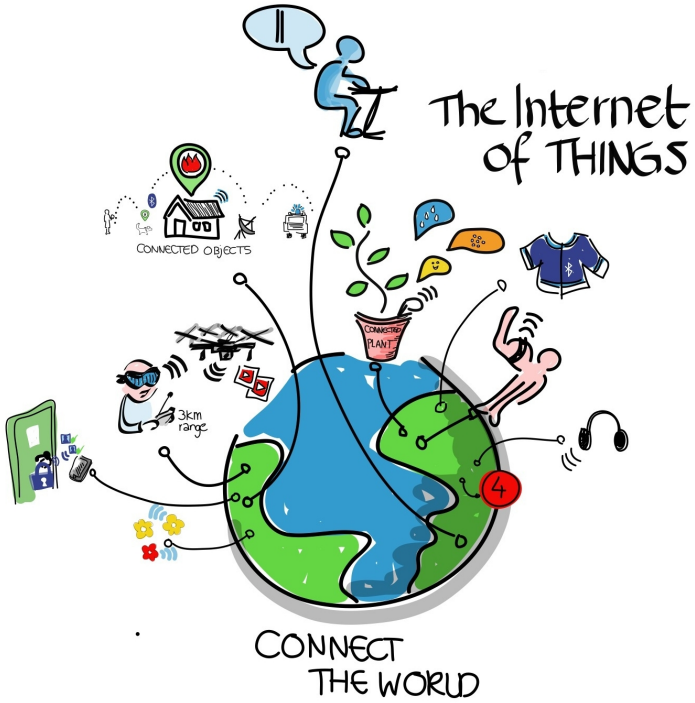
Approche formelle de la sécurité offensive et application à la protection de la vie privée

Pablo Rauzy
pablo.rauzy@inria.fr
pablo.rauzy.name

Audition MCF 4336 – Univ. Paris 8 / LIASD

17 mai 2016 @ Saint-Denis

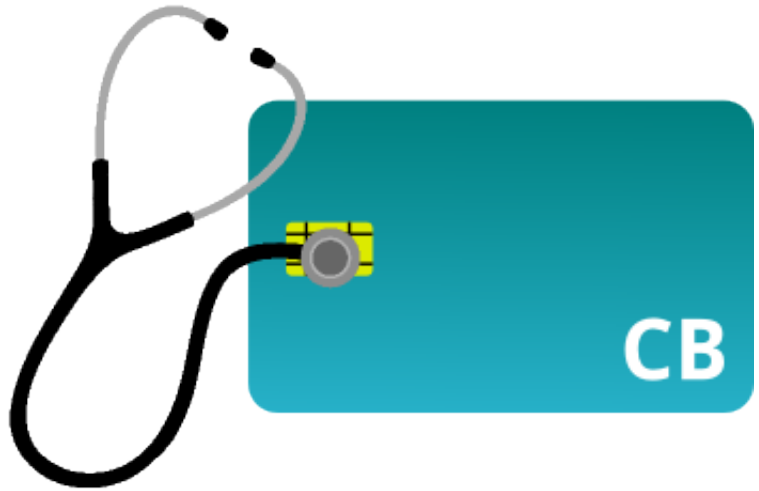
- Systèmes d'information omniprésents et critiques
  - Internet des objets
  - Plateformes mobiles
  - Systèmes cyber-physiques
- Sécurité de l'interface matériel-logiciel jusqu'aux données personnelles ?

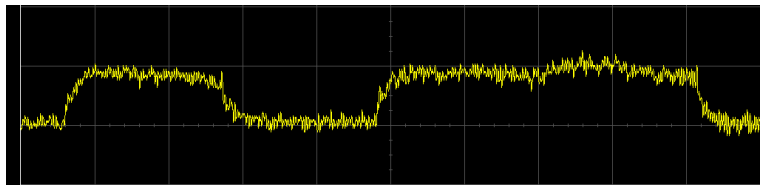


- *Formal Software Methods for Cryptosystems Implementation Security*
- Dans l'équipe SEN du département COMELEC au LTCI (UMR 5141)
- Encadrée par Sylvain Guilley, Professeur à Télécom ParisTech
- Soutenue le 13/07/2015 à l'ENS (mention très honorable)
- Nominée pour le prix de thèse Télécom ParisTech 2016

Canaux auxiliaires

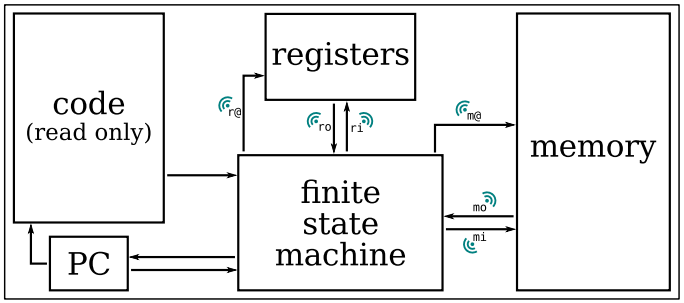
- Mesure de grandeurs physiques
  - Consommation de courant, émanations électromagnétiques, temps de calcul, bruit, lumière, etc.
- Accès à des valeurs intermédiaires du calcul
  - Sortie du cadre de la cryptanalyse classique
  - Cassage de la cryptographie
- État de l'art avant ma thèse = ingénierie
  - Protection à la main des implémentations
  - Pas de preuve formelle
  - Pas de réelle possibilité d'optimisation
  - — Rivain et Prouff (2010) : provable masking



