РЕФЕРАТИ РЕФЕРАТЫ ABSTRACTS

МЕТОДИ ТА МОДЕЛІ КРИПТОГРАФІЧНОГО АНАЛІЗУ ТА КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

МЕТОДЫ И МОДЕЛИ КРИПТОГРАФИЧЕСКОГО АНАЛИЗА И КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

METHODS AND MODELS OF CRYPTOGRAPHIC ANALYSIS AND CRYPTOGRAPHIC TRANSFORMATIONS

УДК 621.391:519.2

Узагальнений диференціально-лінійний криптоаналіз блокових шифрів / *А.М. Олексійчук* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 5 – 15.

Диференціально-лінійний метод криптоаналізу блокових шифрів запропоновано в 1994 р. Він виявляється більш ефективним в порівнянні з (окремо) диференціальним та лінійним методами, проте його наукове обґрунтування залишається предметом подальших досліджень. Відомо декілька публікацій, присвячених формалізації диференціально-лінійного методу та з'ясуванню умов, за яких його трудомісткість може бути оцінено математично строго. Однак проблема наукового обґрунтування диференціально-лінійного методу в повному обсязі залишається невирішеною.

В роботі викладено перші результати, отримані автором у напрямі вирішення цієї проблеми. Розширено клас диференціально-лінійних атак на блокові шифри. А саме, розглянуто як розрізнювальні атаки, так і атаки, спрямовані на відновлення одного біту інформації про ключ. При цьому не робиться жодних припущень (як у відомих публікаціях) про можливість представлення шифру у вигляді певних двох компонент. Отримано нижні оцінки інформаційної складності зазначених атак, вирази яких залежать від усереднених (за ключами) значень квадратів елементів узагальненої автокореляційної таблиці шифрувального перетворення. На відміну від відомих, отримані оцінки інформаційної складності диференціально-лінійних атак не базуються на жодних евристичних припущеннях відносно блокових шифрів, що досліджуються, та є справедливими для більш широкого класу атак в порівнянні з традиційною диференціально-лінійною атакою. Наведено співвідношення, які встановлюють взаємозв'язок між, відповідно, диференціальними, лінійними та диференціально-лінійними властивостями бієктивних булевих відображень. На відміну від відомих робіт, використовується матрична форма запису співвідношень, що дозволяє краще з'ясувати їх сутність та спростити доведення. Отримано нове співвідношення для елементів узагальненої автокореляційної таблиці шифрувального перетворення добутку двох блокових шифрів, яке може бути корисним в подальших дослідженнях.

Ключові слова: симетрична криптографія; блоковий шифр; диференціально-лінійний криптоаналіз; узагальнена таблиця автокореляції; обґрунтування стійкості.

Бібліогр.: 16 назв.

УДК 621.391:519.2

Обобщенный дифференциально-линейный криптоанализ блочных шифров / *А.Н. Алексейчук* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 5 – 15.

Дифференциально-линейный метод криптоанализа блочных шифров предложен в 1994 г. Он оказывается более эффективным по сравнению с (отдельно) дифференциальным и линейным методами, однако его научное обоснование остается предметом дальнейших исследований. Известно несколько публикаций, посвященных формализации дифференциально-линейного метода и выяснению условий, при которых его трудоемкость может быть оценена математически строго. Однако проблема научного обоснования дифференциально-линейного метода в полном объеме остается не решенной.

В работе изложены первые результаты, полученные автором в направлении решения этой проблемы. Расширен класс дифференциально-линейных атак на блочные шифры. А именно, рассмотрены как различающие атаки, так и атаки, направленные на восстановление одного бита информации о ключе. При этом не делается никаких предположений (как в известных публикациях) о возможности представления шифра в виде некоторых двух компонент. Получены нижние оценки информационной сложности указанных атак, выражения которых зависят от усредненных (по ключам) значений квадратов элементов обобщенной автокорреляционной таблицы шифрующего преобразования. В отличие от известных, полученные оценки информационной сложности дифференциально-линейных атак не базируются на каких-либо эвристических допущениях об исследуемых блочных шифрах и справедливы для более широкого класса атак по сравнению с традиционной дифференциально-линейной атакой. Приведены также соотношения, устанавливающие взаимосвязь между, соответственно, дифференциальными, линейными и дифференциально-линейными свойствами биективных булевых отображений. В отличие от известных работ, используется матричная форма записи соотношений, что позволяет лучше выяснить их сущность и упростить доказательства. Получено новое соотношение для элементов обобщенной автокорреляционной таблицы шифрующего преобразования произведения двух блочных шифров, которое может быть полезным в дальнейших исследованиях.

Ключевые слова: симметричная криптография; блочный шифр; дифференциально-линейный криптоанализ; обобщенная таблица автокорреляции; обоснование стойкости.

Библиогр.: 16 назв.

UDC 621.391:519.2

Generalized differential-linear cryptanalysis of block ciphers / *A.N. Alekseychuk* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 5 – 15.

Differential-linear cryptanalysis of block ciphers was proposed in 1994. It turns out to be more efficient in comparison with (separately) differential and linear cryptanalytic methods, but its scientific substantiation remains the subject of further research. There are several publications devoted to formalization of differential-linear cryptanalysis and clarification of the conditions under which its complexity can be mathematically accurately assessed. However, the problem of the differential-linear cryptanalytic method substantiation remains completely unresolved.

This paper presents first results obtained by the author in the direction of solving this problem. The class of differential-linear attacks on block ciphers is expanded. Namely, both distinguishing attacks and attacks aimed at recovering one bit of information about a key are considered. In this case, no assumptions are made (as in well-known publications) about the possibility of representing the cipher in the form of some two components. Lower bounds of information complexity of these attacks are obtained. The expressions of these bounds depend on the averaged (by keys) values of the elements' squares of the generalized autocorrelation table of the encryption transformation. In contrast to the known ones, the obtained bounds are not based on any heuristic assumptions about the investigated block ciphers and are valid for a wider class of attacks as compared to the traditional differential-linear attack. Relations between, respectively, differential, linear and differential-linear properties of bijective Boolean mappings are given. In contrast to the well-known works, the matrix form of the relations is used that makes it possible to clarify better their essence and simplify the proofs. A new relation is derived for the elements of the generalized autocorrelation table of the encryption transformation of the product of two block ciphers, which may be useful in further research.

Key words: symmetric cryptography; block cipher; differential-linear cryptanalysis; generalized autocorrelation table; security proof.

Ref: 16 items.

УДК 004.056.55

Генерація загальносистемних параметрів для схеми електронного підпису Rainbow для 384 та 512 біт безпеки / *М.В. Єсіна, С.О. Кандій, Є.В. Острянська, І.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 16 – 23.

На сьогодні спостерігається стрімкий прогрес у створенні квантових комп'ютерів щодо вирішення обчислювально складних задач та для різних цілей. При цьому особливі зусилля докладаються до створення такого квантового комп'ютера, що зможе вирішувати задачі криптоаналізу існуючих криптосистем – асиметричних шифрів, протоколів інкапсуляції ключів, електронних підписів тощо. Попередження таких загроз може бути досягнуто засобом розробки таких криптографічних систем, що будуть захищені як від квантових, так і від класичних атак, а також зможуть взаємодіяти з протоколами і мережами зв'язку, що вже існують. Також є суттєва необхідність захисту від атак сторонніми каналами. На даний момент значні зусилля криптологів зосереджені на відкритому конкурсі NIST PQC. Основною ідеєю конкурсу NIST PQC є визначення математичних методів, на основі яких можуть бути розроблені стандарти на асиметричні криптоперетворення, в першу чергу електронного підпису, а також асиметричні шифри та протоколи інкапсуляції ключів. За підсумками другого етапу фіналістами третього етапу конкурсу NIST PQC стали три схеми електронного підпису – Crystals-Dilithium, Falcon та Rainbow. Перші дві з них базуються на математиці алгебраїчних решіток, а Rainbow базується на багатовимірних перетвореннях. Наразі всебічний аналіз фіналістів є важливою задачею для усієї світової криптоспільноти. Переважна більшість схем, що стали фіналістами або альтернативним алгоритмами, ґрунтується на проблемах з теорії алгебраїчних решіток. Також особлива увага була приділена схемі електронного підпису Rainbow, що ґрунтується на основі багатовимірних перетворень. Метою даної роботи є попередній аналіз існуючих атак щодо перспективного електронного підпису Rainbow, визначення вимог до загальносистемних параметрів для забезпечення криптографічної стійкості не менше 512 біт включно проти класичного та 256 біт проти квантового криптоаналізу, а також розроблення та практична реалізація щодо Rainbow алгоритмів генерації загальносистемних параметрів для 512 біт проти класичного та 256 біт проти квантового криптоаналізу.

Ключові слова: атаки; багатовимірні перетворення; електронний підпис; загальносистемні параметри; Rainbow.

Табл. 7. Іл. 1. Бібліогр.: 18 назв.

УДК 004.056.55

Генерация общесистемных параметров для схемы электронной подписи Rainbow для 384 и 512 бит безопасности / *М.В. Есина, С.О. Кандий, Е.В. Острянская, И.Д. Горбенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 16 – 23.

Сегодня наблюдается стремительный прогресс в создании квантовых компьютеров по решению вычислительно сложных задач и для различных целей. При этом особые усилия прилагаются к созданию такого квантового компьютера, который сможет решать задачи криптоанализа существующих криптосистем – асимметрич-

ных шифров, протоколов инкапсуляции ключей, электронных подписей и т.д. Предупреждение таких угроз может быть достигнуто средством разработки криптографических систем, которые будут защищены как от квантовых, так и от классических атак, а также смогут взаимодействовать с протоколами и сетями связи, которые уже существуют. Также есть необходимость в защите от атак сторонними каналами. На данный момент значительные усилия криптологов сосредоточены на открытом конкурсе NIST PQC. Основной идеей конкурса NIST PQC является определение математических методов, на основе которых могут быть разработаны стандарты на асимметричные криптопреобразования, в первую очередь электронной подписи, а также асимметричные шифры и протоколы инкапсуляции ключей. По итогам второго этапа финалистами третьего этапа конкурса NIST PQC стали три схемы электронной подписи – Crystals-Dilithium, Falcon и Rainbow. Первые две из них основаны на математике алгебраических решеток, а Rainbow базируется на многомерных преобразованиях. Сейчас всесторонний анализ финалистов является важной задачей для всего мирового криптосообщества. Подавляющее большинство схем, ставших финалистами или альтернативным алгоритмами, основывается на проблемах теории алгебраических решеток. Также особое внимание было уделено схеме подписи Rainbow, основанной на основе многомерных преобразований. Цель данной работы – предварительный анализ существующих атак на перспективную электронную подпись Rainbow, определение требований к общесистемным параметрам для обеспечения криптографической стойкости не менее 512 бит включительно против классического и 256 бит против квантового криптоанализа, а также разработка и практическая реализация для Rainbow алгоритмов генерации общесистемных параметров для 512 бит против классического и 256 бит против квантового криптоанализа.

