

# CRITTOGRAFIA

*Book Series*

3

*Editor in Chief*

Massimiliano SALA  
Università degli Studi di Trento

*Scientific Committee*

Marco BALDI  
Università Politecnica delle Marche

Michele ELIA  
Politecnico di Torino

Norberto GAVIOLI  
Università degli Studi dell'Aquila

Massimo GIULIETTI  
Università degli Studi di Perugia

Elisa GORLA  
Université de Neuchâtel

Gabor KORCHMARÓS  
Università degli Studi della Basilicata

Sihem MESNAGER  
Université Vincennes–Saint–Denis (Paris 8)

Guglielmo MORGARI  
Telsy Elettronica e Telecomunicazioni SpA

Marco PEDICINI  
Università degli Studi Roma Tre

Elizabeth QUAGLIA  
Royal Holloway University of London

Giancarlo RINALDO  
Università degli Studi di Trento

Alessandra SCAFURO  
North Carolina State University – Raleigh

Péter SZIKLAI  
Eötvös Loránd University

Andrea VISCONTI  
Università degli Studi di Milano

# 100 tesi di Crittografia e Codici in Italia 2008–2017

*a cura di*  
Daniele Bartoli  
Nadir Murru  
Francesco Pavese  
Massimiliano Sala

*Prefazione di*  
Michele Elia  
Massimiliano Sala

## *Contributi di*

Francesco Abbruzzese, Andrea Agnesse, Francesco Aldà, Alessandro Amadori, Federica Baiocchi  
Marco Baldi, Daniele Bartoli, Paolo Bartolucci, Massimo Battaglion, Alberto Bedodi  
Emanuele Bellini, Silvia Berlanda, Margherita Bertè, David Bertoldi, Valeria Bodrone  
Matteo Bonini, Domenica Borra, Cecilia Boschini, Giulia Bossi, Cecilia Bracuto  
Alessandro Budroni, Marco Calderini, Cristina Califano, Simon Calimani, Gianluca Caparra  
Wiliam Capraro, Marco Carolla, Luca Casati, Silvia Ceccato, Emanuele Cesena  
Michele Ciampi, Pierpaolo Colagè, Chiara Della Corte, Micaela De Santis, Francesco Devito  
Laura Donizetti, Michele Elia, Mohamad El laz, Stefania Fanali, Edoardo Fasano  
Maria Angela Federici, Sebastiano Ferraris, Emanuela Franzè, Daniele Friolo, Andrea Frisoni  
Giacomo Giuliani, Massimo Giulietti, Federico Carlo Gorla, Francesco Gozzini, Riccardo Grimi  
Stefano Guarino, Andrea Guidolin, Gábor Korchmáros, Valentino Lanzone, Stefania Lippiello  
Riccardo Longo, Mario Mancusi, Rita Manzo, Giulia Maragnani, Valeria Marelli  
Luca Mariot, Annalisa Marrone, Marco Martinoli, Pasqua Valentina Mauri, Silvia Mella  
Ferdinando Montecuollo, Rocco Mora, Nadir Murru, Luca Nizzardo, Ginetta Paladino  
Luca Palmulli, Filomena Panico, Francesco Pavese, Francesco Peverini, Daniel Pinter  
Pierpaolo Polo, Lorenzo Principi, Orazio Puglisi, Gabriele Pulvano, Rosanna Reibaldi  
Francesco Renna, Paolo Riccardi, Giacomo Ricciutelli, Francesco Romeo, Beatrice Rossi  
Matteo Sabbatini Peverieri, Massimiliano Sala, Giordano Santilli, Paolo Santini, Maurizia Saraullo  
Alessandra Scafuro, Daniele Sciarroni, Davide Schipani, Linda Senigagliesi, Simona Silvestri  
Luisa Siniscalchi, Chiara Spadafora, Christopher Spennato, Marco Timpanella  
Salvatore Andrea Tinnirello, Barbara Usai, Stefania Vanzetti, Marco Vargiu, Daniele Venturi  
Irene Villa, Andrea Visconti, Ivan Visconti, Stéphanie Vuillermoz  
Andres Yesid Diaz Pinto, Ferdinando Zullo





Aracne editrice

[www.aracneeditrice.it](http://www.aracneeditrice.it)  
[info@aracneeditrice.it](mailto:info@aracneeditrice.it)

