New England Hardware Security Day

4th Workshop, NEHWS Day
Worcester Polytechnic Institute, Worcester, MA
April 5th, 2024

Organization

General Chair

Daniel Holcomb	University of Massachusetts, Amherst

Program Committee Chairs

Fatemeh Ganji	Worcester Polytechnic Institute
Xiaolin Xu	Northeastern University

Program Committee

Orlando Arias	University of Massachusetts, Lowell
Prabuddha Chakraborty	University of Maine
Joe Chapman	MITRE
Yunsi Fei	Northeastern University
Daniel Holcomb	University of Massachusetts, Amherst
Omer Khan	University of Connecticut
Sandhya Koteshwara	IBM
Yingjie Lao	Tufts University
Yukui Luo	University of Massachusetts, Dartmouth
Koksal Mus	Worcester Polytechnic Institute
Hoda Naghibijouybari	Binghamton University
Satwik Patnaik	University of Delaware
Seetal Potluri	University at Albany
Patrick Schaumont	Worcester Polytechnic Institute
Dean Sullivan	University of New Hampshire
Berk Sunar	Worcester Polytechnic Institute
Shahin Tajik	Worcester Polytechnic Institute
Mengjia Yan	Massachusetts Institute of Technology
Qiaoyan Yu	University of New Hampshire

Poster Chairs

Koksal Mus	Worcester Polytechnic Institute
Qiaoyan Yu	University of New Hampshire

Industry Chairs

Yunsi Fei	Northeastern University
Patrick Schaumont	Worcester Polytechnic Institute

Outreach Chairs

Shahin Tajik	Worcester Polytechnic Institute
Mengjia Yan	Massachusetts Institute of Technology

Publicity Chairs

Yarkin Doroz	Worcester Polytechnic Institute
Jakub Szefer	Yale University

Web Chair

Kemal Derya	Worcester Polytechnic Institute

Preface

The 4th New England Hardware Security (NEHWS) Day was held at Worcester Polytechnic Institute, Worcester, MA on April 5, 2024. The workshop is organized annually by the hardware security research community at these universities: Massachusetts Institute of Technology, Northeastern University, University of Massachusetts, Amherst, University of New Hampshire, Worcester Polytechnic Institute, and Yale.

NEHWS Day aims to initiate a discussion between industry and academia by outlining research priorities and opportunities in *hardware* security and verification according to the strategic visions of semiconductor companies and government agencies. NEHWS DAY 2024 was a one-day regional workshop with a poster session, panel, long and short talks, as well as two keynotes.

NEHWS Day 2024 received 48 submissions, including abstracts of 16 long and 8 short talks, 1 announcement, and 22 posters. The program committee chose proposed talks based on fit for NEHWS, whether the talk was likely to be good, and whether it would stimulate discussion and interest among the audience of hardware security practitioners, academics, and students. With this regard, the NEHWS program committee selected 6 long and 5 short talks to be presented from the podium with slides, followed by a brief Q&A. Authors of talk abstracts not accepted for the presentation were invited to present their work in poster format. In total, 31 posters were displayed at NEHWS 2024.

These proceedings include the program, abstract of 11 accepted talks, and the list of accepted posters.

We are grateful to General Chair Daniel Holcomb for his help and efforts. We are thankful to the workshop's sponsors: Northeast Microelectronics Coalition (NEMC) Hub, National Science Foundation (NSF), Massachusetts Technology Collaborative (MassTech), DRAPER, and Analog Devices.

We would like to also extend our appreciation to President Grace Wang (Worcester Polytechnic Institute) and Dean John A. McNeill (Worcester Polytechnic Institute) for their support.

Finally, we thank all the authors who submitted papers to NEHWS 2024, and program committee members who made this event a truly intellectually stimulating one.

March 2024
Fatemeh Ganji
Xiaolin Xu

NEHWS Day 2024

April 5th, 2024
Campus Center Odeum,
Worcester Polytechnic Institute

9:00 - 9:15	Welcome Remarks		Session chair: Berk Sunar and Shahin Tajik
9:15 - 9:30	Opening remarks by Ben Linville-Engler (MassTech) "ME Commons and CHIPS Act"		Session chair: Fatemeh Ganji
	News from the NEHWS Community		
9:30 - 10:30	Invited Keynote by Sharad Malik (Princeton University)		
10:30 - 10:45	Break		
10:45 - 12:00	Submitted Talks-- Session I		Session chair: Xiaolin Xu
	Long Talk	Breaching Privacy: Memory Scraping Attack on Xilinx FPGAs Bharadwaj Madabhushi, Sandip Kundu and Daniel Holcomb (University of Massachusetts Amherst)	
	Short Talk	Driving into The Unknown: Investigating and Addressing Security Breaches in Vehicle Infotainment System Yingjie Cao, Haoqi Shan, Maisha Mastora and Dean Sullivan (University of New Hampshire)	
	Long Talk	Deep-learning Model Extraction through Software-based Power Side-channel Xiang Zhang, A. Adam Ding and Yunsi Fei (Northeastern University)	
	Short Talk	SecureLoop: Design Space Exploration of Secure DNN Accelerators Kyungmi Lee, Mengjia Yan, Joel Emer and Anantha Chandrakasan (Massachusetts Institute of Technology)	
	Long Talk	LeakyOhm: Secret Bits Extraction using Impedance Analysis Saleh Khalaj Monfared, Tahoura Mosavirik and Shahin Tajik (Worcester Polytechnic Institute)	
	Short Talk	A Full-Stack Approach for Side-Channel Secure ML Hardware Anuj Dubey and Aydin Aysu (North Carolina State University)	
12:00 - 1:30	Lunch and Poster Session		
1:30 - 2:30	Panel Discussion "The Good and the Bad of Hardware Security" - Dominic Rizzo (ZeroRISC) - Gayatri Perlin (BAE) - Silviu Chiricescu (DRAPER) - Ed Suh (Meta/Cornell) - Wajdi K. Feghali (Intel)		Session chair: Mengjia Yan
2:30 - 3:30	Invited Keynote by Andreas Olofsson (Zero ASIC)		Session chair: Xiaolin Xu
3:30 - 3:40	Break		
3:40 - 4:45	Submitted Talks-- Session II		Session chair: Fatemeh Ganji
	Long Talk	Architectures for Secure Quantum Computing Systems Jakub Szefer (Yale University)	
	Short Talk	1/0 Shades of UC: Photonic Side-Channel Analysis of Universal Circuits Dev Mehta, Mohammad Hashemi, Domenic Forte, Shahin Tajik and Fatemeh Ganji (Worcester Polytechnic Institute)	
	Long Talk	Protecting Sensors from Electromagnetic Side-channel Leakage Yan Long and Kevin Fu (Northeastern University)	
	Short Talk	On the Feasibility of Golden-free PCB Verification Maryam Saadat Safa, Patrick Schaumont and Shahin Tajik (Worcester Polytechnic Institute)	
	Long Talk	EntryBleed: A Universal KASLR Bypass against KPTI on Linux William Liu, Joseph Ravichandran and Mengjia Yan (Massachusetts Institute of Technology)	
4:45 - 5:00	Best Poster Award and Closing Remarks		Session chairs: Qiaoyan Yu and Koksal Mus
5:00 - 6:00	Networking reception		

