

Identité & Anonymat dans les Systèmes Communicants (Mobiles)

Traian MUNTEAN
&
Robert ROLLAND

Groupe d'Etudes et Recherche en Informatique des Systèmes Communicants Sécurisés



Aix- Marseille Université

Présentation Succincte d'ERISCS

<http://eriscs.esil.univmed.fr>

Une des activités principale du laboratoire ERISCS est d'établir un lien, sur une base scientifique suffisamment large, entre des travaux de recherches et des projets industriels pour la conception correcte des **systèmes communicants critiques**.

Nos travaux recouvrent donc à la fois, dans un même contexte, des aspects très théoriques et des applications très concrètes (e.g. projets Pôle SCS).

Un de nos domaines de recherche est celui de la Conception des Systèmes Communicants Sécurisés (e.g. données personnelles et confidentielles dans des contextes divers de protocoles et de réseaux hétérogènes et mobiles). En plus de la confidentialité et d'authentification, ces systèmes supportent des applications ayant de plus en plus besoin d'**anonymat** des échanges.

Cet exposé présente les concepts et les outils développés par notre groupe pour la **sécurité des systèmes communicants mobiles**.

Systemes Communicants Critiques

Exemple: Protocoles d'échanges de données personnelles confidentielles

Ce problème est traité par une construction cohérente utilisant les techniques cryptographiques les plus récentes recommandées par des organismes internationaux (NSA, ANSSI, NIST,...).

- Chiffrement à clé secrète (AES-Galois Counter Mode).
- Echange de la clé secrète par cryptographie à clé publique elliptique (ex. Elliptic Curve Station to Station Protocol).
- Production d'une marque d'authentification (ex: utilisation d'AES en mode Galois Counter). Ainsi un intervenant local peut transmettre à travers un téléphone mobile ou une tablette personnelle des données (mesurées sur un patient par exemple à une équipe médicale spécialisée distante qui peut alors prendre les décisions les plus pertinentes).

➤ voir projets Pôle SCS: SNT (DGCIS-DGA); EVASI (PacaLabs)

Anonymat : des données et des échanges

Exemple (suite): anonymisation de données pour un traitement ultérieur

Considérons des données médicales qui doivent être transmises par un personnel de santé à un organisme chargé de statistiques ou de tout autre traitement ultérieur. Les patients auxquels se rapportent ces données doivent rester anonymes tout en étant distinguables les uns des autres afin d'assurer un suivi des événements observés.

Là encore le problème est traité par la mise en place d'un protocole construit à partir de primitives cryptographiques bien choisies.

La CNIL, habilitée à agréer de telles applications, impose à assurer le respect de la vie privée des patients.

- *besoin de plate-forme cryptographique adaptative pour divers protocoles et des interfaces applicatives génériques*
 - ✓ *ERISCS propose une plate-forme de sécurité ARCANA + CryptoBox complète & interfaces applicatives et support pour mobilité*

L'anonymat = composante Identitaire

Protéger la confidentialité

- Secret des contenus des communications privées
 - authentification et anonymat (cryptographie géométrique)
- Routage Anonyme dans les réseaux mobiles :
 - Incapacité pour des tierces parties de déterminer les participants aux échanges
 - Eviter les « traces oubliées » ; prévenir le traçage intempestif/intrusif

Divulgarion contrôlée et hiérarchisée des IDs

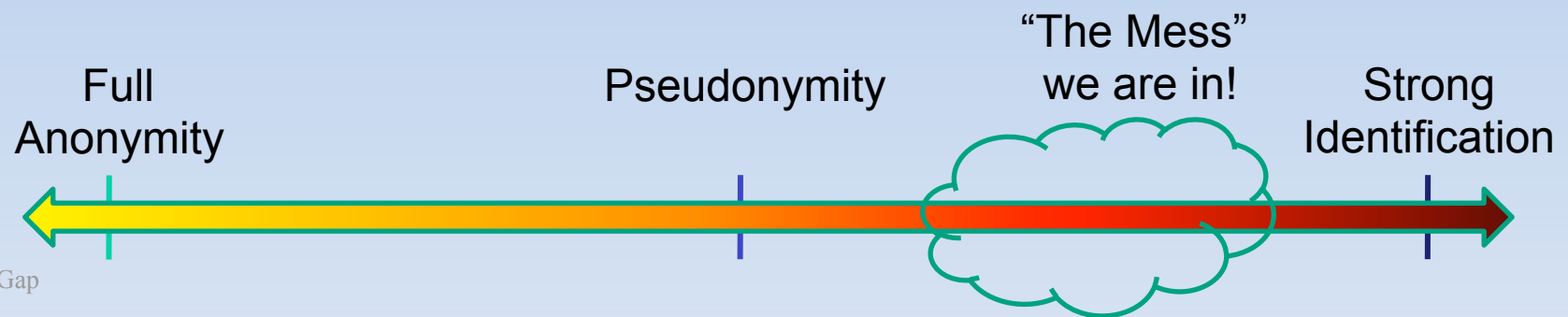
- Chiffrement des contenus ne suffit pas,
Émetteurs et Récepteurs toujours découvrable à tous niveaux des protocoles d'échange,
- → Anonymiser par niveaux de filtrage des communications; Accès aux Services
- Gestion dynamique de Groupes Identifiables (de confiance ou non!)

