Full List of Publications

Fan (Terry) Zhang

Last Updated, 2017-12-28.

Contact Information

College of Information Science & Electronic Engineering, Zhejiang University
Room 603, Administration Builidng, 38 Zheda Road, Zhejiang University, Hangzhou, China
HomePage: http://www.isee.zju.edu.cn/fanzhang
E-mail: fanzhang@zju.edu.cn

Journal Papers: SCI-Indexed

1. L. Geng, J. Shen*, **F. Zhang**. "Dynamic current logic based flip-flop design for robust and low power security ICs," *Electronics Letters*, 2017 accepted

2. X. Zhao, **F. Zhang***, S. Guo, Z. Gong. "Optimal Model Search for Hardware-Trojan-based Bit-level Fault Attacks on Block Ciphers," *SCIENCE CHINA Information Sciences*, 2017 accepted

3. P. Zhou, T. Wang, X. Lou, X. Zhao, **F. Zhang***, S. Guo. "Efficient flush-reload cache attack on scalar multiplication based signature algorithm," *SCIENCE CHINA Information Sciences*, 2017 accepted

4. H. Chen, T. Wang, **F. Zhang***, X. Zhao, W. He, L. Xu, Y. Ma. "Stealthy Hardware Trojan Based Algebraic Fault Analysis of HIGHT Block Cipher," *Security and Communication Networks*, Vol.2017, ArticleID 8051728, 2017. [PDF]

5. **F. Zhang**, X. Zhao, W. He*, S. Bhasin, S. Guo. "Low-cost design of stealthy hardware trojan for bit-level fault attacks on block ciphers," *SCIENCE CHINA Information Sciences*, 2017, 60:048102 [PDF]

6. L. Geng, **F. Zhang***, J. Shen, X. Zhao, W. He, S. Bhasin, S. Guo. "Transistor level SCA-resistant scheme based on fluctuating power logic," *SCIENCE CHINA Information Sciences*, 2017, 60:109401 [PDF]

7. H. Gan, H. Zhang*, M. Khan, X. Wang, **F. Zhang**, P. He. "An improved empirical mode decomposition for power analysis attack," *China Communications*, Vol.14, No.9, pp.94-99, 2017. [PDF]

8. M. Khan, H. Zhang*, **F. Zhang**, S. Shahzad, R. Ullah, S. Ali, Q. Arain, M. Ahmed "X-Band Power Amplifier for Next Generation Networks based on MESFET," *China Communications*, Vol.14, No.4, pp.11-19, 2017 [PDF]

9. H. Chen, T. Wang, S. Guo, X. Zhao, **F. Zhang***, J. Liu, "Improved Differential Fault analysis of SOSEMANUK with Algebraic Techniques," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences.* Vol.E100-A, No.3, pp.811-821, 2017 [PDF]

10. **F. Zhang***, S. Guo, X. Zhao, T. Wang, J. Yang, F. -X. Standaert, and D. Gu. "A Framework for the Analysis and Evaluation of Algebraic Fault Attacks on Lightweight Block Ciphers," *IEEE Transactions on Information Forensics and Security*, Vol.11, No.5, pp.1039-1054, 2016 [PDF]

11. **F. Zhang**, X. Zhao, S. Guo, J. Shen*, J. Huang, and Z. Hu. "A Comprehensive Study of Algebraic Fault Analysis on PRINCE," *China Communications*, Vol.12, No.7, pp.127-141, 2015 [PDF]

12. P. Zhou, T. Wang, G. Li, **F. Zhang***, and X. Zhao. "Analysis on the Parameter Selection Method for FLUSH+RELOAD based Cache Timing Attack on RSA," *China Communications*, Vol.12, No.6, pp.33-45, 2015 [PDF]

13. S. Guo, X. Zhao, **F. Zhang***, T. Wang, Z. Shi, F. -X. Standaert, and C. Ma. "Exploiting the Incomplete Diffusion Feature: A Specialized Analytical Side-Channel Attack Against the AES and Its Application to Microcontroller Implementations," *IEEE Transactions on Information Forensics and Security*, Vol.9, No.6, pp.999-1014, 2014 [PDF]