NSF

MASSACHUSETTS TECHNOLOGY COLLABORATIVE

ANALOG DEVICES

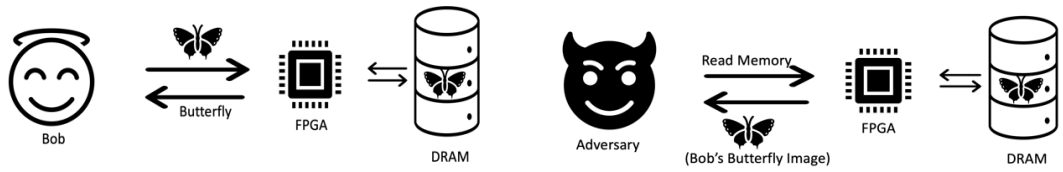
DRAPER

NEMC Northeast Microelectronics Coalition HUB

Breaching Privacy: Memory Scraping Attack on Xilinx FPGAs

Bharadwaj Madabhushi, Daniel Holcomb, Sandip Kundu
University of Massachusetts, Amherst, USA, bmadabhushi@umass.edu, dholcomb@umass.edu, kundu@umass.edu

FPGA-based hardware accelerators are increasingly popular due to their adaptability, customization, energy efficiency, consistent latency, and scalability. These devices can be tailored for specific algorithms, facilitating efficient hardware implementations that leverage algorithm parallelism. This often results in significant performance improvements, particularly for highly parallel applications, surpassing the capabilities of CPUs and GPUs. Notably, recent research indicates that Stratix 10 FPGAs can achieve up to 90\% of the performance of a TitanX Pascal GPU while consuming less than 50% of the power, making FPGAs an appealing choice for accelerating machine learning (ML) workloads. However, our investigation uncovers privacy and security vulnerabilities in existing Xilinx FPGA-based hardware acceleration solutions. These vulnerabilities arise from insufficient memory initialization and inadequate process isolation, creating potential avenues for unauthorized access to private data used by processes. To illustrate this issue, we conducted experiments using a Xilinx ZCU104 board running the PetaLinux embedded OS. We found that, at the software level, the PetaLinux embedded OS fails to effectively clear memory locations associated with terminated processes, leaving them susceptible to Memory Scraping Attacks. Furthermore, at the hardware level, we observed a deficiency in memory clearing by the Xilinx Memory Protection Units (XMPU), enabling an attacker to access the memory region after reassignment, resulting in an invasive private data readout, jeopardizing confidentiality. This paper is motivated by the works of Zhou et al. [1] and Maurice et al. [2], who previously targeted NVIDIA's heterogeneous memory systems in cloud-based environments, enabling adversaries to access and reconstruct data from terminated processes. A similar issue affects ARM Mali GPUs, where a new process can access a terminated process's pages due to the inadvertent reuse of freed pages [3]. This paper makes three main contributions. Firstly, it presents an attack methodology utilizing the Xilinx debugger from a different user space, enabling access to process IDs, virtual address spaces, and pagemaps of one user from a different user space due to inadequate process isolation by the embedded OS. Secondly, it introduces a methodology for characterizing terminated processes and accessing their private data, illustrated on the Xilinx ML application library, showcasing the memory scraping attack. The third contribution brings attention to a vulnerability in the XMPU implementation. While the XMPU security policy protects user memory during active user sessions, it fails to clear the memory region of a terminated process, revealing the resurrection attack. To mitigate these attacks, the memory region of a terminated process must be cleared, a crucial step absent in current FPGA implementations.



(a) Victim (b) Attacker

Figure 1: On the left, Bob interacts with the FPGA to analyze the content of an image and determine its meaning. On the right, the adversary reads and analyzes Bob's image after Bob terminates.

References

[1] Zhou, Z., Diao, W., Liu, X., Li, Z., Zhang, K. and Liu, R. (2016). Vulnerable GPU Memory Management: Towards Recovering Raw Data from GPU. doi: https://doi.org/10.48550/arxiv.1605.06610.
[2] Maurice, C., Neumann, C.K., Heen, O. and Francillon, A. (2014). Confidentiality Issues on a GPU in a Virtualized Environment. pp.119–135. doi: https://doi.org/10.1007/978-3-662-45472-5_9.
[3] Zero, G.P. (n.d.). CVE-2023-4211: Use-after-Free in ARM Mali GPU Driver. [online] 0-days In-the-Wild. Available at: https://googleprojectzero.github.io/0days-in-the-wild//0day-RCAs/2023/CVE-2023-4211.html [Accessed 21 Mar. 2024].

Driving into The Unknown: Investigating and Addressing Security Breaches in Vehicle Infotainment System

Yingjie Cao[1], Haoqi Shan[2], Maisha Mastora[3] and Dean Sullivan[3]

[1] Hong Kong Polytechnic University, Hung Hom, Hongkong, yingjiecao@prontonmail.com
[2] University of Florida, Gainesville, USA, haoqi.shan@certik.com
[3] University of New Hampshire, New Hampshire, USA, maisha.mastora@unh.edu, dean.sullivan@unh.edu

In-vehicle Infotainment (IVI) systems act as an interface to deliver a combination of useful information and entertainment services to users while driving and are an integral part of the internet-of-vehicles (IoV) ecosystem. Previous research has highlighted those integrated components of IoV networks, such as auto-motive sensor communication channels and electronic control units (ECU), are subject to vulnerabilities, exposing the vehicle to cyber-attacks that can impede its functionality and user privacy. However, beyond these IoV communication and control interfaces, vulnerabilities in the IVI system remain under-investigated, which can result in severe consequences. In this work, we propose an evaluation framework to reveal security vulnerabilities in IVI systems. We implement this framework to show that inadequate protection of a vehicle can exploit all connected vehicles within the IoV ecosystem. We address this by first identifying the general hardware and web vulnerabilities through physical and remote access to common and open debug surfaces in IVI systems and web services to identify 3 common hardware vulnerabilities and 5 web service vulnerabilities affecting 7 commercial automotive vendors with major security concerns. To extract IVI web service endpoints. In total, we found 23 vulnerabilities, 7 of which are public and assigned Common Vulnerabilities and Exposures (CVEs) from low to high severity. This analysis led to the discovery of vulnerable web services within Mercedes-Benz, Tesla, and other vendors. We present an end-to-end exploit against Mercedes-Benz that uses several new vulnerabilities with significant ramifications, e.g., enabling an attacker to gain back-end control of all connected vehicles in a web service, access to vehicle peripherals (locks, cameras, engine), and leaks privacy information about anyone registered on the IoV network. We further suggest potential mitigation techniques for the identified threats. All vulnerabilities have been responsibly disclosed to the vendors.

