

МЕТОДЫ СИНТЕЗА И АНАЛИЗА
СИММЕТРИЧНЫХ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙMETHYODS OF SYNTHESIS AND ANALYSIS
FOR SYMMETRIC CRYPTOGRAPHIC TRANSFORMATIONS

УДК 621.3.06

Симметричный блочный шифр «Калина» – новый национальный стандарт шифрования Украины / И.Д. Горбенко, Р.В. Олейников, А.В. Казимиров, В.И. Руженцев, А.А. Кузнецов, Ю.И. Горбенко, О.В. Дырда, В.И. Долгов, А.И. Пушкарёв, Р.И. Мордвинов, Д.С. Кайдалов, В.М. Казими́рова // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2015. – Вып. 181. – С. 5 – 22.

Приведено развернутое альтернативное описание симметричного блочного шифра «Калина» из нового национального стандарта Украины ДСТУ 7624:2014. Используемые в описании обозначения, традиционные для компьютерных наук, упрощают восприятие сути криптографического преобразования для широкого круга специалистов в области информационных технологий.

Табл. 5. Рис. 19. Библиогр.: 5 назв.

УДК 621.3.06

Симетричний блоковий шифр „Калина” – новий національний стандарт України / І.Д. Горбенко, Р.В. Олійников, О.В. Казимиров, В.І. Руженцев, О.О. Кузнецов, Ю.І. Горбенко, О.В. Дирда, В.І. Долгов, А.І. Пушкарёв, Р.І. Мордвінов, Д.С. Кайдалов, В.М. Казими́рова // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 5 – 22.

Наведено розгорнутий альтернативний опис симетричного блокового шифру „Калина” із нового національного стандарту України ДСТУ 7624:2014. Позначення, застосовані в описі, традиційні для комп’ютерних наук, спрощують сприйняття сутності криптографічного перетворення для широкого кола фахівців у галузі інформаційних технологій.

Табл. 5. Рис. 19. Бібліогр.: 5 назв.

UDC 621.3.06

“Kalyna” block cipher – new Ukrainian national standard / I. Gorbenko, R. Oliynykov, O. Kazymyrov, V. Ruzhentsev, O. Kuznetsov, Y. Gorbenko, O. Dyrda, V. Dolgov, A. Pushkaryov, R. Mordvinov, D. Kaidalov, V. Kazymyrova // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2015. – № 181. – P. 5 – 22

A detailed alternative description of the Kalyna block cipher specified in the new Ukrainian national standard DSTU 7624:2014 is given. The notations used in the description, which are traditional for computer science, simplify understanding of the cryptographic transformation for IT-specialists.

5 Tab. 19 Fig. Ref.: 10 items.

УДК 621.3.06

Функция хэширования «Купина» – новый национальный стандарт Украины / Р.В. Олейников, И.Д. Горбенко, А.В. Казимиров, В.И. Руженцев, А.А. Кузнецов, Ю.И. Горбенко, О.В. Дырда, А.А. Бойко, В.И. Долгов, А.И. Пушкарёв, В.Н. Казими́рова, Р.И. Киянчук // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2015. – Вып. 181. – С. 23 – 30.

Приведено развернутое альтернативное описание криптографической функции хэширования «Купина» из нового национального стандарта Украины ДСТУ 7564:2014. Используемые в описании обозначения, традиционные для компьютерных наук, упрощают восприятие сущности криптографического преобразования для широкого круга специалистов в области информационных технологий.

Табл. 2. Рис. 6. Библиогр.: 6 назв.

УДК 621.3.06

Функція гешування „Купина” – новий національний стандарт України / Р.В. Олійников, І.Д. Горбенко, О.В. Казимиров, В.І. Руженцев, О.О. Кузнецов, Ю.І. Горбенко, О.В. Дирда, А.О. Бойко, В.І. Долгов, А.І. Пушкарёв, В.М. Казими́рова, Р.І. Кіяничук // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 23 – 30.

Наведено розгорнутий альтернативний опис криптографічної функції гешування „Купина” із

нового національного стандарту України ДСТУ 7564:2014. Позначення, застосовані в описі, традиційні для комп'ютерних наук, спрощують сприйняття сутності криптографічного перетворення для широкого кола фахівців у галузі інформаційних технологій.

