CURRICULUM VITAE Ernst Gabidulin / October 2017

1. Personal details

Surname	GABIDULIN
First names	ERNST MUKHAMEDOVICH
Date of birth	04.06.1937
Place of birth	Kyrgyzstan (former USSR)
Sex	Male
Nationality	Russia
Married	Yes
Occupation/ Position	Prof. - Dr., Dept. of Radio Engineering and Control Systems National Research University "Moscow Institute of Institute of Physics and Technology" 9 Institutskii per. 141700 DOLGOPRUDNY Moscow Region RUSSIA
Phone/Fax	+7 495 408-4433
E-mail	gabidulin.em@.mipt.ru, ernst.gabidulin@gmail.com

2. Higher Education

Graduated with honours from Moscow Institute of Physics and Technology in 1959. Diploma Thesis is in Radio Engineering and Automatic Control.

Received the Academic Degree of Candidate of Physical and Mathematical Sciences (approx. Ph.D.) from Moscow Institute of Physics and Technology. Thesis is devoted to some Problems of the Algebraic Coding Theory.

Received the Academic Degree of "Doctor of Technical Sciences" from Moscow Institute of Physics and Technology. Thesis is devoted to the Theory of the Non-Hamming Metrics

3. Experience: teaching activity

Teaching activity is in the area of Radio Engineering , Information Theory and Cryptology in the Moscow Institute of Physics and Technology since 1959 up to now (Assistant Professor, Associate Professor, Full Professor).

He was the advisor of 12 PhD (all successful).

8 textbooks in the Radio Engineering, the Information theory and the Cryptology are written

.

4. **Experience: Research activity**

   Research activity is in the field of Shannon Theory, Algebraic Coding Theory, Network Coding, Modulation, Communication, Satellite Navigation Systems, Cryptology, Sequences, and related areas.

   Total 79 Journal Papers, 135 Printed Conference Reports, 8 Textbooks, 12 Joint Monographs, 6 Patents

5. **Experience: Work in European Universities**

   1991 ETH Zurich Swiss , Guest Professor, 1 month;
   1992 TH Darmstadt Germany, Visiting Professor, 3 months;
   1994 Lund University Sweden, Visiting Professor, 2 months;
   1994-1995 Delft University, Guest Professor, 4 months;
   1995 – 1997 Bergen University, Visiting Professor, 4 months.
   1996 - 2010 Ulm University Germany, Visiting Professor, 18 months.
   1996 – 2010 Lancaster University UK, Visiting Professor, 14 months.
   1999-2004 INRIA, Guest Professor, 4 months
   2010 University of Campinas, Brazil, Guest professor, 1 month

6. **Awards**

   2001 г. Медаль к Ордену «За заслуги перед Отечеством» II степени.
   2009 г. Почетное звание «Заслуженный деятель науки Российской Федерации».
   2010 г. Заслуженный профессор МФТИ

7. **Home address**

   Moscowskoe shosse, 39, ap. 10
   141700 Dolgoprudny, Moscow Region
   RUSSIA

Ernst M. Gabidulin was born in Kok-Janchak, Kyrgyzstan (former U.S.S.R.) on June 4, 1937. He received the Candidate of Science and Dr. of Science degrees in cybernetics from the Moscow Institute of Physics and Technology (State University) (MIPT), Moscow, Russia, in 1976 and 1985, respectively.
From 1959 to 1976, he was an Assistant Professor, from 1976 to 1987, an Associate Professor, and from 1987 to 1989, a Professor in the Department of Radio Engineering at MIPT. His research interests include coding theory, communications, cryptology, and sequences. His list of publications contains more than 200 papers and printed conference reports. The most cited are "Theory of codes with maximal rank distance", *Problems of information transmission*, №1, т. 21, 1985, and "Ideals over a Non-Commutative Ring and Their Application in Cryptology," *Lecture Notes in Computer Science*, v. 547, Advances in Cryptology, *Proceedings* of EUROCRYPT'91, Brighton, UK, April 1991, pp. 482-489.

