SECURITY code

10 CTCRYPT 2021

French-Russian Scientific Cooperation in Cryptography and Information Security

Fomichev Vladimir, Doctor of Physics and Mathematics, Professor

Koreneva Alisa, PhD in Physics and Mathematics

SECURITY code

Relevance

- Decree of the President of the Russian Federation on the conduct of "The **Year of Science and Technology** in the Russian Federation" off 25.12.2020 № 812;
- Security Council meeting dated 26.03.2021,
  President of the Russian Federation:

  "…Effective state policy realization implies a more active involvement of the scientific and business community. **To promote Russian approaches, it is essential to enhance the existing international discussion platforms and form the new ones both in Russia and abroad…**"

SECURITY code

Existing Achievements (1)

❑ Technical Committee for Standardization «Cryptography and Security Mechanisms» (TC 26):

- ✓ National Standardization:
  - cryptographic techniques, implementation issues and guidelines;
  - cryptographic protection of information technologies, including encryption, message authentication, digital signature, etc.
- ✓ Supporting the Russian national standardization body in developing international cryptographic standards.

SECURITY code

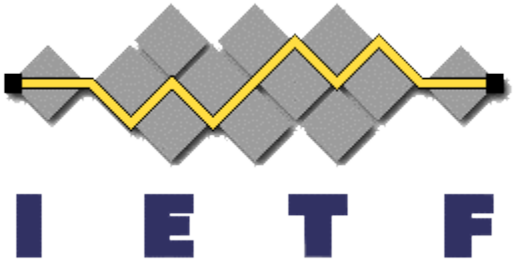
Existing Achievements (2)

- **The TC 26 sub-committee experts in “Information Security, Cybersecurity and Privacy Protection” (SC 27) of a joint technical committee (JTC 1) of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)**
  - ✓ Giving an international status to domestic cryptographic mechanisms
  - ✓ Analysis of the solutions offered by foreign colleagues
  - ✓ The expert review of the standards during their development and revision
  - ✓ Participation in development of regulatory documents regulating the security assessment of cryptographic algorithms

SECURITY code

Existing Achievements (3)

❑ TC 26 experts as part of the Internet Engineering Task Force (IETF):



- ✓ Co-leadership of the international research group titled ‘Crypto Forum Research Group’ (CFRG)
- ✓ Development of cryptographic mechanisms and recommendations (RFC) in all the fields of cryptography to be implemented in the Internet protocols

SECURITY code

Existing Achievements (4)

❑ CTCrypt Symposium:

- ✓ Current trends in cryptography (scientific papers, round table talks on up-to-date issues)
- ✓ Scientific support of the work on standardization
- ✓ The only Russian peer-reviewed conference on cryptography, which materials are published in English
- ✓ Comprehensive foreign representation

SECURITY code

New Project

- Collaboration with the French Scientific and Technical **Journal of Computer Virology and Hacking Techniques (JICV)**
- Editor-in-Chief – Professor **Éric Filiol** from France
- Special issues with results of Russian research on cryptography and information security

SECURITY code

Project Goal

Promoting Russian science abroad and raising awareness of international scientific community on Russian R&D

SECURITY code

About Editor-in-Chief

Éric Filiol

- Professor from France, PhD in Computer Science and Applied Mathematics
- Military crypto-analyst with 20 years of work experience, cyber security expert
- Author of over 45 scientific articles, 80 papers, 20 books and chapters
- Experienced speaker at European, Asian and Russian conferences, including RusCrypto and Positive Hack Days
- Associate member of HSE Univeristy, Faculty of Computer Science, Department of System Programming ISP RAS

SECURITY code

About JICV

- International Publishing House Sringer
- Second Quartile (Q2) Scopus
- Free Publication
- ~ 60 day from submission to publication
- Journal web-site: https://www.springer.com/journal/11416/

SECURITY code

JICV 1st Issue

with Russian Research Results

- Title: **Russian Research in Cryptology and Information Security Systems**
- Period of Work: July 2019 – December 2020
- Guest Editors: Vladimir Fomichev and Alisa Koreneva
- **2** articles from the editors, **8** original papers, **1** invited paper
- https://link.springer.com/journal/11416/volumes-and-issues/16-4