Ключевые слова: атаки; многомерные преобразования; электронная подпись; общесистемные параметры; Rainbow.

Табл. 7. Ил. 1. Библиогр.: 18 назв.

UDC 004.056.55

Generation of general system parameters for Rainbow electronic signature scheme for 384 and 512 security bits / *M.V. Yesina, S.O. Kandiy, E.V. Ostryanska, I.D. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 16 – 23.

Today, there is rapid progress in the creation of quantum computers to solve various computational problems and for different purposes. At the same time, special efforts are made to create such a quantum computer that can solve the problems of cryptanalysis of existing cryptosystems: asymmetric ciphers, key encapsulation protocols, electronic signatures, etc. Prevention of such threats can be achieved by developing cryptographic systems that will be protected against both quantum and classical attacks, and be able to interact with existing protocols and communication networks. There is also a significant need for protection against attacks by side channels. Currently, significant efforts of cryptologists are focused on the NIST PQC open competition. The main idea of the NIST PQC competition is to define mathematical methods based on which standards for asymmetric cryptotransformations, primarily electronic signatures, as well as asymmetric ciphers and key encapsulation protocols can be developed. Three electronic signature schemes – Crystals-Dilithium, Falcon and Rainbow become the finalists of the third stage of the NIST PQC competition according to the results of the second stage. The first two are based on the mathematics of algebraic lattices, and Rainbow is based on multivariate transformations. Currently, a comprehensive analysis of the finalists is an important task for the entire global crypto community. The vast majority of schemes that have become finalists or alternative algorithms are based on problems in the theory of algebraic lattices. Special attention was also paid to the Rainbow electronic signature scheme based on multivariate transformations. The purpose of this work consists in a preliminary analysis of existing attacks on promising electronic signature Rainbow, definition of requirements to the system-wide parameters to ensure cryptographic stability of at least 512 bits against classical and 256 bits against quantum cryptanalysis, as well as development and practical implementation of Rainbow algorithms for generating system-wide parameters for 512 bits against classical and 256 bits against quantum cryptanalysis.

Key words: attacks; multivariate transformations; electronic signature; general system parameters; Rainbow.

7 tab. 1 fig. Ref: 18 items.

УДК 621.391

Концепція синтезу одного класу самосинхронізуючих дискретних сигналів / *І.Д. Горбенко, О.В. Потій, О.А. Замула* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 24 – 29.

Застосування широкосмугових сигналів (ШСС) дозволяє підвищити завадостійкість перед завадами, що присутні в інформаційно-комунікаційних системах (ІКС). Реальна завадостійкість буде нижчою за потенційну. Причинами зниження завадостійкості при входженні в синхронізм і при розрізненні сигналів є наявність бічних піків кореляційних функцій (КФ). Виходячи з цього, ШСС, що застосовуються в ІКС, повинні володіти такими кореляційними властивостями, коли бічні піки КФ ШПС є якомога меншими, тобто в ідеальному випадку повинні прагнути до нуля. При цьому необхідно визначити вплив бічних піків на характеристики виявлення сигналів, вимірювання їх параметрів, розрізнення сигналів, знайти умови отримання малих бічних піків. Сформульована і у загальному виді вирішена задача синтезу класу сигналів із заданими кореляційними, ансамблевими і структурними властивостями, а також властивостями «розмитості» за кореляційними характеристиками. Зазначена властивість («розмитість») означає, що збільшення або зменшення довжини дискретного сигналу не змі-

нює кореляційні властивості дискретної послідовності, на основі якої синтезовано сигнал. Застосування безлічі зазначених систем сигналів в сучасних інформаційно-комунікаційних системах дозволить поліпшити показники ефективності функціонування таких систем, насамперед завадозахищеності, скритності, інформаційної безпеки, завадостійкості прийому сигналів.

Ключові слова: самосинхронізуючий сигнал; скритність; інформаційна безпека; дискретні послідовності; система нелінійних нерівностей; функція кореляції.

Бібліогр.: 11 назв.

УДК 621.391

Концепция синтеза одного класса самосинхронизирующихся дискретных сигналов / *И.Д. Горбенко, А.В. Потий, А.А. Замула* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 24 – 29.

Применение широкополосных сигналов (ШПС) позволяет повысить помехоустойчивость информационно-коммуникационных систем (ИКС) при воздействии структурных (взаимных) и организованных помех. Реальная помехоустойчивость будет ниже потенциальной. Причинами снижения помехоустойчивости при вхождении в синхронизм и при различении сигналов является наличие боковых пиков корреляционных функций. Исходя из этого применяемые в ИКС ШПС должны обладать такими корреляционными свойствами, когда боковые пики КФ ШПС являются как можно меньшими, т.е. в идеальном случае должны стремиться к нулю. При этом необходимо определить влияние боковых пиков на характеристики обнаружения сигналов, измерения их параметров, различения сигналов, найти условия получения малых боковых пиков. Сформулирована и в общем виде решена задача синтеза класса сигналов с заданными корреляционными, ансамблевыми и структурными свойствами, а также свойствами «размытости» по корреляционным характеристикам. Указанное свойство («размытость») означает, что увеличение или уменьшение длины дискретного сигнала не изменяет корреляционные свойства дискретной последовательности, на основе которой синтезирована сигнал. Применение множества указанных систем сигналов в современных информационно-коммуникационных системах позволит улучшить показатели эффективности функционирования таких систем, прежде всего, помехозащищенности, скрытности, информационной безопасности, помехоустойчивости приема сигналов.

Ключевые слова: самосинхронизирующийся сигнал; скрытность; информационная безопасность; дискретные последовательности; система нелинейных неравенств; функция корреляции.

Библиогр.: 11 назв.

UDC 621.391

The concept of synthesis of one class of self-synchronizing discrete signals / *I.D. Gorbenko, O.V. Potii, A.A. Zamula* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 24 – 29.

The use of broadband signals (BSS) makes it possible to increase the noise immunity of information and communication systems (ICS) when exposed to structural (mutual) and organized interference. The real noise immunity will be lower than the potential one. The reason for the decrease in noise immunity, when entering synchronism and when distinguishing signals, is the presence of side peaks of the correlation functions. Proceeding from this, the NLS used in ICS should have such correlation properties when the side peaks of the NLS CF are as small as possible, i.e. ideally should tend to zero. In this case, it is necessary to determine the influence of side peaks on the characteristics of signal detection, measure their parameters, distinguish signals, and find the conditions for obtaining small side peaks. The problem of synthesizing a class of signals with given correlation, ensemble and structural properties, as well as properties of "blurring" in correlation characteristics, is formulated and solved in general form. The specified property ("fuzziness") means that increasing or decreasing the length of the discrete signal does not change the correlation properties of the discrete sequence on the basis of which the signal is synthesized. The use of many of these signal systems in modern information and communication systems will improve the performance indicators of such systems, first of all, noise immunity, secrecy, information security, noise immunity of signal reception.

Key words: self-synchronizing signal; secrecy; information security; discrete sequences; system of nonlinear inequalities; correlation function.

Ref: 11 items.

УДК 004.056

Аналіз формальних моделей забезпечення цілісності даних і їх застосовність для баз даних / *В.І. Єсін, С.Г. Рассомахін, В.В. Вілігура* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 30 – 39.

Інформаційні системи в цілому і бази даних, зокрема. уразливі для випадкових або зловмисних атак, спрямованих на порушення цілісності даних. Забезпечити безпеку легше, якщо є чітка модель, що представляє собою формальне вираження політики безпеки. У статті досліджуються відомі моделі безпеки, пов'язані із забезпеченням цілісності даних, їх можливість застосування і значення для баз даних. Аналіз формальних моделей забезпечення цілісності даних виявив, що кожна з них, маючи певні переваги і недоліки, має право на використання. Вирішальним фактором у прийнятті рішення є оцінка конкретної ситуації, яка дозволить зробити правильний вибір, в тому числі і комплексного їх застосування. Так в роботі відзначається, що модель Кларка – Вілсона, безумовними перевагами якої є її простота і легкість спільного використання з іншими моделями безпеки, доцільно застосовувати як сукупність практичних рекомендацій з побудови системи забезпечення цілісності в інформаційних системах. Констатуючи факт, що традиційні СУБД підтримують багато механізмів мо-

делі Кларка – Вілсона, автори вказують, що реалізації, засновані на стандартному SQL, вимагають деяких компромісних рішень. Аналіз моделі Біба дозволив зробити висновок про її відносну простоту і використання добре вивченого математичного апарату. Відзначається, що на практиці для створення захищених інформаційних систем як систем, що забезпечують конфіденційність і цілісність даних, важливим є об'єднання моделей Белла – ЛаПадули і Біба, причому об'єднання на основі однієї загальної решітки, але з двома мітками безпеки: за конфіденційністю і за цілісністю, з протилежним характером їх визначення. Саме такий варіант об'єднання моделей Белла – ЛаПадули і Біба рекомендується застосовувати в сучасних інформаційних системах і СУБД, де реалізується мандатна політика безпеки.

Ключові слова: модель безпеки; цілісність даних; інформаційна система; база даних.

Табл. 1. Іл. 4. Бібліогр.: 17 назв.

УДК 004.056

Анализ формальных моделей обеспечения целостности данных и их применимость для баз данных / *В.И. Есин, С.Г. Рассомахин, В.В. Вилигура* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 30 – 39.

Информационные системы в целом и базы данных, в частности, уязвимы для случайных или злонамеренных атак, направленных на нарушение целостности данных. Обеспечить безопасность легче, если имеется четкая модель, представляющая собой формальное выражение политики безопасности. В статье исследуются известные модели безопасности, связанные с обеспечением целостности данных, их возможность применения и значение для баз данных. Анализ формальных моделей обеспечения целостности данных выявил, что каждая из них, имея определенные преимущества и недостатки, имеет право на использование. Решающим фактором в принятии решения является оценка конкретной ситуации, которая позволит сделать правильный выбор, в том числе и комплексного их применения. Так в работе отмечается, что модель Кларка – Вилсона, безусловными достоинствами которой являются ее простота и легкость совместного использования с другими моделями безопасности, целесообразно применять как совокупность практических рекомендаций по построению системы обеспечения целостности в информационных системах. Констатируя факт, что традиционные СУБД поддерживают многие механизмы модели Кларка – Вилсона, авторы указывают, что реализации, основанные на стандартном SQL, требуют некоторых компромиссных решений. Анализ модели Биба позволил сделать вывод о ее относительной простоте и использовании хорошо изученного математического аппарата. Отмечается, что на практике для создания защищенных информационных систем, как систем, обеспечивающих конфиденциальность и целостности данных, важным является объединение моделей Белла – ЛаПадулы и Биба, причем объединение на основе одной общей решетки, но с двумя метками безопасности: по конфиденциальности и по целостности, с противоположным характером их определения. Именно такой вариант объединение моделей Белла – ЛаПадулы и Биба рекомендуется применять в современных информационных системах и СУБД, где реализуется мандатная политика безопасности.

Ключевые слова: модель безопасности; целостность данных; информационная система; база данных.

Табл. 1. Ил. 4. Библиогр.: 17 назв.

