Statement of Research Interests

Aydin Aysu

I develop secure systems that prevent advanced cybersecurity threats targeting hardware vulnerabilities. To that end, my research interests lie at the intersection of cryptography, computer architecture, and digital hardware design.

Trusted computing in hardware is fundamental to information security practices. The basis of security guarantees in digital systems is essentially a set of cryptographic operations executing in a hardware root of trust. Advanced cyberattacks therefore deliberately target hardware layer vulnerabilities, especially in the context of security-critical Cyber-Physical Systems (CPS) and Internet-of-Things (IoT) applications—these attacks are difficult to detect and are much harder to thwart from the higher abstraction levels of the system. My research analyzes such vulnerabilities of hardware implementations of cyber-infrastructure. To provide practical security solutions that can be deployed in real-world settings, the systems I develop focus on implementation (side-channel) security, hardware/software efficiency, and end-to-end system demonstration. I ultimately aim to design tools that can quantify a provable security level for a given threat model and enable automated trade-offs for developers between a desired level of security, performance, and cost.

Proposed Research Plan

I plan to pursue a research program on hardware-based security consisting of several research thrusts tackling different but related aspects of hardware-targeted attacks. Specifically, I intend to work on *applied cryptography*, *computer architecture security*, and the design of *hardware security modules* with a future focus on *automation for hardware security*. This research will build on a body of work I developed during my PhD and post-doctoral research experience.

1) **Applied Cryptography: Efficient and Secure Post-Quantum Cryptosystems.** All widely-used, standardized cryptographic constructions base their security on the difficulty of solving mathematical problems such as integer factorization. Quantum algorithms, however, are proven to solve these problems easily, hence quantum computers disable all existing cryptographic systems that are in place today. Recent developments in quantum computing technologies therefore generate an imminent threat to existing security systems, spurring significant interest to post-quantum (PQ) alternatives for long-term security. Recent events showed the growing importance of this field. National Institute of Standards and Technology (NIST) recently decided to consolidate and standardize PQ algorithms [1]. Likewise, Google started to experiment with PQ cryptography for their web browsers [2].

   There are two major problems with existing PQ encryption schemes. First, they are rather complex and optimizing them, especially for constrained real-time systems like IoT devices, is challenging. My prior research revealed that the underlying arithmetic operations of a popular PQ family of cryptosystems can be optimized in hardware [3] through an improved memory organization and careful area-performance trade-offs. Moreover, I show that pre-computation techniques on a PQ digital signature algorithm can achieve over 10× efficiency in energy for energy harvesting systems running embedded software [4], and over 100× reduction in latency for real-time applications using hardware/software co-design [5]. These works made some complex PQ proposals feasible for the next-generation of IoT, embedded, and real-time applications.

   The second major challenge of PQ systems is implementation security. Although these algorithms provide theoretical guarantees, their practical implementations can be vulnerable to side-channel attacks. Such attacks exploit the correlation of secret key to implementation characteristics like execution time, power consumption, or memory access patterns. Physical (hardware-based) side-channels are especially important and difficult to mitigate in embedded settings since adversary can have physical access to the device. Even after decades of intense study, side-channels on traditional cryptosystems is still an active area of research. Extending side-channel attacks and countermeasures to PQ algorithms

is a non-trivial task, as the majority of these new proposals use fundamentally different arithmetic constructions. My most recent contribution reveals that PQ encryption algorithms, on the one hand, exhibit new side-channels in hardware and, on the other hand, provide opportunities to design low-cost countermeasures through algorithm-specific features [6]. This research shows that a constrained IoT device can use a complex PQ encryption even with physical attack countermeasures if there is a careful design and security analysis of the PQ algorithm.

My ongoing research is on the implementation and side-channel analysis of PQ algorithms in the context of end-to-end applications like the PQ Transport Layer Security (TLS) protocol. The standardization effort started by NIST would especially make my research necessary on various PQ candidates. I am one of the few researchers in US with a track record of publications on PQ crypto-engineering and I am planning to extend my expertise towards my goal of realizing efficient and secure PQ cryptosystems. I intend to write my *NSF CAREER* proposal on *"Post-Quantum Cryptosystems: Efficiency, Security, and Education"* for a target timeline of 2018–2022. This proposal will include the extension of my prior work on efficient and secure designs of PQ cryptosystems to proposals at NIST competition. I am also planning to develop a course to teach the next-generation of cryptosystems to the next-generation of engineers and potentially use this experience in my NSF CAREER proposal.

