



CrypTO

Crittografia e Teoria dei Numeri

CRITTOGRAFIA E SICUREZZA

Danilo Bazzanella

`danilo.bazzanella@polito.it`

Percorso in Crittografia e Sicurezza

Laurea Magistrale in Ingegneria Matematica



Politecnico
di Torino





Percorso di studi in **CRITTOGRAFIA E SICUREZZA**

- la Crittografia è fondamentale per garantire la **sicurezza dei dati**
- è alla base di alcune applicazioni dirompenti come la **blockchain**
- è essenziale per progettare **sistemi informatici sicuri e protocolli robusti**
- c'è **grande interesse delle aziende** verso la crittografia e la sicurezza

La carenza di esperti in Crittografia e Sicurezza rappresenta un grave problema sia per lo sviluppo economico di un paese sia per la sua sicurezza nazionale.

- **International Information System Security Certification Consortium:** prima che la pandemia aggravasse ulteriormente la situazione, sarebbero serviti circa 4 milioni di professionisti, a livello mondiale.
- **ENISA (ECSSO curriculum, 2021):** riporta l'enorme problema della carenza di esperti e la necessità di formazione universitaria
- **LinkedIn:** Blockchain, è stata negli scorsi anni l'hard skill più richiesta dalle aziende

PRIMO ANNO

- Calcolatori elettronici
- Reti di calcolatori
- Processi stocastici e Dinamiche su network
- Modelli Statistici
- Model Order Reduction and Machine Learning
- Machine Learning for Mathematical Engineering
- Sicurezza dei sistemi informativi
- Crittografia
- Blockchain e Criptoconomia

SECONDO ANNO

- Management and content delivery for Smart Networks
- AI and Cybersecurity
- Networks and cloud technologies security
- Advanced Cryptography
- Post-Quantum Cryptography
- Tesi

SECONDA LAUREA

Laureandosi in Ingegneria Matematica con il percorso di studi in “**Crittografia e Sicurezza**” è possibile ottenere una SECONDA LAUREA in **Cybersecurity** o in **Ingegneria Informatica** sostenendo solo 5 esami e la tesi:

- Offensive Security
- Threat Intelligence and Incident Management
- Data protection, Privacy and Anonymity
- Advanced Information systems security oppure Security verification and testing
- Cybersecurity laws and regulations oppure Technology and Innovation Management in Cybersecurity

Per qualsiasi informazione potete contattare il responsabile del nostro gruppo
Danilo Bazzanella (danilo.bazzanella@polito.it), visitare il nostro sito

