Yuriy S. Polyakov

Curriculum Vitae

Email: ypolyakov@dualitytech.com

Web: https://ypolyakov.gitlab.io

May 2021

PERSONAL DATA

Citizenship: U.S.A.

Date of birth: September 3, 1980

RESEARCH INTERESTS

Encrypted computing; Applied lattice-based cryptography; Homomorphic encryption; Program obfuscation; Attribute-based encryption; Software engineering of cryptography libraries; Secure genome analysis

EDUCATION

2007	D.Sc. (Dr. habil.), Physics & Mathematics, Karpov Institute of Physical Chemistry
2004	Ph.D., Chemical Engineering, Moscow Polytechnic University
2003	M.Sc., Computer Science, New Jersey Institute of Technology
2002	B.Sc., Computer Information Systems, Excelsior College, University of the State of New York (Summa Cum Laude)

PROFESSIONAL EXPERIENCE

2017-present	Principal Scientist, *Duality Technologies, Inc.*, Newark, NJ
2016-2019	Associate Research Professor, Department of Computer Science & NJIT Cybersecurity Research Center, *New Jersey Institute of Technology (NJIT)*, Newark, NJ
2015-2016	Research Scientist (hosted by Shafi Goldwasser), Computer Science and Artificial Intelligence Laboratory, *Massachusetts Institute of Technology*, Cambridge, MA
2014-2016	Research Scientist, Department of Computer Science, *NJIT*, Newark, NJ
2014-2016	Principal Consultant, *Presidio Networked Solutions*, New York, NY
2012-2018	Adjunct Instructor, Department of Computer Science, *NJIT*, Newark, NJ
2008-2014	Senior Software Engineer/MIS Director, *Presidio Networked Solutions*, New York, NY
2007-2008	R&D Architect (Medical Informatics), *DiagnosisPlus LLC*, Seattle, WA
2005-2014	Research Scientist, *USPolyResearch*, Ashland, PA
2002-2005	Research Affiliate, Cryptography & Telecommunications Laboratory, Department of Computer Science, *NJIT*, Newark, NJ
1999-2007	Software Engineer/Systems Engineer, *MasTec North America Inc.*, Coral Gables, FL

VISITING POSITIONS

2019	Gratis Visitor, *Microsoft Research*, Redmond, WA
2018	Gratis Visitor, *Microsoft Research*, Redmond, WA
2003-2007	Visiting Researcher, *Moscow State University of Environmental Engineering (now Moscow Polytechnic University)*, Moscow, Russia

HONORS & AWARDS

2018	1st place, iDASH Privacy & Security 2018 - Track 2: Secure Parallel Genome Wide Association Studies using Homomorphic Encryption; with Marcelo Blatt, Alexander Gusev, Kurt Rohloff, and Vinod Vaikuntanathan
2008	Higher Attestation Commission of the Russian Federation (HACRF) Outstanding Habilitation Thesis Award
2007	Novel membrane filtration process developed in a paper for Journal of Membrane Science is recognized as a new research trend in the field (Membrane Technology, 2007, Issue 1)
2005	Moscow Mayor's Young Scientist Award

GRANTS & CONTRACT AWARDS

2020-2021	DARPA CSL, ACADEMY, Co-PI, Award: $1M.
2019-2020	IARPA Safe and Secure HECTOR subcontracted to Galois Inc., Senior Personnel. Proposed NJIT Award: $2.1M.
2018	NIH SBIR GEARS, Duality Technologies Award: $150K, Tech Lead, NIH Grant 1R43HG010123-01
2016-2018	IARPA Safe and Secure RAMPARTS Seedling, Subcontracted to Galois, Inc., Tech Lead, NJIT Award: $393K
2015-2019	DARPA I2O, SafeWare, PALISADE. $3.4M, Tech Lead, ARL contract W911NF-15-C-0226
2015-2019	DARPA I2O SafeWare, OPERA, Subcontracted to Applied Communication Sciences / Vencore Labs, Tech Lead, NJIT award: $674K, ARL contract W911NF-15-C-0233

SOFTWARE LIBRARIES & PROTOTYPES (CORE CONTRIBUTOR)

2014-present	PALISADE – Lattice cryptography library (C++): https://palisade-crypto.org
2005-present	Flicker-noise spectroscopy (time series analysis) toolkit [MATLAB]: https://gitlab.com/ypolyakov/fns
2010-2012	Signal analysis toolset for parameterizing nanosurfaces imaged by atomic force microscopy [MATLAB]
2007-2008	OsteoFile – AI computer software for generating, maintaining, and analyzing patient records for the diagnosis, prevention and treatment of osteoporosis [Python]
2006-2008	Software for simulating fast polymerization processes (numerical solution of systems of nonlinear partial differential equations) [Mathematica]

GRADUATE COURSES TAUGHT AT NJIT

2012-2018	Cryptography & Security (CS 608); Developed an online version in 2017
2012-2014	Data Structures & Algorithms (CS 610)
2013	Data Management System Design (CS 631)

EDITORIAL & REVIEW ACTIVITY

Program/Organizing Committee Member

2020	WAHC'20: 8th Workshop on Encrypted Computing & Applied Homomorphic Cryptography, Virtual Edition
2019	WAHC'19: 7th Workshop on Encrypted Computing & Applied Homomorphic Cryptography, London, UK
2018-present	HomomorphicEncryption.org - Homomorphic Encryption Standardization Consortium
2018	WAHC'18: 6th Workshop on Encrypted Computing & Applied Homomorphic Cryptography, Toronto, CA
2018	3rd Homomorphic Encryption Standardization Workshop, Toronto, CA
2016	WAHC'16: 4th Workshop on Encrypted Computing & Applied Homomorphic Cryptography, Barbados

Reviewer for Funding Agencies

NSF Secure and Trustworthy Cyberspace (SaTC); U.S. Civilian Research and Development Foundation (CRDF) [NSF]