Табл. 2. Рис. 6. Бібліогр.: 6 назв.

UDC 621.3.06

“Kupyna” hash function – new Ukrainian national standard / R. Oliynykov, I. Gorbenko, O. Kazymyrov, V. Ruzhentzev, O. Kuznetsov, Y. Gorbenko, O. Dyrda, A. Boiko, V. Dolgov, A. Pushkaryov, V. Kazymyrova, R. Kiyanchuk // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2015. – № 181. – P. 23 – 30.

A detailed alternative description of the Kupyna hash function specified in the new Ukrainian national standard DSTU 7564:2014 is given. The notations used in the description, which are traditional for computer science, simplify understanding of the cryptographic transformation for IT-specialists.

2 Tab. 6 Fig. Ref.: 6 items.

УДК 621.391:519.2

Границы для скорости передачи информации в рандомизированных поточных шифр-системах Михалеви́ча – Имаи / А.Н. Алексейчук, С.В. Гришаков // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2015. – Вып. 181. – С. 31 – 39.

Получены границы для максимальной скорости передачи информации в поточных шифр-системах, основанных на совместном применении шифрования, случайного кодирования и помехоустойчивого кодирования сообщений двоичными линейными кодами. Показано, что эти границы позволяют оценивать практичность указанных шифр-систем при заданных требованиях к их стойкости.

Ил. 2. Библиогр.: 12 назв.

УДК 621.391:519.2

Межі для швидкості передачі інформації рандомізованими потоковими шифросистемами Михалеви́ча – Имаї / А.М. Олексійчук, С.В. Гришаков // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 31 – 39.

Отримано межі для максимальної швидкості передачі інформації потоковими шифросистемами, що базуються на спільному застосуванні шифрування, випадкового кодування та завадостійкого кодування повідомлень двійковими лінійними кодами. Показано, що ці межі дозволяють оцінювати практичність зазначених шифросистем при заданих вимогах до їх стійкості.

Ил. 2. Бібліогр.: 12 назв.

UDC 621.391:519.2

Bounds on the information transmission rate in the Mihaljević-Imai randomized stream ciphers / A.N. Alekseychuk, S.V. Gryshakov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2015. – № 181. – P. 31 – 39.

Bounds on the maximum information transmission rate in the stream ciphers based on joint employment of encryption, random coding and error-correction coding of messages by binary linear codes are obtained. It is shown that these bounds make it possible to evaluate the practicality of the specified ciphers under given requirements for their security.

2 fig. Ref.: 12 items.

УДК 621.3.16

Стратегия широкого следа без сепарабельных кодов / М.Ю. Родинко, К.Е. Лисицкий // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2015. – Вып. 181. – С. 40 – 45.

Предлагается реализация стратегии широкого следа в рамках единого преобразования без разделения на линейную и нелинейную части. Эта возможность состоит в процедуре последовательной активизации S-блоков цикловой функции один за другим с помощью управляемых подстановок. Показано, что предлагаемое преобразование полностью идентично оригинальному преобразованию шифра Rijndael по его дифференциальным и линейным свойствам. Предлагаемая конструкция позволяет получить максимальное число ветвлений. Это означает, что один вход S-блока активизирует последующие S-блоки преобразования.

Табл. 6. Ил. 2. Библиогр.: 12 назв.

УДК 621.3.16

Стратегія широкого сліду без сепарабельних кодів / М.Ю. Родінко, К.Є. Лисицький // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 40 – 45.

Пропонується реалізація стратегії широкого сліду в рамках єдиного перетворення без поділу на

лінійну і нелінійну частини. Ця можливість полягає в процедурі послідовної активізації S-блоків циклової функції один за іншим за допомогою керованих підстановок. Показано, що запропоноване перетворення повністю ідентично оригінальному перетворенню шифру Rijndael за його диференціальними і лінійними властивостями. Запропонована конструкція дозволяє отримати максимальне число розгалужень. Це означає, що один вхід S-блоку активізує подальші S-блоки перетворення.

Табл. 6. Іл. 2. Бібліогр: 12 назв.

UDC 621.3.16

Wide trail strategy without separable codes / M.Yu. Rodinko, K.E. Lisitskiy // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2015. – № 181. – P. 40 – 45.