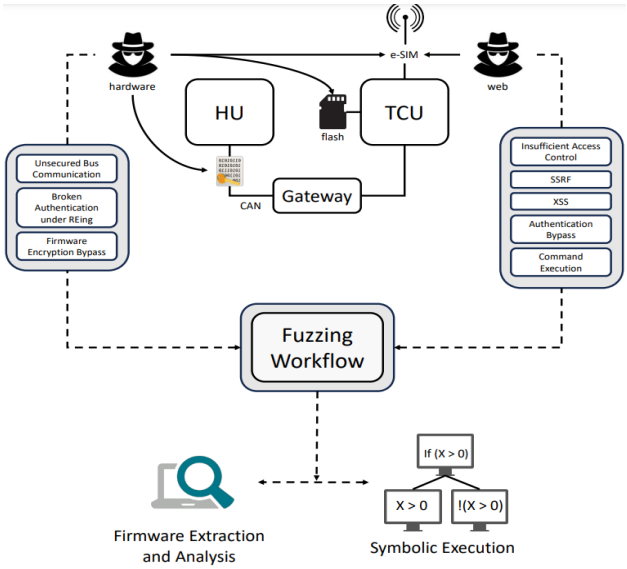


Figure 1: Security Analysis Framework Using Symbolic Execution Engine to Extract Web Services Endpoint Information.

Deep-learning Model Extraction through Software-based Power Side-channel

Xiang Zhang[1], Aidong Adam Ding[2] and Yunsi Fei[1]

[1] Department of Electrical and Computer Engineering, Northeastern University, Boston, USA
zhang.xiang1@northeastern.com, y.fei@enortheastern.com
[2] Department of Mathematics, Northeastern University, Boston, USA a.ding@northeastern.edu

Deep-learning model extraction attack aims at recovering the oracle deep neural network (DNN) model. In general, it is classified into two types. Learning-based model extraction works by training an approximate model with query inputs and the corresponding outputs from the oracle model. Cryptanalytic model extraction[1] applies statistical and cryptographic methods to "solve" equations for model parameters retrieval. However, its utility diminishes as the complexity and depth of the neural network increase, with the number of necessary queries rising exponentially. In this work, we address the limitation of cryptanalytic model extraction through a two-pronged approach, namely, leveraging a software power side-channel and devising an input gradient-based model extraction method. Our software-based power side-channel assisted model extraction is much more efficient than prior work. The improvement becomes more pronounced for deeper networks. To retrieve a 5-layer MLP, we need 211 queries, which is only 0.8% of 217.8 in prior work. Our method presented in [3] is also able to recover weights of a commonly used CNN, Lenet-5 trained on MNIST dataset, while the prior work failed.

RAPL-based side-channel and power leakage: Modern Intel processors have incorporated Running Average Power Limit (RAPL) technique which includes on-chip power sensors and corresponding Model-specific Registers (MSRs). Software interfaces are provided for users to read the accumulated energy consumption of various power domains. Lipp et al.[2] have utilized RAPL to perform software-based power side-channel analysis on common ciphers, including the RSA algorithm in Mbed TLS and AES-NI implementations. We utilize RAPL power monitors to retrieve the direction of a specific neuron activation function (ReLU). The ReLU activation in oneDNN framework is implemented as: if input $x < 0$, the output $f(x)$ is $x * alpha$; otherwise, $f(x) = x$. Such imbalanced two-branch clauses consume different power and form a power side-channel to leak the direction of the ReLU activation.

Input gradient-based model extraction: In our work, we propose an efficient method to recover the model weights through a comparison of the input gradients of two inputs, which form a flip pair, i.e., leading to different activation for the target ReLU neuron but have the same activation pattern for all other neurons in the network. Our method has consistent complexity across different layers, keeping the number of queries linearly dependent on the model depth, instead of exponential as in the prior work. Input gradient illustrates how minute variations in the input can impact the output of a model. With only queries inputs and outputs, assisted by the power side-channel for monitoring the entire model activation pattern, input gradient can be calculated by two queries with the same activation pattern. A property of the input gradient is that it only depends on the activation pattern and the weights, but not the biases.

Weights and Biases Recovery: We start from the last layer, for each neuron, we find a flip pair and calculate their input gradients. The difference between the input gradients gives the values of the neuron's weights up to a positive multiplicative constant. The same methodology is applied to identify flip pairs for neurons in preceding layers, enabling the recovery of their weights. The biases are affected only by the weights and activation patterns of the subsequent layers. By maintaining consistent activation patterns in the layers following the one currently under analysis, it becomes feasible to calculate the biases. Biases are deduced beginning from the first layer towards the last.

References

[1] Carlini, N., Jagielski, M. and Mironov, I., 2020, August. Cryptanalytic extraction of neural network models. In Annual international cryptology conference (pp. 189-218). Cham: Springer International Publishing.
[2] Lipp, M., Kogler, A., Oswald, D., Schwarz, M., Easdon, C., Canella, C. and Gruss, D., 2021, May. PLATYPUS: Software-based power side-channel attacks on x86. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 355-371). IEEE
[3] Zhang, X., Ding, A.A. and Fei, Y., 2023, October. Deep-Learning Model Extraction Through Software-Based Power Side-Channel. In 2023 IEEE/ACM International Conference on Computer Aided Design (ICCAD) (pp. 1-9). IEEE.

SecureLoop: Design Space Exploration of Secure DNN Accelerators

Kyungmi Lee[1], Mengjia Yan[1], Joel S. Emer[2] and Anantha P. Chandrakasan[1]

[1] Massachusetts Institute of Technology, Cambridge, USA, {kyungmi, mengjiay, anantha}@mit.edu
[2] MIT / NVIDIA, Cambridge, USA, jsemer@mit.edu

Deep neural networks (DNNs) are increasingly deployed in security-critical applications that process sensitive user information and make high-stake decisions. However, the security threats exploiting hardware-level vulnerabilities of the off-chip memory components can undermine the privacy and integrity necessary for such applications [3, 4]. While a trusted execution environment (TEE) for DNN computation can provide a solution to these security threats, the exploration in supporting TEEs on custom DNN accelerators is limited. The existing works on extending the TEE support to DNN accelerators only considered a few specific architectures as their baseline designs [1, 2], and generalizing the cost of securing those designs to other diverse DNN architectures with distinct performance goals and budgets is difficult.

