

# Département STIC du CNRS

## RTP 13 Sécurité

*Responsable : Michel Riguidel*

*Rapport rédigé avec le comité de pilotage et en particulier :*

*Jacques Stern, Philippe Grangier, Refik Molva*

*Et les porteurs d'Actions Spécifiques*

*Décembre 2003*

<b>Table des Matières</b>	
<a href="#"><u>Table des Matières</u></a>	2
<a href="#"><u>Introduction – les enjeux de la sécurité</u></a>	4
<a href="#"><u>Nouveaux projets qui démarreront en 2004 et projets en cours</u></a>	6
<a href="#"><u>Projets Européens où le RTP 13 est présent</u></a>	6
<a href="#"><u>Projets Nationaux</u></a>	7
<a href="#"><u>ACI Crypto et Sécurité</u></a>	7
<a href="#"><u>RNRT</u></a>	7
<a href="#"><u>RNTL</u></a>	7
<a href="#"><u>Verrous scientifiques jugés prioritaires pour le RTP, caractéristique de l'orientation de la thématique</u></a>	7
<a href="#"><u>Besoins en plate-forme ou autre instrument</u></a>	8
<a href="#"><u>AS 39 Tatouage</u></a>	11
<a href="#"><u>Résultats de l'AS 39</u></a>	12
<a href="#"><u>Publications récentes</u></a>	12
<a href="#"><u>AS Sécurité logicielle : modèles et vérification (commune avec le RTP 19)</u></a>	14
<a href="#"><u>AS Crypto Quantique</u></a>	14
<a href="#"><u>RTP 13 - AS « Photons uniques à la demande » (Philippe Grangier)</u></a>	16
<a href="#"><u>Objectifs Généraux de l'AS</u></a>	16
<a href="#"><u>Laboratoires partenaires</u></a>	16
<a href="#"><u>Résumé des contributions</u></a>	16
<a href="#"><u>A. Cryptographie quantique utilisant une source à un seul photon.</u></a>	17
<a href="#"><u>B. Sources à photons uniques utilisant des dispositifs à semi-conducteurs.</u></a>	17
<a href="#"><u>Communications présentées dans le cadre de l'AS.</u></a>	19
<a href="#"><u>AS - Nouvelle tendances en Cryptographie</u></a>	20
<a href="#"><u>Atelier sur la sécurité prouvée à l'ENS</u></a>	20
<a href="#"><u>Colloque par l'équipe Crypto du Laboratoire d'informatique de l'École polytechnique et le projet TANC de l'INRIA Futurs</u></a>	21
<a href="#"><u>REUNION RTP 13 AS NOUVELLES TENDANCES EN CRYPTOGRAPHIE</u></a>	22
<a href="#"><u><b>e-JUSTICE</b> : Towards a global security and visibility framework for Justice in Europe</u></a>	25
<a href="#"><u><b>INSPIRED</b> : Integrated Secure Platform for Interactive Personal Devices</u></a>	25

---

<b><u>PRIME</u></b> : <u>Privacy and Identity Management for Europe</u>	26
<b><u>s-BORDER</u></b> : <u>Privacy respectful and threat tuneable traveller smart monitoring system</u>	27
<b><u>SECOQC</u></b> : <u>Development of a Global Network for Secure Communication based on Quantum Cryptography</u>	27
<b><u>SEINIT</u></b> : <u>Security Expert INITiative</u>	28
<b><u>ECRYPT</u></b> : <u>European Network of Excellence in Cryptology</u>	29
<b><u>FIDIS</u></b> : <u>The Future of Identity in the Information Society</u>	30
<b><u>Specific Targeted Research Projects</u></b>	31
<b><u>DIGITAL PASSPORT</u></b> : <u>Next generation European Digital Passport with Biometric Data for Secure and Convenient Boarder Passage</u>	31
<b><u>MEDSI</u></b> : <u>Integration of Geographical Information Systems with DB, decision support management and an auditory system to develop an advanced system that will be able to give support on decisions in a crisis.</u>	31
<b><u>POSITIF</u></b> : <u>Policy-based Security Tools and Framework</u>	32
<b><u>SCARD</u></b> : <u>Side-Channel Analysis Resistant Design Flow</u>	32
<b><u>SECURE JUSTICE</u></b> : <u>Secure communication and collaboration framework for the judicial co-operation environment.</u>	33
<b><u>SECURE PHONE</u></b> : <u>Secure contracts signed by telephone</u>	34

## Introduction – les enjeux de la sécurité

La numérisation du monde développé est en marche et l'univers numérique s'imisce dans tous les secteurs d'activité : industrie, commerce, finance, défense, administration, santé, éducation, justice, environnement.

Les enjeux de la sécurité à l'aube du 3<sup>ème</sup> millénaire soulèvent des questions de souveraineté comme la maîtrise du transport et du stockage de l'information sur le territoire national, des questions économiques comme la valorisation de la distribution des contenus en ligne, des questions sociologiques comme l'instauration de la confiance pour le citoyen dans les édifices numériques (Internet mais aussi la téléphonie mobile, les réseaux bancaires ou logistiques d'étiquetage numérique), ainsi que des questions éthiques comme l'enregistrement à son insu des données numériques personnelles d'un individu, ses dépenses successives à la banque, sa localisation géographique dans une cellule de relais téléphonique chez l'opérateur de télécoms, ses connexions sur les serveurs Web chez le fournisseur d'accès Internet, son apparence et son comportement sur les caméras sur la voie publique...

Les objectifs de sécurité ont évolué depuis une dizaine d'années et les menaces ont radicalement changé suite à l'incursion systématique de la mobilité des acteurs dans le monde numérique, l'obligation de la prise en compte de l'hétérogénéité des systèmes dans les transactions de bout en bout et la massification des contenus, par l'arrivée des contenus multimédia.

La sécurité a changé de visage ces dernières années. Elle restait jadis confinée dans des dispositifs supplémentaires particuliers, un anti-virus sur son ordinateur personnel, un pare-feu dans le réseau son entreprise, un serveur de certificats ou le module IPSec pour sécuriser le protocole IP. Elle était une fonctionnalité additionnelle que l'on greffait sur chaque composant, sur chaque technologie ou sur chaque système. Elle apparaît maintenant scellée aux grands systèmes numériques (le téléphone, les réseaux informatiques d'entreprise, Internet, le GSM, WiFi), organisée comme une archéologie millésimée de concepts et de dispositifs, enfouie dans le cœur des systèmes d'information existants, eux-mêmes, véritables tours de Babel, assemblées de modules et de composants dont les technologies sont de maturités distinctes et d'âges différents.

La sécurité moderne se conçoit de nos jours comme une propriété intrinsèque des systèmes. On a ainsi vu naître la sécurité propriétaire du GSM avec ses protocoles et ses algorithmes spécifiques, celle du WiFi, avec ses modifications rapides pour combler les failles de sécurité de la première génération d'équipements, et celle de Bluetooth avec des modèles de sécurité si particuliers (piconets, scatternets). Mais cette approche se révèle aussi réductrice car elle n'appréhende pas l'hétérogénéité des systèmes. La sécurité doit désormais s'exprimer plus en termes d'écosystèmes dynamiques qui se déploient, se développent et se défendent en étant immergés dans un milieu ambiant, lui-même informatisé, qu'il faut protéger contre les agressions de toute nature (erreur accidentelle, altération malveillante, espionnage, attaque terroriste). C'est par une vision systémique que la nouvelle sécurité pourra absorber les aspérités propres des architectures existantes et prendre toute sa place légitime pour résister à l'accélération de l'irruption des nouvelles technologies qui sont en train de poindre à l'horizon et qui ne manqueront pas de bousculer les dispositifs et les architectures de sécurité établis. Les grilles de calcul ou de stockage, l'informatique diffuse des objets communiquant, les réseaux de recouvrement (Overlay Networks), les architectures P2P appartiennent à ce relief en émergence, à ces architectures distribuées et mobiles qui rendent caduques les paradigmes d'architectures centralisées de sécurité.

La sécurité du monde numérique est devenu un enjeu fondamental pour le **citoyen** dans le respect de sa liberté individuelle et la préservation de son identité et de son intimité numérique, pour l'**entreprise** dans la protection de son patrimoine industriel numérique, la sécurité des transactions et la confiance dans ses réseaux informatiques et pour l'**Etat** dans la fiabilité du fonctionnement des grandes infrastructures critiques et la réduction de leurs vulnérabilités : distribution de l'électricité, de l'eau, voies et moyens de communication, systèmes d'information et de communication de ces infrastructures.

Les modèles et les fonctions de sécurité sont en effet d'ordre distinct, selon que l'on considère la sécurité de l'individu, de l'entreprise ou de l'Etat. Il convient aujourd'hui de spécifier des politiques de sécurité pour ces entités responsables (la personne physique, la personne morale qu'est l'entreprise,

l'entité morale de l'état) et d'implanter des fonctions de sécurité pour protéger ces infosphères qui gravitent autour de ces entités. On ne peut plus imaginer, une sécurité attachée à chacun des dispositifs physiques. Il faut dessiner une infrastructure transversale qui couvre tout le champ de ces diverses niches de réseaux, en tenant compte du facteur d'échelle de ces infosphères mobiles, aux diamètres et contenus fort différents. Il faut imaginer le cycle de vie de ces infosphères aux sécurités différentes, qui se chevauchent, qui s'entrecroisent et se superposent, l'infrastructure étant capable de gérer la négociation des politiques de sécurité conflictuelles. Cette infrastructure ne doit pas être monolithique et uniforme, puisqu'il faut abandonner l'idée d'un espéranto en sécurité, mais doit s'adapter par subsidiarité dans chaque domaine par une virtualisation ad hoc des divers paradigmes de sécurité (concept de Virtuel à Virtuel).

Le raffinement incrémental des politiques de sécurité doit donc s'opérer dans plusieurs dimensions : dans la dimension verticale qui va de la spécification à un haut niveau d'abstraction virtuelle, puis logique et physique, jusqu'à son implantation matérielle et logicielle dans les équipements, dans la dimension géographique qui va de la spécification générique jusqu'à l'instanciation ajustée dans chacun des réseaux ou sites, sécurité ancrée sur les différentes technologies, et enfin dans la dimension temporelle qui va de la spécification de la politique de sécurité générale inscrite dans une charte connue des utilisateurs, jusqu'à l'implantation en temps réel, proactive et réactive suite à un événement quasi instantané.

