GIOVANNI TOGNOLINI

giovannitognolini@gmail.com
(+39) 3343164118

PROFILO PERSONALE

Data di Nascita 11 Agosto 1996
Indirizzo Via Molino 42, Castegnato (BS), 25045, Italia

EDUCAZIONE

PhD in Applied Cryptography *Novembre 2021 - In corso*
Facoltà di Scienze Matematiche, Università degli Studi Di Trento

Master in Matematica *Settembre 2018 - Marzo 2021*
Percorso Cryptography
Facoltà di Scienze Matematiche, Università degli Studi Di Trento
Titolo tesi: *"Post-Quantum Cryptography: Towards Commutative Supersingular Isogeny Key Exchange"*
Votazione: 110/110 e Lode

Laurea Triennale in Matematica *Settembre 2015 - Luglio 2018*
Facoltà di Scienze Matematiche, Università degli Studi Di Trento
Titolo tesi: *"Corrispondenza di Galois per estensioni di grado infinito"*

Diploma di Liceo Scientifico *Settembre 2010 - Giugno 2015*
Liceo Scientifico Leonardo, Brescia

PRINCIPALI ESAMI SOSTENUTI, LAUREA MAGISTRALE

Algebraic Cryptography, Coding Theory and Applications, Computability and Computational Complexity, Computational Algebra, Formal Methods, Formal Techniques for Cryptographic Protocol Analysis, Introduction To Computer and Network Security, Scientific Computing, Advanced Programming Of Cryptographic Methods, Stochastic Processes, Digital Signal Processing, Data Hiding.

PRINCIPALI ESAMI SOSTENUTI, LAUREA TRIENNALE

Informatica, Calcolo delle Probabilità e Statistica, Programmazione 2, Teoria dei Gruppi, Teoria di Galois, Statistica Matematica, Algebra Commutativa, Teoria Algebrica dei Numeri, Algoritmi e Strutture Dati.

CONFERENZE, CONVEGNI E SCUOLE FREQUENTATE

Eurocrypt23 *23-27 Aprile 2023*
Lyon, Francia

CBCrypto23 *22-23 Aprile 2023*
Lyon, Francia

PQCifris2022 *10-14 Ottobre 2022*
Trento, Italia

Summer School in Post-Quantum Cryptography *1-5 Agosto 2022*
Budapest, Ungheria

PROGETTI

Optimized Implementation of MAYO *Spring 2023*
Riadattamento di un codice preesistente con il fine di renderlo compatibile con il framework pqm4 e testabile con qemu.

Hive Ransomware Analysis *Febbraio 2022*
Analisi condotta per e con Treos S.C. (Trento). Il progetto si inserisce all'interno di una consulenza aziendale per il ripristino di dati cifrati da un ransomware di tipo Hive su svariati server. Sfruttando una debolezza dell'implementazione del ransomware siamo riusciti ad effettuare un attacco di tipo known-plaintext, ricostruire buona parte della master key usata per cifrare e abbiamo così ricostruito la maggior parte dei dati cifrati.

Front End Developer *Gennaio 2021 - In corso*
Creazione e manutenzione del sito web dell'iniziativa nazionale De Componendis Cifris.

Security Analysis of a Specific Bitcoin Address *Inverno 2021*
Analisi condotta per il Prof. Massimiliano Sala, Trento

Secure Communication With A Remote Database *Autunno 2020*
Il progetto è svolto in un team di due persone ed è finalizzato all'implementazione di una comunicazione cifrata ad un server remoto. Lo scambio di chiavi pubbliche è gestito da RSA; il resto della comunicazione è invece gestito da AES-128. L'interfaccia è implementata con JavaFX, mentre il layer di comunicazione è simulato con i Java Socket.

Forensics Analysis *Autunno 2019*
Con questo progetto è stato realizzato un algoritmo in Matlab che realizzi la detection passiva di eventuali manomissioni a danno di un'immagine.