UDC 004.056

Analysis of formal models for ensuring data integrity and their applicability to databases / *V.I. Yesin, S.G. Rassomakhin, V.V. Vilihura* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 30 – 39.

Information systems in general and databases in particular are vulnerable to accidental or malicious attacks aimed at compromising data integrity. Security is easier if you have a clear model that is the formal expression of security policy. The paper explores known security models related to data integrity, their applicability and significance for databases. The analysis of formal models for ensuring data integrity revealed that each of them, having certain advantages and disadvantages, has the right to use. The decisive factor in making a decision is an assessment of a specific situation, which will make it possible to make the right choice, including their complex application. In this regard, the paper notes that the Clark-Wilson model, the undoubted advantages of which are its simplicity and ease of joint use with other security models, is advisable to use as a set of practical recommendations for building an integrity assurance system in information systems. While stating the fact that traditional DBMSs support many of the mechanisms of the Clark-Wilson model, the article points out that implementations based on standard SQL require some compromise solutions. Analyzing the Biba model, the paper concludes about its relative simplicity and the use of a well-studied mathematical apparatus. It is noted that in practice, for the creation of secure information systems, as systems that ensure the confidentiality and data integrity, it is important to unite the Bell-LaPadula and Biba models. Moreover, this union should be on the basis of one common lattice, but with two security labels (confidentiality and integrity) with the opposite character of their definition. This is exactly the variant of combining the Bell-LaPadula and Biba models that is recommended for use in modern information systems and DBMSs, where a mandatory security policy is implemented.

Key words: security model; data integrity; information system; database.

1 tab. 4 fig. Ref: 17 items.

УДК 004.056.55

Дослідження та аналіз реалізацій кандидатів другого раунду конкурсу NIST PQC, що орієнтовані на сімейства FPGA Xilinx / *М.В. Єсіна, Б.С. Шахов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 40 – 58.

Сьогодні досить гостро постає питання щодо стійкості сучасних існуючих криптографічних механізмів до квантових алгоритмів криптоаналізу зокрема та квантових комп'ютерів взагалі. Ця проблема активно обговорюється на міжнародному рівні. Тому, задля її вирішення, NIST США вирішив організувати та проводить на сьогодні конкурс на кандидатів на постквантові криптографічні алгоритми NIST PQC. Результатом конкурсу повинне стати прийняття до стандартизації криптографічних алгоритмів різного типу – асиметричне шифрування, інкапсуляція ключів та електронний підпис (як мінімум по одному алгоритму з кожного типу). На момент початку конкурсу на процес стандартизації було представлено 82 алгоритми. На основі критеріїв мінімальної прийнятності, визначених NIST, для 1-го раунду було розглянуто 69 алгоритмів. З урахуванням декількох параметрів – безпека, вартість, продуктивність, характеристики реалізації тощо, – 43 і 11 алгоритмів були виключені при завершенні 1-го і 2-го раундів відповідно, а інші 15 алгоритмів були збережені для 3-го раунду. Алгоритми, які залишилися у 2-му раунді, можна розділити на 5 різних категорій залежно від математичного базису, на якому вони засновуються: на основі ізогеній еліптичних кривих, на основі алгебраїчних решіток, на основі математичного коду, на основі багатовимірних перетворень і на основі геш-функцій. Безпека є основним критерієм оцінки, що визначає конкуренцію в конкурсі NIST, і, зрозуміло, що реалізації програмного забезпечення кандидатів в основному зосереджені на ній. Однак вкрай важливо аби алгоритм мав й ефективну апаратну реалізацію. А своєчасне виявлення апаратної неефективності допоможе сконцентрувати зусилля криптографічної спільноти на більш перспективних кандидатах, потенційно заощадивши велику кількість часу, що може бути витрачена на криптоаналіз. У даній роботі розглядаються та порівнюються між собою FPGA сімейства Xilinx. Наводяться та порівнюються між собою дані щодо реалізацій кандидатів 2-го раунду в процесі стандартизації постквантової криптографії NIST, що орієнтовані на FPGA сімейства Xilinx.

Ключові слова: апаратне забезпечення; електронний підпис; конкурс NIST PQC; постквантова криптографія; FPGA; Xilinx.

Табл. 12. Бібліогр.: 10 назв.

УДК 004.056.55

Исследования и анализ реализаций кандидатов второго раунда конкурса NIST PQC, ориентированных на семейства FPGA Xilinx / *М.В. Есина, Б.С. Шахов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 40 – 58.

Сегодня достаточно остро стоит вопрос о стойкости современных существующих криптографических механизмов к квантовым алгоритмам криптоанализа в частности и квантовым компьютерам вообще. Эта проблема активно обсуждается на международном уровне. Поэтому, для ее решения NIST США решил организовать и проводит конкурс на кандидатов на постквантовые криптографические алгоритмы NIST PQC. Результатом конкурса должно стать принятие к стандартизации криптографических алгоритмов разного типа – асимметричное шифрование, инкапсуляция ключей и электронная подпись (как минимум по одному алгоритму с каждого типа). К началу конкурса на процесс стандартизации было представлено 82 алгоритмы. На основе критериев минимальной приемлемости, определенных NIST, для 1-го раунда было рассмотрено 69 алгоритмов. С учетом нескольких параметров – безопасность, стоимость, производительность, характеристики реализации и т.п., – 43 и 11 алгоритмов были исключены при завершении 1-го и 2-го раундов соответственно, а остальные 15 алгоритмов были сохранены для 3-го раунда. Алгоритмы, которые остались во 2-м раунде, можно разделить на 5 различных категорий в зависимости от математического базиса, на котором они основываются: на основе изогений эллиптических кривых, на основе алгебраических решеток, на основе математического кода, на основе многомерных преобразований и на основе хеш-функций. Безопасность является основным критерием оценки, определяет конкуренцию в конкурсе NIST, и, понятно, что реализации программного обеспечения кандидатов в основном сосредоточены на ней. Однако крайне важно, чтобы алгоритм имел и эффективную аппаратную реализацию. А своевременное выявление аппаратной неэффективности поможет сконцентрировать усилия криптографического сообщества на более перспективных кандидатах, потенциально сэкономив большое количество времени, которое может быть потрачено на криптоанализ. В данной работе рассматриваются и сравниваются между собой FPGA семейства Xilinx. Приводятся и сравниваются между собой данные по реализаций кандидатов 2-го раунда в процессе стандартизации постквантовой криптографии NIST, ориентированные на FPGA семейства Xilinx.

Ключевые слова: аппаратное обеспечение; электронная подпись; конкурс NIST PQC; постквантовая криптография; FPGA; Xilinx.

Табл. 12. Библиогр.: 10 назв.

UDC 004.056.55

Research and analysis of implementations of the NIST PQC competition second round candidates focused on the Xilinx FPGA family / *M.V. Yesina, B.S. Shahov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 40 – 58.

Today, the question of the stability of modern existing cryptographic mechanisms to quantum algorithms of cryptanalysis in particular and quantum computers in general is quite acute. This issue is actively discussed at the interna-

tional level. Therefore, to solve it, NIST USA has decided to organize and is currently holding a competition for candidates for post-quantum cryptographic algorithms NIST PQC. The result of the competition should be the adoption of various types of cryptographic algorithms for standardization, namely, asymmetric encryption, key encapsulation and electronic signature (at least one algorithm of each type). 82 algorithms were submitted by the start of the competition for the standardization process. Based on the minimum eligibility criteria defined by NIST, 69 algorithms were considered for the 1st round. Given several parameters, namely, security, cost, performance, implementation characteristics, etc., 43 and 11 algorithms were excluded at the end of the 1st and 2nd rounds, respectively, and the other 15 algorithms were left for participation in the 3rd round. The algorithms left in the 2nd round can be divided into 5 different categories depending on their mathematical basis: those based on the isogeny of elliptic curves, those based on algebraic lattices, those based on mathematical code, those based on multivariate transformations and those based on hash functions. Security is the main evaluation criterion that determines competition in the NIST competition, and it is clear that candidates' software implementations are focused mainly on it. However, it is extremely important that the algorithm has an effective hardware implementation. Timely identification of hardware inefficiencies will help focus the cryptographic community efforts on more promising candidates, potentially saving a large amount of time that can be spent on cryptanalysis. This paper discusses and compares the FPGAs of Xilinx family. Data on the implementation of the candidates of the 2nd round in the process of standardization of post-quantum cryptography NIST, which are focused on the FPGA of the Xilinx family, are presented and compared.

Key words: hardware; electronic signature; NIST PQC competition; post-quantum cryptography; FPGA; Xilinx.
12 tab. Ref: 10 items.

УДК 003.026:004.056

Аналіз складності атак на мультиваріативні криптографічні перетворення з використанням алгебраїчної структури поля / *С.О. Кандій, Г.А. Малєєва* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 59 – 65.

В останні роки інтерес до криптосистем, що ґрунтуються на багатовимірних квадратичних перетвореннях (MQ-перетвореннях), значно зріс. В першу чергу це пов’язано з конкурсом NIST PQC [1] та необхідністю у практичних схемах електронного підпису, що є стійкими до атак на квантових комп’ютерах. Незважаючи на те, що світовою спільнотою була проведена велика робота з криптоаналізу представлених схем, багато питань потребують подальшого уточнення. Спеціалісти NIST дуже обережно підходять до процесу стандартизації і закликають криптологів [4] у найближчі три роки провести всесторонній аналіз фіналістів конкурсу NIST PQC перед їх стандартизацією.

Одним з фіналістів є схема електронного підпису Rainbow [2]. Вона є узагальненням схеми UOV (Unbalanced Oil and Vinegar) [3]. Нещодавно на інше узагальнення цієї схеми – LUOV (Lifted UOV) [5] була знайдена атака [6], що за поліноміальний час здатна повністю відновити закритий ключ. Особливістю цієї атаки є використання алгебраїчної структури поля, над яким задане MQ-перетворення. Цей напрямок атак з’явився нещодавно і досі не зрозуміло чи можливо використовувати структуру поля у схемі Rainbow.

Метою цієї роботи є систематизація технік, що використовуються у атаках з використанням алгебраїчної структури поля для криптосистем на основі UOV та аналіз перешкод для їх узагальнення на схему Rainbow.

Ключові слова: класичний та квантовий криптоаналіз; диференційні атаки на підполе; аналіз атак; постквантовий період.
Бібліогр.: 8 назв.

УДК 003.026:004.056

Анализ сложности атак на мультивариативные криптографические преобразования с использованием алгебраической структуры поля / *С.О. Кандий, А.А. Малеева* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 59 – 65.

В последние годы интерес к криптосистемам, основанным на многомерных квадратичных преобразованиях (MQ-преобразованиях), значительно возрос. В первую очередь это связано с конкурсом NIST PQC [1] и необходимостью в практических схемах электронной подписи, которые являются стойкими к атакам на квантовых компьютерах. Несмотря на то, что мировым сообществом была проведена большая работа по криптоанализу представленных схем, многие вопросы требуют дальнейшего уточнения. Специалисты NIST очень осторожно подходят к процессу стандартизации и призывают криптологов [4] в ближайшие 3 года провести всесторонний анализ финалистов конкурса NIST PQC перед их стандартизацией.

