 3. Состав групп $\boldsymbol{G}_{k,j}$, формируемых образующими секвентами подмножества $\boldsymbol{\Omega}^{[1]}$

Группа	Секвенты групп																			
$\boldsymbol{G}_{1,j}$	0	1	10	11	12	13	14	15	20	21	22	23	24	25	26	27	28	29	30	31
1	■	■	■					■		■			■				■	■		
2	■	■	■					■			■	■				■			■	
3	■	■		■			■		■					■			■	■		
4	■	■		■			■				■	■			■					■
5	■	■			■	■			■					■		■			■	
6	■	■			■	■				■			■		■					■
$\boldsymbol{G}_{2,j}$	0	2	7	8	9	13	14	15	17	18	19	23	24	25	26	27	28	32	33	34
1	■	■	■					■		■			■				■	■		
2	■	■	■					■			■	■				■			■	
3	■	■		■			■		■					■			■	■		
4	■	■		■			■				■	■			■					■
5	■	■			■	■			■					■		■			■	
6	■	■			■	■				■			■		■					■
$\boldsymbol{G}_{3,j}$	0	3	6	8	9	11	12	15	16	18	19	21	22	25	26	29	30	32	33	35
1	■	■	■					■		■			■				■	■		
2	■	■	■					■			■	■				■			■	
3	■	■		■			■		■					■			■	■		
4	■	■		■			■				■	■			■					■
5	■	■			■	■			■					■		■			■	
6	■	■			■	■				■			■		■					■

Продолжение табл. 3

$G_{4,j}$	0	4	6	7	9	10	12	14	16	17	19	20	22	24	27	29	31	32	34	35
1	■	■	■					■		■			■			■	■	■		
2	■	■	■					■			■	■				■		■	■	
3	■	■		■			■		■					■			■	■		
4	■	■		■			■				■	■			■					■
5	■	■			■	■			■					■		■			■	
6	■	■			■	■				■			■		■					■
$G_{5,j}$	0	5	6	7	8	10	11	13	16	17	18	20	21	23	28	30	31	33	34	35
1	■	■	■					■		■			■				■	■		
2	■	■	■					■			■	■				■		■	■	
3	■	■		■			■		■					■			■	■		
4	■	■		■			■				■	■			■					■
5	■	■			■	■			■					■		■			■	
6	■	■			■	■				■			■		■					■

В приложениях зачастую интересными могут оказаться не сами по себе полные системы (группы) эквидистантных секвентных функций $\boldsymbol{G}_{k,j}$, а их некоторые упорядочения, такие, например, как системы функций Уолша, образующие симметричные базисы, используемые для спектрального представления сигналов или решения других задач обработки дискретных сигналов.

Ниже обсуждается задача построения (синтеза) симметричных базисов на основе полной совокупности эквидистантных секвент $\boldsymbol{s}_i$, образующих группы $\boldsymbol{G}_{k,j}$, исходная последовательность которых (секвент $\boldsymbol{s}_i$) совсем не обязательно представима в виде симметричной матрицы.

Возможны различные подходы к решению поставленной задачи. Конструктивным способом синтеза симметричных базисов является *метод направленного перебора* [2], суть которого кратко поясним на примере синтеза симметричных систем (матриц) секвентных функций восьмого порядка, выбрав из табл. 3 в качестве исходного набора секвент полную группу

$$\boldsymbol{G}_{1,1} = \left\{ \boldsymbol{s}_0, \hat{\boldsymbol{s}}_1, \boldsymbol{s}_{10}, \boldsymbol{s}_{15}, \boldsymbol{s}_{21}, \boldsymbol{s}_{24}, \boldsymbol{s}_{28}, \boldsymbol{s}_{29} \right\}. \qquad (1)$$

В любом симметричном базисе (матрице) секвентных функций в пространстве изображений, обозначим ее (матрицу) через $\boldsymbol{S}_i$, $i = 1, 2, \ldots$, верхняя строчка матрицы преобразования (базиса) состоит из одних нулей и не может быть переставлена ни на какую другую строчку, так как это приводит к потере симметричности матриц $\boldsymbol{S}_i$. В следующей (первой) строке матрицы $\boldsymbol{S}_i$ может находиться любая из оставшихся базисных функций. Пусть в качестве базисной функция первого порядка выбрана секвента $\hat{\boldsymbol{s}}_1$, в результате чего получим первые две строчки и два столбца матрицы $\boldsymbol{S}_i$. Возможности выбора очередной (второй) строки ограничены условием сохранения симметричности матрицы $\boldsymbol{S}_i$. Для того чтобы это условие соблюсти, из оставшихся базисных функций (1) нужно выбрать только такие, начальные элементы которых совпадают с начальными элементами второй строки, образованной двумя левыми столбцами матрицы $\boldsymbol{S}_i$.

Выполняя указанным способом процедуру синтеза, приходим (как и для варианта классических систем функций Уолша) к полному набору, состоящему из 28 перестановок секвент $\boldsymbol{s}_i$ группы $\boldsymbol{G}_{1,1}$, каждая из которых (перестановок базисных функций) порождает симметричную систему (базис) секвентных функций.

Выводы

Простота алгоритма синтеза Уолша-подобных симметричных систем (базисов) секвентных функций, высокие скорости спектральной обработки сигналов, обеспечиваемые предлагаемыми базисами, открывают разрабатываемым системам широкую перспективу применения в различных направлениях науки и техники как для целей спектрального анализа дискретных сигналов, так и криптографической защиты информации.

Література References

[1] Трахтман А. М. Основы теории дискретных сигналов на конечных интервалах. / А. М. Трахтман, В. А. Трахтман. — М.: Сов. радио, 1975. – 208 с.

[2] Білецький А. Я. Синтез симетричних матриць Уолша по методу спрямованої перестановки базисних функцій. / А. Я. Білецький, О. А. Білецький, О. Г. Кучер. // Вісник НАУ, Київ, 2001, № 3. – С. 141-146.

