Les rencontres du NUMÉRIQUE de l'ANR

COGITO

RUNTIME CODE GENERATION TO SECURE DEVICES

- TYPE DE PROJET: INS
- TYPE DE RECHERCHE:
- COUT COMPLET: 1M€
- AIDE DE L'ANR: 310k€
- DATE DE DEMARRAGE: 01/10/2013
- DUREE: 42 mois
- SITE WEB: http://www.cogito-anr.fr/

- Coordinateur du projet: Damien COUROUSSÉ
- Partenaire 1: CEA
- Partenaire 2: INRIA Rennes
- Partenaire 3: École Nationale des Mines de Saint-Étienne
- Partenaire 4: (XLIM. Univ. Limoges)

Objectifs du projet: Propose countermeasures against physical attacks, with runtime code generation

Code polymorphism: regularly changing the behavior of a (secured) component, at runtime, while maintaining unchanged its functional properties, with runtime code generation

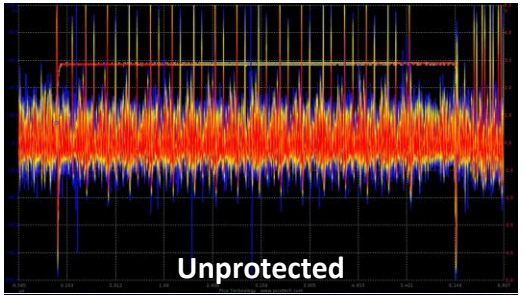
Protection against physical attacks: side channel & fault attacks

- Alters the spatial and temporal properties of the secured code
- Compatible with State-of-the-Art HW & SW Countermeasures

Protection against reverse engineering of SW

- the secured code is not available before runtime
- the secured code regularly changes its form

deGoal (CEA-LIST): **runtime code generation for embedded systems.** Fast code generation, tiny memory footprint



damien.courousse@cea.fr

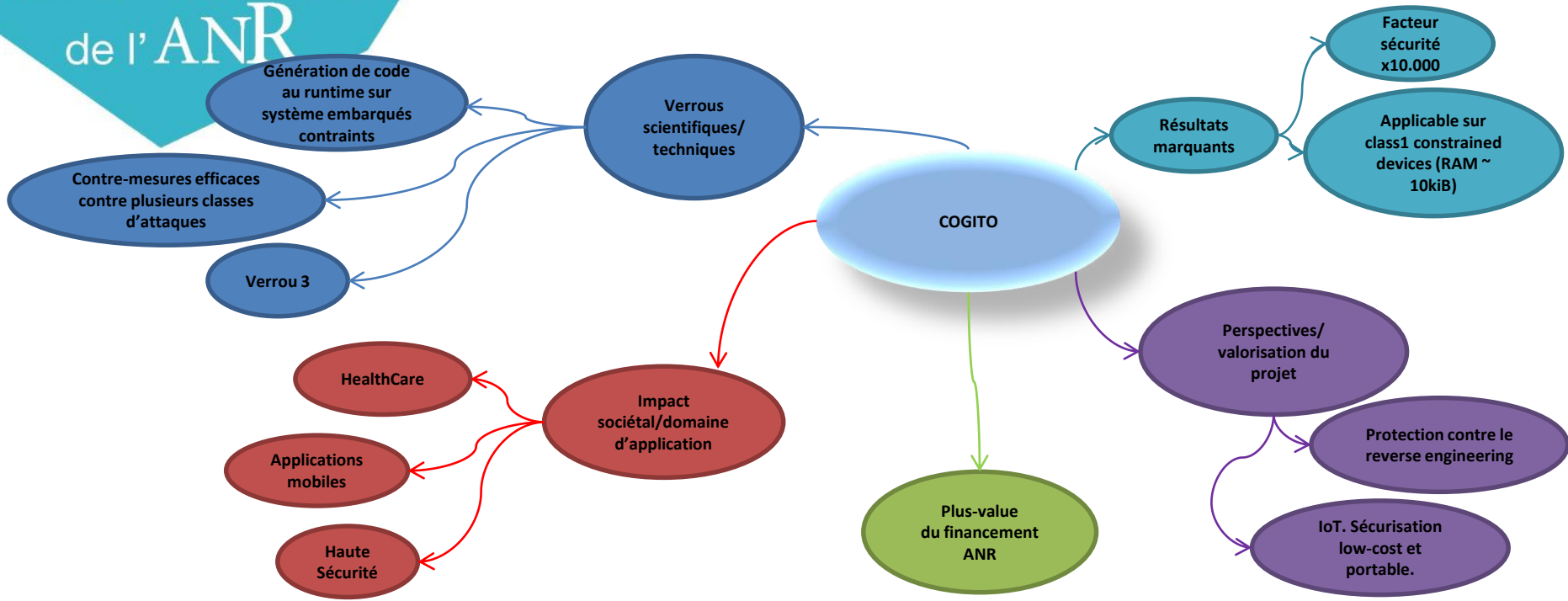
cea Inria Ecole Nationale Supérieure des Mines SAINT-ETIENNE

PROJET FINANCÉ PAR L'ANR

Les rencontres du NUMÉRIQUE de l'ANR

COGITO

RUNTIME CODE GENERATION TO SECURE DEVICES



16|17 NOVEMBRE 2016

cea

Inria

Ecole Nationale Supérieure des Mines SAINT-ETIENNE