Can Aknesil

aknesil@kth.se github.com/canaknesil LinkedIn Extended CV



Hardware security researcher (PhD, KTH) working on power/EM and microarchitectural side-channel attacks, FPGA and GPU security, and LLVM-based countermeasures. Experienced in industry collaboration (Ericsson Research), teaching, and supervising students.

PROFESSIONAL EXPERIENCE

Postdoctoral Researcher *(June 2025 – Present)*
KTH Royal Institute of Technology, Stockholm
School of Electrical Engineering and Computer Science, Department of Network and Systems Engineering

- Combined attacks with power and microarchitectural side channels
- Detection and mitigation of microarchitectural side channels in LLVM
- Side channels on multi-tenant GPUs

Doctoral Researcher (PhD) *(March 2021 – June 2025)*
KTH Royal Institute of Technology, Stockholm
School of Electrical Engineering and Computer Science, Department of Electrical Engineering, Division of Electronics and Embedded Systems
Industry collaboration with Ericsson Research (hybrid fingerprinting, FPGA EM sensor, covert antennas)

- Side-channel fingerprinting of neural networks (Ericsson collaboration)
- Covert EM sensor and antenna implementations on FPGA (Ericsson collaboration)
- EM side-channel analysis on general-purpose computers (Raspberry Pi)
- Malicious-circuit detection in cloud FPGAs without IP disclosure
- Side-channel attacks on Xilinx Artix-7 FPGA bitstream encryption engine
- Bitstream extraction from SPI flash communication

Research Engineer *(June 2020 – January 2021)*
KTH Royal Institute of Technology, Stockholm
School of Electrical Engineering and Computer Science, Department of Electrical Engineering, Division of Electronics and Embedded Systems

- Deep learning-based power side-channel analysis of AES on FPGA
- Machine learning modeling attacks on Physically Unclonable Functions (PUFs)

Intern *(June 2019 – November 2019)*
Ericsson AB, Stockholm
High Performance Broadband/Radio Software Department

- Robust Header Compression (RoHC) for Profile 6 (TCP/IP)
- Interfacing C++ high-performance radio simulation libraries from Julia

Intern *(July 2017 – September 2017)*
CTech Bilişim Teknolojileri San. ve Tic. A.Ş., Istanbul
Hardware Department

- Embedded Linux development for millimeter wave wireless communication

Intern *(February 2017 – June 2017)*
Koç University, Istanbul
IT Department
Communication and Infrastructure Services

Intern *(July 2016 – August 2016)*
OBSS, Istanbul
Technology Department

- HR job advert & application management web application, in Java

OTHER PROJECTS

- FPGA implementation and statistical analysis of Arbiter PUF with 4x4 Switch Blocks *(MSc Embedded Systems thesis, under the supervision of Elena Dubrova)*
- Single-Event Upset Detector (SEUD) Experiment in the Miniature Student Satellite (MIST) *(MSc Embedded Systems final project)*
- CUDA Compilation Support for Snowflake DSL *(Computer Engineering Final Project)*
- MAM: A Memory Allocation Manager for GPUs, in C, compatible with C++ and CUDA *(ParCoreLab)*
- Limon: A simple and powerful general-purpose programming language *(Independent)*
- FPGA C++ Framework for FIR Filtering Applications *(Electrical & Electronics Engineering Final Project)*
- Go (board game, not the programming language) computer game in Rust *(Independent)*
- Cannon's matrix multiplication algorithm, in C, using MPI library *(Independent)*
- Unix-style operating system shell, in C, on Linux *(During undergraduate study)*
- Air traffic control simulator, in C++, using pthread.h library *(During undergraduate study)*
- Cache simulator, in C *(During undergraduate study)*
- Sound Transmission via Amplitude Modulation of Light, electronic circuit and simulation on PSpice *(During undergraduate study)*
- Digital clock, on FPGA board using VHDL *(During undergraduate study)*

PROFESSIONAL SKILLS

Hardware and computer security

- Power/EM side-channel attacks
- Microarchitectural side-channel attacks
- FPGA security
- GPU security
- Machine learning security
- Networking and network security
- Penetration testing

Hardware design

- FPGA design and verification with VHDL and SystemVerilog (using Xilinx Vivado and Intel/Altera Quartus)
- Tcl scripting in the Xilinx Vivado environment
- RTL synthesis with Yosys
- Analysis of digital circuits

Embedded systems design

- Embedded real-time platform and software development with Nios II soft-processor and MicroC/OS
- Embedded software development with Linux and baremetal in AVR, MIPS, ARM assembly, C, C++
- Fault-tolerant systems design