Hash Functions Based on One- and Multy-Dimensional Cellular Automata

O. Konstantynyuk, Yu. Tanasyuk, S. Ostapov
Yuriy Fedkovych Chernivtsi National University
Chernivtsi, Ukraine
y.tanasyuk@chnu.edu.ua

***Abstract*—Cryptographic hash functions on the basis of one-, two- and three-dimensional cellular automata deploying pseudorandom permutation with the use of various processing rules have been developed. The proposed constructions revealed high-quality scattering properties, strong avalanche effect and sufficient processing rates in producing the message digests of 224, 256, 384, 512 bits.**

Keywords—cryptographic hash function, cellular automata, cryptographic sponge, Keccak algorithm

I. Introduction

Cellular automata (CA) are well known to be self-organizing statistical systems, providing ample opportunities for simulation of physical systems, image processing, design of computer architectures and cryptography [1]. Due to their ability to generate high-quality pseudorandom patterns, CA have been considered for design of block and stream ciphers, public key cryptography, message authentication and hash function. A number of CA rules and their combinations with bitwise operations exhibit a desired behavior needed in cryptographic primitives.

Cryptographic hash function is primarily used to create a unique representation of an input message by computing its short fixed-length digest, known as a fingerprint of the message. To be secure, a hash function needs to be irreversible and resistant to collisions [2]. CA based hash functions reviewed in [3] are claimed to be collision free and able to achieve high processing speed, resulting from parallelism and homogeneity of the underlying transition rules.

Recently, a large number of hash function construction approaches have been proposed. Among the most promising there is a Keccak algorithm, adopted for the SHA-3 standard, that doesn't rely on a compression approach of its predecessors but is based on a sponge construction, which provides pseudorandom permutation [4].

The main purpose of the paper is to develop and research cryptographic hash functions, based on the sponge construction of the Keccak algorithm and various processing rules of one- two- and three-dimensional CA.

II. Keccak Fundamentals

The Keccak algorithm is reported to possess many attractive features, including its ability to run well on different computing devices, i.e. embedded or smart, and high performance in hardware implementation, comparing to SHA-2 [4]. Keccak is based on the sponge function, which is, in general, a cryptographic hash function with a varying output.

Sponge has its inner state, which is a binary array of the fixed length b. The array consists of two parts – r and c. Parameter r is called a bit rate. This very part is combined with the equal portions of the input message and is used to produce a resulting hash string. Parameter c is called the capacity, $c=b-r$. This value is not directly affected by input message blocks and is responsible for security level of the hash function. Namely, to derive the hash with defined mathematical stability, the value of capacity must be twice as large as the hash length. For SHA-3 with the state of b=1600 bits the parameters of sponge are given in Table I.

Prior to processing a message by the Keccak hash function, the input message has to be padded to the length, which is the multiple of r bits. Then, the padded message is divided into the blocks of r-length. The sponge construction operates in two phases: absorbing and squeezing.

At the absorbing stage r portion of the sponge inner state is combined with the message block of the same length by means of XOR operation, and the whole state array is processed by a permutation function for a fixed number of rounds. Squeezing phase starts after all message blocks have been absorbed and is aimed at generation of the message digest of the desired length.

In the original Keccak algorithm the sponge state is presented as a three-dimensional array of 5×5 64 bit words. At heart of the described construction there is the permutation function, which consists of five steps, denoted by Greek letters: θ (theta), ρ (rho), π (pi), χ (chi) and ι (iota). The named functions include bitwise operations, and are claimed to be relatively hardware friendly resulting in high performance of the Keccak algorithm [2, 4].

TABLE II. KECCAK PARAMETERS FOR HASH OF VARIOUS LENGTH

Hash Length, *Z* (bits)	Bit Rate, *r* (bits)	Capacity, *c* (bits)	Security Level, Z/2
224	1152	448	112
256	1088	512	128
384	832	768	192
512	576	1024	256

In the research conducted we have focused on the design of cryptographic hash functions that are based on sponge construction, implemented in the shape of one-, two- and three-dimensional cellular automata with the use of specific combinations of the CA processing rules and bitwise operations.

III. DESIGNING HASH FUNCTIONS ON THE BASIS OF CA

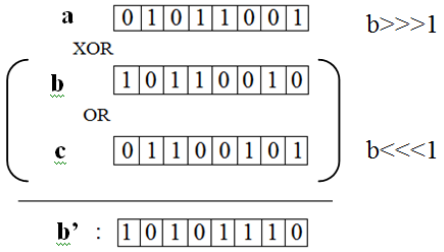
A CA is a collection of simple cells connected in a regular manner. Each cell can assume the value of binary 0 or 1. The cells evolve simultaneously in discrete time steps according to some deterministic rule. The next state of the cell depends on itself and on its neighbors. Our investigations considered the following CA processing rules:

$$\text{rule 30: } b' = a \oplus (b \vee c), \quad (1)$$
$$\text{rule 86: } b' = (a \vee b) \oplus c, \quad (2)$$
$$\text{rule 150: } b' = a \oplus b \oplus c, \quad (3)$$

where b is the current cell, b' is its new value after the rule application, a is the previous cell, c is the next cell, and $\oplus$, $\wedge$, $\vee$ denote the bitwise XOR, AND, and OR operations, respectively. According to [5] the rule 150 (3) is called linear, since it involves only XOR logic. The rules (1) and (2) containing XNOR logic are nonlinear. As recommended in [1], in order to design a reliable hash function a combination of linear and nonlinear CA rules is to be used. Linear rules provide collision resistance, while nonlinear ones bring about one-way property and nonlinearity.

A. *One-dimensional CA*

One-dimensional sponge state is implemented as a 1600-bit long binary array, which is a three neighborhood CA, with extreme cells adjacent to each other. The round permutation is performed through the multiple use of one of the rules of 30, 86, or 150, their joined sequential application, or a combination of the rules with bitwise operations of cyclic shift and negation, depending on the number of iteration [6]. It's noteworthy, that cell processing was implemented not in a bit-to-bit manner, but in parallel. For this purpose at each round two instances of the current state array were created: one-bit cyclically shifted to the right copy represented all previous cells, while one-bit cyclically left-shifted one contained all next cells. This approach enabled us to apply corresponding bitwise operations to the obtained bit sets. Fig. 1 shows schematically application of rule 30 (1) to the 8-bit long string.