Reviewer for Scholarly Journals

IEEE Transactions on Information Forensics & Security; IEEE Transactions on Computers; IEEE Access; Physica A; Journal of Membrane Science; International Journal of Communications, Network and System Sciences; Journal of Engineering Mathematics; Fluctuation and Noise Letters; JSUZ Computers & Electronics; Chemical Engineering Communications; Chemical Engineering Journal; Desalination; Desalination and Water Treatment; Ecological Engineering; Environmental Science: Water Research & Technology; Industrial & Engineering Chemistry Research; Journal of Chemical Technology & Biotechnology; Russian Journal of Electrochemistry; Russian Journal of Physical Chemistry; Separation Science and Technology; Theoretical Foundations of Chemical Engineering

Reviewer for Conferences

Crypto'21, Eurocrypt'21, Asiacrypt'20, PKC'20, Asiacrypt'19, Eurocrypt'19, CHES'17

INVITED TALKS/SEMINARS

2020	Practical Lattice-based Cryptography in PALISADE, Workshop "Lattices: From Theory to Practice", *Simons Institute for the Theory of Computing*, Berkeley, CA
2019	Efficient Lattice Trapdoor Sampling & Its Applications, *Microsoft Research*, Redmond, WA
2018	Cryptographic Program Obfuscation: Current Capabilities & Challenges, *Microsoft Research*, Redmond, WA
2018	An Improved RNS Variant of the BFV Homomorphic Encryption Scheme, 2nd Homomorphic Encryption Standardization Workshop, Computer Science and Artificial Intelligence Laboratory, *Massachusetts Institute of Technology*, Cambridge, MA
2018	Fully Homomorphic Encryption and Cryptographic Program Obfuscation: Current Capabilities and Challenges, Department of Computer Science Seminar, *New Jersey Institute of Technology*, Newark, NJ
2017	The PALISADE Project, Homomorphic Encryption Standardization Workshop, *Microsoft Research*, Redmond, WA
2017	The PALISADE Project, *5th Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC'17)*, Malta
2013	Analysis of Brain Activity Signals: Application to the Diagnosis of Schizophrenia and Photosensitive Epilepsy; Mathematical Biology Seminar, Department of Mathematical Sciences, *New Jersey Institute of Technology*, Newark, NJ
2012	Biomedical Signal Analysis: Application to the Diagnosis of Schizophrenia and Photosensitive Epilepsy; Seminar at Computational Biology Center, *IBM T. J. Watson Research Labs*, Yorktown Heights, NY
2009	Sustainable Development of Hot Deserts; Seminar: Columbia Water Center Seminar; Columbia Water Center, Earth Institute, *Columbia University*, New York, NY
2007	Nonlinear Models of Mass Transfer in Pressure-Driven Processes; Seminar: Nonlinear Dynamics of Chemical Reactions, Processes, and Reactors; Chemistry Department, *Moscow State University*
2007	Nonuniform Particle Deposition on External and Internal Surface of Semipermeable Membranes; *Russian University of Chemical Technology*
2007	Nonuniform Particle Deposition on External and Internal Surface of Semipermeable Membranes; *Moscow State University of Environmental Engineering*

GRADUATE STUDENT ADVISING

2020	Thesis Comittee Member: Gyana Sahu, PhD, NJIT; Summer 2020
2020	Thesis Comittee Member: Gerard W. Ryan, PhD, NJIT; Summer 2020
2019	Thesis Comittee Member: Kamil Doruk Gur, MSc, NJIT; Thesis: Efficient Lattice Trapdoors and Their Applications
2015	Thesis Comittee Member: Mayur Agarkar, MSc, NJIT; Thesis: Advanced Encryption Standard Hybrid Key Chaining; Won NJIT Graduate Student Poster Showcase Award
2007	Adviser: Valeria Kotenko, MSc; Thesis: Design of Telecommunications Infrastructure for Internet Service Providers; Defended at Saint-Petersburg State University of Telecommunications

SELECTED PROFESSIONAL CERTIFICATES

2002-present	Certified Computing Professional, ICCP
2001	Microsoft Certified Systems Engineer (Windows 2000 Track – Early Achiever Certificate)
1999	Microsoft Certified Systems Engineer (Windows NT 4.0 Track)