Copyright © MMXX  
Giacchino Onorati editore S.r.l. – unipersonale

[www.giacchinoonoratieditore.it](http://www.giacchinoonoratieditore.it)  
[info@giacchinoonoratieditore.it](mailto:info@giacchinoonoratieditore.it)

via Vittorio Veneto, 20  
00020 Canterano (RM)  
(06) 4551463

ISBN 978-88-255-2752-0

*I diritti di traduzione, di memorizzazione elettronica,  
di riproduzione e di adattamento anche parziale,  
con qualsiasi mezzo, sono riservati per tutti i Paesi.*

*Non sono assolutamente consentite le fotocopie  
senza il permesso scritto dell'Editore.*

I edizione: gennaio 2020

# Indice

## Parte I **Introduzione**

- 17 **Presentazione**  
*Michele Elia, Massimiliano Sala*
- 19 **Introduzione alla crittografia con cenni storici**  
*Daniele Bartoli, Nadir Murru, Francesco Pavese*

## Parte II **Contributi accademici**

- 35 **La Tecnologia Blockchain e le Cryptocurrency**  
*Ivan Visconti*
- 45 **Crittografia Asimmetrica: Un Viaggio a Cavallo tra Minicritto e Crittomania**  
*Daniele Venturi*
- 61 **Block Cipher**  
*Andrea Visconti*
- 73 **Codici**  
*Marco Baldi, Massimo Giulietti*
- 85 **Elliptic Curve Cryptography**  
*Gábor Korchmáros, Massimo Giulietti*

Parte III  
**Tesi di dottorato**

- 97    Authentication and Integrity Protection at Data and Physical layer for Critical Infrastructures  
*Gianluca Caparra*
- 103   Trace Zero Varieties in Pairing-based Cryptography  
*Emanuele Cesena*
- 109   Applicazioni di curve su campi finiti alla sicurezza informatica  
*Valentino Lanzone*
- 115   Analysis of cryptographic algorithms against theoretical and implementation attacks  
*Silvia Mella*
- 125   Compressione e indicizzazione di dati genomici con protezione della confidenzialità  
*Ferdinando Montecuolo*
- 133   Come autenticare computazioni su gruppi: nuove primitive omomorfe ed applicazioni  
*Orazio Puglisi*
- 141   OFDM in emerging wireless networks: Synchronization algorithms and physical layer security  
*Francesco Renna*
- 149   Modern coding techniques for reliable and secure communications  
*Giacomo Ricciutelli*
- 157   Secure Computation Under Network and Physical Attacks  
*Alessandra Scafuro*
- 163   Decodifica efficiente di codici ciclici e applicazioni in crittografia  
*Davide Schipani*
- 167   Delayed-Input and Non-Malleable Cryptographic Protocols  
*Luisa Siniscalchi*

- 173 Manomissioni nel Paese delle Meraviglie (Tampering in Wonderland)  
*Daniele Venturi*

Parte IV  
**Tesi di laurea**

- 183 Generazione di codici correttori di errori mediante metodi algebrico-geometrici  
*Francesco Abbruzzese*
- 187 Stream Ciphers: from Correlation Attacks to the Cube Attack  
*Andrea Agnesse*
- 193 L'attacco Partial Sum ad una versione di AES ridotta a 6 round: implementazione e miglioramenti  
*Francesco Aldà*
- 197 On Summation Polynomials for Elliptic Curves  
*Alessandro Amadori*
- 201 Crittografia basata su attributi per l'accesso ai dati sanitari  
*Federica Baiocchi*
- 205 Il sistema TextSecure: aspetti crittografici  
*Paolo Bartolucci*
- 211 Ottimizzazione delle proprietà del grafo di Tanner di codici LDPC convoluzionali  
*Massimo Battaglioni*
- 215 Primality Tests in Polynomial Time  
*Alberto Bedodi*
- 219 Applicazioni del Metodo Rho di Pollard al Problema del Logaritmo Discreto e al Problema della Fattorizzazione  
*Emanuele Bellini*

