|  |  |  |  |
| --- | --- | --- | --- |
|  | Name | Citation | Status |
|  | ALGEBRAIC-GEOMETRIC CODES WITH MANY AUTOMORPHISMS ARISING FROM GALOIS POINTS | Fukasawa, S. (2022). *Algebraic-geometric codes with many automorphisms arising from Galois points*. http://arxiv.org/abs/2211.16823 |  |
|  | Minimum weight codewords in dual Algebraic-Geometric codes from the Giulietti-Korchm´aros curve | Bartoli, D., & Bonini, M. (2018). *Minimum weight codewords in dual Algebraic-Geometric codes from the Giulietti-Korchm\’aros curve*. http://arxiv.org/abs/1802.03359 |  |
|  | ANALYSIS AND STUDYING OF THE PROPERTIES OF ALGEBRAIC GEOMETRIC CODES | Kuznetsov, А. А., Kolovanova, I. P., Prokopovych-Tkachenko, D. I., & Kuznetsova, T. Y. (2019). ANALYSIS AND STUDYING OF THE PROPERTIES OF ALGEBRAIC GEOMETRIC CODES \*. In *Telecommunications and Radio Engineering* (Vol. 78, Issue 5). |  |
|  | Analysis\_and\_Investigation\_of\_Properties\_of\_Algebraic\_Geometric\_Codes | *2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo).* (n.d.). IEEE. |  |
|  | An Algorithmic Reduction Theory for Binary Codes: LLL and more | Debris-Alazard, T., Ducas, L., & van Woerden, W. P. J. (n.d.). *An Algorithmic Reduction Theory for Binary Codes: LLL and more*. https://github. | Fin |
|  | BIKE -Bit-Flipping Key Encapsulation | Aragon, N., Barreto, P. S. L. M., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.-C., Gaborit, P., Gueron, S., Güneysu, T., Aguilar, C., Rafael, M., Persichetti, M. E., Sendrier, N., Tillich, J.-P., & Zémor, G. (2018). *BIKE-Bit-Flipping Key Encapsulation*. http://bikesuite.org |  |
|  | A Survey on Code-based Cryptography | Weger, V., Gassner, N., & Rosenthal, J. (2022). *A Survey on Code-Based Cryptography*. http://arxiv.org/abs/2201.07119 |  |
|  | A Mathematical Perspective on Post-Quantum Cryptography | Richter, M., Bertram, M., Seidensticker, J., & Tschache, A. (2022). A Mathematical Perspective on Post-Quantum Cryptography. *Mathematics*, *10*(15). https://doi.org/10.3390/math10152579 |  |
|  | A\_Comparison\_of\_Security\_and\_its\_Performance\_for\_Key\_Agreements\_in\_Post-Quantum\_Cryptography | Borges, F., Reis, P. R., & Pereira, D. (2020). A Comparison of Security and its Performance for Key Agreements in Post-Quantum Cryptography. *IEEE Access*, *8*, 142413–142422. https://doi.org/10.1109/ACCESS.2020.3013250 |  |
|  | On the Lattice Isomorphism Problem, Quadratic Forms, Remarkable Lattices, and Cryptography | Rebane, R.-M. (n.d.). *Intro to Code-Based Schemes*. |  |
|  | Review of the book “Post-Quantum Cryptography" | Bernstein, D. J. (Daniel J., Buchmann, Johannes., & Dahmén, E. (2009). *Post-quantum cryptography*. Springer. |  |
|  | Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: a survey | Seyhan, K., Nguyen, T. N., Akleylek, S., & Cengiz, K. (2022). Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: a survey. *Cluster Computing*, *25*(3), 1729–1748. https://doi.org/10.1007/s10586-021-03380-7 |  |
|  | Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms | Asif, R. (2021). Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms. *IoT*, *2*(1), 71–91. https://doi.org/10.3390/iot2010005 |  |
|  | Quantum-safe cryptography: crossroads of coding theory and cryptography | Wang, J., Liu, L., Lyu, S., Wang, Z., Zheng, M., Lin, F., Chen, Z., Yin, L., Wu, X., & Ling, C. (2022). Quantum-safe cryptography: crossroads of coding theory and cryptography. In *Science China Information Sciences* (Vol. 65, Issue 1). Science Press (China). https://doi.org/10.1007/s11432-021-3354-7 |  |
|  | A TUTORIAL INTRODUCTION TO LATTICE-BASED CRYPTOGRAPHY AND HOMOMORPHIC ENCRYPTION | Li, Y., Ng, K. S., & Purcell, M. (2022). *A Tutorial Introduction to Lattice-based Cryptography and Homomorphic Encryption*. http://arxiv.org/abs/2208.08125 |  |
