

Antoine Bak

26 rue des cordelières
75013 Paris, France
antoine.bak@inria.fr
+33 6 70 31 06 77

PROFILE	In September 2024, I started a Ph.D. in the project-team COSMIQ in the INRIA of Paris under the supervision of Anne Canteaut and Léo Perrin. I am currently working on symmetric cryptology and more precisely on primitives optimized for use in advanced protocols.	
EDUCATION	Master Parisien de recherche en informatique (MPRI)	2023-2024
	Research-oriented master in computer science <ul style="list-style-type: none">• cryptology, quantum algorithms and computer algebra• learn about the state of the art of research in those fields	
	École polytechnique	2020-2023
	Majoring in mathematics and computer science <ul style="list-style-type: none">• algebra, number theory, algebraic geometry• cryptology, error correcting codes	
	Lycée Kléber, Strasbourg	2018-2020
	<i>Classe préparatoire</i> MPSI - MP* A two-year intensive university-level preparation in mathematics and physics to prepare for highly competitive nationwide exams	
EXPERIENCE	Research internship	03/2024-08/2024
	INRIA Paris <ul style="list-style-type: none">• symmetric cryptology under the supervision of Léo Perrin• cryptanalysis of <i>Arithmetization-oriented</i> primitives	
	Research internship	04/2023-08/2023
	DTU, Copenhagen <ul style="list-style-type: none">• cryptology, advanced protocols under the supervision of Luisa Siniscalchi• study of <i>zero-knowledge proofs</i> protocols and their applications to <i>multi-party computation</i>	
	Internship in a Research & Development service	06/2022-09/2022
	Sysnav <ul style="list-style-type: none">• developing algorithms for calibrating magnetic sensors• algorithmics, optimization	
	Internship in the French coast guards	09/2020-04/2021
	Cherbourg-en-Cotentin <ul style="list-style-type: none">• Internship as a military officer	
OTHERS	Ethereum bounties	2024
	Practical attacks on reduced versions of a cryptographic hash function (POSEIDON) <ul style="list-style-type: none">• The team got 53,000\$ of bounties by breaking 7 challenges.	