❖ 期刊論文

[1] Chen, R. J. and Meyer, R. R.(1988)"Parallel Optimization for Traffic Assignment," Mathematical Programming 42. pp. 327-345.

[2] Tsai,Y. D. and Chen, R. J.(1989)"Solving Linear Multicommodity Problems on the Transputers," Journal of Computers, pp. 23-33.

[3] Chen, R. J. and Hou,Y. S. (1991)"A Branch-and-Bound Algorithm for Single-Row Routing," Journal of Information Science and Engineering, Vol. 7, No. 3, pp. 335-345.

[4] Wu, J. S. and Chen, R. J.(1992)"An O(kn) Algorithm for Circular Consecutive-k-out-of-n:F System," IEEE Transactions on Reliability, Vol. 41, No. 2, pp. 303-305.

[5] Chen, R. J. and Hou, Y. S.(1992)"Non-associative Parallel Prefix Computation," Information Processing Letters, Vol. 44, pp. 91-94.

[6] Wu, J. S. and Chen, R. J.(1992)"The Towers of Hanoi Problem with Parallel Moves," Information Processing Letters, Vol. 44, pp. 241- 243.

[7] Wu, J. S. and Chen, R. J.(1993)"Efficient Algorithm for Reliability of a Circular Consecutive-k- out-of-n:F System," IEEE Transactions on Reliability, Vol. 42, No. 1, pp. 163-164.

[8] Wu, J. S. and Chen, R. J.(1993)"The Towers of Hanoi Problem with Cyclic Parallel Moves," Information Processing Letters, Vol. 46, pp. 1-6.

[9] Chien, B. C., Chen, R. J., and Yang, W. P.(1993)"Analysis of the Multigroup Method for Manipulating Multiple Stacks," Computers & Mathematics with Applications, Vol. 25, No. 3, pp.43-57.

[10] Chien, B.C., Yang, W. P., and Chen, R. J.(1993)"Manipulating Multiple Stacks with Ordered- Heap," Information Sciences, Vol. 72, pp. 207-224.

[11] Wu, J. S. and Chen, R. J.(1994)"An Algorithm for Computing the Reliability of Weighted-k-out- of-n Systems," IEEE Transactions on Reliability, Vol. 43, No. 2, pp. 327-328.

[12] Wu, J. S. and Chen, R. J.(1994)"Efficient Algorithms for k-out-of-n and Consecutive-weighted-k- out-of-n:F Systems," IEEE Transactions on Reliability, Vol. 43, No. 4, pp. 650-655.

[13] Chiang, W. K. and Chen, R. J.(1994)"Distributed Fault Tolerant Routing in Kautz Networks," Journal of Parallel and Distributed Computing, Vol. 20, pp.99-106.

[14] Wu, J. S. and Chen, R. J.(1994)"Reliability of Consecutive-weighted- k-out-of-n:F System," Runs and Patterns in Probability, Cluwer Academic Publishers, pp. 205-211.

[15] Chen, C. C. and Chen, R. J.(1995)"Compact Embedding of Binary Trees into Hypercubes," Information Processing Letters, Vol. 54, pp. 69-72.

[16] Hou, Y. S. and Chen, R. J.(1995)"Poisson Generators on Mesh-Connected Computers with Multiple Broadcasting," Journal of Information Science and Engineering, Vol. 11, pp. 663-673.

[17] Chiang, W. K. and Chen, R. J.(1995)"The (n,k)-Star Graph: Generalized Star Graphs," Information Processing Letters, Vol. 56, pp. 259-264.

[18] Chen, C. C. and Chen, R. J.(1996)"Optimal Embedding of Large Complete Binary Trees into Hypercubes," Journal of Information Science and Engineering, Vol. 12, pp. 307-314.

[19] Lu, T. C., Hou, Y. S., and Chen, R. J.(1996)"A Parallel Prefix Poisson Generator," Computers and Mathematics with Application, Vol. 31, No. 3, pp. 33-42.

[20] Chiang, W. K. and Chen, R. J.(1996)"Topological Properties of Hierarchical Cubic Networks," Journal of Systems Architecture, Vol. 42, pp. 289-307.

[21] Chiang, W. K. and Chen, R. J.(1996)"Multilevel-Hypercubes: An Efficient Class of Hypercube Interconnection Networks for Massively Parallel Systems," Journal of Information Science and Engineering, Vol. 12, pp. 317-343.

[22] Chiang, W. K. and Chen, R. J.(1997)"Block-Switch Networks: A Cost-Effective Class of Interconnection Networks," Computer Systems Science & Engineering, Vol. 12, No. 3, pp. 175-185.