FOREIGN LANGUAGES

Native Russian and fluent French

Publications

Selected Recent Papers

1. Geva, R., B. Waissengrin, D. Mirelman, F. Bokstein, D. T. Blumenthal, I. Wolf, S. Pelles, Z. Duchin, L. Liram, Y. Polyakov, and M. Blatt (2021). Verification of Statistical Oncological Endpoints on Encrypted Data: Confirming the Feasibility of Real-World Data Sharing without the Need to Reveal Protected Patient Information. In: *2021 ASCO Annual Meeting, Journal of Clinical Oncology*. Vol. 39. Suppl 15, pp.e18725. https://meetinglibrary.asco.org/record/199851/abstract.
2. Blatt, M., A. Gusev, Y. Polyakov, and S. Goldwasser (2020). Secure large-scale genome-wide association studies using homomorphic encryption. *Proceedings of the National Academy of Sciences* **117**(21), 11608–11613. eprint: https://www.pnas.org/content/117/21/11608.full.pdf.
3. Blatt, M., A. Gusev, Y. Polyakov, K. Rohloff, and V. Vaikuntanathan (2020). Optimized Homomorphic Encryption Solution for Secure Genome-Wide Association Studies. *BMC Medical Genomics* **13**(83). https://eprint.iacr.org/2019/223.
4. Chen, C., N. Genise, D. Micciancio, Y. Polyakov, and K. Rohloff (2020). Implementing Token-Based Obfuscation under (Ring) LWE. Accepted to WAHC'20; https://eprint.iacr.org/2018/1222.
5. Archer, D. W., J. M. Calderón Trilla, J. Dagit, A. Malozemoff, Y. Polyakov, K. Rohloff, and G. Ryan (2019). RAMPARTS: A Programmer-Friendly System for Building Homomorphic Encryption Applications. In: *Proceedings of the 7th ACM Workshop on Encrypted Computing & Applied Homomorphic Cryptography*. WAHC'19. London, United Kingdom: ACM, pp.57–68. http://doi.acm.org/10.1145/3338469.3358945.
6. Badawi, A. A., Y. Polyakov, K. M. M. Aung, B. Veeravalli, and K. Rohloff (2019). Implementation and Performance Evaluation of RNS Variants of the BFV Homomorphic Encryption Scheme. *IEEE Transactions on Emerging Topics in Computing*. https://eprint.iacr.org/2018/589, to appear.
7. Genise, N., D. Micciancio, and Y. Polyakov (2019). Building an Efficient Lattice Gadget Toolkit: Subgaussian Sampling and More. In: *Advances in Cryptology – EUROCRYPT 2019*. Ed. by Y. Ishai and V. Rijmen. https://eprint.iacr.org/2018/946. Cham: Springer International Publishing, pp.655–684.
8. Gür, K. D., Y. Polyakov, K. Rohloff, G. W. Ryan, H. Sajjadpour, and E. Savaş (Apr. 2019). Practical Applications of Improved Gaussian Sampling for Trapdoor Lattices. *IEEE Transactions on Computers* **68**(4), 570–584.
9. Halevi, S., Y. Polyakov, and V. Shoup (2019). An Improved RNS Variant of the BFV Homomorphic Encryption Scheme. In: *Topics in Cryptology – CT-RSA 2019*. Ed. by M. Matsui. Cham: Springer International Publishing, pp.83–105.
10. Cousins, D. B., G. D. Crescenzo, K. D. Gür, K. King, Y. Polyakov, K. Rohloff, G. W. Ryan, and E. Savas (May 2018). Implementing Conjunction Obfuscation Under Entropic Ring LWE. In: *2018 IEEE Symposium on Security and Privacy (SP)*, pp.354–371.
11. Dai, W., Y. Doröz, Y. Polyakov, K. Rohloff, H. Sajjadpour, E. Savaş, and B. Sunar (May 2018). Implementation and Evaluation of a Lattice-Based Key-Policy ABE Scheme. *IEEE Transactions on Information Forensics and Security* **13**(5), 1169–1184.
12. Gür, K. D., Y. Polyakov, K. Rohloff, G. W. Ryan, and E. Savas (2018). Implementation and Evaluation of Improved Gaussian Sampling for Lattice Trapdoors. In: *Proceedings of the 6th Workshop on Encrypted Computing & Applied Homomorphic Cryptography*. WAHC '18. Toronto, Canada: ACM, pp.61–71. http://doi.acm.org/10.1145/3267973.3267975.
13. Hallman, R. A., K. Laine, W. Dai, N. Gama, A. J. Malozemoff, Y. Polyakov, and S. Carpov (2018). Building Applications with Homomorphic Encryption. In: *Proceedings of the 2018 ACM SIGSAC Conference on Com-*

puter and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018, pp.2160–2162. http://doi.acm.org/10.1145/3243734.3264420.

14. Borcea, C., A. B. D. Gupta, Y. Polyakov, K. Rohloff, and G. Ryan (2017). PICADOR: End-to-end encrypted Publish–Subscribe information distribution with proxy re-encryption. *Future Generation Computer Systems* **71**, 177–191.
15. Polyakov, Y., K. Rohloff, G. Sahu, and V. Vaikuntanathan (Sept. 2017). Fast Proxy Re-Encryption for Publish/Subscribe Systems. *ACM Trans. Priv. Secur.* **20**(4), 14:1–14:31.

Manuscripts

1. Kim, A., Y. Polyakov, and V. Zucca (2021). *Revisiting Homomorphic Encryption Schemes for Finite Fields*. Cryptology ePrint Archive, Report 2021/204. https://eprint.iacr.org/2021/204.
2. Kim, A., A. Papadimitriou, and Y. Polyakov (2020). *Approximate Homomorphic Encryption with Reduced Approximation Error*. Cryptology ePrint Archive, Report 2020/1118. https://eprint.iacr.org/2020/1118.
3. Micciancio, D. and Y. Polyakov (2020). *Bootstrapping in FHEW-like Cryptosystems*. Cryptology ePrint Archive, Report 2020/086. https://eprint.iacr.org/2020/086.

