РЕФЕРАТЫ РЕФЕРАТИ ABSTRACTS

ПЕРСПЕКТИВНІ МЕТОДИ ТА СИСТЕМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

ПЕРСПЕКТИВНЫЕ МЕТОДЫ И СИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

PERSPECTIVE METHODS AND SYSTEMS OF CRYPTOGRAPHIC INFORMATION PROTECTION

УДК 004.056.55

Обґрунтування перспективного постквантового національного стандарту електронного підпису на основі решіток / *А.М. Олексійчук, В.А. Кулібаба, М.В. Єсіна, С.О. Кандій, Є.В. Острянська, І.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 5 – 14.

Важливою особливістю постквантового періоду у криптографії є суттєва невизначеність щодо вихідних даних для криптоаналізу та протидії в частині можливостей квантових комп'ютерів, їх математичного та програмного забезпечень, а також застосування квантового криптоаналізу до існуючих криптоперетворень та криптопротоколів. В якості основних методів обрано математичні методи електронного підпису (ЕП), що пройшли суттєвий аналіз та обґрунтування в процесі широких досліджень криптологами та математиками на найвищому рівні. Проаналізовано існуючі алгоритми електронного підпису на основі решіток 2-го етапу конкурсу NIST. Розглядається можливість використання постквантового механізму електронного підпису на основі алгебраїчних решіток у якості постквантового національного стандарту електронного підпису. У якості такого алгоритму електронного підпису пропонується використовувати постквантовий алгоритм Crystals-Dilithium. Розглядається даний алгоритм та обґрунтовується можливість його застосування, параметри алгоритму та правила їх побудування. Аналізуються відмінності та особливості безпечної реалізації алгоритму в порівнянні з 1-м етапом. Проводиться аналіз та робиться висновок, що алгоритм Crystals-Dilithium може бути взятий за основу, одним із кандидатів для розробки національного стандарту електронного підпису з використанням стандартизованих в Україні криптографічних алгоритмів, таких як функція гешування, що описується у ДСТУ 7564:2014. На погляд авторів, національний стандарт України постквантового періоду повинен включати в себе мінімум три алгоритми, що базуються на різних видах математичних перетворень, що визнані світовим криптографічним співтовариством як такі, що можуть забезпечувати необхідний рівень стійкості в умовах квантового криптоаналізу.

Ключові слова: електронний підпис; постквантовий стандарт; алгебраїчні решітки.

Табл. 1. Іл. 3. Бібліогр.: 27 назв.

УДК 004.056.55

Обоснование перспективного постквантового национального стандарта электронной подписи на основе решеток / *А.Н. Алексейчук, В.А. Кулибаба, М.В. Есина, С.А. Кандий, Е.В. Острянская, И.Д. Горбенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 5 – 14.

Важной особенностью постквантового периода в криптографии является существенная неопределенность относительно исходных данных для криптоанализа и противодействия в части возможностей квантовых компьютеров, их математического и программного обеспечения, а также применение квантового криптоанализа к существующим криптопреобразованиям и криптопротоколам. В качестве основных методов выбраны математические методы электронной подписи (ЭП), прошедшие существенный анализ и обоснование в процессе широких исследований криптологами и математиками на высшем уровне. Анализируются существующие алгоритмы электронной подписи на основе решеток 2-го этапа конкурса NIST. Рассматривается возможность использовать постквантовый механизм электронной подписи на основе алгебраических решеток в качестве постквантового национального стандарта электронной подписи. В качестве такого алгоритма электронной подписи предлагается использовать постквантовый алгоритм Crystals-Dilithium. Рассматривается данный алгоритм и обосновывается возможность его применения. Рассматриваются параметры алгоритма и правила их построения. Проводится анализ различий и особенностей безопасной реализации алгоритма по сравнению с 1-м этапом. Проводится анализ и делается вывод, что алгоритм Crystals-Dilithium может быть взят за основу, одним из кандидатов для разработки национального стандарта электронной подписи с использованием стандартизированных в Украине криптографических алгоритмов, таких как функция хеширования, что описывается в ДСТУ 7564: 2014. На взгляд авторов, национальный стандарт Украины постквантового периода должен включать в себя минимум три алгоритма, основанные на различных видах математических преобразований, которые признаны мировым криптографическим сообществом как такие, которые могут обеспечивать необходимый уровень устойчивости в условиях квантового криптоанализа.

Ключевые слова: электронная подпись; постквантовый стандарт; алгебраические решетки.

Табл. 1. Ил. 3. Библиогр.: 27 назв.

UDC 004.056.55

Substantiation of promising post-quantum national lattice-based electronic signature standard / *A.M. Oleksiychuk, V.A. Kulibaba, M.V. Yesina, S.O. Kandy, E.V. Ostryanska, I.D. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 5 – 14.

An important feature of the post-quantum period in cryptography is the significant uncertainty about the input data for cryptanalysis and counteracting the capabilities of quantum computers, their mathematical and software, and the application of quantum cryptanalysis to existing cryptoprotocols and cryptotransformations. Mathematical electronic signature (ES) methods have been selected as the main methods in the work, which have undergone significant analysis and substantiation in the process of extensive research by cryptologists and mathematicians at the highest level. The article analyzes the existing electronic signature algorithms based on the lattices of stage 2 of the NIST competition. The possibility of using the post-quantum electronic signature mechanism based on algebraic lattices as the post-quantum national electronic signature standard is considered. It is proposed to use the post-quantum Crystals-Dilithium algorithm as such electronic signature algorithm. The article considers this algorithm and substantiates the possibility of its application. The algorithm parameters and rules for their construction are considered. The differences and features of safe implementation of the algorithm in comparison with stage 1 are analyzed. The analysis is conducted and it is concluded that the Crystals-Dilithium algorithm can be taken as one of the candidates for the development of a national electronic signature standard using cryptographic algorithms, standardized in Ukraine, such as the hashing function described in DSTU 7564:2014. According to the authors of the article, the post-quantum period national standard of Ukraine should include at least 3 algorithms based on different types of mathematical transformations, which are recognized by the world cryptographic community as those that can provide the necessary level of stability in the conditions of quantum cryptanalysis.

Key words: electronic signature; post-quantum standard; algebraic lattices.

1 tab. 3 fig. Ref: 27 items.

УДК 004.056.55

Оптимізація алгоритму множення поліномів для NTRU-подібних алгоритмів / *О.Г. Качко, Ю.І. Горбенко, В.А. Пономар, М.В. Єсіна, С.О. Кандій* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 15 – 24.

Наразі актуальною стала проблема криптографічного захисту від класичних та потенційних криптоаналітичних атак з використанням квантового комп'ютера та квантової математики. Розуміючи цю проблему, технологічно розвинені держави направляють суттєві зусилля на аналіз криптографічної стійкості існуючих стандартів криптографічного захисту інформації у постквантовий період та ведуть пошук щодо створення постквантових стандартів асиметричної криптографії. Практичне вирішення цієї проблеми здійснюється на світовому рівні в процесі проведення NIST США міжнародного конкурсу. Як показують попередні дослідження, надійною математичною основою, на якій можуть бути створені постквантові АСШ та ПІК, нині вважаються алгебраїчні решітки. NTRU-подібні алгоритми – клас алгоритмів криптоперетворень, які в основному задовольняють вимогам постквантової криптографії. В NTRU-подібних алгоритмах асиметричних криптоперетворень основними складовими є алгоритми генерування ключів та виконання прямих та зворотних криптографічних перетворень. Ряд авторів сьогодні зосереджені на оптимізації множення поліномів для цих алгоритмів за критерієм часової складності. Особливою вимогою до них є незалежність часу виконання операції множення від самих поліномів, що робить неможливим здійснювати атаку сторонніми каналами. В роботі пропонується використання алгоритмів NTT та Тоома – Кука. Запропоновано нове рішення цієї проблеми, яке дозволило отримати прискорення практично в два рази при забезпеченні константного часу множення поліномів. Мета статі – оптимізація алгоритму множення поліномів за критерієм часової складності, який використовується для генерування ключів та виконання прямих та зворотних криптографічних перетворень АСШ та ПІК на алгебраїчних решітках.

Ключові слова: NTRU, NTRUPrime; множення поліномів; оптимізація; константний час.

Табл. 3. Бібліогр.: 18 назв.

УДК 004.056.55

Оптимизация алгоритма умножения полиномов для NTRU-подобных алгоритмов / *Е.Г. Качко, Ю.И. Горбенко, В.А. Пономарь, М.В. Есина, С.А. Кандий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 15 – 24.

Сегодня актуальной стала проблема криптографической защиты от классических и потенциальных криптоаналитических атак с использованием квантового компьютера и квантовой математики. Понимая эту проблему, технологически развитые государства направляют существенные усилия на анализ криптографической стойкости существующих стандартов криптографической защиты информации в постквантовый период и ведут исследования по созданию постквантовых стандартов асимметричной криптографии. Практическое решение этой проблемы осуществляется на мировом уровне в процессе проведения NIST США международного конкурса. Как показывают предварительные исследования, надежной математической основой, на которой могут быть созданы постквантовые АСШ и ПИК, сейчас считаются алгебраические решетки. NTRU-подобные алгоритмы – класс алгоритмов криптопреобразования, которые в основном удовлетворяют требованиям постквантовой криптографии. В NTRU-подобных алгоритмах асимметричных криптопреобразований основными составляющими являются алгоритмы генерации ключей и выполнения прямых и обратных криптографических преобра-

зований. Ряд авторов сосредоточены на оптимизации умножения полиномов для этих алгоритмов по критерию временной сложности. Особым требованием к ним является независимость времени выполнения операции умножения от самых полиномов, что делает невозможным осуществлять атаку сторонними каналами. В работе предлагается использовать алгоритмы NTT и Тоома – Кука. Предложено новое решение этой проблемы, которое позволило получить ускорение практически в два раза при обеспечении константного времени умножения полиномов. Цель статьи – оптимизация алгоритма умножения полиномов по критерию временной сложности, который используется для генерирования ключей и выполнения прямых и обратных криптографических преобразований АСШ и ПИК на алгебраических решетках.

Ключевые слова: NTRU, NTRUPrime; умножение полиномов; оптимизация; константное время.

Табл. 3. Библиогр.: 18 назв.

UDC 004.056.55

Optimization of polynomial multiplication algorithm for NTRU-like algorithms / *O.G. Kachko, Yu.I. Gorbenko, V.A. Ponomar, M.V. Yesina, S.O. Kandiy* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 15 – 24.

The problem of cryptographic protection against classical and potential crypto-analytic attacks with the use of quantum computer and quantum mathematics has become an urgent issue. Understanding this problem, technologically advanced states are making significant efforts to analyze the cryptographic stability of existing standards for cryptographic information security in the post-quantum period and are seeking to establish post-quantum standards for asymmetric cryptography. A practical solution to this problem is being pursued globally during the NIST USA international competition. As previous studies have shown, algebraic lattices are now considered to be a reliable mathematical basis on which post-quantum asymmetric encryptions and PIK can be created. NTRU-like algorithms are a class of crypto-transformations algorithms that satisfy basically the requirements of post-quantum cryptography. Algorithms for key generation direct and reverse cryptographic transformations are the basic components in NTRU-like algorithms for asymmetric crypto-transformations. A number of authors today focus on optimizing polynomial multiplication for these algorithms by the criterion of time complexity. A special requirement for them is the independence of the time of the multiplication operation from the polynomials themselves, which makes it impossible to attack by side channels. This paper proposes the use of the NTT and Toom-Kuk algorithms. It proposes a new solution to this problematic issue, which made it possible to obtain an acceleration of almost 2 times while providing a constant polynomial multiplication time. The objective of this article is to optimize the polynomial multiplication algorithm by the time complexity criterion, used to generate keys and perform direct and reverse cryptographic transformations of asymmetric encryptions and PIK on algebraic lattices.

Key words: NTRU, NTRUPrime; multiplication of polynomials; optimization; constant time.

3 tab. Ref.: 18 items

УДК 621.391:519.2

Рандомізована симетрична криптосистема Мак-Еліса на основі узагальнених кодів Ріда-Соломона / *О.С. Шевчук* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 25 – 36.

Однією з актуальних проблем сучасної криптографії є створення практичних пост квантових криптосистем, стійкість яких базується на складності розв'язання єдиної обчислювально складної задачі, аналогічно тому як стійкість криптосистеми RSA базується на складності факторизації цілих чисел. Перспективний клас таких криптосистем утворюють кодові криптосистеми, найпершою асиметричною з яких є криптосистема Мак-Еліса. Дану роботу присвячено створенню та дослідженню симетричної версії криптосистеми Мак-Еліса, що будується на основі узагальнених кодів Ріда-Соломона (УРС). Вибір цих кодів зумовлено тим, що вони існують для всіх природних значень параметрів (довжини та вимірності коду) і є максимально дистанційно роздільними, що дозволяє в широких межах змінювати характеристики відповідних криптосистем. Крім того, для зазначених кодів відомі дуже швидкі алгоритми декодування (до половини кодової відстані та, навіть, за її межами). Нарешті, асиметричні криптосистеми, побудовані на основі кодів УРС, є нестійкими, оскільки для них існують ефективні алгоритми відновлення секретних ключів за відкритими.

Запропоновано симетричну кодову криптосистему, що є більш ефективнивною (за довжиною секретного ключа при заданих вимогах до стійкості) в порівнянні з криптосистемою LPN-C. Отримано оцінку стійкості запропонованої криптосистеми відносно атаки з підібраним відкритим текстом та запропоновано алгоритм вибору параметрів для побудови цієї криптосистеми. Проведено порівняння запропонованої криптосистеми з криптосистемою LPN-C за довжиною ключа при заданій нижній межі стійкості відносно розглянутої атаки.

