МЕТОДИ ТА АЛГОРИТМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ
МЕТОДЫ И АЛГОРИТМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
METHODS AND ALGORITHMS OF CRYPTOGRAPHIC PROTECTION OF INFORMATION

УДК 004.056.55

Основні положення та результати порівняння властивостей електронних підписів постквантового періоду на алгебраїчних решітках / *І.Д. Горбенко, О.Г. Качко, О.В. Потій, А.М. Олексійчук, Ю.І. Горбенко, М.В. Єсіна, І.В. Стельник, В А. Пономар* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 5 – 21.

Розглядаються постквантові проєкти стандартів електронних підписів (ЕП) Falcon та Dilithium, які є фіналістами конкурсу NIST США. При їх побудуванні використовується математичний апарат алгебраїчних решіток та відповідні методи. При подальшому дослідженні та порівнянні вказаних постквантових проєктів стандартів ЕП, як з теоретичних, так і практичних позицій, основоположним є обґрунтування вимог до параметрів та ключів, та у цілому обчислення основних показників згідно прийнятих умовних та безумовних критеріїв. Важливим при таких дослідженнях є визначення достатності забезпечення гарантованості їх захищеності від класичних, квантових, спеціальних та атак на основі помилок. Вказане може бути забезпечено, у тому числі, засобом обґрунтованого вибору розмірів загальних параметрів та ключів, та практичного їх побудування згідно прийнятої моделі безпеки. Але при виборі розмірів загальних параметрів та ключів виникає суттєве протиріччя між властивостями проєктів стандартів ЕП Falcon та Dilithium, щодо стійкості та складності перетворень. Так, збільшення розмірів загальних параметрів та ключів приводить до збільшення складності перетворень, і навпаки. Метою цієї статі є: аналіз проблемних питань вибору розмірів параметрів та ключів для постквантових проєктів ЕП, побудованих на основі математичних методів Falcon та Dilithium, та особливості їх реалізації, в тому числі і реалізації згідно прийнятої моделі безпеки. Порівняльний аналіз стійкості та складності проєктів стандартів ЕП Falcon та Dilithium у залежності від розмірів параметрів та ключів, в тому числі для 6 та 7 рівнів безпеки. Розробка пропозицій стосовно рішень щодо прийняття в якості національних постквантових стандартів ЕП на основі математичних методів Falcon та Dilithium. Визначення впливу безумовних, умовних та прагматичних критеріїв на переваги при прийнятті рішення щодо стандартизації ЕП на основі математичних методів Falcon та Dilithium, в тому числі з урахуванням наявності патентів та необхідності отримання ліцензій тощо.

Ключові слова: алгебраїчні решітки; алгоритм; електронний підпис; основні параметри; постквантова криптографія.

Табл. 12. Іл. 2. Бібліогр.: 24 назв.

УДК 004.056.55

Основные положения и результаты сравнения свойств электронных подписей постквантового периода на алгебраических решетках / *И.Д. Горбенко, Е.Г. Качко, А.В. Потий, А.Н. Олексийчук, Ю.И. Горбенко, М.В. Есина, И.В. Стельник, В.А. Пономарь* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 5 – 21.

Рассматриваются постквантовые проекты стандартов электронных подписей (ЭП) Falcon и Dilithium, которые являются финалистами конкурса NIST США. При их построении используется математический аппарат алгебраических решеток и соответствующие методы. При дальнейшем исследовании и сравнении указанных постквантовых проектов стандартов ЭП, как с теоретических, так и практических позиций, основополагающим является обоснование требований к параметрам и ключам, и в целом вычисления основных показателей согласно принятых условных и безусловных критериев. Важным при таких исследованиях является определение достаточности обеспечения гарантированности их защищенности от классических, квантовых, специальных и атак на основе ошибок. Это может быть обеспечено, в том числе, посредством обоснованного выбора размеров общих параметров и ключей, и практического их построения согласно принятой модели безопасности. Но при выборе размеров общих параметров и ключей возникает существенное противоречие между свойствами проектов стандартов ЭП Falcon и Dilithium, по устойчивости и сложности преобразований. Так, увеличение размеров общих параметров и ключей приводит к увеличению сложности преобразований, и наоборот. Цель этой статьи: анализ проблемных вопросов выбора размеров параметров и ключей для постквантовых проектов ЭП, построенных на основе математических методов Falcon и Dilithium, и особенности их реализации, в том числе и реализации согласно принятой модели безопасности. Сравнительный анализ устойчивости и сложности проектов стандартов ЭП Falcon и Dilithium в зависимости от размеров параметров и ключей, в том числе для 6 и 7 уровней безопасности. Разработка предложений относительно решений о принятии в качестве национальных постквантовых стандартов ЭП на основе математических методов Falcon и Dilithium. Определение влияния безусловных, условных и прагматических критериев на преимущества при принятии решения о стандартизации ЭП на основе математических методов Falcon и Dilithium, в том числе с учетом наличия патентов и необходимости получения лицензий и тому подобное.

Ключевые слова: алгебраические решетки; алгоритм; электронная подпись; основные параметры; постквантовая криптография.

Табл. 12. Ил. 2. Библиогр.: 24 назв.

UDC 004.056.55

Basic principles and results of comparison of electronic signatures properties of the postquantum period based on algebraic lattices / *I.D. Gorbenko, O.G. Kachko, O.V. Potii, A.M. Oleksiychuk, Yu.I. Gorbenko, M.V. Yesina, I.V. Stelnyk, V.A. Ponomar* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 5 – 21.

The paper considers post-quantum projects of the Falcon and Dilithium electronic signature standards (ES), which are finalists of the NIST USA competition. The mathematical apparatus of algebraic lattices and appropriate methods are used in their construction. In further study and comparison of these post-quantum ES draft standards, both from a theoretical and practical standpoint, it is fundamental to substantiate the requirements for parameters and keys and in general to calculate the main indicators according to the accepted conditional and unconditional criteria. In such studies, it is important to determine the sufficiency of ensuring the guarantee of their security against classical, quantum, special and error-based attacks. This can be ensured, inter alia, through a reasonable choice of the sizes of common parameters and keys, and their practical construction in accordance with the adopted security model. However, when choosing the sizes of common parameters and keys, a significant contradiction arises between the properties of the draft of the Falcon and Dilithium ES standards, So increasing the size of the general parameters and keys leads to an increase in the complexity of transformations, and vice versa. The purpose of this article consists in analysis of problematic issues of choosing the size of parameter and keys for post-quantum ES projects based on mathematical methods of Falcon and Dilithium, and features of their implementation, including implementation according to the adopted security model. Comparative analysis of the stability and complexity of the Falcon and Dilithium ES draft standards depending on the size of the parameters and keys, including for 6 and 7 security levels. Development of proposals for decisions on the adoption of national post-quantum ES standards based on the mathematical methods Falcon and Dilithium. Determining the influence of unconditional, conditional and pragmatic criteria on the advantages when deciding on the ES standardization based on Falcon and Dilithium mathematical methods, including taking into account the availability of patents and the need to obtain licenses, etc.

Key words: algebraic lattices; algorithm; electronic signature; basic parameters; post-quantum cryptography.

12 tab. 2 fig. Ref: 24 items.

УДК 621.391:519.2

Оцінки ефективності атак на основі підібраних відкритих текстів на криптосистему Рао-Нама над скінченною абелевою групою / *А.М. Олексійчук, О.С. Шевчук* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 22 – 31.

Криптосистема Рао – Нама являє собою симетричну версію кодової криптосистеми Мак-Еліса, запропоновану з метою позбутися слабкостей, притаманних найпершим симетричним кодовим схемам шифрування. Майже одразу після опублікування цієї криптосистеми з'явилися атаки на неї на основі підібраних відкритих текстів, що привело до появи різноманітних удосконалень та модифікацій оригінальної криптосистеми.

Секретним ключем у традиційній схемі Рао – Нама є певна булева матриця та множина двійкових векторів, які використовуються для формування спотворень при зашифруванні. Такі вектори повинні мати різні синдроми, тобто бути різними за модулем коду, породженому рядками зазначеної матриці. В оригінальній роботі Рао і Нама розглянуто два способи формування множини цих векторів, перший з яких полягає у використанні заздалегідь визначених векторів достатньо великої ваги, а другий – у випадковому виборі цих векторів за рівноймовірною схемою. Відомо, що перший варіант не забезпечує належну стійкість криптосистеми Рао – Нама (внаслідок невеликої кількості та простої будови зазначених векторів), проте другий варіант є більш змістовним та потребує додаткових досліджень.

Мета статті – отримання оцінок ефективності (трудомісткості при заданій верхній межі ймовірності помилки) атак на криптосистему, яка узагальнює традиційну схему Рао – Нама на випадок скінченної абелевої групи (зауважимо, що необхідність дослідження подібних версій криптосистеми Рао – Нама обумовлена їх розглядом у нещодавніх публікаціях). Представлено дві атаки, які будуються на основі підібраних відкритих текстів. Перша з них не згадується у відомих авторам цієї статті працях і за певних, точно визначених умов дозволяє відновлювати секретний ключ криптосистеми із квадратичною складністю.

Друга атака являє собою узагальнено-спрощений варіант відомої атаки Стройка-ван Тілбурга. Показано, що складність цієї атаки залежить від потужності стабілізатора множини векторів, яка утворює другу частину ключа, у групі зсувів абелевої групи, над якою розглядається криптосистема Рао – Нама. Отримано оцінку ймовірності тривіальності стабілізатора за умови випадкового вибору цієї множини. З отриманої оцінки випливає, що атака Стройка-ван Тілбурга є в середньому помітно більш ефективною в порівнянні із найгіршим випадком, розглянутим раніше.

Ключові слова: кодова криптографія; криптосистема Рао – Нама; атака на основі підібраних відкритих текстів; атака Стройка-ван Тілбурга.

Бібліогр.: 10 назв.

УДК 621.391:519.2

Оценки эффективности атак на основе подобранных открытых текстов на криптосистему Рао – Нама над конечной абелевой группой / *А.Н. Алексейчук, О.С. Шевчук* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 22 – 31.

Криптосистема Рао – Нама представляет собой симметричную версию кодовой криптосистемы Мак-Элиса, предложенную с целью избавиться от недостатков, присущих первым симметричным кодовым схемам шифрования. Почти сразу после опубликования этой криптосистемы на нее появились атаки на основе подобранных открытых текстов, что привело к появлению различных усовершенствований и модификаций оригинальной криптосистемы.

Секретным ключом в традиционной схеме Рао – Нама являются определенная булева матрица и множество двоичных векторов, используемых для формирования искажений при зашифровании. Такие векторы должны иметь различные синдромы, то есть быть разными по модулю кода, порожденного строками указанной матрицы. В оригинальной работе Рао и Нама рассмотрены два способа формирования множества этих векторов, первый из которых заключается в использовании заранее определенных векторов достаточно большого веса, а второй – в случайном выборе этих векторов по равновероятной схеме. Известно, что первый вариант не обеспечивает надлежащую стойкость криптосистемы Рао – Нама (вследствие небольшого количества и простого строения указанных векторов), однако второй вариант является более содержательным и требует дополнительных исследований.

Цель статьи – получение оценок эффективности (трудоемкости при заданной верхней границе вероятности ошибки) атак на криптосистему, которая обобщает традиционную схему Рао – Нама на случай конечной абелевой группы (заметим, что необходимость исследования подобных версий криптосистемы Рао – Нама обусловлена их рассмотрением в недавних публикациях). Представлены две атаки, которые строятся на основе подобранных открытых текстов. Первая из них не упоминается в известных авторам трудах и при некоторых условиях позволяет восстанавливать секретный ключ криптосистемы с квадратичной сложностью.

Вторая атака представляет собой обобщенно-упрощенный вариант известной атаки Стройка-ван Тилбурга. Показано, что сложность этой атаки зависит от мощности стабилизатора множества векторов, которое образует вторую часть ключа в группе сдвигов абелевой группы, над которой рассматривается криптосистема Рао – Нама. В работе получена оценка вероятности тривиальности стабилизатора при условии случайного выбора этого множества. Из полученной оценки следует, что атака Стройка-ван Тилбурга является в среднем заметно более эффективной по сравнению с худшим случаем, рассмотренным ранее.

Ключевые слова: кодовая криптография; криптосистема Рао – Нама; атака на основе подобранных открытых текстов; атака Стройка-ван Тилбурга.

Библиогр.: 10 назв.

UDC 621.391:519.2

Evaluation of effectiveness of chosen-plaintext attacks on the Rao-Nam cryptosystem over a finite Abelian group / *A.N. Alekseychuk, O.S. Shevchuk* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 22 – 31.

The Rao-Nam cryptosystem is a symmetric version of the McEliece code-based cryptosystem proposed to get rid of the shortcomings inherent in the first symmetric code-based encryption schemes. Almost immediately after the publication of this cryptosystem, attacks on it based on selected plaintexts appeared, which led to the emergence of various improvements and modifications of the original cryptosystem.

The secret key in the traditional Rao-Nam scheme is a certain Boolean matrix and a set of binary vectors used to generate distortions during encryption. Such vectors must have different syndromes, that is, be different modulo of the code generated by the rows of the specified matrix. The original work of Rao and Nam considered two methods of forming the set of these vectors, the first of which consists in using predetermined vectors of sufficiently large weight, and the second is random selection of these vectors according to the equiprobable scheme. It is known that the first option does not provide the proper security of the Rao – Nam cryptosystem (due to the small number and simple structure of these vectors), but the second option is more meaningful and requires additional research. The purpose of this paper is to obtain estimates of the effectiveness (time complexity for a given upper bound of the error probability) of attacks on a cryptosystem, which generalizes the traditional Rao – Nam scheme to the case of a finite Abelian group (note that the need to study such versions of the Rao – Nam cryptosystem is due to their consideration in recent publications). Two attacks, based on selected plaintext, are presented. The first of them is not mentioned in the works known to the authors of this article and, under certain well-defined conditions, it allows recovering the secret key of the cryptosystem with quadratic complexity.

