



# UNIVERSITÀ DI PISA

---

## CRITTOGRAFIA POST-QUANTISTICA

**PATRIZIA GIANNI**

Anno accademico 2019/20  
CdS MATEMATICA  
Codice 703AA  
CFU 6

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

### Obiettivi di apprendimento

#### *Conoscenze*

Gli studenti acquisiranno le conoscenze relative ai potenziali attacchi alla sicurezza crittografica derivanti dal possibile futuro sviluppo di calcolatori quantistici di rilevante dimensione, e sui protocolli crittografici che resistono meglio a tali attacchi attualmente noti. A tal fine si illustreranno gli algoritmi quantistici di Shor e Grover, e come il primo renda totalmente insicuri RSA, Diffie-Hellmann e la sua estensione alle curve ellittiche, e il secondo possa richiedere l'uso di chiavi crittografiche più lunghe. Saranno quindi illustrati i vari protocolli resistenti all'algoritmo di Shor, in particolare quelli studiati dal corrente progetto di standardizzazione di protocolli di crittografia post-quantistica, lanciato dal NIST nel 2016, ed attualmente in sviluppo. Saranno delineati i risultati matematici che sono alla base di tali protocolli, e quali algoritmi sono utilizzati per gli attacchi ad essi. In particolare, si studieranno gli algoritmi sui reticoli, i codici correttori, i sistemi di equazioni polinomiali multivariate, e le curve ellittiche.

#### *Modalità di verifica delle conoscenze*

Gli studenti saranno valutati dalla loro dimostrazione di abilità nel discutere i contenuti principali del corso con l'uso della terminologia appropriata.

Metodo:

\* 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, e, soprattutto in caso di impossibilità a frequentare, tenersi aggiornati con colloqui coi docenti.

#### *Modalità di verifica dei comportamenti*

Tramite colloqui durante le lezioni e i ricevimenti

#### *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.



## UNIVERSITÀ DI PISA

### 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.

### Indicazioni metodologiche

Esame: orale

Frequenza: consigliata

Attività di insegnamento:

- \* Frequenza alle lezioni frontali
- \* Preparazione di esposti orali
- \* Studio individuale

Metodologia di Insegnamento:

- \* Lezioni frontali

### Programma (contenuti dell'insegnamento)

- 1 Test di primalità e fattorizzazione (non-quantistica). Logaritmo discreto. Trasformata di Fourier rapida.
- 2 Curve ellittiche
- 3 Sicurezza crittografica: Inadeguatezza della teoria classica della complessità. IND-CPA, IND-CCA, ecc.
- 4 Crittografia pre-quantistica:
  - 4.1 Crittografia simmetrica, hashing. DES, AES, SHA1, SHA2, Keccak (SHA-3)
  - 4.2 Crittografia asimmetrica pre-quantistica: RSA, Diffie-Hellman, curve ellittiche: cifra, KEM, firma.
  - 4.3 Successioni pseudo-casuali, zero-knowledge, autenticazione.
- 5 Calcolo quantistico e crittografia
  - 5.1 Cenni sui modelli matematici di computer quantistici, e loro realizzazione.
  - 5.2 Attacchi quantistici alla crittografia pre-quantistica: algoritmo di Shor, algoritmo di Grover (cenni).
  - 5.3 Progetto NIST di standardizzazione della crittografia post-quantistica.
- 6 Alcuni Protocolli crittografici post-quantistici
  - 6.1 Reticoli, LWE, NTRU e derivati
    - 6.1.1 LLL e applicazioni; reticoli ridotti, SVP e CVP. BKZ.
    - 6.1.2 Complessità generica dei problemi sui reticoli, dimostrazioni di sicurezza.
  - 6.2 Codici di Goppa, McEliece e crittografia sui codici correttori
  - 6.3 HFE e problemi derivati.
  - 6.4 Polly Cracker e Lattice Polly Cracker
  - 6.5 Merkle tree e firma digitale
  - 6.6 SIKE: Isogenie di curve ellittiche supersingolari.
- 7 Conclusioni e prospettive

### Bibliografia e materiale didattico

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>

### Indicazioni per non frequentanti

Gli studenti sono invitati a colloqui coi docenti anche su appuntamento.

### Modalità d'esame

Esame orale finale.

### Stage e tirocini

A richiesta, anche per conto di altri corsi.

### Pagina web del corso

<http://barba.dm.unipi.it/PQC>

### Altri riferimenti web

<https://csrc.nist.gov/Projects/Post-Quantum-Cryptography>

[https://en.wikipedia.org/wiki/Post-quantum\\_cryptography](https://en.wikipedia.org/wiki/Post-quantum_cryptography)

Ultimo aggiornamento 27/09/2019 09:32