École de Printemps
Cryptographie et sécurité informatique

24 – 28 avril 2006
Sorèze, Tarn

www.laas.fr/crypto-sec/

Informations générales

Cette école vise à faire le point sur les avancées récentes dans ces domaines, en apportant un éclairage particulier à certains aspects primordiaux, plutôt qu'une présentation couvrant la totalité de ces domaines, qui ne pourrait être que superficielle. Le public concerné comprend principalement des étudiants et des chercheurs en informatique et en réseau, ainsi que des ingénieurs d'entreprises innovantes dans les technologies de l'information et des communications.

L'école est organisée en ½ journées, chacune animée par un scientifique de haut niveau, passionné par son domaine, et qui aura à cœur de transmettre sa passion. Les conférenciers ont été choisis pour leur compétence reconnue internationalement, et ils sont tous francophones, ce qui devrait favoriser l'interaction et les discussions entre les participants.

L'école est organisée par le LAAS-CNRS, avec le soutien du Conseil Régional de Midi-Pyrénées, la Fédération de Recherche en Informatique et Automatique (FÉRIA) et l'Association pour le Développement de l'Enseignement, de l'Économie et des Recherches de Midi-Pyrénées (ADERMIP).

Thème de l'École

La cryptographie et la sécurité informatique sont des domaines très liés, tout en appartenant à des disciplines scientifiques différentes : la cryptographie fait surtout appel aux mathématiques, alors que la sécurité informatique relève davantage de l'ingénierie, tout en utilisant les algorithmes développés en cryptographie.

La cryptographie est un domaine très actif depuis une trentaine d'années, mais des avancées récentes remettent en cause des résultats qui semblaient définitivement établis. Par exemple, de nouvelles attaques contre les fonctions de hachage fragilisent considérablement les techniques actuelles de signature numérique qui sont couramment utilisées dans le commerce électronique, ainsi que bon nombre des protocoles dits « sécurisés » d'Internet.

De son côté, la sécurité informatique a connu une révolution avec le développement d'Internet : jusqu'alors, c'était principalement un souci limité à quelques centres de traitement sensibles (militaires, bancaires, administrations, etc.), qu'on pouvait rendre très sûrs en contrôlant efficacement les accès et en s'assurant de la probité des personnels autorisés. Avec l'ouverture des réseaux sur Internet, et la prolifération des ordinateurs personnels, les techniques d'attaque se sont diversifiées et multipliées. Contre ces menaces, les techniques classiques de la sécurité sont insuffisantes, et de nouvelles approches sont nécessaires. Ceci conduit à développer des techniques d'authentification forte et de traçabilité, qui en retour sont des menaces contre la vie privée des citoyens. Toutes ces menaces provoquent la méfiance du public vis-à-vis de ces nouvelles technologies, ce qui est un frein au développement économique qu'on pourrait en attendre. Il est donc primordial d'améliorer la sécurité tout en préservant la vie privée, ce qui est crucial pour de nouvelles applications liées à la santé, à la vie démocratique (vote électronique), aux relations entre citoyens et administrations, etc.

Informations pratiques

L'école se tiendra du 24 au 28 avril 2006 à l'Abbaye de Sorèze http://www.abbayeecoledesoreze.com/. Les frais d'inscription sont de 1400 Euros en plein tarif et 400 Euros au tarif étudiant. Les frais d'inscription comprennent :

- la participation à toutes les ½ journées d'étude,
- les supports de cours,
- la pension complète à l'Hôtellerie de l'Abbaye http://www.hotelfp-soreze.com/ :
  - en chambre individuelle au Logis des Pères (***) pour les inscriptions plein tarif,
  - en chambre double au Pavillon des Hôtes (**) pour les étudiants,
- l'excursion (visite guidée de Carcassonne) le mercredi après-midi,
- le transport en bus de Toulouse à Sorèze et retour :
  - Lundi 24 avril : départ aéroport de Toulouse-Blagnac 10h20, départ gare de Toulouse-Matabiau 10h45, arrivée à Sorèze 11h45.
  - Vendredi 28 avril : départ Sorèze 16h30, arrivée aéroport de Toulouse-Blagnac 17h30, arrivée gare de Toulouse-Matabiau 18h15.

