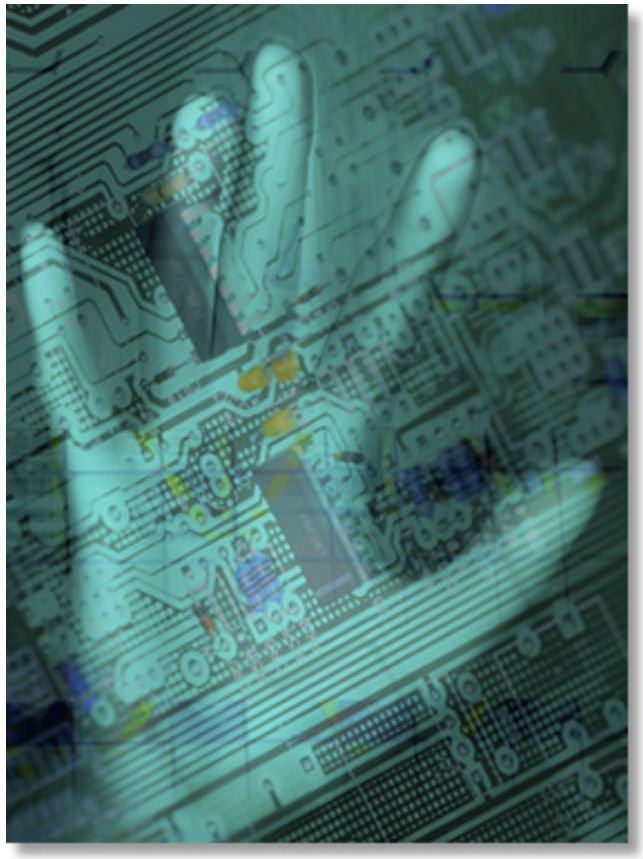
Journée Sécurité Numérique
GDR SoC-SiP

Cartographie

Marie-Lise Flottes,
Giorgio Di Natale,
Guy Gogniat

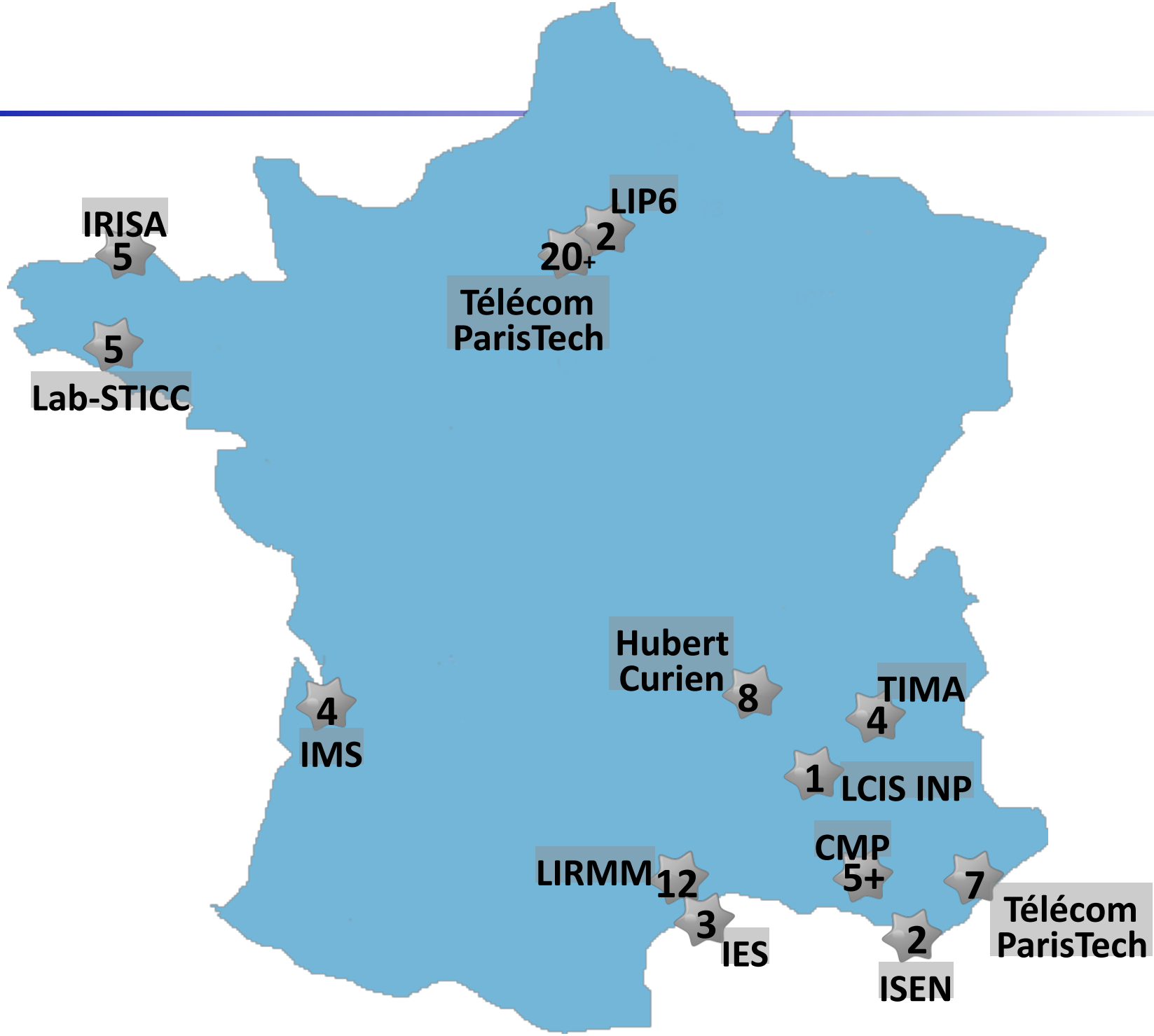


Création de la cartographie

- A partir des données reçues (pas exhaustif)
- A compléter (journees_securite@lirmm.fr)
- Fichier accessible sur internet (adresse site communiquée par email)

