Olivier POTIN
Jean-Baptiste RIGAUD
Raphael VIERA

Projet FPGA Sécurisé

Gevorg ISHKHANYAN
Antoine CHASSAIGNE

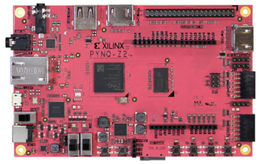
Soutenance du 26/03/2025

Architecture du projet

Modèle de départ

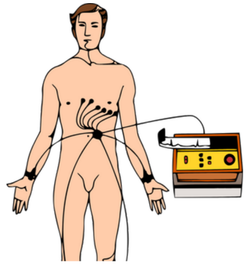
Déchiffrement
Monitoring
Instrumentation

UART



Réception
Chiffrement ASCON
Transmission

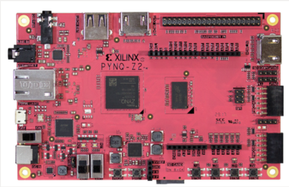
I2C



Capteur ECG

Modèle choisi

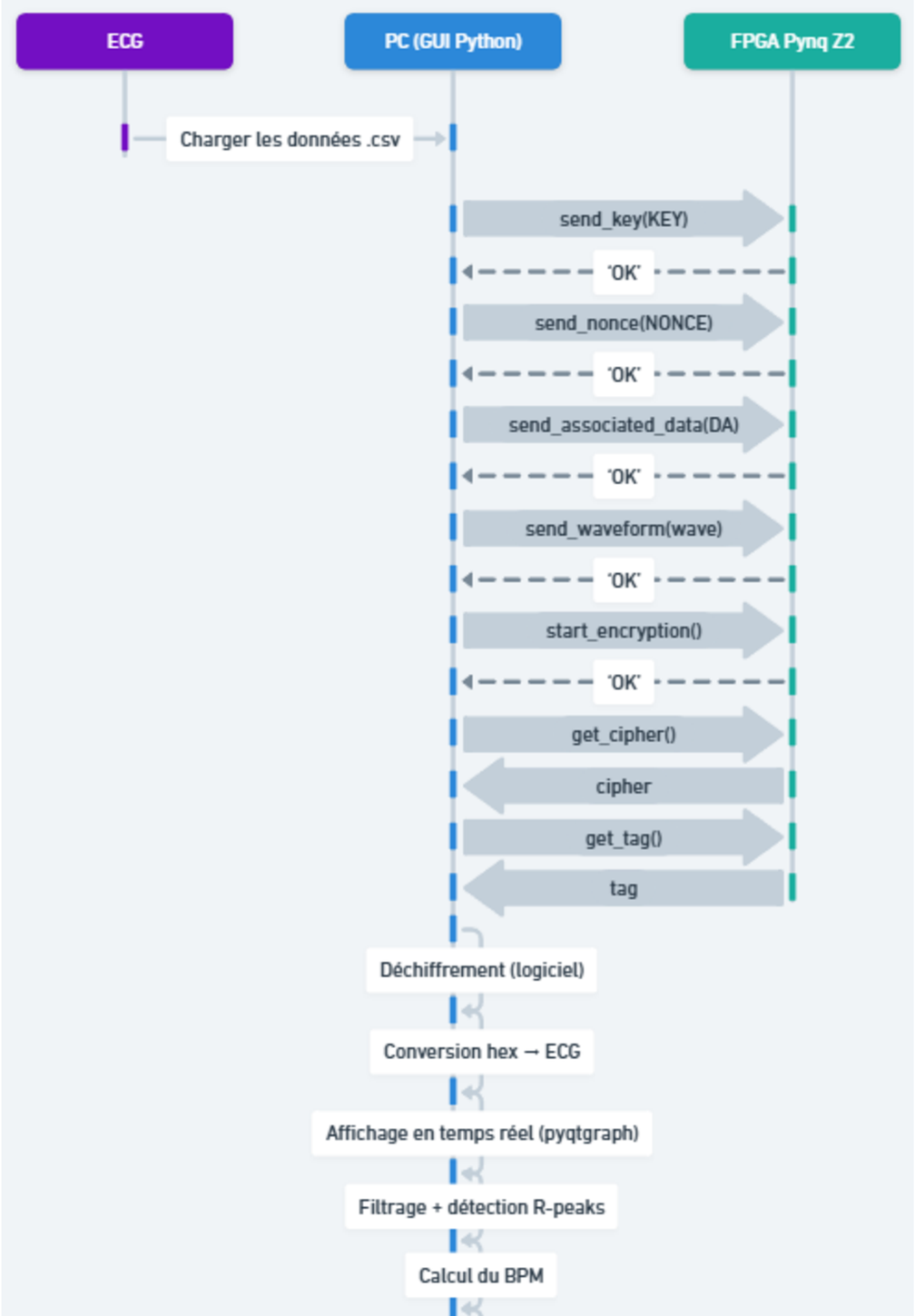
UART



Envoi des ECG en .csv
Déchiffrement
Monitoring
Instrumentation

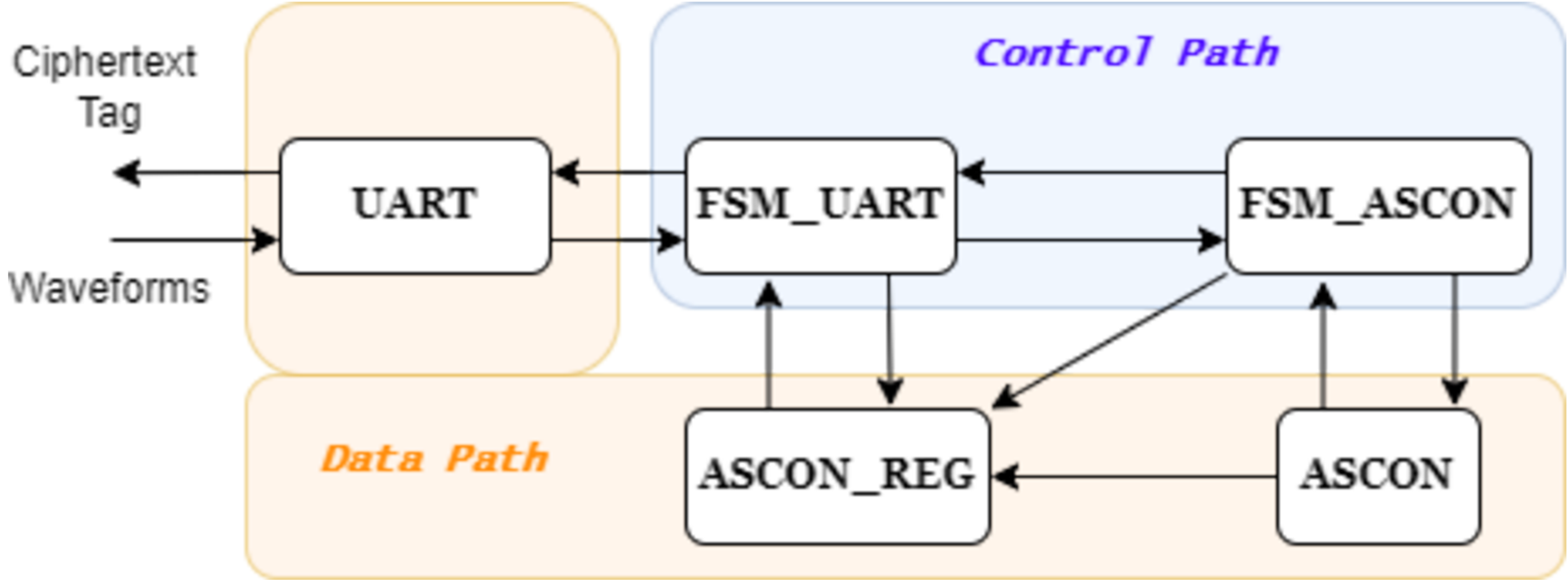
Réception
Chiffrement ASCON
Transmission

