

Резюме

Кабатянский Григорий Анатольевич

Личные данные

Дата рождения: 12 июля 1949 г.

Email: kaba@iitp.ru

Образование

Закончил с отличием механико-математический факультет МГУ в 1971 году

Опыт работы

1971-1990 НИИ АА (автоматической аппаратуры) – мнс, снс, начальник сектора

1990- по н.в. ИППИ(Институт проблем передачи информации) РАН – снс, внс, гнс

Опыт преподавательской деятельности

1979-1984, 1990-1991 МФТИ (совместитель), курсы по теории информации;

1984-1990, МИРЭА (совместитель), курсы по дискретной математике и прикладной алгебре;

1994-1995, 1998-1998 (приглашенный профессор) курсы по дискретной математике Texas A&M University, США;

2002-2004, Московский Независимый Университет (совместитель), курсы по теории кодирования.

Профессиональные достижения

Кандидат физико-математических наук (1979), доктор физико-математических наук (2010),.

Руководитель четырех грантов РФФИ (один из них совместный с CNRS, Франция)

Член редколлегии журнала International Journal on Information Security (Springer)

Приглашенный профессор ИНРИА (Франция) в 1998 (полгода) и 2001 году (год).

Приглашенный профессор-исследователь:

University of California at Riverside (USA), 2007, (1 месяц);

University of Maryland (USA), 2006, (1 месяц);

University of Maryland (USA), 2005, (1 месяц);

Institute of Mathematics, Luminy (France), 2004 (3 месяца);

University of California at Riverside (USA), 2003, (1 месяц);

Universite de la Mediterranee (France), 2003 (1 месяц);

LACO, Universite de Limoges (France), 2002-2004 (3 месяца);

Bell Labs (USA), 2002 (1 месяц);

Center for Discrete Mathematics & Theoretical Computer Science, USA, 2000 (1 месяц);

Pohang University of Science and Technology, Republic of Korea, 2000, (1 месяц);

University of Lund, Sweden, 1996 (5 месяцев), 1994 (4 месяца), 1992 (2 месяца);

Department of Mathematics, Royal Holloway- University of London, UK, 1996 (2 месяца);

Department of Pure Mathematics, University of Delft, the Netherlands, 1995 (1 месяц);

Department of Informatics, University of Bergen, Norway, 1993 (2 месяца);
Department of Mathematics, University of Puerto Rico, 1993 (1 месяц);
Institute of Experimental Mathematics, University of Essen, Germany 1992-1993 (3 месяца);
Research Center of Deutsche Telecom, Darmstadt, Germany, 1993 (1 месяц);
Department of Mathematics, University of Bielefeld, Germany, 1991 (1 месяц);
Department of Mathematics and Computer Science, Technology University of Eindhoven, the Netherlands, 1991 (2 месяца);
Department of Signal Theory and Networks, Technical University of Darmstadt, Germany, 1991 (1 месяц).

Пленарный или приглашенный докладчик на следующих международных конференциях:
5th International Conference on Information Theoretic Security, The Netherland, 2011;
International Conference on Information and Communication Security (Barcelona, Spain), 2010;
European conference "Mathematics in Industry" (Sofia, Bulgaria), 2010;
European school on algebraic geometry and information theory (Luminy, France), 2003;
IMA Conference on Codes, Designs and Cryptography (Minneapolis, USA), 1998;
IEEE International Workshop on Information Theory (Svalbaard, Norway), 1997;
International Workshop on Discrete Geometry (Oberwolfach, Germany), 1991.

Председатель программного комитета:
10th & 11th International Workshops on Algebraic and Combinatorial Coding Theory Moscow, 2006, Pamporovo, Bulgaria, 2008;
International Workshop on Coding and Cryptography (Paris, France), 2003
5-ый Soviet-Swedish International Workshop on Information Theory (Moscow), 1991.

Список реферированных публикаций

I. Монографии

1. G. Kabatiansky, E. Krouk and S. Semenov. Error Correcting Codes and Security for Data Networks. Wiley & Sons, 512 стр, 2005

II. Журнальные статьи

1. Бояринов И.М., Кабатянский Г.А. "Арифметические (n, A) -коды над произвольным основанием", Доклады Академии Наук СССР, т. 221, No 4, стр. 794-797, 1975.