14. X. Zhao, S. Guo, **F. Zhang***, T. Wang, Z. Shi, Z. Liu, and J. Gallais. "A comprehensive study of multiple deductions-based algebraic trace driven cache attacks on AES," *Elsevier Computers & Security*, Vol.39, Part.B, pp.173-189, 2013 [PDF]

15. X. Zhao, S. Guo, **F. Zhang***, T. Wang, Z. Shi, H. Liu, K, Ji, and J. Huang. "Efficient Hamming Weight based Side-Channel Cube Attacks on PRESENT," *Journal of Systems and Software*, Vol.86, No.3, pp.728-743, 2013 [PDF]

16. X. Zhao, S. Guo, **F. Zhang***, T. Wang, Z. Shi, and H. Luo, "Enhanced Side-Channel Cube Attacks on PRESENT," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences.* Vol.E96-A, No.1, pp.332-339, 2013 [PDF]

Conference Papers

1. **F. Zhang**, L. Geng, J. Shen, S. Bhasin, X. Zhao, S. Guo. "Improved low-entropy masking scheme for LED with mitigation against correlation-enhanced collision attacks," In *AsianHOST 2017*, accepted

2. X. Zhao, S. Guo, **F. Zhang**, T. Wang, Z. Shi, M. Chu, D. Gu. "Algebraic Fault Analysis on GOST for Key Recovery and Reverse Engineering," In *FDTC 2014*, pp.29-39, 2014. [PDF]

3. **F. Zhang**, X. Zhao, S. Guo, T. Wang, Z. Shi. "Improved Algebraic Fault Analysis: A Case Study on Piccolo and Applications to Other Lightweight Block Ciphers," In *COSADE 2013*, pp.62-79, 2013. [PDF]

4. X. Zhao, S. Guo, **F. Zhang**, T. Wang, Z. Shi, M. Chu, T. Wang. "Improving and Evaluating Differential Fault Analysis on LED with Algebraic Techniques," In *FDTC 2013*, pp.41-51, 2013. [PDF]

5. X. Zhao, **F. Zhang**, T. Wang, S. Guo, Z. Shi, H. Liu, K. Ji. "MDASCA: An Enhanced Algebraic Side-Channel Attack for Error Tolerance and New Leakage Model Exploitation," In *COSADE 2012*, pp.231-248, 2012. (Best Paper Award) [PDF]

6. **F. Zhang**, Z. Shi, "Differential and Correlation Power Analysis Attacks on HMAC-Whirlpool," In *ITNG 2011*, pp.359-365, 2011. [PDF]

7. S. Wang, **F. Zhang**, J. Dai, Z. Shi, L, Wang, "Making Register File Resistant to Power Analysis Attacks," In *ICCD 2008*, pp.577-582, 2008. [PDF]

8. **F. Zhang**, Z. Shi, "An Efficient Window-Based Countermeasure to Power Analysis of ECC Algorithms," In *ITNG 2008*, pp.120-126, 2008. [PDF]

9. **F. Zhang**, Z. Shi, B. Wang, "Chord-based Key Establishment Schemes for Sensor Networks," In *ITNG 2008*, pp.731-737, 2008. [PDF]

10. **F. Zhang**, Z. J. Shi, "Power Analysis Attacks on ECC Randomized Automata," In *ITNG 2007*, pp. 900-901, 2007. [PDF]

11. Z. Shi, **F. Zhang**, "New Attacks on Randomized ECC Algorithms," In *EITC 2006*, pp.22-25, 2006. [PDF]

Journal Papers: EI-Indexed

1. P. Zhou, T. Wang, X. Zhao, **F. Zhang***, "Flush-Reload Cache timing attack on SM2 digital signature algorithm," *Journal of Huazhong University of Science and Technology (Natural Science Edition)*, accepted.

2. Y. Ma, T. Wang, H. Chen, **F. Zhang***, X. Lou, L. Xu, W. Yang, "Fault Cube Attack on SIMON Family of Lightweight Block Ciphers," *Journal of Zhejiang University (Engineering Science)*, Vol.51, No.9, pp.1770-1779, 2017. In Chinese. [PDF]

3. H. Chen, T. Wang, **F. Zhang***, X. Zhao, "Fault-based guess-and-determine attack on SOSEMANUK," *Journal of Huazhong University of Science and Technology (Natural Science Edition)*, Vol.45, No.2, pp.72-77, 2017. In Chinese. [PDF]