SECURITY code

Participants:
Authors and Reviewers

The project was supported by the authors and reviewers from over 20 organizations which include:

- Prominent Russian universities and institutes
- Technical Committee for Standardization “Cryptography and Security Mechanisms” (TC 26)
- Commercial companies-leaders at cryptography market and in information security

SECURITY code

Participants:

Universities and Institutes

LOMONOSOV MOSCOW STATE UNIVERSITY

MEPhI
NATIONAL RESEARCH NUCLEAR UNIVERSITY MEPHI
Moscow Engineering Physics Institute

FINANCIAL UNIVERSITY
UNDER THE GOVERNMENT OF THE RUSSIAN FEDERATION

HSE University

MIPT
MOSCOW INSTITUTE OF PHYSICS AND TECHNOLOGY

Bauman MOSCOW STATE TECHNICAL UNIVERSITY

POLYTECH
Peter the Great St.Petersburg Polytechnic University

P. G. Demidov Yaroslavl State University

Steklov Mathematical Institute of Russian Academy of Sciences

VLADIMIR STATE UNIVERSITY
NAMED AFTER ALEXANDER AND NIKOLAY STOLETOVS

SECURITY code

Participants:

Companies and Organizations

NPK KRYPTONITE

Real Security

SECURITY code

Requirements

- Compliance with international academic standards
- Original results on the topic of the special issue
- Well-structured paper with transparently described objectives, results and conclusions
- Comprehensive references
- Competent English
- Page range: 5-20 pages
- Formatting with the use of the LaTeX or Microsoft Word
- https://www.springer.com/journal/11416/submission-guidelines#Instructions%20for%20Authors

SECURITY code

Publishing Process

- **Springer Electronic Submission System**:
  submission --> review --> acceptance for publication
- 2-3 reviewers, **including Russian experts**
- **Reviewing is formalized**: reviewer's personal account, filling in a questionnaire, review submission, final decision on the paper
- **Several review iterations**
- **Final decision on the paper** is made by guest editors and approved by the Editor-in-Chief
- Successfully reviewed papers are published on the journal web-site (Springer Online First)

SECURITY code

Scientific Articles

- **[1] M. Cherepniov, Comparison of the complexity of Diffie–Hellman and discrete logarithm problems, pp. 265 – 268:**

  - The author presents an algorithm for discrete logarithm problem solution which uses an oracle solving the Diffie-Hellman problem.
  - The study result is extended to the integer factorization problem.
  - The relation between the complexities of the algorithms is determined.

SECURITY code

Scientific Articles

- **[2] L. Akhmetzyanova, E. Alekseev, E. Griboedova, and A. Sokolov, On post-handshake authentication and external PSKs in TLS 1.3, pp. 269 – 274:**

  - TLS 1.3 is the main Internet cryptographic protocol.
  - The post-handshake authentication is found to be vulnerable if more than one pair of entities possesses the same (external) PSK shared secret.
  - Several practical scenarios, where the required condition can be achieved, are provided, appropriate measures to prevent this vulnerability are proposed.

SECURITY code

Scientific Articles

- **[3] N. Shenets, Multi-party pairwise key agreement in linear number of Diffie–Hellman key exchanges, pp. 275 – 284:**

  - The author considers a classical problem of multi-party pairwise key agreement in the *n*-user group, when some parties are known to be compromised and the trusted key distribution and translation centers are inaccessible.
  - The proposed protocol requires a linearly varying number of Diffie-Hellman key exchanges. The efficiency of the protocol is proved by computational experiments.
  - The authors state the second secret-sharing protocol phase to be perfectly safe against semi-honest threshold adversary.

