Hardware Security in Emerging Technologies: Vulnerabilities, Attacks, and Solutions

THIS Special Issue of the IEEE JOURNAL ON EMERGING AND SELECTED TOPICS IN CIRCUITS AND SYSTEMS (JETCAS) is dedicated to demonstrating the latest research progress in the area of hardware security in emerging technologies.

High complexity and cost associated with the design and manufacturing of integrated circuits (ICs) have led to the outsourcing of design and fabrication to different parties across the globe. Such globalization of IC development flow has introduced new security threats that can jeopardize the trustworthiness of ICs and impose a significant financial burden to the public and private sectors as well as to the end-users. In order to address emerging threats and advance the field of hardware security, this article covers the recent hardware attacks, countermeasures, and solutions in the following five areas:

1) Security of machine learning (ML) hardware and ML for hardware security
2) Security of physical unclonable functions (PUFs) as hardware root of trust
3) Side-channel attacks and countermeasures
4) Low-complexity and energy-efficient implementations of encryption schemes
5) Security-aware hardware design and verification methodologies

I. SECURITY OF ML HARDWARE AND ML FOR HARDWARE SECURITY

Adversarial attack is one of the most potent attack vectors in ML systems. Since several research thrusts are now utilized to implement ML at the edge, through ML accelerators, suitable compilers, and commercially available toolkits, it is imperative to observe the impact of adversarial attacks on such edge ML platforms, as well as devise a possible defense against those attacks. Existing system-based methodologies rely mainly on offline analysis to detect adversarial inputs, assuming that the deep learning model is implemented on a 32-bit floating-point graphical processing unit (GPU) instance. In the article titled "A new lightweight in-situ adversarial sample detector for edge deep neural network," the authors propose a new hardware-oriented approach for *in-situ* detection of adversarial inputs feeding through a spatial DNN accelerator architecture or a third-party DNN intellectual property (IP) implemented on the edge. This approach exploits controlled glitch injection into the clock signal of the DNN accelerator to maximize the information gain for the discrimination of adversarial and benign inputs. Experiments on large realistic ML models show that the proposed technique can improve the accuracy while reducing the false positive rate. Therefore, the approach proposed in this article is fundamental to make secure edge ML devices.

It is extremely expensive to train large DNN models, in terms of memory, time, and resources. In fact, most popular DNN models like Alexnet, VGG, and so on are available pretrained to be used by researchers. Therefore, protecting these models, which are valuable storehouses of intellectual properties (IPs), against model stealing/cloning attacks is of paramount importance. DNN accelerators, such as neural processing units (NPUs), are vulnerable to side-channel attacks and bus monitoring attacks. In the article titled "Preventing DNN model IP theft via hardware obfuscation," the authors developed a novel method to prevent model stealing attacks by obfuscating the NPU hardware utilizing a lightweight, keyed model obfuscation scheme. Incorrect keys lead to non-deterministic classification; thus, reducing the classification performance of the NPU. Furthermore, the authors present an ideal end-to-end deep learning trusted system composed of 1) model distribution via hardware root-of-trust and public-key cryptography infrastructure and 2) model execution via low latency memory encryption. The proposed obfuscation scheme is seen to achieve IP protection objectives without requiring specialized training or sacrificing the model's accuracy. Thus, this article provides a vital insight into protecting software DNN models using carefully obfuscated hardware.

ML has been broadly used in the distributed computing architectures in recent years. Accordingly, developing secure ML hardware accelerators has received more attention among high technology industry sectors. On the other hand, ML schemes have been widely deployed to protect ICs against recycling, counterfeiting, Trojan insertion, and data leakage. Therefore, ML for hardware security and security of ML architectures are among the main topics this Special Issue focuses on. In the article titled "Sniffer: A machine learning approach for DoS attack localization in NoC-based SoCs," the authors benefit from ML to locate malicious nodes that launch flooding-based denial of service attacks in network-on-chip structures. The proposed framework, so-called Sniffer, uses ML along with a collective decision-making strategy to accurately categorize the congestion status of a router port to attack and nonattack scenarios. In this article, the ML model is trained by the data related to the time interval a flit waits in the buffer on a network router, the number of flits received in each router port in a specific time duration, and the amount of

Digital Object Identifier 10.1109/JETCAS.2021.3084498

2156-3357 © 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

virtual channel space occupied by the incoming flits at each router node. The trained model demonstrates high accuracy in detecting malicious nodes in a timely manner with the least traffic disruption.

