

Ежегодная международная научно-практическая конференция

«РусКрипто'2022»

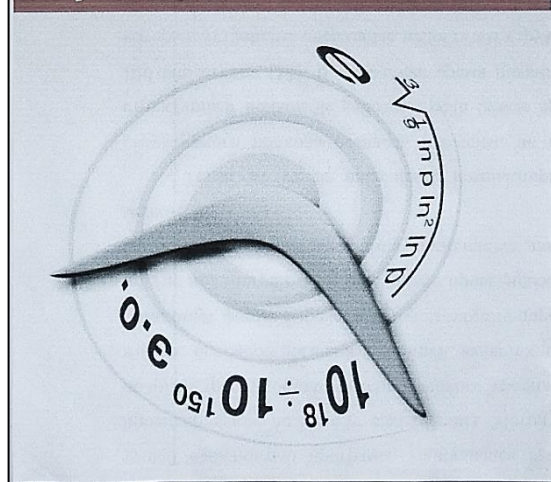
**Международное
сотрудничество «РусКрипто»**

Алексей Евгеньевич Жуков,
Ассоциация «РусКрипто»

Издание трудов конференции РусКрипто

Издание трудов конференции РусКрипто

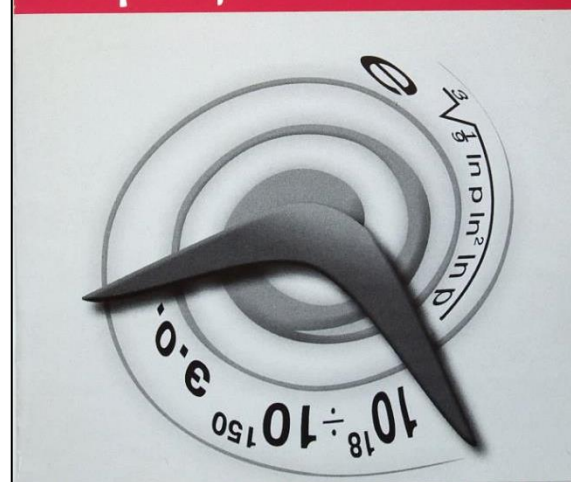
РусКрипто 2001



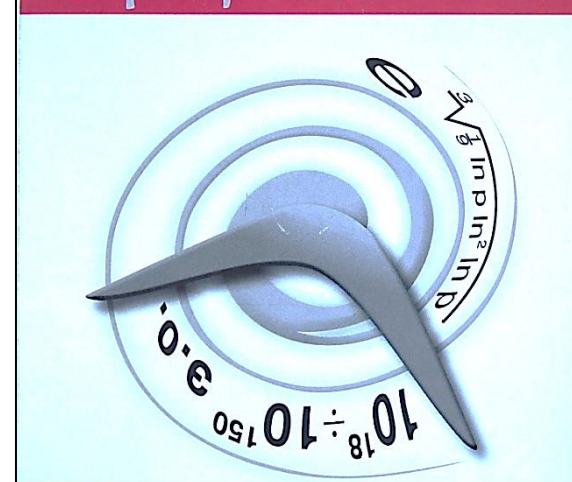
РусКрипто 2002



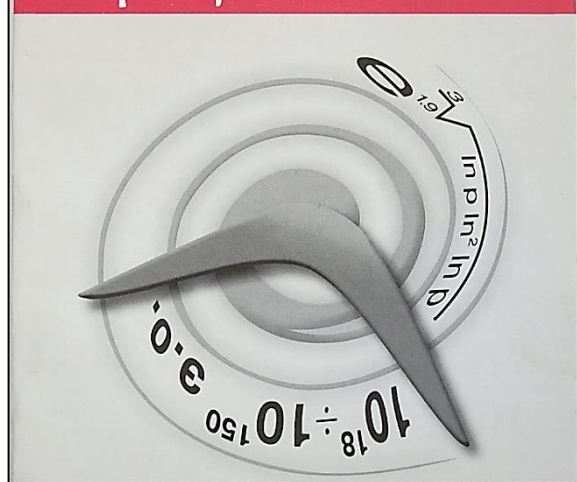
РусКрипто 2003



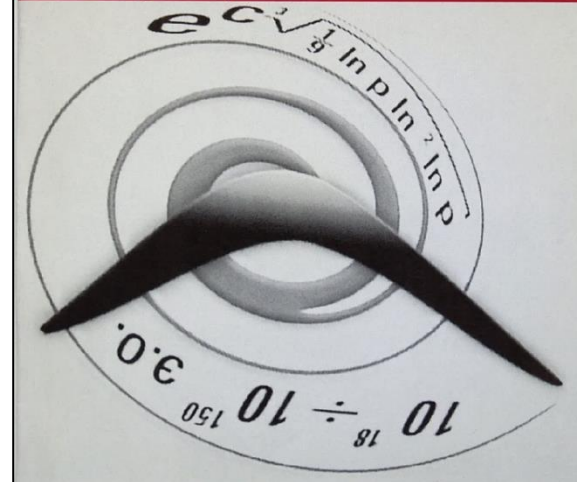
РусКрипто 2004



РусКрипто 2005



РусКрипто 2006



Издание трудов конференции РусКрипто

Компакт-диски с презентациями и тезисами докладов.

Сейчас материалы всех конференций РусКрипто доступны на сайте РусКрипто:

<http://www.ruscrypto.org/association/archive/>

The screenshot shows a web browser window displaying the archive page of the RusCrypto website. The browser's address bar shows the URL <https://www.ruscrypto.ru/association/archive/>. The website header includes a navigation menu with years from 2021 to 2014, a 'ЗАРЕГИСТРИРОВАТЬСЯ' button, and social media icons. The main content area features a green banner with