The second attack is a generalized and simplified version of the well-known Struik-van Tilburg attack. It is shown that the complexity of this attack depends on the power of the stabilizer of the set of vectors, which forms the second part of the key, in the translation group of the Abelian group, over which the Rao – Nam cryptosystem is considered. In this paper, a bound is obtained for the probability of triviality of the stabilizer under the condition of random choice of this set. From the obtained bound, it follows that Struik-van Tilburg attack is, on average, noticeably more efficient than the worst case considered earlier.

Key words: code-based cryptography; Rao – Nam cryptosystem; chosen-plaintext attack; Struik-van Tilburg attack.

Ref: 10 items.

УДК 004.056.5

Стеганографічні методи в векторній графіці / *О.О. Кузнецов, Г.В. Кононченко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 32 – 41.

Для приховування інформації застосовуються різні стеганографічні техніки. Зазвичай інформацію приховують у зображеннях, аудіо- та відеофайлах, текстових документах, тощо. В статті розглянуто векторні зобра-

ження, що складаються із різних математичних об'єктів (точки, лінії, криві першого та другого порядку, криві Без'є, вузли, дотичні, керуючі точки, тощо). Техніки приховування інформації змінюють ці математичні об'єкти, наприклад, через кодування координат базових точок. Найбільш вдалим для проведення стеганографічних перетворень є формат векторної графіки SVG, який завдяки своїй структурі дозволяє легко маніпулювати об'єктами, з яких складається. Його широка підтримка різними платформами також дозволяє підвищити рівень скритності при проведенні передачі секретних даних шляхом передачі звичайних на перший погляд файлів медіа. В статті розглянуто два методи (побітовий та метод паттернів) приховування інформації в векторні зображення, вивчено їх особливості, переваги та недоліки. Також досліджено різні афінні перетворення, які можна застосовувати для порушення роботи стеганосистеми. Найпоширенішими видами афінних перетворень є операції перенесення, повороту, зсуву та масштабування з можливими варіаціями (зсуву за осями абсцис та ординат, масштабування пропорційне та непропорційне, зі стисненням та із розширенням). Більшість методів вбудовування інформації у векторні зображення забезпечують одноразову стійкість до афінних перетворень, при цьому при повторному накладенні операцій зміни положення об'єктів, повідомлення може зруйнуватися взагалі. Досліджені в роботі методи реалізують більший рівень стійкості до різного роду перетворень при їх багаторазовому проведенні і проведені експерименти це наочно доводять. Отримані результати показують, що векторні зображення дійсно можуть застосовуватися для приховування інформації, але стійкість проти певних афінних атак не завжди є високою.

Ключові слова: приховування інформації; векторна графіка; стеганографія; афінні перетворення.

Табл. 1. Іл. 15. Бібліогр.: 14 назв.

УДК 004.056.5

Стеганографические методы в векторной графике / *А.А. Кузнецов, А.В. Кононченко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 32 – 41.

Для сокрытия информации применяются различные стеганографические техники. Обычно информацию скрывают в изображениях, аудио и видео файлах, текстовых документах и тому подобное. В статье рассмотрены векторные изображения, состоящие из различных математических объектов (точки, линии, кривые первого и второго порядка, кривые Безье, узлы, касательные, базовые точки и т.д.). Техники сокрытия информации меняют эти математические объекты, например, через кодирование координат базовых точек. Наиболее удачным для проведения стеганографических преобразований является формат векторной графики SVG, который благодаря своей структуре позволяет легко манипулировать объектами, из которых состоит. Его широкая поддержка различными платформами также позволяет повысить уровень скрытности при передаче секретных данных путем пересылки обычных на первый взгляд файлов медиа. В статье рассмотрены два метода (побитовый и метод паттернов) сокрытия информации в векторные изображения, изучены их особенности, преимущества и недостатки. Также были исследованы различные аффинные преобразования, которые можно применять для нарушения работы стеганосистемы. Наиболее распространенными видами аффинных преобразований являются операции переноса, поворота, сдвига и масштабирования с возможными вариациями (смещения по осям абсцисс и ординат, масштабирование пропорциональное и непропорциональное, со сжатием и с расширением). Большинство методов встраивания информации в векторные изображения обеспечивают единовременную устойчивость к аффинным преобразованиям, при этом при повторном наложении операций изменения положения объектов, сообщение может разрушиться вообще. Исследованные в работе методы реализуют больший уровень устойчивости к различного рода преобразованиям при их многократном проведении, проведенные эксперименты это наглядно демонстрируют. Полученные результаты показывают, что векторные изображения действительно могут применяться для сокрытия информации, но устойчивость против определенных аффинных атак не всегда высока.

Ключевые слова: сокрытие информации; векторная графика; стеганография; аффинные преобразования.

Табл. 1. Ил. 15. Библиогр.: 14 назв.

UDC 004.056.5

Steganographic methods in vector graphics / *A.A. Kuznetsov, Г.В. Кононченко* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 32 – 41.

Various steganographic techniques are used to hide information. Usually, information is hidden in images, audio and video files, text documents, and the like. The article deals with vector images consisting of various mathematical objects (points, lines, curves of the first and second order, Bezier curves, nodes, tangents, base points, etc.). Information hiding techniques alter these mathematical objects, for example, by encoding the coordinates of the base points. The most successful for carrying out steganographic transformations is the SVG vector graphics format, which, due to its structure, makes it easy to manipulate the objects of which it consists. Its broad support across platforms also allows for increased secrecy when transferring sensitive data by sending seemingly ordinary media files. The article discusses two methods (bitwise and the method of patterns) of hiding information in vector images, studied their features, advantages and disadvantages. Various affine transformations that can be used to disrupt the operation of the steganosystem were also investigated. The most common types of affine transformations are the operations of transfer, rotation, shift and scaling with possible variations (offsets along the abscissa and ordinate axes, proportional and non-proportional scaling, with compression and expansion). Most of the methods for embedding information into vector images provide a one-time resistance to affine transformations, while the repeated imposition of operations for changing the position of objects may destroy the message altogether. The methods investigated in the work (bitwise and the method of patterns) implement a higher level of resistance to various kinds of transformations when they are repeated many times, and the

conducted experiments clearly demonstrate this. The results obtained show that vector images can indeed be used to hide information, but the resistance against certain affine attacks is not always high.

Key words: information concealing; vector graphics; steganography; affine transformations

1 tab. 15 fig. Ref: 14 items.

УДК 004.056.55

Аналіз апаратних реалізацій алгоритмів електронного підпису qTesla, Crystals-Dilitium і MQDSS на різних рівнях безпеки / *М.В. Єсіна, Б.С. Шахов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 42 – 52.

Відомо, що існують алгоритми криптографії з відкритим ключем, що засновані на RSA та еліптичних кривих, надають гарантії безпеки, які супроводжуються складністю. Можна казати про неможливість вирішення завдань цілочисельної факторизації і дискретного логарифма. Але експерти прогнозують, що створення квантового комп'ютера зможе зламати класичні криптографічні алгоритми. Через цю майбутню проблему національний інститут стандартів і технологій (NIST) разом із провідними вченими у галузі криптографії розпочав відкритий процес стандартизації алгоритмів з відкритим ключем для квантових атак. Важливою особливістю постквантового періоду у криптографії є суттєва невизначеність щодо вихідних даних для криптоаналізу та протидії в частині можливостей квантових комп'ютерів, їх математичного та програмного забезпечень, а також застосування квантового криптоаналізу до існуючих криптоперетворень та криптопротоколів. В якості основних методів NIST США обрано математичні методи електронного підпису (ЕП), що пройшли суттєвий аналіз та обґрунтування в процесі широких досліджень криптографами та математиками на найвищому рівні. Вони детально описані та пройшли дослідження на першому та другому етапах міжнародного конкурсу NIST США PQC. З історичної точки зору, у 1997 р. NIST запросив рекомендації у громадськості для визначення заміни стандарту шифрування даних (DES), Advanced Encryption Standard (AES). Відтоді відкриті криптографічні оцінки стали способом вибору криптографічних стандартів. Наприклад, NESSIE (2000-2002), eSTREAM (2004-2008), CRYPTREC (2000-2002), SHA-3 (2007-2012) і CAESAR (2013-2019) прийняли цей підхід. У цих оцінках головним параметром була безпека. Продуктивність у програмному забезпеченні, продуктивність у прикладних специфічних інтегральних схемах (ASIC), продуктивність у FPGA та можливість реалізації з використанням обмежених ресурсів (невеликих мікропроцесорів та малопотужних апаратних засобів) є вторинними критеріями. У роботі описується порівняння апаратного забезпечення трьох алгоритмів підпису (qTesla, Crystals-Dilitium, MQDSS), які зокрема є кандидатами 2-го раунду конкурсу NIST PQC, а алгоритм Crystals-Dilitium – фіналістом цього конкурсу. Метою цієї роботи є аналіз та порівняння трьох апаратних реалізацій кандидатів другого раунду конкурсу NIST PQC на алгоритм електронного підпису.

Ключові слова: постквантова криптографія; електронний підпис; qTesla; Crystals-Dilitium; MQDSS.

Табл. 12. Іл. 10. Бібліогр.: 8 назв.

УДК 004.056.55

Анализ аппаратных реализаций алгоритмов электронной подписи qTesla, Crystals-Dilitium и MQDSS на различных уровнях безопасности / *М.В. Есина, Б.С. Шахов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 42 – 52.

Известно, что существуют алгоритмы криптографии с открытым ключом, основанные на RSA и эллиптических кривых предоставляют гарантии безопасности сопровождающихся сложностью. Исходя из этого, можно говорить о невозможности решения задач целочисленной факторизации и дискретного логарифма.) Но эксперты прогнозируют, что создание квантового компьютера сможет сломать классические криптографические алгоритмы. Из-за этой будущей проблемы национальный институт стандартов и технологий (NIST) вместе с ведущими учеными в области криптографии начал открытый процесс стандартизации алгоритмов с открытым ключом для квантовых атак. Важной особенностью постквантового периода в криптографии является существенная неопределенность относительно исходных данных для криптоанализа и противодействия в части возможностей квантовых компьютеров, их математического и программного обеспечения, а также применение квантового криптоанализа к существующим криптопреобразованиям и криптопротоколам. В качестве основных методов NIST США избрал математические методы электронной подписи (ЭП), прошедшие существенный анализ и обоснование в процессе широких исследований криптографами и математиками на высшем уровне. Они подробно описаны и прошли исследования на первом и втором этапах международного конкурса NIST США PQC. С исторической точки зрения, в 1997 г. NIST запросил рекомендации общественности для определения замены стандарта шифрования данных (DES), Advanced Encryption Standard (AES). С тех пор открытые криптографические оценки стали способом выбора криптографических стандартов. Например, NESSIE (2000-2002), eSTREAM (2004-2008), CRYPTREC (2000-2002), SHA-3 (2007-2012) и CAESAR (2013-2019) приняли этот подход. В этих оценках главным параметром была безопасность. Производительность в программном обеспечении, производительность в приложениях специфических интегральных схем (ASIC), производительность в FPGA и возможность реализации с использованием ограниченных ресурсов (небольших микропроцессоров и маломощных аппаратных средств) являются вторичными критериям. В работе описывается сравнение аппаратного обеспечения трех алгоритмов подписи (qTesla, Crystals-Dilitium, MQDSS), которые, в частности, являются кандидатами 2-го раунда конкурса NIST PQC, а алгоритм Crystals-Dilitium – финалистом этого конкурса. Цель работы – анализ и

сравнение трех аппаратных реализаций кандидатов второго раунда конкурса NIST PQC на алгоритм электронной подписи.

Ключевые слова: постквантовая криптография; электронная подпись; qTesla; Crystals-Dilitium; MQDSS.

Табл. 12. Ил. 10. Библиогр.: 8 назв.

UDC 004.056.55

Analysis of hardware implementations of electronic signature algorithms qTesla, Crystals-Dilitium and MQDSS at different levels of security / *M.V. Yesina, B.S. Shahov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 42 – 52.

It is known, that existing public-key cryptography algorithms based on RSA and elliptic curves provide security guarantees accompanied by complexity. Based on this one can talk about the impossibility to solve problems of integer factorization and discrete logarithm. However, experts predict that the creation of a quantum computer will be able to crack classical cryptographic algorithms. Due to this future problem, the National Institute of Standards and Technologies (NIST), together with leading scientists in the field of cryptography, began an open process of standardizing public-key algorithms for quantum attacks. An important feature of the post-quantum period in cryptography is the significant uncertainty regarding the source data for cryptanalysis and counteraction in terms of the capabilities of quantum computers, their mathematical and software, as well as the application of quantum cryptanalysis to existing cryptotransformations and cryptoprotocols. Mathematical methods of electronic signature (ES) have been chosen as the main methods of NIST USA, which have undergone significant analysis and substantiation in the process of extensive research by cryptographers and mathematicians at the highest level. These methods are described in detail and passed the research at the first stage of the international competition NIST USA PQC. Historically, in 1997, NIST sought public advice to determine the replacement of the data encryption standard (DES), Advanced Encryption Standard (AES). Since then, open cryptographic estimations have become a way of choosing cryptographic standards. For example, NESSIE (2000-2002), eSTREAM (2004-2008), CRYPTREC (2000-2002), SHA-3 (2007-2012) and CAESAR (2013-2019) have adopted this approach. Security was the main parameter in these estimations. Performance in software, performance in application-specific integrated circuits (ASICs), performance in FPGAs, and feasibility with limited resources (small microprocessors and low-power hardware) are secondary criteria. This paper presents the comparison of the hardware of three signature algorithms (qTesla, Crystals-Dilitium, MQDSS), which, in particular, are the candidates for the 2nd round of the NIST PQC competition, and the Crystals-Dilitium algorithm is the finalist of this competition. The objective of this work is to analyze and compare three hardware implementations of candidates for the second round of the NIST PQC contest for an electronic signature algorithm.