Ключові слова: постквантова криптографія; кодова криптосистема; криптосистема Мак-Еліса; узагальнений код Ріда-Соломона; криптосистема LPN-C; система лінійних рівнянь зі спотвореними правими частинами.

Табл. 4. Бібліогр.: 18 назв.

УДК 621.391:519.2

Рандомизированная симметричная криптосистема Мак-Елиса на основе обобщенных кодов Рида-Соломона / *О.С. Шевчук* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 25 – 36.

Одной из актуальных проблем современной криптографии является создание практичных постквантовых криптосистем, стойкость которых базируется на сложности решения одной вычислительно сложной задачи, аналогично тому как стойкость криптосистемы RSA базируется на сложности факторизации целых чисел. Пер-

спективный класс таких криптосистем образуют кодовые криптосистемы, первой асимметричной из которых есть криптосистема Мак-Элиса. Работа посвящена созданию и исследованию симметричной версии криптосистемы Мак-Элиса, которая строится на основе обобщенных кодов Рида-Соломона. Выбор этих кодов обусловлен тем, что они существуют для всех естественных значений параметров (длины и размерности кода) и являются максимально дистанционно разделимыми, что позволяет в широких пределах изменять характеристики соответствующих криптосистем. Кроме того, для указанных кодов известны очень быстрые алгоритмы декодирования. Наконец, асимметричные криптосистемы, построенные на основе обобщенных кодов Рида-Соломона, являются нестойкими, поскольку для них существуют эффективные алгоритмы восстановления секретных ключей по открытым.

Предложена симметричная кодовая криптосистема, более эффективная (с точки зрения длины секретного ключа при заданных требованиях к стойкости) по сравнению с криптосистемой LPN-C. Получена оценка стойкости предложенной криптосистемы относительно атаки с подобранным открытым текстом и предложен алгоритм выбора параметров для построения этой криптосистемы. Проведено сравнение предложенной криптосистемы с криптосистемой LPN-C по длине ключа при заданной нижней границе стойкости относительно рассматриваемой атаки.

Ключевые слова: постквантовая криптография; кодовая криптосистема; криптосистема Мак-Элиса; обобщенный код Рида-Соломона; криптосистема LPN-C; система линейных уравнений с искаженными правыми частями.

Табл. 4. Библиогр.: 18 назв.

UDC 621.391:519.2

Randomized symmetric McEliece cryptosystem based on generalized Reed-Solomon codes / *O.S. Shevchuk* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 25 – 36.

One of the actual problems of modern cryptography is the design of practical post-quantum cryptosystems whose security is based on the complexity of solving one computationally challenging problem, in the same way as the security of the RSA cryptosystem is based on the complexity of integer factorization. A promising class of such cryptosystems is formed by code-based cryptosystems the first asymmetric of which is the McEliece cryptosystem. The purpose of this work is to design and research a symmetric version of the McEliece cryptosystem based on generalized Reed-Solomon codes. These codes were chosen because they exist for all natural values of the parameters (the length and dimension of the code) and they are maximal distance separable allowing a wide range to change the characteristics of the relevant cryptosystems. In addition, very fast decoding algorithms are known for these codes. Asymmetric cryptosystems based on the generalized Reed-Solomon codes are not secure because for them there are efficient algorithms for recovering private keys from public keys.

A symmetric code cryptosystem is proposed that is more efficient (in terms of the length of the secret key for given security requirements) compared to the LPN-C cryptosystem. An estimate of the security of the proposed cryptosystem relative to an attack with the chosen plaintext is obtained and an algorithm for selecting parameters for constructing this cryptosystem is proposed. The proposed cryptosystem is compared with the LPN-C cryptosystem along the key length for a given lower limit of security to the attack in question.

Key words: post-quantum cryptography; code-based cryptosystem; McEliece cryptosystem; generalized Reed-Solomon code; LPN-C cryptosystem; system of noised linear equations.

4 tab. Ref.: 18 items.

УДК 621.391.15:519.7

Алгоритми і оцінки складності обчислень 3- і 5-ізогеній суперсингулярних кривих Едвардса / *А.В. Бессалов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 37 – 50.

Дано аналіз властивостей і умов існування 3- і 5-ізогеній повних і квадратичних суперсингулярних кривих Едвардса над полями непарної характеристики $p>3$. Для задачі інкапсуляції ключів на основі алгоритму постквантової криптографії SIDH пропонується використовувати ізогенії мінімального непарного ступеня 3 і 5, що дозволяє обійти проблему особливих точок 2-го і 4-го порядків, які характерні для 2-ізогеній класів нециклічних кривих Едвардса. Дано огляд основних властивостей класів кривих Едвардса. Проаналізовано властивості ізогеній непарних степенів кривих Едвардса з одним параметром d в афінних координатах, приведено приклади їх обчислення. Відомі формули 3- і 5-ізогеній в афінних координатах трансформовані в проективні координати. Для зростання швидкості обчислення ізогеній застосовується лише x-координата афінної точки кривої. Отримано формули для координат і оцінок складності обчислень 3-ізогеній у класах повних і квадратичних кривих Едвардса у проективних координатах. Для ядра 5-го порядку параметр d кривої вдалось виразити через x-координати точок ядра, що дозволило отримати не залежні від d формули для координат 5-ізогеній. Проведено порівняльний аналіз складності чотирьох алгоритмів обчислення координат 5-ізогеній. Побудовані алгоритми обчислення 3- і 5-ізогеній в класах повних і квадратичних суперсінгулярних кривих Едвардса. Розглянуто деякі вимоги до параметрів криптосистеми.

Ключові слова: крива в узагальненої формі Едвардса; повна крива Едвардса; скручена крива Едвардса; квадратична крива Едвардса; порядок кривої; порядок точки; ізоморфізм; ізогенія; степінь ізогенії; ядро ізогенії; квадратичний лишок; квадратичний не лишок.

Бібліогр.: 11 назв.

УДК 621.391.15:519.7

Алгоритмы и оценки сложности вычислений 3- и 5-изогений суперсингулярных кривых Эдвардса / *А.В. Бессалов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 37 – 50.

Дан анализ свойств и условий существования 3- и 5-изогений полных и квадратичных суперсингулярных кривых Эдвардса над полями нечетной характеристики $p>3$. Для задачи инкапсуляции ключей на основе алгоритма постквантовой криптографии SIDH предложено использовать изогении минимальных нечетных степеней 3 и 5, что позволяет обойти проблему особых точек 2-го и 4-го порядков, характерную для 2-изогений классов нециклических кривых Эдвардса. Приведен обзор основных свойств классов кривых Эдвардса. Дан анализ свойств изогений нечетных степеней кривых Эдвардса с одним параметром *d* в аффинных координатах, приведены примеры их вычисления. Известные формулы 3- и 5-изогений в аффинных координатах трансформированы в проективные координаты. Для увеличения скорости вычисления изогений используется лишь *x*-координата аффинной точки кривой. Получены формулы для координат и оценок сложности вычислений 3-изогений в классах полных и квадратичных кривых Эдвардса в проективных координатах. Для ядра 5-го порядка параметр *d* кривой удалось выразить через *x*-координаты точек ядра, что позволило получить не зависящие от *d* формулы для координат 5-изогений. Проведен сравнительный анализ сложности четырех алгоритмов вычисления координат 5-изогений. Построены алгоритмы вычисления 3- и 5-изогений в классах полных и квадратичных суперсингулярных кривых Эдвардса. Рассмотрены некоторые требования к параметрам криптосистемы.

Ключевые слова: кривая в обобщенной форме Эдвардса; полная кривая Эдвардса; скрученная кривая Эдвардса; квадратичная кривая Эдвардса; порядок кривой; порядок точки; изоморфизм; изогения; степень изогении; ядро изогении; квадратичный вычет; квадратичный невычет.

Библиогр.: 11 назв.

UDC 621.391.15:519.7

Algorithms and complexity evaluation of 3- and 5-isogeny calculation of super singular Edwards curves / *A.V. Bessalov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 37 – 50.

The properties and existence conditions of 3- and 5-isogenies for complete and quadratic super singular Edwards curves over the fields of p>3 odd characteristic are analyzed. It is proposed to use the minimum odd degrees 3- and 5—isogenies for the task of keys encapsulation based on the SIDH algorithm of post quantum cryptography, which allows bypassing the problem of special points of the 2nd and 4th orders. These points always arise on 2-isogenies for the classes of noncyclic Edwards curves. A review of the main properties of the Edwards curve classes is given. An analysis of the properties of isogenies of odd degrees of Edwards curves with one parameter *d* in affine coordinates and examples of their calculation are given The known formulas of 3- and 5-isogeny in affine coordinates are transformed into projective coordinates. To increase the rate of isogeny calculation, only the *x*-coordinate of the affine point of the curve is used. Formulas for the coordinates and complexity evaluation for 3-isogeny calculations in the classes of complete and quadratic Edwards curves in projective coordinates are obtained. The parameter *d* of the curve was expressed in terms of the *x*-coordinates of the points of the nucleus for the 5th order nucleus, which allowed us to obtain formulas independent of *d* for the coordinates of 5-isogenies. A comparative analysis of the complexity of 4 algorithms for calculating the coordinates of 5 isogenies is carried out. Algorithms for computing 3- and 5-isogenies in the classes of complete and quadratic super singular Edwards curves are constructed. Some requirements for the parameters of the cryptosystem are considered.

Key words: Edwards curve in generalized form; complete Edwards curve; twisted Edwards curve; quadratic Edwards curve; curves order; points order; isomorphism; isogeny; isogeny kernel; square; non square.

Ref.: 11 items.

УДК 621.3.06

Дослідження продуктивності малоресурсного блокового шифру «Кипарис» на різних платформах / *М.Ю. Родінко, Р.В. Олійников* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 51 – 57.

Блоковий шифр «Кипарис» є малоресурсним алгоритмом, що представляє собою мережу Фейстеля з ARX-перетворенням у якості циклової функції. Блоковий шифр «Кипарис» підтримує довжину блока та ключа 256 та 512 біт. У статті досліджено продуктивність малоресурсних блокових шифрів «Кипарис-256» і «Кипарис-512» та порівняно з продуктивністю інших відомих блокових шифрів таких, як AES-256, SPECK-64/128, SPECK-128/128, SPARX-128/128, ДСТУ ГОСТ 28147: 2009. Продуктивність оцінювалась на платформах Windows, Linux та Android шляхом вимірювання швидкості зашифрування в режимі простої заміни, у Мбіт/с. Блоковий шифр «Кипарис» продемонстрував високу продуктивність на всіх досліджуваних програмно-апаратних платформах. На платформі Windows 10 з 32-бітовою архітектурою найкращий результат показав шифр «Кипарис-256» (майже 3,5 Гбіт/с). На платформі Windows 10 з 64-бітовою архітектурою найкращий результат показав шифр «Кипарис-512» (майже 5 Гбіт/с). На платформі Linux з 64-бітовою архітектурою блоковий шифр «Кипарис-256» показав надвисокий результат зі швидкодії (понад 8 Гбіт/с). На платформі Android найкращими також були блокові шифри «Кипарис-256» та «Кипарис-512» (1,3 Гбіт/с та 1 Гбіт/с відповідно). З точки зору продуктивності та зручності реалізації на різних програмно-апаратних платформах алгоритм «Кипарис» має ряд переваг: два варіанти шифру («Кипарис-256» та «Кипарис-512») орієнтовані на 32-бітову та 64-бітову архітектури відповідно; висока швидкодія та компактна реалізація перетворень незалежно від платформи, що використовується (сервер, робоча станція або мобільний пристрій); мінімальний необхідний об’єм пам’яті для швидкодію-

чої реалізації, відсутність таблиць передобчислень; можливість організації ефективних захищених високошвидкісних каналів зв'язку між мобільними системами та серверами, у тому числі тими, що використовують апаратні прискорювачі.

Ключові слова: блоковий шифр; малоресурсна криптографія; швидкість зашифрування; ARX-перетворення; мережа Фейстеля.

Табл. 5. Іл. 2. Бібліогр.: 18 назв.

УДК 621.3.06

Исследование производительности малоресурсного блочного шифра «Кипарис» на разных платформах / *М.Ю. Родинко, Р.В. Олейников* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 51 – 57.

Блочный шифр «Кипарис» является малоресурсным алгоритмом, который представляет собой сеть Фейстеля с ARX-преобразованием в качестве цикловой функции. Блочный шифр «Кипарис» поддерживает длину блока и ключа 256 и 512 бит. В статье исследуется производительность малоресурсных блочных шифров «Кипарис-256» и «Кипарис-512» и сравнивается с производительностью других известных блочних шифров, таких как AES-256, SPECK-64/128, SPECK-128/128, SPARX-128/128, ДСТУ ГОСТ 28147: 2009. Производительность оценивалась на платформах Windows, Linux и Android путем измерения скорости зашифрования в режиме простой замены, в Мбит/сек. Блочный шифр «Кипарис» продемонстрировал высокую производительность на всех исследуемых программно-аппаратних платформах. На платформе Windows 10 с 32-битовой архитектурой лучший результат показал шифр «Кипарис-256» (почти 3,5 Гбит/с). На платформе Windows 10 с 64-битовой архитектурой лучший результат показал шифр «Кипарис-512» (почти 5 Гбит/с). На платформе Linux с 64-битовой архитектурой блочный шифр «Кипарис-256» показал очень высокий результат по скорости (более 8 Гбит/с). На платформе Android лучшими также были блочные шифры «Кипарис-256» и «Кипарис-512» (1,3 и 1 Гбит/с соответственно). С точки зрения производительности и удобства реализации на различных программно-аппаратных платформах алгоритм «Кипарис» имеет ряд преимуществ: два варианта шифра («Кипарис-256» и «Кипарис-512») ориентированы на 32-битную и 64-битную архитектуры соответственно; высокое быстродействие и компактная реализация преобразований независимо от используемой платформы (сервер, рабочая станция или мобильное устройство); минимальный необходимый объем памяти для быстродействующей реализации, отсутствие таблиц предвычислений; возможность организации эффективных защищенных высокоскоростных каналов связи между мобильными системами и серверами, в том числе теми, которые используют аппаратные ускорители.