2. Бояринов И.М., Кабатянский Г.А. "Совершенные арифметические AN –коды, исправляющие одиночные ошибки", Проблемы передачи информации, т. 12, No 1, стр. 16-23, 1976.

3. Кабатянский Г.А. "Границы для числа кодовых слов в двоичных арифметических кодах", Проблемы передачи информации, т. 12, No 4, стр. 46-54, 1976.

4. Кабатянский Г.А. "О существовании хороших почти линейных кодов над непростыми полями", Проблемы передачи информации, т. 13, No 3, стр. 18-21, 1977.

5. Кабатянский Г.А. "Два обобщения произведения кодов", Доклады Академии Наук СССР, т. 232, No 6, стр. 1277-1280, 1977.

6. Кабатянский Г.А., Левенштейн В.И. ``Границы для упаковок на сфере и в пространстве", Проблемы передачи информации, т. 14, No 1, стр. 3-25, 1978.
7. Бояринов И.М., Кабатянский Г.А. ``Арифметические итеративные коды, исправляющие независимые ошибки", Проблемы передачи информации, т. 15, No 1, стр. 38-49, 1979.
8. Кабатянский Г.А., Панченко В.И. ``Упаковки и покрытия пространства Хэмминга единичными шарами", Доклады Академии Наук СССР, т. 303, No 3, стр. 550-552, 1988.
9. Кабатянский Г.А., Панченко В.И. ``Упаковки и покрытия пространства Хэмминга шарами радиуса один", Проблемы передачи информации, т. 24, No 4, стр. 3-16, 1988.
10. Геворкян Д.Н., Кабатянский Г.А., ``О кодах Варшавова-Тененгольца и одной гипотезе Л.А. Бассалыго", Проблемы передачи информации, т. 28, No 4, стр. 106-108, 1992.
11. Кабатянский Г.А., ``Конструкция кодов, исправляющих одиночные локализованные ошибки", Проблемы передачи информации, т. 30, No 2, стр. 96-98, 1994.
12. Kabatianskii, G.A., Smeets, B. and Johansson, T. ``On the cardinality of systematic authentication codes via error-correcting codes", IEEE Transactions on Information Theory, vol.42, No 2, pp.566-578, 1996.
13. Кабатянский Г.А., Лебедев В.С. ``Разностные множества и коды, исправляющие локализованные ошибки известной величины", Проблемы передачи информации, т. 32, No 2, стр. 31-35, 1996.
14. Блейкли Г.Р., Кабатянский Г.А. ``Обобщенные схемы разделения секрета и матроиды", Проблемы передачи информации, т. 33, No 3, стр. 102-110, 1997.
15. Кабатянский Г.А. ``Математика разделения секрета", Математическое просвещение, т. 2, No 3, стр. 115-126, 1998.
16. Кабатянский Г.А. ``О кодах, разделяющих пары", Проблемы передачи информации, т. 37, No 4, стр. 60-62, 2001.
17. A. Barg, G. Cohen, S. Encheeva, G. Kabatiansky, and G. Zemor, ``A Hypergraph Approach to the Identifying Parent Property: The Case of Multiple Parents," SIAM J. Discrete Math., vol.14, No.3, pp.423-431, 2001.
18. A. Barg, G.R. Blakley and G. Kabatiansky, ``Digital fingerprinting codes: problem statements, constructions, identification of traitors," IEEE Trans. on Information Theory, v.49, pp. 852--865, 2003.
19. A. Barg and G. Kabatiansky ``Class of i.p.p codes with effective tracing algorithm", Journal of Complexity, vol. 20, no 2-3, pp.137-147, 2004.
20. Кабатянский Г.А. ``Коды для защиты от копирования: случай двух пиратов", Проблемы передачи информации, т. 41, No 2, стр. 123-127, 2005.
21. Думер И., Кабатянский Г.А., Тавернье С., ``Списочное декодирование двоичных кодов Рида-Маллера первого порядка", Проблемы передачи информации, т. 43, No 3, стр. 66-74, 2007.