SECURITY code

Scientific Articles

- **[4] E. Alekseev, K. Goncharenko, and G. Marshalko, Provably secure counter mode with related-key-based internal re-keying, pp. 285 – 294:**

  - The authors study the Russian block cipher “Kuznyechik” in the related-key adversary model.
  - The block cipher new mode of operation with internal rekeying called CTRR is proposed.
  - The authors prove security of the proposed mode in the assumption that the underlying cipher (i.e. “Kuznyechik”) is secure in the related-key adversary model.

SECURITY code

Scientific Articles

- **[5] A. Urivskiy, M. Borodin, and A. Rybkin, Finding distinguishers for pseudorandom number generators based on permutations, pp. 295 – 303:**

  - Using a specific adversary model, the authors analyze the properties of a pseudorandom number generator (PRNG), based on two random permutations.
  - The characteristics for distinguishing such a PRNG from an ideal one are identified.
  - The PRNG on two permutations exhibits good probabilistic properties.

SECURITY code

Scientific Articles

- **[6] A. Nesterenko and A. Semenov, On the practical implementation of Russian protocols for low-resource cryptographic modules, pp. 305 – 312:**

  - The authors describe cryptographic mechanisms for secure interaction of control and measuring devices for key generation and for encrypted data exchange.
  - The authors thoroughly study the practical implementation for low-resource devices.
  - The performance evaluation results of the software developed by the authors are provided.

SECURITY code

Scientific Articles

- **[7] V. Vasenin, A. Itkes, M. Krivchikov, and E. Yavtushenko, ChRelBAC data access control model for large-scale interactive informational-analytical systems, pp. 313 – 331:**

  - The authors introduce an access control relational model (ChRelBAC) designed and implemented for a large scientometric system “ISTINA” [*].
  - Two software tools for the model support are described.
  - There is a discussion about the problem of testing the relational model on real data sets.

[*] Intellectual System of Topical Investigation od Scientometric Data

SECURITY code

Scientific Articles

- **[8] M. Kudinov, A. Chilikov, E. Kiktenko, and A. Fedorov, Advanced attribute-based encryption protocol based on the modified secret sharing scheme, pp. 333 – 341:**

  - The authors present two new cryptographic primitives:
    - for improving a well-known secret sharing scheme,
    - for designing an attribute-based encryption scheme.
  - The security proofs for both constructions are given.

SECURITY code

Invited Paper

- **E. Griboedova and V. Shishkin**,
  Not so long, but very rich: a history of Russian crypto standardization

- Multi-faceted history of Russian standardization in cryptography
- Contemporary Russian basic cryptographic mechanisms (algorithms, protocols, schemes), standardized in Russia, and cryptographic standards based on such mechanisms

Active standardization is of vital importance to the cryptographic sovereignty of a state.

SECURITY code

2021-2022: New Proposals

- **Selected Papers of RusCrypto Conference for 2018-2020**, eds. A.E. Zhukov and Yu.V. Malinin
- **Special Issue on Cybersecurity**, eds. A.M. Koreneva and V.M. Fomichev, requests for participation are accepted at: science@securitycode.ru

- International recognition and high estimate of Russian research results
- Involvement of European readers interested in information security and cryptography
- Promotion of Russian scientific solutions and proposals abroad

SECURITY code

Prospects

- ✓ Publication of academic papers in the prestigious journal and enhancement of scientific results globally
- ✓ Promotion of Russian scientists within the scientific environment
- ✓ Increasing international trust
- ✓ Russian expansion within the international scientific community, enhancing the country’s standing
- ✓ Involvement of the global scientific community to the objectives under consideration
- ✓ Open scientific discussion with foreign scientists and experts
- ✓ Participation of various scientific teams in joint work

SECURITY code

Conclusion

- **Acknowledgements extend to the authors, reviewers, Springer Publisher, Editor-in-Chief E. Filiol, A.A. Istomin, G.B. Marshalko, D.I. Zadorozhny and everyone who has contributed to the release of the issue.**

- **We look forward to prospective authors and reviewers to participate in new issues!**

КОД безопасности

Thank you for your attention!

science@securitycode.ru

+7 495 982 30 20, add. 404 (Alisa Koreneva)

https://www.securitycode.ru/