

СОДЕРЖАНИЕ

МЕТОДЫ СИНТЕЗА И АНАЛИЗА СИММЕТРИЧНЫХ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

<i>І.Д. Горбенко, Р.В. Олійников, О.В. Казимиров, В.І. Руженцев, О.О. Кузнєцов, Ю.І. Горбенко, О.В. Дирда, В.І. Долгов, А.І. Пушкаръов, Р.І. Мордвінов, Д.С. Кайдалов, В.М. Казимирова</i> Симетричний блоковий шифр „Калина” – новий національний стандарт України	5
<i>Р.В. Олійников, І.Д. Горбенко, О.В. Казимиров, В.І. Руженцев, О.О. Кузнєцов, Ю.І. Горбенко, О.В. Дирда, А.О. Бойко, В.І. Долгов, А.І. Пушкаръов, В.М. Казимирова, Р.І. Кіянчук</i> Функція гешування „Купина” – новий національний стандарт України	23
<i>А.Н. Алексейчук, С.В. Гришаков</i> Границы для скорости передачи информации в рандомизированных поточных шифрсистемах Михалевича – Имаи	31
<i>М.Ю. Родинко, К.Е. Лисицкий</i> Стратегия широкого следа без сепарабельных кодов	40
<i>І.Д. Горбенко, Р.І. Мордвінов</i> Порівняльний аналіз стійкості сучасних алгоритмів блокового симетричного шифрування	46

АСИММЕТРИЧНЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ И ИХ ПРИМЕНЕНИЕ

<i>І. Д. Горбенко, Р. С. Ганзя</i> Аналіз обчислювальної складності арифметико-геометричного методу обчислення кількості точок на еліптичній кривій	51
<i>А.В. Бессалов, О.В.Цыганкова</i> Производительность групповых операций на скрученной кривой Эдвардса над простым полем	58
<i>Л.В. Макутоніна</i> Гібридний метод направленного шифрування, який базується на ідентифікаторах і алгебраїчних решітках	64
<i>О.В. Шевцов</i> Сутність та оцінка стійкості криптографічних перетворень в NTRUSign	68
<i>М.В. Єсіна, І.Д. Горбенко</i> Використання системи GPS у багатофакторній автентифікації	79
<i>А.А.Кузнєцов, А.С.Швагер, Д.А.Фесенко</i> Соккрытие данных в кластерных файловых системах	86
<i>О. С. Акользіна, О.О. Бакликов</i> Порівняльний аналіз перспективних стандартів ЕП в групі точок еліптичних кривих	101

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

<i>І.Д. Горбенко, А.А. Замула, Е.А. Семенко</i> Ансамблевые и корреляционные свойства криптографических сигналов для приложений телекоммуникационных систем и сетей	110
<i>Г. К. Бронштак; А.Н. Ващенко, С. И. Доценко; Е. Л. Перчик</i> Парадигма защиты информации Игоря Громыко: гидродинамический ракурс	118
<i>Е.В. Котух, В.М. Карташов, О.Г. Халимов, Д.П. Цанко, А.В. Самойлова</i> Анализ современных требований к криптографическим примитивам нового поколения	133
<i>Р.О. Гаврилко, Ю.І. Горбенко</i> Квантовий генератор випадкових чисел на основі розщеплення пучка фотонів	143
РЕФЕРАТЫ	150

CONTENT

METHYODS OF SYNTHESIS AND ANALYSIS FOR SYMMETRIC CRYPTOGRAPHIC TRANSFORMATIONS

<i>I.D. Gorbenko, R.V. Oliynykov, O.V. Kazymyrov, V.I. Ruzhentzev, O.O. Kuznetsov, Y. I. Gorbenko, O. V. Dyrda, V. I. Dolgov, A.I. Pushkaryov, R. I. Mordvinov, D.S. Kaidalov, V. M. Kazymyrova</i> “Kalyna” block cipher – new Ukrainian national standard	5
<i>R.V.Oliynykov, I.D. Gorbenko, O.V. Kazymyrov, V.I. Ruzhentzev, O.O. Kuznetsov, Y. I. Gorbenko, O. V. Dyrda, A.O. Boiko, V. I. Dolgov, A.I. Pushkaryov, V. M. Kazymyrova, R. I. Kiyanchuk</i> “Kupyna” hash function – new Ukrainian national standard	23
<i>A.N. Alekseychuk, S.V. Gryshakov</i> Bounds on the information transmission rate in the Mihaljević-Imai randomized stream ciphers	31
<i>M.Yu. Rodinko, K.E. Lisitskiy</i> Wide trail strategy without separable codes	40
<i>I.D. Gorbenko, R.I. Mordvinov</i> Comparative analysis of stability of modern block symmetric ciphering algorithms	46

ASYMMETRIC CRYPTOGRAPHIC TRANSFORMATIONS AND THEIR APPLICATION

<i>I. D. Gorbenko, R. S. Hanzia</i> Analysis of the computational complexity of arithmetic geometric mean for calculating the number of points on the elliptic curve	51
<i>A.V. Bessalov, O.V. Tsygankova</i> Performance of batch operations on a twisted Edwards curve over a simple field	58
<i>L.V. Makutonina</i> Hybrid method of directional encryption based on identifiers and algebraic lattices	64
<i>O.V. Shevtsov</i> Essence and evaluation of resistance of cryptographic transformations in NTRUSign	68
<i>M.V. Yesina, I.D. Gorbenko</i> GPS system use in multi-factor authentication	79
<i>O.O.Kuznetsov, A.S.Shvaheer, D.A.Fesenko</i> Hiding of data in the cluster file systems	86
<i>O. Akolzina, O. Baklykov</i> Comparative analysis of ES prospective standarts in the group of points of eliptic curves	101

MEANS OF INFORMATION PROTECTION

<i>I.D. Gorbenko, A.A. Zamula, E.A. Semenko</i> Ensemble and correlation properties of cryptographic signals for telecom applications munication systems and networks	110
<i>G. K. Brodspec, A. N. Vashchenko, S. I. Dotsenko E. L. Perchik</i> Paradigm of information security by Igor Gromyko: a hydrodynamic perspective	118
<i>Y.V. Kotukh, V.M. Kartashov, O.G. Khalimov, D.P. Tsapko, A.V. Samoilova</i> Analysis of modern requirements to the new generation of cryptographic primitives	133
<i>R.O. Gavrilko, Yu.I. Gorbenko</i> Quantum random number generator based on splitting the beam of photons	143
ABSTRACTS	150