binary code and the title 'АССОЦИАЦИЯ «РУСКРИПТО»'. Below the banner are three tabs: 'Новости и публикации', 'Материалы конференций' (which is selected), and 'Фотогалерея'. The 'Материалы конференций' section is titled 'МАТЕРИАЛЫ КОНФЕРЕНЦИЙ' and displays a grid of eight conference entries, each with a title, dates, and the number of presentations.

Конференция	Даты	Количество докладов
РусКрипто'2021	23.03.2021 – 26.03.2021	73 доклада
РусКрипто'2020	17.03.2020 – 20.03.2020	58 докладов
РусКрипто'2019	19.03.2019 – 22.03.2019	78 докладов
РусКрипто'2018	20.03.2018 – 23.03.2018	63 доклада
РусКрипто'2017	21.03.2017 – 24.03.2017	
РусКрипто'2016	22.03.2016 – 25.03.2016	
РусКрипто'2015	17.03.2015 – 20.03.2015	
РусКрипто'2014	25.03.2014 – 28.03.2014	

АССОЦИАЦИЯ «РУСКРИПТО»

[Главная](#) / [Материалы ассоциации](#) / [Материалы конференций](#)

[Новости и публикации](#)

[Материалы конференций](#)

[Фотогалерея](#)

МАТЕРИАЛЫ КОНФЕРЕНЦИЙ

[РусКрипто'2021](#)

23.03.2021 – 26.03.2021

73 доклада

[РусКрипто'2020](#)

17.03.2020 – 20.03.2020

58 докладов

[РусКрипто'2019](#)

19.03.2019 – 22.03.2019

78 докладов

[РусКрипто'2018](#)