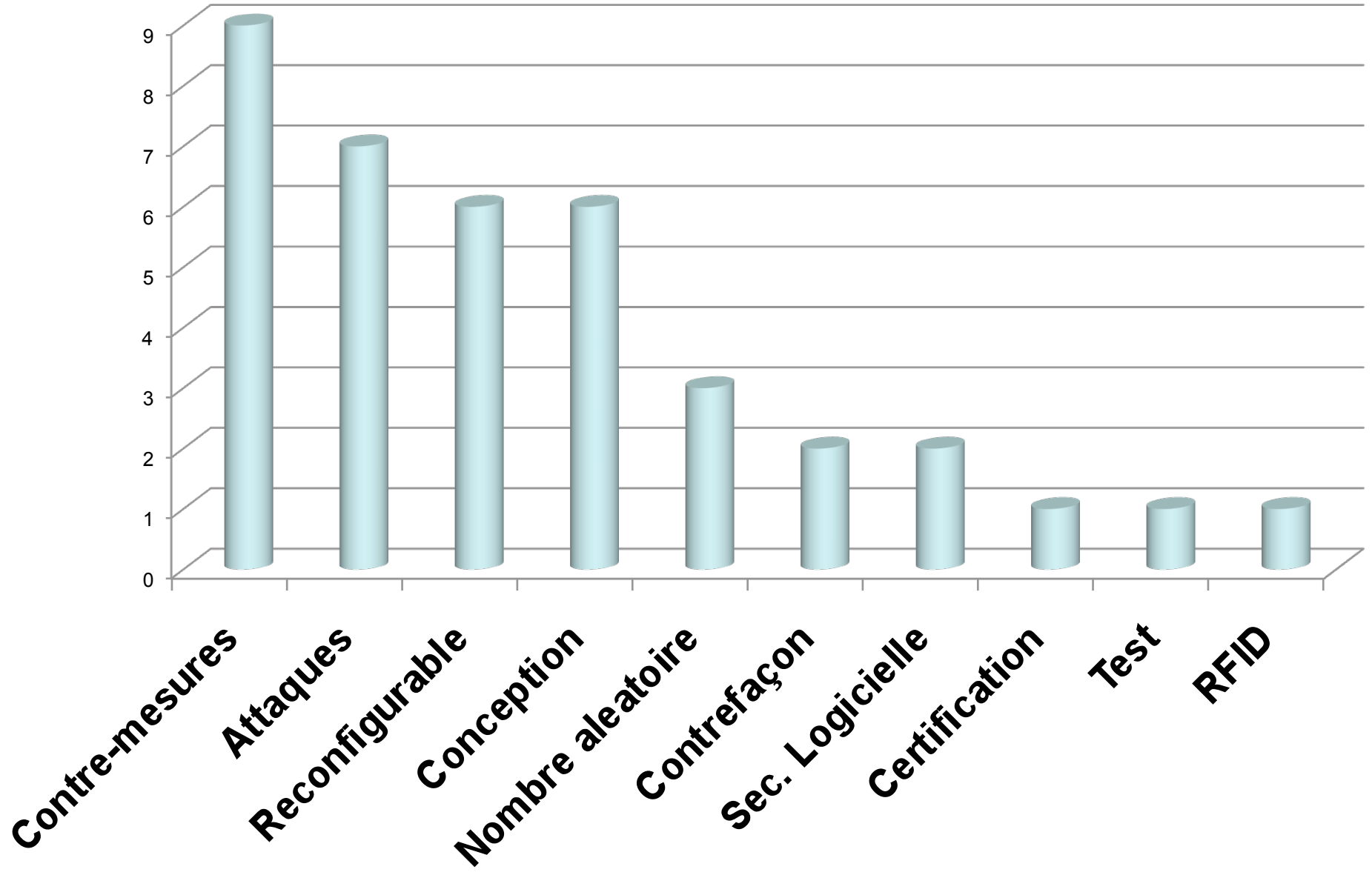
Thèmes

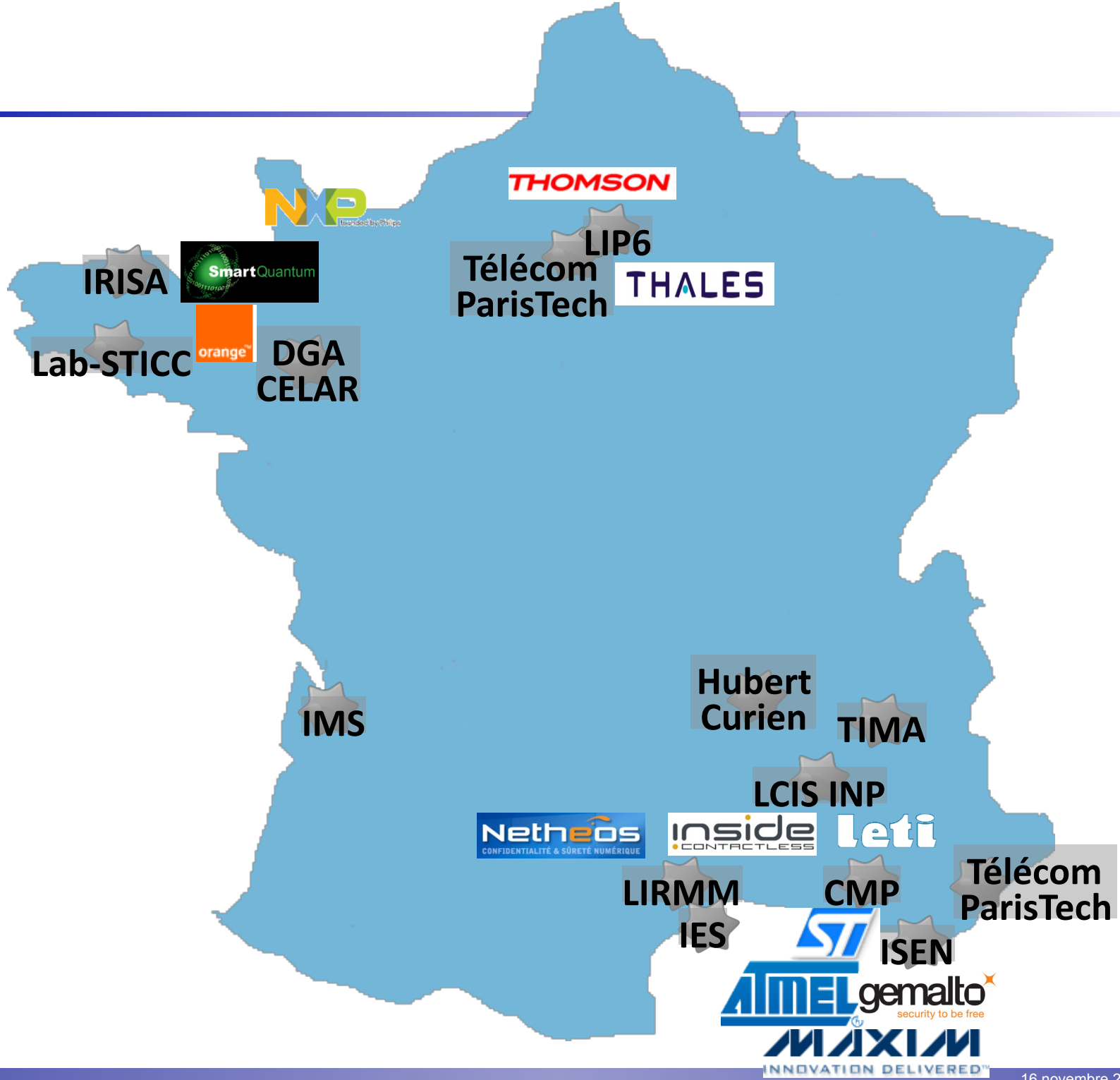
- Conception des systèmes embarqués sécurisés
- Sécurité pour et par les architectures reconfigurables
- Attaque par canaux cachés et contre-mesures
- Attaque en fautes et contre-mesures
- Test et sécurité
- Sécurité logicielle
- Générateurs de nombres aléatoires
- Sécurité des systèmes RFID
- Protection contre la contrefaçon
- Certification


