Post-quantum secure encryption and cybersecurity education

Encryption systems that are capable of surviving quantum computer attacks are urgently required, but the cybersecurity talent gap militates against securing cyberinfrastructure. Dr Aydin Aysu, Assistant Professor at North Carolina State University, is advancing the research and teaching of post-quantum secure encryption. He has developed a quantum-secure encryption system together with a new graduate program on hardware security and is currently developing design automation for lattice-based post-quantum cryptosystems.

whiteMocca/Shutterstock.com

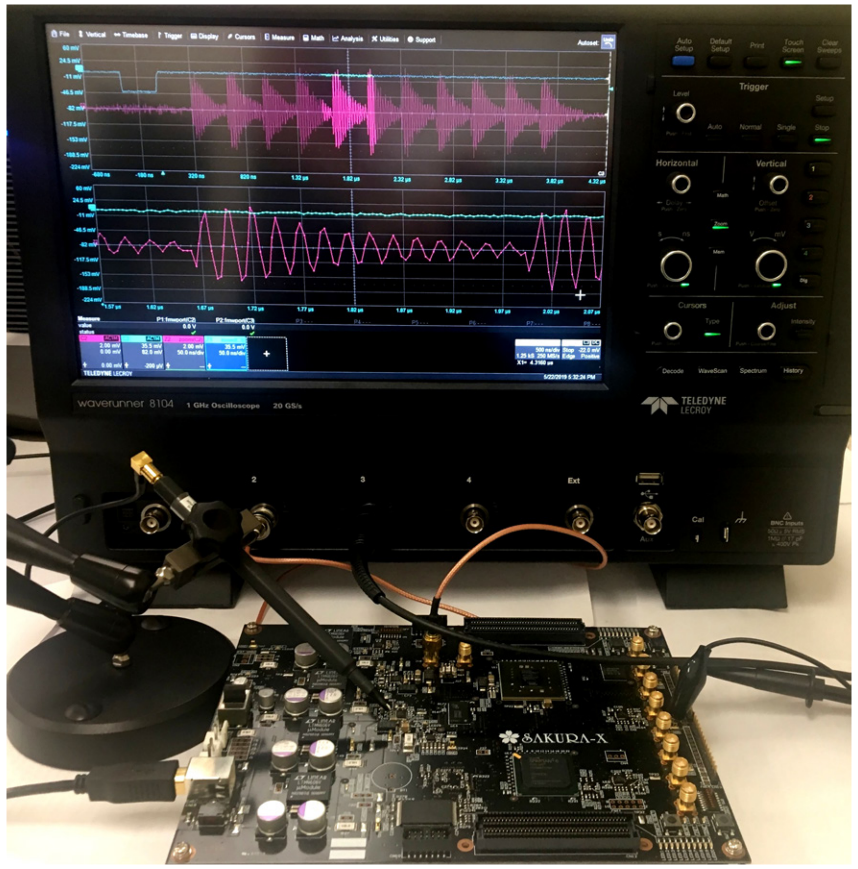
The future of cybersecurity relies on developing quantum-secure algorithms, implementing them on trusted hardware, and training cybersecurity professionals at scale. Indeed, the emergence of quantum computers places existing security standards under severe threat. New encryption systems that can survive quantum computer attacks are urgently required. At the same time, hardware attacks are a growing concern among cybersecurity exploits, particularly as reliable computing hardware is essential to all information security practices. Cryptographic operations executing in a hardware root-of-trust underpins the security guarantees in a system. If this hardware root gets compromised, the security enforcement mechanisms will fail. Finally, the supply of cybersecurity specialists capable of developing such post-quantum secure encryption system is lagging far behind the demand for expertise, creating the cybersecurity talent gap. It is anticipated that there will be 3.5 million unfilled cybersecurity positions globally by 2021, highlighting the need to train hardware security specialists to secure cyberinfrastructure.

Dr Aydin Aysu, Assistant Professor at the Department of Electrical and Computer Engineering, North Carolina State University is advancing the research and teaching of post-quantum secure encryption. In his project 'Secure Instruction Set Extensions for Lattice-Based Post-Quantum Cryptosystems' funded by the National Science Foundation (NSF) Computer and Information Science and Engineering (CISE) Secure and Trustworthy Cyberspace (SaTC) Research Initiation Initiative (CRII) program, Dr Aysu is developing a quantum-secure encryption system together with a new graduate program on hardware security. He explains how "existing encryption techniques are proven to be vulnerable to quantum computing because their mathematical foundations are solvable with a quantum computer". The development of new encryption systems capable of surviving quantum computer attacks is therefore crucial. These encryption systems are still classical algorithms that can be executed on classical computer. They are founded, however, on hard mathematical problems, such as the shortest vector problem, that cannot be practically solved by any computer, be it quantum or classical.