Ainsi, Astrid gère au mieux son réseau personnel privé constitué de ses objets communicants traditionnels, de ses connexions intermittentes et permanentes et de ses propres données volatiles ou persistantes sur les réseaux, stockées de manière rhizomorphe comme des bulbes autonomes de données personnelles dans les serveurs de ses fournisseurs de service (banquier, opérateur de télécoms, fournisseur d'accès Internet, médecin spécialiste à l'hôpital, ...).

De façon analogue, Bertrand, l'entrepreneur, maîtrise le réseau de son entreprise en mettant en vigueur une politique de sécurité simple et configurée à chacun de ses collègues selon leur rôle, en sécurisant le système d'information et en particulier la périphérie de son réseau sans fil et les connexions de ses collaborateurs nomades à l'extérieur des murs de l'entreprise. Il gère aussi au mieux les interconnexions avec les fournisseurs et partenaires de son entreprise reliée par des réseaux virtuels privés (VPN) pour assurer une gestion d'entreprise en flux tendus. Il installe des pare-feu, des systèmes de détection d'intrusion, des attrape-nigauds (« honey pots ») pour piéger des attaquants extérieurs, bref tout l'arsenal des solutions actuelles de sécurité.

De même, Charlotte qui distribue en ligne des contenus installe un système de gestion de droits numériques, sur ses serveurs connectés à Internet et aux infrastructures de Télécoms, met en place une architecture de paiement et un modèle de service en utilisant les outils puissants fournis par la cryptographie.

Enfin, l'administration et les grandes entreprises qui couvrent l'Hexagone ou l'Europe, ouvertes aux citoyens ou à des anonymes, doivent définir des politiques de sécurité, des modèles de gestion de crise pour elles-mêmes. Il s'agit de lutter contre les incivilités, le cyber-terrorisme en mettant en œuvre des politiques de sécurité et des gestions de crise, fonction des architectures et des flux de ces infrastructures. Mais ce n'est pas suffisant. Il faut aussi modéliser les interdépendances, mesurer et contrôler les flux entrant et sortant de chaque infrastructure, pour analyser les scénarios et agir lorsque des catastrophes naturelles, des accidents à grande échelle ou des attaques organisées futures assailliront l'une de ces infrastructures critiques, provoquant par des effets de dominos des catastrophes gigantesques en cascade. La sécurisation conjointe de ces infrastructures est un problème ardu, car il faut décrire la politique de sécurité transversale, puisque ces infrastructures sont interdépendantes et vulnérables vis-à-vis de sinistres étendus, d'origine physique comme les tempêtes pour le réseau électrique ou vis-à-vis d'agressions d'origine humaine comme de longs dénis de service pour les technologies de l'information et de la communication.

Par ailleurs, depuis les événements de 2001, une compétition rude est en cours pour gagner les standards de l'identification physique, biométrique de chaque individu (passeport électronique en Europe, initiative américaine pour les passeports). La France ne peut pas être absente de ces débats et de cet enjeu crucial pour la sécurité des citoyens du XXI<sup>ème</sup> siècle.

Les recherches sur la sécurité en 2003 portent essentiellement sur :

La cryptologie ;

Les modélisations de politiques de sécurité ;

L'identification et authentification des acteurs, des contenus et la gestion des droits

- La biométrie ;
- Le tatouage d'images, de sons et de flux vidéos Le tatouage d'images, de sons et de flux vidéos (protection des ayants droit, contrôle des copies, authentification, intégrité) ;

La sécurité des systèmes d'information ;

- Les techniques de détection d'intrusion ;
- La sécurité des grilles ;
- Les architectures de systèmes de leurres, attrape-nigauds (honey pots et honey nets)

La sécurité des réseaux ;

- La sécurité des réseaux fixes
- La sécurité des réseaux actifs, configurables, ad hoc ;
- La sécurité des mondes virtuels et dans l'intelligence ambiante ;

La cryptographie quantique :

- Recherche amont pour la distribution des attributs de sécurité

### **Nouveaux projets qui démarreront en 2004 et projets en cours**

Le RTP 13 a obtenu de nombreux succès au premier Appel d'Offre de l'IST / FP6. Les membres du RTP se sont répartis dans quasiment tous les projets importants (NoE et IP) des objectifs stratégiques concernant la sécurité.

La France a obtenu un taux de succès remarquable dans ce domaine.

Les résumés des projets sont en annexe.

Il y a aussi quelques projets suite aux appels français Oppidum et RIAM.

### **Projets Européens où le RTP 13 est présent**

Projets IP et NoE du FP6

- NoE FP6 - ECRYPT : Le groupe de cryptologie de l'ENS est fortement impliqué. J Stern préside le comité stratégique.
- IP FP6 - SEINIT : Sécurité sur les réseaux. M Riguidel est le responsable scientifique du Projet.
- IP FP6 - SECOQC : Cryptographie quantique. Philippe Grangier et M Riguidel font partie de la core team du Projet.
- IP FP6 - PRIME : protection des données privées (Privacy) et la gestion des identités. R Molva y participe.
- IP FP6 - e-JUSTICE : plate-forme d'échange sécurisée entre les entités impliquées dans la justice (tribunaux, police, avocats, etc.). R Molva y participe.

Projets du FP5 encore en cours

- STREP FP5 - Witness : sécurisation des échanges B-to-E dans les environnements mobiles (R Molva)
- Forward and Emerging Technologies (FET) FP5 - Mobileman : réseaux Mobiles Ad Hoc, comportant une composante sur la sécurité. (R Molva)

## Projets Nationaux

### ACI Crypto et Sécurité

Le RTP est présent aussi dans les ACI 2003. Ci dessous quelques ACI du RTP.

- crypto 2002 : Projet NFS nouvelles fonctionnalités pour la signature (ENS)
- sécurité 2003 : Projet Courbes Elliptiques pour la Sécurité des Appareils Mobiles CESAM (ENS)
- sécurité 2003 : Projet SPLASH sur la sécurité des réseaux mobiles ad hoc (Eurécom)
- sécurité 2003 : Projet PRESTO sur la sécurité des réseaux GMPLS (ENST)
- sécurité 2003 : Projet Edemoi sur la sécurité des avions et aéroports (ENST)

### RNRT

Le RTP est largement présent dans les projets RNRT impliqués dans la sécurité. Ci dessous quelques projets caractéristiques.

- Epis : Internet sécurisé de bout en bout avec carte à puce et IPv6 (Thales, Gemplus, ENST, ...)
- Infradio : sécurité des communautés ouvertes dans les réseaux sans fils (LIP6, ENST, Cégétel, ...)
- Résodo : sécurité des réseaux domestiques (FT R&D, ENST, ...)
- ADSR (FT R&D, ENST, ...)
- X-CRYPT (Schlumberger, ENS, ...)
- CRYPTO++ (France Telecom, ENS, ...)

### RNTL

## **Verrous scientifiques jugés prioritaires pour le RTP, caractéristique de l'orientation de la thématique**

Les verrous sur la sécurité portent donc essentiellement sur :

Les modélisations de politiques de sécurité

- Introduction du temps, de l'espace, du contexte, de la mobilité...
- Gestion des conflits de politiques
- Grandes infrastructures

La cryptologie

- verrou 1: proposer des mécanismes cryptographiques moins gourmands en ressources notamment en environnement contraint
- verrou 2: proposer des mécanismes cryptographiques pour la gestion des droits (DRM)
- verrou 3: proposer des méthodes de chiffrement par flot (stream cipher) aussi sûres que les méthodes actuelles de chiffrement par blocs mais plus rapides

La sécurité de l'Intelligence Ambiante

- Nouveaux paradigmes de sécurité répondant aux besoins des applications ubiquitaires :
  - établissement de confiance sans se baser sur une infrastructure existante ou une organisation a priori
  - faible connectivité ou connectivité intermittente
  - niveaux de garanties intermédiaires par rapport à la recherche habituelle d'une assurance absolue
- Evaluation réaliste des vulnérabilités sur le plan opérationnel (quelle est la "vraie" réalité des attaques sur Internet, qui sont les attaquants, comment opèrent-ils vraiment?)

La sécurité des réseaux fixes ;

La sécurité des réseaux actifs, configurables, des réseaux ad hoc ;

La sécurité des réseaux sans fils ;

Les techniques de détection d'intrusion ;

- approche en rupture vis-à-vis du « misuse » par « pattern matching » et du comportement par apprentissage
- test et testabilité des IDS (méthode, critères, étalonnage, ...)
- Les architectures de systèmes attrape-nigauds (honey pots et honey nets)

La sécurité des grilles ;

La biométrie : banque de données pour étalonnage des algorithmes de reconnaissance, signature électronique avec biométrie ;

Le tatouage d'images, de sons et de flux vidéos ;

La reconnaissance du comportement par suivi de la tête et analyse des gestes faciaux. Les méthodes de suivi à base de filtrage se montrent robustes et peuvent permettre à la fois le suivi et la reconnaissance d'objets vidéos.

La cryptographie quantique. Les infrastructures de confiance fondées sur la cryptographie classique sont en général centralisées et à la merci de l'autorité qui gère les éléments secrets. Les PKIs ou infrastructure de gestion de clés (IGCs) ont du mal à franchir le stade d'une utilisation sans retenue, car les utilisateurs n'ont aucune raison de faire confiance aux logiciels importants, souvent fermés et propriétaires que sont ces IGCs, la plupart du temps non évalués avec la méthodologie des Critères Communs, seule garante d'une assurance de sécurité correcte. La cryptographie quantique permet de transporter des photons sur un lien de communication, en toute sécurité, à l'abri des écoutes indiscretes. L'objectif du projet intégré est de valider la faisabilité d'un concept de réseau quantique où toutes les couches de communication ont été définies et où la topologie du réseau des liens et les protocoles de communication stochastiques participent à la sécurité globale du système de distribution d'éléments secrets ou de certificats. Les objectifs immédiats sont ceux décrits dans SECOQC :

- Réalisation d'un démonstrateur opérationnel de cryptographie quantique utilisant des états cohérents à 1550 nm, basé sur des technologies télécoms
- Amélioration des systèmes de cryptographie quantique utilisant des sources de photons uniques (en cours dans le cadre de l'AS "Photons uniques à la demande").
- Il existe aussi des questions plus "futuristes", dans le sens où des réponses théoriques existent, mais on ne sait pas encore les mettre en oeuvre en pratique. L'exemple le plus important est celui des "répéteurs quantiques", qui permettraient la distribution quantique de clé à des distances arbitraires. Nous avons déposé une demande de STREP pour étudier ce problème dans le cadre de IST/FET/QIPC.