List of *recent* papers in English and Russian

1. Gabidulin E. A brief survey of metrics in coding theory // Mathematics of Distances and Applications. MDA-2012 / Deza M., Petitjean M., Markov K. (Eds.) -- Sofia: ITHEA, 2012. P. 66-84.
2. Khan E., Gabidulin E.M., Honary B., Ahmed H. Matrix-based memory efficient symmetric key generation and pre-distribution scheme for wireless sensor networks // IET Wireless Sensor Systems. -- 2012. -- V. 2, No. 2. -- P. 108-114.
3. Габидулин Э.М., Пилипчук Н.И., Трушина О.В. “Защита информации в телекоммуникационных сетях” // Труды Московского физико-технического института (государственного университета). 2013. Т. 5. № 3. С. 97-111.
4. Габидулин Э.М., Пилипчук Н.И. "Ранговые подкоды в многокомпонентном сетевом кодировании" // Проблемы передачи информации. 2013. Т.49. Вып. 1. С. 46-60.
5. Габидулин Э.М., Пилипчук Н.И., Хонари Б., Рашван Х. "Защита информации в сети со случайным сетевым кодированием" // Проблемы передачи информации. 2013. Т. 49. Вып.2. С. 92-106.
6. Rashwan H., Gabidulin E.M., Honary B., Cruckshank H. “Enhancing the Security of the GPT Cryptosystem Against Attacks” // International Journal of Computers & Technology. 2013. V. 11. P. 2457-2475.
7. Gabidulin E.M., Pilipchuk N.I. “Modified GPT cryptosystem for information network security” // Intern. Journal for Information Security Research (IJISR). 2013. V. 3. Issue 3/4. P. 432-438.
8. Khan E., Gabidulin E.M., Honary B., Ahmed H. Modified Niederreiter Type of GPT Cryptosystem Based on Reducible Rank Codes // Designs Codes and Cryptography. 2013.
9. Gabidulin E.M., Pilipchuk N.I. GPT Cryptosystem for information network security // i-Society 2013 Proceedings, June 24-26, 2013, Toronto, Canada, pp. 21-25.
10. Сысоев И.Ю., Габидулин Э.М. “Декодирование ранговых кодов с использованием слабоортогонального базиса” // Труды Московского физико-технического института (государственного университета). 2014. Т. 6. № 4. С. 126-138.
11. Габидулин Э.М., Пилипчук Н.И. О мощности подпространственных сетевых кодов // International Conference "Engineering & Telecommunication” En&T 2014. Book of Abstracts. Moscow—Dolgoprudny.
12. Khan E., Gabidulin E.M., Honary B., Ahmed H. “Modified Niederreiter Type of GPT Cryptosystem Based on Reducible Rank Codes” // Designs, Codes and Cryptography. 2014. V. 70. Issue 1-2. P. 231-239.
13. Э.М. Габидулин, А.А. Григорьев, Н.И. Пилипчук, И. Ю. Сысоев, А.В. Уривский, А.Л. Шишкин "Подпространственные коды на основе ранговой метрики – новое направление в теории кодировании"// Труды Московского физико-технического института (государственного университета). 2015. Т. 7. № 1. С. 1-22.
14. Э. М. Габидулин, Н. И. Пилипчук "Эффективность подпространственных сетевых кодов"// Труды Московского физико-технического института (государственного университета). 2015. Т. 7. № 1. С. 104-111.
15. Трушина О.В., Габидулин Э.М. "Новый метод обеспечения анонимности и секретности в сетевом кодировании" // Проблемы передачи информации. 2015. Т. 51 . Вып. 1. С. 82-89.
16. Габидулин Э.М., Пилипчук Н.И. «Эффективность подпространственных сетевых кодов»// Труды МФТИ-- 2015.-Том 7, №1. С.104-111.
17. E. M. Gabidulin, N. I. Pilipchuk “Subspace Network Codes with Large Cardinality” // 2015 International Conference on Engineering and Telecommunication (EnT) 18-19 Nov. 2015 IEEE

Computer Society Order Number E5754 ISBN-13: 978-1-4673-8482-7 BMS Part # CFP1570Z-ART