IRISA
5
5
Lab-STICC
LIP6
2
20+
Télécom
ParisTech
Hubert
Curien
8
4
IMS
TIMA
4
1
LCIS INP
CMP
5+
LIRMM
12
3
IES
7
Télécom
ParisTech
2
ISEN

LIP6	Reconfigurables
Télécom ParisTech (Paris)	Nombres aléatoires, Attaques et Contre-mesures, Reconfigurables, Contrefaçon
IRISA	Aléatoires, Conception, Contre-mesures attaques
Lab-STICC	Conception, Contre-mesures attaques, Reconfigurables
IMS	Contrefaçon, Contre-mesures attaques, Reconfigurables
Hubert Curien	Nombres aléatoires, Attaques et Contre-mesures, Reconfigurables
TIMA	Conception, Attaques et Contre-mesures
LCIS INP	Conception, Certification
LIRMM	Conception, Attaques et Contre-mesures, Reconfigurables, Test et sécurité
IES	Attaques
CMP	Conception, Attaques et Contre-mesures
Télécom ParisTech (Sophia)	Attaques et Contre-mesures, Sécurité logicielle
ISEN	Sécurité logicielle, RFID

Thèmes (synthèse)



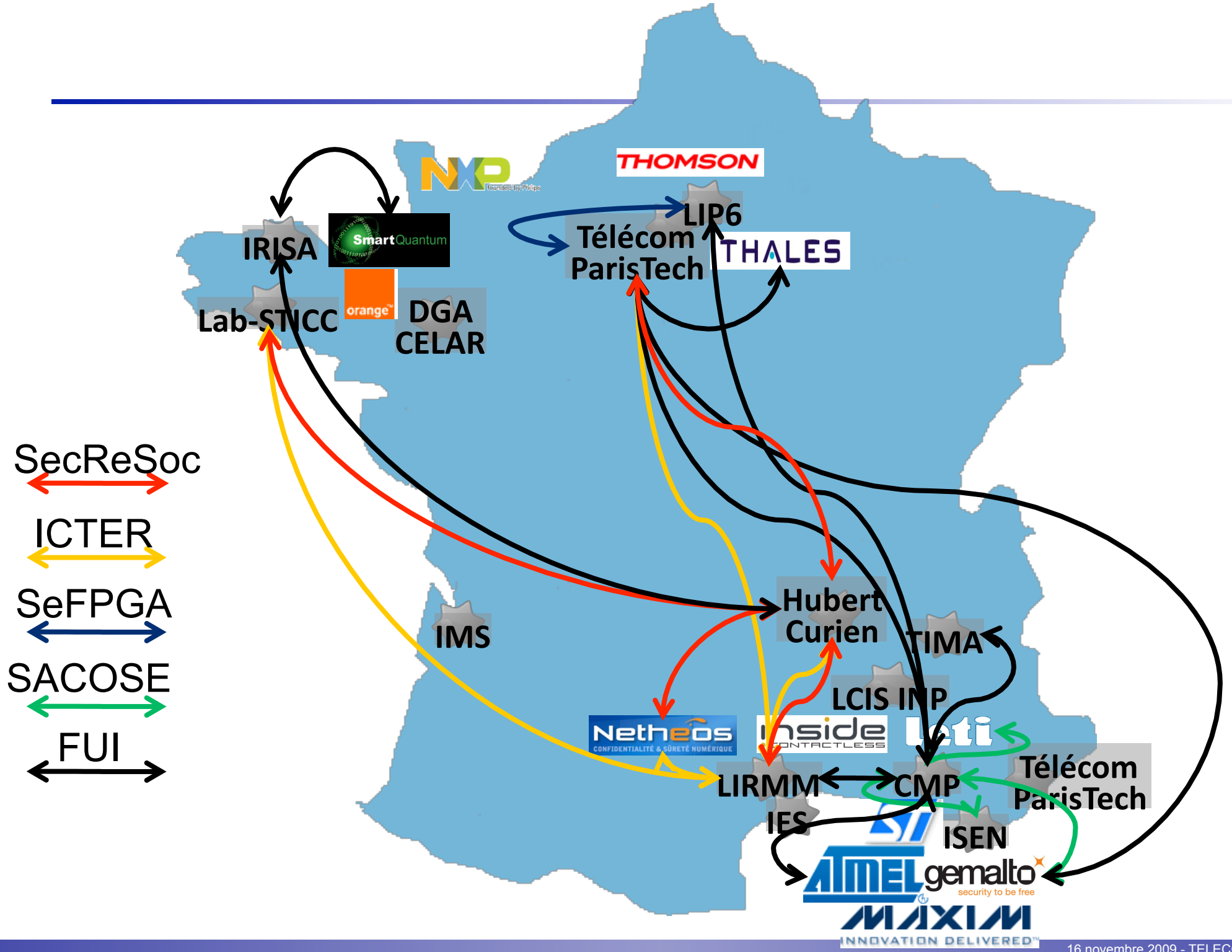

NXP
THOMSON
LIP6
IRISA
SmartQuantum
Télécom ParisTech
THALES
orange
Lab-STICC
DGA CELAR
IMS
Hubert Curien
TIMA
LCIS INP
Netheos
CONFIDENTIALITÉ & SÛRETÉ NUMÉRIQUE
inside CONTACTLESS
leti
LIRMM
CMP
Télécom ParisTech
IES
ISEN
ATMEL
gemalto
security to be free
MAXIM
INNOVATION DELIVERED

Projets

- **ANR**
  - **SecReSoc** : architecture multiprocesseur sécurisée (FPGA)
  - **ICTER** : intégration des primitifs cryptographiques (FPGA)
  - **SeFPGA** : Architectures FPGA sécurisées pour les systèmes sur puce
  - **SACOSE** : SAns COntact SEcurisé
