ЗМІСТ

МЕТОДИ ТА АЛГОРИТМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

І.Д. Горбенко, О.Г. Качко, О.В. Потій, А.М. Олексійчук, Ю.І. Горбенко, М.В. Єсіна, І.В. Стельник, В А. Пономар Основні положення та результати порівняння властивостей електронних підписів постквантового періоду на алгебраїчних решітках 5

А.М. Олексійчук, О.С. Шевчук Оцінки ефективності атак на основі підібраних відкритих текстів на криптосистему Рао-Нама над скінченною абелевою групою 22

О.О. Кузнецов, Г.В. Кононченко Стеганографічні методи в векторній графіці 32

М.В. Єсіна, Б.С. Шахов Аналіз апаратних реалізацій алгоритмів електронного підпису qTesla, Crystals-Dilitium і MQDSS на різних рівнях безпеки 42

В.В. Вілігура Аналіз формальних моделей управління доступом і особливості їх застосування для баз даних (*рос.*) 53

В.А Кулібаба Процеси та методи вибору загальносистемних параметрів та аналіз стійкості проти атак сторонніми каналами для алгоритму направленого шифрування та інкапсуляції ключів стандарту ДСТУ 8961:2019 (*англ.*) 71

Д.В. Гармаш Властивості багатовимірного алгоритму Rainbow та його здатність протистояти різноманітним методам криптоаналізу і атаці сторонніми каналами 79

Г.А. Малєєва Аналіз захищеності постквантового алгоритму електронного підпису Rainbow від потенційних атак 85

Є.В. Котух, О.В. Северинов, А.В. Власов, Л.С. Козіна, А.О. Теницька, Е. О. Зарудна Методи побудови та властивості логарифмічних підписів 94

ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ

Аль-Судані Хайдер Алі Принципи побудови гіроскопа на базі фотонно-кристалічних волокон з фотонною забороненою зоною (*рос.*) 100

К.С. Яцун Модифікація активної області резонансно-тунельного діоду 108

В.В. Рапін Похибка методів малого параметру при вирішенні укорочених рівнянь синхронізованого автогенератора (*рос.*) 113

АНТЕНИ ТА ПРИСТРОЇ МІКРОХВИЛЬОВОЇ ТЕХНІКИ

В.В. Должиков Поздовжній розподіл інтенсивності поля круглої сфокусованої апертури (*рос.*) 118

РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ

В.В. Жирнов, С.В. Солонська Метод перетворення символьних радарних відміток малопомітних рухомих об'єктів на основі ефекту Тальбота (*рос.*) 129

В.М. Карташов, В.О. Посошенко, В.В. Воронін, В.І. Колесник, А.І. Капуста, М.В. Рибников, Є.В. Першин Методи виявлення-розпізнавання радіолокаційних, акустичних, оптичних і інфрачервоних сигналів безпілотних літальних апаратів (*рос.*) 138

І.В. Свид, І.І. Обод, О.С. Мальцев, М.Г. Ткач, С.В. Старокожев, А.О. Глущенко, В.С. Чумак Метод підвищення завадозахищеності радіолокаційних систем ідентифікації «свій-чужий» при дії навмисних корельованих завад 154

РАДІОТЕХНІЧНІ ПРИСТРОЇ ТА ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ

Ю.Ю. Коляденко, М.О. Чурсанов Моделі поширення сигналів мереж зв'язку 5 G (*рос.*) 161

РАДІОТЕХНІЧНІ СИСТЕМИ

С.П. Сергієнко, В.Г. Крижановський, Д.В. Чернов, Л.В. Загорулько Ефективні режими роботи радіозакладних пристроїв для потайного знімання інформації у полі шумових завад 169

О.О. Кузнецов, О.А. Смирнов, Т.Ю. Кузнецова Шумоподібні дискретні сигнали для асинхронних систем кодового поділу радіоканалів (*рос.*) 175

РЕФЕРАТИ 184

CONTENT

METHODS AND ALGORITHMS OF CRYPTOGRAPHIC PROTECTION OF INFORMATION

I.D. Gorbenko, O.G. Kachko, O.V. Potii, A.M. Oleksiychuk, Yu.I. Gorbenko, M.V. Yesina, I.V. Stelnyk, V.A. Ponomar Basic principles and results of comparison of electronic signatures properties of the postquantum period based on algebraic lattices 5

A.N. Alekseychuk, O.S. Shevchuk Evaluation of effectiveness of chosen-plaintext attacks on the Rao - Nam cryptosystem over a finite Abelian group 22

A.A. Kuznetsov, Г.В. Кононченко Steganographic methods in vector graphics 32

M.V. Yesina, B.S. Shahov Analysis of hardware implementations of electronic signature algorithms qTesla, Crystals-Dilitium and MQDSS at different levels of security 42

V.V. Vilihura Analysis of formal models for access control and specific features of their applicability to databases 53

V.A. Kulibaba Processes and methods for selecting system-wide parameters and analysis of resistance against third-party channel attacks for the key encapsulation mechanism DSTU 8961:2019 71

D.V. Harmash Properties of the Rainbow multi-variant algorithm and its ability to resist various crypto-analysis methods and attack by outside channels 79

G.A. Maleeva Analysis of security of post-quantum algorithm of Rainbow electronic signature against potential attacks 85

E.V. Kotukh, O.V. Severinov, A.V. Vlasov, L.S. Kozina, A.O. Tenytska, E.O. Zarudna Methods of construction and properties of logariphmic signatures 94

PHYSICS OF INSTRUMENTS, ELEMENTS AND SYSTEMS

Al-Sudani Haider Ali Muse Principles of constructing gyroscopes based on photonic crystal (band-gap) fibers 100

K.S. Yatsun Modification of active region of resonant tunnel diode 108

V.V. Rapin Error of small parameter methods in solving shortened equations of a synchronized oscillator 113

ANTENNAS AND MICROWAVE DEVICES

V.V. Dolzhikov Longitudinal distribution of the field intensity of a circular focused aperture 118

RADIOLOCATION AND NAVIGATION

V. Zhyrnov, S. Solonskaya Method for transforming symbolic radar marks of low-noticeable moving objects based on the Talbot effect 129

V.M. Kartashov, V.A. Pososhenko, V.V. Voronin, V.I. Kolesnik, A.I. Kapusta, N.V. Rybnikov, E.V. Pershin Methods for detection-recognition of radar, acoustic, optical and infrared signals of unmanned aerial vehicles 138

I.V. Svyd, I.I. Obod, O.S. Maltsev, M.G. Tkach, S.V. Starokozhev, A.O. Hlushchenko, V.S. Chumak Method for increasing noise immunity of radar "friend or foe" identification systems under the action of intentional correlated interference 154

RADIO ENGINEERING DEVICES AND TELECOMMUNICATION METHODS

Yu.Yu. Kolyadenko, N.A. Chursanov 5 G communication network signal propagation models 161

RADIO ENGINEERING SYSTEMS

S.P. Serhiienko, V.G. Krizhanovski, D.V. Chernov, L.V. Zahoruiko Effective modes of operation of radio-bombing devices for covert information gathering in the field of noise interference 169

A.A. Kuznetsov, O.A. Smirnov, T.Y. Kuznetsova Noise-like discrete signals for asynchronous code division radio systems 175

ABSTRACTS 184