4. J. Huang, X. Zhao*, **F. Zhang**, S. Guo, P. Zhou, J. Yang, "Improvement and Evaluation for Algebraic Fault Attacks on PRESENT," *Journal on Communications*, Vol.37, No.8, pp.144-156, 2016. In Chinese. [PDF]

5. H. Gan*, H. Zhang, J. Li, **F. Zhang**, X. Zhao, P. He, "Independent component analysis applied in electromagnetic attack," *Chinese Journal of Radio Science*, Vol.31, No.2, pp.401-405, 2016. In Chinese. [PDF]

6. H. Gan, H. Zhang, **F. Zhang***, X. Zhao, P. He, "Electromagnetic Information Leakage Acquisition and Pretreatment," *Chinese Journal of Radio Science*, Vol.30, No.5, pp.1004-1008, 2015. In Chinese. [PDF]

7. H. Zhang, J. Li, **F. Zhang***, H. Gan, P. He, "A Study on Template Attack of Chip Base on Side Channel Power Leakage," *Chinese Journal of Radio Science*, Vol.30, No.5, pp.987-992, 2015. In Chinese. [PDF]

8. H. Chen, T. Wang, **F. Zhang***, X. Zhao, Y. Sun, "Research on Algebraic Fault Analysis on HIGHT," *Journal of Shanghai Jiaotong University*, Vol.49, No.12, pp.1817-1825, 2015. In Chinese. [PDF]

9. X. Wang, S. Guo, X. Zhao, M. Song, **F. Zhang**, "Research of power preprocessing optimization-based template attack on LED," *Journal on Communications*, Vol.35, No.3, pp.157-167, 2014. In Chinese. [PDF]

10. X. Zhao, S. Guo, T. Wang, **F. Zhang**, H. Liu, J. Huang, P. Wang, "Research of Algebraic Fault Analysis on Piccolo," *Chinese Journal of Computers*, Vol.36, No.4, pp.882-894, 2013. In Chinese. [PDF]

11. H. Liu, X. Zhao, T. Wang, S. Guo, **F. Zhang**, J. Ke, "Research of Hamming Weight-Based Algebraic Side-Channel Attacks on SMS4," *Chinese Journal of Computers*, Vol.36, No.6, pp.1183-1193, 2013. In Chinese. [PDF]

12. X. Zhao, S. Guo, T. Wang*, **F. Zhang** Z. Shi, "Fault-Propagate Pattern based DFA on PRESENT and PRINTcipher," *Wuhan University Journal of Natural Sciences*, Vol.17, No.6, pp.485-493, 2012 [PDF]

13. T. Wang, X. Zhao*, S. Guo, **F. Zhang**, H. Liu, T. Zheng, "Research of Cache Timing Template Attacks on AES," *Chinese Journal of Computers*, Vol.2, No.1, pp.325-341, 2012. In Chinese. [PDF]

14. **F. Zhang**, S. Zhang, Y. Tang, W. Dai, "Design on Smart card-based Secure Logon System," *Information Security and Communications Privacy*, 2004(3):38-41. In Chinese.

Books and Chapters

1. Z. Shi, B. Wang, **F. Zhang**, "CBKE: Chord-based Key Establishment Schemes for Wireless Sensor Networks,", *Chapter in Handbook on Sensor Networks, (Xiao, Chen and Li, eds.)*, pp. 399-418, World Scientific Publishing Company, August 2010

Other Papers

1. Y. Wang, X. Zhao, **F. Zhang***, S. Guo, L. Wu, W. Li, X. Lou. "Security Evaluation for Fault Attacks on Lightweight Block Cipher Midori,", *Journal of Cryptologic Research*, Vol.4, No.1, pp.58-78, 2017. In Chinese. [PDF]

2. J. Wu, C. Kuang, K. Zeng, W. Qiao, **F. Zhang***, X. Zhang, Z. Xu. "RGB-D Camera based Human Limb Movement Recognition and Tracking in Supine Positions," In *PCM 2016*, pp.705-714, 2016. [PDF]

Thesis

1. **F. Zhang**, Ph.D Thesis, "Towards Comprehensive Countermeasures to Power Analysis Attacks," December 2011.

2. **F. Zhang**, Master Thesis, "Identity Authentication and Access Control Based On Smart Card," January 2004. In Chinese.