- 225    Protezione crittografica per processare dati condivisi su una piattaforma non attendibile  
*Silvia Berlanda*
- 231    Curve ellittiche ed algoritmi di fattorizzazione  
*Margherita Bertè*
- 233    Strumenti per l'Analisi di Implementazioni crittografiche White-box  
*David Bertoldi*
- 237    Curve Algebriche applicate alla Teoria dei Codici Correttori  
*Valeria Bodrone*
- 241    Linear Network Codes and Algebraic Curves  
*Matteo Bonini*
- 245    Automi cellulari e applicazioni crittografiche  
*Domenica Borra*
- 251    NTWO: uno schema di cifratura post-quantistico  
*Cecilia Boschini*
- 255    Hashing into Elliptic and Hyperelliptic Curves  
*Giulia Bossi*
- 259    Secret Sharing Schemes multilivello  
*Cecilia Bracuto*
- 265    Funzioni hash nella crittografia ellittica con i pairing  
*Alessandro Budroni*
- 269    Codici Algebrico Geometrici Generalizzati da Curve Massimali  
*Marco Calderini*
- 273    Schemi di condivisione di segreti basati su automi cellulari  
*Cristina Califano*
- 277    Unconditionally secure authentication for quantum key distribution  
*Simon Calimani*



- 281 Euristiche per la minimizzazione circuitale di funzioni booleane e loro applicazioni alla crittografia leggera  
*Wiliam Capraro*
- 285 Crittografia Ellittica  
*Marco Carolla*
- 289 Come rilevare la perdita di informazioni: un'app per testare la sicurezza su dispositivi mobili  
*Luca Casati*
- 295 Uno Schema di key Management per il Controllo d'Accesso a Servizi GNSS  
*Silvia Ceccato*
- 301 Round and Computational Efficiency of Two-Party Protocols  
*Michele Ciampi*
- 307 Sicurezza di Shannon e Sicurezza Computazionale  
*Pierpaolo Colagè*
- 311 Fattorizzazione di numeri interi e applicazioni alla crittografia  
*Chiara Della Corte*
- 315 Counting Point on Elliptic Curves: Schoof Algorithm  
*Micaela De Santis*
- 321 Un'applicazione delle curve ellittiche di Edwards al protocollo Ripple  
*Francesco Devito*
- 323 La crittografia come garanzia di sicurezza: il voto elettronico  
*Laura Donizetti*
- 327 Errori di implementazione, codifiche e dimostrazioni per il critto-sistema El Gamal  
*Mohamad El laz*
- 333 Codici algebrico-geometrici da curve massimali  
*Stefania Fanali*

- 337   Reti neurali e crittografia  
*Edoardo Fasano*
- 343   Distribuzione dei Pesi di Codici Ciclici Polinomi Idempotenti e  
Polinomi di Mattson-Solomon  
*Maria Angela Federici*
- 349   La Trasformata di Winograd nella Teoria dei Codici Correttori  
*Sebastiano Ferraris*
- 353   Polinomi di permutazione  
*Emanuela Franzè*
- 357   Argomenti Predicibili  
*Daniele Friolo*
- 361   Curve ellittiche, DSA ed ECDSA  
*Andrea Frisoni*
- 365   Alcune dimostrazioni per l'analisi della sicurezza di broadcast  
authentication con catene di hashing  
*Giacomo Giuliani*
- 371   Analisi e testing di KDFs per la generazione di chiavi crittografica-  
mente sicure  
*Federico Carlo Gorla*
- 375   RLWE-based Somewhat Homomorphic Encryption with an ap-  
plication to the Symmetric Searchable Encryption problem  
*Francesco Gozzini*
- 379   Gli sviluppi della Blockchain: studio e implementazione di Smart  
Contract  
*Riccardo Grimi*
- 383   Ciphertext-only reconstruction of LFSR-based stream ciphers  
*Stefano Guarino*
- 387   Crittosistemi Polly Cracker  
*Andrea Guidolin*