During COVID-19, many companies have encouraged employees to work from home. The distributed workforce drives a sharp increase in the amount of data being shared. At the same time, cybersecurity companies have reported massive increases in cyberattack attempts since the pandemic has begun. The capability to support security breach investigation and forensic analysis retroactively becomes invaluable. In the article titled "TPE: A hardware-based TLB profiling expert for workload reconstruction," the authors propose a hardware-based workload instrumentation framework that attempts to characterize process behavior through profiling sequence of user-space instructions that causes instruction translation lookaside buffer (TLB) misses. Unlike other software-based approaches where instrumentations are performed at the OS or hypervisor level, hence vulnerable to software tampering, TPE performs logging and feature extraction inside the hardware. The resulting data are uploaded over a dedicated port inaccessible to software to an offline module for forensic analysis. ML techniques are then employed to perform process identification and outlier detection. A prototype was evaluated with x86 and RISC-V simulators to demonstrate that the proposed solution is architecture-agnostic.

II. Security of PUF as Hardware Root of Trust

The use of strong PUFs in security applications is leveraged on the assumption of their large space of unpredictable challenge–response pairs (CRPs). Unfortunately, the unpredictability can be defeated by ML-based modeling attacks. Countermeasures based on complicated design to increase the modeling complexity may not be efficient, as they require more hardware but still can be defeated by advanced ML algorithms with more computing power. If lightweight ML-resistant PUFs are hard to achieve, an alternative approach to throw off a ML-equipped adversary in reverse-engineering the CRPs is to attack the ML directly. One common way to attack ML algorithms is by poisoning their training data. In the article "Modeling attack resistant PUFs based on adversarial attack against machine learning," the authors propose a new mechanism to poison the CRP data of the attacker's ML algorithms by inverting the PUF response in a manner that is deterministic to the authentic parties. Response inversion is performed postgeneration and pretransmission based on certain triggering conditions. Multiple triggering mechanisms with varying triggering probabilities are explored under various threat models. The authors showcase their work on the easily broken Arbiter PUF by attacking it using logistic regression and evolutionary strategies to show that their modifications can significantly increase the modeling resistance. The hardware overhead of the protection is minimal. Moreover, the method can be used with other hardware-strengthening schemes for PUFs, and leakage of the internal protection mechanism cannot be exploited to crack other PUFs with the same protection mechanism.

In the article titled "Introducing recurrence in strong PUFs for enhanced machine learning attack resistance," the authors develop a recurrence-based PUF (Rec-PUF), which uses feedback and XOR function together to significantly improve ML-attack resistance, without significant reduction in reliability. Although PUFs are being introduced in various IoT devices for improving security, traditional strong PUFs like Arbiter-PUF are susceptible to ML attacks. The proposed method is generic and works for both analog and digital PUF cores. To validate their proposed solution, the authors used recurrence on an analog PUF using a current mirror array validated on ASIC libraries, referred to as Rec-CMAPUF. The authors also design and evaluate a digital PUF fortified with recurrence, called Rec-DAPUF, based on double arbiter logic and prototyped on FPGAs. The experimental results show that ML resistance of Rec-CMAPUF is within 62% with 138 000 CRPs, with a reliability of 95%. Similarly, ML resistance of Rec-DAPUF is around 64%, with an average reliability of 95.9%. The proposed method has the potential of designing more robust PUFs and thus, improve IoT security.

With the advance of quantum computing, existing encryption algorithms like RSA will become obsolete. In order to improve the security of quantum computers, the article titled "Quantum PUF for security and trust in quantum computing" proposes a Quantum PUF. Existing quantum computing platforms are typically cloud-based (e.g., IBM, Rigetti, and D-Wave), which can lead to several threat models: 1) less trustworthy entities can provide poor quality quantum hardware or services; 2) poor quality scheduling algorithm can result in vulnerabilities in the service; and 3) rogue employee in a trusted organization can sabotage the output or steal sensitive information. The authors of this article propose two flavors of quantum PUFs (QuPUF) to address this issue. Their experiments on real IBM quantum hardware show that the proposed QuPUF can achieve inter-die hamming distance (HD) of 55% and intra-HD as low as 4%. This work has the possibility of improving the IoT security in the quantum era.