Refereed Journal Papers

1. Blatt, M., A. Gusev, Y. Polyakov, and S. Goldwasser (2020). Secure large-scale genome-wide association studies using homomorphic encryption. *Proceedings of the National Academy of Sciences* **117**(21), 11608–11613. eprint: https://www.pnas.org/content/117/21/11608.full.pdf.
2. Blatt, M., A. Gusev, Y. Polyakov, K. Rohloff, and V. Vaikuntanathan (2020). Optimized Homomorphic Encryption Solution for Secure Genome-Wide Association Studies. *BMC Medical Genomics* **13**(83). https://eprint.iacr.org/2019/223.
3. Badawi, A. A., Y. Polyakov, K. M. M. Aung, B. Veeravalli, and K. Rohloff (2019). Implementation and Performance Evaluation of RNS Variants of the BFV Homomorphic Encryption Scheme. *IEEE Transactions on Emerging Topics in Computing*. https://eprint.iacr.org/2018/589, to appear.
4. Gür, K. D., Y. Polyakov, K. Rohloff, G. W. Ryan, H. Sajjadpour, and E. Savaş (Apr. 2019). Practical Applications of Improved Gaussian Sampling for Trapdoor Lattices. *IEEE Transactions on Computers* **68**(4), 570–584.
5. Dai, W., Y. Doröz, Y. Polyakov, K. Rohloff, H. Sajjadpour, E. Savaş, and B. Sunar (May 2018). Implementation and Evaluation of a Lattice-Based Key-Policy ABE Scheme. *IEEE Transactions on Information Forensics and Security* **13**(5), 1169–1184.
6. Borcea, C., A. B. D. Gupta, Y. Polyakov, K. Rohloff, and G. Ryan (2017). PICADOR: End-to-end encrypted Publish–Subscribe information distribution with proxy re-encryption. *Future Generation Computer Systems* **71**, 177–191.
7. Polyakov, Y., K. Rohloff, G. Sahu, and V. Vaikuntanathan (Sept. 2017). Fast Proxy Re-Encryption for Publish/Subscribe Systems. *ACM Trans. Priv. Secur.* **20**(4), 14:1–14:31.
8. Polyakov, Y. S., G. V. Ryabinin, A. B. Solovyeva, and S. F. Timashev (July 2015). Is It Possible to Predict Strong Earthquakes? *Pure and Applied Geophysics* **172**(7), 1945–1957.
9. Polyakov, Y. S. (July 2014). Pore constriction in ultrafiltration: A discrete multilayer deposition model with steric exclusion of solutes at the pore inlet. *Theoretical Foundations of Chemical Engineering* **48**(4), 382–396.
10. Verkhovsky, B. and Y. Polyakov (2014). Binary Division Attack for Elliptic Curve Discrete Logarithm Problem. *Transactions on Networks and Communications* **2**(4), 1–15.
11. Litak, G., Y. S. Polyakov, S. F. Timashev, and R. Rusinek (2013). Dynamics of stainless steel turning: Analysis by flicker-noise spectroscopy. *Physica A: Statistical Mechanics and its Applications* **392**(23), 6052–6063.
12. Polyakov, Y. S. and A. L. Zydney (2013). Ultrafiltration membrane performance: Effects of pore blockage/constriction. *Journal of Membrane Science* **434**, 106–120.
13. Timashev, S. F., S. G. Lakeev, P. I. Misurkin, Y. S. Polyakov, P. S. Timashev, Y. Y. Tomashpol'skiy, N. V. Sadovskaya, G. I. Terent'ev, S. V. Medvedskikh, A. B. Solov'eva, N. I. Kargin, P. S. Vorontsov, S. M. Ryndya, and V. A. Timofeeva (2013). Parametrization of the Texture of Chaotic Surfaces in Nanometer Range Imaged by Atomic Force Microscopy. *Zavodskaya Laboratoriya: Diagnostika Materialov (Industrial Laboratory: Diagnostics of Materials)* **79**(3). [In Russian], 26–38.
14. Polyakov, Y. S., J. Neilsen, and S. F. Timashev (2012). Stochastic Variability in X-Ray Emission from the Black Hole Binary GRS 1915+105. *The Astronomical Journal* **143**(6), 148.

15. Ryabinin, G. V., V. A. Gavrilov, Y. S. Polyakov, and S. F. Timashev (June 2012). Cross-correlation earthquake precursors in the hydrogeochemical and geoacoustic signals for the Kamchatka peninsula. *Acta Geophysica* **60**(3), 874–893.
16. Timashev, S. F., S. A. Demin, O. Y. Panischev, Y. S. Polyakov, A. Y. Kaplan, and Y. A. Nefedov (2012). Flicker-Noise Spectroscopy as a Tool for the Personalized Medicine of the Future. *Kazanskii Gosudarstvennyi Universitet. Uchenye Zapiski* **154**(4). [In Russian], 161–177.
17. Timashev, S. F., O. Y. Panischev, Y. S. Polyakov, S. A. Demin, and A. Y. Kaplan (2012). Analysis of cross-correlations in electroencephalogram signals as an approach to proactive diagnosis of schizophrenia. *Physica A: Statistical Mechanics and its Applications* **391**(4), 1179–1194.
18. Mirsaidov, U., S. F. Timashev, Y. S. Polyakov, P. I. Misurkin, I. Musaev, and S. V. Polyakov (2011). Analytical method for parameterizing the random profile components of nanosurfaces imaged by atomic force microscopy. *Analyst* **136** (3), 570–576.
19. Ryabinin, G. V., Y. S. Polyakov, V. A. Gavrilov, and S. F. Timashev (2011). Identification of earthquake precursors in the hydrogeochemical and geoacoustic data for the Kamchatka peninsula by flicker-noise spectroscopy. *Natural Hazards and Earth System Sciences* **11**(2), 541–548.
20. Kholpanov, L. P., Y. S. Polyakov, and A. A. Berlin (June 2010). Coupled turbulent heat and mass transfer in fast polymerization processes in a tubular reactor. *Theoretical Foundations of Chemical Engineering* **44**(3), 236–248.
21. Polyakov, Y. S., I. Musaev, and S. V. Polyakov (2010). Closed bioregenerative life support systems: Applicability to hot deserts. *Advances in Space Research* **46**(6). Life Sciences in Space, 775–786.
22. Timashev, S. F., Y. S. Polyakov, S. G. Lakeev, P. I. Misurkin, and A. I. Danilov (Jan. 2010). Fundamentals of fluctuation metrology. *Russian Journal of Physical Chemistry A* **84**(10), 1807–1825.
23. Timashev, S. F., Y. S. Polyakov, R. M. Yulmetyev, S. A. Demin, O. Y. Panischev, S. Shimojo, and J. Bhattacharya (Mar. 2010). Frequency and phase synchronization in neuromagnetic cortical responses to flickering-color stimuli. *Laser Physics* **20**(3), 604–617.
24. Timashev, S. F., Y. S. Polyakov, P. I. Misurkin, and S. G. Lakeev (Apr. 2010). Anomalous diffusion as a stochastic component in the dynamics of complex processes. *Phys. Rev. E* **81** (4), 041128.
25. Polyakov, Y. S. (Dec. 2009). Effect of operating parameters and membrane characteristics on the permeate rate and selectivity of ultra- and microfiltration membranes in the depth filtration model. *Theoretical Foundations of Chemical Engineering* **43**(6), 926.
26. Timashev, S. F., Y. S. Polyakov, R. M. Yulmetyev, S. A. Demin, O. Y. Panischev, S. Shimojo, and J. Bhattacharya (Apr. 2009). Analysis of biomedical signals by flicker-noise spectroscopy: Identification of photosensitive epilepsy using magnetoencephalograms. *Laser Physics* **19**(4), 836–854.
27. Polyakov, Y. S. (Feb. 2008b). Nonuniform deposition of particles inside the pores of a semipermeable membrane. *Theoretical Foundations of Chemical Engineering* **42**(1), 77–84.
28. Polyakov, Y. S. (2008c). Depth filtration approach to the theory of standard blocking: Prediction of membrane permeation rate and selectivity. *Journal of Membrane Science* **322**(1), 81–90.
29. Timashev, S. F. and Y. S. Polyakov (2008b). Analysis of discrete signals with stochastic components using flicker noise spectroscopy. *International Journal of Bifurcation and Chaos* **18**(09), 2793–2797. eprint: https://doi.org/10.1142/S0218127408022020.
30. Kholpanov, L. P. and Y. S. Polyakov (Nov. 2007b). Turbulent conjugate heat-and mass transfer in chemical conversions in a tubular reactor. *Journal of Engineering Physics and Thermophysics* **80**(6), 1140–1153.
31. Polyakov, Y. S. (Oct. 2007c). Use of cake deposition to improve the efficiency of ultra- and microfiltration plants. *Theoretical Foundations of Chemical Engineering* **41**(5), 475–482.
32. Polyakov, Y. S. and D. A. Kazenin (Feb. 2007). Selection of membranes for deadend micro- and ultrafiltration outside-in hollow fiber filters. *Theoretical Foundations of Chemical Engineering* **41**(1), 56–65.
33. Polyakov, Y. S. (2007e). Phenomenological theory of depth membrane filtration. *Chemical Engineering Science* **62**(7), 1851–1860.
34. Timashev, S. F. and Y. S. Polyakov (2007b). Flicker Noise Spectroscopy: Extraction of Information from Chaotic Signals Generated by Complex Systems. *Nauka - Proizvodstvu (Science for Industry)* (1). [In Russian], 54–63.
35. Timashev, S. F. and Y. S. Polyakov (2007c). Review of flicker noise spectoscopy in elecrochemistry. *Fluctuation and Noise Letters* **07**(02), R15–R47. eprint: https://doi.org/10.1142/S0219477507003829.