|  | Ultra\_High-Speed\_Polynomial\_Multiplications\_for\_Lattice-Based\_Cryptography\_on\_FPGAs | Kundi, D. e. S., Zhang, Y., Wang, C., Khalid, A., Oneill, M., & Liu, W. (2022). Ultra High-Speed Polynomial Multiplications for Lattice-Based Cryptography on FPGAs. *IEEE Transactions on Emerging Topics in Computing*, *10*(4), 1993–2005. https://doi.org/10.1109/TETC.2022.3144101 |  |
|  | NIST Post-Quantum Cryptography-A Hardware Evaluation Study | Basu, K., Soni, D., Nabeel, M., & Karri, R. (n.d.). *NIST Post-Quantum Cryptography-A Hardware Evaluation Study*. http://cyber.nyu.edu |  |
|  | A\_Survey\_on\_NIST\_Selected\_Third\_Round\_Candidates\_for\_Post\_Quantum\_Cryptography | Hasija, T., Ramkumar, K. R., Kaur, A., Mittal, S., & Singh, B. (2022). A Survey on NIST Selected Third Round Candidates for Post Quantum Cryptography. *7th International Conference on Communication and Electronics Systems, ICCES 2022 - Proceedings*, 737–743. https://doi.org/10.1109/ICCES54183.2022.9835864 |  |
|  | A Framework for Cryptographic Problems from Linear Algebra | Bootland, C., Castryck, W., Szepieniec, A., & Vercauteren, F. (n.d.). *A Framework for Cryptographic Problems from Linear Algebra*. |  |
|  | Analysis of Error-Correcting Codes for Lattice-Based Key Exchange | Cid, C., & Jacobson, M. J. (Eds.). (2019). *Selected Areas in Cryptography – SAC 2018* (Vol. 11349). Springer International Publishing. https://doi.org/10.1007/978-3-030-10970-7 |  |
|  | Ring-LWE Ciphertext Compression and Error Correction | Saarinen, M. J. O. (2017). Ring-LWE ciphertext compression and error correction tools for lightweight post-quantum cryptography. *IoTPTS 2017 - Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, Co-Located with ASIA CCS 2017*, 15–22. https://doi.org/10.1145/3055245.3055254 |  |
|  | kody-kompozitsii-i-reshetki | Кутьин, А. М. (n.d.). *П Р И К Л А Д Н А Я Д И С К Р Е Т Н А Я М А Т Е М А Т И К А 2008 Теоретические основы прикладной дискретной математики № 1(1) КОДЫ, КОМПОЗИЦИИ И РЕШЕТКИ*. |  |
|  | ANALIZ POSTKVANTOVYH KRIPTOGRAFIChESKIH ALGORITMOV | *ANALIZ POSTKVANTOVYH KRIPTOGRAFIChESKIH ALGORITMOV*. (n.d.). |  |
|  | SKFUnit\_2\_2017 | *SKFUnit\_2\_2017*. (n.d.). |  |
|  | Lattice Based Cryptography | Micciancio, D. (2003). *Lattice Based Cryptography*. |  |
|  | Cryptanalysis of the McEliece Public Key Cryptosystem Based on Polar Codes | Takagi, T. (Ed.). (2016). *Post-Quantum Cryptography* (Vol. 9606). Springer International Publishing. https://doi.org/10.1007/978-3-319-29360-8 |  |
|  | Analysis of Information Set Decoding for a Sub-linear Error Weight | Takagi, T. (Ed.). (2016). *Post-Quantum Cryptography* (Vol. 9606). Springer International Publishing. https://doi.org/10.1007/978-3-319-29360-8 |  |
|  | Lattice Cryptography for the Internet | Peikert, C. (n.d.). *Lattice Cryptography for the Internet*. |  |
|  | A Note on Quantum Security for Post-Quantum | Song, F. (n.d.). *A Note on Quantum Security for Post-Quantum Cryptography*. |  |
|  | A New Rank Metric Codes Based Encryption Scheme | Lange, T., & Takagi, T. (Eds.). (2017). *Post-Quantum Cryptography* (Vol. 10346). Springer International Publishing. https://doi.org/10.1007/978-3-319-59879-6 |  |
|  | EXAMINING A POSSIBILITY TO USE AND THE BENEFITS OF POST-QUANTUM ALGORITHMS DEPENDENT ON THE CONDITIONS OF THEIR APPLICATION |  |  |
|  | A Performance Comparison of Post-Quantum Algorithms in Blockchain | Gan, L., & Yokubov, B. (2023). A Performance Comparison of Post-Quantum Algorithms in Blockchain. *The Journal of The British Blockchain Association*, *6*(1), 1–10. https://doi.org/10.31585/jbba-6-1-(1)2023 |  |
|  | A usability study of post-quantum algorithms | Kindberg, M. (n.d.). *A usability study of post-quantum algorithms*. |  |
|  | Investigation on lattices- and code-based post-quantum signature cryptosystems | Feldman, A., Liang, K., & Chen, H. (n.d.). *Investigation on lattices-and code-based post-quantum signature cryptosystems*. |  |