Key words: post-quantum cryptography; electronic signature; qTesla; Crystals-Dilitium; MQDSS.

12 tab. 10 fig. Ref: 8 items.

УДК 004.056

Аналіз формальних моделей управління доступом і особливості їх застосування для баз даних / *В.В. Віліґура* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 53 – 70.

Невід'ємною частиною будь-якого проекту по створенню або оцінки безпеки інформаційних систем і баз даних є наявність моделі безпеки. В роботі розглядаються основні положення найбільш поширених моделей безпеки, заснованих на контролі доступу суб'єктів до об'єктів. Проведений аналіз формальних моделей управління доступом 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. Так, в роботі відзначається, що моделі безпеки на основі дискреційної політики доцільно застосовувати при проведенні формальної верифікації коректності побудови систем розмежування доступу в добре захищених інформаційних системах і базах даних. При цьому однак підкреслюється, що цим моделям властиві певні недоліки, що обмежують їх застосування. В роботі констатується, що незважаючи на те, що моделі безпеки на основі мандатної політики доступу відіграють важливу роль в теорії інформаційної безпеки і їх положення введені в якості обов'язкових вимог до систем, що обробляють секретну інформацію, а також в стандартах захищених систем, при практичній реалізації цих моделей може виникнути ряд проблем: завищення рівня безпеки, запис наосліп, проблема привілейованих суб'єктів, що виконують операції, які не вписуються в рамки моделі. Також робиться висновок про те, що використання моделей безпеки на основі рольової політики дозволяє реалізувати правила розмежування доступу, що динамічно змінюються в процесі функціонування інформаційних систем, баз даних, ефективність яких особливо помітно проявляється при організації доступу до ресурсів систем з великою кількістю користувачів і об'єктів.

Ключові слова: модель безпеки; управління доступом; інформаційна система; база даних.

Табл. 3. Іл. 3. Бібліогр.: 31 назв.

УДК 004.056

Анализ формальных моделей управления доступом и особенности их применимости для баз данных / *В.В. Вилигура* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 53 – 70.

Неотъемлемой частью любого проекта по созданию или оценке безопасности информационных систем и баз данных является наличие модели безопасности. В работе рассматриваются основные положения наиболее распространенных моделей безопасности, основанных на контроле доступа субъектов к объектам. Проведенный анализ формальных моделей управления доступом выявил, что каждая из них, имея определенные пре-

имущества и недостатки, имеет право на использование. Решающим фактором в принятии решения является оценка конкретной ситуации, которая позволит сделать правильный выбор. Так, в работе отмечается, что модели безопасности на основе дискреционной политики целесообразно применять при проведении формальной верификации корректности построения систем разграничения доступа в хорошо защищенных информационных системах и базах данных. При этом, однако, подчеркивается, что этим моделям свойственны определенные недостатки, ограничивающие их применение. В работе констатируется, несмотря на то, что модели безопасности на основе мандатной политики доступа играют значимую роль в теории информационной безопасности и их положения введены в качестве обязательных требований к системам, обрабатывающим секретную информацию, а также в стандартах защищенных систем, при практической реализации этих моделей может возникнуть ряд проблем: завышение уровня безопасности, запись вслепую, проблема привилегированных субъектов, выполняющих операции не вписывающиеся в рамки модели. Делается вывод о том, что использование моделей безопасности на основе ролевой политики позволяет реализовать динамически изменяющиеся в процессе функционирования информационных систем, баз данных правила разграничения доступа, эффективность которых особенно заметно проявляется при организации доступа к ресурсам систем с большим количеством пользователей и объектов.

Ключевые слова: модель безопасности; управление доступом; информационная система; база данных.

Табл. 3. Ил. 3. Библиогр.: 31 назв.

UDC 004.056

Analysis of formal models for access control and specific features of their applicability to databases / *V.V. Vilihura* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 53 – 70.

An integral part of any project to create or assess the security of information systems and databases is the presence of a security model. The paper considers the main positions of the most common security models based on controlling the access of subjects to objects. The analysis of formal models for access control has revealed that each of them, having certain advantages and disadvantages, has the right to be used. The decisive factor in making a decision is an assessment of a specific situation, which will allow one to make the right choice. In this regard, the paper notes that security models based on discretionary policies are advisable to be applied when conducting formal verification of the correctness of building access control systems in well-protected information systems and databases. However, it is emphasized that these models have certain drawbacks that limit their use. The paper states that despite the fact that security models based on the mandatory access policy play a significant role in information security theory and their provisions have been introduced as mandatory requirements for systems that process secret information, as well as in the standards of secure systems, a number of problems may arise in the practical implementation of these models. Among these problems there are the problems associated with overestimating the security level, blind recordings, performing operations that do not fit into the framework of the model by privileged subjects. The paper also concludes that the use of security models based on role-based policy allows one to implement access control rules dynamically changing during the operation of information systems and databases, the effectiveness of which is especially noticeable when organizing access to the resources of systems with a large number of users and objects.

Key words: security model; access control; information system; database.

3 tab. 3 fig. Ref: 31 items.

УДК 004.056.55

Процеси та методи вибору загальносистемних параметрів та аналіз стійкості проти атак сторонніми каналами для алгоритму направленого шифрування та інкапсуляції ключів стандарту ДСТУ 8961:2019 / *В.А Кулібаба* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 71 – 78.

В останні роки відбувся значний прогрес у створенні квантових комп'ютерів. Якщо масштабовані квантові комп'ютери будуть впроваджені найближчим часом, це поставить під загрозу безпеку найбільш широко використовуваних криптосистем з відкритим ключем. Найбільш вразливими є ключові схеми, засновані на факторизації, дискретних логарифмах та криптографії еліптичної кривої. Зараз головним завданням є розробка, оцінка, дослідження та стандартизація асиметричних крипто перетворень на міжнародному рівні, включаючи механізми інкапсуляції ключів та направленого шифрування, стійкі до атак порушників постквантового періоду. Важливою особливістю перехідного та постквантового періоду є застосування нових математичних методів для протидії квантовому криптоаналізу. У роботі розглядаються основні атаки на механізми інкапсуляції ключів та направленого шифрування, а також загальносистемні параметри стандарту ДСТУ 8961:2019, що впливають на стійкість від атак та складність перетворень. Розглядаються методи генерування загальносистемних параметрів 5 та 7 рівнів стійкості – 512 біт класичної та 256 біт квантової безпеки, а також захищеність алгоритму від атак сторонніми каналами. Проаналізовано залежність часу шифрування та розшифрування від рівня стійкості. Наведено результати обчислень загальносистемних параметрів для рівнів стійкості 256/128, 384/192 та 512/256, а також надано рекомендації щодо вибору загальносистемних параметрів в залежності від оточення та обчислювальних можливостей. Наведено обрані та рекомендовані до застосування у стандарті ДСТУ 8961:2019 набори параметрів. Зроблено висновки про можливість застосування стандарту ДСТУ 8961 в постквантовий період.

Ключові слова: загальносистемні параметри; протоколи інкапсуляції ключів; направлене шифрування; алгебраїчні решітки; криптографічна стійкість.

Табл. 5. Іл. 3. Бібліогр.: 14 назв.

УДК 004.056.55

Процессы и методы выбора общесистемных параметров и анализ устойчивости против атак сторонними каналами для алгоритма направленного шифрования и инкапсуляции ключей стандарта ДСТУ 8961:2019 / *В.А Кулибаба* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 71 – 78.

В последние годы произошел значительный прогресс в создании квантовых компьютеров. Если масштабируемые квантовые компьютеры будут внедрены в ближайшее время, это поставит под угрозу безопасность наиболее широко используемых криптосистем с открытым ключом. Наиболее уязвимыми являются ключевые схемы, основанные на факторизации целых чисел, дискретных логарифмах и криптографии на эллиптической кривой. Сейчас главной задачей является разработка, оценка, исследование и стандартизация асимметричных криптопреобразований на международном уровне, включая механизмы инкапсуляции ключей и направленного шифрования, устойчивые к атакам нарушителей постквантового периода. Важной особенностью переходного и постквантового периода является применение новых математических методов для противодействия квантовому криптоанализу. В работе рассматриваются основные атаки на механизмы инкапсуляции ключей и направленного шифрования, а также общесистемные параметры стандарта ДСТУ 8961:2019, влияющие на устойчивость от атак и сложность преобразований. Рассматриваются методы генерирования общесистемных параметров 5 и 7 уровней устойчивости – 512 бит классической и 256 бит квантовой безопасности, а также защищенность алгоритма от атак сторонними каналами. Проанализирована зависимость времени шифрования и расшифровки от уровня устойчивости. Приведены результаты вычислений общесистемных параметров для уровней устойчивости 256/128, 384/192 и 512/256, а также даны рекомендации по выбору общесистемных параметров в зависимости от окружения и вычислительных возможностей. Приведены рекомендованные к применению в стандарте ДСТУ 8961: 2019 наборы параметров. Сделаны выводы о возможности применения стандарта ДСТУ 8961 в постквантовый период.

Ключевые слова: общесистемные параметры; протоколы инкапсуляции ключей; направленное шифрование; алгебраические решетки; криптографическая стойкость.

Табл. 5. Ил. 3. Библиогр.: 14 назв.

UDC 004.056.55

Processes and methods for selecting system-wide parameters and analysis of resistance against third-party channel attacks for the key encapsulation mechanism DSTU 8961:2019 / *V.A. Kulibaba* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 71 – 78.

In recent years, there has been significant progress in the creation of quantum computers. If scalable quantum computers are implemented in the near future, this will jeopardize the security of the most widely used public key cryptosystems. The most vulnerable are public-key schemes based on factorization, discrete logarithms and elliptic curve cryptography. Currently, the main task is to develop, evaluate, study and standardize asymmetric crypto transformations at the international level, including mechanisms of key encapsulation and directional encryption, resistant to attacks by violators of the post-quantum period. An important feature of the transition and post-quantum period is the usage of new mathematical methods to opposite quantum crypto analysis. The paper considers the main attacks on the mechanisms of key encapsulation and directional encryption, as well as system-wide parameters of the DSTU 8961: 2019 standard, which affect the resistance to attacks and the complexity of transformations. Methods for generating system-wide parameters of 5 and 7 levels of stability – 512 bits of classical and 256 bits of quantum security, as well as the protection of the algorithm from attacks by third-party channels are considered. The dependence of encryption and decryption time on the level of stability is analyzed. The results of calculations of system-wide parameters for stability levels 256/128, 384/192 and 512/256 are presented, as well as recommendations for the selection of system-wide parameters depending on the environment and computing capabilities. Sets of parameters selected and recommended for use in the DSTU 8961: 2019 standard are given. Conclusions are drawn about the possibility of applying the DSTU 8961 standard in the post-quantum period.

Key words: system parameters; key encapsulation mechanisms; direct encryption; algebraic lattices; cryptographic stability.

5 tab. 3 fig. Ref: 14 items.

УДК 003.026:004.056

Властивості багатовимірного алгоритму Rainbow та його здатність протистояти різноманітним методам криптоаналізу і атаці сторонніми каналами / *Д.В. Гармаш* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 79 – 84.

Розглядається аналіз сутності та можливості захисту постквантового криптографічного алгоритму Rainbow. Визначаються основні властивості алгоритму Rainbow та загальна суть криптографічних алгоритмів шифрування та електронного підпису на основі мультиваріативних квадратичних перетворень. Наводяться основні положення стосовно протоколів. Наводяться аналізи стосовно здатності захисту алгоритму від різноманітних атак. Досліджується вразливість алгоритму до атаки сторонніми каналами. Розглядаються загальні положення алгоритму. Алгоритм зображується та розглядається з математичної точки зору, також викладається математична суть криптографічних алгоритмів шифрування та електронного підпису на основі мультиваріативних квадратичних перетворень. Вивчається застосування різноманітних методів криптоаналізу против криптографічного алгоритму на основі мультиваріативних квадратичних перетворень Rainbow. Аналізується метод знижен-

ня рангу проти алгоритму Rainbow. Вивчається метод криптоаналізу за допомогою атаки на Oil-Vinegar схему та метод криптоаналізу "метод мінранку". Досліджується атака за допомогою структури багатошаровості.

Ключові слова: Rainbow; криптоаналіз; вразливість; мінранк; схема; алгоритм.

Бібліогр.: 9 назв.

УДК 003.026:004.056

Свойства мультивариативного алгоритма Rainbow и его способность противостоять различным методам криптоанализа и атаке посторонними каналами / *Д.В. Гармаш* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 79 – 84.

Рассматривается анализ сущности и возможности защиты постквантового криптографического алгоритма Rainbow. Определяются основные свойства алгоритма Rainbow и общая суть криптографических алгоритмов шифрования и электронной подписи на основе мультивариативних квадратичных преобразований. Приводятся основные положения относительно протоколов. Приводятся анализы относительно способности защиты алгоритма от различных атак. Исследуется уязвимость алгоритма к атаке сторонними каналами. Рассматриваются общие положения алгоритма. Алгоритм изображается и рассматривается с математической точки зрения, излагается математическая суть криптографических алгоритмов шифрования и электронной подписи на основе мультивариативних квадратичных преобразований. Изучается применение различных методов криптоанализа против криптографического алгоритма на основе мультивариативних квадратичных преобразований Rainbow. Анализируется метод снижения ранга против алгоритма Rainbow. Изучается метод криптоанализа с помощью атаки на Oil-Vinegar схему и метод криптоанализа "метод минранку". Исследуется атака с помощью структуры многослойности.