Identité Réseau

- Communications

- Relation entre identités et routage efficace
- « Today, no network privacy = no privacy ! »

- Le spectre de l'Identification:



Anonymité dans les communications

■ Applications Spécialisées

- “Vote électronique”
- E-commerce
- Incidents et leur suivi
- Protection des témoins
- Protection vie privée

■ General applications

- Droit à la parole
- Profilage
- Investigation marchés
- Protection contre la censure

Développement d'une Plateforme Logicielle de Sécurité ARCANA

- **A quel niveau sécuriser ? Avec quels protocoles?**
- **Niveaux d'anonymat autorisés; contrôle?**

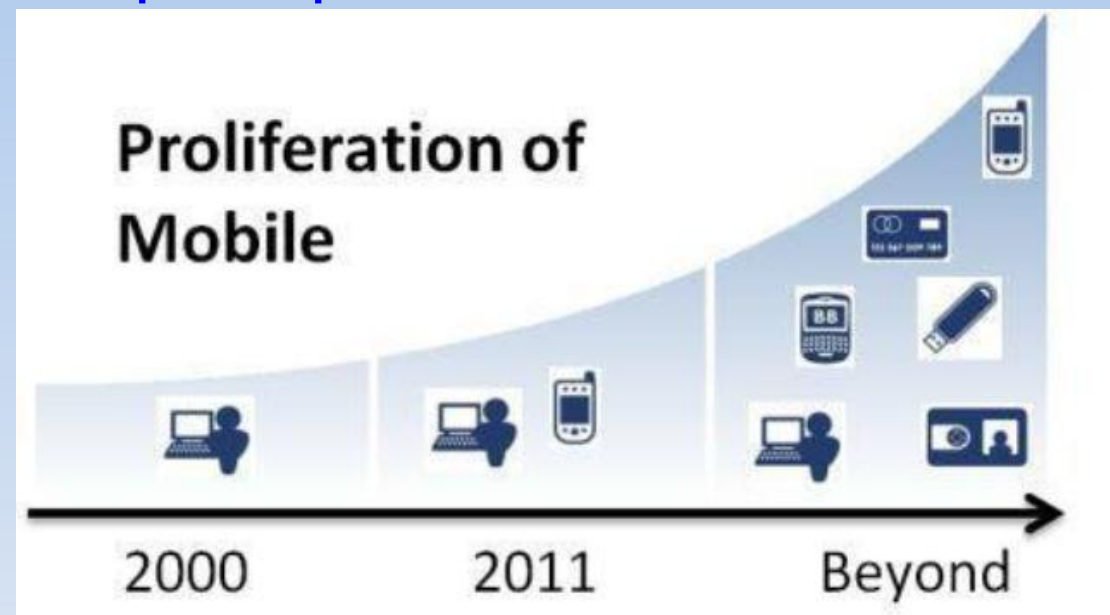
Au niveau applicatif

- Indépendant du moyen de communication
- Sécurité adaptable aux types de données
- Sécurité sur les couches inférieures contrôlable
- Hiérarchies de Visibilité et Anonymat
- Primitives génériques et adaptatives nécessaires

Mobilité et Sécurité : un enjeu capital

La généralisation des Smartphones a engendré de nouveaux comportements et classes d'utilisations

- le "nomadisme professionnel"
- le "nomadisme grand publique"



Mobilité et Sécurité : un enjeu capital

La sécurité des données embarqués

Types de données à sécuriser

- Données internes au matériel
- Données étendues par une carte SD, USB ...
- Sauvegarde à l'extérieur du mobile (Cloud Backup)

Android depuis Version Froyo 2.2 :

- Déplacement vers la carte SD
- Sauvegarde sur le serveur de Google

➤ **Protéger les données par chiffrement applicatif**

Plateforme Logicielle de Sécurité

ARCANA (© ERISCS)

ECDB

- Base de données de courbes elliptiques (par opposition à la position du NIST qui utilise une seule courbe)
- Intégré à une CryptoBox

KTB-CryptoBox

- Un noyau complet de primitives cryptographiques
- Indépendance vis-à-vis des protocoles
- Maîtrise de toute la chaîne de sécurité

Fonctionnalités ARCANA

■ Primitives de base

- Classes d'algorithmes:
 - Générateur pseudo-aléatoire
 - Fonctions de hachage
 - Chiffrement symétrique
 - Signature ECDSA – courbes elliptiques
 -

Fonctionnalités ARCANA (2)

