

Reticulados e Criptografia Pós-Quântica

Prof. Dr. Agnaldo José Ferrari
Departamento de Matemática, Unesp, Bauru

IV Workshop de Álgebra da UFG-CAC

27 de Maio de 2015



Tópicos



Tópicos

- Criptografia clássica - RSA



Tópicos

- Criptografia clássica - RSA
- Criptografia Pós-Quântica - Motivação



Tópicos

- Criptografia clássica - RSA
- Criptografia Pós-Quântica - Motivação
- Criptografia Pós-Quântica - Criptossistemas robustos



Tópicos

- Criptografia clássica - RSA
- Criptografia Pós-Quântica - Motivação
- Criptografia Pós-Quântica - Criptossistemas robustos
- Reticulados - Conceitos básicos



Tópicos

- Criptografia clássica - RSA
- Criptografia Pós-Quântica - Motivação
- Criptografia Pós-Quântica - Criptossistemas robustos
- Reticulados - Conceitos básicos
- Criptossistema baseado em reticulados



Tópicos

- Criptografia clássica - RSA
- Criptografia Pós-Quântica - Motivação
- Criptografia Pós-Quântica - Criptossistemas robustos
- Reticulados - Conceitos básicos
- Criptossistema baseado em reticulados
- Referências



Criptografia clássica - RSA

RSA é um algoritmo de criptografia de dados baseado em teoria dos números (Rivest, Shamir, Adleman), e envolve a geração de um par de chaves.

Criptografia clássica - RSA

RSA é um algoritmo de criptografia de dados baseado em teoria dos números (Rivest, Shamir, Adleman), e envolve a geração de um par de chaves.



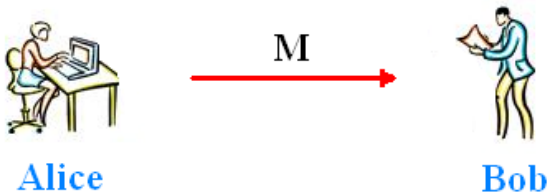
Alice



Bob

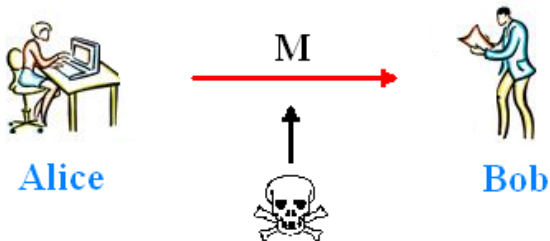
Criptografia clássica - RSA

RSA é um algoritmo de criptografia de dados baseado em teoria dos números (Rivest, Shamir, Adleman), e envolve a geração de um par de chaves.



Criptografia clássica - RSA

RSA é um algoritmo de criptografia de dados baseado em teoria dos números (Rivest, Shamir, Adleman), e envolve a geração de um par de chaves.



Criptografia clássica - RSA

Geração de chaves

Bob (destinatário) gera um par de chaves da seguinte maneira:

- 1- Escolhe de forma aleatória dois números primos p, q (grandes).
- 2- Computa $n = pq$.
- 3- Computa a função de Euler $\phi(n)$, onde

$$\phi(n) = \#\{a \in \mathbb{N} : 1 \leq a \leq n \text{ e } \text{mdc}(a, n) = 1\}$$

Para $n = pq$, temos $\phi(n) = (p - 1)(q - 1)$.

- 4- Escolhe um inteiro e tal que $1 < e < \phi(n)$ e $\text{mdc}(e, \phi(n)) = 1$.
- 5- Escolhe d tal que $de \equiv 1(\text{mod } \phi(n))$.

Chave Pública: (n, e)

Chave Privada: (n, d)

Criptografia clássica - RSA

Encriptação

Para transformar uma mensagem M , onde $0 < M < n$, numa mensagem cifrada c , Alice usa a chave pública (n, e) do destinatário (Bob) e computa

$$c \equiv M^e \pmod{n}$$

Criptografia clássica - RSA

Encriptação

Para transformar uma mensagem M , onde $0 < M < n$, numa mensagem cifrada c , Alice usa a chave pública (n, e) do destinatário (Bob) e computa

$$c \equiv M^e \pmod{n}$$

Deciptação

Para recuperar a mensagem M da mensagem cifrada c , o receptor (Bob) usa a sua chave privada (n, d) e computa

$$c^d \pmod{n} = M$$

Criptografia clássica - RSA

Segurança

Uma maneira de derivar a Chave Privada a partir da Chave pública é decompor n em fatores primos, e na computação clássica não existe algoritmo que faça isto em tempo polinomial.

