СОДЕРЖАНИЕ

ПЕРСПЕКТИВНЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ И ПРОТОКОЛЫ
ПЕРСПЕКТИВНІ КРИПТОГРАФІЧНІ СИСТЕМИ ТА ПРОТОКОЛИ

И.Д. Горбенко, Е.Г. Качко, Ю.И. Горбенко, И.В. Стельник, С.А. Кандий, М.В. Есина Методы построения общесистемных параметров и ключей для NTRU PRIME UKRAINE 5 - 7 уровней стойкости. Product form 5

И.Д. Горбенко, А.Н. Алексейчук, О.Г. Качко, М.В. Есина, В.А. Бобух, С.О. Кандий, *В.А. Пономарь* Вычисление общих параметров для NTRU PRIME UKRAINE 6-7 уровней стойкости 17

Е.Г. Качко, Д.К. Телевный Криптоанализ хеш-функции Купина при использовании в схемах подписи Меркла 27

О.О. Кузнецов, Ю.І. Горбенко, М.С. Луценко, Д.І. Прокопович-Ткаченко, М.В. Пастухов NIST PQC: Кодові криптосистеми 32

О.А. Мельникова, О.В. Джурик, А.О. Маслєннікова Еліптичні криві Едвардса. Порівняння криптографічних бібліотек 41

І.Д. Горбенко, І.С. Кудряшов, В.В. Онопрієнко Порівняльний аналіз постквантових стандартів електронного підпису на основі мультиваріативних квадратичних перетворень 46

О.О. Кузнецов, Ю.І. Горбенко, А.С. Кіян, А.О. Уварова, Т.Ю. Кузнецова Порівняльні дослідження та аналіз ефективності гібридної кодової криптосистеми 61

А.А. Кузнецов, Е.П. Колованова, Д.И. Прокопович-Ткаченко, Т.Ю. Кузнецова Анализ и исследование свойств алгеброгеометрических кодов 70

Ю.І. Горбенко, Є.Ю. Каптьол Сутність та особливості реалізації методу Гровера на класичному комп'ютері для симетричного крипто аналізу 89

А.А. Кузнецов, А.В. Потий, Н.А. Полуяненко, С.Г. Вдовенко Комбинирующие и фильтрующие функции на основе регистров сдвига с нелинейными обратными связями 101

М.Ю. Родінко Оцінка стійкості симетричного блокового шифру «Кипарис» до диференційного криптоаналізу 113

А.А. Кузнецов, А.В. Потий, Н.А. Полуяненко, И.В. Стельник Нелинейные функции усложнения для потоковых симметричных шифров 125

МЕТОДЫ И АЛГОРИТМЫ ЗАЩИТЫ И СОКРЫТИЯ ИНФОРМАЦИИ
МЕТОДИ ТА АЛГОРИТМИ ЗАХИСТУ ТА ПРИХОВУВАННЯ ІНФОРМАЦІЇ

І.Ф. Аулов, К.Є. Лисицький Засоби моделювання та аналізу ризиків в середовищі хмарних обчислень 138

С.М. Конюшок Дослідження *k*-вимірності булевої функції шифру LILI-128 144

А.А. Кузнецов, И.В. Московченко, Д.И. Прокопович-Ткаченко, Т.Ю. Кузнецова Эвристические методы градиентного поиска криптографических булевых функций 150

Г.В. Ахмаметьєва, Мпуту Крістофер Бвабва Стеганоаналіз цифрових зображень в умовах різного ступеню наповненості контентів 165

Д.Г. Биличенко, Е.Ю. Витюк, Р.В. Олейников Сравнительный анализ алгоритмов консенсуса для технологии распределенных реестров 174

В.І. Єсін, В.В. Вілігура Метод розробки баз даних, що легко адаптуються до змін в предметній області 184

О.О. Кузнецов, О.О.Стефанович, Д.И. Прокопович-Ткаченко, К.О.Кузнецова 3D стеганографічне приховування інформації 193

Е.В. Исирова, А.В. Потий Децентрализованные протоколы консенсуса: возможности и рекомендации по применению 203

МЕТОДЫ ВЫЯВЛЕНИЯ, РАСПОЗНАВАНИЯ И УПРАВЛЕНИЯ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ
МЕТОДИ ВИЯВЛЕННЯ, РОЗПІЗНАВАННЯ ТА УПРАВЛІННЯ ЛІТАЛЬНИМИ АПАРАТАМИ

В.Н. Олейников, О.В. Зубков, В.М. Карташов, И.В. Корытцев, С.И. Бабкин, С.А. Шейко Исследование эффективности обнаружения и распознавания малоразмерных беспилотных летательных аппаратов по их акустическому излучению 209

І.Д. Горбенко, О.А. Замула, С.Г. Вдовенко, В.І Черниш Метод оцінки зрілості системи управління безпекою при організації повітряного руху 218