Implementation of the wide trail strategy within a single transformation without separation into linear and nonlinear parts is proposed. This possibility consists in the procedure of a consistent activation of S-boxes of the round function one by one by using managed substitutions. It is shown that the proposed transformation is completely identical to the original transformation of Rijndael on its differential and linear properties. The proposed construction allows obtaining maximum branch number. It means that one S-box input activates the subsequent S-boxes of transformation.

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

УДК 004.056.55

Сравнительный анализ стойкости современных алгоритмов блочного симметричного шифрования / И.Д. Горбенко, Р.И. Мордвинов // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2015. – Вып. 181. – С. 46 – 50.

Сравнивается стойкость современных БСШ, включая новый государственный стандарт симметричного блочного преобразования ДСТУ 7624:2014. Приводится описание нового метода тестирования последовательностей для получения вероятностных оценок статистической безопасности выходных последовательностей. Тестирование проводится с использованием всех режимов, которые описаны в новом стандарте, для пяти БСШ.

Табл. 6. Библиогр.: 4 назв.

УДК 004.056.55

Порівняльний аналіз стійкості сучасних алгоритмів блокового симетричного шифрування / І.Д. Горбенко, Р.І. Мордвінов // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 46 – 50.

Порівнюється стійкість сучасних БСШ, включаючи новий державний стандарт симетричного блокового перетворення ДСТУ 7624:2014. Надається опис нового методу тестування послідовностей для отримання імовірнісних оцінок статистичної безпеки вихідних послідовностей. Тестування проводиться з використанням всіх режимів, що описані в новому державному стандарті, для п'яти БСШ.

Табл. 6. Бібліогр.: 4 назв.

UDC 004.056.55

Comparative analysis of stability of modern block symmetric ciphering algorithms / I.D. Gorbenko, R.I. Mordvinov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2015. – № 181. – P. 46 – 50.

Comparison of the modern BSC resistance, including the DSTU 7624:2014 new state standard of symmetric block transform is considered. A new method of testing the sequences for probabilistic safety assessments of statistical output-sequences is given. Testing is conducted using all modes described in the standard for five BSC.

6 tab. Ref.: 4 items.

АСИММЕТРИЧНЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ И ИХ ПРИМЕНЕНИЕ

ASYMMETRIC CRYPTOGRAPHIC TRANSFORMATIONS AND THEIR APPLICATION

УДК 004.056.55

Анализ вычислительной сложности арифметико-геометрического метода вычисления количества точек на эллиптической кривой / И. Д. Горбенко, Р. С. Ганзя // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2015. – Вып. 181. – С. 51 – 57.

Анализируются методы генерирования общесистемных параметров для эллиптических кривых. Показана актуальность генерирования общесистемных параметров больших размеров для обеспече-

ния безопасности в национальных системах. Показана возможность использования арифметико-геометрического метода для национальных криптоалгоритмов, а также эффективность вычисления нормы через результат.

На практике разработано программное средство на языке C++ с использованием библиотеки NTL. Программное средство в состоянии построить общесистемные параметры для эллиптической кривой с размером базовой точки 1031 бит для криптосистемы в соответствии с национальным стандартом.

Табл. 2. Ил. 1. Библиогр.: 9 назв.

УДК 004.056.55

Аналіз обчислювальної складності арифметико-геометричного методу обчислення кількості точок на еліптичній кривій / І. Д. Горбенко, Р. С. Ганзя // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 51 – 57.

Аналізуються методи генерування загальносистемних параметрів для еліптичних кривих. Показана актуальність генерування загальносистемних параметрів великих розмірів для забезпечення безпеки в національних системах. Показана можливість використання арифметико-геометричного методу для національних криптоалгоритмів, а також ефективність обчислення норми через результат.

На практиці розроблено програмний засіб мовою C++ з використанням бібліотеки NTL. Програмний засіб зможе побудувати загальносистемні параметри для еліптичної кривої з розміром базової точки 1031 біт для криптосистеми відповідно до національного стандарту.

Табл. 2. Іл. 2. Бібліогр.: 9 назв.

UDC 004.056.55

Analysis of the computational complexity of arithmetic geometric mean for calculating the number of points on the elliptic curve / I. D. Gorbenko, R. S. Hanzia // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2015. – № 181. – P. 51 – 57.