Один из финалистов схема электронной подписи Rainbow [2]. Она является обобщением схемы UOV (Unbalanced Oil and Vinegar) [3]. Недавно на другое обобщение этой схемы – LUOV (Lifted UOV) [5] была найдена атака [6], которая за полиномиальное время способна полностью восстановить закрытый ключ. Особенностью этой атаки является использование алгебраической структуры поля, над которым задано MQ-преобразования. Это направление атак появилось недавно и до сих пор не понятно возможно ли использовать структуру поля в схеме Rainbow.

Целью настоящей работы является систематизация техник, используемых в атаках с использованием алгебраической структуры поля для криптосистем на основе UOV, и анализ препятствий для их обобщения на схему Rainbow.

Ключевые слова: классический и квантовый криптоанализ; дифференциальные атаки на подполе; анализ атак; постквантовий период.

Библиогр.: 8 назв.

UDC 003.026:004.056

Analysis of the complexity of attacks on multivariate cryptographic transformations using algebraic field structure / *S. Kandiy, G. Maleeva* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 59 – 65.

In recent years, interest in cryptosystems based on multidimensional quadratic transformations (MQ transformations) has grown significantly. This is primarily due to the NIST PQC competition [1] and the need for practical electronic signature schemes that are resistant to attacks on quantum computers. Despite the fact that the world community has done a lot of work on cryptanalysis of the presented schemes, many issues need further clarification. NIST specialists are very cautious about the standardization process and urge cryptologists [4] in the next 3 years to conduct a comprehensive analysis of the finalists of the NIST PQC competition before their standardization.

One of the finalists is the Rainbow electronic signature scheme [2]. It is a generalization of the UOV (Unbalanced Oil and Vinegar) scheme [3]. Recently, another generalization of this scheme – LUOV (Lifted UOV) [5] was found to attack [6], which in polynomial time is able to recover completely the private key. The peculiarity of this attack is the use of the algebraic structure of the field over which the MQ transformation is given. This line of attack has emerged recently and it is still unclear whether it is possible to use the field structure in the Rainbow scheme.

The aim of this work is to systematize the techniques used in attacks using the algebraic field structure for UOV-based cryptosystems and to analyze the obstacles for their generalization to the Rainbow scheme.

Key words: classical and quantum cryptanalysis; differential attacks on the underground; attack analysis; postquantum period.

Ref: 8 items.

УДК 621.391:519.2

Деякі результати розробки схем криптографічних перетворень з використанням неабелевих груп / *Є.В. Котух, О.В. Северинов, А.В. Власов, А.О. Теницька, Е. О. Зарудна* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 66 – 72.

З появою практичних результатів в реалізації алгоритмів Шора і Гровера на квантових комп'ютерах реалізація успішної атаки на класичні криптосистеми з відкритим ключем стає дедалі реальною. Сучасні результати у вирішенні завдання побудови квантового комп'ютера достатньої потужності обґрунтовують необхідність до перегляду існуючих підходів і визначення найбільш ефективних, з точки зору вирішення завдань постквантової криптографії. Одним з таких перспективних дослідницьких пріоритетів є дослідження криптосистем на основі неабелевих груп.

Проблеми пошуку пов'язаності, пошуку членства й інші варіанти є складно вирішувані в теорії неабелевих груп і є основою для побудови доказово безпечних криптосистем з відкритим ключем. В роботі надано огляд найбільш часто обговорюваних алгоритмів з використанням неабелевих груп: групи матриць, групи кіс, напівпрямі добутки і алгебраїчні ластики (AE). Наведено аналіз побудови схем шифрування і дешифрування, механізмів обміну ключами. Багато неабелевих протоколів встановлення ключів на основі груп пов'язані з протоколом Діффі – Хеллмана (DH). В роботі проаналізовано властивості неабелевих групових схем шифрування з відкритим ключем. Розглядаються різні криптографічні примітиви, які використовують некомутативні групи в якості основи для постквантових схем.

Ключові слова: постквантова криптографія; напівпрямі добутки; групи матриць; групи кіс; логарифмічні підписи; алгебраїчний ластик.

Бібліогр.: 22 назв.

УДК 621.391:519.2

Некоторые результаты разработки схем криптографических преобразований с использованием неабелевых групп / *Е.В. Котух, А.В. Северинов, А.В. Власов, А.А. Теницкая, Е. А. Зарудная* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 66 – 72.

С появлением практических результатов в реализации алгоритмов Шора и Гровера на квантовых компьютерах, реализация успешной атаки на классические криптосистемы с открытым ключом становится все более реальной. Современные результаты в решении задачи построения квантового компьютера достаточной мощности обосновывают необходимость к пересмотру существующих подходов и определению наиболее эффективных с точки зрения решения задач постквантовой криптографии. Одним из таких перспективных исследовательских приоритетов является исследование криптосистем на основе неабелевых групп.

Проблемы поиска сопряженности, поиска членства и другие варианты являются сложно решаемыми в теории неабелевых групп и являются основой для построения доказуемо безопасных криптосистем с открытым ключом. В работе дается обзор наиболее часто обсуждаемых алгоритмов с использованием неабелевых групп: группы матриц, группы кос, полупрямые произведения и алгебраические ластики (AE). Приводится анализ построения схем шифрования и дешифрования, механизмов обмена ключами. Многие неабелевы протоколы установления ключей на основе групп связаны с протоколом Диффи – Хеллмана (DH). В работе анализируются

свойства неабелевых групповых схем шифрования с открытым ключом. Рассматриваются различные криптографические примитивы, использующие некоммутативные группы в качестве основы для постквантовых схем.

Ключевые слова: постквантовая криптография; полупрямые произведения; группы матриц; группы кос; логарифмические подписи; алгебраический ластик.

Библиогр.: 22 назв.

UDC 621.391:519.2

Towards results of cryptographic transformations schemes development with application of nonabelian groups / *E.V. Kotukh, O.V. Severinov, A.V. Vlasov, A.O. Tenytska, E.O. Zarudna* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 66 – 72.

The implementation of a successful attack on classical public key cryptosystems becomes real with the advent of practical results in the implementation of Shor's and Grover's algorithms on quantum computers. Modern results in solving the problem of the powerful enough quantum computer construction substantiate the need to revise the existing approaches and determine the most effective from the post-quantum cryptography point of view. One of these promising research priorities is the study of cryptosystems based on non-abelian groups.

The problems of conjugacy search, membership search, and others are difficult to solve in the theory of non-abelian groups and can be considered as a basis for constructing provably secure public key cryptosystems. This paper gives an overview of the most frequently discussed algorithms using non-abelian groups: matrix groups, braid groups, semidirect products, and algebraic erasers (AE). The analysis of the construction of encryption and decryption schemes, key establishment mechanisms is given. Many non-abelian group-based key establishment protocols are associated with the Diffie – Hellman (DH) protocol. The paper analyzes the properties of non-abelian group public key encryption schemes. Various cryptographic primitives are considered that using non-commutative groups as a basis for post-quantum schemes.

Key words: post-quantum cryptography; semidirect products; matrix groups, braid groups; logarithmic signatures; algebraic eraser.

Ref: 22 items.

РАДІОТЕХНІЧНІ ТА ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ ТА СИСТЕМИ
РАДИОТЕХНИЧЕСКИЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ
RADIO AND TELECOMMUNICATION NETWORKS AND SYSTEMS

УДК 621.3.006.357

Метод оптимізації розподілу частотного ресурсу з повторним використанням частот для систем когнітивного радіо / *Ю.Ю. Коляденко, О.В. Коляденко, Б.П. Муляр* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 73 – 79.

Концепція когнітивного радіо може бути охарактеризована як радіо з вивченням можливостей, тобто як радіо, яке в змозі отримати знання про радіосередовище і коригувати свої експлуатаційні параметри і протоколи відповідно.

На етапі функціонування мережі когнітивного радіо при розподілі частотного ресурсу між абонентськими станціями актуальною є задача мінімізації смуги частот. В умовах постійно зростаючого попиту на смуги частот постановка такого завдання обумовлена необхідністю підвищення ефективного використання радіочастотного спектру із застосуванням методів повторного використання частот.

В роботі запропонований метод забезпечення повторного використання частот, заснований на отриманні оцінок взаємних відстаней між абонентськими станціями в реальному масштабі часу. Запропоновано алгоритм розв'язання задачі оптимізації розподілу частотного ресурсу для мережі когнітивного радіо з повторним використанням частот. В основі алгоритму лежить метод локальної оптимізації – один з наближених методів дискретного програмування. В даному випадку умовою локальної оптимальності є те, що робоча частота, яка присвоюється черговій абонентській станції, повинна бути найближчою до присвоєної на попередньому кроці частоті.

За допомогою імітаційного моделювання проведено аналіз ефективності алгоритму оптимізації розподілу частотного ресурсу для мережі LTE. Отримано залежності ширини смуги частот від кількості абонентських станцій, що обслуговуються. Аналіз показав, що використання даного алгоритму дозволяє в 2 – 3 рази скоротити смугу частот. Також аналіз показав, що з ростом числа абонентських станцій, які одночасно обслуговуються, ефективність алгоритму підвищується.

Ключові слова: розподіл частотного ресурсу; мережа когнітивного радіо; повторне використання частот.

Іл. 7. Бібліогр.: 9 назв.

УДК 621.3.006.357

Метод оптимизации распределения частотного ресурса с повторным использованием частот для систем когнитивного радио / *Ю.Ю. Коляденко, А.В. Коляденко, Б.П. Муляр* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 73 – 79.

Концепция когнитивного радио может быть охарактеризована как радио с изучением возможностей, то есть как радио, которое в состоянии получить знания о радиосреде и корректировать свои эксплуатационные параметры и протоколы соответственно.

На этапе функционирования сети когнитивного радио при распределении частотного ресурса между абонентскими станциями актуальна задача минимизации полосы частот. В условиях постоянно растущего спроса на полосы частот постановка такой задачи обусловлена необходимостью повышения эффективного использования радиочастотного спектра с применением методов повторного использования частот.

В работе предложен метод обеспечения повторного использования частот, основанный на получении оценок взаимных расстояний между абонентскими станциями в реальном масштабе времени. Предложен алгоритм решения задачи оптимизации распределения частотного ресурса для сети когнитивного радио с повторным использованием частот. В основе алгоритма лежит метод локальной оптимизации – один из приближенных методов дискретного программирования. В данном случае условием локальной оптимальности является то, что рабочая частота, присваиваемая очередной абонентской станции, должна быть ближайшей к присвоенной на предыдущем шаге частоте.

С помощью имитационного моделирования проведен анализ эффективности алгоритма оптимизации распределения частотного ресурса для сети LTE. Получены зависимости ширины полосы частот от количества обслуживаемых абонентских станций. Анализ показал, что использование данного алгоритма позволяет в 2 – 3 раза сократить полосу частот. Также анализ показал, что с ростом числа абонентских станций, которые одновременно обслуживаются, эффективность алгоритма повышается.

