"Kevin Gni"

great engineer, great researcher, great coworker, and great laugh

git.loqyu.com | loqyu.com | bin.ni@cispa.de

Education

CISPA Helmholtz Center for Information Security & Universität des Saarlandes

MSc. in Computer Science; thesis ongoing; Conversational German; GPA 1.3 — *Apr 2023 - now*

New York University

BSc. in Computer Science; BSc. in Interactive Media Arts; GPA 3.84; English C2 — *Sep 2014 - May 2018*

Major Research and Professional Experience

Research Assistant (HiWi) — Nov 2023 - now

With Dr. Wouter Lueks at CISPA Helmholtz Center for Information Security

- Implementation of comprehensive cryptographic systems & applications in `Rust/C/C#/Kotlin/Python/Java`
- Traffic analysis & censorship resistance, especially application layer ones (e.g., ALPACA, TrafficSilver, etc. ⇒ *see thesis*)
- Anonymous payment systems based on compact e-cash schemes (e.g., Pointcheval's family of divisible e-cash schemes) for real-life use cases (e.g., humanitarian missions with ICRC)
- Security application based on TEE, such as secure payment systems using oblivious RAM
- Supporting the course *Privacy-Enhancing Technologies*: subjects include secure multi-party computation, private information retrieval, anonymous credentials, homomorphic encryption, differential privacy, etc.

Payment Engineer — Nov 2019 - Oct 2022

Thales China, Shanghai

- Customizing secure card payment solutions based on payment processor standards (e.g., VISA, Master, JCB, etc.) for various banks to support particular features
- Implementing cryptographic and operational routines on specific smartcards
- Supporting, incorporating and deploying secure data processing facilities on premise: for secure exchange and storage of client data, secure key management, and data protection law compliance, etc.

Research Associate & Teaching Assistant — Early 2018 - mid 2022

With Prof. Olivier Marin on reliable distributed systems & operating systems

- Comparative study of ML-driven failure detection algorithm with conventional ones on efficiency and accuracy
- Implementing and benchmarking a distributed/cloud-tailored database for geospatial data based on GeoTrie
- Task orchestration and management on in-house and commercial HPC

Relevant skills

Extensive and diverse software engineering experience w/ secure software systems

* 15+ years of coding, extensive experience with a wide range of technology stacks & tools, high & low level => `C/Assembly (x86/ARM); C++; Rust; C#/WPF/ASP.NET/COM; Python; Scala; Kotlin/Java/Android; Java/Typescript; Golang; Git; Gitlab CI/CD; GitHub Actions; Docker/Kubernetes; SQL(ite).`
* Hands-on and in-depth understanding of modern computer & OS architecture
* 5+ years of experience developing and incorporating security and cryptographic features into applications (esp. for financing institutions) => `ECDSA/RSA/AES/DES/DH; HSM/KMS; PKI; Anonymous credentials; e-Cash; Wireguard/Shadowsocks; OWASP; SDLC; VISA/Mastercard; Banking data processing & storage compliance.`
* Solid experience with low-level programming in C/Rust with security & cryptographic facilities
* Experience working with AI-assisted & agent-based automations/workflows
* Extensive experience & charm working in an international setting: made in NYC™ & Shanghai

Extensive research + engineering esp. in cyber security & privacy

* **Thesis**: *Chamade: An Application Layer Framework Against Traffic Analysis for Mobile Platforms*, advised by Dr. Wouter Lueks, CISPA => `Traffic analysis; Rust/Kotlin/Android; ML; Signal processing; HTTP(/2), TLS, TCP/IP; CDN.`
* **Paper**: *CrossLink: Breaking Location Privacy by Linking Device Identifiers Across Protocols*, with Aneet Dutta et al., CISPA; ACM CCS 2026. => `LTE/BLE/802.11; Triangulation; Traffic simulation; Rust/Python.`
* **Paper**: *Wall-e: Smartphone-Based Digital Wallet for Humanitarian Aid Distribution*, with David Pulio et al., CISPA => `ZKP (Groth-Sahai, Schnorr); Anonymous credentials; Pairing-based crypto (BLS12-381); e-Cash (Pointcheval); AEAD (AES-GCM); NFC wallet; HEC; Rust/Kotlin/Android.`
* **Paper**: *A Low-Cost Privacy-Preserving Digital Wallet for Humanitarian Aid Distribution*, with Luvison et al., CISPA; IEEE S&P 2025. => `Oblivious RAM; PIR; Oblivious transfer; Smartcard (GlobalPlatform); Java.`
* Experience with other cryptographic, security and privacy fields => `Tor/Onion routing; Blockchain; ZKP; e-Cash; ANC; SMC; Differential privacy; Side-channel attacks; Database injection; Web application security; Reverse engineering; Fuzzing; Virtualization.`