Image Watermarking Embedding and Attacks *Autunno 2019*
Con questo progetto è stato realizzato un algoritmo in Matlab che, dato un watermark e un'immagine, incorpori il primo all'interno della seconda. In aggiunta, è stato implementato un programma per attaccare una data immagine, con il fine di manomettere il watermark e preservare la qualità della stessa.

Elliptic Curves on Finite Fields: Schoof's Algorithm *Primavera 2019*
Con questo progetto è stato sviluppato un programma in Magma che implementi l'algoritmo di Schoof, il quale conta il numero di punti di una curva ellittica difinita su un campo finito. A seguito dell'implementazione è stato steso un report individuale. Particolare enfasi è data alle scelte implementative, ai paragoni con altri algoritmi noti e alle varianti dell'algoritmo stesso.

Symmetric Key Cryptography Using TwoFish *Inverno 2018*
Con questo progetto è stato realizzato un programma in Magma che implementi il cifrario a chiave simmetrica TwoFish. Nel report individuale, steso successivamente, vengono elencati i principi cardine su cui è stata ideata l'implementazione, che viene quindi discussa in dettaglio.

ELENCO DELLE PUBBLICAZIONI

- Longo, Riccardo, et al. "Adaptable Cryptographic Primitives in Blockchains via Smart Contracts." Cryptography 6.3 (2022): 32.
- Meneghetti, Alessio, et al. "A Post-Quantum Digital Signature Scheme from QC-LDPC Codes". https://eprint.iacr.org/2022/1477.pdf

TALK E SEMINARI TENUTI

Information Leackage and Code-Based Cryptography *Primavera 2023*
Università di Trento, Trento
In questo talk ho descritto lo stato dell'arte della crittografia code-based nel contesto delle firme digitali, ponendo enfasi alle varie problematiche legate al paradigma Hash&Sign.

Towards a Post Quantum OTS Scheme using QC-LDPC Codes *1 Dicembre 2022*
Università Politecnica delle Marche, Ancona
Studio della sicurezza del protocollo presentato nel seminario del 14 Ottobre.

A Digital Signature Scheme from QC-LDPC Codes *14 Ottobre 2022*
PQCifris2022, Trento
In questo talk ho presentato un lavoro a cui mi sono dedicato con il mio gruppo di ricerca a Trento. Abbiamo costruito uno schema di firma post quantum basato su reticoli, che sfrutta i codici quasi ciclici per ottenere chiavi compatte, e i codici LDPC per avere buone performance di esecuzione.

A Cryptographic Kernel for Post-Quantum Support in Blockchains *12 Ottobre 2022*
PQCifris2022, Trento
In questo talk ho presentato un paper che abbiamo pubblicato nel 2022 riguardo la gestione delle primitive crittografiche nelle blockchain che permettono l'uso di smart contracts.

The Bombieri-Vinogradov Theorem *21 Luglio 2022*
Università di Trento, Trento
Descrizione del teorema di Bombieri-Vinogradov, un risultato riguardo il termine di errore nel teorema dei numeri primi in progressione aritmetica.

Latest Developments in Rainbow Cryptanalysis *17 Maggio 2022*
Università di Trento, Trento
Descrizione dello stato dell'arte della crittoanalisi di Rainbow, con particolare riferimento ai lavori di Beullens pubblicati nel 2022.

An Improvement on Ajtai-GGH Hash Function *14 Aprile 2022*
Università di Trento, Trento
Descrizione una famiglia di funzioni hash proposte a inizi 2000, basate su reticoli, che generalizzano e migliorano le funzioni hash di Ajtai-GGH.

Buone e Cattive Implementazioni di Algoritmi Crittografici *27 Gennaio 2022*
Digital Innovation Hub, Vicenza
Il talk fornisce un'introduzione alle tre principali famiglie di algoritmi crittografici, ovvero i protocolli a chiave pubblica, a chiave privata e di firma digitale. Per ognuno di questi ho discusso il delicato equilibrio che ne regola il funzionamento, mostrando esempi di implementazioni ben fatte e implementazioni che invece minano la sicurezza dei protocolli stessi.

