Kris Kwiatkowski

Cryptography Engineer

Legal name:	Krzysztof Kwiatkowski
Current place of residence:	London, UK
Telephone:	+44 7759 654328
e-mail:	contact@amongbytes.com
LinkedIn profile:	https://www.linkedin.com/in/krzysiekkwiatkowski
Blog:	https://amongbytes.com

Professional objectives

Cryptography Software Engineer with 20 years of experience designing high-performance, certified cryptographic solutions — from embedded post-quantum libraries to internet-scale TLS deployments. Focused on secure, efficient, and standards-compliant cryptographic software. Active contributor to standardization efforts through the IETF, with hands-on experience across x86 and ARM platforms. A lifelong learner who thrives on mastering new technologies and collaborating with experts to push the boundaries of applied cryptography.

Technical Profile

- Cryptographic implementations
- Post-quantum cryptography
- High-performance cryptography
- Side-channel resistant implementations
- Cryptography for embedded systems
- Network security protocols

Summary of qualifications

Cryptography	Post-Quantum cryptography (ML-KEM, ML-DSA, SLH-DSA, LMS), ECC, Key Exchange Protocols, Digital Signatures, TLS, X.509, PKI
Languages	C++ (very good), C (very good), Go (proficient), Rust (initial), Python (proficient), ASM (x86 & ARM)
Security	Constant-time Programming, Secure Coding Practices, Software Security
Security Standards	FIPS 140-3 (CAVP testing, CMVP validation); IETF Cryptographic Standards (TLS, LAMPS, SUIT)
Embedded Systems	ARM Cortex-M, low-level peripheral access, memory-constrained environments
Testing & Evaluation	Unit Testing, Performance Benchmarking, Static Analysis, Fuzzing, ACVP
Natural Languages	Polish (native), English (fluent)

Education

2001 - 2006 **Poznan University of Technology**, Poznań, Poland
MSc in Mathematics
Completed three years of pure mathematics before specializing in mathematical methods for computer science in the final two years.
Master's thesis: Computational complexity of number-theoretic algorithms using the RSA public-key cipher as a case study.

2006 - 2007 **AGH University of Science and Technology**, Kraków, Poland
Software Engineering
Postgraduate studies focusing on software engineering and project management in IT. Focused on modern software engineering methodologies, IT project management, and practical aspects of software development lifecycle, including requirements analysis, architecture, and team collaboration.

Employment History

Jun 2019 - current

PQShield, Oxford, UK

Developing post-quantum cryptographic solutions for embedded systems, secure protocols, and certification standards. Founding engineer collaborating directly with the CEO to deliver PQShield's core post-quantum cryptographic libraries and certification roadmap.

Staff Cryptography Architect **Jun 2022 - Current**

Design and implementation of post-quantum cryptographic solutions. Focusing on both greenfield post-quantum cryptographic schemes as well as production grade, FIPS 140-3 certified cryptographic libraries.

- Led the full FIPS 140-3 Level 1 certification lifecycle for company's first FIPS-certified product - from initial development and documentation to successful submission and approval (Certificate #4800), ensuring compliance with U.S. federal cryptographic standards.
- Designed and implemented PQCryptoLib Embedded, a lightweight, CAVP-compliant cryptographic library for ARM Cortex-M microcontrollers optimized for memory-constrained platforms such as IoT and industrial systems.
- Architected a hardware/software co-design for LMS and XMSS, leveraging external hash engines to enhance performance and side-channel resistance in embedded environments.
- Collaborated with industry partners to drive adoption of post-quantum standards in real-world applications.

Senior Cryptography Engineer **Apr 2020 – Jun 2022**

Design and development of PQCryptoLib, a software cryptographic library supporting multi-precision arithmetic, elliptic curve cryptography, and post-quantum key exchange schemes.

- Implemented and optimized post-quantum algorithms, including Kyber and Dilithium, as well as elliptic curve–based cryptographic schemes.
- Applied SIMD acceleration techniques (AVX2 and NEON) to enhance performance.
- Contributed to research by implementing experimental post-quantum schemes for integration into the Signal protocol. Work has been accepted by two main cryptologic conferences - Asiacrypt2020 and PKC2021.

Cryptography Engineer **Dec 2019 – Apr 2020**

Implementation of post-quantum cryptographic algorithms and integration into existing protocols. As founding engineer collaborating directly with the CEO to deliver PQShield's core post-quantum cryptographic libraries and certification roadmap.

- Designed and developed an OpenSSL plugin to integrate post-quantum schemes into the TLS stack, supporting experimentation and deployment.
- Led the Post-Quantum VPN project (see PQVPN in Selected Projects).

Mar 2017 - current

Among Bytes LTD, London, UK

Self-employed cryptography consultant and software engineer.

- Delivering expert advisory services in IETF standardization, security engineering, internet technologies, communication systems, and FIPS certification processes for cryptographic products.
- Experienced in leveraging and tailoring open-source software to meet specific client requirements, ensuring practical and effective solutions.

