Robin **Carpentier**

Research Fellow · Security & Privacy
Sydney, Australia
(+61) 415 255 213 | robin.carpentier@use.startmail.com | https://carpentier.page | robincarpentier

Summary

Cybersecurity researcher specializing in trusted execution environments (Intel SGX/TDX) and privacy-preserving system design. Experienced in secure systems engineering, threat modeling, and applied machine learning for privacy-sensitive applications. Proven ability to translate research into practical, industry-ready solutions.

Work Experience

Macquarie University — Sydney, Australia

Research Fellow — Dec 2023 - Present

- Designed a system to reduce the monetary cost of privacy-preserving LLM prompts in a company setting, lowering API costs by 20% while maintaining output quality. Implemented an open-source Python prototype evaluated on self-hosted and proprietary models via API.
- Identified and exploited a flaw in a widely cited differential privacy method for text sanitization, demonstrating a trade-off where privacy and utility fails. Implemented both the attack and a countermeasure in Python.
- Co-developed a phone scam prevention system using LLM-based scam baiting, applying game-theoretic principles to improve baiting capabilities through in-context learning, reducing operational cost over fine-tuning.
- Managed shared research computing resources, including model hosting and experimentation infrastructure.

Inria & Paris-Saclay University — Versailles, France

Researcher (PhD & Postdoctoral) — Oct 2018 - May 2023

- Designed and analyzed privacy-preserving data processing systems using trusted execution environments (Intel SGX) in personal cloud scenarios.
- Developed a secure execution model enabling data analytics over sensitive datasets processed by adversarial code.
- Devised multi-enclave execution strategies to balance privacy guarantees and system performance.
- Co-developed an experimental prototype in C++ with OpenEnclave and conducted performance evaluations on real SGX hardware.

Inria — Versailles, France

Research Intern — Apr 2018 - Sep 2018

- Conducted an in-depth performance and security analysis of Intel SGX for data-intensive workloads in a personal cloud setting.
- Benchmarked and optimized data-processing algorithms under Intel SGX constraints, identifying EPC memory, sealing, and paging as key performance bottlenecks.
- Designed C/C++ prototypes and proposed algorithmic and data-structure adaptations to balance security guarantees and performance.

Education

Paris-Saclay University — Versailles, France

Doctor of Philosophy (PhD) in Computer Science — Oct 2018 - Dec 2022

Paris-Saclay University — Versailles, France

Master of Science (MSc) in Cybersecurity — Sep 2016 - Sep 2018

- End-to-end cybersecurity: cryptography, network and system security, secure software development, and intrusion detection.

Selected Publications

Preempting Text Sanitization Utility in Resource-Constrained Privacy-Preserving LLM Interactions
Robin Carpentier, Benjamin Zi Hao Zhao, Hassan Jameel Asghar, Dali Kaafar
Under Review

d_X-Privacy for Text and the Curse of Dimensionality
Hassan Jameel Asghar, Robin Carpentier, Benjamin Zi Hao Zhao, Dali Kaafar
Proceedings on Privacy Enhancing Technologies (PoPETS), 2026

Enabling Secure Data-Driven Applications: An Approach to Personal Data Management using TEEs
Robin Carpentier, Iulian Sandu Popa, Nicolas Anciaux
Distributed and Parallel Databases (DAPD), 2025

An Extensive and Secure Personal Data Management System Using SGX
Robin Carpentier, Floris Thiant, Iulian Sandu Popa, Nicolas Anciaux, Luc Bouganim
EDBT, 2022