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

Andrea Bellani

January 19, 2025

Contents

Chapter 0

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

Chapter 1

Specifiche

1.1 Obbiettivo

Lo scopo dell'analisi è quello di fornire una visione di insieme su alcuni cifrari post-quantum basati su codici casuali. In particolare, mantenendo un approccio didattico, l'analisi illustra e confronta i crittosistemi di Alekhnovich con lo schema quasi-ciclico, sia sotto il profilo delle meccaniche di funzionamento, che sotto l'aspetto dell'utilità pratica.

Al tempo stesso, l'analisi riassume e riorganizza i concetti preliminari affrontati nei corsi della laurea triennale di *Ingegneria Informatica* necessari ad approcciare lo studio della crittografia basata su codici.

1.2 Specifica

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;
- 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.

1.3 Analisi della specifica

L'analisi è stata così suddivisa:

1. **Concetti preliminari** : vengono riassunti e ordinati tutti i concetti preliminari utili ad affrontare la crittografia basata su codici;

2. **Considerazioni preliminari sugli algoritmi presentati** : si delineano le assunzioni e le procedure di base con cui sono stati scritti tutti gli algoritmi illustrati nelle sezioni seguenti;

3. **La crittografia basata su reticoli** : breve introduzione sui crittosistemi (non approfonditi successivamente) da cui si ispirano i crittosistemi di Alekhnovich e lo schema quasi-ciclico;

4. **I crittosistemi di Alekhnovich** : si illustrano il primo e il secondo crittosistema di Alekhnovich (chiavi e processi di criptazione e decrittazione), più le relative prove formali di sicurezza;

5. **Lo schema quasi-ciclico** : si illustra lo schema quasi-ciclico (chiavi e processo di criptazione e decrittazione), senza le prove formali di sicurezza;

6. **Analogie tra i crittosistemi analizzati** : si utilizza un argomento per ibridi per mostrare come sotto determinate ipotesi, sia possibile trasformare il processo di criptazione del secondo crittosistema di Alekhnovich nello schema quasi-ciclico;

7. **Analisi comparativa dei cifrari analizzati** : si delinea un set di parametri per confrontare quantitativamente i cifrari e lo si utilizza per mostrare come, tra i crittosistemi analizzati, solo lo schema quasi-ciclico possa essere di utilità pratica.

Ciascuna definizione, assunzione o dimostrazione cita opportunamente gli articoli, menzionati nella bibliografia, da cui è stata estrapolata.

Chapter 2

Realizzazione

2.1 Riordino dei concetti preliminari

I concetti preliminari sono stati delineati a cominciare da quelli logico-matematici, per poi spostarsi su quelli prettamente informatici e quelli di teoria dei codici lineari (i quali sono gli unici, insieme all'argomento per ibridi, a non essere affrontati in altri corsi di *Ingegneria Informatica*):

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

2.2 Analisi dei crittosistemi

Ciascun crittosistema è stato illustrato dettagliando:

- il set di informazioni pubbliche;
- il set di informazioni private;
- il processo di criptazione (in pseudo-codice);
- il processo di decrittazione (in pseudo-codice).

Mentre per approfondire le analogie teoriche:

- si sono illustrati brevemente i crittosistemi di Ajtai-Dwork e Regev;
- costruito un argomento per ibridi per mostrare come, sotto le assunzioni riportate, il secondo crittosistema di Alekhnovich sia equivalente allo schema quasi-ciclico.

2.3 Formulazione delle prove formali di sicurezza

Abbiamo distinto due tipologie di attacchi (i nomi sono di nostra invenzione):

- *Third Man Decryption Attack* : attacco finalizzato a decodificare con successo informazioni criptate senza l'utilizzo della chiave privata;
- *Private Key Deduction Attack* : attacco finalizzato al calcolo della chiave privata da quella pubblica.

Le dimostrazioni di sicurezza per Third Man Decryption Attack sono state prese dagli articoli forniti, mentre le dimostrazioni contro il Private Key Deduction Attack sono state ideate dall'autore e sono entrambe "per riduzione": si dimostra come un attaccante in grado di effettuare con successo l'attacco, sarebbe anche in grado di risolvere in complessità polinomiale uno dei problemi che si assume siano irrisolvibili (in complessità polinomiale). Queste, sono presentate come algoritmi in pseudo-codice.

2.4 Confronto tra i cifrari

Il primo passo per il confronto tra i cifrari è stato quello di delineare un corpus di parametri che fossero allo stesso tempo:

- utilizzabili per confrontare quantitativamente i crittosistemi;
- già precedentemente illustrati nell'analisi;
- non strettamente legati ai cifrari analizzati (e dunque estendibili al confronto di altri cifrari);
- utili ad evidenziare come lo schema quasi-ciclico è l'unico ad avere un'utilità pratica.

In particolare, i crittosistemi sono stati confrontati per:

- 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;
- 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.

Chapter 3

Conclusioni ottenute

In questo lavoro:

- 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 (nel momento in cui li si volesse utilizzare per un'implementazione pratica);
- siamo riusciti a evidenziare (grazie a un argomento per ibridi e ai parametri delineati nel confronto) 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*).

Chapter 4

Bibliografia

Possiamo suddividere i documenti utilizzati per redarre l'analisi in:

- *Appunti corsi*: appunti presi dallo studente nei corsi di interesse per l'analisi:
  - 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* : materiale didattico (esterno ai corsi seguiti) per integrare le conoscenze preliminari non coperte dai corsi sostenuti:
  - 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)
- *Articoli di riferimento* : articoli forniti dal docente per affrontare l'analisi:
  - 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)
- *Articoli di approfondimento* : articoli trovati dallo studente per approfondire e/o chiarificare gli argomenti trattati/accennati negli articoli di riferimento:
  - 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)

- *Articoli riepilogativi* : articoli utili ad avere una visione di insieme più chiara e uniforme:
  - 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)

Chapter 5

Report di svolgimento

- 15/09/2023 : riordino materiali forniti dal docente;
- 11/07/2024 : prima versione dell'analisi. Raggruppamento dei concetti preliminari, analisi dettagliata dei crittosistemi, definizione parametri per il confronto e prima versione del confronto;
- 21/08/2024 : aggiunte procedure di criptazione e decrittazione in pseudo-codice. Aggiunta capitolo sui crittosistemi di Ajtai-Dwork e Regev. Prima definizione delle analogie teoriche tra i crittosistemi analizzati;
- 27/08/2024 : aggiunta prove di sicurezza;
- 21/11/2024 : aggiunta argomento per ibridi;
- 19/12/2024 : presentazione sintetica;
- 19/01/2025 : stesura documentazione.