To pursue my future research plans in this topic, I am looking forward to collaborating with researchers in the department (or across departments) working on VLSI and circuits to tape-out world's first PQ encryption chip along with energy optimization and side-channel security. To that end, I see approximate computing as a special enabler for low-energy designs that is not yet explored. Traditional cryptosystems cannot use approximate computing as a single-bit difference within cryptographic computations would reveal completely different results. However, lattice-based and coding-based PQ constructions such as Learning-with-Errors (LWE) or Medium-Dense-Parity-Check (MDPC) codes work by introducing errors into computations and recovering them later on, providing an opportunity for approximately computed cryptographic systems. More broadly, I also look forward to collaborating with theoretical cryptographers to develop an efficient and secure implementations of their cryptographic constructions. Research on this thrust would require EDA tools for chip tape-out and measurement equipments like high-end oscilloscopes, electromagnetic probes, and microscopes to investigate various side-channels such as power consumption, electromagnetic radiation, and photonic emissions.

2) **Hardware Security Modules: From Circuits to Systems with New Applications.** Root of trust in digital devices is the secure-by-design source typically implemented in hardware that higher abstraction levels rely on. Especially in IoT settings, physical unclonable functions (PUFs) have been promoted as a practical and more secure enabler in roots of trust for security applications. PUFs extract a unique, hardware-intrinsic information on electronic devices by exploiting the process variations that occur during silicon fabrication. This information can act like a digital fingerprint of the device, which is difficult to clone because the fabrication imperfections are indeed hard to replicate. Therefore, the PUF fingerprint can be used, for instance, to authenticate the device, which is useful to tackle the growing counterfeit digital device problem.

Although I have contributed to the design of IoT-specific PUF components such as a MEMS sensor PUF [7] and microprocessor compatible PUFs [8] [9], my research extends beyond the PUF core and further focuses on new systems and applications with PUFs. To that end, my contributions include designing the first end-to-end authentication solution using PUFs [10], devising an efficient method to combine multiple PUF components into a single board-level identifier with a new scheme for its hardware attestation [11], integrating PUFs with wireless communication technologies to enable more secure protocols [12], designing scalable PUF-based protocols for multi-vendor services in IoT applications [13], formulating efficient processing techniques for PUF-based authentications to reduce system cost [14], and constructing an Application Specific Instruction Set Processor (ASIP) for executing various PUF protocols with different design principles [15].

My ongoing research in this thrust is on a proof-of-concept design of a physical-attack secure system

that can use a special PUF along with several other components such as random number generators and lightweight encryption units to deliver a comprehensive system security. The premise of the PUF in such an envisioned system is to produce a stream of keys that are intrinsically immune to any kind of physical attacks that break prior encryption schemes. This system would require a PUF that can generate an exponential number of output bits. Moreover, unlike prior PUF constructions, this PUF has to be provably secure against machine-learning and side-channel attacks. Such a system could enable the IoT device to securely update its secret key or perform a secure boot on-demand and in the field in case of a security breach or device failure (e.g. in the case of a trojan activation). The advantage of a special PUF in this scenario is being able to securely enroll its physical function to a trusted server once, before deployment, and to later evaluate the function for a given input to generate a unique digital key. The server can apply the same evaluation on its side to achieve the same result, thus no further synchronization is needed between the IoT device and the server after deployment.

My background on PUF based systems combined with my expertise on designing lightweight cryptographic units for IoT devices [16], [17], [18] puts me in a unique position to conduct this research. I am planning a short-term research on PUFs and in the long-run my goal is to use PUFs as part of a secure system. I already have active collaborations in this thrust who work on theoretical or system aspects but I am also looking forward to building further partnerships with researchers working on circuit-level designs. I am planning to write a 'small' proposal, for a target timeline of 2018–2020, for the *NSF Secure and Trustworthy Cyberspace (SaTC)* program with a *Transition To Practice (TTP)* component. *NSF/Intel Partnership on Cyber-Physical Systems Security and Privacy (CPS-Security)* is also another suitable program to sponsor this line of research.

