Ekaterina Maro

Date of birth:	October 24, 1987
E-mail:	marokat@gmail.com, eamaro@sfedu.ru
Phone:	+79185209219
Address:	App. 7, 24A Transportnaya str, Taganrog, Rostov region, 347927, Russia

Area of scientific interests

Cryptography, Cryptanalysis, Software and Hardware Information Security System, Personal Data Protection, Protocol Verification.

Education

PhD

"The development of algorithms based on algebraic cryptanalysis methods for the Feistel scheme", supervisor - Doctor of Science, Professor L.K. Babenko, 2016

Postgraduate course

"Methods and systems of information protection. Information Security", Southern Federal University, Taganrog, Rostov-on-Don region, 2009-2012

Master of Science
(Specialist Degree in Russia)

Information Security, Southern Federal University, Taganrog, Rostov-on-Don region, 2004-2009

Employment

Assistant, Department of Information Security, Southern Federal University, Taganrog, 2010 - 06/2017.

Associate Professor, Department of Information Security, Southern Federal University, Taganrog, 07/2017 - Present.

"Fundamentals of information security"
"Software and hardware protection of confidential information"
"Applying of PKI for e-commerce and electronic document management"
"Certification and licensing on information security"
"Reliability analysis of cryptographic data protection protocols"

Skills

- Knowledge of regulatory legal acts that establish requirements for the technical information protection.
- Compliance information systems and premises with legal requirements (security certification process for personal data (GDPR, Russian Federal Law №152) and confidential information).
- Development of organizational and administrative documents on information security (threat model, intruder model, access matrix, security instructions and etc.).
- Preparing and participation of the licensing by the Federal Service for Technical and Export Control (technical protection of confidential information) and the Federal Security Service of the Russian Federation (development, production, distribution of CIPF).
- Implementation of cryptographic tools: public key infrastructure ("CryptoPro" solutions), authentication tokens (eToken, RuToken), software license protections tools (HASP, Guardant).
- Verification of information security protocols by AVISPA, Scyther, ProVerif.

Research Experience

Researcher in scientific group of the Russian Foundation for Basic Research (RFBR) projects:

- “Research of reliability of symmetric encryption algorithms by methods of algebraic cryptanalysis” (Head - Maro E.A., №12-07-31032-mol_a);
- “Research and development of parallel algorithms for evaluating cryptographic protection of information” (Head - Professor of the Department of BIT, Dr. Babenko L.K., №09-07-00245-a);
- “Research of reliability modern hashing functions to different methods of analysis” (Head - Professor of the Department of IS, Dr. Babenko L.K., №12- 07-00037-a);
- “Assessment of vulnerability of modern cryptographic systems using analytical methods based on solving systems of equations” (Head - Associate Professor of the Department of IS, Ph.D. Ishchukova E.A., №12-07-33007- mol_a_ved);
- “Development and research of algorithms of fully homomorphic encryption” (Head - Professor of the Department of IS, Dr. Babenko L.K., №15-07-00597-a);
- “Development and research of parallel algorithms for evaluation of reliability of encryption standard GOST” (Head - Associate Professor of the Department of IS, Ph.D. Ishchukova E.A., №15-37-20007-mol_a_ved).
- “Research and development of models of safe interaction of participants on the basis of social networks in the gamified educational environment” (Head - Doctor of Science in physics and mathematics, Safonov K.V., №19-013- 00711-a).

Grant of the Russian Science Foundation (RSF) “Development and research of algorithms for assessing the strength of modern cryptographic tools based on the side channel attacks” (Head - Maro E.A., №19-71-00041).

Additional Education and Advanced Trainings

- Internship in JSC “Moscow department of Penza Research Electrotechnical Institute” theme “Verba PKI Certification Authority” (2010).
- Diploma of retraining “Enterprise economics and management” (2010).
- Seminar “Protection of personal data. The new legislation. Creating Protection Systems” (2010).
- Course “Multiprocessor computer systems and parallel programming” (2011).
- Course “Improving foreign language communicative competence (English, advanced level) administrative, scientific and pedagogical staff SfedU” (2011).
- Course “New information technologies in educational activities” (2011).
- Online Course “Cryptography I” (Stanford University, Coursera Inc., 2015).
- "Solving the problems of information security in stressful situations" ("Cybernetics", Plekhanov Russian Academy of Economics, 2017).
- "English for professional communication" (SFedU, 2017).
- Cisco CCNA “Routing and Switching” (netacad.com, 2017).
- E-learning system based on Moodle (SFedU, 2017).
- Online learning technologies in teacher activities (SFedU, 2017).
- Course “Basics of network technologies” (MEPhI, 2018).
- Course “Attack and protection of web and mobile applications”, GeekBrains, 2019, https://geekbrains.ru