### Besoins en plate-forme ou autre instrument

Il est clair que la sécurité a besoin d'être testée sur des plates-formes d'attaques et de défense, pour vérifier la « scalabilité » des paradigmes.

- Equipements et partenariat pour un réseau collaboratif de leurres, d'attrape-nigauds ou de pots de miel (honeypots)
- Plate forme de Test de détection d'intrusion
- Plate-forme d'attaques et de défense avec politique de sécurité proactive
- Plate-forme d'interopérabilité Bluetooth-WiFi-Internet-GPRS pour valider les concepts de V2V (Virtual à Virtual)
- Plate-forme de Réseau quantique

# Les Actions Spécifiques

## AS 39 Tatouage

Responsables : F. Davoine et J.-M. Chassery

L'AS No 39 (RTP 13) "Tatouage et dissimulation de données pour les communications audiovisuelles" est terminée depuis février 2003 (une autre AS No 184 (RTP 25) "Contenus sécurisés et tatouage" est en cours, depuis cet automne 2003).

L'intégration des flux audiovisuels dans l'Internet fixe ou mobile constitue aujourd'hui un enjeu technologique majeur, qui tend à rendre la **préservation des droits de propriété** des contenus indispensable. Cette nécessité a conduit dès 1993-95 de nombreux chercheurs à se pencher sur le problème de la sécurisation des données numériques face au piratage et à la contrefaçon, par **tatouage robuste**, afin notamment de faciliter le développement économique des techniques de communication audiovisuelle en réseaux.

Il est à noter que la cryptographie et la dissimulation d'information (par tatouage, *fingerpint* ou stéganographie) traitent toutes deux de la protection de l'information, mais leurs objectifs premiers sont différents. La cryptographie offre des outils permettant d'assurer la confidentialité (chiffrement), l'intégrité<sup>1</sup> (hachage, signature) ou encore l'authentification (protocoles de type défi-réponse). La dissimulation d'information a quant à elle pour objectif de cacher un message utile dans un message de couverture. Selon le contexte, on distingue :

la **stéganographie** : il doit être impossible de distinguer si le message de couverture contient un message utile ou non ;

le **tatouage** : le message utile est lié à l'identité de l'ayant droit du document de couverture, et doit donc rester présent même si celui-ci subit des modifications ;

le **fingerpinting** : lorsqu'un document est cédé à un nouvel acquéreur, il est préalablement marqué d'un nouveau message utile. Ceci permet de tracer les fraudes.

Le tatouage robuste (aquamarquage, *watermarking*) est aujourd'hui un sujet qui dispose d'un large champ de théories et de résultats. Il consiste à enfouir au sein-même de l'**information numérique** audio (parole ou musique) ou image (fixe ou vidéo), une **signature**<sup>2</sup> indélébile et non perceptible. Dans le cas de la **protection** des informations numériques, la signature permet d'en **identifier le propriétaire** ou l'**origine**. L'information, entendue au sens large du terme, peut avoir différentes représentations : dans sa forme originelle (échantillons, pixels) ou transformée (Fourier, ondelettes, etc.), ou dans sa forme compressée (flux numérique de transport).

Les utilisations des méthodes de tatouage peuvent être triées en fonction de **contraintes d'imperceptibilité**, de **robustesse**, de **sécurité**, de **capacité** et de **complexité**. Selon l'application, la présence de la signature doit être imperceptible (voire insoupçonnable dans le cas de la stéganographie). Elle doit être retrouvée dans le document tatoué, après dégradation volontaire ou pas de ce dernier, à condition bien sûr qu'il garde une valeur commerciale suffisante. La signature doit être sûre vis-à-vis de l'attaquant (illisible, indélébile) : le schéma de tatouage doit contribuer à la sécurisation de données audiovisuelles. Enfin, la capacité correspondant à la quantité de bits dissimulés dans le document hôte doit pouvoir être importante pour satisfaire certaines applications.

Ces applications englobent une **grande variété de supports** numériques tels que par exemple les images satellitaires et médicales, les cartes géographiques, les documents textuels, les logiciels et les codes informatiques, les paramètres de formes et d'animation d'objets synthétiques et d'avatars 3D, etc.

Nous voyons aujourd'hui l'émergence d'**applications nouvelles** qui font appel, comme le tatouage robuste pour la protection, à des techniques de dissimulation de données dans des documents numériques.

Toujours dans un **cadre sécuritaire**, ces techniques sont étudiées pour vérifier l'**intégrité** des documents ou permettre leur **authentification**. Dans le cas de la stéganographie, elles permettent de transmettre une **information** secrète de manière totalement **cachée**, non détectable, au travers de

documents publics (on parle dans ce cas d'imperceptibilité statistique de la signature). Elles sont également utiles pour le **traçage** des documents circulant sur Internet, le **contrôle d'accès** ou la **protection des copies** (DVD, etc.).

Elles doivent être utiles pour le **tatouage conjoint** de sources multimodales (textes, audio et vidéo, etc.), l'**indexation**, la **correction des erreurs** de transmission, le transfert d'informations au travers de **canaux cachés** à des fins d'**augmentation des contenus**.

Le tatouage conjoint permet par exemple de synchroniser ou de rendre indissociables un visage synthétique ou naturel de son signal de parole ou d'inclure une traduction automatique directement dans une séquence audiovisuelle. La correction automatique des erreurs après transmission ou attaques est possible en incrustant dans l'image une représentation d'elle-même (on parle dans ce cas de *self-correcting images*). Enfin, les techniques de dissimulation de données (*data hiding*) doivent permettre de transmettre une information supplémentaire au travers de données porteuses telles que des images ou des sons numériques. On bénéficie dans ce cas d'un canal (caché) auxiliaire ou le contenu numérique est « augmenté » d'informations supplémentaires. Les techniques d'indexation peuvent par exemple exploiter des informations utiles qui peuvent être retrouvées à partir d'une signature dissimulée dans une image ; cette signature code l'origine de l'image, sa destination, ses usages et caractéristiques - contenu sémantique, post-traitements,

### Résultats de l'AS 39

1. publication d'un rapport pour le STIC incluant un état des recherches internationales, des perspectives, et listant les acteurs nationaux (thèses soutenues et en cours).
2. trois réunions de travail avec invitations de chercheurs européens,
3. prises de contacts et visibilité du groupe de laboratoire vis-à-vis du FP6.

Des perspectives de recherche ont été définies au terme de l'AS 39 :

- \_ Le tatouage et la cryptographie asymétrique,
- \_ Le tatouage et l'authentification cryptographique,
- \_ Le tatouage et la stéganalyse.
- \_ Le tatouage pour la protection des contenus et des transmissions, à la frontière entre les communications numériques et la cryptologie,
- \_ Le tatouage tirant partie de la théorie de l'information et de la théorie des jeux,
- \_ Le tatouage pour l'augmentation ou l'enrichissement des contenus (indexation multimédia, canal caché).

Ces perspectives ont été reprises par certains des partenaires, impliqués dans des nouveaux projets, notamment ECRYPT (FP6, NoE), FABRIANO (ACI Sécurité).

### Publications récentes

F. Cayre, F. Davoine, "Vers un tatouage d'images mou", *Traitement du Signal*, Vol. 18, No. 4, déc. 2001.

F. Davoine, S. Baudry and P. Nguyen, *Data hiding and digital watermarking*, in *Eurasip News Letter*, Vol. 13, No. 1, 2002.

F. Davoine et S. Pateux (Eds.), "Tatouage de documents audiovisuels numériques", Ouvrage du *traité IC2*, Hermès Science. A paraître en 2003.

H. Joumaa, F. Davoine, "Tatouage substitutif d'images intégrant un masque de pondération psychovisuelle", *Actes de CORESA*, Lyon, France, pp. 249-252, 16-17 janvier 2003.

F. Raynal, F.A. Petitcolas and C. Fontaine, « Évaluation automatique des méthodes de tatouage », *Traitement du Signal*, 2002.

- C. Fontaine, F. Raynal, « About the links between cryptography and information hiding », in Proc. of IS&T/SPIE International Symposium on Electronic Imaging 2002: Security and Watermarking of Multimedia Contents IV, SPIE, Vol. 4675, January 2002.
- S. Baudry, P. Nguyen and H. Maître, “Optimal decoding for watermarks subject to geometrical attacks”, in Signal processing: Image communication, 18, pp. 297-307, 2003.
- F. Cayre, P. Rondao-Alface, F. Schmitt, B. Macq and H. Maître, “Application of spectral decomposition to compression and watermarking of 3D triangle mesh geometry”, in Signal processing: Image communication, 18, pp. 297-307, 2003.
- S. Baudry, P. Nguyen and H. Maître, “Use of synchronisation patterns to estimate geometric distortions in digital watermarking”, in Proc. of Eusipco, Toulouse, France, Oct. 2002.
- S. Baudry, P. Nguyen and H. Maître, “Estimation of geometric Distorsions in digital watermarking”, in Proc. of IEEE-ICIP, Rochester, USA, 2002.
- S. Baudry, J.-F. Delaigle, B. Sankur, B. Macq and H. Maitre, “Analyses of Error correction Strategies for Typical communication channels in Watermarking”, Signal Processing, Vol. 81, n° 6, June 2001, pp.1239-1250.
- Q. Chen, H. Maître and B. Pesquet-Popescu, “Oblivious image watermarking combined with JPEG compression”, in Proc. of IS&T/SPIE International Symposium on Electronic Imaging 2002: Security and Watermarking of Multimedia Contents IV, SPIE, Vol. 5020, January. 2003.
- F. Cayre and B. Macq, « Data hiding on 3D triangle meshes », IEEE Transactions on Signal Processing, Special Issue on Signal Processing for Data Hiding in Digital Media & Secure Content Delivery, à paraître en avril 2003.
- P. Bas, J-M Chassery and Benoît Macq, "Image Watermarking: an evolution to content based approaches", Pattern Recognition, Special Issue on Image/Video Communication edited by D. Aboutajdine, 2002, pp. 545-561.
- P. Bas et Benoît Macq, "Tatouage d'objets vidéos résistant aux manipulations", Traitement du Signal 2001 numéro spécial volume 18 N° 4, pp. 249-257.
- P. Bas, J-M Chassery and Benoît Macq, "Geometrically Invariant Watermarking Using Feature Points ", IEEE Transactions on Image Processing , September 2002
- P. Bas et Benoît Macq, "Méthode de tatouage fondée sur le contenu", Traitement du Signal 2002, vol 19, num1 pp. 11-18.
- G. Le Guelvouit and S. Pateux, “Wide spread spectrum watermarking with side information and interference cancellation”, *Proc. SPIE*, Santa Clara, CA, Janvier, 2003.
- S. Pateux and G. Le Guelvouit, “Practical watermarking scheme based on wide spread spectrum and game theory”, to appear in IEEE Transactions on Image Processing, 2003.
- J. Delhumeau and T. Furon and N. Hurley and G. Silvestre, “Improved Polynomial Detectors for Side-Informed Watermarking”, *Proc. SPIE*, Santa Clara, CA, Janvier, 2003.
- G. Le Guelvouit and S. Pateux and C. Guillemot, “Information-theoretic resolution of perceptual WSS watermarking of non i.i.d. Gaussian signals”, *Proc. Eur. Signal Processing Conf.*, vol. 1, pp. 454-457, Toulouse, France, Septembre, 2002.
- G. Le Guelvouit and S. Pateux and C. Guillemot, “Perceptual watermarking of non i.i.d. signals based on wide spread spectrum using side information”, *Proc. Int. Conf. on Image Processing*, Rochester, NY, Septembre, 2002.
- T. Furon, N. Moreau and P. Duhamel, "Audio public key watermarking technique," in *Proceedings of the Int. Conf. on Audio Speech and Sig. Proc.*, 2000.