Methods for generating general system sets of parameters for elliptic curves are analysed. Actuality of generating general set of parameters of large sizes for national security cryptosystem is demonstrated. The possibility to use arithmetic–geometric method for national algorithms and the effectiveness to count points by resultants are shown.

The software tool in the C++ language using the NTL library was developed in practice. This software is able to build elliptic curves with the size of the base point of 1031 bits for crypto transformation according to the national digital signature standard.

Tab. 2. Fig. 1. Ref.: 9 items.

УДК 681.3.06

Производительность групповых операций на скрученной кривой Эдвардса над простым полем / А.В. Бессалов, О.В.Цыганкова // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 58 – 63.

Дан критический анализ свойств скрученной кривой Эдвардса в сравнении с кривой Эдвардса. Показано, что введение нового параметра a не расширяет класс кривых Эдвардса в силу их изоморфизма, но число полезных кривых нарастает вдвое снятием ограничения на неквадратичность параметра d . Дан сравнительный анализ производительности вычислений на кривой Эдвардса с модификацией закона сложения точек и на кривой в канонической форме.

УДК 681.3.06

Продуктивність групових операцій на скрученій кривій Едвардса над простим полем / А.В. Бессалов, О.В.Цыганкова // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 58 – 63.

Дано критичний аналіз властивостей скрученої кривої Едвардса в порівнянні з кривої Едвардса. Показано, що введення нового параметра a не розширює клас кривих Едвардса в силу їх ізоморфізму, однак кількість корисних кривих наростає вдвічі зняттям обмеження на неквадратичність параметру d . Дано порівняльний аналіз продуктивності обчислень на кривої Едвардса з модифікацією закону додавання точок і на кривої у каноничній формі.

UDC 681.3.06

Performance of batch operations on a twisted Edwards curve over a simple field / A. V. Bessalov, O. V. Tsygankova // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2015. – № 181. – P. 58 – 63.

Critical analysis of the properties of the twisted Edwards curve compared with the Edwards curve is given. It is shown that the introduction of a new parameter a does not extend the class of Edwards curves due

to their isomorphism, but the number of useful curves is incremented twice as much by the removal of restrictions on nonquadratic nature of d parameter. The comparative analysis of performance on the Edwards curve with a modification of the law of addition of points on the curve and in canonical form is given.

УДК 004.056.55

Гибридный метод направленного шифрования, основанный идентификаторах и алгебраических решетках / Л.В. Макутонина // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2015. – Вып. 181. – С. 64– 67.

Приводится гибридный метод направленного шифрования, который отличается от классических методов на идентификаторах улучшенными показателями стойкости и быстродействия.

Табл. 4. Библиогр.: 6 назв.

УДК 004.056.55

Гібридний метод направленного шифрування, який базується ідентифікаторах і алгебраїчних решітках / Л.В. Макутоніна // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 64– 67.

Наводиться гібридний метод направленного шифрування, який відрізняється від класичних методів на ідентифікаторах поліпшеними показниками стійкості і швидкодії.

Табл. 4. Бібліогр.: 6 назв.

UDC 004.056.55

Hybrid method of directional encryption based on identifiers and algebraic lattices / L.V. Makutonina // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2015. – № 181. – P. 64– 67.

The hybrid method of directional encryption, which differs from the classical methods based on identifiers by the improved resistance and speed indicators, is given.

4 tab. Ref.: 6 items.

УДК 004 056 55

Сущность и оценка стойкости криптографических преобразований в NTRUSign / А.В. Шевцов // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2015. – Вып. 181. – С. 68 – 78.

The essence of cryptographic transformations NTRUSign signature in the quotient rings of polynomials.

Рассматривается сущность криптографических преобразований подписи NTRUSign в фактор-кольцах полиномов. Также изучаются математическая модель, история возникновения, современное состояние и перспективы развития подписи в фактор-кольцах срезанных полиномов. Излагаются основные положения и результаты оценки стойкости криптопреобразования в фактор-кольцах полиномов на примере подписи NTRUSign.

Табл. 7. Библиогр.: 13 назв.

УДК 004 056 55

Сутність та оцінка стійкості криптографічних перетворень в NTRUSign / О.В. Шевцов // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 68 – 78.

