РЕФЕРАТЫ РЕФЕРАТИ ABSTRACTS

ЗАЩИЩЕННЫЕ ТЕЛЕКОМУНИКАЦИОННЫЕ СИСТЕМЫ И ПЕРЕДАЧА ДАННЫХ
PROTECTED TELECOMMUNICATION SYSTEMS AND DATA TRANSFER

УДК 681.3.06:519.248.681

Криптографические сигналы: требования, методы синтеза, свойства, применение в телекоммуникационных системах / *И.Д. Горбенко, А.А. Замула* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 7 - 23.

Приведены математическая постановка и решение задачи синтеза системы нелинейных дискретних сложных сигналов с заданными ансамблевыми, корреляционными, статистическими свойствами. Представлен метод синтеза одного класса нелинейных дискретних сложных - криптографических сигналов (КС). Приведены результаты исследования свойств данного класса сигналов. Указаны возможные сферы применения КС в современных телекоммуникационных системах.

Табл. 5. Библиогр.: 16 назв.

УДК 681.3.06:519.248.681

Криптографічні сигнали: вимоги, методи синтезу, властивості, застосування в телекомунікаційних системах / *І.Д. Горбенко, О.А. Замула* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 7 - 23.

Наведено математичну постановку та вирішення задачі синтезу системи нелінійних дискретних складних сигналів з заданими ансамблевими, кореляційними, статистичними властивостями. Надано метод синтезу одного класу нелінійних дискретних складних сигналів - криптографічних сигналів (КС). Наведено результати досліджень властивостей даного класу сигналів. Вказані можливі сфери застосування КС в сучасних телекомунікаційних системах.

Табл. 5. Бібліогр.: 16 назв.

UDC 681.3.06:519.248.681

Cryptographic signals: requirements, synthesis methods, properties, application in telecommunication systems / *I.D. Gorbenko, A.A. Zamula* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 7 - 23.

Mathematical formulation and solution of theproblem of synthesis of the system of nonlinear discrete complex signals with predetermined ensemble, correlation, statistical properties are presented. The method of the synthesis of certain nonlinear discrete complex – cryptographic signals (CS) class is presented. The results of the given signals class properties research are cited. The possible scopes of CS application in modern telecommunications systems are indicated.

Tab. 5. Ref.: 16 items.

УДК 621.396

Информационные технологии передачи данных в современных телекоммуникационных системах / *А.А. Замула, В.Л. Морозов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 24 - 31.

В оптических системах с кодовым разделением каналов одной из основных задач является распознавание конкретного информационного сигнала среди множества других сигналов, присутствующих в канале, а также увеличение количества пользователей, одновременно работающих в системе. В целях решения данной задачи необходимо использовать последовательности с улучшенными корреляционными, и ансамблевыми характеристиками. В работе приводится анализ классов двоичных последовательностей, которые могут найти применение в современных широкополосных телекоммуникационных системах, использующих технологию прямого расширения спектра.

Ил. 6. Библиогр.: 7 назв.

УДК 621.396

Інформаційні технології передачі даних в сучасних телекомунікаційних системах / *О.А.Замула, В.Л. Морозов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 24 - 31.

В оптичних системах з кодовим поділом каналів однією з основних задач є розпізнавання конкретного інформаційного сигналу серед безлічі інших сигналів, присутніх в каналі, а також збільшення кількості користувачів, що одночасно працюють в системі. З метою вирішення даної задачі необхідно використовувати послідовності з поліпшеними кореляційними і ансамблевими характеристиками. Наводиться аналіз класів бінарних послідовностей, які можуть знайти застосування в сучасних широкосмугових телекомунікаційних системах, які використовують технологію прямого розширення спектра.

Іл. 6. Бібліогр.: 7 назв.

UDC 621.396

Informationtransmissiontechnologyinmoderntelecommunicationssystems / *A.A. Zamula, V.L. Morozov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 24 - 31.

One of the main problems in optical systems with CDMA consists in recognition of a specific information signal among many other signals present in the channel, as well as increase in the number of simultaneous users working in the system. To solve this problem it is necessary to use codes with improved correlation and ensemble performance. The paper provides an analysis of binary sequences that can be used in modern broadband telecommunication systems using direct spread-spectrum technology.

6 fig. Ref.: 7 items.

ПРОБЛЕМЫ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ И ВОЗМОЖНЫЕ НАПРАВЛЕНИЯ ИХ РАЗРЕШЕНИЯ В БУДУЩЕМ
PROBLEMS OF POST-QUANTUM CRYPTOGRAPHY AND POSSIBLE DIRECTIONS FOR THEIR RESOLUTION IN THE FUTURE

УДК 004.056.55

Постквантовая криптография и механизмы ее реализации / *И.Д. Горбенко, А.А. Кузнецов, А.В. Потий, Ю.И. Горбенко, Р.С. Ганзя, В.А. Пономарь* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 32 - 52.

Приводятся результаты анализа достижений в построении квантового компьютера. Предлагается подход определения моделей нарушителя и угроз постквантового периода. Приводятся и анализируются требования NISTи ETSI к квантово защищенным алгоритмам электронной цифровой подписи. Рассматриваются и сравниваются перспективные кандидаты и стандарты цифровой подписи в постквантовый период.

Табл. 8. Ил. 2. Библиогр.: 33 назв.

УДК 004.056.55

Постквантова криптографія та механізми її реалізації / *І.Д. Горбенко, О.О. Кузнєцов, О.В. Потій, Ю.І. Горбенко, Р.С. Ганзя, В.А.Пономар* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 32 - 52.

