РЕФЕРАТЫ РЕФЕРАТИ ABSTRACTS

ПЕРСПЕКТИВНЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ И ИХ ПРИМЕНЕНИЕ

ПЕРСПЕКТИВНІ КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ ТА ЇХ ЗАСТОСУВАННЯ

PERSPECTIVE CRYPTOGRAPHIC TRANSFORMATIONS AND THEIR APPLICATION

УДК 004.056.55

Алгоритмы асимметричного шифрования и инкапсуляции ключей постквантового периода 5-7 уровней стойкости и их применение / *И.Д. Горбенко, О.Г. Качко, А.Н. Олексейчук, А.А. Кузнецов, Ю.И. Горбенко, В.В. Онопрієнко, М.В. Есина, С.А. Кандий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2019. Вып. 198. С. 5 – 18.

Подаются и рассматриваются построенные алгоритмы асимметричного шифрования и инкапсуляции ключей в кольцах полиномов (алгебраических решетках), анализируется сущность криптографических преобразований асимметричного шифрования и протоколов инкапсуляции ключей, которые применяемых. Рассматриваются механизмы шифрования и инкапсуляции с различными наборами параметров, определяющих устойчивость.

Ключевые слова: асимметричный шифр; инкапсуляция ключей; постквантовый период; уровни стойкости.

Табл. 6. Библиогр.: 17 назв.

УДК 004.056.55

Алгоритми асиметричного шифрування та інкапсуляції ключів постквантового періоду 5-7 рівнів стійкості та їх застосування / *І.Д. Горбенко, О. Г. Качко, А. М. Олексійчук, О.О.Кузнєцов, Ю.І. Горбенко, В.В.Онопрієнко, М. В. Єсіна, С. О. Кандій* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 5 – 18.

Подаються та розглядаються побудовані алгоритми асиметричного шифрування та інкапсуляції ключів в кільцях поліномів (алгебраїчних решітках), аналізується сутність криптографічних перетворень асиметричного шифрування та протоколів інкапсуляції ключів, що застосовуються. Розглядаються механізми шифрування та інкапсуляції з різними наборами параметрів, що визначають стійкість.

Ключові слова: асиметричний шифр; інкапсуляція ключів; постквантовий період; рівні стійкості.

Табл. 6. Бібліогр.: 17 назв.

UDC 004.056.55

Algorithms of asymmetric encryption and encapsulation of keys of post-quantum period of 5 -7 stability stability levels and their applications / *I.D. Gorbenko, O.G. Kachko, O.M. Oleksijchuk, O.O. Kuznetsov, Yu.I. Gorbenko, V.V. Onoprienko, M.V. Yesina, S.O. Kandy* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. №198. P. 5 – 18.

The asymmetric encryption and keys encapsulation in polynomial rings (algebraic lattices) built algorithms are presented and considered, the essence of used asymmetric encryption transformations and key encapsulation protocols are analyzed. Encryption and encapsulation mechanisms with different sets of parameters that determine stability are considered.

Key words: asymmetric cipher; key encapsulation; post-quantum period; stability levels.

6 tab. 17 items.

УДК 004.056.5

Стеганоаналитический метод, эффективный в условиях малой пропускной способности скрытого канала связи / *И.И. Бобок, А.А. Кобозева* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2019. Вып. 198. С. 19 – 31.

Одним из основных стеганографических методов, используемых при организации скрытого канала связи, остается на сегодняшний день метод модификации наименьшего значащего бита (LSB-method). Возможной особенностью современного использования LSB-метода является малая пропускная способность организуемого с его помощью скрытого канала связи. В таких условиях подавляющее большинство существующих стеганоаналитических методов являются малоэффективными. В работе на основе теории возмущений и матричного анализа разработан новый стеганоаналитический метод выявления наличия вложенной методом модификации наименьшего значащего бита дополнительной информации в цифровое изображение, эффективный в условиях малой пропускной способности скрытого канала связи. Основой метода является анализ нормированной отделенности максимальных сингулярных чисел непересекающихся блоков матрицы изображения, полученных путем ее стандартного разбиения. Показано, что для цифровых изображений, хранимых в формате без потерь, при их пересохранении в формат с потерями с различными коэффициентами качества будет иметь место монотон-

ное возрастание количества блоков, для которых увеличивается нормированная отделенность максимального сингулярного числа блока, с уменьшением коэффициента качества, используемого при сжатии исходного изображения. Указанная монотонность будет нарушаться в случае, когда пересохранению с потерями подвергается изображение, которое первоначально хранилось в формате с потерями. Сделанный вывод является основой для разработанного стеганоаналитического метода и реализующего его алгоритма, являющегося полиномиальным степени 2. Предложенный алгоритм превосходит по эффективности существующие аналоги в условиях пропускной способности скрытого канала связи меньше 0,1 бит/пиксель, эффективен как для цветных, так и для монохромных изображений. Выводы подтверждаются приведенными результатами вычислительного эксперимента, в котором было задействовано более 5000 цифровых изображений.

Ключевые слова: стеганоаналитический метод; цифровое изображение; малая пропускная способность скрытого канала связи; сингулярные числа; отделенность сингулярного числа; метод модификации наименьшего значащего бита.

Табл. 6. Ил. 4. Библиогр.: 28 назв.

УДК 004.056.5

Стеганоаналітичний метод, ефективний в умовах малої пропускної спроможності прихованого каналу зв'язку / *І.І. Бобок, А.А. Кобозєва* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 19 – 31.

Одним з основних стеганографічних методів, що використовуються при організації прихованого каналу зв'язку, залишається на сьогоднішній день метод модифікації найменшого значущого біта (LSB-method). Можливою особливістю сучасного використання LSB-метода є мала пропускна спроможність прихованого каналу зв'язку, що організується з його допомогою. У таких умовах переважна більшість існуючих стеганоаналітичних методів є малоефективними. У роботі на основі теорії збурень і матричного аналізу розроблений новий стеганоаналітичний метод виявлення наявності вбудованої методом модифікації найменшого значущого біта додаткової інформації в цифрове зображення, ефективний в умовах малої пропускної спроможності прихованого каналу зв'язку. Основою методу є аналіз нормованої відокремленості максимальних сингулярних чисел непересічних блоків матриці зображення, отриманих шляхом її стандартної розбивки. Показано, що для цифрових зображень, збережених у форматі без втрат, при їхнім перезбереженні у формат із втратами з різними коефіцієнтами якості буде мати місце монотонне зростання кількості блоків, для яких збільшується нормована відокремленість максимального сингулярного числа блоку, зі зменшенням коефіцієнта якості, використовуваного при стиску вхідного зображення. Зазначена монотонність буде порушуватися у випадку, коли перезбереженню із втратами піддається зображення, яке спочатку зберігалося у форматі із втратами. Зроблений висновок є основою для розробленого стеганоаналітичного методу і алгоритму, що його реалізує, який є поліноміальним ступеня 2. Запропонований алгоритм перевищує по ефективності існуючі аналоги в умовах пропускної спроможності прихованого каналу зв'язку менше 0,1 біт/піксель, є ефективним як для кольорових, так і для монохромних зображень. Висновки підтверджуються наведеними результатами обчислювального експерименту, у якому було задіяне більш 5000 цифрових зображень.