Le nombre de places est limité. Il est donc recommandé de s'inscrire le plus tôt possible.

Bourses : Des bourses en nombre limité pourront être accordées à certains étudiants, sur dossier (lettre de motivation de l'étudiant, lettre de recommandation d'un encadrant), pour réduire de moitié leurs frais d'inscription.

Les informations pratiques détaillées seront disponibles sur le site http://www.laas.fr/crypto-sec/.

Programme

Lundi 24 avril après-midi

Jean-Jacques Quisquater (Université Catholique de Louvain, Belgique)

La cryptographie par la théorie des graphes

La théorie des graphes et la cryptologie interagissent de plus en plus : voici quelques sujets que nous évoquerons de façon très abordable par chacun :

- preuves d'apports nuls de connaissances (*zero-knowledge*) par isomorphisme de graphes,
- graphes réguliers de faible diamètre pour le transport physique de secrets,
- preuves de sécurité utilisant les graphes d'expansion (*expanders*),
- graphes de chiffrement utilisant ou non des graphes de Cayley,
- les fonctions de hachage et leurs généralisations (la fonction de Zemor-Tillich et ses généralisations), utilisées pour vérifier l'intégrité des données,
- problème de la sécurité du logarithme discret,
- ...

Jean-Jacques Quisquater *est ingénieur en mathématiques appliquées (UCL, Louvain,1970) et a un doctorat d'Etat en science informatique (1987) du 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 de recherche 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-la-Neuve (Belgique) et responsable du groupe UCL Crypto. 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 est titulaire d'une Chaire Pierre de Fermat de la Région Midi-Pyrénées (2004-2006), en coopération avec le LAAS-CNRS.*

Mardi 25 avril matin

Yves Deswarte (LAAS-CNRS, France)

Protection de la vie privée sur Internet

Alors que la protection de la vie privée est considérée dans notre société comme l'un des droits fondamentaux, elle est constamment menacée dans le cyber-espace, soit de par la négligence ou la malveillance de certains opérateurs ou fournisseurs de services, soit de par des demandes toujours plus importantes de traçabilité et d'authentification forte pour lutter contre le crime et le terrorisme. Cet exposé présentera les technologies de protection de la vie privée (ou PETs pour *Privacy-Enhancing Technologies*) qu'on peut mettre en œuvre sur Internet : gestion d'identités virtuelles, communications anonymes, autorisation préservant la vie privée, gestion des données personnelles. On montrera aussi comment ces technologies permettent de protéger les internautes contre les abus, sans pour autant protéger les criminels.

Yves Deswarte *est directeur de recherche au CNRS, membre du groupe "Tolérance aux fautes et sûreté de fonctionnement informatique" du LAAS-CNRS. Après quelques années de recherche et développement dans l'industrie (CII et CIMSA), il a rejoint l'INRIA et le LAAS-CNRS où ses travaux de recherche ont porté principalement sur la tolérance aux fautes et la sécurité dans les systèmes répartis. Plus récemment, il s'est aussi intéressé aux critères d'évaluation de la sûreté de fonctionnement, à l'évaluation quantitative de la sécurité des systèmes d'informations, à la protection de systèmes critiques multi-niveaux, aux modèles et politiques de sécurité pour les systèmes d'information et de communication dans le domaine de la santé, et aux technologies de protection de la vie privée. Il a été consultant auprès de différentes entreprises françaises (Aérospatiale, Matra-Espace, CNES, Airbus, Dassault Aviation, EADS), ainsi que de SRI International aux États-Unis. Il est membre de l'IEEE, de l'ACM et de la SEE. Il est le représentant de l'IEEE Computer Society auprès de l'IFIP TC-11 (Technical Committee on Security and Protection in Information Processing Systems).*

Mardi 25 avril après-midi

Yannick Chevalier (IRIT, France)

Analyse de protocoles dans un modèle abstrait

Je présenterai un modèle d'étude de protocoles cryptographiques dans lequel les détails des primitives cryptographiques utilisées sont abstraits via des hypothèses de correction des opérations de chiffrement. Dans ce modèle, je présenterai différentes études réalisables, telles que :

- la recherche d'attaques sur des traces de longueur bornée, par rapport à un attaquant actif,
- la notion plus forte de non-divulgation, qui est au centre des protocoles de vote, vis-à-vis d'un attaquant qui se contente de regarder passer les messages échangés.

