РЕФЕРАТЫ РЕФЕРАТИ ABSTRACTS

ПЕРСПЕКТИВНЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ И ПРОТОКОЛЫ
ПЕРСПЕКТИВНІ КРИПТОГРАФІЧНІ СИСТЕМИ ТА ПРОТОКОЛИ
PERSPECTIVE CRYPTOGRAPHIC SYSTEMS AND PROTOCOLS

УДК 004.056.55

Методы построения общесистемных параметров и ключей для NTRU PRIME UKRAINE 5 – 7 уровней стойкости. Product form / *И.Д. Горбенко, Е.Г. Качко, Ю.И. Горбенко, И.В. Стельник, С.А. Кандий, М.В. Есина* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 5 – 16.

Проведено исследование и выполнена разработка эффективного практического алгоритма построения общесистемных параметров и ключей криптопреобразования типа несимммметричный шифр для специальной формы задания полиномов Product Form. Приведен экспериментально определенный набор параметров для алгоритма **NTRU PRIME UKRAINE** для 5 – 7 уровней стойкости с учетом комбинированной атаки.

Ключевые слова: несимммметричный шифр, общесистемные параметры, квантовая стойкость, уровень стойкости, конечные поля, Product Form

Табл. 7. Библиогр.: 18 назв.

УДК 004.056.55

Методи побудування загальних параметрів та ключів для NTRU PRIME UKRAINE 5 – 7 рівнів стійкості. Product form / *І.Д. Горбенко, О.Г. Качко, Ю.І. Горбенко, І.В. Стельнік, С.О. Кандій, М.В. Єсіна* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 5 – 16.

Проведено дослідження та виконано розробку ефективного практичного алгоритму побудування загальносистемних параметрів та ключів криптоперетворень типу асиметричний шифр для спеціальної форми завдання поліномів Product Form. Наводиться експериментально визначений набір параметрів для алгоритму **NTRU PRIME UKRAINE** для 5 – 7 рівнів стійкості з урахуванням комбінованої атаки.

Ключові слова: асиметричний шифр, загальні параметри, квантова стійкість, рівень стійкості, скінчені поля, Product Form.

Табл. 7. Бібліогр.: 18 назв.

UDC 004.056.55

Methods for constructing system-wide parameters and keys for NTRU PRIME UKRAINE 5 – 7 stabvility levels. Product form / *I.D. Gorbenko, O.G. Kachko, Yu. I. Gorbenko, I.V. Stelnik, S.O. Kandy, M.V. Yesina* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 5 – 16.

The research was carried out and the development of an effective practical algorithm for the construction of system-wide parameters and keys of cryptographic transformations such as asymmetric ciphers for a special form of setting the Product Form polynomial was performed. The experimental confirmation of the built-in system-wide parameters for 5 – 7 stability levels **NTRU PRIME UKRAINE,** taking into account a combined attack. is given.

Key words: asymmetric cipher, general parameters, quantum stability, stability level, finite fields, Product Form.

7 tab. Ref.: 18 items.

УДК 004.056.55

Вычисление общих параметров для NTRU PRIME UKRAINE 6-7 уровней стойкости / *И.Д. Горбенко, А.Н. Алексейчук, О.Г. Качко, М.В. Есина, В.А. Бобух, С.О. Кандий, В.А. Пономарь* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 17 – 26.

Проведено исследование и выполнена разработка эффективного практического алгоритма построения общесистемных параметров и ключей криптопреобразований типа асимметричный шифр и протокол инкапсуляции ключей. Приводится экспериментальное подтверждение построенных общесистемных параметров и ключей криптопреобразования типа асимметричный шифр и протокол инкапсуляции ключей 6-7 уровней стойкости на основе преобразований в кольце полиномов над конечным полями. Приводятся виды атак, которые являются возможными касательно указанных криптопреобразований.

Ключевые слова: общие параметры, квантовая стойкость, кольцо полиномов, уровень стойкости, конечные поля.

Табл. 1. Библиогр.: 15 назв.

УДК 004.056.55

Обчислення загальних параметрів для NTRU PRIME UKRAINE 6 – 7 рівнів стійкості / *І.Д. Горбенко, А.М. Олексійчук, О.Г. Качко, М.В. Єсіна, В.А. Бобух, С.О. Кандій, В.А. Пономар* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 17 – 26.

Проведено дослідження та виконано розробку ефективного практичного алгоритму побудування загальносистемних параметрів та ключів криптоперетворень типу асиметричний шифр та протокол інкапсуляції ключів. Наводиться експериментальне підтвердження побудованих загальносистемних параметрів та ключів криптоперетворень типу асиметричний шифр та протокол інкапсуляції ключів 6 – 7 рівнів стійкості на основі перетворень в кільці поліномів над скінченими полями. Наводяться види атак, які є можливими щодо зазначених криптоперетворень.

Ключові слова: загальні параметри, квантова стійкість, кільце поліномів, рівень стійкості, скінчені поля.

Табл. 1. Бібліогр.: 15 назв.

UDC 004.056.55

General parameters for NTRU PRIME UKRAINE 6 – 7 stability levels calculation / *I.D. Gorbenko, A.N. Alekseychuk, O.G. Kachko, M.V. Yesina, V.A. Bobukh, S.O. Kandy, V.A. Ponomar* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 17 – 26.

The research was carried out and the development of an effective practical algorithm for the construction of system-wide parameters and keys for cryptographic transformations such as asymmetric ciphers and the key encapsulation protocol was performed. The experimental confirmation of the built-in system-wide parameters and keys of cryptographic transformations such as asymmetric cipher and the key encapsulation protocol of 6 – 7 stability levels based on transformations in the ring of polynomials over the finite fields is presented. The types of attacks that are possible with respect to the specified cryptographic transformations are also presented in this work.

Key words: general parameters, quantum stability, ring of polynomials, stability level, finite fields.

1 tab. Ref.: 15 items

УДК 004.056.55

Криптоанализ хеш-функции Купина при использовании в схемах подписи Меркла / *Е.Г. Качко, Д.К. Телевный* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 27 – 31.

Статья посвящена анализу уровня безопасностиб хеш-функции Купина ДСТУ 7564:2014 при использовании в схемах подписи Меркла. Робота описывает возможные атаки на хеш, и их последствия для схемы подписи. Результати покзывают целесообразность использования хеша в схеме, основанные на результатах производительности, уровня безопасности и стойкости.

Ключевые слова: проблема обхода дерева, схемы деревьев меркла, купина, криптоанализ, схемы подписей, эцп.

Табл. 3. Ил. 1. Библиогр.: 9 назв.

УДК 004.056.55

Криптоаналіз геш-функції Купина при використанні у схемах підпису Меркла / *О.Г. Качко, Д.К. Телевний* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 27 – 31.

Стаття присвячена аналізу рівня безпеки хеш-функції Купина ДСТУ 7564:2014 при використанні у схемах підпису Меркла. Робота описує можливі аттаки на геш, та їх наслідки у схемі підпису. Результати показують доцільність використання гешу у схемі, що базубться на результатах потужності, рівня безпеки та стійкості.

Ключові слова: проблема обходу дерева, схеми дерев меркла, купина, криптоаналіз, схемі підпису, ецп.

Табл. 3. Іл. 1. Бібліогр.: 9 назв.

UDC 004.056.55

The Kupyna hash function cryptanalysis with Merkle Trees Signature schemes / *O. Kachko, D. Televnyi* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 27 – 31.

The paper is devoted to the security analysis of the Kupyna (DSTU 7564:2014) hash function applied to Merkle tree signature schemes. The paper lists possible attacks on the hash, and their application for signature schemes. The results show expediency of using the Kypuna hash in Merkel schemes based on the performance, security levels and strength against known cryptanalytic attacks.

Key words: tree traversal problem, merkle tree schemes, kupyna, cryptanalisys, dsa. mss.

3 tab. 1 fig. Ref.: 9 items.

УДК 004.056.5

NIST PQC: Кодовые криптосистемы / *А.А. Кузнецов, Ю.И. Горбенко, М.С. Луценко, Д.И. Прокопович-Ткаченко, Н.В. Пастухов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 32 – 40.

Исследуются кодовые схемы, которые были представлены на конкурс постквантовых криптографических алгоритмов NIST PQC. Рассмотрены общие характеристики алгоритмов, их основные свойства и параметры. Проведен сравнительный анализ схем электронной цифровой подписи, направленного шифрования и схем инкапсуляции ключей по критериям скорости и длины основных криптографических параметров.

Ключевые слова: постквантовая криптография; подписи в кодах; криптосистемы с открытым ключом; механизмы инкапсуляции ключей; криптографические параметры.

Ил. 6. Библиогр.: 24 назв.

УДК 004.056.5

NIST PQC: Кодові криптосистеми / *О.О. Кузнецов, Ю.І. Горбенко, М.С. Луценко, Д.І. Прокопович-Ткаченко, М.В. Пастухов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 32 – 40.

Досліджуються кодові схеми, які були представлені на конкурс постквантових криптографічних алгоритмів NIST PQC. Розглянуто загальні характеристики алгоритмів, їх основні властивості і параметри. Проведено порівняльний аналіз схем електронного цифрового підпису, направленого шифрування і схем інкапсуляції ключів за критеріями швидкості і довжини основних криптографічних параметрів.

Ключові слова: постквантова криптографія; підписи на кодах; криптосистеми з відкритим ключем; механізми інкапсуляції ключів; криптографічні параметри.