Наведено результати аналізу досягнень в побудові квантового комп’ютера. Пропонується підхід до визначення моделей порушника та загроз пост квантового періоду. Наводяться та аналізуються вимоги NIST та ETSI до квантово захищених алгоритмів електронного підпису(ЕП). Розглядаються та порівнюються перспективні кандидати на стандартиЕП у постквантовий період.

Табл. 8. Іл. 2. Бібліогр.: 33 назви.

UDC 004.056.55

Post quantum cryptography and mechanisms for its implementation / *I.D.Gorbenko, O. Kuznetsov, O.V.Potii, Y.I.Gorbenko, R.S. Ganzya, V.A.Ponomar* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 32 - 52.

The analysis of the achievements in the construction of a quantum computer is presented. The approach to determining of offending patterns and threats of the post-quantum period is offered. The NIST andETSI requirements to quantum secure algorithms of digital signatures are given and analyzed. Perspective candidates and digital signature standards in thepost-quantum period are considered and compared.

Tab. 8. Fig. 2. Ref.: 33 items.

УДК 004 056 55

Модель злоумышленника для систем електронной цифровой подписи в условиях квантового криптоанализа / *Ю.И. Горбенко, А.В. Шевцов, Т.Ю. Кузнецова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 53 - 69.

Рассматривается модель нарушителя в системах электронной цифровой подписи в постквантовой среде. Анализируется возможность действий злоумышленника с доступом к квантовому случайному оракулу. Анализируется аппарат теории игр и ее применение для построения модели нарушителя в условиях квантового криптоанализа. Разрабатывается модель угроз системы электронной цифровой подписи в постквантовых условиях.

Табл. 1. Ил. 2. Библиогр.: 21 назв.

УДК 004 056 55

Модель порушника систем електронних цифрових підписів в умовах квантового криптоаналізу / *Ю.І. Горбенко, О.В. Шевцов, Т.Ю. Кузнецова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 53 - 69.

Розглядається модель порушника в системах електронного цифрового підпису в постквантовому середовищі. Аналізується можливість дій зловмисника із доступом до квантового випадкового оракула. Аналізується апарат теорії ігор та його застосування для формування моделі порушника в умовах квантового криптоаналізу. Розробляється модель загроз системи електронного цифрового підпису в постквантовому середовищі.

Табл. 1. Іл. 2. Бібліогр.: 21 назв.

UDC 004 056 55

Adversary model of digital signatures schemes in terms of quantum cryptanalysis / *Y.I. Gorbenko, O.V. Shevtsov, T.U. Kuznetsova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 53 - 69.

The article is dedicated to adversary model of post-quantum digital signatures schemes. The capabilities and strategies of an attacker with access to the quantum random oracle are considered. Also, we concern game theoretic approach and its application for construction of adversarial model in terms of the quantum cryptanalysis. To this end, we present a general threat model for post-quantum digital signatures.

1 tab. 2 fig. Ref.: 21 items.

УДК 004 056 55

Несимметричные криптосистемы на алгебраических кодах для постквантового периода / *А.А. Кузнецов, А.И. Пушкарев, И.И. Сватовский, А.В. Шевцов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 70 - 90.

Рассматриваются несимметричные криптосистемы на основе алгебраического кодирования, исследуются современное состояние, существующие противоречия и перспективы практического использования на постквантовый период. Описывается алгоритм цифровой подписи на основе помехоустойчивого кодирования. Показывается перспективность использования помехоустойчивых кодов для аутентификации сообщений и намечаются направления дальнейших исследований.

Табл. 3. Ил. 1. Библиогр.: 54 назв.

УДК 004 056 55

Асиметричні криптосистеми на алгебраїчних кодах для постквантового періоду / *О.О. Кузнецов, А.І. Пушкарьов, І.І. Сватовський, О.В. Шевцов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 70 - 90.

Розглядаються несиметричні криптосистеми на основі алгебраїчного кодування, досліджується сучасний стан, існуючі протиріччя і перспективи практичного використання на постквантовий період. Описується алгоритм цифрового підпису на основі завадостійкого кодування. Показується перспективність використання завадостійких кодів для автентифікації повідомлень і намічаються напрямки подальших досліджень.

Табл. 3. Іл. 1. Бібліогр.: 54 назви.

UDC 004 056 55

Asymmetric cryptosystems on algebraic codes for post quantum period Public-key Code-Based Cryptography for the post-quantum period / *A.A. Kuznetsov, A.I. Pushkarev, I.I. Svatovskiy, O.V.Shevtsov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 70 – 90.

Code-Based Public-Key Cryptosystems based on algebraic coding are considered. In addition, The current state, existing contradictions and prospects of practical use in the post-quantum period are studied.

The digital signature algorithm based onthe error-correcting codeis presented. The perspectives of the error-correcting codes for messages authentication are shownand further research directions areshown.

3 tab. 1 fig. Ref.: 54 items.

УДК 004.056

Реализация постквантового алгоритма электронно-цифровой подписи / *А.В. Потий, А.С. Карпенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 91 - 95.

Работа посвящена реализации и анализу пост квантового алгоритма электронно-цифровой подписи (ЭЦП) с использованием хеш-функций SHA-2 и ДСТУ 7564:2014. Демонстрируются временные рамки работы алгоритма с хеш-функциями. Результаты получены в ходе вычислительных экспериментов.

