LAAS-CNRS
Unité propre de recherche du CNRS
7 avenue du Colonel Roche
31077 TOULOUSE Cedex 4 FRANCE
Tél. : +33 (0) 5 61 33 62 00
Fax. : +33 (0) 5 61 55 35 77
Courriel : laas-contact@laas.fr
www.laas.fr

Séminaires du LAAS-CNRS

Laboratoire d'Analyse et d'Architecture des Systèmes du CNRS

USAGES PUBLICS ET CACHÉS DES FONCTIONS DE HACHAGE

par
M. le Professeur Jean-Jacques Quisquater
Université Catholique de Louvain - Belgique

Mercredi 15 novembre 2006 à 10 h 00
LAAS-CNRS - Salle de Conférences

Pôle
SINC

résumé de l'exposé

Nous verrons en termes simples les différents usages de ces fonctions dans les différents champs de l'informatique et de la sécurité. De façon informelle, une fonction de hachage associe un grand ensemble de données à un petit ensemble, représentatif du premier. On parlera aussi de condensé ou d'empreinte.

Les applications sont nombreuses. Si on utilise astucieusement plusieurs fonctions de hachage, on parlera alors de filtres de Bloom.

On utilise diverses variantes de fonctions de hachage en pratique pour :

- les dictionnaires,
- la gestion des droits d'auteurs,
- le stockage de mots de passe,
- les signatures électroniques,
- le chiffrement,
- les protocoles cryptographiques,
- les générateurs de nombres aléatoires,
- l'anonymat,
- le décodage d'erreurs,
- le routage de paquets (IPv6),
- les réseaux peer-to-peer,
- la localisation de ressources en général,
- le stockage efficace de mesures dans des réseaux,
- etc.

Nous verrons tout cela y compris les problèmes d'implantations.

l'orateur

Le Professeur Jean-Jacques QUISQUATER est de nationalité belge. Il est marié (Myriam), a deux enfants dont Michaël, chercheur … en cryptographie (à l'INRIA).

Il est ingénieur civil en mathématiques appliquées (1970) et a un doctorat d'Etat en science informatique obtenu en 1987 au Laboratoire de Recherche en Informatique (LRI) d'Orsay.

Il a travaillé entre 1970 et 1991 au laboratoire de recherches Philips où il dirigeait une équipe en cryptographie : il a ainsi contribué à l'étude de la mise en œuvre de la cryptographie dans les cartes à puce (2 premières mondiales : première carte à puce avec le DES, système standard de cryptographie à clé secrète, première carte à puce avec un coprocesseur RSA standard de cryptographie à clé publique).

Il est aujourd'hui professeur de cryptographie et de sécurité multimédia au département d'électricité, à la Faculté de Sciences appliquées de l'Université Catholique de Louvain, à Louvain-la-Neuve (Belgique).

Il est le principal concepteur des coprocesseurs cryptographiques Philips actuels pour les cartes à puce. Il détient 17 brevets dans le domaine de la carte à puce. Il a publié plus de 150 papiers dans des revues de conférences internationales, dans les domaines de la théorie des graphes et surtout de la cryptographie. Il est co-inventeur d'un schéma cryptographique fort connu, le protocole GQ, utilisé par environ 100 millions d'ordinateurs – clients dans le monde, sous licence Novell (NDS, netware). Il a un nombre d'Erdös de deux.

Il est un directeur de l'IACR (International Association for Cryptology Research), membre du comité d'organisation de CARDIS et ESORICS, et de plusieurs comités IFIP. Il a reçu un doctorat honoris causa de l'Université de Limoges, le prix Montefiore, l'Award Kristian Beckman et la chaire Fermat (sans compter la chaire Franqui, en Belgique) pour 2004.