Іл. 6. Бібліогр.: 24 назв.

UDC 004.056.5

NIST PQC: Code-Based Cryptosystems / *A.A. Kuznetsov, Yu.I. Gorbenko, M.S. Lutsenko, D.I. Prokopovych-Tkachenko, M.V. Pastukhov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 32 – 40.

The code-based schemes, which were submitted to the contest of post-quantum crypto algorithms NIST PQC, are studied in this work. The general characteristics of the algorithms are explored and basic properties and parameters are estimated. A comparative analysis of the electronic digital signature schemes, public-key cryptosystems and key encapsulation schemes are carried out according to the criteria of speed and length of the main cryptographic parameters.

Keywords: Post-Quantum Cryptography; Code-Based Signatures; Public-Key Cryptosystems; Key Encapsulation Mechanisms; Cryptographic Parameters

6 fig. Ref.: 24 items.

УДК 004.428.4

Эллиптические кривые Эдвардса. Сравнение криптографических библиотек / *О.А. Мельникова, О.В. Джурик, А.О. Масленникова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 41 – 45.

Кривые Эдвардса – это форма представления эллиптических кривых, которая поддерживает быстрый, унифицированный и полный закон сложения точек. Кривые Эдвардса приобрели большую популярность благодаря эффективным формулам сложения и удвоения точек. Рассматриваются и сравниваются программные библиотеки, которые поддерживают кривые Эдвардса и цифровую подпись EdDSA.

Ключевые слова: эллиптические кривые Эдвардса, электронная цифровая подпись, криптографические библиотеки, несимметричная криптография.

Табл. 3. Библиогр.: 7 назв.

УДК 004.428.4

Еліптичні криві Едвардса. Порівняння криптографічних бібліотек / *О.А. Мельникова, О.В. Джурик, А.О. Маслєннікова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 41 – 45.

Криві Едвардса – це форма представлення еліптичних кривих, яка підтримує швидкий, уніфікований та повний закон додавання точок. Криві Едвардса набули великої популярності завдяки

ефективним формулам додавання та подвоєння точок. Розглядаються та порівнюються програмні бібліотеки, які підтримують криві Едвардса та цифровий підпис EdDSA.

Ключові слова: еліптичні криві Едвардса, електронний цифровий підпис, криптографічні бібліотеки, несиметрична криптографія

Табл. 3. Бібліогр.: 7 назв.

UDC 004.428.4

Edwards elliptic curves. Comparison of cryptographic libraries / *O. Melnykova, O. Dzhuryk, A. Masliennikova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 41 – 45.

Edwards Curves is a form of representing elliptic curves that supports fast, unified, and complete law of addition of points. Edwards curves have attracted great interest for their efficient addition and doubling formulas. In this paper, we described and compared programming libraries, which implemented Edwards curves and EdDSA signature.

Key words: Edwards elliptic curves, digital signature, cryptographic programming libraries, public-key cryptography

3 tab. Ref.: 7 items.

УДК 004.056.55

Сравнительный анализ пост квантовых стандартов электронной подписи на основе мультивариативних квадратичных преобразований / *И.Д. Горбенко, И.С. Кудряшов, В.В. Оноприенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 46 – 60.

Приводятся результаты анализа и сравнения механизмов электронной подписи с использованием многомерных преобразований в квадратичных конечных полях. В качестве основных критериев использованы длины ключей и электронной подписи, а также вычислительная эффективность подписи и проверки подписи. Сравнение сделано по электронным подписям LUOV, Gui, Rainbow, MQDSS, TPSig, DualModeMS, HiMQ-3 и GeMSS. Указанные кандидаты выбраны по безусловным частным и интегральному безусловному критерию криптографической устойчивости к атаке на основе адаптивного подбора сообщений.

Ключевые слова: асимметричный ключ, асимметричные криптопреобразования, многомерные преобразования, электронная подпись, квадратичные поля, постквантовые электронные подписи.

Табл. 3. Ил. 9. Библиогр.: 14 назв.

УДК 004.056.55

Порівняльний аналіз пост квантових стандартів електронного підпису на основі мультиваріативних квадратичних перетворень / *І.Д. Горбенко, І.С. Кудряшов, В.В. Онопрієнко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 46 – 60.

Наведено результати аналізу та порівняння механізмів електронного підпису з використанням баготовимірних перетворень в квадратичних скінченних полях. В якості основних критеріїв використані довжини ключів та електронного підпису, обчислювальна ефективність підпису та перевірки підпису. Порівняння зроблено щодо електронних підписів LUOV, Gui, Rainbow, MQDSS, TPSig, DualModeMS, HiMQ-3 та GeMSS. Кандидати вибрані по безумовних часткових та інтегральному безумовному критерію криптографічної стійкостіі до атаки на основі адаптивного підбору повідомлень.

Ключові слова: асиметричний ключ, асиметричні криптоперетворення, багатовимірні перетворення, електронний підпис, квадратичні поля, постквантові електронні підписи.

Табл. 3. Іл. 9. Бібліогр.:14 назв.

UDC 004.056.55

Comparative analysis of post quantum standards for electronic signature based on multivariate quadratic transformations / *I.D. Gorbenko, I.S. Kudryashov, V.V. Onoprienko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 46 – 60.

The results of the analysis and comparison of electronic signature mechanisms using multidimensional transformations in quadratic finite fields are presented. The key and electronic signature lengths, as well as the computational efficiency of the signature and signature verification are used as the main criteria. Comparison made by electronic signatures LUOV, Gui, Rainbow, MQDSS, TPSig, DualModeMS, HiMQ-3 and GeMSS. These candidates are selected by unconditional private and integral unconditional criterion for cryptographic resistance to attack based on adaptive selection of messages.

Key words: asymmetric key, asymmetric crypto-transformations, multidimensional transformations, electronic signature, quadratic fields, post-quantum electronic signatures.

3 tab. 9 fig. Ref.: 14 items.

УДК 004.056.55

Сравнительные исследования и анализ эффективности гибридной кодовой криптосистемы / *А.А. Кузнецов, Ю.И. Горбенко, А.С. Киян, А.А. Уварова, Т.Ю. Кузнецова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 61 – 69.

Рассмотрены основные принципы построения и функционирования криптосистем Мак-Элиса и Нидеррайтера, в основе которых лежит использование кодов. Предложена новая гибридная криптосистема, которая объединяет принципы шифрования согласно упомянутым схемам. Также осуществлено анализ и сравнительные исследования с точки зрения стойкости, объема ключевых данных и относительной скорости передачи информации новой схемы и криптосистем Мак-Элиса и Нидеррайтера, который представлен как в аналитическом виде, так и с помощью графического изображения. В ходе сравнительных исследований выявлено, что гибридная криптосистема сохраняет позитивные аспекты своих предшественников, а также позволяет увеличить относительную скорость передачи с одновременным сохранением показателей стойкости к классическому и квантовому криптоанализу, однако, к сожалению, до сих пор сохраняется одно важное ограничение- большие объемы необходимых ключевых данных.

Ключевые слова: алгебраические коды; криптография на основе кодов; криптосистема Мак-Элиса; криптосистема Нидеррайтера; криптосистема с открытым ключом; пост-квантовая криптосистема.

Табл. 2. Іл. 4. Бібліогр.: 20 назв.

УДК 004.056.55

Порівняльні дослідження та аналіз ефективності гібридної кодової криптосистеми / *О.О. Кузнецов, Ю.І. Горбенко, А.С. Кіян, А.О. Уварова, Т.Ю. Кузнецова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 61 – 69.

Розглянуто основні принципи побудови та функціонування криптосистем Мак-Еліса і Нідеррайтера, в основі яких лежить використання кодів. Запропоновано нову гібридну криптосистему, що поєднує принципи зашифрування згідно зі згаданими схемами. Здійснено аналіз та порівняльні дослідження з точки зору стійкості, обсягу ключових параметрів, довжини шифртексту і відносної швидкості передачі інформації нової схеми і криптосистем Мак-Еліса та Нідеррайтера, що представлено в аналітичному вигляді та за допомогою графічного зображення. У ході порівняльних досліджень виявлено, що гібридна криптосистема зберігає позитивні аспекти своїх попередників, а також дозволяє збільшити відносну швидкість передачі зі збереженням показника стійкості до класичного та квантового криптоаналізу, однак, на жаль, досі зберігається важливе обмеження - великі розміри необхідних ключових даних.

Ключові слова: алгебраїчні коди; криптографія на основі кодів; криптосистема Мак-Еліса; криптосистема Нідеррайтера; асиметрична криптосистема; постквантова криптосистема.

Табл. 2. Іл. 4. Бібліогр.: 20 назв.

UDC 004.056.55

Comparative studies and analysis of efficiency code-based hybrid cryptosystem / *A.A. Kuznetsov, Y.I. Gorbenko, A.S. Kiian, A.A. Uvarova, T.Y. Kuznetsova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 61 – 69.

The basic principles of construction and operation of McEliece and Niederreiter cryptosystems based on the use of error-correcting codes are considered. A new hybrid cryptosystem, that combines rules of encryption according to the above-mentioned schemes, is proposed. Also, an analysis and comparative studies are carried out in terms of stability, volume of public and private keys, length of ciphertext and relative speed of information transmission of the new proposed scheme and McEliece and Niederreiter cryptosystems presented both in an analytical form and by means of a graphic. Comparative studies revealed that the hybrid cryptosystem retains the positive aspects of its predecessors, as well as allows increase in the relative transmission rate with the preservation of the stability indicator to the classical and quantum cryptanalysis, but, unfortunately, one important limitation is still preserved - a large size of the required key data.