Табл. 3. Ил. 3. Библиогр.:4 назв.

УДК 004.056

Реалізація постквантового алгоритма цифрового підпису / *О.В. Потій, А.С. Карпенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 91 - 95.

Робота присвячена реалізації і аналізу постквантового алгоритму цифрового підпису (ЦП) з використанням хеш-функцій SHA-2 і ДСТУ 7564: 2014. Продемонстровано часові межі роботи алгоритму з геш-функціями. Результати отримано в ході обчислювальних експериментів.

Табл. 3. Іл.3. Бібліогр.: 4 назви.

UDC 004.056

Implementation of post-quantum algorithm of electronic-digital signature / *O.V.Potii, A.S. Karpenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 91 - 95.

The work is dedicated to implementation and post quantum analysis of the electronic digital signature (EDS)algorithmusing the SHA-2 and DSTU 7564:2014hash functions. The periods of operation of the algorithm with the hash functions are demonstrated. The results are obtained during the computational experiments.

Tab. 3. Fig. 3. Ref.: 4 items.

УДК 004.056.55

Особенности и проблематика создания криптосистем, основанных на использовании изогений элиптических кривих / *В.А. Пономарь* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 96 - 102.

Рассматриваются особенности создания криптосистем на основе использования изогений элиптических кривых, которые являются стойкими к методам квантового криптоанализу. Проводится анализ защищенности таких систем и основные проблемы их создания.

Ил. 4. Библиогр.: 6 назв.

УДК 004.056.55

Особливості та проблематика створення криптосистем, заснованих на використанні ізогеній еліптичних кривих / *В.А. Пономар* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 96 - 102.

Розглядаються особливості створення криптосистем, заснованих на використанні ізогеній еліптичних кривих, що є стійкими до методів квантового криптоаналізу. Наведено аналіз захищеності таких систем та основні проблеми їх створення.

Іл. 4. Бібліогр.: 6 назв.

UDC 004.056.55

Features and problems of creating cryptosystems based on using isogeniesof elliptic curves / *V.A. Ponomar* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 96 - 102.

The paper deals with features of creating cryptosystems based on using isogenies of elliptic curves resistant to the methods of quantum cryptanalysis. The analysis of these systemssecurity and basic problems of their creation are given.

Fig. 4. Ref.: 6items.

МЕТОДЫ, МЕХАНИЗМЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
METHODS, MECHANISMS AND TOOLS OF CRYPTOGRAPHIC PROTECTION OF INFORMATION

УДК 004.056.55

Анализ, оценки и предложения относительно метода генерации системных параметров в NTRU-подобных асимметрических системах / *И.Д. Горбенко, Е.Г. Качко, К.А. Погребняк, Л.В. Макутонина* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 103 - 109.

Представлены оценки базовых возможных атак для NTRU-подобных асимметрических систем. Полученные результаты позволяют вычислить новые системные параметры с учетом текущих возможностей атак.

Табл.: 5.Библиогр.: 8 назв.

УДК 004.056.55

Аналіз, оцінки та пропозиціївідносно методу генерації системних параметрів у NTRU-подібних асиметричних системах / *І.Д. Горбенко, О.Г. Качко, К.А. Погребняк, Л.В. Макутоніна* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 103 - 109.

Надано оцінки базових можливих атак для NTRU-подібних асиметричних систем. Отримані результати дозволяють обчислювати нові системні параметри з урахуванням поточних можливостей атак.

Табл.: 5. Бібліогр.: 8 назв.

UDC 004.056.55

Analysis, assessment and proposals regarding the method of the system parameters generation in the NTRU-similar asymmetric systems / *I.D. Gorbenko, O.G. Kachko, K.A. Pogrebnyak, L.V. Makutonina* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 103 - 109.

Assessments of basic possible attacks on the NTRU-like asymmetric systems are provided. The results allow calculating new system parameters including current attacks possibilities.

Tabl.: 5.Ref.: 8items.

УДК 681.3.06

Метод нахождения порядка точки скрученной кривой Эдвардса / *А.В. Бессалов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 110 - 118.

Дан анализ свойств точек малых порядков скрученных кривых Эдвардса с параметрами $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = -1$. Доказана теорема о необходимых и достаточных условиях делимости точки кривой на 2. Предложен быстрый метод нахождения порядка точки скрученной кривой Эдвардса с почти простым порядком 4*n*.

Табл. 1. Ил. 1. Библиогр.:7 назв.

УДК 681.3.06

Метод нахождения порядка точки скрученной кривой Эдвардса / *А.В.Бессалов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 110 - 118.

Надано аналіз властивостей точок малих порядків скручених кривих Едвардса з параметрами (a/p)=(d/p)=-1. Доведена теорема про необхідні і достатні умови подільності точки кривої на 2. Запропоновано швидкий метод знаходження порядку точки скрученої кривої Едвардса з майже простим порядком 4n.

Табл. 1. Іл.1. Бібліогр.: 7 назв.

UDC 681.3.06

Method for finding of the point's order of the Edwards twisted curve / *A.V. Bessalov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 110 - 118.

The analysis of small order points properties of the Edwards twisted curves with parameters $(a/p) = (d/p) = -1$ is given. A theorem about necessary and sufficient conditions for divisibility of points of a curve by2 is proved. A fast method for finding the point'sorder of the Edwards twisted curve with nearly prime order of 4n is proposed.

