Guest Editorial
Special Issue on the Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2022)

ASIAN Hardware Oriented Security and Trust Symposium (AsianHOST) is an annual symposium that aims to facilitate the rapid growth of hardware-based security research and development. Hardware security is a fashionable research area in both industry and academia. Its scope is consistently growing to embrace secure design, manufacturing, and deployment of modern and emerging interoperable computing, communication, storage devices, and circuits and systems. The 7th Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2022) was held in hybrid mode on December 14–16 in Singapore. Among all the accepted contributions presented at the conference, a subset of top-rated articles was selected and invited for this Special Issue. The invited articles included extended new technical contributions and results and went through a peer-review process consisting of expert reviewers in the related topics. A brief description of the selected articles is as follows.

In [A1], Xu et al. present an attack that overcomes the stiff restriction and strong conflict in simultaneous optimization of attack stealth, success rate, and utility of the poisoned model by using amalgamated data augmentation as the backdoor trigger. The attack is comprehensively evaluated on four different network models and four image classification datasets. It outperforms state-of-the-art clean-label backdoor attacks with lower injection rate, stealthier poisoned samples, higher attack success rate, and greater backdoor mitigation resistance without compromising benign accuracy. The embedded backdoor is not affected by weight pruning and quantization as demonstrated by the equally high attack success rates on the Intel Neural Compute Stick 2 edge AI device implementation of the same poisoned models.

In [A2], Zhao et al. evaluate the side-channel security of the parallel and pipelined hardware implementations of Kyber, which is a NIST-selected key encapsulation mechanism (KEM) for post-quantum cryptography (PQC). They make a comprehensive analysis of their decryption procedure including two vulnerable regions and multiple points of interest. Correspondingly, different types of SCA attacks are exploited to recover the secret keys of Kyber. The experimental results show that Kyber designs on FPGA boards are vulnerable to SCA attacks including electromagnetic (EM) and power side channels—an attacker only needs 27–1600 power traces or 60–2680 EM traces to recover the decryption key successfully.

In [A3], Woralert et al. employ a semi-supervised machine-learning method to detect ransomware using low-level hardware information. To increase the detection accuracy and reduce the number of false positives, a long-short term memory network is used with a weighted majority voting ensemble and exponential moving average to learn the temporal hardware-level information for detecting the deviation in system behavior. In addition, a separate classifier machine is used to enforce strict protection and offload the heavy-weight classification work to avoid affecting the performance of the user machine that is under monitoring.

In [A4], Qiu et al. propose a new side-channel attack called the PMU-Spill that exploits the hardware vulnerability found on the performance monitor unit (PMU) of mainstream processors that record executed but not successfully retired events. The study carried out on five Intel processors reveals 162 vulnerable PMU counters out of 383 PMU counters, and 112 vulnerable PMU counters can be exploited by PMU-Spill attack to leak the secret data protected by Intel Software Guard Extensions (SGX). The PMU-Spill attack has a throughput of up to 291.2 bytes/s with an average error rate of only 2.45%. The limitations and possible extensions of this attack are analyzed, and some possible solutions are suggested toward the end of the paper.

In [A5], Chen et al. aim to design a TRNG satisfying both on-chip entropy assurance and high output bitrate simultaneously. An improved stochastic model and a measurement method are established to quantify the entropy of coherent sampling-based TRNG. Moreover, an on-chip entropy assurance module is provided to realize the robustness of the proposed design under various operating conditions. The experimental results indicate that the generated data has sufficient entropy ($\geq$0.999 per bit) under various operating conditions. In addition, all the outputs passed the NIST SP800-22 and AIS 31 statistical tests. The output bitrate is 4.2 Mb/s, which is two orders of magnitude faster than the elementary oscillator-based TRNG.

In [A6], Ni et al. observe a phenomenon of periodic loss of short pulses in nonlinear oscillators. By modeling the time of the Fibonacci Ring Oscillator (FIRO), they found that this phenomenon suppresses the accumulation of clock jitter, which limits the randomness when incorporating a simple feedback structure into the ring oscillator. To overcome this limitation, they propose a multi-ring convergence oscillator, which uses independent sub-rings to accumulate jitter so that the main ring can generate short pulses rapidly to provide

Digital Object Identifier 10.1109/TCSI.2023.3331939

analog randomness. Their design can achieve a throughput rate of up to 500 Mb/s on Xilinx Virtex-6 FPGA implementation with only four flip-flops and a minimum of 13 LUTs. The generated random sequence passed both NIST SP800-22 and SP800-90B tests.

The Guest Editors would like to thank the authors for their contribution to this Special Issue, without whom we could not meet the high standard expected of this Special Issue. The Organizing Committee of AsianHOST 2022 and anonymous reviewers deserve special recognition for their generous voluntary service, comments, and valuable suggestions to improve the quality of the papers finally published in this Special Issue. We would also like to thank the Editor-in-Chief, Prof. Weisheng Zhao, the Deputy Editor-in-Chief, Prof. Helen Hai Li, and the Editorial Assistant of IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS for their continuous support and guidance throughout the process. To the readers, we hope you will enjoy these articles and find them useful for your future research.

CHIP HONG CHANG, *Guest Editor*
School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore 639798
echchang@ntu.edu.sg

PINGQIANG ZHOU, *Guest Editor*
School of Information Science and Technology
ShanghaiTech University
Shanghai 201210, China
zhoupq@shanghaitech.edu.cn

YUAN CAO, *Guest Editor*
College of IoT
Hohai University
Changzhou 213022, China
caoyuan0908@gmail.com

QIANG LIU, *Guest Editor*
School of Microelectronics
Tianjin University
Tianjin 300072, China
qiangliu@tju.edu.cn

APPENDIX: RELATED ARTICLES

[A1] C. Xu, W. Liu, Y. Zheng, S. Wang, and C.-H. Chang, "An imperceptible data augmentation based blackbox clean-label backdoor attack on deep neural networks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 70, no. 12, pp. 5011–5024, Dec. 2023.

[A2] Y. Zhao et al., "Side channel security oriented evaluation and protection on hardware implementations of kyber," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 70, no. 12, pp. 5025–5035, Dec. 2023.

[A3] C. Woralert, C. Liu, and Z. Blasingame, "HARD-Lite: A lightweight hardware anomaly realtime detection framework targeting ransomware," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 70, no. 12, pp. 5036–5047, Dec. 2023.

[A4] P. Qiu et al., "PMU-Spill: A new side channel for transient execution attacks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 70, no. 12, pp. 5048–5059, Dec. 2023.

[A5] T. Chen et al., "A design of high-efficiency coherent sampling based TRNG with on-chip entropy assurance," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 70, no. 12, pp. 5060–5073, Dec. 2023.

[A6] T. Ni et al., "Design of true random number generator based on multi-ring convergence oscillator using short pulse enhanced randomness," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 70, no. 12, pp. 5074–5085, Dec. 2023.