Key words: Algebraic codes; Code-based cryptography; McEliece cryptosystem; Niederreiter cryptosystem; Public-key cryptosystem; Post-quantum cryptosystem.

2 tab. 4 fig. Ref.: 20 items.

УДК 621.394.147

Анализ и исследование свойств алгеброгеометрических кодов / *А.А. Кузнецов, Е.П. Колованова, Д.И. Прокопович-Ткаченко, Т.Ю. Кузнецова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 70 – 88.

Рассматриваются линейные блоковые помехоустойчивые коды, построенные по алгебраическим кривым (алгеброгеометрические коды), оцениваются их конструктивные свойства, изучаются алгоритмы построения и декодирования. Исследуется энергетическая эффективность передачи дискретных сообщений М-ми ортогональными сигналами при применении алгеброгеометрических кодов, оценивается достигаемый энергетический выигрыш от использования помехоустойчивого кодирования. Показано, что в дискретных каналах без памяти удается получить значительный энергетический выигрыш, который возрастает при переходе к длинным алгеброгеометрическим кодам, построенным по кривым с большим числом точек по отношению к роду кривой. Установлено, что вычислительная сложность реализации алгеброгеометрических кодов сопоставима с другими известными помехоустойчивыми кодами, например кодами Рида – Соломона, и др. Таким образом, высокая энергетическая эффективность в сочетании с приемлемой вычислительной сложностью реализации подтверждают перспективность использования алгеброгеометрических кодов в современных телекоммуникационных системах и сетях для повышения помехоустойчивости каналов передачи данных.

Ключевые слова: алгеброгеометрический код, энергетический выигрыш, ортогональный сигнал, помехоустойчивое кодирование.

Табл. 8. Ил. 8. Библиогр.: 11 назв.

УДК 621.394.147

Аналіз і дослідження властивостей алгеброгеометричних кодів / *О.О. Кузнецов, Є.П. Колованова, Д.І. Прокопович-Ткаченко, Т.Ю. Кузнецова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 70 – 88.

Розглядаються лінійні блокові завадостійкі коди, побудовані по алгебраїчним кривим (алгеброгеометричні коди), оцінюються їх конструктивні властивості, вивчаються алгоритми побудови та декодування. Досліджується енергетична ефективність передачі дискретних повідомлень М-ми ортогональними сигналами при застосуванні алгеброгеометричних кодів, оцінюється енергетичний виграш від використання завадостійкого кодування. Показано, що в дискретних каналах без пам'яті вдається отримати значний енергетичний виграш, який зростає при переході до довгих алгеброгеометричних кодів, побудованих за кривими з великим числом точок по відношенню до роду кривої. Встановлено, що обчислювальна складність реалізації алгеброгеометричних кодів порівнянна з іншими відомими завадостійкими кодами, наприклад кодами Ріда – Соломона, та ін. Таким чином, висока енергетична ефективність в поєднанні з прийнятною обчислювальною складністю реалізації підтверджують перспективність використання алгеброгеометричних кодів в сучасних телекомунікаційних системах і мережах для підвищення завадостійкості каналів передачі даних.

Ключові слова: алгеброгеометричний код, енергетичний виграш, ортогональний сигнал, завадостійке кодування.

Табл. 8. Іл. 8. Бібліогр.: 11 назв.

UDC 621.394.147

Analysis and investigation of algebraic geometric codes properties / *A.A. Kuznetsov, I.P. Kolovanova, D.I. Prokopovych-Tkachenko, T.Y. Kuznetsova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 70 – 88.

Linear block noise-proof codes constructed according to algebraic curves (algebraic geometric codes) are considered, their design properties are evaluated, algorithms of construction and decoding are studied. The energy efficiency of the transmission of discrete messages by M-ary orthogonal signals in the application of algebraic geometric codes is studied; the achievable energy gain from the use of noise-immune coding is estimated. It is shown that in discrete channels without memory it is possible to obtain a significant energy gain, which increases with the transition to long algebraic geometric codes constructed by curves with a large number of points with respect to the genus of the curve. It is established that the computational complexity of implementing algebraic geometric codes is comparable to other known noise-resistant codes, for example, Reed-Solomon codes and others. Thus, high energy efficiency in combination with acceptable computational complexity of implementation confirm the prospects of algebraic geometric codes using in modern telecommunication systems and networks to improve the noise immunity of data transmission channels.

Keywords: algebraic geometric code, energy gain, orthogonal signal, noise-immune coding

8 tab. 8 fig. Ref.: 11 items.

УДК 519.2: 519.7: 003.026

Сущность и особенности реализации метода Гровера на классическом компьютере для симметричного криптоанализа / *Ю.И. Горбенко, Е.Ю Каптьол* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 89 – 100.

Статья посвящена детализации, освоению для применения, проверке криптоаналитических свойств и демонстрации применения метода Гровера при криптоанализе симметричных криптографических преобразований. Приводится суть метода и его детализация с целью реализации квантового алгоритма Гровера на классическом компьютере.

Ключевые слова: метод Гровера, сложность поиска в несортированной базе, примеры поиска на классическом компьютере

Табл. 1. Ил. 1. Библиогр.: 5 назв.

УДК 519.2:519.7 : 003.026

Сутність та особливості реалізації методу Гровера на класичному комп'ютері для симетричного криптоаналізу / *Ю.І. Горбенко, Є.Ю. Каптьол* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 89 – 100.

Стаття присвячена деталізації, засвоєнню для застосування, перевірці криптоаналітичних властивостей та демонстрації застосування методу Гровера при криптоаналізі симетричних криптографічних перетворень. Наводиться сутність методу та його деталізація з метою реалізації квантового алгоритму Гровера на класичному комп'ютері.

Ключові слова: метод Гровера, складність пошуку в несортованій базі, приклади пошуку на класичному комп**'**ютері.

Табл. 1. Іл. 1. Бібліогр.: 5 назв.

UDC 519.2: 519.7: 003.026

Essence and features of Grover's method implementation on a classical computer for symmetric cryptanalysis / *Yu.I. Gorbenko, Ye.Yu Kaptyol* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 89 – 100.

This paper is devoted to detailing, mastering for use, checking cryptanalytic properties and demonstrating the use of Grover's method for cryptanalysis of symmetric cryptographic transformations. The essence of the method and its refinement are presented in order to implement Grover's quantum algorithm on a classical computer.

Key words: Grover method, search complexity in the unsorted database, examples of search on a classical computer.

1 tab. 1 fig. Ref.: 5 items.

УДК 004.056.5

Комбинирующие и фильтрующие функции на основе регистров сдвига с нелинейными обратными связями / *А.А. Кузнецов, А.В. Потий, Н.А. Полуяненко, С.Г. Вдовенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 101 – 112.

Рассмотрены возможности применения регистров сдвига с нелинейными обратными связями, формирующих последовательность максимального периода, в качестве комбинирующей или фильтрующей функции. Исследованы основные показатели криптографической стойкости таких функций, такие как сбалансированность, наличие запретов, корреляционная иммунность и нелинейность. Проанализированы и приведены экспериментальные значения корреляционной иммунности и нелинейности для всех регистров сдвига с нелинейными обратными связями, формирующие последовательность максимального периода, для размера регистра до шести ячеек включительно, а также регистры с размерностью до девяти ячеек включительно с алгебраической степенью образующего многочлена не выше 2. Изучена возможность оптимизации выбора булевых функций по критериям максимальной корреляционной иммунности и нелинейности при различной алгебраической степени и минимизации количества мономов в образующем полиноме.

Ключевые слова: генераторы псевдослучайных последовательностей; фильтрующие функции; комбинирующие функции; криптографический анализ; нелинейные полиномы.

Табл. 9. Ил. 2. Библиогр.: 13 назв.

УДК 004.056.5

Комбінуючі та фільтруючі функції на основі регістрів зсуву з нелінійними зворотними зв'язками / *О.О. Кузнецов, О.В. Потій, М.О. Полуяненко, С.Г. Вдовенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 101 – 112.

Розглянуто можливості застосування регістрів зсуву з нелінійними зворотними зв'язками, які формують послідовність максимального періоду, в якості комбінучої або фільтрувальної функції. Досліджено основні показники криптографічного стійкості таких функцій, такі як збалансованість, наявність заборон, кореляційний імунітет і нелінійність. Проаналізовано та наведено експериментальні значення кореляційної імунності та нелінійності для всіх регістрів зсуву з нелінійними зворотними зв'язками, що формують послідовність максимального періоду, для розміру регістра до шести осередків включно, а також регістри з розмірністю до дев’яти осередків включно з алгебраїчним ступенем утворюючого многочлена не вище 2. Вивчено можливість оптимізації вибору булевих функцій за критеріями максимальної кореляційної імунності та нелінійності при різному алгебраїчному ступеню та мінімізації кількості одночленів в утворюючому поліномі.

Ключові слова: генератори псевдовипадкових послідовностей; фільтруючі функції; комбінуючі функції; криптографічний аналіз; нелінійні поліноми.

Табл. 9. Іл. 2. Бібліогр.: 13 назв.