22. I.Dumer, G. Kabatiansky, C. Tavernier, "List Decoding of Biorthogonal Codes and the Hadamard Transform with Linear Complexity" , IEEE Transactions on Information Theory, 2008, vol 54, No 10, pp 4488-4492.
23. Ф.Галан, Г.А. Кабатянский, «Покрытия, центрированные коды и комбинаторная криптография», Проблемы передачи информации, т. 45, No 3, С. 106-111, 2009.
24. G. Kabatiansky, G.Oshanin "Finding passwords by random walks: how long does it take?" Journal of Physics A: Mathematical and Theoretical, vol.42, №43, 2009.
25. А.Акопян, Г.Кабатянский, О.Мусин, « Контактные числа, коды и сферические многочлены», Математическое просвещение, т.16, стр. 57-74, 2012.
26. A.Barg, G. Kabatiansky, "Robust Parent Identifying Codes and Combinatorial Arrays" , IEEE Transactions on Information Theory, vol 59, No 2, pp 994-1003, 2013.

III. Части книг

1. Кабатянский Г.А. " Математика разделения секрета ", часть 5, стр. 118-129, в *Введение в криптографию*, Москва, МЦНМО, «ЧеРо», ISBN 5-900916-26-X, 272 стр, 1998.
2. Kabatiansky, G.A. , Rush J.A, "Sphere Packing and Coding Theory". Часть 61, стр. 1355-1376, в *Handbook on Discrete and Computational Geometry*, второе издание, J.E.Goodman and J.O.Rurke editors, CRC Press, xvii+1539 pages, 2004

IV. Избранные публикации в трудах конференций (рецензируемые)

1. G. A. Kabatianskii, "On decoding of Reed-Muller codes in semi-continuous channels", In Proc. Second Intern. Workshop ACCT, Leningrad, USSR, 1990, pp. 87-91.
2. G. A. Kabatianskii, "About metrics and decoding domains of Forney's algorithm", In Proc. Soviet-Swedish International Workshop on Information Theory, Moscow, USSR, 1991, pp.81-85
3. G. A. Kabatianskii, "On decoding concatenated codes in certain spaces", In Proc. Soviet-Swedish International Workshop on Information Theory, Moscow, USSR, 1991, pp.86-90.
4. Kabatianskii, G.A. ; Krouk, E.A. "Coding Decreases Delay of Messages in Networks ", In Proceedings 1993 IEEE International Symposium on Information Theory, 1993, page 255.
5. Kabatianskii, G.A. "Codes correcting localized errors of known value", In Proceedings 1994 IEEE International Symposium on Information Theory, 1994.
6. Johansson, T., Kabatianski, G.A. and Smeets, B., "On the relation between A-codes and codes correcting independent errors". In Advances in Cryptology(EuroCrypt-93), Lecture Notes in Computer Science, No. 765, Springer, pp. 1-11, 1994.

7. Bierbrauer, J., Johansson, T., Kabatianski, G.A. and Smeets, B., "On families of hash functions via geometric codes and concatenation". In *Crypto'93, Lecture Notes in Computer Science*, No. 773, Springer, pp. 331-342, 1994.
8. Kabatianski, G.A. and Lobstein, A., "On Elias-Plotkin type bounds for binary arithmetic codes". In *Algebraic Coding, Lecture Notes in Computer Science*, No 781, Springer, pp. 263-274, 1994.
7. Blakley, G.R., Kabatianski, G.A., "Linear algebra approach to secret sharing schemes". In *Error Control, Cryptology and Speech Compression, Lecture Notes in Computer Science*, N 829, Springer, pp. 33-40, 1994.
9. Blakley, G.R., Kabatianski, G.A., "On generalized perfect secret sharing schemes". In *Advances in Cryptology - CRYPTO'95, Lecture Notes in Computer Science*, N 963, Springer, pp. 367-371, 1995.
10. Blakley, G.R. ; Kabatianski, G.A. "Ideal perfect threshold schemes and MDS codes ", In *Proceedings., 1995 IEEE International Symposium on Information Theory*, 1995.
11. Blakley, G.R., Johansson, T., Kabatianski, G.A., "Coding problems of cryptography or codesets vs codewords". In *97'th IEEE Information Theory Workshop, Longyerbyen, Norway*, pp. 43-45, 1997.
12. Kabatianskii, G., Krouk, E., Smeets, B. "A digital signature scheme based on random error-correcting codes". In *Cryptography and Coding, Lecture Notes in Computer Science*, N 1355, Springer, pp. 161--167, 1997.
13. Bassalygo, L.A. Burmester, M. Dyachkov, A. Kabatianski, G. "Hash codes ", In *Proceedings 1997 IEEE International Symposium on Information Theory, Ulm, Germany*, 1997.
14. Kabatianski, G. ; Lebedev, V. ; Thorpe, J. "The Mastermind game and the rigidity of the Hamming space", In *Proceedings IEEE International Symposium on Information Theory*, 2000.
15. Barg, A. ; Blakley, G.R. ; Kabatiansky, G., "Good digital fingerprinting codes ", In *Proceedings 2001 IEEE International Symposium on Information Theory*, 2001.
16. Barg, A. ; Kabatiansky, G. "A class of i.p.p. codes with efficient identification", In *Proceedings 2002 IEEE International Symposium on Information Theory*, 2002.
17. Galand F., Kabatiansky G., "Steganography via Covering Codes", *Proc. 2003 IEEE Int. Symposium on Information Theory, Yokohama, Japan*, p. 192, 2003.
18. Galand F., Kabatiansky G., "Information Hiding by Coverings", In *Proc. 2003 IEEE Information Theory Workshop, Paris, France*, pp. 151–154, 2003.
19. Blakley, G.R. , Kabatiansky, G. "Random coding technique for digital fingerprinting codes: fighting two pirates revisited", In *Proc. 2004 IEEE Int. Symposium on Information Theory, ISIT' 04, Chicago, USA*, 2004.
20. Kabatiansky, G. "Good ternary 2-traceability codes exist", In *2004 IEEE Int. Symposium on Information Theory, ISIT' 04, Chicago, USA*, 2004.