Fonctionnement global



Partie FPGA

Architecture FPGA

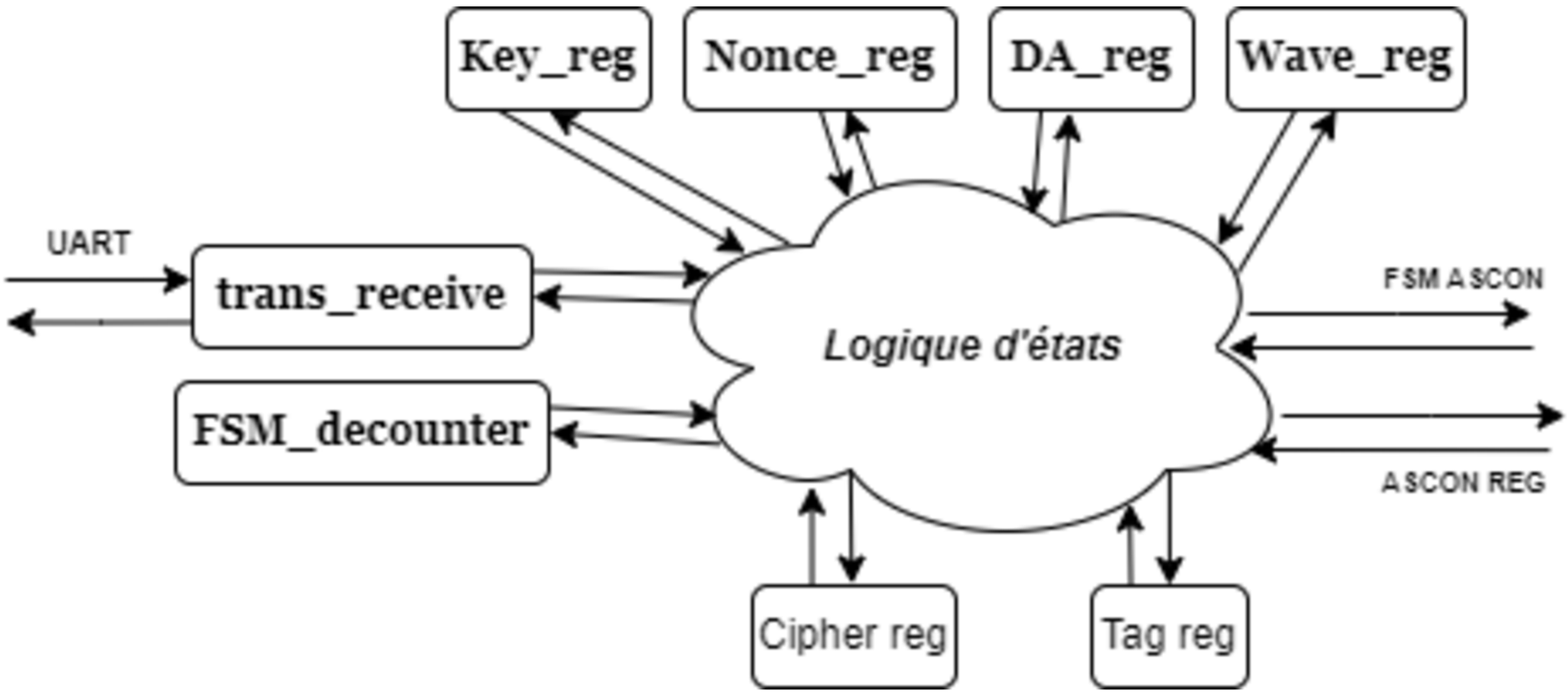


Sans oublier le Clock_converter (125MHz to 50 MHz)

