# Pascal Lafourcade 26 Avril 1977, 30 ans.

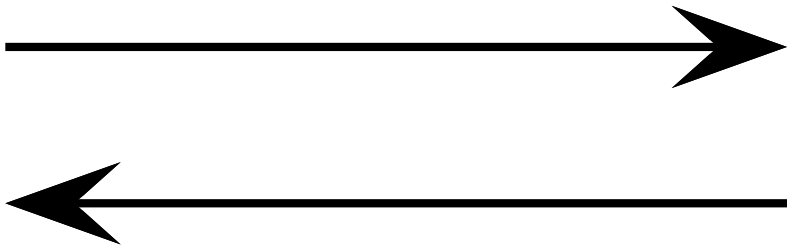
**"Analyse automatique et formelle des propriétés des protocoles de nouvelle génération."**

- **Formation** à l'*Université Paul Sabatier, Toulouse*.
  - DEUG A, 1997.
  - Licence de mathématiques, 1999.
  - Maîtrise de mathématiques, 2001 (Théorie des nœuds).
  - Licence d'informatique, 2001.
  - Maîtrise d'informatique, 2002 (Analyse d'image).
  - DEA RCFR à l'IRIT, Toulouse, 2003 (Aide à la décision).
- **Moniteur et docteur au LSV**, *CNRS & ENS de Cachan*, ACI ROSSIGNOL et RNTL Prouvé, soutenue le 25 Sept 2006.

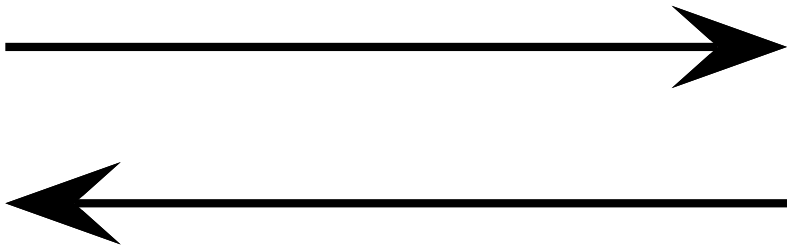
**"Vérification de protocoles cryptographiques en présence de théories équationnelles".**

- **Assistant et post-doctorant** à *l'ETH Zürich*, bourse DGA/CNRS dans l'équipe "Information Security" de D. Basin, 1er Oct 2006.

# Protocoles cryptographiques.

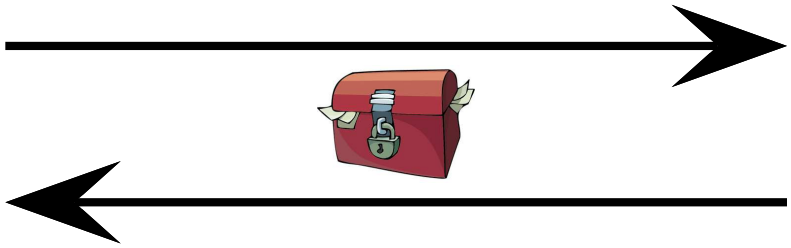


# Protocoles cryptographiques.



Intrus

# Protocoles cryptographiques.



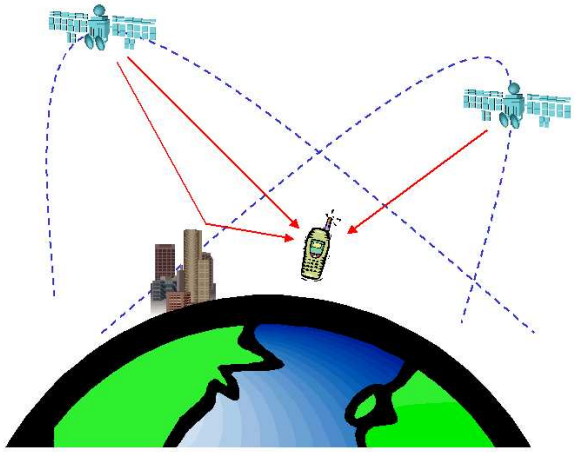
Intrus

Passif : Écoute

Actif : Écoute, intercepte, efface, (re)joue les messages

Propriété de secret : L'intrus ne connaît pas la donnée *confidentielle.*

# Applications.






# Vérification de protocoles cryptographiques.

- Hypothèse de chiffrement parfait.