Concurrent application of rule 30 (1) to the entire bit string

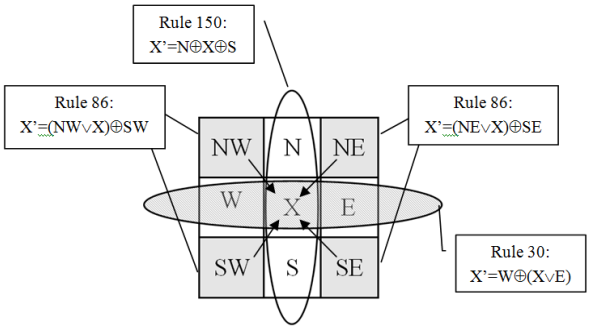
B. *Two-dimentional CA*

In two-dimensional CA representation the sponge state is arranged as an array of 25 64-bit long strings, making 1600 bits in total. The cells are localized according to the Moore neighborhood [5], when two cells are considered adjacent if they have either a common edge or a vertex. Therefore, each cell interacts with its eight direct neighbors, denoted as parts of the world (Fig. 2). Extreme cells are connected in tor with their counterparts on the opposite edge (row/column) of the array.

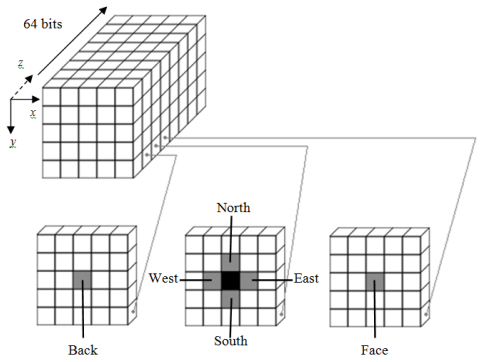
To ensure effective permutation, combinations of adjacent cells were processed with different CA transformation rules, as shown in Fig.2. The rule deals with the entire rows concurrently, according to the technique, described above.

C. *Three-dimensional CA*

The sponge state is arranged as a two-dimensional array (5x5) of 64-bit vectors (b=5×5×64=1600 bits). As in the constructions, described above, r and c portions were defined by the desired hash length (see Table I). First r/64 vectors were initialized with binary 1s, while a bit corresponding to a vector's index was inverted. This procedure is chosen to improve scattering properties of the developed construction. Each cell of the proposed three-dimensional CA possesses 6 neighbors with common edges (Fig. 3), denoted as North, South, East and West within the same plate, while Face and Back are shown as neighboring cells of the adjacent plates.



Interaction rules for a cell X with its neighbors in two-dimensional CA, where N, W, NE, NW are treated as previous cells, while S, E, SE, SW are the next ones.



A group of cells, participating in interaction in three-dimensional CA. With respect to the central cell, North, West and Back are considered as previous neighbors, and South, East and Face are the next ones.

In order to apply CA processing rules to each cell and explain the interaction of the current cell with its neighbors, we've introduced the following notations: along X axis West is a previous cell and East is a next one. In the direction of Y axis (as shown in Fig. 3) North and South are previous and next cells, respectively. And along Z axis Back is a previous neighbor and Face is the following one.

To implement any rule of CA all previous cells and all next cells are combined by XOR operation with each other. Namely, rule 86 (2) is performed as follows:

b' = (([North] xor [West] xor [Back]) **OR** [b]) **XOR** ([South] xor [East] xor [Face])

Interaction with compliance to the described rules is carried out between the entire binary vectors, rather than individual cells, which can significantly accelerate the processing rate.

With regard to transformations between the cells of the face and back within the current vector, two copies of it are created: one bit cyclically shifted to the left, and to the right, denoting the Back and the Face, respectively.

A permutation function on the basis of the designed three-dimensional CA includes a combination of CA processing rules and binary functions, applied at each round of absorbing and squeezing. The processing involves two empty two-dimensional (5x5) arrays of 64-bit vectors newArrayRC and tempArray. Each 64-bit vector of the original array (ArrayRC) is processed with the use of rule 30, followed by 23-bit cyclic shift to the right, and the resulting vectors are consistently written into tempArray.

As the transformation is complete, ArrayRC is combined with tempArray as its shifted copy through XOR operation. Then, similarly, the basic array is updated by XOR with its copy tempArray, obtained through application of rule 86 with further 3-bit cyclic shift to the left. After that the vectors of the basic array undergo processing by rule 150. When the manipulation of the main array is over, the content of its first column of 64-bit vectors is copied to the last column of the newArrayRC, followed by one-position horizontal and vertical shift of the vectors to the left and down, respectively. The whole procedure is accomplished in 5 steps. On completion of the transformations, the newArrayRC becomes a main array. Its final processing is performed with the use of rule 86, 3-bit left cyclic shift, XOR and rule 150 operations, in the manner described above.

IV. Results and Discussion

Computer program to implement the proposed permutation functions has been developed. The parameters of the inner state of cryptographic sponge comply with those, proposed by the Keccak algorithm. Although, the created software enables generation of the hash strings of 224, 256, 384 and 512 bits, message digest of any other desired length may be calculated, if corresponding ratio between r and c parameters is preserved. In order to provide a sufficient level of security, value of c must be twice as large as the hash length.

Scattering properties of the developed hash functions were studied using the NIST STS technique. The binary sequences of 10^8 bits were generated by the proposed one-, two- and three-dimensional constructions with such parameters (bits): b=1600, hash length Z= 512, r=576, c=1024.

According to the obtained statistical data, at least 96 % of the sequences have successfully passed all the NIST STS tests. It points out, that binary strings generated by the constructed hash functions on the basis of both one- and multi-dimensional CA, by their properties approach the pseudorandom ones.

Fig. 4 and 5 shows typical statistical portraits of the cryptographic hash functions, built on the proposed construction of multi-dimensional CA. The generalized results of the conducted statistical investigation are given in Table II.