- 39I Sulla crittografia omomorfa  
*Stefania Lippiello*
- 397 Attribute Based Encryption con metodi algebrici  
*Riccardo Longo*
- 403 Crittosistemi a Chiave Pubblica su Curve Ellittiche  
*Mario Mancusi*
- 407 Biometric / Cryptographic Keys Binding based on Function Minimization  
*Rita Manzo*
- 41I Reticoli, Crittosistemi e l'Algoritmo LLL in Crittoanalisi  
*Giulia Maragnani*
- 415 Enigma come strumento per la didattica della matematica  
*Valeria Marelli*
- 419 Cryptographic Pseudorandom Number Generators Based on Chaotic Cellular Automata  
*Luca Mariot*
- 425 Crittografia non commutativa  
*Annalisa Marrone*
- 429 Glitch Propagation Model and Cryptography  
*Marco Martinoli*
- 435 PKI e IBE: metodi di autenticazione e background algebrico  
*Pasqua Valentina Mauri*
- 439 Crittografia su reticoli  
*Rocco Mora*
- 445 Message Authentication Codes Omomorfici  
*Luca Nizzardo*
- 45I Codici Correttori di Errori  
*Ginetta Paladino*

- 453    AES: Studio e Implementazione dello Square-6 Attack  
*Luca Palmulli*
- 457    Il problema Learning With Errors: un approccio probabilistico  
basato su un GPU Direct Scheme  
*Filomena Panico*
- 463    Schemi di Condivisione di Segreti  
*Francesco Peverini*
- 467    Applicazioni crittografiche della Teoria dei Numeri all'Online  
Banking  
*Daniel Pinter*
- 473    ZCash: analisi critica delle specifiche del protocollo proposto da  
Zhong  
*Pierpaolo Polo*
- 479    Progetto software di funzioni di generazione di chiavi per schemi  
di firma digitale basati su codici  
*Lorenzo Principi*
- 483    Fattorizzazione e Test di Primalità con Curve Ellittiche  
*Gabriele Pulvano*
- 489    Teoria e algoritmi per la crittografia e gli stream ciphers  
*Rosanna Reibaldi*
- 495    Distributed Ledger Technology: la Blockchain oltre i sistemi di  
pagamento  
*Paolo Riccardi*
- 499    Cryptography in Digital Cash: Cryptocurrencies  
*Francesco Romeo*
- 503    Crittografia basata sulle dualità: generazione di curve ellittiche  
pairing-friendly  
*Beatrice Rossi*

- 507 Una variante dello schema di denaro elettronico di Brands con le curve ellittiche  
*Matteo Sabbatini Peverieri*
- 511 Una dimostrazione della Congettura Ternaria di Goldbach  
*Giordano Santilli*
- 515 Progetto di sistemi crittografici basati su codici QC-LDPC con chiavi compatte  
*Paolo Santini*
- 519 Protocolli crittografici per monete digitali  
*Maurizia Saraullo*
- 523 Tecniche basate su blockchain per la firma digitale  
*Daniele Sciarroni*
- 529 Sicurezza a livello fisico raggiungibile con pratici schemi di modulazione e codifica  
*Linda Senigagliesi*
- 533 Un'applicazione della Teoria dei Grafi in Crittografia  
*Simona Silvestri*
- 539 Il problema del logaritmo discreto e della fattorizzazione attraverso l'algoritmo  $\rho$  di Pollard  
*Chiara Spadafora*
- 543 Come proteggere le informazioni riservate  
*Christopher Spennato*
- 547 Codici da curve massimali  
*Marco Timpanella*
- 551 Crittografia. Applicazioni matematiche ed il loro ruolo nella sicurezza delle informazioni  
*Salvatore Andrea Tinnirello*
- 555 Funzioni Hash e loro applicazioni  
*Barbara Usai*

- 561    Attacchi ai sistemi crittografici basati sul logaritmo discreto: il caso delle curve iperellittiche  
*Stefania Vanzetti*
- 565    Fast Algebraic Cryptanalysis in Finite Fields of Higher Order with the Cube Attack  
*Marco Vargiu*
- 569    Funzioni vettoriali Booleane in dimensione pari  
*Irene Villa*
- 573    Applicazione delle frazioni continue alla crittografia: attacchi al sistema RSA e generazione di sequenze pseudo-casuali  
*Stéphanie Vuillermoz*
- 577    Authentication in Remote Controls  
*Andres Yesid Diaz Pinto*
- 581    Geometrie di Galois e Codici Lineari  
*Ferdinando Zullo*
- 585    Bibliografia

Parte I

# INTRODUZIONE





## Presentazione

Michele Elia, Massimiliano Sala

La rivoluzione culturale e cognitiva nata dall'invenzione di Johannes Gensfleisch zum Gutenberg della stampa a caratteri mobili parse immediatamente ai contemporanei come una meraviglia inaspettata e irripetibile. Non potevano certamente immaginare che la rivoluzione era appena iniziata e che secoli dopo ci saremmo trovati in un mondo dominato da nuove e straordinarie forme di scritte.