■ Primitives de base

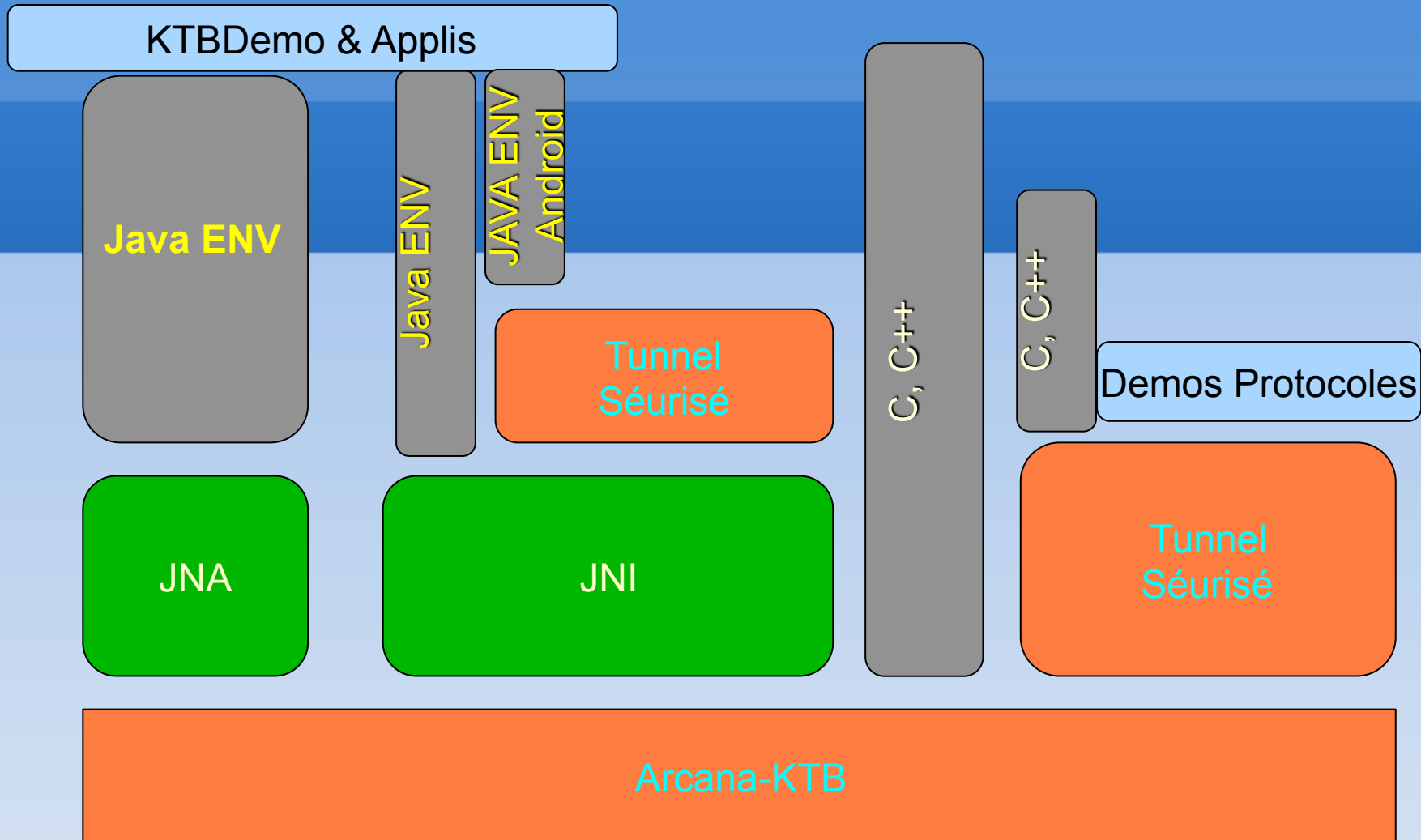
- Classes d'algorithmes
- Algorithmes standards et plus
 - AES, SHA-2...
 - SHA-3: exemple de nouvel algorithme de hachage - [Parralel Skein](#) (proposition NIST)
 - Cryptographie sur courbes elliptiques (Courbes du NIST + [Arcana-ECDB](#))
 - Flexibilité permettant d'étendre la bibliothèque avec de nouveaux résultats et/ou algorithmes

Fonctionnalités ARCANA (3)

■ Développement de protocoles de plus haut niveau

- Échange de clés « classique » (DH, S2S)
- Protocole d'échange de clés (KTP) et **gestion de clés hiérarchiques pour anonymat des émetteurs dans les réseaux mobiles** (application M-Pub –projet DGCIS)
- Applications: projets de recherche ERISCS s'appuyant sur les « briques » ARCANA-CryptoBox
 - Satellite Network Terminal
 - Télémédecine
 - Dossier Médical Anonymisé
 - Archivage pérennisé