III. Side-Channel Attacks and Countermeasures

Side-channel attacks are potential attack vectors on both encryption and ML algorithms for extracting sensitive parameters. Both power and electromagnetic (EM) radiation emanating from hardware implementing the particular algorithm can be leveraged to release secret keys or model parameters. In order to protect against side-channel attacks, several countermeasures, either at the algorithm level or at the hardware level, have been proposed over the years.

In the article titled "Dual-hiding side-channel-attack resistant FPGA-based asynchronous-logic AES: Design, countermeasures and evaluation," the authors developed a countermeasure against side-channel attacks on AES encryption algorithm, implemented on a FPGA. The proposed approach is dual-hiding, i.e., amplitude moderation (vertical dimension) and time moderation (horizontal dimension). The authors propose an asynchronous logic-driven design with relative timing to simplify the AES hardware implementation. Next, the authors optimize the completion detection circuits

to reduce the power overhead. Furthermore, the authors propose a randomized delay line control and a data-propagation control to amplify the proposed countermeasure. The proposed approach is evaluated on Sakura-X and Arty-A7 FPGA boards. The authors have shown that compared to a synchronous logic-based design, which is breakable within 30 K EM traces, the proposed defense is unbreakable at 1 million EM traces. This defense, if adopted by the industry, will immensely help protect encryption hardware from EM side channels.

In the article titled "Power side-channel attacks on BNN accelerators in remote FPGAs," the authors have shown how remote power side channels can be utilized to attack binary neural network (BNN) accelerators, implemented on a FPGA. To reduce cost and increase the utilization of Cloud FPGAs, multitenant FPGAs are being explored, where multiple independent users simultaneously share the same remote FPGA. Despite its benefits, multitenancy opens up the possibility of malicious users colocating on the same FPGA as a victim user, and extracting sensitive information. A ML algorithm is being implemented on such a platform is susceptible to losing secrets, like model parameters through side-channel attacks. This article demonstrates a power-based side-channel attack on a binarized convolutional network accelerator, performing MNIST digit recognition and running in a variety of Xilinx FPGAs and also on Cloud FPGAs using amazon web services (AWS) F1 instances. The authors present how to remotely obtain voltage estimates as a deep neural network inference circuit executes, and how the information can be used to recover the inputs to the neural network. Since the attack requires no physical access, this can be a potential strong attack vector for future FPGA-based ML systems, especially those in sensitive applications like the military.

In the article titled "Automatic on-chip clock network optimization for electromagnetic side-channel protection," the authors have developed a tool to secure ICs against EM side-channel attacks. The proposed tool tunes the clock network automatically to desynchronize the power consumption and the EM emanation of the underlying sequential logics, thereby hindering the side-channel attacks while meeting other design constraints. In practice, in this article, based on a preanalysis and modeling of the relationship between on-chip clock networks and side-channel security, the clock network is adjusted to spread out the leakage temporally. Moreover, its amplitude is reduced to lower the leaked information.

IV. Low-Complexity and Energy-Efficient Implementations of Encryption Schemes

In the era of quantum computers, traditional encryption algorithms like RSA won't be efficient. In order to address this challenge, researchers are developing postquantum cryptography (PQC) algorithms. Ring-learning-with-errors (Ring-LWE)-based scheme is an essential type of the lattice-based PQC due to its strong security proof and ease of implementation. Binary ring-LWE (BRLWE)-based scheme possesses even smaller computational complexity and thus is more suitable for resource-constrained applications. In the article titled "Novel low-complexity polynomial multiplication over hybrid fields for efficient implementation of binary ring-LWE post-quantum cryptography," the authors present a novel implementation of the BRLWE-based scheme on the hardware platform with very low complexity with this point of view. The experimental results demonstrate that the proposed BRLWE structure involves significantly lower area-time complexities over existing designs. This article provides a path toward defining low-power, secure quantum encryption algorithms.

Temperature sensors are one of the most important building blocks of wearable devices. As in the case of the ongoing pandemic, body temperature is one of the most important signs of diseases and infections. Temperature sensors are also used for lab-on-chip systems where the temperature of a cell culture or reaction is monitored or used for calibration. The article titled "An encryption architecture suitable for on chip integration with sensors" shows a lightweight implementation of an encryption algorithm based on the Lorenz chaotic system. It was implemented as time scaling chaotic shift keying (TS-CSK) and integrated directly with the sensors on the same chip to secure temperature sensing applications. The security is derived from a chaos-based oscillator, which is used to scramble data in the analog domain, thereby side-stepping digitization and complex digital encryption algorithms. The data can be deciphered at the receiver based on the dependence of chaotic equations on their initial state and the fact that two identical chaotic systems can synchronize when they share a common state. The coupled differential equations of TS-CSK were implemented using low-power integrators, multiplexers, switches, and passive components. Experimental measurements of the differential encryption/decryption system implemented in 180-nm technology show that the chip operating with a 1.8-V supply can encrypt and decrypt the transmitted signal with a power dissipation of only 15 mW, making it a practical solution for the IoT and wearable devices. Since the used sensor output is quasi-digital, any other sensor with quasi-digital output, such as a pH or an impedance sensor, can also be used with this mode of security circuit.