Ключевые слова: Rainbow; криптоанализ; уязвимость; минранк; схема; алгоритм.

Библиогр.: 9 назв.

UDC 003.026:004.056

Properties of the Rainbow multi-variant algorithm and its ability to resist various crypto-analysis methods and attack by outside channels / *D.V. Harmash* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 79 – 84.

This work presents the analysis of the essence and possibilities of protection of the Rainbow post-quantum cryptographic algorithm. The main properties of the Rainbow algorithm and the general essence of cryptographic encryption and electronic signature algorithms based on multivariate quadratic transformations are determined. The main provisions regarding the protocols are given. Analyses are given regarding the ability to protect the algorithm against various attacks. The vulnerability of the algorithm to attack by third-party channels is investigated. The general provisions of the algorithm are considered. The algorithm is presented and considered from a mathematical point of view, as well as the mathematical essence of cryptographic algorithms for encryption and electronic signature based on multivariate quadratic transformations. The application of various methods of cryptanalysis against cryptographic algorithm based on multivariate quadratic Rainbow transformations is studied. The method of decreasing rank against the Rainbow algorithm is analyzed. The method of cryptanalysis by attacking the Oil-Vinegar scheme and the method of cryptanalysis "minranku method" are investigated. The attack is studied using a multilayer structure.

Key words: Rainbow; cryptanalysis; vulnerability; minrank; scheme; algorithm.

Ref: 9 items.

УДК 003.026:004.056

Аналіз захищеності постквантового алгоритму електронного підпису Rainbow від потенційних атак / *Г.А. Малєєва* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 85 – 93.

Багатовимірна криптографія на основі відкритого ключа є кандидатом для постквантової криптографії, і це дозволяє генерувати особливо короткі підписи та швидку перевірку. Схема підписів Rainbow, запропонована Дж. Діном та Д. Шмідтом, є такою багатовимірною криптосистемою і вважається захищеною від усіх відомих атак. Необхідність проведення досліджень ЦП Rainbow обґрунтовується тим, що назріла необхідність розроблення та прийняття постквантового національного стандарту ЦП, а також тим, що в процесі проведення конкурсу NIST США стосовно математичних основ застосування методу криптографічного перетворення Rainbow отримано перспективні результати. Тому вважається важливим їх врахування та використання в Україні. Схема підпису Rainbow може бути реалізована просто та ефективно за допомогою лінійних методів алгебри над невеликим кінцевим полем і, зокрема, створює коротші підписи, ніж ті, що використовуються в RSA та інших постквантових підписах. У 2-му раунді NIST PQC пропонуються захищені набори параметрів Rainbow і проаналізовано кілька атак на них. При порівнянні ЕП перевага віддається алгоритмам ЕП, що пройшли відбір за безумовними критеріями, а також, що мають кращі показники щодо інтегральних умовних критеріїв, оскільки така методика є більш раціональною. Зокрема, атака Rainbow-Band-Separation (RBS) є найкращою серед відомих атак на Rainbow з певним набором параметрів і є важливою. Атака Rainbow-Band-Separation відновлює секретний ключ Rainbow, розв'язуючи певні системи квадратичних рівнянь, а його складність оцінюється за відомим показником, який називається ступенем регулярності. Однак, як правило, ступінь регулярності більша, ніж ступінь розв'язання в експериментах, і точної оцінки отримати неможливо. У роботі запропоновано новий показник складності атаки Rainbow-Band-Separation за допомогою алгоритму F_4, який дає більш точну оцінку порівняно з показником, що використовує ступінь регулярності.

Мета роботи – порівняльний аналіз ЕП на основі MQ-перетворень за критерієм стійкість-складність та спроба зрозуміти безпеку Rainbow від атаки RBS за допомогою F_4.

Ключові слова: : багатовимірна криптографія; аналіз атак; постквантовий період.

Табл. 4. Іл. 1. Бібліогр.: 6 назв.

УДК 003.026:004.056

Анализ защищенности постквантового алгоритма электронной подписи Rainbow от потенциальных атак / *А.А. Малеева* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 85 – 93.

Многомерная криптография на основе открытого ключа является кандидатом для постквантовой криптографии, и это позволяет генерировать особенно короткие подписи и быструю проверку. Схема подписей Rainbow, предложенная Дж. Дином и Д. Шмидтом, является такой многомерной криптосистемой и считается защищенной от всех известных атак. Необходимость проведения исследований ЦП Rainbow обосновывается тем, что назрела необходимость разработки и принятия постквантового национального стандарта ЦП, а также тем, что в процессе проведения конкурса NIST США математических основ применения метода криптографического преобразования Rainbow получены перспективные результаты. Поэтому считается важным их учет и использование в Украине. Схема подписи Rainbow может быть реализована просто и эффективно с помощью линейных алгебраических методов над небольшим конечным полем и, в частности, создает короткие подписи, в отличие от тех, что используются в RSA и других постквантовых подписях. Во 2-м раунде NIST PQC предлагаются защищенные наборы параметров Rainbow и проанализированы несколько атак на них. При сравнении ЭП предпочтение отдается методам ЭП, которые прошли отбор по безусловными критериям, а также имеют лучшие показатели по интегральным условным критериям, поскольку такая методика является более рациональной. В частности, атака Rainbow-Band-Separation (RBS) является лучшей среди известных атак на Rainbow с определенным набором параметров и важна. Атака Rainbow-Band-Separation восстанавливает секретный ключ Rainbow, решая определенные системы квадратичных уравнений, а его сложность оценивается по известному показателю, который называется степенью регулярности. Однако, как правило, степень регулярности больше, чем степень решения в экспериментах, и точной оценки получить невозможно. В работе предложен новый показатель сложности атаки Rainbow-Band-Separation с помощью алгоритма F_4, который дает более точную оценку по сравнению с показателем, использует степень регулярности.

Цель работы – сравнительный анализ ЭП на основе MQ-преобразований по критерию устойчивость-сложность и попытка понять безопасность Rainbow от атаки RBS с помощью F_4.

Ключевые слова: многомерная криптография; анализ атак; постквантовий период.

Табл. 4. Ил. 1. Библиогр.: 6 назв.

UDC 003.026:004.056

Analysis of security of post-quantum algorithm of Rainbow electronic signature against potential attacks / *G.A. Maleeva* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 85 – 93.

Multidimensional public key cryptography is a candidate for post-quantum cryptography, and it makes it possible to generate particularly short signatures and quick verification. The Rainbow signature scheme proposed by J. Dean and D. Schmidt is such a multidimensional cryptosystem and it is considered to be protected against all known attacks. The need for research on Rainbow ES is justified by the fact that there is a need to develop and adopt a post-quantum national securities standard, and that in the process of the US NIST competition on the mathematical basis of cryptographic transformation method Rainbow, promising results. Therefore, it is considered important to take them into account and use them in Ukraine. The Rainbow signature scheme can be implemented simply and efficiently using linear algebra methods over a small finite field and, in particular, creates shorter signatures than those used in RSA and other post-quantum signatures [1]. In the 2nd round of NIST PQC, protected sets of Rainbow parameters are offered and several attacks on them are analyzed [1]. When comparing ES, preference is given to ES algorithms that have been selected according to unconditional criteria, as well as those that have better indicators for integral conditional criteria, because such a technique is more rational. In particular, the Rainbow-Band-Separation (RBS) attack [2] is the best known Rainbow attack with a certain set of parameters and is important. The Rainbow-Band-Separation attack restores the Rainbow secret key by solving certain systems of quadratic equations, and its complexity is measured by a well-known measure called the degree of regularity. However, as a rule, the degree of regularity is greater than the degree of solution in experiments, and it is impossible to obtain an accurate estimate. The paper proposes a new indicator of the complexity of the Rainbow-Band-Separation attack using F_4 algorithm, which gives a more accurate estimate compared to the indicator that uses the degree of regularity.

The aim of the work is a comparative analysis of ES based on MQ-transformations on the criterion of stability-complexity and an attempt to understand the security of Rainbow against RBS attack using F_4.

Key words: multidimensional cryptography; attack analysis; postquantum period.

4 tab. 1 fig. Ref: 6 items.

УДК 621.391:519.2

Методи побудови та властивості логарифмічних підписів / *Є.В. Котух, О.В. Северинов, А.В. Власов, Л.С. Козіна, А.О. Теницька, Е. О. Зарудна* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 94 –99.

Розвиток та перспективні напрями досліджень у побудові практичних моделей квантових комп'ютерів сприяє пошуку та розробці ефективних криптографічних примітивів. Разом зі зростанням практичних можливостей використання квантових обчислень зростає загроза класичним схемам шифрування та електронного підпису, які використовують як основу класичні математичні проблеми, що долаються обчислювальними можливостями квантових комп'ютерів. Цей факт мотивує дослідження фундаментальних теорем, що стосуються математичних та обчислювальних аспектів постквантових криптосистем-кандидатів. Однією з актуальних проблем є розробка нової квантово стійкої асиметричної криптосистеми. Перспективним напрямом розробки асиметричних криптосистем є використання логарифмічних підписів і покриттів кінцевих груп. Актуальний стан цього напряму й праці останніх років дають підстави припускати, що завдання факторизації елемента кінцевої групи в теорії побудови криптосистем на основі неабелевих груп з використанням логарифмічних підписів є обчислювально складні, що потенційно забезпечує необхідний рівень криптографічного захисту перед атаками, що використовують можливості квантових обчислень. У роботі представлено логарифмічні підписи як особливий тип факторизації в кінцевих групах, розглянуто їх властивості та методи побудови.

Ключові слова: постквантова криптографія, логарифмічні підписи, покриття, неабелеві групи.

Бібліогр.: 13 назв.

УДК 621.391:519.2

Методы построения и свойства логарифмических подписей / *Е.В. Котух, А.В. Северинов, А.В. Власов, Л.С. Козина, А.А. Теницкая, Е. А. Зарудная* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. С. 94 –99.

Развитие и перспективные направления исследований в построении практических моделей квантовых компьютеров способствуют поиску и разработке эффективных криптографических примитивов. Вместе с ростом практических возможностей использования квантовых вычислений растет угроза классическим схемам шифрования и электронной подписи, которые используют как основу классические математические проблемы, преодолеваются вычислительными возможностями квантовых компьютеров. Этот факт мотивирует исследования фундаментальных теорем, касающихся математических и вычислительных аспектов постквантовых криптосистем-кандидатов. Одной из актуальных проблем является разработка новой квантово-устойчивой асимметричной криптосистемы. Перспективным направлением разработки ассиметричных криптосистем является использование логарифмических подписей и покрытий конечных групп. Актуальное состояние этого направления и работы последних лет дают основания предполагать, что задача факторизации элемента конечной группы в теории построения криптосистем на основе неабелевых групп с использованием логарифмических подписей является вычислительно сложной, потенциально обеспечивает необходимый уровень криптографической защиты перед атаками, использующими возможности квантовых вычислений. Представлены логарифмические подписи как особый тип факторизации в конечных группах, рассмотрены их свойства и методы построения.

Ключевые слова: постквантовая криптография, логарифмические подписи, накрытия, неабелевые группы.

Библиогр.: 13 назв.

UDC 621.391:519.2

Methods of construction and properties of logariphmic signatures / *E.V. Kotukh, O.V. Severinov, A.V. Vlasov, L.S. Kozina, A.O. Tenytska, E.O. Zarudna* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. C. 94 –99.

Development and promising areas of research in the construction of practical models of quantum computers contributes to the search and development of effective cryptographic primitives. Along with the growth of the practical possibilities of using quantum computing, the threat to classical encryption and electronic signature schemes using classical mathematical problems as a basis, being overcome by the computational capabilities of quantum computers. This fact motivates the study of fundamental theorems concerning the mathematical and computational aspects of candidate post-quantum cryptosystems. Development of a new quantum-resistant asymmetric cryptosystem is one of the urgent problems. The use of logarithmic signatures and coverings of finite groups a promising direction in the development of asymmetric cryptosystems. The current state of this area and the work of recent years suggest that the problem of factorizing an element of a finite group in the theory of constructing cryptosystems based on non-Abelian groups using logarithmic signatures is computationally complex; it potentially provides the necessary level of cryptographic protection against attacks using the capabilities of quantum calculations. The paper presents logarithmic signatures as a special type of factorization in finite groups; it also considers their properties and construction methods.

Key words: post-quantum cryptography, logarithmic signatures, coverings, non-abelian groups.

Ref: 13 items.

ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ
ФИЗИКА ПРИБОРОВ, ЭЛЕМЕНТОВ И СИСТЕМ
PHYSICS OF INSTRUMENTS, ELEMENTS AND SYSTEMS

УДК 621.373.826

Принципи побудови гіроскопа на базі фотонно-кристалічних волокон з фотонною забороненою зоною / *Аль-Судані Хайдер Алі* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 100 – 107.

Гіроскоп – пристрій, який дозволяє вимірювати зміну кутів орієнтації зв'язаного з ним тіла обертання відносно інерціальної системи координат. Гіроскопи з фотонно-кристалічними волокнами є свого роду оптичні

гіроскопи, які дають безліч нових і поліпшених характеристик, крім тих, які можуть запропонувати звичайні волоконно-оптичні гіроскопи. У будь-якому випадку властивості оптичного волокна можуть зіграти велику роль у визначенні характеристик гіроскопа. Принцип дії більшості оптичних гіроскопів оснований на ефекті Саньяка (Sagnac) або інтерферометрі Саньяка, суть якого полягає в наступному. Якщо в замкнутому оптичному контурі (інтерферометрі) в протилежних напрямках поширюються дві світлові хвилі, то у випадку нерухомого контура фазові набіги обох хвиль, що пройшли увесь контур в протилежних напрямках, будуть однаковими. При обертанні контура навколо осі, нормальної до площини контуру, фазові набіги хвиль стають неоднаковими, а їх різниця (фазовий зсув) в загальному випадку буде пропорційний кутовій швидкості обертання контура, площі, яку охоплює контур, і частоті електромагнітної хвилі (ЕМХ). Оскільки під час роботи гіроскопа площа і частота ЕМХ залишаються незмінними, фазовий зсув буде пропорційний тільки кутовій швидкості. Використання фотонно-кристалічного волокна для підвищення чутливості є дуже перспективним, воно значно зменшує дрейф через термічні поляризаційні нестійкості і ефект Керра. У статті запропоновано використовувати в порожнистій серцевині оптичного гіроскопу фотонно-кристалічне волокно 1550nmλ, Ø10 мкм замість звичайних волокон.