SIDE-CHANNEL ATTACKS

There is in-depth scrutiny of the theoretical analysis of post-quantum secure encryption; conversely, their implementation security is mostly uncharted. Dr Aysu points out that cryptography schemes that are mathematically sound, are still vulnerable to being attacked at the implementation level. These attacks are known as side-channel attacks.

The adversary can extract the secret key by measuring either the power consumption or electromagnetic radiation of a computer while it is executing encryption. Dr Aysu's recent work demonstrates that the attacker can discover the entire secret key from as little as a single post-quantum encryption operation. To avoid such attacks, computers implementing post-quantum secure encryption will therefore require a countermeasure to be incorporated into the execution. The development of side-channel countermeasures is the main research objective of this CRII project.



The side-channel attack in real time. The power and electromagnetic measurements obtained from the quantum-secure encryption hardware leaks information about the cryptographic secret keys.

> ***It is anticipated that there will be 3.5 million unfilled cybersecurity positions globally by 2021.***

POST-QUANTUM ENCRYPTION

Using secure multi-party computation allows Dr Aysu to achieve protection from attacks. This technique involves dividing all computations into randomised shares in such a way that prevents any individual computation having a statistical correlation with the secret key. This project will take these techniques and efficiently tune them for a variety of post-quantum encryption algorithms that are already available and develop methods for their automatic application.

This research builds on ongoing work on post-quantum encryption that started in 2013. During this time, Dr Aysu had identified the first implementation vulnerabilities of post-quantum key exchange protocols. He also designed faster hardware for post-quantum encryption use in real-time systems, and developed efficient software for use in Internet-of-Things (IoT) devices.

LATTICE-BASED POST-QUANTUM CRYPTOSYSTEMS

The current research focus is enabling design automation for lattice-based post-quantum cryptosystems. These are public-key encryption schemes that employ lattice problems to enable quantum-secure alternatives of existing systems. Lattice-based cryptography is centred on some lattice-based constructions that cannot be solved efficiently and are therefore resistant to attack by both classical and quantum computers. Public-key, or asymmetric, encryption schemes use two keys: a public key to encrypt, and a private key to decrypt. It is computationally infeasible to compute the private key from the public key, so public keys can be shared freely. This allows anyone to encrypt a message using the public key, and ensures that only the owners of the private keys can decrypt content or create digital signatures.

AUTOMATICALLY GENERATE HARDWARE DESIGNS

Encryption algorithms have a variety of arithmetic structures that require the hardware designs to be manually tuned for each setting. In addition, these applications have an assortment of throughput/area requirements, yet the hardware is designed to handle a fixed, pre-defined number of processing elements. This project will also deliver a system that can automatically generate hardware designs providing the desired parameters and throughput for a diverse range of algorithms. The publication describing this recent work won the best application paper award at the 2020 Design, Automation and Test in Europe (DATE) conference.

CYBERSECURITY EDUCATION

An integral part of the project is the teaching of post-quantum encryption. Dr Aysu has developed an innovative graduate course on hardware security that focuses on post-quantum cryptography. The course targets students with little or no experience of cryptography or hardware vulnerabilities. This approach combines theory with practical hands-

The future of cybersecurity relies on developing quantum-secure algorithms, implementing them on trusted hardware, and training cybersecurity professionals at scale.

ra2 studio/Shutterstock.com

on experiments. Dr Aysu explains, “the objective of the course is to provide a breadth of understanding of hardware security and an in-depth comprehension of the implementations of cryptographic hardware, potential exploits, and associated defences.” During their studies, students design specialised hardware accelerators for post-quantum cryptography, they execute implementation attacks, such as side-channel and fault attacks, and they build countermeasures for hardware designs. Dr Aysu recognises the challenge in covering the required concepts in, for instance, hardware design, applied cryptography, computer architectures, and statistics, yet still maintain a balance in the breadth and depth of the relevant subjects.