Ключевые слова: распределение частотного ресурса; сеть когнитивного радио; повторное использование частот.

Ил. 7. Библиогр.: 9 назв.

UDC 621.3.006.357

Method for optimization of frequency resource allocation with frequency reuse for cognitive radio systems / *Yu.Yu. Kolyadenko, O.B. Kolyadenko, B.P. Mulyar* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 73 – 79.

The concept of cognitive radio can be described as a radio with the study of capabilities, i.e. as a radio that is able to gain knowledge about the radio environment and adjust its operating parameters and protocols accordingly.

The task of minimizing the frequency band is relevant at the stage of the cognitive radio network functioning when distributing the frequency resource between subscriber stations. With the ever-growing demand for frequency bands, this challenge is driven by the need to improve the efficient use of the radio frequency spectrum through frequency reuse methods.

This paper proposes a method for ensuring the reuse of frequencies based on obtaining estimates of mutual distances between subscriber stations in real time. An algorithm is proposed for solving the problem of frequency resource allocation optimization for a cognitive radio network with frequency reuse. The algorithm is based on the method of local optimization, one of the approximate methods of discrete programming. In this case, the condition of local optimality is that the operating frequency assigned to the next subscriber station must be the closest to the frequency assigned in the previous step.

The efficiency of the frequency resource optimization algorithm for the LTE network was analyzed using simulation modeling. The dependences of the bandwidth on the number of subscriber stations served are obtained. The analysis showed that the use of this algorithm allows to reduce the frequency band by 2 -3 times. The analysis also showed that the efficiency of the algorithm increases with the growth of the number of subscriber stations served simultaneously.

Key words: frequency resource allocation; cognitive radio network; frequency reuse.

7 fig. Ref: 9 items.

УДК 355.457.2:358.11.6 (043.3)

Архітектура сітьової бази знань складної системи воєнного призначення / *М.О. Єрмошин, А.А Побережний, О.С. Онопрієнко, М.П. Шурига* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 80 – 92.

Розглядається архітектура сітьової бази знань та організаційна структура складної системи воєнного призначення, що будується при створенні угруповання військ (сил) та підтриманні його у стані, коли воно здатне вирішувати покладені на нього завдання. Це вимагає глибокого розроблення питань не тільки сучасної тактики щодо підготовки та ведення бойових дій, а й ще більш складних питань наукового обґрунтування архітектури сітьової бази знань та структури складної системи воєнного призначення з сітьовою базою знань. Внутрішню уяву знань у базі знань (формальний програмно-логічний зміст) доцільно реалізовувати у вигляді матриці суміжності, що відображає відношення та взаємозв'язок між цільовими установами; початковими умовами; ресурсами угруповання військ (часовими, матеріальними, бойовими та кількісного складу), їх витратами та поповненням; правил витрати ресурсів і вибору критеріїв їх розподілу. У базі знань здійснюється синтез математичної сітьової моделі вироблення рішень, що забезпечує зміну (корекцію) структури цільових установок при поповненні бази знань. Задачі, що розв'язуються у базі знань, такі: виділення вершин і відношень при поповненні

каталогів; внесення зміни до матриці суміжності у відповідності до виявлених або змінених відношень між цільовими установками. Необхідним елементом синтезу математичної сітьової моделі вироблення рішень щодо підготовки та ведення бойових дій є побудова структури цільових установок системи для конкретної ситуації. Особливістю контролю коректності знань, що надані у вигляді цільових установок, є необхідність сумісного аналізу всієї сукупності цільових установок і початкових умов у їх взаємозв'язку. Для цього здійснюється об'єднання матриці відношень цільових установок і матриці відношень початкових умов. Контроль коректності бази знань здійснюється при поповненні бази знань, він включає: виявлення протиріч в структурі цільових установок при внесенні змін в цю структуру; пошук та виявлення протиріч графу семантичної мережі згідно наявним ресурсам і часу; перевірку повноти графу математичної сітьової моделі; видачу виявлених протиріч експерту та їх усунення. Практичний підхід щодо побудови архітектури сітьової бази знань та організаційної структури складної системи воєнного призначення може бути реалізований під час обґрунтування компонентів та елементів системи при створенні угруповання військ (сил).

Ключові слова: структура системи воєнного призначення; сітьова база знань.

Іл. 3. Бібліогр.: 12 назв.

УДК 355.457.2:358.11.6 (043.3)

Архитектура сетевой базы знаний сложной системы военного назначения / *М.А. Ермошин, А.А Побережный, А.С. Оноприенко, М.П. Шурыга* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 80 – 92.

Рассматривается архитектура сетевой базы знаний и организационная структура сложной системы военного назначения, которая строится при создании группировки войск (сил) и поддержании ее в состоянии, когда она способна решать возложенные на нее задачи. Это требует глубокой проработки вопросов не только современной тактики относительно подготовки и ведения боевых действий, но и более сложных вопросов научного обоснования архитектуры сетевой базы знаний и структуры сложной системы военного назначения с сетевой базой знаний. Внутреннее представление знаний в базе знаний (формальное программно-логическое содержание) целесообразно реализовывать в виде матрицы смежности, которая отображает отношения и взаимосвязь между целевыми установками; начальными условиями; ресурсами группировки войск (временными, материальными, боевыми и количественного состава), их затратами и пополнением; правилами расходования ресурсов и выбора критериев их распределения. В базе знаний осуществляется синтез математической сетевой модели выработки решений, которая обеспечивает изменение (коррекцию) структуры целевых установок при пополнении базы знаний. Задачи, решаемые в базе знаний: выделение вершин и отношений при пополнении каталогов; внесение изменений в матрицу смежности в соответствии с выявленными или измененными отношениями между целевыми установками. Необходимым элементом синтеза математической сетевой модели выработки решений по подготовке и ведению боевых действий является построение структуры целевых установок системы для конкретной ситуации. Особенностью контроля корректности знаний, представленных в виде целевых установок, есть необходимость совместного анализа всей совокупности целевых установок и начальных условий в их взаимосвязи. Для этого осуществляется объединение матрицы отношений целевых установок и матрицы отношений начальных условий. Контроль корректности базы знаний осуществляется при пополнении базы знаний, он включает: выявление противоречий в структуре целевых установок при внесении изменений в эту структуру; поиск и обнаружение противоречий в графе семантической сети согласно располагаемым ресурсам и времени; проверку полноты графа математической сетевой модели; выдачу выявленных противоречий эксперту и их устранение. Практический подход относительно построения архитектуры сетевой базы знаний и организационной структуры сложной системы военного назначения может быть реализован во время обоснования компонентов и элементов системы при создании группировки войск (сил).

Ключевые слова: структура системы военного назначения; сетевая база знаний.

Ил. 3. Библиогр.: 12 назв.

UDC 355.457.2:358.11.6 (043.3)

Architecture of network knowledge base of a complex military system / *M. Yermoshyn, A. Poberezhnyi, O. Onopriyenko, M. Shuryha* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 80 – 92.

The article examines the architecture of a networked knowledge base and the organizational structure of a complex military-purpose system, which is built when a group of troops (forces) is created and kept in a state where it is capable of solving the tasks assigned to it. This requires a deep study of issues not only of modern tactics regarding the preparation and conduct of hostilities, but also more complex issues of scientific substantiation of the architecture of a networked knowledge base and the structure of a complex military system with a networked knowledge base. The internal representation of knowledge in the knowledge base (formal programmatic and logical content) is advisable to implement in the form of an adjacency matrix, which displays the relationship and relationship between target settings; initial conditions; the resources of the grouping of troops (temporary, material, combat and quantitative composition), their costs and replenishment; rules for the use of resources and the choice of criteria for their distribution. The knowledge base synthesizes a mathematical network model for making decisions, which provides a change (correction) of the structure of target attitudes when replenishing the knowledge base. Tasks solved in the knowledge base: selection of vertices and relations when replenishing catalogs; making changes to the adjacency matrix in accordance with the identified or changed relationships between targets. A necessary element of the synthesis of a mathematical network model for making decisions on the preparation and conduct of hostilities is the construction of the structure of the target

systems of the system for a specific situation. A feature of controlling the correctness of knowledge presented in the form of target attitudes is the need for a joint analysis of the entire set of target attitudes and initial conditions in their relationship. For this, the matrix of the relations of target attitudes and the matrix of the relations of initial conditions are combined. The control of the correctness of the knowledge base is carried out when replenishing the knowledge base, it includes: identification of contradictions in the structure of target attitudes when making changes to this structure; search and detection of contradictions in the graph of the semantic network according to available resources and time; checking the completeness of the graph of the mathematical network model; issuance of revealed contradictions to an expert and their elimination. A practical approach to building the architecture of a networked knowledge base and the organizational structure of a complex military system can be implemented during the substantiation of the components and elements of the system when creating a grouping of troops (forces).

Key words: structure of the military system; network knowledge base.

3 fig. Ref: 12 items.

УДК 621.396

Про ефект Доплера в радіолокації / *О.В. Рязанцев, С.В. Марченко, М.В. Кулик* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 93 – 98.

Аналізуються можливості одночасного використання поздовжнього і поперечного ефектів Доплера, а також отримано вирази відповідних частот биття між випромінюваним і прийнятим сигналами.

Як правило, в сучасних радіотехнічних системах використовується тільки поздовжній ефект Доплера, що дозволяє визначити радіальну складову швидкості руху об'єкта. Крім того, існують ситуації, для яких взагалі неможливо визначити швидкість об'єкта без урахування поперечного ефекту Доплера.

В роботі проведено аналіз принципових можливостей вдосконалення функціонування радіолокаційних станцій, одночасно використовуються обидва типи ефектів Доплера – поздовжній і поперечний, що дозволяє визначити повну швидкість об'єкта, що спостерігається в будь-яких ситуаціях.

Проаналізовано поздовжній і поперечний ефекти Доплера для випадку рухомого об'єкта, що випромінює, та отримано вирази для доплерівського зсуву, а також визначено вирази частоти биття в разі активної радіолокаційної станції для обох видів ефектів Доплера, що дозволяють отримати величину швидкості об'єкта в будь-яких ситуаціях.

Запропоновано варіанти визначення повної швидкості рухомого об'єкту з урахуванням визначення її радіальної і тангенціальної компонент. Розглянуто ідеалізовані ситуації, в яких проявляється тільки один з ефектів Доплера.

Ключові слова: поперечний та повздовшній ефекти Доплера; швидкість об’єкта; радіолокаційна станція; система відліку.

Іл. 5. Бібліогр.: 5 назв.

УДК 621.396

Об эффекте Доплера в радиолокации / *О.В. Рязанцев, С.В. Марченко, М.В. Кулик* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 93 – 98.

Анализируются возможности одновременного использования продольного и поперечного эффектов Доплера, а также получены выражения соответствующих частот биений между излучаемым и принимаемым сигналами.

Как правило, в современных радиотехнических системах используется только продольный эффект Доплера, позволяющий определить радиальную составляющую скорости движения объекта. Кроме того, существуют ситуации, для которых вообще невозможно определить скорость объекта без учета поперечного эффекта Доплера.