Feb 2018 - Dec 2019

Cloudflare, London, UK

Deployed post-quantum TLS (CECPQ2) at scale and co-authored Cloudflare's cryptographic library.

- Co-authored CIRCL, Cloudflare's high-performance, Go-based cryptographic library.
- As a Cryptography Engineer in Cloudflare's Research team, deployed Post-Quantum Cryptography (PQC) in TLS on production servers using BoringSSL, collaborating with Google to drive adoption through CECPQ2. This work informed ongoing experimentation published on Cloudflare's blog.
- Contributed to implementing and optimising TLS 1.3.

May 2015 - Jan 2018

Trustonic, Cambridge, UK
Implementing the Trusted Execution Environment (TEE) based on ARM TrustZone technology.

Security Engineer **Oct 2016 - Jan 2018**

- Implemented cryptography for the Trusted Execution Environment (TEE) based on ARM TrustZone technology.
- Developed cryptographic APIs and validated secure components for ARM TrustZone-based Trusted Execution Environments. Delivered certified GlobalPlatform-compliant crypto stack deployed across millions of Android devices.

Security Validation Engineer **May 2015 - Oct 2016**

- Focused on performing security validation of cryptographic implementations targeting ARMv8 platforms within the TEE.
- Provided Trusted Execution Environment (TEE) based system authentication for Android devices (Gatekeeper).

Jun 2008 - May 2015

Amadeus, Sophia Antipolis, France
Focused on TLS security, system resilience, and performance optimization in distributed backends for the Global Distribution System (GDS).

- Responsible for the design, implementation, and maintenance of various functionalities within the C++-based security and communication framework of the Amadeus core system, with a primary focus on failure-resilient architecture, performance optimization, and the security and stability of TLS connections.
- Improved performance in a backend performing low-latency operations by modifying memory allocation strategy. Overall CPU consumption was reduced by ~20%, which reduced running costs as the backend was composed of a few hundred processes distributed over a server farm.

Jan 2007 - May 2008

Tieto, Wrocław, Poland
Largest Nordic IT services provider. Managing teams developing PC software tools for Nokia/Symbian based mobile phones.

- Progressed from Software Engineer to Manager, leading the development of PC software tools for Nokia/Symbian-based mobile phones supporting features such as firmware flashing, data backup and restore, and service-level recovery.
- Successfully built and managed a distributed team of 20 developers and testers across Poland, the Czech Republic, and China, delivering multiple software projects for Nokia.

Dec 2005 - Jan 2007

BenQ-Siemens, Wrocław, Poland
Producer of consumer electronics, computing and communication products. C/C++ software developer. Member of a team that was developing diagnostic and recovery toolset for embedded, Qualcomm based mobile phone platform. Those tools were used for the design of the mobile phone platform by the BenQ/Siemens research centres.

Selected Projects

- **PQCryptoLib and PQMicroLib:** Designed and implemented two post-quantum cryptographic libraries - PQCryptoLib and PQMicroLib - providing CNSA 2.0–compliant key exchange for TLS 1.3 and similar protocols and optimized implementations for memory-constrained IoT platforms. Responsible for software implementations, performance and memory optimizations across architectures, and security hardening against side-channel attacks.
- **Post-Quantum TLS (CECPQ2):** Deployed CECPQ2 on Cloudflare production servers in collaboration with Google. Authored an IETF draft standardizing hybrid ECDHE+ML-KEM key exchange for TLS 1.3 (draft-ietf-tls-ecdhe-mlkem) - now implemented by major browsers (Chrome, Firefox) and cloud providers (Google, Cloudflare, AWS).
- **CIRCL (Cloudflare):** Co-authored CIRCL, Cloudflare's high-performance cryptographic library written in Go, supporting post-quantum and elliptic-curve primitives.
- **TEE Crypto Stack (Trustonic):** Developed cryptographic APIs for ARM TrustZone–based Trusted Execution Environments (TEEs), compliant with GlobalPlatform standards. Deployed across millions of Android devices.

Publications

- **On the Expected Number of Iterations in ML-DSA Signing**
  K. Kwiatkowski — Oct 2026
- **RFC 10024: Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3**
  P. Kampanakis, K. Kwiatkowski, D. Stebila, B. E. Westerbaan — Aug 2026
- **Scalable Ciphertext Compression Techniques for Post-Quantum KEMs with Applications**
  Shuichi Katsumata, Kris Kwiatkowski, Federico Pintore, Thomas Prest — Dec 2020

Courses and Certifications

Stanford University (Coursera)	Cryptography
	Algorithms: Design and Analysis
University of Maryland (Coursera)	Cryptography
	Computer Networks
Linux Foundation	Linux kernel internals (LFD 320)
	Linux Performance tuning (LFS 426)
Jean-Paul Rigault (C++ committee member)	Design Patterns
	Generic programming and Boost library
	Multithreading
IKM	97% in C++ test