Ключевые слова: блочный шифр; малоресурсная криптография; скорость зашифрования; ARX-преобразование; сеть Фейстеля.

Табл. 5. Ил. 2. Библиогр.: 18 назв.

UDC 621.3.06

The research of performance of the "Cypress" lightweight block cipher on different platforms / *M.Yu. Rodinko, R.V. Oliynykov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 51 – 57.

The Cypress block cipher is a lightweight algorithm based on the Feistel network with ARX-transformation as a round function. The Cypress block cipher supports 256-bit and 512-bit block and key length. The paper presents results of researches on the performance of lightweight block ciphers Cypress-256 and Cypress-512 and it gives comparison of performance of other well-known block ciphers such as AES-256, SPECK-64/128, SPECK-128/128, SPARX-128/128, DSTU GOST 28147: 2009. Performance was evaluated on Windows, Linux and Android platforms by measuring the encryption speed in the Electronic Code Book mode, in Mbps. The Cypress block cipher has demonstrated high performance on all selected platforms. Cypress-256 showed the best result (almost 3.5 Gbps) on the Windows 10 platform with 32-bit architecture. Cypress-512 also showed the best result (almost 5 Gbps) on the Windows 10 platform with 64-bit architecture. On the Linux platform with a 64-bit architecture, Cypress-256 showed a very high speed result (more than 8 Gbps). Cypress-256 and Cypress-512 block ciphers were also the best (1.3 Gbps and 1 Gbps, respectively) on the Android platform. In terms of performance and simplicity of implementation on different software and hardware platforms, Cypress algorithm has several advantages. Two variants of cipher (Cypress-256 and Cypress-512) are oriented on 32-bit and 64-bit architectures, respectively; high speed and compact implementation of transformations regardless of the platform used (server, workstation or mobile device). Minimum amount of memory is required for high-speed implementation, there is no need in pre-computed tables; there is an ability to organize efficient secure high-speed communication channels between mobile systems and servers, including those using hardware accelerators.

Keywords: block cipher; lightweight cryptography; encryption speed; ARX-transformation; Feistel network.

5 tab. 2 fig. Ref.: 18 items

УДК 004.056.5

Тестування кодових генераторів псевдовипадкових чисел для пост-квантового застосування / *О.О. Кузнецов, А.С. Кіян, А.І. Пушкарьов, Т.Ю. Кузнецова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 58 – 67.

Останні досягнення в області квантових обчислень, заснованих на нових принципах і явищах квантової механіки, показують, що квантовий криптоаналіз сучасних криптографічних алгоритмів може стати реальним вже в найближчі роки. Наприклад, за прогнозами національного інституту стандартів і технологій (NIST) США

в найближче десятиліття буде доступний квантовий криптоаналіз більшості використовуваних сьогодні несиметричних криптосистем. З цієї причини NIST оголосив про проведення конкурсу постквантових (тобто стійких до квантового криптоаналізу) криптографічних алгоритмів направленого шифрування, електронного підпису та інкапсуляції ключів. У найближчі роки очікується стандартизація обраних алгоритмів і їх якнайшвидше впровадження. Очевидно, що подальшої ревізії будуть піддаватися і інші криптоалгоритми, наприклад генератори псевдовипадкових чисел, засновані на вирішенні теоретико-складних завдань (дискретного логарифмування, факторизації та ін.). Ці генератори також підлягають заміні на надійні та безпечні алгоритми, придатні до використання навіть в умовах можливого застосування квантового криптоаналізу (тобто у постквантовий період). Дана стаття присвячена дослідженню доказово стійких генераторів, безпека яких ґрунтується на складності рішення задачі синдромного декодування. Подібна схема дозволяє генераторам зберігати стійкість як до класичного криптоаналізу, так і до криптоаналізу із застосуванням квантових обчислень. Представлені особливості функціонування класичного представника кодових генераторів, запропонованого Фішером і Штерном, вивчені її переваги і недоліки. Запропоновано схему нового генератору на основі кодів, в якій, за рахунок використання лінійних рекурентних регістрів зсуву, вдається формувати послідовності максимального періоду. Наведено результати евристичного тестування розглянутих генераторів, досліджено можливості їх застосування в постквантовий період.

Ключові слова: постквантова криптографія; доказово стійкий генератор; кодова криптографія; синдромне декодування.

Табл. 1. Іл. 9. Бібліогр.: 18 назв.

УДК 004.056.5

Тестирование кодовых генераторов псевдослучайных чисел для постквантового применения / *А.А. Кузнецов, А.С. Киян, А.И. Пушкарев, Т.Ю. Кузнецова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 58 – 67.

Последние достижения в области квантовых вычислений, основанных на новых принципах и явлениях квантовой механики, показывают, что квантовый криптоанализ современных криптографических алгоритмов может стать реальным уже в ближайшие годы. Например, по прогнозам национального института стандартов и технологий (NIST) США в ближайшее десятилетие будет доступен квантовый криптоанализ большинства используемых сегодня несимметричных криптосистем. По этой причине NIST объявил о проведении конкурса постквантовых (т.е. устойчивых к квантовому криптоанализу) криптографических алгоритмов направленного шифрования, электронной подписи и инкапсуляции ключей. В ближайшие годы ожидается стандартизация выбранных алгоритмов и их скорейшее внедрение. Очевидно, что дальнейшей ревизии будут подвергаться и другие криптоалгоритмы, например генераторы псевдослучайных чисел, основанные на решении теоретико-сложностных задач (дискретного логарифмирования, факторизации и пр.). Эти генераторы также подлежат замене на надежные и безопасные алгоритмы, пригодные к использованию даже в условиях возможного применения квантового криптоанализа (т.е. в постквантовый период). Статья посвящена исследованию доказуемо стойких генераторов, безопасность которых основывается на сложности решения задачи синдромного декодирования. Подобная схема позволяет генераторам сохранять стойкость как к классическому криптоанализу, так и к криптоанализу с применением квантовых вычислений. Представлены особенности функционирования классического представителя кодовых генераторов, предложенного Фишером и Штерном, изучены ее достоинства и недостатки. Предложена схема нового генератора на основе кодов, в которой, за счет использования линейных рекуррентных регистров сдвига, удается формировать последовательности максимального периода. Приведены результаты эвристического тестирования рассмотренных генераторов, исследованы возможности их применения в постквантовый период.

Ключевые слова: постквантовая криптография; доказуемо стойкий генератор; кодовая криптография; синдромное декодирование.

Табл. 1. Ил. 9. Библиогр.: 18 назв.

UDC 004.056.5

Testing of code-based pseudorandom number generators for post-quantum application / *A.A. Kuznetsov, A.S. Kiian, A.I. Pushkar'ov, T.Yu. Kuznetsova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 58 – 67.

Recent advances in quantum computing based on new principles and phenomena of quantum mechanics show that quantum cryptanalysis of modern cryptographic algorithms can become real in the coming years. For example, according to the forecasts of the US National Institute of Standards and Technology (NIST) in the next decade, quantum cryptanalysis of most asymmetric cryptosystems used today will be available. For this reason, NIST announced a contest of post-quantum (i.e., resistant to quantum cryptanalysis) cryptographic algorithms for directional encryption, electronic signature, and key encapsulation. In the coming years, standardization of the selected algorithms and their early implementation is expected. Obviously, other cryptographic algorithms, for example, pseudorandom number generators based on solving complex theoretical problems (discrete logarithm, factorization, etc.), will also be subject to further revision. These generators must also be replaced by reliable and safe algorithms suitable for use even in the conditions of the possible application of quantum cryptanalysis (i.e., in the post-quantum period). This paper is devoted to the study of provably secure generators whose resistance is based on the complexity of solving the syndrome decoding problem. This structure allows the generators to keep the resistance to both classical cryptanalysis and cryptanalysis using quantum computing. The design features of classic code-based generator representative proposed by Fisher and

Stern are presented, and a new generator scheme is proposed to overcome the drawback of its predecessor, such as a reduced practical maximum period length, by using a linear feedback shift register. Within this paper Results of heuristic testing of the above-mentioned generators is conducted in terms of the sequence period, the speed of sequence generation, the cryptographic resistance of the generators and the possibility of their use in the post-quantum period.

Keywords: post-quantum cryptography; provable secure generator; code-based cryptography; syndrome decoding.

1 tab. 9 fig. Ref.: 18 items

УДК 004.056.5

Обчислювальні алгоритми розрахунку алгебраїчного імунітету нелінійних вузлів заміни симетричних шифрів / *К.Є. Лисицький, О.О. Кузнецов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 68 – 84.

Важливим елементом більшості сучасних симетричних шифрів є блок нелінійних замін (вузол ускладнення, блок підстановок, S-box). Це елементарний криптографічний примітив, призначений для перемішування вхідних даних і внесення нелінійності. За допомогою заміни блоків невеликого розміру іншими блоками досягається замішування та розсіювання даних, а багаторазове циклічне повторення такої процедури дозволяє добитися необхідних криптографічних властивостей шифру. До блоків підстановок висувається багато різних критеріїв (збалансованість, висока нелінійність, низька автокореляція, кореляційний імунітет, необхідні лавинні властивості та ін). Кожен критерій виражає формалізовану вимогу стійкості до певних видів криптографічного аналізу (диференціального, лінійного і т.д.), тобто при проектуванні шифрів використовують комплексний підхід, обираючи S-блоки по сукупності окремих показників. З розвитком алгебраїчного криптоаналізу з'явився новий показник ефективності вузлів замін – алгебраїчний імунітет, який розраховується як мінімальна ступінь найпростішого (в певному сенсі) алгебраїчного рівняння, що описує S-блок. Для пошуку такого рівняння використовують спеціальні методи, засновані на побудові базисів Гребнера. Якщо задати вузол замін через булеву функцію, тоді для розрахунку алгебраїчної імунності достатньо знайти функцію найменшого ступеня з простору анігіляторів. У статті розглядаються різні способи обчислення алгебраїчного імунітету, аналізується їх обчислювальна ефективність, обговорюються деталі реалізації, обґрунтовуються способи оптимізації обчислень за часовими (по числу операцій) і ємнісними (за витратами пам'яті) показниками складності. Пропонується удосконалений алгоритм розрахунку алгебраїчного імунітету, оптимізований по обчислювальних ресурсах, в тому числі за необхідними розмірами оперативної пам'яті. Наведено результати експериментальних досліджень, зокрема, результати обчислень алгебраїчного імунітету 8x8 S-блоків для деяких відомих сучасних шифрів (AES, Калина, Коник, BelT), а також результати, отримані для випадкових 8x8, 9x9 і 10x10 S-блоків.

Ключові слова: симетричний шифр; алгебраїчний імунітет; анігілюючий поліном; булева функція.

Табл. 5. Іл. 3. Бібліогр.: 26 назв.

УДК 004.056.5

Вычислительные алгоритмы расчета алгебраического иммунитета нелинейных узлов замены симметричных шифров / *К.Е. Лисицкий, А.А. Кузнецов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 68 – 84.

Важным элементом большинства современных симметричных шифров является блок нелинейных замен (узел усложнения, блок подстановок, S-box). Это элементарный криптографический примитив, предназначенный для перемешивания входных данных и внесения нелинейности. Посредством замены блоков небольшого размера другими блоками достигается замешивание и рассеивание данных, а многократное циклическое повторение такой процедуры позволяет добиться требуемых криптографических свойств шифра. К блокам подстановок выдвигается много различных критериев (сбалансированность, высокая нелинейность, низкая автокорреляция, корреляционная иммунность, требуемые лавинные свойства и др). Каждый критерий выражает формализованное требование устойчивости к определенным видам криптографического анализа (дифференциального, линейного и т.д.), т.е. при проектировании шифров используют комплексный подход, выбирая S-блоки по совокупности отдельных показателей. С развитием алгебраического криптоанализа появился новый показатель эффективности узлов замен – алгебраическая иммунность, которая рассчитывается как минимальная степень простейшего (в некотором смысле) алгебраического уравнения, описывающего S-блок. Для поиска такого уравнения используют специальные методы, основанные на построении базисов Гребнера. Если задать узел замен через булеву функцию, тогда для расчета алгебраической иммунности достаточно найти функцию наименьшей степени из пространства аннигиляторов. В статье рассматриваются различные способы вычисления алгебраической иммунности, анализируется их вычислительная эффективность, обсуждаются детали реализации, обосновываются способы оптимизации вычислений по временным (по числу операций) и емкостным (по затратам памяти) показателям сложности. Предлагается усовершенствованный алгоритм расчета алгебраической иммунности, оптимизированный по вычислительным ресурсам, в том числе, по необходимым размерам оперативной памяти. Приводятся результаты экспериментальных исследований, в частности результаты вычислений алгебраического иммунитета 8x8 S-блоков для некоторых известных современных шифров (AES, Калина, Кузнечик, BelT), а также результаты, полученные для случайных 8x8, 9x9 и 10x10 S-блоков.

Ключевые слова: симметричный шифр; алгебраическая иммунность; аннигилирующий полином; булева функция.

Табл. 5. Ил. 3. Библиогр.: 26 назв.

UDC. 004.056.5

Computational algorithms for calculating the algebraic immunity of nonlinear nodes of replacing symmetric ciphers / *K. Lisitsky, O. Kuznetsov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 68 – 84.