Проведен анализ принципиальных возможностей совершенствования функционирования радиолокационных станций, одновременно использующих оба типа эффектов Доплера – продольный и поперечный, что позволяет определить полную скорость наблюдаемого объекта в любых ситуациях.

Авторами проанализированы продольный и поперечный эффекты Доплера для случая движущегося излучающего объекта, получены выражения для доплеровского сдвига, а также определены выражения частоты биений в случае активной радиолокационной станции для обоих видов эффектов Доплера, позволяющие получить величину скорости объекта в любых ситуациях.

Предложены варианты определения полной скорости движущегося объекта с учетом определения ее радиальной и тангенциальной компонент. Рассмотрены идеализированные ситуации, в которых проявляется только один из эффектов Доплера.

Ключевые слова: поперечный и продольный эффекты Доплера; скорость объекта; радиолокационая станция; система отсчета.

Ил. 5. Библиогр.: 5 назв.

UDC 621.396

On the Doppler effect in radar / *O.V. Ryazantsev, S.V. Marchenko, M.V. Kulik* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 93 – 98.

The possibilities of simultaneous use of the longitudinal and transverse Doppler effects have been analyzed, and expressions have been derived for the corresponding beat frequencies between the emitted and received signals.

As a rule, only the longitudinal Doppler effect is used in modern radio engineering systems, which makes it possible to determine the radial component of the object's speed. In addition, there are situations for which it is generally impossible to determine the speed of an object without taking into account the transverse Doppler effect.

The authors analyze the fundamental possibilities of improving the functioning of radar stations that simultaneously use both types of Doppler effects – longitudinal and transverse ones – making it possible to determine the total speed of the observed object in any situations.

The authors have analyzed the longitudinal and transverse Doppler effects for the case of a moving emitting object, derived expressions for the Doppler shift and expressions for the beat frequency in the case of an active radar station for both types of Doppler effects, which make it possible to obtain the value of the object's speed in any situations.

Variants of determining the total speed of a moving object have been proposed, accounting the determination of its radial and tangential components. Idealized situations in which only one of the Doppler effects appeared have been considered.

Key words: the longitudinal and transverse Doppler effects; object speed; radar station; reference system

5 fig. Ref: 5 items.

УДК 621.391.5: 004.056.53

Підслуховування NFC-зв'язку на частотах вищих гармонік / *В.Г. Крижановський, С.П. Сергієнко, Д.В. Чернов, В.В. Крижановський* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 99 – 104.

Широке використання технології NFC-комунікації у близькому полі спонукає розглядати різні аспекти безпеки її використання. Відомі приклади обміну інформацією з карткою на відстані, яка значно більше ніж типові максимальні 5 – 10 см. Також привертає увагу можливість отримати сигнал з картки на частотах вищих гармонік, які потенційно можуть випромінюватися у вигляді електромагнітних хвиль, а не тільки існувати як індуктивне поле котушки зв'язку. В роботі досліджено випромінювання третьої гармоніки частоти 13,36 МГц карткою стандарту ISO 14443-3A у різних режимах збудження, – за допомогою пристрою RFID-RC522, смартфона Sony Xperia Z5 Premium та сигналом 13,36 МГц з прямокутною модуляцією 10 % на частоті піднесучої відповіді картки 847,5 кГц. В програмі аналізу електронних схем проведено моделювання відгуку картки в діапазоні третьої гармоніки. І моделювання і експеримент підтвердили, що найбільшим сигналом (крім основного) є сигнал на частоті третьої гармоніки та її бокових частотах 40,68 ± 0,8475 МГц. Для прийому сигналу на частоті третьої гармоніки було виготовлено резонансну антену у вигляді кільцевого вібратора, що навантажений на ємність. Це дозволяє зменшити розміри приймальної системи, хоча проблема складної взаємодії електромагнітних полів та антенних структур у ближній зоні залишається відкритою. За результатами вимірювання характеристик імпедансу цієї антени було визначено її вузьку смугу частот, що ускладнює прийом сигналу відповіді картки. Експерименти з використання трьох методів генерації сигналу відповіді картки показали, що сигнал третьої гармоніки реєструється на відстані більше 1,5 м, що може скласти загрозу для безпеки транзакцій за допомогою платіжних банківських карт. Разом з тим, великий вплив шуму при такій відстані може зробити неможливим детектування короткочасного сигналу від картки, що потребує додаткового вивчення.

Ключові слова: NFC пристрої; RFID пристрої; вищі гармоніки робочої частоти; спектральний склад випромінювання; кібербезпека.

Табл. 1. Іл. 12. Бібліогр.: 11 назв.

УДК 621.391.5: 004.056.53

Прослушивание NFC-связи на частотах высших гармоник / *В.Г. Крыжановский, С.П. Сергиенко, Д.В. Чернов, В.В. Крыжановский* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 99 – 104.

Широкое использование технологии NFC-коммуникации в ближнем поле вызывает интерес к различным аспектам безопасности ее использования. Известны примеры обмена информацией с карточкой на расстоянии большем, чем стандартные 5–10 см. Также интересна возможность использовать сигналы высших гармоник, которые потенциально могут излучаться в виде электромагнитных волн, а не только существовать как индуктивное поле рассеяния. В работе исследовано излучение третьей гармоники частоты 13,56 МГц карточкой стандарта ISO 14443-3A в разных режимах возбуждения, – с помощью устройства RFID-RC522, смартфона Sony Xperia Z5 Premium и сигналом 13,56 с прямоугольной модуляцией 10 % на частоте поднесущего ответа карточки 847,5 кГц. В программе анализа электронных схем промоделировано отклик карточки в диапазоне третьей гармоники. И моделирование, и эксперимент подтвердили, что наибольшим сигналом (кроме сигнала на основной частоте) есть сигнал на частоте третьей гармоники и ее боковых частотах 40,68 ± 0,8475 МГц. Для приема сигнала на частоте третьей гармоники была изготовлена резонансная антенна в виде кольцевого вибратора, нагруженного на емкость. Это позволяет уменьшить размеры приемной системы, но остается проблема сложной структуры полей в ближней зоне излучающих структур. При измерении входного импеданса антенны отмечена ее узкая полоса рабочих частот, что затрудняет регистрацию сигнала ответа карточки. Эксперименты с исполь-

зованием трех методов генерации сигнала подтвердили, что сигнал третьей гармоники регистрируется на расстоянии больше 1,5 м, что может представлять угрозу для безопасности транзакций с помощью бесконтактных карт. Вместе с тем, влияние высокого уровня шума на таком расстоянии может сделать невозможным декодирование кратковременного сигнала от карточки, что требует дополнительного изучения.

Ключевые слова: NFC устройства; RFID метки; высшие гармоники рабочей частоты; спектральный состав излучения; кибербезопасность.

Табл. 1. Ил. 12. Библиогр.: 11 назв.

UDC 621.391.5: 004.056.53

Listening to NFC at higher harmonic frequencies / *V.G. Kryzhanovskyi, S.P. Serhiienko, D.V. Chernov, V.V. Kryzhanovskyi* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 99 – 104.

The widespread use of the NFC technology (Near Field Communication) arouses interest to various security aspects. There are known examples of information exchange with card at a distance greater than standard 5-10 cm. It is also interesting to use signals of higher harmonics, which potentially may be radiated in the form of electromagnetic waves, rather than exists as a magnetic field of scattering. In this work, the radiation of third harmonic by card of standard ISO 14443-3A with the fundamental frequency 13.56 MHZ for various excitation modes using the RFID-RC522 reader, smartphone Sony Xperia Z5 Premium, and continuous 10% amplitude modulated 13.56 MHz signal from generator with the subcarrier of imitated smart card response 847.5 kHz was investigated. The card response at third harmonic was simulated in circuit analysis software. Both simulation and experiment proved, that the third harmonic with its side frequencies 40,68 ± 0,8475 MHz have the highest level after the fundamental. To receive the third harmonic signal, the resonant loop antenna in the form of ring vibrator loaded on capacitor was used. This allows the sizes of the received system to be reduced, but the problem of complex field structure in the near-field zone remains. Due to narrow bandwidth of the receiver antenna, the registration of card response signal was complicated. The experiments with three methods of signal generation proved, that third-harmonic signal is registered at the distance more than 1.5m, which may pose a threat for contactless smart-cards transactions security. At the same time, the influence of high level of noise at such a distance may cause difficulties to decode the short-duration signals, which requires further study.

Key words: NFC devices; RFID devices; higher operating frequency harmonics; radiation spectrum; cybersecurity.

1 tab. 12 fig. Ref: 11 items.

ФІЗИКА ПРИЛАДІВ ТА СИСТЕМ
ФИЗИКА ПРИБОРОВ И СИСТЕМ
PHYSICS OF INSTRUMENTS AND SYSTEMS

УДК 621.793:678.073

Дисперсія наночасток в оптично прозорі полімерні матриці / *В.М. Борщов, О.М. Лістратенко, М.А. Проценко, І.Т. Тимчук, О.В. Кравченко, О.В. Суддя, М.І. Сліпченко, Б.М. Чічков* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 105 – 114.

Проведено пошук і аналіз даних, результатів теоретичних і експериментальних досліджень, матеріалів дисертацій, літературних джерел та патентів в області оптичного і оптико-електронного приладобудування. Узагальнено отримані дані та рекомендації з розробки методів дисперсії наночасток в полімерні матриці при створенні оптично прозорих нанокомпозитів для застосування у багатьох областях науки та техніки. Аналіз розглянутих робіт дозволяє зробити висновок, що для створення гібридних органо-неорганічних композитів з високим рівнем дисперсності неорганічного компоненту доводиться вирішувати проблеми, пов'язані з сумісністю компонент і стабілізацією наночасток наповнювача в полімерній матриці. У зв'язку з обмеженою кількістю гідрофільних полімерів, здатних до формування композитів з наночастками без стабілізаторів, основними підходами до отримання гібридних композитів є використання модифікуючих добавок поверхнево активних речовин, а також проведення складних хімічних реакцій на поверхні наночасток неорганічного наповнювача. Дані способи отримання нанокомпозитів з наночастками трудомісткі пов'язані з утворенням побічних продуктів і додатковим очищенням. Показано, що серед великої кількості нанодисперсних наповнювачів полімерних матриць при отриманні композиційних матеріалів великою увагою користуються діоксид титану (TiO_2) і оксид цинку (ZnO). Існує безліч методів синтезу наночасток ZnO та TiO_2 з різними формами і розмірами, в тому числі метод лазерної абляції, який є зручним і універсальним способом отримання наносуспензій твердофазних матеріалів в рідині. Переваги перед іншими способами синтезу наночасток, як простота методу, екологічність, низька вартість і можливість отримувати більш чисті колоїдні розчини без використання поверхнево-активних речовин та інших домішок, зробили лазерну абляцію в рідкому середовищі популярною серед дослідників.

Ключові слова: дисперсія наночасток; наноматеріали; оптично прозорі полімерні матриці.

Іл. 3. Бібліогр.: 23 назв.