Ключові слова: оптичний гіроскоп; ефект Саньяка; фотонно-кристалічне волокно.

Іл. 6. Бібліогр.: 11 назв.

УДК 621.373.826

Принципы построения гироскопов на базе фотонно-кристаллических волокон с фотонной запрещенной зоной / *Аль-Судани Хайдер Али* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 100 – 107.

Гироскоп – устройство, которое позволяет измерять изменение углов ориентации связанного с ним тела вращения относительно инерциальной системы координат. Гироскопы с фотонно-кристаллическими волокнами представляют собой своего рода оптические гироскопы, которые дают множество новых и улучшенных характеристик, кроме тех, которые могут предложить обычные волоконно-оптические гироскопы.

В любом случае свойства оптического волокна могут сыграть большую роль в определении характеристик гироскопа. Принцип действия большинства оптических гироскопов основан на эффекте Саньяка (Sagnac) или интерферометре Саньяка, суть которого заключается в следующем. Если в замкнутом оптическом контуре в противоположных направлениях распространяются две световые волны, то в случае недвижимого контура фазовые набеги обеих волн, прошедших весь контур в противоположных направлениях, будут одинаковыми. При вращении контура вокруг оси, нормальной к плоскости контура, фазовые набеги волн становятся неодинаковыми, а их разница в общем случае будет пропорциональна угловой скорости вращения контура, площади, охватывающей контур, и частоте электромагнитной волны (ЭМВ). Поскольку во время работы гироскопа площадь и частота ЭМВ остаются неизменными, фазовый сдвиг будет пропорционален только угловой скорости. Использование фотонно-кристаллического волокна для повышения чувствительности является перспективным, оно значительно уменьшает дрейф через термические поляризационные нестойкости и эфект Керра. В статье предложено использовать в полой сердцевине оптического гироскопа фотонно-кристаллическое волокно 1550nmλ, Ø10 мкм вместо обычных волокон.

Ключевые слова: оптический гироскоп; эффект Саньяка; фотонно-кристаллическое волокно.

Ил. 6. Библиогр.: 11 назв.

UDC 621.373.826

Principles of constructing gyroscopes based on photonic crystal (band-gap) fibers / *Al-Sudani Haider Ali Muse* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 100 – 107.

The gyroscope is a device that makes it possible to measure the change in the orientation angles associated rotation of the body relative to an inertial coordinate system. Photonic crystal fiber gyroscopes are a kind of optical gyroscopes that offer many new features beyond that conventional fiber optic gyroscopes can offer. In any case, the properties of the optical fiber can play a large role in determining the characteristics of the gyroscope. The principle of operation of most optical gyroscopes is based on the Sagnac effect or the Sagnac interferometer, the essence of which is as follows. If two light waves propagate in a closed optical circuit in opposite directions, then in the case of an immovable circuit, the phase incursions of both waves that have passed the entire circuit in opposite directions will be the same. When the contour rotates around an axis normal to the contour plane, the phase incursions of the waves become unequal, and their difference in the general case will be proportional to the angular velocity of the contour rotation, the area covered by the contour, and the frequency of the electromagnetic wave (EMW). Since the area and frequency of the EMW remain unchanged during the operation of the gyroscope, the phase shift will be proportional only to the angular velocity. The use of photonic crystal fiber to increase the sensitivity is very promising; it significantly reduces the drift through thermal polarization, resistance, and the Kerr effect. This article suggests the use of photonic-crystal (hollow-core) fiber in optical gyroscope instead of conventional fibers.

Key words: optical gyroscope; photonic crystal (hollow core) fiber; Sagnac effect.

6 fig. Ref: 11 items.

УДК 621.382.232

Модифікація активної області резонансно-тунельного діоду / *К.С. Яцун* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 108 – 112.

В останні роки зріс інтерес до вивчення мезоскопічних структур. У першу чергу це обумовлено розвитком напівпровідникової технології, яка дозволяє створювати структури із розмірами порядку одиниць та десятків нанометрів. Лінійні розміри таких структур поступаються довжині хвилі де-Бройля електронів, тому транспорт електронів визначається, в основному, їх хвильовими властивостями що, у свою чергу приводить до появи цілого ряду нових ефектів.

До мезоскопічних структур можна віднести резонансно-тунельний діод (РТД), вперше запропонований Есакі та Тсу, і який є одним із перших приладів наноелектроніки. Він складається із шару напівпровідника з доволі вузькою забороненою зоною – шару квантової ями (КЯ), розташованого між двома шарами напівпровідника (бар'єрами) з більш широкою забороненою зоною. Ці шари, у свою чергу, розташовуються між шарами (спейсерами) слабко легованого вузького напівпровідника, за якими слідують сильно леговані шари емітера і колектора. У КЯ виникають один або декілька енергетичних рівнів розмірного квантування. Під дією напруги зміщення струм через РТД проходить лише у тому випадку, якщо у емітері присутні електрони які можуть тунелювати. Резонансне тунелювання відбувається на енергетичний рівень у КЯ, а з нього – у колектор, де спектр енергетичних станів – зонний. РТД має дуже високу швидкодію, наприклад відомо, що нелінійні властивості РТД зберігаються аж до 10^4 ТГц. Також РТД має і інші унікальні властивості: він являється єдиним приладом наноелектроніки який може працювати при кімнатній температурі, а на ВАХ РТД спостерігаються ділянки негативної диференційної провідності (НДП).

У статті досліджується принцип дії резонансно-тунельного діоду та детально розглядаються явища тунелювання у нанофізиці. Проводиться розрахунок моделі вольт-амперної характеристики (ВАХ) двохбар'єрного резонансно-тунельного діоду. Досліджено, як зміна коефіцієнтів прозорості та відбиття потенційного бар′єру прямокутної форми впливають на ВАХ РТД. Це дослідження може бути базовим для подальшого розгляду того, як модифікація активної області резонансно-тунельного діоду впливає на його характеристики. Окрім того, результати досліджень дозволяють якісно оцінювати енергію, необхідну електронам для тунелювання крізь структуру РТД.

Ключові слова: потенційний бар′єр; квантове обмеження; тунелювання; квантова яма; рівняння Шредінгера; негативна диференційна провідність; резонансно-тунельний діод.

Іл. 1. Бібліогр.: 6 назв.

УДК 621.382.232

Модификация активной области резонансно-туннельного диода / *К.С. Яцун* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 108 – 112.

В последние годы значительно возрос интерес к изучению мезоскопических структур. В первую очередь это обусловлено развитием полупроводниковой технологии, которая позволяет создавать структуры с размерами порядка единиц и десятков нанометров. Линейные размеры таких структур уступают длине волны де-Бройля электронов, поэтому транспорт электронов определяется, в основном, их волновыми свойствами что, в свою очередь приводит к появлению целого ряда новых эффектов.

К мезоскопическим структурам можно отнести резонансно-туннельный диод (РТД), впервые предложенный Эсаки и Тсу, и который является одним из первых приборов наноэлектроники. Он состоит из слоя полупроводника с довольно узкой запрещенной зоной – слоя квантовой ямы (КЯ), расположенного между двумя слоями полупроводника (барьерами) с более широкой запрещенной зоной. Эти слои, в свою очередь, располагаются между слоями (спейсерами) слабо легированного узкого полупроводника, за которыми следуют сильно легированные слои эмиттера и коллектора. В КЯ возникают один или несколько энергетических уровней размерного квантования. Под действием напряжения смещения ток через РТД проходит только в том случае, если в эмиттере присутствуют электроны, которые могут туннелировать. Резонансное туннелирование происходит на энергетический уровень в КЯ, а из него – в коллектор, где спектр энергетических состояний – зонный. РТД имеет очень высокое быстродействие, например, известно, что нелинейные свойства РТД сохраняются до 10^4 ТГц. Также РТД имеет и другие уникальные свойства: он является единственным прибором наноэлектроники, который может работать при комнатной температуре, а на ВАХ РТД наблюдаются участки отрицательной дифференциальной проводимости (НДП).

В статье исследуется принцип действия резонансно-туннельного диода и рассматриваются явления туннелирования в нанофизике. Проводится расчет модели вольтамперной характеристики (ВАХ) двухбарьерного резонансно-туннельного диода. Исследовано, как изменение коэффициентов прозрачности и отражения потенциального барьера прямоугольной формы влияют на ВАХ РТД. Это исследование может быть базовым для дальнейшего рассмотрения того, как модификация активной области резонансно-туннельного диода влияет на его характеристики. Кроме того, результаты исследований позволяют качественно оценивать энергию, необходимую электронам для туннелирования через структуру РТД.

Ключевые слова: потенциальный бартер; квантовое ограничение; тунелирование; квантовая яма; уравнение Шредингера; отрицательная дифференциальная проводимость; резонансно-туннельный диод.

Ил. 1. Библиогр.: 6 назв.

UDC 621.382.232

Modification of active region of resonant tunnel diode / *K.S. Yatsun* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 108 – 112.

Interest in the study of mesoscopic structures has grown significantly in recent years. This is primarily due to the development of semiconductor technology, which makes it possible to create structures with sizes of the order of units

and tens of nanometers. The linear dimensions of such structures are inferior to the de Broglie wavelength of electrons, so the transport of electrons is determined mainly by their wave properties, which, in turn, leads to a number of new effects.

Mesoscopic structures include the resonant tunnel diode (RTD), first proposed by Esaki and Tsu, and which is one of the first nanoelectronic devices. It consists of a semiconductor layer with a fairly narrow band gap, a quantum well (QW) layer located between two semiconductor layers (barriers) with a wider band gap. These layers, in turn, are located between the layers (spacers) of weakly doped narrow semiconductor, followed by highly doped layers of the emitter and collector. There are one or more energy levels of dimensional quantization in the QW. Under the action of bias voltage, the current passes through the RTD only if the emitter contains electrons that can tunnel. Resonant tunneling occurs at the energy level in the QW, and from there to the collector, where the spectrum of energy states is band. RTD has a very high speed of action, for example, it is known that the nonlinear properties of RTD persist up to 104 THz. The RTD is also of great power: it is the only device of nanoelectronics that can be used at room temperatures, and on the VAC of the RTD the areas of negative differential conductivity (NDC) are observed.

In this article, the principle of a resonant tunneling diode is revealed, and the phenomena of tunneling in nanophysics are examined in detail. The volt-ampere characteristic (VAC) model of a two-barrier resonance tunnel diode is calculated. The paper investigates how the change of transparency coefficients and the reflection of the potential barrier of a rectangular shape affect the VAC of the RTD. This study can be the basis for further consideration of how the modification of the active region of the resonant tunnel diode affects its characteristics. In addition, the results of the research allow us to estimate qualitatively the energy required by electrons for tunneling through the structure of the RTD.

Key words: potential barrier; quantum constraint; tunneling; quantum well; Schrödinger equation; negative differential conductivity; resonant-tunnel diode.

1 fig. Ref: 6 items.

УДК 621.373.072.9

Похибка методів малого параметру при вирішенні укорочених рівнянь синхронізованого автогенератора / *В.В. Рапін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 113 – 117.

Розглядається застосування аналітичних методів вирішення укорочених рівнянь синхронізованого автогенератора. Це метод квазімалого параметра та комбінований метод малого параметра. В обох методах використовується класичний метод малого параметра. Особливістю його застосування є те, що в даному випадку він використовується для вирішення нелінійних диференційних рівнянь, які не містять малий параметр. Відмінність вказаних методів полягає в отриманні рівнянь першого наближення.

У методі квазімалого параметра – це лінійні диференціальні рівняння, отримані шляхом лінеаризації вихідних нелінійних диференційних рівнянь в області нульової частотної розстройки. У комбінованому методі малого параметра рівняння першого наближення отримані методом аппроксимації вихідних нелінійних диференційних рівнянь. Звичайно для цього було здійснено ряд перетворювань цих рівнянь. Апроксимація дозволила краще представити вихідні нелінійні диференціальні рівняння лінійними диференційними рівняннями. Це призвело до отримання меншої похибки, яка в обох випадках представлялася у вигляді нев'язки, з якої безпосередньо не представляється можливим отримати відносну похибку і дослідити її особливість.

Дослідження відносної похибки методу квазімалого параметра залежно від частотної розлади показало, що це безперервна функція з нульовим значенням при нульовій частотній розладі.

Для комбінованого методу малого параметру функція, що представляє відносну похибку, має розрив при нульовій частотній розстройці. Однак розрив такого виду, тобто з існуючою загальною межею, відноситься до категорії розривів, які можливо усунути.

Ключові слова: синхронізований автогенератор; укорочені рівняння; методи малого параметра; нев 'язка; похибка.

Іл. 4. Бібліогр.: 15 назв.

УДК 621.373.072.9

Погрешность методов малого параметра при решении укороченных уравнений синхронизированного автогенератора / *В.В. Рапин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 113 – 117.

