

Università degli Studi di Trento  
Facoltà di Scienze Matematiche Fisiche e Naturali  
Dipartimento di Matematica

# Laboratorio di Matematica Industriale e Crittografia

11 agosto 2011

## 1 Chi siamo

- Come nasce il Lab
- Dove ci collochiamo
- Obiettivi
- I membri del Lab
- Collaboratori

## 2 Che cosa facciamo

- Le nostre competenze
- Strumenti informatici
- Punti di forza del gruppo

## 3 Attività recenti o in corso

- Attività con aziende
- Corsi per professionisti
- Potenziali Partner

## 1 Chi siamo

- Come nasce il Lab
- Dove ci collochiamo
- Obiettivi
- I membri del Lab
- Collaboratori

## 2 Che cosa facciamo

- Le nostre competenze
- Strumenti informatici
- Punti di forza del gruppo

## 3 Attività recenti o in corso

- Attività con aziende
- Corsi per professionisti
- Potenziali Partner

Nel 2010 il Laboratorio nasce da una concomitanza di eventi:

- 1 la *crescente* collaborazione del Prof. Sala con il mondo delle aziende e dell'industria;
- 2 la *nascente* collaborazione tra il Prof. Sala (teoria dei codici e crittografia) ed il Prof. Bertolazzi (ottimizzazione numerica);
- 3 la *presenza* di un gruppo di giovani matematici interessati ad affinare/sviluppare tecniche matematiche per applicazioni.

Il Laboratorio raccoglie un *insieme di esperienze e competenze*, anche molto diverse tra loro, per affrontare un'ampia gamma di problemi.

Nel 2010 il Laboratorio nasce da una concomitanza di eventi:

- 1 la *crescente* collaborazione del Prof. Sala con il mondo delle aziende e dell'industria;
- 2 la *nascente* collaborazione tra il Prof. Sala (teoria dei codici e crittografia) ed il Prof. Bertolazzi (ottimizzazione numerica);
- 3 la *presenza* di un gruppo di giovani matematici interessati ad affinare/sviluppare tecniche matematiche per applicazioni.

Il Laboratorio raccoglie un *insieme di esperienze e competenze*, anche molto diverse tra loro, per affrontare un'ampia gamma di problemi.

Nel 2010 il Laboratorio nasce da una concomitanza di eventi:

- 1 la *crescente* collaborazione del Prof. Sala con il mondo delle aziende e dell'industria;
- 2 la *nascente* collaborazione tra il Prof. Sala (teoria dei codici e crittografia) ed il Prof. Bertolazzi (ottimizzazione numerica);
- 3 la *presenza* di un gruppo di giovani matematici interessati ad affinare/sviluppare tecniche matematiche per applicazioni.

Il Laboratorio raccoglie un *insieme di esperienze e competenze*, anche molto diverse tra loro, per affrontare un'ampia gamma di problemi.

Nel 2010 il Laboratorio nasce da una concomitanza di eventi:

- 1 la *crescente* collaborazione del Prof. Sala con il mondo delle aziende e dell'industria;
- 2 la *nascente* collaborazione tra il Prof. Sala (teoria dei codici e crittografia) ed il Prof. Bertolazzi (ottimizzazione numerica);
- 3 la *presenza* di un gruppo di giovani matematici interessati ad affinare/sviluppare tecniche matematiche per applicazioni.

Il Laboratorio raccoglie un *insieme di esperienze e competenze*, anche molto diverse tra loro, per affrontare un'ampia gamma di problemi.

- Ci troviamo presso il *Dipartimento di Matematica* dell'Università di Trento.
- Nasciamo dal gruppo di *Algebra* del Dipartimento di Matematica.
- Stiamo collaborando con il *Laboratorio di Meccatronica* del Dipartimento di Ingegneria Meccanica e Strutturale.

- Ci troviamo presso il *Dipartimento di Matematica* dell'Università di Trento.
- Nasciamo dal gruppo di *Algebra* del Dipartimento di Matematica.
- Stiamo collaborando con il *Laboratorio di Meccatronica* del Dipartimento di Ingegneria Meccanica e Strutturale.

- Ci troviamo presso il *Dipartimento di Matematica* dell'Università di Trento.
- Nasciamo dal gruppo di *Algebra* del Dipartimento di Matematica.
- Stiamo collaborando con il *Laboratorio di Meccatronica* del Dipartimento di Ingegneria Meccanica e Strutturale.

Vorremmo interfacciarci con aziende che necessitano di competenze di matematica di livello medio alto,

- sia sfruttando le nostre esperienze pregresse,
- sia adattandoci alle necessità aziendali.

|                    |                         |
|--------------------|-------------------------|
| Massimiliano Sala  | Professore              |
| Chiara Marcolla    | Dottoranda              |
| Emanuele Bellini   | Dottorando              |
| Matteo Piva        | Dottorando              |
| Marco Frego        | Dottorando              |
| Daniele Giovannini | Laurea II livello       |
| Valentina Pulice   | Laureanda di II livello |
| Stefano Martin     | Laureando di II livello |
| .....              | Laureandi di I livello  |
| Francesca Stanca   | Project Management      |

Tra i nostri collaboratori accademici ricordiamo

- prof. Bertolazzi (Dip. Ing.)  
Ottimizzazione numerica e controllo ottimo.
- prof. Caranti (Dip. Mat.)  
Campi finiti, teoria dei gruppi e crittografia.
- prof. De Graaf (Dip. Mat.)  
Algebra computazionale e crittografia.
- prof. Fontanari (Dip. Mat.)  
Multimedia Geometry.

