applied sciences

MDPI

Editorial

Special Issue on "Side Channel Attacks"

Seokhie Hong [1,2]

[1] School of Cyber Security, Korea University, Seoul 02841, Korea; shhong@korea.ac.kr
[2] Center for Information Security Technologies (CIST), Institute of Cyber Security and Privacy (ICSP), Korea University, Seoul 02841, Korea

Received: 25 April 2019; Accepted: 29 April 2019; Published: 8 May 2019

Cryptosystems are widely used in a growing number of embedded applications, such as smart cards, smart phones, Internet of Things (IoT) devices, and so on. Although these cryptosystems have been proven to be safe using mathematical tools, they are potentially susceptible to physical attacks which exploit additional sources of information, including timing information, power consumption, electromagnetic emissions (EM), and sound, amongst others. Introduced by Kocher, these types of attacks are referred to as side-channel attacks (SCAs) [1,2]. These attacks pose a very serious threat to embedded systems with cryptographic algorithms. There has been a great deal of effort put into finding various SCAs and developing secure counter-measures, recently [3–16].

This special issue has been organized to provide a possibility for researchers in the area of SCAs to highlight the most recent and exciting technologies. The research papers selected for this special issue represent recent progress in the field, including power analysis attacks [17–19], cache-based timing attacks [20–41], system-level counter-measures [42–48], and so on [49–60]. The thirteen papers in this special issue can be classified into the following four research themes:

Power analysis attacks and counter-measures: This special issue contains various power analysis attacks and counter-measures on well-known crypto algorithms: Elliptic curve cryptosystems (ECCs), the block cipher SEED, and the post-quantum cryptographies (PQCs). A new side channel leakage of the SEED in financial IC cards in the Republic of Korea was detected in [61]; and new vulnerabilities, using a single power consumption trace obtained in the elliptic curve scalar multiplication algorithm, were established in [62,63]. Recently, PQCs, cryptographic algorithms executed on a classical computer which are expected to be secure against adversaries with quantum computers, have been actively studied. This special issue contains two papers about power analysis attacks on PQCs: The well-known NTRU algorithm, and a cumulative distribution table (CDT) sampler used in the lattice-based PQCs [64,65].

Cache-based timing attacks: This special issue contains two research papers with regard to cache-based timing attacks, utilizing the timing difference between cache hits and cache misses. One paper proposes a new constant-time method for RSA modular exponentiation, which is resistant against fine-grained cache attacks [66]. The other one shows a non-access attack, a novel approach for exploiting the information gained from cache misses [67].

System-level counter-measures and their weaknesses: Two research papers in this special issue introduce a new system-level counter-measure and a new vulnerability of the existing physically un-clonable function (PUF), respectively. One paper deals with the re-keying scheme, a system-level counter-measure against SCAs, which makes attackers unable to collect enough power consumption traces for their analyses [68]. The authors of this paper define a new security model and propose two provably secure re-keying schemes. The other paper shows that a PUF key can be derived from a chaotic circuit [69].

Recent technologies in the field of Side Channel Attacks: This special issue also contains papers documenting recent technologies in the field of SCAs: A machine-learning based side-channel evaluation technique [70], a Merkle tree-based on-line data authentication technique with leakage resilience [71], an ID-based side-channel authentication technique [72], and a technique to distinguish ad-related network behavior [73].

In summary, this special issue contains many excellent studies, covering a wide range of SCA-related topics. This collection of 13 papers is highly recommended, and is believed to benefit readers in various aspects.

Funding: This work was supported by the Institute for Information and Communications Technology Promotion (IITP) grant, funded by the Korean government (MSIT) (No. 2017-0-00520, Development of SCR-Friendly Symmetric Key Cryptosystem and Its Application Modes).

Conflicts of Interest: The author declares no conflict of interest.

