NEW TRENDS IN CRYPTOLOGY : BIOMETRICS, QUANTUM CRYPTOGRAPHY AND PAIRINGS [3 ECTS]

Cryptologie : biométrie, quantique et par couplages

Code ECTS

Total course volume: 30h
Period : 1, 2 bimester

Professors : Jean François MAINGUET, Pablo ARRIGHI, Philippe ELBAZ-VINCENT

E-mail: jean-francois.mainguet@atmel.com, pablo.arrighi@imag.fr, Philippe.Elbaz-Vincent@ujf-grenoble.fr

Objectives

Introduce new trends in cryptography and/or cryptanalysis which are currently hot topics.
For 2008, the chosen topics are Biometrics, Quantum cryptography and Pairing-based cryptography.

Biometrics (JF Mainguet) : what is biometrics, how biometrics can replace passwords and keys, integration with cryptography, testing biometrics is difficult.

Quantum cryptography (P Elbaz-Vincent): About twenty years ago a number of physicists and computer scientists (Bennett & Brassard) have begun to understand the tremendous advantages which phenomena of quantum physics -- such as entanglement and wavepacket collapse -- could bring to information processing. After a brief introduction to the postulates of quantum mechanics as formulated in terms of basic Linear Algebra, we shall study the main quantum key distribution protocol actually implemented and commercialized nowadays.

Pairings (P Arrighi): Since the introduction of pairings in constructive cryptographic applications, an ever increasing number of protocols have been appearing in the literature: identity-based encryption, short signature, and efficient broadcast encryption to mention but a few. An appropriate mix of theoretical foundations and practical considerations is essential to fully exploit the possibilities offered by pairings: cryptographic protocols, software and hardware implementations, new security applications, etc.

Contents

Biometrics : objectives, fundamentals, verification/authentication, biometric modalities (fingerprint, iris, face…), the biometric market, applications, testing biometrics, standards, security and biometrics, integration with cryptography, privacy, myths.

Quantum cryptography: introduction to the postulates of quantum mechanic, quantum key distribution protocol, practical applications to commerce and industry.

Pairings : mathematical foundation, cryptographic protocol, software/hardware implementations, applied security (security ubiquitous computing, security management, network security, grid computing, PKI model, internent and web security, e-business)

Prerequisites

Biometrics : none

Quantum cryptography : basic linear algebra

Pairings : SAC: PKI

Examination
1 final exam in 3 parts (one part for each topic)

Final mark session1 : 30%ET1 (Biometrics) + 40% ET2 (Pairings) + 30%ET3 (Quantum cryptography)

DESCRIPTION IN FRENCH

Objectifs de l'enseignement

Présenter de nouvelles méthodes en cryptographie et/ou cryptanalyse qui sont particulièrement d'actualités et en plein essor. Pour 2008, les thèmes choisis sont Biométrie, Cryptographie quantique et cryptographie basée sur les couplages.

Biométrie : découverte de la biométrie, dans quelle mesure elle peut remplacer les mots de passe et les clés, comment elle s'intègre avec la cryptographie, la difficulté de tester les systèmes biométriques.

Cryptographie quantique : Depuis une vingtaine d'année des physiciens et des informaticiens (Bennett & Brassard 1984) découvrent les formidables atouts que peuvent représenter des phénomènes de la mécanique quantiques tels que l'intrication et la réduction du paquet d'onde pour le traitement de l'information. Après une brève introduction aux postulats de la mécanique quantique formulés en terme d'algèbre linéaire de base nous étudierons le principal protocole de distribution de clé quantique, dont les implémentations existent et sont commercialisées actuellement.

Couplages : Depuis l'introduction effective des couplages en cryptographie, un nombre croissant de protocoles sont apparus dans la littérature: chiffrement basé sur l'identité, signature courte, chiffrement effectif de broadcasting. Un mélange judicieux de méthodes théoriques et de considérations pratiques est essentiel pour exploiter pleinement les possibilités offertes par les couplages: protocoles cryptographiques, implémentations matériels et logiciels, nouvelles applications de sécurité, etc.

Contenu

Biométrie : objectifs, principe fondamental, vérification/authentification, les diverses modalités biométriques, examen des modalités les plus usitées (empreinte digitale, reconnaissance faciale, iris) tant du coté capteur que du coté algorithme, le marché de la biométrie, les déjà nombreuses applications existantes (commerciales, gouvernementales), évaluation des performances biométriques (FAR & FRR), normalisation, le sécurité des systèmes biométriques (cryptographie / détection de vitalité), introduction à la biométrie intriquée avec la cryptographie (le Grâal de la biométrie), protection de la vie privée, mythes et réalités.

Cryptographie quantique : introduction à la mécanique quantique, protocoles quantiques de distribution de clefs, applications dans le commerce et l'industrie.

Couplages : fondements mathématiques, protocoles cryptographiques, implémentations, sécurité appliquée.

Pré requis

Biométrie : aucun.

Cryptographie quantique : algèbre linéaire élémentaire.

Couplages : SAC: PKI

Forme d'examen

1 examen final en 3 parties (une pour chaque thème)

Bibliographie / textbooks

Biometrics :
Guide to Biometrics by Ruud Bolle**,** Jonathan Connell**,** Sharanthchandra Pankanti**,** Nalini Ratha**,** Andrew Senior, Springer Verlag 2003.
La Biometrie de Jacky Pierson, Hermes 2007
Hand book of Fingerprint Recognition by David Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, Springer 2005
Quantum cryptography :
Quantum Computation and Quantum Information by Michael A. Nielsen, Issak L. Chuang, Cambridge University Press 2000.
Pairings :
Advances in Elliptic Curve Cryptography: Further Topics v. 2 (London Mathematical Society Lecture Note Series) by Ian F. Blake **,** Gadiel Seroussi **,** Nigel P. Smart **, Cambride University Press, 2005.**