|  | PopularScience | Mårtensson, E. (2020). *Populärvetenskaplig sammanfattning*. |  |
|  | Post-Quantum Cryptography State of the Art | Buchmann, J. A., Butin, D., Göpfert, F., & Petzoldt, A. (n.d.). *Post-Quantum Cryptography: State of the Art*. |  |
|  | From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things | Fernandez-Carames, T. M. (2020). From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. In *IEEE Internet of Things Journal* (Vol. 7, Issue 7, pp. 6457–6480). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/JIOT.2019.2958788 |  |
|  | Recent Advances in Post-Quantum Cryptography for Networks: A Survey | Zeydan, E., Turk, Y., Aksoy, B., & Bugrahan Ozturk, S. (n.d.). *Recent Advances in Post-Quantum Cryptography for Networks: A Survey*. |  |
|  | cvp | *Lecture 3 CVP Algorithm Lecturer: Oded Regev Scribe: Eyal Kaplan*. (n.d.). |  |
|  | AGNotes |  |  |
|  | ON CYCLIC ALGEBRAIC-GEOMETRY CODES | Cabaña, G., Chara, M., Podestá, R. A., & Toledano, R. (2021). *On cyclic algebraic-geometry codes*. <http://arxiv.org/abs/2106.08884> |  |
|  | MODERN CODING THEORY | Richardson, T. J. (Thomas J., & Urbanke, R. L. (2008). *Modern coding theory*. Cambridge University Press. |  |
|  | On Metric Dimension of Nonbinary Hamming Spaces | Kabatiansky, G. A., & Lebedev, V. S. (2018). On Metric Dimension of Nonbinary Hamming Spaces. *Problems of Information Transmission*, *54*(1), 48–55. https://doi.org/10.1134/S0032946018010040 |  |
|  | Algebraic Geometric Codes over Rings | Bartley, K. G., & Walker, J. L. (2008). *Algebraic Geometric Codes over Rings*. |  |
|  | Algebraic\_Geometry\_Codes | Tomlinson, M., Tjhai, C. J., Ambroze, M. A., Ahmed, M., & Jibril, M. (2017). *Algebraic Geometry Codes* (pp. 181–203). <https://doi.org/10.1007/978-3-319-51103-0_8> |  |
|  | Algebraic\_Geometry\_Codes\_Basic\_Notions | Tsfasman, M., Vlˇadut¸, S., Vlˇadut¸, V., & Nogin, D. (n.d.). *Algebraic Geometry Codes Basic Notions*. |  |
|  | AlgGeoCodes | Manber, S. (2011). *Algebraic Geometry Codes Shelly Manber Linear Codes Algebraic Geometry Codes Example: Hermitian Codes Decoding Algebraic Geometry Codes*. |  |
|  | An introduction to Algebraic Geometry codes | Munuera, C., & Olaya-León, W. (2015). *An Introduction to Algebraic Geometry codes*. http://arxiv.org/abs/1505.03020 |  |
|  | AGNotes | Rosen, Z., & Borcherds, R. (2012). *Algebraic Geometry Notes*. http://math.berkeley.edu/ |  |
|  | Algebraic Algorithms and Coding Theory | Sudan, M. (n.d.). *Algebraic Algorithms and Coding Theory*. |  |
|  | Error-Correction Coding and Decoding | Tomlinson Cen Jung Tjhai Marcel Ambroze Mohammed Ahmed Mubarak Jibril, M. A. (n.d.). *Signals and Communication Technology Error-Correction Coding and Decoding*. http://www.springer.com/series/4748 |  |
|  | Foundations of Algebraic Geometry | *THE RISING SEA Foundations of Algebraic Geometry*. (2022). |  |
|  | Improved Decoding of Reed-Solomon and Algebraic-Geometric Codes | Guruswami, V., & Sudan, M. (n.d.). *Improved Decoding of Reed-Solomon and Algebraic-Geometric Codes*. |  |
|  | Introduction to Algebraic Geometry | Dolgachev, I. v. (2013). *Introduction to Algebraic Geometry*. |  |
|  | Linear Algebra Done Right | Axler, S. (n.d.). *Undergraduate Texts in Mathematics Linear Algebra Done Right*. http://www.springer.com/series/666 |  |
|  | Practical\_Cryptography\_in\_Python\_Learning\_Correct\_Cryptography\_by | Nielson, S. J., & Monson, C. K. (2019). Practical cryptography in python: Learning Correct Cryptography by Example. In *Practical Cryptography in Python: Learning Correct Cryptography by Example*. Apress Media LLC. https://doi.org/10.1007/978-1-4842-4900-0 |  |
|  | Tutte | *tutte*. (n.d.). |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Gil Cohen - algebraic geometric codes