Block of nonlinear replacements (complication node, substitution block, S-box) is an important element of most modern symmetric ciphers. This is an elementary cryptographic primitive designed to mix input data and introduce nonlinearity. By replacing small blocks with other blocks, mixing and scattering of data is achieved, and repeated cyclic repetition of such a procedure makes it possible to achieve the required cryptographic properties of the cipher. Many different criteria are put forward to substitution blocks (balance, high nonlinearity, low autocorrelation, correlation immunity, required avalanche properties, and many others). Each criterion expresses a formalized requirement of resistance to certain types of cryptographic analysis (differential, linear, etc.), i.e. when designing ciphers, they use an integrated approach, choosing S-blocks according to the totality of individual indicators. With the development of algebraic cryptanalysis, a new indicator of the effectiveness of substitution nodes has appeared – algebraic immunity, which is calculated as the minimum degree of the simplest (in a sense) algebraic equation describing the S-block. To search for such an equation, special methods are used, based on the construction of Gröbner bases. If you specify a knot of substitutions through a Boolean function, then to calculate algebraic immunity it is enough to find a function of the least degree from the annihilator space. This article discusses various methods of calculating algebraic immunity, analyzes their computational efficiency, discusses implementation details, substantiates methods for optimizing calculations in terms of time (in terms of number of operations) and capacitive (in terms of memory costs) of complexity. An advanced algorithm for calculating algebraic immunity is proposed, optimized for computing resources, including the necessary RAM sizes. The results of experimental studies are presented, in particular, the results of calculations of the algebraic immunity of 8x8 S-blocks for some well-known modern ciphers (AES, Kalina, Grasshopper, BelT), as well as the results obtained for random 8x8, 9x9 and 10x10 S-blocks.

Keywords: symmetric cipher; algebraic immunity; annihilating polynomial; Boolean function.

5 tab. 3 fig. Ref.: 26 items

МЕТОДИ ТА МЕХАНІЗМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ БЛОКЧЕЙН

МЕТОДЫ И МЕХАНИЗМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМЕ БЛОКЧЕЙН

METHODS AND MECHANISMS OF CRYPTOGRAPHIC INFORMATION PROTECTION IN THE BLOCKCHAIN SYSTEM

УДК 004.056.5

Проблеми, принципи побудови та перспективи розвитку національної системи електронного голосування в Україні / *І.Д. Горбенко, В.В. Онопрієнко, Ю.І. Горбенко, О.О. Кузнецов, К.В. Ісірова, М.Ю. Родінко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 85 – 97.

Розглядаються проблеми, принципи побудови та перспективи розвитку національної системи електронного голосування в Україні. Під електронним голосуванням розуміється спосіб здійснення волевиявлення, при якому процес голосування, підрахунку та оприлюднення результатів здійснюється за допомогою електронних засобів та систем. Більшість існуючих систем голосування побудовано за централізованими принципами і це дозволяє забезпечити певні переваги, наприклад, високу керованість системи, її надійність та автономність. Однак ієрархічним системам притаманні і суттєві недоліки, зокрема, наявність єдиного центру прийняття рішень та централізованого сховища зумовлює вразливість до кібернетичних атак на центр зберігання та прийняття рішень. Слід відзначити, що в централізованих системах можливі спотворення результатів волевиявлення через зловживання адміністративним ресурсом, і це є найбільшою загрозою сучасного демократичного інформаційного суспільства. Отже перспективним є дослідження, розробка та впровадження нових технологій електронного голосування, які б унеможливлювали втручання та викривлення результатів волевиявлення через децентралізацію із збереженням всіх системних якостей з безпеки та надійності. В статті зроблено конкретні пропозиції з обґрунтування архітектури, базової моделі та протоколів взаємодії децентралізованої системи електронного блокчейн-голосування. Запропоновано, досліджено та випробувано шляхом фізичного прототипування дворівневу архітектуру блокчейн-голосування. Її практичне впровадження підвищить довіру до інформаційних ресурсів та сервісів (що є особливо актуальним для державних установ); зменшить час та накладні витрати; унеможливить втручання централізованих установ та можливі корупційні дії; підвищить надійність збереження інформації та якість наданих послуг.

Ключові слова: електронне голосування; децентралізація; інформаційні технології; блокчейн-мережі; інформаційна та кібербезпека.

Табл. 1. Іл. 5. Бібліогр.: 17 назв.

УДК 004.056.5

Проблемы, принципы построения и перспективы развития национальной системы электронного голосования в Украине / *И.Д. Горбенко, В.В. Оноприенко, Ю.И. Горбенко, А.А. Кузнецов, К.В. Исирова, М.Ю. Родинко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 85 – 97.

Рассматриваются проблемы, принципы построения и перспективы развития национальной системы электронного голосования в Украине. Под электронным голосованием понимается способ осуществления волеизъявления, при котором процесс голосования, подсчета и обнародования результатов осуществляется с помощью электронных средств и систем. Большинство существующих систем голосования построено по централизованным принципам, и это позволяет обеспечить определенные преимущества, например, высокую управляемость системы, ее надежность и автономность. Однако иерархическим системам присущи и существенные недостатки, в частности, наличие единого центра принятия решения и централизованного хранилища приводит к уязвимости перед кибернетическими атаками на центр хранения и принятия решений. Следует отметить, что в централизованных системах возможны искажения результатов волеизъявления из-за злоупотребления административным ресурсом, и это является самой большой угрозой современного демократического информационного общества. Перспективным является исследование, разработка и внедрение новых технологий электронного голосования, которые бы делали невозможными вмешательство и искажения результатов волеизъявления через децентрализацию с сохранением всех системных качеств по безопасности и надежности. В статье представлены конкретные предложения по обоснованию архитектуры, базовой модели и протоколов взаимодействия децентрализованной системы электронного блокчейн-голосования. Предложена, исследована и проверена посредством физического прототипирования двухуровневая архитектура блокчейн-голосования. Ее практическое внедрение повысит доверие к информационным ресурсам и сервисам (что особенно актуально для государственных учреждений) уменьшит время и накладные расходы; сделает невозможными вмешательство централизованных учреждений и возможные коррупционные действия; повысит надежность хранения информации и качество предоставляемых услуг.

Ключевые слова: электронное голосование; децентрализация; информационные технологии; блокчейн-сети; информационная и кибербезопасность.

Табл. 1. Ил. 5. Библиогр.: 17 назв.

UDC 004.056.5

Problems, construction principles and development prospects of the national electronic voting system in Ukraine / *I.D. Gorbenko, V.V. Onoprienko, Yu.I. Gorbenko, A.A. Kuznetsov, K.V. Isirova, M.Yu. Rodinko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 85 – 97.

The present paper considers national electronic voting system problems in Ukraine, principles of construction and development prospects. Electronic voting refers to a way to exercise will, in which the voting, counting, and publication of the results processes are carried out by electronic means and systems. Most existing voting systems are built on centralized principles and this allows providing certain advantages, for example, high controllability of the system, its reliability, and autonomy. However, hierarchical systems also have significant drawbacks, in particular, single decision center and centralized storage leads to vulnerability to cyberattacks on them. Also it should be noted, that in centralized systems due to the abuse of administrative resources distortions of the results of expression of will are possible. This is the biggest threat to the modern democratic information society. Research, development, and implementation of new technologies of electronic voting, which would make it impossible to intervene and distort the results of the will through decentralization while maintaining all the system qualities for safety and reliability are promising. This article proposes particular proposals for architecture substantiating as well as a basic model and interaction protocols of a decentralized electronic blockchain voting system. A two-level blockchain voting architecture is proposed, researched and verified through physical prototyping. Its implementation will increase confidence in information resources and services (which is especially important for government agencies) will reduce time and overhead costs; make it impossible for centralized institutions to intervene and possible corrupt practices; will increase the reliability of information storage and the quality of services provided.

Keywords: electronic voting; decentralization; information technology; blockchain networks; information and cybersecurity.

1 tab. 5 fig. Ref.: 17 items

УДК 004.056.55

Можливості застосування механізмів повністю гомоморфного шифрування в системах електронного голосування / *І.Д. Горбенко, О.Г. Качко, Ю.І. Горбенко, М.В. Єсіна, С.О. Кандій, Є.В. Острянська, А.С. Д'яченко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 98 – 113.

Розглядається поняття гомоморфного шифрування та можливість його застосування у механізмі електронного голосування. Однією із проблемних вимог, що висунута до систем електронного голосування, є забезпечення анонімності виборців. З однієї сторони, кожен виборець повинен бути ідентифікований, а з іншої – зміст його голосу має бути невідомим. Запропоновані нині методи та механізми, що використовуються у реальних системах голосування, не забезпечують реальної анонімності. Тому як в теоретичному, так і практичному змісті актуальною та необхідною є проблема розроблення механізмів анонімного підрахунку голосів виборців з забезпеченням захищеності від їх викривлення. У роботі також проводиться узагальнений аналіз рівня безпеки перс-

пективних схем гомоморфного шифрування. Сутність гомоморфного шифрування полягає у тому, що існує деякий набір операцій, результат виконання яких над шифротекстами (з подальшим розшифруванням) співпадає з аналогічними діями над відкритими текстами. Гомоморфне шифрування дозволяє виконувати деякі обчислення над інформацією, при цьому не маючи доступу до самої інформації. Проте при спробі застосувати такі обчислення на практиці виникає ряд проблем. Основними з них є вибір методу асиметричного шифрування, що забезпечує необхідну криптографічну стійкість як від класичних, так і квантових атак, визначення можливих кандидатів асиметричних криптоперетворень при гомоморфному шифруванні, їх оцінка порівняння між собою та вибір найбільш раціональних при заданій множині загроз та обмежень. Порівнюються асиметричні схеми гомоморфного шифрування за допомогою методу аналізу ієрархій. Обґрунтовується метод асиметричного шифрування з нульовими знаннями. Мета статі – обґрунтування можливостей, умов і обмежень щодо застосування стандартизованих асиметричних криптоперетворень при створенні сучасних гомоморфних перетворень типу шифрування, коли повинна бути забезпечена анонімність електронного голосування та практична реалізація анонімного голосування на основі доведення нульових знань.

Ключові слова: асиметричні криптосистеми; гомоморфне шифрування; електронне голосування; механізм.

Табл. 6. Іл. 11. Бібліогр.: 36 назв.

УДК 004.056.55

Возможности применения механизмов полностью гомоморфного шифрования в системах электронного голосования / *И.Д. Горбенко, Е.Г. Качко, Ю.И. Горбенко, М.В. Есина, С.А. Кандий, Е.В. Острянская, А.С. Дьяченко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 98 – 113.

Рассматривается понятие гомоморфного шифрования и возможность его применения в механизме электронного голосования. Одним из проблемных требований, выдвинутых к системам электронного голосования, является обеспечение анонимности избирателей. С одной стороны, каждый избиратель должен быть идентифицирован, а с другой – содержание его голоса должно быть неизвестным. Методы и механизмы, используемые в реальных системах голосования, не обеспечивают реальной анонимности. Потому как в теоретическом, так и практическом смысле актуальной и необходимой является проблема разработки механизмов анонимного подсчета голосов избирателей с обеспечением защищенности от их искажения. В статье проводится обобщенный анализ уровня безопасности перспективных схем гомоморфного шифрования. Сущность гомоморфного шифрования заключается в том, что существует некоторый набор операций, результат выполнения которых над шифротекстами (с последующей расшифровкой) совпадает с аналогичными действиями над открытыми текстами. Гомоморфное шифрование позволяет выполнять некоторые вычисления над информацией, при этом не имея доступа к самой информации. Однако при попытке применить такие вычисления на практике возникает ряд проблем. Основными из них являются выбор метода асимметричного шифрования, что обеспечивает необходимую криптографическую стойкость как от классических, так и квантовых атак, определение возможных кандидатов асимметричных криптопреобразований при гомоморфном шифровании, их оценка сравнения между собой, и выбор наиболее рациональных при заданном множестве угроз и ограничений. Сравниваются асимметричные схемы гомоморфного шифрования с помощью метода анализа иерархий. Обосновывается метод асимметричного шифрования с нулевыми знаниями. Цель статьи – обоснование возможностей, условий и ограничений по применению стандартизированных асимметричных криптопреобразования при создании современных гомоморфных преобразований типа шифрования, когда должна быть обеспечена анонимность электронного голосования и практическая реализация анонимного голосования на основе доказательства нулевых знаний.

Ключевые слова: асимметричные криптосистемы; гомоморфное шифрование; электронное голосование; механизм.

Табл. 6. Ил. 11. Библиогр.: 36 назв.

UDC 004.056.55

Possibilities of using full homomorphic encryption mechanisms in electronic voting systems / *I.D. Gorbenko, O.G. Kachko, Yu.I. Gorbenko, M.V. Yesina, S.O. Kandy, E.V. Ostryanska, A.S. Dyachenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 98 – 113.

The paper deals with the concept of homomorphic encryption and the possibility of its use in the mechanism of electronic voting. One of the problematic requirements for electronic voting systems is voter anonymity. On the one hand, each voter must be identified, and on the other, the content of his or her vote must be unknown. Currently, the methods and mechanisms used in real voting systems do not provide real anonymity. Therefore, both theoretical and practical content is an urgent and necessary problem of developing mechanisms for anonymous counting of votes with the protection of their distortion. The paper also provides a general analysis of the security level of prospective homomorphic encryption schemes. The essence of homomorphic encryption is that there is some set of operations whose result of executing over ciphertexts (with subsequent decryption) coincides with similar actions over plaintexts. Homomorphic encryption allows you to perform some calculations on information without having access to the information itself. However, there are a number of problems when trying to apply such calculations. The main ones are the choice of the method of asymmetric encryption, which provides the necessary cryptographic stability from both classical and quantum attacks, the identification of possible candidates for asymmetric cryptotransformations in homomorphic encryption, their evaluation of comparison with each other, and, of course, the choice of the most rational for a given multiple restrictions. The asymmetric schemes of homomorphic encryption are compared using the hierarchy analysis process. The method of asymmetric encryption with zero knowledge is substantiated. The objective of this

article is to substantiate the possibilities, conditions, and constraints on the use of standardized asymmetric cryptotransformations in the creation of modern homomorphic encryption-type transformations, when anonymity of electronic voting and practical implementation of anonymous voting based on proof of zero knowledge must be guaranteed.

