Antoon Purnal *(Toon)*

PhD in Security. Pivots quickly. Enjoys public speaking.

toon.purnal@gmail.com | antoonpurnal.github.io | toonpurnal

Education

PhD, Electrical Engineering · **FWO Fellow** · **COSIC, KU Leuven**
Greatest distinction with congratulations of the jury *Oct. 2018 - Jun. 2023*
PhD Thesis: *Cache Side-Channel Attacks on Existing and Emerging Computing Platforms.*
Microarchitectural security research with several publications in flagship (A*) security venues.
Thesis student mentor, teaching assistant, ombudsperson.

MSc, Electrical Engineering · **KU Leuven**
Embedded systems · Greatest Distinction · MSc thesis prize *Sept. 2016 - Jun. 2018*
MSc Thesis: *Protecting* Keccak *against combined side-channel and fault attacks.*
Student teaching for EM Waves, Calculus III, Problem Solving.

Selected Publications

USENIX SEC '22 *Double Trouble: Combined Heterogeneous Attacks on Non-inclusive Cache Hierarchies*
AR: 18% (**Antoon Purnal**, Furkan Turan, Ingrid Verbauwhede)

ACM CCS '21 *Prime+Scope: Overcoming the Observer Effect for High-Precision Cache Contention Attacks*
AR: 22% (**Antoon Purnal**, Furkan Turan, Ingrid Verbauwhede)

IEEE S&P '21 *Systematic Analysis of Randomization-based Protected Cache Architectures*
AR: 12% (**Antoon Purnal**, Lukas Giner, Daniel Gruss, Ingrid Verbauwhede)

Experience

Senior Product Security Analyst
PQShield *Aug. 2023 - PRESENT*
I am responsible for the implementation security testing of PQShield's software and hardware post-quantum cryptography IP, with a focus on timing side-channel analysis and fuzzing.

Public-facing: I discovered **clangover**, an exploitable compiler-introduced timing leak in ML-KEM implementations, affecting several high-profile open-source libraries.

CVE-2024-37880 **CVE-2024-36405** **blog** **code** **outreach**

Security Research Intern
Intel Corporation *Jun. 2022 - Aug. 2022*
I joined the forward-looking Intel Labs for microarchitectural hardware security research.

Student Researcher
National Chiao Tung University (NCTU), Taiwan *Jul. 2017 - Aug. 2017*
I designed real-time and low-power cryptographic hardware, with tape-out in TSMC 90nm.

Skills

Programming	Software: **C, Python, Rust, Assembly (arm/x86/RISC-V)**	Hardware: **VHDL, Verilog**
	Enablers: **Linux, Git, Docker, CI/CD, Fuzzing, LaTeX, llm**	
Languages	Proficient: **Dutch, English**	Intermediate: **Spanish, French**
Miscellaneous	Rump Session Award at CHES 2022, 2023 & 2024. Former lead guitarist in local band and university big band.	