**L'intrus contrôle le réseau (Modéle de Dolev-Yao [DY801])**

- Chiffrement, déchiffrement.
- Construction, déconstruction de paire.

# Vérification de protocoles cryptographiques.

- Hypothèse de chiffrement parfait.

L'intrus contrôle le réseau (Modéle de Dolev-Yao [DY801])

- Chiffrement, déchiffrement.
- Construction, déconstruction de paire.

En général problème de secret est indécidable. [DLMS'99, AC'01]

# Vérification de protocoles cryptographiques.

- Hypothèse de chiffrement parfait.

L'intrus contrôle le réseau (Modéle de Dolev-Yao [DY801])

- Chiffrement, déchiffrement.
- Construction, déconstruction de paire.

En général problème de secret est indécidable. [DLMS'99, AC'01]

Nombre borné de session : Décidabilité [AL'00, RT'01]

# Vérification de protocoles cryptographiques.

- Hypothèse de chiffrement parfait.

L'intrus contrôle le réseau (Modéle de Dolev-Yao [DY801])

- Chiffrement, déchiffrement.
- Construction, déconstruction de paire.

En général problème de secret est indécidable. [DLMS'99, AC'01]

Nombre borné de session : Décidabilité [AL'00, RT'01]

Affaiblissement de l'hypothèse de chiffrement parfait :

- Dolev-Yao et XOR [CS'03, CKRT'03]
- Autres propriétés algébriques :

$$h(a \oplus b) = h(a) \oplus h(b),$$

$$\{a \oplus b\}_k = \{a\}_k \oplus \{b\}_k \text{ et } \{\{m\}_{k1}\}_{k2} = \{\{m\}_{k2}\}_{k1}$$

# Travaux effectués en thèse.

| | Complexité | |
|---|---|---|
| | **Intrus passif** | **Intrus actif** |
| **ACh** | *NP-Complete* [RTA'05] | *Undecidable* |
| **ACUNh** | *EXP-TIME* [RTA'05] | *Decidable* [ICALP'06] |
| **AGh** | *EXP-TIME* [RTA'05] | *Undecidable* |
| **ACUN{.}. & AG{.}.** | *EXP-TIME* I & C'07 | *?* |
| **ACUN{.}. & AG{.}. Commutatif** | *2EXP-TIME* [Secret'06] | *?* |

Unification, réécriture, systèmes de contraintes, preuve automatique, normalisation de preuves, résolution de systèmes d'équations, $Z$-module.

# Analyse automatique et formelle des propriétés des protocoles de nouvelle génération.

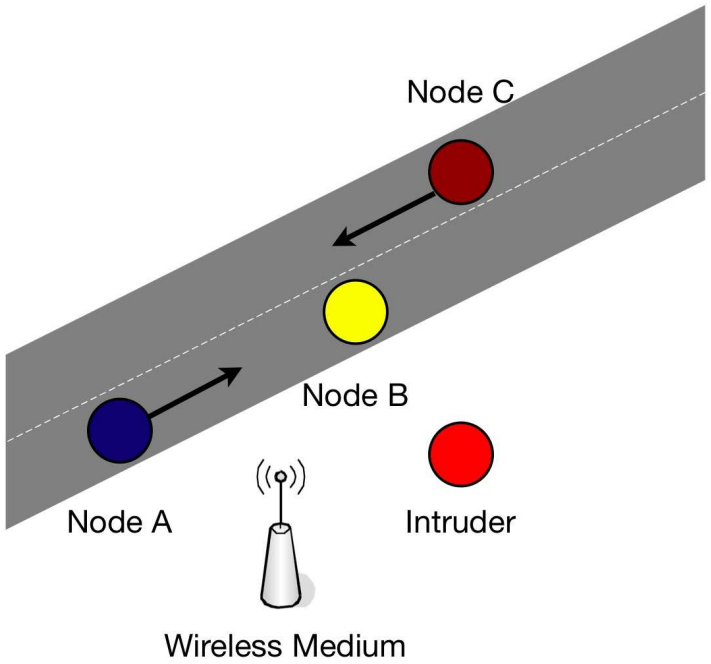
- Propriétés à satisfaire.
- Environnement.
- Implantation.
- Opérateurs algébriques utilisés.

