

CURRICULUM VITÆ

October 9, 2020

1. Biographical and Personal Information

Name: D. J. Guan 官大智
Birthday: 1951/12/10
Birthplace: Hsinchu, Taiwan

2. Academic History

Purdue University, 1984/05 – 1989/08;
Master of Science in Computer Science, 1986/05;
Doctor of Philosophy in Computer Science, 1989/08.
Thesis: “Vehicle Routing in Simple Graphs.”

3. Current Position and Professional Experience

2017/02 – present. **Adjunct professor**, Department of Applied Mathematics, National Chiao Tung University,
2017/02 – present. **Adjunct professor**, Department of Computer Science, National Sun Yat-Sen University,
2017/02 – present. **Adjunct professor**, Department of Applied Mathematics, National Sun Yat-Sen University,
1999/02 – 2017/02 (retired). **Professor**, Department of Computer Science, National Sun Yat-Sen University,
1989/08 – 2017/02: **Associate Professor, Professor**, Department of Applied Mathematics, National Sun Yat-Sen University.
1991/08 – 1993/07: **Director**, Computing Science Research Center, National Sun Yat-Sen University.
1993/08 – 1996/07: **Chairman**, Department of Applied Mathematics, National Sun Yat-Sen University.
2003/08 – 2008/07: **Director**, Computer and Network Center, National Sun Yat-Sen University.
2007/08 – 2008/07: **University Librarian**, National Sun Yat-Sen University.
2008/08 – 2009/07: **Director**, Library and Information Services, National Sun Yat-Sen University.
2012/08 – 2015/07: **University Librarian**, National Chung Hsing University.

4. Fields of Specialty

Algorithms
Combinatorics
Cryptography
Information Security

5. Professional Societies

Chinese Cryptology and Information Security Association (CCISA) 中華民國資訊安全學會
Member of the Board of Directors, 1994 – 2015.
President, 2015 – 2018.
Computer Society of the Republic of China 中華民國電腦學會
Member of the Board of Directors, 2005 – .
Member of the Steering Committee of International Conference on the Theory and Application of Cryptology and Information Security (AsiaCrypt), 2006 – .
International Association for Cryptologic Research (IACR)
Member of the Board of Directors, 2012 – 2015.
Member of the Honor Society of *Phi Kappa Phi*, April 1987.

6. Professional Activities

General Chair of the 20th Annual International Conference on the Theory and Application of Cryptology and Information Security (AsiaCrypt 2014).

Guest Editor of the Journal of Combinatorial Optimization, 2011

General Chair of many local and Asian workshops and conferences in Graph Theory, Combinatorics, and Information Security

Reviewers of many Journals, including Acta Informatica, Communications of the ACM, Combinatorica, Discrete Applied Mathematics, Discrete Mathematics, Journal of Graph Theory, Journal of the ACM, ACM Computing Surveys, etc.

Mathematical Reviews Reviewer, Reviewer Number: 48537 of American Mathematical Society (Review of recently published papers, not submitted papers.)