SecureLoop [5] is a framework for design space exploration of secure DNN accelerators equipped with a hardware support for cryptographic operations. The goal of SecureLoop is to enable a systematic investigation of the performance, area, and energy trade-off for supporting a TEE in diverse DNN accelerator designs. We propose a scheduling search engine that identifies the optimal mapping of a DNN workload to a given hardware, such that a fair comparison among diverse designs can be achieved.

A key challenge for scheduling of secure DNN accelerators is that cryptographic operations are required for every off-chip data traffic, thus the schedule has to be coordinated with the cryptographic operations. We introduce two key techniques, the optimal authentication block assignment and the cross-layer fine tuning, to address this challenge and obtain a schedule that is up to 33% faster and 50% better in energy-delay product (EDP) compare to the baseline algorithm. Using SecureLoop, we perform design space exploration with sweeps over different design parameters and provide insights on which designs can be the Pareto front of the area versus performance trade-off for secure DNN accelerators.

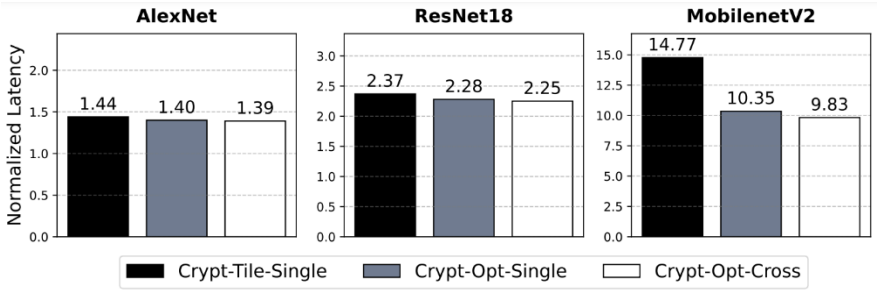


Figure 1: Performance overhead using different scheduling algorithms, measured by the number of cycles normalized to the unsecure baseline accelerator.

References

[1] Hua, W., Umar, M., Zhang, Z. & Suh, G. E., 2022. MGX: Near-Zero Overhead Memory Protection for Data-Intensive Accelerators. Proceedings of the 49th Annual International Symposium on Computer Architecture, p. 726–741.

[2] Lee, S. et al., 2022. TNPU: Supporting Trusted Execution with Tree-less Integrity Protection for Neural Processing Unit. IEEE International Symposium on High-Performance Computer Architecture (HPCA), pp. 229-243.

[3] Mutlu, O. & Kim, J. S., 2020. RowHammer: A Retrospective. Trans. Comp.-Aided Des. Integ. Cir. Sys., 39(8), p. 1555–1571.

[4] Szekeres, L., Payer, M., Wei, T. & Song, D., 2013. SoK: Eternal War in Memory. IEEE Symposium on Security and Privacy (SP).

[5] Lee, K., Yan, M., Emer, J. and Chandrakasan, A., 2023, October. SecureLoop: Design Space Exploration of Secure DNN Accelerators. In *Proceedings of the 56th Annual IEEE/ACM International Symposium on Microarchitecture* (pp. 194-208).

LeakyOhm: Secret Bits Extraction using Impedance Analysis

Saleh Khalaj Monfared, Tahoura Mosavirik, Shahin Tajik
Worcester Polytechnic Institute, Worcester, USA, {skmonfared,tmosavirik,stajik}@wpi.edu

The threats of physical side-channel attacks and their countermeasures have been widely researched. Most physical side-channel attacks rely on the unavoidable influence of computation or storage on current consumption or voltage drop on a chip. Such data dependent influence can be exploited by, for instance, power or electromagnetic analysis.

While current and voltage alterations have been considered the root cause of side-channel leakages, the data-dependent variation of the parameter relating current and voltage to each other via Ohm's law, i.e., impedance, has always been ignored. The primary assumption has been that impedance is a constant parameter that is determined by the materials used in the fabrication of the PCB, chip's die, and package. Hence, it is defined by the physical structure and size of the chip rather than the running computation on a system or stored content on a chip. For instance, adding/removing a circuit to/from a chip can cause changes in the impedance of the die. Such changes have been the basis of some hardware Trojan and tamper detection methods [1], where the malicious circuits modify the impedance of the system and, thus, can be detected. However, the effect of the circuit state or content of memory elements inside the chip on information leakage through the die's impedance has not been studied so far. In this work, we introduce a novel noninvasive physical side-channel attack, which exploits the data dependent changes in the impedance of the chip. Our attack relies on the fact that the temporarily stored contents in registers alter the physical characteristics of the circuit, which results in changes in the die's impedance. To sense such impedance variations, we deploy a well-known RF/microwave method called scattering parameter analysis, in which we inject sine wave signals with high frequencies into the system's power distribution network (PDN) and measure the echo of the signals. By deploying the highlighted scheme shown in Figure 1, we demonstrate that according to the content bits and physical location of a register, the reflected signal is modulated differently at various frequency points enabling the simultaneous and independent probing of individual registers.

Such side-channel leakage challenges the t-probing security model assumption used in masking, which is a prominent side-channel countermeasure. To validate our claims, we mount non-profiled and profiled impedance analysis attacks on hardware implementations of unprotected and high-order masked AES. We show that in the case of the profiled attack, only a single trace is required to recover the secret key. Finally, we discuss how a specific class of hiding countermeasures might be effective against impedance leakage.

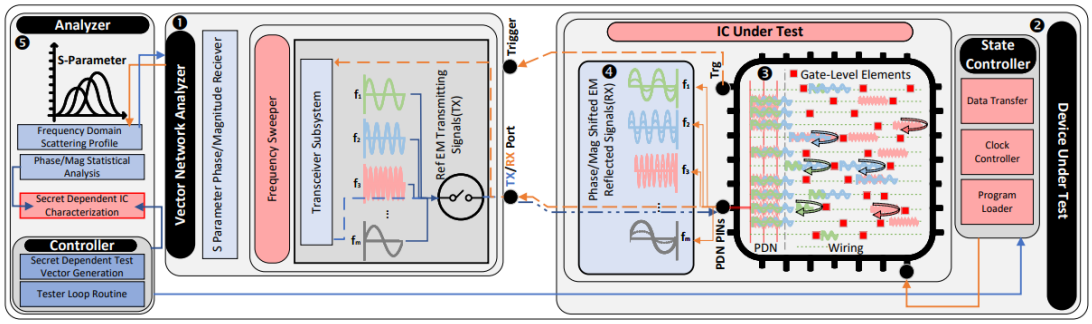


Figure 1: Overview of the proposed scheme.

References

[1] Mosavirik, T., Monfared, S.K., Safa, M.S. and Tajik, S., 2023. Silicon Echoes: Non-Invasive Trojan and Tamper Detection using Frequency-Selective Impedance Analysis. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023(4), pp.238-261.

