Dipartimento di Matematica – UniTN

CryptoLabTN

Presentazione ricerca e attività

Daniele Taufer
cryptolabmat@unitn.it

22 gennaio 2018

CryptoLabTN
Cosa facciamo

Il laboratorio di matematica industriale e crittografia, fondato nel 2010 dal professor Massimiliano Sala all'interno del dipartimento di matematica, si occupa di:

- Ricerca scientifica in crittografia e codici.
- Curriculum *Cryptography* della laurea magistrale in matematica.
- Progetti finanziati da aziende.
- Divulgazione e corsi per professionisti.

CryptoLabTN
Membri

Direttore:	Prof. Massimiliano Sala
Ricercatori:	Dr. Giancarlo Rinaldo
4 Post-Doc:	Dr. Riccardo Aragona Dr. Michela Ceria Dr. Alessio Meneghetti Dr. Federico Pintore
7 Dottorandi:	Matteo Bonini Roberto Civino Riccardo Longo Carla Mascia Augustine Musukwa Giordano Santilli Daniele Taufer
Studenti:	23 studenti di Master
Personale amministrativo:	Francesca Stanca

Ricerca: Funzioni Booleane

Studio delle proprietà crittografiche di funzioni booleane.

- Dimostrazione teorica della non-esistenza di permutazioni APN in dimensione 4.
- Dimostrazione teorica della non-esistenza di permutazioni cubiche APN in dimensione 6.
- Proprietà di S-box con bassa *weak differential uniformity*.
- Studio della *differential uniformity* rispetto ad operazioni alternative.

Ricerca: Block Ciphers

Studio delle proprietà gruppali di un cifrario a blocchi.

- Gruppo generato dalle funzioni di round di cifrari di tipo:
  - *AES*,
  - *Lightweight*,
  - *GOST*.
- Cifrari *Wave*.
- Studio di *trapdoors* algebriche.
- Crittanalisi differenziale rispetto a operazioni alternative.

Ricerca: ECC e ECDLP

Crittografia su curve ellittiche e problema del logaritmo discreto

Studio di proprietà crittografiche di curve ellittiche e relativo problema del logaritmo discreto.

- Applicazione di *Index Calculus* per curve ellittiche su campi primi sfruttando i *Summation Polynomials*.
- Risoluzione efficiente di sistemi di equazioni polinomiali applicate al *Index Calculus*.

Ricerca: *Attribute Based Encryption*

Ideazione e progettazione di schemi ABE.

- Accesso pubblico di dati cifrati su cloud.
- Ideazione e dimostrazione di sicurezza di schemi RS-ABE.
- Ideazione e dimostrazione di sicurezza di uno schema ABE con più autorità.

Ricerca: Codici

Ciclici, non-lineari, algebra computazionale

Studio della teoria dei codici e relative applicazioni.

- Classificazione codici binari ottimali.
- Estrattori di entropia.
- Applicazione dei quasi-polinomi di Hilbert agli *Order Domain Codes*.
- Sparsità del Polinomio Locatore.
- Riconoscimento sindromi non correggibili tramite *Error Detector Polynomial*.
- Intersezioni tra curve algebriche e applicazioni alla distribuzione dei pesi di codici AG.

Ricerca: Algebra
Risultati di algebra generale

Ricerca in vari campi dell'algebra.

- Criteri per definire una divisione involutiva a partire da monomi con grado e numero di variabili dati.
- Basi di Gröbner su algebre di Ore.
- Invarianti algebrici di sottoclassi di *Binomial Edge Ideals*.
- Analisi di proprietà degli interi per attaccare crittosistemi a chiave pubblica.
- Decomposizione di tensori simmetrici.

Percorso di studi selettivo (~15 iscritti all'anno) focalizzato sulla applicazione dell'algebra alla teoria dei codici e alla crittografia.

Due possibili orientamenti:

- *Stage oriented*
- *Research oriented*

Dottorato

Studio avanzato dell'algebra applicata ai campi di teoria dei codici e crittografia con l'obiettivo di produrre risultati originali in questi campi.

Progetti con aziende: analisi di sicurezza

- Creazione di un modello per attaccare chiavi RSA impiegate da una *Certification Authority* per certificare determinate transazioni.
- Valutazioni di sicurezza.

Progetti con aziende: algoritmi

- Progettazione di un sistema *End-to-End* per lo scambio di documenti confidenziali.
- Progettazione di un algoritmo di tokenizzazione e relativa dimostrazione di sicurezza.

Progetti con aziende: *Blockchain*

- Nuovi sistemi di pagamento tramite fidelity card e crittovalute.
- Applicazione della tecnologia Blockchain alla verifica dell'integrità dei dati.
- *Foodchain*: applicazione della tecnologia Blockchain alla filiare alimentare.

Corsi per professionisti ad aziende

Corsi offerti negli ultimi anni

- *Bitcoin, Blockchain and their new frontiers*.
- *Monero: the dark side of cryptocurrencies*.
- *Post-Quantum Cryptography*.
- *Advanced analysis of block chipers*.
- *Cryptographic aspects of cloud and distributed computing*.
- *Cryptography for telephone transmissions: video calling*.

Corso online per professionisti

BoAB: *Bitcoin and other applications of Blockchain*.

Divulgazione

- BunnyTN.
- Gare crittografiche:
  - Digital Signature Awareness Contest.
  - ECC Awareness Contest.
  - RSA Contest.
  - Cryptowars.
  - The dark side of cryptography.

Grazie per l'attenzione!

CryptoLabTN