[23] Chan, W. C., Lu, T. C., and Chen, R. J.(1997)"On the Pollaczek-Khinchin Formula for the M/G/1 Queue in Discrete Time with Vacations," IEE Proc. Comput. Digit. Tech., Vol. 144, pp. 222-226.

[24] Chang, H. Y. and Chen, R. J.(1997)"Embedding Cycles in IEH Graphs," Information Processing Letters, Vol. 64, pp. 23-27.

[25] Chiang, W. K. and Chen, R. J.(1997)"Topological Properties of (n,k)-Star Graph," International Journal of Foundations of Computer Science, Vol. 9, No. 2, pp.235-248.

[26] Chiang, W. K. and Chen, R. J.(1998)"On the arrangement graph," Information Processing Letters(EI), Vol. 66, pp. 215-219.

[27] Chang, J. C., Chen, R. J., and Hwang, F. K.(1998)"A Fast Reliability Algorithm for the Consecutive-Weighted-k-out-of-n:F System," IEEE Transactions on Reliability(EI), Vol. 47, No. 4, pp. 472-474.

[28] Chang, H. Y. and Chen, R. J.(2001)"Graph Embedding Aspect of IEH Graphs," Journal of Information Science and Engineering(EI), Vol. 17, pp. 23-33.

[29] Chen, R. J., Lin, T. Y., and Lin, Y. B.(1999)"Reducing Power Consumption for Mobile Multimedia Handset," to appear in Tamkang Journal of Science and Engineering special issue on Multimedia Computing and Network.

[30] Lin, Y. B., Lai, W. R., and Chen, R. J.(2000)"Performance Analysis for Dial Band PCS Networks," IEEE Transactions on Computers(SCI/EI), Vol. 49, 148-159.

[31] Chang, H. Y. and Chen, R. J.(2000)"Incrementally Extensible Folded Hypercube Graphs," Journal of Information Science and Engineering(EI), Vol. 16, pp. 291-300.

[32] Akyildiz, I. F., Lin, Y. B., Lai, W. R., and Chen, R. J.(2000)"A New Model for Random Walks in PCS Networks," IEEE Journal on Selected Areas in Communications(SCI/EI), Vol. 18, No. 7, pp. 1254-1260.

[33] Chang, H. W., Chen, R. J., and Hwang, F. K.(2002)"The Structural Birnbaum Importance of Consecutive-k Systems," Journal of Combinatorial Optimization(EI), Vol. 6, No. 2, pp. 183-197.

[34] Chen, R. J., Lin, T. Y., and Lin, Y. B.(2001)"Adaptive Schemes for Reducing Power Consumption of Mobile Data Handsets," Journal of Interconnection Networks, Vol. 2, No. 1, pp. 69-84.

[35] Chang, J. C., Chen, R. J., and Hwang, F. K.(2001)"A minimal-automaton-based algorithm for the reliability of Con(d, k, n) systems," Methodology and Computing in Applied Probability, Vol. 3, No. 4, pp.379-386.

[36] Chang, J. C., Chen, R. J., and Hwang, F. K. (2001)"On the regular reliability models," Systems and Bayesian Reliability, Eds. Y. Hayakawa, T. Irony and M. Xie.

[37] Chang, J. C., Chen, R. J., and Hwang, F. K. (2003)"An efficient algorithm for the reliability of consecutive-k-n networks," Journal of Information Science and Engineering(EI), Vol. 19, pp. 159-166.

[38] Chang, J. C., Chen, R. J., Klove, T., and Tsai, S. C. (2003) "Distance preserving mappings from binary vectors to permutations," IEEE Transactions on Information Theory(SCI/EI), Vol. 49, No. 4, pp. 1054-1059.

[39] Lin, J. S., Chang, J. C., and Chen, R. J. (2006)"New Simple Constructions of Distance-Increasing Mappings from Binary Vectors to Permutations," Information Processing Letters, Vol. 100, No. 2, pp. 83-89.

[40] Hwu, J. S., Chen, R. J., and Lin, Y. B. (2006)"An Efficient Identity-Based Cryptosystem for End-to-End Mobile Security," IEEE Trans. On Wireless Communications, Vol. 5, pp.2586-2593..

[41] Hwu, J. S., Hsu, S. F., Lin, Y. B., and Chen, R. J. (2006)" End-to-end Security Mechanisms for SMS," International Journal of Security and Networks, pp. 177-183.