A medical system designed for measuring patients' neurologic activities is another example where security robustness and energy efficiency need to be optimized together. A typical setup involves a portable, battery-powered neural recorder streaming sensitive patient data wirelessly to an authorized receiving station. The wireless communication needs to be secured against eavesdropping while meeting the ultra-low-power consumption budget of the portable neural recorder. In the article titled "An energy-efficient compressed sensing based encryption scheme for wireless neural recording," the authors present a novel compressed sensing (CS)-based encryption scheme to secure such communication. Given neural signals are intrinsically sparse, CS is adapted to simultaneously enable data compression and encryption to meet the low-power requirement. The sampling matrix serving as the cryptographic key for data encryption is exchanged using an elliptic-curve cryptography (ECC)-based key exchange protocol. ECC was implemented with constant-time execution to mitigate timing side-channel attacks. A prototype of the wireless neural recorder on 180-nm CMOS technology

was developed, where experimental results on functionality, performance, attack resistance, and energy consumption were measured from. With an overall power consumption of 422 μW during encrypted wireless transmission, the promising results demonstrate the methodology can be applied to other application areas where energy efficiency and security robustness both need to be met at the same time.

V. Security-Aware Hardware Design and Verification Methodologies

In an attempt to build robust hardware solutions that are free from security weaknesses and resilient against attacks, electronic design automation (EDA) tools play a crucial role to assist design and verification teams to deliver products with security assurance in an efficient and timely manner. A security-aware EDA tool would enable users, with or without deep security expertise, to identify security flaws in their designs early in the product development lifecycle and offer robust options to mitigate any findings. It would also offer insightful guidance and control to enable users to balance security robustness, performance, power consumption, die size, and other requirements. Unfortunately, the current state-of-the-art is still in its infancy, and there are a lot of opportunities for innovations and growth in this important domain. Breakthroughs in security-aware hardware design and verification methodologies are much needed to feed the technology pipeline to significantly improve the effectiveness of the security assurance effort that is largely performed by security experts manually today.

The article titled "Proof-carrying hardware-based information flow tracking in analog/mixed-signal designs" attempts to fill a long-standing methodology gap concerning the use of information flow tracking (IFT) technique on hardware. IFT has been widely used for digital hardware designs represented in hardware description languages (HDL) such as Verilog. However, confidentiality and integrity requirements extend beyond the digital domain into the analog domain. The authors propose an automated IFT-based methodology to verify properties such as information leakage and unauthorized tampering for analog and mixed-signal designs. By bridging across the digital and analog domains, the proposed solution enables IFT properties to be verified seamlessly across HDL and transistor level without the modification of the existing hardware design flow. It also enables security properties of third-party IPs to be verified without access to the HDL.

Acknowledgment

The Guest Editors would like to thank the authors for their contribution to this Special Issue. Without such outstanding contribution, the high standards of JETCAS for this Special Issue could not have been met. The Guest Editors would also like to thank the reviewers for their generous voluntary service in providing valuable suggestions for the articles submitted to this Special Issue. The Guest Editors are greatly thankful to the Editor-in-Chief (EiC), Prof. An-Yeu (Andy) Wu, Associate EiCs, Prof. Herbert Lu and Prof. Wen-Hsiao Peng, as well as the Senior Editorial Board for their continuous support and guidance throughout the process.

Naghmeh Karimi, *Corresponding Guest Editor*
Department of Computer Science and Electrical Engineering
University of Maryland Baltimore County
Baltimore, MD 21250 USA

Kanad Basu, *Guest Editor*
Electrical and Computer Engineering Department
University of Texas at Dallas
Richardson, TX 75080 USA

Chip-Hong Chang, *Guest Editor*
School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore 639798

Jason M. Fung, *Guest Editor*
Intel Product Assurance and Security
Intel Corporation
Hillsboro, OR 97124 USA

Naghmeh Karimi (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in computer engineering from the University of Tehran, Iran, in 1997, 2002, and 2010, respectively.