3) **Computer Architecture Security: Remote Physical Side-Channels in the Cloud.** Academic and industrial secure computer architecture solutions like Aegis, Sanctum, Intel SGX, or Arm TrustZone do not consider physical side-channel attacks in their threat model [19]. There are two main reasons for this exclusion. First, physical side-channel attacks, like the differential power attacks [20], are regarded a threat only for cryptographic applications, which already execute in their isolated hardware. Second, the majority of these secure computer architectures assume that such side-channel attacks require a physical access and expensive equipments to carry out the attack.

These two assumptions are, however, starting to change. First, researchers started to use power side-channels for other purposes such as detecting the web site being visited [21] or detecting the mobile applications that are running in a smartphone [22]. In the near future, it is not unrealistic to expect more sophisticated attacks on general applications to extract secret information like machine-learning model parameters or health-care records of patients. In fact, any secret information, and not just secret cryptographic keys, can potentially be recovered using power side-channel attacks given that there is a power monitor with sufficient sampling granularity. Second, advances in smart batteries [23] and energy management systems [24] can, in near future, provide external monitoring with fine-grained power measurements. These on-board monitors could allow remote side-channel attacks. Furthermore, recent cloud services like Amazon are starting to offer reconfigurable FPGA components on which one can employ a fine-grained power sensor [25] to remotely apply side-channel attacks, which especially threatens FPGA-based SoCs.

I envision that these new research developments will ultimately enable physical side-channels in the cloud, especially for FPGA-based servers, and that eventually all hardware architectures would be forced to consider power-based side-channels and employ associated defenses. This will effectively broaden the scope of hardware-security research which so far has been limited to cryptographic applications and standalone hardware. I am planning to extend my prior research on hardware design and power side-channel analysis to this promising new field, first by demonstrating the attack potential on remote servers and beyond cryptographic applications, and then by proposing efficient countermeasures that use a synergy between power-aware compilers and secure instructions in hardware. To realize this vision, I am looking forward to collaborating with researchers in the department (or across

departments) that are working on compilers, computer architectures, and system security. My plan is to first establish a credible research group on the first two thrusts and then to apply for grants in this topic for a target timeline of 2020–2023. This research would require an infrastructure of servers with FPGA-based accelerators to run the attacks and test their effectiveness in a cloud setting.

Although physical side-channels are typically considered as an attack vector, for applications that use no secret information, analog behavior such as power consumption can also be an integrity check mechanism—an orthogonal method to evaluate if the device indeed follows the desired set of operations with the desired data. My ongoing research is on the detection of emerging micro-architectural attacks such as hardware-based covert-channels and rowhammer attacks on state-of-the-art computer architectures in real-time and embedded systems. Our preliminary results show that these type of attacks, although hard to detect using conventional security mechanism, can easily be captured due to the anomalies they introduce in power consumption. Therefore, I envisage that the use of power based detector combined with advanced machine learning classifiers to be an efficient identifier of otherwise difficult to detect zero-day attacks on computer architectures.