Ключові слова: стеганоаналітичний метод; цифрове зображення; мала пропускна спроможність прихованого каналу зв'язку; сингулярні числа; відокремленість сингулярного числа; метод модифікації найменшого значущого біта.

Табл. 6. Іл. 4. Бібліогр.: 28 назв.

UDC 004.056.5

Steganalysis method efficient for the hidden communication channel with low capacity / *I.I. Bobok, A.A. Kobozeva //* Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. №198. P. 19 – 31.

The Least Significant Bit (the LSB-method) remains one of the main steganalysis methods used nowadays for the hidden communication channel organization. One of the features of the current use of the LSB method is an organizing of the hidden communication channel with low capacity. Under such conditions, the vast majority of existing steganalysis methods is ineffective. This paper is dedicated to the development of a new steganalysis method for detection of additional information in digital images embedded by the least significant bit modification. The method is based on the perturbation theory and matrix analysis and effective under the low capacity of the hidden communication channel. This method is based on the analysis of the normalized gap of maximum singular numbers for non-intersecting blocks of an image matrix, obtained by its standard splitting. It is shown that conversion of a digital image from the lossless format to the lossy format with different quality factors will lead to a monotonous increase in the number of blocks for which the normalized gap of block's maximum singular number increases with a decrease in the quality factor used in compression of the source image. This monotony will be broken in the case when the image originally stored in lossy format is being re-stored in lossy format. The conclusion made is the basis for the developed steganalysis method and the algorithm that implements it, which has polynomial complexity of degree 2. The proposed algorithm exceeds in efficiency the existing analogues when the embedding rate is less then 0.1 bits per pixel and effective for color and grayscale images. The conclusions are confirmed by the given results of a computational experiment, which have involved more than 5,000 digital images.

Key words: steganalysis method; digital image; low capacity of the hidden communication channel; singular numbers; singular number gap; the Least Significant Bit method.

6 tab. 4 fig. Ref.: 28 items.

УДК 681.3.06:519.248.681

Математическая модель сигналов с ортогональным частотным разделением и мультиплексированием (OFDM) / *И.Д. Горбенко, А.А. Замула, В.Л. Морозов, С.В. Родионов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2019. Вып. 198. С. 32 – 43.

Рассматриваются проблемные вопросы построения помехозащищенных систем связи на основе использования технологии мультиплексирования сигналов с ортогональным частотным разделением каналов (OFDM). Предоставлено описание технологии формирования сигналов с OFDM, используемых в системах связи и телекоммуникаций, а также приводится анализ перспективных технологий, которые могут найти применение в системах широкополосной беспроводной связи с множеством несущих, к которым предъявляются повышенные требования по информационной безопасности, помехоустойчивости приема сигналов, скорости приема-передачи данных. Основной целью публикации является достаточно детальное рассмотрение некоторых проблем, связанных с разработками физически систем OFDM, получение математических моделей преобразований при реализации OFDM. Особое внимание при этом обращается на возможности обмена между качественными характеристиками системы связи и ее сложностью.

Ключевые слова: помехозащищенность; информационная безопасность; широкополосный доступ; сигнал; целостность; модуляция; преобразование Фурье; частотное разделение.

Ил. 6. Библиогр.: 13 назв.

УДК 681.3.06:519.248.681

Математична модель сигналів з ортогональним частотним розподілом і мультиплексуванням (OFDM) / *І.Д. Горбенко, О.А. Замула, В.Л. Морозов, С.В Родіонов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 32 – 43.

Розглядаються проблемні питання побудови завадозахищених систем зв’язку на основі використання технології мультиплексування сигналів з ортогональним частотним розділенням каналів (OFDM). Надано опис технології формування сигналів з OFDM, що використовуються в системах зв'язку і телекомунікацій, а також наводиться аналіз перспективних технологій, які можуть знайти застосування в системах широкосмугового бездротового зв'язку з багатьма несійними, до яких висуваються підвищені вимоги щодо інформаційної безпеки, завадостійкості прийому сигналів, швидкості прийому-передачі даних. Основною метою публікації є достатньо детальний розгляд деяких проблем, пов'язаних з розробками на фізичному рівні систем OFDM, отримання математичних моделей перетворень при реалізації OFDM. Особу увагу при цьому звертається на можливості обміну між якісними характеристиками системи зв'язку і її складністю.

Ключові слова: завадо захищеність; інформаційна безпека; широкосмуговий доступ; сигнал; цілісність; модуляція; перетворення Фур’є; частотне розділення.

Іл. 6. Бібліогр.: 13 назв.

UDC 681.3.06:519.248.681

Mathematical model of orthogonal frequency distribution and multiplexing (OFDM) signals / *I.D. Gorbenko, O.A. Zamula, V.L. Morozov, S.V. Rodionov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. №198. P. 32 – 43.

The problematic issues of building noise immunity systems based on the use of orthogonal frequency division-division (OFDM) signal multiplexing are considered. The description of OFDM signaling technology used in telecommunication and telecommunication systems is given, as well as the analysis of promising technologies that can be used in multi-carrier broadband wireless systems, which have high requirements for information security, noise immunity signal reception, data rate. The main purpose of the publication is a sufficiently detailed discussion of some of the problems associated with the development at the physical level of OFDM systems, obtaining mathematical models of transformations in the implementation of OFDM. Particular attention is paid to the possibility of exchange between the quality characteristics of the communication system and its complexity.

Key words: noise immunity; information security; broadband access; signal; integrity; modulation; Fourier transform; frequency division.

6 fig. Ref.: 13 items.

УДК 004.056.5

Алгоритмы криптографического хеширования, которые применяются в современных блокчейн-системах / *А.А. Кузнецов, Ю.И. Горбенко, В.В. Оноприенко, И.В. Стельник, Д.В. Мялковский* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2019. Вып. 198. С. 44 – 53.

Проводится анализ функций хеширования, которые применяются или могут применяться в различных блокчейн-системах. В частности, рассматриваются наиболее распространенные национальные и международные стандарты, в которых приведены спецификации всемирно известных алгоритмов криптографического хеширования, и исследуются различные проекты по построению децентрализованных блокчейн-систем, где эти функции могут быть применены.

Ключевые слова: хеширования; криптографический алгоритм; блокчейн; криптовалюта.

Табл. 2. Ил. 1. Библиогр.: 31 назв.

УДК 004.056.5

Алгоритми криптографічного гешування, які застосовуються в сучасних блокчейн-системах / *О.О. Кузнецов, Ю.І. Горбенко, В.В. Онопрієнко, І.В. Стельник, Д.В. Мялковський* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 44 – 53.

Проводиться аналіз функцій гешування, які застосовуються або можуть застосовуватися в різних блокчейн-системах. Зокрема, розглядаються найбільш поширені національні та міжнародні стандарти, в яких наведено специфікацію всесвітньо відомих алгоритмів криптографічного гешування, та досліджуються різні проекти з побудови децентралізованих блокчейн-систем, де ці функції можуть бути застосовані.

Ключові слова: гешування; криптографічний алгоритм; блокчейн; криптовалюта.

Табл. 2. Іл. 1. Бібліогр.: 31 назв.

UDC 004.056.5

Cryptographic hashing algorithms used in modern blockchain systems / *A.A. Kuznetsov, Yu.I. Gorbenko, V.V. Onoprienko, I.V. Stelnik, D.V. Myalkovsky* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. №198. P. 44 – 54.