А.А. Кузнецов, Р.В. Сергиенко, А.А. Уварова Нечеткий экстрактор на помехоустойчивых кодах для биометрической криптографии 224

В.М. Карташов, В.Н. Олейников., С.А. Шейко, С.И. Бабкин, И.В. Корытцев., О.В. Зубков Особенности обнаружения и распознавания малых беспилотных летательных аппаратов 235

РЕФЕРАТЫ 244

CONTENT

PERSPECTIVE CRYPTOGRAPHIC SYSTEMS AND PROTOCOLS

I.D. Gorbenko, O.G. Kachko, Yu. I. Gorbenko, I.V. Stelnik, S.O. Kandy, M.V. Yesina Methods for constructing system-wide parameters and keys for NTRU PRIME UKRAINE 5 – 7 stabvility levels. Product form 5

I.D. Gorbenko, A.N. Alekseychuk, O.G. Kachko, M.V. Yesina, V.A. Bobukh, S.O. Kandy, V.A. Ponomar General parameters for NTRU PRIME UKRAINE 6 – 7 stability levels calculation 17

O. Kachko, D. Televnyi The Kupyna hash function cryptanalysis with Merkle Trees Signature schemes 27

A.A. Kuznetsov, Yu.I. Gorbenko, M.S. Lutsenko, D.I. Prokopovych-Tkachenko, M.V. Pastukhov NIST PQC: Code-Based Cryptosystems 32

O. Melnykova, O. Dzhuryk, A. Masliennikova Edwards elliptic curves. Comparison of cryptographic libraries 41

I.D. Gorbenko, I.S. Kudryashov, V.V. Onoprienko Comparative analysis of post quantum standards for electronic signature based on multivariate quadratic transformations 46

A.A. Kuznetsov, Y.I. Gorbenko, A.S. Kiian, A.A. Uvarova, T.Y. Kuznetsova Comparative studies and analysis of efficiency code-based hybrid cryptosystem 61

A.A. Kuznetsov, I.P. Kolovanova, D.I. Prokopovych-Tkachenko, T.Y. Kuznetsova Analysis and investigation of algebraic geometric codes properties 70

Yu.I. Gorbenko, Ye.Yu Kaptyol Essence and features of Grover's method implementation on a classical computer for symmetric cryptanalysis 89

A.A. Kuznetsov, A.V. Potii, N.A. Poluyanenko, S.G. Vdovenko Combining and filtering functions in the framework of nonlinear-feedback shift register 101

M.Yu. Rodinko Evaluation of block cipher "Cypress" strength against differential cryptanalysis 113

A.A. Kuznetsov, A.V. Potii, N.A. Poluyanenko, I.V. Stelnik Combining and filtering functions in the framework of nonlinear-feedback shift register 125

METHODS AND ALGORITHMS FOR PROTECTION AND CONCEALING INFORMATION

I.F. Aulov, K.E. Lisickiy Tools for modeling and analysis of risks in the cloud computing environment 138

S.M. Koniushok Investigation of the k-dimensionality of the LILI-128 cipher Boolean function 144

A.A. Kuznetsov, I.V. Moskovchenko, D.I. Prokopovych-Tkachenko, T.Y. Kuznetsova Heuristic methods for gradient search of cryptographic Boolean functions 150

A. V. Akhmametieva, Mputu Chrisopher Bwabwa Steganananalysis of digital images in conditions of varying degrees of contents fullness 165

D. Bilichenko, K. Vitiuk, R. Oliynykov Comparative analysis of consensus algorithms for distributed ledger technologies 174

V.I. Yesin, V.V. Vilihura Method for developing databases being easily adaptable to changes in the subject domain 184

A.A. Kuznetsov, O.O. Stefanovych, D.I. Prokopovych-Tkachenko, K.O. Kuznetsova 3D steganography hiding of information 193

K.V. Isirova, O.V. Potii Decentralized consensus protocols: possibilities and recommendations for use 203

METHODS FOR AIRCRAFT DETECTION, RECOGNITION AND CONTROL

V.N. Oleynikov, O.V. Zubkov, V.M. Kartashov, I.V. Korytsev, S.I. Babkin, S.A. Sheiko Investigation of the efficiency of detection and recognition of small-sized unmanned aerial vehicles by their acoustic radiation 209

I.D. Gorbenko,O.A. Zamula, S.G. Vdovenko, V.I. Chernysh Method of Maturity Assessment of Air Traffic Management Security System 218

A.A. Kuznetsov, R.V. Serhiienko, A.A. Uvarova Code based fuzzy extractor for biometric cryptography 224

V.M. Kartashov, V.N. Oleynikov, S.A. Sheyko, S.I. Babkin, I.V. Koryttsev, O.V. Zubkov Peculiarities of small unmanned aerial vehicles detection and recognition 235

ABSTRACTS 244