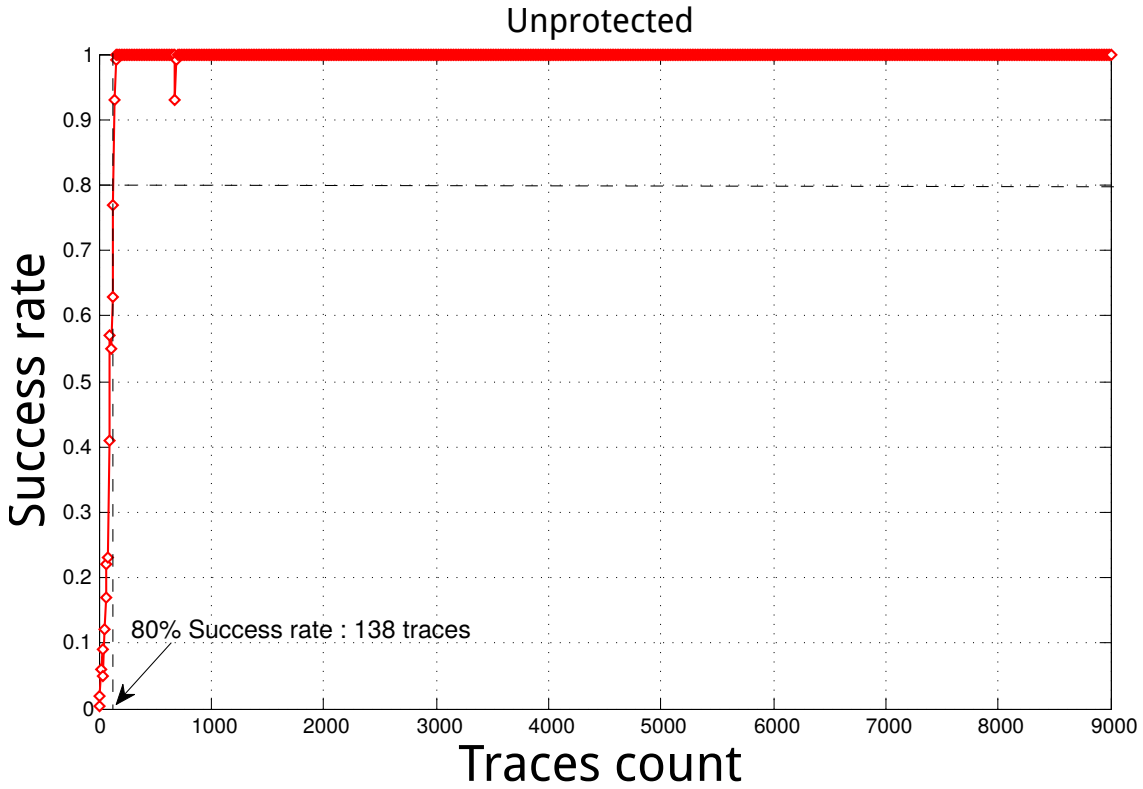


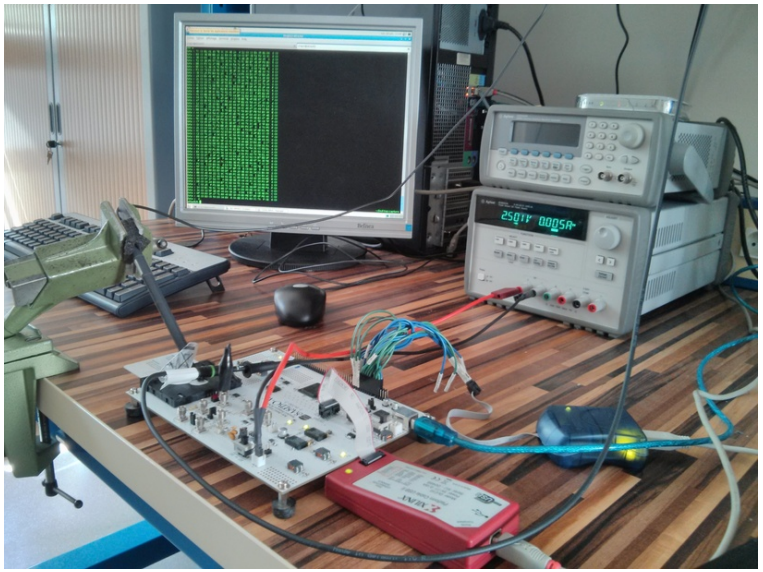
Contributions

- Automatisation de la protection
  - Compilateur assembleur → assembleur protégé
  - Transformation du code prouvée correcte
- Preuve formelle de sécurité
  - Vérification statique de l'équilibre de la consommation par évaluation symbolique sur un processeur logiciel

