Nadim Kobeissi

Contact Information

25 Avenue de la Division Leclerc
92290 Châtenay-Malabry, France

E-mail: n@nadim.email
WWW: https://nadim.computer

Personal Information

Date of birth: September 1990. French and Lebanese dual citizenship. Fluent in English, French and Arabic.

Research Interests

Applied cryptography, symbolic protocol modeling, formal verification, web security, verifiably secure protocol implementation, secure messaging.

Education

Inria, Paris, France
Accredited by École Normale Supérieure, Paris

Ph.D. Computer Science, December 2018

- Dissertation Topic: *"Formal Verification for Real-World Cryptographic Protocols and Implementations"*
- Thesis Advisors: Karthikeyan Bhargavan, Bruno Blanchet

Concordia University, Montréal, Canada

B.A. Philosophy, May 2013

- Courses in Computer Science
- Participation in open source software projects

Academic Experience

Proceedings on Privacy Enhancing Technologies Symposium
Program Committee, Editorial Board **2024**
Guest Reviewer **2017 – 2023**

International Conference on Cryptology and Information Security in Latin America (IACR Latincrypt)
Program Committee **2023**

Conference for Failed Approaches and Insightful Losses in Cryptology
Program Committee **2023**

New York University, Paris, France
Adjunct Professor **2018 – 2019**
https://nadimkobeissi.github.io/nyu-paris-cs/

IEEE European Symposium on Security and Privacy
Organizing Committee Member **2017 – 2018**

Conservatoire National des Arts et Métiers, Paris, France
Lecturer **2015 – 2017**

Professional Experience

Cure53, https://cure53.de
Senior Applied Cryptography Auditor **2024 – Present**
After a three-year career shift towards working in startups, I returned as a full time senior applied cryptography auditor at Cure53 (see previous career experience entry for context). Working on auditing deeply critical real-world cryptographic systems, which I wish I could say more about if it weren't for NDAs.

Symbolic Software, https://symbolic.software
Director **2017 – Present**
Software publisher and boutique applied cryptography consultancy based in Paris. Has participated in over 250 software security audits and has published research software for applied cryptographers. Also publishes small indie video game projects.

Polygon Technologies, https://polygon.technology
Prover Developer **2023**
Contributing to the Polygon zero-knowledge EVM research and development. Implemented SHA256 support into the zkEVM prover C++ codebase. Largest single contributor to the Polygon Knowledge Layer, which was built and launched during my tenure.

Capsule Social, https://capsule.social
Founder, Research Lead **2021 – 2023**
Led the development and launch of Blogchain, a decentralized writing and publishing platform with high quality content on Web3 with best-in-class user experience. Built on top of IPFS and NEAR protocol. Hired and led a team of 15+ full-time employees. Successfully led a multi-million-dollar financing round. Acquired by Nym Technologies SA.

Cure53, https://cure53.de
Applied Cryptography Auditor **2017 – 2021**
As part of an extended partnership between Cure53 and Symbolic Software, participated in over 150 audits for critical applied cryptography software components of companies, startups as well as the public sector around the world. Identified hundreds of security vulnerabilities including many critical vulnerabilities.

Microsoft Research, Cambridge, United Kingdom
Research Intern **2016**
Participated in the development of formal verification techniques for smart contracts and formally verified parsers for X.509 certificates in F⋆, both of which led to peer-reviewed academic publications.

Software Projects

Verifpal, https://verifpal.com
New software for verifying the security of cryptographic protocols. Building upon contemporary research in symbolic formal verification, Verifpal's main aim is to appeal more to real-world practitioners, students and engineers without sacrificing comprehensive formal verification features. Used by Google, Zoom, Bosch and others. Led to peer-reviewed academic publication.

Noise Explorer, https://noiseexplorer.com
Online engine for designing, reasoning about, formally verifying and implementing arbitrary Noise Handshake Patterns. Based on our formal treatment of the Noise Protocol Framework, Noise Explorer can validate any Noise Handshake Pattern and then translate it into a model ready for automated verification and also into a production-ready software implementation written in Go or in Rust. Led to peer-reviewed academic publication.