Criptografia clássica - RSA

Segurança

Uma maneira de derivar a Chave Privada a partir da Chave pública é decompor n em fatores primos, e na computação clássica não existe algoritmo que faça isto em tempo polinomial.

- Em 1994, Peter Shor (Lab. AT&T Bell) publica um artigo intitulado "*Algorithms for Quantum Computation: Discrete Logarithms Factoring*", onde apresenta um algoritmo quântico para a fatoração de números inteiros.

Computador Quântico

No Computador Quântico a unidade básica de informação é o *qubit* (*quantum bit*). Um *qubit* pode assumir os valores 0 ou 1, assim como um *bit* (*binary digit*) convencional. A diferença é que o *qubit* pode assumir ambos os valores 0 e 1 ao mesmo tempo, aqui faz-se uso direto do Princípio da Superposição, observado na Mecânica Quântica.

Computador Quântico

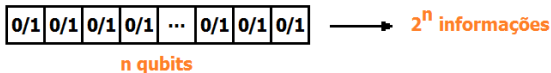
No Computador Quântico a unidade básica de informação é o *qubit* (*quantum bit*). Um *qubit* pode assumir os valores 0 ou 1, assim como um *bit* (*binary digit*) convencional. A diferença é que o *qubit* pode assumir ambos os valores 0 e 1 ao mesmo tempo, aqui faz-se uso direto do Princípio da Superposição, observado na Mecânica Quântica.

0/1	0/1	0/1	0/1	...	0/1	0/1	0/1
-----	-----	-----	-----	-----	-----	-----	-----

n qubits

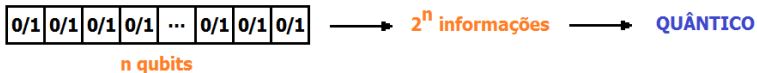
Computador Quântico

No Computador Quântico a unidade básica de informação é o *qubit* (*quantum bit*). Um *qubit* pode assumir os valores 0 ou 1, assim como um *bit* (*binary digit*) convencional. A diferença é que o *qubit* pode assumir ambos os valores 0 e 1 ao mesmo tempo, aqui faz-se uso direto do Princípio da Superposição, observado na Mecânica Quântica.



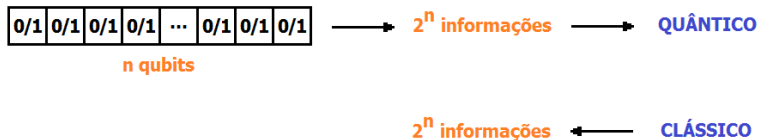
Computador Quântico

No Computador Quântico a unidade básica de informação é o *qubit* (*quantum bit*). Um *qubit* pode assumir os valores 0 ou 1, assim como um *bit* (*binary digit*) convencional. A diferença é que o *qubit* pode assumir ambos os valores 0 e 1 ao mesmo tempo, aqui faz-se uso direto do Princípio da Superposição, observado na Mecânica Quântica.



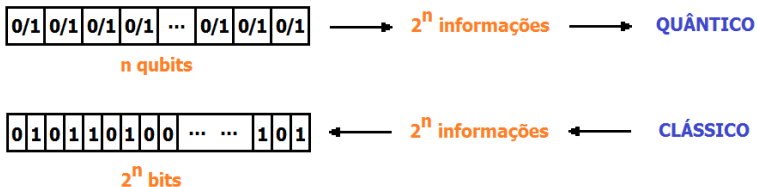
Computador Quântico

No Computador Quântico a unidade básica de informação é o *qubit* (*quantum bit*). Um *qubit* pode assumir os valores 0 ou 1, assim como um *bit* (*binary digit*) convencional. A diferença é que o *qubit* pode assumir ambos os valores 0 e 1 ao mesmo tempo, aqui faz-se uso direto do Princípio da Superposição, observado na Mecânica Quântica.



