General information

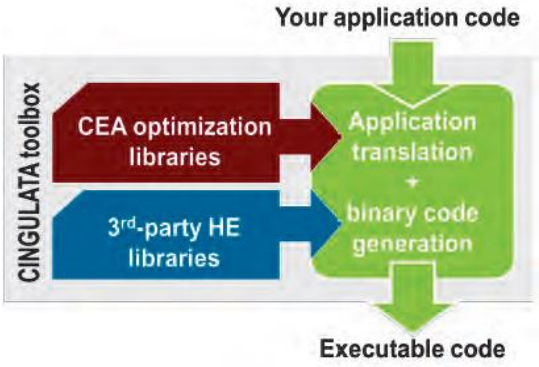
CEA Agnes Lancelot agnes.lancelot@cea.fr +33169081735

Targeted topics

ICT-08-2019	Security and resilience for collaborative manufacturing environments	RIA
SU-DS05-2018-2019	Digital security, privacy, data protection and accountability in critical sectors	IA & RIA
SU-ICT-02-2020	Building blocks for resilience in evolving systems	RIA

Encryption Competencies for data privacy protection

- ***Homomorphic encryption (computing on encrypted data)***
  - Open source Cingulata toolbox: compiler toolchain for running C++ programs over encrypted data by means of fully homomorphic encryption techniques



Example of major use case: healthcare Clear link to SU-DS-O5 Digital security, privacy and personal data protection in healthcare ecosystem

- ***High performance lightweight cryptography***
  - A library implementing many variants of lightweight stream-ciphers for different trade-offs
  - Software countermeasures to physical attacks
  - Compatibility of fast, low-power and securely implemented ciphers deployed in the resource-limited IoT nodes with more complex homomorphic schemes that can be deployed on the server side

Competencies in attacks detection and code protection

- ***Detection of cyber-attacks in IoT***
  - **Monitoring and light-weight machine learning techniques**
- ***COGITO: Automated application of software countermeasures against physical attacks***
  - **A toolchain for the compilation of secured programs**
  - **side-channel, fault injection, reverse engineering**