4) **Automation for Hardware Security.** Unfortunately, security evaluation and countermeasures for cryptographic and other systems are carried out manually and in an ad-hoc manner for each setting. For example, research on PQ side-channels require a domain-expert to fully understand new algorithms, to know how to implement them on specific platforms, to figure out the associated side-channel vulnerabilities, to propose new countermeasures for effectively mitigating vulnerabilities, and to finally evaluate the proposed solution thoroughly on the target platform with respect to some metric/method. Given that there are N algorithms, M possible implementations, and P side-channel attacks, there is a space of N×M×P configurations to evaluate. Performing an entire side-channel evaluation for a single configuration is typically sufficient today to publish a paper at premiere security conferences. Even for that single setting, the evaluation process is error-prone hence each year there is yet another analysis/improvement on a prior work. While this procedure may be possible in the short-term, e.g. for PQ cryptosystems, in the long-run, we need new tools to automate security analysis. For hardware implementations, I envisage the use of high-level synthesis (HLS) tools that are becoming popular especially for FPGA based implementations (e.g. Vivado HLS) to produce secure hardware. These tools generate a hardware design from a high-level description like a C program. Recent work showed that existing HLS tools can provide a reasonable design compared to hand-coded hardware for cryptographic applications [26] and academic tools show a similar success for limited use cases [27]. No prior work, however, considered security aspects in their analysis. The main challenge is to express hardware security properties into the tools in such a way that the resulting hardware will have formal guarantees. This research therefore requires a collaboration of a domain expert like me with researchers working on electronic design automation (EDA), and test and verification.

Funding Opportunities

In addition to the funding programs I discuss in my research plan such as *NSF CAREER* and *SaTC*, *NIST*, and *NSF/Intel CPS-Security*, there are additional opportunities to sponsor my research. Security against quantum cryptanalysis is a *national security* issue because quantum computers are likely to be developed by motivated nation states to break into military grade encryptions. Therefore, research on post-quantum cryptography is suitable for Defense Advanced Research Projects Agency (*DARPA*), Homeland Security Advanced Research Projects Agency (*HSARPA*), and Office of Naval Research (*ONR*) proposals. Physical side-channel attacks in the cloud is a threat to applications processing sensitive health-care data, hence this research is also suitable for National Institute for Health (*NIH*) proposals. I also have been in close contact with Semiconductor Research Corporation (*SRC*) industry liaisons and researchers in charge of cybersecurity funding programs at *Qualcomm*, *CISCO*, *NXP*, *Lockheed Martin*, *Envieta*, *Accenture*, and *NIST*.

References

[1] National Institute of Standards and Technology, "Post-Quantum cryptography," https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

[2] M. Braithwaite, "Experimenting with post-quantum cryptography," https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html.

[3] **A. Aysu**, C. Patterson, and P. Schaumont, "Low-cost and area-efficient FPGA implementations of lattice-based cryptography," in *Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on*, June 2013, pp. 81–86.

[4] **A. Aysu** and P. Schaumont, "Precomputation methods for hash-based signatures on energy-harvesting platforms," *IEEE Transactions on Computers*, vol. 65, no. 9, pp. 2925–2931, 2016.

[5] **A. Aysu**, B. Yuce, and P. Schaumont, "The future of real-time security: Latency-optimized lattice-based digital signatures," *ACM Trans. Embed. Comput. Syst.*, vol. 14, no. 3, pp. 43:1–43:18, Apr. 2015.

[6] **A. Aysu**, M. Tiwari, and M. Orshansky, "A novel hardware design for binary Ring-LWE with power side-channel countermeasures," in *2018 Design, Automation Test in Europe Conference Exhibition (DATE)*, Accepted 2018.

[7] **A. Aysu**, N. F. Ghalaty, Z. Franklin, and P. Schaumont, "Digital fingerprints for low-cost platforms using MEMS sensors," in *Proceedings of the Workshop on Embedded Systems Security*, ser. WESS '13, 2013, pp. 2:1–2:6.

[8] **A. Aysu** and P. Schaumont, "PASC: Physically authenticated stable-clocked soc platform on low-cost FPGAs," in *2013 International Conference on Reconfigurable Computing and FPGAs (ReConFig)*, 2013, pp. 1–6.

[9] **A. Aysu** and P. Schaumont, "Hardware/software co-design of physical unclonable function based authentications on fpgas," *Microprocess. Microsyst.*, vol. 39, no. 7, pp. 589–597, Oct. 2015.

[10] **A. Aysu**, E. Gulcan, D. Moriyama, P. Schaumont, and M. Yung, "End-to-end design of a PUF-based privacy preserving authentication protocol," in *Cryptographic Hardware and Embedded Systems – CHES 2015*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2015, vol. 9293, pp. 556–576.

