

# ANDERSSON CALLE VIERA

## Doctorant en Cryptographie







Passionné par l'apprentissage continu, je suis toujours en quête de solutions innovantes. Ma curiosité, mon attention aux détails et mon autonomie me permettent d'atteindre des résultats probants. Je crois que la collaboration enrichit chaque projet.

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

## EXPÉRIENCES.....

- **Doctorat en Cryptographie Post-Quantique**  MAI 2021-  
LiP6 Sorbonne Université - Thales DIS  Meyreuil, France
  - Développement et **évaluation** sur **ChipWhisperer** d'une nouvelle **attaque profilée** contre Dilithium (Decompose).
  - Développement et implémentation d'une **version optimisée en mémoire** de l'algorithme de signature de Dilithium **sans surcoût en temps**. Reprise et utilisée comme **version de référence en interne** dans plusieurs équipes.
  - Analyse de la sensibilité aux **fautes** de l'algorithme de **vérification** de Dilithium. **Simulation de fautes** en C et **évaluation** d'un scénario (**clock glitch**) sur **ChipWhisperer**. Développement de **contremesures efficaces**.
  - Analyse de l'exploitabilité de **fautes** sur l'algorithme de **signature** de Dilithium. **Développement** en Python d'un **solveur** LP basé sur la librairie Ipsolve. Développement de **contremesures efficaces**.
  - **Développement** d'un **solveur** en C basé sur Ipsolve permettant de **recupérer une partie de la clé secrète** de Dilithium en exploitant des signatures normales.
  - Développement et **évaluation sur ChipWhisperer** d'une nouvelle **attaque par SPA** contre Kyber (poly\_tomsg). Développement et évaluation de **contremesures efficaces**.
- **Stage : Ingénieur Cryptographie Post-Quantique**  MAR 2021-AOU 2021  
Thales DIS  Meudon, France
  - État de l'art des **attaques** et **contres-mesures** de **Dilithium et Kyber**
  - Implémentation d'une version **Python/Sage** de **Dilithium**, utilisée en interne dans plusieurs équipes
  - Développement d'un **outil pour récupérer les valeurs intermédiaires**, utilisé en interne dans plusieurs équipes
  - **Simulations d'attaques par faute** en Python/Sage avec **études** de performances et implémentation de **contremesures**
  - Analyse de **fuite d'information** et **parallélisation** d'une **CPA** contre une **version non protégée embarquée** de Dilithium
- **Professeur Particulier**  NOV 2018-AOU 2023  
Academia  France
  - **Cours individuels** et **collectifs** de mathématiques et informatique (niveau collège à licence)

## FORMATION.....

- **Doctorat : Implantations d'Algorithmes de Cryptographie Post-Quantique Sécurisées Contre les Attaques Physiques**  2022-  
LiP6 Sorbonne Université - Thales DIS  Meyreuil, France
- **Master Informatique : Sécurité, Fiabilité et Performances**  2019-2021  
Science Sorbonne Université  Paris, France
- **Licence Mathématiques et Informatique**  2015-2019  
Science Sorbonne Université  Paris, France

## COMPÉTENCES..... PUBLICATIONS.....

- **Mathématiques :**  
Réseaux, Moindres Carrés, Programmation Linéaire
- **Informatique :**  
C, Assembleur, Python, Sage, Jupyter Notebooks, librairie scared, Linux
- **Attaques par Canaux Auxiliaires :**  
Analyse (CPA, t-test, SNR, ANOVA, NICV), SPA, DPA, CPA, Template
- **Attaques par Fautes :**  
DFA, Simulation en Python, Clock Glitch
- **Présentations :**  
Écriture d'articles scientifiques en LaTeX, diapositives et poster scientifique en LaTeX, animations scientifique en Manim
- **Uncompressing Dilithium's Public Key**  
Paco Azevedo Oliveira, Andersson Calle Viera, Benoît Cogliati, Louis Goubin  
IACR ePrint - En cours de soumission
- **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 - Présenté à Amsterdam, Pays-Bas
- **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 - Présenté à Prague, Tchéquie

## LANGUES..... BREVETS.....

- Français - Langue maternelle
- Espagnol - Niveau C2
- Anglais - Certificat B2
- **Quatre brevets sur les implémentations sécurisées embarquées de Dilithium (optimisations et contremesures efficaces).**

## INTÉRÊTS.....

- Travail du cuir (conception de petite maroquinerie)
- Randonnée avec mon chat (Sainte Victoire, calanques)
- Poterie (débutant, confection de petite vaisselle)
- Guitare (4 ans, autodidacte)