Tab. 1. Fig. 1. Ref.: 7 items

УДК 621. 3.06

Усовершенствованный блочный симметричный шифр Калина / *В.И. Долгов, И.В. Лисицкая, К.Е. Лисицкий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 119 - 131.

Предлагается усовершенствованная конструкция шифра Калина, построенная на основе введения в шифр дополнительного смешивающего преобразования на его входе, позволяющего сделать шифр инвариантным к дифференциальным и линейным показателям используемых при построении его цикловых преобразований S-блоков без снижения показателей стойкости. Это достигается, что за счёт улучшения динамических показателей прихода шифра к состоянию случайной подстановки (увеличения числа S-блоков, активизируемых на первых циклах шифрования). Обсуждаются возможности использования в усовершенствованном шифре сменных узлов замены (заменяемых S-блоков). Показывается, что случайные S-блоки позволяют существенно увеличить мощность ключевого множества по отношению к оригинальной разработке.

Табл. 13. Ил. 4. Библиогр.:11 назв.

УДК 621. 3.06

Вдосконалений блоковий симетричний шифр Калина / *В.І. Долгов, І.В. Лисицька, К.Є. Лисицький* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 119 - 131.

Пропонується вдосконалена конструкція шифру Калина, що побудована на основі введення в шифр додаткового змішуючого перетворення на його вході, що дозволяє зробити шифр інваріантним до диференціальних і лінійних показників використаних при побудові його циклових перетворень S-блоків без зниження показників стійкості. Це досягається за рахунок поліпшення динамічних показників приходу шифру до стану випадкової підстановки (збільшення числа S-блоків, що активізуються на перших циклах шифрування). Обговорюються можливості використання в удосконаленому шифрі змінних вузлів заміни (змінних S-блоків). Показано, що випадкові S-блоки дозволяють істотно збільшити потужність ключової множини по відношенню до оригінальної розробки.

Табл. 13. Іл. 4. Бібліогр. 11 назв.

UDC 621. 3.06

Improved Kalina symmetric block cipher / *V.I. Dolgov, I.V. Lysytskaya, K.E. Lysytsky* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 119 - 131.

The advanced design of Kalinacipher,based on the introduction of additional mixing conversion on the cipher input, is proposed. This innovation allows you to make the cipher invariant to differential and linear indicators used in the construction of its cyclic transformations of the S-boxes without compromising durability indicators. It is achieved by improving the dynamic performance of the cipher to the arrival of a random permutation (an increase in the number of S-boxes activated in the first cycle of encryption). The possibility to use interchangeable replacement units (S-replaceable units) in the improved cipher is discussed. It is shown that random S-boxes make it possible to increase significantly the capacity of a key set with respect to the original design.

Tab.13. Fig. 4. Ref.: 11 items.

УДК 621. 3.06

Новая концепция проектирования блочных симметричных шифров / *В.І. Долгов, И.В. Лисицкая, К.Е. Лисицкий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 132 - 152.

Рассматриваются принципы построения шифра Rijndael, применённые разработчиками, позволившие этому шифру занять лидирующие позиции в технологиях проектирования и разработки блочных симметричных шифров. В качестве второй прогрессивной разработки отмечается шифр IDEA NXT. Приводятся результаты анализа перспективности решений, принятых в этих разработках. Отмечается, что, несмотря на их новизну и достигнутые высокие показатели эффективности рассматриваемых решений, исследования, проведенные в последнее время, свидетельствуют о возможностях их дальнейшего улучшения, о возможностях построения более совершенной конструкции шифрующего преобразования. Эти возможности учтены в предлагаемой новой концепции проектирования блочных симметричных шифров, строящейся на ряде выдвинутых положений. Её реализация демонстрируется на примере разработки одной из новых конструкций шифра и его модификации, построенных на основе использования принципов управляемых подстановочных преобразований. Предложенные конструкция по простоте и прозрачности решений, по показателям доказуемой стойкости к атакам дифференциального и линейного криптоанализа, а также по показателям производительности

не уступают признанному лидеру технологий блочного симметричного шифрования шифру Rijndael (AES), а по динамике прихода шифра к состоянию случайной подстановки они превосходят практически все известные решения.

Табл. 3. Ил. 4. Библиогр.:33 назв.

УДК 621. 3.06

Нова концепція проектування блокових симетричних шифрів / *В.І. Долгов, І.В. Лисицька, К.Є. Лисицький* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 132 - 152.

Розглядаються принципи побудови шифру Rijndael, застосовані розробниками, що дозволили цьому шифру зайняти лідируючі позиції в технологіях проектування та розробки блокових симетричних шифрів. В якості другої прогресивної розробки відзначається шифр IDEA NXT. Наводяться результати аналізу перспективних рішень прийнятих в цих розробках. Відзначається, що не-дивлячись на їх новизну і досягнуті високі показники ефективності розглянутих рішень, дослідження, проведені останнім часом, свідчать про можливість їх подальшого поліпшення, про можливості побудови більш досконалої конструкції шифрувального перетворення. Ці можливості враховані в запропонованій новій концепції проектування блочних симетричних шифрів, що будується на ряді висунутих положень. Її реалізація демонструється на прикладі розробки однієї з нових конструкцій шифру і його модифікації, побудованих на основі використання принципів керованих підстановлювальних перетворень. Запропоновані конструкції по простоті і прозорості рішень, за показниками доказовою стійкості до атак диференціального і лінійного криптоаналізу, а також за показниками продуктивності не поступаються визнаному лідеру технологій блокового симетричного шифрування шифру Rijndael (AES), а по динаміці приходу шифру до стану випадкової підстановки (по мінімальному числу активізуємих S-блоків першого і другого циклів) вони перевершують практично всі відомі рішення.