[42] Lin, J. S., Chang, J. C., Chen, R. J., and Klove, T. (2008) "Distance preserving mappings from ternary vectors to permutations," IEEE Transactions on Information Theory(SCI/EI), Vol. 54, No. 3, pp. 1334-1339.

[43] Tseng, F. K., Liu, Y. H., Hwu, J. S., and Chen, R. J. (2011) "A Secure Reed-Solomon Code Incentive Scheme for Commercial Ad Dissemination over VANETs," IEEE Transactions on Vehicular Technology, Vol.60, No.9, pp.4598-4608.

[44] Tseng, F. K. and Chen, R. J. (2015) “Cryptanalysis and Improvement of an Encoding Method for Private-key Hidden Vector Encryptions,” IEICE Transaction on Fundamentals of Electronics Communications and Computer Sciences, Vol.E98-A, No. 9, pp. 1982-1984.

[45] Tseng, F. K. and Chen, R. J. (2016) “Towards Position-Aware Symbol-Based Searches on Encrypted Data from Symmetric Predicate Encryption Schemes,” IEICE Transaction on Fundamentals of Electronics Communications and Computer Sciences, Vol.E98-A, No. 1, pp. 1-3.

[46] Liu, Y. H. and Chen, R. J. (2017) “An asymptotically perfect secret sharing scheme based on the Chinese Remainder Theorem,” accepted and to appear in International Journal of Computer Mathematics.

,

❖ 研討會論文

[1] Chen, R. J. and Meyer, R. R. (1987) "A Scaled Trust Region Method for a Class of Convex Optimization Problems," ORSA, New Orleans, May 1987.

[2] Lo, S. Y, and Chen, R. J.(1989)"On Generalized Networks," 1st Conference for Computational Foundation and Discrete Mathematics, Taiwan.

[3] Chen, R. J.(1989) "A Lagrangian Relaxation Approach for Global Routing," 2nd Conference for Computational Foundation and Discrete Mathematics, Taiwan.

[4] Chiang,W. K. and Chen, R. J.(1992) "Distributed Fault Tolerant Routing in Kautz Networks," 3rd IEEE Workshop on Future Trends in Distributed Computer System.

[5] Chien, B. C., Chen, R. J., and Yang, W. P. (1992) "The Probability Analysis of Garwick's Method for Multiple Stacks Manipulation," Proceedings of International Computer Symposium, Taichung, Taiwan, pp. 425-432.

[6] Chien, B. C., Chen, R. J.,and Yang, W. P. (1992) "Competitive Analysis of the On-line Algorithms for Multiple Stacks Systems," 3rd International Symposium on Algorithm & Computation (ISACC'92), Nagoya, Japan, December.

[7] Chen, R. J., Meyer, R. R., and Yackel, J. (1993)"A Genetic Algorithm for Diversity Minimization and Its Parallel Implementation," 5th International Conference on Genetic Algorithms, UI-Urbana-Champaign, July.

[8] Wu, J. S. and Chen, R. J.(1993) "The Non-recursive Algorithms for the Parallel Towers of Hanoi Problem," 29th Mathematics Symposium, Hsinchu, Taiwan, December.

[9] Chen, C. C. and Chen, R. J.(1994) "Compact Embedding of Binary Trees into Hypercubes," Proceedings of International Computer Symposium, Hsinchu, Taiwan, pp. 829-834.

[10] Wu, J. S. and Chen, R. J.(1994) "Reliability Analysis on K-Terminal Networks," Proceedings of International Computer Symposium, Hsinchu, Taiwan, pp.265-270.

[11] Chiang, W. K. and Chen, R. J.(1994) "Pyramided Hypercube: An Extendable Cubic Network with Fixed Degree," Proceedings of International Conference on Parallel and Distributed Systems, Hsinchu, Taiwan, pp. 690-697.

[12] Chiang, W. K. and Chen, R. J.(1995) "Optimal Routing on Hierarchical Cubic Networks," Proceedings of the 11th Workshop on Combinatorial Mathematics and Computation Theory, May.

[13] Chiang, W. K. and Chen, R. J.(1995) "An Efficient Class of Reduced Hypercubes for Parallel Computations," Proceedings of the Workshop on High Performance Multiprocessor Systems, July 4.

[14] Chang, H. Y. and Chen, R. J.(1997) "Cycle Structure in IEH Graphs," 14th Workshop on Combinatorial Mathematics and Computation Theory, Taiwan.

[15] Chang, H. Y. and Chen, R. J.(1997) "Embedding Graphs onto IEH Graphs," Proceedings of National Computer Symposium, Taiwan, Vol. 3, pp. E7-E11.