Full-Stack Approach to Secure ML Hardware Side-Channels

Anuj Dubey and Aydin Aysu

North Carolina State University, aanujdu@ncsu.edu, aaysu@ncsu.edu

Machine learning (ML) has recently emerged as an application with confidentiality needs. A trained ML model is indeed a high-value intellectual property (IP), making it a lucrative target for notorious side-channel attacks. Recent works have already shown the possibility of reverse engineering the model internals by exploiting side channels like timing and power consumption. But the defenses are largely unexplored. Preventing ML IP theft is highly relevant given that the demand for ML will only increase in the coming years.

Securing ML hardware against side-channel attacks requires analyzing the vulnerabilities in the current ML applications and developing full-stack countermeasures from the ground up, covering cryptographic proofs, circuit design, firmware support, architecture/microarchitecture integration, compiler extensions, software design, and physical testing. There is a need to work on all abstraction levels because focusing on just one or a few level(s) cannot provide a complete solution to this nascent problem.

Our research achieves four key objectives to realize the first complete solution for side-channel protected ML. First, we analyze the side-channel vulnerabilities in the various hardware blocks of an ML accelerator and assess the feasibility of model parameter extraction. Second, we design provably secure gadgets, implement them on FPGA, and empirically validate possible countermeasures. Third, we add usability and flexibility to the solution – the ability to support multiple ML architectures via secure software APIs and compiler extensions on a RISC-V core. Fourth, we fabricate the final solution at Skywater 130nm node. Figure 1 shows the resulting PCB, the layout of the chip and some further details about our design. The full version of our work can be found in our recent publication [1].

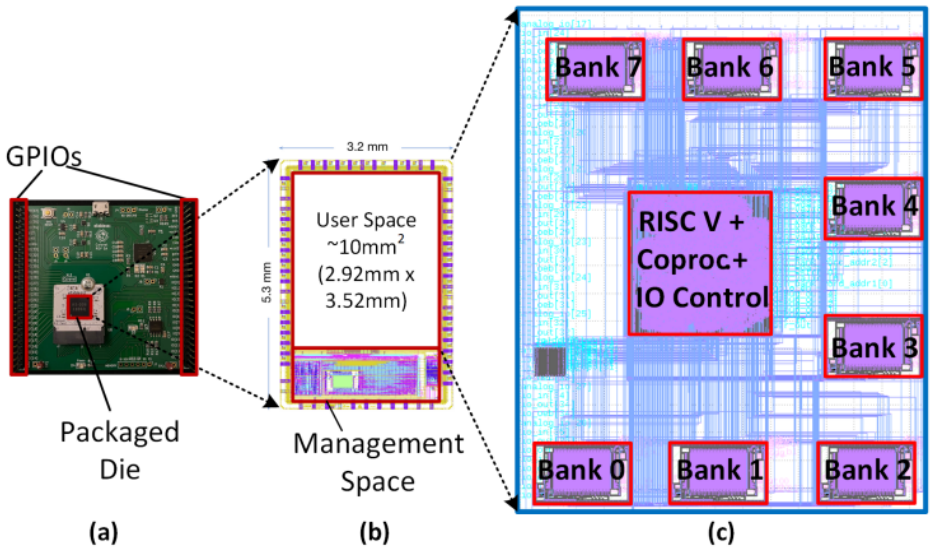


Figure 1: The layout of the fabricated chip. The final solution fits into 10mm² with 8 SRAM banks for on-chip memory, RISC-V core, and our developed co-processors. This is placed into the Caravel architecture that allows communication with the outside world through UART.

References

[1] Dubey, A. and Aysu, A., 2023, October. A Full-Stack Approach for Side-Channel Secure ML Hardware. In 2023 IEEE International Test Conference (ITC) (pp. 186-195). IEEE.

Architectures for Secure Quantum Computing Systems

Jakub Szefer

Department Of Electrical Engineering, Yale University, New Haven, CT, jakub.szefer@yale.edu

Quantum computing systems continue to advance rapidly in their size and fidelity. In parallel, there is an increasing number of deployments of these quantum computing systems into cloud-based services for use by researchers and the public. More and more of these quantum computing systems are becoming available as cloud-based services thanks to IBM Quantum, Amazon Braket, Microsoft Azure, and other cloud providers. Ease of access to these computing systems by almost anybody can help democratize quantum computing, democratize the development of algorithms or compilers, as well as democratize research since people can experiment with quantum computation on real devices without having a physical quantum computer. However, cloud-based access may make these systems vulnerable to novel security threats, both for users and cloud providers. Trusted, secure quantum computer architectures are one solution and defense against the number of security threats faced by cloud-based quantum computing systems. This talk will present several architectures for secure quantum computing systems under different threat models, along with the security protections they can offer. An example of one architecture is shown in Figure 1. The goal of this talk will be to introduce the audience to recent research on architectures for secure quantum computing systems, as well as in general, to make the audience aware of the need to protect quantum computing systems, of what can be achieved today, and of the many open research directions in the security of quantum computing systems.

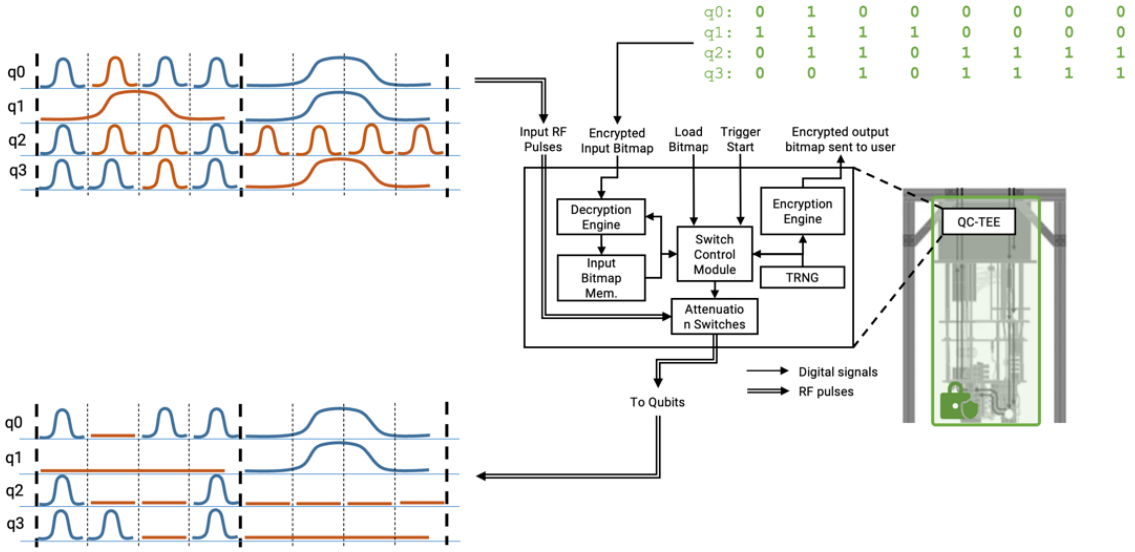


Figure 1: Example diagram of the operation of one of the proposed architectures for secure quantum computing systems: the diagram shows trusted hardware introduced for attenuation of control pulses sent to the quantum computers, allowing for introduction (in software) of decoy pulses and attenuation of the decoy pulses (in hardware) before they reach qubits.