Табл. 3. Іл. 4. Бібліогр. 33 назв.

UDC 621. 3.06

A new concept for designing of block symmetric ciphers / *V.I. Dolgov, I.V. Lysytskaya, K.E. Lysytsky* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 132 - 152.

The principles are discussed of building the Rijndael cipher, used by the developers, these principles have allowed this cipher to take a leading position in the technologies of theblock symmetric ciphers design and development,. The cipher IDEA NXT is marked as the second progressive development.It is noted that, despite their novelty and achieved high rates of efficiency of the considered solutions, the research conducted recently indicate the ways to improve them further, the possibilities of building more advanced design of encryption conversion.These opportunities are reflected in the proposed new design concept for block symmetric ciphers based on a number of extended positions.Its implementation is demonstrated on the example of the development of one of the new designs of the cipher and its modifications based on the use of principles of managed permutational transformations.The proposed design is the simplicity and transparency of solutions, in terms of provable resistance to differential attacks and linear cryptanalysis, as well as indicators of performance is not inferior to the acknowledged leader of the technology of the Rijndael (AES)symmetric encryption block cipher. On the dynamics of arrival of the code as a random mapping (for the minimum number of the activated S-blocks of the first and second cycles)they are superior to practically all known solutions.

Tab.3. Fig. 4. Ref.: 33 items.

УДК 004.056.55

Сравнение объема ансамбля М-РСЛОС и М-РСНОС, скорости генерации на их основе для $GF(2)$ и в расширениях поля $GF(2^2)$ / *Н.А. Полуяненко, А.В. Потий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 153 - 159.

Рассмотрена модель генератора псевдослучайной последовательности на основе регистров сдвига с нелинейной обратной связью. Проведено количественное сравнение, в том числе различных комбинаций обратных связей, генерирующих последовательность максимального периода, с регистрами сдвига с линейной обратной связью. Дано сравнение производительности генераторов на основе М-РСНОС и М-РСЛОС. Сравнение проводилось для $GF(2)$ и в расширениях поля $GF(2^2)$.

Табл.: 4. Ил.: 2. Библиогр.: 8 назв.

УДК 004.056.55

Порівняння об'єму ансамблю М-РЗЛЗЗ та М-РЗНЗЗ, швидкості генерування на їх основі для $GF(2)$ та у поширеннях поля $GF(2^2)$ / *М.О. Полуяненко, О.В. Потій* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 153 - 159.

Розглянуто модель генератора псевдовипадкової послідовності з основою регістрів зсуву з нелінійним зворотним зв'язком. Проведено кількісне порівняння, крім іншого кількість різноманітних комбінацій зворотних зав'язків, що генерують послідовність максимального періоду, з регістрами зсуву з лінійним зворотним зв'язком. Надано порівняння швидкості генераторів на основі М-РЗНЗЗ та М-РЗЛЗЗ. Порівняння проведено для $GF(2)$ та в поширеннях поля $GF(2^2)$.

Табл. 4. Іл. 2. Бібліогр.: 8 назв.

UDC 004.056.55

Comparison of the M-LSFR and M-NLSFRensembles'volume, the rate of generation on their basis for the $GF(2)$ and in expansions of the $GF(2^2)$field / *N.A.Poluyanenko, O.V.Potii* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 153 - 159.

The model of the pseudo random sequence generatorbased on shift registers with a nonlinear feedback is considered. The quantitative comparison is done including the amount of different feedback combinations generating the sequence of the maximum period with shift registers linear feedback. Comparison of performance of the generators based on the M-NLSFR and M-LSFR is given. This comparison was carried out for the $GF(2)$ and in expansions of the $GF(2^2)$ field.

Tabl. 4. Fig. 2. Ref.: 8 items.

УДК 004.056.55

Сравнительный анализ свойств электронной подписи согласно ДСТУ ISO/IEC 9796-3:2014 / *М.В.Есина, Н.В. Ковалёва, И.Д.Горбенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 160 - 171.

Рассмотрены методы сравнительного анализа свойств механизмов электронной подписи (ЭП) ДСТУ ISO/IEC 9796-3:2014. Исследованы и проанализированы существующие методы сравнительного анализа ЭП на основе метода анализа иерархий и методов весовых коэффициентов. Приведены некоторые критерии и показатели, которые могут быть использованы при сравнительном анализе свойств механизмов ЭП.

Ил. 7. Библиогр.: 24 назв.

УДК 004.056.55

Порівняльний аналіз властивостей електронного підпису згідно з ДСТУ ISO/IEC 9796-3:2014 / *М.В. Єсіна, Н.В. Ковальова, І.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 160 - 171.

Розглянуто методи порівняльного аналізу властивостей механізмів електронного підпису (ЕП) ДСТУ ISO/IEC 9796-3:2014. Досліджено та проаналізовано існуючі методи порівняльного аналізу ЕП на основі методу аналізу ієрархій та методів вагових коефіцієнтів. Наведено певні критерії та показники, що можуть бути використані при порівняльному аналізі властивостей механізмів ЕП.

Іл. 7. Бібліогр.: 24 назв.

UDC 004.056.55

Comparative analysis of electronic signature properties according to the DSTU ISO/IEC 9796-3:2014 / *M.V. Yesina, N.V. Kovaleva, I.D. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 160 - 171.