L. de C.T. Gomes, E. Gomez, N. Moreau, "Resynchronization methods for audio watermarking", 110th Convention of Audio Engineering Society, New York, September 2001.

L. de C.T. Gomes, E. Gomez, M. Bonnet, N. Moreau, "Méthodes de resynchronisation pour le tatouage audio", Dix-huitième Colloque GRETSI, Toulouse, Septembre 2001

L. de C.T. Gomes, M. Mboup, M. Bonnet, N. Moreau, "Cyclostationarity-based audio watermarking with private and public hidden data", 109th Convention of Audio Engineering Society Los Angeles, September 2000

## AS Sécurité logicielle : modèles et vérification (commune avec le RTP 19)

L'action a pour but de réunir les équipes travaillant sur les aspects formels de la sécurité logicielle en France, et qui sont actuellement éparpillées et peu coordonnées. En particulier, il existe une grande variété de modèles spécifiques à des systèmes informatiques tenant compte d'un environnement hostile. Les applications sont aussi variées: carte à puce, détection d'intrusion, protocoles cryptographiques. Il existe enfin une grande variété de techniques de vérification de propriétés de sécurité.

L'action est structurée selon trois axes spécifiques:

La vérification de protocoles cryptographiques

La vérification de code embarqué

Les modèles pour la disponibilité et la survivabilité

Les trois questions principales (transversales aux axes) auxquelles s'intéresse l'action sont:

Quelles propriétés de sécurité ?

Quels sont les mécanismes et fonctions de sécurité censés satisfaire ces propriétés ?

Les propriétés sont elles satisfaites? Si non, proposer des scenarii d'attaque

L'action regroupe 13 équipes de recherche et un certain nombre de chercheurs et industriels, soit, en tout, une cinquantaine de personnes. La première réunion a eu lieu en février 2003 à Cachan (cf <http://www.lsv.ens-cachan.fr/Events/as-securite-2002/>).

Après une interruption de 4 mois due à l'absence de financement (et en particulier l'incertitude sur le remboursement des missions de février), l'action a repris cet été et se prolongera jusqu'en mai/juin 2004, en accord avec le département STIC.

Une deuxième réunion a eu lieu à Grenoble le 4 décembre 2003.

Sur le plan du bilan, l'action a surtout permis jusqu'ici de monter quelques projets ACI ou RNTL (ou européens). Des articles de synthèse, des catalogues de problèmes, de logiciels et des pointeurs seront disponibles à partir du site de l'action. ([http://www.lsv.ens-cachan/AS\\_SL/](http://www.lsv.ens-cachan/AS_SL/)).

## AS Crypto Quantique

Responsable Philippe Grangier et Jean-Philippe Poizat

Cryptographie quantique utilisant une source de photons individuels émis "à la demande".

[1] Alexios Beveratos, Sergei Kuhn, Rosa Brouri, Thierry Gacoin, Jean-Philippe Poizat et Philippe Grangier, "Room temperature stable single-photon source", Eur. Phys. J. D 18, 191-196 (2002)

[2] Alexios Beveratos, Rosa Brouri, Thierry Gacoin, André Villing, Jean-Philippe Poizat et Philippe Grangier, "Single photon quantum cryptography", Phys. Rev. Lett. 89, 187901 (november 2002)

[3] Philippe Grangier et Izo Abram, "Single photons on demand", Physics World 16 - Feature Article, 31-35 (february 2003)

Ces articles décrivent la mise au point d'une source impulsionnelle émettant des photons uniques "à la demande", en utilisant la fluorescence de centres colorés individuels dans des nanocristaux de diamant. Cette source stable et compacte, fonctionnant à température ambiante, a été utilisée pour réaliser la première démonstration complète de cryptographie quantique utilisant une source à photons uniques [2]. La référence [3] est un article général sur ce domaine de recherche, écrit à la demande de l'éditeur de "Physics World".

Cryptographie quantique utilisant des états cohérents modulés en phase et en amplitude.

[4] Frédéric Grosshans et Philippe Grangier, "Continuous variable quantum cryptography using coherent states", Phys. Rev. Lett. 88, 057902 (2002)

[5] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas Cerf et Philippe Grangier, "Quantum key distribution using gaussian-modulated coherent states", Nature 421, 238-241 (january 2003)

Ces articles décrivent les bases théoriques [4, 5] et la démonstration expérimentale [5] d'un nouveau protocole de cryptographie quantique utilisant des impulsions lasers modulées et une détection cohérente (homodyne), plutôt que des méthodes de comptage de photons. Cette nouvelle méthode est très attrayante, car elle peut en principe être mise en oeuvre en n'utilisant que des technologies télécoms bien maîtrisées. Nous avons déposé un brevet relatif à ce dispositif, et nous nous proposons de réaliser un démonstrateur opérationnel à 1550 nm, dans le cadre du projet intégré FP6 "SECOQC". Ce travail donnera lieu à diverses collaborations nationales (en particulier avec Thales TRT) et européennes (en particulier avec l'Université Libre de Bruxelles).

Remarque : D'autres groupes de chercheurs ont aussi participé à cet AS, mais leurs rapports d'avancement ne sont pas parvenus à temps pour la rédaction de ce rapport.

---

**RTP 13 - AS « Photons uniques à la demande » (Philippe Grangier)****Objectifs Généraux de l'AS**

Les sources émettant des impulsions lumineuses contenant un photon et un seul ont de nombreuses applications potentielles en information quantique, en particulier pour la mise en oeuvre de dispositifs de cryptographie quantique plus sûrs et plus robustes vis à vis des pertes en ligne, et pour la réalisation de portes logiques quantiques simples utilisant des non-linéarités induites par le processus de photodétection lui-même.

Les équipes françaises sont bien placées au niveau international, et elles ont déjà adopté des approches très complémentaires. Le but de cette AS est de regrouper ces équipes afin d'optimiser et de coordonner leurs efforts, ce qui permettra de renforcer leur position dans ce domaine extrêmement actif au niveau international.

**Laboratoires partenaires**

- \* Laboratoire Charles Fabry de l'Institut d'Optique (LCFIO - Philippe Grangier, Gaétan Messin)
- \* Laboratoire de Photonique Quantique et Moléculaire (LPQM / ENS Cachan, Jean-François Roch, François Treussart)
- \* Laboratoire de Physique des Nanostructures (LPN - Izo Abram, Isabelle Robert)
- \* Equipe mixte UJF-CNRS-CEA « Nanophysique et semi-conducteurs », Laboratoire de Spectrométrie Physique (Jean-Michel Gérard, Jean-Philippe Poizat)
- \* Laboratoire Kastler-Brossel (LKB / ENS, Elisabeth Giacobino, Jean-Pierre Hermier)

**Résumé des contributions**

Au cours des derniers mois le LCFIO et le LPQM ont directement collaboré pour réaliser un système « réaliste » de distribution de clé quantique, utilisant une source émettant des trains d'impulsions à un seul photon. Ce dispositif fonctionne entre deux bâtiments de l'Institut d'Optique, et distribue une clé secrète à une cadence de 16 kbits / sec.

Par ailleurs, les groupes du LSP et du LPN ont accompli des progrès significatifs en vue de la réalisation de sources de photons uniques et de photons intriqués « à la demande », utilisant des boîtes quantiques semi-conductrices (III / V au LPN, et II / VI au LSP), et le groupe du LKB poursuit ses travaux sur les nanocristaux semi-conducteurs.

## A. Cryptographie quantique utilisant une source à un seul photon.

Notre travail a été axé sur la réalisation de sources de photons uniques à partir du contrôle temporel de l'émission d'un centre coloré unique dans un nanocristal de diamant. Ce travail a été réalisé en étroite collaboration entre **les groupes du LCFIO et du LPQM**.

1) Etude du comportement des centres NV sous excitation femtoseconde. Ce travail a donné lieu à une publication actuellement soumise à Journal of Luminescence.

2) Etude préliminaire du couplage de l'émission d'un centre NV à une microcavité. Nous avons réalisé la microcavité composée de deux miroirs plans dont la distance est réglable. Ce dispositif est compatible avec les systèmes de microscopie confocale dont disposent les groupes du LCFIO et du LPQM.

3) Réalisation d'une distribution quantique de clé de cryptage, à partir d'une source de photons uniques. Cette distribution est réalisée en espace libre, Alice et Bob étant situés dans les deux ailes du bâtiment de l'Institut d'Optique. Le processus complet d'échange de clé a été mis en œuvre (envoi de photons codés en polarisation suivant le protocole BB84, puis échanges classiques sur Internet pour filtrer la clé, corriger les erreurs, et appliquer la fonction de hachage). Les résultats obtenus montrent un avantage significatif par rapport à l'utilisation d'impulsions laser atténuées contenant le même nombre moyen de photons par impulsion.

Deux publications portant sur la statistique des photons émis par une source de photons uniques moléculaires et sur la réalisation de l'expérience de cryptographie quantique en "plein air" sont actuellement en cours de rédaction. Elles seront soumises au numéro spécial de New Journal of Physics faisant l'état de l'art sur les sources de photons uniques.