The analysis of hashing functions that are applied or can be used in various blockchain systems is carried out. In particular, the most common national and international standards are considered, which contain specifications of world-famous cryptographic hashing algorithms, and various projects for the construction of decentralized blockchain systems where these functions can be applied are investigated.

Key words: hashing; cryptographic algorithm; blockchain; cryptocurrency.

2 tab. 1fig. Ref.: 31 items.

УДК 004.056.5

Исследование алгоритмов криптографического хеширования, которые применяются в современных блокчейн-системах / *А.А. Кузнецов, Ю.И. Горбенко, В.В. Ономриенко, И.В. Стельник, Д.В. Мялковский* // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2019. Вып. 198. С. 54 – 74.

Исследуются современные алгоритмы хеширования, которые применяются или могут применяться в различных блокчейн-системах. В частности, рассматриваются наиболее распространенные и применяемые алгоритмы криптографического хеширования, которые стандартизированы на международном и национальном уровнях, а также алгоритмы, хотя и не стандартизированные, но которые применяются в большинстве современных децентрализованных системах, построенных по технологии блокчейн.

Ключевые слова: хеширование; криптографический алгоритм; блокчейн; криптовалюта.

Табл. 1. Библиогр.: 94 назв.

УДК 004.056.5

Дослідження алгоритмів криптографічного гешування, які застосовуються в сучасних блокчейн-системах / *О.О. Кузнецов, Ю.І. Горбенко, В.В. Онопрієнко, І.В. Стельник, Д.В. Мялковський* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 54 – 74.

Досліджуються сучасні алгоритми гешування, які застосовуються або можуть застосовуватися в різних блокчейн-системах. Зокрема, розглядаються найбільш поширені та застосовувані алгоритми криптографічного гешування, які стандартизовані на міжнародному та національному рівнях, а також алгоритми, які хоча і не стандартизовані, але застосовуються у більшості сучасних децентралізованих системах, побудованих за технологією блокчейн.

Ключові слова: гешування; криптографічний алгоритм; блокчейн; криптовалюта.

Табл. 1. Бібліогр.: 94 назв.

UDC 004.056.5

The study of cryptographic hashing algorithms used in modern blockchain systems / *A.A. Kuznetsov, Yu.I. Gorbenko, V.V. Onoprienko, I.V. Stelnik, D.V. Myalkovsky* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. №198. P. 54 – 74.

Modern hashing algorithms that are or can be used in various blockchain systems are studied in this work. In particular, the most common and used cryptographic hashing algorithms are considered, which are standardized at the international and national levels, as well as algorithms, although not standardized, but used in most modern decentralized systems built on blockchain technology.

Key words: hashing; cryptographic algorithm; blockchain; cryptocurrency.

1 tab. Ref.: 94 items.

УДК 004.056.5

Исследование быстродействия и статистической безопасности алгоритмов криптографического хеширования / *А.А. Кузнецов, В.А. Тимченко, К.Е. Лисицкий, М.Ю. Родинко, М.С. Луценко, К.Ю. Шеханин, А.А. Колгатин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2019. Вып. 198. С. 75 – 95.

Проводятся сравнительные исследования алгоритмов криптографического хеширования, которые применяются (или могут применяться) в современных децентрализованных блокчейн системах. В частности исследуется быстродействие хеширования на разных десктопных системах, оценивается количество тактов вычисли-

тельной системы на один байт (Cycles / byte), объем гешованого сообщения за одну секунду (MB / s) и количество сформированных хеш-кодов в секунду (KHash / s). Дополнительно исследуется быстродействие отдельных криптографических функций хеширования на графических вычислителях. Для оценки статистической безопасности исследуются исходные последовательности криптографических функций хеширования при обработке ими чрезмерных входных данных (которые сформированы с помощью обычного счетчика). Для сравнительных исследований показателей статистической безопасности используется методика NIST STS (Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications), которая рекомендована Национальным институтом стандартов и технологий США для исследования генераторов случайных и псевдослучайных чисел для криптографических приложений.

Ключевые слова: хеширование; быстродействие; криптографический алгоритм; блокчейн; криптовалюта.

Табл. 5. Ил. 42. Библиогр.: 21 назв.

УДК 004.056.5

Дослідження швидкодії та статистичної безпеки алгоритмів криптографічного гешування / *О.О. Кузнецов, В.А. Тимченко, К.Є. Лисицький, М.Ю. Родінко, М.С. Луценко, К.Ю. Шеханін, А.О. Колгатін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 75 – 95.

Проводяться порівняльні дослідження алгоритмів криптографічного гешування, які застосовуються (або можуть застосовуватися) в сучасних децентралізованих блокчейн системах. Зокрема досліджується швидкодія гешування на різних десктопних системах, оцінюється кількість тактів обчислювальної системи на один байт (Cycles/byte), обсяг гешованого повідомлення за одну секунду (MB/s) та кількість сформованих геш-кодів за секунду (KHash/s). Додатково досліджується швидкодія окремих криптографічних функцій гешування на графічних обчислювачах. Для оцінки статистичної безпеки досліджуються вихідні послідовності криптографічних функцій гешування при обробці ними надмірних вхідних даних (які сформовано за допомогою звичайного лічильника). Для порівняльних досліджень показників статистичної безпеки використовується методика NIST STS (Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications), яку рекомендовано Національним інститутом стандартів і технологій США для дослідження генераторів випадкових і псевдовипадкових чисел для криптографічних застосувань.

Ключові слова: гешування; швидкодія; криптографічний алгоритм; блокчейн; криптовалюта.

Табл. 5. Іл. 42. Бібліогр.: 21 назв.

UDC 004.056.5

The study of the speed and statistical security of cryptographic hashing algorithms / *A.A. Kuznetsov, V.A. Timchenko, K.E. Lisitzky, M.Yu. Rodinko, M.S. Lutsenko, K.Yu. Shehanin, A.A.* // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. 2019. №198. P. 75 – 95.

Comparative studies of cryptographic hashing algorithms are being carried out, which are used (or can be applied) in modern decentralized blockchain systems. In particular, hashing speed of action is studied on different desktop systems, the number of clock cycles of the computing system per byte (Cycles / byte), the volume of the hashed message per second (MB / s) and the number of generated hash codes per second (KHash / s) are estimated. Additionally, the speed of action speed of action of individual cryptographic hashing functions on graphical computers is investigated. To evaluate statistical security, we study the initial sequences of cryptographic hash functions when they process excessive input data (which are generated using a conventional counter). For comparative studies of statistical security indicators, the NIST STS (Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications) technique is used, which is recommended by the National Institute of Standards and Technology for the study of random and pseudorandom number generators for cryptographic applications.

Key words: hashing; speed of action performance; cryptographic algorithm; blockchain; cryptocurrency.

5 tab. 42 fig. Ref.: 21 items.

АНАЛИЗ И ИСПОЛЬЗОВАНИЕ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ В ДЕЦЕНТРАЛИЗОВАННЫХ ТЕХНОЛОГИЯХ

АНАЛІЗ ТА ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ МЕТОДІВ В ДЕЦЕНТРАЛІЗОВАНИХ ТЕХНОЛОГІЯХ

ANALYSIS AND USE OF CRYPTOGRAPHIC METHODS IN DECENTRALIZED TECHNOLOGIES

УДК 004.056.5

Установление протоколов доверия в сети взаимного недоверия путем формирования консенсуса / *Е.В. Исирова, А.В. Потий, Jens Christian Claussen* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2019. Вып. 198. С. 96 – 104.