Tra i nostri collaboratori accademici ricordiamo

- prof. Bertolazzi (Dip. Ing.)  
Ottimizzazione numerica e controllo ottimo.
- prof. Caranti (Dip. Mat.)  
Campi finiti, teoria dei gruppi e crittografia.
- prof. De Graaf (Dip. Mat.)  
Algebra computazionale e crittografia.
- prof. ... (Dip. Mat.)  
Multimedia Geometry.

Tra i nostri collaboratori accademici ricordiamo

- prof. Bertolazzi (Dip. Ing.)  
Ottimizzazione numerica e controllo ottimo.
- prof. Caranti (Dip. Mat.)  
Campi finiti, teoria dei gruppi e crittografia.
- prof. De Graaf (Dip. Mat.)  
Algebra computazionale e crittografia.
- prof. Fontanari (Dip. Mat.)  
Multimedia Geometry.

Tra i nostri collaboratori accademici ricordiamo

- prof. Bertolazzi (Dip. Ing.)  
Ottimizzazione numerica e controllo ottimo.
- prof. Caranti (Dip. Mat.)  
Campi finiti, teoria dei gruppi e crittografia.
- prof. De Graaf (Dip. Mat.)  
Algebra computazionale e crittografia.
- prof. Fontanari (Dip. Mat.)  
Multimedia Geometry.

- 1 Chi siamo
  - Come nasce il Lab
  - Dove ci collochiamo
  - Obiettivi
  - I membri del Lab
  - Collaboratori
- 2 Che cosa facciamo
  - Le nostre competenze
  - Strumenti informatici
  - Punti di forza del gruppo
- 3 Attività recenti o in corso
  - Attività con aziende
  - Corsi per professionisti
  - Potenziali Partner

- Teoria dei codici.
- Crittografia.
- Algebra computazionale.
- Biomatematica.
- Ottimizzazione numerica e controllo ottimo.
- Visione artificiale e 3D.
- Multimedia geometry.

- Sistemi operativi: Linux, Windows, MacOS.
- Manipolazione simbolica: Magma, Maple, Mathematica, Singular, Gap, Cocoa.
- Procedurali: Matlab, C, Fortran.
- Object oriented: C++, VB.

- *Forma mentis* incentrata sulla capacità di astrazione e sulla logica.
- Competenze diverse, ma con ampie zone di *sovrapposizione*.
- Attitudine a *sporcarsi le mani*: non solo dimostrazioni teoriche, ma anche implementazioni efficienti.

- *Forma mentis* incentrata sulla capacità di astrazione e sulla logica.
- Competenze diverse, ma con ampie zone di *sovrapposizione*.
- Attitudine a *sporcarsi le mani*: non solo dimostrazioni teoriche, ma anche implementazioni efficienti.

- *Forma mentis* incentrata sulla capacità di astrazione e sulla logica.
- Competenze diverse, ma con ampie zone di *sovrapposizione*.
- Attitudine a *sporcarsi le mani*: non solo dimostrazioni teoriche, ma anche implementazioni efficienti.

- 1 Chi siamo
  - Come nasce il Lab
  - Dove ci collochiamo
  - Obiettivi
  - I membri del Lab
  - Collaboratori
- 2 Che cosa facciamo
  - Le nostre competenze
  - Strumenti informatici
  - Punti di forza del gruppo
- 3 Attività recenti o in corso
  - Attività con aziende
  - Corsi per professionisti
  - Potenziali Partner

- *Azienda di moneta elettronica.* Validazione crittografica per un sistema proprietario di pagamento online (Moneta Elettronica).
- *IDT (Integrated Device Technology Silicon Valley).* Valutazione performance di codici (a correzione d'errore) nelle memorie Flash per Hard Disk di nuova generazione.
- *Ansaldo.* Studio della codifica migliore per la comunicazione (*commutazione*) tra treni e dispositivi di segnalamento (*balise*) posti lungo i binari.

- *Azienda di moneta elettronica.* Validazione crittografica per un sistema proprietario di pagamento online (Moneta Elettronica).
- *IDT (Integrated Device Technology Silicon Valley).* Valutazione performance di codici (a correzione d'errore) nelle memorie Flash per Hard Disk di nuova generazione.
- *Ansaldo.* Studio della codifica migliore per la comunicazione (*commutazione*) tra treni e dispositivi di segnalamento (*balise*) posti lungo i binari.

- *Azienda di moneta elettronica*. Validazione crittografica per un sistema proprietario di pagamento online (Moneta Elettronica).
- *IDT (Integrated Device Technology Silicon Valley)*. Valutazione performance di codici (a correzione d'errore) nelle memorie Flash per Hard Disk di nuova generazione.
- *Ansaldo*. Studio della codifica migliore per la comunicazione (*commutazione*) tra treni e dispositivi di segnalamento (*balise*) posti lungo i binari.

