ABE-Lattice

Coordonator: Ferucio Laurențiu Țiplea
Mocanu Răzvan 3B6 *

April 2021

Contents

Abstract

In această lucrare voi introduce o tehnică generală de folosire a laticilor pentru a face o criptare funcțională, pornind de la presupunerea dificultății post-quantum. În special voi construi un model criptare bazată pe atribute și politică pe cheie care va înlocui curbele eliptice cu latici. Voi dovedi securitatea acestui model în sensul selectiv în modelul standard.

1 Introducere

1.1 Motivație

Criptografia este situată la baza nevoii de a avea o viața privată. De-a lungul deceniilor diverse metode au fost folosite pentru a ascunde mesaje dar această problemă devine din ce în ce mai greu de controlat cu avansarea rapidă a tehnologiei. Criptarea bazată pe atribute face parte cele mai recente metode de securizarea a informației cu o multitudine de beneficii si variante. De la controlul accesului bazat pe atribute la căutari fără decriptări, ABE reprezintă o variantă flexibilă și rapidă de criptare care poate schimba industria. Totuși, în ultimii ani conceptul de criptografie post-quantum devine un viitor sigur, astfel apare o problemă majoră în felul cum sunt securizate toate serviciile disponibile azi. Majoritatea tipurile de criptare, inclusiv ABE, pot fi reduse la rezolvarea problemei factorizării. Asumând criptografia post-quantum, problema factorizării devine nepractică și nesigură. Aici intervin laticile și problema celui mai scurt vector dintr-o latice sau CSV pe scurt. Problema CSV este greu de rezolvat chiar și de către calculatoare cuantice, deoarece aceastea au un avantaj specific legat pe combinații mari de numere.

1.2 Definiții și Termeni Folosiți

Latici

O latice $L \subset \mathbb{R}^n$ este mulțimea tuturor combinațiilor liniare a vectoriilor bază $b_1, \ldots, b_n \in \mathbb{R}, L = \{\sum a_i b_i : a_i \in \mathbb{Z}\}$. În această lucrare voi lucra cu latici pe $mathbbZ$

Curbe Eliptice

O curbă eliptică este o funcție de forma: $E(a, b) = y^2 = x^3 + ax + b$

Criptarea bazată pe atribute

Un tip de criptare care se folosește de condiții exprimate ca predicate ce preiau multiple atribute la intrare, cu două dintre cele mai populare variante separate de situarea predicatului:

Key Policy (KP-ABE) Criptare ABE unde predicatul este situat pe cheie și atributele sunt dependente de informația criptată.

Ciphertext Policy (CP-ABE) Criptare ABE unde predicatul este situat pe criptotext și atributele sunt puse pe cheie.

Shortest Vector Problem(SVP)

În problema SVP, sunt date o bază a spațiului vectorial V și o normă N pentru laticea L, și trebuie găsit cel mai scurt vector de lungime diferită de zero în V, măsurat cu norma N, în latice. În varianta cu aproximare γ, trebuie găsit un vector de lungime aproximativ $\gamma * \lambda(L)$ pentru orice $\gamma \geq 1$.

Securitate

1.3 Utilitate ABE

1.4 Criptografia Cuantică

2 Attribute Based Encryption

2.1 Tipuri de ABE

2.2 CP-ABE vs KP-ABE

2.3 Mod de funcționare

• **Setup**
This is a randomized algorithm that takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.
• **Encryption**
This is a randomized algorithm that takes as input a message m, a set of attributes γ, and the public parameters PK. It outputs the ciphertext E. 12 Attribute-Based Encryption and Access Control
• **Key Generation**
This is a randomized algorithm that takes as input an access structure A, the master key MK, and the public parameters PK. It outputs a decryption key D.
• **Decryption**
This algorithm takes as input the ciphertext E that was encrypted under the set S of attributes, the decryption key D for access control structure A and the public parameters PK. It outputs the message M if S $\in$ A.