The paper deals with the comparative analysis methods of electronic signature (ES) mechanisms properties according to the DSTU ISO/IEC 9796-3:2014. The existing comparative analysis methods of the ES based on the hierarchies analysis and weight indices methods are investigated and analyzed. Some criteria and indicators that can be used in the comparative analysis of the ES mechanisms properties are presented.

Fig. 7. Ref.: 24 items.

УДК 681.3.07 (3.06)

Методика измерения спектральной плотности мощности шума квантовой радиооптической системы генератора случайных чисел / *Т.А. Гриненко, А.П. Нарежний, И.Д. Горбенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 172 - 183.

Предложена методика измерения спектральной плотности мощности шума квантовых генераторов случайных чисел. Экспериментальные исследования проводились на опытной установке (прототипе) квантового генератора случайных чисел и включали сборку и настройку оптического тракта и систем магнитных катушек, а также наладку сверхвысокочастотной части и волноводного тракта квантового дискриминатора. Полученные результаты служат основой для создания экспериментального образца оптического квантового генератора случайных чисел с высокими криптографическими характеристиками в режиме гаммирования.

Ил. 5. Библиогр.: 15 назв.

УДК 681.3.07 (3.06)

Методика вимірювання спектральної щільності потужності шуму квантової радіооптичної системи генератора випадкових чисел / *Т.О. Гріненко, О.П. Нарєжній, І.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 172 - 183.

Запропоновано методику вимірювання спектральної щільності потужності шуму квантових генераторів випадкових чисел. Експериментальні дослідження проводилися на дослідній установці (прототипі) квантового генератора випадкових чисел та включали зборку й настройку оптичного тракту і систем магнітних котушок, а також налагодження надвисокочастотної частини і хвилеводного тракту квантового дискримінатора. Отримані результати служать основою для створення експериментального зразка оптичного квантового генератора випадкових чисел з високими криптографічними характеристиками в режимі гамування.

Іл. 5. Бібліогр. 15 назв.

UDC 681.3.07 (3.06)

Methods for spectral density noise power measurement of quantum radio-optical system of random number generator / *T.A.Grinenko,O.P.Nariezhnii, I.D.Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 172 - 183.

Methods for spectral density noise power measurement of quantum radio-optical system of random number generator is proposed. Experimental research were held using a testing prototype of the quantum random number generator and included assembly and tuning of optical section and system of magnetic coil as well as quantum discriminator microwave part and waveguide tuning. The obtained results are the basis for creation of an experimental sample of the quantum random number generator with perfect cryptographic characteristics for the keystream mode.

5 fig. Ref.: 15 items.

РАДИОТЕХНИЧЕСКИЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И УСТРОЙСТВА
RADIO ENGINEERING AND TELECOMMUNICATIONS SYSTEMS AND DEVICES

УДК 551.508.8

Особенности построения и примения комплексных систем дистанционного зондирования атмосферы / *В.М. Карташов, В.А. Тихонов, В.В. Воронин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 184-188.

Проанализирована тенденция создания и развития комплексных систем дистанционного зондирования атмоферы с использованем акустических и электромагнитных волн. Отмечена необходимость повышения информативности получаемых данных измерений путем совместной (комплексной) их обработки и интерпретации. Предложен алгоритм совместной обработки данных в комплексной системе акустического и радиоакустического зондирования.

Библиогр.: 11 назв.

УДК 551.508.8

Особливості побудови і використання комплексних систем дистанційного зондування атмосфери / *В.М. Карташов, В.А. Тихонов, В.В. Воронін, А.А. Замула* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 184-188.

Проаналізовано тенденцію створення й розвитку комплексних систем дистанційного зондування атмосфери з використанням акустичних і електромагнітних хвиль. Відзначено необхідність підвищення інформативності одержуваних даних вимірів шляхом спільної (комплексної) їхній обробки

та інтерпретації. Запропоновано алгоритм спільної обробки даних у комплексній системі акустичного та радіоакустичного зондування.

Бібліогр .: 11 назв.

UDC 551.508.8

Features of construction and application of complex systems for the atmosphere remote sounding / *V.M. Kartashov, V.A. Tikhonov, V.V. Voronin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 184-188.

The trend of creation and development of complex systems for the atmosphere remote sounding using acoustic and electromagnetic waves is analyzed. The necessity to improve the information capacity of the measurement data by their joint (complex) processing and interpretation is noted. The algorithm of joint data processing in the complex system of acoustic and radio acoustic sounding is proposed.

Ref.: 11 items

УДК 551.501.7

Координатный метод оценки радиальной скорости в системах акустического зондирования атмосферы / *В.В. Семенец, В.И. Леонидов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 189-193.

На примере анализа экспериментальных данных акустического зондирования показана возможность использования координатного метода в системах акустического зондирования атмосферы для определения малых величин вертикальной скорости движения воздушной массы.

Ил. 3. Библиогр.: 16 назв.

УДК 551.501.7

Координатний метод оцінки радіальної скорості в системах акустичного зондування атмосфери / *В. В. Семенец, В. І. Леонідов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 189-193.

На прикладі аналізу експериментальних даних акустичного зондування показана можливість використання координатного методу в системах акустичного зондування атмосфери для визначення малих величин вертикальної швидкості руху повітряної маси.

Іл. 3. Бібліогр.: 16 назв.

UDC 551.501.7

Coordinate method for estimation of radial velocity in systems of acoustic sounding of the atmosphere / *V.V. Semenetz, V.I. Leonidov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 189-193.