COMPETENZE PERSONALI

Competenze Digitali

- Buona padronanza dei sistemi operativi Windows e GNU/Linux.
- Linguaggi di programmazione noti: Java, Javascript, TypeScript, C, Magma, Matlab, R, Python.
- Linguaggi specifici per il model checking: Promela-Spin, SMV-nuXmv.
- Linguaggi specifici per lo sviluppo web: HTML, CSS.

Competenze Comunicative
Buone competenze comunicative acquisite con i progetti di gruppo e le esposizioni individuali svolte durante tutto il percorso formativo.

Competenze Gestionali
Buone conoscenze organizzative e di lavoro in gruppo acquisite durante il percorso universitario.

Competenze Linguistiche
Italiano (madrelingua), Inglese (First certificate, B2)

ESPERIENZE LAVORATIVE

Consulenza Esterna *Ottobre 2022*
Treos S.C., Trento
Stesura di un report riguardo la crittografia post-quantum, con particolare riferimento ai sostituti drop-in per il protocollo di Diffie-Hellman.

Collaboratore Esterno *Giugno 2021 - Ottobre 2021*

Università degli Studi di Trento & Quadrans, Trento
Borsa post laurea: collaborazione a tempo determinato volta a studiare alcuni aspetti teorici ed implementativi delle primitive crittografiche post-quantum in corso di standardizzazione nel NIST PQC. Il mio ambito specifico riguarda le firme hash-based, con particolare riferimento a SPHINCS+. L'implementazione è pensata per la blockchain Quadrans.

Collaboratore Esterno *Aprile 2021 - Maggio 2021*
Università degli Studi di Trento & MicroFabSolutions, Trento
Collaborazione a tempo determinato volta a realizzare una analisi dettagliata sulle primitive crittografiche implementate correttamente nei dispositivi hardware open source. Più precisamente, sono state approfondite le primitive crittografiche utili all'integrazione sicura con architetture blockchain, con particolare riferimento agli algoritmi di firma digitale basati su curve ellittiche e le funzioni di hash SHA-256 e RIPEMD. Il report si prefigge esplicitamente di descrivere lo stato dell'arte a riguardo.

Full Stack Developer *Marzo 2020 - Luglio 2020*
BVTech S.p.A, Milano
Sviluppo di un applicativo web: l'attività è stata finalizzata alla realizzazione del software "CGR WEB" (Catasto Georeferenziato impianti Rifiuti) per conto di Regione Lombardia; questo è un database condiviso da Regione e Province e contiene i dati tecnici ed amministrativi relativi a tutti gli impianti autorizzati ad effettuare operazioni di gestione dei rifiuti, agli impianti a fonte rinnovabile ed agli impianti autorizzati al trattamento in deroga dei rifiuti liquidi negli impianti di depurazione acque reflue urbane. Lo sviluppo di questo software ha visto presenti diversi linguaggi di programmazione e di markup: il lato frontend è stato gestito con il framework Angular-8, in modo da integrare in modo efficiente HTML5, CSS e Typescript; il lato backend è gestito unicamente da Java, mentre per il lato database abbiamo usato SQLDeveloper. In aggiunta a ciò abbiamo utilizzato SVN come software di versionamento.

Tutor - Informatica *Settembre 2019 - Dicembre 2019*
Università degli Studi di Trento
sotto guida del Dr. Roberto Zunino, presso il Dipartimento di Matematica.

Tutor - Probabilità e Statistica *Febbraio 2019 - Giugno 2019*
Università degli Studi di Trento
sotto guida del Dr. Andrea Pugliese, presso il Centro di Biologia Integrata.

TRATTAMENTO DEI DATI PERSONALI

Acconsento alla pubblicazione del mio CV in ottemperanza alle disposizioni di legge dettate in materia di trasparenza (D.Lgs. 33/2013).