References

1. Kocher, P.C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Proceedings of the Annual International Cryptology Conference (CRYPTO), Santa Barbara, CA, USA, 18–22 August 1996; pp. 104–113.
2. Kocher, P.; Jaffe, J.; Jun, B. Differential power analysis. In Proceedings of the Annual International Cryptology Conference (CRYPTO), Santa Barbara, CA, USA, 15–19 August 1999; pp. 388–397.
3. Gandolfi, K.; Mourtel, C.; Olivier, F. Electromagnetic analysis: Concrete results. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Paris, France, 14–16 May 2001; Springer: Berlin/Heidelberg, Germany, 2001; pp. 251–261.
4. Brier, E.; Clavier, C.; Olivier, F. Correlation power analysis with a leakage model. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Cambridge, MA, USA, 11–13 August 2004; Springer: Berlin/Heidelberg, Germany, 2004; pp. 16–29.
5. Gierlichs, B.; Batina, L.; Tuyls, P.; Preneel, B. Mutual information analysis. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Washington, DC, USA, 10–13 August 2008; Springer: Berlin/Heidelberg, Germany, 2008; pp. 426–442.
6. Chari, S.; Rao, J.R.; Rohatgi, P. Template attacks. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Redwood Shores, CA, USA, 13–15 August 2002; Springer: Berlin/Heidelberg, Germany, 2002; pp. 13–28.
7. Schindler, W.; Lemke, K.; Paar, C. A stochastic model for differential side channel cryptanalysis. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Edinburgh, UK, 29 August–1 September 2005; Springer: Berlin/Heidelberg, Germany, 2005; pp. 30–46.
8. Mangard, S.; Oswald, E.; Popp, T. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2008; Volume 31.
9. Prouff, E.; Rivain, M.; Bevan, R. Statistical analysis of second order differential power analysis. *IEEE Trans. Comput.* **2009**, *58*, 799–811. [CrossRef]
10. Kim, H.S.; Hong, S. New type of collision attack on first-order masked AESs. *ETRI J.* **2016**, *38*, 387–396. [CrossRef]
11. Coron, J.S.; Goubin, L. On boolean and arithmetic masking against differential power analysis. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Worcester, MA, USA, 17–18 August 2000; Springer: Berlin/Heidelberg, Germany, 2000; pp. 231–237.
12. Goubin, L. A sound method for switching between boolean and arithmetic masking. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Paris, France, 14–16 May 2001; Springer: Berlin/Heidelberg, Germany, 2001; pp. 3–15.
13. Coron, J.S.; Tchulkine, A. A new algorithm for switching from arithmetic to boolean masking. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Cologne, Germany, 8–10 September 2003; Springer: Berlin/Heidelberg, Germany, 2003; pp. 89–97.
14. Tunstall, M.; Whitnall, C.; Oswald, E. Masking tables-an underestimated security risk. In Proceedings of the International Workshop on Fast Software Encryption, Washington, DC, USA, 11–13 March 2013; Springer: Berlin/Heidelberg, Germany, 2003; pp. 425–444.
15. Balasch, J.; Faust, S.; Gierlichs, B. Inner product masking revisited. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, 26–30 April 2015; pp. 486–510.