36. Kholpanov, L. P. and Y. S. Polyakov (Oct. 2006c). Mathematical modeling of turbulent heat and mass transfer with chemical conversions. *Theoretical Foundations of Chemical Engineering* **40**(5), 454–464.
37. Polyakov, Y. S. (2006c). Deadend outside-in hollow fiber membrane filter: Mathematical model. *Journal of Membrane Science* **279**(1), 615–624.
38. Polyakov, Y. S. (2006d). Hollow-fiber membrane adsorber: Mathematical model. *Journal of Membrane Science* **280**(1), 610–623.
39. Polyakov, Y. S. (2006e). Particle deposition in outside-in hollow fiber filters and its effect on their performance. *Journal of Membrane Science* **278**(1), 190–198.
40. Polyakov, Y. S. and V. V. Dil'man (2006b). Approximate method for nonlinear differential and integrodifferential equations. *AIChE Journal* **52**(11), 3813–3824. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/aic.10995.
41. Polyakov, Y. S. (2005b). Membrane Fouling at the Service of UF/MF: Hollow Fiber Membrane Adsorber. *Membrane Quarterly* **20**(3), 7–11.
42. Polyakov, Y. S. (Sept. 2005c). Membrane Separation in Deadend Hollow Fiber Filters at Constant Transmembrane Pressure. *Theoretical Foundations of Chemical Engineering* **39**(5), 471–477.
43. Polyakov, Y. S. and D. A. Kazenin (Mar. 2005d). Membrane filtration with reversible adsorption: Hollow fiber membranes as collectors of colloidal particles. *Theoretical Foundations of Chemical Engineering* **39**(2), 118–128.
44. Polyakov, Y. S. and D. A. Kazenin (July 2005e). Membrane Filtration with Reversible Adsorption: The Effect of Transmembrane Pressure, Feed Flow Rate, and the Geometry of Hollow Fiber Filters on Their Performance. *Theoretical Foundations of Chemical Engineering* **39**(4), 402–406.
45. Polyakov, Y. S., D. A. Kazenin, E. D. Maksimov, and S. V. Polyakov (Sept. 2003). Kinetic Model of Depth Filtration with Reversible Adsorption. *Theoretical Foundations of Chemical Engineering* **37**(5), 439–446.
46. Polyakov, Y. S., E. D. Maksimov, and V. S. Polyakov (1999). On the Design of Microfilters. *Theoretical Foundations of Chemical Engineering* **33**(1), 64–71.

