Functional Locking Modules for Design Protection of Intellectual Property Cores

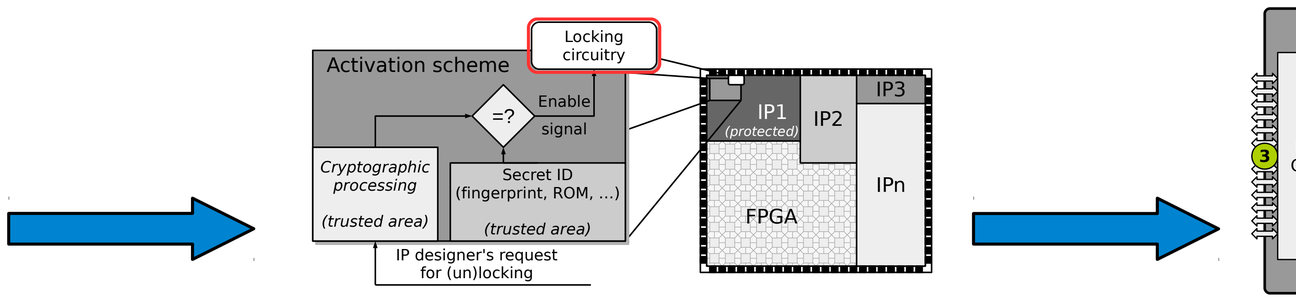
Brice Colombier Lilian Bossuet

Hubert Curien Laboratory, UMR CNRS 5516

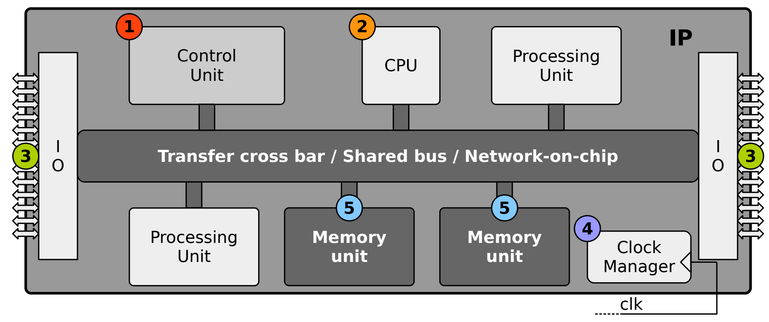
University of Lyon, Saint-Étienne, France