Рассматривается применение недавно появившихся аналитических методов решения укороченных уравнений синхронизированного автогенератора. Это метод квазималого параметра и комбинированный метод малого параметра. В обоих методах используется классический метод малого параметра. Особенностью его применения является то, что в данном случае он используется для решения нелинейных дифференциальных уравнений, которые не содержат малый параметр. Отличие указанных методов состоит в получении уравнений первого приближения. В методе квазималого параметра – это линейные дифференциальные уравнения, полученные путем линеаризации исходных нелинейных дифференциальных уравнений в окрестности нулевой частотной расстройки. В комбинированном методе малого параметра уравнения первого приближения получены методом аппроксимации исходных нелинейных дифференциальных уравнений. Конечно, был произведен ряд преобразований этих уравнений. Аппроксимация позволила лучше представить исходные нелинейные дифференциальные уравнения линейными дифференциальными уравнениями. Это обеспечило меньшую погреш-

ность, которая в обоих случаях представлялась в виде невязки, из которой непосредственно невозможно получить относительную погрешность и исследовать ее особенность.

Исследование относительной погрешности метода квазималого параметра в зависимости от частотной расстройки позволило установить, что это непрерывная функция с нулевым значением при нулевой частотной расстройке.

Для комбинированного метода малого параметра функция, представляющая относительную погрешность, имеет разрыв при нулевой частотной расстройке. Однако разрыв такого вида, т.е. с существующим общим пределом, относится к категории устранимых разрывов.

Ключевые слова: синхронизированный автогенератор; укороченные уравнения; методы малого параметра; невязка; погрешность.

Ил. 4. Библиогр.: 15 назв.

UDC 621.373.072.9

Error of small parameter methods in solving shortened equations of a synchronized oscillator / *V.V. Rapin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 113 – 117.

The paper considers the use of recently appeared analytical methods for solving shortened equations of a synchronized oscillator. These are a quasi-small parameter method and a combined small parameter method. Both methods use the classic small parameter method. A peculiarity of their application is that in this case they are used for solving nonlinear differential equations that do not contain a small parameter. The difference between the above methods is in obtaining the equations of the first approximation. In the quasi-small parameter method, they are linear differential equations obtained by linearizing the original nonlinear differential equations in the area of the zero frequency detuning. In the combined small parameter method, the equations of the first approximation are obtained by approximating the original nonlinear differential equations. Of course, a number of transformations of these equations were made for this. The approximation made it possible to obtain better representation of the original nonlinear differential equations by means of linear differential equations. This representation provided a smaller error, which in both cases was presented as a discrepancy. The discrepancy does not allow obtaining a relative error and investigating its peculiarity.

A study of the relative error of the quasi-small parameter method shows that this error is a continuous function of the frequency detuning with a zero value for a zero frequency detuning.

A function representing relative error has a gap at zero frequency detuning for the combined small parameter method. However, this kind of gap can be eliminated by additional function definition.

Key words: synchronized oscillator; shortened equations; small parameter methods; discrepancy; error.

4 fig. Ref: 15 items.

АНТЕНИ ТА ПРИСТРОЇ МІКРОХВИЛЬОВОЇ ТЕХНІКИ
АНТЕННЫ И УСТРОЙСТВА МИКРОВОЛНОВОЙ ТЕХНИКИ
ANTENNAS AND MICROWAVE DEVICES

УДК 662.396.67

Поздовжній розподіл інтенсивності поля круглої сфокусованої апертури / *В.В. Должиков* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 118 – 128.

Антени мікрохвильового і міліметрового діапазонів, сфокусовані в зону Френеля, які зазвичай називають антенами з фокусуванням в зону Френеля, стають все більш популярними. У порівнянні зі звичайними антенами, сфокусованими в далеку зону (синфазними), вони можуть забезпечити найкращі характеристики при відносно невеликій вартості реалізації в системах зв'язку малого радіусу дії, в пристроях бездротової передачі енергії, в установках дистанційного неруйнівного зондування, в пристроях радіочастотної ідентифікації та багатьох інших. В роботі отримано аналітичні вирази для розрахунку основних параметрів, що характеризують поздовжній розподіл інтенсивності поля антени у вигляді круглої сфокусованої апертури з відносно великим діаметром $\left(2R/\lambda \geq 10\right)$: зміщення максимуму інтенсивності щодо точки фокусування, посилення фокусування, глибини фокусування. Розглянуто випадки рівномірного і спадаючого амплітудних розподілів поля збудження. Знайдені наближені співвідношення дозволяють визначити значення згаданих параметрів для будь-яких значень поздовжньої координати точки фокусування, що лежать як в зоні Френеля, так і в далекій зоні. Порівняння з чисельними розрахунками показало, що похибка одержуваних значень параметрів не перевищує 5 %. Результати роботи будуть корисними при розрахунку поля антен у вигляді круглої сфокусованої апертури, а також сфокусованих антенних решіток, що працюють в зоні Френеля.

Ключові слова: сфокусовані апертурні антени; зона Френеля; посилення фокусування; глибина фокусування.

Іл. 13. Бібліогр.: 14 назв.

УДК 662.396.67

Продольное распределение интенсивности поля круглой сфокусированной апертуры / *В.В. Должиков* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 118 – 128.

Антенны микроволнового и миллиметрового диапазонов, сфокусированные в зону Френеля, которые обычно называют антеннами с фокусировкой в зону Френеля, становятся все более популярными. По сравне-

нию с обычными антеннами, сфокусированными в дальнюю зону (синфазными), они могут обеспечить лучшие характеристики при относительно небольшой стоимости реализации в системах связи малого радиуса действия, в устройствах беспроводной передачи энергии, в установках дистанционного неразрушающего зондирования, в устройствах радиочастотной идентификации и многих других. В работе получены аналитические выражения для расчета основных параметров, характеризующих продольное распределение интенсивности поля антенны в виде круглой сфокусированной апертуры с относительно большим диаметром $\left(2R/\lambda \geq 10\right)$: смещения максимума интенсивности относительно точки фокусировки, усиления фокусировки, глубины фокусировки. Рассмотрены случаи равномерного и спадающего амплитудных распределений поля возбуждения. Найденные приближенные соотношения позволяют определить значения упомянутых параметров для любых значений продольной координаты точки фокусировки, лежащих как в зоне Френеля, так и в дальней зоне. Сравнение с численными расчетами показало, что погрешность получаемых значений параметров не превышает 5 %. Результаты работы будут полезны при расчете поля антенн в виде круглой сфокусированной апертуры, а также сфокусированных антенных решеток, работающих в зоне Френеля.

Ключевые слова: сфокусированные апертурные антенны; зона Френеля; усиление фокусировки; глубина фокусировки.

Ил. 13. Библиогр.: 14 назв.

UDC 662.396.67

Longitudinal distribution of the field intensity of a circular focused aperture / *V.V. Dolzhikov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 118 – 128.

Microwave and millimeter-wave antennas focused in their Fresnel zone, which are usually named as near-field focused (NFF) antennas, are becoming increasingly popular. Indeed, when compared to conventional far-field focused antennas, they can guarantee performance improvement at a relatively limited implementation cost, in short-range communication systems, wireless power transfer arrangements, remote nondestructive sensing setups, and radiofrequency identification apparatus, among many others. In this paper, analytical expressions are obtained for calculating the main parameters characterizing the longitudinal distribution of the circular focused aperture field intensity with a relatively large diameter $\left(2R/\lambda \geq 10\right)$: the displacement of the intensity maximum relative to the focal point, focusing gain and depth of focus. Cases of uniform and decreasing amplitude distributions of the excitation field are considered. The found approximate relations make it possible to determine the values of the above parameters for any values of the longitudinal coordinate of the focal point, lying both in the Fresnel zone and in the far zone. Comparison with numerical calculations showed that the error in the obtained parameter values does not exceed 5%. The results of this paper will be useful when calculating the field of antennas in the form of a circular focused aperture, as well as focused antenna arrays operating in the Fresnel zone.

Key words: focused aperture antennas; Fresnel zone; focal shift; focusing gain; depth of focus.

13 fig. Ref: 14 items.

РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ
РАДИОЛОКАЦИЯ И НАВИГАЦИЯ
RADIOLOCATION AND NAVIGATION

УДК 004.89: 621.396

Метод перетворення символьних радарних відміток малопомітних рухомих об'єктів на основі ефекту Тальбота / *В.В. Жирнов, С.В. Солонська* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 129 – 137.

Розглядається метод перетворення символьних зображень радарних відміток малопомітних рухомих повітряних об’єктів з мерехтливими міжперіодними флуктуаціями, що приводять іноді до повного зникнення сигналу, за допомогою ефекту Тальбота. Ці перетворення зводяться до встановлення певної відповідності асимптотичної рівності сприйняття зорових картин, довільним чином мінливих в часі і просторі, до твердження про умови простої рівності сприйняття зображень радіолокаційних відміток, які мають різні частоти флуктуацій. Пропоноване перетворення символьних зображень – це математично обґрунтований метод перетворення символьного зображення малопомітних радарних відміток на основі ефекту Тальбота. Показано, як цей підхід може використовуватися для інтелектуального аналізу радіолокаційних даних за рахунок перетворення й згладжування невидимих на тлі завад мерехтливих флуктуацій сигналу у видимі символьні зображення. По-перше, для автоматичного виявлення й розпізнавання повітряних об’єктів з аналізу зв’язків та функціональних (семантичних) залежностей між ознаками. По-друге, для прийняття рішення на основі семантичних складових символьних зображень радарних відміток. Експериментально перевірено можливість використання таких перетворень для формування частотно-імпульсних кодів символьних зображень флуктуацій радарних відміток типу ангел-луна як важливої характеристики для їх розпізнавання. Сформульовано алгоритми автоматичного формування символьних зображень в асинхронному та синхронному частотно-імпульсному коді. Символьне зображення, представлене таким кодом, є додатковою ознакою для розпізнавання та відсіювання природних завад типу ангел-луна.

Ключові слова: символьне зображення; нестаціонарна радарна відмітка; ефект Табольта; виявлення; розпізнавання; інтелектуальний аналіз.

Іл. 7. Бібліогр.: 13 назв.

УДК 004.89: 621.396

Метод преобразования символьных радарных отметок малозаметных подвижных объектов на основе эффекта Тальбота / *В.В. Жирнов, С.В. Солонская* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 129 – 137.

Рассматривается метод преобразования символьных изображений радарных отметок малозаметных подвижных воздушных объектов с мерцающими межпериодными флуктуациями, приводящими иногда к полному исчезновению сигнала, с помощью эффекта Тальбота. Эти преобразования сводятся к установлению определенного соответствия асимптотического равенства восприятия зрительных картин, произвольным образом меняющихся во времени и пространстве, к утверждению об условиях простого равенства восприятия изображений радиолокационных отметок, которые имеют разные частоты флуктуаций. Предлагаемое преобразование символьных изображений – это математически обоснованный метод преобразования символьного изображения малозаметных радарных отметок на основе эффекта Тальбота. Показано, как этот подход может использоваться для интеллектуального анализа радиолокационных данных за счет преобразования и сглаживания, невидимых на фоне помех мерцающих флуктуаций сигнала в видимые символьные изображения. Во-первых, для автоматического обнаружения и распознавания объектов локации из анализа связей и функциональных (семантических) зависимостей между признаками. Во-вторых, для принятия решения на основе семантических составляющих символьных изображений радарных отметок. Экспериментально проверена возможность использования таких преобразований для формирования частотно-импульсных кодов символьных изображений флюктуаций радарных отметок типа «ангел-эхо» как важной характеристики для их распознавания. Сформулированы алгоритмы автоматического формирования символьных изображений в асинхронном и синхронном частотно-импульсном коде. Символьное изображение, представленное таким кодом, является дополнительным признаком для распознавания и отсеивания естественных помех типа ангел-эхо.

Ключевые слова: символьное изображение; нестационарная радарная отметка; эффект Табольта; обнаружение; распознавание; интеллектуальный анализ.

Ил. 7. Библиогр.: 13 назв.

UDC 004.89: 621.396

Method for transforming symbolic radar marks of low-noticeable moving objects based on the Talbot effect / *V. Zhyrnov, S. Solonskaya* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 129 – 137.

In this paper a method to transform radar images of moving aerial objects with scintillating inter-period fluctuations, sometimes resulting to complete signal fading, using the Talbot effect is considered. These transformations are reduced to the establishment of a certain correspondence of the asymptotic equality of perception of visual images, arbitrarily changing in time and space, in the statement about the conditions of simple equality of perception of images of radar marks that have different frequencies of fluctuations. It is shown how this approach can be used to analyze radar data by transforming and smoothing scintillating signal fluctuations, invisible in the presence of interference, into visible symbolic images. First, to detect and recognize the aerial objects from the analysis of relations and functional (semantic) dependencies between attributes, second, to make a decision based on semantic components of symbolic radar images. The possibility of using such transformation to generate pulse-frequency code of fluctuations of the symbolic radar angel-echo images as an important characteristic for their recognition has been experimentally verified. Algorithms for generating symbolic images in asynchronous and synchronous pulse-frequency code are formulated. The symbolic image represented by such a code is considered as an additional feature for recognizing and filtering out natural interferences such as angel-echoes.

Key words: symbolic image; non-stationary radar marker; Tabolt effect; detection; recognition; intellectual analysis.

7 fig. Ref: 13 items.

УДК 621.396.96, 621.397.48:004.932.2

Методи виявлення-розпізнавання радіолокаційних, акустичних, оптичних і інфрачервоних сигналів безпілотних літальних апаратів / *В.М. Карташов, В.О. Посошенко, В.В. Воронін, В.І. Колесник, А.І. Капуста, М.В. Рибников, Є.В. Першин* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 138 – 153.