Любое взаимодействие между субъектами происходит через сети связей между ними. Важной целью является обеспечение безопасности таких взаимодействий, особенно при появлении технологий квантовых вычислений. Возможно, что в постквантовом периоде наиболее выгодными архитектурами сетей для проведения верификации будут именно распределенные. В работе приводится обоснование данного вопроса, подробно

проводится аналогия между распределенным формированием доверия согласно предложенным протоколам и формированием консенсуса в социальных сетях для различных топологий сетей. Иерархические сети в обеих областях демонстрируют самые медленные временные рамки формирования консенсуса. Сделан вывод, что это может служить аргументом в пользу создания механизмов распределенных протоколов, где важна масштабируемость с размером сети.

Ключевые слова: Формирование консенсуса в социальных сетях; voter model; формирования консенсуса в компьютерных сетях; иерархическая инфраструктура открытых ключей; распределенная инфраструктура открытых ключей; распределенные протоколы верификации; постквантовый период; технология Blockchain.

Іл. 7. Бібліогр.: 17 назв.

УДК 004.056.5

Встановлення протоколів довіри в мережі взаємної недовіри шляхом формування консенсусу / *К.В. Ісірова, О.В. Потій, Jens Christian Claussen* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 96 – 104.

Будь-яка взаємодія між суб'єктами відбувається через мережі зв'язків між ними. Важливою метою є забезпечення безпеки таких взаємодій, особливо при появі технологій квантових обчислень. Можливо, що в постквантовому періоді найбільш вигідними архітектурами мереж для проведення верифікації будуть саме розподілені. У роботі наведено обґрунтування даного питання, докладно проведено аналогію між розподіленим формуванням довіри згідно із запропонованими протоколам і формуванням консенсусу в соціальних мережах для різних топологій мереж. Ієрархічні мережі в обох областях демонструють самі повільні тимчасові рамки формування консенсусу. Зроблено висновок, що це може служити аргументом на користь створення механізмів розподілених протоколів, де важлива масштабованість з розміром мережі.

Ключові слова: Формування консенсусу в соціальних мережах; voter model; формування консенсусу в комп'ютерних мережах; ієрархічна інфраструктура відкритих ключів; розподілена інфраструктура відкритих ключів; розподілені протоколи верифікації; постквантовий період; технологія Blockchain.

Іл. 7. Бібліогр.: 17 назви.

UDC 004.056.5

Establishing trust protocols in mutual distrust network by consensus formation / *K. Isirova, O. Potii, J. Claussen* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. №198. P. 96 – 104.

Any interactions between actors take place through networks of connections between them. An important goal is to ensure the security of such interactions, especially in advent of quantum computing technologies. It might be that in the post-quantum world, the avatar of verification architectures will be manifested through distributed protocols. Here we augment the discussion by explicitely drawing the analogy between distributed protocol consensus formation and consensus formation in social networks in various topologies. Hierarchical networks, in both domains, exhibit slowest timescale of consensus formation. We conclude this supports universal argument towards establishment of distributed protocol mechanisms, wherever the scaleability with network size is of relevance.

Key words: Consensus Formation in Social Networks; Voter Model; Trust Formation in Computer networks; Hierarchical PKI; Distributed PKI; Distributed Verification Protocols; Post-quantum Period; Blockchain Technology.

7 fig. Ref.: 17 items.

УДК 004.773.2

Метод сравнения Proof of Work алгоритмов консенсуса / *М.О. Осадчук, Р.В. Олейников* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2019. Вып. 198. С. 105 – 112.

Алгоритм консенсуса представляет собой наиболее важную часть любой блокчейн системы. Существует множество алгоритмов консенсуса, которые разработчики могут использовать для своих решений, однако принятие такого решения не может быть полностью формализировано из-за неопределенности в требованиях и среде приложения. Предложен метод, который позволяет выбрать наиболее оптимальный Proof of Work алгоритм консенсуса для новых блокчейн-систем, который основан на процессе анализа иерархий. Применение этого метода для разных PoW алгоритмов и привлечение независимых экспертов позволяет выбрать dPoW в качестве наилучшего решения для существующих условий.

Ключевые слова: блокчейн; алгоритм консенсуса; децентрализованные вычисления; Proof of Work; атака двойной траты.

Табл. 7. Библиогр.: 25 назв.

УДК 004.773.2

Метод порівняння Proof of Work алгоритмів консенсусу / *М.О. Осадчук, Р.В. Олійников* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 105 – 112.

Алгоритм консенсусу є найбільш важливою частиною будь-якої блокчейн-системи. Існує багато алгоритмів консенсусу, які розробники можуть використовувати для своїх рішень, але прийняття такого рішення не може бути повністю формалізованим через невизначеність у вимогах та у середовищі додатку. Ми запропонували метод, який дозволяє обрати оптимальний Proof of Work алгоритм консенсусу для новостворених блокчейн-систем, який заснований на процесі аналізу ієрархій. Застосування цього методу для різних PoW алгорит-

мів із залученням незалежних експертів дозволяє обрати dPoW у якості найкращого рішення для існуючих умов.

Ключові слова: блокчейн; алгоритм консенсусу; децентралізовані обчислення; Proof of Work; атака подвійного витрачання.

Табл. 7. Бібліогр.: 25 назв.

UDC 004.773.2

Method of Proof of Work consensus algorithms comparison / *M. Osadchuk, R. Oliynykov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. №198. P. 105 – 112.

A consensus algorithm is the most important part of any blockchain system. There are available various consensus algorithms that developers can utilize in their solutions, and such a decision making cannot be fully formalized due uncertainty in requirements and application environment. We propose a method that allows selecting of an optimal Proof of Work (PoW) consensus algorithm for newly developed blockchain system based on Analytic Hierarchy Process. Application of this method to various PoW algorithms with involvement of independent experts allowed to select dPoW as the best solution for the given conditions.

Key words: blockchain; consensus algorithm; decentralized computation; Proof of Work; double spend attack.

7 tab. Ref.: 25 items.

УДК 004.056.5

Некоторый подход к маскированию данных как средство противодействия угрозе логического вывода / *В.И. Есин, В.В. Вилигура* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2019. Вып. 198. С. 113 – 130.

Цель статьи – раскрытие сути некоторого подхода к маскированию данных, хранящихся в базе данных, как средства противодействия угрозе логического вывода. В основу подхода положены принципы случайной перестановки элементов поля данных столбца строки таблицы производственной базы данных и динамического маскирования. Отличительной особенностью предлагаемого решения является подход к процессу перемешивания данных, а именно, перемешиванию элементов значения данных внутри требуемого поля строки. С помощью данного решения возможно маскирование как всего значения поля столбца строки таблицы, так и его части. Предлагаемый подход отличается от большей части типичных коммерческих инструментов маскирования критических данных тем, что в базе данных выполняются предварительные физические изменения конфиденциальных данных, и эти изменения при необходимости можно отменить пользователем, который имеет соответствующие права на это. Легитимный пользователь получает доступ к конфиденциальным данным за счет возможности осуществить преобразование (перезапись) запроса «на лету», а злоумышленник может только считать хранящиеся в базе заранее измененные определенным образом с сохранением исходного формата данные. Предлагаемый подход к маскированию данных может быть использован как в производственных, так и в непроизводственных базах данных, расширяя возможности, так называемого, статического маскирования данных.