Using the analysis of experimental data of the atmosphere acoustic sounding as an example, the possibility is shown to use the coordinate method in the atmosphere acoustic sounding systems for estimation of small values of the vertical velocity of the air mass movement.

3 fig. Ref.: 16 items.

УДК 621.391

Координационный метод управления ресурсами многоуровневой транспортной оптической сети по критерию минимума энергопотребления / *О.Ю. Евсеева, Е. Н. Ильяшенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 194-201.

Предлагается динамическая математическая модель и построенный на ее основе метод управления разнородными ресурсами многоуровневой транспортной оптической сети по критерию минимума потребления электроэнергии. Метод обеспечивает комплексное распределение ресурсов нижележащей оптической сети с целью создания совокупности виртуальных топологий для ряда одновременно функционирующих поверх нее IP-сетей, согласованное с распределением ресурсов этих топологий между обсуживаемыми потоками IP-пакетов. Модель предполагает приоритетное использование оптических ресурсов разными IP-сетями, раздельное управление которыми достигается за счет введения функции координатора, применяющего принцип оценки взаимодействия.

Ил. 4. Библиогр.: 10 назв.

УДК 621.391

Координаційний метод управління ресурсами багаторівневої транспортної оптичної мережі за критерієм мінімуму енергоспоживання / *О.Ю.Євсєєва, Є. М. Ільяшенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 194-201.

Пропонується динамічна математична модель і побудований на її основі метод управління різнорідними ресурсами багаторівневої транспортної оптичної мережі за критерієм мінімуму споживання електроенергії. Метод забезпечує комплексний розподіл ресурсів оптичної мережі з метою створення сукупності віртуальних топологій для ряду одночасно функціонуючих поверх неї IP-мереж, яке є узгодженим з розподілом ресурсів цих топологій між потоками IP-пакетів, які обслуговуються. Модель реалізує пріоритетне використання оптичних ресурсів різними IP-мережами, роздільне управління якими досягається за рахунок введення функції координатора на основі принципу оцінки взаємодії.

Іл. 4. Бібліогр.: 10 назв.

UDC 621.391

Coordination method for resources management in multilevel transport optical network according to minimum energy consumption criterion / *O. Yu.Yevsieieva, Y. N. Ilyashenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 194-201.

A dynamic mathematical model and a method, based on it, for managing heterogeneous resources of multilevel optical transport network according to the criterion of minimum energy consumption, are proposed. The method provides consistent allocation of the resources of the underlying optical network in order to create a set of virtual topologies for a number of IP-networks, simultaneously operating over it, and allocation of the resources within these topologies among arriving IP-packet flows. The model assumes prioritized optical resources allocation among different IP-networks, separate management over which is achieved through the coordinator, based on the principle of assessment of the interaction.

4fig. Ref.: 10 items.

УДК621.391

Применение теории формальных грамматик и аппарата Е-сетей для анализа корректности распределения сетевых ресурсов инфраструктуры NFV / *Е.В. Дуравкин*, *Е.Б. Ткачева, Салим Мухамед Джамал* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 202-206.

Работа посвящена разработке новых методов анализа корректности распределения ресурсов в сетях с поддержкой технологии NFV. Приведен обзор функциональных и нефункциональных требований, предъявляемых к инфраструктуре NFV и методов проверки их соблюдения. В результате анализа предложено использовать аппарат Е-сетей для моделирования процессов предоставления услуг. В качестве инструмента анализа распределения сетевых ресурсов предложено применять теорию формальных грамматик. Сформирован и апробирован алгоритм построения цепочек вывода языка Р-типа для анализируемой модели Е-сети.

Ил. 1.Библиогр.: 8 назв.

УДК621.391

Застосування теорії формальних граматик та апарату Е-мереж для аналізу коректності розподілу мережевих ресурсів у інфраструктурі NFV / *Є.В. Дуравнкін, О.Б. Ткачова, Салім Мухамед Джамал* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 202-206.

Робота присвячена розробці нових методів аналізу коректності розподілу ресурсів в мережах з підтримкою технології NFV. Огляд особливих та не функціональних вимог, що пред'являються до інфраструктури NFV та методів перевірки їх дотримання. В результаті аналізу запропоновано використовувати апарат Е-мереж для моделювання процесів надання послуг. Як інструмент аналізу розподілу мережевих ресурсів запропоновано застосовувати теорію формальних граматик. Сформовано та апробовано алгоритм побудови ланцюгів виведення мови Р-типу для аналізованої моделі Е-мережі.

Іл. 1. Бібліогр.: 8назв.

UDC 621.391

Application of the theory of formal grammars and the E-nets tools for analysis of correctness of network resources distribution in the NFV infrastructure / *E.V. Duravki*n, *O.B. Tkachova, Mohammed Jamal Salim* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 202-206.

The work is devoted to the development of new methods for the analysis of the correctness of resource allocation in networks with the NFV support. An overview of functional and non-functional requirements for

the NFV infrastructure and methods of their verification is presented. As a consequence of the analysis it is proposed to use the E-networks tools for modeling processes of providing services. It is suggested to use the theory of formal grammars as a tool of analysis of the network resources allocation. The algorithm of constructing chains of derivation of the language of R-type for the analyzed model of the E-network is generated and tested.

Fig. 1. Ref.: 8 items

УДК 621.391

Оптимизация нерегулярных кодов с малой плотностью проверок на четность на основе природных вычислений / *Н.А. Штомпель* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 207 - 210.