> **The development of new encryption systems capable of surviving quantum computer attacks is crucial.**

COURSE STRUCTURE

The course is structured using five components. Regular lectures are given either by the instructor or an invited guest lecturer from industry or academia. These provide the breadth of topics, while the remaining elements provide students with the depth of knowledge. Students complete a set of course assignments, in which they design hardware and analyse implementation attacks/ defences, which they then apply to real cryptosystems during hands-on experiments. Early in the course students select papers which they study and then present to their peers. The paper presentations cover valuable concepts that are not covered in lectures. Several students are randomly selected to review each presenter and paper, and encourage students to read the papers before their presentations. In addition, students complete their final research projects, where they tackle self-proposed open-ended problems. Towards the end of the course, students present their research projects and submit a report. A number of these projects have the potential to be turned into research papers.

BROADER IMPACTS

Disseminating publications, distributing open-source hardware and software, and bridging the research on computer architectures and hardware security are among the broader impacts of this research. Currently, secure computer architectures leave physical side-channels out of their threat model, so bridging this research is vital.

Dr Aysu also draws attention to how this research project can assist in the quantum-secure encryption standardisation, currently being led by the National Institute of Standards and Technology (NIST), by providing an evaluation of those proposals involving lattice cryptography. He believes that all university electrical and computer engineering departments should run a hardware security course. While hardware security courses are taught in some universities in the US, public information suggests that this is the only one focusing on next-generation cryptographic systems. Dr Aysu is happy to share his experience of developing this course and offers useful advice to future adopters.

Behind the Research

Dr Aydin Aysu

E: aaysu@ncsu.edu **T:** +1 919-515-7907 **W:** https://research.ece.ncsu.edu/aaysu/

Research Objectives

Aydin Aysu’s research interests include applied cryptography, computer architecture, and digital hardware design. He also works on cybersecurity education and the societal impacts of cybersecurity.

Detail

Aydin Aysu
The Department of Electrical and Computer Engineering
890 Oval Drive, Raleigh, NC, 27606

Bio

Dr Aysu is an assistant professor at NC State. He was a post-doctoral researcher at UT Austin from 2016 to 2018. He received his PhD degree from Virginia Tech in 2016. He won the best paper award at 2019 GLS-VLSI and 2020 DATE conferences. He is an IEEE senior member.

Funding

The National Science Foundation Grant #1850373
The National Science Foundation Grant #16-244770 (Center for Advanced Electronics through Machine Learning)

Collaborators

- Dr Paul Franzon (Collaborator)
- Dr Patrick Schaumont (PhD Advisor)
- Dr Michael Orshansky (Post-Doc Advisor)
- Dr Mohit Tiwari (Post-Doc Advisor)
- Dr Andreas Gerstlauer (Collaborator)
- Dr Michela Becchi (Collaborator)

References

- Mert, A.C., Karabulut, E., Ozturk, E., Savas, E., Becchi, M., Aysu, A. (2020). A Flexible and Scalable NTT Hardware: Applications from Homomorphically Encrypted Deep Learning to Post-Quantum Cryptography. *Design, Automation and Test in Europe Conference* 2020, 1-6, Grenoble, France, March 2020, 1-6.
- Aysu, A. (2019). Teaching the Next Generation of Cryptographic Hardware Design to the Next Generation of Engineers. *Great Lakes Symposium on VLSI*, Tysons Corner, USA, May 2019, 237-242. https://doi.org/10.1145/3299874.3317994
- Aysu, A., Orshansky, M., Tiwari, M. (2018). Binary Ring-LWE hardware with power side-channel countermeasures, *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Dresden, 2018, 1253-1258.
- Aysu, A., Tobah, Y., Tiwari, M., Gerstlauer, A., Orshansky, M. (2018). Horizontal side-channel vulnerabilities of post-quantum key exchange protocols, *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, Washington, DC, 81-88.
- Aysu, A., Schaumont, P. (2016). Precomputation Methods for Hash-Based Signatures on Energy-Harvesting Platforms. *IEEE Transactions on Computers*, 65(9), 2925-2931.
- Aysu, A., Yuce, B., Schaumont, P. (2015). The Future of Real-Time Security: Latency-Optimized Lattice-Based Digital Signatures. *ACM Transactions on Embedded Computing Systems*, [online] 14(3), 43. https://doi.org/10.1145/2724714.
- Aysu, A., Patterson, C., Schaumont, P. (2013). Low-cost and area-efficient FPGA implementations of lattice-based cryptography, *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, Austin, TX, 81-86.

Personal Response

What do you envisage as the next key development in post-quantum secure encryption?

“There has been a barrage of algorithms for post-quantum secure encryption and they are fairly well developed. But the current state of implementations are far from mass deployment. The next key development, therefore, would be the outcome of NIST’s standardisation, which will allow cryptographic engineers to focus on the selected algorithm(s) among others and to implement them securely and efficiently on a wide-array of computing platforms.”