She was a Visiting Researcher at Yale University, USA, from 2007 to 2009, and a Post-Doctoral Researcher at Duke University, USA, from 2011 to 2012. She has been a Visiting Assistant Professor at New York University and Rutgers University from 2012 to 2016. She joined the University of Maryland, Baltimore County, as an Assistant Professor in 2017, where she leads the SECure, REliable, and Trusted Systems (SECRETS) Research Laboratory. She has published three book chapters and authored/coauthored more than 50 articles in referred conference proceedings and journals. Her current research interests include hardware security, VLSI testing, design-for-trust, design-for-testability, and design-for-reliability. She was a recipient of the National Science Foundation CAREER Award in 2020. She serves as an Associate Editor for the *Journal of Electronic Testing: Theory and Applications (JETTA)* (Springer).

Kanad Basu (Senior Member, IEEE) received the Ph.D. degree from the Department of Computer and Information Science and Engineering, University of Florida. His Ph.D. thesis was focused on improving signal observability for postsilicon validation.

He worked in various semiconductor companies, such as IBM and Synopsys. During his Ph.D. degree, he interned at Intel. He is currently an Assistant Professor at the Electrical and Computer Engineering Department, University of Texas at Dallas. Prior to this, he was an Assistant Research Professor with the Electrical and Computer Engineering Department, New York University. He has authored one book, two U.S. patents, two book chapters, and several peer-reviewed journal and conference articles. His current research interests are hardware and systems security. He was awarded the Best Paper Award at the International Conference on VLSI Design in 2011.

Chip-Hong Chang (Fellow, IEEE) received the B.Eng. degree (Hons.) from the National University of Singapore in 1989, and the M.Eng. and Ph.D. degrees from Nanyang Technological University (NTU), Singapore, in 1993 and 1998, respectively.

He is currently an Associate Professor with the School of Electrical and Electronic Engineering (EEE), NTU. He held joint appointments with a university as the Deputy Director of the Center for High Performance Embedded Systems from 2000 to 2011, the Program Director of the Center for Integrated Circuits and Systems from 2003 to 2009, and the Assistant Chair of Alumni from 2008 to 2014. He has coedited five books, published 13 book chapters, more than 100 international journal articles (more than 70 are in IEEE), and more than 180 refereed international conference papers (mostly in IEEE), and delivered over 40 colloquia. His current research interests include hardware security, machine learning security, unconventional computer arithmetic circuits, and low-power and fault-tolerant digital signal processing algorithms and architectures. He is a fellow of IET and a Distinguished Lecturer of the IEEE Circuits and Systems Society from 2018 to 2019. He guest-edited around ten special issues and served in the organizing and technical program committee of more than 60 international conferences (mostly IEEE). He currently serves as Senior Area Editor for IEEE TRANSACTIONS ON INFORMATION FORENSIC AND SECURITY and the Associate Editor for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS and IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS. He served as the Associate Editor for the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS from 2010 to 2013, the *VLSI Journal* from 2013 to 2015, IEEE ACCESS from 2013 to 2019, *Microelectronics Journal* from 2014 to 2020, IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS from 2016 to 2019, *Journal of Hardware and System Security* (Springer) from 2016 to 2020, and *Integration*.

Jason M. Fung received the two B.S. degrees in computer science and mathematics and in electrical and computer engineering, and the M.S. degree in electrical and computer engineering from Carnegie Mellon University in 1997 and 1998, respectively.

He is currently the Director of Offensive Security Research and Academic Research Engagement at Intel Corporation. He oversees the security assurance and emerging threat research of key technologies that power Intel's edge, communication, and data center products. In addition, he leads the academic and industry collaborations that advance product security assurance best practices for the semiconductor industry. Recent contributions include the creation of the community-driven hardware common weakness enumeration (CWE) and the industry-first hardware capture-the-flag competitions (HackAtEvent.org) that inspire researchers to address some of the toughest challenges in hardware security. He is the Founding Member of the CAPEC/CWE Advisory Board. He has over two decades of industry experience in SoC architecture and performance, verification automation, product security penetration testing, consultation, research and path-finding, engineering, and risk management. He has been serving in steering committees and founded the security tracks for several premier conferences at Intel since 2013. He has authored five U.S. patents and over 20 publications in peer-reviewed academic, industry, and Intel internal conferences.