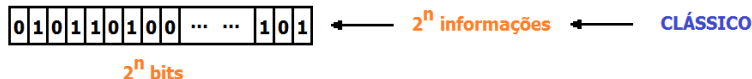
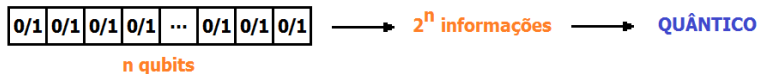
Computador Quântico

No Computador Quântico a unidade básica de informação é o *qubit* (*quantum bit*). Um *qubit* pode assumir os valores 0 ou 1, assim como um *bit* (*binary digit*) convencional. A diferença é que o *qubit* pode assumir ambos os valores 0 e 1 ao mesmo tempo, aqui faz-se uso direto do Princípio da Superposição, observado na Mecânica Quântica.



Computador Quântico

No Computador Quântico a unidade básica de informação é o *qubit* (*quantum bit*). Um *qubit* pode assumir os valores 0 ou 1, assim como um *bit* (*binary digit*) convencional. A diferença é que o *qubit* pode assumir ambos os valores 0 e 1 ao mesmo tempo, aqui faz-se uso direto do Princípio da Superposição, observado na Mecânica Quântica.



2 qubits = 4 bits
6 qubits = 64 bits
10 qubits = 1024 bits
20 qubits = 1048576 bits
40 qubits = 109950533632 bits



Computador Quântico

HISTÓRICO



HISTÓRICO

- (2001) I. Chung e N. Gershenfeld implementam o algoritmo de Shor na decomposição do número 15, numa máquina de 7 qubits.



HISTÓRICO

- (2001) I. Chung e N. Gershenfeld implementam o algoritmo de Shor na decomposição do número 15, numa máquina de 7 qubits.
- (2006) R. Schutzhold e G. Schaller implementam o algoritmo de Shor na decomposição do número 21.

HISTÓRICO

- (2001) I. Chung e N. Gershenfeld implementam o algoritmo de Shor na decomposição do número 15, numa máquina de 7 qubits.
- (2006) R. Schutzhold e G. Schaller implementam o algoritmo de Shor na decomposição do número 21.
- (2012) N. Xu, J. Zhu, D. Lu, X. Zhou, X. Peng e J. Du implementam o algoritmo de Shor na decomposição do número 143.



Tópicos

- Criptografia clássica - RSA
- Criptografia Pós-Quântica - Motivação
- Criptografia Pós-Quântica - Criptossistemas robustos
- Reticulados - Conceitos básicos
- Criptossistema baseado em reticulados
- Área de pesquisa
- Referências



Criptografia Pós-Quântica

Motivação: Ameaças à Criptografia Clássica (RSA)



Criptografia Pós-Quântica

Motivação: Ameaças à Criptografia Clássica (RSA)

- Algoritmo de Shor (Fatoração de números inteiros)



Motivação: Ameaças à Criptografia Clássica (RSA)

- Algoritmo de Shor (Fatoração de números inteiros)
 - Derivação da Chave Privada a partir da Chave Pública.



Motivação: Ameaças à Criptografia Clássica (RSA)

- Algoritmo de Shor (Fatoração de números inteiros)
 - Derivação da Chave Privada a partir da Chave Pública.
 - Decifração de textos cifrados.



Criptografia Pós-Quântica

Motivação: Ameaças à Criptografia Clássica (RSA)

- Algoritmo de Shor (Fatoração de números inteiros)
 - Derivação da Chave Privada a partir da Chave Pública.
 - Decifração de textos cifrados.

Pesquisa:



Criptografia Pós-Quântica

Motivação: Ameaças à Criptografia Clássica (RSA)

- Algoritmo de Shor (Fatoração de números inteiros)
 - Derivação da Chave Privada a partir da Chave Pública.
 - Decifração de textos cifrados.

Pesquisa: Criptosistemas resistentes a algoritmos quânticos.

Tópicos

- Criptografia clássica - RSA
- Criptografia Pós-Quântica - Motivação
- Criptografia Pós-Quântica - Criptosistemas robustos
- Reticulados - Conceitos básicos
- Criptosistema baseado em reticulados
- Área de pesquisa
- Referências



Criptossistemas robustos

Objetivos: Desenvolver sistemas criptográficos baseados em problemas intratáveis num computador quântico.