***Yannick Chevalier** a soutenu en décembre 2003 sa thèse au Loria (Nancy) sur le thème de la résolution de problèmes d'accessibilités liés à l'analyse de protocoles cryptographiques. Il a notamment travaillé sur le renforcement des pouvoirs de déduction d'un intrus essayant d'attaquer activement un protocole en utilisant des propriétés fines non prises en compte dans le cadre de la cryptographie "boite noire". En collaboration avec M. Rusinowitch, il a aussi montré comment il était possible de modulariser la recherche d'attaque par rapport aux différentes opérations que l'intrus pouvait effectuer. Il est actuellement maître de conférences à l'Université Paul Sabatier (Toulouse), et travaille au sein du groupe LiLaC à l'IRIT.*

Mercredi 26 avril matin

Jean-Marc Couveignes (GRIMM, France)

Cryptologie asymétrique, factorisation et logarithme discret

Je présenterai quelques notions fondamentales et quelques uns des principaux protocoles de la cryptologie asymétrique ainsi que les problèmes algorithmiques sur lesquels reposent la sécurité de ces protocoles. Je présenterai ensuite des résultats d'algorithmique et de complexité qui vont dans le sens d'une preuve de cette sécurité, ou qui, au contraire, tendent à la compromettre. Cela me conduira à introduire quelques notions et résultats mathématiques concernant les corps finis, les courbes algébriques (et en particulier elliptiques), les réseaux euclidiens et l'algorithme LLL, mais aussi des notions et le vocabulaire de la théorie de la complexité, indispensables à cette exposition.

***Jean-Marc Couveignes** est professeur à l'université de Toulouse 2, directeur de l'équipe GRIMM (EA3686). Il est depuis 2005 membre de la commission enseignement de la Société Mathématique de France. De 2003 à 2005 il était chargé de mission à la MSTP (MENRT) pour l'expertise des Masters de mathématiques. De 2002 à 2003, il était membre du jury de l'agrégation, et membre de la section 25 du CNU de 1999 à 2003. De 1990 à 1997, il était ingénieur de l'armement, détaché au laboratoire A2X de Bordeaux de 1994 à 1997. Il a préparé sa thèse de 1991 à 1994 sous la direction d'Henri Cohen et Jacques Stern.*

Mercredi 26 avril après-midi : Excursion (visite de Carcassonne)

Mercredi 26 avril soir

Paulo Veríssimo (Université de Lisbonne, Portugal)

Architectures tolérant les intrusions : concepts et conception

Les architectures informatiques distribuées ont donné lieu à de nombreuses recherches sur les méthodes et algorithmes, à la fois dans les domaines de la tolérance aux fautes et de la sécurité. Cependant l'approche classique de la sécurité a privilégié, à peu d'exceptions près, la prévention des intrusions. La tolérance aux intrusions (TaI) est une nouvelle approche qui a émergé petit à petit durant la dernière décennie, pour prendre un élan considérable récemment. Au lieu d'essayer d'empêcher chaque intrusion individuellement, on les accepte, mais en les tolérant : le système déclenche des mécanismes qui évitent que l'intrusion ne mette en défaut la sécurité, et cela automatiquement. Dans cette présentation, nous décrivons les concepts fondamentaux ainsi que les stratégies et les mécanismes principaux pour réaliser des systèmes tolérant les intrusions, et nous ferons le point sur les récentes avancées des architectures de systèmes TaI distribués.

Paulo Veríssimo *est actuellement professeur au Département d'Informatique de la Faculté des Sciences à l'Université de Lisbonne (http://www.di.fc.ul.pt/~pjv). Il a présidé le comité technique Fault-Tolerant Computing de l'IEEE et le comité de pilotage de la conférence DSN. Il a été membre de l'European Security & Dependability Advisory Board et a coordonné le projet CORTEX (http://cortex.di.fc.ul.pt) du programme européen IST/FET. Il faisait partie du bureau exécutif du Réseau d'Excellence européen CaberNet. Il est éditeur associé de l'IEEE Transactions on Dependable and Secure Computing. Paulo Veríssimo dirige le groupe de recherche Navigators du LASIGE, et ses recherches actuelles portent sur l'architecture, les intergiciels et les protocoles pour les systèmes distribués, ubiquitaires, et embarqués, pour les aspects d'adaptativité temps-réel et de tolérance aux fautes et aux intrusions. Il est l'auteur de plus de 130 publications dans des conférences et des revues internationales, et il est co-auteur de cinq livres (voir par exemple, http://www.navigators.di.fc.ul.pt/dssa/).*