20.03.2018 – 23.03.2018

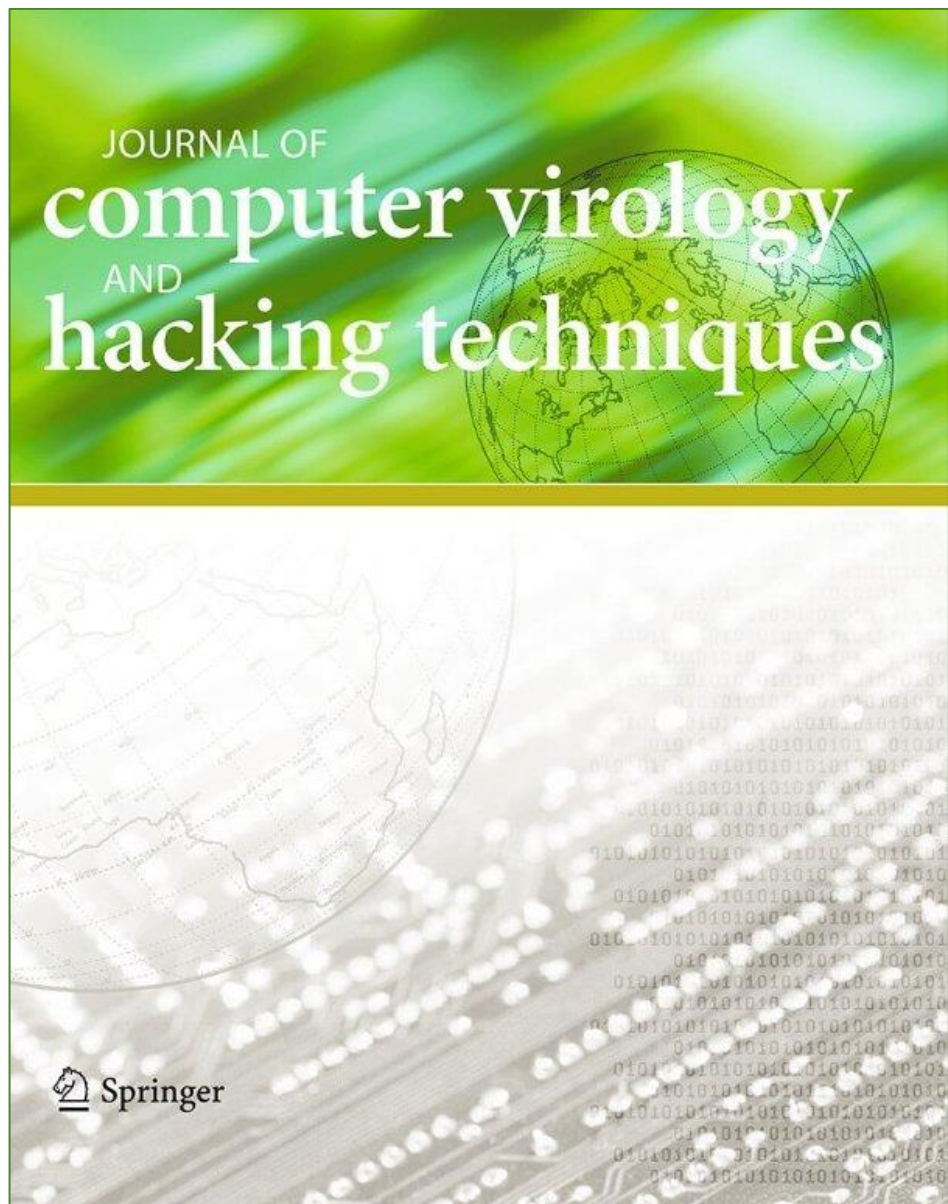
63 доклада

Издание трудов конференции РусКрипто





Springer

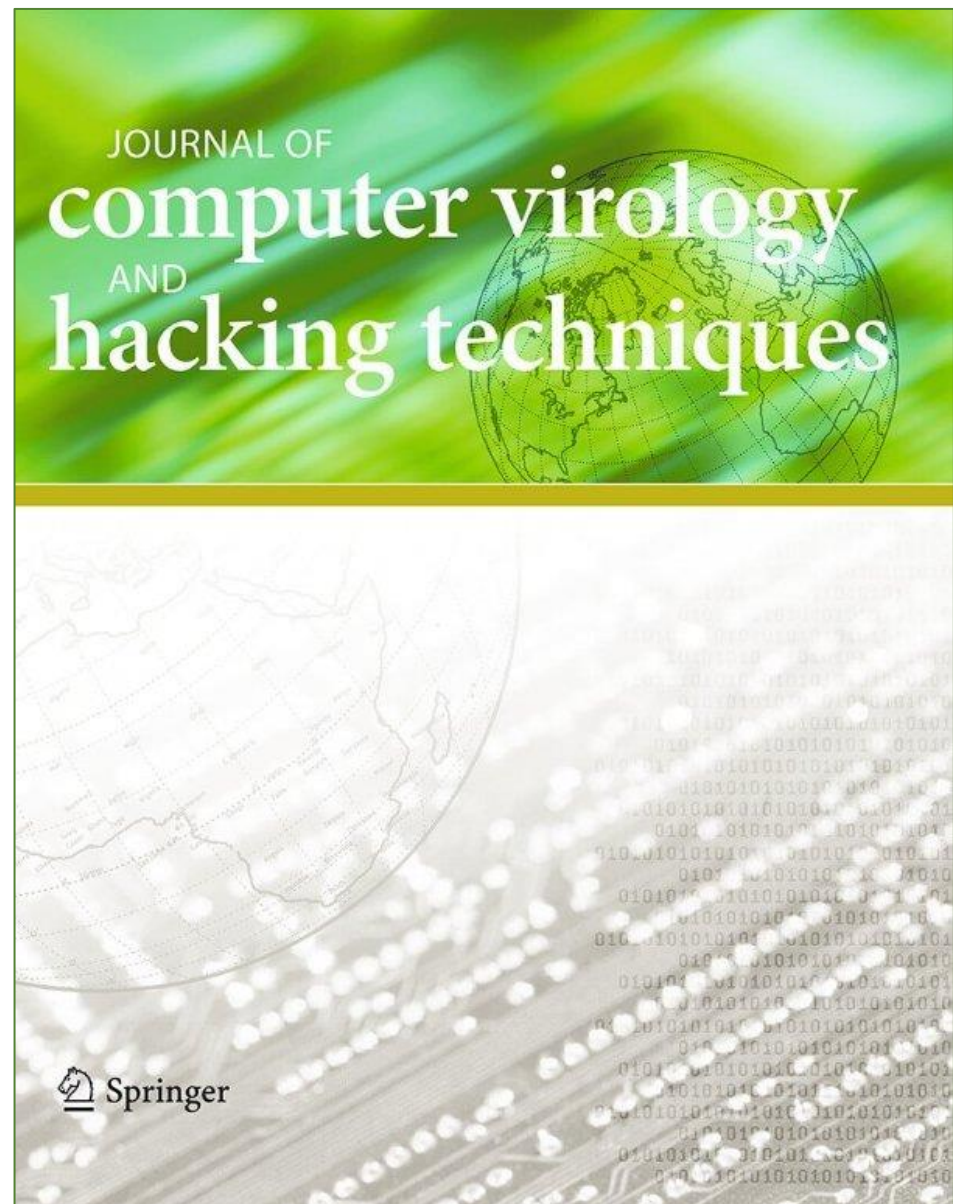


«Journal of Computer Virology» Volume 1, iss. 1-2 (November 2005)

С 2013 г.:

«Journal of Computer Virology and Hacking Techniques»

© Springer-Verlag France SAS,
part of Springer Nature



- ACM Digital Library
- CLOCKSS
- CNKI
- CNPIEC
- DBLP
- Dimensions
- EBSCO Discovery Service
- EI Compendex
- Emerging Sources Citation Index
- Google Scholar
- INSPEC
- Japanese Science and Technology Agency (JST)
- Naver
- OCLC WorldCat Discovery Service
- Portico
- ProQuest Advanced Technologies & Aerospace Database
- ProQuest-ExLibris Primo
- ProQuest-ExLibris Summon
- SCImago
- SCOPUS
- TD Net Discovery Service
- UGC-CARE List (India)



Название журнала	IF	Quartile in SJR Category (2020)	H-index