Conference Papers

1. Geva, R., B. Waissengrin, D. Mirelman, F. Bokstein, D. T. Blumenthal, I. Wolf, S. Pelles, Z. Duchin, L. Liram, Y. Polyakov, and M. Blatt (2021). Verification of Statistical Oncological Endpoints on Encrypted Data: Confirming the Feasibility of Real-World Data Sharing without the Need to Reveal Protected Patient Information. In: *2021 ASCO Annual Meeting, Journal of Clinical Oncology*. Vol. 39. Suppl 15, pp.e18725. https://meetinglibrary.asco.org/record/199851/abstract.
2. Chen, C., N. Genise, D. Micciancio, Y. Polyakov, and K. Rohloff (2020). Implementing Token-Based Obfuscation under (Ring) LWE. Accepted to WAHC'20; https://eprint.iacr.org/2018/1222.
3. Archer, D. W., J. M. Calderón Trilla, J. Dagit, A. Malozemoff, Y. Polyakov, K. Rohloff, and G. Ryan (2019). RAMPARTS: A Programmer-Friendly System for Building Homomorphic Encryption Applications. In: *Proceedings of the 7th ACM Workshop on Encrypted Computing & Applied Homomorphic Cryptography*. WAHC'19. London, United Kingdom: ACM, pp.57–68. http://doi.acm.org/10.1145/3338469.3358945.
4. Genise, N., D. Micciancio, and Y. Polyakov (2019). Building an Efficient Lattice Gadget Toolkit: Subgaussian Sampling and More. In: *Advances in Cryptology – EUROCRYPT 2019*. Ed. by Y. Ishai and V. Rijmen. https://eprint.iacr.org/2018/946. Cham: Springer International Publishing, pp.655–684.
5. Halevi, S., Y. Polyakov, and V. Shoup (2019). An Improved RNS Variant of the BFV Homomorphic Encryption Scheme. In: *Topics in Cryptology – CT-RSA 2019*. Ed. by M. Matsui. Cham: Springer International Publishing, pp.83–105.
6. Cousins, D. B., G. D. Crescenzo, K. D. Gür, K. King, Y. Polyakov, K. Rohloff, G. W. Ryan, and E. Savas (May 2018). Implementing Conjunction Obfuscation Under Entropic Ring LWE. In: *2018 IEEE Symposium on Security and Privacy (SP)*, pp.354–371.
7. Crescenzo, G. D., L. Bahler, B. Coan, K. Rohloff, and Y. Polyakov (Aug. 2018). Intrusion-Resilient Classifier Approximation: From Wildcard Matching to Range Membership. In: *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pp.1885–1890.
8. Gür, K. D., Y. Polyakov, K. Rohloff, G. W. Ryan, and E. Savas (2018). Implementation and Evaluation of Improved Gaussian Sampling for Lattice Trapdoors. In: *Proceedings of the 6th Workshop on Encrypted Computing & Applied Homomorphic Cryptography*. WAHC '18. Toronto, Canada: ACM, pp.61–71. http://doi.acm.org/10.1145/3267973.3267975.

9. Hallman, R. A., K. Laine, W. Dai, N. Gama, A. J. Malozemoff, Y. Polyakov, and S. Carpov (2018). Building Applications with Homomorphic Encryption. In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018*, pp.2160–2162. http://doi.acm.org/10.1145/3243734.3264420.
10. Bahler, L., G. D. Crescenzo, Y. Polyakov, K. Rohloff, and D. B. Cousins (July 2017). Practical Implementation of Lattice-Based Program Obfuscators for Point Functions. In: *2017 International Conference on High Performance Computing Simulation (HPCS)*, pp.761–768.
11. Crescenzo, G. D., L. Bahler, B. Coan, Y. Polyakov, K. Rohloff, and D. B. Cousins (July 2016). Practical implementations of program obfuscators for point functions. In: *2016 International Conference on High Performance Computing Simulation (HPCS)*, pp.460–467.
12. Gupta, A. D., Y. Polyakov, K. Rohloff, and G. Ryan (June 2016). Securely Sharing Encrypted Medical Information. In: *2016 IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, pp.330–331.
13. Gupta, A. D., Y. Polyakov, and K. Rohloff (Mar. 2016). Secure access delegation of encrypted medical information. In: *2016 10th International Symposium on Medical Information and Communication Technology (ISMICT)*, pp.1–5.
14. Geller, J., S. T. Klein, and Y. Polyakov (2015). Identifying Pairs of Terms with Strong Semantic Connections in a Textbook Index. In: *Proceedings of the 7th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management - Volume 2: KEOD, (IC3K 2015)*. INSTICC. SciTePress, pp.307–315.
15. Rohloff, K. and Y. Polyakov (Oct. 2015). An end-to-end security architecture to collect, process and share wearable medical device data. In: *2015 17th International Conference on E-health Networking, Application Services (HealthCom)*, pp.615–620.
16. Polyakov, Y. S., S. A. Demin, O. Y. Panishchev, A. Y. Kaplan, and S. F. Timashev (2014). Diagnosis of Schizophrenia Spectrum Disorders Based on the Correlation Analysis of Electroencephalograms. In: *Proceedings of the 6th Troitsk Conference on Medical Physics and Innovations in Medicine*. [In Russian]. Moscow: Institute for Spectroscopy Russian Academy of Sciences, pp.15–18.
17. Timashev, S. F. and Y. S. Polyakov (2013). Fluctuation Metrology for Astrometric Problems. In: *Proceedings of All-Russian Astrometric Conference Pulkovo - 2012; Izvestiya Glavnoy Astronomicheskoy Observatorii v Pulkovo (Bulletin of the Main Astronomical Observatory in Pulkovo)*. [In Russian]. Pulkovo, Russia: Institute for Spectroscopy of Russian Academy of Sciences, pp.485–492.
18. Demin, S. A., O. Y. Panishchev, Y. S. Polyakov, and S. F. Timashev (2012). Frequency and Phase Synchronization in MEG Responses: Problems of Early Diagnosis and Therapy of Photosensitive Epilepsy. In: *Proceedings of X International Conference on Physics and Radioelectronics in Medicine and Ecology*. Vol. 3. Suzdal, Russia, pp.101–105.
19. Timashev, S. F., O. Y. Panishchev, S. A. Demin, and Y. S. Polyakov (2012). Principles for Applying 3D Cross-Correlation Analysis of MEG Responses in Diagnosis and Therapy of Photosensitive Epilepsy. In: *Proceedings of the 5th Troitsk Conference on Medical Physics and Innovations in Medicine*. [In Russian]. Moscow: Institute for Spectroscopy of Russian Academy of Sciences, pp.53–55.
20. Timashev, S. F., O. Y. Panishchev, S. A. Demin, Y. S. Polyakov, and J. Bhattacharya (2012). Flicker-Noise Spectroscopy Analysis of Magnetoencephalogram Signals in Diagnosis and Treatment of Photosensitive Epilepsy. In: *20th International Conference on Advanced Laser Technologies ALT'12 - Book of Abstracts*. Thun, Switzerland, pp.327–328.
21. Polyakov, Y. S., J. Neilsen, and S. F. Timashev (June 2011). Anomalous diffusion in the dynamics of X-ray emission of astrophysical objects. In: *2011 21st International Conference on Noise and Fluctuations*, pp.115–118.
22. Timashev, S. F. and Y. S. Polyakov (2010). Flicker-Noise Spectroscopy as a Tool for the Personalized Medicine of the Future. In: *Proceedings of 3rd Eurasian Congress on Medical Physics and Engineering "Medical Physics - 2010"*. Vol. 3. [In Russian]. Moscow: Moscow State University, pp.64–68.
23. Timashev, S. F., Y. S. Polyakov, and S. G. Lakeev (2010). Fluctuation Metrology and Parameterization of Time Signals. In: *Proceedings of the 41th International Seminar on Fluctuation and Degradation Processes in Semiconductor Devices*. [In Russian]. Moscow: MNTORES im. A.S. Popova, Moscow Power Engineering Institute.

