Les rencontres du NUMÉRIQUE de l'ANR

SIMPATIC

SIM and PAiring Theory for Information and Communications security

- TYPE DE PROJET : INS 2012
- TYPE DE RECHERCHE : Industrielle
- COUT COMPLET : 3 M€
- AIDE DE L'ANR : 1 M€
- DATE DE DEMARRAGE : 12/12/2016
- DUREE : 42 mois
- SITE WEB : http://simpatic.orange-labs.fr

- Coordinateur du projet : Orange
- Partenaire 1 : ENS
- Partenaire 2 : INVIA
- Partenaire 3 : Oberthur Technologies
- Partenaire 4 : STMicroelectronics
- Partenaire 5 : Université Bordeaux 1
- Partenaire 6 : Université Caen Normandie
- Partenaire 7 : Université Paris 8

Objectifs du projet:

- Les couplages mathématiques
  - fonction e : $G_1 \times G_2 \rightarrow G_T$ ayant une propriété de bilinéarité

$e([x]P_1,[y]P_2) = e([xy]P_1,P_2) = e(P_1,[xy]P_2) = e([y]P_1,[x]P_2) = e(P_1, P_2)^{xy} = \ldots$

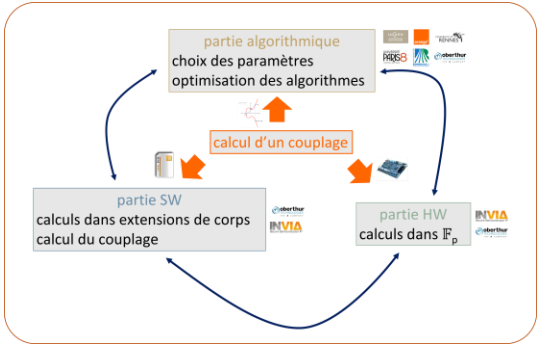
⇒ amélioration de l'algorithmique de calcul d'un couplage
⇒ implémentation d'un couplage efficace sur une carte à puce

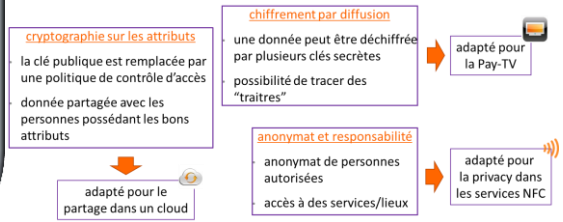
- La cryptographie à base de couplage
  - échange de clé tri-partite
  - signatures électroniques courtes
  - …

⇒ protocoles cryptographiques plus sûrs, plus efficaces

- Sécurité des services
  - confidentialité des données dans un cloud
  - confidentialité des données diffusées
  - anonymat et responsabilité

⇒ des services de télécommunication plus sécurisés





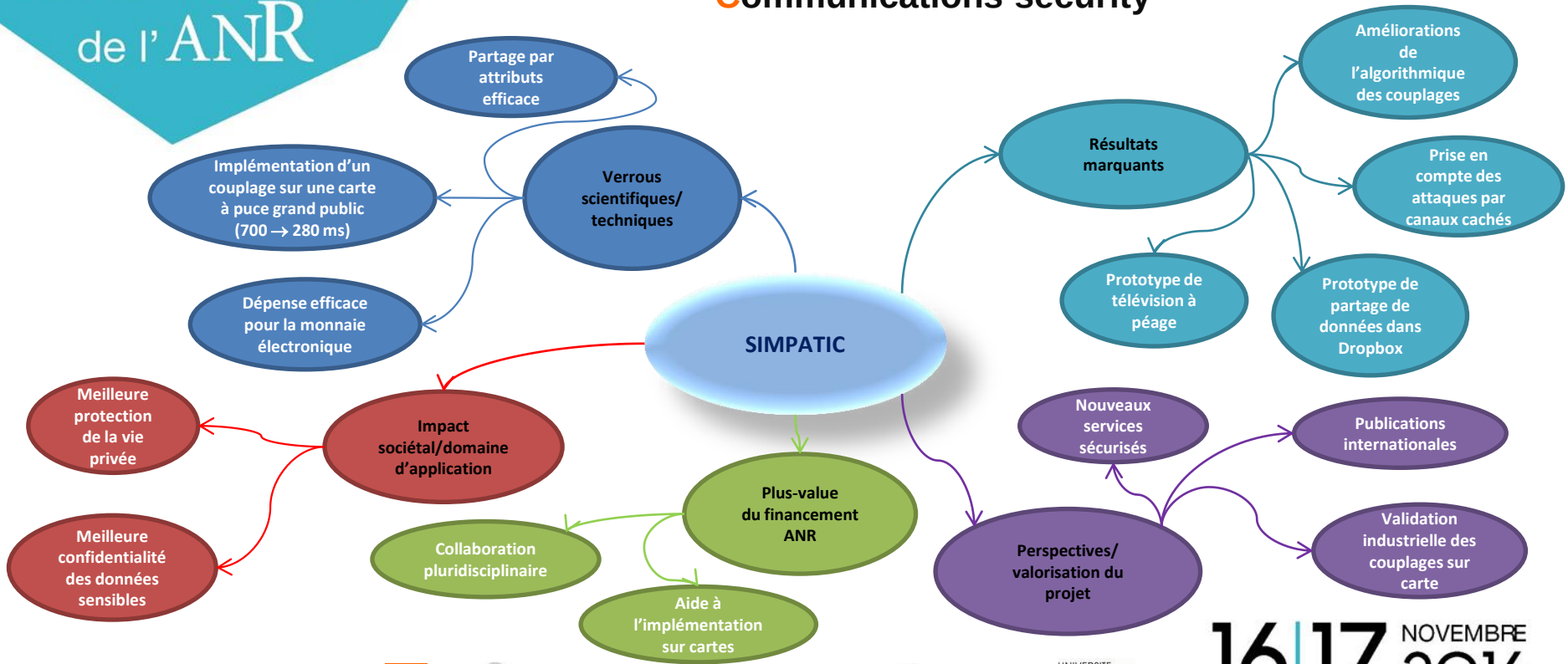
sebastien.canard@orange.com

16|17 NOVEMBRE 2016

Les rencontres du NUMÉRIQUE de l'ANR

SIMPATIC

SIM and PAiring Theory for Information and Communications security



16|17 NOVEMBRE 2016