Dr. Kobushi's Labyrinthine Laboratory, https://drkobushi.com
Ambitious indie puzzle adventure video game project. Conceived, designed, programmed and directed game, which features over 100 levels, story, dialog, and innovative gameplay. Led a team of five people, including a pixel artist, musician and sound designer. Published on Steam and Nintendo Switch. Overwhelmingly positive press reviews. Only the third ever commercial video game to be written in the Go programming language.

Runes of Ardun, https://runesofardun.app
Reimagining of the ancient Japanese strategy game Mini Shogi, transforming it into a strategic duel of wits and cunning on iPhone, iPad, Mac and Android. Includes original Shogi AI written from scratch in Rust, which plays at a competitive 2200 Elo rating. Featured in Apple's

New Games We Love. Top 10 Board Game in the Japan, France Switzerland and 20 other countries' App Stores in February 2024.

Piccolo: Othello, https://piccolo.click
Othello software for macOS and iOS written in Rust and Swift. Featured in Apple's *What We're Playing*, *Games We Love*, and *Best Games Made in France*. #1 top overall game in the Japan Mac App Store from April to July 2021.

Selected Publications

Verifpal: Cryptographic Protocol Analysis for the Real World (with G. Nicolas, M. Tiwari), 21st International Conference on Cryptology in India, 2020

EverParse: Verified Secure Zero-Copy Parsers for Authenticated Message Formats (with A. Delignat-Lavaud, C. Fournet, T. Ramananandro, N. Swamy, T. Chahed), 28th USENIX Security Symposium, 2019

Noise Explorer: Fully Automated Modeling and Verification for Arbitrary Noise Protocols (with G. Nicolas, K. Bhargavan), 4th IEEE European Symposium on Security and Privacy, 2019

Ledger Design Language: Designing and Deploying Formally Verified Public Ledgers (with N. Kulatova) in 3rd IEEE European Symposium on Security and Privacy – Workshop on Security Protocol Implementations, 2018

Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate (with K. Bhargavan, B. Blanchet), 38th IEEE Symposium on Security and Privacy, 2017

Formal Modeling and Verification for Domain Validation and ACME (with K. Bhargavan, A. Delignat-Lavaud), Financial Cryptography and Data Security, 2017

Automated Verification for Secure Messaging Protocols and their Implementations: A Symbolic and Computational Approach (with K. Bhargavan, B. Blanchet), 2nd IEEE European Symposium on Security and Privacy, 2017

Formal Verification of Smart Contracts (with K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier, A. Rastogi, T. Sibut-Pinote, N. Swamy, S. Zanella-Bèguelin), 11th ACM SIGPLAN Workshop on Programming Languages and Analysis for Security, 2016

FlexTLS: A Tool for Testing TLS Implementations (with B. Beurdouche, A. Delignat-Lavaud, A. Pironti, K. Bhargavan), 9th USENIX Workshop on Offensive Technologies, 2015

Invited Talks

The Broader Implications of Apple's Content Scanning Push, Swiss Cyber Storm, 2021

Verifpal: Cryptographic Protocol Analysis for the Real World (with G. Nicolas, M. Tiwari), 9th IACR Real World Cryptography Symposium, 2021

Noise Explorer: Fully Automated Modeling and Verification for Arbitrary Noise Protocols, 7th IACR Real World Cryptography Symposium, 2019

Capsule: A Protocol for Secure Collaborative Document Editing, École Polytechnique Fédérale de Lausanne, 2018

Formal Verification for Cryptographic Systems in Web Applications, OWASP Gothenburg, 2018

Bringing Formal Verification to the Real Web: Three Years of Interconnected Work, Formal Methods Meets JavaScript Workshop, Imperial College London, 2018

Certifications

Certified national expert in cryptography, French Ministry for Research and Innovation. Authorized to lead Research and Development projects for 2017 – 2026

Selected Honors

Distinguished Paper Award, 38th IEEE Symposium on Security and Privacy, 2017
Best Hackathon Project, Runner Up, Microsoft Research Cambridge, 2016

Best Paper Award, 9th USENIX Workshop on Offensive Technologies, 2015
Wall Street Journal Data Transparency Award for Outstanding Data Control Project, 2012

Programming Languages

- Strong: Go, JavaScript, Kotlin, Rust, Swift, TypeScript
- Intermediate: C, C++, Java, OCaml, PHP, Python
- Beginner: Bash, C#, F#, Ruby