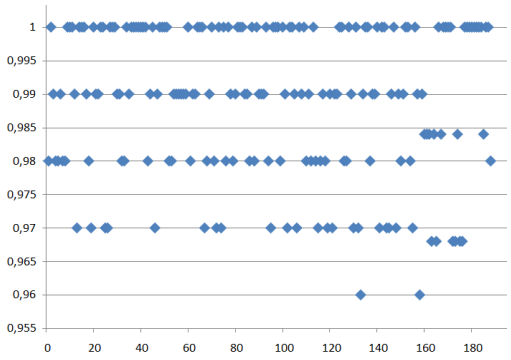


Fig. 4. Statistical portrait of the cryptographic hash function on the basis of two-dimensional CA after 5 rounds of permutation, where N is a number of a test, P is the portion of test sequences, which passed the test

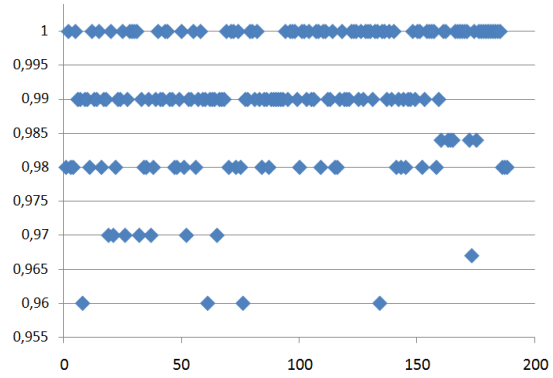


Fig. 5. Statistical portrait of the cryptographic hash function on the basis of three-dimensional CA after 2 rounds of permutation, where N is a number of a test, P is the portion of test sequences, which passed the test

TABLE III. GENERALIZED RESULTS OF STATISTICAL TESTIG OF VARIOUS PERMUTATION FUNCTIONS ON THE BASIS OF CA

Hash algorithm version[a]	NIST STS testing results				
	<0.96	*0.96*	*0.98-0.97*	*1-0.99*	*Average*
1.	0	2	56	130	0.9897
2.	0	2	65	121	0.9889
3.	2	6	41	139	0.99
4.	4	4	55	125	0.9883
5.	0	4	46	140	0.9907

[a] where 1 - one-dimensional CA, 25 rounds; 2, 3 - two-dimensional CA, 5 rounds and 10 rounds, respectively; 4, 5 – three-dimensional CA, 1 round and 2 rounds, respectively.

The performance of the cryptographic hash functions, given in Table II, was estimated on the computer with CPU Intel Core i5 4200U, 1.5 GHz and RAM 4GB by processing rates of forming a 100 MB text file of 512-bit binary hash strings, used in the NIST STS statistical tests. As Table III shows, the highest processing rates were achieved for two-dimensional CA construction at 5 rounds of permutation (hash algorithm of version 2). The second best result applies to the functions built on one-dimensional CA that underwent processing by the set of rules and binary operations for at least 25 rounds (version 1).Keccak Parameters For Hash of Various Length

Hash algorithm version[a]	Number of rounds	Time to form a 100 MB text file of 512-bit hash strings (seconds)	Processing rate (KB/s)
1.	25	213	492.3
2.	5	136	771
3.	10	288	364.1
4.	1	408	257
5.	2	834	125.7

[a] where 1 - one-dimensional CA, 25 rounds; 2, 3 - two-dimensional CA, 5 rounds and 10 rounds, respectively; 4, 5 – three-dimensional CA, 1 round and 2 rounds, respectively.

The application of the developed permutation functions for obtaining a hash image revealed the dependence of the scattering properties on the length of the hash, the type of the function, and the number of processing rounds. For all proposed hash functions, strong avalanche effect was observed, i.e. the digest of the incoming message was completely updated when changing the hash length (224, 256, 384, 512 bits) or at the smallest changes in the message. It should be noted, that for various hash functions the avalanche effect was observed at different number of the processing rounds. Namely, the one-dimensional permutation functions based on the use of one CA transformation rule need up to 100 rounds, while application of several rules brings about satisfactory outcomes after 50 iterations [6]. A full change in the resulting hash occurs for two-dimensional hash functions starting from 5 processing rounds, while three-dimensional constructions produce a completely different hash string after 1 round of permutation, without significant degrading a processing rate.

V. CONCLUSION

Summarizing the conducted investigations the following conclusions can be made:

1. The permutation functions, based on one-, two- and three-dimensional CA, with the use of various rules of CA interactions have been developed.

2. Joint application of both linear and nonlinear CA processing rules together with bitwise operations enabled us to achieve high-quality scattering properties and provide satisfactory level of security in the designed constructions.

3. Concurrent manipulation of the inner state's vectors of the cryptographic sponge ensured reasonable processing rates, while deployment of multi-dimensional CA significantly reduces the number of iterations.

4. All the designed transformation functions under investigation revealed the appearance of the avalanche effect, considered to be a desirable characteristic of cryptographic hash function.

REFERENCES

[1] J.-Ch. Jeon Analysis of hash functions and cellular automata based schemes. International Journal of Security and Applications, 2013. – Vol. 7, No. 3, pp.303–316.

[2] Ch. Paar, J. Peltz. Understanding cryptography. – Springer-Verlag Berlin Heidelberg, 2010. – 372 p.

[3] N. Jamil A new cryptographic hash function based on cellular automata rules 30, 134 and omega-flip network. ICICN 2012, 2012. – Vol. 27, pp. 163 – 169.

[4] G. Bertoni [Electronic resource]. – The Keccak sponge function family. – Access mode : http://keccak.noekeon.org/.

[5] S. Wolfram S. A New Kind of Science Wolfram Media, Inc. – 2002. 1197 p. – [Electronic resource]. – Access mode: http://www.wolframscience.com/nksonline/toc.html.

[6] Yu. Tanasyuk, Kh. Melnychuk, S. Ostapov. Development and research of cryptographic hash funcions on the basis of cellular automata. – Information Processing Systems, 2017. – Vol. 4(150), pp. 122 – 127

Comparative overview of basic cybervulnerabilities of mobile applications for android operating system

S. Semenov, T. Shypova, O. Movchan
Department «Computer Engineering and programming»,
National Technical University «Kharkiv Politechnical Institute»
Kharkiv, Ukraine
s_semenov@ukr.net

Abstract: With the market for mobile applications for Android platform constantly growing and more security-dependent tasks moving to mobile platforms, security of Android applications is a major concern for developers and users. In this paper, an overview of Android operating system security model is given. Components of Android application are studied, with special attention given to mechanisms of Inter-process communication via Intents. An overview of basic vulnerabilities of Android applications and vulnerabilities of IPC in Android applications is performed. Recommendations for avoiding described vulnerabilities are given.