Розглянуто сутність криптографічних перетворень підпису NTRUSign в фактор-кільцях зрізаних поліномів. Також вивчається математична модель, історія виникнення, сучасний стан та перспективи розвитку підпису в фактор-кільцях зрізаних поліномів. Викладаються основні положення та результати оцінки стійкості криптоперетворень в фактор-кільцях зрізаних поліномів на прикладі підпису NTRUSign.

Табл. 7. Бібліогр.: 13 назв.

UDC 004 056 55

Essence and evaluation of resistance of cryptographic transformations in NTRUSign / O.V. Shevtsov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2015. – № 181. – P. 68 – 78.

The essence of cryptographic transformations of the NTRUSign signature in the factor-rings of truncated polynomials is considered. The mathematical model, the history of origin, the modern state and prospects of development of the signature in the factor-rings of truncated polynomials are also studied. The essentials and results of estimation of cryptographic transformations resistance in the factor-rings of truncated polynomials are exemplified by the NTRUSign signature.

7 tab. Ref.: 13 items.

УДК 004.056.55

Использование системы GPS в многофакторной аутентификации / М.В. Есина, И.Д. Горбенко // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2015. – Вып. 181. – С. 79 – 85.

Рассматривается механизм защиты информации на основе многофакторной аутентификации. GPS координаты рассматриваются как фактор аутентификации. Описывается принцип аутентификации, когда используются GPS координаты. Рассматриваются варианты криптографических протоколов аутентификации.

Ил. 5. Библиогр.: 13 назв.

УДК 004.056.55

Використання системи GPS у багатофакторній автентифікації / М.В. Єсіна, І.Д. Горбенко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 79 – 85.

Розглядається механізм захисту інформації на основі багатофакторної автентифікації. GPS координати розглядаються як фактор автентифікації. Описується принцип автентифікації, коли використовуються GPS координати. Розглядаються варіанти криптографічних протоколів автентифікації.

Іл. 5. Бібліогр.: 13 найм.

UDC 004.056.55

GPS system use in multi-factor authentication / M.V. Yesina, I.D. Gorbenko // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2015. – № 181. – P. 79 – 85.

The mechanism of information protection based on multi-factor authentication is considered. GPS coordinates are considered as the authentication factor. The principle of authentication, when using GPS-coordinates, is described. Variants of cryptographic authentication protocols are considered.

Fig. 5. Ref.: 13 items.

УДК 004.056.55

Соккрытие данных в кластерных файловых системах / А.А.Кузнецов, А.С.Швагер, Д.А.Фесенко // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2015. – Вып. 181. – С. 86 – 100.

Рассматриваются методы стеганографической защиты, построение которых основано на использовании кластерных файловых систем, установленного порядка организации, хранения и именования данных на физических носителях информации. Основная идея состоит в сокрытии секретного сообщения при помощи кодирования относительных позиций кластеров специально выбранных файлов (cover files) друг относительно друга. Другие файлы в файловой системе игнорируются, анализируются и обрабатываются только кластеры, принадлежащие cover files. Такой подход позволяет без изменения объема хранимых на физическом носителе данных дополнительно встраивать информационные сообщения, скрывая как смысловое содержание сообщений, так и сам факт их существования (передачи).

Ил.6. Библиогр.: 4 назв.

УДК 004.056.55

Приховування даних у кластерних файлових системах / О.О.Кузнецов, А.С.Швагер, Д.А.Фесенко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 86 – 100.

Розглядаються методи стеганографічної захисту, побудова яких заснована на використанні кластерних файлових систем, встановленого порядку організації, зберігання та іменування даних на фізичних носіях інформації. Основна ідея полягає в приховуванні секретного повідомлення за допомогою кодування відносних позицій кластерів спеціально вибраних файлів (cover files) один щодо одного. Інші файли у файловій системі ігноруються, аналізуються і обробляються тільки кластери, що належать cover files. Такий підхід дозволяє без зміни обсягу збережених на фізичному носії даних додатково вбудовувати інформаційні повідомлення, приховуючи як смисловий зміст повідомлень, так і сам факт їх існування (передачі).

Іл.6. Бібліогр.: 4 назв.