Key words: asymmetric cryptosystems; homomorphic encryption; electronic voting; mechanism.

6 tab. 11 fig. Ref: 36 items.

УДК 004.75

Аналіз площин атак на Blockchain системи / *П.І. Стеценко, Г.З. Халімов, Є.В. Котух* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 114 – 121.

Представлено дослідження площин атак і можливі способи проведення різних атак на децентралізовані системи на основі технології Blockchain. Розглянуто ефективність атаки відносно площини її застосування: криптографічних конструкцій технології Blockchain, розподіленої архітектури систем на основі технології Blockchain, контексту додатки Blockchain. Для кожної з цих площин виділено кілька атак, в тому числі стратегії злочинного Майнінг, узгоджена поведінка тимчасових вузлів, атаки 51 %, атаки на доменні імена (DNS), атаки «відмова в обслуговуванні», затримування досягнення консенсусу, розгалуження регістра Blockchain, відкинуті і застарілі блоки, крадіжки цифрового гаманця і атаки на конфіденційність.

Атака злочинного майнінгу дозволяє зловмисникові збільшити винагороду, навмисно зберігаючи свої блоки закритими, щоб отримати довшу версію регістра Blockchain, ніж поточна головна версія регістра. Атака 51 % відбувається, коли один зловмисник, група вузлів або майнінг-пул (об'єднання майнерів) в мережі досягає більшої частини загальної обчислювальної потужності майнінгу в системі і отримує можливість маніпулювати функціональністю Blockchain-системи. У площині DNS-атак зловмисник може потенційно ізолювати одноранговi вузли Blockchain-системи, поширювати серед нових вузлів підроблені блоки з шахрайськими транзакціями, робити недійсними транзакції. Прояви DDoS-атаки можуть різноманітними, залежно від характеру функціональності Blockchain-додатків, особливостей його мережевої архітектури та поведінки тимчасових вузлів. Розглянуто заходи протидії атакам на однорангову піринговy архітектуру.

Ключові слова: технологія Blockchain; зловмисний Майнінг; атака 51 %; DDoS-атаки і DNS-атаки.

Іл. 4. Бібліогр.: 19 назв.

УДК 004.75

Анализ плоскостей атак на Blockchain системы / *П.И. Стеценко, Г.З. Халимов, Е.В. Котух* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 114 – 121.

Представлено исследование плоскостей атак и возможные способы проведения различных атак на децентрализованные системы на основе технологии Blockchain. Рассмотрена эффективность атаки относительно плоскости ее применения: криптографических конструкций технологии Blockchain, распределенной архитектуры систем на основе технологии Blockchain, контекста приложения Blockchain. Для каждой из этих плоскостей выделено несколько атак, в том числе стратегии злоумышленного майнинга, согласованное поведение одноранговых узлов, атаки 51 %, атаки на доменные имена (DNS), атаки «отказ в обслуживании», задержка достижения консенсуса, разветвление регистра Blockchain, отброшенные и устаревшие блоки, кражи цифрового кошелька и атаки на конфиденциальность.

Атака злоумышленного майнинга позволяет злоумышленнику увеличить вознаграждение, намеренно сохраняя свои блоки закрытыми, чтобы получить более длинную версию регистра Blockchain, чем текущая главная версия регистра. Атака 51 % происходит, когда один злоумышленник, группа узлов или майнинг-пул (объединение майнеров) в сети достигает большей части общей вычислительной мощности майнинга в системе и получает возможность манипулировать функциональностью Blockchain-системы. В плоскости DNS-атак злоумышленник может потенциально изолировать одноранговые узлы Blockchain-системы, распространять среди новых узлов поддельные блоки с мошенническими транзакциями, делать недействительными транзакции. Проявления DDoS-атаки могут разнообразными, в зависимости от характера функциональности Blockchain-приложения, особенностей его сетевой архитектуры и поведения одноранговых узлов. Рассмотрены меры противодействия атакам на одноранговую пиринговую архитектуру.

Ключевые слова: технология Blockchain; злоумышленный майнинг; атака 51 %; DDoS-атаки и DNS-атаки.

Ил. 4. Библиогр.: 19 назв.

UDC 004.75

Analysis of planes of attacks on the Blockchain system / *P.I. Stetsenko, G.Z. Khalimov, E.V. Kotukh* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 114 – 121.

This paper presents a study of attack planessurfaces and possible ways of conducting various attacks on decentralized systems based on Blockchain technology. To accomplish the task, the effectiveness of the attack is studied relative to the plane of its application, namely, relatively: cryptographic designs of Blockchain technology, distributed architecture of systems based on Blockchain technology, Blockchain application context. Several attacks have been identified for each of these planes, including malicious mining strategies, coordinated peer behavior, 51% attacks, domain name attacks (DNS), distributed denial of service attacks, delayed consensus achieving, Blockchain branching, orphaned and obsolete blocks, digital wallet thefts and privacy attacks.

An attack by malicious mining allows an attacker to increase rewards by intentionally keeping his blocks closed in order to obtain a longer version of the Blockchain register than the current main version of the register. A 51% attack occurs when a single attacker, a group of nodes, or a mining pool (a combination of miners) in a network reaches most of the total processing power of mining in the system and gets the ability to manipulate the functionality of the Blockchain system. In the plane of DNS attacks, an attacker can potentially isolate peers of the Blockchain system, distribute fake blocks with fraudulent transactions among new nodes, and invalidate transactions. Manifestations of DDoS attacks can vary, depending on the nature of the functionality of the Blockchain application, the features of its network architecture and the behavior of peer nodes. Measures to counter attacks on peer-to-peer peer-to-peer architecture are considered.

Keywords: Blockchain technology; malicious mining; 51% attack; DDoS attacks and DNS attacks.

4 fig. Ref.: 19 items

УДК 004.056.5

Прототипування децентралізованої системи електронного блокчейн-голосування / *І.Д. Горбенко, О.О. Кузнецов, М.О. Полуяненко, А.С. Кіян, К.Є. Лисицький, С.О. Кандій* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 122 – 139.

Сучасна система електронного голосування являє собою взаємопов'язану сукупність правил, методів, процесів, засобів і технологій, а також правових норм, що забезпечують і регулюють дистанційне легітимне волевиявлення авторизованих користувачів (виборців). В статті запропоновано, досліджено та випробувано шляхом фізичного прототипування дворівневу архітектуру системи електронного блокчейн-голосування. Нижній (перший) рівень дозволяє забезпечити виконання всіх складових процесу електронної ідентифікації за допомогою вже існуючих систем, таких, наприклад, як BankID, MobileID, електронний підпис, тощо. Це забезпечить інтероперабельність електронного голосування, успадковуваність вже впроваджених національних інформаційних систем, зокрема, національної системи електронних довірчих послуг, відтворюваність результатів фізичного прототипування блокчейн-голосування. Верхній (другий) рівень призначено для реалізації волевиявлення та підрахунку голосів із забезпеченням незалежного контролю за правильністю складання списків виборців; можливості анонімного голосування тільки тими особами, які мають на це право; незмінності та неспростовності результатів волевиявлення; легкості та прозорості перевірки правильності підрахунку голосів, тощо. Отримані результати фізичного прототипування дозволяють стверджувати про ґрунтовність та виваженість розробленої архітектури, її спроможність забезпечити виконання базових вимог децентралізованого електронного голосування, вимог інформаційної та функціональної безпеки та надійності інформаційних технологій. Практичне впровадження розробленої архітектури блокчейн-голосування підвищить довіру до інформаційних ресурсів та сервісів (що є особливо актуальним для державних установ); зменшить час та накладні витрати; унеможливить втручання централізованих установ та можливі корупційні дії; підвищить надійність збереження інформації та якість наданих послуг.

Ключові слова: електронне голосування; децентралізація; інформаційні технології; блокчейн-мережі; інформаційна та кібербезпека.

Табл. 2. Іл. 7. Бібліогр.: 14 назв.

УДК 004.056.5

Прототипирование децентрализованной системы электронного блокчейн-голосования / *И.Д. Горбенко, А.А. Кузнецов, Н.А. Полуяненко, А.С. Киян, К.Е. Лисицкий, С.А. Кандий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 122 – 139.

Современная система электронного голосования представляет собой взаимосвязанную совокупность правил, методов, процессов, средств и технологий, а также правовых норм, обеспечивающих и регулирующих дистанционное легитимное волеизъявления авторизованных пользователей (избирателей). В статье предложена, исследована и проверена путем физического прототипирования двухуровневая архитектура системы электронного блокчейн-голосования. Нижний (первый) уровень позволяет обеспечить выполнение всех составляющих процесса электронной идентификации с помощью уже существующих систем, таких, например, как BankID, MobileID, электронная подпись и тому подобное. Это обеспечит интероперабельность электронного голосования, наследуемость уже внедренных национальных информационных систем, в частности, национальной системы электронных доверительных услуг, воспроизводимость результатов физического прототипирования блокчейн-голосования. Верхний (второй) уровень предназначен для реализации волеизъявления и подсчета голосов с обеспечением независимого контроля за правильностью составления списков избирателей; возможности анонимного голосования только теми лицами, которые имеют на это право; неизменности и неотказуемости результатов волеизъявления; легкости и прозрачности проверки правильности подсчета голосов и тому подобное. Полученные результаты физического прототипирования позволяют утверждать об обоснованности и взвешенности разработанной архитектуры, ее способности обеспечить выполнение базовых требований децентрализованного электронного голосования, требований информационной и функциональной безопасности и надежности информационных технологий. Практическое внедрение разработанной архитектуры блокчейн-голосования повысит доверие к информационным ресурсам и сервисам (что особенно актуально для государственных учреждений); уменьшит время и накладные расходы; сделает невозможным вмешательство централи-

зованных учреждений и возможные коррупционные действия; повысит надежность хранения информации и качество предоставляемых услуг.

Ключевые слова: электронное голосование; децентрализация; информационные технологии; блокчейн-сети; информационная и кибербезопасность.

Табл. 2. Ил. 7. Библиогр.: 14 назв.

UDC 004.056.5

Prototyping decentralized electronic blockchain voting system / *I.D. Gorbenko, A.A. Kuznetsov, N.A. Poluyanenko, A.S Kiyan, K.E. Lisitsky, S.A. Kandy* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 122 – 139.

The modern electronic voting system is an interconnected set of rules, methods, processes, tools and technologies, as well as legal norms that ensure and regulate the remote legitimate will of authorized users (voters). This article proposes, investigates, and verifies by physical prototyping the two-tier architecture of the electronic blockchain voting system. The lower (first) level enables all components of the electronic identification process to be fulfilled by existing systems such as BankID, MobileID, electronic signature, and the like. This will ensure interoperability of electronic voting, inheritance of already implemented national information systems, in particular, of the national system of electronic confidential services, reproducibility of the results of physical prototyping of blockchain voting. The upper (second) level is intended for the implementation of the expression of votes and the counting of votes, with the provision of independent control over the correctness of the compilation of voter lists; the possibility of anonymous voting only by those who are entitled to it; the invariability and irrevocability of the results of the will; ease and transparency of checking the correctness of the vote count and the like. The obtained results of physical prototyping make it possible to confirm the validity and weight of the developed architecture, its ability to meet the basic requirements of decentralized electronic voting, the requirements of information and functional security and reliability of information technologies. The practical implementation of the developed blockchain voting architecture will increase trust in information resources and services (which is especially relevant for government agencies) and will reduce time and overhead; will make impossible the intervention of centralized institutions and possible corruption; will increase the reliability of information storage and the quality of services provided.

Keywords: electronic voting; decentralization; information technology; blockchain networks; information and cybersecurity.

2 tab. 7 fig. Ref.: 14 items

УДК 004.056.5

Аналітичне моделювання атаки подвійної витрати на блокчейн-системи із ймовірнісним протоколом консенсусу / *М.О. Полуяненко, О.О. Кузнецов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 140 – 152.

Для побудови безпечних та надійних розподілених децентралізованих систем за технологією блокчейн створюється безперервний ланцюжок блоків, несанкціонована зміна яких унеможливлюється застосованими криптографічними механізмами. Це досягається використанням односпрямованих, стійких до колізій та пошуку прообразів криптографічних функцій, геш-значення яких від попередніх блоків включаються у наступні блоки. В результаті несанкціоновану зміну бодай одного біту даних в попередніх блоках буде відразу виявлено. Але у разі розподіленого зберігання інформації виникає додаткова вимога синхронізації окремих ланцюгів блоків, які зберігаються різними вузлами. Ці та інші питання вирішуються шляхом застосування механізмів встановлення консенсусу, за допомогою яких після виконання певної послідовності дій безперервна послідовність блоків (блокчейн-ланцюг) стає однаковою на всіх вузлах децентралізованої мережі. В роботі досліджується одна з основних вразливостей блокчейн систем, побудованих за допомогою консенсусу з ймовірнісною завершеністю, а саме – атака подвійної витрати. На підставі моделі «незалежних гравців» отримано аналітичний вираз розрахунку ймовірності успішного проведення зловмисником атаки подвійної витрати. Наведено кількісні значення ймовірності вдалої атаки для різних можливостей зловмисника, різної кількості сформованих блоків та різною тривалістю гонки. За допомогою комп'ютерного моделювання експериментально перевірено розраховані значення. Всі емпіричні оцінки отримані для високої точності (відносна помилка не гірше 1 %) і достовірності (довірча ймовірність не менш 99 %). Для підтвердження адекватності отриманих результатів наведено порівняння емпіричних результатів з теоретичними розрахунками.

Ключові слова: децентралізована система; технологія блокчейн; протокол консенсусу; модель незалежних гравців; атака подвійної витрати.

Табл. 2. Іл. 11. Бібліогр.: 8 назв.