Ключевые слова: безопасность данных; база данных; маскирование данных; конфиденциальные данные.

Табл. 4. Ил. 2. Библиогр.: 34 назв.

УДК 004.056.5

Деякий підхід до маскування даних як засіб протидії загрозі логічного висновку / *В.І. Єсін, В.В. Вілігура* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 113 – 130.

Мета статті – розкриття суті деякого підходу до маскування даних, що зберігаються в базі даних, як засобу протидії загрозі логічного висновку. В основу підходу було покладено принципи випадкової перестановки елементів поля даних стовпця рядка таблиці виробничої бази даних і динамічного маскування. Відмінною особливістю запропонованого рішення є підхід до процесу перемішування даних, а саме – перемішування елементів значення даних всередині потрібного поля рядка. За допомогою даного рішення можливо маскування як всього значення поля стовпця рядка таблиці, так і його частини. Запропонований підхід відрізняється від більшої частини типових комерційних інструментів маскування критичних даних тим, що в базі даних виконуються попередні фізичні зміни конфіденційних даних, і ці зміни при необхідності можна скасувати користувачем, який має відповідні права на це. Легітимний користувач отримує доступ до конфіденційних даних за рахунок можливості здійснити перетворення (перезапис) запиту «на льоту», а зловмисник може тільки зчитувати заздалегідь змінені певним чином зі збереженням вихідного формату дані, що зберігаються в базі. Запропонований підхід до маскування даних може бути використаний як в виробничих, так і в невиробничих базах даних, розширюючи можливості так званого статичного маскування даних.

Ключові слова: безпека даних; база даних; маскування даних; конфіденційні дані.

Табл. 4. Іл. 2. Бібліогр.: 34 назв.

UDC 004.056.5

Some approach to data masking as means to counteract the inference threat / *V.I. Yesin, V.V. Vilihura* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. №198. P. 113 – 130.

The goal of the article is to reveal the essence of some approach to data masking stored in the database as a means to counteract the inference threat. This approach is based on the principles of random permutation of the elements of a

data field of the row column of the production database table data and dynamic masking. A distinctive feature of the proposed solution is the approach to the process of data shuffling, namely, shuffling data value elements within the demanded row field. It is possible to mask both an entire value of the field of the table row column and its part using this solution. The proposed approach differs from most of the typical commercial tools for masking sensitive data in that a preliminary physical change of sensitive data is made in the production database, and a user who has the appropriate rights can cancel these changes if it is necessary. The legitimate user in the proposed approach gets access to sensitive data due to the ability to transform (rewrite) the query "on the fly", and the attacker can only read the previously modified data that is stored in the database. The proposed approach to data masking can be used in both production and non-production databases, expanding the possibilities of so-called static data masking.

Key words: data security; database; data masking; sensitive data.

4 tab. 2 fig. Ref.: 34 items.

УДК 004.056.55

Современные проблемы централизованных технологий типа «клиент-сервер» и возможности их усовершенствования на основе децентрализации / *Ю.И. Горбенко, М.В. Есина, Д.В. Мялковский, О.С. Акользина, В.А. Пономарь* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2019. Вып. 198. С. 131 – 145.

Приводится анализ основных принципов построения децентрализованных технологий с использованием технологии блокчейн и требования к ним в части безопасности, а также анализ особенностей и условий применения защищенных технологий блокчейн. Описываются и анализируются потенциальные атаки, когда применение блокчейна является существенным механизмом защиты от них. Приводится сущность и предложения относительно противодействия атакам специального вида.

Ключевые слова: децентрализация, информационные технологии, клиент-серверная технология, централизованная технология.

Табл. 5. Ил. 1. Библиогр.: 28 назв.

УДК 004.056.55

Сучасні проблеми централізованих технологій типу «клієнт – сервер» та можливості їх удосконалення на основі децентралізації / *Ю.І. Горбенко, М.В. Єсіна, Д.В. Мялковський, О.С. Акользіна, В.А. Пономарь* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 131 – 145.

Наводиться аналіз основних принципів побудування децентралізованих технологій з використанням технології блокчейн та вимоги до них в частині безпеки, а також аналіз особливостей та умов застосування захищених технологій блокчейн. Описуються та аналізуються потенційні атаки, коли застосування блокчейну є суттєвим механізмом захисту від них. Наводиться сутність та пропозиції відносно протидії атакам спеціального виду.

Ключові слова: децентралізація, інформаційні технології, клієнт-серверна технологія, централізована технологія.

Табл. 5. Іл. 1. Бібліогр.: 28 назв.

UDC 004.056.55

Modern problems of centralized technologies of the client-server type and possibilities of their improvement on the basis of decentralization / *Yu.I. Gorbenko, M.V. Yesina, D.V. Myalkovskiy, O.S. Akolzina, V.A. Ponomar* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. №198. P. 131 – 145.

The paper analyzes the basic principles of building decentralized technologies with the use of blockchain technology and their requirements in terms of security, as well as the analysis of the features and conditions of the use of secure blockchain technologies. Potential attacks are described and analyzed when the use of blockchain is a significant defense mechanism against them. The essence and suggestions concerning counteraction to attacks of a special kind are given.

Key words: decentralization, information technology, client-server technology, centralized technology.

5 tab. 1 fig. Ref.: 28 items.

УДК 004.056.5

Моделирование атаки двойной траты на протокол консенсуса «Proof of work» / *Н.А. Полуяненко, А.А. Кузнецов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2019. Вып. 198. С. 146 – 161.

Проведен критический анализ известных аналитических оценок вероятности успешной реализации атаки двойной траты на протокол консенсуса «Proof of work». В частности, рассмотрена «задача о разорении игрока», показано, что базовые предположения о вероятностном пространстве (множество элементарных исходов и вероятности их наступления) не соответствуют реальным процессам, протекающим при установлении консенсуса «Proof of work» в блокчейн-системе. Предложена модель «независимых игроков», которая устраняет основные неточности и несоответствия. Показана сходимость результатов теоретических расчетов с данными экспериментов по имитации «гонки» между честными игроками и злоумышленниками.

Ключевые слова: блокчейн; протокол консенсуса; атака двойной траты; имитационное моделирование.

Табл. 1. Ил. 11. Библиогр.: 16 назв.

УДК 004.056.5

Моделювання атаки подвійної витрати на протокол консенсусу «Proof of work» / *М.О. Полуяненко, О.О. Кузнецов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 146 – 161.

Проведено критичний аналіз відомих аналітичних оцінок ймовірності успішної реалізації атаки подвійної витрати на протокол консенсусу «Proof of work». Зокрема, розглянуто «завдання про розорення гравця», показано, що базові припущення про імовірнісний простір (безліч елементарних фіналів і ймовірності їх настання) не відповідають реальним процесам, що протікають при встановленні консенсусу «Proof of work» в блокчейн-системі. Запропоновано модель «незалежних гравців», яка усуває основні неточності і невідповідності. Показана збіжність результатів теоретичних розрахунків з даними експериментів з імітації «гонки» між чесними гравцями і зловмисниками.

