# Vidal Attias

*Computer Science at*
*ENS Paris-Saclay*

*12 Quai Koch*
*67000 Strasbourg*
*FRANCE*
*+33 6 69 74 14 48*
*vidal.attias@ens-rennes.fr*
*vidal-attias.io*

## Fields of interest

I am a computer science graduate from École normale supérieure (ENS) in Rennes and from MPRI, a highly competitive computer science master from parisian top universities. I am currenlty working as a Junior Researcher for the IOTA Foundation, a leader non-profit institution in the field of DLT (distributed ledger technology).
I have experience in research in blockchain, networking and applied cryptography. I have been working last year on Verifiable Delay Functions (VDF) and low level implementation as well as their integration in the IOTA protocol and have published several papers on the subject. I have experience with theoretical studies, in-depth understanding of multi-precision computing libraries such as OpenSSL and excellent interpersonal skills.

## Formations

2022-? **PhD in Computer Science**, *École Normale Supérieure Paris.*
Cryptography & cybersecurity Supervisor: Pr. David Naccache

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).*

## Experiences

Summer 2021 **Research internship**, *École normale supérieure*, Paris.
I have worked under the 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.
I am currently working for the IOTA Foundation in the Networking team. I have spent the six first months working on Verifiable Delay Functions[1] and its applications in the network and then I helped designing a packet drop policy algorithm for the IOTA protocol and the last six months have been dedicated to studying multiexponentiation algorithms and implementing them using GMP library.

2018 - 2020 **Student Research Project**, *Percept Team*, Irisa Rennes.
As part of the ENS scholarship, we have spent time on a research project. We studied human gaze on paitings. We conducted eye-tracking experiments on subjects and provided the first database of gazes on paintings. The reports and presentations can be found 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. You can see my report on my website. I was in a networking laboratory and learnt a lot there on this topic although it was not my research topic.

---
`VDF Research`

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

## Publications

- **Journal of Cryptographic Engineering** (pending) 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 2020** Preventing Denial of Service Attacks in IoT Networks through Verifiable Delay Functions - *Vidal Attias, Luigi Vigneri, Vassil Dimitrov*
- **Tokenomics 2020** 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 2019** How To Select its Parents in the Tangle - *Vidal Attias, Quentin Bramas*

## Activities

2020 **Paper reviewing**, *IEEE Internet of Things Journal*.
I have been invited by the Globecom conference to review one papers on IoT topics.

2020 **Paper reviewing**, *Globecom 2020 SAC IoTSCC*.
I have been invited by the Globecom conference to review two papers on IoT and networking topics.

September 2019 - Now **Organizing team**, *Stanford Blockchain Club*, Stanford University.
I have joined the Stanford Blockchain Club as an active member to discuss weekly on Blockchain topics, increase my knowledge and meet people working in the field.

February 2020 **Talking**, *VDF Day*, Stanford University.
Alongside the Stanford Blockchain Conference, the VDF Alliance organizes a day of talks about applying Verifiable Delay Functions to blockchain projects and my team have been invited talk about IOTA's work in which I had an important participation.

Summer 2019 **Teaching**, *ORT Strasbourg*.
I have prepared a selection of students from the preparatory class to engineering schools competitive exams in computer science, teaching algorithms, Python programming and introduction to complexity analysis during two months

## Skills

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

Languages French (native), English (professional), Hebrew (Intermediate), Spanish (Intermediate)

## Interests

I really do love wonders of nature and hiking. Due to the COVID-19, I decided to live in a RV and travel across the US to discover this continent while studying. I've visited 46 states over 50.000km and 40+ national parks.
I also have played violin for 14 years and keep being passionate about music.
I spend a lot of time documenting myself on the major societal subjects of our days, about privacy, degrowth theory, environmental issues. I believe in *low-tech*[2] associated with *high-tech* devices strongly limited and in the decentralized systems.

---

`Wikipedia`