Architecture ARCANA



Arcana-KTB

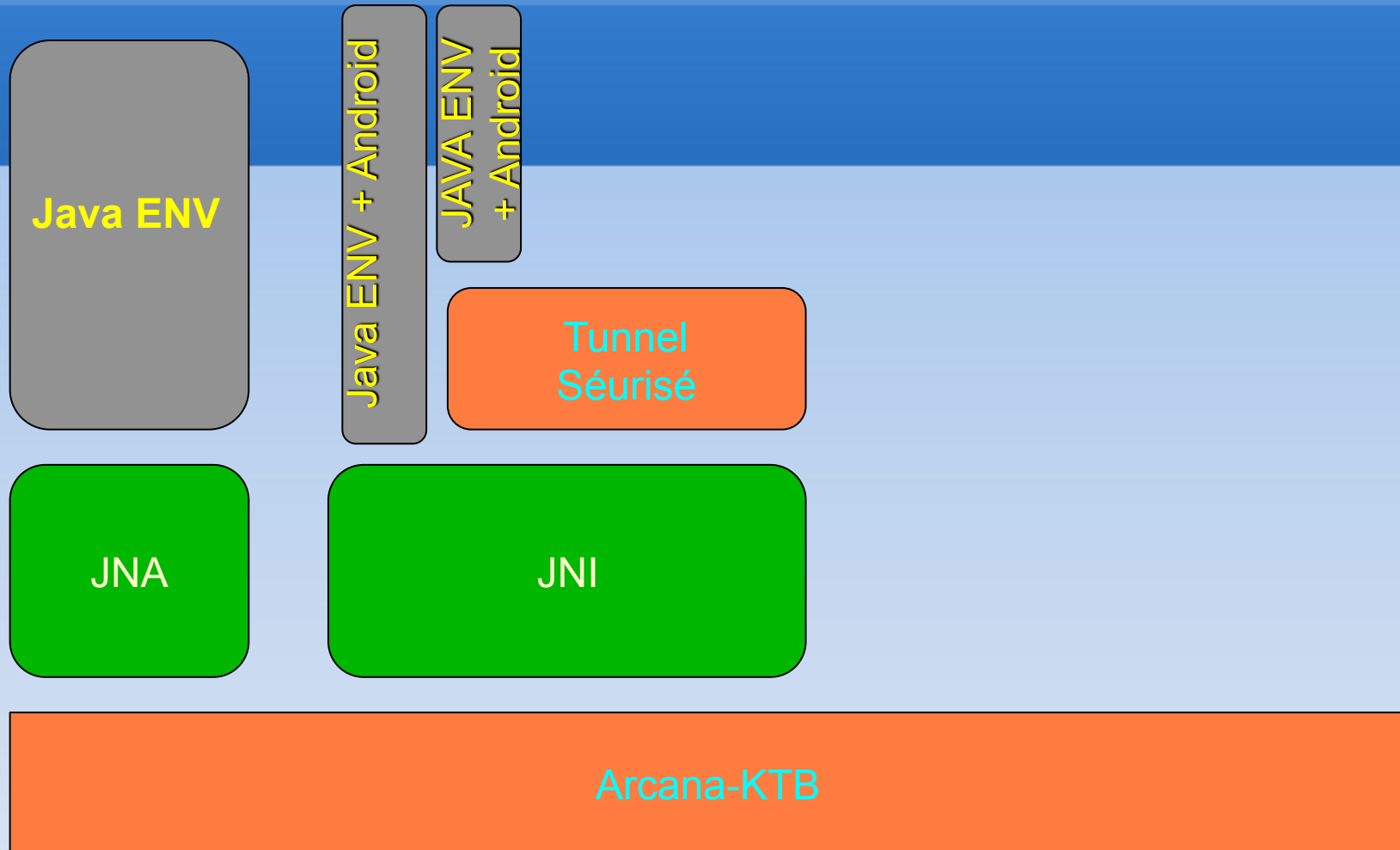
- Écrite en C
- Plusieurs primitives cryptographiques
- Composé de différents modules :
 - Pseudo-Random Number Generation
 - Hash and HMAC
 - Symmetric encryption
 - Key Derivation Functions
 - Key Exchange Protocols
 - Key Encapsulation Mechanisms
 - Elliptic Curves Digital Signatures