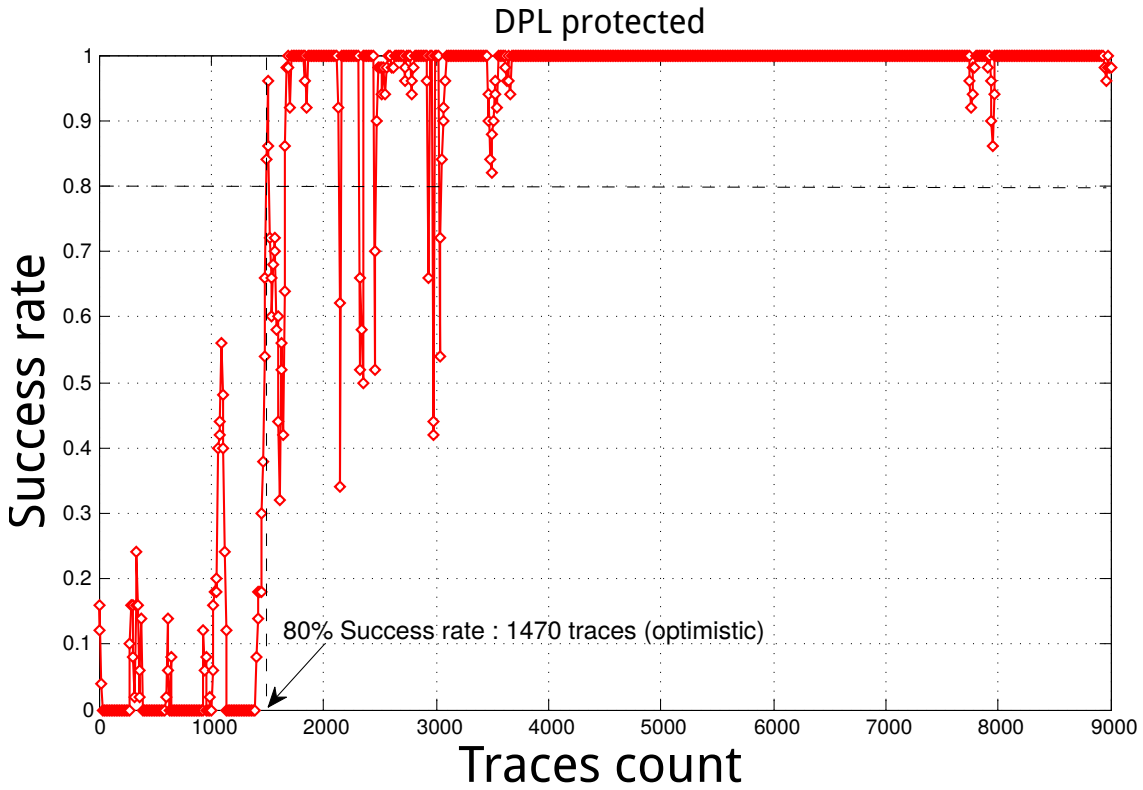


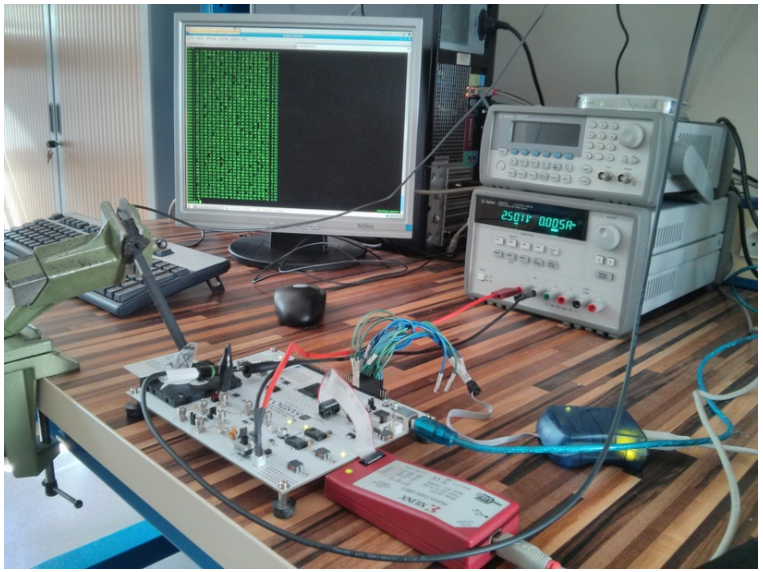
Contributions



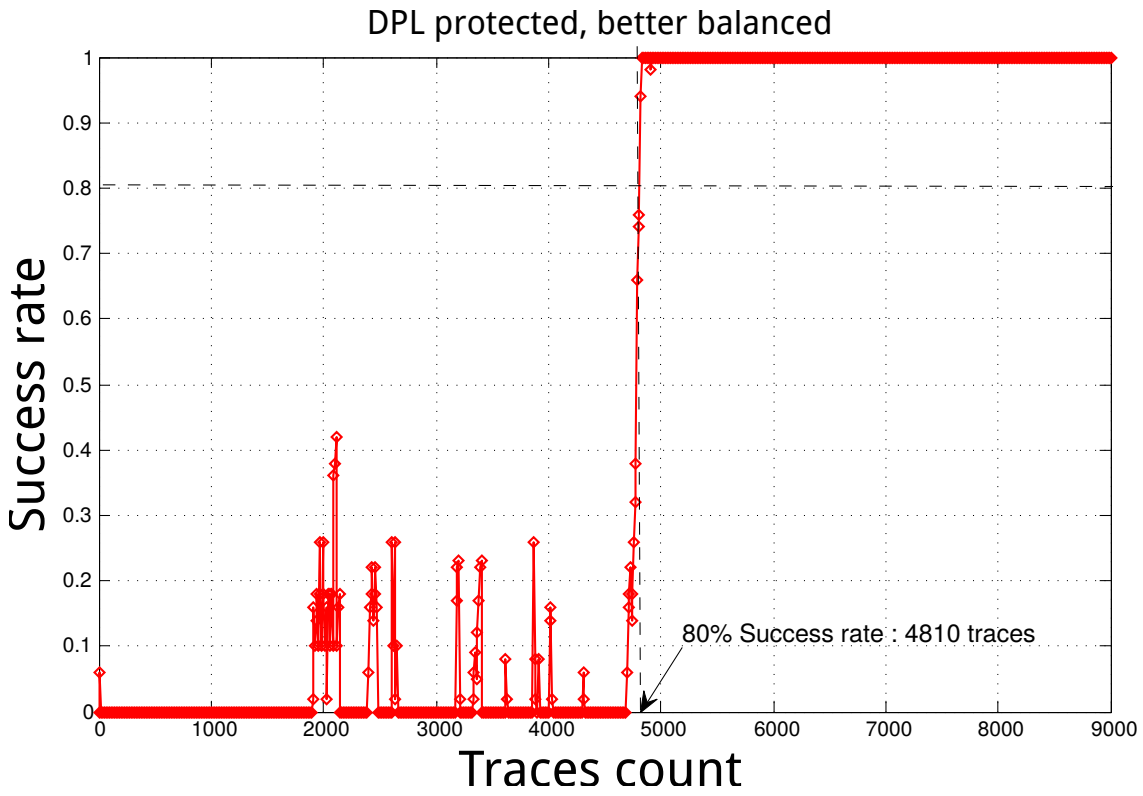


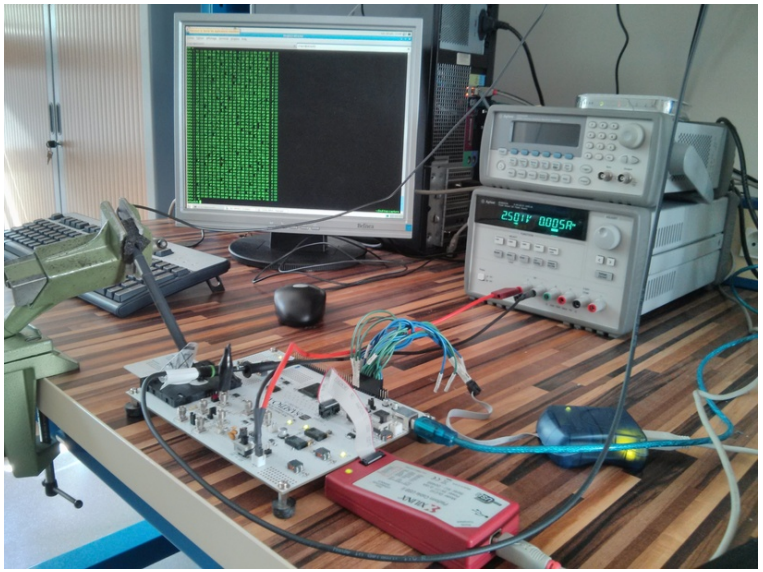
Contributions





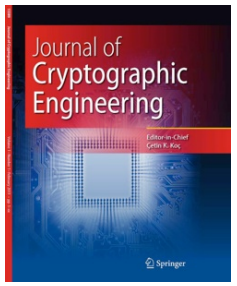
Contributions





Contributions

- Outil open source (paioli)
  - Réutilisé/étudié dans l'académie et l'industrie
- Approche scientifique
  - Preuve de sécurité dans un modèle formel
  - Validation expérimentale du modèle formel
  - Bénéfices :
    - possibilités d'optimisations
    - démonstration de la faisabilité de l'approche formelle
- Dissémination
  - COSADE'13, CHES'13, PROOFS'14, JCEN



Pourquoi la cryptographie ?