21. G. Kabatiansky, C. Tavernier, "List decoding of Reed-Muller codes", In Proc. Intern. Workshop on Algebraic and Combinatorial Coding Theory (ACCT), 2004.
22. G. Kabatiansky and C. Tavernier, "List decoding of second order Reed-Muller codes", In ISCTA'05, Martin's College, Ambleside, UK, 2005.
23. Dumer, I. ; Kabatiansky, G. ; Tavernier, C. "List decoding of Reed-Muller codes up to the Johnson bound with almost linear complexity", In 2006 IEEE International Symposium on Information Theory, pp: 138 – 142, 2006.
24. Dumer, I. ; Kabatiansky, G. ; Tavernier, C. "Soft-Decision List Decoding with Linear Complexity or the First-Order Reed-Muller Codes", In 2007 IEEE International Symposium on Information Theory, pp: 1346 – 1349, 2007.
25. I. Dumer, G. Kabatiansky and C. Tavernier "On complexity of decoding Reed-Muller codes within their code distance", In Proc. 11-th International Workshop On Algebraic and Combinatorial Coding Theory, Pamporovo, Bulgaria, 2008.
26. Barg, A. ; Blakley, G.R. ; Kabatiansky, G. ; Tavernier, C. "Robust parent-identifying codes" In Proceedings of Information Theory Workshop, 2010 IEEE , Dublin, Ireland, pp:1-4, 2010.
27. A.Barg and G.Kabatiansky, "Digital Fingerprinting under and (Somewhat) Beyond the Marking Assumption", S. Fehr (ed.), ICITS 2011, Lect. Notes Comput. Science, vol. 6673, pp. 202-205, 2011.
28. Ilya Dumer, Grigory Kabatiansky, Cedric Tavernier, "Soft-decision list decoding of Reed-Muller codes with linear complexity", In IEEE International Symposium on Information Theory, pp. 2303-2307, 2011.
29. Marcel Fernandez, Grigory Kabatiansky, Jose Moreira: "Almost separating and almost secure frameproof codes". In IEEE International Symposium on Information Theory, St-Petersburg, Russia, pp. 2696-2700, 2011.
30. Jose Moreira, Grigory Kabatiansky, Marcel Fernandez: "Lower bounds on almost-separating binary codes". In Proceedings WIFS 2011, Brazil, pp. 1-6, 2011.
31. A.S. Abdouli, I. Dumer, G. Kabatiansky, C. Tavernier, "The Goldreich-Levin Algorithm with reduced complexity", In Proc. Intern. Workshop on Algebraic and Combinatorial Coding Theory (ACCT 2012), Pomorie, Bulgaria, 2012.
32. Ilya Dumer, Grigory Kabatyanskiy and Cedric Tavernier, "More steganography via covering codes", In Proceedings YACC'12, Porquerolles Island, France, 2012.