DISMA Dipartimento di Scienze Matematiche G. L. Lagrange

ECCELLENZA 2018 • 2022

Crittografia @Torino
Proposte didattiche e linee di ricerca

Danilo Bazzanella
danilo.bazzanella@polito.it

14 Ottobre 2019 - Politecnico di Torino

POLITECNICO DI TORINO

Crittografia @Torino : Proposte didattiche e linee di ricerca

Crittografia @Torino : Proposte didattiche e linee di ricerca

- In questi ultimi anni c'è stata una forte ripresa dell'attività didattica e di ricerca in ambito crittografico a Torino grazie a un nuovo gruppo di ricerca interateneo

Crittografia @Torino : Proposte didattiche e linee di ricerca

- In questi ultimi anni c'è stata una forte ripresa dell'attività didattica e di ricerca in ambito crittografico a Torino grazie a un nuovo gruppo di ricerca interateneo
- Sono stati attivati nuovi corsi, nelle Lauree Magistrali di Ingegneria del Politecnico e nel Dottorato di Ricerca interateneo in Matematica Pura e Applicata

Crittografia @Torino : Proposte didattiche e linee di ricerca

- In questi ultimi anni c'è stata una forte ripresa dell'attività didattica e di ricerca in ambito crittografico a Torino grazie a un nuovo gruppo di ricerca interateneo
- Sono stati attivati nuovi corsi, nelle Lauree Magistrali di Ingegneria del Politecnico e nel Dottorato di Ricerca interateneo in Matematica Pura e Applicata
- È ripresa una attività di ricerca teorica ed applicata in ambito crittografico, con il relativo sbocco nel trasferimento tecnologico

Attività didattica

Attività didattica

- Laurea Triennale

Attività didattica

- Laurea Triennale
  - sono attivi vari corsi di base propedeutici a una formazione in campo crittografico
  - Codici correttori e Crittografia (UniTo)
  - offerta di tesi triennali, sia a UniTo che a PoliTo

Attività didattica

- Laurea Triennale
  - sono attivi vari corsi di base propedeutici a una formazione in campo crittografico
  - Codici correttori e Crittografia (UniTo)
  - offerta di tesi triennali, sia a UniTo che a PoliTo
- Laurea Magistrale

Attività didattica

- Laurea Triennale
  - sono attivi vari corsi di base propedeutici a una formazione in campo crittografico
  - Codici correttori e Crittografia (UniTo)
  - offerta di tesi triennali, sia a UniTo che a PoliTo
- Laurea Magistrale
  - Crittografia (Ingegneria Matematica - PoliTo)
  - Cryptography (Orientamento Cybersecurity - Ingegneria Informatica - PoliTo)
  - offerta di tesi magistrali, sia a UniTo che a PoliTo

Attività didattica

- Laurea Triennale
  - sono attivi vari corsi di base propedeutici a una formazione in campo crittografico
  - Codici correttori e Crittografia (UniTo)
  - offerta di tesi triennali, sia a UniTo che a PoliTo
- Laurea Magistrale
  - Crittografia (Ingegneria Matematica - PoliTo)
  - Cryptography (Orientamento Cybersecurity - Ingegneria Informatica - PoliTo)
  - offerta di tesi magistrali, sia a UniTo che a PoliTo
- Dottorato di ricerca (Interateneo - Matematica Pura e Applicata)

Attività didattica

- Laurea Triennale
  - sono attivi vari corsi di base propedeutici a una formazione in campo crittografico
  - Codici correttori e Crittografia (UniTo)
  - offerta di tesi triennali, sia a UniTo che a PoliTo
- Laurea Magistrale
  - Crittografia (Ingegneria Matematica - PoliTo)
  - Cryptography (Orientamento Cybersecurity - Ingegneria Informatica - PoliTo)
  - offerta di tesi magistrali, sia a UniTo che a PoliTo
- Dottorato di ricerca (Interateneo - Matematica Pura e Applicata)
  - Introduzione alla Crittografia
  - Aspetti algebrici della crittografia
  - Blockchain e criptoeconomia
  - nel gruppo interateneo ci sono attualmente 4 dottorandi

Attività di ricerca e di trasferimento tecnologico

Attività di ricerca e di trasferimento tecnologico

- Number Theory and cryptographic applications

Attività di ricerca e di trasferimento tecnologico

- Number Theory and cryptographic applications
  - Analytic and algebraic number theory
  - Linear recurrences and continued fractions
  - Elliptic curves and conics cryptosystem and primality testing

Attività di ricerca e di trasferimento tecnologico

- Number Theory and cryptographic applications
  - Analytic and algebraic number theory
  - Linear recurrences and continued fractions
  - Elliptic curves and conics cryptosystem and primality testing
- Post-quantum cryptography

Attività di ricerca e di trasferimento tecnologico

- Number Theory and cryptographic applications
  - Analytic and algebraic number theory
  - Linear recurrences and continued fractions
  - Elliptic curves and conics cryptosystem and primality testing
- Post-quantum cryptography
  - Code-based and lattice-based
  - Multivariate-based, Hash-based, Isogeny-based, ZKP-based...

Attività di ricerca e di trasferimento tecnologico

- Number Theory and cryptographic applications
  - Analytic and algebraic number theory
  - Linear recurrences and continued fractions
  - Elliptic curves and conics cryptosystem and primality testing
- Post-quantum cryptography
  - Code-based and lattice-based
  - Multivariate-based, Hash-based, Isogeny-based, ZKP-based...
- Cryptanalysis of ARX (Addition/Rotation/XOR) ciphers

Attività di ricerca e di trasferimento tecnologico

- Number Theory and cryptographic applications
  - Analytic and algebraic number theory
  - Linear recurrences and continued fractions
  - Elliptic curves and conics cryptosystem and primality testing
- Post-quantum cryptography
  - Code-based and lattice-based
  - Multivariate-based, Hash-based, Isogeny-based, ZKP-based...
- Cryptanalysis of ARX (Addition/Rotation/XOR) ciphers
  - ChaCha and Blake
  - NIST candidates

Attività di ricerca e di trasferimento tecnologico

- Number Theory and cryptographic applications
  - Analytic and algebraic number theory
  - Linear recurrences and continued fractions
  - Elliptic curves and conics cryptosystem and primality testing
- Post-quantum cryptography
  - Code-based and lattice-based
  - Multivariate-based, Hash-based, Isogeny-based, ZKP-based...
- Cryptanalysis of ARX (Addition/Rotation/XOR) ciphers
  - ChaCha and Blake
  - NIST candidates
- Blockchain technology applications

Attività di ricerca e di trasferimento tecnologico

- Number Theory and cryptographic applications
  - Analytic and algebraic number theory
  - Linear recurrences and continued fractions
  - Elliptic curves and conics cryptosystem and primality testing
- Post-quantum cryptography
  - Code-based and lattice-based
  - Multivariate-based, Hash-based, Isogeny-based, ZKP-based...
- Cryptanalysis of ARX (Addition/Rotation/XOR) ciphers
  - ChaCha and Blake
  - NIST candidates
- Blockchain technology applications
  - Supply chain (gestione della catena di distribuzione e tracciabilità dei prodotti)
  - Sostenibilità e risparmio energetico
  - Stable coin

Thank you for the attention

POLITECNICO
DI TORINO