UDC 004.056.55

Hiding of data in the cluster file systems / O.O.Kuznetsov, A.S.Shvagher, D.A.Fesenko // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2015. – № 181. – P. 86 – 100

The methods of steganography protection are considered, the construction of which is based on the use of cluster file systems of the established order of organizing, storing and naming of data on physical media. The basic idea consists in hiding a secret message using the encoding of relative positions of the clusters of specially selected files (cover files) relative to each other. Other files in the file system are ignored, analyzed and only clusters belonging to cover files are processed. This approach makes it possible to integrate infor-

mation messages, hiding both the semantic content of the messages, and the fact of their existence (transmission) without changing the volume of the data stored on a physical medium.

6 fig. Ref.: 4 items.

УДК 004.056.55

Сравнительный анализ перспективных стандартов ЭП в группе точек эллиптических кривых / О. С. Акользина, А.А. Баклыков // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2015. – Вып. 181. – С. 101 – 109.

Проведен обзор основных стандартов электронной подписи (ISO/IEC 9796-3, ДСТУ ISO/IEC 14888 – 3, ДСТУ 4145-2002, Fips 186-3 та ГОСТ Р 34.10-2012) и их сравнительный анализ по критерию «стойкость-сложность». Также разработаны соответствующие рекомендации по применению. Стандарты сравнивались по значению модуля, показателем безопасного времени и сложности выполнения операций. Сделаны выводы насчет их защищенности от существующих атак. Каждая схема уязвима к определенным видам атак.

Табл. 3. Библиогр.: 3 назв.

УДК 004.056.55

Порівняльний аналіз перспективних стандартів ЕП в групі точок еліптичних кривих / О.С. Акользіна, О.О. Бакликов // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 101 – 109.

Проведений огляд основних стандартів електронного підпису (ISO/IEC 9796-3, ДСТУ ISO/IEC 14888 – 3, ДСТУ 4145-2002, Fips 186-3 та ГОСТ Р 34.10-2012) та їх порівняльний аналіз по критерію «стійкість-складність». Розроблено рекомендації із застосування. Стандарти були порівняні за значенням модуля, показником безпечного часу та складністю виконання операцій. Зроблено висновки стосовно їх захищеності від існуючих атак. Кожна розглянута схема підпису вразлива до певного виду атак.

Табл. 3. Бібліогр.: 3 назв.

UDC 004.056.55

Comparative analysis of ES prospective standards in the group of points of elliptic curves / O. Akozina, O. Baklykov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2015. – № 181. – P. 101 – 109.

Review of the main ES standards (such as ISO/IEC 9796-3, ДСТУ ISO/IEC 14888 – 3, ДСТУ 4145-2002, Fips 186-3 and ГОСТ Р 34.10-2012) and comparative research for criterion “capability-complexity” were carried out. Some recommendations for applying these algorithms were offered. The modulus size, secure time, operation complexity were compared. The conclusions about security against existing attacks were made. Every scheme has vulnerability against some attack(s).

3 tab. Ref.: 3.

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ MEANS OF INFORMATION PROTECTION

УДК 681.3.06:519.248.681

Ансамблевые и корреляционные свойства криптографических сигналов для приложений телекоммуникационных систем и сетей / И.Д. Горбенко, А.А. Замула, Е.А. Семенко // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2015. – Вып. 181. – С. 110 – 117.

Приводится описание метода синтеза нового класса дискретных последовательностей, – криптографических последовательностей. Сравниваются и анализируются корреляционные свойства данного класса сигналов с граничными значениями для соответствующих корреляционных функций и с значениями для широко используемых классов дискретных сигналов. Даются оценки ансамблевых свойств исследуемого класса сигналов.

Табл. 3. Ил. 3. Библиогр.: 7 назв.

УДК 681.3.06:519.248.681

Ансамблеві та кореляційні властивості криптографічних сигналів для додатків телекомунікаційних систем і мереж / І.Д. Горбенко, О.А. Замула, Є.О. Семенко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 110 – 117.

Наводиться опис методу синтезу нового класу дискретних послідовностей – криптографічних послідовностей. Порівнюються та аналізуються кореляційні властивості даного класу сигналів з граничними значеннями для відповідних кореляційних функцій і з значеннями для широко використовуваних класів дискретних сигналів.

