Editorial

Vladimir M. Fomichev^{1,2,3} · Alisa M. Koreneva¹

Published online: 8 October 2020

© Springer-Verlag France SAS, part of Springer Nature 2020

This *Journal of Computer Virology and Hacking Techniques* special issue covers works of Russian researchers on fundamental problems and applications of cryptography and information security. Cryptography, as one of the most science-intensive branches of information security, offers a fairly reliable approach to solving a wide range of secure data processing and storing problems.

Dating back to the fifteenth–sixteenth century, Russian cryptography has developed a considerable practical background. Since the eighteenth century (under the Empress Elisabeth of Russia), cryptographic methods have acquired a sound scientific foundation in Mathematics and later in Computer Sciences. Due to a vast experience accumulated through centuries, Russian researchers made significant advances in the field of information security as well as performed a detailed analysis of practical cryptographic problems.

Russia is looking forward to the cooperation with other countries based on the principles of open science. At present we are glad to accept the invitation of the French journal to publish Russian cryptography and information security studies. We present eight selected articles on different topics.

The article titled “*Comparison of the Complexity of Diffie-Hellman and Discrete Logarithm Problems*” presents an algorithm for discrete logarithm problem solution. The algorithm uses an oracle solving the Diffie-Hellman problem. The study result is also applied to the integer factorization problem. The relation between the complexities of the algorithms is determined.

The article “*On Post-Handshake Authentication and External PSKs in TLS 1.3*” deals with 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 easily achieved, will be provided in the article to illustrate the vulnerability. The authors propose appropriate measures to prevent this vulnerability.

The article “*Multi-Party Pairwise Key Agreement in Linear Number of Diffie-Hellman Key Exchanges*” 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.

The authors of the article “*Provably Secure Counter Mode with Related-Key-based Internal Re-keying*” present 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 its security in the assumption that the underlying cipher (e.g. Kuznyechik) is secure in the related-key adversary model.

The article “*Finding Distinguishers for Pseudorandom Number Generators Based on Permutations*” considers the properties of a pseudorandom number generator (PRNG), based on two random permutations, in a black-box setting. The characteristics for distinguishing such PRNG from an ideal one are identified. All distinguishers are also shown to require a very large amount of the PRNG output to analyze before they can tell the difference with high certainty, which indicated that the PRNG on two permutations exhibits very good probabilistic properties.

The authors of the article “*On the Practical Implementation of Russian Protocols for Low-Resource Cryptographic Modules*” describe cryptographic mechanisms for secure interaction of control and measuring devices. The mechanisms under study are designed for key information generation as well as for encrypted information exchange. The authors thoroughly study the practical implementation approach for low-resource devices and also solve several

✉ Alisa M. Koreneva
a.koreneva@securitycode.ru

¹ Security Code, LLC, Moscow, Russia

² Financial University Under the Government of the Russian Federation, Moscow, Russia

³ Federal Research Center “Informatics and Management” of the Russian Academy of Sciences, Moscow, Russia

technical problems. The performance evaluation results of the software developed by the authors will be provided in the body of the article.

The article “*ChRelBAC Data Access Control Model for Large-Scale Interactive Informational-Analytical Systems*” introduces an access control relational model (*ChRelBAC*) designed and implemented for a large scientometric system. The authors describe two software tools for the model support. The problem of testing the relational model on real data sets will be discussed in the article.

The authors of the article “*Advanced Attribute-based Encryption Protocol Based on the Modified Secret Sharing Scheme*” present the new constructions of two cryptographic primitives. The first construction improves a well-known secret sharing scheme. The second one is designed to allow an attribute-based encryption scheme. The security proofs for both constructions will be given in the body of the article.

All articles presented were thoroughly peer-reviewed by three independent anonymous experts. The final decision on articles was made by Guest Editors and the Editor-in-Chief.

The Editorial Team would like to express the acknowledgements to:

- the Authors—for submitting the scientific articles and for the efforts made to finalize them;
- the Reviewers—for their thorough work on article materials;
- the Springer Team—for prompt technical support.

Our appreciation also extends to A.A. Istomin, G.B. Marshalko, D.I. Zadorozhny and the management of Security Code, LLC. We thank the Editor-in-Chief, Professor Eric Filiol, for the opportunity to present works of Russian researchers in the *Journal of Computer Virology and Hacking Techniques*.

We hope that the materials of this collection will attract the attention of a wide range of readers interested in information security and cryptography.

Alongside with enriching our experience, the collaboration with the French journal allows our joint work on the further issues covered by the journal in the fields of cryptography and information security. The editorial team is looking forward to all kinds of comments and suggestions from the readers and will take them into account in future.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.