 - Public/Private keys management
 - Elliptic Curves Management

Couche Accessibilité

JNA : Java Native Access

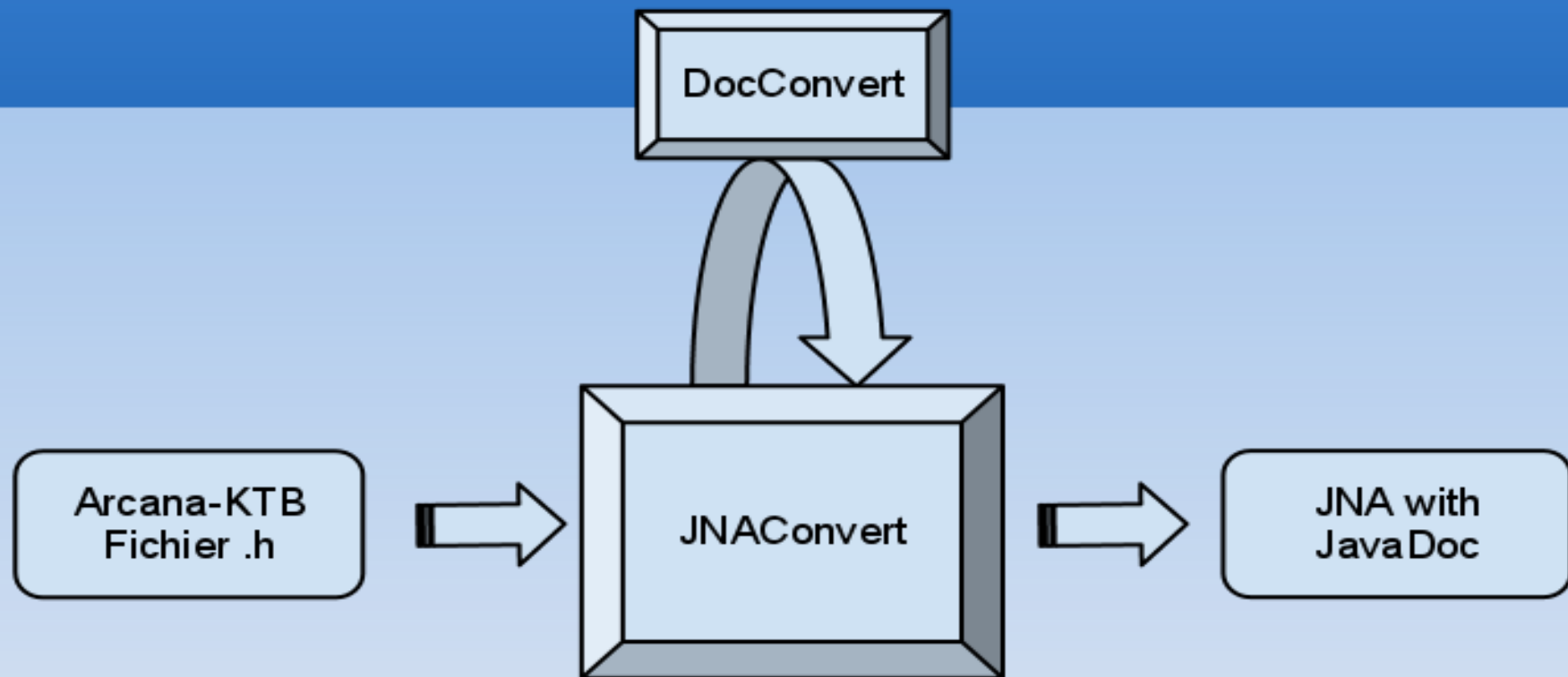
- Permet l'utilisation du code de bibliothèques natives en C
- Utilise une bibliothèque native pour dynamiquement invoquer du code natif
- Écrire des classes Java spécifiques en reprenant les noms des fonctions et leurs paramètres .

