

CONTENTS

(Continued from front cover)

Garmash D.V., Baklykov O.O., Filatova N.V., Gorbenko I.D. Quantum cryptographic algorithms of electronic signature based on multivariate quadratic transformations.....215

METHODS AND MEANS OF INFORMATION SECURITY

Veklych S.G., Lavrovska T.V., Rassomakhin S.G. Statistical model of functioning an information transmission system using algebraic methods of processing pseudorandom codes.....226

Stetsenko P.I., Khalimov G.Z. Method of countering attacks on routing tables based on the botnet architectures for Bitcoin peer-to-peer network232

Stetsenko P.I., Perekopskiy A.A., Khalimov G.Z. Infrastructure attack on a Bitcoin peer-to-peer network.....240

Poluyanenko N.A. The searching of non-linear feedback shift registers forming a maximal length sequence.....245

Krasnobayev V.A., Koshman S.A., Yanko A.S. Methods of data control in a residual class system that are based on the principle of parallel nulevisation253

In memory of Aleksandr Alekseevich Zelenskiy (24.06 1943 – 15. 05. 2016).....266



APPLIED RADIO ELECTRONICS

Scientific and Technical Journal **2016 Volume 15 № 3**

**Special issue devoted to problems of ensuring
information security**

CONTENTS

METHODS AND MEANS OF ASYMMETRIC CRYPTOGRAPHIC TRANSFORMATIONS

Gorbenko I.D., Kachko O.G., Naumenko G.S. Experimental study of the possibility of using NTRUPrime parameters for asymmetric encryption in accordance with ANSI X9.98 – 2010 standard135

Bessalov A.V., Oleshko K.A., Porechna D.M., Tsygankova O.V., Chorny O.M. Secure twisted Edwards curves with minimal complexity of group operations.....141

Yesina M.V. Mathematical model of an anonymous electronic signature protocol based on identity151

Yesina M.V., Kulibaba V.A. Mathematical and program models of related keys attack implementation on electronic signature IBS-1 mechanism.....157

Kachko O.G., Televnyi D.K. Studying the possibility of using functional programming languages in modelling methods of cryptographic transformations162

Kuznetsov O.O., Lutsenko M.S., Andrushkevych A.V., Melkozerova O.M., Novikova D.V., Loban A.V. Statistical studies of modern stream ciphers.....167

METHODS AND MEANS OF SYMMETRIC CRYPTOTRANSFORMATIONS

Rodinko M.Yu., Oliynykov R.V. A mathematical model of non-injective key schedules properties evaluation of symmetric block ciphers.....179

Ruzhentsev V.I. Analysis of the method of proving the resistance of block ciphers to impossible differential attack184

Torba A.A., Bobuch V.A., Torba M.O., Torba A.O. Deterministic pseudorandom sequence generators for stream-based encryption D L R R191

POSTQUANTUM AND ELECTRONIC SIGNATURES

Kovaleva N.V., Gorbenko Yu.I. Analysis of postquantum digital signature schemes based on hash functions195

Ponomar V.A., Berezhnyi O.G. Fast algorithms for calculating isogeny of elliptic curves.....203

Харьковский национальный университет радиоэлектроники

Академия наук прикладной радиоэлектроники

ПРИКЛАДНАЯ РАДИОЭЛЕКТРОНИКА

Научно-технический журнал

И.о. главного редактора

Чурюмов Г.И.

Зам. главного редактора

Дохов А.И.

Редакционный совет

Гузь В.И., Довбня А.Н., Егоров А.М., Калугин В.В., Кравченко В.И.,
Назаренко И.П. (Россия), Неклюдов И.М., Пресняк И.С., Симонов К.Г. (Россия),
Симанков В.С. (Россия), Слипченко Н.И., Чабдаров Ш.М. (Россия),
Яковенко В.М., Ярошенко В.С. (Россия)

Редакционная коллегия

Абрамович Ю.И. (США), Бодянский Е.В., Борисов А.В., Буц В.А., Бых А.И.,
Гомозов В.И., Жуйков В.Я., Зарицкий В.И., Кипенский А.В., Кульпа К. (Польша),
Леховицкий Д.И., Литвинов В.В., Лукин К.А., Мачехин Ю.П.,
Модельский Й. (Польша), Нерух О.Г., Поляков Г.А., Ролинг Г. (Германия),
Седышев Ю.Н., Серков А.А., Сухаревский О.И., Чурюмов Г.И.,
Шифрин Я.С., Шкварко Ю.В. (Мексика)

Адрес редакции:

Редакция журнала «Прикладная радиоэлектроника»
Харьковский национальный университет радиоэлектроники
просп. Науки, 14, 61166, Харьков, Украина
Тел.: + 38 (057) 702 10 57
Факс: + 38 (057) 702 10 13
E-mail: are@nure.ua
<http://www.anpre.org.ua>