b.colombier@univ-st-etienne.fr

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

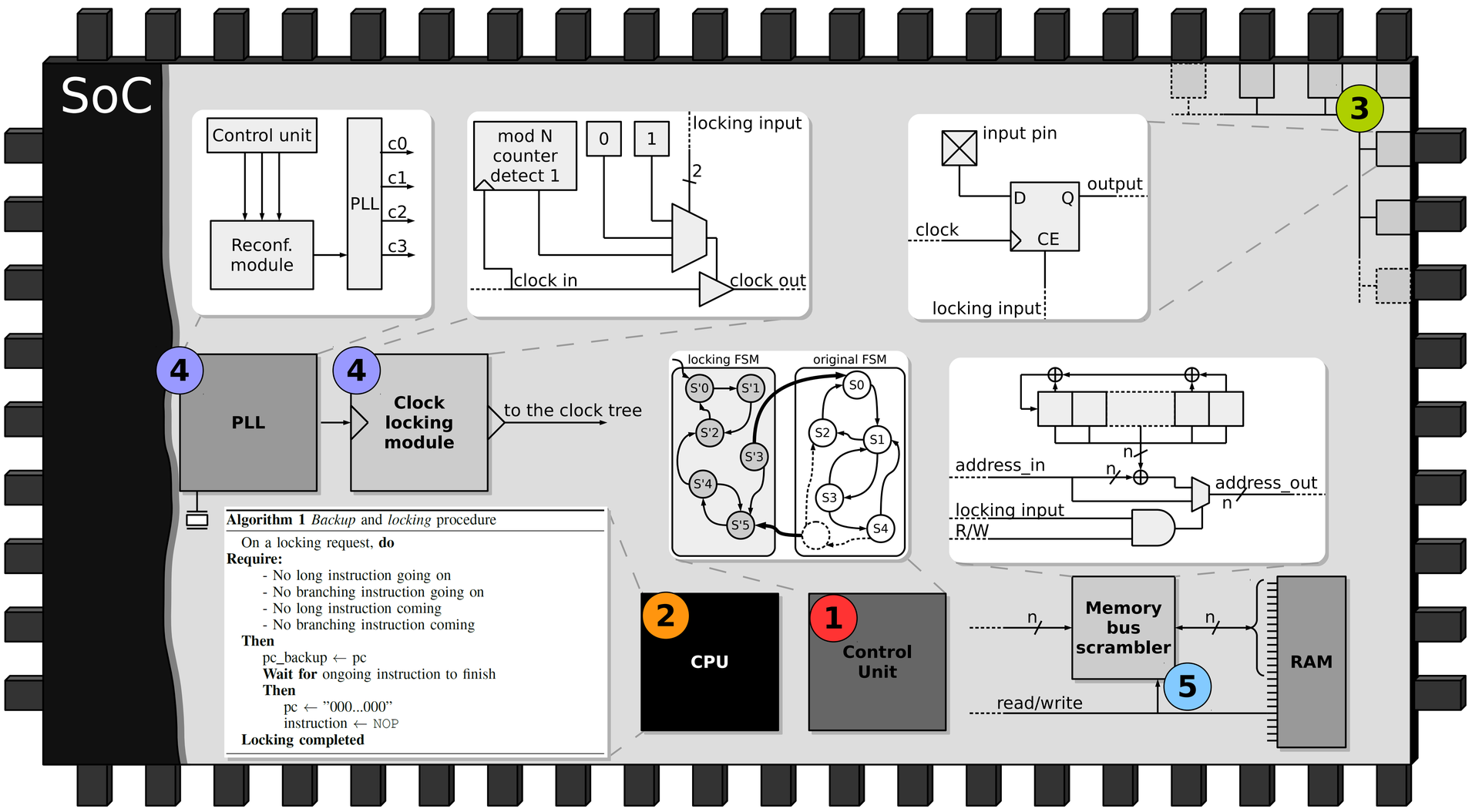


An efficient and secure protection scheme is required



Several common features can be leveraged to lock the SoC

Designed Locking Modules



Algorithm 1 *Backup* and *locking* procedure

On a locking request, **do**

Require:
- No long instruction going on
- No branching instruction going on
- No long instruction coming
- No branching instruction coming

Then
pc_backup ← pc
Wait for ongoing instruction to finish
Then
pc ← "000...000"
instruction ← NOP

Locking completed

1. Add **dummy start states** to the FSM to control access to the normal behaviour.
2. Stop progress of the **program counter** (PC) to lock the processor in a specified state.
3. Prevent the SoC from receiving new data by disabling **input flip-flops or latches**.
4. **Reduce** the frequency of the chip, or **shut down** a clock domain.
5. **Scramble** data when it's being read from the memory to make it unreliable.

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

Xilinx Spartan 3

Name	Area-optimized Slices	Area-optimized F_{max} (MHz)	Speed-optimized Slices	Speed-optimized F_{max} (MHz)
FSM (256 bits)	187 (+9%)	89.9 (-1%)	202 (+1%)	109.5 (-11%)
Memory bus	203 (+18%)	88.6 (-2%)	216 (+8%)	111.5 (-10%)
Inputs locking	172 (+0%)	90.5 (+0%)	200 (+0%)	123.3 (+0%)
Clock signal	175 (+2%)	90.4 (+0%)	202 (+1%)	123.4 (+0%)

Altera Cyclone III

Name	Area-optimized LEs	Area-optimized F_{max} (MHz)	Speed-optimized LEs	Speed-optimized F_{max} (MHz)
FSM (256 bits)	320 (+16%)	108.6 (-37%)	328 (+16%)	110.4 (-45%)
Memory bus	322 (+17%)	161.4 (-6%)	324 (+14%)	176.1 (-12%)
Inputs locking	280 (+2%)	159.5 (-7%)	278 (-2%)	181.1 (-9%)
Clock signal	288 (+5%)	154.7 (+10%)	289 (+2%)	191.7 (-4%)

Ethernet controller

Xilinx Spartan 3

Name	Area-optimized Slices	Area-optimized F_{max} (MHz)	Speed-optimized Slices	Speed-optimized F_{max} (MHz)
Memory bus	1524 (+2%)	16.5 (-0%)	1818 (+2%)	40.5 (+5%)
Inputs locking	1498 (+0%)	16.3 (-1%)	1842 (+3%)	40.7 (+6%)
Clock signal	1508 (+1%)	16.2 (-2%)	1888 (+6%)	38.6 (+0%)
Backup & restore	1629 (+9%)	12.5 (-25%)	1918 (+8%)	24.3 (-37%)

Altera Cyclone III

Name	Area-optimized LEs	Area-optimized F_{max} (MHz)	Speed-optimized LEs	Speed-optimized F_{max} (MHz)
Memory bus	2476 (+2%)	18.42 (+4%)	3044 (+2%)	18.24 (+3%)
Inputs locking	2441 (+1%)	17.86 (+0%)	2979 (+0%)	17.91 (+1%)
Clock signal	2431 (+0%)	18.09 (+2%)	2906 (-2%)	17.57 (-1%)

Plasma CPU

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

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

http://www.univ-st-etienne.fr/salware/