De Cifris: our research lines

Massimo Giulietti

Università degli Studi di Perugia

ITASEC18
8 February 2018

Research in Cryptography

Cryptography vs general research in Cybersecurity

Research in Cryptography

Cryptography vs general research in Cybersecurity

Research in crypto needs:

- deep knowledge of mathematical topics
- amount of time necessary to perform a research and to make it applicable
- integration and cooperation with research in Cybersecurity

State of the art Crypto

- Symmetric: Block ciphers, Stream ciphers
- Hash functions
- Public Key: RSA, ECC

- Technological innovations stimulated new lines of research in Cryptography and determined dramatic advances in the last ten years

Innovations in modern Cryptography

- Homomorphic encryption
- Blockchain
- Post-Quantum Crypto
- Cryptography for IoT

Homomorphic encryption

- traditional cryptosystems are not suitable when confidential data are meant to be stored for future rework, for instance in **cloud computing**
- the aim of homomorphic encryption is to make it possible to **perform complex operations on encrypted data without decrpting it**

Nowadays challenges

- *fully homomorphic* cryptosystems have been known for a few years
- the problem of **efficiency** remains open (and compelling)

Blockchain

distributed public database, which uses cryptographic techniques to guarantee integrity and to make data immutable once written in the database

Blockchain

distributed public database, which uses cryptographic techniques to guarantee integrity and to make data immutable once written in the database

- *unpermissioned blockchain*: no central authority, no shared secrets among participants, does not rely on honest behaviour
- *permissioned blockchain*: applicable in controlled scenarios; central authority needed, but availability and integrity of data, as well as efficient implementation, are still there
- not only cryptocurrencies: real estate registries, health national or local systems, e-voting, smart contracts

Post-quantum Crypto

Security of public key cryptosystems in use (RSA, DH, ECC) is based on the difficulty of solving certain mathematical problems:

1. factorization
2. discrete logarithm in finite fields
3. discrete logarithm in the group of points of an elliptic curve

Post-quantum Crypto

Theorem (Shor, 1997)

A quantum computer can factor an integer in polynomial time.

P.W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM J. Comput., pp. 1484 – 1509, 1997.

All the three mathematical problems above are **weak** for a quantum computer

Post-quantum crypto

How can we defend ourselves?

- **Post-quantum cryptography**: public key cryptosystems which can resist quantum computer attacks, but at the same time can be used on traditional devices

Post-quantum Cryptosystems

- Error correcting codes:
  - **McEliece-Niederreiter**
- Lattices
  - **NTRU**
  - **New Hope**
  - **Ring-LWE Signature**
- Polynomials
  - **Hidden Field Equations**
  - **Unbalanced Oil and Vinegar Cryptosystems**
- Hash-based cryptography
  - **Merkle signature scheme**
- Isogenies of supersingular elliptic curves

Crypto for IoT

- many **emergent areas** where **devices with limited computational/memory resources are connected**
  Ex: automotive systems, wireless networks, distributed control systems, home automation
- exponential growth of number and types of common objects connected to internet

Lightweight crypto

- in all such areas security is crucial
- most of modern cryptosystems have been designed for a desktop/server environment; cannot be implemented in devices with limited resources

- solution: **Lightweight cryptography**
- a lot of work to do in terms of **standardization**, **transpacrency** and **certification** of algorithms

De Cifris matrix: who does what?

Block ciphers

- Università di Milano - DI: Optimization of linear components
- Politecnico di Milano: Side-channel cryptanalysis
- Università di Trento: Boolean functions (S-boxes); algebraic properties of AES-like block ciphers
- Università di Roma Tre - DMF: Algebraic attacks
- Università di Roma La Sapienza - DI: Cryptosystems resisting leakage and tampering attacks with the memory

Other classical topics

- Hashing/Signing
  - Università di Padova - DM, DEI: Physical layer signature/authentication
  - CNR - ICAR: Crypto for new authentication and integrity services; Physical authentication codes
- RSA attacks
  - Università di Torino
  - Università di Trento
- ECC
  - Università di Trento: Index calculus for prime fields and summation polynomials
  - Università dell'Aquila, della Basilicata, di Perugia, di Torino

Homomorphic encryption

- Università di Catania: Homomorphic MAC and signature
- Politecnico di Milano: Access privacy aware data structures for cloud data outsourcing; Cryptanalysis of noise free FHE schemes
- Università di Trento: Attribute based encryption for cloud
- Università della Campania: Integrated techniques for compression and encryption of genome; efficient search on encrypted data
- Università Politecnica delle Marche: Encryption, encoding and slicing for dispersed cloud systems

Lightweight

- Università di Milano: Protocols and implementation
- Politecnico di Milano: Scalable and energy efficient realizations
- Università di Trento, L'Aquila: Algebraic properties

Blockchain

- Università di Milano: BC and copyright
- Università di Firenze: BC and *buoni pasto* management
- Università di Salerno - DIEM: Privacy enhancing crypto in BC
- Università di Trento: New payment systems; BC for data integrity; *Foodchain*
- CNR - ICAR: Crypto for massively scalable systems
- Università Politecnica delle Marche: Applications
- Università di Roma La Sapienza - DI: Redactable blockchain (making the blockchain mutable in case of emergency situations); Security models for distributed futures market exchange

Post-quantum Crypto

- Politecnico di Milano: based on QC-LDPC codes
- Università dell'Aquila
- Università di Trento: based on isogenies of elliptic curves
- Università Politecnica delle Marche: based on linear codes

Coding theory

- Università di Milano: for optical systems
- Università della Basilicata, Padova, Napoli, Campania, Trento, Perugia, Torino, Bari
- Università Politecnica delle Marche: LDPC, QC-LDPC, SC-LDPC

Other mathematical topics related to crypto

- Group theory
  - Università dell'Aquila: Primitive permutation groups
  - Università di Salerno DM: Supersolvable groups; 2-Engels groups
- Galois and Algebraic Geometry
  - Università della Basilicata, Perugia, Napoli, Campania, Bari
- Permutation Polynomials
  - Università di Perugia e Torino

More specific topics

- Secret sharing
  - Basilicata, Perugia
- Zero knowledge proofs
  - Salerno DIEM, La Sapienza DI
- Multiparty computation
  - Salerno DIEM
- Quantum crypto
  - Padova DM-DEI
- Identity based cryptography
  - Politecnico di Milano, CNR ICAR
- Cryptography and machine learning
  - Roma Tre DMF