CryptoLabTN

02.02.2016

CryptoLabTN

The Mathematics Department of the University of Trento established in 2010 the

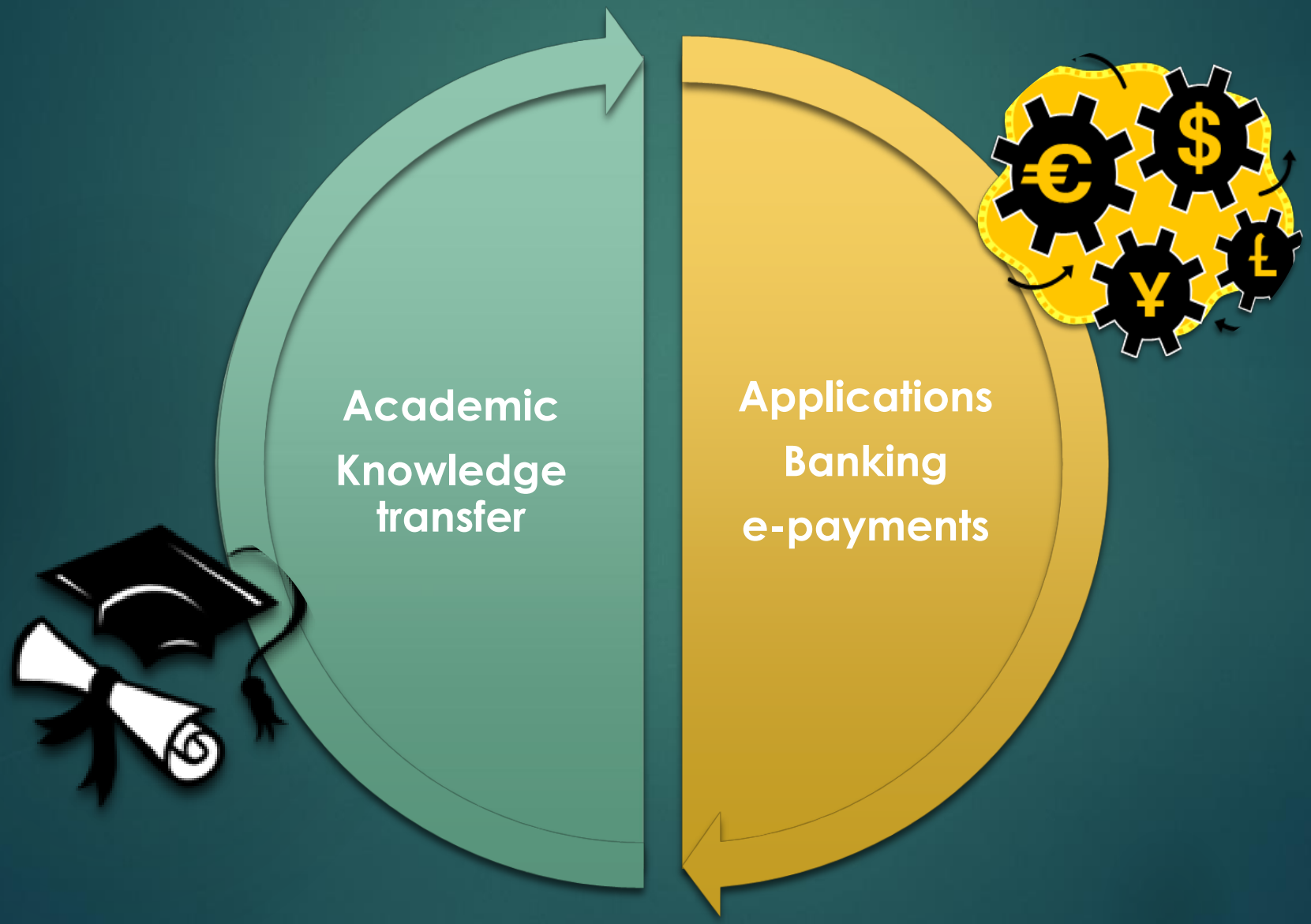
Laboratorio di Matematica Industriale e Crittografia

as key driver of innovation strengthened by the scientific expertise of the Department.