5 modules dans le top level

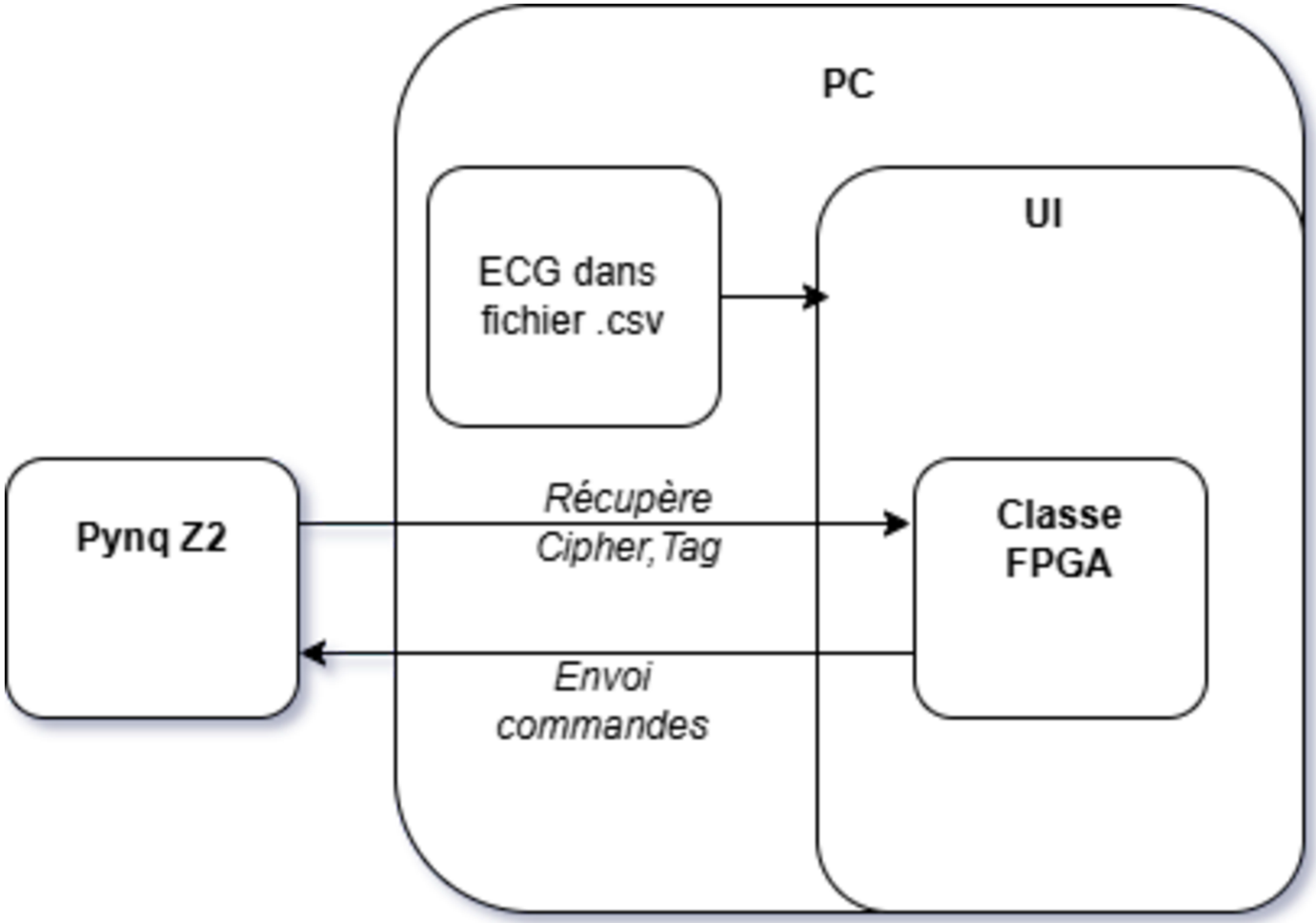
Gestion de données UART

FSM_UART



Partie applicative

Instrumentation du FPGA

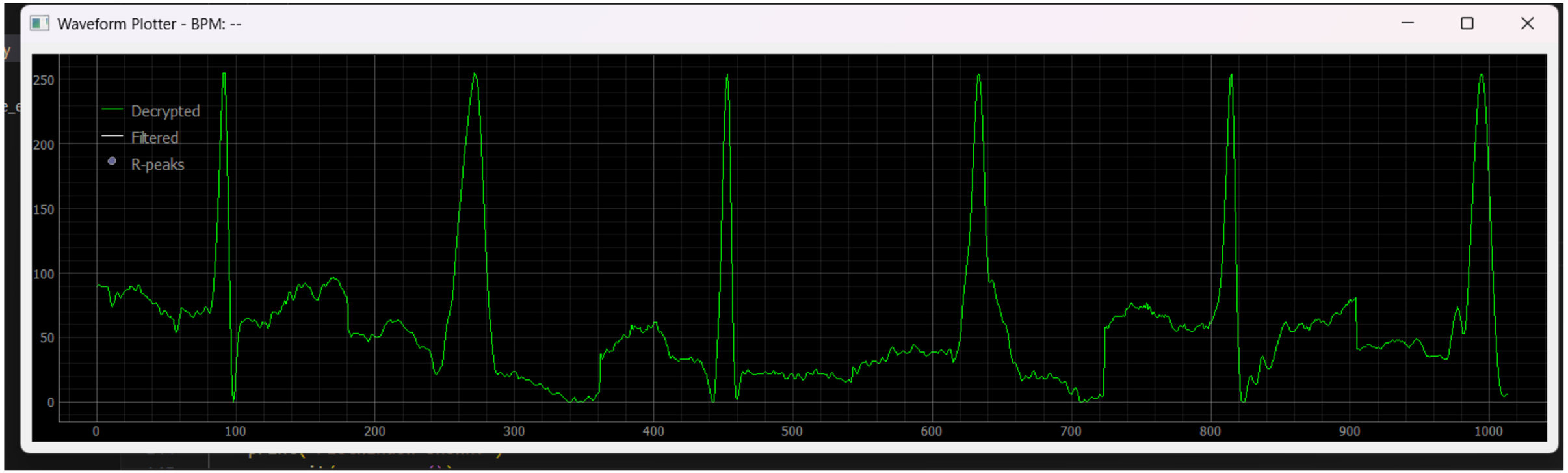


Driver d'instrumentation

```python
from FPGA import *

KEY =   bytes.fromhex('4B8A55114D1CB6A9A2BE263D4D7AECAAFF')
NONCE = bytes.fromhex('4E4ED0EC0B98C529B7C8CDDF37BCD0284A')
DA =    bytes.fromhex('444120746F20428000')
WAVE =  bytes.fromhex('575A5B5B5A5A5A5A5A59554E4A4C4F5455535153545657585 75A5A595756


fpga = FPGA('COM5', 115200)
fpga.open_instrument()
fpga.send_key(KEY)
fpga.send_nonce(NONCE)
fpga.send_associated_data(DA)
fpga.send_waveform(WAVE)
fpga.start_encryption()
cipher = fpga.get_cipher()
tag = fpga.get_tag()
fpga.close_instrument()

plain = fpga.decrypt_waveform_python(cipher[:-3]+tag, KEY[1:], NONCE[1:], DA[1:-2])
```

Interface utilisateur

Visualisation



Analyses ECG

Bibliothèques importées:

sys, PyQt5, pyqtgraph, pyqtgraph, collections, neurokit2, numpy

Démonstration

Méthodes de travail

Organisation

Outils utilisés :

Electron Sculptor

- Partie Python
- Verification
- Débug FPGA

Disperseur

- Design des FSM
- Testbench
- Débug FPGA

Conclusion

Feedback sur le projet

- Très intéressant
- Techniquement challengeant
- Perfectionnement de nos méthodes de débug Hardware (Testbench et ILA)
- Prise en main d'un vrai FPGA

- On aurait bien aimé avoir plus de temps pour finaliser en entier, (2-3 séances de +)
- Timing entre les séances (Corrélation Python et FPGA)

Difficultés rencontrées

- Manque de compréhension du fonctionnement des registres d'envoi du Cipher et Tag.
- Format des commandes pas clairs

MERCI