- Course “Cryptography and Information Theory”, Coursera,2020, https://coursera.org/share/211f08e801f664d7b7ab095680652db3
- Course “The practice of using blockchain technologies in the medical industry”, MEPhI, 2020
- Course “Hardware security”, MIREA, 2020
- Course “Information security monitoring and incident management systems”, MIREA, 2020
- Course “Security analysis of information systems“, MTUCI, 2021
- Sber Digital Summer School. Track "Cybersecurity“, 2022
- Course “Secure Information Systems“, PSUTI, 2022
- CyberCamp, https://cybercamp.su/, 2022

Awards, Distinctions and Fellowships

- Winner of the All-Russian competition in the field of information security research of young professionals “INFOFORUM-NEW GENERATION” in the “Student of the Year” (2009).
- The Medal of the open competition of the Ministry of Education and Science of the Russian Federation “For the best student scientific work” (2009).
- Scholar Fund “Education and Science on Southern Federal Region” (2010).
- DAAD scholarship (2010), our group of graduate and postgraduate students have visited four technical universities: RWTH Aachen University (RWTH Aachen University), Darmstadt Centre for Advanced Security Research (CASED), University of Mannheim, Institute Horst Gërttsa Ruhr University in Bochum (HGI RUB).
- Finalist of competition young researcher of the conference “RusCrypto 2011”.
- Winner of the All-Russian competition in the field of information security work of young professionals “INFOFORUM-NEW GENERATION” in the "Young Professional of the Year" (2012).
- Scholar fund of the Russian Federation President's program to support young scientists and graduate students engaged in advanced research and development in priority areas of modernization of the Russian economy (2012- 2014).
- Honorable Diploma (team competition) of the Siberian Student’s olympiad in Cryptograhy with International Participation “NSUCRYPTO-2015” in category “professionals” (http://nsucrypto.nsu.ru/).
- Presentation at International Workshop on Cryptography, Robustness, and Provably Secure Schemes for Female Young Researchers «CrossFyre’2016», «CrossFyre’2019», TU, Darmstadt.
- Diploma for the 3rd place (team competition) of the Siberian Student’s olympiad in Cryptograhy with International Participation “NSUCRYPTO- 2016” in category “professionals” (http://nsucrypto.nsu.ru/).
- Participated in Workshop “Sage Days #82: Women in Sage”, France, January 9 - 13, 2017 (https://wiki.sagemath.org/days82).
- Member of program committee of International conference on Intelligent communication and computational techniques (https://icct.co.in/), International conference on Security of Information and networks (http://sinconf.org), International Conference on Next Gen Information Systems and Technologies (http://ngist18.com), International conference «Information Security» and All- Russian conference for young researcher «Perspectiva».
- Member of the Expert Council of the All-Russian Competition for Scientific and Technical Creativity of Youth "NTTM-2017".

- Prize of the Government of Rostov region for Youth researchers engaged in scientific and innovative activities (2015, 2017, 2018, 2020-2022).
- Ambassador Mail.Ru Group (2018-2019).
- Scholar fund of the Russian Federation President's program to support young scientists and graduate students engaged in advanced research and development in priority areas of modernization of the Russian economy (2019- 2021).

Publications

Researches presented at 81 papers, 20 of which were indexed in the Scopus database, section in Book «Theory and Practice of Cryptography Solutions for Secure Information Systems» (https://www.igi-global.com/book/theory-practice-cryptography-solutions-secure/73568)
Author Scopus ID 54684715000