- Quels sont les rôles de la cryptographie ?
  - ...
  - Protection de la vie privée
  - ...
- Qu'est ce que c'est "protéger la vie privée" ?

- *Formal Model for Privacy as Control*
- Dans l'équipe-projet Inria Privatics au CITI (EA 3720)
- Encadré par Daniel Le Métayer, Directeur de recherche Inria

Contrôle des données personnelles

- Contexte
  - La privacy n'est plus "le droit d'être laissé tranquille"
  - Elle est de plus en plus définie comme "la capacité des individus à exercer un contrôle sur leurs données personnelles"
- Contribution
  - Formaliser cette notion de *privacy as control* prédominante dans la littérature
  - Proposer une mesure de contrôle
- Méthodologie
  1. Identification de ce qui caractérise le contrôle
  2. Proposition d'un calcul du contrôle équipé d'une sémantique formelle
  3. Description de niveaux de contrôle sur lesquels on peut définir un ordre partiel
- But : apporter une garantie formelle de privacy

AbsoluteCtrl(a,r):
$\mathsf{in_r}(r,o) \Rightarrow \quad a$ can $o\ c\ \varnothing\ \varnothing$
$\wedge\ a$ holds $b\ o\ c\ \varnothing\ \varnothing$

IndirectCtrl(a,r):
$\mathsf{in_r}(r,o) \Rightarrow \exists D_1, \exists D_2,$
a can $o\ c\ D_1\ \varnothing$
$\wedge\ a$ holds $b\ o\ c\ D_2\ \varnothing$
$\wedge\ (d \in D_1 \cup D_2$
$\Rightarrow \mathsf{trust_d}(a,d))$

LegitimatelySharedCtrl(a,r):
$\mathsf{in_r}(r,o) \Rightarrow \exists D_1, \exists W_1, \exists D_2, \exists W_2,$
a can $o\ c\ D_1\ W_1$
$\wedge\ a$ holds $b\ o\ c\ D_2\ W_2$
$\wedge\ (x \in D_1 \cup D_2 \cup W_1 \cup W_2$
$\Rightarrow \mathsf{pers}(r,x))$

Approche formelle de la sécurité offensive et application à la protection de la vie privée

Approche formelle de la sécurité offensive
et application à la protection de la vie privée

Approche formelle de la sécurité offensive
et application à la protection de la vie privée

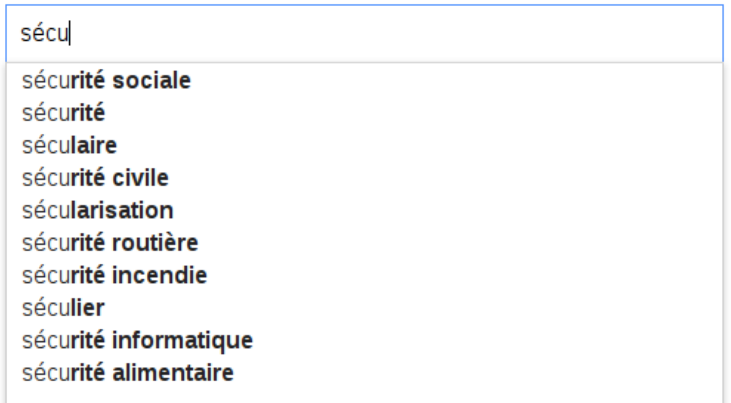
Approche formelle de la sécurité offensive
et application à la protection de la vie privée

Problématiques

- Remettre l'utilisateur dans la boucle
  - La cryptographie ne marche pas : trop compliquée
  - Certifier / prouver la privacy
- Quelles vulnérabilités dans les systèmes actuels ?
  - Internet des objets
  - Plateformes mobiles
  - Systèmes cyber-physiques

Problématiques

- Remettre l'utilisateur dans la boucle
  - La cryptographie ne marche pas : trop compliquée
  - Certifier / prouver la privacy
- Quelles vulnérabilités dans les systèmes actuels ?
  - Internet des objets
  - Plateformes mobiles
  - Systèmes cyber-physiques



Vers un cadre unifié pour la sécurité et la privacy

- Verrou : comprendre la privacy
  - Contrôler ses données personnelles ?
  - Informations déductibles d'un ensemble de données ?
  - Vérifier ou même quantifier la privacy ?
- Verrou : comprendre l'effet d'une vulnérabilité
  - Impact de l'exploitation d'une vulnérabilités sur la privacy ?
  - Rester sécurisé hors spécifications ?
- Verrou : auditer les systèmes
  - Découvrir les vulnérabilités ?
  - Détecter les vulnérabilités connues ?
  - Exploiter l'interface matériel-logiciel ?

Sécurité

+

Privacy

Vers un cadre unifié pour la sécurité et la privacy

- Verrou : comprendre la privacy
  - Contrôler ses données personnelles ?
  - Informations déductibles d'un ensemble de données ?
  - Vérifier ou même quantifier la privacy ?
- Verrou : comprendre l'effet d'une vulnérabilité
  - Impact de l'exploitation d'une vulnérabilités sur la privacy ?
  - Rester sécurisé hors spécifications ?
- Verrou : auditer les systèmes
  - Découvrir les vulnérabilités ?
  - Détecter les vulnérabilités connues ?
  - Exploiter l'interface matériel-logiciel ?

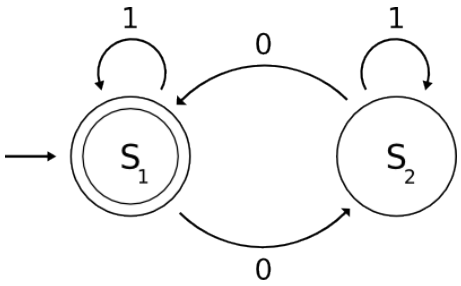
Protéger
les systèmes

+

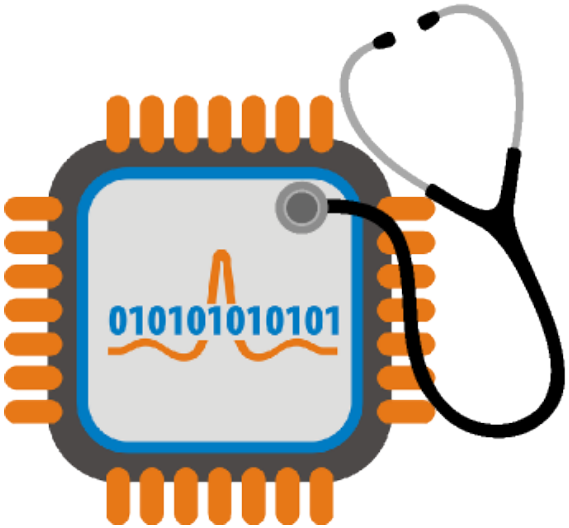
Protéger
les personnes

1/2 — Analyses de vulnérabilités

- Modèles formels de vulnérabilités
  - Modéliser les comportements de vulnérabilités cataloguées
    - dépasser les modèles actuels en tirant parti des canaux auxiliaires
  - Chercher de nouvelles vulnérabilités par approche offensive
    - méthodes d'ingénierie, fuzzing, expertise