УДК 621.793:678.073

Дисперсия наночастиц в оптически прозрачные полимерные матрицы / *В.Н. Борщев, А.М. Листратенко, М.А. Проценко, И.Т. Тымчук, А.В. Кравченко, А.В. Судья, Н.И. Слипченко, Б.Н. Чичков* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 105 – 114.

Проведен поиск и анализ данных, результатов теоретических и экспериментальных исследований, материалов диссертаций, литературных источников и патентов в области оптического и оптико-электронного приборостроения. Обобщены полученные данные и рекомендации по разработке методов дисперсии наночастиц в полимерные матрицы при создании оптически прозрачных нанокомпозитов для применения в многих областях науки и техники. Анализ рассмотренных работ позволяет сделать вывод, что для создания гибридных органо-неорганических композитов с высоким уровнем дисперсности неорганического компонента приходится решать проблемы, связанные с совместимостью компонент и стабилизацией наночастиц наполнителя в полимерной матрице. В связи с ограниченным кругом гидрофильных полимеров, способных к формированию композитов с наночастицами без стабилизаторов, основными подходами к получению гибридных композитов являются использование модифицирующих добавок поверхностно активных веществ, а также проведение сложных химических реакций на поверхности наночастиц неорганического наполнителя. Данные способы получения нанокомпозитов с наночастицами трудоемки, связаны с образованием побочных продуктов и дополнительной очисткой. Показано, что среди большого числа нанодисперсных наполнителей полимерных матриц при получении композиционных материалов большим вниманием пользуются диоксид титана (TiO_2) и оксид цинка (ZnO). Существует множество методов синтеза наночастиц ZnO и TiO_2 с различными формами и размерами, в том числе метод лазерной абляции, который является удобным и универсальным способом получения наносуспензий твердофазных материалов в жидкости. Преимущества перед другими способами синтеза наночастиц, такими как простота метода, экологичность, низкая стоимость и возможность получать более чистые коллоидные растворы без использования поверхностно-активных веществ и других примесей, сделали лазерную абляцию в жидкой среде популярной среди исследователей.

Ключевые слова: дисперсия наночастиц; наноматериалы; оптически прозрачные полимерные матрицы.

Ил. 3. Библиогр.: 23 назв.

UDC 621.793:678.073

Dispersion of nanoparticles in optically transparent polymer matrices / *V.M. Borshchov, O.M. Listratenko, M.A. Protsenko, I.T. Tymchuk, O.V. Kravchenko, O.V. Syddia, M.I. Slipchenko, B.M. Chichkov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 105 – 114.

Search and analysis of results of theoretical and experimental studies, materials of dissertations, literature sources and patents in the field of optical and optoelectronic instrumentation were carried out. Obtained data and recommendations on the development of methods for dispersing nanoparticles into polymer matrices for the creation of optically transparent nan composites for use in many fields of science and technology are generalized. Analysis of considered results makes it possible to conclude that for creating hybrid organic-inorganic composites with high level of dispersion of inorganic component, it is necessary to solve problems relating to compatibility of components and stabilization of filler nanoparticles in polymer matrix. Due to the limited range of hydrophilic polymers capable of forming composites with nanoparticles without stabilizers, the main approaches to the preparation of hybrid composites are using modifying additives of surfactants, as well as complex chemical reactions on the surface of inorganic filler nanoparticles. Such methods of obtaining nanocomposites with nanoparticles are laborious and involve formation of by-products and additional purification. It is shown that titanium dioxide (TiO_2) and zinc oxide (ZnO) are of great interest among a large number of nanodispersed fillers of polymer matrices in preparing composite materials. There are many methods for synthesis of ZnO and TiO_2 nanoparticles with various shapes and sizes, including laser ablation method, which is convenient and universal method for preparing nanosuspensions of solid-phase materials in liquid. Advantages over other methods for nanoparticle synthesis, such as the simplicity of method, environmental friendliness, low cost, and the ability to obtain cleaner colloidal solutions without using surfactants and other impurities, have made laser ablation in a liquid medium very popular among researchers.

Key words: dispersion of nanoparticles; nanomaterials; optically transparent polymer matrices

3 fig. Ref: 23 items.

УДК 681.128.82

Контроль різниці рівнів рідини в суміжних резервуарах / *Б.В. Жуков, А.В. Одновол* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 115 – 119.

Розглянуто можливість синхронного контролю рівнів охолоджувальної рідини в системах охолоджування атомних і теплових електростанцій до і після загороджувальної сітки за допомогою спеціалізованого рівнеміра.

Представлено структурну схему рівнеміра, що забезпечує поточний синхронний контроль рівнів рідини в двох суміжних каналах (резервуарах), а також різниці рівнів рідини в них. Особливість структурної схеми спеціалізованого акустичного рівнеміра полягає у використанні загального для обох каналів джерела випромінювання і пристрою поділу спільного хвилеведучого тракту по двох каналах.

Розроблено алгоритм функціонування спеціалізованого рівнеміра, в якому на підставі часових діаграм показано як проводиться контроль рівня в кожному каналі і розраховується різниця рівнів рідини до і після загороджувальної сітки. Опис алгоритму супроводжується розрахунковими виразами для визначення рівнів та різниці рівнів рідини.

Для рівнеміра, виконаного в акустичному діапазоні хвиль, наведена умова, яка необхідна для створення пристрою, що забезпечує узгодження при розподілі загального каналу на два незалежні канали поширення

імпульсного сигналу. Дана умова дозволила встановити взаємозв'язок між внутрішніми діаметрами циліндричних труб, що застосовуються в якості хвилеведучих трактів акустичної хвилі.

Запропоновано варіанти реалізації спеціалізованого рівнеміра на базі двох модифікацій рівнеміра ЗОНД-3М, у яких в якості хвилеведучих систем застосовуються циліндричні труби. Наведено, що при використанні приємо-передавача АП-7Т рівнемір матиме робочий діапазон до 10 м при розрішенні рівнів ± 1мм, а при використанні приємо-передавача АП-70Т – робочий діапазон до 20 м при розрішенні рівнів ± 1см.

Ключові слова: рівнемір; різниця рівнів; імпульсний сигнал; хвилеведучий тракт; контроль рівня; розподільник каналів; розрішення рівнів; суміжні резервуари.

Іл. 4. Бібліогр.: 4 назв.

УДК 681.128.82

Контроль разности уровней жидкости в смежных резервуарах / *Б.В. Жуков, А.В. Одновол* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 115 – 119.

Рассмотрена возможность синхронного контроля уровней охлаждающей жидкости в системах охлаждения атомных и тепловых электростанций до и после заграждающей сетки с помощью специализированного уровнемера.

Представлена структурная схема уровнемера, обеспечивающего текущий синхронный контроль уровней жидкости в двух смежных каналах (резервуарах), а также разности уровней жидкости в них. Особенность структурной схемы специализированного акустического уровнемера заключается в использовании общего для обоих каналов источника излучения и устройства разделения общего волноведущего тракта по двум каналам.

Разработан алгоритм функционирования специализированного уровнемера, в котором на основании временных диаграмм показано как производится контроль уровня в каждом канале и рассчитывается разность уровней жидкости до и после заграждающей сетки. Описание алгоритма сопровождается расчетными выражениями для определения уровней и разности уровней жидкости.

Для уровнемера, выполненного в акустическом диапазоне волн, приведено условие необходимое для создания устройства, обеспечивающего согласование при разделении общего канала на два независимых канала распространения импульсного сигнала. Данное условие позволило установить взаимосвязь между внутренними диаметрами цилиндрических труб, применяемых в качестве волноводных трактов акустической волны.

Предложены варианты реализации специализированного уровнемера на базе двух модификаций уровнемера ЗОНД-3М, в которых в качестве волноведущих систем применяются цилиндрические трубы. Приведено, что при использовании приемо-передатчика АП-7ВТ уровнемер будет иметь рабочий диапазон до 10м при разрешении уровней ±1мм, а при использовании приемо-передатчика АП-70Т – рабочий диапазон до 20м при разрешении уровней ±1см.

Ключевые слова: **у**ровнемер; разность уровней; импульсный сигнал; волноведущий тракт; контроль уровня; разделитель каналов; разрешение уровней; смежные резервуары.

Ил. 4. Библиогр.: 4 назв.

UDC 681.128.82

Monitoring the difference in liquid levels in adjacent tanks / *B.V. Zhukov, A.V. Odnovol* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 115 – 119.

The possibility of synchronous monitoring of coolant levels in the cooling systems of nuclear and thermal power plants before and after the barrier mesh using a specialized level gauge is considered.

The block diagram of a level gauge providing current synchronous control of liquid levels in two adjacent channels (reservoirs), as well as the difference in liquid levels in them, is presented. A feature of the structural diagram of a specialized acoustic level gauge is the use of a radiation source common to both channels and a device for dividing the common waveguide path into two channels.

An algorithm for the functioning of a specialized level gauge has been developed, in which, based on time diagrams, it is shown how the level is controlled in each channel and the difference in liquid levels before and after the barrier grid is calculated. The description of the algorithm is accompanied by calculated expressions for determining the levels and the difference in liquid levels.

For a level gauge made in the acoustic wavelength range, a condition is given that is necessary for the creation of a device that provides matching when dividing a common channel into two independent channels of pulse signal propagation. This condition made it possible to establish the relationship between the inner diameters of cylindrical pipes used as waveguide paths of an acoustic wave.

Variants of the implementation of a specialized level gauge based on two modifications of the ZOND-3M level gauge are proposed, in which cylindrical pipes are used as waveguiding systems. It is shown that when using the AP-7VT transceiver, the level gauge will have an operating range of up to 10m with a level resolution of ± 1mm, and when using the AP-70T transceiver, it will have an operating range of up to 20m with a level resolution of ± 1cm.

Key words: level gauge; level difference; pulse signal; wave-guiding tract; level control; channel separator; level resolution; adjacent tanks.

4 fig. Ref: 4 items.

РАДІОТЕХНІЧНІ ПРИСТРОЇ ТА ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ
РАДИОТЕХНИЧЕСКИЕ УСТРОЙСТВА И СРЕДСТВА ТЕЛЕКОММУНИКАЦИЙ
RADIO ENGINEERING DEVICES AND TELECOMMUNICATIONS MEANS

УДК 621.375.4

Дослідження підсилювача класу E/F3 з паралельним контуром / *Д.Г. Макаров, Д.В. Чернов, В.В. Крижановський, Ю.В. Рассохіна, В.Г. Крижановський, А. Гребєнніков* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 120 – 127.