Members of CryptoLabTN

- Director: Prof. **Massimiliano Sala**
- Senior research fellow: **Giancarlo Rinaldo**
- 6 Post-docs: **Riccardo Aragona, Marco Calderini, Michela Ceria, Federico Pintore, Matteo Piva, Alessandro Tomasi**
- 6 PhD students: **Matteo Bonini, Roberto Civino, Riccardo Longo, Alessio Meneghetti, Giordano Santilli, Claudia Tinnirello**
- 25 Masters degree students
- Administrative staff: **Francesca Stanca**

CryptoLabTN Activities



CryptoLabTN Activities

- **Academic** research
- Scientific publications
- **Masters** Courses
- **International conferences**

  (MEGA 2015)
- **KNOWLEDGE TRANSFER**

Knowledge Transfer

IKS

paybay networks

Raiffeisen BANK

PHOENIX Informatica Bancaria

BANCA SELLA GRUPPO BANCA SELLA

SOCIETA' GESTIONE SERVIZI BP GRUPPO BANCO POPOLARE

Banking

Others

mediaservice.net CORPORATE SECURITY & IMAGE

GRUPPO ITAS ASSICURAZIONI

seeweb HIGH QUALITY HOSTING

Posteitaliane

Advisory board

- Strategic partnership
- Internships
- Scholarships for outstanding and motivated students

AliasLab

TELSY Crypto Devices

id Quantique

ARGENTEA IT FOR SERVICES

IKS

UniCredit Business Integrated Solutions

tasgroup

Raiffeisen Federazione Cooperative Raiffeisen Società cooperativa

Who welcomes our interns

International companies

National companies

Argentea, AliasLab, CWS, IKS, Paybay Networks, Raiffeisen BZ, SGS, Telsy, UBIS-Unicredit…

Selected events

- E-payment security. March 8, 2013
- Trust and Cloud Computing. May 10, 2013
- Randomness in cryptography and cryptanalysis. June 3, 2013
- 5th cryptography workshop BunnyTN. Dec 22, 2014
- Bitcoin and altcoins: applications and limitations. May 27, 2015
- Mathematical trapdoors in block ciphers. Sept 21-25, 2015

Online courses

Applied cryptography: a course for professionals. 2014

- From Shannon to modern cryptography
- Stream ciphers
- Block ciphers, hash functions, and their applications
- Public-key cryptography
- Other primitives

Applications of cryptography to security and privacy. 2015

- Certified email and e-voting
- e-payment systems
- Cryptocurrencies
- Biometric data protection
- Cryptography in smartphone security

CryptoLabTN Activities

- **Evaluation** of security
  (Risk and threat analysis)
- Comparison and design of
  ALGORITHMS
- Development of **PROTOTYPES**

Evaluations

Our experiences

- Authentication method, including mobile banking
- e-payments
- Security of interbank transactions
- Protection of patient records

Evaluations

Expert advice on systems proposed by vendors

Supervision on security of projects to develop in-house

Algorithms

Our experiences

- Encryption for:
  - online banking
  - mobile banking
  - cloud
- Generation of strong keys
- Crypto-currencies
- End-to-End encryption
- Biometrics for fraud detection

Development of prototypes

Developed prototypes

- Strong authentication for online banking
- Handwritten signature recognition
- Protection of biometric signatures