References

[1] Trochatos, T., Deshpande, S., Xu, C., Lu, Y., Ding, Y., Szefer, J., 2024, May. Dynamic Pulse Switching for Protection of Quantum Computation on Untrusted Clouds. In International Symposium on Hardware Oriented Security and Trust.

[2] Trochatos, T., Deshpande, S., Xu, C., Lu, Y., Ding, Y., Szefer, J., 2023, May. A Quantum Computer Trusted Execution Environment. In Computer Architecture Letters.

1/0 shades of UC: Photonic Side-Channel Analysis of Universal Circuits

Dev M. Mehta[1], Mohammad Hashemi[1], Domenic Forte[2], Shahin Tajik[1] and Fatemeh Ganji[1]

[1] Worcester Polytechnic Institute, Worcester, USA, dmmehta2@wpi.edu, mhashemi@wpi.edu, stajik@wpi.edu, fganji@wpi.edu

[2] University of Florida, dforte@ece.ufl.edu

A universal circuit (UC) can be thought of as a programmable circuit that can simulate any circuit up to a certain size by specifying its secret *configuration bits*. UCs have been incorporated into various applications, such as private function evaluation (PFE). Recently, studies have attempted to formalize the concept of semiconductor intellectual property (IP) protection in the context of UCs. This is despite the observations made in theory and practice that, in reality, the adversary may obtain additional information about the secret when executing cryptographic protocols. This talk aims to answer the question of whether UCs leak information unintentionally, which can be leveraged by the adversary to disclose the configuration bits. In this regard, we propose the first photon emission analysis against UCs relying on computer vision-based approaches. We demonstrate that the adversary can utilize a cost-effective solution to take images to be processed by off-the-shelf algorithms to extract configuration bits. We examine the efficacy of our method in two scenarios: (1) the design is small enough to be captured in a single image during the attack phase, and (2) multiple images should be captured to launch the attack by deploying a divide-and-conquer strategy. To evaluate our attack's effectiveness, we use metrics commonly applied in side-channel analysis, namely rank and success rate. By doing so, we show that our profiled photon emission analysis achieves a success rate of 1 by employing a few templates (concretely, only 18 images were used as templates) [1].

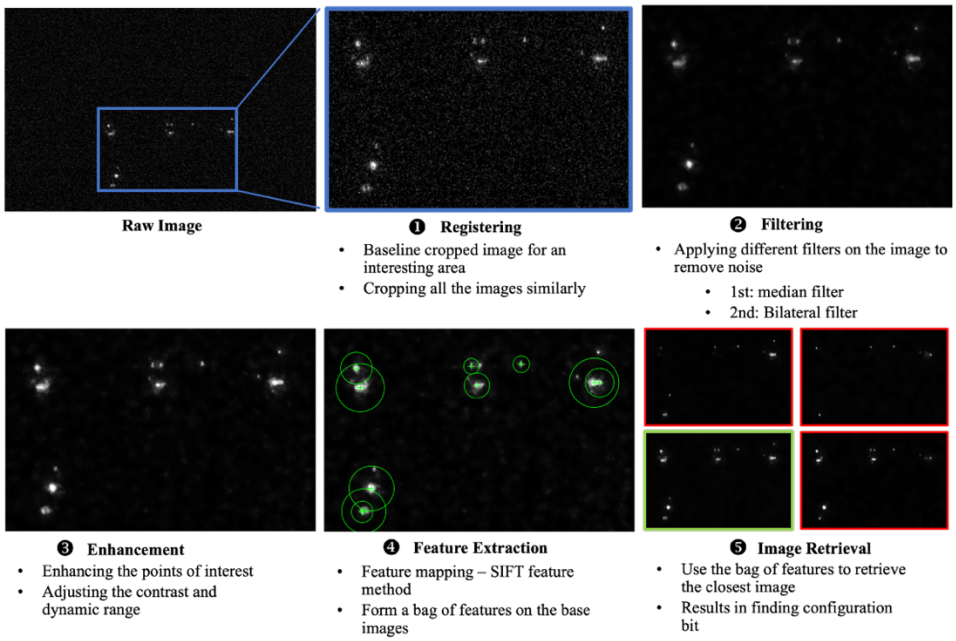


Figure 1: Applying image processing and computer vision-based techniques to extract configuration bits.

References

[1] Mehta, D.M., Hashemi, M., Forte, D., Tajik, S. and Ganji, F., 2024. 1/0 Shades of UC: Photonic Side-Channel Analysis of Universal Circuits. Cryptology ePrint Archive (conditionally accepted for publication in IACR Transactions on Cryptographic Hardware and Embedded Systems, 2024(3)).

Protecting Sensors from Electromagnetic Side-channel Leakage

Yan Long[1], and Kevin Fu[2]

[1] University of Michigan, Ann Arbor, USA, yanlong@umich.edu
[2] Northeastern University, Boston, USA, k.fu@northeastern.edu

Modern cyber-physical systems (CPS) depend on sensors to acquire physical information and make control decisions. For example, IoT devices and other embedded systems are increasingly equipped with camera sensors that can sense critical visual information in private spaces. While researchers have explored the data security of IoT cameras and the TEMPEST risks of computer monitors [1], a less explored problem is understanding how much camera data leaks through analog side channels of modern camera hardware interconnects such as MIPI CSI-2 cabling.

Our NDSS 2024 paper [2] presents the first attempt to analyze the attack surface of physical-channel eavesdropping on embedded cameras. We characterize EM Eye—a vulnerability in the digital image data transmission interface that allows adversaries to reconstruct real-time image streams from the camera circuits' unintentional electromagnetic emissions using software-defined radio (SDR), even from meters away and through walls. Our research shows EM Eye poses threats to a wide range of camera devices, from smartphones to dash cams and home security cameras. Demo and tutorial are available at: https://emeyeattack.github.io/Website/

This talk will demonstrate how standardized but unprotected data transmission interfaces allow for physical eavesdropping attacks and explain the underlying causality. I will discuss how this vulnerability connects to the long-standing problem of TEMPEST eavesdropping attacks against computer displays and how it could generalize over other types of sensing-based information systems, such as smart locks that employ fingerprint sensors. The talk aims to call attention to the fundamental problem of hardware and physical layer protections in sensor peripherals.

