

ЗМІСТ

ПЕРСПЕКТИВНІ МЕТОДИ ТА СИСТЕМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

<i>А.М. Олексійчук, В.А. Кулібаба, М.В. Єсіна, С.О. Кандій, Є.В. Остряньська, І.Д. Горбенко</i> Обґрунтування перспективного постквантового національного стандарту електронного підпису на основі решіток	5
<i>О.Г. Качко, Ю.І. Горбенко, В.А. Пономар, М.В. Єсіна, С.О. Кандій</i> Оптимізація алгоритму множення поліномів для NTRU-подібних алгоритмів	15
<i>О.С. Шевчук</i> Рандомізована симетрична криптосистема Мак-Еліса на основі узагальнених кодів Ріда – Соломона	25
<i>А.В. Бессалов</i> Алгоритми і оцінки складності обчислень 3- і 5-ізогеній суперсингулярних кривих Едвардса (рос. мовою)	37
<i>М.Ю. Родінко, Р.В. Олійников</i> Дослідження продуктивності малоресурсного блокового шифру «Кипарис» на різних платформах	51
<i>О.О. Кузнецов, А.С. Кіян, А.І. Пушкарьов, Т.Ю. Кузнецова</i> Тестування кодових генераторів псевдовипадкових чисел для постквантового застосування	58
<i>К.Є. Лисицький, О.О. Кузнецов</i> Обчислювальні алгоритми розрахунку алгебраїчного імунітету нелінійних вузлів заміни симетричних шифрів (рос. мовою)	68

МЕТОДИ ТА МЕХАНІЗМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ БЛОКЧЕЙН

<i>І.Д. Горбенко, В.В. Онопрієнко, Ю.І. Горбенко, О.О. Кузнецов, К.В. Ісірова, М.Ю. Родінко</i> Проблеми, принципи побудови та перспективи розвитку національної системи електронного голосування в Україні	85
<i>І.Д. Горбенко, О.Г. Качко, Ю.І. Горбенко, М.В. Єсіна, С.О. Кандій, Є.В. Остряньська, А.С. Д'яченко</i> Можливості застосування механізмів повністю гомоморфного шифрування в системах електронного голосування	98
<i>П.І. Стеценко, Г.З. Халімов, Є.В. Котух</i> Аналіз площин атак на Blockchain системи (англ. мовою)	114
<i>І.Д. Горбенко, О.О. Кузнецов, М.О. Полуяненко, А.С. Кіян, К.Є. Лисицький, С.О. Кандій</i> Прототипування децентралізованої системи електронного блокчейн-голосування	122
<i>М.О. Полуяненко, О.О. Кузнецов</i> Аналітичне моделювання атаки подвійної витрати на блокчейн-системи із ймовірнісним протоколом консенсусу	140
<i>Н.А. Полуяненко, О.О. Кузнецов</i> Ймовірність успішної атаки подвійної витрати на блокчейн-системи із ймовірнісним протоколом консенсусу	153

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ В КОМУНІКАЦІЙНИХ СИСТЕМАХ

<i>І.Д. Горбенко, О.А. Замула</i> Теоретичні основи синтезу квазіортогональних систем складних сигналів (англ. мовою)	162
<i>І.Д. Горбенко, О.А. Замула, Хо Чі Лик</i> Методи пошуку оптимальних за мінімаксним критерієм систем складних нелінійних дискретних сигналів	175
<i>І.Є. Антіпов, Б.В. Бочаров, Д.Р. Найдьонова</i> Оцінка безпеки користувачів інтернет-банкінгу	188
<i>Р.С. Гриньов, О.В. Северінов, А.В. Власов</i> Метод виявлення та протидії вірусам у зображеннях формату BMP	195
<i>О.В. Циганкова</i> Аналіз можливостей використання алгоритму Ель-Гамалія з детермінованим внесенням для інкапсуляції ключей (англ. мовою)	201
РЕФЕРАТИ	206

CONTENT

PERSPECTIVE METHODS AND SYSTEMS OF CRYPTOGRAPHIC INFORMATION PROTECTION

<i>A.M. Oleksiychuk, V.A. Kulibaba, M.V. Yesina, S.O. Kandy, E.V. Ostryanska, I.D. Gorbenko</i> Substantiation of promising post-quantum national lattice-based electronic signature standard	5
<i>O.G. Kachko, Yu.I. Gorbenko, V.A. Ponomar, M.V. Yesina, S.O. Kandy</i> Optimization of polynomial multiplication algorithm for NTRU-like algorithms	15
<i>O.S. Shevchuk</i> Randomized symmetric McEliece cryptosystem based on generalized Reed-Solomon codes	25
<i>A.V. Bessalov</i> Algorithms and complexity evaluation of 3- and 5-isogeny calculation of super singular Edwards curves	37
<i>M.Yu. Rodinko, R.V. Oliynykov</i> The research of performance of the “Cypress” lightweight block cipher on different platforms	51
<i>A.A. Kuznetsov, A.S. Kiian, A.I. Pushkar’ov, T.Yu. Kuznetsova</i> Testing of code-based pseudorandom number generators for post-quantum application	58
<i>K. Lisitsky, O. Kuznetsov</i> Computational algorithms for calculating the algebraic immunity of nonlinear nodes of replacing symmetric ciphers	68

METHODS AND MECHANISMS OF CRYPTOGRAPHIC INFORMATION PROTECTION IN THE BLOCKCHAIN SYSTEM

<i>I.D. Gorbenko, V.V. Onoprienko, Yu.I. Gorbenko, A.A. Kuznetsov, K.V. Isirova, M.Yu. Rodinko</i> Problems, construction principles and development prospects of the national electronic voting system in Ukraine	85
<i>I.D. Gorbenko, O.G. Kachko, Yu.I. Gorbenko, M.V. Yesina, S.O. Kandy, E.V. Ostryanska, A.S. Dyachenko</i> Possibilities of using full homomorphic encryption mechanisms in electronic voting systems	98
<i>P.I. Stetsenko, G.Z. Khalimov, E.V. Kotukh</i> Analysis of planes of attacks on the Blockchain system	114
<i>I.D. Gorbenko, A.A. Kuznetsov, N.A. Poluyanenko, A.S. Kiyan, K.E. Lisitsky, S.A. Kandy</i> Prototyping decentralized electronic blockchain voting system	122
<i>N.A. Poluyanenko, A.A. Kuznetsov</i> Analytical modeling of the attack of double costs on a blockchain system with a probabilistic consensus protocol	140
<i>N.A. Poluyanenko, A.A. Kuznetsov</i> Probability of a successful attack of double costs on a blockchain system with a probabilistic consensus protocol	153

METHODS AND MEANS OF PROTECTION IN COMMUNICATION SYSTEMS

<i>I.D. Gorbenko, A.A. Zamula</i> Theoretical bases of synthesis of quasi-orthogonal systems of complex signals	162
<i>I.D. Gorbenko, A.A. Zamula, Ho Tri Luc</i> Methods of searching for systems of complex nonlinear discrete signals optimal by the minimax criterion	175
<i>I.E. Antipov, B.V. Bocharov, D.R. Naydenova</i> Estimate of the Internet banking user security	188
<i>R.S. Grynov, A.V. Sievierinov, A.V. Vlasov</i> Method for detecting and counteracting Virus Detection in BMP images	195
<i>O.V. Tsygankova</i> Analysis of possibility to use El Gamal algorithm with deterministic embedding for key encapsulation	201
ABSTRACTS	206