1. Babenko L., Ischukova E., Maro E. Algebraic analysis of GOST encryption algorithm // Proceedings of the 4th international conference on Security of information and networks (SIN 2011), ACM, New York, NY, USA, ISBN: 978-1-4503-1020-8, pp. 57-62, doi: 10.1145/2070425.2070437
2. Babenko L., Ischukova E., Maro E. Research about Strength of GOST 28147-89 Encryption Algorithm // Proceedings of the 5th international conference on Security of information and networks (SIN 2012), ACM, New York, NY, USA, ISBN: 978-1-4503-1668-2, pp. 80-84, doi: 10.1145/2388576.2388595
3. Babenko L., Ischukova E., Maro E. GOST Encryption Algorithm and Approaches to its Analysis. Book "Theory and Practice of Cryptography Solutions for Secure Information Systems" // «IGI-Global», 2013, pp. 34-61, doi: 10.4018/978-1-4666-4030-6.ch002
4. Maro E., Ischukova E., Babenko L. Strength assessment of modern cryptosystems using methods of the analysis based on the solutions of combined equations // International Review on Computers and Software (IRECOS), Praise Worthy Prize, Vol. 10, №2 (2015), pp. 208-221, doi: 10.15866/irecos.v10i2.4676
5. Babenko L., Maro E., Anikeev M. Modeling of algebraic analysis of GOST+ cipher in SageMath // Proceedings of the 7th international conference on Security of information and networks (SIN 2016), ACM, New York, pp. 100-103, doi: 10.1145/2947626.2947656
6. Maro E., Kovalchuk M. Bypass Biometric Lock Systems With Gelatin Artificial Fingerprint // Proceedings of the 11th International Conference On Security Of Information and Networks (SIN'2018), ACM, New York, doi: 10.1145/3264437.3264439
7. Zolotarev V, Maro E., Kulikova S. New Approach to Activity Evaluation for Social Network Based Student Collaboration // 2018 IEEE 12th International Conference on Application of Information and Communication Technologies (AICT), Almaty, Kazakhstan, 2018, pp. 1-6, doi: 10.1109/ICAICT.2018.8747150.
8. Nissenbaum O., Maro E., Ischukova E., Zolotarev V. Markov and Semi-Markov Models of Real-Time Quests in Information Security Education // 2019 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russia, 2019, pp. 221-224, doi: 10.1109/USBEREIT.2019.8736621.
9. Krasovsky A., Maro E. Actual and Historical State of Side Channel Attacks Theory // Proceedings of the 12th International Conference On Security Of Information and Networks (SIN'2019), ACM, New York, doi: 10.1145/3357613.3357627
10. Zolotarev V., Povazhnyuk A., Maro E. Liveness detection methods implementation to face identification reinforcement in gaming services // Proceedings of the 12th International Conference On Security Of Information and Networks (SIN'2019), ACM, New York, doi: 10.1145/3357613.3357619

11. Ishchukova E., Maro E., Veselov G. Development of information security quest based on use of information and communication technologies // Proceedings of the 12th International Conference On Security Of Information and Networks (SIN'2019), ACM, New York, doi: 10.1145/3357613.3357632
12. Ishchukova E., Maro E., Pristalov P. Algebraic analysis of a simplified encryption algorithm GOST R 34.12-2015 // Computation, 2020, 8(2), 51, doi: 10.3390/computation8020051
13. Maro E. Modeling of algebraic analysis of PRESENT cipher by SAT solvers // IOP Conference Series: Materials Science and Engineering, 2020, doi: 10.1088/1757-899X/734/1/012101
14. Zhdanov S., Maro E. Power Analysis Side-Channel Attacks on Symmetric Block Cipher Magma // Proceedings of the 13th International Conference On Security Of Information and Networks (SIN'2020), ACM, New York, doi: 10.1145/3433174.3433601
15. Girichev V., Maro E. Power Analysis of Symmetric Block Cipher Kuznyechik // 2020 2nd International Conference on Computer Communication and the Internet, ICCCI 2020, 2020, стр. 106–109, doi: 10.1109/ICCCI49374.2020.9145964.
16. Safonov K., Zolotarev V., Romme N., Parotkin N., Maro E. An Approach to Phishing Attacks Modeling for Network Gamified Educational Projects // Proceedings of the 4th International Conference on Informatization of Education and E-learning Methodology: Digital Technologies in Education (IEELM-DTE 2020), Krasnoyarsk, Russia, October 6-9, 2020, pp 204-209 // https://ceur-ws.org/Vol-2770/paper24.pdf
17. Maro E., Girichev V., Us I. Power Analysis of Kuznyechik cipher on Arduino Nano board // Proceedings of the 2021 IEEE Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology, USBEREIT 2021, pp. 0440-0443, doi: 10.1109/USBEREIT51232.2021.9455095.

References

Babenko Ludmila Klimentevna
Doctor of Science, Professor
Department of Information Security, SfedU
e-mail: blk@tsure.ru
Tel./Fax: +7(8634) 312-018

Ishchukova Evgeniya
PhD, Associate Professor
Department of Information Security, SfedU
e-mail: jekky82@mail.ru
Tel./Fax: +7 9281435898

Anikeev Maxim
Senior Researcher at Fraunhofer Institute for Secure Information Technology SIT
Darmstadt, Hesse, Germany
e-mail: maxim.anikeev@gmail.com

Zolotarev Vyacheslav
PhD, Associate Professor
Department of Information Security,
Siberian State Aerospace University (SibSAU)
e-mail: amida.2@yandex.ru
Tel./Fax: +79059738091