Journal of Computer Virology and Hacking Techniques	4.214	Computer Science (miscellaneous): Q1 Computational Theory and Mathematics: Q2 Hardware and Architecture: Q2 Software: Q2	37

ПОВЫШЕНИЕ ИНДЕКСА ХИРША

ГЛАВНАЯ - УСЛУГИ - ПОВЫШЕНИЕ ИНДЕКСА ХИРША



Сергей Сергеев

9 мар в 20:27

Уважаемые коллеги, наш авторский коллектив предлагает Вам стать соавторами научных статей или процитировать свои работы. В процессе подготовки к отправке в научные журналы следующие рукописи:

- 1) ВАК - экономика, цитата - 1000 руб (актуально до 13.03.22)
- 2) ВАК - лингвистика, место автора - 5000, цитата - 1000 руб
- 3) ВАК - психология, место автора - 5000 руб , цитата - 1000 руб

[Показать полностью...](#)

ПОВЫШЕНИЕ ИНДЕКСА ХИРША

Стоимость	от 1500 руб. (за одно цитирование)
Выполнение	от 3 месяцев
Срочно	от 2000 руб.

ПОВЫШЕНИЕ ИНДЕКСА ЦИТИРУЕМОСТИ В SCOPUS И WEB OF SCIENCE.