UDC 004.056.5

Combining and filtering functions in the framework of nonlinear-feedback shift register / *A.A. Kuznetsov, A.V. Potii, N.A. Poluyanenko, S.G. Vdovenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 101 – 112.

Strong cryptography of stream ciphers is determined, among other things, by the ability of a generated pseudorandom sequence to resist analytical attacks. One of the main components of the pseudorandom stream cipher sequence generating algorithm are Boolean functions for combining and filtering. The paper considers the possibility of applying nonlinear-feedback shift registers that generate a maximum length sequence as a combining or filtering function. This work examines the main indicators of cryptographic strength of such functions, as: balance, the prohibitions presence, correlation immunity and nonlinearity. The study analyzes and demonstrates correlation immunity’s and nonlinearity’s experimental values for all nonlinear feedback shift registers, that generate a maximum length sequence, for register sizes up to 6 cells inclusively, and registers sizes up to 9 cells inclusively with algebraic degree of the polynomial under 2. The possibility of optimizing the process of selecting Boolean functions according to the criteria of maximum correlation immunity and nonlinearity with various algebraic degree and minimization of the number of monomials in the polynomial are studied.

Key words: generators of the pseudorandom sequence; filtering function; combining function; cryptanalysis; nonlinear polynomials

9 tab. 2 fig. Ref.: 13 items.

УДК 621.3.06

Оценка стойкости симметричного блочного шифра «Кипарис» к дифференциальному криптоанализу / *М.Ю. Родинко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 113 – 124.

Представлена оценка практической стойкости малоресурсного блочного шифра «Кипарис» к дифференциальному криптоанализу, которая определяется вероятностью лучшей найденной дифференциальной характеристики. Предложена математическая модель оценки стойкости блочного шифра «Кипарис» к дифференциальному криптоанализу и методы поиска многоцикловых дифференциальных характеристик. В основе первого метода лежит комбинирование высоковероятностных одноциклових дифференциальных характеристик в многоцикловые, в основе второго - продолжение одноциклових характеристик на несколько циклов. В результате применения второго метода поиска к блочному шифру «Кипарис-256» найдена дифференциальная характеристика для шести циклов шифрования. Поскольку больше, чем для шести циклов шифрования дифференциальных характеристик с вероятностью выше вероятности атаки полного перебора, не найдено, блочный шифр «Кипарис-256» является практически стойким к дифференциальному криптоанализу.

Ключевые слова: дифференциальный криптоанализ, дифференциальная характеристика, симметричный блочный шифр, малоресурсная криптография.

Табл. 6. Ил. 2. Библиогр: 17 назв.

УДК 621.3.06

Оцінка стійкості симетричного блокового шифру «Кипарис» до диференційного криптоаналізу / *М.Ю. Родінко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 113 – 124.

Представлено оцінку практичної стійкості малоресурсного блокового шифру «Кипарис» до диференційного криптоаналізу, що визначається ймовірністю кращої знайденої диференційної характеристики. Запропоновано математичну модель оцінки стійкості блокового шифру «Кипарис» до диференційного криптоаналізу та методи пошуку багатоциклових диференційних характеристик. В основі першого методу лежить комбінування високоймовірнісних одноциклових диференційних характеристик у багатоциклові, в основі другого – продовження одноциклових характеристик на декілька циклів. В результаті застосування другого методу пошуку до блокового шифру «Кипарис-256» знайдено диференційну характеристику для шести циклів шифрування. Оскільки більше, ніж для шести циклів шифрування не знайдено диференційних характеристик з ймовірністю вищою за ймовірність атаки повного перебирання, блоковий шифр «Кипарис-256» є практично стійким до диференційного криптоаналізу.

*Ключові слова:*диференційний криптоаналіз, диференційна характеристика, симетричний блоковий шифр, малоресурсна криптографія.

Табл. 6. Іл. 2. Бібліогр: 17 назв.

UDC 621.3.06

Evaluation of block cipher “Cypress” strength against differential cryptanalysis / *M.Yu. Rodinko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 113 – 124.

This paper presents an evaluation of the practical strength of the lightweight block cipher “Cypress” to the differential cryptanalysis, which is determined by the probability of the best found differential characteristic. The paper proposes a mathematical model for evaluating the block cipher “Cypress” to differential cryptanalysis and methods for searching for multi-round differential characteristics. The first method is based on the combination of highly probable one-round differential characteristics into multi-round ones, while the second method is based on the extension of one-round characteristics for several rounds. As a result of the application of the second search method to the block cipher Cypress-256, a 6-round differential characteristic was found. Since it was not found a differential characteristics for more than six rounds with a probability which is higher than the probability of a brute-force attack, the block cipher Cypress-256 is practically resistant to differential cryptanalysis.

Key words: differential cryptanalysis, differential characteristic, block cipher, lightweight cryptography.

6 tab. 2 fig. Ref.: 17 items.

УДК 004.056.5

Нелинейные функции усложнения для потоковых симметричных шифров / *А.А. Кузнецов, А.В. Потий, Н.А. Полуяненко, И.В. Стельник* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 125 – 137.

Нелинейные булевы функции исследуются по всему миру очень активно. Тем не менее, в этой области остается множество открытых вопросов. Теория нелинейных булевых функций, пригодных для использования в криптографических стойких алгоритмах, в значительной степени неполна. Несмотря на наличие многочисленных публикаций на эти темы, многие вопросы, связанные с взаимосвязью конструктивных характеристик, влияющей на производительность генератора и его криптографические характеристики, пока ещё остаются открытыми. Генерация особого типа последовательностей, называемых последовательностями де Брейна, с минимальными аппаратно-программными затратами, обоснование возможности их применения в качестве нелинейных функций усложнения системах поточного шифрования, является главной темой работы. Приведены оценки криптографических показателей нелинейных функций усложнения итеративных генераторов битовых последовательностей при различных характеристиках формируемой последовательности, таких как линейная сложность и автокорреляция.

Ключевые слова: генераторы псевдослучайных последовательностей; последовательность де Брейна; криптографический анализ; булевы функции; нелинейные функции усложнения.

Табл. 13. Ил. 2. Библиогр.: 25 назв.

УДК 004.056.5

Комбінуючі та фільтруючі функції на основі регістрів зсуву з нелінійними зворотними зв’язками / *О.О. Кузнецов, О.В. Потій, М.О. Полуяненко, І.В. Стєльнік* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 125 – 137.

Нелінійні булеві функції досліджуються по всьому світу дуже активно. Проте, в цій області залишається безліч відкритих питань. Теорія нелінійних булевих функцій, придатних для використання в криптографічно стійких алгоритмах, в значній мірі неповна. Незважаючи на наявність численних

публікацій на ці теми, багато питань, пов'язаних з взаємозв'язком конструктивних характеристик, що впливає на продуктивність генератора і його криптографічних характеристик, поки ще залишаються відкритими. Генерація особливого типу послідовностей, званих послідовностями де Брейна, з мінімальними апаратно-програмними витратами, обґрунтування можливості їх застосування в якості нелінійних функцій ускладнення системах потокового шифрування, є головною темою роботи. В роботі наведено оцінки криптографічних показників нелінійних функцій ускладнення ітеративних генераторів бітових послідовностей при різних характеристиках формованої послідовності, таких як лінійна складність і автокореляція.

Ключові слова: генератори псевдовипадкових послідовностей; послідовність де Брейна; криптографічний аналіз; булеві функції; нелінійні функції ускладнення.

Табл. 13. Іл. 2. Бібліогр.:25 назв.

UDC 004.056.5

Combining and filtering functions in the framework of nonlinear-feedback shift register / *A.A. Kuznetsov, A.V. Potii, N.A. Poluyanenko, I.V. Stelnik* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 125 – 137.

Currently, nonlinear Boolean functions are being investigated very actively around the world. However, many open questions remain in this area. The theory of nonlinear Boolean functions suitable for use in robust cryptographic algorithms is largely incomplete. Despite the presence of numerous publications on these topics, many issues related to the interrelation of design characteristics affecting the performance of the generator and its cryptographic characteristics are still open. The generation of a special type of sequences, called de Brain sequences, with minimal hardware and software costs, the rationale for their use as non-linear functions of the complexity of stream encryption systems, is the main theme of this work. The paper presents estimates of cryptographic indicators of nonlinear complexity functions of iterative bit sequence generators with various characteristics of the generated sequence, such as linear complexity and autocorrelation.

Keywords: pseudo-random sequence generators; de Brain sequence; cryptographic analysis; Boolean functions; nonlinear complication functions

13 tab. 2 fig. Ref.: 25 items.

МЕТОДЫ И АЛГОРИТМЫ ЗАЩИТЫ И СОКРЫТИЯ ИНФОРМАЦИИ
МЕТОДИ ТА АЛГОРИТМИ ЗАХИСТУ ТА ПРИХОВУВАННЯ ІНФОРМАЦІЇ
METHODS AND ALGORITHMS FOR PROTECTION AND CONCEALING INFORMATION

УДК 004.056.5

Средства моделирования и анализа рисков в среде облачных вычислений / *И.Ф. Аулов, К.Е. Лисицкий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 138 – 143.