- *Piaggio*. Ottimizzazione della linea di produzione dei motori e ottimizzazione del magazzino.
- *Tecnigold*. Sviluppo di tool per la visione artificiale applicati all'industria orafa per il controllo della qualità.
- *TELSY Elettronica e Telecomunicazioni*. Studio di cifrari per trasmissioni riservate.
- *Heads Italia*. Studio di cifrari per trasmissioni riservate.

- *Piaggio*. Ottimizzazione della linea di produzione dei motori e ottimizzazione del magazzino.
- *Tecnigold*. Sviluppo di tool per la visione artificiale applicati all'industria orafa per il controllo della qualità.
- *TELSY Elettronica e Telecomunicazioni*. Studio di cifrari per trasmissioni riservate.
- *Heads Italia*. Studio di cifrari per trasmissioni riservate.

- *Piaggio*. Ottimizzazione della linea di produzione dei motori e ottimizzazione del magazzino.
- *Tecnigold*. Sviluppo di tool per la visione artificiale applicati all'industria orafa per il controllo della qualità.
- *TELSY Elettronica e Telecomunicazioni*. Studio di cifrari per trasmissioni riservate.
- *Heads Italia*. Studio di cifrari per trasmissioni riservate.

- *Piaggio*. Ottimizzazione della linea di produzione dei motori e ottimizzazione del magazzino.
- *Tecnigold*. Sviluppo di tool per la visione artificiale applicati all'industria orafa per il controllo della qualità.
- *TELSY Elettronica e Telecomunicazioni*. Studio di cifrari per trasmissioni riservate.
- *Heads Italia*. Studio di cifrari per trasmissioni riservate.

- *Corsi avanzati sulla sicurezza dei cifrari*, in collaborazione con la **Presidenza del Consiglio dei Ministri** e il **Ministero della Difesa**.
- *La crittografia nei telefonini anti intercettazione*, in collaborazione con **Telsy** e **PrivateWave**.
- *Pagamenti elettronici e online banking*, in collaborazione con **Alpha Orionis** e società di sicurezza informatica bancaria.
- *Protezione dati e crittografia nel Cloud Computing*, in collaborazione con **Alba St**, **Microsoft Italia** e **SeeWeb**.

- *Corsi avanzati sulla sicurezza dei cifrari*, in collaborazione con la **Presidenza del Consiglio dei Ministri** e il **Ministero della Difesa**.
- *La crittografia nei telefonini anti intercettazione*, in collaborazione con **Telsy** e **PrivateWave**.
- *Pagamenti elettronici e online banking*, in collaborazione con **Alpha Orionis** e società di sicurezza informatica bancaria.
- *Protezione dati e crittografia nel Cloud Computing*, in collaborazione con **Alba St**, **Microsoft Italia** e **SeeWeb**.

- *Corsi avanzati sulla sicurezza dei cifrari*, in collaborazione con la **Presidenza del Consiglio dei Ministri** e il **Ministero della Difesa**.
- *La crittografia nei telefonini anti intercettazione*, in collaborazione con **Telsy** e **PrivateWave**.
- *Pagamenti elettronici e online banking*, in collaborazione con **Alpha Orionis** e società di sicurezza informatica bancaria.
- *Protezione dati e crittografia nel Cloud Computing*, in collaborazione con **Alba St**, **Microsoft Italia** e **SeeWeb**.

- *Corsi avanzati sulla sicurezza dei cifrari*, in collaborazione con la **Presidenza del Consiglio dei Ministri** e il **Ministero della Difesa**.
- *La crittografia nei telefonini anti intercettazione*, in collaborazione con **Telsy** e **PrivateWave**.
- *Pagamenti elettronici e online banking*, in collaborazione con **Alpha Orionis** e società di sicurezza informatica bancaria.
- *Protezione dati e crittografia nel Cloud Computing*, in collaborazione con **Alba St**, **Microsoft Italia** e **SeeWeb**.

- *Corsi avanzati sulla sicurezza dei cifrari*, in collaborazione con la **Presidenza del Consiglio dei Ministri** e il **Ministero della Difesa**.
- *La crittografia nei telefonini anti intercettazione*, in collaborazione con **Telsy** e **PrivateWave**.
- *Pagamenti elettronici e online banking*, in collaborazione con **Alpha Orionis** e società di sicurezza informatica bancaria.
- *Protezione dati e crittografia nel Cloud Computing*, in collaborazione con **Alba St**, **Microsoft Italia** e **SeeWeb**.

- *MediaService.net*. Nota società di sicurezza informatica con servizi di sicurezza proattiva.
- *Gruppo MPBA della Fondazione Bruno Kessler*. metodi predittivi e integrazione in sistemi per l'apprendimento automatico algebrico/statistico.

- *MediaService.net*. Nota società di sicurezza informatica con servizi di sicurezza proattiva.
- *Gruppo MPBA della Fondazione Bruno Kessler*. metodi predittivi e integrazione in sistemi per l'apprendimento automatico algebrico/statistico.