Keywords: Android, security, inter-process communication, vulnerability, attack vectors.

I. INTRODUCTION

At the current moment of time, mobile devices are extremely widely used and the numbers of mobile device users is growing more and more. In its core, a modern mobile device is a portable computer with telephony capabilities. And, as is the case with regular computers, functionality of mobile device is limited to software installed on the device. Today mobile applications are used for various tasks like social media, communication and entertainment. However, more and more security-dependent tasks, for example banking and enterprise management, are going mobile as well. And it is important to provide the necessary security level to protect the system from attacks.

The purpose of the paper is to present the overview of basic vulnerabilities in applications for Android platform with regard to the architecture of Android applications and the programming language used in development, with special attention towards vulnerabilities in Inter-process communication mechanisms as a primary source of application vulnerabilities. It should be noted that this paper focuses on individual vulnerabilities of the application under testing rather than overall testing methodology.

II. ANDROID SECURITY MODEL OVERVIEW

In order to analyze vulnerabilities in Android applications, it is required to have the knowledge of the security system provided by the OS. The security system that is enforced by Android can be described as a two-tier system.

Android, at its core, relies on one of the security features provided by Linux kernel – running each application as a separate process with its own set of data structures and preventing other processes from interfering with its execution [1, 2]. Parts of the system are also separated into distinct identities. Linux thereby isolates applications from each other and from the system. This mechanism is called sandbox and it is displayed in figure 1.

More detailed security mechanism of “permissions” allows finer control of access of application to device and OS features [3]. A basic Android application has no permissions associated with it by default, meaning it cannot do anything that would adversely affect the user experience or any data on the device. To make use of protected features of the device, you must include one or more <uses-permission> tags in your app manifest.

If your app lists *normal* permissions in its manifest (that is, permissions that don't pose much risk to the user's privacy or the device's operation), the system automatically grants those permissions.

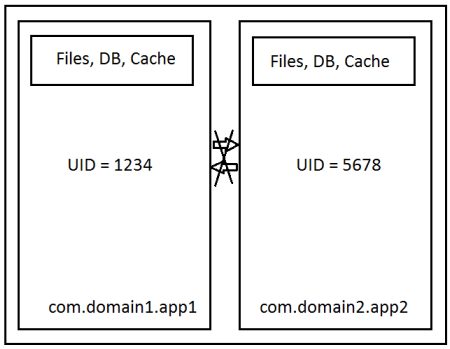


Figure 1 – Android application sandbox

If your app lists *dangerous* permissions in its manifest (that is, permissions that could potentially affect the user's privacy or the device's normal operation), the system asks the user to explicitly grant those permissions.

III. ANDROID APPLICATION STRUCTURE OVERVIEW

Android applications are developed using Java programming and Android SDK in a majority of cases, with the exception of games and other CPU-intensive

apps, where Android NDK and native languages like C and C++ are used. Considering the fact that most Android applications are built using Java and Android SDK, only Android SDK elements will be overviewed.

There are four main components of the Android application: activities, BroadcastReceivers, ContentProviders and services. They communicate between each other using messages called Intents [4].

An Activity is an application component that provides a screen with which users can interact in order to do something, such as dial the phone, take a photo, send an email, or view a map. Each activity is given a window in which to draw its user interface.

Intents are messages through which other application components (activities, services, and Broadcast Receivers) are activated. They can be thought of as messages stating which operations/actions need to be performed. Intents can be explicit and implicit. Explicit intents specify the component to start by name (the fully-qualified class name). Explicit intent are usually used to start a component in the same app, because the class name of the activity or service that is intended to start, is known. Implicit intents do not name a specific component, but instead declare a general action to perform, which allows a component from another app to handle it.

A service is an application component that can perform long-running operations in the background for an application. It does not have a UI component to it, but it executes tasks in the background. Other applications can be running in the front while services will be active behind the curtain even after the user switches to a different application component or application.

Content providers provide applications with a means to share persistent data. A content provider can be thought of as a repository of data, and different applications can define content providers to access it. Providers and provider clients enable a standard interface to share data in a secure and efficient manner. When an application wants to access data in a content provider, it does so through ContentResolver.

Component can be declared exported (public) in order to be accessible to other applications. This can be done by setting the EXPORTED flag in the manifest or by including at least one IntentFilter. After being declared exported, component can be launched via an implicit Intent that confines to an IntentFilter, or via an explicit Intent, which bypasses IntentFilters entirely. This mechanism of launching exported components enables many attack surfaces for basing attack on.

IV. Android Application Basic Attack Surfaces

Considering the platform and the language used in development of the application for Android platform, vulnerabilities of Android applications can be divided into following:

[1] general vulnerabilities of mobile and web applications;

[2] vulnerabilities specific to the Android platform.

General vulnerabilities are vulnerabilities that do not feature Android specific application elements as an attack vector. Vulnerabilities in this category are quite common in mobile and web applications and are based on application architecture flaws or development bad habits. The list of these vulnerabilities consists of, but not limited to:

[3] using raw user input as query parameters;

[4] weak or no cryptography on sensitive user data;

[5] insecure data storage;

[6] poor authentication and authorization controls;

[7] security decisions vie untrusted inputs;

[8] logging sensitive user information.

One of the more common mobile vulnerabilities, insecure data storage vulnerability is a result of storing sensitive user information in an insecure storage like a database on the device. Insecure data storage vulnerabilities occur when development teams assume that users or malware will not have access to a mobile device's filesystem and subsequent sensitive information in data-stores on the device, which is usually never the case. Filesystems are easily accessible for malicious users. It is possible to extract the data from the filesystem using special tools. Insecure data storage can result in data loss for one or more users. Common valuable pieces of data seen stored include usernames, authentication tokens, passwords, cookies, personal information like date of birth, address, credit card data and application data like logs and configuration files.