Стоимость	от 7000 руб.
Выполнение	от 5 месяцев
Оплата	100%

SCOPUSCOM.RU

ГЛАВНАЯ УСЛУГИ

Прайс, услуги, соавторство

Услуги, прайс

- публикация научных статей (технические науки) в изданиях, индексируемых в базе Scopus (Q4, Q3, Q2) от 24,5 т.р.;
- подготовка и публикация научных статей (В СОАВТОРСТВЕ), в изданиях, индексируемых в Scopus (технические, гуманитарные науки и др.) от 8,5 - 9,5 т.р.;
- публикация научных статей (гуманитарные науки и др.) в изданиях, индексируемых в базе Scopus (Q4, Q3, Q2) от 25 т.р.;
- публикация научных статей (технические науки) в изданиях, индексируемых в базе Web of Science (Q4, Q3, Q2) от 32 т.р.;

ПОВЫШЕНИЕ

ПОВЫШЕНИЕ ИНДЕКСА

в базе Scopus (Q4, Q3, Q2) от 24,5 т.р.;

индексируемых в Scopus (технические, гуманитарные науки и др.) от 8,5 - 9,5 т.р.;

индексируемых в базе Scopus (Q4, Q3, Q2) от 25 т.р.;

в базе Web of Science (Q4, Q3, Q2) от 32 т.р.;

от 7000 руб.

от 5 месяцев

ПОВЫШЕНИЕ ИНДЕКСА ИНДЕКСИРУЕМОСТИ В БАЗАХ SCOPUS И WEB OF SCIENCE.

Стоимость	от 7000 руб.
Выполнение	от 5 месяцев
Оплата	100%

Прайс, услуги, авторство

Услуги, прайс

- публикация научных статей (технические науки) в изданиях, индексируемых в базе Scopus (Q4, Q3, Q2) от 24,5 т.р.;
- подготовка и публикация научных статей (В СОАВТОРСТВЕ), в изданиях, индексируемых в Scopus (технические, гуманитарные науки и др.) от 8,5 - 9,5 т.р.;
- публикация научных статей (гуманитарные науки и др.) в изданиях, индексируемых в базе Scopus (Q4, Q3, Q2) от 25 т.р.;
- публикация научных статей (технические науки) в изданиях, индексируемых в базе Web of Science (Q4, Q3, Q2) от 32 т.р.;

ПОВЫШЕНИЕ ИНДЕКСА ХИРША

ГЛАВНАЯ - УСЛУГИ - ПОВЫШЕНИЕ ИНДЕКСА ХИРША



Сергей Сергеев
9 мар в 20:27

Уважаемые коллеги, наш авторский коллектив предлагает Вам стать автором научных статей или процитировать свои работы. В процессе подготовки к отправке в научные журналы следующие рукописи.

- 1) ВАК, цитата - 1000 руб (актуально до 13.03.22)
- 2) Вестник, место автора - 5000, цитата - 1000 руб
- 3) Вестник психологии, место автора - 5000 руб, цитата - 1000 руб

SCOPUSCOM.RU

ка, цитата - 1000 руб (актуально до 13.03.22)

тика, место автора - 5000, цитата - 1000 руб

я, место автора - 5000 руб, цитата - 1000 руб

- публикация научных статей

- публикация научных статей (технические науки) в журнале Web of Science (Q4, Q3, Q2) от 32 т.р.;

от 1500 руб.

цитирование)

от 3 месяцев

от 2000 руб.

ПОВЫШЕНИЕ ИНДЕКСА ХИРША

от 1500 руб. (за одно цитирование)

от 3 месяцев

от 2000 руб.

ПОВЫШЕНИЕ ИНДЕКСА

УСТОЙЧИВОСТИ В SCOPUS И WEB

SCIENCE.

от 7000 руб.

от 5 месяцев

100%



Сергей Сергеев
9 мар в 20:27

руб. (за одно

Уважаемые коллеги, наш авторский коллектив готов помочь вам в продвижении научных статей или процитировать свои работы в научных журналах. Для этого необходимо отправить в научные журналы следующие материалы:

- 1) ВАК - цитата, цитата - 1000 руб (акт)
 - 2) Вестник - цитата, место автора - 500 руб
 - 3) Вестник психологии - место автора - 5000 руб
- Получить полностью...

