Attività scientifica e didattica negli ambiti affini alla crittografia

Nicola Laurenti

Università degli Studi di Padova

Riunione dell'Associazione De Componendis Cifris
Bologna - Napoli - Roma - Torino, 22 gennaio 2018

Aree di ricerca e docenti coinvolti

Teoria dei Numeri Alessandro Languasco (DM)

Information theoretic security Nicola Laurenti, Stefano Tomasin (DEI)

Teoria dei Codici Tomaso Erseghe (DEI)

Crittografia quantistica sperimentale Nicola Laurenti, Giuseppe Vallone, Paolo Villoresi (DEI)

Sicurezza delle reti wireless Mauro Conti, Nicola Laurenti, Stefano Tomasin (DM, DEI)

DM: Dipartimento di Matematica
DEI: Dipartimento di Ingegneria dell'Informazione

Teoria dei numeri

- teoria analitica delle funzioni zeta e L
- teoria additiva dei numeri e partizioni
- teoria moltiplicativa dei numeri

Experimental Quantum Cryptography

Quantum key agreement

- Free space and satellite QKA
- Finite length security analysis

Quantum random number generators

Bell certified QRNG

Wireless communication security

GNSS authentication, integrity protection, access control

- Digital signature amortization
- Key management architectures
- Security analysis of hash chains
- Physical layer signatures

Wireless and mobile authentication and secure positioning

- physical layer authentication
- authenticated ranging / positioning

Information theoretic security

Physical layer security for MIMO-OFDM systems

- PHY secrecy
- PHY key agreement
- PHY authentication

Physical layer security for 5G and IoT

- PHY authentication graphs in random networks

Coding theory

- finite length performance bounds
- decoding with distributed algorithms

Corsi di Laurea Magistrale in Matematica e in ICT

Corso di Crittografia (A. Languasco)

Scopo Fornire le basi teoriche per uno studio critico dei protocolli crittografici

Contenuti Modular arithmetic. Prime numbers. Little Fermat theorem. Chinese remainder theorem. Finite fields. Pseudoprimality tests. AKS test. RSA method, Rabin's method. Discrete logarithm methods. Elementary factorization methods.
Fundamental crypto algorithms. Symmetric methods (DES, AES). Asymmetric methods. Attacks. Digital signature. Pseudorandom generators. Key exchange, secret splitting, secret sharing, secret broadcasting, timestamping.

Esame scritto

Durata 48 ore, 6 cfu

Corsi di Laurea Magistrale in Ing. Telecomunicazioni ed Informatica

Corso di Sicurezza delle Reti (N. Laurenti)

Scopo Guidare lo studente tra i concetti e gli strumenti della sicurezza dell'informazione, ai vari livelli di una moderna rete di comunicazioni.

Contenuti Concetti fondamentali di sicurezza dell'informazione.
Meccanismi di sicurezza crittografici e non.
Protocolli di sicurezza ai vari strati dei modelli di rete.
Ulteriori problematiche di sicurezza specifiche per reti wireless, ad hoc e mobili.

Esame (tesina $\vee$ progetto) $\wedge$ orale

Durata 48 ore, 6 cfu

Corsi di Dottorato in Ing. Informazione e in Matematica

Corso di Information Theoretic Methods in Security (N. Laurenti)

Scopo providing the students with an information theoretic framework that will allow formal modeling, understanding of the fundamental performance limits, and derivation of unconditionally secure mechanisms for several security-related problems.

Contenuti Physical layer secrecy and secrecy capacity
Information theoretic and quantum key agreement
Information theoretic physical layer authentication
Mutual information jamming games
True random number generators
Steganography, watermarking and other information hiding techniques
Universal composability and unconditional security
Info theoretic anonymity measures and differential privacy

Esame Project. Students are encouraged to work from an information theoretic point of view on a security problem related to their research activity.

Durata 20 ore, 5 cfu