In Internet e nel World Wide Web, i messaggi sono della natura più disparata, dal tradizionale testo scritto ai brani musicali, dalla voce alle immagini, da operazioni più astratte quali autorizzazioni e attività notarili, al riconoscimento di persone o al controllo di oggetti volanti. Non è esagerato affermare che l'evoluzione tecnologica verso il digitale dei sistemi di comunicazione e dei calcolatori negli ultimi due secoli ha esteso il significato che si può attribuire ai termini "scrittura" e "messaggio".

La segretezza di qualsiasi tipo di messaggio è diventata una caratteristica indispensabile, anzi vitale, in un mondo globalmente connesso sia elettronicamente, sia per mobilità di persone. Le millenarie tecniche di protezione dei dispacci militari e diplomatici sono così entrate in modo pervasivo nel quotidiano di ogni attività sociale, industriale ed economica. La "parola magica" è crittografia, la cui definizione classica, di arte delle scritte segrete, è molto più propriamente diventata l'arte per la protezione dei messaggi. Abbiamo allora assistito al singolare fenomeno di come tale arte, nel passaggio dalle corti alle genti comuni, sia diventata una disciplina scientifica. In questo scenario, sono richiesti algoritmi sempre più astratti, e l'invenzione di paradigmi per imprevedibili applicazioni.

Questa situazione mondiale coinvolge senza eccezioni anche il nostro paese Italia. Con la speranza di far cosa utile alla comunità nazionale scientifica e di governo, ha preso corpo, nella comunità De Componendis Cyfris, il progetto di raccogliere i sommari di 100 tesi (Laurea, Laurea Magistrale e Dottorato) sulla crittografia prodotte negli ultimi dieci anni nelle università italiane. Il duplice scopo è stato sia ottenere in modo indiretto un censimento, se pur parziale, di

quanti hanno lavorato e ancora si occupano di crittografia, sia fornire un quadro degli interessi, competenze e stato dell'arte crittografica nell'accademia e indirettamente, nell'industria italiana.

I tre giovani curatori del libro hanno svolto un lavoro egregio, avvicinando relatori e tesisti, estraendo dalle tesi le bibliografie, raccolte poi in una sintesi posta al termine del volume, e accompagnando ogni sommario di tesi, scritto dall'autore, con una sua succinta biografia che include anche il cammino lavorativo o di carriera dopo la laurea.

Inoltre sono rimarchevoli cinque capitoli, posti a preambolo dei sommari di tesi, scritti da esperti del settore che illustrano i principali argomenti trattati e che si presentano come una panoramica succinta, ma non banale, dello stato dell'arte concernente la crittografia. Tali capitoli sono *La Tecnologia Blockchain e le Cryptocurrency* di Ivan Visconti, *Crittografia Asimmetrica: Un Viaggio a Cavallo tra Minicritto e Crittomania* di Daniele Venturi, *Block Cipher* di Andrea Visconti, *Codici* di Marco Baldi e Massimo Giulietti, *Elliptic Curve Cryptography* di Gabor Korchmaros e Massimo Giulietti. Come si evince dai titoli, sono coperti gli aspetti principali sia della crittografia classica, sia della relazione tra crittografia e codici, sia dell'uso della crittografia contemporanea.

I professori Daniele Bartoli, Nadir Murru e Francesco Pavese hanno curato un'opera che ha ampiamente superato le aspettative del progetto iniziale. Ne emergono un quadro confortante sullo status della crittografia in Italia, una miriade di spunti di ricerca, nonché un'indicazione degli sviluppi futuri.

## Introduzione alla crittografia con cenni storici

Daniele Bartoli, Nadir Murru, Francesco Pavese

Fin dall'antichità uno dei maggiori problemi, fondamentale almeno quanto quello di conservare mediante la scrittura informazioni importanti, è consistito nell'evitare l'accesso a dati sensibili da parte di soggetti non autorizzati. In innumerevoli situazioni la segretezza con la quale messaggi di una certa rilevanza dovevano raggiungere il destinatario o i destinatari senza poter essere comprese da qualsiasi altro agente è stata di fondamentale importanza ed ha determinato la vittoria o la sconfitta in guerre e battaglie, la vita e la morte di molte persone, la riuscita o meno di rivoluzioni.