According to OWASP, in order to prevent insecure data storage vulnerabilities, it is recommended to avoid storing data on the device unless necessary [5]. When it is impossible to avoid storing sensitive data on the device, the following actions are advised for Android platform:

[9] force encryption on local file storages with setStorageEncryption;

[10] use manual encryption for data on SD card;

[11] ensure any shared preferences properties are not MODE_WORLD_READABLE unless explicitly required for information sharing between app;

[12] avoid hardcoding encryption or decryption keys when storing sensitive information.

Another common class of vulnerabilities, security vulnerabilities via untrusted inputs exist when application has no validation of inputs in secure method realizations. Developers can assume that only high-level user can call specific secure method and, because of it, do not validate status of the caller. This allows attacker to gain access to secure functionality or even gain higher-level permissions.

In order to avoid these vulnerabilities, it is advised to follow the rules:

[13] if IPC is required, only white-listed applications should have access to the API and mechanisms;

[14] all input parameters, that are received from IPC entry points, like Intents and broadcasts, should undergo thorough validation, especially their origin;

[15] if possible, passing of sensitive data using IPC should be avoided.

Android specific vulnerabilities are vulnerabilities that feature Android specific elements and OS features as attack vector. The majority of these vulnerabilities are located in IPC mechanisms of the system [6]. Attacks that target vulnerabilities in IPC using mechanism of Intents are:

[16] Intent interception;

[17] Intent spoofing.

Intent interception involves a malicious app receiving an intent that was not intended for it. This can cause a leak of sensitive information, but more importantly, it can result in the malicious component being activated instead of the legitimate component. The attacks are:

[18] Broadcast Theft;

[19] Activity hijacking;

[20] Service hijacking.

Broadcast Theft is an attack that targets vulnerability that is present when an application uses implicit Intent to send data. Any component is able to intercept an implicit Intent so, if a malicious component is able to intercept the intent, then it can access the data. An attacker could perform a denial-of-service attack on the Ordered Broadcasts, since an Intent can only be spread on them if the first component receiving the Intent to uses it for output. Additionally, it could be used to perform Man-in-the-Middle attacks with its subsequent data injection on the spread Intents.

By taking advantage of Activity hijacking vulnerability, a malicious Activity is launched instead of the expected one, so the user will be in a wrong application without being aware. This happens when the change of an Activity depends on an implicit Intent. The attacker registers a more accurate Intent Filter and controls it. The presence of this vulnerability allows executing phishing attacks, as well as leaks of the information handled by the user in the involved Activity. Additionally, this vulnerability allows the attacker modifying the data, putting at risk its integrity.

Service hijacking is a vulnerability similar to Activity hijacking with only difference being that it targets services instead of activities. This vulnerability is more persistent, however, due to the fact that it is transparent to the user because the services do not include graphic interface for it.

For intent spoofing, a typical scenario is that the vulnerable application has a component which only expects to receive intents from other components of the same application. However, if the component is exported, and it becomes exported when declaring intent filter, then any application can send intents to it. Moreover, they do not have to be implicit intents, and if they are explicit then they do not even have to match the intent filter.

These vulnerabilities share the cause – mechanism of implicit Intents and their inherent lack of security. It is advised to avoid using implicit Intents for IPC and instead use explicit Intents when possible, because explicit Intents always target specific component and cannot be intercepted by malicious component. When use of implicit Intents is required, parameters of the intent, especially its origin, should be validated.

Vulnerabilities, described above, can be avoided if developers of the application are aware of both the vulnerabilities, and rules and guidelines to develop secure applications. Security specialists offer guidelines to secure coding for various platforms and programming languages. For example, CERT (Computer Emergency Response Team) offers “The CERT Oracle Secure Coding Standard for Java” that covers the rules for developing secure Java applications. Most of these rules apply to Android platform as well. CERT also offers a set of rules for Android specifically. Another set of guidelines is provided by developers of Android and is featured in the official developers guide to Android [7]

Conclusion

As a result of the Android security model and IPC mechanisms overview, basic IPC vulnerabilities of Android applications are described. It is shown, that mechanism of implicit Intents is the source of the most of IPC vulnerabilities, which is connected to the inherent lack of security of the mechanism. Considering this, it is advised to minimize usage of implicit Intents for IPC. When it is impossible to avoid using implicit Intents, source of them should be validated.

References

[1] System and kernel security | Android open source project: [Electronic resource]. – Mode of access: https://source.android.com/security/overview/kernel-security.html.

[2] Dubey Abhishek Android Security – Attacks and Defenses / Abhishek Dubey, Anmol Misra // Taylor & Francis Group 2013 P. 272.

[3] System permissions | Android developers: [Electronic resource]. – Mode of access: http://developer.android.com/guide/topics/security/permissions.html.

[4] Application fundamentals | Android developers: [Electronic resource]. – Mode of access: http://developer.android.com/guide/components/fundamentals.html.

[5] Exploring the OWASP Mobile Top 10: M1 Insecure data storage: [Electronic resource]. – Mode of access: http://community.hpe.com/t5/Protect-Your-Assets/Exploring-The-OWASP-Mobile-Top-10-M1-Insecure-Data-Storage/ba-p/5904609#.Vtd0A9CjXeg

[6] Chin E., Porter Felt A., Grenwood k., Wagner D. Analyzing Inter-Application Communication in Android [Electronic resource] / Erika Chin, Adrienne Porter Felt, Kate Greenwood, David Wagner. Mode of access: https://www.eecs.berkeley.edu/~daw/papers/intents-mobisys11.pdf

[7.] Security Tips | Android developers: [Electronic resource]. – Mode of access: http://developer.android.com/training/articles/security-tips.html

Захист акустичної інформації методом протифазного придушення

Цирульник С. М.
Вінницький технічний коледж
Вінниця, Україна
svom@ukr.net.

Бородай Я. О.
Вінницький технічний коледж
Вінниця, Україна
bortamu@mail.ru

Роптанов В. І.
кафедра обчислювальної техніки
Вінницький національний технічний університет
roptanov.volodymyr@vntu.edu.ua

Protect acoustic information by antipodal suppression

Tsyrulnyk S.
Vinnytsia Technical College,
Vinnytsia, Ukraine
svom@ukr.net.