Статья посвящена средствам, которые могут применяться для моделирования и анализа рисков в среде облачных вычислений. Рассматривается бесплатное программное обеспечение с открытым кодом: OWASP Threat Dragon, CAIRIS, Mozilla Seasponge и коммерческое с закрытым кодом: Microsoft Threat Modeling Tool, RiskWatch, vsRisk, а также анализируются его преимущества и недостатки. Предложены требования к программам моделирования и анализа рисков в среде облачных вычислений. На основе оценки соответствия предъявляемым требованиям было выполнено сравнение существующего программного обеспечения в результате которого было определено, что хотя Microsoft Threat Modeling Tool не в полной мере им соответствует, но в данный момент является лучшей для моделирования и анализа рисков в облаках.

Ключевые слова: моделирование угроз, облачные вычисления, анализ рисков.

Табл. 1. Библиогр.: 10 назв.

УДК 004.056.5

Засоби моделювання та аналізу ризиків в середовищі хмарних обчислень / *І.Ф. Аулов, К.Є. Лисицкий* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 138 – 143.

Стаття присвячена засобам, що можуть застосовуватися для моделювання та аналізу ризиків в середовищі хмарних обчислень. Розглядається безкоштовне програмне забезпечення з відкритим кодом: OWASP Threat Dragon, CAIRIS, Mozilla Seasponge та комерційне з закритим програмним кодом: Microsoft Threat Modeling Tool, RiskWatch, vsRisk, а також аналізуються його перевагм та недоліки. Запропоновано вимоги до програм моделювання та аналізу ризиків в середовищі хмарних обчислень. На основі оцінки відповідності висунутим вимогам було виконано порівняння існуючого програмного забезпечення в результаті якого було визначено, що хоча Microsoft Threat Modeling Tool не в повній мірі їм відповідає, але наразі є найкращою для моделювання та аналізу ризиків в хмарах.

Ключові слова: моделювання загроз, хмарні обчислення, аналіз ризиків.

Табл. 1. Бібліогр.: 10 назв.

UDC 004.056.5

Tools for modeling and analysis of risks in the cloud computing environment / *I.F. Aulov, K.E. Lisickiy* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 138 – 143.

This article focuses on tools that can be used to model and analyze risks in a cloud computing environment. The article discusses free open source software: OWASP Threat Dragon, CAIRIS, Mozilla Seasponge and commercial with closed code: Microsoft Threat Modeling Tool, RiskWatch, vsRisk, as well as an analysis of its advantages and disadvantages. The article proposes requirements for modeling programs and risk analysis in the cloud computing environment. Based on the compliance assessment, a comparison was made of existing software, which resulted in the determination that although the Microsoft Threat Modeling Tool does not fully comply with them, it is currently the best for modeling and analyzing risks in the clouds.

Key words: threat modeling, cloud computing, risk analysis.

1 table. Ref.: 10 items.

УДК 621.391:519.2

Исследование *k*-мерности булевой функции шифра LILI-128 / *С.Н. Конюшок* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 144 – 149.

Представлены результаты экспериментального исследования *k*-мерности булевой функции шифра LILI-128, которые продемонстрировали потенциальную возможность реализации статистической атаки, основанной на приближении булевых функций алгебраически вырожденными функциями.

Ключевые слова: криптографические свойства булевых функций, k-мерная функция, вероятностный алгоритм, усовершенствованный тест k-мерности, шифр LILI-128.

Табл. 1. Ил. 1. Библиогр.: 23 назв.

УДК 621.391:519.2

Дослідження *k*-вимірності булевої функції шифру LILI-128 / *С.М. Конюшок* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 144 – 149.

Представлено результати експериментального дослідження *k*-вимірності булевої функції шифру LILI-128, що продемонстрували потенційну можливість реалізації статистичної атаки, яка базується на наближенні булевих функцій алгебраїчно виродженими функціями.

Ключові слова: криптографічні властивості булевих функцій, k-вимірна функція, імовірнісний алгоритм, вдосконалений тест k-вимірності, шифр LILI-128.

Табл. 1. Іл. 1. Бібліогр.: 23 назви.

UDC 621.391:519.2

Investigation of the k-dimensionality of the LILI-128 cipher Boolean function / *S.M. Koniushok* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 144 – 149.

The paper presents results of the experimental study of the k-dimensionality of the LILI-128 cipher Boolean function, which demonstrated the potential for the realization of a statistical attack based on near-proximity of Boolean functions with algebraically degenerate functions.

Keywords: cryptographic properties of boolean functions, k-dimensional function, probabilistic algorithm, improved k-dimensional test, LILI-128 cipher.

1 tab. 1 fig. Ref.: 23 items.

УДК 004.056.5

Эвристические методы градиентного поиска криптографических булевых функций / *А.А. Кузнецов, И.В. Московченко, Д.И. Прокопович-Ткаченко, Т.Ю. Кузнецова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 150 – 164.

Рассматриваются эвристические методы градиентного поиска криптографических булевых функций, удовлетворяющих требуемым свойствам сбалансированности, нелинейности, автокорреляции и др. показателям стойкости. Исследуется предложенный метод градиентного спуска, в частности приводятся оценки нелинейности и корреляционной иммунности синтезируемых булевых функций. Предлагается методика оценки вычислительной эффективности методов градиентного поиска, основанная на построении выборочных (эмпирических) функций распределения, характеризующих вероятность формирования булевых функций с показателями стойкости не ниже требуемых. В качестве показателя вычислительной эффективности предлагается среднее число попыток, которое по-

требуется выполнить с использованием эвристического метода, для формирования криптографической булевой функции с требуемыми свойствами. Приводятся сравнительные оценки эффективности рассмотренных эвристических методов. Показано, что предложенный метод градиентного спуска позволяет формировать криптографические функции с требуемыми показателями стойкости за меньшее число шагов. Приводятся результаты исследований криптографических свойств формируемых булевых функций в сравнении с наилучшими известными оценками.

Ключевые слова: симметричная криптография; нелинейные блоки замен; булевы функции; сбалансированность, нелинейность, автокорреляция.

Табл. 6. Ил. 10. Библиогр.: 40 назв.

УДК 004.056.5

Евристичні методи градієнтного пошуку криптографічних булевих функцій / *О.О. Кузнецов, І.В. Московченко, Д.І. Прокопович-Ткаченко, Т.Ю. Кузнецова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 150 – 164.

Розглядаються евристичні методи градієнтного пошуку криптографічних булевих функцій, що задовольняють необхідним властивостям збалансованості, нелінійності, автокореляції та ін. показникам стійкості. Досліджується запропонований метод градієнтного спуску, зокрема наводяться оцінки нелінійності і кореляційної імунності синтезованих булевих функцій. Пропонується методика оцінки обчислювальної ефективності методів градієнтного пошуку, заснована на побудові вибіркових (емпіричних) функцій розподілу, що характеризують ймовірність формування булевих функцій з показниками стійкості не нижче необхідних. Як показник обчислювальної ефективності пропонується середнє число спроб, яке буде потрібно виконати з використанням евристичного методу, для формування криптографічної булевої функції з необхідними властивостями. Наводяться порівняльні оцінки ефективності розглянутих евристичних методів. Показано, що запропонований метод градієнтного спуску дозволяє формувати криптографічні функції з необхідними показниками стійкості за менше число кроків. Наводяться результати досліджень криптографічних властивостей формованих булевих функцій в порівнянні з найкращими відомими оцінками.

Ключові слова: симетрична криптографія; нелінійні блоки замін; булеві функції; збалансованість, нелінійність, автокореляція.

Табл. 6. Іл. 10. Бібліогр.:40 назв.

UDC 004.056.5

Heuristic methods for gradient search of cryptographic Boolean functions / *A.A. Kuznetsov, I.V. Moskovchenko, D.I. Prokopovych-Tkachenko, T.Y. Kuznetsova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 150 – 164.

Heuristic methods of gradient search of cryptographic Boolean functions that satisfy the required properties of balance, nonlinearity, autocorrelation, and other stability indicators are considered. The proposed method of gradient descent is investigated, in particular, estimates of nonlinearity and correlation immunity of the synthesized Boolean functions are given. A method for evaluating the computational efficiency of gradient search methods is proposed, based on the construction of sample (empirical) distribution functions, which characterize the probability of the formation of Boolean functions with persistence indicators not lower than those required. As an indicator of computational efficiency, we propose the average number of attempts that need to be performed using the heuristic method to form a cryptographic Boolean function with the required properties. It is shown that the proposed gradient descent method allows the formation of cryptographic functions with the required durability indicators in fewer steps. The results of investigations of the cryptographic properties of the formed Boolean functions in comparison with the best known assessments are given.

Keywords: heuristic methods, cryptographic Boolean functions, symmetric cryptography, nonlinear substitute blocks

6 tab. 10 fig. Ref.: 40 items.

УДК 004.056.5

Стеганоанализ цифровых изображений в условиях различной степени наполненности контентов / *А.В. Ахмаметьева, Мпуту Кристофер Бвабва* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 165 – 173.

