Analisi comparativa e sistematizzazione di cifrari post-quantum basati su codici casuali

Andrea Bellani

Politecnico di Milano

andrea1.bellani@mail.polimi.it

January 19, 2025

Informazioni generali

Informazioni studente

- nome: Andrea Bellani (codice persona: 10733192, matricola: 956505)
- corso di studi: Ingegneria Informatica (laurea di primo livello)

Informazioni progetto

- nome progetto: Analisi comparativa e sistematizzazione di cifrari post-quantum basati su codici casuali
- docente responsabile: prof. Alessandro Barenghi
- aree di competenza: algoritmi, crittografia

Obbiettivi del progetto

Il progetto ha lo scopo di offrire allo studente un'occasione per applicare le conoscenze acquisite durante il percorso di laurea triennale. Lo studente, partendo da una bibliografia di riferimento dovrà:

- riassumere i concetti preliminari (affrontati nel proprio percorso di studi) necessari ad affrontare l'analisi che andrà a redarre;
- descrivere i crittosistemi di Alekhnovich e lo schema quasi-ciclico;
- riportare (e se necessario ideare) dimostrazioni di sicurezza per i crittosistemi di Alekhnovich;
- utilizzare un *argomento per ibridi* per trasformare i crittosistemi di Alekhnovich nello schema quasi-ciclico;

Introduzione (cont.)

- delineare un set di parametri per confrontare i cifrari analizzati (con particolare enfasi sull'efficienza computazionale e le prove formali di sicurezza).

Si valuta anche la capacità dello studente di ricercare, consultare e riportare ulteriori fonti bibliografiche (attendibili) se necessario. Lo studente redarrà l'analisi in Tex, seguendo le linee editoriali della letteratura scientifica del settore.

Conoscenze preliminari

Probabilità

Distribuzione di probabilità uniforme

Strutture algebriche

Gruppi, *Anelli*, *Campi*, *Ideali generati da polinomi*, *Anelli quozienti generati da polinomi*

Teoria dei codici lineari

Codice duale, *Matrice generatrice*, *Matrice di parità*, *Sindrome*, *Peso di un vettore*, *Distanza di Hamming*,*Rotazione di un vettore*, *Codici ciclici*

Teoria della computazione

La complessità computazionale, *La complessità asintotica*, *Macchina di Turing*, *Tesi di Church-Turing*, *Problemi NP ed NP-Hard*

Conoscenze preliminari (cont.)

Crittografia

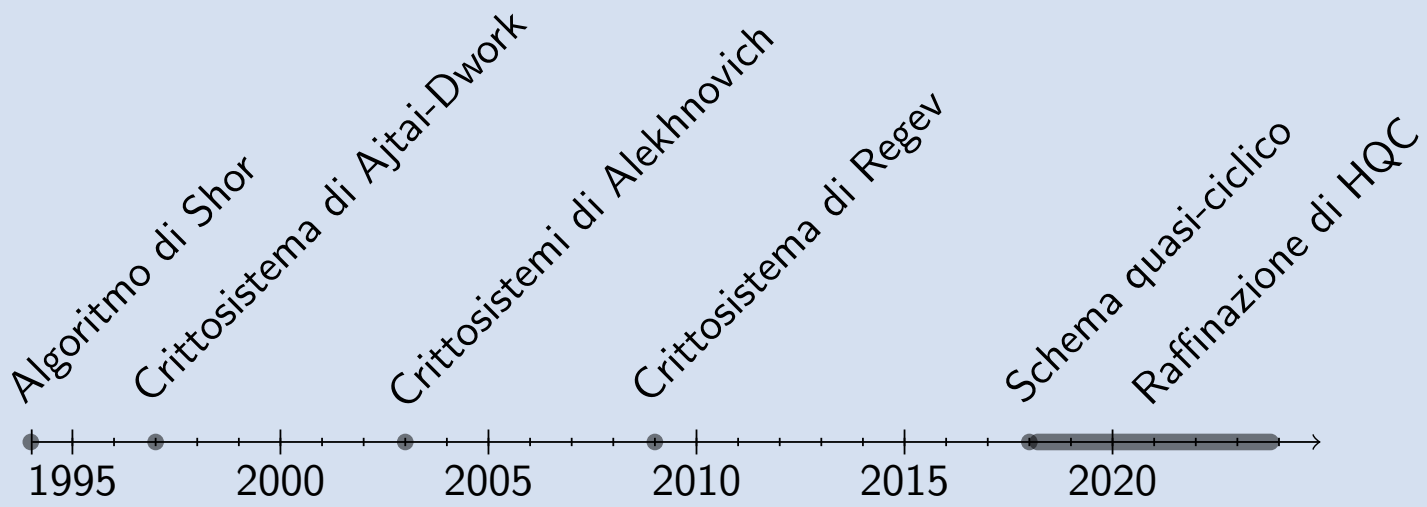
Crittografia asimmetrica, *Search decoding problem*, *Decisional decoding problem*, *Ipotesi di Fisher-Stern*, *Argomento per ibridi*