CORUSCOM.RU

ка, цитата - 1000 руб

тика, место авт

- публикация научных статей

- подготовка

- публикация научных статей

- публикация научных статей (технические науки) в журнале "Journal of Science (Q4, Q3, Q2) от 32 т.р.:

Повысим Ваш индекс Хирша в РИНЦ!



Всего 500 рублей за цитирование любой Вашей научной публикации.

Оставляйте заявку!
nauchnik.org

US И WEB

Название журнала	IF	Quartile in SJR Category (2020)	H-index
Journal of Computer Virology and Hacking Techniques	4.214	Computer Science (miscellaneous): Q1 Computational Theory and Mathematics: Q2 Hardware and Architecture: Q2 Software: Q2	37
Доклады Академии Наук. Математика	0.619	Mathematics (miscellaneous): Q2	27
Известия РАН. Серия математическая	1.189	Mathematics (miscellaneous): Q1	24
Математический сборник	0.986	Mathematics (miscellaneous): Q1	27
Успехи математических наук	1.909	Mathematics (miscellaneous): Q1	43

Название журнала	IF	Quartile in SJR Category (2020)	H-index
Алгебра и логика	0.753	Algebra and Number Theory: Q1 Logic: Q1 Analysis: Q2	26
Вестник Московского университета. Серия 1. Математика. Механика	0.153	Mathematics (miscellaneous): Q3	7
Математические заметки	0.673	Mathematics (miscellaneous): Q2	26
Теория вероятностей и ее применения	0.773	Statistics and Probability: Q3	32
Труды Математического института им. В. А. Стеклова	0.478	Mathematics (miscellaneous): Q2	23
Труды Московского мат. общества	1.417	Mathematics (miscellaneous): Q2	12

Название журнала	IF	Quartile in SJR Category (2020)	H-index
Дискретная математика	0.390	Applied Mathematics: Q3	14
Прикладная дискретная математика	0.425	Applied Mathematics: Q4 Computational Theory and Mathematics: Q4 Discrete Mathematics and Combinatorics: Q4 Signal Processing: Q4 (2020) Theoretical Computer Science: Q4	4
Проблемы передачи информации	1.082	Computer Networks and Communications: Q2 Computer Science Applications: Q2 Information Systems: Q2	19
Математические вопросы криптографии	0.413		

Название журнала	IF	Quartile in SJR Category (2020)	H-index
Journal of Cryptology	1.221	Applied Mathematics: Q1 Computer Science Applications: Q2 Software: Q2	77
Cryptologia	0.933	Applied Mathematics: Q4 Computer Science Applications: Q4	17
Designs, Codes, and Cryptography	1.492	Applied Mathematics: Q2 Computer Science Applications: Q2 Discr. Math. and Combinatorics: Q1 Theoretical Computer Science: Q2	61
International Journal of Information and Computer Security	0.842	Computer Networks and Communications: Q4 Hardware and Architecture: Q4 Safety, Risk, Reliability & Quality: Q3 Software: Q4	14
Journal of Mathematical Cryptology	0.643	Applied Mathematics: Q4 Computational Mathematics: Q4 Computer Science Applications: Q4	18

Название журнала	IF	Quartile in SJR Category (2020)	H-index
Journal of Computer Virology and Hacking Techniques	4.214	Computer Science (miscellaneous): Q1 Computational Theory and Mathematics: Q2 Hardware and Architecture: Q2 Software: Q2	37

**Издание трудов российских криптографов в журнале *Journal of Computer Virology and Hacking Techniques*.
Тематические выпуски.**

Journal of Computer Virology and Hacking Techniques.

Тематические выпуски.

Volume 16, issue 4, December 2020

**Special Issue: Russian Research in Cryptology and
Information Security Systems**

Issue editors: Vladimir M. Fomichev, Alisa M. Koreneva

9 научных статей

Journal of Computer Virology and Hacking Techniques.

Тематические выпуски.

Special Issue: Russian Research in Cybersecurity

Editor-in-Chief: Prof. Eric Filiol

Guest Editors: Vladimir M. Fomichev, Alisa M. Koreneva

Publication of the issue: 2022

Journal of Computer Virology and Hacking Techniques.

Тематические выпуски.