Jeudi 27 avril matin

Peter Ryan (Université de Newcastle, Grande-Bretagne)

"Prêt à Voter" : Un système de vote électronique pratique et vérifiable par les votants

Récemment, les systèmes de vote électronique ont attiré l'attention, à propos de la légitimité des élections présidentielles de 2000 et 2004 aux États-Unis, ou du vote par correspondance au Royaume-Uni. C'est aujourd'hui un défi considérable que de concevoir des technologies et des systèmes de vote qui soient à la fois sûrs, pratiques et acceptables par toutes les parties prenantes (électorat, politiciens, responsables d'élections, experts en sécurité, etc.). Cet exposé présentera le schéma "Prêt-à-Voter", qui possède la propriété surprenante d'être vérifiable par les votants, qui peuvent confirmer que leur vote est bien pris en compte, tout en préservant le secret de leur vote. La satisfaction de cette propriété ne repose que d'une façon minimale des composants du système, tout en fournissant la plus grande transparence possible. Les hypothèses sous-tendant le schéma actuel seront discutées, ainsi que les vulnérabilités potentielles qui en découlent, et les contre-mesures qui permettent de s'en prémunir. Je décrirai aussi comment le schéma supervisé originel peut-être adapté au contexte du vote à distance, avec des capacités de résister à la coercition.

Peter Ryan *a rejoint la School of Computing Science et le CSR de Newcastle en janvier 2002, et il y dirige les recherches sur la sécurité du projet DIRC (Dependability Interdisciplinary Research Collaboration). Il a plus de 20 ans d'expérience dans les domaines de la vérification formelle et de la garantie de l'information. Il a été à l'origine de l'application de l'algèbre des processus à la modélisation et à l'analyse des protocoles de sécurité. Il est l'auteur de nombreuses publications sur la cryptographie, les protocoles cryptographiques, les politiques de sécurité, les modèles mathématiques de la sécurité informatique, et plus récemment des systèmes de vote électronique. Avant de rejoindre l'Université de Newcastle en 2002, il a travaillé aux GCHQ, CESG, Defence Research Agency, SRI International et au Software Engineering Institute (CMU, Pittsburg). Il a obtenu un PhD en physique mathématique à l'Université de Londres. Peter Ryan a été membre des comités de programmes de plusieurs conférences prestigieuses en sécurité, notamment : IEEE Security and Privacy, IEEE Computer Security Foundations Workshop, the European Symposium On Research In Computer Security (ESORICS), WITS (Workshop on Issues in the Theory of Security). Il a présidé WITS'04, co-présidé ESORICS'04 et Frontiers of Electronic Elections FEE 2005. Depuis 1999, il preside le comité de pilotage d'ESORICS. Il est aussi member de l'IFIP WG 1.7 et de l' UK Grid Security Task Force.*

Jeudi 27 avril après-midi

Pierre Paradinas (CNAM-CEDRIC, France)

La présentation sera axée autour de deux thèmes distincts.

(i) Mesures de performances des systèmes embarqués du type Java Card

Après avoir introduit la technologie de la Java Card, et les notions de *benchmarking* on s'attachera à étudier les spécificités du domaine de la mesure de performance des cartes. On présentera la démarche du projet MESURE et les premiers résultats.

(ii) Virtualisation de système et sécurité

La tendance dans les systèmes d'exploitation -mais pas uniquement- est à la virtualisation des ressources matérielles mais aussi de plus en plus de services de niveau divers. On montrera les problèmes de sécurité liés à la virtualisation. Un WIP (*work in progress*) en cours sur la plateforme Jaluna sera exposé.