Аналітично сформульована система рівнянь для процесів у вихідній ланці підсилювача, в якій враховано параметри коливальних контурів на частотах вищих гармонік. Для розрахунку була складена система з п’яти рівнянь для п’яти невідомих, до яких була додана умова на те, що друга похідна в точці екстремуму напруги стокового імпульсу буде більше нуля. Два рівняння відповідають умовам класу Е, два – квадратурні форми для напруги на навантаженні та на додатковому контурі і одне рівняння – умова екстремуму в точці поблизу середини імпульсу напруги. Дану систему розв’язувалось у програмі комп’ютерної алгебри. За знайденими параметрами розраховуються форми сигналів та елементів схеми. Обираючи різні параметри, можна отримати варіанти реалізації підсилювачів, які будуть за принципом роботи мати риси інших варіантів класу F. Отримані параметри кіл перевірялися у програмі гармонійного балансу та проводилось порівняння форм сигналів стокової напруги та струму через транзистор (ключ) з результатами розрахунку у програмі. Варіант, який був ближче до режиму класу E/F_3, було обрано для створення експериментального макету на частоту 2 МГц з використанням транзистору IRF530, макет перевіряли у діапазоні напруги живлення до 24 В. Отримано вихідну потужність більше 6 Вт при ККД більше 80 %. В експерименті було виміряно відношення максимальної напруги на стоці польового транзистору до напруги живлення, воно склало значення 3,3 при коефіцієнті заповнення 50 % на відміну від підсилювача класу Е, де теоретичне значення 3,65, а на практиці, з урахуванням нелінійності ємності стік-витік, може бути і 4. В експерименті значення другої гармоніки на виході на рівні -29 дБ відносно першої, а третьої -28,5 дБ, що обумовлено впливом додаткового фільтру на частоту другої гармоніки. Результати роботи корисні для впровадження таких схем у практику.

Ключові слова: підсилювач класу Е; підсилювач класу E/F_3; коефіцієнт корисної дії; аналіз у часовій області; метод гармонійного балансу.

Табл. 2. Іл. 9. Бібліогр.: 12 назв.

УДК 621.375.4

Исследование усилителя класса E/F3 с параллельным контуром / *Д.Г. Макаров, Д.В. Чернов, В.В. Крыжановский, Ю.В. Рассохина, В.Г. Крыжановский, А. Гребенников* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 120 – 127.

Сформулирована аналитическая система уравнений, описывающая процессы в выходной цепи усилителя, учитывающая параметры колебательных контуров на высших гармониках сигнала. Для расчетов составлена система из пяти уравнений для пяти неизвестных, к которым было добавлено условие положительности второй производной в точке экстремума напряжения на стоке. Два уравнения отвечают условиям класса Е, два – квадратурным формам для напряжения на нагрузке и на дополнительном контуре и еще одно уравнение – условие экстремума в точке вблизи середины импульса напряжения. Эту систему решали в программе компьютерной алгебры. По найденным параметрам рассчитывались формы сигналов и элементы схемы. Выбирая разные значения, можно получить варианты реализации усилителя, которые будут иметь черты класса F. Полученные схемы проверялись в программе гармонического баланса и сравнивались формы сигналов на ключе. Для экспериментального исследования был выбран вариант, близкий к E/F_3, частота 2 МГц, транзистор IRF530 при напряжении питания 24 В. Получена выходная мощность более 6 Вт при КПД больше 80%. Экспериментально измерено отношение максимального напряжения на стоке к напряжению питания, оно равно 3,3 при коэффициенте заполнения 50 % в отличие от усилителя класса Е, где теоретическое значение 3,65, а на практике, с учетом нелинейности емкости сток-исток, может быть и 4. Значение второй гармоники в эксперименте -29 дБ относительно первой, а третьей -28,5 дБ, что обусловлено влиянием дополнительного фильтра на частоту второй гармоники. Результаты работы будут полезны для внедрения таких схем на практике.

Ключевые слова: усилители класса Е; усилители класса E/F_3; коэффициент полезного действия; анализ во временной области; метод гармонического баланса.

Табл. 2. Ил. 9. Библиогр.: 12 назв.

UDC 621.375.4

Investigation into Class E/F3 with Parallel Network / *D.G. Makarov, D.V. Chernov, V.V. Kryzhanovskyi, Yu.V. Rassokhina, V.G. Kryzhanovskyi, A. Grebennikov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 120 – 127.

The system of equations for processes in the amplifier output network is analytically formulated. This system of equations considers parameters of resonant networks at higher harmonics. To calculate amplifier output network, the system of five equations was built for five unknowns, to which the condition of positive second voltage derivative at extremum of drain voltage was added. Two equations correspond to class E conditions, another two — quadrature waveforms at load and at additional resonant network. The last equation is the condition of extremum at the point near

middle of drain voltage pulse. This system was solved using computer algebra program. The circuit elements and waveforms were calculated using the derived parameters. By choosing different parameters, it is possible to obtain various amplifier realizations, which will demonstrate features of different class F variants. The obtained amplifier parameters drain voltage and current waveforms were verified with calculated ones using the harmonic balance simulating software. The variant, which is closer to class E/F_3 mode, was chosen to build an experimental amplifier prototype on frequency 2MHz using IRF530 MOSFET as a switch. The prototype was tested in the range of supply dc voltage up to 24V with the output power greater than 6W, while the amplifier efficiency was >80%. In the experiment, the ratio of peak drain voltage to dc supply voltage was measured to be 3.3 at the duty ratio 50%, unlike class E amplifier, where this value is around 3.65, and on practice, considering non-linear drain to source capacitance, it may achieve 4. The experimental second harmonic level amounted to be -20 dB relatively to fundamental, and the third one — 28.5 dB, which is due to an additional second harmonic filter. The paper results are useful for introduction of such circuits to practice.

Key words: class E amplifier; class E/F_3; efficiency; transient analysis; harmonic balance.

2 tab. 9 fig. Ref: 12 items.

ПІДГОТОВКА СПЕЦІАЛІСТІВ В ОБЛАСТІ РАДІОТЕХНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ

ПОДГОТОВКА СПЕЦИАЛИСТОВ В ОБЛАСТИ РАДИОТЕХНИКИ И ТЕЛЕКОММУНИКАЦИЙ

TRAINING OF SPECIALISTS IN THE FIELD OF RADIO AND TELECOMMUNICATIONS

УДК 004.94

Можливості застосування СМК Maple для дослідження законів розподілу випадкових величин / *І.О. Мощенко, О.М. Нікітенко, Ю.В. Козлов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 128 – 134.

Описано використання СМК Maple для практичної та самостійної роботи студентів при вивченні законів розподілу випадкових величин.

Статистичні розрахунки без допомоги ЕОМ є складними й потребують використання багатьох таблиць функцій та квантилів стандартних розподілів. Це не сприяє тому, щоб відчути елемент новизни в матеріалі, який вивчається, мати можливість змінити задовільно умови задач тощо, потребує багато часу під час вирішення прикладних виробничих завдань, що є недоцільним.

Тому для визначення та дослідження законів розподілу випадкових величин як в практичній діяльності, так і під час навчання, використовують спеціальні математичні програмні пакети прикладних програм, найбільш поширеними серед яких є Mathcad, MatLab, Mathematica, Maple.

Таким чином метою цієї публікації є опис можливостей вивчення законів розподілу випадкових величин за допомогою СМК Maple та застосування отриманих навичок у самостійній роботі студентів.

Бібліотека Statistics має великий набір команд для аналізу даних з обчисленням різноманітних числових характеристик випадкових величин, графічного зображення їх законів розподілу, а також для статистичної обробки даних.

Таким чином, СМК Maple завдяки потужному набору статистичних інструментів, можливості символьних обчислень та обробки виразів та даних, широким можливостям графічної інтерпретації отриманих результатів не тільки в статичному, але і в динамічному виді (дво- та тривимірна анімація) доцільно використовувати під час вивчення теми «Закони розподілу випадкових величин» на практичних заняттях та у самостійній роботі студентів для подальшого використання ними набутих навичок при вирішенні прикладних завдань науки та техніки.

Ключові слова: статистика; закон розподілу; випадкова величина; система комп'ютерної математики; Maple.

Табл. 1. Іл. 2. Бібліогр.: 8 назв.

УДК 004.94

Возможности использования СМК Maple для исследования законов распределения случайных величин / *И.А. Мощенко, А.Н. Никитенко, Ю.В. Козлов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 128 – 134.

Описано использование СМК Maple для практической и самостоятельной работы студентов при изучении законов распределения случайных величин.

Статистические расчеты без помощи ЭВМ являются сложными и требуют использования множества таблиц функций и квантилей стандартных распределений. Это не способствует тому, чтобы почувствовать элемент новизны в материале, который изучается, иметь возможность изменить произвольно условия задач и т.п., требует много времени при решении прикладных производственных задач, что является нецелесообразным.

Поэтому для определения и исследования законов распределения случайных величин, как в практической деятельности, так и во время обучения, используют специальные математические программные пакеты прикладных программ, наиболее распространенными из которых являются Mathcad, MatLab, Mathematica, Maple.

Таким образом, целью данной публикации является описание возможностей изучения законов распределения случайных величин с помощью СМК Maple и использование полученных навыков в самостоятельной работе студентов.

Библиотека Statistics имеет большой объем команд для анализа данных с вычислением числовых характеристик случайных величин и графического изображения их законов распределения.

СМК Maple благодаря мощному набору статистических инструментов, возможности символьных вычислений и обработки данных, широким возможностям графической интерпретации полученных результатов не только в статическом, но и в динамическом виде целесообразно использовать при изучении темы «Законы распределения случайных величин» на практических занятиях и в самостоятельной работе студентов для использования ими приобретенных навыков при решении прикладных задач науки и техники.

Ключевые слова: статистика; закон распределения; система компьютерной математики; Maple.

Табл. 1. Ил. 2. Библиогр.: 8 назв.

UDC 004.94

Possibility of using CMS Maple to study laws of distribution of random variables / *I. Moshchenko, O. Nikitenko, Yu.V. Kozlov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 128 – 134.

The use of CMS Maple for students' practical and independent work is described. The study of random variable distribution laws is actual.

Statistical calculations without computer are difficult and require many functional and quintiles tables of standard distributions. This does not contribute to feeling the element of novelty in the material being studied, to be able to arbitrarily change the conditions of tasks, etc., it takes a lot of time in solving applied production problems, which is inappropriate

Thus to determine and research random variable distribution laws both in practical applications and in studying we must use special mathematical packages. The most extended of them are Mathcad, MatLab, Mathematica, Maple. Specialized statistical packages (SAS, SPSS, STATISTIKA, STATGRAPHICS) are not relevant to study. Their use for studying requires very high education level in mathematical statistics.

Most of the existing math packages allow users to operate at random variables, including the Computer Mathematics System (CMS) Maple.

Thus, the purpose of this article is a description of the studying possibilities of the random variables distribution laws with CMS Maple and the application of the acquired skills to the independent work of students.

The Maple Statistics Library has a large set of commands for analyzing data, computing various numerical characteristics of random variables, graphing their distribution laws, and for statistical data processing.

Thanks to a powerful set of statistical tools, the possibility of symbolic calculations and data processing of CMS Maple, wide possibilities of graphical interpretation of the results obtained not only in a static but also in a dynamic form, it is advisable to use it when studying the topic "Distribution Laws of Random Variables" in students' practical and independent work to use their acquired skills in solving applied problems of science and technology.

Key words: statistics; distribution law; random variable; computer mathematics system; Maple.

1 tab. 2 fig. Ref: 8 items.