La parola "crittografia" deriva dall'unione di due parole greche: "kryptós" che significa nascosto, e "gráphein" che significa scrivere. Con il termine crittografia quindi si intende un insieme di tecniche e algoritmi che consentono di trasformare un messaggio in modo da renderlo comprensibile solamente alle persone che sono a conoscenza del metodo tramite cui si è codificato il messaggio stesso.

I primi esempi a noi noti dell'utilizzo di una modalità per modificare il significato di un messaggio risalgono addirittura all'antico Egitto durante il periodo dell'Antico Regno. Sono stati infatti rinvenuti alcuni geroglifici, scolpiti sopra antichi monumenti, non standard o parzialmente riprodotti. Rimane il mistero se tali modifiche avessero lo scopo di occultare una qualche informazione oppure appartenessero più in generale ad un particolare culto misterico.

Secondo gli storici, anche i Babilonesi avrebbero potuto utilizzare un'arcaico sistema crittografico: sono state rinvenute tavolette risalenti al 2500 a.C. nelle quali manca la prima consonante delle parole e si ipotizza che ciò sia stato fatto per proteggere un possibile segreto industriale relativo alla produzione di ceramica vetrificata.

Chiaramente l'utilizzo della crittografia viaggia di pari passo con il diffondersi della scrittura e assume nel corso dei secoli forme via via più complicate. Si assiste quindi ad una corsa alla sicurezza che vede opposti chi vuole conservare e diffondere una certa informazione e chi invece cerca in tutti i modi di venire a conoscenza di tale segreto. Questa lotta antitetica si avvale chiaramente dei più moderni

ritrovati tecnologici di ogni epoca: l'uomo ha chiaro fin dall'antichità il ruolo centrale di comunicazioni sicure e chi ha il controllo su di esse ha una posizione di vantaggio spesso decisiva sui concorrenti.

La crittografia non deve tuttavia essere confusa con la steganografia, il cui scopo è quello di nascondere l'intero messaggio a individui non autorizzati: la crittografia infatti non vuole celare il messaggio stesso ma il suo significato. Lo stesso Erodoto nelle sue "Storie" ci racconta ingegnosi esempi di steganografia. Uno di essi permise, secondo la tradizione, al re spartano Demarato, esiliato in Persia, di avvertire i suoi compatrioti del progetto di invasione ideato dal re persiano Serse: incise sul legno di una tavoletta il messaggio e poi ricoprì con della cera la tavoletta stessa, facendola apparire nuova. Una volta recapitata a Sparta, solo dopo molte riflessioni gli Spartani capirono di dover rimuovere la cera e poterono quindi leggere l'importante messaggio recapitatogli dal loro re. Un esempio più moderno di Steganografia è rappresentato dall'utilizzo di inchiostro invisibile, di solito succo di limone o linfa di piante, che una volta sottoposto ad un modesto calore diventa visibile, mostrando il messaggio celato. Come già accennato tutti questi esempi non costituiscono espedienti crittografici, ma hanno sicuramente rivestito una notevole importanza storica.

Considerando ancora il mondo greco, durante la guerra tra ateniesi e spartani per l'egemonia sul Peloponneso, un espediente utilizzato fornisce uno dei primi esempi della cosiddetta crittografia per trasposizione. Il messaggio iniziale (detto nel gergo moderno "messaggio in chiaro") veniva trasformato nel "messaggio cifrato" attraverso l'inserzione di simboli superflui. Tale messaggio cifrato veniva poi inviato al destinatario che doveva essere in grado di risalire al messaggio originale. L'operazione di cifratura (ovvero il passaggio da messaggio in chiaro a messaggio cifrato) e di decifratura (da messaggio cifrato a messaggio in chiaro) era resa possibile da particolari bastoni (detti scitali): i caratteri aggiunti infatti scomparivano una volta che il messaggio cifrato, scritto su di una lunga striscia di tela, veniva arrotolato su tale bastone. Di fondamentale importanza in questo processo è che, nonostante la tecnica utilizzata fosse conosciuta da tutti, solo la conoscenza esatta delle dimensioni del bastone utilizzato avrebbe potuto permettere la decodifica corretta del messaggio cifrato.