Ключові слова: блокчейн; протокол консенсусу; атака подвійної витрати; імітаційне моделювання.

Табл. 1. Іл. 11. Бібліогр.: назв.

UDC 004.056.5

Simulation of double spend attack on the “Proof of Work” consensus protocol / *N.A. Poluyanenko, A.A. Kuznetsov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. №198. P. 146 – 161.

A critical analysis of the well-known analytical estimates of the probability of successful implementation of a double-spending attack on the “Proof of work” consensus protocol has been carried out. In particular, the so-called “Player ruin problem” is considered, it is shown that the basic assumptions about the probability space (the set of elementary outcomes and the likelihood of their occurrence) do not correspond to the real processes that occur when the “Proof of work” consensus is established in the blockchain system. A model of “independent players” is proposed, which eliminates the main inaccuracies and inconsistencies. The convergence of the results of theoretical calculations with the data of experiments to simulate the "race" between honest players and attackers is shown.

Key words: blockchain; consensus protocol; double waste attack; simulation modeling.

1 tab. 11 fig. Ref.: 16 items.

УДК 004.056.55

Принципы построения и анализа инфраструктур открытого ключа на основе применения технологии блокчейн / *И.Д. Горбенко, А.В. Потий, Ю.И. Горбенко, А.И. Пушкарёв, М.В. Есина* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2019. Вып. 198. С. 162 – 181.

Обоснованы возможности и необходимость создания инфраструктуры открытых ключей на основе технологии блокчейн. Анализируется усовершенствованная модель инфраструктуры открытых ключей с прозрачностью сертификатов на основе блокчейна, а также основные проблемные вопросы перспективных инфраструктур открытых ключей на базе блокчейна. Проводится общая оценка устойчивости инфраструктуры открытых ключей на основе блокчейна к известным атакам.

Ключевые слова: блокчейн; децентрализация; информационные технологии; технология блокчейн.

Табл. 1. Ил. 3. Библиогр.: 40 назв.

УДК 004.056.55

Принципи побудування та аналізу інфраструктур відкритого ключа на основі застосування технології блокчейн / *І.Д. Горбенко, О.В. Потій, Ю.І. Горбенко, А.І. Пушкарьов, М.В. Єсіна* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 162 – 181.

Наводиться обґрунтування можливостей та необхідності створення інфраструктури відкритих ключів на основі технології блокчейн. Аналізується удосконалена модель інфраструктури відкритих ключів з прозорістю сертифікатів на основі блокчейну, а також основні проблемні питання перспективних інфраструктур відкритих ключів на базі блокчейну. Проводиться загальна оцінка стійкості інфраструктури відкритих ключів на основі блокчейну до відомих атак.

Ключові слова: блокчейн; децентралізація; інформаційні технології; технологія блокчейн.

Табл. 1. Іл. 3. Бібліогр.: 40 назв.

UDC 004.056.55

Principles of building and analyzing public key infrastructures based on the use of blockchain technology / *I.D. Gorbenko, O.V. Potii, Yu.I. Gorbenko, A.I. Pushkarov, M.V. Yesina* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. №198. P. 162 – 181.

The paper provides a rationale for the possibilities and the need to create blockchain-based public key infrastructure. An improved public key infrastructure model with blockchain-based certificate transparency as well as the main problematic issues of promising blockchain-based public key infrastructures are analyzed. A general assessment of the public key infrastructure based on the blockchain stability in conditions of well-known attacks is carried out.

Key words: blockchain, decentralization, information technology, blockchain technology.

1 tab. 3 fig. Ref.: 40 items.

УДК 004.728:004.728.3, 004.056.055

Оптимизация методов синтеза дискретных сложных сигналов в современных многопользовательских системах связи широкополосного доступа / *А.А. Замула* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2019. Вып. 198. С. 182 – 191.

Среди основных направлений улучшения показателей эффективности функционирования информационно-коммуникационных систем (ИКС), в частности помехозащищенности, скрытности, информационной безопасности, можно выделить направления, связанные с применением фазоманипулированных широкополосных сигналов (ФМ ШПС). Многочисленные приложения ИКС указывают на важность периодических автокорреляционной свойств сигналов: дальномерные системы с непрерывным излучением, пилотный канал и канал синхронизации в цифровых системах передачи данных, радарные и сонорные системы и др. Кроме того, хорошая периодическая автокорреляционная функция автокорреляции (АКФ) сигнала указывает на возможность отбора сигналов с хорошими апериодическими АКФ. В данной работе сформулирована и решена задача оптимизации синтеза нелинейных дискретных последовательностей, которые имеют улучшенные ансамблевые, структурные и автокорреляционные свойства. Применение нелинейных дискретных сигналов, образованные на основе таких последовательностей, позволит обеспечить необходимые значения помехозащищенности, информационной и структурной скрытности функционирования ИКС.

Ключевые слова: дискретная последовательность; криптографический сигнал; функция корреляции; конечное поле; база сигнала.

Табл. 2. Ил. 3. Библиогр.: 9 назв.

УДК 004.728:004.728.3, 004.056.055

Оптимізація методів синтезу дискретних складних сигналів у сучасних багатокористувачевих системах зв'язку широкосмугового доступу / *О.А. Замула* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 182 – 191.

Серед основних напрямків покращення показників ефективності функціонування інформаційно-комунікаційних систем (ІКС), зокрема завадозахищеності, скритності, інформаційної безпеки, можна виділити напрямки, пов'язані із застосуванням фазоманіпульованих широкосмугових сигналів (ФМ ШПС). Чисельні додатки ІКС вказують на важливість періодичних автокореляційних властивостей сигналів: дальномірні системи з безперервним випромінюванням, пілотний канал і канал синхронізації в цифрових системах передачі даних, радарні і сонорні системи і ін. Крім того, хороша періодична автокореляційна функція автокореляції (АКФ) сигналу вказує на можливість відбору сигналів з хорошими аперіодичними АКФ. У даній роботі сформульована і вирішена задача оптимізації синтезу нелінійних дискретних послідовностей, які мають покращені ансамблеві, структурні і автокореляційні властивості. Застосування нелінійних дискретних сигналів, які утворені на основі таких послідовностей, дозволить забезпечити необхідні значення завадозахищеності, інформаційної та структурної скритності функціонування ІКС.

Ключові слова: дискретна послідовність; криптографічний сигнал; функція кореляції; кінцеве поле; база сигналу.

Табл. 2. Іл. 3. Бібліогр.: 9 назв.

UDC 004.728:004.728.3, 004.056.055

Optimization of the method for the synthesis of discrete folding signals in the most common bag-box-and-bag systems / *A.A. Zamula* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. №198. P. 182 – 191.

