DAVID BALBÁS GUTIÉRREZ

Cryptographer | Mathematician and Computer Scientist

@ dbalbasg@gmail.com ☎ +34 676185966 ● Madrid, Spain 🌐 davidbalbas.github.io

I am David, a final-year PhD student in cryptography. My expertise lies on the **design and analysis of cryptographic primitives and protocols**, as well as their application in practice. I enjoy working on **challenging projects** that require a combination of **technical knowledge, creativity**, and **abstract reasoning**.

EXPERIENCE

Research Assistant – PhD Candidate

Oct 2021 – now

IMDEA Software Institute — Madrid, Spain

- Work on **theory and practice of public-key cryptographic primitives and protocols**. Advised by Prof. Dario Fiore and Prof. Maribel González-Vasco.
- **Main topics:** zero-knowledge proofs, succinct primitives, homomorphic cryptography, and end-to-end encryption in real-world systems.
- Multiple **international collaborations** and **research visits** (ETH Zurich, Max Planck Institute, Aalto University, etc.). Published **5 articles at top-tier conferences** in cryptography and security with over 50 citations.

Research Intern

Sep 2024 – Dec 2024

NTT R&D — Tokyo, Japan

- Currently working on **proof systems** and **advanced post-quantum digital signatures** at the NTT Social Informatics Laboratories, hosted by Prof. Masayuki Abe.

Research Intern

Feb 2021 – Jul 2021

École Polytechnique Fédérale de Lausanne (EPFL) — Lausanne, Switzerland

- Masters thesis on **secure group messaging** @ Security and Cryptography Lab (LASEC). Published at a top security venue (USENIX Security '23). Advised by Prof. Serge Vaudenay and Prof. Johan Håstad.

Cryptography Engineer

Jun 2020 – Dec 2020

BERTEN DSP — Santander, Spain – Remote

- Research, design and implementation of **Elliptic Curve Crypto** IP Core on **FPGAs**, supporting ECDH, ECDSA for arbitrary prime-field curves. Improved efficiency of reference model by 30%. Included side-channel protections.

PAST EXPERIENCE: Research Intern in **cosmology** at **Institute of Physics of Cantabria** (Aug 2018 - Jul 2019) and at **Brown University** (Jun - Aug 2018).

EDUCATION

PhD in Cryptography

Oct 2021 – now

IMDEA Software Institute — Madrid, Spain

MSc in Computer Science

Aug 2019 – Sep 2021

KTH Royal Institute of Technology — Stockholm, Sweden

- Grade: **A** (4.93/5). Track: **Theory, Cryptography and Algorithms**.

BSc in Mathematics & BSc in Physics

Sep 2014 – Sep 2019

University of Cantabria — Santander, Spain

- Grades: 8.9/10 (Mathematics), 9.1/10 (Physics). Independent degrees.

CORE SKILLS

Global

- **Creative problem solving, abstract reasoning, critical thinking.**
- Experience on **long-term team projects** and strict deadlines.
- Writing and understanding of **scientific and technical reports**.
- **Communication** of technical content to **diverse audiences**.

Technical

- **Cryptographic algorithms and protocols, pre- and post-quantum**.
- **Programming languages:** familiar with Python, Java, MATLAB & Simulink. Acquainted with C, C++, Rust.
- **Tools:** Linux, Windows, Git, SVN, LaTeX, usual productivity software.
- Familiar with **computer security**, internet protocols and ethical hacking.

Languages

Proficient in Spanish, English. Basic knowledge of German, French.

ADDITIONAL MERITS

Selected Awards and Grants

- Recipient of a **FPU Grant, 2023-2026**. This is the most prestigious and competitive grant awarded by the Spanish Government for doctoral studies.
- **First Prize** to the **best MSc/BSc thesis in Cryptology and IT Security** by ITEFI (CSIC) & CCN, 2022.
- Summer@EPFL Scholarship, 2020.
- ScottishPower Masters Scholarship, 2019.
- Collaboration Fellowship, 2018-2019. State research grant at Universidad de Cantabria.
- Bronze Medal - Spanish Physics Olympiad, 2014.

Others

- Given over 20 **talks and seminars** in conferences and as invited speaker in research institutions worldwide.
- Over 90 hours of **teaching experience** at Universidad Politécnica de Madrid.
- Peer-**reviewed** academic articles for multiple top-tier venues in security and cryptography. Program committee member of national conferences (RECSI).
- **Hobbies:** Outdoor **sports** (running, hiking, rock climbing, cycling...), **music** (piano, guitar), and **nature**.

Publications

For a complete list of publications, visit my personal webpage or my DBLP profile.