Accessibilité Java



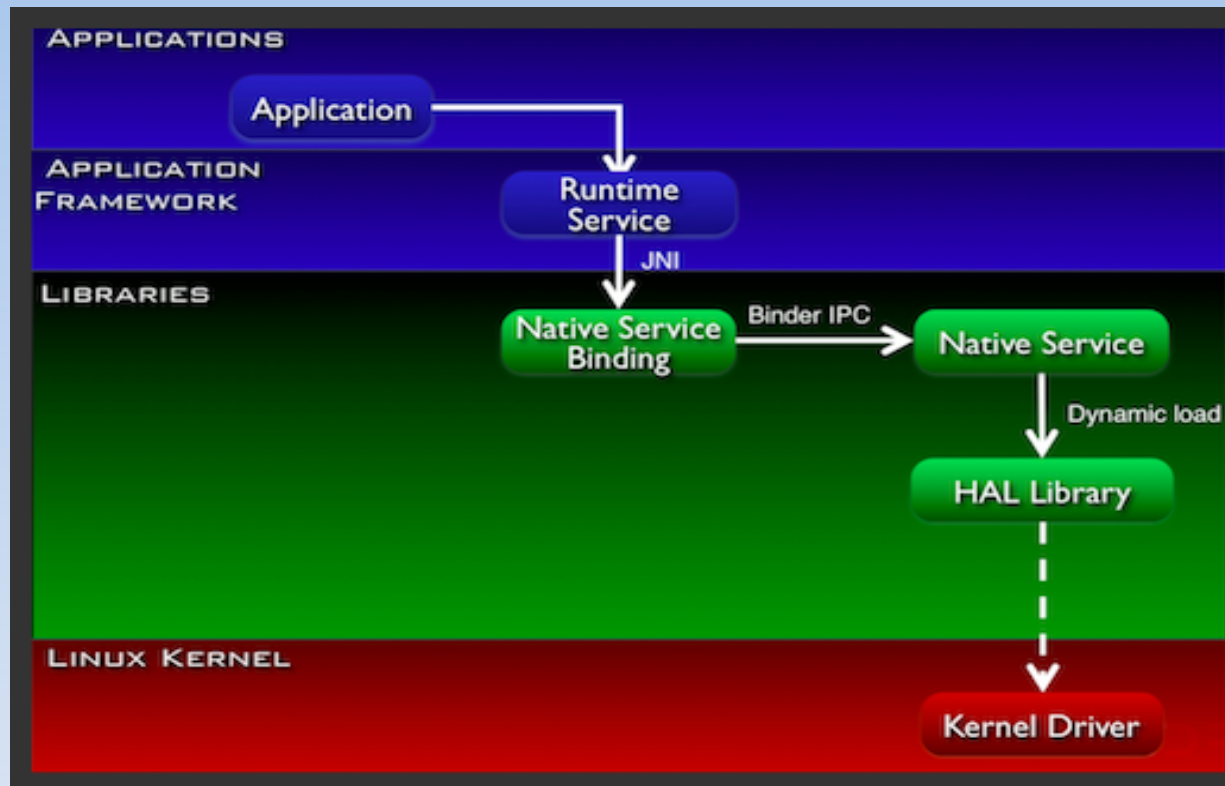
Couche Accessibilité

JNA : Java Native Access



Couche Accessibilité

JNI : Java Native Interface



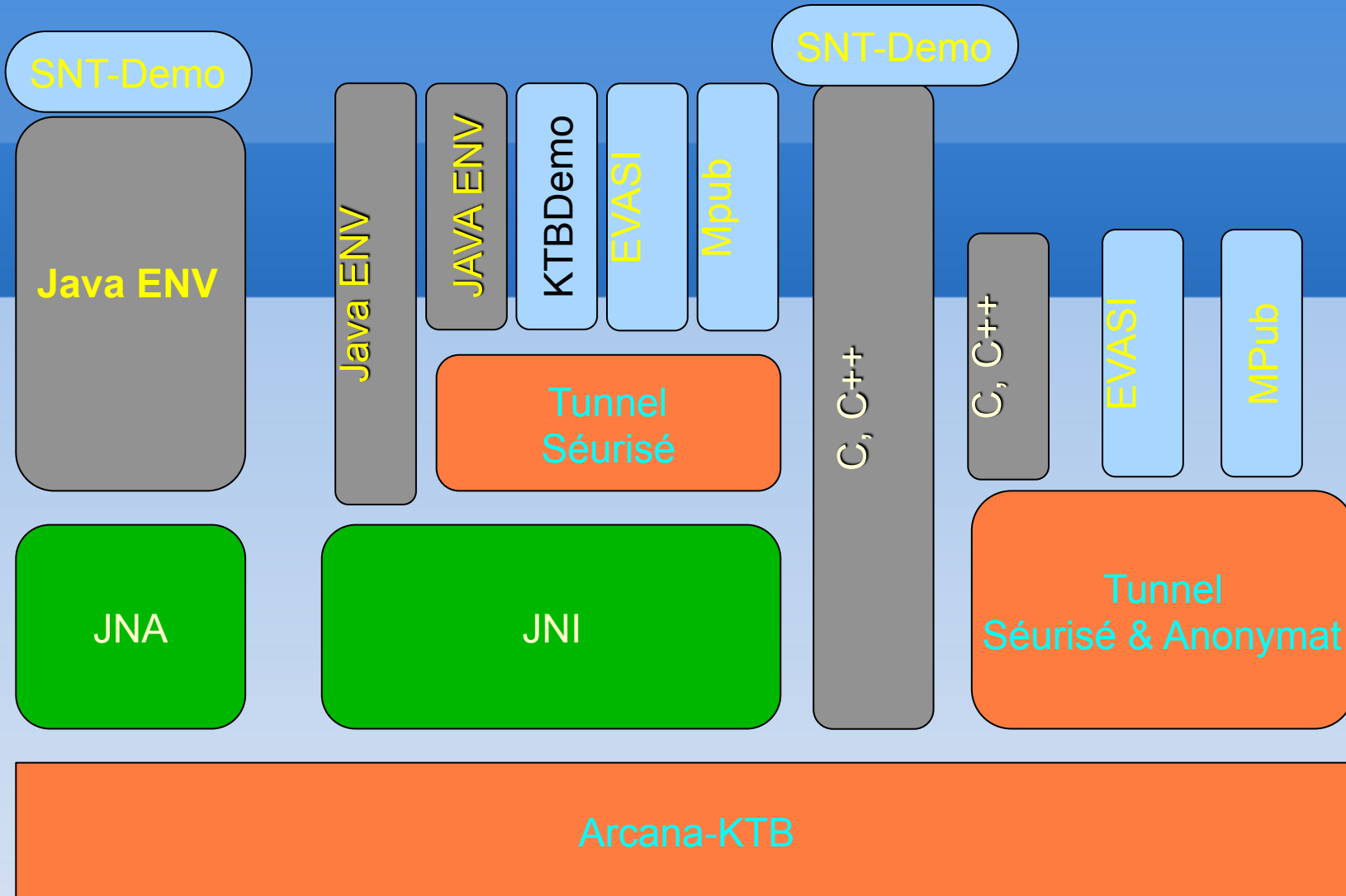
Plateforme Arcana-Cryptobox

Tunnel Virtuel Sécurisé

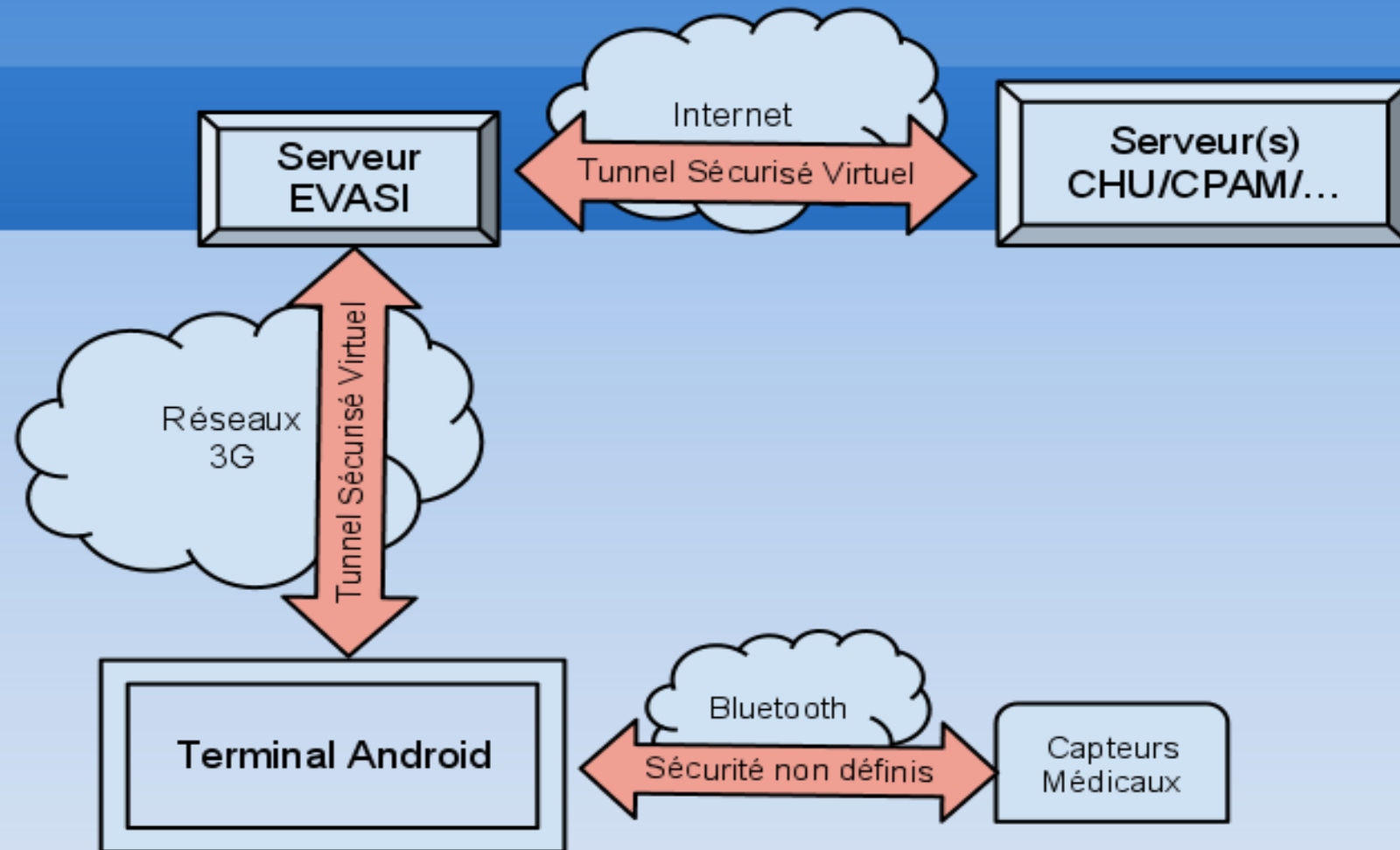
- Les contraintes :
 - Connexion sécurisée entre deux hôtes distants
 - Compatible avec tous les moyens de communication
 - Au moins un des hôtes est “peu puissant”

- Les principales pistes de solutions :
 - Choix des courbes elliptiques
 - Mode d'utilisation des algorithmes

Projets et Applications



Projet EVASI (PacaLabs)



Projets d'applications

Projet EVASI

Functionalité de la démo

- Créer un patient
- Modifier le dossier d'un patient :
 - Température
 - Rythme cardiaque
 - Pronostique
 - Photo
- Mise à jour en temps réel sur les terminaux connectés sur le même dossier

Projet AndroChat

Objectif

Démontrer les capacités du Tunnel Sécurisé Virtuel

Architecture

- Client Android
- Serveur C
- Réseau TCP/IP

Projet livré à un partenaire industriel .

KTBDemo

Objectif

- Mise en place d'exemples d'utilisation de la KTB sous Android
- Effectuer des Tests de performance

Functionalités

- Gestion de clés
- Transfert de clés
- Test Tunnel Virtuel Sécurisé

Développements futurs

- Echange hiérarchique de clés
- Intégration des différents modules

Arcana-KTB

- **Portabilité de la plate-forme de sécurité**
 - Faible dépendance externes (GMP)
 - Majorité de la bibliothèque en code C standard
 - Testé sur des systèmes Linux (32/64bits), Windows (32bits), Android (Tablettes, Téléphones),...

Boîte à outils cryptographique

Arcana-KTB

Exemple de protocole : Échange de clé Station-to-Station

- Basé sur Diffie-Hellman
- Inclue un mécanisme de signature (ECDSA)
- Indépendant des moyens de communication

Interfaces ARCANA

Interface de développement Java

- 1 - Mise à disposition du code natif en Java (JNA)
- 2 – Intégration Java complète (JCA)