High-performance computing (HPC)

- Parallel programming with pthread library, MPI, and CUDA

Computer science

- C, C++, Rust, Java, Julia, Python, Matlab, Lisp, Haskell, Bash, PowerShell, Tcl
- Git, Subversion, GNU Make, CMake
- Software engineering
- Scientific programming
- Machine learning (supervised and unsupervised)
- Proficiency in Linux (daily use, system administration, driver and application development)
- Compiler and interpreter design with Lex, Yacc, LLVM, and PLY

Other

- PCB design using KiCad
- Mixed-signal IC design using Cadence Virtuoso
- Image analysis and computer vision
- Mobile application development for iOS (Objective-C) and Android (Java)
- Web development with HTML, JavaScript, CSS, PHP, Java EE, and Django
- Database design with SQL and MongoDB
- Electronic circuit simulation with PSpice and LTspice
- Emacs Lisp programming
- Amateur radio (SA0NCA)

EDUCATION

Doctoral Study in Information and Communication Technology *(2021 – 2025)*
KTH Royal Institute of Technology, Stockholm
School of Electrical Engineering and Computer Science
Specialization: Electronic Systems
Title: Protecting Remote FPGAs and Embedded Devices from Non-Invasive Physical Attacks
Supervisor: Prof. Elena Dubrova

Master of Science in Embedded Systems (Platform track) *(2018 – 2020)*
KTH Royal Institute of Technology, Stockholm
School of Electrical Engineering and Computer Science

Bachelor of Science in Electrical & Electronics Engineering *(2013 – 2018)*
Double Major in Computer Engineering
Koç University, Istanbul
College of Engineering
(25% Scholarship)
GPA: 3.44 / 4
Vehbi Koç Scholar in 2014 and 2016
Member of Koç University - Parallel and Multicore Computing Laboratory

High School *(2008 – 2013)*
Notre Dame de Sion French High School, Istanbul

PUBLICATIONS

Can Aknesil, Andreas Lindner, Roberto Guanciale, Hamed Nemati. "Spectre Without Dependent Load". Cryptology ePrint Archive, Paper 2026/806. 2026.

Can Aknesil. "Protecting Remote FPGAs and Embedded Devices from Non-Invasive Physical Attacks". Doctoral Thesis, Royal Institute of Technology (KTH), Stockholm, Sweden. 2025.

Can Aknesil, Elena Dubrova, Niklas Lindskog, Jakob Sternby, Håkan Englund. "Hybrid Fingerprinting for Effective Detection of Cloned Neural Networks". Cryptology ePrint Archive, Paper 2025/673. 2025.

Can Aknesil, Elena Dubrova, Niklas Lindskog, Jakob Sternby, Håkan Englund. "Hybrid Fingerprinting for Effective Detection of Cloned Neural Networks". 2025 IEEE 55th International Symposium on Multiple-Valued Logic (ISMVL). 2025.

Can Aknesil, Elena Dubrova. "Circuit Disguise: Detecting Malicious Circuits in Cloud FPGAs without IP Disclosure". 2024 27th Euromicro Conference on Digital System Design (DSD). 2024.

Can Aknesil, Elena Dubrova, Niklas Lindskog and Håkan Englund. "A Near-Field EM Sensor Implemented in FPGA Configurable Fabric". 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). 2023.

Can Aknesil, Elena Dubrova, Niklas Lindskog and Håkan Englund. "Is Your FPGA Transmitting Secrets: Covert Antennas from Interconnect". 2023 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW). 2023.

Can Aknesil and Elena Dubrova. "Towards Generic Power/EM Side-Channel Attacks: Memory Leakage on General-Purpose Computers". 2022 IFIP/IEEE 30th International Conference on Very Large Scale Integration (VLSI-SoC). 2022.

Can Aknesil and Elena Dubrova. "An FPGA Implementation of 4x4 Arbiter PUF". 2021 IEEE 51st International Symposium on Multiple-Valued Logic (ISMVL). 2021.

Can Aknesil. "An FPGA Implementation of Arbiter PUF with 4x4 Switch Blocks". Master's Thesis, Royal Institute of Technology (KTH), Stockholm, Sweden. 2020.

Can Aknesil and Didem Unat. "MAM: A Memory Allocation Manager for GPUs". 5. Ulusal Yüksek Başarımlı Hesaplama Konferansı, Istanbul, Turkey. September 2017.