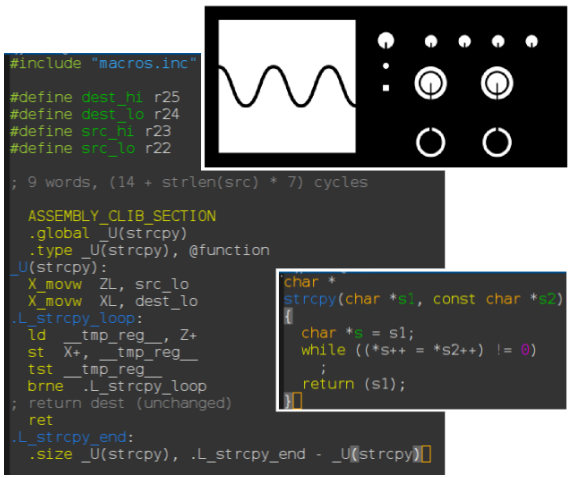
- Analyses hybrides
  - Détecter en boîte-noire les comportements modélisés
    - analyse de binaires : tests concoliques, analyses dynamiques teintées, etc.
    - + traces canaux auxiliaires
  - Tirer parti de la connaissance du code source
    - élimination de faux-positifs, rétroconception en boîte-blanche



- Scénarios d'attaques
  - Prendre en compte l'exploitation de vulnérabilités
    - attaques actives, exploitation de vulnérabilités multiples
    - nouveaux états accessibles du système en dehors des spécifications

1/2 — Analyses de vulnérabilités

- Modèles formels de vulnérabilités
  - Modéliser les comportements de vulnérabilités cataloguées
    - dépasser les modèles actuels en tirant parti des canaux auxiliaires
  - Chercher de nouvelles vulnérabilités par approche offensive
    - méthodes d'ingénierie, fuzzing, expertise
- Analyses hybrides
  - Détecter en boîte-noire les comportements modélisés
    - analyse de binaires : tests concoliques, analyses dynamiques teintées, etc.
    - + traces canaux auxiliaires
  - Tirer parti de la connaissance du code source
    - élimination de faux-positifs, rétroconception en boîte-blanche
- Scénarios d'attaques
  - Prendre en compte l'exploitation de vulnérabilités
    - attaques actives, exploitation de vulnérabilités multiples
    - nouveaux états accessibles du système en dehors des spécifications

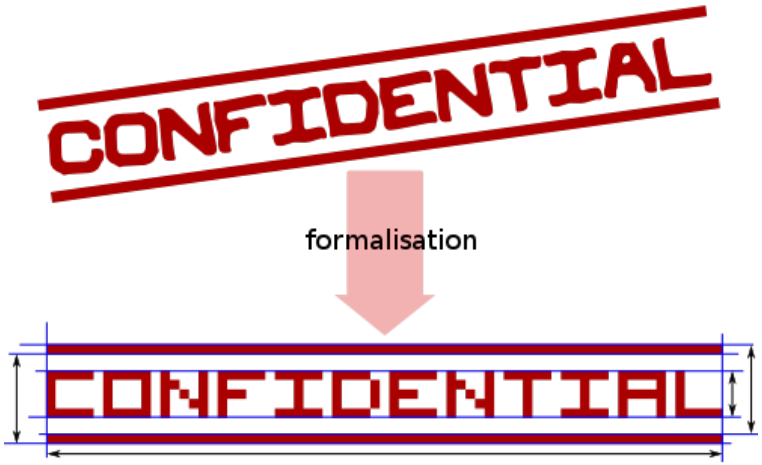


1/2 — Analyses de vulnérabilités

- Modèles formels de vulnérabilités
  - Modéliser les comportements de vulnérabilités cataloguées
    - dépasser les modèles actuels en tirant parti des canaux auxiliaires
  - Chercher de nouvelles vulnérabilités par approche offensive
    - méthodes d'ingénierie, fuzzing, expertise
- Analyses hybrides
  - Détecter en boîte-noire les comportements modélisés
    - analyse de binaires : tests concoliques, analyses dynamiques teintées, etc.
    - + traces canaux auxiliaires
  - Tirer parti de la connaissance du code source
    - élimination de faux-positifs, rétroconception en boîte-blanche
- Scénarios d'attaques
  - Prendre en compte l'exploitation de vulnérabilités
    - attaques actives, exploitation de vulnérabilités multiples
    - nouveaux états accessibles du système en dehors des spécifications

2/2 — Application à la protection de la vie privée

- Formalisation de la privacy
  - Définir une mesure de la privacy
    - contrôle sur les données personnelles
    - catégories d'attaquants, capacités d'inférences, ontologies
  - Unifier la sécurité et la privacy
    - impacts d'une vulnérabilités sur le modèle de privacy
    - scénarios d'attaques
- Approche offensive de la privacy
  - Mettre en œuvre les outils développés
    - vérifications pratiques, démonstrations, sensibilisation
  - Étudier des systèmes sensibles
    - machines de vote, compteurs linky, boitiers assureurs auto, etc.
    - vérification de contrats



2/2 — Application à la protection de la vie privée

- Formalisation de la privacy
  - Définir une mesure de la privacy
    - contrôle sur les données personnelles
    - catégories d'attaquants, capacités d'inférences, ontologies
  - Unifier la sécurité et la privacy
    - impacts d'une vulnérabilités sur le modèle de privacy
    - scénarios d'attaques
- Approche offensive de la privacy
  - Mettre en œuvre les outils développés
    - vérifications pratiques, démonstrations, sensibilisation
  - Étudier des systèmes sensibles
    - machines de vote, compteurs linky, boitiers assureurs auto, etc.
    - vérification de contrats

CNIL
Commission Nationale de l'Informatique et des Libertés

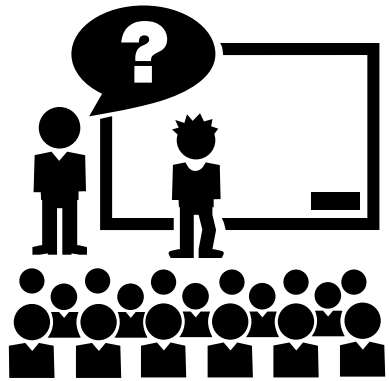
Intégration

- Problématiques de sécurité et privacy au LIASD
  - Informatique des systèmes embarqués pour le handicap et la robotique
  - Intégration de réseaux d'information
  - Informatique médicale embarquée
- À Paris 8
  - Axe de recherche "protection de l'information" côté maths
  - Privacy en lien avec les sciences sociales et juridiques
- Région parisienne et plus
  - Collaborations académiques
    - Collaboration prévue avec D. Naccache (Groupe Sécurité de l'Information au DI ENS)
    - En contact avec G. Barthe (IMDEA Software Institute, Madrid)
    - En contact avec l'équipe Sécurité Électronique Numérique (Télécom ParisTech)
  - Collaborations extérieures
    - Industriels, ANSSI, CNIL...