http://crypto.polito.it/didattica/percorso_crittografia_e_sicurezza



Grazie per l'attenzione



Politecnico
di Torino



Telsy and Cryptography

Telsy



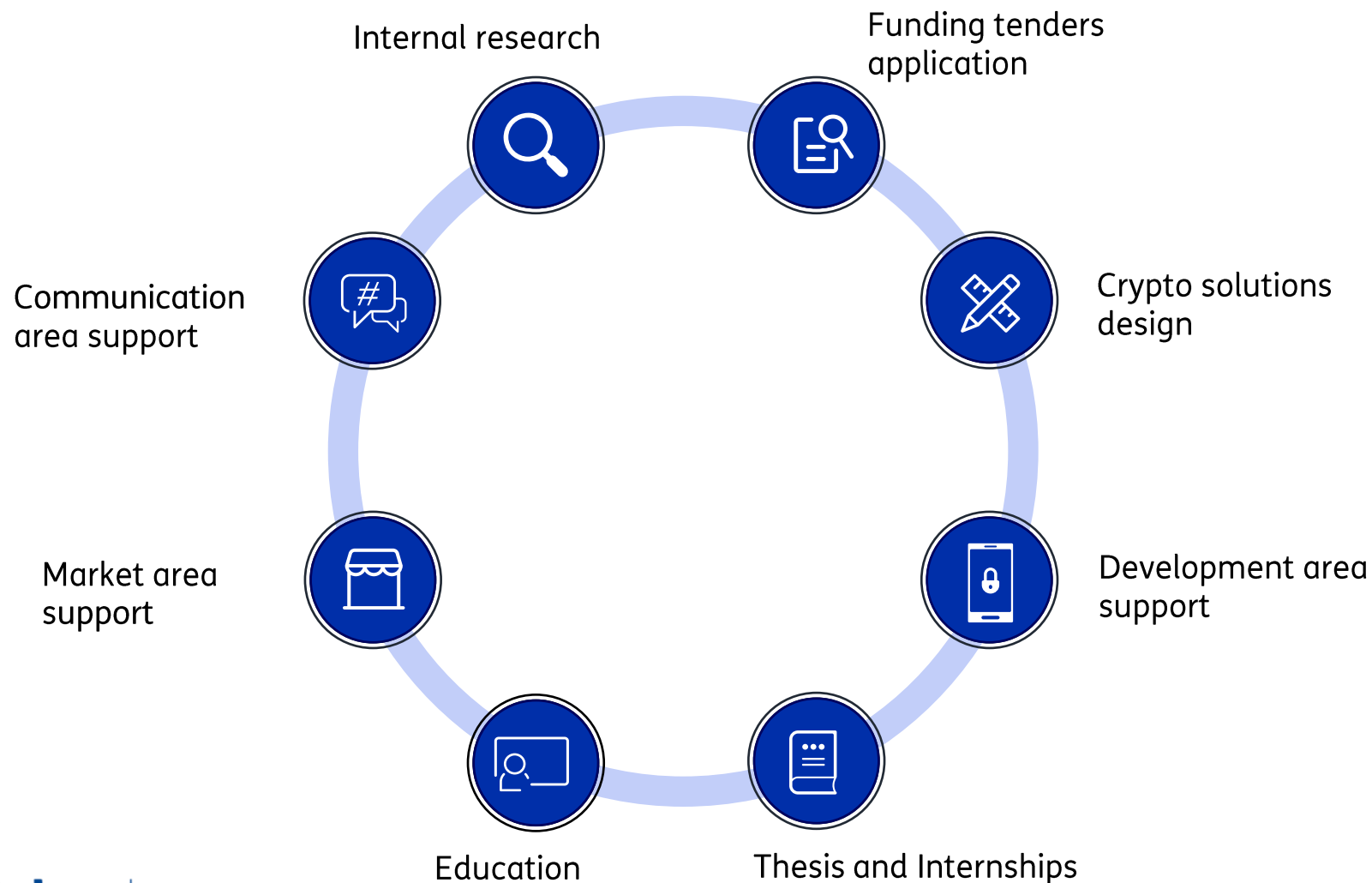
Telsy is the **TIM Group**'s competence center for the development of cryptographic and cybersecurity solutions, both in government and business scenarios, always ready to support Defense and Institutions.



Strongly active in research and participation in national and international projects, Telsy has started important strategic and technological partnerships with companies, startups, research institutes and academia.

Founded in 1971, today **Telsy** is 100% part of **TIM Group**.

Telsy Cryptography Research Group



PQC
Post Quantum
Cryptography

QKD
Quantum Key
Distribution

FHE
Fully Homomorphic
Encryption

Cryptographic
protocols

Random Number
Generators

Thank you



guglielmo.morgari@telsy.it



alessio.lovisetto@telsy.it



marco.rinaudo@telsy.it

Fondazione Links è un ente strumentale della



Fondazione
Compagnia
di San Paolo



Chi siamo ▾

Innovazione ▾

Ricerca ▾

Comunicazione ▾

Lavora con noi ▾

Contatti



PASSION FOR INNOVATION

Combiniamo tecnologia e competenza per garantire a tutti un futuro migliore.

SCOPRI DI PIÙ

■ SOCI FONDATORI •

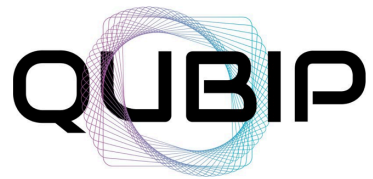


Fondazione
Compagnia
di San Paolo



Politecnico
di Torino

<https://linksfoundation.com>

[About](#) ▾[Transitions](#)[Consortium](#) ▾[Resources](#) ▾[Blogposts](#)[QSNS2024](#)[Contact](#)

Transition to Post-Quantum Cryptography



QUBIP project leads the integration of **Post-Quantum** algorithms into **protocols, networks and systems** we use today



<https://qubip.eu>