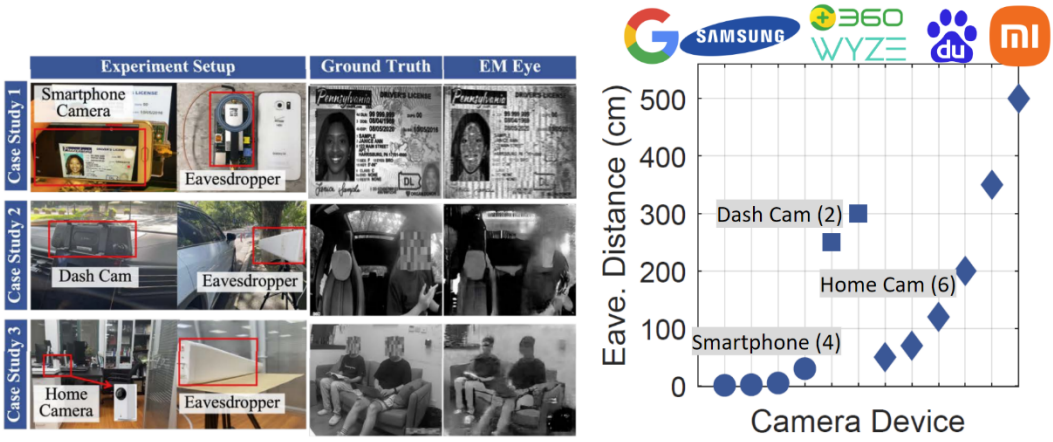


Figure 1: Example scenarios and susceptible devices of EM Eye attacks.

References

[1] Kuhn, M.G., 2006. Eavesdropping attacks on computer displays. Information security summit, pp.24-25.

[2] Long, Y., Jiang, Q., Yan, C., Alam, T., Ji, X., Xu, W. and Fu, K., 2024, EM Eye: Characterizing Electromagnetic Side-channel Eavesdropping on Embedded Cameras. In Network and Distributed System Security Symposium 2024.

On the Feasibility of Golden-free PCB Verification

Maryam Saadat Safa, Patrick Schaumont, and Shahin Tajik

Worcester Polytechnic Institute, Worcester, USA, msafa@wpi.edu, pschaumont@wpi.edu, stajik@wpi.edu

Printed Circuit Boards (PCBs) play a crucial role in electronic systems. Given the globalization of the PCB manufacturing and assembly process, they are susceptible to various attacks, rendering them potentially insecure. The conventional verification methods rely on the existence of a physical golden sample for signature comparisons. However, placing trust in the physical golden sample is not a secure option and obtaining these golden samples poses a significant challenge, requiring the presence of a reliable PCB assembly factory for their production. In practical situations, this prerequisite may not always be fulfilled. Often, verifiers may only have access to the system's design files, such as the PCB netlist, bill of materials, and IC package specifications. Therefore, it is crucial to develop a detection technique that does not rely on a physical golden sample and solely depends on the design file [1].

In this talk, we investigate a generic method for leveraging PCB design files to generate an estimated golden signature, which is then compared to the measured signature of untrusted boards. In the first phase, a trusted PCB design file is employed to generate the golden sample signature. The process involves importing and extracting the electrical characteristics of the PCB from its design file, followed by exporting the S-parameter (|S11|) signature of the PCB using simulation software. In the second phase, the verifier performs |S11| measurements using a vector network analyzer (VNA) on the power delivery networks (PDNs) of a population of PCB samples [2]. Afterward, the verifier will apply a similarity measure called Dynamic Time Warping (DTW) metric on the generated simulated golden signature and each of collected measured signatures. If the DTW score is below a predefined threshold, the test will be passed, and the sample is verified as genuine, otherwise, the test fails, and th1e sample will be considered dissimilar.

To validate this approach, we utilized an in-house designed PCB which contains three distinct and isolated PDNs. The process involves importing and extracting the electrical characteristics of the PCB from its design file, followed by exporting the S-parameter signature using ANSYS SIwave 2023 R2, which is a powerful 2.5D electromagnetic (EM) simulation tool. To emulate PCB tampering, decoupling capacitors of varying capacitances are added into the PDN under test on the board, conducted over six trials. The addition of capacitors to the PDN causes a change in the PDN's impedance, thereby affecting the |S11|. Finally, we compare the trusted simulated data to the measured signature derived from the same physical layout using DTW [3].

We demonstrate that the parasitic impedance of the PCB components including Equivalent Series Resistance (ESR) and Equivalent Series Inductance (ESL) is pivotal in achieving successful verification. The verifier should set a threshold during the design phase of the PCB. Based on the applications where the PCB will be implemented, the verifier has the discretion to determine different tolerances for the parasitic of components. To detect more advanced tampering, a higher degree of precision in parasitic impedance values is requisite. Having the approximate values of parasitic inductance and resistance in simulation tools enables more accurate predictions of the impedance behavior and the discrepancy between collected signatures from simulation and measurements would be minimum.

We also show that the mutual coupling between PDNs allows us to detect alterations in the impedance within one PDN by leveraging another PDN. This becomes especially valuable in situations where access is typically limited to a single PDN, yet we maintain the ability to identify tampers associated with other PDNs.

References

[1] Bhattacharyay, A., Chakraborty, P., Cruz, J. and Bhunia, S., 2022, July. VIPR-PCB: a machine learning based golden-free PCB assurance framework. In Proceedings of the 59th ACM/IEEE Design Automation Conference (pp. 793-798).

[2] Mosavirik, T., Monfared, S.K., Safa, M.S. and Tajik, S., 2023. Silicon Echoes: Non-Invasive Trojan and Tamper Detection using Frequency-Selective Impedance Analysis. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023(4), pp.238-261.

[3] Sakoe, H. and Chiba, S., 1978. Dynamic programming algorithm optimization for spoken word recognition. IEEE transactions on acoustics, speech, and signal processing, 26(1), pp.43-49.

EntryBleed:

A Universal KASLR Bypass against KPTI on Linux

William Liu, Joseph Ravichandran, and Mengjia Yan

MIT CSAIL, Cambridge, MA, wliu1@mit.edu,jravi@mit.edu, mengjiay@mit.edu

For years, attackers have compromised systems by developing exploits that rely on known locations of kernel code and data segments. KASLR (Kernel Address Space Layout Randomization) is a key mitigation in modern operating systems that hampers these attacks through runtime randomization of the kernel image base address. KPTI (Kernel Page Table Isolation) is another defense mechanism, originally introduced to defend against the 2018 Meltdown attack by unmapping kernel addresses during user code execution. This security mechanism makes it harder for attackers to leak kernel address mappings through micro-architectural side channels. However, a few pages for system call and interrupt handling were exempted from isolation for the sake of user to kernel context transitions.