LIASD
Laboratoire informatique avancée de Saint-Denis
Université Paris 8

UNIVERSITÉ PARIS 8
VINCENNES-SAINT-DENIS

- Passionné et motivé
  - Conserver une connaissance en largeur de l'informatique
  - 200+ heures d'expérience
  - Très bons retours des étudiant·e·s
- Attrait spécifique pour Paris 8
  - Le "Bocal"
  - Institut d'enseignement à distance
  - Interface avec les SHS (mention "Humanités numériques")
  - `#lang` **`racket`**
  - ...



Expérience détaillée

- Informatique scientifique par la pratique (3 × 6h)
  - Projets de L3 à l'ENS par groupe de 2 à 4 étudiants
  - Dont un à donné lieu à une publication
- Programmation en C (32h + 32h)
  - TP de langage C et programmation modulaire (Makefile)
  - ∼15 étudiant·e·s en 3ème année
- Développement web (32h + 40h)
  - TP de HTML, CSS, PHP, et MySQL
  - ∼15 étudiant·e·s en 3ème année

POLYTECH PARIS-UPMC

- Introduction à GNU/Linux et à la ligne de commande (6h)
  - Encadrement du "TP Zéro" de familiarisation avec GNU/Linux
  - ∼30 étudiant·e·s en 1ère année
- Programmation objet et C++ (54h)
  - Cours magistraux, TP, projets, examens sur machine et sur papier
  - ∼30 étudiant·e·s en 4ème année

Possibilités de prise en charge dès l'an prochain

- Licence
  - Programmation (différents langages et paradigmes)
  - Compilation
  - Systèmes et réseaux
  - Technologies web et base de données
  - Fondements mathématiques (logique, calculabilité, etc.)
- M1
  - S1 : UE Fondamentale : Programmation Avancée / $*$
  - S2 : UE Génie logiciel / $*$
- M2 ISE
  - S1 : UE Architectures logicielles des systèmes embarqués / $*$
  - S1 : UE Découverte et initiation à la recherche / Cryptographie

UNIVERSITÉ PARIS 8 VINCENNES-SAINT-DENIS

Assez rapidement par la suite

- M1
  - S1 : UE Découverte
    - Fouille de données
    - Représentation des connaissances
    - Web sémantique et intelligence artificielle
  - S2 : UE Architecture des ordinateurs
    - Microprocesseurs / microcontrôleurs
  - S2 : Initiation à la recherche / Stage pratique en laboratoire
- M2 ISE
  - S1 : UE Architectures matérielles des systèmes embarqués / $*$
  - S1 : UE Découverte et initiation à la recherche
    - Langages de description d'architecture
    - Aide à la décision
    - Technologies et serious games
  - S2 : Stage en laboratoire
- Conférences industrielles et propositions de stages
  - Connexions directes
    - industriels : Gemalto, Oberthur, Google, Secure-IC
    - semi-industriels : ANSSI, CEA
    - start-ups (data processing et images processing principalement)
  - Connexions possibles bien plus nombreuses (à distance 1)

UNIVERSITÉ PARIS 8 VINCENNES-SAINT-DENIS

Programme de recherche

- Approche formelle de la sécurité offensive et application à la protection de la vie privée

Parcours

- DEUG MIAS — Univmed
- L3 Informatique — ENS
- MPRI — ENS
- Thèse — Télécom ParisTech
- Post-doc — Inria

Encadrement

- Stage M2 recherche de Martin Moreau (UPMC, master SFPN)

Enseignement

- 200+ heures de cours, TD, TP, et projets en L3 et M1
- Qualification MCF en sections CNU **27** et 61

Production & Dissémination

- Publications 14 (+3)

Revues internationales à comité de lecture 2
Chapitres d'ouvrage 1
Conf. internationales à comité de lecture 7
Conf. internationales à comité de lecture sans acte 4
(Articles soumis ou en préparation ..... 3)

- Exposés et posters 17

Exposés lors de conférences internationales 6
Exposés lors de conférences nationales 1
Séminaires 8
Présentations de posters en conférence internationale .. 2

- Logiciels 3

Services à la communauté scientifique

- Organisation COSADE'13 et '14, PROOFS'15
- Comité de lecture COSADE'14, SPACE'15, CARDIS'15
- Relecture Journal of Cryptographic Engineering '13 et '16

Collaborations & Mobilité

- Collaboration Á. Kiss, J. Krämer, J.-P. Seifert

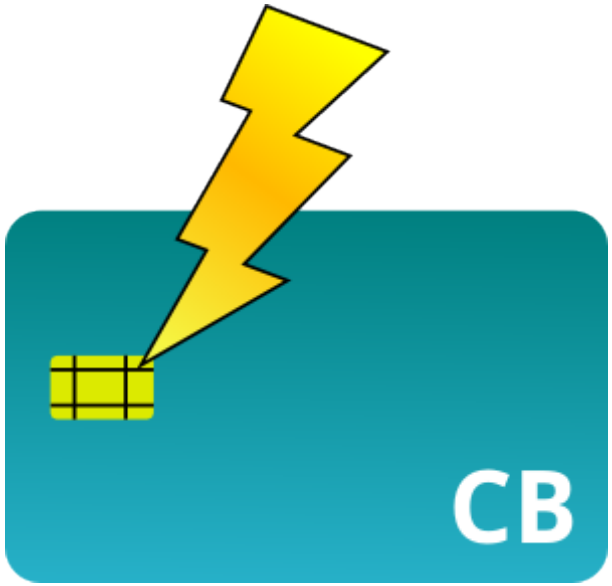
TU Darmstadt et TU Berlin

- Visite de l'équipe de G. Barthe

IMDEA Software Institute, Madrid

Injections de fautes

- Perturbation du système en cours d'exécution
  - Laser, pulse électromagnétique, glitch d'alimentation, etc.
- Résultat fauté
  - Information indirecte sur des valeurs intermédiaires
  - Cassage de la cryptographie
- État de l'art avant ma thèse = ingénierie
  - Contre-mesures développées par essai-erreur
  - Pas de preuve
  - Objectifs de sécurité non-identifiés
  - Christofi (2012) : proved BellCoRe countermeasure



Contributions

- Abstraction et modélisation
  - Conditions de succès d'attaque
  - Modèles de fautes
- Vérification et optimisations de contre-mesures
  - Preuve par réécriture suivant les règles de l'arithmétique modulaire
- Cassage de l'état de l'art
  - Proposition de meilleures contre-mesures
- Automatisation de la méthode de protection

finja report for "crt-rsa_vigilant-fixed_simplified.fia"

Options:
transient faults: disabled.
fault types: randomizing.
Maximum number of faults: 1.

