

Analyse automatique et formelle des propriétés des protocoles de nouvelle génération

Projet LANDE - IRISA Rennes

Pascal Lafourcade

Information Security ETH Zürich

pascal.lafourcade@inf.ethz.ch



Pascal Lafourcade 26 Avril 1977, 30 ans.



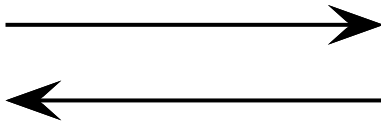
- **Formation** à l'Université Paul Sabatier, Toulouse.
 - DEUG A, 1997.
 - Licence de mathématiques, 1999.
 - Maîtrise de mathématiques, 2001 (Théorie des nœuds).
 - Licence d'informatique, 2001.
 - Maîtrise d'informatique, 2002 (Analyse d'image).
 - DEA RCFR à l'IRIT, Toulouse, 2003 (Aide à la décision).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

“Vérification de protocoles cryptographiques en présence de théories équationnelles”.

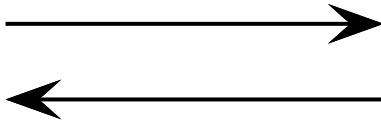
- **Post-doctorant et assistant** à l'ETH Zürich, bourse DGA/CNRS dans l'équipe “Information Security” de D. Basin, 1er Oct 2006.

“Analyse automatique et formelle des propriétés des protocoles de nouvelle génération.”

Protocoles cryptographiques.



Protocoles cryptographiques.



Intrus



Protocoles cryptographiques.



Intrus



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

Protocoles cryptographiques.



Intrus

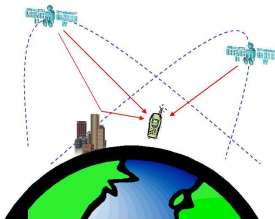


Passif : Écoute.

Actif : Écoute, intercepte, bloque, (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 (Modèle de Dolev-Yao [DY81])

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

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

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

Vérification de protocoles cryptographiques.

- Hypothèse de chiffrement parfait.

L'intrus contrôle le réseau (Modèle de Dolev-Yao [DY81])

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

En général le 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.

Théories	Complexité	
	Intrus passif	Intrus actif
ACh	<i>NP-Complet</i> [RTA'05]	<i>Indécidable</i>
ACUNh	<i>EXP-TIME</i> [RTA'05]	<i>Decidable</i> [ICALP'06]
AGh	<i>EXP-TIME</i> [RTA'05]	<i>Indécidable</i>
ACUN{.}. & AG{.}.	<i>EXP-TIME</i> I & C'07	?
ACUN{.}. & AG{.}. Commutatif	<i>2EXP-TIME</i> [Secret'06]	?

Model-checking, unification, réécriture, systèmes de contraintes, preuve automatique, résolution de systèmes d'équations, Z-module.

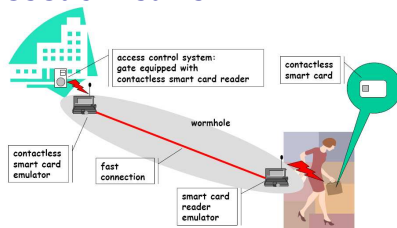
Analyse automatique et formelle des propriétés des protocoles de nouvelle génération.

- a) Propriétés à satisfaire
 - b) Environnement
 - c) Implantation
 - d) Opérateurs algébriques utilisés
-
- I *Étude des propriétés des réseaux sans fil (a,b)*
 - II *Modélisation et vérification des services web (c,d)*
 - III *Analyse formelle des protocoles de groupe (a,b,d)*
 - IV *Vérification des protocoles d'enchères et de vote (a,d)*

I Étude des propriétés des réseaux sans fil.

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

- Modélisation de la propriété de **voisinage**.
- Vérification de protocoles de voisinage (**mobilité, wireles ...**).



Collaboration avec D. Basin, S. Capkun, P. Schaller
(ETH Zürich, Suisse)

Projet LANDE : User Supervised Device Pairing
Nouveau modèle de l'intrus.
T. Jensen & T. Genet (Thomson R&D)



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

II Modélisation et vérification des services web.



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

Collaboration avec Y. 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:

Obtenir une sous-classe décidable de protocoles "*récurifs*".

Collaboration avec R. Kuester & T. Truderung
(ETH Zürich, Suisse & Wroclaw Pologne).
T. Genet (IRISA)

Propriétés à satisfaire et propriétés algébriques.

IV Vérification des protocoles de vente aux enchères et de vote. (I)

- **Protocoles de vente aux enchères.**

- Secret des données.
- Intégrité des informations.
- Non-répudiation des offres.
- Authentification et anonymité des participants...



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

Propriétés à satisfaire et propriétés algébriques.

IV Vérification des protocoles de vente aux enchères et de vote. (II)

- **Protocoles de vote.**
 - Secret des votes.
 - Intégrité des votes.
 - Authentification des votant.
 - Anonymité de votants : chiffrement homomorphique



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

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

Mise à jour

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** 2006
- Lafourcade. *Intruder Deduction for the Equational Theory of Exclusive-or with Commutative and Distributive Encryption*. ENTCS, **SecReT'06**

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**

Soumissions :

- Basin, Capkun, Lafourcade, Schaller, *Verification of Neighbourhood*. **CCS'07**
- Cremers, Lafourcade, *Comparing State Spaces in Automatic Security Protocol Verification*. **CONCUR'07**
- Ksiezopolski, Lafourcade. *Attack and Revision of an Electronic Auction Protocol using OFMC*. **IBIZA'07**
- Delaune, Lafourcade, Lugiez, Treinen. *Symbolic Protocol Analysis for Monoidal Equational Theories*. **Information & Computation'07**

Projet LANDE - IRISA Rennes

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

Pascal LAFOURCADE

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