La crittografia post-quantistica

La crittografia pre-quantistica è stata in larga misura basata su problemi matematici computazionalmente "difficili" (algoritmi di complessità non polinomiale), quali fattorizzazione (es. algoritmo RSA) o calcolo di logaritmi discreti (es. algoritmo Diffie-Hellman). Queste tecniche sono così divenute insicure nel momento in cui sono stati inventati algoritmi, per calcolatori quantistici, in grado performare in tempo polinomiale questi calcoli (si veda, ad esempio, l'algoritmo di Shor), almeno a livello teorico. I calcolatori quantistici di cui si dispone allo stato attuale non sono in grado di eseguire con successo questi algoritmi su casi di utilità pratica, ma nell'attesa che si realizzino calcolatori quantistici sufficientemente performanti, è necessario sviluppare crittosistemi in grado di resisterli, ma che siano anche abbastanza efficienti da avere un'utilità pratica.

La crittografia post-quantistica basata su codici (cont.)

I crittosistemi considerati



La crittografia post-quantistica basata su codici (cont.)

I crittosistemi di Ajtai-Dwork e di Regev

Benché la nostra analisi sia focalizzata sulla schematizzazione e il confronto tra i crittosistemi di Alekhnovich e lo schema quasi-ciclico, è doveroso menzionare i crittosistemi che hanno gettato le basi per questi ultimi. Di questi non abbiamo dunque dettagliato la struttura e le meccaniche, ci siamo limitati a:

- illustrare brevemente i principi su cui si basano;
- discutere brevemente la loro utilità pratica;
- evidenziare le analogie più evidenti coi crittosistemi di Alekhnovich.

La crittografia post-quantistica basata su codici (cont.)

I crittosistemi di Alekhnovich

I crittosistemi di Alekhnovich sono il punto centrale della nostra analisi. Di questi abbiamo infatti abbiamo sia dettagliato la definizione e che i processi di criptazione e decrittazione (in pseudocodice).
In più abbiamo fornito dimostrazioni formali di sicurezza contro:

- attacchi volti a decifrare il testo criptato senza l'ausilio della chiave privata;
- attacchi volti a dedurre la chiave privata da quella pubblica.

In particolare, per quest'ultima tipologia di attacchi, abbiamo ideato delle dimostrazioni per assurdo ad hoc (sotto forma di *riduzioni*), essendo la letteratura di riferimento manchevole di queste.

La crittografia post-quantistica basata su codici (cont.)

Lo schema quasi-ciclico

Illustrati i crittosistemi di Alekhnovich, abbiamo dettagliato struttura e processi dello schema quasi-ciclico (in maniera analoga a quanto fatto per i crittosistemi di Alekhnovich). Infine, abbiamo utilizzato un *argomento per ibridi* per dimostrare come, sotto determinate assunzioni (o *ipotesi*), il processo di criptazione del secondo crittosistema di Alekhnovich è analogo a quello dello schema quasi-ciclico.

Confronto tra i cifrari

I parametri scelti

Il corpus di parametri scelti per confrontare i crittosistemi in esame è costituito da:

- parametri legati alle dimensioni:
  - dimensione delle chiavi: dimensioni di chiave pubblica e privata sul numero di bit messaggio;
  - dimensione dei messaggi: rapporto tra numero di simboli di controllo sul numero di simboli di informazione;
- parametri legati alle complessità temporali:
  - complessità del processo di codifica;
  - complessità del processo di decodifica;

Confronto tra i cifrari (cont.)

- parametri legati alla sicurezza:
  - teoremi a cui è ridotta la loro sicurezza;
- parametri legati alla correttezza:
  - probabilità di decrittare correttamente il contenuto di un messaggio.

La scelta di questi parametri è stata fatta tenendo conto di quali sono i parametri che per primi vengono utilizzati per valutare l'affidabilità e l'utilità pratica di un crittosistema. Si noti come i parametri scelti non sono definiti ad hoc per i crittosistemi in analisi e potrebbero essere applicati a qualunque tipologia di crittosistemi.

Confronto tra i cifrari (cont.)