16. Bettale, L.; Coron, J.S.; Zeitoun, R. Improved high-order conversion from boolean to arithmetic masking. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2018**, *2018*, 22–45.
17. Espitau, T.; Fouque, P.A.; Gérard, B.; Tibouchi, M. Side-Channel Attacks on BLISS Lattice-Based Signatures: Exploiting Branch Tracing Against strongSwan and Electromagnetic Emanations in Microcontrollers. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; ACM: New York, NY, USA, 2017; pp. 1857–1874.
18. Park, A.; Shim, K.A.; Koo, N.; Han, D.G. Side-Channel Attacks on Post-Quantum Signature Schemes based on Multivariate Quadratic Equations. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2018**, *2018*, 500–523.
19. Saarinen, M.J.O. Arithmetic Coding and Blinding Countermeasures for Lattice Signatures. 2016. Available online: https://eprint.iacr.org/2016/276 (accessed on 7 May 2019).
20. Yarom, Y.; Falkner, K. FLUSH+RELOAD: A High Resolution, Low Noise, L3 Cache Side-Channel Attack. In Proceedings of the 23rd USENIX Security Symposium (USENIX Security 14), San Diego, CA, USA, 20–22 August 2014; pp. 719–732.
21. Liu, F.; Yarom, Y.; Ge, Q.; Heiser, G.; Lee, R.B. Last-Level Cache Side-Channel Attacks are Practical. In Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 18–20 May 2015; pp. 605–622.
22. Lipp, M.; Schwarz, M.; Gruss, D.; Prescher, T.; Haas, W.; Fogh, A.; Horn, J.; Mangard, S.; Kocher, P.; Genkin, D.; et al. Meltdown: Reading kernel memory from user space. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, USA, 15–17 August 2018; pp. 973–990.
23. Kocher, P.; Genkin, D.; Gruss, D.; Haas, W.; Hamburg, M.; Lipp, M.; Mangard, S.; Prescher, T.; Schwarz, M.; Yarom, Y. Spectre attacks: Exploiting speculative execution. *arXiv* **2018**, arXiv:1801.01203.
24. Irazoqui, G.; Eisenbarth, T.; Sunar, B. Cross Processor Cache Attacks. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, Xi'an, China, 30 May–3 June 2016; pp. 353–364.
25. Xu, Y.; Cui, W.; Peinado, M. Controlled-channel attacks: Deterministic side channels for untrusted operating systems. In Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 18–20 May 2015; pp. 640–656.
26. Zhang, Y.; Juels, A.; Reiter, M.K.; Ristenpart, T. Cross-tenant side-channel attacks in PaaS clouds. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 990–1003.
27. Gruss, D.; Maurice, C.; Wagner, K.; Mangard, S. Flush+ Flush: A fast and stealthy cache attack. In Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, San Sebastián, Spain, 7–8 July 2016; Volume 9721, pp. 279–299.
28. Gruss, D.; Spreitzer, R.; Mangard, S. Cache template attacks: Automating attacks on inclusive last-level caches. In Proceedings of the 24th USENIX Security Symposium (USENIX Security 15), Washington, DC, USA, 12–14 August 2015; pp. 897–912.
29. Yarom, Y.; Genkin, D.; Heninger, N. CacheBleed: A timing attack on OpenSSL constant-time RSA. *J. Cryptogr. Eng.* **2017**, *7*, 99–112. [CrossRef]
30. Doychev, G.; Köpf, B.; Mauborgne, L.; Reineke, J. Cacheaudit: A tool for the static analysis of cache side channels. *ACM Trans. Inf. Syst. Secur.* **2015**, *18*, 4:1–4:32. [CrossRef]
31. Yarom, Y.; Benger, N. Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack. *IACR Cryptol. ePrint Archi.* **2014**, *2014*, 140.
32. Lipp, M.; Gruss, D.; Spreitzer, R.; Maurice, C.; Mangard, S. ARMageddon: Cache attacks on mobile devices. In Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, USA, 10–12 August 2016; pp. 549–564.
33. Aldaya, A.C.; García, C.P.; Tapia, L.M.A.; Brumley, B.B. Cache-Timing Attacks on RSA Key Generation. *IACR Cryptol. ePrint Arch.* **2018**, *2018*, 367.
34. Deng, S.; Xiong, W.; Szefer, J. Analysis of Secure Caches and Timing-Based Side-Channel Attacks. *IACR Cryptol. ePrint Arch.* **2019**, *2019*, 167.
35. Irazoqui, G.; Guo, X. Cache Side Channel Attack: Exploitability and Countermeasures. *Black Hat Asia* **2017**, *2017*, 3.
36. Zhou, Z.; Reiter, M.K.; Zhang, Y. A software approach to defeating side channels in last-level caches. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 871–882.