24. Timashev, S. F., Y. S. Polyakov, A. B. Solovieva, and P. I. Misurkin (2010). Nanometrology of the Surfaces in Biological Systems. In: *Proceedings of 2nd International Conference "Nanooncology", Rossiysky Bioterapevticheskiy Zhurnal (Russian Biotherapeutical Journal)*. Vol. 9. 3. [In Russian], pp.25–25.
25. Timashev, S. F., Y. S. Polyakov, P. I. Misurkin, and S. G. Lakeev (2009). Anomalous Diffusion in the Dynamics of Complex Processes. In: *Proceedings of the 40th International Seminar on Fluctuation and Degradation Processes in Semiconductor Devices*. [In Russian]. Moscow: Moscow Power Engineering Institute.
26. Polyakov, Y. S. (2008a). Depth Filtration Model for Standard Pore Blocking in Ultra- and Microfiltration Membranes. In: *Proceedings of the 21th International Scientific Conference "Mathematical Methods in Engineering"*. Vol. 3. [In Russian]. Saratov: Saratov State Technical University, pp.102–106.
27. Timashev, S. F., R. M. Yulmetyev, S. A. Demin, O. Y. Panischev, and Y. S. Polyakov (2008). Flicker-Noise Spectroscopy in the Analysis of Magnetoencephalograms: Photosensitive Epilepsy. In: *Almanac of Clinical Medicine: Proceedings of the 3rd Troitsk Conference on Medical Physics and Innovations in Medicine*. Vol. XVII. 1. [In Russian]. Moscow: MONIKI, pp.233–237.
28. Kholpanov, L. P. and Y. S. Polyakov (2007a). Numerical Analysis of the Hyperbolic Model for Turbulent Heat and Mass Transfer with Chemical Conversions. In: *Proceedings of the 20th International Scientific Conference "Mathematical Methods in Engineering"*. Vol. 3. [In Russian]. Yaroslavl: Yaroslavl State Technical University, pp.202–204.
29. Kholpanov, L. P., S. E. Zakiev, and Y. S. Polyakov (2007). Turbulent Heat and Mass Transfer with Exothermic Reactions. In: *Proceedings of the International Conference "The XVIII session of the International School on the Models of Continuum Mechanics"*. [In Russian]. Saratov: Saratov State Technical University.
30. Polyakov, Y. S. (2007a). Mathematical Modeling of Standard Blocking in Semipermeable Membranes. In: *Proceedings of the 20th International Scientific Conference "Mathematical Methods in Engineering"*. Vol. 3. [In Russian]. Yaroslavl: Yaroslavl State Technical University, pp.216–217.
31. Polyakov, Y. S. (2007b). Optimal Organization of Ultra- and Microfiltration in Hollow Fiber Membrane Filters. In: *Proceedings of the All-Russian Scientific Conference "Membranes 2007"*. [In Russian]. Moscow, pp.85.
32. Timashev, S. F. and Y. S. Polyakov (2007a). Phenomenological Analysis of Medical Time Series with Regular and Stochastic Components. In: *Noise and Fluctuations in Biological, Biophysical, and Biomedical Systems (Proceedings of "Fluctuations and Noise 2007"*. Ed. by S. M. Bezrukov. Vol. 6602. Bellingham, WA: SPIE.
33. Kholpanov, L. P. and Y. S. Polyakov (2006a). Coupled Turbulent Heat and Mass Transfer with Chemical Conversions. In: *Proceedings of the 4th Russian National Conference on Heat Transfer*. Vol. 3. [In Russian]. Moscow: Moscow Power Institute, pp.329–332.
34. Kholpanov, L. P. and Y. S. Polyakov (2006b). Numerical Simulation of Fast Polymerization Processes. In: *Proceedings of the 19th International Scientific Conference "Mathematical Methods in Engineering"*. Vol. 1. [In Russian]. Voronezh: Voronezh State Technological Academy, pp.113–116.
35. Polyakov, Y. S. (2006b). Phenomenological Model of Depth Membrane Filtration. In: *Proceedings of the 19th International Scientific Conference "Mathematical Methods in Engineering"*. Vol. 1. Voronezh: Voronezh State Technological Academy, pp.88–93.
36. Polyakov, Y. S. and V. V. Dil'man (2006a). Approximate Method for Solving Unsteady Nonlinear Mass Transfer Problems. In: *Proceedings of the 19th International Scientific Conference "Mathematical Methods in Engineering"*. Vol. 1. Voronezh: Voronezh State Technological Academy, pp.94–96.
37. Polyakov, Y. S. and L. P. Kholpanov (2006). Coupled Turbulent Heat and Mass Transfer with Chemical Conversions. In: *Proceedings of the 9th All-Russian Congress on Theoretical and Applied Mechanics*. Vol. 2. [In Russian]. Nizhniy Novgorod: Nizhniy Novgorod State University, pp.146–147.
38. Polyakov, Y. S. (2005a). Beneficial Effect of Particle Adsorption in UF/MF Outside-In Hollow Fiber Filters. In: *Proceedings of the 2005 Annual Meeting of the North American Membrane Society*. Providence, Rhode Island, pp.66–67.
39. Polyakov, Y. S. and D. A. Kazenin (2005a). Nonlinear Mass Transfer with Reversible Adsorption on Semipermeable Membranes in Deadend Filters. In: *Proceedings of the 18th International Scientific Conference "Mathematical Methods in Engineering"*. Vol. 1. [In Russian]. Kazan: Kazan State Technical University, pp.146–151.
40. Polyakov, Y. S. and D. A. Kazenin (2005b). Nonlinear Mass Transfer with Reversible Adsorption on Semipermeable Membranes in Membrane Adsorbers. In: *Proceedings of the 18th International Scientific Conference "Mathematical Methods in Engineering"*. Vol. 1. [In Russian]. Kazan: Kazan State Technical University, pp.156–160.