Предложен метод оптимизации нерегулярных кодов с малой плотностью проверок на четность с уменьшенной вычислительной сложностью. Представленный метод оптимизации основан на совместном использовании обобщенных процедур природных вычислений, известном методе построения графов Таннера и компьютерном моделировании с применением метода Монте-Карло.

Библиогр.: 9 назв.

УДК 621.391

Оптимізація нерегулярних кодів з малою щільністю перевірок на парність на основі природних обчислень / *М.А. Штомпель* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 207 - 210.

Запропоновано метод оптимізації нерегулярних кодів з малою щільністю перевірок на парність зі зменшеною обчислювальною складністю. Представлений метод заснований на спільному використанні узагальнених процедур природних обчислень, відомому методі побудови графів Таннера та комп'ютерному моделюванні із застосуванням методу Монте-Карло.

Бібліогр.: 9 назв.

UDC 621.391

Optimization of irregular low-density parity-check codes based on natural computing / *M.A. Shtompel* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 207-210.

The optimization method of irregular low-density parity-check codes with reduced computational complexity is proposed. The presented optimization method is based on the joint use of the generalized procedures of the natural computing, known method of Tanner graphs construction and computer simulation with Monte-Carlo method.

Ref.: 9 items.

УДК 621.396.62.33

Синтез модулированного фильтра с самосинфазированием для следящего приема и обработки частотно-модулированного сигнала методом имитационного моделирования / *В.В. Печенин, К.А. Щербина, М.А. Вонсович, Ю.В. Съедина* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 211 - 216.

Синтезирована схема модулированного фильтра с самосинфазированием для следящего приема и обработки частотно-модулированного сигнала на основе имитационного моделирования. Приведены результаты тестирования имитационной модели, подтверждающие высокую достоверность эффективной работы схемы при заданных исходных данных. Сравнительный анализ схем следящего модулированного фильтра с самосинфазированием и следящего измерителя с перестраиваемым гетеродином и узкополосным фильтром в петле автоподстройки показал, что разработанная схема обладает простотой технической реализации и улучшенной помехоустойчивостью.

Ил. 5. Библиогр.: 6 назв.

УДК 621.396.62.33

Синтез модульованого фільтра з самосинфазуванням для слідкуючого прийому та обробки частотно-модульованого сигналу методом імітаційного моделювання / *В.В. Печенін, К.О. Щербина, М.А. Вонсович, Ю. В. С'єдіна* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 211 - 216.

Синтезовано схему модельованого фільтра з самосинфозуванням для слідкуючого прийому та обробки частотно-модульованого сигналу на основі імітаційного моделювання. Наведені результати тестування імітаційної моделі підтверджують високу вірогідність ефективної роботи схеми при зада-

них початкових даних. Порівняльний аналіз схем слідкуючого модульованого фільтра з самосинфазуванням та слідкуючим вимірювачем з перестроюваним гетеродином і вузькосмуговим фільтром в петлі автопідстроювання показав, що розроблена схема володіє простотою технічної реалізації і покращеною завадостійкістю.

Іл. 5. Бібліогр.: 6 назв.

UDC 621.396.62.33

Synthesis of the modulated filter with self-cophasing for tracking and processing of frequency-modulated signal by means of simulation method / *V.V. Pechenin, K.A. Scherbina, M.A. Vonsovitch, J. V. Syedina* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 211 - 216.

The simulation approach has been used to synthesis the modulated filter model with self-cophasing for tracking and processing modulated signal. The high reliability of the efficient circuit performance for the given initial data has been proved by the results of the simulation model test. The comparative analysis of self-cophasing modulated tracking filter circuit and tracking meter circuit with tuned heterodyne and narrow-band filter in the locking loop has shown that the developed circuit has simple technical implementation and shows improved noise immunity.

Fig. 5. Ref.: 6 items.

УДК 621.396.677.3

Широкополосная двухкольцевая планарная антенна / *Т.А. Цалиев, К.В.Куцук* // Радиотехника : Всеукр. межвед. науч.-техн. сб. - 2016. - Вып. 186. - С. 217 - 222.

Исследованы электродинамические характеристики двухкольцевой планарной антенны, образованной кольцами переменного радиуса. Проведен сравнительный анализ характеристик двукольцевой антенны и широкополосной кольцевой антенны. Исследования проводились путём численного анализа с помощью компьютерных технологий.

Ил. 5. Библиогр : 6 назв.

УДК 621.396.677.3

Широкополосна двухкільцева планарна антена / *Т.А. Цалієв, К.В. Куцук* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2016. – Вип. 186. – С. 217 - 222.

Досліджено електродинамічні характеристики двокільцевой планарной антени створеної кільцями радіуса, що змінюється. Проведено порівняльний аналіз характеристик двокільцевой планарной антени та широкополосной кільцевой антени. Дослідження проводились шляхом численого аналізу за допомогою комп'ютерних технологій.

Іл. 5. Бібліогр : 6 назв.

UDC 621.396.677.3

Broadband double-ring planar antenna / *T.A. Tsaliev, K.V.Kutsuk* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. - 2016. - №186. - P. 217 - 222.

The electromagnetic characteristics of the planar antenna, formed by rings of a variable radius, were investigated. Comparative analysis of the double-ring antenna and broadband ring antenna characteristics was carried out. The studies were conducted by numerical analysis using computer technology.

Fig. 5. Ref : 6 items.