Предложено усовершенствование стеганоаналитического метода выявления вложений дополнительной информации в цветные цифровые изображения, основанного на учёте последовательных триад триплетов в матрице уникальных цветов и показавшего высокую эффективность выявления стеганосообщений, сформированных при условии заполнения только одной цветовой составляющей контейнера. Однако в процессе стеганопреобразования возможны случаи погружения конфиденци-

альных данных в две и три цветовые составляющие изображений, что обеспечивает сокрытие большего объёма информации и требует доработки существующего метода стеганоанализа. В ходе проведенных исследований проанализирован характер возмущений количества средних триплетов в матрице уникальных цветов в результате погружения дополнительной информации в две и три цветовые составляющие изображений, изначально хранимых в формате с потерями, а также с учётом полученных результатов уточнены параметры оригинального метода выявления стеганосообщений. Установлено, что характер изменений количества последовательных триад триплетов в результате стеганопреобразования отличается в случаях использования контейнеров в формате с потерями и контейнеров в формате без потерь. На основании полученных данных проведено усовершенствование стеганоаналитического метода путём интеграции его с методом выявления факта сжатия цифровых контентов, разработанного ранее. По результатам вычислительных экспериментов разработанный метод обеспечивает высокую эффективность при выявлении стеганосообщений, сформированных с разной степенью наполненности контейнеров, не снижая при этом правильность выявления заполненных цветовых составляющих, если дополнительная информации погружалась только в одну цветовую составляющую цифровых изображений. Разработанный метод может использоваться как основа для комплексного стеганоанализа цифровых контентов с применением существующих методов, анализирующих отдельные цветовые матрицы изображений.

Ключевые слова: стеганоанализ, цифровое изображение, последовательные триады триплетов, пространственная область, формат с потерями, формат без потерь.

Табл. 3. Ил. 1. Библиогр. 12 назв.

УДК 004.056.5

Стеганоаналіз цифрових зображень в умовах різного ступеню наповненості контентів / *Г.В. Ахмаметьєва, Мпуту Крістофер Бвабва //* Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 165 – 173.

Запропоновано удосконалення стеганоаналітичного методу виявлення вкладень додаткової інформації в кольорові цифрові зображення, заснованого на врахуванні послідовних тріад триплетів в матриці унікальних кольорів, який показав високу ефективність виявлення стеганоповідомлень, сформованих за умови заповнення тільки однієї колірної складової контейнера. Однак в процесі стеганоперетворення можливі випадки вбудови конфіденційних даних в дві або три колірні складові зображень, що забезпечує приховування більшого обсягу інформації і вимагає доопрацювання існуючого методу стеганоаналізу. В ході проведених досліджень проаналізовано характер збурень кількості середніх триплетів в матриці унікальних кольорів в результаті вбудови додаткової інформації в дві і три колірні складові зображень, спочатку збережених в форматі з втратами, а також з урахуванням отриманих результатів уточнені параметри оригінального методу виявлення стеганоповідомлень. Встановлено, що характер змін кількості послідовних тріад триплетів в результаті стеганоперетворення відрізняється у випадках використання контейнерів в форматі з втратами і контейнерів в форматі без втрат. На підставі отриманих даних проведено удосконалення стеганоаналітичного методу шляхом інтеграції його з методом виявлення факту стиску цифрових контентів, розробленого раніше. За результатами обчислювальних експериментів розроблений метод забезпечує високу ефективність при виявленні стеганоповідомлень, сформованих з різним ступенем наповненості контейнерів, не знижуючи при цьому правильність виявлення заповнених колірних складових, якщо додаткова інформації була вбудована тільки в одну колірну складову цифрових зображень. Розроблений метод може використовуватися як основа для комплексного стеганоаналізу цифрових контентів із застосуванням існуючих методів, які аналізують окремі колірні матриці зображень.

Ключові слова: стеганоаналіз, цифрове зображення, послідовні тріади триплетів, просторова область, формат з втратами, формат без втрат

Табл. 3. Іл. 1. Бібліогр. 12 назв.

UDC 004.056.5

Steganalysis of digital images in conditions of varying degrees of contents fullness / *Anna V. Akhmametieva, Mputu Chrisopher Bwabwa //* Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 165 – 173.

An improvement of the steganalytic method for detection of the presence of additional information in color digital images which showed high efficiency in identifying stego formed by embedding of secret data only into one color component of the container is presented. The proposed method analyses digital image in the spatial domain and is based on the accounting of sequential color triads in the matrix of unique colors of the digital content. However, in the process of steganographic transformation cases of embedding of confidential data into two and three color components of images are possible that ensures the concealment of a

larger amount of information and requires the improvement of the existing method of steganalysis. In the course of the conducted research the character of perturbations in the quantity of sequential triads of triplets in a matrix of unique colors as a result of embedding of additional information into two and three color components of images originally stored in a losses format was analyzed. Considering obtained results the parameters of the original method for detecting of stego was refined. It has been established that the character of changes in the quantity of sequential triads of triplets as a result of steganographic transformation is different in cases of using containers in a losses format and containers in a lossless format. Based on the obtained data the steganalytic method has been improved by integrating it with the method of detection the fact of compression of digital content developed earlier. The developed method provides high efficiency in detecting stego formed with different degree of container fullness without reducing the accuracy of identifying the filled color components if the additional information was embedded into only one color component of the digital images. This method can be used as a basis for complex steganalysis of digital contents by using existing methods that analyzes color matrixes of images separately.

Keywords: steganalysis, digital image, sequential triads of triplets, spatial domain, losses format, lossless format

3 tab. 1 fig. Ref.: 12 items.

УДК 004.043

Сравнительный анализ алгоритмов консенсуса для технологии распределенных реестров / *Д.Г. Биличенко, Е.Ю. Витюк, Р.В. Олейников* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 174 – 183.

Приведена сравнительная характеристика алгоритмов достижения консенсуса в распределенных реестрах, основанных на разных технологиях, таких как блокчейн и направленный ациклический граф. Приведены преимущества и недостатки алгоритмов консенсуса GHOST, Tangle и Hashgraph, а также рекомендации по выбору оптимального варианта.

Ключевые слова: блокчейн, алгоритм консенсуса, GHOST, Tangle, Hashgraph.

Табл. 1. Ил. 5. Библиогр.: 14 назв.

УДК 004.043

Порівняльний аналіз алгоритмів консенсусу для технології розподілених реєстрів / *Д.Г. Біліченко, К.Ю. Вітюк, Р.В. Олійников* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 174 – 183.

Наведено порівняльну характеристику алгоритмів досягнення консенсусу в розподілених реєстрах, які засновані на різних технологіях, таких як блокчейн та направлений ациклічний граф. Наведені переваги та недоліки алгоритмів коненсусу GHOST, Tangle и Hashgraph, а також рекомедації щодо вибору оптимального варіанту.

Ключові слова: блокчейн, алгоритм консенсусу, GHOST, Tangle и Hashgraph.

Табл. 1. Іл. 5. Бібліогр.: 14 назв.

UDC 004.043

Comparative analysis of consensus algorithms for distributed ledger technologies / *D. Bilichenko, K. Vitiuk, R. Oliynykov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 174 – 183.

The comparative characteristic of consensus algorithms in distributed ledgers based on different technologies such as blockchain and directed acyclic graph is given in the article. Advantages and disadvantages of GHOST, Tangle and Hashgraph consensus algorithms are given, as well as recommendations of optimal variant selection.

Keywords: blockchain, consensus algorithm, GHOST, Tangle, Hashgraph.

1 Tab. 5. Fig. Ref.: 14 items.

УДК 004.652: 004.658.3

Метод разработки баз данных, легко адаптируемых к изменениям в предметной области / *В.И. Есин, В.В. Вилигура* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 184 – 192.

Предлагается метод разработки реляционных баз данных с инвариантной к предметным областям схемой, применение которого в отличие от традиционной технологии проектирования позволяет: создавать в процессе реинжиниринга отвечающие требованиям потребителей информационного продукта базы данных для различных моделируемых предметных областей при меньших временных и

финансовых затратах; адаптировать реляционные БД, построенные на основе схемы с универсальным базисом отношений, к динамичным изменениям предметных областей, без изменения схемы БД, за счет использования созданной предопределенной структуры базовых отношений.

Ключевые слова: база данных, реляционная база данных, схема базы данных, модель данных, модель данных с универсальным базисом отношений, модель данных «объект-событие».

Ил. 3. Библиогр.: 56 назв.

УДК 004.652: 004.658.3

Метод розробки баз даних, що легко адаптуються до змін в предметній області / *В.І. Єсін, В.В. Вілігура* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 184 – 192.

Пропонується метод розробки реляційних баз даних з інваріантної до предметних областей схемою, застосування якого на відміну від традиційної технології проектування дозволяє: створювати в процесі реінжинірингу бази даних для різних модельованих предметних областей, що відповідають вимогам споживачів інформаційного продукту, при менших часових і фінансових витратах; адаптувати реляційні БД, побудовані на основі схеми з універсальним базисом відношень, до динамічних змін предметних областей, без зміни схеми БД, за рахунок використання створеної зумовленої структури базових відношень.

Ключові слова: база даних, реляційна база даних, схема бази даних, модель даних, модель даних з універсальним базисом відношень, модель даних «об'єкт-подія».

Іл. 3. Бібліогр.: 56 назв.

UDC 004.652: 004.658.3

Method for developing databases being easily adaptable to changes in the subject domain / *V.I. Yesin, V.V. Vilihura* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 184 – 192.

A method for developing relational databases with the schema invariant to subject domains is proposed. The use of this method unlike the traditional technology of designing relational databases allows: creating databases for various simulated subject domains that meet the requirements of consumers of the information product in the process of reengineering, with less time and financial costs; adapting relational databases built on the basis of a scheme with a universal basis of relations to dynamic changes in subject domains, without changing the database schema, due to the use of the created predetermined structure of basic relations.

Key words: database, relational database, database schema, data model, data model with an universal basis of relations, "object-event" data model.

3 fig. Ref.: 56 items.