JNA – Java Native Access

Permet d'appeler du code depuis un fichier objet natif en Java

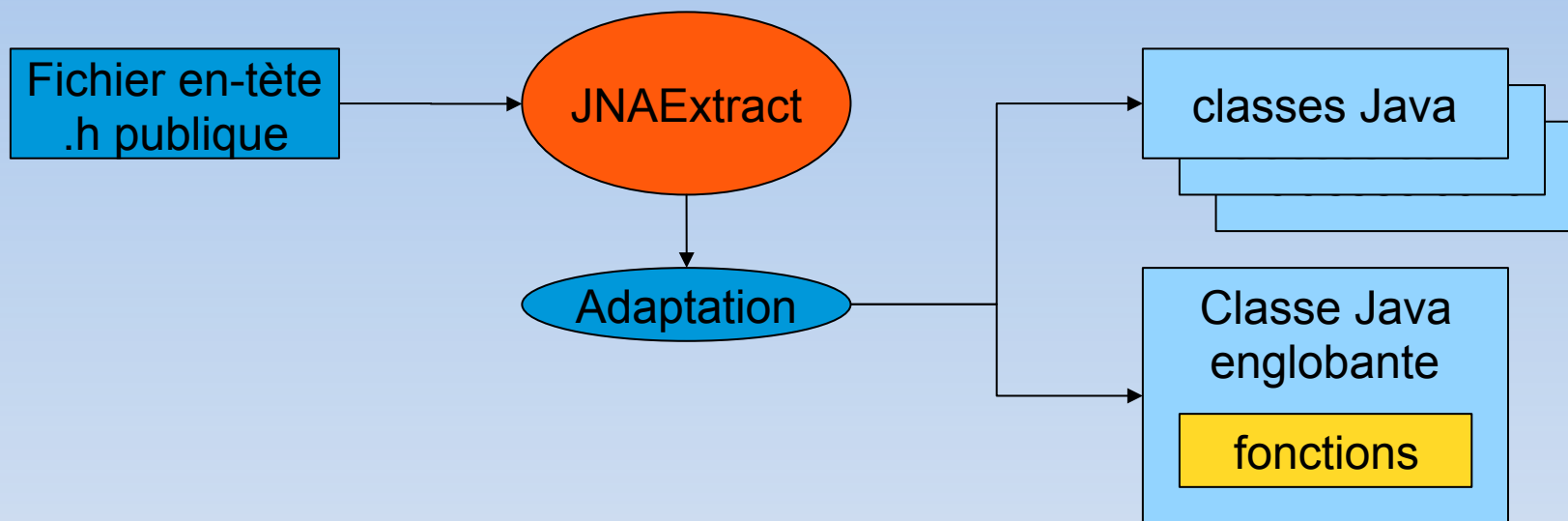
JCA – Java Cryptographic Architecture

Un ensemble de classes coopérant pour fournir à l'utilisateur une abstraction similaire à celle décrite précédemment

Boîte à outils cryptographique

Arcana-KTB

Mise à disposition du code natif en Java (JNA)



Boîte à outils cryptographique

Arcana-KTB

Intégration Java complète (JCA)

Principe de JCA : des interfaces génériques masquant différentes implémentations

Boîte à outils cryptographique

Arcana-KTB

■ Extension de la plateforme

- Amélioration des algorithmes
 - Performances (parallélisation, optimisations)
 - Fiabilité (correction de défauts)
 - Spécialisation pour matériels spécifiques (GPGPU...)
- Ajouts de nouveaux algorithmes / protocoles
 - Exemple SHA-3 : Skein, etc.
 - Protocole d'échange de clefs développé par eRISCS

PUBLICATIONS RECENTES ASSOCIÉES

- Kévin Atighehchi, Traian Muntean; Parallelization of cryptographic primitives-Application to SKEIN ; ePrint 2011
- Gabriel Risterucci; Boîte à outils cryptographique Arcana-KTB; Crypto'Puces 2011
- Robert Rolland, Elliptic curves - Edwards curves, Crypto'Puces 2011
- K. Atighehchi, T. Muntean, R. Rolland, L. Vallet : « A Keys Transfer Protocol for Secure Communicating Systems », SYNASC'2010-IEEE
- S. Ballet, J. Pielant : « On the tensor rank of multiplication in any extension of F_2 », preprint 2010
- S. Ballet, R. Rolland : « A note on a Yao's theorem about pseudo-random generators », preprint 2010
- A. Enache, K. Atighehchi, T. Muntean, G. Risterucci, R. Rolland : « An Efficient Parallel Algorithm for SKEIN hash functions », IEEE-PDCS 2010
- T. Muntean : « Anonymity and Privacy in Communicating Critical Systems », Keynote Talk ICCP'2010
- H. Ivey-Law, R. Rolland : « Constructing a database of cryptographically strong elliptic curves », Proceedings of SAR-SSI 2010: Fifth Conference on Network and Information Systems Security (SAR/SSI 2010), Roquebrune Cap-Martin, France
- D. Kohel, R. Rolland (editors) : « Arithmetic, Geometry, Cryptography and Coding Theory », Contemporary Mathematics, AMS, Vol. 521 (2010)
- S. Ballet, R. Rolland : « Families of Curves over any finite field attaining the generalized Drinfeld-Vladut », Publications Mathématiques de Besançon, Algèbre et Théorie des Nombres.2009
- S. Ballet, R. Rolland : « Families of curves over any finite field with a class number greater than the Lachaud », Martin-Deschamps bounds. arXiv: 2009
- A. Bonnetcaze, A. Gabillon : « On Key Distribution in MANETs », IEEE International Conference on Signal-Image Technology and Internet-based Systems (SITIS'09). December 2009. Proc of IEEE Computer Society.
- Duc-Phong Le, A. Bonnetcaze, A. Gabillon : « Multisignatures as Secure as the Diffie-Hellman Problem in the Plain Public-Key Model », Pairing2009, August 12-14, Stanford university Palo Alto, USA, (LNCS), 2009
- T. Muntean, L. Vallet : « Anonymat par diffusion sélective de clés dans les réseaux mobiles », Crypto'Puces 2009