## B. Sources à photons uniques utilisant des dispositifs à semi-conducteurs.

**L'équipe du LPN** a pu obtenir en 2002-2003 trois résultats marquants ouvrant d'importantes perspectives pour les sources de photons uniques à base de boîtes quantiques à semi-conducteur.

### **(1) Observation de photons uniques émis par des boîtes quantiques pyramidales à sites contrôlés :**

Ces boîtes, en  $\text{In}_{0.1}\text{Ga}_{0.9}\text{As}$ , sont fabriquées par MOCVD de manière contrôlée à l'intérieur d'encoches pyramidales submicroniques réalisées par photolithographie dans un substrat GaAs orienté (111)B. Ce procédé permet la maîtrise des positions des boîtes ainsi qu'une réduction importante de la dispersion de leur taille, par rapport aux méthodes classiques de fabrication de boîtes basées sur le relâchement local des contraintes aléatoires (procédé Stranski-Krastanov). Notre démonstration de l'émission de photons uniques par ces boîtes (par l'observation du phénomène de dégroupement dans la corrélation des photons émis) ouvre la perspective d'utilisation des boîtes pyramidales pour la réalisation de sources de photons uniques en tant que composants reproductibles et fiables. Ces travaux, réalisée en collaboration avec l'école polytechnique fédérale de Lausanne ont donné lieu à une communication à la conférence CLEO, ainsi qu'à la rédaction d'un article soumis à Appl. Phys. Lett.

### **(2) Observation de photons uniques émis par des boîtes quantiques à fluctuations d'interfaces :**

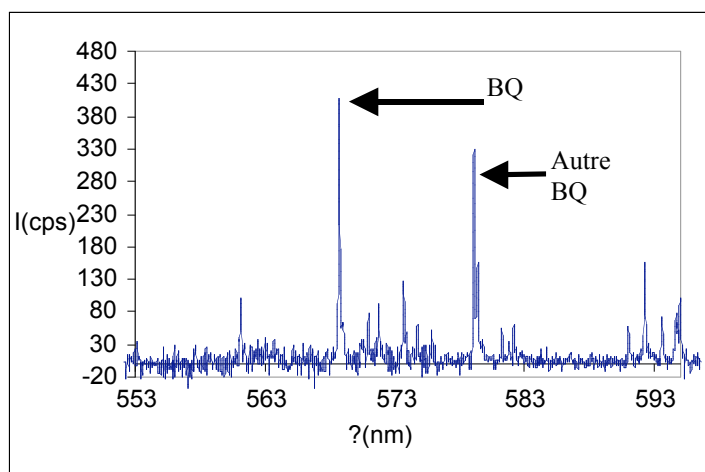
Ces boîtes quantiques sont produites sur les interfaces GaAs/AlGaAs des puits quantiques GaAs étroits, sur lesquels des fluctuations d'épaisseur d'une ou deux monocouches produisent un confinement tridimensionnel des électrons et des trous. À cause des dimensions latérales des boîtes à fluctuations d'interfaces, qui sont supérieures au rayon de Bohr de l'exciton, l'émission radiative de ces boîtes bénéficie de l'effet de « force d'oscillateur géante » qui produit une durée de vie radiative de quelques dizaines de picosecondes. Nous avons pu démontrer le caractère mono-photonique de l'émission de ces boîtes, par des expériences de corrélation de photons. Cette démonstration ouvre d'importantes perspectives pour l'utilisation des boîtes à fluctuations d'interfaces dans des expériences d'optique quantique, car la courte durée de vie radiative de ces systèmes pourrait permettre de s'affranchir des problèmes liés aux processus de déphasage des états excités de la boîte. De plus, au-delà de l'intérêt pour l'optique quantique, l'observation de photons uniques dans ces boîtes démontre qu'aucune relaxation de porteurs n'a lieu à des temps supérieurs à la durée de vie des excitons de la boîte, à partir du puits quantique adjacent. Ces travaux ont donné lieu à une publication, Appl. Phys. Lett. 82, 2206 (2003).

**(3) Mise au point de cavités optiques à micro piliers semiconducteur** : Un élément important dans le développement de sources de photons uniques est la réalisation de microcavités de dimensions de l'ordre de la longueur d'onde (quelques centaines de nm) qui permettent la mise en oeuvre d'effets d'Electrodynamique quantique pour augmenter l'efficacité extraction et de collection des photons uniques et pour raccourcir la durée de vie radiative des excitons et s'affranchir ainsi des effets du déphasage. Nous avons mis au point un protocole de gravure de micro piliers donnant lieu à des cavités de dimensions de l'ordre de quelques  $\mu\text{m}^3$  et présentant un facteur de qualité de l'ordre de 1500. L'obtention de ces cavités est un pas important vers la réalisation de sources de photons uniques avec de très bonne propriétés de cohérence, un préalable à la conduite d'expériences sur l'intrication ou sur la logique quantique.

Les résultats obtenus cette première année de l'AS permettront au LPN d'atteindre les objectifs affichés, notamment la réalisation d'expériences d'interférences multiphotoniques et de coalescence de photons, vers le développement de portes logiques quantiques.

L'objectif du **groupe du LSP** (Equipe mixte CEA/CNRS/UJF « Nanophysique et semi-conducteurs ») est d'obtenir des photons uniques indiscernables à partir de boîtes semiconductrices de type II/VI. Le groupe a donc monté un dispositif de microphotoluminescence à la température de 4.2 K associé à un système de corrélation de photons ultra-rapide. L'originalité de ce montage est justement la rapidité de ce système (résolution temporelle inférieure à 100 ps) qui permet d'étudier des boîtes quantiques dont la durée de vie est de quelques centaines de ps (typiquement 250 ps). Ce système utilise des photomultiplicateurs à galette de microcanaux, qui ont été prêtées par Ph. Grangier (LCFIO), et une carte d'acquisition ultra-rapide.

Les premiers résultats préliminaires ont été obtenus sur des boîtes auto-assemblées de CdTe/ZnTe fabriquées dans notre équipe par Frank Tinjod. Les échantillons sont masqués par un film d'aluminium percé de trous de tailles connues comprises entre 0.2 et 10 microns. L'excitation est faite par la raie à 488 nm d'un laser argon continu. La figure 1 montre un spectre de microphotoluminescence où l'on peut distinguer différents pics provenant de boîtes quantiques individuelles différentes.

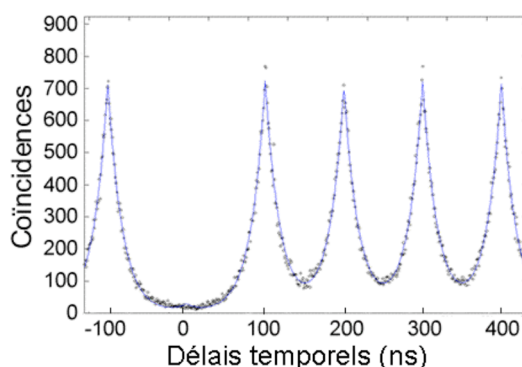


*Fig.1 Spectre de microphotoluminescence de boîtes quantiques individuelles de CdTe/ZnTe à la température 4.2 K. Les deux pics principaux correspondent à la raie excitonique de deux boîtes quantiques (BQ) différentes*

En sélectionnant à l'aide d'un monochromateur la raie à 570 nm, nous avons mesuré la fonction d'autocorrélation d'ordre deux de la lumière émise par une seule boîte quantique, et observé le dégroupement de photons caractéristique des émetteurs de lumière individuels. A notre connaissance, c'est la première fois que cette propriété est observée sur des boîtes de CdTe/ZnTe. Une analyse détaillée des résultats obtenus est en cours.

Les travaux réalisés au **Laboratoire Kastler Brossel** ont surtout concerné la *caractérisation de l'émission de nanocristaux semiconducteurs sous excitation impulsionnelle*. L'utilisation des nanocristaux comme source de photons uniques requiert en effet une excitation impulsionnelle, où chaque impulsion produit un photon et un seul dans le cas idéal. A l'aide d'une diode impulsionnelle fibrée qui émet des impulsions de 40 picosecondes (l'achat et le montage de la fibre a été rendu possible par l'Action Spécifique Photons Uniques), nous avons pu observer un dégroupement supérieur à 99% après extraction du bruit noir des photodiodes (voir figure ci-dessous). Le taux de photons uniques ainsi produits et détectés s'est révélé très prometteur puisqu'il est de l'ordre de 3 %.

Un article concernant l'émission de photons uniques sous excitation impulsionnelle est actuellement en préparation. L'étape suivante de l'expérience consistera à inclure les nanocristaux dans un miroir multidiélectrique, afin d'améliorer sensiblement la directionnalité de la lumière émise par le nanocristal. Par ailleurs, l'utilisation de ce simple miroir peut s'avérer très intéressante pour augmenter le taux de collection de notre montage de microscopie à basse température.



Histogramme des coïncidences des photons émis par un nanocristal unique sous excitation impulsionnelle. L'absence de pic à délai nul démontre le dégroupement des photons émis par le nanocristal.

#### Communications présentées dans le cadre de l'AS.

EGAS (35th conference of the European Group for Atomic Spectroscopy, Bruxelles, 15-18 juillet 2003)

Conférence invitée présentée par J.-F. Roch  
"Emission properties of single photon sources"

Coloq 8 (Toulouse, 3-5 septembre 2003)

Conférence invitée présentée par J.-F. Roch  
"Emission de photons uniques : propriétés et applications"

Affiche présentée par Romain Alléaume

"Fluorescence de centres colorés uniques de nanocristaux de diamant en microcavité"

C. COUTEAU, S. MOEHL, F. TINJOD, J. SUFFCZYNSKI, R. ROMESTAIN, J.C. VIAL, J.-M. GERARD, K. KHENG, et J.P. POIZAT, poster à la Conférence sur les Lasers et l'Optique Quantique (COLOQ 8) à Toulouse du 3 au 5 septembre 2003

Conférences invitées présentées par Philippe Grangier :

QELS Baltimore, juin 2003

Conférence de la SFP, Lyon, juillet 2003

Conférence du réseau « QUIST », Abingdon, UK, juillet 2003

Symposium « Heraeus », Bad Honnef, Allemagne, octobre 2003

## AS - Nouvelle tendances en Cryptographie

### Atelier sur la sécurité prouvée à l'ENS

Lundi 23 juin 2003, salle S16

14h30: Introduction à la sécurité prouvée  
Jacques Stern (ENS)

Public key cryptography was proposed in the 1976 by Diffie and Hellman. One year later, Rivest, Shamir and Adleman introduced the RSA cryptosystem as a first example.