URL of the reviews <https://mathscinet.ams.org/mresubs/reviewHist.html>

PUBLICATIONS OF D. J. GUAN

1. Selected Journal Papers

1. Greg N. Frederickson and **D. J. Guan**. Preemptive ensemble motion planning on a tree. *SIAM Journal on Computing*, 21(6):1130–1152, December 1992.
2. Greg N. Frederickson and **D. J. Guan**. Nonpreemptive ensemble motion planning on a tree. *Journal of Algorithms*, 15(1):29–60, July 1993.
3. Z. C. Li, T. T. Lu, **D. J. Guan**, and C. B. Yang. Boundary approximation methods for solving eigenvalue problems. *Zeitschrift für Angewandte Mathematik und Mechanik*, 76:455–456, 1996.
4. **D. J. Guan** and Xuding Zhu. A coloring problem for weighted graphs. *Information processing Letters*, 61(2):77–81, January 1997.
5. **D. J. Guan**. Routing a vehicle of capacity greater than one. *Discrete Applied Mathematics*, 81(1):41–57, January 1998.
6. **D. J. Guan**. An optimal message routing algorithm for double-loop networks. *Information Processing Letters*, 65(5):255–260, March 1998.
7. **D. J. Guan** and Xuding Zhu. Multiple capacity vehicle routing on paths. *SIAM Journal on Discrete Mathematics*, 11(4):590–602, November 1998.
8. **D. J. Guan**. Generalized gray codes with applications. *Proceedings of the National Science Council, Part A: Physical Science and Engineering*, 22(6):841–848, November 1998.
9. **D. J. Guan**, Z. C. Li, Y. L. Chen, and J. H. Chuang. Wire-frame method for blending surface design. *Proceedings of the National Science Council, Part A: Physical Science and Engineering*, 23(1):20–30, January 1999.
10. **D. J. Guan** and Xuding Zhu. Game chromatic number of outerplanar graphs. *Journal of Graph Theory*, 30(1):67–70, January 1999.
11. Chun-Yen Chou, **D. J. Guan**, and Kuei-Lin Wang. A dynamic fault-tolerant message routing algorithm for double-loop networks. *Information Processing Letters*, 70(6):259–264, June 1999.
12. **D. J. Guan**, Chun-Yen Chou, and Chiou-Wei Chen. Computational complexity of similarity retrieval in pictorial database. *Information Processing Letters*, 75(3):113–117, August 2000.
13. Tzong-Chen Wu, Shih-Chan Huang, and **D. J. Guan**. Delegated multi-signature scheme with document decomposition. *Journal of Systems and Software*, 55(3):321–328, January 2001.
14. Yu-Liang Liu, Yue-Li Wang, and **D. J. Guan**. An optimal fault-tolerant routing algorithm for double-loop networks. *IEEE Transactions on Computers*, 50(5), May 2001.
15. Chun-Yen Chou, **D. J. Guan**, and Jiun-Ming Chen. A systematic construction of a q_{2^k} -module in TTM. *Communications in Algebra*, 30(2):551–562, 2002.
16. W. C. Yang, **D. J. Guan**, and C. S. Lai. Algorithm of asynchronous binary signed-digit recording on fast multi-exponentiation. *Applied Mathematics and Computation*, 167(1):108–117, 2005.
17. W. C. Yang, **D. J. Guan**, and C. S. Lai. Fast multi-computations with integer similarity strategy. In Serge Vaudenay, editor, *Proceedings of the Eighth International Workshop on Theory and Practice in Public-key Cryptography*, pages 138–153. Springer, January 2005. LNCS 3386.
18. W. C. Yang, **D. J. Guan**, and C. S. Lai. Fast multi-computation with asynchronous strategy. *IEEE Transactions on Computers*, 56(2):234–242, February 2007.
19. Chun-I Fan, **D. J. Guan**, Chih-I Wang, and Dai-Rui Lin. Cryptanalysis of Lee-Hwang-Yang blind signature scheme. *Computer Standards & Interfaces*, 31(2):319–320, February 2009.
20. Dai-Rui Lin, Chih-I Wang, and **D. J. Guan**. A forward-backward secure signature scheme. *Journal of Information Science and Engineering*, 26(6):2319–2329, November 2010.
21. Dai-Rui Lin, Chih-I Wang, Zhi-Kai Zhang, and **D. J. Guan**. A digital signature with multi-subliminal channels and its applications. *Computers and Mathematics with Applications*, 60(2):276–284, July 2010.
22. Dai-Rui Lin, Chih-I Wang, and **D. J. Guan**. Efficient vehicle ownership identification scheme based on triple-trapdoor chameleon hash function. *Journal of Network and Computer Applications*, 34(1):12–19, January 2011.
23. Chun-I Fan, Wei-Zhe Sun, Chih-I Wang, and D. J. Guan. Efficient and flexible encoding scheme for date attachable electronic cash. *Far East Journal of Applied Mathematics*, 51:141–154, 2011.

24. Dai-Rui Lin, Chih-I Wang, and **D. J. Guan**. An efficient blind verifying for firewall using online/offline signcryption. *Journal of Internet Technology*, 13(4):607–614, July 2012.
25. **D. J. Guan**, Yuan-Jun Wang, and Er-Shuo Zhuang. Quantum key evolution and its applications. *International Journal of Quantum Information*, 10(4):1250044, July 2012.
26. **D. J. Guan** and Yuan-Jun Wang. Information leakage on four-state quantum bits. *Journal of Computational Information Systems*, 8(21):8847–8854, November 2012.
27. **D. J. Guan**, Yuan-Jun Wang, and E. S. Zhuang. A practical protocol for three-party authenticated quantum key distribution. *Quantum Information Processing*, 13(11):2355–2374, November 2014. DOI: 10.1007/s11128-014-0767-1.
28. Chia-Mei Chen, **D. J. Guan**, and Qun-Kai Su. Feature set identification for detecting suspicious urls using bayesian classification in social networks. *Information Sciences*, 289(1):133–147, December 2014.
29. Albert Guan and **D. J. Guan**. An efficient and privacy protection communication scheme for smart grid. *IEEE Access*, 8:179047–179054, 2020.

2. Selected Conference Papers

1. Greg N. Frederickson and **D. J. Guan**. Ensemble motion planning on a tree. In *Proceedings of the Thirtieth IEEE Symposium on Foundations of Computer Science*, pages 66–71, November 1989.
2. **D. J. Guan**, Chia-Mei Chen, and Jia-Bin Lin. Anomaly based malicious URL detection in instant messaging. In *Proceedings of the Fourth Joint Workshop on Information Security*, (Best Paper Award) 2009.
3. Chia-Mei Chen, **D. J. Guan**, Qun-Kai Su, and Tse-Yao Wang. Malicious URL detection on facebook. In *Proceedings of the Sixth Joint Workshop on Information Security*, (Best Paper Award) 2011.

3. Other Publications

1. **D. J. Guan et al.** *Current Status in Cryptology Research and Development*. National Science Concile, 2005, 2008, 2014.
2. **D. J. Guan**. Reviews at least 6 recently published papers a year for Mathematical Reviews from 2005.