УДК 004.056.5

Аналитическое моделирование атаки двойной затраты на блокчейн-системы с вероятностным протоколом консенсуса / *Н.А. Полуяненко, А.А. Кузнецов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 140 – 152.

Для построения безопасных и надежных распределенных децентрализованных систем по технологии блокчейн создается непрерывная цепочка блоков, несанкционированное изменение которых не допускается применяемыми криптографическими механизмами. Это достигается использованием однонаправленных, устойчивых к коллизиям и поиску прообразов криптографических функций, хеш-значения которых от предыду-

щих блоков включаются в последующие блоки. В результате несанкционированное изменение хотя бы одного бита данных в предыдущих блоках будет сразу обнаружено. Однако в случае распределенного хранения информации возникает дополнительное требование синхронизации отдельных цепочек блоков, которые хранятся различными узлами. Эти и другие вопросы решаются путем применения механизмов установления консенсуса, с помощью которых после выполнения определенной последовательности действий непрерывная последовательность блоков (блокчейн-цепочка) становится одинаковой на всех узлах децентрализованной сети. В работе исследуется одна из основных уязвимостей блокчейн-систем, построенных с помощью консенсуса с вероятностной завершенностью, а именно – атака двойной траты. На основании модели «независимых игроков» получено аналитическое выражение расчета вероятности успешного проведения злоумышленником атаки двойной траты. Приведены количественные значения вероятности удачной атаки для различных возможностей злоумышленника, разного количества сформированных блоков и разной продолжительности гонки. С помощью компьютерного моделирования экспериментально проверены рассчитанные значения. Все эмпирические оценки получены с высокой точностью (относительная ошибка не выше 1 %) и достоверности (доверительная вероятность не менее 99 %). Для подтверждения адекватности полученных результатов приведено сравнение эмпирических результатов с теоретическими расчетами.

Ключевые слова: децентрализованная система; технология блокчейн; протокол консенсуса; модель независимых игроков; атака двойной расходы.

Табл. 2. Ил. 11. Библиогр.: 8 назв.

UDC 004.056.5

Analytical modeling of the attack of double costs on a blockchain system with a probabilistic consensus protocol / *N.A. Poluyanenko, A.A. Kuznetsov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 140 – 152.

To build safe and reliable distributed decentralized systems using blockchain technology, a continuous chain of blocks is created, the unauthorized modification of which is not allowed by the applied cryptographic mechanisms. This is achieved by using unidirectional, collision resistant and search prototypes of cryptographic functions whose hash values from previous blocks are included in subsequent blocks. As a result, an unauthorized change in at least one bit of data in the previous blocks will be immediately detected. However, in the case of distributed storage of information, there is an additional requirement of synchronization of individual chains of blocks that are stored by various nodes. These and other issues are resolved by applying consensus building mechanisms, through which, after a certain sequence of actions, a continuous sequence of blocks (blockchain chain) becomes the same on all nodes of a decentralized network. This work examines one of the main vulnerabilities of blockchain systems built by consensus with probabilistic completion, namely, a double-spend attack. Based on the model of “independent players”, an analytical expression is obtained for calculating the probability of an attacker's successful double-spending attack. The quantitative values of the probability of a successful attack are given for various abilities of an attacker, a different number of generated blocks and a different race duration. Using computer simulation, the calculated values are experimentally verified. All empirical estimates were obtained with high accuracy (relative error not higher than 1%) and reliability (confidence level of at least 99%). To confirm the adequacy of the results obtained, a comparison of empirical results with theoretical calculations is given.

Key words: decentralized system; blockchain technology; consensus protocol model of independent players; attack double costs.

2 tab. 11 fig. Ref.: 8 items

УДК 004.056.5

Ймовірність успішної атаки подвійної витрати на блокчейн-системи із ймовірнісним протоколом консенсусу / *Н.А. Полуяненко, О.О. Кузнецов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 153 – 161.

Більшість традиційних інформаційних систем побудовано за централізованим ієрархічним принципом. В таких системах існує єдиний центр прийняття рішень, щодо якого інші вузли є підлеглими, отже повинні безумовно сприймати та виконувати централізовані інструкції. Крім того, наявність центру прийняття рішень зумовлює і додаткові загрози, оскільки для порушення роботи всієї системи достатньо знищити або скомпрометувати головний вузол. Отже більш стійкими та безпечними, особливо в ситуації повної недовіри один до одного, є децентралізовані системи. Вони є більш надійними для збереження важливої інформації, наприклад цифрових активів, реєстрів, кадастрів, тощо. Саме тому технології блокчейн для побудови децентралізованих систем стають все більш популярними та поширеними. Однак при розгортанні децентралізованих систем виникає завдання узгодження стану різних вузлів мережі. Це особливо актуально, коли вузли функціонують в режимі повної недовіри один до одного, тобто якщо можливі ситуації, коли частка вузлів контролюється зловмисниками. Цю задачу вирішують за допомогою протоколів консенсусу, тобто таких правил та алгоритмів, при виконанні яких досягається однаковий стан більшості вузлів децентралізованої системи. В статті розглядаються ймовірнісні протоколи консенсусу, тобто коли виникнення певного стану є випадковою подією. Отже погодження станів системи можливе різними шляхами, в тому числі можливі хибні випадки, які нав’язуються зловмисниками. Наприклад, зловмисники можуть подвоїти свої електронні активи шляхом їх подвійної витрати. Звісно, якщо більшість вузлів контролюється зловмисниками, система буде працювати хибно. Але навіть при меншій частці ресурсів зловмисники також можуть з певною ймовірністю нав’язати хибний стан системи та

реалізувати у такий спосіб атаку подвійної витрати. В статті розглядаються різні ситуації та можливі стани системи, аналітичним шляхом виводяться формули розрахунку ймовірності успішної атаки подвійної витрати на блокчейн-системи із ймовірнісним протоколом консенсусу. При проведенні досліджень застосовувалася модель незалежних гравців, яка, на відміну від відомих робіт, враховує повну множину елементарних подій та станів системи. На основі отриманих результатів наведено рекомендації щодо безпечного функціонування децентралізованої системи.

Ключові слова: децентралізована система; технологія блокчейн; протокол консенсусу; модель незалежних гравців; атака подвійної витрати.

Іл. 3. Бібліогр.: 11 назв.

УДК 004.056.5

Вероятность успешной атаки двойной затраты на блокчейн-системы с вероятностным протоколом консенсуса / *Н.А. Полуяненко, А.А. Кузнецов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 153 – 161.

Большинство традиционных информационных систем построено по централизованному иерархическому принципу. В таких системах существует единый центр принятия решений, по отношению к нему другие узлы являются подчиненными, следовательно, должны безусловно воспринимать и выполнять централизованные инструкции. Кроме того, наличие центра принятия решений обуславливает и дополнительные угрозы, поскольку для нарушения работы всей системы достаточно уничтожить или скомпрометировать главный узел. Более устойчивыми и безопасными, особенно в ситуации полного недоверия друг к другу, являются децентрализованные системы. Они более надежны для сохранения важной информации, например цифровых активов, реестров, кадастров и тому подобное. Именно поэтому технологии блокчейн для построения децентрализованных систем становятся все более популярными и распространенными. Однако при развертывании децентрализованных систем возникает задача согласования состояния различных узлов сети. Это особенно актуально, когда узлы функционируют в режиме полного недоверия друг к другу, то есть если возможны ситуации, когда доля узлов контролируется злоумышленниками. Эту задачу решают с помощью протоколов консенсуса, то есть таких правил и алгоритмов, при выполнении которых достигается одинаковое состояние большинства узлов децентрализованной системы. В статье рассматриваются вероятностные протоколы консенсуса, то есть когда возникновение определенного состояния является случайным событием. Согласование состояний системы возможно различными путями, в том числе возможные ложные случаи, которые навязываются злоумышленниками. Например, злоумышленники могут удвоить свои электронные активы путем их двойной траты. Конечно, если большинство узлов контролируется злоумышленниками, система будет работать неправильно. Но даже при меньшей доле ресурсов злоумышленники также могут с определенной вероятностью навязать ложное состояние системы и реализовать атаку двойной траты. В статье рассматриваются различные ситуации и возможные состояния системы, аналитическим путем выводятся формулы расчета вероятности успешной атаки двойной траты на блокчейн системы с вероятностным протоколом консенсуса. При проведении исследований применялась модель независимых игроков, которая, в отличие от известных работ, учитывает полное множество элементарных событий и состояний системы. На основе полученных результатов приведены рекомендации по безопасному функционированию децентрализованной системы.

Ключевые слова: децентрализованная система; технология блокчейн; протокол консенсуса; модель независимых игроков; атака двойной траты.

Ил. 3. Библиогр.: 11 назв.

UDC 004.056.5

Probability of a successful attack of double costs on a blockchain system with a probabilistic consensus protocol / *N.A. Poluyanenko, A.A. Kuznetsov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 153 – 161.

Most traditional information systems are built on a centralized hierarchical principle. In such systems, there is a single decision-making center, to which other nodes are subordinate, therefore, they must certainly perceive and follow centralized instructions. In addition, the presence of a decision center causes additional threats, since to disrupt the operation of the entire system it is enough to destroy or compromise the main node. Decentralized systems are more stable and secure, especially in a situation of complete distrust of each other. They are more reliable for storing important information, such as digital assets, registries, inventories and the like. That is why blockchain technologies for building decentralized systems are becoming increasingly popular and widespread. However, when deploying decentralized systems, the task of coordinating the state of various network nodes arises. This is especially true when the nodes operate in a mode of complete distrust of each other, that is, if situations are possible where the proportion of nodes is controlled by intruders. This problem is solved using consensus protocols, that is, such rules and algorithms that, when executed, achieve the same state for most nodes of a decentralized system. This article discusses probabilistic consensus protocols, that is, when the occurrence of a certain state is a random event. Coordination of system states is possible in various ways, including possible false cases that are imposed by attackers. For example, attackers can double their electronic assets by spending them twice. Of course, if most nodes are controlled by intruders, the system will not work properly. But even with a smaller share of resources, attackers can also with a certain probability impose a false state of the system and thus implement a double-spend attack. The article discusses various situations and possible states of the system, analytically deriving formulas for calculating the probability of a successful double spending attack on a

blockchain system with a probabilistic consensus protocol. When conducting research, the model of independent players was used, which, unlike the well-known works, takes into account the complete set of elementary events and system states. Based on the results obtained, recommendations are given on the safe functioning of a decentralized system.

Key words: decentralized system; blockchain technology; consensus protocol; independent player model; double waste attack.

3 fig. Ref.: 11 items.

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ В КОМУНІКАЦІЙНИХ СИСТЕМАХ
МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ В КОММУНИКАЦИОННЫХ СИСТЕМАХ
METHODS AND MEANS OF PROTECTION IN COMMUNICATION SYSTEMS

УДК 621.391

Теоретичні основи синтезу квазіортогональних систем складних сигналів / *І.Д. Горбенко, О.А. Замула* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 162 – 174.

Функціонування низки сучасних інфокомунікаційних систем (ІКС) здійснюється в умовах зовнішніх і внутрішніх впливів, обумовлених, з одного боку, дією природних перешкод, перешкод від інших радіотехнічних систем, що функціонують на близьких частотах або в спільній ділянці діапазону частот, з іншого боку – навмисних завад, створюваних станціями протидії з метою радіоелектронного подавлення діючих систем. Можливими стратегіями станції протидії є: визначення змісту повідомлень при використанні легальними абонентами алгоритмів криптографічного захисту даних; фальсифікація повідомлень; порушення цілісності даних; постановка різних типів перешкод і інше. Тому, до ІКС, особливо критичного призначення, пред'являються все більш жорсткі вимоги щодо забезпечення ефективності їх функціонування: достовірності і швидкості передачі інформації, живучості, завадозахищеності, інформаційної безпеки. У таких умовах особливого значення набуває наявність і застосування захищених інформаційно-комунікаційних систем. Під захищеністю систем розуміють, перш за все, їх здатність забезпечувати необхідні показники з завадозахищеності, імітостійкості, інформаційної, енергетичної і структурної скритності, швидкості передавання інформації, частотної і енергетичної ефективності. Необхідність застосування захищених радіоканалів змушує дослідників по-новому подивитися як на режими функціонування захищених радіоканалів, так і на аспекти формування і застосування складних сигналів – фізичних переносників даних для таких систем. У роботі на основі дослідження алгебраїчної структури систем нелінійних параметричних нерівностей сформульовані і у загальному виді вирішені задачі синтезу низки класів квазіоптимальних рівномірних, нерівномірних, складних дискретних сигналів із заданими кореляційними, ансамблевими і структурними властивостями, в тому числі таких систем сигналів, які мають властивості «розмитості» за кореляційними властивостями. Зазначена властивість означає, що збільшення або зменшення довжини дискретного сигналу не змінює кореляційні властивості дискретної послідовності, на основі якої синтезовано сигнал. Показано, що застосування безлічі зазначених систем сигналів в сучасних інформаційно-комунікаційних системах дозволить поліпшити показники функціонування таких систем, насамперед, завадозахищеності, скритності функціонування, інформаційної безпеки, завадостійкості прийому сигналів.

Ключові слова: функція кореляції; ортогональні сигнали; дискретні послідовності; складові системи сигналів; синтез систем сигналів; шумоподібний сигнал..

Бібліогр.: 8назв.

УДК 621.391

Теоретические основы синтеза квазиортогональных систем сложных сигналов / *И.Д. Горбенко, А.А. Замула* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 162 – 174.