I risultati ottenuti

Confrontare i crittosistemi secondo i parametri scelti ci ha permesso di:

- quantificare le complessità dei processi di codifica e decodifica e le dimensioni di chiavi e messaggi ci ha permesso di valutare l'effettivo miglioramento (asintotico) delle prestazioni. In particolare, lo schema quasi-ciclico è l'unico ad avere processi complessità al più quadratica mantenendo lineare la dimensione delle chiavi e dei messaggi;
- verificare che entrambi i crittosistemi basano la propria sicurezza su problemi di difficoltà non strettamente diversa tra di loro;
- verificare se la probabilità di decrittazione corretta è ragionevolmente alta.

Confronto tra i cifrari (cont.)

Con questo confronto abbiamo evidenziato come crittosistemi di Alekhnovich, benché forniscano dimostrazioni di sicurezza e correttezza "formale" analoghe allo schema quasi ciclico, essi offrono prestazioni significativamente inferiori a quelle dello schema quasi-ciclico, rendendoli così inutilizzabili in un caso di utilità pratica.

Le conclusioni ottenute

- abbiamo organizzato le informazioni utili allo studio dei crittosistemi (estrapolandole sia dai corsi seguiti nella laurea triennale di Ingegneria Informatica che dalla lettura scientifica di interesse);
- si sono individuate analogie tra crittosistemi basati su teorie differenti (i crittosistemi basati su reticoli coi crittosistemi basati su codici);
- abbiamo applicato un argomento per ibridi per trasformare i crittosistemi di Alekhnovich nello schema quasi-ciclico;
- abbiamo, ove necessario, ideato dimostrazioni di sicurezza dei crittosistemi "per riduzione";
- si è stabilito un set di parametri per il confronto di cifrari che ci ha permesso di evidenziarne i punti di forza e debolezza di questi ultimi.

Le conclusioni ottenute (cont.)

Inoltre, l'argomento per ibridi utilizzato ci ha permesso di evidenziare come la differenza tra le meccaniche utilizzate dai crittosistemi di Alekhnovich e quelle utilizzate dallo schema quasi-ciclico non sia così significativa. Ciononostante, quest'ultimo offre prestazioni sufficientemente buone da poter essere la base per un'effettiva implementazione pratica (*HQC: Hamming Quasi-Cyclic*).

Bibliografia

Panoramica

- *Appunti corsi*: appunti presi dallo studente nei corsi di interesse per l'analisi;
- *Altro materiale didattico* : materiale didattico (esterno ai corsi seguiti) per integrare le conoscenze preliminari non coperte dai corsi sostenuti;
- *Articoli di riferimento* : articoli forniti dal docente per affrontare l'analisi;
- *Articoli di approfondimento* : articoli trovati dallo studente per approfondire e/o chiarificare gli argomenti trattati/accennati negli articoli di riferimento;
- *Articoli riepilogativi* : articoli utili ad avere una visione di insieme più chiara e uniforme.

Bibliografia (cont.)

Appunti corsi

- A. Bellani - Algoritmi e principi dell'informatica (2022)
- A. Bellani - Geometria e algebra lineare (2021)
- A. Bellani - Logica e algebra (2022)
- A. Bellani - Probabilità e statistica per l'informatica (2023)

Altro materiale didattico

- J.T. Gill - Algebraic Error Correcting Codes (lectures notes) (2015)
- M. Francischello, O. Papini - Teoria dei Codici e Crittografia (2012)
- M. Sudan, V. Guruswami, A. Rudra - Essential Coding Theory (2023)
- M. Rosulek - The Joy of Cryptography (2021)

Bibliografia (cont.)

Articoli di riferimento sui crittosistemi di Alekhnovich

- M. Alekhnovich - More on average case vs approximation complexity (2003)
- G. Zémor - Notes on Alekhnovich's cryptosystems (2016)

Articoli di riferimento sullo schema quasi-ciclico

- HQC team - HQC: Hamming Quasi-Cyclic (2021)

Bibliografia (cont.)

Articoli di approfondimento

- M. Bombar, A. Couvreur, T. Debris-Alazard - On Codes and Learning With Errors Over Function Fields (2022)
- M. Bombar, A. Couvreur, T. Debris-Alazard - Pseudorandomness of Decoding, Revisited: Adapting OHCP to Code-Based Cryptography (2023)
- C. Dwork, M. Ajtai - A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence (1997)
- O. Regev - On Lattices, Learning with Errors, Random Linear Codes, and Cryptography (2009)
- C. Aguilar-Melchor, O. Blazy, J. Deneuville, P. Gaborit, G. Zémor - Efficient Encryption From Random Quasi-Cyclic Codes (2018)

Bibliografia (cont.)

Articoli riepilogativi

- C. Peikert - A Decade of Lattice Cryptography (2016)
- V. Weger, N. Gassner, J. Rosenthal - A Survey on Code-based Cryptography (2024)
- V. Lyubashevsky - Basic Lattice Cryptography (2020)