ANDERSSON CALLE VIERA

PhD Candidate in Cryptography

Passionate about continuous learning, I am always seeking innovative solutions. My curiosity, attention to detail, and autonomy enable me to achieve significant results. I believe that collaboration enriches every project.

2 rue Paul Bert, 13100, Aix-en-Provence
+33 6 26 44 56 82
anderssonroberto@hotmail.fr
/andersson-calle-viera
/anders1901

EXPERIENCES

- **PhD in Post-Quantum Cryptography** — MAY 2021-
  LiP6 Sorbonne Université - Thales DIS — Meyreuil, France
  — Development and **evaluation** on **ChipWhisperer** of a new **profiled attack** against Dilithium (Decompose).
  — Development and implementation of a **memory optimized version** of the signing algorithm of Dilithium **without timing overhead**. Used internally across multiple teams as the **reference implementation**.
  — **Fault attack** analysis of the **verification** algorithm of Dilithium. **Faults simulation** in C and **evaluation** of a scenario (**clock glitch**) on **ChipWhisperer**. Development of **efficient countermeasures**.
  — Exploitability analysis of **fault attacks** on the **signature** algorithm of Dilithium. **Development** in Python of an LP **solver** based on lpsolve library. Development of **efficient countermeasures**.
  — **Development** of an LP **solver** in C based on lpsolve. Allows to **retrieve part of the secret key** of Dilithium by exploiting standard signatures.
  — Development and **evaluation** on **ChipWhisperer** of a new **Simple Power Analysis attack** on Kyber (poly_tomsg). Development and evaluation of **efficient countermeasures**.

- **Internship: Post-Quantum Cryptography Engineer** — MAR 2021-AUG 2021
  Thales DIS — Meudon, France
  — **Attacks** and **countermeasures** state of the art of **Dilithium et Kyber**
  — Implementation of a **Python/Sage** version of **Dilithium**, used internally by multiple teams
  — Development of a **tool** to get **intermediate values**, used internally by multiple teams
  — **Simulations** of a **Fault attack** in Python/Sage with performance **study** and **countermeasures implementation**
  — Analysis of **leakage** and **parallelization** of a CPA against an **embedded implementation** of Dilithium

- **Private Tutor** — NOV 2018-AUG 2023
  Acadomia — France
  — **Individual** and **group** lessons of mathematics and computer science (middle school to undergraduate level)

EDUCATION

- **PhD: Secure Implementations of Post-Quantum Cryptography Algorithms Against Physical Attacks** — 2022-
  LiP6 Sorbonne Université - Thales DIS — Meyreuil, France
- **Master in Computer Science: Security, Reliability and Performance** — 2019-2021
  Science Sorbonne Université — Paris, France
- **Bachelor in Mathematics and Computer Science** — 2015-2019
  Science Sorbonne Université — Paris, France

SKILLS

- **Mathematics:** Lattices, Least Squares, Linear Programming
- **Informatique :** C, Assembly, Python, Sage, Jupyter Notebooks, scared library, Linux
- **Side Channel Attacks:** Analysis (CPA, t-test, SNR, ANOVA, NICV), SPA, DPA, CPA, Template
- **Fault Attacks:** DFA, Simulation in Python, Clock Glitch
- **Presentations:** Writing scientific articles in LaTeX, creating slides and scientific posters in LaTeX, scientific animations in Manim

PUBLICATIONS

- **Uncompressing Dilithium's Public Key**
  Paco Azevedo Oliveira, Andersson Calle Viera, Benoît Cogliati, Louis Goubin
  IACR ePrint - Submitted
- **Fault Attacks Sensitivity of Public Parameters in the Dilithium Verification Algorithm**
  Andersson Calle Viera, Alexandre Berzati, Karine Heydemann
  International Conference on Smart Cards Research and Advanced Applications (CARDIS) 2023 - Presented in Amsterdam, Netherlands
- **Exploiting Intermediate Value Leakage in Dilithium: A Template-Based Approach**
  Alexandre Berzati, Andersson Calle Viera, Maya Chartouny, Steven Madec, Damien Vergnaud, David Vigilant
  Transactions on Cryptographic Hardware and Embedded Systems (TCHES) 2023 - Presented in Prague, Czechia

LANGUAGES

- French - Native
- Spanich - C2
- English - B2 Certificate

PATENTS

- **Four** patents on **secure embedded implementations** of Dilithium (**optimizations** and **efficient countermeasures**).

HOBBIES

- Leather craft (designing small leather goods)
- Hiking with my cat (Sainte Victoire, calanques)
- Pottery (beginner, making small tableware)
- Guitar (self-taught for 4 years)