Volume 18, issue 1, March 2022

Special Issue: Ruscrypto 2020

Issue editor: Alexey E. Zhukov

– 7 научных статей

JOURNAL OF
computer virology
AND
hacking techniques



TABLE OF CONTENTS

VOLUME 18 • NUMBER 1 • MARCH 2022

EDITORIAL

EDITORIAL

A.E. Zhukov P.1

INVITED PAPERS

QUANTUM DIFFERENTIAL CRYPTANALYSIS

D. Denisenko P.3

HAMSI-BASED PARAMETRIZED FAMILY OF HASH-FUNCTIONS

K.D. Ermakov P.11

ORIGINAL PAPERS

IS MERKLE TREE THE BEST OPTION TO ORGANIZE KEYS?

A. Guselev · I. Lavrikov P.25

DATA INTEGRITY ALGORITHM BASED ON ADDITIVE GENERATORS AND HASH FUNCTION

V. Fomichev · D. Bobrovskiy · A. Koreneva · T. Nabiev · D. Zadorozhny P.31

INVITED PAPER

ON THE COMPARISON OF METHODS FOR ASYMMETRIC EXECUTION OF CRYPTOGRAPHIC PRIMITIVES AND PROTOCOLS IN THE CONTEXT OF USING SMALL PARAMETERS AND SHORT KEYS

A.A. Varfolomeev P.43

ORIGINAL PAPERS

MODIFICATION OF THE KEY SCHEDULE OF THE 2-GOST BLOCK CIPHER AND ITS IMPLEMENTATION ON FPGA

A. Dmukh · D. Trifonov · A. Chookhno P.49

ON THE IMPOSSIBILITY OF AN INVARIANT ATTACK ON KUZNYECHIK

D. Fomin P.61

- Denis Denisenko. *Quantum differential cryptanalysis.*
- Kirill Dmitrievich Ermakov. *Hamsi-based parametrized family of hash-functions.*
- Anton Guselev, Ivan Lavrikov. *Is Merkle tree the best option to organize keys?*
- Vladimir Fomichev, Dmitry Bobrovskiy, Alisa Koreneva, Timur Nabiev, Dmitry Zadorozhny. *Data integrity algorithm based on additive generators and hash function.*
- Alexander A. Varfolomeev. *On the comparison of methods for asymmetric execution of cryptographic primitives and protocols in the context of using small parameters and short keys.*
- A. Dmukh, D. Trifonov, A. Chookhno. *Modification of the key schedule of the 2-GOST block cipher and its implementation on FPGA.*
- Denis Fomin. *On the impossibility of an invariant attack on Kuznyechik.*



Eric Filiol

- **ENSIBS (Ecole Nationale Supérieure d'Ingénieurs Bretagne-Sud), Vannes, France**
- **Национальный исследовательский университет «Высшая школа экономики» (НИУ ВШЭ), Москва, РФ**



TABLE OF CONTENTS

SPECIAL ISSUE: RUSCRYPTO 2020

VOLUME 18 • NUMBER 1 • MARCH 2022

EDITORIAL

EDITORIAL
A.E. Zhukov P.1

INVITED PAPERS

QUANTUM DIFFERENTIAL CRYPTANALYSIS
D. Denisenko P.3

HANSI-BASED PARAMETRIZED FAMILY OF
HASH-FUNCTIONS
K.D. Ermakov P.11

ORIGINAL PAPERS

IS MERKLE TREE THE BEST OPTION TO
ORGANIZE KEYS?
A. Guselev · I. Lavrikov P.25

DATA INTEGRITY ALGORITHM BASED ON
ADDITIVE GENERATORS AND HASH FUNCTION
V. Fomichev · D. Bobrovskiy · A. Koreneva ·
T. Nabiev · D. Zadorozhny P.31

INVITED PAPER

ON THE COMPARISON OF METHODS FOR
ASYMMETRIC EXECUTION OF CRYPTOGRAPHIC
PRIMITIVES AND PROTOCOLS IN THE CONTEXT
OF USING SMALL PARAMETERS AND
SHORT KEYS
A.A. Varfolomeev

ORIGINAL PAPERS

MODIFICATION OF THE KEY SCHEDULE
OF THE 2-GOST BLOCK CIPHER AND ITS
IMPLEMENTATION ON FPGA
A. Dmukh · D. Trifonov · A. Chookhno

ON THE IMPOSSIBILITY OF AN INVARIANT
ATTACK ON KUZNYECHIK
D. Fomin



Indexed in DBLP (<http://dblp.uni-trier.de>)



Eric Filiol

Вопросы