37. Zhang, Y. Cache Side Channels: State of the Art and Research Opportunities. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 2617–2619.
38. Gruss, D.; Lettner, J.; Schuster, F.; Ohrimenko, O.; Haller, I.; Costa, M. Strong and efficient cache side-channel protection using hardware transactional memory. In Proceedings of the 26th USENIX Security Symposium (USENIX Security 17), Vancouver, BC, Canada, 16–18 August 2017; pp. 217–233.
39. Wang, S.; Wang, P.; Liu, X.; Zhang, D.; Wu, D. CacheD: Identifying cache-based timing channels in production software. In Proceedings of the 26th USENIX Security Symposium (USENIX Security 17), Vancouver, BC, Canada, 16–18 August 2017; pp. 235–252.
40. Dong, X.; Shen, Z.; Criswell, J.; Cox, A.L.; Dwarkadas, S. Shielding Software From Privileged Side-Channel Attacks. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, USA, 15–17 August 2018; pp. 1441–1458.
41. Gras, B.; Razavi, K.; Bos, H.; Giuffrida, C. Translation Leak-aside Buffer: Defeating Cache Side-channel Protections with TLB Attacks. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, USA, 15–17 August 2018; pp. 955–972.
42. Medwed, M.; Standaert, F.X.; Großschädl, J.; Regazzoni, F. Fresh Re-Keying: Security against Side-Channel and Fault Attacks for Low-Cost Devices. In *Progress in Cryptology—AFRICACRYPT 2010, Proceedings of the Third International Conference on Cryptology in Africa, Stellenbosch, South Africa, 3–6 May 2010*; Bernstein, D., Lange, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6055, pp. 279–296.
43. Medwed, M.; Petit, C.; Regazzoni, F.; Renauld, M.; Standaert, F.X. Fresh Re-keying II: Securing Multiple Parties Against Side-channel and Fault Attacks. In Proceedings of the 10th IFIP WG 8.8/11.2 International Conference on Smart Card Research and Advanced Applications, Stellenbosch, South Africa, 3–6 May 2011; Springer: Berlin/Heidelberg, Germany, 2011; pp. 115–132.
44. Rührmair, U.; Sölter, J.; Sehnke, F. On the Foundations of Physical Unclonable Functions. *IACR Cryptol. ePrint Arch.* **2009**, *2009*, 277.
45. Merli, D.; Schuster, D.; Stumpf, F.; Sigl, G. Side-channel analysis of PUFs and fuzzy extractors. In Proceedings of the International Conference on Trust and Trustworthy Computing, Pittsburgh, PA, USA, 22–24 June 2011; Volume 6740, pp. 33–47.
46. Tuyls, P.; Škorić, B.; Stallinga, S.; Akkermans, A.H.; Ophey, W. Information-theoretic security analysis of physical uncloneable functions. In Proceedings of the International Conference on Financial Cryptography and Data Security, Roseau, MN, USA, 28 February–3 March 2005; Volume 3570, pp. 141–155.
47. Rührmair, U.; Sehnke, F.; Sölter, J.; Dror, G.; Devadas, S.; Schmidhuber, J. Modeling attacks on physical unclonable functions. In Proceedings of the 17th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 4–8 October 2010; pp. 237–249.
48. Škorić, B.; Tuyls, P.; Ophey, W. Robust key extraction from physical uncloneable functions. In Proceedings of the International Conference on Applied Cryptography and Network Security, New York, NY, USA, 7–10 June 2005; Volume 3531, pp. 407–422.
49. Lerman, L.; Bontempi, G.; Markowitch, O. Side channel attack: An approach based on machine learning. In Proceedings of the International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE), Darmstadt, Germany, 14 February 2011; pp. 29–41.
50. Hospodar, G.; Gierlichs, B.; De Mulder, E.; Verbauwhede, I.; Vewalle, J. Machine learning in side-channel analysis: A first study. *J. Cryptogr. Eng.* **2011**, *1*, 293–302. [CrossRef]
51. Bartkewitz, T.; Lemke-Rust, K. Efficient template attacks based on probabilistic multi-class support vector machines. In Proceedings of the International Conference on Smart Card Research and Advanced Applications (CARDIS), Graz, Austria, 28–30 November 2012; pp. 263–276.
52. Heuser, A.; Zohner, M. Intelligent machine homicide. In Proceedings of the International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE), Darmstadt, Germany, 3–4 May 2012; pp. 249–264.
53. Heyszl, J.; Ibing, A.; Mangard, S.; De Santis, F.; Sigl, G. Clustering Algorithms for Non-profiled Single-Execution Attacs on Exponentiations. In Proceedings of the International Conference on Smart Card Research and Advanced Applications (CARDIS), Paris, France, 5–7 November 2013; pp. 79–93.