УДК 004.056.5

3D стеганографическое сокрытие информации / *А.А. Кузнецов, О.О. Стефанович, Д.И. Прокопович-Ткаченко, Е.А. Кузнецова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 193 – 202.

Исследовано новое направление технической стеганографии, связанное с сокрытием информационных данных в процессе послойного создания (выращивания) твердотельного объекта при использовании различных технологий 3D-печати. Информационные данные преобразуются в цифровую 3D-модель элементарных физических объектов, которые размещаются внутри 3D-модели изделия-контейнера. После распечатки твердый объект физически содержит скрытую информацию, которую невозможно удалить или исказить без повреждения контейнера. Кроме того, применяемые методы не снижают эксплуатационных, эстетических и любых других свойств готового изделия, поскольку технологии, применяемые для нанесения слоев, не модифицируются, сокрытие является инвариантным к способу послойного выращивания, то есть могут применяться различные устройства 3D-печати с любыми материалами и принципами послойного создания.

Ключевые слова: стеганография; 3D-принтер; сокрытие информационных данных; 3D-модель; лазерные сканеры.

Табл. 2. Ил. 9. Библиогр.: 17 назв.

УДК 004.056.5

3D стеганографічне приховування інформації / *О.О. Кузнецов, О.О. Стефанович, Д.И. Прокопович-Ткаченко, К.О. Кузнецова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 193 – 202.

Досліджено новий напрямок технічної стеганографії, який пов'язаний із приховуванням інформаційних даних в процесі пошарового створення (вирощування) твердотільного об'єкта при використанні різних технологій 3D-друку. Інформаційні дані перетворюються в цифрову 3D-модель елемен-

тарних фізичних об’єктів, які розміщуються всередині 3D-моделі виробу-контейнеру. Після роздрукування твердий об'єкт фізично містить приховану інформацію, яку неможливо видалити або спотворити без пошкодження контейнеру. Крім того, застосовані методи не знижують експлуатаційних, естетичних та будь яких інших властивостей готового виробу, оскільки технології, що застосовуються для нанесення шарів, не модифікуються, приховування є інваріантним способу пошарового вирощування, тобто можуть застосовуватися різні пристрої 3D-друку з будь-якими матеріалами і принципами пошарового створення.

Ключові слова: стеганографія; 3D-друк; приховування інформаційних даних; 3D-модель; лазерні сканери.

Табл. 2. Іл. 9. Бібліогр.:17 назв.

UDC 004.056.5

3D steganography hiding of information / *A.A. Kuznetsov, O.O. Stefanovych, D.I. Prokopovych-Tkachenko, K.O. Kuznetsova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 193 – 202.

A new direction of technical steganography related to the concealment of information in the process of layer-by-layer creation (cultivation) of a solid-state object using various 3D-printing technologies is investigated. Information data are converted into a digital 3D-model of elementary physical objects that are placed inside this 3D-model of the container product. After printing, a solid object physically contains the hidden information that cannot be deleted or distorted without damaging the container product. In addition, the applied methods do not reduce the operational, aesthetic and any other properties of the finished product. The proposed complex is invariant to the method of layer-by-layer growing, that is, it can be equipped with any peripheral devices of 3D-printing of various manufacturers with any materials and principles of layer-by-layer creation.

Keywords: steganography; 3D-printing; hiding information data; 3D-model; laser scanners

2 tab. 9 fig. Ref.: 17 items.

УДК 004.056

Децентрализованные протоколы консенсуса: возможности и рекомендации по применению / *Е.В. Исирова, А.В. Потий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 203 – 208.

Освещены проблемные вопросы построения централизованных систем. Предложено проектирование децентрализованных систем, в том числе для критических инфраструктур. Проведен сравнительный анализ существующих децентрализованных протоколов консенсуса и даны рекомендации по их применению.

Ключевые слова: децентрализованные системы, технология blockchain, протоколы консенсуса, PoW протоколы, PoS протоколы, BFT протоколы.

Табл. 2. Ил. 3. Библиогр.: 12 назв.

УДК 004.056

Децентралізовані протоколи консенсусу: можливості та рекомендації щодо використання / *К.В. Ісірова, О.В. Потій* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 203 – 208.

Висвітлено проблемні питання побудови централізованих систем. Запропоноване проектування децентралізованих систем в тому числі для критичної інфраструктури. Проведений аналіз існуючих децентралізованих протоколів консенсусу та надані рекомендації щодо їх застосування.

Ключові слова: децентралізовані системи, технологія blockchain, протоколи консенсусу, PoW протоколи, PoS протоколи, BFT протоколи.

Табл. 2. Іл. 3. Бібліогр .: 12 назв.

UDK 004.056

Decentralized consensus protocols: possibilities and recommendations for use / *K.V. Isirova, O.V. Potii* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 203 – 208.

Centralised systems development problematic issues are described. Decentralized systems development including for critical infrastructures is proposed. Existing decentralized consensus protocols comparative analysis is carried out and recommendations for their use are proposed.

Key words: decentralized systems, blockchain technology, consensus protocols, PoW protocols, PoS protocols, BFT protocols.

2 tab. 3 fig. Ref.: 12 items.

МЕТОДЫ ВЫЯВЛЕНИЯ, РАСПОЗНАВАНИЯ И УПРАВЛЕНИЯ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ
МЕТОДИ ВИЯВЛЕННЯ, РОЗПІЗНАВАННЯ ТА УПРАВЛІННЯ ЛІТАЛЬНИМИ АПАРАТАМИ
METHODS FOR AIRCRAFT DETECTION, RECOGNITION AND CONTROL

УДК 629.7.022

Исследование эффективности обнаружения и распознавания малоразмерных беспилотных летательных аппаратов по их акустическому излучению / *В.Н. Олейников, О.В. Зубков, В.М. Карташов, И.В. Корытцев, С.И. Бабкин, С.А. Шейко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 209 – 217.

Рассмотрены особенности спектрального состава акустических излучений беспилотных летательных аппаратов, природных шумов, индустриальных излучений автомобильного и рельсового транспорта, речевых звуков человека. Для распознавания акустических излучений беспилотного летательного аппарата предложен метод на основании коэффициентов мел-кепстарльного анализа. Также предложен универсальный метод обнаружения акустических излучений беспилотного летательного аппарата по характерным особенностям спектра. Оба метода апробированы с использованием экспериментальных записей акустических излучений и дают идентичные качественные результаты. Получены зависимости эффективности распознавания от расстояния для предложенных методов. Универсальный метод уступает методу распознавания по надежности распознавания и вероятности ложного обнаружения, но не требует создания базы образов акустических излучений.

Ключевые слова: беспилотный летательный аппарат, акустическое излучение, обнаружение, распознавание.

Табл. 1. Ил. 6. Библиогр.: 8 назв.

УДК 629.7.022

Дослідження ефективності виявлення і розпізнавання малорозмірних безпілотних літальних апаратів по їх акустичному випромінюванню / *В.М. Олейников, О.В. Зубков, В.М. Карташов, І.В. Корытцев, С.І. Бабкин, С.О. Шейко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 209 – 217.

Розглянуто особливості спектрального складу акустичних випромінювань безпілотних літальних апаратів, природних шумів, індустріальних випромінювань автомобільного та рейкового транспорту, мовних звуків людини. Для розпізнавання акустичних випромінювань безпілотного літального апарату запропонований метод на підставі коефіцієнтів мел-кепстарльного аналізу. Також запропонований універсальний метод виявлення акустичних випромінювань безпілотного літального апарату за характерними особливостями спектру. Обидва методи апробовані з використанням експериментальних записів акустичних випромінювань і дають ідентичні якісні результати. Отримано залежності ефективності розпізнавання від відстані для запропонованих методів. Універсальний метод поступається методу розпізнавання по надійності розпізнавання і ймовірності помилкового виявлення, але не вимагає створення бази образів акустичних випромінювань.

Ключові слова: безпілотний літальний апарат, акустичне випромінювання, виявлення, розпізнавання.

Табл. 1. Іл. 6. Бібліограф.: 8 назв.

UDC 629.7.022

Investigation of the efficiency of detection and recognition of small-sized unmanned aerial vehicles by their acoustic radiation / *V.N. Oleynikov, O.V. Zubkov, V.M. Kartashov, I.V. Korytsev, S.I. Babkin, S.A. Sheiko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 209 – 217.

The features of acoustic spectrum of UAVs, spectrum of natural and industrial acoustic noise, noise spectrum of automobile and rail transport, and human speech spectrum were investigated. The method for recognition of UAV sound based on the Mel-frequency cepstral coefficients was proposed. The universal method for detecting UAV based on characteristic features of acoustic spectrum was proposed as well. Both methods were tested using experimental recordings of UAVs and noise sounds and got close well results. The universal recognition method has some worse recognition reliability and false alarm probability, but does not need creation of sound and noise images base.

Key words: unmanned aerial vehicle, acoustic radiation, detection, recognition

1 tab. 6 fig. Ref. 8 items.

УДК 004.413.7

Метод оценки зрелости системы управления безопасностью при организации воздушного движения / *И.Д. Горбенко, А.А. Замула, С.Г. Вдовенко, В.И Черныш* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 218 – 223.

