

СОДЕРЖАНИЕ ЗМІСТ

ПЕРСПЕКТИВНЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ И ИХ ПРИМЕНЕНИЕ

ПЕРСПЕКТИВНІ КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ ТА ЇХ ЗАСТОСУВАННЯ

<i>И.Д. Горбенко, О.Г. Качко, А.Н. Олексейчук, А.А. Кузнецов, Ю.И. Горбенко, В.В. Оноприенко, М.В. Есина, С.А. Кандий</i> Алгоритмы асимметричного шифрования и инкапсуляции ключей постквантового периода 5-7 уровней стойкости и их применение	5
<i>И.И. Бобок, А.А. Кобозева</i> Стеганоаналитический метод, эффективный в условиях малой пропускной способности скрытого канала связи	19
<i>И.Д. Горбенко, А.А. Замула, В.Л. Морозов, С.В. Родионов</i> Математическая модель сигналов с ортогональным частотным разделением и мультиплексированием (OFDM)	32
<i>О.О. Кузнецов, Ю.И. Горбенко, В.В. Оноприенко, І.В. Стельник, Д.В. Мялковський</i> Алгоритми криптографічного гешування, які застосовуються в сучасних блокчейн-системах	44
<i>О.О. Кузнецов, Ю.И. Горбенко, В.В. Оноприенко, І.В. Стельник, Д.В. Мялковський</i> Дослідження алгоритмів криптографічного гешування, які застосовуються в сучасних блокчейн-системах	54
<i>О.О. Кузнецов, В.А. Тимченко, К.Є. Лисицький, М.Ю. Родінко, М.С. Луценко, К.Ю. Шеханін, А.О. Колгатін</i> Дослідження швидкодії та статистичної безпеки алгоритмів криптографічного гешування	75

АНАЛИЗ И ИСПОЛЬЗОВАНИЕ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ В ДЕЦЕНТРАЛИЗОВАННЫХ ТЕХНОЛОГИЯХ

АНАЛІЗ ТА ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ МЕТОДІВ В ДЕЦЕНТРАЛІЗОВАНИХ ТЕХНОЛОГІЯХ

<i>Е.В. Исирова, А.В. Потий, Jens Christian Claussen</i> Установление протоколов доверия в сети взаимного недоверия путем формирования консенсуса	96
<i>М.О. Осадчук, Р.В. Олейников</i> Метод сравнения Proof of Work алгоритмов консенсуса	105
<i>В.И. Есин, В.В. Вилигура</i> Некоторый подход к маскированию данных как средство противодействия угрозе логического вывода	113
<i>Ю.И. Горбенко, М.В. Есина, Д.В. Мялковський, О.С. Акользіна, В.А. Пономарь</i> Сучасні проблеми централізованих технологій типу «клієнт – сервер» та можливості їх удосконалення на основі децентралізації	131
<i>Н.А. Полуяненко, А.А. Кузнецов</i> Моделирование атаки двойной траты на протокол консенсуса «Proof of work»	146
<i>І.Д. Горбенко, О.В. Потій, Ю.І. Горбенко, А.І. Пушкарьов, М.В. Есіна</i> Принципи побудування та аналізу інфраструктур відкритого ключа на основі застосування технології блокчейн	162
<i>О.А. Замула</i> Оптимізація методів синтезу дискретних складних сигналів у сучасних багатокористувачевих системах зв'язку широкосмугового доступу	182
<i>Р.С. Гриньов, О.В. Северінов</i> Метод подолання засобів захисту з використанням вразливостей графічних файлів формату BMP	192
<i>В.А. Кулібаба</i> Порівняльний аналіз криптоперетворень на еліптичних кривих та кривих Едвардса	203
<i>А. Бессалов, Л. Ковальчук, Н. Кучинская, А. Телиженко</i> Стойкость модифицированной цифровой подписи EdDSA	209
<i>Д. Телевний</i> Применение хэш-функции Купина в схеме подписей SPHINCS+	215
РЕФЕРАТЫ	220

CONTENT

PERSPECTIVE CRYPTOGRAPHIC TRANSFORMATIONS AND THEIR APPLICATION

<i>I.D. Gorbenko, O.G. Kachko, O.M. Oleksijchuk, O.O. Kuznetsov, Yu.I. Gorbenko, V.V. Onoprienko, M.V. Yesina, S.O. Kandy</i> Algorithms of asymmetric encryption and encapsulation of keys of post-quantum period of 5 -7 stability stability levels and their applications	5
<i>I.I. Bobok, A.A. Kobozeva</i> Steganalysis method efficient for the hidden communication channel with low capacity	19
<i>I.D. Gorbenko, O.A. Zamula, V.L. Morozov, S.V. Rodionov</i> Mathematical model of orthogonal frequency distribution and multiplexing (OFDM) signals	32
<i>A.A. Kuznetsov, Yu.I. Gorbenko, V.V. Onoprienko, I.V. Stelnik, D.V. Myalkovsky</i> Cryptographic hashing algorithms used in modern blockchain systems	44
<i>A.A. Kuznetsov, Yu.I. Gorbenko, V.V. Onoprienko, I.V. Stelnik, D.V. Myalkovsky</i> The study of cryptographic hashing algorithms used in modern blockchain systems	54
<i>A.A. Kuznetsov, V.A. Timchenko, K.E. Lisitzky, M.Yu. Rodinko, M.S. Lutsenko, K.Yu. Shehanin, A.A. Kolgatin</i> The study of the speed and statistical security of cryptographic hashing algorithms	75

ANALYSIS AND USE OF CRYPTOGRAPHIC METHODS IN DECENTRALIZED TECHNOLOGIES

<i>K. Isirova, O. Potii, J. Claussen</i> Establishing trust protocols in mutual distrust network by consensus formation	96
<i>M. Osadchuk, R. Oliynykov</i> Method of Proof of Work consensus algorithms comparison	105
<i>V.I. Yesin, V.V. Vilihura</i> Some approach to data masking as means to counteract the inference threat	113
<i>Yu.I. Gorbenko, M.V. Yesina, D.V. Myalkovskiy, O.S. Akolzina, V.A. Ponomar</i> Modern problems of centralized technologies of the client-server type and possibilities of their improvement on the basis of decentralization	131
<i>N.A. Poluyanenko, A.A. Kuznetsov</i> Simulation of double spend attack on the “Proof of Work” consensus protocol	146
<i>I.D. Gorbenko, O.V. Potii, Yu.I. Gorbenko, A.I. Pushkarov, M.V. Yesina</i> Principles of building and analyzing public key infrastructures based on the use of blockchain technology	162
<i>A.A. Zamula</i> Optimization of the method for the synthesis of discrete folding signals in the most common bag-box-and-bag systems	182
<i>R.S. Grynov, A.V. Severinov</i> The method of overcoming protection using vulnerabilities of graphic files in BMP	192
<i>V. Kulibaba</i> Comparative analysis of cryptoprimitives on canonical elliptic curves and Edwards curves	203
<i>A. Bessalov, L. Kovalchuk, N. Kuchynska, O. Telizhenko</i> Security of modified digital public-key signature EdDSA	209
<i>D. Televnyi</i> The Kupyna hash function application to SPHINCS+ signatures	215
ABSTRACTS	220