- **FUI**
  - **Calisson** : CAractérisation, modéLIsation et Spécifications Sécuritaires de circuits prOtotypes iNtégrés
  - **EPOMI** : Evaluation Plateforme Ouverte Modulaire & Incrémentale
  - **SecureAlgorithms**
  - **SHIVA**
- **Europe**
  - **Toets, Evita**

ANR SecReSoc

- **Objectifs :** Développer une architecture multiprocesseur permettant l'intégration dans une cible FPGA (standard ou spécifique) d'une application nécessitant différents niveaux de sécurisation des données.
- **Porteurs Laboratoire :** Hubert Curien, Université de Saint Etienne
- **Entreprises :** NETHEOS
- **Recherche / Académie :**
  - Telecom ParisTech
  - LIRMM
  - LAB STICC


NXP
THOMSON
LIP6
Télécom ParisTech
THALES
IRISA
SmartQuantum
orange
Lab-STICC
DGA CELAR
IMS
Hubert Curien
TIMA
LCIS INP
Netheos
CONFIDENTIALITÉ & SÛRETÉ NUMÉRIQUE
inside CONTACTLESS
leti
Télécom ParisTech
LIRMM
CMP
IES
ISEN
ATMEL
gemalto
security to be free
MAXIM
INNOVATION DELIVERED
SecReSoc
ICTER
SeFPGA
SACOSE
FUI

Programme de la journée

- 10:35-11:35 **Hugues de Perthuis – NXP**
  Conception des systèmes numériques embarqués sécurisés
- 11:40-12:40 **Frédéric Valette - CELAR**
  Attaques contre les cryptoprocesseurs et contres mesures
- 14:00-15:00 **Alain Merle - CEA CESTI**
  Certification, avancées et axes de R&D en protection
- 15:05-16:05 **Antoine Delautre & Eric Saliba - THALES**
  Sécurité côté "manufacturing" : PUF et Trojan
- 16:05-16:30 **Discussion**