From an epistemological perspective, one can say that Diffie and Hellman have drawn the most extreme consequence of the second principle stated by Auguste Kerckhoffs in the XIXth century: "le mécanisme de chiffrement doit pouvoir tomber sans inconvénient aux mains de l'ennemi".

Indeed, Diffie and Hellman understood that only the deciphering operation has to be controlled by a secret key: the enciphering method may perfectly be executed by means of a publicly available key, provided it is virtually impossible to infer the secret deciphering key from the public data.

Very quickly, it was understood that the naive textbook RSA algorithm could not be used as it stands: in particular, it has algebraic multiplicative properties which are highly undesirable from a security perspective. Accordingly, it was found necessary to define formatting schemes adding some redundancy. For several years, this worked by trials and errors, until a more formal approach appeared necessary. Provable security is an attempt to offer mathematical proofs as a basis for these schemes. From an epistemological perspective, it is a strengthening of Kerckhoffs' first principle: "Le système doit être matériellement, sinon mathématiquement, indéchiffrable".

The talk will discuss provable security by means of two case studies covering the OAEP encryption standard for RSA and the proposed signature standard ESIGN.

----

15h15: Scalable Protocols for Authenticated Group Key Exchange  
Moti Yung (Columbia University)

We consider the fundamental problem of authenticated group key exchange with forward secrecy among  $n$  parties within a larger and insecure public network. A number of solutions to this problem have been proposed as well as formal models; however, all provably-secure solutions thus far are not scalable and, in particular, require  $n$  rounds.

Our main contribution is the first scalable protocol for this problem along with a rigorous proof of security in the standard model under the DDH assumption; our protocol uses a constant number of rounds and requires only  $O(1)$  modular exponentiations per user (for key derivation).

Toward this goal and of independent interest, we first present a scalable compiler that transforms any group key-exchange protocol secure against a passive eavesdropper to an authenticated protocol which is secure against an active adversary who controls all communication in the network. This compiler adds only one round and  $O(1)$  communication (per user) to the original scheme.

We then prove secure --- against a passive adversary --- a variant of the two-round group key-exchange protocol of Burmester and Desmedt.

Applying our compiler to this protocol results in a provably-secure three-round protocol for authenticated group key exchange which also achieves forward secrecy.

This is joint work with Jonathan Katz.

----

16h00: Le chiffrement asymétrique sans redondance  
Duong Hieu Phan (ENS)

Nous proposons un schéma de chiffrement asymétrique pour lequel tous les chiffres sont valides (ce qui signifie que la fonction de chiffrement est non seulement une injection probabiliste, mais également une surjection).

Tout d'abord, nous présentons le chiffrement "Full-Domain Permutation" qui utilise une permutation aléatoire. Ceci fournit le premier chiffrement asymétrique qui soit IND-CCA2, base sur n'importe quelle permutation à sens-unique à trappe, sans aucune redondance. De plus, la bande passante est optimale: le chiffre n'est que  $k$  bits plus long que le clair, pour une sécurité en  $1/2^k$ .

Ensuite, nous étudions les transpositions de cette méthode au modèle de l'oracle aléatoire, en réalisant la permutation aléatoire avec un réseau de Feistel (OAEP, sur 2 ou 3 tours).

Travail fait en commun avec David Pointcheval.

### **Colloque par l'équipe Crypto du Laboratoire d'informatique de l'École polytechnique et le projet TANC de l'INRIA Futurs**

"Cryptographie fondée sur l'identité et les couplages".

Ce colloque est le troisième et dernier dans notre série de rencontres dans le cadre de l'Action spécifique "Nouvelles tendances en cryptographie" avec l'ENS et l'ENST.

Nous vous donnons rendez-vous le 20 novembre 2003 à 14h dans la salle de séminaire du Laboratoire d'informatique de l'École polytechnique. Veuillez trouver en bas le programme détaillé et les résumés des exposés.

Pour l'accès au laboratoire, consultez la page web

[http://www.lix.polytechnique.fr/Francais/visit\\_us.html](http://www.lix.polytechnique.fr/Francais/visit_us.html)

Pour tout renseignement, merci de vous adresser à Andreas Enge, [enge@lix.polytechnique.fr](mailto:enge@lix.polytechnique.fr), 01 69 33 46 34.

#### Programme

14h - 14h45

Andreas Enge, INRIA Futurs and École polytechnique:  
"Identity based cryptography - a leisurely introduction"

14h50 - 15h35

Régis Dupont, INRIA Futurs and École polytechnique:  
"Provably secure non interactive key distribution based on pairings."

\* coffee break \*

16h - 16h45

Steven Galbraith, Royal Holloway University of London:  
"Easy decisions: applications of pairings in cryptography"

#### Abstracts / résumés:

Andreas Enge:

"Identity based cryptography - a leisurely introduction"

A major problem in public key cryptography stems from the fact that before being able to communicate securely, one already needs to have communicated securely. In fact, it is necessary to verify the authenticity of public keys before using them; that is, one needs to make sure that the public keys belong indeed to the participants in the system. The usual solution consists of installing a rather heavy public key infrastructure.

A different, recent approach is taken by identity based cryptography.

Here, a participant's public key is nothing but their identity (name, e-mail address, etc.), so that its authenticity is immediate. However, the distribution of the corresponding private keys now poses a problem. I will give an overview of identity based systems suggested in the past and explain why these are not usable in practice. Then I will present recently invented systems that rely on pairings on algebraic curves. If time permits, I will also touch on the problem of finding suitable curves.

Régis Dupont:

"Provably secure non interactive key distribution based on pairings"

We present a protocol, initially due to Sakai, Ohgishi and Kasahara, that enables two entities possessing private keys to compute a shared secret key without ever communicating between themselves. This protocol is one of the simplest constructive applications of pairings in cryptology.

After defining a notion of security for such a protocol, we show how, in the random oracle model, the protocol security can be reduced to the hardness of a well-identified mathematical problem connected to the used pairing, the Generalised Bilinear Diffie-Hellman problem.

Steven Galbraith:

"Easy decisions: applications of pairings in cryptography"

We describe some applications of pairings in cryptography. In particular, we discuss how pairings make some decision Diffie-Hellman problems easy and recall how this can be used to build short digital signature schemes.

## **REUNION RTP 13 AS NOUVELLES TENDANCES EN CRYPTOGRAPHIE**

Lundi 29 Septembre à 14 heures en C.229.

Trois exposés:

Capacities of graphs and digraphs

Janos Korner, "La Sapienza University", Rome (Italy)

Sperner capacity is a natural generalization of Shannon capacity from graphs to directed graphs. In combinatorics, it has proved to be a valuable tool to obtain asymptotically tight estimates for several hard problems in extremal set theory. Some of these results have found exciting applications in computer science. Yet the precise value of Sperner capacity is very hard to determine even for some orientations of the edges of a complete graph. Improving on earlier bounds of Calderbank et al., Blokhuis and Noga Alon, we introduce a novel upper bound for the Sperner capacity of arbitrary digraphs. Our bound, obtained in joint work with Concetta Pilotto (Rome) and Gabor Simonyi (Budapest), is based on a suitable generalization for directed graphs of the concept of "local chromatic number", as defined by Erdos, Furedi, Hajnal, Komjath, Rodl and Seress (1986). The exposition will be self-contained. In particular, the first part is a survey on Shannon's graph capacity and our generalization to directed graphs; Sperner capacity.

Codes séparant

Hugues Randriam, ENST

On expose diverses constructions et bornes existentielles sur les codes séparant, en insistant notamment sur la construction par Xing de bons codes issus de la géométrie algébrique.

Identification et révocation par codes séparant

Gerard Cohen et Gilles Zémor

Le contexte est le suivant. Un flot de données (une émission) est chiffré par une clé de session appelée  $S$ . Ce flot est précédé par un en-tête  $F(S)$ , qui contient la clé de session  $S$  chiffrée par une fonction  $F$ . La fonction de chiffrement est choisie de manière à admettre un grand nombre  $N$  de fonctions (ou clés) de déchiffrement, égal au nombre d'utilisateurs du système.

On distingue deux préoccupations du diffuseur: l'identification des décodeurs et la révocation. On montre comment l'emploi de codes séparant permet de les traiter.

**Projet Intégrés**

**&**

**Réseaux d'Excellence**

**du 6<sup>ème</sup> PCRD en Sécurité**

## **e-JUSTICE : Towards a global security and visibility framework for Justice in Europe**

*Co-ordinator* : e-Forum for European e-Public Services ASBL (BE)

17 partners

Forum for European e-Public Services ASBL BE

Bayerisches Staatsministerium der Justiz DE

Bundeskanzleramt der Republik Oesterreich AT

Bundesverfassungsgericht DE

German Research Centre for Artificial Intelligence (DFKI) GmbH DE

Infocamere IT

Institut Eurécom FR

Max-Planck-Gesellschaft z.F.d.W. DE

Ministère de l'Intérieur, de la Sécurité intérieure et des Libertés locales FR

La Poste FR

University of Leeds, Jean Monnet European Centre of Excellence UK

Universität des Saarlandes DE

SAP Labs France FR

Thales Identification SA FR

Tribunal de Commerce de Paris FR

UNISYS Belgium SA/NV BE

ZN Vision Technologies AG DE

*Objective* :

To define, develop, teach, test and prepare the deployment of a complete and innovative system to improve security of the communities and the privacy of the bearers, and to provide interoperable keys to digital information. Research on security will focus on smart identity cards, on-chip combined biometrics, cryptography and PKI interoperability, and rights management. Visibility of the judicial processes, which is critical to restore confidence of the citizens and enable justice administrations to develop total quality management, will be enhanced by a common representation of judicial processes in Europe (workflow representation, ontology, optimisation and proof), and by the development of tools that analyse workflow descriptions to guide the actors of justice in their tasks and record their actions.

The main research breakthroughs of the project could concern rights management, i.e. the link between personal authentication, digital signature and need-to-know, and the integration of security, workflow processing and knowledge management, i.e. the possibility that different people automatically receive different views of the same information.