ваних класів дискретних сигналів. Дано оцінки ансамблевих властивостей досліджуваного класу сигналів.

Табл. 3. Лл. 3. Бібліогр.: 7 назв.

UDC 681.3.06:519.248.681

Ensemble and correlation properties of cryptographic signals for telecom applications munication systems and networks / I.D. Gorbenko, A.A. Zamula, E.A. Semenko // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2015. – № 181. – P. 110 – 117.

Description of the synthesis method of the new class of discrete sequences – cryptographic sequences is provided. A comparative analysis of the correlation properties of this class of signals with limit values for the corresponding correlation functions and with the values for commonly used classes of discrete signals is held. Estimates of the ensemble properties of the signal class under study are given.

3 tab. 3 fig. Ref.: 7 items.

УДК 519.2: 530.1

Парадигма защиты информации Игоря Громыко: гидродинамический ракурс / Г. К. Бронишак; А.Н. Ващенко, С. И. Доценко; Е. Л. Перчик // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2015. – Вып. 181. – С. 118 – 132.

На основании аналитического обзора профильных источников выяснилась неприменимость теории Шеннона для расчетно-теоретического сопровождения выдвинутой парадигмы, из-за ее предметной общности. В качестве базиса адекватной теории принята сравнительно элементарная модель распространения звука в трубе наряду с использованием потенциала гидродинамических аналогий, детерминистской методологии, а также аксиоматики М. Мазура. Расчетная оценка «коммуникабельности» сопряженных носителей информации сводится к исследованию корректной разрешимости интегральных уравнения Вольтерра первого рода.

Бібліогр.: 41 назв.

УДК 519.2: 530.1

Парадигма захисту інформації Ігора Громыко: гідродинамічний ракурс / Г.К. Бронишак; А.Н. Ващенко, С. И. Доценко; Е. Л. Перчик // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 118 – 132.

На основі аналітичного огляду профільних джерел з'ясовано, що теорія Шеннона не може використовуватись для розрахунково-теоретичного супроводу запропонованої парадигми через її предметну загальність. В якості базису адекватної теорії прийнято порівняно елементарну модель розповсюдження звука в трубі разом з використанням потенціалу гідродинамічних аналогій, детерміністської методології, а також аксіоматики М. Мазура. Розрахункова оцінка «комунікабельності» спряжених носіїв інформації зводиться до дослідження коректного вирішення інтегральних рівнянь Вольтера першого роду.

Бібліогр.: 41 назв.

UDC 519.2: 530.1

Paradigm of information security by Igor Gromyko: a hydrodynamic perspective / G.K. Brodspec, A. N. Vashchenko, S. I. Dotsenko E. L. Perchik // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2015. – N 181. – P. 118 – 132.

Shannon's theory was considered as an inapplicable for the design-theoretical maintenance of the suggested paradigm because of its object generality on the basis of the profile sources analytic review. Comparatively elementary model of the sound propagation in the pipe was accepted as a basis of an adequate theory. At the same time there were used the potential of hydrodynamic analogies, deterministic methodology and Mazur's axiomatics. Calculation estimate of the "communicability" of the conjugate data mediums is reduced to the investigation of the correct solvability of integral Volterra equations of the first kind.

Ref.: 41 items.

УДК 681.3.06

Анализ современных требований к криптографическим примитивам нового поколения / Е.В. Котух, В.М. Карташов, О.Г. Халимов, Д.П. Цапко, А.В. Самойлова // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2015. – Вып. 181. – С. 133 – 142.

Представлен анализ современных требований к конструкциям финалистов конкурса SHA-3 (Blake, JH, Groestl, Skein, Кессак). Показано, что универсальные криптографические примитивы Skein и Кессак имеют ряд существенных преимуществ перед классическими схемами, основанными на

функциях сжатия. Рассмотрены новые свойства криптографических примитивов. Показано, что поддержка различных комбинаций исходных параметров без использования дополнительных средств и приложений позволяет добиться универсальности в реализации нового поколения криптографических примитивов на различных архитектурах современных процессоров. Сделан вывод, что очевидной причиной выбора функции Кескак в качестве победителя стала его конструкция, которая позволила обосновать универсальность Кескак, реализовать доказуемую стойкость к целому классу атак без увеличения сложности реализации.