41. Polyakov, Y. S. and D. A. Kazenin (2005c). Process Flow Diagram and Parameter Selection for Closed-Loop Wastewater Ultrafiltration Hollow-Fiber Plants. In: *Proceedings of the 2nd International Scientific & Industrial Conference "Environmental Problems of Industrial Megapolises"*. [In Russian]. Moscow: Moscow State University of Environmental Engineering, pp.147–148.
42. Polyakov, Y. S. and D. A. Kazenin (2004). Design of Novel Hollow Fiber Membrane Filters for Closed-Loop Wastewater Plants Treating Paint, Power Plant, and Car Repair Effluents. In: *Proceedings of the 1st International Scientific & Industrial Conference "Environmental Problems of Industrial Megapolises"*. Vol. 1. [In Russian]. Donetsk: Donetsk: Donetsk State Technical University, pp.221–226.

Book Chapters

1. Timashev, S. F., V. A. Nivin, V. L. Syvorotkin, and Y. S. Polyakov (2011). "Flicker-Noise Spectroscopy Analysis of Hydrogen Gas Release Dynamics in Khibiny and Lovozerovo Massifs (Kola Peninsula)". In: *Dynamic Phenomena in Complex Systems*. [In Russian]. Kazan: MOiN RT, pp. 263–278.
2. Timashev, S. F., O. Y. Panischev, S. A. Demin, P. Y. S., and A. Y. Kaplan (2011). "Dynamics of Cross-Correlations in Human Electroencephalograms for Diagnostics of Psychiatric Disorders". In: *Dynamic Phenomena in Complex Systems*. [In Russian]. Kazan: MOiN RT, pp. 279–296.
3. Timashev, S. F. and Y. S. Polyakov (2008a). "A reveiw of flicker-noise spectroscopy: information in chaotic signals". In: *Simultaneity: Temporal Structures and Observer Perspectives*. Singapore: World Scientific Publishing, pp. 270–285. https://www.worldscientific.com/doi/abs/10.1142/9789812792426_0017.
4. Verkhovsky, B. S. and Y. S. Polyakov (2006). "Non-Linear Algorithms for Parametric Markov Programming". In: *Current Computing Developments in E-Commerce, Security, HCI, DB, Collaborative and Cooperative Systems*. Athens, Greece: Athens Institute for Education and Research, pp. 179–194.
5. Verkhovsky, B. S. and Y. S. Polyakov (2003a). "Algorithms for Optimal Switch Location: Concave Cost Functions". In: *Advances in Decision Technology and Intelligent Information Systems, Volume IV*. Windsor, Canada: The International Institute for Advanced Studies in Systems Research and Cyberneticsh, pp. 16–20.
6. Verkhovsky, B. S. and Y. S. Polyakov (2003b). "Feedback Algorithm for the Single-Facility Minisum Problem". In: *Annals of the European Academy of Sciences*. Vol. 1, pp. 127–136.
7. Verkhovsky, B. S. and Y. S. Polyakov (2003c). "Highly Efficient Algorithm for Two-Switch Location Problem". In: *Advances in Decision Technology and Intelligent Information Systems, Volume IV*. Windsor, Canada: The International Institute for Advanced Studies in Systems Research and Cyberneticsh, pp. 51–55.

Patents and Patent Applications

1. Polyakov, Y. S. (2006a). *Hollow Fiber Membrane Adsorber and Process for the Use Thereof*. Application No. 11/380,637, Filed on April 27, 2006.

Theses and Dissertations

1. Polyakov, Y. S. (Nov. 2007d). "Nonuniform Particle Deposition on External and Internal Surface of Semipermeable Membranes". DSc (Habil.) Thesis [In Russian]. Moscow State University of Environmental Engineering (now Moscow Polytechnic University).
2. Polyakov, Y. S. (Dec. 2004). "Ultra- and Microfiltration in Hollow-Fiber Filters with Cake Formation on the Membrane Surface". PhD Thesis [In Russian]. Moscow State University of Environmental Engineering (now Moscow Polytechnic University).
3. Polyakov, Y. (May 2003). "Feedback Algorithm for Switch Location: Analysis of Complexity and Application to Network Design". Master's Thesis. Computer Science Department, New Jersey Institute of Technology.