<https://www.youtube.com/results?search_query=algebraic+geometric+codes>

Prof. María Chara - An Introduction to Algebraic Geometry Codes

<https://www.youtube.com/watch?v=A8lb45WlhOo>

Peter Beelen - Algebraic Geometric Codes (2 of 5)

<https://www.youtube.com/watch?v=-SYT6lTyN_I>

Elena Berardini – Riemann–Roch spaces and algebraic geometry codes

<https://www.youtube.com/watch?v=4W6tT489MYc>

Math Cryptography - Algebraic Geometry Codes 1

<https://www.youtube.com/watch?v=RIvu1FOrMrc>

Math Cryptography - Cyclic Codes 1

<https://www.youtube.com/watch?v=QYItV-POgJ4&list=PLp6V5-Qloiv-Gnu2sg9DXHJ5zfL5_vODU&index=4>

Richard E. BORCHERDS - algebraic geometry 7 weak nullstellensatz

<https://www.youtube.com/watch?v=hBQXqIkUUyY>

Lothar Göttsche - Algebraic Geometry - Lecture 01

<https://www.youtube.com/watch?v=ceAtMOmyu1A>

Mary Wootters - Lecture 5, Video 2: Berlekamp Welch Algorithm

<https://www.youtube.com/watch?v=0WfAGR-vVwk&list=PLkvhuSoxwjI_UudECvFYArvG0cLbFlzSr&index=21>

تئوری کدینگ - دکتر فرزاد پرورش

<https://maktabkhooneh.org/course/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%DA%A9%D8%AF%DB%8C%D9%86%DA%AF-mk1496/>

همکاری در آینده

Mathematics Sin Fronteras

<https://www.dam.brown.edu/MSF/Archives/Spring2021/index.html>

List of unsolved problems in mathematics

<https://en.wikipedia.org/wiki/List_of_unsolved_problems_in_mathematics>

<https://researchrabbitapp.com/>

<https://github.com/sobolevn/awesome-cryptography#python>