Vidal Attias

Cybersecurity PhD candidate
CEA List ×Loria

Paris, France
+33 6 69 74 14 48
vidal.attias@gmail.com
vidal-attias.fr

Fields of interest

I am a **final-year Cybersecurity PhD candidate** at CEA List and Loria, supervised by Grégoire Menguy, Sébastien Bardin, and Jean-Yves Marion. My research is supported by the **French national priority program PEPR Cyber/DefMal**.
My work focuses on **low-level reverse engineering** and **automated code deobfuscation**, specializing in *black-box* semantic analysis. My research drives the development of new symbolic approaches for the state-of-the-art **Xyntia** synthesizer, pushing the boundaries of automated binary deobfuscation. **Our latest work on this topic was accepted at CCS'25 (read it here).**
I am an alumnus of **École normale supérieure (ENS) Rennes** and the **MPRI** (Parisian Master of Research in Computer Science). Prior to my PhD, I was a **Junior Researcher** at the **IOTA Foundation**, where I focused on **Verifiable Delay Functions (VDF)** and their integration into **DLT protocols**. This trajectory has built my core expertise in **applied cryptography**, **multi-precision computing** (OpenSSL), and **low-level protocol security**.

Education

2023-2026 **PhD Candidate**, *Université de Lorraine*, Nancy, France.
Supervised by Pr. Jean-Yves Marion in collaboration with CEA List. Thesis title: *Automatic code reverse engineering: combining artificial intelligence and formal reasoning for deobfuscation*

2021-2022 **Talmudic studies**, *Mirrer Yeshiva Central Institute*, Brooklyn, New York.
Intensive talmudic studies focusing on critical thinking and extensive reasoning

2020-2021 **Parisian Master of Research in Computer Science**, *École Normale Supérieure Paris-Saclay- Université de Paris.*
Fundamental computer sciences

2018-2019 **First year of Master's degree in Computer Sciences**, *École Normale Supérieure de Rennes - Rennes 1 University.*
Fundamental computer sciences track

2017-2018 **Bachelor in Computer Science**, *École Normale Supérieure de Rennes.*
Fundamental computer sciences track

2015-2017 **Scientific preparatory class MPSI/PSI**, *ORT Strasbourg*, ranked 2nd.

2015 **French Baccalauréat**, *École Aquiba (Strasbourg)*, *Summa cum Laude.*

Experiences

October 2023 - Now **PhD Candidate**, *CEA List*, Paris.
PhD candidate in the French Nuclear Energy Commission's technology innovation department in collaboration with Lorraine University and Pr. Jean-Yves Marion. Under supervision of Sébastien Bardin and Grégoire Menguy.

Summer 2021 **Research internship**, *École normale supérieure*, Paris.
Under supervision of Pr. David Naccache on different subjects related to blockchain and arithmetic, including a visualization of the Tangle structure from the IOTA protocol.

May 2019 - Now **Research internship**, *IOTA Foundation*, Berlin.
In the Networking team. Six months working on Verifiable Delay Functions[1] and its applications in the network and helped designing a packet drop policy algorithm for the IOTA protocol. Six months dedicated to multiexponentiation algorithms and implementation using GMP library.

2018 - 2020 **Student Research Project**, *Percept Team*, Irisa Rennes.
Study of human gaze on paintings. We conducted eye-tracking experiments on subjects and provided the first database of gazes on paintings. Reports and presentations available on my website.

Summer 2018 **Research internship**, *ICube Laboratory - Strasbourg.*
Two months internship, working on the Tangle structure, a generalization of the Blockchain. I wrote a C++ simulator and designed a compression algorithm for the Tangle.

2015-2017 **Initiation to research**.
Initiation to research during my preparatory classes, in theoretical physics under supervision of Haggai Landa from Tel Aviv University.

Teaching

Fall 2025 **Teaching Assistant**, *ENSTA Engineering School*, Paris.
ENSTA-IN101 : Algorithms and programming

Fall - Winter 2024 **Teaching Assistant**, *Télécom Paris*, Paris.
CSC_0EL10_TP : Web Development

Summer 2018 **Teaching Assistant**, *ORT Strasbourg.*
Introduction to Computer Science

Publications

- **ACM CCS'25** XYNTIA+: Augmenting Search-based Program Synthesis with Local Inference Rules to Improve Blackbox Deobfuscation - *Vidal Attias, Nicolas Bellec, Grégoire Menguy, Sébastien Bardin, Jean-Yves Marion*
- **Journal of Cryptographic Engineering** Rethinking Modular Multi-Exponentiation in Real-World Applications - *Vidal Attias, Vassil Dimitrov, Luigi Vigneri*
- **IEEE Transactions on Computers** Fast Generation of RSA Keys using Smooth Integers - *Vassil Dimitrov, Luigi Vigneri, Vidal Attias*
- **IEEE Globecom'20** Preventing Denial of Service Attacks in IoT Networks through Verifiable Delay Functions - *Vidal Attias, Luigi Vigneri, Vassil Dimitrov*
- **Tokenomics'20** Implementation Study of Two Verifiable Delay Functions - *Vidal Attias, Luigi Vigneri, Vassil Dimitrov*
- **arXiv:1912.11401** On the Decentralized Generation of the RSA Moduli in Multi-Party Settings - *Vidal Attias, Luigi Vigneri, Vassil Dimitrov*
- **IOTA Foundation** The Coordice White Paper - *Popov et al.*
- **NETYS'19** How To Select its Parents in the Tangle - *Vidal Attias, Quentin Bramas*

Presentations

Sept. 2025 **GT MFS**.
20mn presentation of CCS paper

Sept. 2025 **Paris-Saclay Cyber Research Symposium**.
40mn presentation of CCS paper

July. 2024 **Journées des thèses du DILS**, *CEA List.*
5mn presentation of PhD work

June. 2024 **DefMal Workshop**, *PEPR Defmal.*
10mn presentation of PhD work

May. 2024 **RESSI**, *GDR Sécurité.*
Short paper submission + poster presentation

Feb. 2024 **Winter School**, *PEPR Cybersécurité*.
15mn presentation

Feb. 2020 **Stanford Blockchain Club**, *Stanford University*.
Presented my work on VDF to Stanford students

Feb. 2020 **Stanford Block Conference**, *Stanford University*.
VDF-focused workshop at Stanford Blockchain Conference, presenting IOTA's work on VDFs

Activities

2020 **Paper review**.
IEEE IoT journal, Globecom 2020 SAC IoTSCC

Sept. 2019 - March 2020 **Organizing team**, *Stanford Blockchain Club*, Stanford University.

Skills

Coding Python, C/C++ (OpenSSL/GMP/NTL), OCaml, Web, Bash

Languages **Professional**.
French (native), English (professional)

Languages **Hobby**.
Hebrew (biblical/medieval/modern), Spanish (intermediate), Aramaic (reading)

Interests

- Nature, hiking
- Travelling
- Amateur photography
- Aviation
- Music (15+ years of violin)
- History
- Languages