# Delaram Kahrobaei

List of Publications by Year
in descending order

| | | | |
|---|---|---|---|
| 44 papers | 326 citations | 1163117 8 h-index | 996975 15 g-index |
| 45 all docs | 45 docs citations | 45 times ranked | 212 citing authors |

| # | Article | IF | Citations |
|---|---------|-----|-----------|
| 1 | A Survey on Delegated Computation. Lecture Notes in Computer Science, 2022, , 33-53. | 1.3 | 2 |
| 2 | An algebraic characterization of ?–colorability. Proceedings of the American Mathematical Society, 2021, 149, 2249-2255. | 0.8 | 2 |
| 3 | Hamiltonicity via cohomology of right-angled Artin groups. Linear Algebra and Its Applications, 2021, 631, 94-110. | 0.9 | 1 |
| 4 | Secure and Efficient Delegation of Pairings with Online Inputs. Lecture Notes in Computer Science, 2021, , 84-99. | 1.3 | 4 |
| 5 | A closer look at the tropical cryptography. International Journal of Computer Mathematics: Computer Systems Theory, 2021, 6, 137-142. | 1.1 | 10 |
| 6 | A note on fully homomorphic encryption of real-life data. International Journal of Computer Mathematics: Computer Systems Theory, 2021, 6, 381-385. | 1.1 | 0 |
| 7 | Single-Server Delegation of Ring Multiplications from Quasilinear-time Clients. , 2021, , . | | 3 |
| 8 | Solving the Conjugacy Decision Problem via Machine Learning. Experimental Mathematics, 2020, 29, 66-78. | 0.7 | 5 |
| 9 | Efficient and Secure Delegation of Exponentiation in General Groups to a Single Malicious Server. Mathematics in Computer Science, 2020, 14, 641-656. | 0.4 | 4 |
| 10 | A cryptographic application of the Thurston norm. International Journal of Computer Mathematics: Computer Systems Theory, 2020, 5, 15-24. | 1.1 | 2 |
| 11 | Secure and Efficient Delegation of Elliptic-Curve Pairing. Lecture Notes in Computer Science, 2020, , 45-66. | 1.3 | 5 |
| 12 | Secure Delegation to a Single Malicious Server: Exponentiation in RSA-type Groups. , 2019, , . | | 8 |
| 13 | Some applications of arithmetic groups in cryptography. Groups, Complexity, Cryptology, 2019, 11, 25-33. | 0.3 | 1 |
| 14 | ON THE CONJUGACY PROBLEM IN CERTAIN METABELIAN GROUPS. Glasgow Mathematical Journal, 2019, 61, 251-269. | 0.3 | 2 |
| 15 | Private naive bayes classification of personal biomedical data: Application in cancer data analysis. Computers in Biology and Medicine, 2019, 105, 144-150. | 7.0 | 39 |
| 16 | Algorithmic problems in right-angled Artin groups: Complexity and applications. Journal of Algebra, 2019, 519, 111-129. | 0.7 | 7 |
| 17 | Practical private-key fully homomorphic encryption in rings. Groups, Complexity, Cryptology, 2018, . | 0.3 | 1 |
| 18 | Fully Automated Spleen Localization And Segmentation Using Machine Learning And 3D Active Contours. , 2018, 2018, 53-56. | | 5 |

| # | Article | IF | Citations |
|---|---------|----|-----------|
| 19 | Private-Key Fully Homomorphic Encryption for Private Classification. Lecture Notes in Computer Science, 2018, , 475-481. | 1.3 | 5 |
| 20 | Efficient and Secure Delegation to a Single Malicious Server: Exponentiation over Non-abelian Groups. Lecture Notes in Computer Science, 2018, , 137-146. | 1.3 | 6 |
| 21 | The Hidden Subgroup Problem and Post-quantum Group-Based Cryptography. Lecture Notes in Computer Science, 2018, , 218-226. | 1.3 | 4 |
| 22 | Quadratic Time Algorithm for Inversion of Binary Permutation Polynomials. Lecture Notes in Computer Science, 2018, , 19-27. | 1.3 | 0 |
| 23 | Algorithmic recognition of infinite cyclic extensions. Journal of Pure and Applied Algebra, 2017, 221, 2157-2179. | 0.6 | 3 |
| 24 | Practical and Secure Outsourcing of Discrete Log Group Exponentiation to a Single Malicious Server. , 2017, , . | | 13 |
| 25 | Deep Convolutional Neural Networks for left ventricle segmentation. , 2017, 2017, 668-671. | | 10 |
| 26 | Computing multiple exponentiations in discrete log and RSA groups: From batch verification to batch delegation. , 2017, , . | | 7 |
| 27 | The status of polycyclic group-based cryptography: A survey and open problems. Groups, Complexity, Cryptology, 2016, 8, . | 0.3 | 10 |
| 28 | Using Semidirect Product of (Semi)groups in Public Key Cryptography. Lecture Notes in Computer Science, 2016, , 132-141. | 1.3 | 8 |
| 29 | Length-based attacks in polycyclic groups. Journal of Mathematical Cryptology, 2015, 9, 33-43. | 0.7 | 7 |
| 30 | Efficient and Secure Delegation of Group Exponentiation to a Single Server. Lecture Notes in Computer Science, 2015, , 156-173. | 1.3 | 24 |
| 31 | A family of polycyclic groups over which the uniform conjugacy problem is NP-complete. International Journal of Algebra and Computation, 2014, 24, 515-530. | 0.5 | 4 |
| 32 | Heisenberg Groups as Platform for the AAG Key-Exchange Protocol. , 2014, , . | | 1 |
| 33 | On the dimension of matrix representations of finitely generated torsion free nilpotent groups. Groups, Complexity, Cryptology, 2013, 5, . | 0.3 | 1 |
| 34 | Classification of embeddings of abelian extensions of into. Journal of Pure and Applied Algebra, 2013, 217, 1942-1954. | 0.6 | 8 |
| 35 | Public key exchange using matrices over group rings. Groups, Complexity, Cryptology, 2013, 5, . | 0.3 | 46 |
| 36 | Public Key Exchange Using Semidirect Product of (Semi)Groups. Lecture Notes in Computer Science, 2013, , 475-486. | 1.3 | 23 |

| # | Article | IF | Citations |
|---|---------|-----|-----------|
| 37 | Non-commutative digital signatures. Groups, Complexity, Cryptology, 2012, 4, . | 0.3 | 9 |
| 38 | On the Residual Solvability of Generalized Free Products of Finitely Generated Nilpotent Groups. Communications in Algebra, 2011, 39, 647-656. | 0.6 | 5 |
| 39 | Growth rate of an endomorphism of a group. Groups, Complexity, Cryptology, 2011, 3, . | 0.3 | 6 |
| 40 | Decision and Search in Non-Abelian Cramer-Shoup Public Key Cryptosystem. Groups, Complexity, Cryptology, 2009, 1, . | 0.3 | 6 |
| 41 | Doubles of Residually Solvable Groups. , 2008, , . | | 1 |
| 42 | The true prosoluble completion of a group: Examples and open problems. Geometriae Dedicata, 2007, 124, 5-26. | 0.3 | 9 |
| 43 | NIS05-6: A Non-Commutative Generalization of ElGamal Key Exchange using Polycyclic Groups. IEEE Global Telecommunications Conference (GLOBECOM), 2006, , . | 0.0 | 9 |
| 44 | A closer look at the multilinear cryptography using nilpotent groups. International Journal of Computer Mathematics: Computer Systems Theory, 0, , 1-5. | 1.1 | 0 |