[16] Chang, H. Y. and Chen, R. J.(1998) "Incrementally Extensible Folded Hypercube Graphs," International Conference on Parallel and Distributed Systems, Tainan, Taiwan, December.

[17] Hwu, J. S. and Chen, R. J.(1998) "DNA Solution to Traveling Salesman Optimization Problem," International Computer Symposium, Tainan, Taiwan, December.

[18] Chen, J. R., Chang, M. F., and Chen, R. J.(1998) "Genetic Algorithms for Channel Assignment in PCS," International Computer Symposium, Tainan, Taiwan, December.

[19] Chang, J. C. and Chen, R. J.(1998) "The Birnbaum Importance and the Optimal Replacement of the Consecutive k-out-of-n System," International Computer Symposium, Tainan, Taiwan, December.

[20] Lin, T. Y., Chen, R. J., and Lin, Y. B.(1999) "Reducing Power Consumption for Mobile Data Handsets," Proceedings of CSIA 1999-Mobile Computing, Taiwan, pp. 46-53.

[21] Hung, J. H., Hwu, J. S. and Chen, R. J.(2000) "Parallel RSA Factoring," Proceedings of the 10th National Conference on Information

Security, Taiwan, pp. 51-61.

[22] Huang, K. C., Chen, R. J., and Hou, Y. S.(2000) "Genetic Algorithm for Optimal Correlation- Immune Functions in Stream Cipher," Proceedings of the 10th National Conference on Information Security, Taiwan, pp. 168-174.

[23] Yang, S. H., Hwu, J. S., Huang, K. C., and Chen, R. J.(2001) "Performance Analysis for Arithmetic in Finite Field GF(p^n)," Proceedings of the 11th National Conference on Information Security, Taiwan, pp. 185-192.

[24] Chang, J. C., Hsu, W. C., and Chen, R. J.(2001) "An Efficient Oblivious Transfer Scheme with Optimal Base," Proceedings of the 11th National Conference on Information Security, Taiwan, pp. 241-247.

[25] Chang, J. C., Tsai, S. C., and Chen, R. J.(2002) "A Space-efficient Godel Numbering with Chinese Remainder Theorem," Proceedings of the 19th Workshop on Combinatorial Mathematics and Computation Theory, March, pp. 192-195.

[26] Lin, C. H., Tsai, S. C., and Chen, R. J.(2002) "Two New Constructions of Resilient Boolean Functions Satisfying Propagation Criterion," International Computer Symposium, Hualien, Taiwan, December, pp. 977-988

[27] Yeh, N. C., Tzeng, W. G., and Chen, R. J.(2002) "Cryptographic Protocols for Sealed-Bid Auctions without Trusted Servers," International Computer Symposium, Hualien, Taiwan, December, pp. 941-950.

[28] Hwu J. S., Chen R. J., Lue H. S., Lin J. S. (2004) "Efficient Computation of the Weil Pairing in ID-based Cryptosystems," International Computer Symposium, Taipei, Taiwan, December, pp. 1297-1301.

[29] Huang K. Q., Chang J. C., Chen R. J. (2004) "A new construction of resilient functions over GF(p) with good cryptographic properties," International Computer Symposium, Taipei, Taiwan, December, pp. 1213-1217.

[30] Liang H. C., Chang J. C., Chen R. J. (2004) "New Efficient Constructions of Binary Asymmetric Error-Correcting Codes," International Computer Symposium, Taipei, Taiwan, December, pp. 1036-1038.

[31] Liu, Wei-Ting, Chen Cheng-Kai, and Chen, Rong-Jaye (2005) "Experimental Linear Attacks on Substitution-Permutation Networks," Proceedings of the 15th National Conference on Information Security, Kaoshiung, Taiwan.

[32] Liang, Han-Chang and Chen, Rong-Jaye (2005) "A Trichotomy Reaction Attack on McEliece Public-Key Cryptosystem," Proceedings of the 15th National Conference on Information Security, Kaoshiung, Taiwan.

[33] Hwu, J. S., Chen, R. J., and Lin, Y. B. (2005) "Authenticated Public-Key Distribution over WLAN/Cellular Dual Networks." Proceedings of International Conference on Information Technology: Research and Education, Taiwan.

[34] Chen, Rong-Jaye and Tsai, Jr-Bing (2006) " Design of Secure Stream Ciphers on Sensor Networks," Proceedings of the 16th National Conference on Information Security, Taichung, Taiwan, pp. 122-130.