18. Габидулин Э. М., Пилипчук Н. И. «Многокомпонентные коды с максимальным кодовым расстоянием» // Проблемы передачи информации. 2016. Т. 52. Вып. 3. С. 84-91.
E. M. Gabidulin ; N. I. Pilipchuk "State of Art in Subspace Coding" // International Conference on Engineering and Telecommunication (EnT) 29-30 Nov. 2016 Publication Year: 2016, Page(s):58 – 63
19. Габидулин Э. М., Пилипчук Н. И. «Двойственные многокомпонентные коды максимальной мощности» // Труды МФТИ-- 2016.-Том 8 (29), №1. С.32-40.
20. O. Trushina, E. Gabidulin "Anonymous Coherent Network Coding Against Eavesdropping and Jamming" // Electronic Notes in Discrete Mathematics. Volume 57, March 2017, Pages 199–204.
21. Габидулин Э.М., Пилипчук Н.И. Оптимальные и субоптимальные подпространственные коды. // Труды МФТИ-- 2017.-Том 9 (30), №2.

Papers in the Proceedings of *recent* conferences in English

1. Gabidulin E. New Subcodes of Rank Codes // Proc. 13-th International Workshop on Algebraic and Combinatorial Coding Theory (ACCT2012). Pomorie, Bulgaria. 2012, P. 157-161.
2. Pilipchuk N., Gabidulin E., Afanassiev V. Decoding multicomponent codes based on rank subcodes. // Proc. 13-th International Workshop on Algebraic and Combinatorial Coding Theory (ACCT2012). Pomorie, Bulgaria. 2012, P. 275-281.
3. Asif H.M., Gabidulin E.M., Honary B. Rank codes over Gaussian integers and space time block codes // Mathematics of Distances and Applications. MDA-2012 / Deza M., Petitjean M., Markov K. (Eds.) -- Sofia: ITHEA, 2012. P. 118-128.
4. Gabidulin E.M., Trushina O.V. Anonymous and secure network coding scheme // Proceedings of Seventh International Workshop on Optimal Codes and Related Topics OC 2013, Albena, Bulgaria, September 6-12, pp. 85-90.
5. Gabidulin E.M., Pilipchuk N.I. GPT Cryptosystem for information network security // i-Society 2013 Proceedings, June 24-26, 2013, Toronto, Canada, pp. 21-25.
6. Shishkin A., Gabidulin E., Pilipchuk N. "On cardinality of network subspace codes" // Proceedings of 14-th International Workshop On Algebraic And Combinatorial Coding Theory ACCT-2014. – Svetlogorsk, Russia, 2014. - P. – ISBN~978-5-901158-26-5.
7. Gabidulin E., Urivskiy A. "Structural attacks against the GPT cryptosystem"// Intern. Conf.on Information Theory and Applications. February 9-14. 2014. San-Diego, USA.
8. Afanassiev V.B., Gabidulin E.M., Pilipchuk N.I. "Bounds on Cardinality of Multicomponent Network Codes" // XIV International Symposium "Problems of Redundancy in Information and Control Systems." 01-05 June, 2014. St. Petersburg, Russia.
9. Urivskiy A.V., Gabidulin E.M. "On the Equivalence of Different Variants of the GPT Cryptosystem" // XIV International Symposium "Problems of Redundancy in Information and Control Systems." 01-05 June, 2014. St. Petersburg, Russia.
10. E. M. Gabidulin, N. I. Pilipchuk "Subspace Network Codes with Large Cardinality" // 2015 International Conference on Engineering and Telecommunication (EnT) 18-19 Nov. 2015 IEEE Computer Society Order Number E5754 ISBN-13: 978-1-4673-8482-7 BMS Part # CFP1570Z-ART
11. E. Gabidulin, N. Pilipchuk «New constructions of multicomponent codes»// Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT2016) Albena, Bulgaria, on June 18-24, 2016.

12. E. Gabidulin, N. Pilipchuk, I. Sysoev "Decoding multicomponent network codes" // XV International Symposium "Problems of Redundancy in Information and Control Systems". September 26-29, 2016. St. Petersburg, Russia.

13. E.M. Gabidulin, N.I. Pilipchuk, I.U. Sysoev Decoding new multicomponent codes // XV International Symposium on Problems of Redundancy in Information and Control Systems. Saint-Petersburg, Russia, 2016.~--- P.~53--57.