## **INSPIRED : Integrated Secure Platform for Interactive Personal Devices**

*Co-ordinator* : GEMPLUS Development (FR)

15 partners

Gemplus Development FR

Schlumberger FR

Giesecke & Devrient DE

Oberthur Card Systems FR

Orga DE

Philips Semiconductors DE

Orange France FR

Atmel FR

University of Twente NL

INRIA FR

Université Catholique de Louvain BE

Infineon DE

NDS IL

Activcard FR

Everbee FR

*Objective* :

To specify and develop a new generation of secure portable devices called Trusted Personal Device (TPD), addressing the main requirements for trust and security of the information society, and relying upon the expertise of European leaders in smart card and security technology. The project aims at defining the common technical foundations to allow cost-efficient product developments of devices with extended features and performances that can better be integrated in heterogeneous networks. The TPD technology can provide devices that will combine a fully integrated security architecture (HW, SW, OS, communications...) with ultra-portability, low-cost, and advanced networking and mobile communication features. The project is innovative at different levels : technology (architecture, extended connectivity, high

speed communications and full network support, real time operating system, autonomous mobile devices supporting direct user interactivity), concept (the future TPD will depend on the software and hardware interoperability with the IT environment), and approach (large collaboration of smart card companies to create consensus on a common platform to be used by industry before the issuing of commercial products).

## **PRIME : Privacy and Identity Management for Europe**

*Co-ordinator* : Compagnie IBM France (FR)

22 partners

Compagnie IBM France FR

IBM Research, Zürich Research Laboratory CH

Unabhängiges Landeszentrum für Datenschutz DE

Technische Universität Dresden DE

Deutsche Lufthansa AG DE

Katholieke Universiteit Leuven, Research & Development BE

Siemens Aktiengesellschaft DE

Hewlett-Packard Ltd. UK

Karlstad University SE

Università di Milano IT

Joint Research Centre IT

Centre National de la Recherche Scientifique, Délégation

Midi-Pyrénées - LAAS FR

Johann Wolfgang Goethe – Universität Frankfurt DE

Chaum LLC USA

Aachen University of Technology / Rwth Aachen DE

Institut Eurécom FR

Erasmus University Rotterdam NL

JaTeK GmbH DE

Tilburg University NL

Fondazione Centro San Raffaele Del Monte Tabor IT

Swisscom AG CH

T-Mobile Deutschland GmbH DE

*Objective* :

To research and develop approaches and solutions for privacy-enhancing identity management that can make the European citizens empowered to exercise their privacy rights, and thus enable them to gain trust and confidence in the information society. The project will address foundational technologies (human-computer interface, ontologies, authorisation, cryptology), assurance and trust, and architectures. It will validate the results on the basis of prototypes and experiments with end-users, taking into account legacy applications and interoperability with existing and emerging identity management standards.

The project will carry out a search for solutions to a set of well defined application scenarios, including on-line healthcare systems, location based services, privacy preserving customer databases, anonymous access to infrastructure for mobile workers, privacy enhancing ambient intelligence. It will support the following seven technical design principles for privacy enhancing identity management : “Design must start from maximum privacy”; “Explicit privacy rules govern system usage”; “Privacy rules must be enforced, not just stated”; “Privacy enforcement must be trustworthy”; “Users need easy and intuitive abstractions of privacy”; “Privacy needs an integrated approach”; “Privacy must be integrated with applications”.

## **s-BORDER : Privacy respectful and threat tuneable traveller smart monitoring system**

*Co-ordinator* : EADS Systems and Defence Electronics SA (FR)

26 partners

EADS System & Defence Electronics FR

SAGEM S.A. FR

Société Internationale de Télécommunications

Aéronautiques Information Network and Computing Bv NL

KFKI Computer Systems HU

Cognitec Systems GmbH DE

Indra Sistemas S.A. ES

Gemplus S.A. FR

Daon Limited IE

Securitas ABs BE

Ente Publico Empresarial Aeropuertos Españoles

Y Navegación Aerea ES

Alitalia IT

France Telecom S.A. FR

Société Générale de Surveillance S.A. CH

White Balance – Projects Pool Agency GmbH DE

White & Case Llp BE

Universität Des Saarlandes DE

A4vision S.A. CH

Net1nordic LV

UK Immigration Service UK

The University of Liverpool UK

London City Airport Ltd. UK

International Civil Aviation Organization CA

Data Explorer HU

Planimeter Data Processing HU

Dartagnan TM Biometric Solutions NL

CANDESIS UK

Objective :

To promote the early adoption of Automated Travel Document Control and Risk Assessment systems during the various phases of the travel, including the border control. This will be part of a global system encompassing leading edge technologies such as advanced biometrics, contactless chip circuits, digital certificates and scoring systems to both automate the flow of no-risk passengers and allow detecting potential risky ones. The project will set up a modular platform that will basically combine three complementary approaches to travellers: identification and verification; profiling and threat detection; travel document issuance and authentication. Several trials will be run to validate 1/ the setting up of enrolment procedures for travellers relying on ICAO/IATA recommendations, 2/ the integration of biometrics and bio data within encrypted chip circuit contactless tokens, 3/ recommended practices for profiling and threat detection to achieve interoperable solutions across immigration agencies, airports and airlines, 4/ standardisation, certification and legal approach to respect EU privacy and regulations, 5/ the provision of a relevant business model for the international deployment of these solutions.

The project therefore proposes a R&D bottom-up approach, starting from real technological and societal problems, to reach efficient security solutions impacting the total transport value chain.

## **SECOQC : Development of a Global Network for Secure Communication based on Quantum Cryptography**

*Co-ordinator* : ARC Seibersdorf Research GmbH (AT)

42 partners (for the first 18 months)

ARC Seibersdorf research GmbH AT

AvenTec AT

BearingPoint INFONOVA GmbH AT

Biometric Technologies Ltd. RU  
BRICS, University of Aarhus DK  
Cavendish Laboratory, University of Cambridge UK  
CNRS, Université de Nice FR  
CNRS, Laboratoire Charles Fabry de l'Institut d'Optique FR  
Consiglio Nazionale delle Ricerche IT  
Avanex Corporation – Sede Secondaria IT  
Department of Computer Science, University of Warwick UK  
Department of Electrical and Electronic Engineering, University  
Of Bristol UK  
Department of Optics, Palacky Univerity CZ  
Department of Optics, University of Erlangen-Nürnberg DE  
Department of Mathematics, University of Klagenfurt AT  
Dipartimento di Fisica, Università degli studi di Pavia IT  
Ecole Nationale Supérieure des Télécommunications FR  
Ernst & Young IT-Security GmbH DE  
European Institute for System Security, University of Karlsruhe DE  
Heriot-Watt University, Edinburgh UK  
Hewlett Packard Ltd. UK  
Id Quantique S.A. CH  
Institut d'Informatique et Organisation, Université de Lausanne CH  
Institut für Angewandte Physik, Technical University Darmstadt DE  
Institut für Experimentalphysik, Universität Wien AT  
Institut für Quantenoptik, University of Hannover DE  
Ludwig-Maximilians-Universität München DE  
Politecnico di Milano IT  
QIT, Department of Optics, University of Erlangen-Nürnberg DE  
QUIC Group, Université Libre de Bruxelles BE  
Kungl Tekniska Högskolan, Stockholm SE  
Scuola Normale Superiore, Pisa IT  
SIEMENS AG AUSTRIA AT  
System Security, University of Klagenfurt AT  
Steinbeis Transfer Center, Klagenfurt AT  
THALES Research and Technology FR  
Thales Communications FR  
Toshiba Research, Cambridge UK  
University of Sheffield UK  
University of Copenhagen DK  
University of Geneva CH

Objective :

To specify, design and validate the feasibility of an open Quantum Key Distribution (QKD) infrastructure dedicated to secure communication as well as to fully develop the basic enabling technology. The goal is to be able to use the tools developed for network security services. The S&T objectives are: to realise physical devices ready to allow applicable Quantum Key Distribution; to provide necessary interfaces to QKD devices enabling prospective users the reliable application; to develop a network infrastructure for long-range highly secure communication.

By achieving its goals, the project will enhance the existing landscape of security technologies with novel and reliable secure ways of long range communication. Enhanced communication security will increase the trust in applications such as electronic voting, e-commerce, etc. Moreover, future developments of quantum cryptography are likely to bring about the development of relevant applications (e.g. in mobile communication) and thus additional security for the citizens.

## **SEINIT : Security Expert INITiative**

*Co-ordinator* : Thales Communications S.A. (FR)

13 partners

Thales Communications S.A. FR

6WIND S.A. FR

British Telecommunications Plc UK

T-Systems Nova GmbH DE  
Ecole Nationale Supérieure des Télécommunications FR  
Industrieanlagen-Betriebsgesellschaft MbH DE  
Kyos S.A.R.L. CH  
Telscom A.G. CH  
Thales Research and Technology (UK) UK  
University College London UK  
University of Murcia ES  
Waterford Institute of Technology IE  
Internet Society CH

Objective :

To ensure a trusted and dependable security framework, ubiquitous, working across multiple devices, heterogeneous networks, being organisation independent (interoperable) and centred on the ambient intelligence around an end-user. The technological objectives are to design, and then develop the components to be implemented, to integrate existing and new components on security assessment platforms capable of running real life scenarios. The project will explore new security models and build the architecture and components to address the nomadic, pervasive, multi-players communicating world. The research will rely on the availability of IPv6 networks and deal with the usage of such networks as well as co-existence of IPv4 and IPv6 equipment and sub-networks.

The areas of research include : threats analysis, security audits; specific security issues of ambient intelligence; network infrastructure; mobility and security; monitoring mechanism; interdependence of QoS, accounting and security in emerging converged networks; law enforcement and privacy.

## **ECRYPT : European Network of Excellence in Cryptology**

*Co-ordinator* : Katholieke Universiteit Leuven (BE)  
33 partners  
Katholieke Universiteit Leuven BE  
Ecole Normale Supérieure FR  
Ruhr-Universität Bochum DE  
Royal Holloway, University of London UK  
BRICS, University of Aarhus DK  
University of Salerno IT  
Institut National de Recherche en Informatique et en Automatique FR  
University of Bristol UK  
Gemplus Developpement FR  
France Telecom R&D FR  
IBM Corporation, Research, Zurich Research Laboratory CH  
Technische Universiteit Eindhoven NL  
Université Catholique de Louvain BE  
Universität Duisburg-Essen DE  
Technical University of Denmark DK  
University of Bergen NO  
Lund University, Dept. of Information Technology SE  
Institute for Applied Information Processing and Communications (TU Graz) AT  
Institute of Mathematics at Polish Academy of Sciences PL  
Cryptolog International SAS FR  
Vodafone Group Services Ltd. UK  
Ericsson AB SE  
Schlumberger Systèmes FR  
MasterCard Europe sprl BE  
EDIZONE GmbH Electronic Business Communications and Security DE  
Fraunhofer Gesellschaft zur Foerderung der angewandten Forschung e.V. DE  
Otto-von-Guericke University Magdeburg DE  
Centre National de la Recherche Scientifique (CNRS) FR  
University of Vigo ES

National Inter-University Consortium for  
Telecommunications IT  
University of Geneva CH  
Aristotle University of Thessaloniki GR  
Columbia University USA

Objective :

To ensure a durable integration of European research in both academia and industry and to maintain and strengthen the European excellence in these areas. To reach this goal, 35 leading players will integrate their research capabilities within 5 virtual labs focused on the following core research areas: symmetric key algorithms, public key algorithms, protocols, implementation, watermarking. These labs will advance the state of the art in their domains and develop common tools.