TALKS (excluding presentations of my own research at conferences)

Invited Talk *(10 June 2026)*
Uppsala University, Uppsala, Sweden
Department of Electrical Engineering, Integrated Smart Systems Technology
Title: Side Channels with Can

Guest Lecture *(29 September 2025)*
KTH Royal Institute of Technology, Stockholm
Title: Physical Attacks & Hardware Trojans
Course: EP2780 Digital Forensics and Incident Response

ACADEMIC SERVICE

USENIX Security Program Committee member *(2027)*

TEACHING EXPERIENCE

Course Development
KTH Royal Institute of Technology, Stockholm
Developed the following lectures, associated laboratory exercises, and quizzes for EP2780 Digital Forensics and Incident Response, to be delivered in Fall 2026:

- Mobile Forensics
- Physical Attacks & Hardware Trojans

Lecturer *(Fall 2026)*
KTH Royal Institute of Technology, Stockholm

- EP2780 Digital Forensics and Incident Response *(Fall 2026)*

Teaching Assistant
KTH Royal Institute of Technology, Stockholm

- IL1333/FIL3030 Hardware Security *(during doctoral studies)*
- ID2218/FIL3200 Design of Fault-Tolerant Systems *(during doctoral studies)*
- IL2203 Digital Design and Hardware Description Languages *(during doctoral studies)*
- EP2780 Digital Forensics and Incident Response *(during postdoc)*

Undergraduate Teaching Assistant
Koç University, Istanbul

- Comp200 Structure and Interpretation of Computer Programs *(Fall 2017)*

Instructor *(20 – 30 June 2016)*
Stanford University & Koç University, Istanbul
CS Bridge Program

SUPERVISION EXPERIENCE

Master's Student Supervision
KTH Royal Institute of Technology, Stockholm

- Federico Mercurio. Enhanced RAN Security Test Planning Through LLM-Driven Test Selection and Structured RAG Workflows. *(Spring 2026)*
- Miguel Valgañón Soria. Reproducible and Relational Method for Detecting Constant-Time Violations in LLVM Optimization Passes. *(Spring 2026)*

Doctoral Student Supervision
KTH Royal Institute of Technology, Stockholm

- Siyao Liu *(Spring 2026)*
  (In addition to the main and co-supervisors)

PEDAGOGICAL TRAINING

KTH Royal Institute of Technology, Stockholm

- FLH3000 Basic Communication and Teaching, 3 credits
- LH207V Doctoral Supervision, 3 credits (ongoing)

LANGUAGE SKILLS

Turkish: Native

English: Professional

Swedish: Intermediate

French: Intermediate

AWARDS

- Vehbi Koç Scholar 2014, 2016
- International mathematical competition named "Le Kangourou des mathématiques", 22nd among 10627 participants, 2011

CONFERENCES & WORKSHOPS

- FPGAworld Conference in Stockholm. *(2026)*
- Challenges and Opportunities of PQC Deployment Workshop. *(2026)*
- IEEE 55th International Symposium on Multiple-Valued Logic (ISMVL). Presented a research paper. *(2025)*
- 27th Euromicro Conference Series on Digital System Design. Presented a research paper. *(2024)*
- Cybersecurity and Privacy (CySeP) Summer School. *(2024)*
- 30th Reconfigurable Architectures Workshop (RAW). Presented a research paper. *(2023)*

- 30th IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC). Presented a research paper. *(2022)*
- FPGAworld Conference in Stockholm. *(2022)*
- IEEE 51st International Symposium on Multiple-Valued Logic (ISMVL). Presented a research paper. *(2021)*
- Solid-State Circuits Directions Inaugural Workshop: Hardware Security. *(2020)*
- TECoSA Federated Learning Workshop. *(2020)*
- FPGAworld Conference in Stockholm. *(2019)*
- FPGAworld Conference in Stockholm. *(2018)*
- National High Performance Computing Conference (BAŞARIM) (Ulusal Yüksek Başarımlı Hesaplama Konferansı). Presented a research paper. *(2017)*
- Training named "Neuroscience for Leadership" at Kariyer.Net *(2017)*
- Training named "Idea Production Techniques" at Kariyer.Net *(2017)*
- Training named "Communication Mastery" at Kariyer.Net *(2017)*
- Training named "Personal Quality" at Kariyer.Net *(2017)*
- Training named "Sustainable Motivation" at Kariyer.Net *(2017)*
- Training named "Gamification" at Kariyer.Net *(2017)*

HOBBIES & OTHER INTERESTS

- Music: Piano, oud (a classical Turkish instrument), and guitar
- Summer sports: Sailing, windsurfing
- Tennis, table tennis, badminton
- Winter sports: Skiing, ice skating