Функционирование ряда современных инфокоммуникационных систем (ИКС) осуществляется в условиях внешних и внутренних воздействий, обусловленных, с одной стороны, действием естественных помех, помех от других радиотехнических систем, функционирующих на близких частотах или в общем участке диапазона частот, с другой стороны – умышленных помех, создаваемых станциями противодействия с целью радиоэлектронного подавления действующих систем. Возможными стратегиями станции противодействия являются: определение содержания сообщений при использовании легальными абонентами алгоритмов криптографической защиты данных; фальсификация сообщений; нарушение целостности данных; постановка различных типов помех и др. Поэтому, к ИКС, особенно критического назначения, предъявляются все более жесткие требования по обеспечению эффективности их функционирования: достоверности и скорости передачи информации, живучести, помехозащищенности, информационной безопасности. В таких условиях особое значение приобретает наличие и применение защищенных ИКС. Под защищенностью систем понимают, прежде всего, их способность обеспечивать необходимые показатели по помехозащищенности, информационной, энергетической и структурной скрытности, скорости передачи информации, частотной и энергетической эффективности. Необходимость применения защищенных систем заставляет исследователей по-новому посмотреть на режимы функционирования защищенных радиоканалов и на аспекты формирования и применения сложных сигналов – физических переносчиков данных для таких систем. В работе на основе исследования алгебраической структуры систем нелинейных параметрических неровностей сформулированы и в общем виде решены задачи синтеза ряда

классов квазиоптимальных равномерных, неравномерных, сложных дискретных сигналов с заданными корреляционными, ансамблевыми и структурными свойствами, в том числе таких систем сигналов, которые обладают свойствами «размытости» по корреляционным свойствам. Указанное свойство означает, что увеличение или уменьшение длительности дискретной последовательности не изменяет корреляционные свойства сигнала, на основе которой синтезирован сигнал. Показано, что применение множества указанных систем сигналов в современных информационно-коммуникационных системах позволит улучшить такие показатели функционирования таких систем, как помехозащищенность, скрытность функционирования, информационная безопасность, помехоустойчивость приема сигналов.

Ключевые слова: функция корреляции; ортогональные сигналы; дискретные последовательности, составные системы сигналов; синтез систем сигналов; шумоподобный сигнал.

Библиогр.: 8 назв.

UDC 621.391

Theoretical bases of synthesis of quasi-orthogonal systems of complex signals / *I.D. Gorbenko, A.A. Zamula* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 162 – 174.

Functioning of a number of modern infocommunication systems (ICS) is carried out under external and internal influences, caused, on the one hand, by natural interference, interference from other radio systems operating at close frequencies or in a common part of the frequency range, on the other hand, intentional interference created by counteraction stations with the aim of electronic suppression of existing systems. Possible strategies of the counter station are as follows: determining the content of messages when legal subscribers use cryptographic data protection algorithms; falsification of messages; violation of data integrity; staging of various types of interference, etc. Therefore, more stringent requirements are imposed on the ICS, especially for critical purposes, to ensure the effectiveness of their functioning: reliability and speed of information transfer, survivability, noise immunity, information security. In such conditions, the presence and use of protected ICS is of particular importance. Under the security systems one should understand, first of all, their ability to provide the necessary indicators for noise immunity, information, energy and structural secrecy, information transfer speed, frequency and energy efficiency. The need for the use of secure systems makes researchers take a fresh look at both the modes of operation of secure radio channels and the aspects of formation and use of complex signals – physical data carriers for such systems. In this paper, based on the study of the algebraic structure of systems of non-linear parametric irregularities, the problems of synthesis of a number of classes of quasi-optimal uniform, non-uniform, complex discrete signals with specified correlation, ensemble and structural properties, including such signal systems that have the properties “blur" by correlation properties. This property means that an increase or decrease in the duration of a discrete sequence does not change the correlation properties of the signal, on the basis of which the signal is synthesized. It is shown that the use of many of the indicated signal systems in modern information and communication systems will improve such indicators of the functioning of such systems as noise immunity, operational secrecy, information security, noise immunity of signal reception.

Key words correlation function; orthogonal signals; discrete sequences, composite signal systems; synthesis of signal systems; noise-like signal.

Ref.: 8 items

УДК 621.391

Методи пошуку оптимальних за мінімаксним критерієм систем складних нелінійних дискретних сигналів / *І.Д. Горбенко, О.А. Замула, Хо Чі Лик* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 175 – 187.

Серед основних напрямків поліпшення показників інформаційної безпеки, завадозахищеності і скритності інформаційно-комунікаційних систем (ІКС) можна виділити напрямки, які пов'язані із застосуванням каналів з великою частотною надмірністю, значною просторовою, структурною, енергетичною та часовою скритністю. Для забезпечення частотної надмірності на фізичному рівні широке застосування отримали дискретні сигнали, в яких маніпульовані параметри (амплітуда, фаза, частота) змінюються через строго фіксовані інтервали часу. Закон зміни зазначених параметрів задається дискретними послідовностями, які повністю визначають властивості дискретних сигналів і часто ототожнюються з ними. При синтезі систем сигналів (для застосування у захищених ІКС) прагнуть забезпечити певні властивості сигналів, насамперед: задано структурну скритність щодо визначення законів формування сигналів; поліпшено ансамблеві властивості (існування практично для будь-якого значення періоду, значний об’єм системи сигналів); визначено (для забезпечення необхідного значення завадостійкості прийому) кореляційні властивості. На основі критеріїв максимальної правдоподібності, мінімаксного критерію, фундаментальної границі оцінювання Крамера – Рао сформульовано вимоги до вибору систем сигналів для широкого спектру додатків багатокористувацьких ІКС. Зокрема, запропоновано великі ансамблі нелінійних складних сигналів в якості сигналів – фізичних переносників даних в ІКС. Показано, що такі сигнали мають поліпшені (в порівнянні з широко використовуваними класами лінійних сигналів) ансамблеві, кореляційні, структурні та інші властивості. Зазначене дозволяє поліпшити такі показники функціонування ІКС як завадозахищеність, електромагнітна сумісність, скритність і інформаційна безпека, що є дуже важливим для деяких додатків ІКС загального і критичного призначення. Показана можливість використання запропонованих систем сигналів при вирішенні класичних завдань оптимального прийому: виявлення та розрізнення сигналів, оцінка параметрів сигналів. При цьому (внаслідок хороших кореляційних властивостей запропонованих систем

сигналів) забезпечуються необхідні (для відповідних завдань) показники завадостійкості прийому сигналів і точності оцінки параметрів сигналів.

Ключові слова: функція кореляції; дискретні послідовності; синтез систем сигналів; шумоподібний сигнал, оцінка параметрів сигналу; завадостійкість прийому сигналів; криптографічний сигнал.

Табл. 4. Іл. 5. Бібліогр.: 15 назв.

УДК 621.391

Методы поиска оптимальных по минимаксному критерию систем сложных нелинейных дискретных сигналов / *И.Д. Горбенко, А.А. Замула, Хо Чи Лык* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 175 – 187.

Среди основных направлений улучшения показателей информационной безопасности, помехозащищенности и скрытности информационно-коммуникационных систем (ИКС) можно выделить направления, связанные с применением каналов с большой частотной избыточностью, значительной пространственной, структурной, энергетической и временной скрытностью. Для обеспечения частотной избыточности на физическом уровне широкое применение получили дискретные сигналы, в которых манипулируемые параметры (амплитуда, фаза, частота) меняются через строго фиксированные интервалы времени. Закон изменения указанных параметров задается дискретными последовательностями, которые полностью определяют свойства дискретных сигналов и часто отождествляются с ними. При синтезе систем сигналов (для применения в защищенных ИКС) стремятся обеспечить определенные свойства сигналов, прежде всего: заданная структурная скрытность по определению законов формирования сигналов; улучшенные ансамблевые свойства (существование практически для любого значения периода, значительный объем системы сигналов); необходимые (для обеспечения требуемого значения помехоустойчивости приема) корреляционные свойства. На основе критериев максимального правдоподобия, минимаксного критерия, фундаментальной границы оценивания Крамера – Рао сформулированы требования к выбору систем сигналов для широкого спектра приложений многопользовательских ИКС. В частности, предложены большие ансамбли нелинейных сложных сигналов в качестве сигналов – физических переносчиков данных в ИКС. Показано, что такие сигналы обладают улучшенными (по сравнению с широко используемыми классами линейных сигналов) ансамблевыми, корреляционными, структурными и другими свойствами. Указанное позволяет улучшить такие показатели функционирования ИКС как помехоустойчивость, электромагнитная совместимость, скрытность и информационная безопасность, что важно для некоторых приложений ИКС общего и критичного назначения. Показана возможность использования предложенных систем сигналов при решении классических задач оптимального приема: обнаружение и различение сигналов, оценка параметров сигналов. При этом (вследствие хороших корреляционных свойств предложенных систем сигналов) обеспечиваются необходимые (для соответствующих задач) показатели помехоустойчивости приема сигналов и точности оценки параметров сигналов.

Ключевые слова: функция корреляции; дискретные последовательности; синтез систем сигналов; шумоподобный сигнал, оценка параметров сигнала; помехоустойчивость приема сигналов; криптографический сигнал.

Табл. 4. Ил. 5. Библиогр.: 15 назв.

UDC 621.391

Methods of searching for systems of complex nonlinear discrete signals optimal by the minimax criterion / *I.D. Gorbenko, A.A. Zamula, Ho Tri Luc* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 175 – 187.

Among the main directions of improving information security indicators, noise immunity and secrecy of information and communication systems (ICS), we can single out areas related to the use of channels with high frequency redundancy, significant spatial, structural, energy and temporal secrecy. To ensure frequency redundancy at the physical level, discrete signals are widely used, in which the manipulated parameters (amplitude, phase, frequency) change at strictly fixed time intervals. The law of variation of these parameters is set by discrete sequences that completely determine the properties of discrete signals and are often identified with them. In the synthesis of signal systems (for use in protected ICS), they strive to provide certain properties of signals, first of all: a given structural secrecy in determining the laws of signal formation; improved ensemble properties (existence for almost any period value, a significant amount of the signal system); necessary (to ensure the desired value of the noise immunity of the reception) correlation properties. Based on the criteria of maximum likelihood, minimax criterion, the fundamental boundary of the Cramer-Rao assessment, the requirements to the choice of signal systems for a wide range of multi-user ICS applications are formulated. In particular, large ensembles of nonlinear complex signals are proposed as signals — physical data carriers in ICS. It is shown that such signals have improved (in comparison with the widely used classes of linear signals) ensemble, correlation, structural and other properties. The aforementioned allows to improve such performance indicators of the ICS as noise immunity, electromagnetic compatibility, secrecy and information security, which is very important for some general and critical ICS applications. The possibility of using the proposed signal systems in solving classical problems of optimal reception is shown: detection and discrimination of signals, estimation of signal parameters. In this case (due to the good correlation properties of the proposed signal systems), the necessary (for the corresponding tasks) indicators of noise immunity of signal reception and the accuracy of the estimation of signal parameters are provided.

Keywords: correlation function; discrete sequences; synthesis of signal systems; noise-like signal, estimation of signal parameters; noise immunity of signal reception; cryptographic signal.

4 tab. 5 fig. Ref.: 15 items.

УДК 004.056.53

Оцінка безпеки користувачів інтернет-банкінгу / *І.Є. Антіпов, Б.В. Бочаров, Д.Р. Найдьонова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 188 – 194.

Стаття присвячена загрозам безпеки в популярному сервісі – інтернет-банкінгу, який останнім часом стає все більш поширеним. У статті узагальнено і проаналізовано загрози для користувачів інтернет-банкінгу, пов'язані з використанням телекомунікаційних мереж і засобів зв'язку. Виділено чотири основні вразливості: викрадення телефону, методи соціальної інженерії, перехоплення даних переданих або тих, щозберігаються на мобільному пристрої, і викрадення даних sim-карти. Запропоновано методику чисельної оцінки вразливості користувача інтернет-банкінгу, обумовлену цими погрозами, в основі якої лежить метод експертних оцінок. Отримані чисельні оцінки дозволять скористатися існуючими методами розрахунку ризику. Показано, що в даний час найбільшу загрозу становлять методи соціальної інженерії. Запропоновано набір заходів для користувачів інтернет-банкінгу з протидії розглянутим загрозам і методику оцінки їх ефективності, також засновану на методі експертних оцінок. Показано, що найбільш ефективним заходом є використання для інтернет-банкінгу окремого телефону без операційної системи. Запропоновані методики можуть бути використані для оцінки ефективності будь-яких інших заходів щодо підвищення рівня безпеки користувачів інтернет-банкінгу від загроз, пов'язаних з використанням телекомунікаційних мереж і засобів зв'язку. Методики можуть доопрацьовуватися і підлаштовуватися під інші об'єкти інформаційної безпеки або тимчасові зміни в області захисту інформації.

Ключові слова: Інтернет-банкінг; телекомунікації; безпека; користувачі; метод експертних оцінок; загрози та вразливості.

Табл. 5. Іл. 1. Бібліогр.: 17 назв.

УДК 004.056.53

Оценка безопасности пользователей интернет-банкинга / *И.Е. Антипов, Б.В Бочаров, Д.Р. Найденова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 188 – 194.

Статья посвящена угрозам безопасности в популярном сервисе – интернет-банкинге, который в последнее время становится все более распространенным. Обобщены и проанализированы угрозы для пользователей интернет-банкинга, связанные с использованием телекоммуникационных сетей и средств связи. Выделены четыре основные уязвимости: похищение телефона, методы социальной инженерии, перехват данных передаваемых или хранящихся на мобильном устройстве и похищение данных sim-карты. Предложена методика численной оценки уязвимости пользователя интернет-банкинга, обусловленная этими угрозами, в основе которой лежит метод экспертных оценок. Полученные численные оценки позволят воспользоваться существующими методами расчета риска. Показано, что в настоящее время наибольшую угрозу представляют методы социальной инженерии. Предложены набор мер для пользователей Интернет-банкинга по противодействию рассмотренным угрозам и методика оценки их эффективности, также основанная на методе экспертных оценок. Показано, что наиболее эффективной мерой является использование для интернет-банкинга отдельного телефона без операционной системы. Предложенные методики могут быть использованы для оценки эффективности любых других мер по повышению уровня безопасности пользователей интернет-банкинга от угроз, связанных с использованием телекоммуникационных сетей и средств связи. Методики могут дорабатываться и подстраиваться под другие объекты информационной безопасности или временные изменения в области защиты информации.