Рис. 7. Табл.: 3. Библиогр.: 14 назв.

УДК 681.3.06

Аналіз сучасних вимог до криптографічних примітивів нового покоління / Є.В. Котух, В.М. Карташов, О.Г. Халімов, Д.П. Цапко, А.В. Самойлова // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 133 – 142.

Представлено аналіз сучасних вимог до конструкцій фіналістів конкурсу SHA-3 (Blake, JH, Groestl, Skein, Keccak). Показано, що універсальні криптографічні примітиви Skein і Keccak мають ряд істотних переваг перед класичними схемами, заснованими на функціях стиснення. Розглянуто нові властивості криптографічних примітивів. Показано, що підтримка різних комбінацій вихідних параметрів без використання додаткових засобів і додатків дозволяє домогтися універсальності в реалізації нового покоління криптографічних примітивів на різних архітектурах сучасних процесорів. Зроблено висновок, що очевидною причиною вибору функції Keccak в якості переможця стала його конструкція, яка дозволила обґрунтувати універсальність Keccak, реалізувати доказову стійкість до цілого класу атак без збільшення складності реалізації.

Іл. 7. Табл.: 3. Бібліогр.: 14 назв.

UDC 681.3.06

Analysis of modern requirements to the new generation of cryptographic primitives / Y.V. Kotukh, V.M. Kartashov, O.G. Khalimov, D.P. Tsapko, A.V. Samoilova // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2015. – № 181. – P. 133 – 142.

The analysis of the modern design requirements of the SHA-3 competition finalists (Blake, JH, Groestl, Skein, Keccak) is presented. It is shown that the universal cryptographic primitives Skein and Keccak have a number of significant advantages over classical schemes based on the compression function. Some new properties cryptographic primitives are presented. It is shown that support of various combinations of the initial parameters without the use of additional tools and applications allows having flexibility in the implementation of the new generation of cryptographic primitives on different architectures of modern CPUs. It is concluded that the apparent cause of the Keccak function as the winner was its design, which made it possible to substantiate the versatility of the Keccak and realize a provable resistance to a whole class of attacks without increasing the complexity of the implementation.

Tab. 3. Il. 7. Ref.: 14 items.

УДК 004.056.55

Квантовый генератор случайных чисел на основе расщепления пучка фотонов / Р.О. Гаврилко, Ю.И. Горбенко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 143 – 149.

Случайные числа очень широко используются. Они являются важным компонентом во многих областях, начиная от вычислительных методов и программирования, заканчивая большой областью криптографии. Большой диапазон областей, которые используют случайные числа, привел к развитию разных генераторов случайных чисел, а также средств для проверки их исходных данных на случайность. Одним из таких генераторов является физическое квантовый генератор случайных чисел.

Іл. 4. Библиогр.: 2 назв.

УДК 004.056.55

Квантовый генератор випадкових чисел на основі розщеплення пучка фотонів / Р.О. Гаврилко, Ю.І. Горбенко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2015. – Вип. 181. – С. 143 – 149.

Випадкові числа дуже широко використовуються. Вони є важливим компонентом у багатьох областях, починаючи від обчислювальних методів і програмування, закінчуючи великою областю криптографії. Великий діапазон областей, які використовують випадкові числа, привів до розвитку різних генераторів випадкових чисел, а також засобів для перевірки їх вихідних даних на випадковість. Одним з таких генераторів є фізичний квантовий генератор випадкових чисел.

Ил. 4. Бібліогр.: 2 назви.

UDC 004.056.55

Quantum random number generator based on splitting the beam of photons / *R.O. Gavrilko, Yu.I. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2015. – № 181. – P. 143 – 149.

Random numbers are very widespread. They are important component in many fields, starting with computing methods and programming, ending with a great field of cryptography. A wide range of fields, where random numbers are used had lead to development of different random number generators, and also some methods for checking their output data for randomness. One of these generators is quantum random number generator. The goal of this work consists in the description of quantum RNG's principles and justification of its advantages and disadvantages corresponding correlation functions and with the values for commonly used classes of discrete signals is held. Estimates of the ensemble properties of the signal class under study are given.

4 fig. Ref.: 2 items.