Ongoing projects

ARGENTEA IT FOR SERVICES

New mobile payment systems with loyalty cards, debit cards, and cryptocurrencies

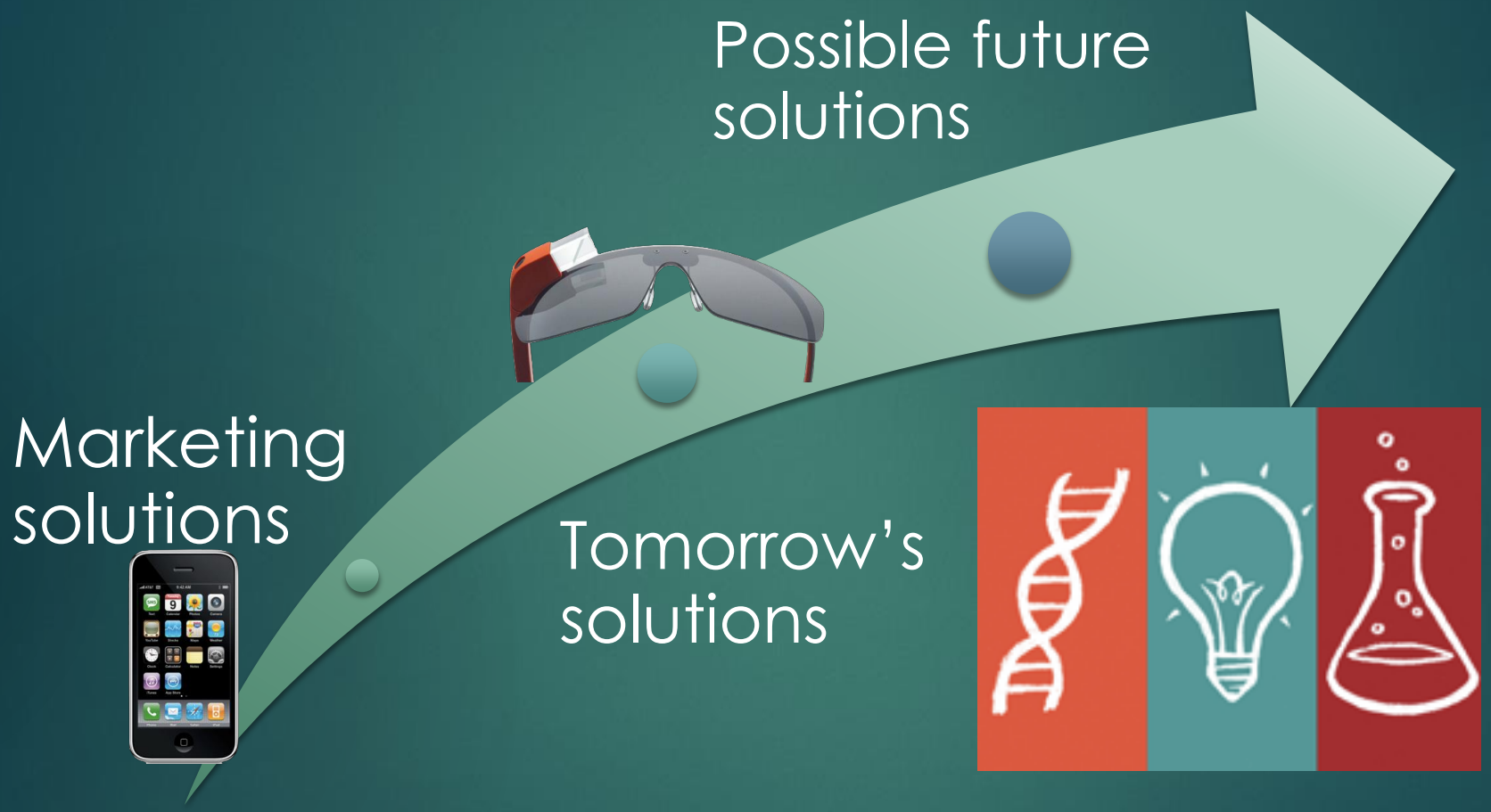
SIQURO

On silicon chip quantum optics for secure communications

Posteitaliane

End-to-End encryption: design of an E2E system to share encrypted documents with privileged users

Project view



Thanks for your attention!

HTTP://WWW.SCIENCE.UNITN.IT/~SALA/