Pierre Paradinas *a obtenu un doctorat en Informatique à l'Université de Lille en 1988, sur la carte à microprocesseur appliquée au domaine de la santé. Il a été fondateur et directeur technique de Biocarte Technologie SA qui concevait et distribuait des cartes santé en 1988. Il a ensuite rejoint Gemplus, comme chercheur, responsable des produits avancés (carte SCQL), et auditeur technologique. En 1995, il co-dirige le laboratoire RD2P commun aux universités lilloises et à Gemplus.*

Jeudi 27 avril soir

Sandra Marcello (Thales, France)

Cryptosystèmes basés sur l'identité

Les cryptosystèmes basés sur l'identité sont apparu récemment en cryptologie, en 2001, Boneh et Franklin avec leur proposition répondait à une question de Shamir qui datait de 1984. Nous évoquerons les principes des cryptosystèmes basés sur l'identité. Le cadre utilisé sera celui des courbes elliptiques.

***Sandra Marcello** est cryptologue chez Thales depuis 2005. De 2002 à 2004, elle était chercheure au Max-Planck Institut fuer Mathematik (Bonn, Allemagne), après un séjour postdoctoral de 2001-2002 à l'Université de Regensburg (Allemagne, dans le cadre du réseau européen Arithmetic Algebraic Geometry). Elle a soutenu fin 2000 une thèse de mathématiques sur la théorie des nombres à l'Université Paris 7. Elle est auteur de plusieurs publications en théorie des nombres.*

Vendredi 28 avril matin

Serge Vaudenay (EPFL, Suisse)

Comment échanger une clef après 30 ans de Diffie-Hellman ?

Bien que l'échange de clef de Diffie-Hellman soit connu depuis 1976, il n'est toujours pas évident d'échanger une clef entre deux participants de manière sûre. Dans cet exposé, on passe en revue les méthodes classiques pour établir une communication sécurisée avec des études de cas comme SSL et Bluetooth. On étudie aussi de nouvelles méthodes fondées sur l'existence de canaux intègres de communication authentifiée qui permettent de transmettre une faible quantité de donnée. On présente de nouveaux résultats parus à CRYPTO 2005, CT-RSA 2006 et PKC 2006.

***Serge Vaudenay** est un ancien élève de l'École Normale Supérieure. Il a reçu son doctorat de l'Université de Paris 7 en 1995 avant d'entrer au CNRS. En 1999, il fut nommé professeur à l'École Polytechnique Fédérale de Lausanne (EPFL). Ses travaux portent sur la cryptographie et la sécurité des informations numériques. Il a écrit une cinquantaine d'articles scientifiques et un ouvrage sur la cryptographie publié aux éditions Springer. Il fut le directeur du comité de programme de plusieurs conférences, dont EUROCRYPT 2006, PKC 2005, SAC 2001 et FSE 1998.*

Vendredi 28 avril après-midi

Yvo Desmedt (University College London, Grande-Bretagne)

Déni de service et sécurité des réseaux de télécommunication

La plupart des attaques contre les réseaux de télécommunication sont dirigées contre les terminaux, et pas contre les routeurs. Néanmoins, à la conférence "BlackHat 2005", il a été montré que la sécurité des systèmes d'exploitation des routeurs était loin d'être idéale. Dans ce contexte, une attaque contre les routeurs n'est pas une hypothèse farfelue et purement académique : elle pourrait se révéler critique. Les protocoles TCP/IP et IPSEC par exemple, n'offrent pas de résistance contre ce type d'attaque.

Bien entendu, si l'adversaire est capable de contrôler tout le réseau, il n'y a pas de solution. C'est la raison pour laquelle nous ferons l'hypothèse que (i) soit l'adversaire peut contrôler un nombre limité de noeuds, (ii) soit les noeuds que l'adversaire contrôle peuvent être spécifiés par une structure de l'adversaire. Par ailleurs, ce dernier peut adopter une stratégie passive ou active (Byzantine) pour écouter clandestinement le trafic véhiculé sur le réseau. Des solutions seront présentées pour des réseaux point-à-point, et pour des réseaux de diffusion générale (*broadcast*).