Boroday Y.
Vinnytsia Technical College,
Vinnytsia, Ukraine
bortamu@mail.ru

Roptanov V.
Department of Computer Technique
Vinnytsia National Technical University,
Vinnytsia, Ukraine
roptanov.volodymyr@vntu.edu.ua

***Анотація* — Обґрунтовано застосування активного методу захисту мовної інформації, який призводить до зменшення співвідношення сигнал/шум на межі контрольованої зони шляхом придушення корисного сигналу. Наведені результати експериментальних досліджень придушення акустичної інформації шляхом генерації протифазного акустичного сигналу. Проаналізовані причини збудження системи активного придушення сигналу та запропоновані шляхи підвищення ефективності їх функціонування.**

Ключові слова: методи активного захисту мовної інформації, захист акустичної інформації, акустичні канали витоку інформації.

***Abstract* —Application of the method of active protection of speech information that leads to a decrease in signal / noise ratio at the border areas controlled by suppressing signal that contains confidential information. The results of experimental studies of suppression of acoustic information by generating an antipodal acoustic signal are presented. The causes of excitation of the system of active suppression of the signal are analyzed and ways of increasing the efficiency of their operation are proposed.**

Keywords: methods of active protection of speech, protection of acoustic information, acoustic channels of information leakage

I.Вступ

Зростання потужностей сучасних комп'ютеризованих систем обробки великих об’ємів інформації спрощує процес статистичного аналізу масивів існуючих технічних, технологічних, управлінських та ін. рішень. Однак, генерування нових ідей, які стосуються реформування соціального, економічного та політичного життя держави пов’язане із творчою роботою людського інтелекту що, як правило, проявляється у нестандартних, парадоксальних діях та вчинках членів суспільства, які не підлягають «оцифровуванню» та передбачають переважно вербальний шлях обміну інформацією. Таким чином людська мова залишається одним з найважливіших шляхів інформаційної взаємодії, відповідно зберігається необхідність у забезпеченні конфіденційності мовного обміну інформацією у виділеному приміщені чи визначеній контрольованій зоні.

Убезпечення від можливого витоку інформації з обмеженим доступом, яка згенерована вербально та поширюється у виділеному просторі у вигляді акустичних сигналів досягається шляхом запровадженням відповідного комплексу технічного захисту інформації, в якому використовують активні і пасивні методи захисту [1, 2]. До пасивних методів захисту відносять такі, що створюють перешкоди поширенню акустичних коливань відповідними каналами витоку інформації (звукоізоляція акустичними екранами та звукопоглинальними матеріалами). Активні методи захисту мовної інформації застосовують у випадку, якщо використання пасивних засобів захисту не

забезпечують необхідних норм по звукоізоляції виділених для циркуляції акустичних сигналів приміщень.

Основна ідея покладена в основу роботи активних методів захисту мовної інформації полягає в тому, щоб певними засобами досягнути зменшення співвідношення сигнал/шум на межі контрольованої зони за рахунок підвищення рівня шуму (перешкоди), що забезпечує маскування інформативного сигналу або зниження його розбірливості до рівня, який унеможливлює неконтрольований доступ до мовної інформації.

Недоліком активних методів захисту інформації реалізованих на зазначених принципах є необхідність створювати підвищений рівень шумової завади, що являє собою демаскуючий фактор, який виявляється засобами розвідки, дає можливість встановити конфігурацію контрольованої зони, зробити висновки щодо конфіденційності поширюваної в ній інформації, слугувати сигналом для активації інших засобів неконтрольованого доступу до інформації, які відстежують не акустичні канали витоку.

Ефективно протидіяти витоку мовної інформації акустичними каналами можна за рахунок ослаблення (в ідеалі повного придушення) інтенсивності акустичного поля згенерованого джерелом корисного мовного сигналу на межі контрольованої зони без зменшення рівня інших складових сумарного акустичного сигналу, що генерується в об'ємі виділеного приміщення, а також шумів.

Авторами розвивається напрямок дослідження та розробки методів і засобів активного захисту акустичної інформації шляхом генерації протифазного сигналу необхідної інтенсивності та спрямованості з метою придушення мовного сигналу за рахунок інтерференції на виділеній поверхні чи межі контрольованої зони.

III. Основи методу активного придушення мовного сигналу

Принцип придушення акустичного сигналу за допомогою додаткового протифазного сигналу отримав поширення як метод зменшення шуму який відчуває людина в зашумленому середовищі. Перший патент на такий пристрій був виданий винахіднику Полу Люгу (Paul Lueg) в США в 1934 році [2]. В патенті описаний метод придушення синусоїдальних сигналів та довільних звуків в просторі навколо гучномовця шляхом інвертування полярності. В подальшому описаний метод широко застосувався для виготовлення накладних навушників для роботи персоналу в зашумлених приміщеннях [3]. Приклади сучасної реалізації зазначеного методу наведені в [4, 5]. В [6] описана робота активної системи придушення шуму для вікон, яка призначена для зменшення рівня шуму, що проникає ззовні в контролюємо зону (кімнату). Пристрій складається з мікрофону та гучномовця, який притискається до віконного скла і використовує його в якості резонатора і здатний, залежно від заданої програми придушувати або вибрані звуки або загальний шумовий вуличний сигнал.

Аналогічний принцип пропонується покласти в основу активної системи придушення мовного сигналу на межі контрольованої зони для протидії витоку конфіденційної інформації акустичними каналами.

II. Експериментальне дослідження методу протифазного придушення мовного сигналу

На рис. 1 наведено функціональну схему експериментальної установки для дослідження придушення вібраційних коливань акустичного екрану на межі контрольованої зони.