[11] **A. Aysu**, S. Gaddam, H. Mandadi, C. Pinto, L. Wegryn, and P. Schaumont, "A design method for remote integrity checking of complex PCBs," in *2016 Design, Automation Test in Europe Conference Exhibition (DATE)*, March 2016, pp. 1517–1522.

[12] C. Huth, **A. Aysu**, J. Guajardo, P. Duplys, and T. Güneysu, *Secure and Private, yet Lightweight, Authentication for the IoT via PUF and CBKA*. Cham: Springer International Publishing, 2017, pp. 28–48.

[13] X. Guo and **A. Aysu**, "Security protocols for unified near field communication infrastructures," Nov. 15 2016, US Patent 9,497,573.

[14] **A. Aysu**, Y. Wang, P. Schaumont, and M. Orshansky, "A new maskless debiasing method for lightweight physical unclonable functions," in *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2017, pp. 134–139.

[15] **A. Aysu**, E. Gulcan, D. Moriyama, and P. Schaumont, "Compact and low-power ASIP design for lightweight PUF-based authentication protocols," *IET Information Security*, vol. 10, no. 5, pp. 232–241, 2016.

[16] **A. Aysu**, E. Gulcan, and P. Schaumont, "SIMON says: Break area records of block ciphers on FPGAs," *Embedded Systems Letters, IEEE*, vol. 6, no. 2, pp. 37–40, June 2014.

[17] E. Gulcan, **A. Aysu**, and P. Schaumont, "A flexible and compact hardware architecture for the SIMON block cipher," in *Lightweight Cryptography for Security and Privacy*, ser. Lecture Notes in Computer Science. Springer International Publishing, 2015, vol. 8898, pp. 34–50.

[18] E. Gulcan, **A. Aysu**, and P. Schaumont, *Progress in Cryptology – INDOCRYPT 2015: 16th International Conference on Cryptology in India, Bangalore, India, December 6-9, 2015, Proceedings*, 2015, ch. BitCryptor: Bit-Serialized Flexible Crypto Engine for Lightweight Applications, pp. 329–346.

[19] V. Costan and S. Devadas, "Intel SGX explained." *IACR Cryptology ePrint Archive*, vol. 2016, p. 86, 2016.

[20] P. Kocher, J. Jaffe, and B. Jun, *Differential Power Analysis*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397.

[21] M. Philipose, M. Halpern, P. Lifshits, M. Silberstein, and M. Tiwari, "Inferno: Side-channel attacks for mobile web browsers," 2015.

[22] M. Dong, P.-H. Lai, and Z. Li, "Can we identify smartphone app by power trace?" in *Design Automation Conference (ASP-DAC), 2013 18th Asia and South Pacific*. IEEE, 2013, pp. 373–375.

[23] A. Badam, R. Chandra, J. Dutra, A. Ferrese, S. Hodges, P. Hu, J. Meinershagen, T. Moscibroda, B. Priyantha, and E. Skiani, "Software defined batteries," in *Proceedings of the 25th Symposium on Operating Systems Principles*, ser. SOSP '15, 2015, pp. 215–229.

[24] J. Han, C. S. Choi, W. K. Park, I. Lee, and S. H. Kim, "Smart home energy management system including renewable energy based on ZigBee and PLC," in *2014 IEEE International Conference on Consumer Electronics*, 2014, pp. 544–545.

[25] D. R. E. Gnad, F. Oboril, S. Kiamehr, and M. B. Tahoori, "Analysis of transient voltage fluctuations in FPGAs," in *2016 International Conference on Field-Programmable Technology (FPT)*, 2016, pp. 12–19.

[26] E. Homsirikamol and K. Gaj, "Can high-level synthesis compete against a hand-written code in the cryptographic domain? A case study," in *ReConFigurable Computing and FPGAs (ReConFig), 2014*. IEEE, 2014, pp. 1–8.

[27] A. Khalid, M. Hassan, G. Paul, and A. Chattopadhyay, "Runfein: a rapid prototyping framework for feistel and spn-based block ciphers," *Journal of Cryptographic Engineering*, vol. 6, no. 4, pp. 299–323, Nov 2016.