We present the EntryBleed vulnerability (CVE-2022-4543) as a universal bypass against the KASLR protection mechanism through a combination of micro-architectural side channels and design flaws in the KPTI mitigation on Intel CPUs. We demonstrate that the bug we identified can accurately de-randomize the kernel address space within a second on modern Intel CPUs in both physical host and hardware-accelerated virtual machine environments. We then provide a root cause analysis to locate the core micro-architectural behaviors that enable EntryBleed, both on physical and under virtualized environments. Furthermore, we propose a performant mitigation based closely upon a pre-existing KASLR hardening mechanism. If left unpatched, attackers will be able to easily bypass KASLR, greatly lowering the barrier for exploit development and increasing the risk of serious threats against the Linux operating system.

This work has already been previously published and presented at HASP (Hardware and Architectural Support for Security and Privacy) 2023 in Toronto [1], where it won best paper.

References

[1] Liu, W., Ravichandran, J. and Yan, M., 2023, October. EntryBleed: A Universal KASLR Bypass against KPTI on Linux. In Proceedings of the 12th International Workshop on Hardware and Architectural Support for Security and Privacy (pp. 10-18).

List of Accepted Posters

Authors	Title
Anthony Etim, Shanquan Tian and Jakub Szefer	Extending FPGA Information Leaks with Trojan Phantom Circuits
Antian Wang and Yingjie Lao	NNTesting: Neural Network Fault Attacks Detection Using Gradient-Based Test Vector Generation
Ruyi Ding, Shijin Duan, Xiaolin Xu and Yunsi Fei	VertexSerum: Poisoning Graph Neural Networks for Link Inference
Davis Ranney and Yufei Wang	USBSnoop: Revealing Devices Activities via USB Congestion
Tianhong Xu and Yunsi Fei	TrustZoneTunnel: A Cross-world Pattern History Table-based Microarchitectural Side-channel Attack
Tahoura Mosavirik, Saleh Khalaj Monfared, Maryam Saadat Safa and Shahin Tajik	SiliconEchoes: Non-Invasive Trojan and Tamper Detection using Frequency-Selective Impedance Analysis
Mashrafi Alam Kajol, Sandeep Sunkavilli and Qiaoyan Yu	Voltage-Drop Attack Mitigation in Multi-Tenant FPGA Environments
Chuanqi Xu and Jakub Szefer	Information Leakage in Quantum Computers
Sanjay Deshpande, James Howe, Cansu Karakuzu, Yongseok Lee, Yunheung Paek, Jakub Szefer and Dongze Yue	PQC-DSA in Hardware
Haoqi Shan, Sravani Nissankararao, Yujia Liu, Moyao Huang, Shuo Wang, Yier Jin and Dean Sullivan	LightEMU: Hardware-Assisted Fuzzing of Trusted Applications
Ferhat Erata, Chuanqi Xu, Ruzica Piskac and Jakub Szefer	Power Side-Channel Attacks on Quantum Computer Controllers & Quantum Circuit Reconstructions
Akshita Mavurapu, Haoqi Shan, Xiaolong Guo, Orlando Arias and Dean Sullivan	HeisenTrojans: A New Class of Hardware Attacks
Sandeep Sunkavilli, Nishanth Chennagouni and Qiaoyan Yu	Dynamic Attack Resilience for New FPGA Use Model
Theodoros Trochatos	SoteriaQ: Securing Quantum Circuits
Nina Shamsi, Kaeshav Chandrasekar, Yan Long, Christopher Limbach, Keith Rebello, Kevin Fu	Developing a Threat Model of Laser-Induced Acoustic Interference in Computer Vision-Assisted Vehicles
Nishanth Chennagouni, Mohammad Monjur, Wei Lu and Qiaoyan Yu	A Hybrid Neural Network for Simultaneous Multi-Attack Detection in Sensor Networks
Negar Neda, Austin Ebel and Brandon Reagen	Homomorphic Encryption Dataflow Optimizations With Evaluation on the Ring Processing Unit (RPU)
Antonio Torres, Mohammad Hashemi and Fatemeh Ganji	Efficient Privacy-preserving NN Inference at the Edge
Seyedmohammad Nouraniboosjin and Fatemeh Ganji	Too Hot To Be True: Temperature Calibration for Higher Confidence in NN-assisted Side-channel Analysis
Hao Wang, Andrew Malnicof and Patrick Schaumont	T-Scope: Side-channel Leakage Assessment with a Hardware-accelerated Online TVLA Test
Zhenyuan Liu, Dillibabu Shanmugam, Adithya Ramesh and Patrick Schaumont	CAPRI6: An ASIC for Fault Root-Causing

Trey Marcantonio, Samuel Karkache, Amit Virchandbhai Prajapati, Dev Mehta, Dillibabu Shanmugam, Mohammad Hashemi, Fatemeh Ganji and Patrick Schaumont	SCAPEgoat: A Side Channel Analysis Library
Shabd Swaroop Kandarpa, Ankit Mittal and Aatmesh Shrivastava	Energy Detection-Based Framework for Detecting and Mitigating Jamming Attacks in Ultra-Low Power IoT Systems
Aymane El Jerari, Frank Rossi, Kaustubh Shivdikar, Alexander Ingare and David Kaeli	Architecting GPUs for Practical Fully Homomorphic Encryption
Zhaoxiang Liu, Kejun Chen, Dean Sullivan, Orlando Arias and Xiaolong Guo	Microscope: Causality Inference Crossing the Hardware and Software Boundary from Hardware Perspective
Dillibabu Shanmugam, Zhenyuan Liu, Adithya Ramesh and Patrick Schaumont	CAPRI6: Front-end, Simulation and Back-end
Arna Roy, Zhenyuan Charlotte Liu and Patrick Schaumont	Decoding Processor Secrets: Exploring Side-Channel Vulnerabilities in Instructions
Adithya Ramesh, Zhenyuan Liu, Dillibabu Shanmugam and Patrick Schaumont	CAPRI6: FPGA prototyping a 6-core MSP430 for Fault Root Cause Analysis
Theodoros Trochatos, Chuanqi Xu, Sanjay Deshpande, Yao Lu, Yongshan Ding and Jakub Szefer	SoteriaQ: Securing Quantum Circuits
Weimin Fu, Xuan Zhang and Xiaolong Guo	Leveraging Large Language Models for Addressing Hardware Security Challenges
Kemal Derya, M. Caner Tol and Berk Sunar	Fault+Probe: A Generic Rowhammer-based Bit Recovery Attack
Haoqi Shan, Dean Sullivan and Orlando Arias	When Memory Mappings Attack: On the (Mis)use of the ARM Cortex-M FPB Unit