I *Étude des propriétés des réseaux sans fil.*
II *Modélisation et vérification des Web Services.*
III *Analyse formelle des protocoles de groupe.*
IV *Vérification des protocoles de vente aux enchères et de vote.*

# I Étude des propriétés des réseaux sans fil.

VerSePro : Verification of Security and privacy Protocols for wireless networks (MICS).

- Modélisation et vérification de la propriété de **voisinage**.
- Analyse de protocoles en tenant compte de la **mobilité** des agents.




Collaboration avec David Basin, Srdjan Capkun, Patrick Schaller (ETH Zürich, Suisse).

NCCR MICS
National Competence Center In Research
Mobile Information and Communication Systems

# II Modélisation et vérification des Web Services.



- Composition de plusieurs protocoles.
- Implantation en XML.
- Propriétés algébriques.

Collaboration avec Yannick Chevalier
(IRIT, Toulouse).

# III Analyse formelle des protocoles de groupe.

- Création d'un groupe.
- Ajout d'un membre.
- Exclusion d'un membre.

Le nombre de participants n'est pas fixe.

**Objectif**: Etendre le modèle de clauses de Horn de B. Blanchet afin d'obtenir une sous-classe décidable de protocoles "*récursifs*" pour vérifier formellement les protocoles de groupe.

Collaboration avec Ralf Kuester
(ETH Zürich, Suisse).

# IV Vérification des protocoles de vente aux enchères et de vote.

- **Protocoles de vente aux enchères.**
  - Secret / Intergrité des informations.
  - Non-répudiation des offres.
  - Authentification et anonymité des participants...

Collaboration avec Bogdan Księżopolski et Cas Cremers
(Université de Lublin, Pologne & ETH Zürich Suisse).

- **Protocoles de vote.**
  - Secret / Intergrité des votes.
  - Anonymité de votants : chiffrement homomorphique

$$\Pi\{m_i\}_k = \{\Sigma m_i\}_k$$

Collaboration avec Luca Viganò et Sebastian Mödersheim
(Université de Vérone, Italie & IBM Zürich, Suisse).

**Journaux internationaux:**

• Lafourcade, Lugiez, Treinen. *Intruder Deduction for the Equational Theory of Abelian Groups with Distributive Encryption.* Information & Computation, 2007

• Cortier, Delaune, Lafourcade. *A Survey of Algebraic Properties Used in Cryptographic Protocols.* Journal of Computer Security 14(1), 2006

• Lafourcade.*Intruder Deduction for the Equational Theory of Exclusive-or with Commutative and Distributive Encryption.* SecReT'06, ENTCS

**Conférences internationales :**

• Delaune, Lafourcade, Lugiez, R. Treinen. *Symbolic Protocol Analysis in Presence of a Homomorphism Operator and Exclusive Or.* ICALP'06

• Lafourcade, Lugiez, Treinen. *Intruder Deduction for AC-like Equational Theories with Homomorphisms.* RTA'05

**Autres publications et soumissions :**

• S. Delaune, P. Lafourcade, D. Lugiez, R. Treinen. Symbolic Protocol Analysis for Monoidal Equational Theories. Information & Computation'07

• Ksiezopolski, Lafourcade. *Attack and Revison of an Electronic Auction Protocol using OFMC.* IBIZA'07

• Lafourcade, Lugiez, R. Treinen. ACUNh: Unification and Disunification Using Automata Theory. Workshop UNIF'06

• Lafourcade.*Vérification des protocoles cryptographiques en présence de théories équationnelles.* Thèse , LSV, ENS Cachan, Sept 2006