Захист різноманітних об'єктів від впливу безпілотних літальних апаратів (БПЛА), що несуть потенційну загрозу у військовій, господарській і повсякденній областях діяльності людини, – одна з актуальних задач сучасності. У даний час відома велика кількість публікацій, присвячених опису методів і систем, заснованих на різних фізичних принципах, які призначені для виявлення і спостереження БПЛА на тлі наявних перешкод. У них розглядаються канали прийому, способи обробки прийнятих інформаційних сигналів і подальшого їх інтелектуального аналізу. Показано, що відомі методи енергетичного виявлення сигналів БПЛА недостатньо ефективні, оскільки операція виконується, як правило, на тлі перешкод, що мають певні структурні подібності з сигналом БПЛА. Значна увага приділяється методам інтерпретації одержуваних даних з використанням навчаємих нейронних мереж. Оскільки кількість публікацій в даній області постійно збільшується, то актуальним відповідно до цього є завдання аналізу, узагальнення та систематизації наявних в літературі даних.

Стаття є оглядовою і присвячена узагальненню і систематизації відомих методів прийому та обробки радіолокаційних, акустичних, оптичних і інфрачервоних сигналів з метою виявлення-розпізнавання, вимірювання координат і параметрів руху БПЛА.

Ключові слова: безпілотний літальний апарат; виявлення; розпізнавання; радіолокаційна станція; содар; відеокамера; зображення; акустичний сигнал.

Іл. 4. Бібліогр.: 86 назв.

УДК 621.396.96, 621.397.48:004.932.2

Методы обнаружения-распознавания радиолокационных, акустических, оптических и инфракрасных сигналов беспилотных летательных аппаратов / *В.М. Карташов, В.О. Посошенко, В.В. Воронин, В.И. Колесник, А.И. Капуста, Н.В. Рыбников, Е.В. Першин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 138 – 153.

Защита разнообразных объектов от воздействия беспилотных летательных аппаратов (БПЛА), несущих потенциальную угрозу в военной, хозяйственной и повседневной областях деятельности человека, – одна из актуальных задач современности. Известно большое количество публикаций, посвященных описанию методов и систем, основанных на разных физических принципах, которые предназначены для обнаружения и наблюдения БПЛА на фоне имеющихся помех. В них рассматриваются каналы приема, способы обработки принимаемых информационных сигналов и последующего их интеллектуального анализа. Показано, что известные методы энергетического обнаружения сигналов БПЛА недостаточно эффективны, поскольку операция выполняется, как правило, на фоне помех, имеющих определенные структурные сходства с сигналом БПЛА. Большое внимание уделяется методам интерпретации получаемых данных с использованием обучаемых нейронных сетей. Поскольку количество публикаций в данной области постоянно увеличивается, то актуальной в соответствии с этим является задача анализа, обобщения и систематизации имеющихся в литературе данных.

Статья является обзорной и посвящена обобщению и систематизации известных методов приема и обработки радиолокационных, акустических, оптических и инфракрасных сигналов с целью обнаружения-распознавания, измерения координат и параметров движения БПЛА.

Ключевые слова: беспилотный летательный аппарат; обнаружение; распознавание; радиолокационная станция; содар; видеокамера; изображение; акустический сигнал.

Ил. 4. Библиогр.: 86 назв.

UDC 621.396.96, 621.397.48:004.932.2

Methods for detection-recognition of radar, acoustic, optical and infrared signals of unmanned aerial vehicles / *V.M. Kartashov, V.A. Pososhenko, V.V. Voronin, V.I. Kolesnik, A.I. Kapusta, N.V. Rybnikov, E.V. Pershin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 138 – 153.

The protection of various objects against the impact of unmanned aerial vehicles (UAVs), which carry a potential threat in the military, economic and everyday areas of human activity, is one of the urgent tasks of our time. Currently, there are a large number of publications devoted to the description of methods and systems based on different physical principles designed to detect and observe UAVs against the background of existing interference. They consider the reception channels, methods of processing the received information signals and their subsequent intelligent analysis. It is shown, that the known methods of energy detection of UAV signals are insufficiently effective, since the operation is performed, as a rule, against a background of noise that has certain structural similarities with the UAV signal. Considerable attention is paid to the methods for interpreting the obtained data using trained neural networks. Since the number of publications in this area is constantly increasing, the task of analyzing, generalizing and systematizing the data available in the literature is relevant in accordance with this.

The article is an overview and it is devoted to the generalization and systematization of known methods of receiving and processing radar, acoustic, optical and infrared signals for detection-recognition, measurement of coordinates and parameters of UAV movement.

Key words: unmanned aerial vehicle; detection; recognition; radar station; sodar; video camera; image; acoustic signal.

4 fig. Ref: 86 items.

УДК 621.396.96

Метод підвищення завадозахищеності радіолокаційних систем ідентифікації «свій-чужий» при дії навмисних корельованих завад / *І.В. Свид, І.І. Обод, О.С. Мальцев, М.Г. Ткач, С.В. Старокожев, А.О. Глущенко, В.С. Чумак* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 154 – 160.

Проаналізовано принципи побудови і структуру систем ідентифікації «свій-чужий» та виявлено, що у існуючій системі зацікавлена сторона має можливість несанкціоновано використати даний інформаційний ресурс для дальнього визначення координат повітряних об’єктів, з одного боку, та перекручування інформації цього інформаційного ресурсу, з другого боку, що призводить до непередбачуваних наслідків. Показано, що найбільш вразливим місцем в системах ідентифікації «свій-чужий» є літаковий відповідач, який істотно впливає на завадостійкість та завадозахищеність ідентифікаційних систем повітряних об'єктів. Запропоновано метод спадкоємного переходу до завадостійких систем ідентифікації «свій-чужий» на основі синхронних мереж систем ідентифікації, який дозволяє істотно розширити методи обслуговування заявок та методи побудови систем. Така методика побудови ідентифікаційних систем виключає наявну проблему розосереджених ідентифікаційних си-

стем, а також проблему часового узгодження сигналів, що поступають з систем первинної та вторинної радіолокації. Запропонований метод спадкоємного переходу до завадостійких систем ідентифікації «свій-чужий» дозволяє виключити можливість несанкціонованого доступу зацікавленої сторони до ідентифікаційних інформаційних ресурсів, що значною мірою підвищує завадозахищеність ідентифікаційної системи в цілому.

Ключові слова: радіолокаційна система; система ідентифікації «свій-чужий»; управління повітряним рухом; повітряний об'єкт; літаковий відповідач; завадозахищеність; завадостійкість; сигнал запиту; сигнал відповіді; оптимізація; мережева структура; відносна пропускна здатність.

Іл. 1. Бібліогр.: 25 назв.

УДК 621.396.96

Метод повышения помехозащищенности радиолокационных систем идентификации «свой-чужой» при действии преднамеренных коррелированных помех / *И.В. Свид, И.И. Обод, А.С. Мальцев, М.Г. Ткач, С.В. Старокожев, А.А. Глущенко, В.С. Чумак* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 154 – 160.

Проанализированы принципы построения и структура систем идентификации «свой-чужой» и выявлено, что в существующей системе заинтересованная сторона имеет возможность несанкционированно использовать данный информационный ресурс для дальнего определения координат воздушных объектов, с одной стороны, и искажения информации этого информационного ресурса, с другой стороны, что приводит к непредсказуемым последствиям. Показано, что наиболее уязвимым местом в системах идентификации «свой-чужой» является самолетный ответчик, который существенно влияет на помехоустойчивость и помехозащищенность идентификационных систем воздушных объектов. В работе предложен метод наследственного перехода к помехоустойчивых систем идентификации «свой-чужой» на основе синхронных сетей систем идентификации, который позволяет существенно расширить методы обслуживания заявок и методы построения систем. Такая методика построения идентификационных систем исключает имеющуюся проблему рассредоточенных идентификационных систем, а также проблему временного согласования сигналов, поступающих из систем первичной и вторичной радиолокации. Предложенный метод наследственного перехода к помехоустойчивых систем идентификации «свой-чужой» позволяет исключить возможность несанкционированного доступа заинтересованной стороной в идентификационные информационные ресурсы, в значительной мере повышает помехозащищенность идентификационной системы в целом.

Ключевые слова: радиолокационная система; система идентификации «свой-чужой»; управления воздушным движением; воздушный объект; самолетный ответчик; помехозащищенность; помехоустойчивость; сигнал запроса; сигнал ответа; оптимизация; сетевая структура; относительная пропускная способность.

Ил. 1. Библиогр.: 25 назв.

UDC 621.396.96

Method for increasing noise immunity of radar "friend or foe" identification systems under the action of intentional correlated interference / *I.V. Svyd, I.I. Obod, O.S. Maltsev, M.G. Tkach, S.V. Starokozhev, A.O. Hlushchenko, V.S. Chumak* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 154 – 160.

The paper analyzes the principles of construction and structure of "friend or foe" identification systems. It is revealed, that the party, interested in the existing system, has the ability of unauthorized use of this information resource for long-range determination of air objects coordinates, on the one hand, and distortion of information of this information resource, on the other hand, which leads to unpredictable consequences. It is shown, that the most vulnerable place in the "friend or foe" identification systems is the aircraft transponder, which significantly affects noise stability and noise immunity of the identification systems of air objects. The paper proposes a method of hereditary transition to noise-immune "friend or foe" identification systems based on synchronous networks of identification systems, which allows expanding significantly the methods of servicing requests and methods of constructing systems. This method of constructing identification systems eliminates the existing problem of dispersed identification systems, as well as the problem of temporal matching of signals coming from primary and secondary radar systems. The proposed method of hereditary transition to noise-immune "friend or foe" identification systems makes it possible to exclude the possibility of unauthorized access to identification information resources by an interested party, significantly increases the noise immunity of the identification system as a whole.

Key words: radar system; "friend or foe" identification system; air traffic control; air object; aircraft transponder; noise immunity; noise stability; request signal; answer signal; optimization; network structure; relative bandwidth.

1 fig. Ref.: 25 items.

РАДІОТЕХНІЧНІ ПРИСТРОЇ ТА ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ
РАДИОТЕХНИЧЕСКИЕ УСТРОЙСТВА И СПОСОБЫ ТЕЛЕКОММУНИКАЦИИ
RADIO ENGINEERING DEVICES AND TELECOMMUNICATION METHODS

УДК 621.396.677.49

Моделі поширення сигналів мереж зв'язку 5 G / *Ю.Ю. Коляденко, М.О. Чурсанов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 161 – 168.

Технологія нового покоління 5G / IMT-2020, як і будь-яка нова технологія, привносить свої специфічні особливості в усі аспекти, що стосуються практики її застосування. Одним з таких особливо важливих аспектів

є електромагнітна сумісність. На етапі підготовки до впровадження радіомереж технології 5G, названої NewRadio, необхідно завчасно подбати про вжиття заходів щодо ефективної оцінки умов електромагнітної сумісності для цих мереж на основі ретельного аналізу особливостей технології 5G, а правильно і точно оцінивши ці умови – успішно забезпечити електромагнітну сумісність радіозасобів нових мереж.

На Всесвітній конференції радіозв'язку ВКР-15 були визначені нові діапазони радіочастот для 5G, в тому числі діапазони сантиметрових і міліметрових хвиль. Цей радіочастотний спектр розміщений в трьох областях: нижче 1 ГГц, від 1 ГГц до 6 ГГц і вище 6 ГГц (до 100 ГГц). В якості головних особливостей спектра, з точки зору ЕМС, можна виділити наступне: різний характер втрат при поширенні сигналу, зокрема значний вплив на рівень втрат додаткових раніше невідомих в стільниковому зв'язку факторів (гази – кисень, водяна пара та ін.).

Розроблено математичну модель поширення сигналів мереж зв'язку 5 G, яка враховує ослаблення сигналів у вільному просторі, ослаблення сигналів, викликане впливом стін і перекриттів поверхів, втрати енергії сигналу при заповненні простору різними предметами, ослаблення сигналів, викликане втратою енергії радіохвиль при поширенні через дощі, ослаблення сигналів, викликане втратою енергії радіохвиль через туман, ослаблення сигналів при поширення через листя дерев, повільні і швидкі випадкові завмирання.

Ключові слова: мережі зв'язку 5G; електромагнітна сумісність; математична модель поширення сигналів.

Табл. 4. Бібліогр.: 26 назв.

УДК 621.396.677.49

Модели распространения сигналов сетей связи 5 G / *Ю.Ю. Коляденко, Н.А. Чурсанов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 161 – 168.

Технология нового поколения 5G / IMT-2020, как и любая новая технология, привносит свои специфические особенности во все аспекты, касающиеся практики ее применения. Одним из таких особо важных аспектов является электромагнитная совместимость. На этапе подготовки к внедрению радиосетей технологии 5G, названной NewRadio, необходимо заблаговременно позаботиться о принятии мер по эффективной оценки условий электромагнитной совместимости для этих сетей на основе тщательного анализа особенностей технологии 5G, а правильно и точно оценив эти условия – успешно обеспечить электромагнитную совместимость радиосредств новых сетей.

На Всемирной конференции радиосвязи ВКР-15 были определены новые диапазоны радиочастот для 5G, в том числе диапазоны сантиметровых и миллиметровых волн. Этот радиочастотный спектр размещен в трех областях: ниже 1 ГГц, от 1 ГГц до 6 ГГц и выше 6 ГГц (до 100 ГГц). В качестве главных особенностей спектра, с точки зрения ЭМС, можно выделить следующее: различный характер потерь при распространении сигнала, в частности, значительное влияние на уровень потерь дополнительных ранее неизвестных в сотовой связи факторов (газы – кислород, водяной пар и др.).

Разработана математическая модель распространения сигналов сетей связи 5 G, которая учитывает ослабление сигналов в свободном пространстве, ослабление сигналов, вызванное влиянием стен и перекрытий этажей, потери энергии сигнала при заполнении пространства различными предметами, ослабление сигналов, вызванное потерей энергии радиоволн при распространении через дожди, ослабление сигналов, вызванное потерей энергии радиоволн из-за тумана, ослабление сигналов при распространение через листья деревьев, медленные и быстрые случайные замирания.