[35] Lin, Chia-Wei and Chen, Rong-Jaye (2007) "Performance Evaluation on Index Calculus Algorithms for Hyperelliptic Curves," Proceedings of the 17th Information Security Conference, Chia-Yi, Taiwan.

[36] Lin, Chia-Wei and Chen, Rong-Jaye (2008) " A fast graph algorithm for genus-2 hyperelliptic curve discrete logarithm problems," Proceedings of 25th Workshop on Combinatorial Mathematics and Computation Theory, Hsinchu, Taiwan.

[37] Liu, Yung-Hsiang, Tsai, Pei-Chuan, and Chen, Rong-Jaye (2008) "A Dynamic Selection Strategy of Atkin Primes in SEA Algorithm for Elliptic Curves," Proceedings of the 18th Cryptology and Information Security Conference, Hualien, Taiwan.

[38] Lin, Jyh-Shyan, Tseng, Fu-Kuo and Chen, Rong-Jaye (2009) "An Analysis of Hierarchical Identity-Based Cryptosystems," Proceedings of the 2009 International Conference on Foundations of Computer Science (FCS'09), July 13-16, 2009, Las Vegas, Nevada USA, pp. 27-31.

[39] Tseng, Fu-Kuo and Chen, Rong-Jaye (2009) "(n, t) Threshold Key Generation in Identity-based Cryptosystems," Proceedings of 2009 National Computer Symposium (NCS '09), Nov. 27-28, 2009, Taipei, Taiwan.

[40] Tseng, Fu-Kuo, Chen, Rong-Jaye and Hwu, Jing-Shyang (2010) "An Escrow-Free Hierarchical IBE Framework for VANETs," Proceedings of the 10th Anniversary of International Conference on Intelligent Transport Systems Telecommunications (ITST2010), Nov. 9-11, 2010, Kyoto, Japan.

[41] Shun-Lung Hsu, Rong-Jaye Chen (2011) "An Efficient Fully Homomorphic Encryption over Integers," Proceedings of the 21th

Cryptology and Information Security Conference, Yunlin, Taiwan.

[42] Chia-Wen Hsieh, Li-Ting Tsai, Jyh-Shyan Lin, and Rong-Jaye Chen (2011) “A Meet-In-The-Middle Attack against NTRU with Trinary Parameters,” Proceedings of the 21th Cryptology and Information Security Conference, Yunlin, Taiwan.

[43] Yung-Hsiang Liu, Li-Ting Tsai, Chia-Wen Hsieh, Rong-Jaye Chen (2011) “A Lattice Solution to Approximate Common Divisors,” Proceedings of the 28th Workshop on Combinatorial Mathematics and Computation Theory, Penghu, Taiwan.

[44] Fu-Kuo Tseng, Yung-Hsiang Liu and Rong-Jaye Chen, "Toward Authenticated and Complete Query Results from Cloud Storages," Trust, Security and Privacy in Computing and Communications (TrustCom'12) 2012 IEEE 11th International Conference on, pp.1204-1209, 25-27 June 2012.

[45] Fu-Kuo Tseng and Rong-Jaye Chen, "Enabling Searchable Dynamic Data Management for Collaboration in Cloud Storages," The 2012 International Conference on Security and Management (SAM'12), 16-19 Jul., 2012, Las Vegas, USA.

[46] Fu-Kuo Tseng, Yung-Hsiang Liu and Rong-Jaye Chen, "Ensuring correctness of range searches on encrypted cloud data," Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on , vol., no., pp.570,573, 3-6 Dec. 2012

[47] George Hsieh and Rong-Jaye Chen, "Design for a secure interoperable cloud-based Personal Health Record service," Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on , vol., no., pp.472,479, 3-6 Dec. 2012

[48] Fu-Kuo Tseng, Rong-Jaye Chen and Bao-Shuh Paul Lin, "iPEKS: Fast and Secure Cloud Data Retrieval from the Public-Key Encryption with Keyword Search," Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on , vol., no., pp.452,458, 16-18 July 2013

[49] Fu-Kuo Tseng, Yung-Hsiang Liu, Rong-Jaye Chen and Bao-Shuh Paul Lin, "Statistics on Encrypted Cloud Data," Security (IWSEC), 2013 8th International Workshop on, LNCS vol. 8231, pp.133-150, 18-20 November 2013

[50] Anrin Chakraborti, Yung-Hsiang Liu and Rong-Jaye Chen, "Applications of Homomorphic Encryption," 2013 National Computer Symposium (NCS 2013), 13-14 December 2013