



# UNIVERSITÀ DI PISA

---

## CRITTOGRAFIA POST-QUANTISTICA

**EMMANUELA ORSINI**

Anno accademico 2021/22  
CdS MATEMATICA  
Codice 703AA  
CFU 6

Moduli	Settore/i	Tipo	Ore	Docente/i
CRITTOGRAFIA POST- QUANTISTICA	MAT/02	LEZIONI	42	PATRIZIA GIANNI EMMANUELA ORSINI

### Obiettivi di apprendimento

#### *Conoscenze*

Gli studenti acquisiranno le conoscenze relative ai concetti di base della crittografia moderna e degli attacchi crittografici derivanti dal potenziale sviluppo di grandi computer quantistici, e sui protocolli crittografici che sembrano essere più resistenti agli attuali attacchi quantistici. A tal fine, illustreremo gli attacchi di Shor e Grover, e come il primo renda completamente insicuri tutti i sistemi crittografici a chiave pubblica in uso.

Illustreremo poi alcuni protocolli che resistono all'algoritmo di Shor, in particolare quelli considerati dall'attuale progetto di standardizzazione di crittografia post-quantistica del NIST, attualmente in fase di sviluppo.

Descriveremo i risultati matematici su cui si basano questi protocolli e gli algoritmi utilizzati per attaccarli. Studieremo principalmente algoritmi sui reticoli, codici correttori di errore e curve ellittiche.

#### *Modalità di verifica delle conoscenze*

Si valuterà l'abilità dello studente di discutere con competenza e chiarezza i contenuti principali del corso.

Modalità'

\* Esame orale finale

#### *Capacità*

Gli studenti acquisiranno le conoscenze necessarie per partecipare alla ricerca nel campo della crittografia post-quantistica, e collaborare all'implementazione di algoritmi in questo campo, compresi algoritmi di crittanalisi.

#### *Modalità di verifica delle capacità*

Verifica nel corso dell'esame orale finale, che comprenderà anche una breve relazione tecnica su un argomento a scelta

#### *Comportamenti*

Gli studenti sono consigliati a frequentare le lezioni e a studiare gli argomenti via via presentati.

#### *Modalità di verifica dei comportamenti*

Nessuna

#### *Prerequisiti (conoscenze iniziali)*

I prerequisiti di aritmetica, fondamenti di algebra, algebra polinomiale, campi finiti, algebra lineare sono insegnati nei corsi del primo anno, e saranno comunque ripresi a lezione.

I prerequisiti necessari di carattere crittografico e algebro-geometrico insegnati in altri corsi saranno richiamati e saranno date precise indicazioni bibliografiche.

#### *Corequisiti*

Il corso è indipendente da altri corsi, anche se sinergie sono possibili.

#### *Prerequisiti per studi successivi*

Indicazioni su studi utili per la continuazione delle ricerche illustrate nel corso saranno date a lezione o in documentazione resa disponibile.



## UNIVERSITÀ DI PISA

---

### Programma (contenuti dell'insegnamento)

#### INTRODUZIONE ALLA CRITTOGRAFIA MODERNA

- Sicurezza incondizionata vs sicurezza computazionale, crittografia simmetrica, funzioni unidirezionali, PRF e PRG, funzioni hash
- Crittografia a chiave pubblica. Sicurezza CPA/CCA. Diffie-Hellman, RSA, Curve ellittiche
- Firme digitali, definizione di sicurezza
- Dimostrazioni a conoscenza zero

#### ARITMETICA

- Teorema dei numeri primi. Il simbolo di Lagrange. Criterio di Eulero. Reciprocità quadratica. Simbolo di Jacobi. Radice quadrata su un campo finito: algoritmi di Cipolla e Tonelli-Shanks.
- Test di primalità: pseudoprimi. Pseudoprimi di Eulero, pseudoprimi forti. Test di Miller Rabin. Fattorizzazione di interi: algoritmo Rho di Pollard. Fattorizzazione di interi: algoritmi di Fermat, di Dixon e Crivello quadratico. Logaritmo discreto

#### CALCOLO QUANTISTICO

- Introduzione al calcolo quantistico. Qubits. Quantum circuits. Modelli di calcolo. Quantum Gates.
- Trasformata di Fourier quantistica. Algoritmo per il calcolo della fase, algoritmo per il calcolo di un autovalore, algoritmo per il calcolo dell'ordine di un elemento
- Algoritmo di Shor: fattorizzazione e logaritmo discreto. Algoritmo di Grover

#### CRITTOGRAFIA POST-QUANTISTICA

- Progetto NIST di standardizzazione della crittografia post-quantistica
- Reticoli, geometria dei reticoli, problemi difficili su reticoli (SVP, CVP, LWE, NTRU), LLL e applicazioni, BKZ. Esempi di schemi.
- Codici correttori d'errore: codici lineari, codici ciclici, codici Goppa, McEliece e altri schemi. Codici quantistici, Reed-Muller.
- Isogenie: scambio di chiavi, CRS, SIDH e SIKE
- Schemi basati su primitive simmetriche: PICNIC

#### CONCLUSIONI E PROSPETTIVE

### Bibliografia e materiale didattico

Note e slides

N. Koblitz A course in number theory and cryptography

N. Koblitz Algebraic aspects of cryptography

D. Micciancio, S. Goldwasser Complexity of lattice problems: a cryptographic perspective,

Post-quantum cryptography (D. Bernstein, J. Buchmann, E. Dahmen, eds.)

S. Goldwasser and M. Bellare Lecture Notes on Cryptography (MIT notes) <https://cseweb.ucsd.edu/~mihir/papers/gb.html>

J. Silverman, The Arithmetic of Elliptic Curves

J. Katz and Y. Lindell, Introduction to Modern Cryptography

N. Smart, Cryptography Made Simple

### Indicazioni per non frequentanti

Gli studenti sono invitati a colloqui coi docenti anche su appuntamento

### Modalità d'esame

Esame orale

### Stage e tirocini

A richiesta, anche per conto di altri corsi

Ultimo aggiornamento 15/09/2021 11:58