Ключевые слова: сети связи 5G; электромагнитная совместимость; математическая модель распространения сигналов.

Табл. 4. Библиогр.: 26 назв.

UDC 621.396.677.49

5 G communication network signal propagation models / *Yu.Yu. Kolyadenko, N.A. Chursanov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 161 – 168.

The next generation 5G / IMT-2020 technology, like any new technology, brings its own specific features to all aspects related to the practice of its application. One of these particularly important aspects is electromagnetic compatibility. At the stage of preparation for the introduction of 5G radio networks, called NewRadio, it is necessary to take early measures to assess effectively the electromagnetic compatibility conditions for these networks based on a thorough analysis of the features of 5G technology. Correct and accurate assessments of these conditions means successful provision of the electromagnetic compatibility of radio equipment of new networks.

The World Radio Communication Conference WRC-15 identified new radio frequency bands for 5G, including centimeter and millimeter wave bands. In general, this RF spectrum is located in three regions: below 1 GHz, 1 GHz to 6 GHz, and above 6 GHz (up to 100 GHz). From the EMC standpoint, the following can be distinguished as the main features of this spectrum: different nature of losses during signal propagation, in particular, a significant influence of additional factors (gases – oxygen, water vapor, etc.) on the level of losses previously unknown in cellular communication.

The mathematical model of signal propagation of 5 G communication networks has been developed which takes into account: the attenuation of signals in free space; attenuation of signals caused by the influence of walls and floor slabs, loss of signal energy, when space is filled with various objects; attenuation of signals caused by loss of energy of radio waves, when propagating through rains; signal attenuation due to loss of radio wave energy due to fog; signal attenuation, when propagating through tree leaves, slow and fast random fading.

Key words: 5G communication networks; electromagnetic compatibility; mathematical model of signal propagation.

4 tab. Ref: 26 items.

РАДІОТЕХНІЧНІ СИСТЕМИ
РАДИОТЕХНИЧЕСКИЕ СИСТЕМЫ
RADIO ENGINEERING SYSTEMS

УДК 621.391.82: 004.056.53

Ефективні режими роботи радіозакладних пристроїв для потайного знімання інформації у полі шумових завад / *С.П. Сергієнко, В.Г. Крижановський, Д.В. Чернов, Л.В. Загорулько* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 169 – 174.

Інформаційна безпека сучасного суспільства знаходиться у постійній протидії і постійному удосконаленні технічних засобів, які використовуються для несанкціонованого знімання інформації, і технічних засобів, які цьому заважають. В роботі проаналізовано приклади методів застосування шумових завад для протидії несанкціонованому зніманню інформації. Проаналізовано та показано можливість несанкціонованого знімання інформації пасивними радіопристроями з використанням шумових завад, які застосовуються для боротьби з підслуховуючими пристроями. Передача несакціоновано знятої інформації можливо по радіохвильовим каналам і по низькочастотним каналам з використанням металевих конструкцій або комунікацій будівель. В якості моделі шумових завад використовувався випадковий вузько-смуговий сигнал з законом розподілу Гауса. Електрична модель пристрою моделювалася довгою лінію з високочастотним діодом на кінці. В якості вольт-амперної характеристики діоду використовувалась ідеалізована експонентна залежність струму від напруги. Отримано спектри відбитої хвилі при різних співвідношеннях опору довгої лінії і диференційного опору діоду та зовнішньої напруги зміщення прикладеної до діоду. Проаналізовано режими і особливості передачі аналогової і цифрової інформації радіозакладним пристроєм з використанням енергії радіошумових завад. В радіозакладному пристрої інформація передається відбитою хвилею, спектр якої спотворюється на нелінійним елементі на кінці довгої лінії. Роботу пристрою проаналізовано у всьому можливому частотному діапазоні, пов’язаному з частотним спектром падаючої шумової завади. Розраховано оптимальні параметри елементів пасивної електричної схеми: опір довгої лінії, диференційний опір діоду, напруга зміщення та режим модуляції в залежності від частотного діапазону, в якому можливий витік інформації.

Ключові слова: пасивні радіозаставні пристрої; радіозашумлення що маскує; нелінійне перетворення спектра шуму; захист інформації.

Іл. 8. Бібліогр.: 11 назв.

УДК 621.391.82: 004.056.53

Эффективные режимы работы радиозакладных устройств для скрытого снимания информации в поле шумовых помех / *С.П. Сергиенко, В.Г. Крыжановский, Д.В. Чернов, Л.В. Загорулько* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 169 – 174.

Информационная безопасность современного общества находится в постоянном противодействии и постоянном совершенствовании технических средств, используемых для несанкционированного съема информации, и технических средств, которые этому мешают. В работе проанализированы примеры методов применения шумовых помех для противодействия несанкционированному съему информации. Показана и проанализирована возможность несанкционированного съема информации пассивными радиоустройствами с использованием шумовых помех, которые применяются для борьбы с подслушивающими устройствами. Передача несанкционированно снятой информации возможна как по радиоволновым каналам, так и по низкочастотным каналам с использованием металлических конструкций или коммуникаций зданий. В качестве модели шумовых помех использовался случайный узкополосный сигнал, имеющий закон распределения Гаусса. Электрическая модель устройства моделировалась длинной линией с высокочастотным диодом на конце. В качестве вольтамперной характеристики диода использовалась идеализированная экспоненциальная зависимость тока от напряжения. Получены спектры отраженной волны при различных соотношениях сопротивления длинной линии, дифференциального сопротивления диода и внешнего напряжения смещения, приложенного к диоду. Проанализированы режимы и особенности передачи аналоговой и цифровой информации радиозакладным устройством с использованием энергии радиошумовых помех. В радиозакладном устройстве информация передается отраженной волной, спектр которой искажается на нелинейном элементе, стоящем на конце длинной линии. Работа устройства проанализирована по всему возможному частотному диапазону, связанному с частотным спектром падающей шумовой помехи. Рассчитаны оптимальные параметры элементов пассивной электрической схемы: сопротивление длинной линии, дифференциальное сопротивление диода, напряжение смещения и режим модуляции в зависимости от частотного диапазона, в котором возможна утечка информации.

Ключевые слова: пассивные радиозакладные устройства; маскирующие радио зашумление; нелинейное преобразование спектра шума; защита информации.

Ил. 8. Библиогр.: 11 назв.

UDC 621.391.82: 004.056.53

Effective modes of operation of radio-bombing devices for covert information gathering in the field of noise interference / *S.P. Serhiienko , V.G. Krizhanovski, D.V. Chernov, L.V. Zahoruiko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 169 – 174.

The information security of modern society is in constant counteraction and constant improvement of technical means used for unauthorized information pickup, and technical means that prevent it. The paper analyzes examples of

methods of applying noise interference to counteract the unauthorized pickup. The possibility of unauthorized pickup by passive radio devices using noise interferences is shown and analyzed using noise interferences, which are used to suppress the eavesdropping devices. The transfer of picked up information is possible both by radio wave and low-frequency channels using metal structures or water pipes. As a model of noise interference, a random narrow-band signal with a Gaussian distribution was used. The electrical model of the device was simulated by a transmission line with a high-frequency diode at its end. The idealized exponential dependence of the diode current on the voltage was used. The reflected wave spectra are obtained for different ratios of the transmission line resistance, the differential resistance of diode, and the external offset voltage at the diode. The modes and features of analog and digital information transmission by the radio tab device using energy of radio noises are analyzed. In the radio tab device, the information is transmitted by reflected wave, the spectrum of which is distorted at a nonlinear element placed at the end of transmission line. An analysis of the device operation was carried out along the full possible frequency range associated with the spectrum of the incident noise interference. The optimal elements parameters for the passive electrical circuit are calculated: the resistance of the transmission line, the differential resistance of the diode, the offset voltage, and the modulation mode, depending on the frequency range in which the leak is possible.

Key words: passive radio embedded devices; masking radio noise; nonlinear noise spectrum transformation; information protection.

8 fig. Ref: 11 items.

УДК 621.396

Шумоподібні дискретні сигнали для асинхронних систем кодового поділу радіоканалів / *О.О. Кузнецов, О.А. Смирнов, Т.Ю. Кузнецова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205. С. 175 – 183.

Розглянуто шумоподібні дискретні сигнали (псевдовипадкові послідовності) для асинхронних систем кодового розподілу радіоканалів. Асинхронність передбачає використання послідовностей, статистично некорельованих для довільної циклічно зрушеної копії сигналів, тобто коефіцієнт їх взаємної кореляції для довільно обраних початкових точок близький до нуля. Фундаментальною теоретичною межею для цієї характеристики є відома межа Велча. Проведено порівняння кореляційних властивостей різних множин (коди Голда, послідовності Касамі та ін.) З цією фундаментальною межею. Проведено оцінку параметрів різних кодів, наведено відповідну межу і порівняння її з реальними кореляційними характеристиками кодів. Для апроксимації використовувалося розкладання в ряд Лорана і ряд Пюїзе. Також оцінювалися асимптотичні властивості. Розглянуто нові ансамблі шумоподібних дискретних сигналів для асинхронних систем. Ці коди статистично некорельовані, асимптотично квадрат їх взаємної кореляції для довільно обраних початкових точок прагне до теоретичної межі Велча. При цьому кардинальність (потужність безлічі) нових ансамблів сигналів значно вище, ніж у кодів Голда і множин Касамі. Отже, практичне використання таких шумоподібних дискретних сигналів дозволить підвищити ємність асинхронних систем кодового розподілу радіоканалів і здешевити послуги зв'язку. Крім того, нові набори розширювальних сигналів будуть корисні для реалізації так званої м'якої ємності (Soft Capacity), тобто коли при необхідності базова станція може збільшити абонентську ємність при незначному зниженні якості обслуговування.

Ключові слова: шумоподібні дискретні сигнали; розширювальна послідовність; множинний доступ; пряме розширення спектра; асинхронні системи кодового поділу радіоканалів.

Табл. 1. Бібліогр.: 26 назв.

УДК 621.396

Шумоподобные дискретные сигналы для асинхронных систем кодового разделения радиоканалов / *А.А. Кузнецов, А.А. Смирнов, Т.Ю. Кузнецова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 205. С. 175 – 183.

Рассмотрены шумоподобные дискретные сигналы (псевдослучайные последовательности) для асинхронных систем кодового разделения радиоканалов. Асинхронность предполагает использование последовательностей, статистически некоррелированных для произвольной циклически сдвинутой копии сигналов, т.е. коэффициент их взаимной корреляции для произвольно выбранных начальных точек близок к нулю. Фундаментальным теоретическим пределом для этой характеристики является известная граница Велча. Проведено сравнение корреляционных свойств различных множеств (коды Голда, последовательности Касами и пр.) с этим фундаментальным пределом. Проведена оценка параметров разных кодов, приведена соответствующая граница и сравнение ее с реальными корреляционными характеристиками кодов. Для аппроксимации использовалось разложение в ряд Лорана и ряд Пюизо. Также оценивались асимптотические свойства. Рассмотрены новые ансамбли шумоподобных дискретных сигналов для асинхронных систем. Эти коды статистически некоррелированы, асимптотически квадрат их взаимной корреляции для произвольно выбранных начальных точек стремится к теоретической границе Велча. При этом кардинальность (мощность множества) новых ансамблей сигналов значительно выше, чем у кодов Голда и множеств Касами. Следовательно, практическое использование таких шумоподобных дискретных сигналов позволит повысить емкость асинхронных систем кодового разделения радиоканалов и удешевить услуги связи. Кроме того, новые наборы расширяющих сигналов будут полезны для реализации так называемой мягкой емкости (Soft Capacity), т.е. когда при необходимости базовая станция может увеличить абонентскую емкость при незначительном снижении качества обслуживания.

Ключевые слова: шумоподобные дискретные сигналы; расширяющая последовательность; множественный доступ; прямое расширение спектра; асинхронные системы кодового разделения радиоканалов.

Табл. 1. Библиогр.: 26 назв.

UDC 621.396

Noise-like discrete signals for asynchronous code division radio systems / *A.A. Kuznetsov, O.A. Smirnov, T.Y. Kuznetsova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №205. P. 175 – 183.

This article discusses noise-like discrete signals (pseudo-random sequences) for asynchronous code division systems for radio channels. Asynchrony implies the use of sequences that are statistically uncorrelated for an arbitrary cyclically shifted copy of the signals, i.e. their cross-correlation coefficient for arbitrarily chosen starting points is close to zero. The fundamental theoretical limit for this characteristic is the well-known Welch boundary. In this paper, we compare the correlation properties of various sets (Gold codes, Kasami sequences, etc.) with this fundamental limit. The parameters of different codes are estimated, the corresponding bound is shown and compared with the real correlation characteristics of the codes. For the approximation, the Laurent series expansion and the Puiseau series were used. The asymptotic properties were also estimated. The paper also considers new ensembles of noise-like discrete signals for asynchronous systems. These codes are statistically uncorrelated, asymptotically the square of their cross-correlation for arbitrary starting points tends to the theoretical Welch bound. Moreover, the cardinality (power of the set) of new signal ensembles is much higher than that of Gold codes and Kasami sets. Consequently, the practical use of such noise-like discrete signals will increase the capacity of asynchronous code division systems for radio channels and reduce the cost of communication services. In addition, new sets of spreading signals will be useful for the implementation of the so-called. soft capacity, i.e. when, if necessary, the base station can increase the subscriber capacity with a slight decrease in the quality of service.

Key words: noise-like discrete signals; spreading sequence; multiple access; direct spreading of the spectrum; asynchronous code division radio system.

1 tab. Ref: 26 items.