DR. CAROLIN GEOMETRIE-PRIES

SENIOR KRYPTOGRAPHIE-REFERENTIN BSI (DR. RER. NAT.)

CONTACT

carolin.pries@example.de

+49 228 9582 1207

Bonn, Deutschland

carolin-pries.crypto

linkedin.com/in/carolin-pries-crypto

iacr.org/cryptodb/data/author.php?authorkey=pries

PROFIL

Kryptographie-Spezialistin beim Bundesamt fuer Sicherheit in der Informationstechnik (BSI) Bonn mit M.Sc. Mathematik (HU Berlin) und Promotion in algebraischer Zahlentheorie (Universitaet Bonn). 5 Jahre Erfahrung in Post-Quantum-Migration, Bewertung kryptographischer Verfahren nach BSI TR-02102 und Co-Autorenschaft an 3 BSI-Technischen-Richtlinien. Teilnahme als deutsche Delegierte am NIST PQC Standardization Process.

AUSBILDUNG

Promotion Dr. rer. nat. Mathematik

10/2017 - 09/2020

Universitaet Bonn Mathematisches Institut

Bonn, Deutschland

Algebraische Zahlentheorie / Iwasawa-Theorie

summa cum laude (1,0)

M.Sc. Mathematik

10/2015 - 09/2017

Humboldt-Universitaet zu Berlin (HU Berlin)

Berlin, Deutschland

Mathematik (Schwerpunkt Algebra, Zahlentheorie)

1,1

BERUFSERFAHRUNG

Senior Kryptographie-Referentin (Referat S 21) 10/2022 - heute

Bundesanstalt fuer Finanzdienstleistungsaufsicht BaFin Bonn/Frankfurt

Bonn, Deutschland

Senior Kryptographie-Referentin beim BSI Referat S 21 Krypto-Mechanismen und Verfahren (parallel mit BaFin-Kooperation TR-Bewertung)

- Co-Lead der BSI-PQC-Migrations-Roadmap fuer 38 Bundesbehoerden, Aufwand 124 Mio. EUR, Migration auf ML-KEM und ML-DSA
- Co-Autor von 3 BSI-Technischen-Richtlinien (TR-02102-1, TR-02102-2, TR-03116) zu kryptographischen Empfehlungen
- Mathematische Bewertung von 14 kryptographischen Verfahren im Rahmen von Common-Criteria-Zertifizierungen EAL4+
- Vertretung Deutschlands im NIST PQC Standardization Round 4 sowie in ISO/IEC JTC 1/SC 27
- Vortrag CHES 2024 Halifax zur Side-Channel-Analyse von ML-KEM ARM-Cortex-M4

Postdoc Cryptography 10/2020 - 09/2022

Max-Planck-Institut fuer Mathematik Bonn Bonn, Deutschland

Postdoc-Stelle Forschungsgruppe Algebraische Zahlentheorie mit Kryptographie-Fokus

- Hauptautorin von 4 Publikationen in IEEE Transactions on Information Theory und Journal of Cryptology
- Co-Autorin der ersten quantum-sicheren Variante einer pairing-basierten Signatur, eingereicht im NIST-PQC-Standardisierungsverfahren
- Lehrauftrag Universitaet Bonn, Master-Vorlesung 'Mathematische Kryptographie' fuer 2 Semester
- Mentoring von 2 Doktoranden, beide mit Erstautoren-Papern in IACR-Konferenzen

B.Sc. Mathematik

10/2012 - 09/2015

Universitaet Goettingen
Georg-August-Universitaet
Goettingen, Deutschland

Mathematik mit Nebenfach Informatik

GPA: 1,2

FÄHIGKEITEN

- Algebraische Zahlentheorie
- Post-Quantum Cryptography
- Lattice-Based Cryptography
- C/C++ & Constant-Time Code
- Python (SageMath, PARI/GP)
- Magma & Mathematica
- BSI TR-Compliance & Common Criteria
- Side-Channel-Analyse

ZERTIFIKATE

CISSP Certified Information Systems Security Professional

11/2024

BSI Pruefer fuer Common Criteria EAL4+ Zertifizierungen

06/2023

Otto-Hahn-Medaille der Max-Planck-Gesellschaft

10/2020

PROJEKTE

BSI Post-Quantum-Migrations-Roadmap fuer Bundesbehoerden

10/2024 - heute

Co-Lead der Migrationsstrategie 38 Bundesbehoerden, Aufwand 124 Mio. EUR, Zielarchitektur ML-KEM + ML-DSA

Side-Channel-Analyse von ML-KEM auf ARM-Cortex-M4

06/2024 - 12/2024

Wissenschaftliche Untersuchung der Constant-Time-Implementierungen, Vortrag CHES 2024 Halifax

PUBLIKATIONEN

07/2024

Pries, C. (2024): Lattice-based signature schemes with tight quantum security proofs

11/2023

Pries, C. et al. (2023): Side-channel attacks on lattice-based KEMs - vulnerabilities and countermeasures

International Mathematical Olympiad (IMO) Silbermedaille

06/2013

SPRACHEN

Deutsch	Muttersprache
Englisch	C1
Russisch	B2

STÄRKEN

Mathematisch-Kryptographische Tiefe

Promotion in algebraischer Zahlentheorie ermoeglicht die unabhaengige mathematische Bewertung kryptographischer Verfahren ohne Vendor-Abhaengigkeit

Behoerden-Reife

Sicherer Umgang mit BSI-Schutzbedarfs-Analyse, Common Criteria, TR-Compliance und Vorbehalt-Erstellung

Internationale Standardisierung

Aktive Teilnahme an NIST PQC Standardization (Round 4 / FIPS 203/204), ENISA und ISO/IEC SC 27 als deutsche Vertreterin