54. Lerman, L.; Bontempi, G.; Markowitch, O. A machine learning approach against a masked AES. In Proceedings of the International Conference on Smart Card Research and Advanced Applications (CARDIS), Paris, France, 5–7 November 2013; pp. 61–75.
55. Specht, R.; Heyszl, J.; Kleinsteuber, M.; Sigl, G. Improving non-profiled attacks on exponentiations based on clustering and extracting leakage from multi-channel high-resolution EM measurements. In Proceedings of the International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE), Berlin, Germany, 13–14 April 2015; pp. 3–19.
56. Whitnall, C.; Oswald, E. Profiling DPA: Efficacy and efficiency trade-offs. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES), Santa Barbara, CA, USA, 20–23 August 2013; pp. 37–54.
57. Maghrebi, H.; Portigliatti, T.; Prouff, E. Breaking cryptographic implementations using deep learning techniques. In Proceedings of the International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE), Hyderabad, India, 14–18 December 2016; pp. 3–26.
58. Cagli, E.; Dumas, C.; Prouff, E. Convolutional neural networks with data augmentation against jitter-based countermeasures. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES), Taipei, Taiwan, 25–18 September 2017; pp. 45–68.
59. Picek, S.; Samiotis, I.P.; Kim, J.; Heuser, A.; Bhasin, S.; Legay, A. On the performance of convolutional neural networks for side-channel analysis. In Proceedings of the International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE), Goa, India, 13–17 December 2018; pp. 157–176.
60. Carbone, M.; Conin, V.; Cornélie, M.A.; Dassance, F.; Dufresne, G.; Dumas, C.; Prouff, E.; Venelli, A. Deep Learning to Evaluate Secure RSA Implementations. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2019**, *2*, 132–161.
61. Won, Y.S.; Lee, J.; Han, D.G. Side Channel Leakages Against Financial IC Card of the Republic of Korea. *Appl. Sci.* **2018**, *8*, 2258. [CrossRef]
62. Sim, B.Y.; Kang, J.; Han, D.G. Key Bit-Dependent Side-Channel Attacks on Protected Binary Scalar Multiplication. *Appl. Sci.* **2018**, *8*, 2168. [CrossRef]
63. Cho, S.M.; Jin, S.; Kim, H. Side-Channel Vulnerabilities of Unified Point Addition on Binary Huff Curve and Its Countermeasure. *Appl. Sci.* **2018**, *8*, 2002. [CrossRef]
64. Kim, S.; Hong, S. Single Trace Analysis on Constant Time CDT Sampler and Its Countermeasure. *Appl. Sci.* **2018**, *8*, 1809. [CrossRef]
65. An, S.; Kim, S.; Jin, S.; Kim, H.; Kim, H. Single Trace Side Channel Analysis on NTRU Implementation. *Appl. Sci.* **2018**, *8*, 2014. [CrossRef]
66. Shin, Y. Fast and Secure Implementation of Modular Exponentiation for Mitigating Fine-Grained Cache Attacks. *Appl. Sci.* **2018**, *8*, 1304. [CrossRef]
67. Briongos, S.; Malagón, P.; de Goyeneche, J.M.; Moya, J.M. Cache Misses and the Recovery of the Full AES 256 Key. *Appl. Sci.* **2019**, *9*, 944. [CrossRef]
68. Komano, Y.; Hirose, S. Re-Keying Scheme Revisited: Security Model and Instantiations. *Appl. Sci.* **2019**, *9*, 1002. [CrossRef]
69. Gołofit, K.; Wieczorek, P.Z. Chaos-Based Physical Unclonable Functions. *Appl. Sci.* **2019**, *9*, 991. [CrossRef]
70. Mukhtar, N.; Mehrabi, M.A.; Kong, Y.; Anjum, A. Machine-Learning-Based Side-Channel Evaluation of Elliptic-Curve Cryptographic FPGA Processor. *Appl. Sci.* **2019**, *9*, 64. [CrossRef]
71. Koo, D.; Shin, Y.; Yun, J.; Hur, J. Improving Security and Reliability in Merkle Tree-Based Online Data Authentication with Leakage Resilience. *Appl. Sci.* **2018**, *8*, 2532. [CrossRef]
72. Li, Y.; Kasuya, M.; Sakiyama, K. Comprehensive Evaluation on an ID-Based Side-Channel Authentication with FPGA-Based AES. *Appl. Sci.* **2018**, *8*, 1898. [CrossRef]
73. Su, M.Y.; Wei, H.S.; Chen, X.Y.; Lin, P.W.; Qiu, D.Y. Using Ad-Related Network Behavior to Distinguish Ad Libraries. *Appl. Sci.* **2018**, *8*, 1852. [CrossRef]