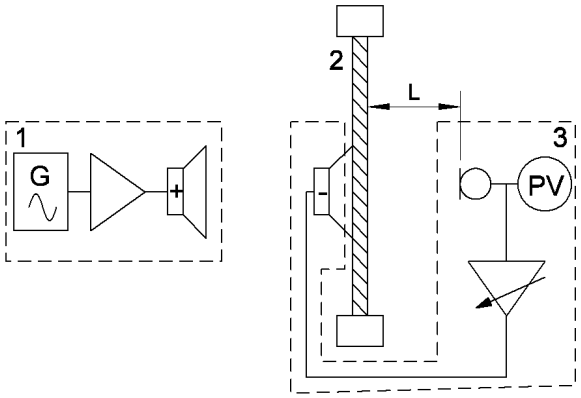


Рисунок 1 – Функціональна схема системи активного придушення мовного сигналу на межі контрольованої зони

Дослідна установка складається з джерела акустичної інформації 1, реалізованого на основі генератора синусоїдальних коливань звукового діапазону та підсилювача навантаженого на гучномовець, скляного акустичного екрану 2, та системи акустичного придушення 3, збудованої із мікрофона, регульованого підсилювача навантаженого на додатковий гучномовець, який закріплений на акустичному екрані та вольтметра. Джерело акустичної інформації та система активного придушення знаходяться в ізольованих приміщеннях, між якими існує канал поширення звукових коливань через акустичним екран. Гучномовці ввімкнені протифазно.

В результаті проведення експерименту отримало підтвердження явище зниження рівня акустичних коливань, що проникають за контрольовану зону, обмежену акустичними екранами через канали витоку акустичної інформації при застосуванні системи активного придушення, реалізованої на принципах складання протифазних сигналів. Величина зниження сигналу за акустичним екраном, що фіксується мікрофоном залежить від рівня підсилення в колі зворотного зв'язку системи придушення і досягає значення -3дБ. Спроба збільшити підсилення в колі системи придушення призводили до збудження.

Проведення додаткових експериментів виявили, що дана схемна реалізація системи активного

акустичного придушення збуджується навіть у випадку відсутності сигналу корисної інформації від джерела 1 на частотах, залежних від відстані L (рис. 1) між акустичним екраном та мікрофоном.

Аналіз побудови системи активного придушення за схемою наведеною на рис. 1 дозволив встановити причину виникнення паразитної генерації. Так коло мікрофон – підсилювач – гучномовець – акустичний екран – мікрофон являє собою петлю зворотного зв'язку. На частотах, для яких виконується умова, при якій на відстані L вкладається непарна кількість напівперіодів петля зворотного зв'язку негативна, збудження не виникає. Якщо цю умову виконати на першій гармоніці, автоматично вона виконається і на всіх непарних гармоніках сигналу, однак, на всіх вищих парних гармоніках на відстані L вкладається парна кількість що призведе до збудження.

Таким чином, у системі активного акустичного придушення мовної інформації реалізованих за схемою наведеною на рис. 1, для яких корисний сигнал не монохромний, а складається із багатьох складових, при достатньому підсиленні в колі зворотного зв'язку завжди виникне збудження.

Для винесення частот паразитної генерації за межі діапазону мовного сигналу необхідно зменшувати відстань L між мікрофоном та акустичним екраном, або застосувати віброелектричний перетворювач закріплений на самому екрані.

Паразитну генерацію можна використати як додаткове джерело шумової завади в діапазоні мовного сигналу.

Висновки

Метод придушення мовного сигналу у виділеному об'ємі дозволяє видалити із загального акустичного сигналу сигнал, що містить конфіденційну інформацію без зміни інтенсивності шумового сигналу.

Система зменшення співвідношення сигнал/шум у виділеному об'ємі (на виділеній поверхні) акустичних каналів витоку інформації шляхом придушення мовного сигналу має перевагу над системами активного захисту мовної інформації, реалізованих за принципом генерації шумової завади в першу чергу через відсутність демаскуючих ознак під час своєї роботи.

Використання запропонованого методу придушення мовного сигналу в комплексі технічного захисту інформації дозволить зменшити вірогідність витоку інформації з обмеженим доступом через акустичні канали на межі контрольованої зони.

Системам активного придушення з інтегрованою петлею зворотного зв'язку властиве збудження. Частоти, на яких відбувається паразитна генерація можна використати в якості додаткової шумової завади.

References

[1] Цирульник С. М. Розв'язування задачі технічного захисту інформації за умови впливу "мовоподібної завади"/ С. М. Цирульник, В. І. Роптанов, О. С. Рехлецький// Інформаційні технології та комп'ютерна інженерія. – 2009. – №1 (14). – с. 44-47

[2] Цирульник С.М. Захист акустичної інформації методом активного придушення / С. М. Цирульник, Я. О. Бородай// Тези доповідей V МНПК «Методи та засоби кодування захисту й ущільнення інформації» м. Вінниця, 19-21 квітня 2016р. – Вінниця : ТОВ «Нілан-ЛТД», 2016. – с. 88-90.

[3] Активное шумоподавление. [Електронний ресурс] / – Режим доступу: https://ru.wikipedia.org/wiki, вільний. – Загол. з екрану. – Мова укр.

[4] Офіційна веб-сторінка компанії SONY. [Електронний ресурс] / Digital Noise Cancelling Headset MDR-NC31EM – Режим доступу: http://www.sonymobile.com/global-en/products/accessories/digital-noise-cancelling-headset-mdr-nc31em/, вільний. – Загол. з екрану. – Мова англ.

[5] Система активного шумоподавления. [Електронний ресурс] / – Режим доступу: http://systemsauto.ru/another/anc.html, вільний. – Загол. з екрану. – Мова рос.

[6] Sono: активная система шумоподавления для окон. [Електронний ресурс] / – Режим доступу: https://habrahabr.ru/post/217601/, вільний. – Загол. з екрану. – Мова рос.

Наукове видання

Методи та засоби кодування, захисту й ущільнення інформації

Тези доповідей
Шостої Міжнародної
науково-практичної конференції
м. Вінниця, Україна
24-25 жовтня 2017 року

Матеріали подаються в авторській редакції

Гарнітура TimesNewRoman
Формат 29,7×421 1/2. Папір офсетний
Ум. друк. арк. 20,04.
Наклад 30 прим. Зам № В2017-26

Вінницький національний технічний університет
ІРВЦ ВНТУ
21021, м. Вінниця, Хмельницьке шосе, 95,
ВНТУ, ГНК, к. 114
Тел.: (0432) 59-85-32
Свідоцтво суб'єкту видавничої справи
серія ДК № 3516 від 01.07.2009 р.

Виготовлювач ФОП Барановська Т. П.
21021 м. Вінниця, вул. Порика, 7.
Свідоцтво суб'єкта видавничої справи
ДК № 4377 від 31.07.2012.