Summary PROTECTED
Total number of different fault injections: 62.
Total number of successful attack: 0 (hide others).

Computation

```
noprop ERR1, ERR2, ERR3, M, e, r ;
prime {p}, {q} ;
dp := { e^-1 mod (p - 1) } ;
dq := { e^-1 mod (q - 1) } ;
iq := { q^-1 mod p } ;
N := p × q ;
p' := p × r × r ;
Mp := M mod p' ;
ipr := p^-1 mod (r × r) ;
Bp := p × ipr ;
Ap := 1 - Bp mod p' ;
M'p := Ap × Mp + Bp × (1 + r) mod p' ;
if M'p + N ≠ M [mod p] abort with ERR1 ;
Spr := M'p^dp mod p' ;
miniSp := 1 + dp × r ;
q' := q × r × r ;
Mq := M mod q' ;
iqr := q^-1 mod (r × r) ;
Bq := q × iqr ;
Aq := 1 - Bq mod q' ;
M'q := Aq × Mq + Bq × (1 + r) mod q' ;
if M'q + N ≠ M [mod q] abort with ERR2 ;
Sqr := M'q^dq mod q' ;
miniSq := 1 + dq × r ;
S := Sqr + q × (iq × (Spr - Sqr) mod p') ;
miniS := miniSq + q × iq × (miniSp - miniSq) ;
if S ≠ miniS [mod r × r] abort with ERR3 ;
return S mod N ;
```

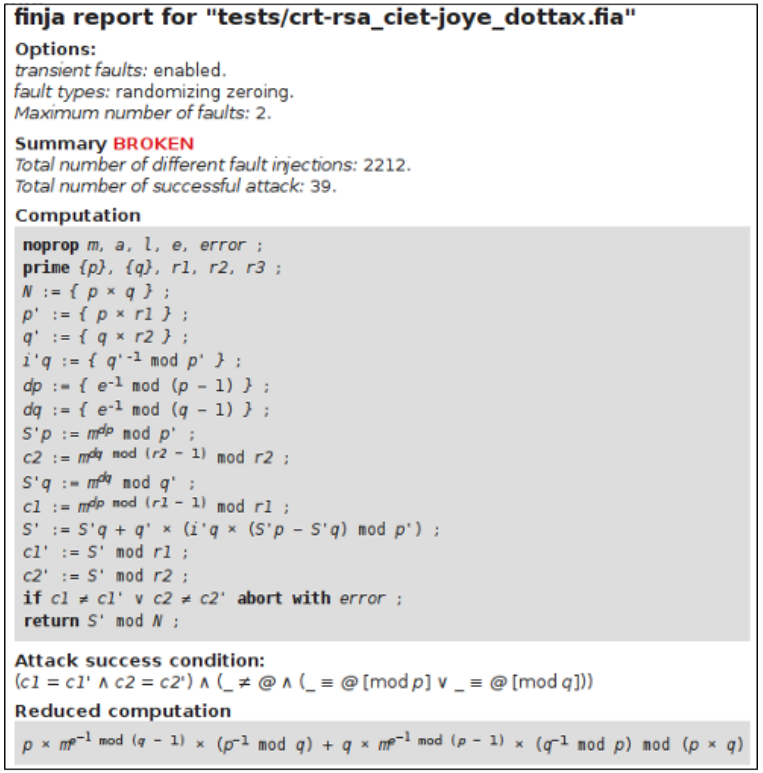
Attack success condition:
$\_ \neq @ \wedge (\_ \equiv @ \ [\mathrm{mod}\ p] \vee \_ \equiv @ \ [\mathrm{mod}\ q])$

Reduced computation

$$p \times M^{e^{-1} \bmod (q-1)} \times (p^{-1} \bmod q) + q \times M^{e^{-1} \bmod (p-1)} \times (q^{-1} \bmod p) \bmod (p \times q)$$

Contributions

- Abstraction et modélisation
  - Conditions de succès d'attaque
  - Modèles de fautes
- Vérification et optimisations de contre-mesures
  - Preuve par réécriture suivant les règles de l'arithmétique modulaire
- Cassage de l'état de l'art
  - Proposition de meilleures contre-mesures
- Automatisation de la méthode de protection



finja report for "tests/crt-rsa_ciet-joye_dottax.fia"

Options:
transient faults: enabled.
fault types: randomizing zeroing.
Maximum number of faults: 2.

Summary BROKEN
Total number of different fault injections: 2212.
Total number of successful attack: 39.

Computation

```
noprop m, a, l, e, error ;
prime {p}, {q}, r1, r2, r3 ;
N := { p × q } ;
p' := { p × r1 } ;
q' := { q × r2 } ;
i'q := { q'^-1 mod p' } ;
dp := { e^-1 mod (p - 1) } ;
dq := { e^-1 mod (q - 1) } ;
S'p := m^dp mod p' ;
c2 := m^dq mod (r2 - 1) mod r2 ;
S'q := m^dq mod q' ;
c1 := m^dp mod (r1 - 1) mod r1 ;
S' := S'q + q' × (i'q × (S'p - S'q) mod p') ;
c1' := S' mod r1 ;
c2' := S' mod r2 ;
if c1 ≠ c1' ∨ c2 ≠ c2' abort with error ;
return S' mod N ;
```

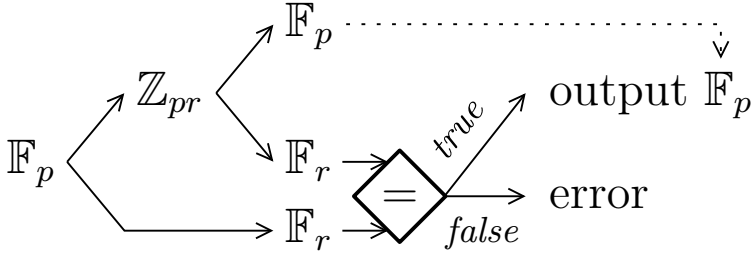
Attack success condition:
$(c1 = c1' \wedge c2 = c2') \wedge (\_ \neq @ \wedge (\_ \equiv @ \,[\mathrm{mod}\, p] \vee \_ \equiv @ \,[\mathrm{mod}\, q]))$