Among the main areas of improvement of the performance indicators of information and communication systems (ICS), in particular, noise immunity, secrecy, and information security, it is possible to identify the areas associated with the use of phase-manipulated broadband signals (FM SHPS). Numerous ICS applications point to the importance of periodic autocorrelation properties of the signals used: continuous-beam systems with continuous radiation, pilot channel and channel of synchronization in digital data systems, radar and sonar systems, and others. In addition, a good periodic AKF signal indicates the ability to select signals with good aperiodic ACF. The minimization of the level of the side petals of the AKF is of greatest importance when designing a signal for such applications as measuring the lag time, time resolution, etc. In this paper, the problem of optimizing the synthesis of nonlinear discrete sequences, which have improved ensemble, structural and autocorrelation properties, is formulated and solved. The use of nonlinear discrete signals, which are formed on the basis of such sequences, will provide the necessary values of impedance protection, information and structural secrecy of the operation of the ICS.

Key words: discrete sequence; cryptographic signal; correlation function; isomorphism; finite field; base of signal.

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

УДК 004.491.4

Метод преодоления средств защиты с использованием уязвимостей графических файлов формата BMP / *Р.С. Гринев, А.В. Северинов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2019. Вып. 198. С. 192 – 202.

Цель статьи – исследование уязвимостей современных систем защиты от атак с использованием графических файлов формата BMP. Рассматриваются особенности изображений формата BMP, способ их использования для внедрения компьютерных вирусов и проведения атак с целью преодоления средств защиты. Проанали-

зирована эффективность предложенного метода сокрытия компьютерных вирусов по сравнению с известными, показана возможность преодоления средств защиты.

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

Табл. 3. Ил. 23. Библиогр.: 11 назв.

УДК 004.491.4

Метод подолання засобів захисту з використанням вразливостей графічних файлів формату BMP / *Р.С. Гриньов, О.В. Сєвєрінов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 192 – 202.

Мета статті – дослідження вразливостей сучасних систем захисту від атак з використанням графічних файлів формату BMP. Розглядаються особливості зображень формату BMP, спосіб їх використання для впровадження комп'ютерних вірусів та проведення атак з метою подолання засобів захисту. Проаналізована ефективність запропонованого методу приховування комп'ютерних вірусів в порівнянні з відомими, показана можливість подолання засобів захисту.

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

Табл. 3. Іл. 23. Бібліогр.: 11 назв.

UDC 004.491.4

The method of overcoming protection using vulnerabilities of graphic files in BMP / *R.S. Grynov, A.V. Severinov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. №198. P. 192 – 202.

The aim of the article – study attacks on modern protection systems by using vulnerabilities of BMP image files. This article describes the features of BMP format images. The method of injecting computer viruses in BMP image and attacks in order to overcome the means of protection. The analysis of the efficiency of the proposed method of hiding computer viruses in comparison with the known ones showed the possibility of overcoming the means of protection.

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

3 tab. 23 fig. Ref.: 11 items.

УДК 004.056

Сравнительный анализ криптопреобразований на эллиптических кривых и кривых Эдвардса / *В.А. Кулибаба* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2019. Вып. 198. С. 203 – 208.

Выполнен сравнительный анализ основных преобразований на канонических эллиптических кривых и кривых Эдвардса. Приведены сравнения производительности групповых операций в группах точеки эллиптических кривых и кривых Эдвардса. Показана возможность использовать алгоритм Полларда для криптоанализа кривых Эдвардса, а также ускорение генерации последовательности для алгоритма ро-Поларда для кривых Эдвардса, что позволяет ускорить выполнение криптоанализа. Предложена оценка стойкости кривых Эдвардса против атаки типа «полное раскрытие» с использованием дискретного логарифма в группе точек кривых Эдвардса.

Ключевые слова: эллиптические кривые, кривые Эдвардса, криптоанализ, цифровая подпись.

Табл. 1. Библиогр.: 7 назв.

УДК 004.056

Порівняльний аналіз криптоперетворень на еліптичних кривих та кривих Едвардса / *В.А. Кулібаба* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 203 – 208.

Виконано порівняльний аналіз основних перетворень на канонічних еліптичних кривих та кривих Едвардса. Наведено порівняння швидкодії групових операцій в групах точок еліптичних кривих та кривих Едвардса. Показана можливість використання алгоритму Полларда для криптоаналізу кривих Едвардса, а також прискорення генерації послідовності для алгоритму ро-Поларда для кривих Едвардса, що дозволяє пришвидшити виконання криптоаналізу. Запропоновано оцінку стійкості кривих Едвардса проти атаки типу «повне розкриття» з використанням дискретного логарифму в групі точок кривих Едвардса.

Ключові слова: еліптичні криві, криві Едвардса, криптоаналіз, електронний підпис.

Табл. 1. Бібліогр.: 7 назв.

UDC 004.056

Comparative analysis of cryptoprimitives on canonical elliptic curves and Edwards curves / *V. Kulibaba* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. №198. P. 203 – 208.

The article provides a comparative analysis of the basic transformations on canonical elliptic curves and Edwards curves. Comparisons of the performance of group operations in groups of points of elliptic curves and Edwards curves are given. The possibility of using the Pollard algorithm for cryptanalysis of Edwards curves, as well as the acceleration of the sequence generation for the ro-Polard algorithm for Edwards curves is shown, which allows to accelerate the execution of cryptanalysis. The paper proposes an assessment of the resistance of Edwards curves against attacks of the type "full disclosure" using the discrete logarithm in the Edwards curve point group.

Key words: elliptic curves, Edwards curves, cryptanalysis, digital signature.

1 tab. Ref.: 7 items.

УДК 004.056 55

Стойкость модифицированной цифровой подписи EdDSA / *А. Бессалов, Л. Ковальчук, Н. Кучинская, А. Телиженко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2019. Вып. 198. С. 209 – 214.

Украинский Национальный Стандарт Цифровой Подписи ДСТУ 4145-2002 используется уже почти 17 лет. За это время в области информационных технологий произошли существенные изменения, которые непосредственно влияют на применение этого стандарта и указывают на необходимость его модернизации.

В связи с необходимостью пересмотра и обновления Национального стандарта цифровой подписи ДСТУ 4145-2002 авторы рассматривают несколько конструкций цифровых подписей. Среди требований к современной цифровой подписи следует упомянуть как минимум 128-битовый уровень стойкости, быстрые алгоритмы подписи и её проверки, быструю генерацию ключей, надёжность сеансовых ключей, стойкость к коллизиям, безопасная программная реализация и тд. Существует множество очевидных вариантов среди классических и эллиптических систем подписи, Эль-Гамаля, Шнорра, ECDSA, другие, которые могут использоваться в переходный период к постквантовой криптографии.

Предлагается одна из возможных модификаций схемы цифровой подписи, базирующейся на алгоритме The Edwards-curve Digital Signature Algorithm (EdDSA). Основные преимущества предложенной в этой работе модификации состоят в следующем:

1) схема подписи является стойкой даже в случае сбоя генератора сеансовых ключей;

2) время реализации подписи не зависит от длины сообщения;

3) стойкость к атаке со связанными ключами.

Ключевые слова: кривая Эдвардса; цифровая подпись; EdDSA.

Библиогр.: 12 назв.

УДК 004.056 55

Стійкість модифікованого цифрового підпису EdDSA / *А. Бессалов, Л. Ковальчук, Н. Кучиньска, О. Теліженко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 209 – 214.

Український Національний Стандарт Цифрового Підпису ДСТУ 4145-2002 використовується вже майже 17 років. За цей час у галузі інформаційних технологій відбулись суттєві зміни, які безпосередньо впливають на використання цього стандарту та вказують на необхідність його модернізації.