***Yvo Desmedt** a reçu son Ph.D. (Summa cum Laude) de l'Université de Leuven en Belgique (1984). Il est actuellement BT Chair of Information Security à l'University College London, UK. Il est aussi professeur honoraire à Florida State University, USA. Ses travaux de recherche s'intéressent principalement à la cryptographie, la sécurité des réseaux et la sécurité des ordinateurs. Il a été co-président du comité de programme de CANS 2005, et président du comité de programme de PKC 2003, ACM Workshop on Scientific Aspects of Cyber Terrorism (2002) et Crypto'94. Il est également éditeur en chef (avec le Professeur Cox) de la revue IEE Proceedings of Information Security, éditeur du Journal of Computer Security, ainsi que de Information Processing Letters. De renommée internationale, il est régulièrement invité à donner des présentations lors de conférences.*

Découper selon le pointillé

FORMULAIRE D'INSCRIPTION

École de Printemps

Cryptographie et sécurité informatique

Abbaye de Sorèze, 24-28 avril 2006

A renvoyer au plus tard le 15 avril 2006 à :

Sylvie Barrouquère — ADERMIP
32 rue des Cosmonautes — 31400 TOULOUSE
tel : 05 62 47 49 89 — fax : 05 62 47 49 85 — email : barrouquere@adermip.com

Mme / Mlle / M. NOM : ..... Prénom : .....

Société/Laboratoire : .....

Adresse : .....

.....

Téléphone : ..... Télécopie : .....

E-mail :.....

Moyen de transport prévu : ❑ Avion ❑ Train ❑ Voiture

Date, heure et lieu d'arrivée : .....

Date, heure et lieu de départ : .....

	Forfait journées d'études plein tarif	1 400,00 Euros
	Forfait journées d'études tarif étudiant (joindre copie de la carte d'étudiant)	400,00 Euros

Montant total à régler : .....

Les frais d'inscription comprennent les supports de cours, la pension complète à l'Hôtellerie de l'Abbaye (en chambre individuelle pour les inscriptions plein tarif, en chambre double pour les étudiants), l'excursion (visite guidée de Carcassonne), le transport en bus entre Toulouse et Sorèze et le retour vers Toulouse :
• 24 avril : départ aéroport de Toulouse-Blagnac à 10h20, départ gare de Toulouse-Matabiau à 10h45
• 28 avril : départ Sorèze 16h30, arrivée Toulouse-Blagnac 17h30, arrivée Toulouse-Matabiau à 18h15.

Adresse de facturation si celle-ci est différente de celle indiquée ci-dessus :

Règlement :

❑ par bon de commande à l'ordre de l'ADERMIP (joindre le bon de commande),

❑ par chèque bancaire à l'ordre de l'ADERMIP (joindre le chèque),

❑ par virement : compte n° 10268 - 02504 - 12719500200 – 49
IBAN : FR76 1026 8025 0412 7195 0020 049 - BIC : COURFR2T
Banque COURTOIS, 33 rue de Rémusat, 31000 TOULOUSE.

❑ par carte bleue :

Titulaire de la carte : _____ Date et signature :

N° de carte : _____

Date expiration : _____

Pour toute information complémentaire ou demande particulière, contactez :

Mme Marie-José Fontagne – Service Communication
LAAS/CNRS, 7 Av. Colonel Roche — 31077 Toulouse cedex 4
tél : 05 61 33 69 35, fax : 05 61 55 35 77, email : fontagne@laas.fr

Note : Il est possible de s'inscrire en ligne sur le site http://www.laas.fr/crypto-sec/

École de Printemps

Cryptographie et sécurité informatique

24 – 28 avril 2006
Sorèze, Tarn

Conférenciers

Jean-Jacques Quisquater (*Prof., Université Catholique de Louvain, Belgique*)

Yves Deswarte (*Directeur de Recherche, LAAS-CNRS, France*)

Yannick Chevalier (*Maître de Conférence, IRIT, France*)

Jean-Marc Couveignes (*Professeur, GRIMM, France*)

Paulo Veríssimo (*Professeur, Université de Lisbonne, Portugal*)

Peter Ryan (*Professeur, Université de Newcastle, Grande-Bretagne*)

Pierre Paradinas (*Professeur, CNAM-CEDRIC, France*)

Sandra Marcello (*Cryptologue, Thales, France*)

Serge Vaudenay (*Professeur, EPFL, Suisse*)

Yvo Desmedt (*Professeur, University College London, Grande-Bretagne*)

www.laas.fr/crypto-sec/