Reduced computation

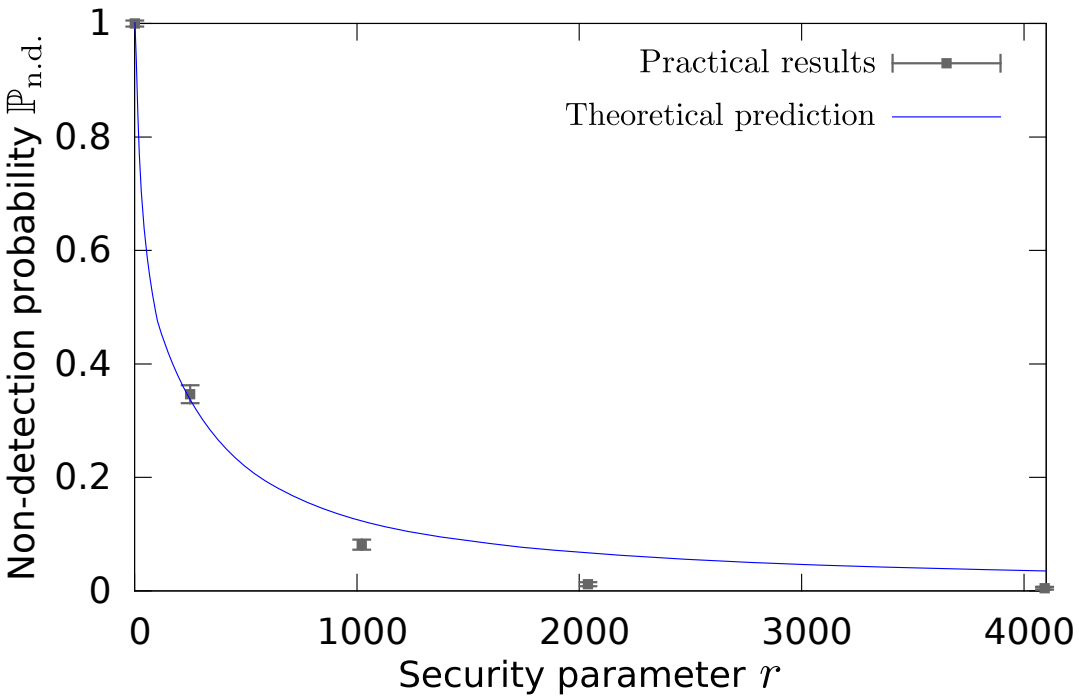
$$p \times m^{e^{-1} \bmod (q-1)} \times (p^{-1} \bmod q) + q \times m^{e^{-1} \bmod (p-1)} \times (q^{-1} \bmod p) \bmod (p \times q)$$

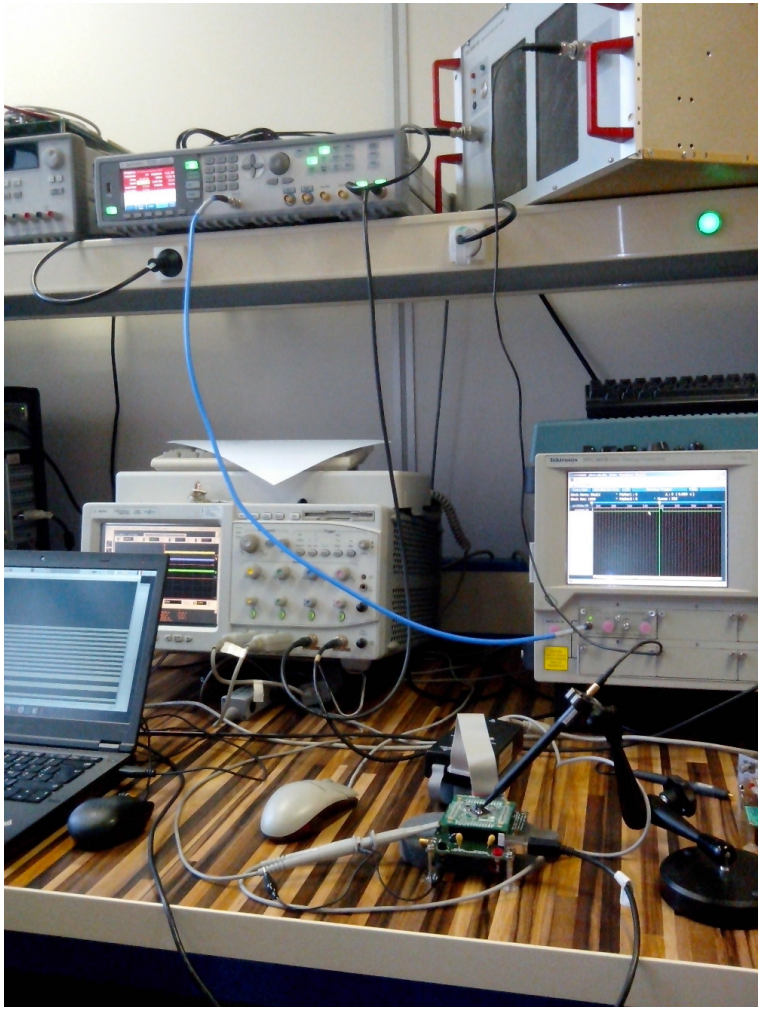
Contributions

- Abstraction et modélisation
  - Conditions de succès d'attaque
  - Modèles de fautes
- Vérification et optimisations de contre-mesures
  - Preuve par réécriture suivant les règles de l'arithmétique modulaire
- Cassage de l'état de l'art
  - Proposition de meilleures contre-mesures
- Automatisation de la méthode de protection



Contributions





Contributions

- Outils open source (finja, enredo)
  - réutilisés/étudiés dans l'académie et l'industrie
- Approche scientifique
  - Modélisation et vérification de contre-mesures
  - Preuve de sécurité dans un modèle formel
  - Validation expérimentale du modèle formel
  - Bénéfices :
    - découverte d'attaques sur l'état de l'art
    - proposition de meilleures contre-mesures
    - généralisation et automatisation de la méthode de protection
- Dissémination
  - PROOFS'13, JCEN, PPREW'14, FDTC'14, HOST'15, TRUDEVICE'15, IACR ePrint + CHES'15, COSADE'16
  - *Handbook of Pairing-Based Cryptography*