Защита инфраструктуры системы организации воздушного движения провайдера аэронавигационного обслуживания осуществляется путем обеспечения безопасности информационно-телекоммуникационных систем, физической безопасности, кадровой безопасности и обеспечения непрерывности предоставления услуг по аэронавигационному обслуживанию. Впервые предложен метод оценки зрелости системы управления безопасностью при организации воздушного движения провайдера аэронавигационного обслуживания, который позволяет определить фактический и прогнозируемый уровни соответствия системы управления безопасностью при организации воздушного движения действующим требованиям нормативно-правовых актов, международных стандартов с учетом весовых коэффициентов.

Ключевые слова: риск, управление безопасностью, провайдер, информационная безопасность, зрелость системы.

Табл. 1. Ил. 1. Библиогр.: 5 назв.

УДК 004.413.7

Метод оцінки зрілості системи управління безпекою при організації повітряного руху / *І.Д. Горбенко, О.А. Замула, С.Г. Вдовенко, В.І Черниш* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 218 – 223.

Питання забезпечення захисту інфраструктури системи організації повітряного руху провайдера аеронавігаційного обслуговування здійснюється шляхом забезпечення безпеки інформаційно-телекомунікаційних систем, фізичної безпеки, кадрової безпеки та забезпечення безперервності надання послуг з аеронавігаційного обслуговування. Вперше запропоновано метод оцінки зрілості системи управління безпекою при організації повітряного руху провайдера аеронавігаційного обслуговування. Зазначений метод дозволяє визначити фактичний та прогнозований рівні відповідності системи управління безпекою при організації повітряного руху чинним вимогам нормативно-правових актів, міжнародних стандартів та з урахуванням вагових коефіцієнтів.

Ключові слова: ризик, управління безпекою, провайдер, інформаційна безпека, зрілість системи.

Табл. 1. Іл. 1. Бібліогр.: 5 назв.

UDC 004.413.7

Method of Maturity Assessment of Air Traffic Management Security System / *I.D. Gorbenko, O.A. Zamula, S.G. Vdovenko, V.I. Chernysh* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 218 – 223.

The protection of the air traffic management system infrastructure of the air navigation services provider is carried out by ensuring the security of information and telecommunications systems, physical security, personnel security and ensuring the continuity of air navigation services provision. Here the authors first proposed a method for assessing the maturity of a security management system in the air traffic management system of air navigation service provider. The proposed method allows determining the actual and predicted levels of compliance of the security management system in the air traffic management system to the current requirements of regulatory legal acts, international standards, taking into account the weight coefficients.

Keywords: risk, management security, provider, information security, system maturity.

1 tab. 1 fig. Ref.: 5 items.

УДК 004.056.5

Нечеткий экстрактор на помехоустойчивых кодах для биометрической криптографии / *А.А. Кузнецов, Р.В. Сергиенко, А.А. Уварова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 224 – 234.

Рассмотрены методы формирования криптографических ключей из биометрических образов с использованием нечетких экстракторов. Предложена схема нечеткого экстрактора, в основе которой лежит кодовая криптосистема Мак-Элиса. Показано, что новая конструкция нечеткого экстрактора позволяет формировать криптографические пароли из биометрических образов даже без использования несекретных подсказок (helper string). При использовании helper string значительно возрастает доля корректируемых искажений биометрических образов. Предлагаемая конструкция относится к классу постквантовых методов защиты информации, т.е. ожидается ее безопасное использование в условиях применения универсальных квантовых компьютеров для решения задач криптоанализа.

Ключевые слова: криптосистема на основе кода; нечеткий экстрактор; биометрическая криптография; криптографические ключи.

Ил. 5. Библиогр.: 18 назв.

УДК 004.056.5

Нечіткий екстрактор на перешкодостійких кодах для біометричної криптографії / *О.О. Кузнецов, Р.В. Сергиенко, А.О. Уварова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 224 – 234.

Розглянуто методи формування криптографічних ключів з біометричних образів з використанням нечітких екстракторів. Запропоновано нову схему нечіткого екстрактора, в основі якої лежить кодова криптосистема Мак-Еліса. Показано, що нова конструкція нечіткого екстрактора дозволяє формувати криптографічні паролі з біометричних образів навіть без використання несекретних підказок (helper string). При використанні helper string значно зростає частка коректованих спотворень біометричних образів. Крім того, пропонована конструкція відноситься до класу постквантових методів захисту інформації, тобто очікується її безпечне використання навіть в умовах застосування універсальних квантових комп'ютерів для вирішення завдань криптоаналізу.

Ключові слова: криптосистема на основі коду; нечіткий екстрактор; біометрична криптографія; криптографічні ключі.

Іл. 5. Бібліогр.:18 назв.

UDC 004.056.5

Code based fuzzy extractor for biometric cryptography / *A.A. Kuznetsov, R.V. Serhiienko, A.A. Uvarova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 224 – 234.

Methods of forming cryptographic keys of biometric images using fuzzy extractors are considered. A new scheme of a fuzzy extractor based on the McEliece cryptosystem is proposed. It is shown that the new design of the fuzzy extractor allows forming cryptographic passwords from biometric images even without the use of non-secret helper string. When using helper string, the proportion of corrected distortions of biometric images increases significantly. In addition, the proposed design relates to a class of post-quantum information security methods, i.e. it is expected to be safely used even for solving cryptanalysis problems with universal quantum computers.

Keywords: code based cryptosystem; fuzzy extractor; biometric cryptography; cryptographic keys

5 fig. Ref.: 18 items.

УДК 629.7.022

Особенности обнаружения и распознавания малых беспилотных летательных аппаратов / *В.М. Карташов, В.Н. Олейников., С.А. Шейко, С.И. Бабкин, И.В. Корытцев., О.В. Зубков* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 235 – 243.

Проведен обзор и анализ методов обнаружения и распознавания беспилотных летательных аппаратов (БПЛА). Рассмотрены каналы для обнаружения БПЛА – акустический, оптический, радиолокационный, инфракрасный, канал радиоразведки. Сравнены и оценены преимущества и недостатки используемых каналов. В случае малых БПЛА имеется ряд существенных сложностей и ограничений. Одним из направлений в обнаружении БПЛА являются акустические наблюдения. Шум, создаваемый силовой установкой БПЛА и воздушным винтом, является существенным демаскирующим признаком. Создание и совершенствование методов обнаружения, пеленгации и распознавания малых БПЛА путем приёма и обработки их звуковых сигналов является актуальной задачей. При применении такого метода обнаружения БПЛА используются частотные спектры, спектрограммы, нормированные автокорреляционные функции и фазовые портреты акустических сигналов. Информационными признаками звукового образа БПЛА могут служить оценки спектральных коэффициентов, определяемые по дискретной реализации, содержащей заданное количество отсчетов, а также параметры моделей авторегрессии.

*Ключевые слова:*обнаружение, распознавание. беспилотный летательный аппарат, акустический шум.

Ил. 1. Библиогр.: 32 назв.

УДК 629.7.022

Особливості виявлення та розпізнавання малих безпілотних літальних апаратів / *В.М. Карташов, В.М. Олейніков, С.О. Шейко, С.І. Бабкін, І.В. Коритцев., О.В. Зубков* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 235 – 243.

Проведено огляд та аналіз методів виявлення та розпізнавання безпілотних літальних апаратів (БПЛА).Розглянуті канали для виявлення БПЛА – акустичний, оптичний, інфрачервоний, радіолокаційний, канал радіорозвідки. Порівняні та оцінені переваги і недоліки каналів, які використовуються. У випадку малих БПЛА є ряд суттєвих складнощів та обмежень. Одним з напрямків у виявленні БПЛА є акустичні спостереження. Шум, що створюється силовою установкою БПЛА та повітряним гвинтом, є суттєвим демаскуючою ознакою. Створення та удосконалення методів виявлення , пеленгації і розпізнавання малих БПЛА шляхом прийому та обробки їх акустичних сигналів є актуальне завдання. При застосуванні такого методу виявлення БПЛА використовуються частотні спектри, спектрограми, нормовані автокореляційні функції і фазові портрети. Інформаційними ознаками звукового обліку БПЛА можуть слугувати оцінки спектральних коефіцієнтів, які визначаються за дискретною реалізацією, що містить задану кількість відліків, а також параметри моделей авторегресії.

Ключові слова: виявлення, розпізнавання, безпілотний літальний апарат, акустичний шум.

Іл. 1. Бібліогр.: 32 назв.

UDC 629.7.02

Peculiarities of small unmanned aerial vehicles detection and recognition / *V.M. Kartashov, V.N. Oleynikov, S.A. Sheyko, S.I. Babkin, I.V. Koryttsev, O.V. Zubkov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 235 – 243.

Review and analysis of methods for detection and recognition of unmanned aerial vehicles (UAVs) are conducted. The channels for the detection of UAVs - acoustic, optical, radar, infrared, radio channel are considered. The advantages and disadvantages of the channels used are compared and appreciated. In the case of small UAVs, there are a number of significant difficulties and limitations. One of the directions in the UAVs detection is acoustic observation. The noise generated by the UAV propulsion system and the air propeller is a significant demasking feature. Creating and improving methods for detecting, guiding and recognizing small UAVs by the reception and processing their sound signals is an urgent task. When using such a method of detecting UAVs, frequency spectra, spectrograms, normalized autocorrelation functions, and phase portraits of acoustic signals are used. Estimates of spectral coefficients, determined by a discrete realization containing a predetermined number of samples, as well as parameters of autoregression models can serve as information signs of the UAVs sound image.

Keywords: detection, recognition, unmanned aerial vehicles, acoustic noise.

1 fig. Ref.: 32 items.