У зв'язку з необхідністю перегляду та оновлення Національного стандарту цифрового підпису ДСТУ 4145-2002 автори розглядають кілька конструкцій цифрових підписів. Серед вимог до сучасного цифрового підпису слід зазначити як мінімум 128-бітовий рівень стійкості, швидкі алгоритми підпису та його перевірки, швидку генерацію ключів, надійність сеансових ключів, стійкість до колізій, безпечну програмну реалізацію і т. і. Існує багато очевидних варіантів серед класичних та еліптичних систем цифрового підпису, Ель-Гамаля, Шнорра, ECDSA, інші, які можна використовувати у перехідний до постквантового періода.

Пропонується одна з можливих модифікацій схеми цифрового підпису, що базується на алгоритмі The Edwards-curve Digital Signature Algorithm (EdDSA). Основними перевагами модифікації, яка запропонована у цій роботі, є наступні:

1) схема підпису є стійкою навіть у випадку збоїв у роботі генератора сеансовіх ключів;

2) час реалізації підпису не залежить від довжини повідомлення;

3) стійкість до атаки зі зв'язаними ключами.

Ключові слова: крива Едвардса; цифровий підпис; EdDSA.

Бібліогр.: 12 назв.

UDC 004.056 55

Securuty of modified digital public-key signature EdDSA / *A. Bessalov, L. Kovalchuk, N. Kuchynska, O. Telizhenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. №198. P. 209 – 214.

The Ukrainian National Standard for Digital Signature DSTU 4145-2002 has been in use about 17 years. During this time, significant changes have occurred in the field of information technology, which directly affect the implementation of the current National Standard for Digital Signature DSTU 4145-2002 and indicate the need for its modernization.

Due to the need to revise and update national digital signature standard DSTU 4145-2002, the authors considered several digital signature constructions. Among the requirements to modern public-key signatures it is worth to highlight at least 128-bit security, fast signing and fast signature verification, fast keys generation, foolproof session keys, collision resistance, secure software implementation, etc. There are a lot of obvious variants in classic and elliptic signature systems, ElGamal, Schnorr`s, ECDSA, etc, which can be used in transitional to post quantum period.

This paper introduces one of possible modifications for signature schemes based on the Edwards-curve Digital Signature Algorithm (EdDSA). The main advantages of the modification proposed in this work are:

1) the signature scheme is secure even if the session key generator fails;

2) signature implementation time does not depend on message length;

3) security against related-key attacks.

Key words: Edwards curve; digital signature; EdDSA.

12 items.

УДК 004.056.55

Применение хэш-функции купина в схеме подписей SPHINCS+ / *Д. Телевний* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2019. Вып. 198. С. 215 – 219.

В последние годы проведено значительное количество исследований по квантовым компьютерам, использующим квантово-механические явления для решения математических задач, которые являются сложными или неразрешимыми для обычных компьютеров. Возможность квантовых атак сформировала новую главу в области криптологии – постквантовую криптологию, где схемы ЭЦП стали одним из основных векторов исследований. Наиболее представительными выборками являются схемы, основанные на хэш-преобразованиях. Схемы подписи на основе хэша разработаны Лемпортом в качестве схемы одноразовой подписи в конце 1970-х годов и расширены для большего числа подписей Мерклом. В дальнейшем были введены более сложные схемы. NIST объявил о конкурсе новых стандартов постквантовой криптографии как для шифрования (генерации ключей), так и для подписей. На 2-й тур претендуют 9 кандидатов цифровой подписи. SPHINCS + (бывший SPHINCS) находится в списке. Алгоритм может быть кратко описан как схема подписи на основе хэша без сохранения состояния. Он использует много компонентов из XMSS, но работает с большими ключами и сигнатурой для устранения состояния. Схема может быть использована с различными хеш-функциями. Цель статьи – проанализировать применение хэш-функции национального стандарта в схеме кандидата NIST-кандидата SPHINCS +. Исследование показало, что хэш национального стандарта может быть применен к генерации случайных чисел и хешированию входного сообщения. Поскольку функция Kupyna возвращает выходные данные фиксированного размера, ее применение выглядит подобно хэш-функции SHA-256.

Ключевые слова: постквантовая криптография; схема подписи; хэш-функция; Купина; SPHINCS +; Меркле деревья.

Табл. 3. Ил. 1. Библиогр.: 9 назв.

УДК 004.056.55

Застосування хеш-функції Купина в схемі підпису SPHINCS+ / *Д. Телевний* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 215 – 219.

В останні роки проведено значну кількість досліджень квантових комп'ютерів – машин, які використовують квантові механічні явища для вирішення математичних задач, важких або нерозв'язних для звичайних комп'ютерів. Можливість квантових атак сформувала нову главу в галузі криптології – постквантову криптологію, де схеми DSA стали одним з основних векторів досліджень. Найбільш репрезентативними вибірками є схеми, засновані на хеш-перетвореннях. Схеми підписів Лемпорта на основі хешу були розроблені як одноразові схеми підпису в кінці 1970-х і розширені Меркле на багаторазові підписи. Надалі були запроваджені складніші схеми. NIST заявив про конкуренцію нових стандартів potquantum як для шифрування (генерації ключів), так і для підписів. У II турі є 9 кандидатів у цифровий підпис. SPHINCS + (колишній SPHINCS) є у списку. Алгоритм можна коротко охарактеризувати як схему підписів без збереження стану. Він використовує багато компонентів з XMSS, але працює з більшими ключами та підписом для усунення стану. Схему можна використовувати з різними хеш-функціями. Мета роботи – проаналізувати застосування національної стандартної хеш-функції схеми кандидата, що подає NIST SPHINCS +. Дослідження показало, що національний стандарт хеш може бути застосований до генерації випадкових випадків насіння та хешування вхідного повідомлення. Оскільки Fuction fuction повертає вихід фіксованого розміру, його застосування виглядає аналогічно хешам SHA-256.

Ключові слова: постквантова криптографія; схема підпису; хеш-фукція; Купина; SPHINCS+; дерева Меркла.

Табл. 3. Іл. 1. Бібліогр.: 9 назв.

UDC 004.056.55

The Kupyna hash function application to SPHINCS+ signatures / *D. Televnyi* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. №198. P. 215 – 219.

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. The possibility of quantum attacks formed a new chapter in cryptology field – postquantum cryptology, where DSA schemes became one of the main research vectors. The most representative samples are schemes based on hash transformations. Hash-based signature schemes were developed as one-time signature schemes in the late 1970s by Lamport and extended to more signatures by Merkle. In further more complicated schemes were introduced. NIST declared about the competition of new postquantum standards both for encryption (key generation) and signatures As for the 2nd round there are 9 Digital signature candidates. SPHINCS+ (former SPHINCS) is in the list. The algorithm can be briefly described as a stateless hash-based signature scheme. It uses many components from XMSS but works with larger keys and signature to eliminate state. The scheme can be used with different hash functions. The main goal of this paper is to analyze the application of the national standard hash function the scheme of the NIST submission candidate SPHINCS+. The research showed the national standard hash could be applied to the seed randomness generation and hashing the input message. Since Kupyna function returns fixed-size output, its application looks similar to SHA-256 hashes.

Key words: postquantum cryptography; signature scheme; hash function; Kupyna; SPHINCS+; Merkle trees.

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