The general objectives of the network of excellence are the following: maintain and strengthen the excellence of European research and industry in the areas of cryptology and watermarking; strengthen and integrate research in cryptology and watermarking in Europe and decrease fragmentation by creating a research infrastructure and by organising research into virtual laboratories; improve the state of the art of practice and theory in cryptology and watermarking; and develop a joint infrastructure for the evaluation of cryptographic algorithms and for a benchmarking environment.

A second type of objectives is to improve the interaction between the research community and the users of cryptology (government, industry, end-users, standardisation bodies).

A third type of objectives is oriented towards fostering integration in the research community.

## **FIDIS : The Future of Identity in the Information Society**

*Co-ordinator* : Goethe University Frankfurt (DE)

www.fidis.net

24 partners

Goethe University Frankfurt DE

AXSionics AG CH

Institute for Prospective Technological Studies – JRC ES

Vrije Universiteit Brussel BE

Unabhängiges Landeszentrum Für Datenschutz DE

European Institute of Business Administration FR

University of Reading UK

Katholieke Universiteit Leuven, Research & Development BE

Tilburg University NL

Karlstad University SE

Technische Universität Berlin DE

Technische Universität Dresden DE

University of Freiburg DE

Masaryk University Brno CZ

VaF. S.R.O. SI

London School of Economics & Political Science UK

Bute-Unesco Information Society Research Institute HU

International Business Machines Corporation CH

Institut de Recherche Criminelle de la Gendarmerie

Nationale FR

Netherlands Forensic Institute NL

Virtual Identity and Privacy Research Center, University

Of Applied Sciences of Bern CH

Europäisches Microsoft Innovations Center GmbH DE

National Technical University of Athens GR

Sirrix Ag Security Technologies DE

Objective :

To shape the requirements for the future management of identity in the European information society and contributing to the technologies and infrastructures needed. The 7 research activities will include: “identity of identity”, profiling, interoperability of IDs and ID management systems, forensic implications, de-identification, HighTechID, mobility and identity.

The project will carry out multidisciplinary research addressing notably the following areas : How the concepts of physical, digital, virtual, partial and cyber identity will be used by the citizen, how they could be abused, the nature of the impact that they will have in shaping the e Society as well as its supporting technologies, and how they need to be defined in order to respect the fundamental rights of the citizens.

The management of identity by the citizen through Identity Management Systems which will both allow identity to be used as a means of navigation in the emerging knowledge society, and open and facilitate access to on-line services.

A deeper understanding about the multiplicity of Identities and Identity Management Systems as they are used in different European cultures as well as in different areas of life and work. Liability and responsibility in the virtual world.

### Specific Targeted Research Projects

#### **DIGITAL PASSPORT : Next generation European Digital Passport with Biometric Data for Secure and Convenient Border Passage**

*Co-ordinator* : Infineon Technologies AG (DE)

7 partners

Infineon Technologies AG. DE

Smaticware AB SE

Smartrac Technology AG. DE

Mirage Holography Studio SI

Centre National de la Recherche Scientifique (CNRS) FR

Microdatec GmbH DE

Siemens AG Österreich AT

Objective :

Development and production of a new generation of digital passports based on the combination of a traditional booklet with a large capacity IC microcontroller containing and processing the cardholder's relevant personal data and biometric data and a new terminal supporting biometry, contactless connection to the digital passport and connection to remote applications. The project will effectively demonstrate how innovative application of state of the art technology can resolve the apparent conflict of requirements in international travel : the need to increase security and the need to increase convenience and efficiency of border passage. It will show how to make border passage secure, smooth and comfortable and it will contribute to equip the industry with the tools to build solutions.

#### **MEDSI : Integration of Geographical Information Systems with DB, decision support management and an auditory system to develop an advanced system that will be able to give support on decisions in a crisis.**

*Co-ordinator* : GRUPO APEX (ES)

10 partners

GRUPO APEX<sub>1</sub> ES

Expert Team Geosysteme Company DE

Fraunhofer Institute for Factory Operation and Automation IFF DE

GISAT s.r.o. – Geoinformation Company CZ

INESC Porto PT

INTEGRAPH Romania RO

Intro solutions TR

Municipality of HOLON IL

Temida SI

T-Soft CZ

Objective :

Integration of Geographical Information Systems together with databases, decision support management tools and an auditory system to develop an advanced system to manage and support decision making in critical situations.

The geographical space of future use will be the current member countries of the European Union and also the candidate countries. The project will emphasise the demonstration of the system in EU candidate countries, thus facilitating the adaptation of the procedures and coordination

of initiatives in the enlarged European Union. The wide range of applications (crisis management, environmental protection, security plans of big infrastructures, events, administration of airport and seaport infrastructures, healthcare, etc.) is likely to strengthen the EU social cohesion.

## **POSITIF : Policy-based Security Tools and Framework**

*Co-ordinator* : Politecnico di Torino (IT)

10 partners

Politecnico di Torino IT

BearingPoint Infonova AT

Bull S.A. FR

Ministero della Giustizia IT

PRESECURE Consulting GmbH DE

Wroclaw University of Technology PL

Secure Information and Communication Technologies AT

St. Petersburg Institute of Informatics and Automation

Of the Russian Academy of Sciences RU

Universidad de Murcia ES

Vodafone Omnitel N.V. IT

Objective :

The project aims to create a policy-based unified security framework, to which different kinds of security tools can be linked. A multi-level policy language will be used to describe the desired security policy (high level requirements and/or detailed controls) while a system language will be used to describe the target system (interconnection topology, functional and security capabilities). A checker will evaluate if the desired policy can be implemented on the target system and will measure the achieved security level. Configurations for the security elements will then be automatically generated and deployed through the network. A monitor will use the security policy for proactive intrusion detection in addition to standard reactive intrusion detection. The framework will be usable by any producer of a specific security block or tool due to the use of open standard based languages, interfaces and protocols for policy and system description, configuration instructions and deployment, threat monitoring. This framework will be complemented by a suite of security tools including high speed firewall, VPN and IDS that target the current challenges and a lightweight security module to protect them against network attacks, make them part of the security system and allow secure downloading of new configurations.

## **SCARD : Side-Channel Analysis Resistant Design Flow**

*Co-ordinator* : Technikon Forschungs- und Planungsgesellschaft mbH (AT)

9 partners

Technikon Forschungs- und Planungsgesellschaft mbH AT

Institute for Applied Information Processing and

Communications, University of Graz AT

Infineon Technologies AG DE

Institute for Information Processing and computer

Supported new Media, University of Graz AT

cv cryptovision GmbH DE

University of Kuopio FI

TUBITAK-UEKAE TR

K.U. Leuven Research & Development BE

Université Catholique de Louvain BE

Objective :

The project will pursue the following objectives :

To research side-channel attacks and countermeasures at both hardware and software levels

To model and simulate side channel effects, and

To establish a semi-custom design flow for micro chips or parts thereof with clear guidelines

and appropriate synthesis tools in order to be able to design and implement side-channel

analysis (SCA) resistant circuits.

One important goal is to intensify the study of attacks - such knowledge is critical for the evaluation of security issues. The project will develop and perform high level analysis (SCA attacks scenarios and attacks), timing jitter attacks, fault insertion attacks, and will exploit a combination of side-channels.

## **SECURE JUSTICE : Secure communication and collaboration framework for the judicial co-operation environment.**

*Co-ordinator* : Project Automation S.p.A. (IT)

20 partners

Project Automation S.p.A. IT

European Dynamics GR

ARAM sp. z.o.o. PL

SchlumbergerSema ES

Aquitaine Europe Communication FR

GL2006 Europe UK

Computas AS NO

Chorus Call GR

Cryptomathic DK

A4Vision CH

Telecom Italia IT

Sineura Spa IT

Centre for Research and Training in Information Technology IT

SDA Bocconi IT

Vrije Universiteit Amsterdam NL

Italian Ministry of Justice IT

Polish Ministry of Justice PL

Greek Ministry of Justice GR

Department of Justice and Security Canaries Islands Regional

Government ES

Cour d'Appel de Bordeaux FR

Objective :

Design and development of innovative secure technologies to be embedded in a distributed environment communication and collaboration framework to be implemented within the judicial multi-sited domain.

The project will develop, test and verify technologies for the protection, security and trustable distribution of digital assets, by reliably and dependably addressing issues of virtual identity management (with authentication based on biometrics and secure access to web based context management system portal), privacy enhancing (with cryptography, secure audio/video transmission, VPN and SSL communication protocols and secure procedures), security and mobility (with secure and efficient mobile communication).

Research is expected to result in a communication platform enabling a secure judicial cooperation process management all along the criminal justice cycle, i.e. from the preliminary investigations phase to the criminal action phase ending with the debate phase. The overall platform will consist in a technological product based on the embedding of the most innovative security technologies into a unique technological solution that enables secure communication and knowledge sharing in large multi-site organisation context.

## **SECURE PHONE : Secure contracts signed by telephone**

*Co-ordinator* : SchlumbergerSema S.A.E. (ES)

7 partners

SchlumbergerSema S.A.E. ES

Informa S.r.l. IT

Telefónica Móviles España, S.A. ES

Nergal S.r.l. IT

University of Saarbrücken DE

The University of Buckingham UK

Groupe des Ecoles des Télécommunications – Institut National

Des Télécommunications FR

Objective :

Realisation of an innovative prototype 3G/B3G enabled PDA enhanced with a biometric recogniser to enable users to mutually recognise each other and to securely authenticate. Secure exchange, modification and electronic signing of audio, image and text files during a phone call. The solution will allow to realise a usable, user-friendly system, avoiding complicated identification paradigms as well as a secure, strong biometrical identification method for use on PDA. It will also seek to avoid social drawbacks of some identification techniques by adopting non intrusive modalities. Lastly it will make it possible for speakers on mobile phone to agree upon multi-format content (audio, image, text) in an easy though legally binding way.