The work presented in this poster was realized in the frame of the SALWARE project number ANR-13-JS03-0003 supported by the French "Agence Nationale de la Recherche" and by the French "Fondation de Recherche pour l’Aéronautique et l’Espace", funding for this project was also provided by a grant from la région Rhône-Alpes.

Brice Colombier  Lilian Bossuet
Hubert Curien Laboratory, UMR CNRS 5516
University of Lyon, Saint-Étienne, France
b.colombier@univ-st-etienne.fr

Functional Locking Modules for Design Protection of Intellectual Property Cores

Moore’s law
Increasing complexity
Horizontal business model
Design & Reuse
Counterfeiting ?
Overbuilding ?

An efficient and secure protection scheme is required

Several common features can be leveraged to lock the SoC

Designed Locking Modules

Moore’s law
Increasing complexity
Horizontal business model
Design & Reuse
Counterfeiting ?
Overbuilding ?

An efficient and secure protection scheme is required

Several common features can be leveraged to lock the SoC

Experimental Results

Two reference designs:
- Ethernet controller
- Plasma CPU

Two target FPGAs:
- Xilinx Spartan 3
- Altera Cyclone III

Two P&R strategies:
- area-optimized
- speed-optimized

Conclusion:
- Several common features can be identified on a SoC,
- These features can be used to efficiently lock the SoC,
- Associated with a strong authentication protocol, they are a powerful protection scheme.

To do:
- Measure locking efficiency
- Implement a lightweight authentication scheme
- Integrate the system into real-life designs
- Evaluate resilience to side-channel attacks