Tancrède Lepoint

Principal Applied Scientist | Security Research & Engineering

tancrede.lepoint@gmail.com | tancre.de | LinkedIn | GitHub

Profile

I lead security research and engineering across AI systems, cryptography, and privacy. Over 15+ years, I have connected rigorous research with production systems, working across research, engineering, security, and legal teams.

Selected impact

- **Post-quantum standards:** Co-designed CRYSTALS-Kyber and CRYSTALS-Dilithium, standardized by NIST as ML-KEM (FIPS 203) and ML-DSA (FIPS 204) in 2024.
- **Privacy-preserving technologies:** Deployed private information retrieval, secure aggregation, anonymous credentials, and verified differential privacy in industry.

Experience

Amazon Web Services 2025-present
Principal Applied Scientist, AI Security

- Lead technical and scientific work on AI security, including testing and debugging agentic AI applications, securing agentic systems, and neurosymbolic approaches.
- Work on data protection for AI, including differentially private synthetic data generation.

Amazon Web Services 2022-2025
Principal Applied Scientist, Provable Security & Automation

- Led technical and scientific work on security, privacy, and compliance automation, using automated reasoning and data-protection techniques.
- Contributed to formally verified differential privacy technologies deployed in AWS Clean Rooms; PLDI 2025 Distinguished Artifact award.

Apple 2021-2022
Cryptographic Engineer, Cryptography Engineering

- Worked on Exposure Notifications, post-quantum cryptography for iCloud and Apple corecrypto, and homomorphic encryption for private information retrieval.

Google 2018-2021
Senior Research Scientist, Private Computing

- Built production privacy infrastructure spanning homomorphic encryption, private set membership, secure aggregation, and anonymous credentials.
- Contributed to Exposure Notifications Privacy-preserving Analytics and the open-source shell-encryption library.

SRI International 2016-2018
Senior Computer Scientist

- Led DARPA-funded privacy-preserving computation research, including the Brandeis program; co-designed CRYSTALS-Kyber and CRYSTALS-Dilithium.

CryptoExperts 2011-2016
Junior Security Expert

- Co-designed the BLISS lattice-based signature scheme; designed and implemented fully homomorphic encryption schemes.

Selected research

Co-authored work; full author lists and publications at tancre.de/publications/.

Delta Debugging for LLM-integrated Systems ICSE-SEIP 2026

Uses semantic markers and delta debugging to reduce complex inputs to the segments associated with an LLM application's failure.

The Question Is a Region NeSy 2026

Combines language models, symbolic execution, and verification to handle under-specified questions over rule engines.

Verified Foundations for Differential Privacy PLDI 2025

Machine-checked foundations for differential privacy. Deployed in AWS Clean Rooms Differential Privacy. **Distinguished Artifact award.**

CRYSTALS-Kyber & CRYSTALS-Dilithium 2018; NIST standards 2024

Lattice-based key encapsulation and digital signatures, forming the basis of ML-KEM and ML-DSA.

Communication-Computation Trade-offs in PIR USENIX Security 2021

Practical homomorphic-encryption protocols for private database queries, with deployments by Google and Apple.

Secure Single-Server Aggregation with (Poly)logarithmic Overhead CCS 2020

Secure aggregation for privacy-preserving machine learning; deployed by Google for federated learning with distributed differential privacy.

Technical leadership & community

- **IACR Board of Directors:** IT Manager (2026-present); Director (2018-2024).
- **CRYPTO 2024:** General Chair.
- **Cryptology ePrint Archive:** Co-editor (2016-2023).
- **Callisto:** Cryptography Advisory Board (2018-2021).

Open source

fhe.rs — Fully homomorphic encryption library in pure Rust, implementing BFV.
shell-encryption — Contributed to Google's RLWE-based homomorphic encryption library.

Education & recognition

Ph.D. in Computer Science 2011-2014
École Normale Supérieure & University of Luxembourg. Industrial doctorate at CryptoExperts.
Thesis: Design and Implementation of Lattice-Based Cryptography.
Advisors: Jean-Sébastien Coron and David Pointcheval.

- **Gilles Kahn Dissertation Award**, 2014.
- **Best Paper**, Asiacrypt 2015, for improved security proofs using Rényi divergence.
- **Best Paper**, Eurocrypt 2021, for *On the (in)Security of ROS*.
- **Distinguished Artifact**, PLDI 2025, for verified differential privacy.