Ключевые слова: Интернет-банкинг; телекоммуникации; безопасность; пользователи; метод экспертных оценок; угрозы и уязвимости.

Табл. 5. Ил. 1. Библиогр.: 17 назв.

UDC 004.056.53

Estimate of the Internet banking user security / *I.E. Antipov, B.V. Bocharov, D.R. Naydenova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 188 – 194.

The paper deals with security threats in the popular Internet banking service, the spread of which is becoming more common. Threats to the Internet banking users related to the use of telecommunication networks and means of communication are summarized and analyzed. Four main vulnerabilities have been identified: phone theft, social engineering methods, interception of data transmitted or stored on a mobile device, theft of SIM card data. Methods for numerically assessing the vulnerability of an Internet banking user due to these threats have been proposed. They are based on expert assessment method. The obtained numerical estimates will make it possible to use the existing methods for calculating risk. It is shown that currently the greatest threat is posed by methods of social engineering. A set of measures is proposed for users to counter the considered threats and a methodology for assessing their effectiveness, based on the expert assessment method too. It is shown that the most effective measure is the use of a separate telephone for Internet banking without an operating system. The proposed methods can be used to assess the effectiveness of any other measures to improve the security level of Internet banking users from threats associated with the use of telecommunication networks and communications. This method can be refined and adjusted to other information security objects or temporary changes in the field of information protection

Key words: Internet-banking; telecommunication; security; users; method of expert evaluations; threat and vulnerability.

5 tab. 1 fig. Ref.: 17 items

УДК 004.491.4

Метод виявлення та протидії вірусам у зображеннях формату BMP / *Р.С. Гриньов, О.В. Сєвєрінов, А.В. Власов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 195 – 200.

Мета статті – розробка методу захисту сучасних систем від атак з використанням графічних файлів формату BMP та HID-атак. Розглядаються особливості зображень формату BMP, спосіб їх використання для впровадження комп'ютерних вірусів та проведення атак з метою подолання засобів захисту. Також розглядаються HID-атаки та можливість поєднання цих атак; особливості функціонування сучасних засобів захисту IDS, IPS, антивірусів, брандмауерів та їх недоліки. Подібні атаки можливі через те, що засоби захисту аналізуватимуть тільки виконувані файли, бібліотеки DLL, документи Word, аплети Java. Більшість із засобів захисту просто не звертають уваги на зображення або інший безпечний тип файлу, оскільки вважають, що немає причин витрачати процесорний цикл на аналіз зображення. HID пристрої сприймаються засобами захисту як простий інтерфейс між комп'ютером та користувачем, тому є цілком довіреними. Запропоновано методи виявлення вірусів у графічних файлів формату BMP, засновані на перевірці зарезервованих полів, що мають бути нульовими; відповідності справжнього розміру файлу зазначеному у заголовку файлу; відповідності розміру зображення у пікселях, що зазначений у заголовку справжньому, Також запропоновано метод протидії HID-атакам, що заснований на аналізі швидкості введення тексту. Розроблено програми, що демонструють ефективність захисту від розглянутих атак.

Ключові слова: файл зображення формату BMP; комп'ютерний вірус; шелл-код; подолання систем захисту; приховування вірусу; антивірус; IDS; IPS; вразливість, експлойт; HID-атака; протидія атакам; методи захисту.

Іл. 5. Бібліогр.: 11 назв.

УДК 004.491.4

Метод выявления и противодействия вирусам в изображениях формата BMP / *Р.С. Гринев, А.В. Северинов, А.В. Власов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 195 – 200.

Цель статьи – разработка метода защиты современных систем от атак с использованием графических файлов формата BMP и HID-атак. Рассматриваются особенности изображений формата BMP, способ их использования для внедрения компьютерных вирусов и проведения атак с целью преодоления средств защиты. Рассматриваются HID-атаки и возможность сочетания этих атак; особенности функционирования современных средств защиты IDS, IPS, антивирусов, брандмауэров и их недостатки. Подобные атаки возможны из-за того, что средства защиты будут анализировать только исполняемые файлы, библиотеки DLL, документы Word, апплеты Java. Большинство из средств защиты просто не обращают внимания на изображения или другой безопасный тип файла. Поскольку считают, что нет причин тратить процессорный цикл на анализ изображения. HID устройства воспринимаются средствами защиты как простой интерфейс между компьютером и пользователем, поэтому являются доверенными. Предложены методы выявления вирусов в графических файлах формата BMP, основанные на проверке зарезервированных полей, которые должны быть нулевыми, соответствии настоящего размера файла значению в заголовке файла, соответствии размера изображения в пикселях указанному в заголовке настоящему. Также предложен метод противодействия HID атакам, основанный на анализе скорости ввода текста. Разработаны программы, демонстрирующие эффективность защиты от рассмотренных атак.

Ключевые слова: файл изображения формата BMP; компьютерный вирус; шелл-код; преодоление систем защиты; сокрытия вируса; антивирус; IDS; IPS; уязвимость; эксплойт; HID-атака; противодействие атакам; методы защиты.

Ил. 5. Библиогр.: 11 назв.

UDC 004.491.4

Method for detecting and counteracting Virus Detection in BMP images / *R.S. Grynov, A.V. Sievierinov, A.V. Vlasov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 195 – 200.

The aim of the article is to develop a method for protecting modern systems against attacks using BMP image files and HID attacks. This article describes the features of BMP format images. The method of injecting computer viruses in BMP image and attacks to overcome the means of protection. HID attacks and the possibility of combining these attacks are also considered. Features of functioning of modern means of protection IDS, IPS, antiviruses, firewalls and their shortcomings are presented. Such attacks are possible due to the fact that security tools will only analyze executable files, DLLs, Word documents, Java applets. Most of the protection tools simply do not pay attention to images or another secure file type. Because they believe, that there is no reason to spend the processor cycle on image analysis. HID devices are perceived by security tools as a simple interface between a computer and a user, therefore they are trusted. The article suggests methods for detecting viruses in BMP image files based on checking reserved fields that should be zero, matching the real file size with the value in the file header, matching the pixel size specified in the header with real. The article also offers a method to counteract HID attacks based on analysis of text input speed. Developed programs demonstrate the effectiveness of protection against the considered attacks.

Key words: BMP image file; computer virus; shell code; overcoming protection systems; virus hiding; antivirus; IDS; IPS; vulnerability; exploit; HID attack; protection methods.

5 fig. Ref.: 11 items.

УДК 621.391.15:519.7

Аналіз можливостей використання алгоритму Ель-Гамаля з детермінованим внесенням для інкапсуляції ключей / *О.В. Циганкова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 201 – 205.

Припустимо що дві сторони, А та В, використовують деякий симетричний алгоритм шифрування (наприклад, AES) для шифрування повідомлень, що надсилаються від А до В та від В до А. Вони отримують свої спільні секретні ключі від деякого Довіреного Центру (ДЦ). ДЦ генерує ключі і потім доставляє їх до відповідних користувачів. Найпростіший, та, мабуть, і найоптимальніший спосіб доставляти ключі до користувача А полягає у зашифруванні його (деяким асиметричним алгоритмом шифрування) публічним ключем користувача А і надсилати цьому користувачу відкритим каналом. Така процедура називається "інкапсуляція ключа".

Алгоритми інкапсуляції ключа широко використовуються у сучасній криптології та є представленими у національних стандартах та стандартах ISO/IEC. Побудова алгоритму інкапсуляції ключа, який можна було б використовувати як Національний стандарт, на сьогодні залишається актуальною проблемою. Українські криптологи також зараз працюють над таким стандартом. У проекті Національного стандарту інкапсуляції ключа запропоновано використати модифіковану схему шифрування на еліптичних кривих (ECIES), включену в стандарти ANSI X9.63, ISO/IEC 18033-2, IEEE 1363a та SECG SEC1.

У роботі запропоновано деякий альтернативний алгоритм шифрування на еліптичних кривих, який також можна використовувати для інкапсуляції ключів.

Для інкапсуляції ключа можна використовувати довільний асиметричний алгоритм шифрування. Одним з найпростіших таких алгоритмів є алгоритм Ель-Гамаля. Але для використання цього алгоритму на еліптичних кривих потрібно спочатку вкласти ключ у деяку точку еліптичної кривої, а потім виконати зворотне перетворення. Багато робіт, як з теорії чисел, так і з криптології, розглядали проблему побудови детермінованого відображення елементів поля у точки еліптичної кривої. Проте лише у 2016 р. вдалось побудувати алгоритм вкладення геш-значення у точку кривої, а до того існували лише імовірнісні алгоритми was proposed. Зазначимо, що алгоритм вкладення ключа побудувати складніше, оскільки відповідне відображення має бути бієктивним.

Показано, як можна побудувати такий алгоритм вкладення ключа, а також обговоримо проблеми, які виникають при його використанні як складової алгоритму інкапсуляції ключа.

Ключові слова: ключовий алгоритм інкапсуляції ключа; алгоритм Ель-Гамаля; еліптична крива.

Бібліогр.: 9 назв.

УДК 621.391.15:519.7

Анализ возможности использования алгоритма Эль-Гамаля с детерминированным вложением для инкапсуляции ключей / *О.В. Цыганкова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 201 – 205.

Предположим, что две стороны А и В, используют некоторый симметричный алгоритм шифрования (например AES) для шифрования сообщений, посылаемых от А до В и от В к А. Они получают свои общие секретные ключи от некоторого Доверенного Центра (ДЦ). ДЦ генерирует ключи и затем доставляет их к соответствующим пользователям. Самый простой, и, пожалуй, самый оптимальный способ доставлять ключи к пользователю А заключается в зашифровании его (некоторым асимметричным алгоритмом шифрования) публичным ключом пользователя А и направлении этому пользователю открытым каналом. Такая процедура называется "инкапсуляция ключа".

Алгоритмы инкапсуляции ключа широко используются в современной криптологии и представлены в национальных стандартах и стандартах ISO / IEC. Построение алгоритма инкапсуляции ключа, который можно было бы использовать как Национальный стандарт, на сегодня остается актуальной проблемой. Украинские криптологи также сейчас работают над таким стандартом. В проекте Национального стандарта инкапсуляции ключа предложено использовать модифицированную схему шифрования на эллиптических кривых (ECIES), включенную в стандарты ANSI X9.63, ISO / IEC 18033-2, IEEE 1363a и SECG SEC1.

В работе предлагается некоторый альтернативный алгоритм шифрования на эллиптических кривых, который также можно использовать для инкапсуляции ключей.

Для инкапсуляции ключа можно использовать произвольный асимметричный алгоритм шифрования. Одним из самых простых таких алгоритмов является алгоритм Эль-Гамаля. Но, для использования этого алгоритма на эллиптических кривих, нужно сначала вложить ключ в некоторую точку эллиптической кривой, а затем выполнить обратное преобразование. Во многих работах, как по теории чисел, так и по криптологии, рассматривалась проблема построения детерминированного отображения элементов поля в точке эллиптической кривой, однако только в 2016 г. удалось построить алгоритм вложения геш-значения в точку кривой, до этого же существовали только вероятностные алгоритмы was proposed. Отметим, что алгоритм вложения ключа построить сложнее, поскольку соответствующее отражение должно быть биективним.

Показано, как можно построить такой алгоритм вложения ключа, а также обговорены проблемы, которые возникают при его использовании в качестве составляющей алгоритма инкапсуляции ключа.

Ключевые слова: алгоритм инкапсуляции ключа; алгоритм Эль-Гамаля; эллиптическая кривая.

Библиогр.: 9 назв.

UDC 621.391.15:519.7

Analysis of possibility to use El Gamal algorithm with deterministic embedding for key encapsulation / *O.V. Tsygankova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 201 – 205.

Suppose some parties, A and B, use some symmetrical encryption algorithm (for example, AES) to encrypt their messages from A to B and from B to A. They get their secret keys from some Trusted Authority (TA). TA generates keys and then delivers them to correspondent users. The simplest and, may be, the optimal way to deliver the secret key to user A is to encrypt it (using some asymmetrical encryption algorithm) with A's public key and then to send it to A via public channel. Such procedure is called "key encapsulation".

Key encapsulation algorithms are widely used in the modern cryptography and represented in national and ISO/IEC standards of key encapsulations. Building the key encapsulation algorithm, which may be used as a national standard, is an actual problem nowadays. Ukrainian cryptographers are also working on such standard. Modified Elliptic Curve Integrated Encryption Scheme (ECIES), included in the ANSI X9.63, ISO/IEC 18033-2, IEEE 1363a and SECG SEC1 standards, was used in the project of national standard for key encryption.

In this article we propose some alternative encryption algorithm on elliptic curve which also may be used for this purpose.

Generally speaking we can use arbitrary asymmetric encryption algorithm for key encapsulation. One of the simplest and preferable algorithms is El Gamal encryption algorithm. To use this algorithm on elliptic curve, we need algorithms for embedding key into point on elliptic curve and for retrieving it back. Several lines of work in both the number theory and cryptography literature have considered the problem of deterministically mapping field element to point on elliptic curve. However, only probabilistic algorithms of such embedding existed until 2016, when deterministic algorithm for hash embedding was proposed. But key embedding is much more complicated procedure than hash embedding, because the correspondent mapping must be bijection.

In what follows we describe how this algorithm for key embedding can be built and then discuss the problems that appear if we want to use it in key encapsulation.

Key words: key encapsulation algorithm; El Gamal algorithm; elliptic curve.

Ref.: 9 items