Criptossistemas robustos

Objetivos: Desenvolver sistemas criptográficos baseados em problemas intratáveis num computador quântico.

Fontes de Problemas Intratáveis



Criptossistemas robustos

Objetivos: Desenvolver sistemas criptográficos baseados em problemas intratáveis num computador quântico.

Fontes de Problemas Intratáveis

- Códigos Corretores de Erros.

Criptossistemas robustos

Objetivos: Desenvolver sistemas criptográficos baseados em problemas intratáveis num computador quântico.

Fontes de Problemas Intratáveis

- Códigos Corretores de Erros.
- Funções Hash.

Criptossistemas robustos

Objetivos: Desenvolver sistemas criptográficos baseados em problemas intratáveis num computador quântico.

Fontes de Problemas Intratáveis

- Códigos Corretores de Erros.
- Funções Hash.
- Reticulados.



Tópicos

- Criptografia clássica - RSA
- Criptografia Pós-Quântica - Motivação
- Criptografia Pós-Quântica - Criptossistemas robustos
- Reticulados - Conceitos básicos
- Criptossistema baseado em reticulados
- Área de pesquisa
- Referências

Definição

Seja $\{v_1, v_2, \dots, v_m\}$ um conjunto de vetores linearmente independentes no espaço vetorial $\mathbb{R}^n$, tal que $m \leq n$. O conjunto

$$\Lambda = \left\{ \sum_{i=1}^m \alpha_i v_i : \alpha_i \in \mathbb{Z} \right\}.$$

é chamado um **reticulado** de posto m , e o conjunto $\{v_1, v_2, \dots, v_m\}$ é chamado uma **base** do reticulado Λ .

Definição

Seja $\{v_1, v_2, \dots, v_m\}$ uma base do reticulado Λ . Se $v_i = (v_{i1}, v_{i2}, \dots, v_{in})$, para $i = 1, \dots, m$, então a matriz

$$M = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ & & \ddots & \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{pmatrix}$$

é chamada uma **matriz geradora** para o reticulado Λ .

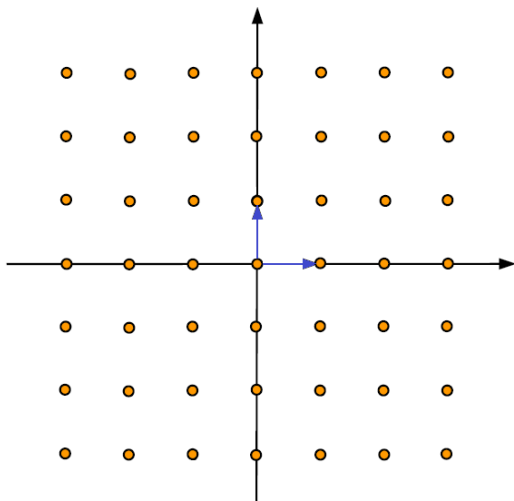
Definição

Seja M uma matriz geradora para o reticulado Λ . Então

$$\Lambda = \{xM \mid x \in \mathbb{Z}^m\}$$



Reticulado $\mathbb{Z}^2$



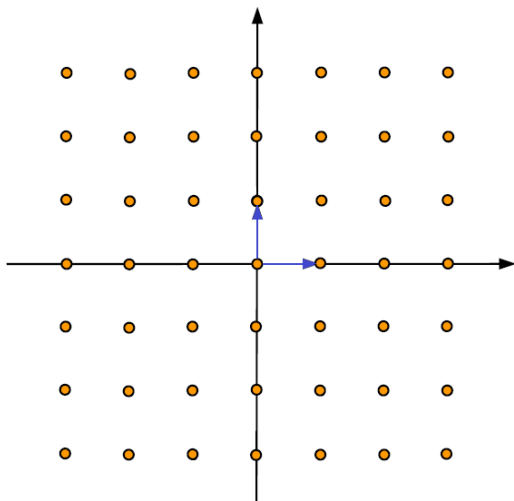
$$B = \{(1, 0), (0, 1)\}$$

Observação

A matriz geradora de um reticulado não é única, dado um reticulado Λ gerado por uma base B , uma base C será base deste reticulado se, e somente se, a respectiva matriz mudança de base possui entradas inteiras e determinante ± 1 .



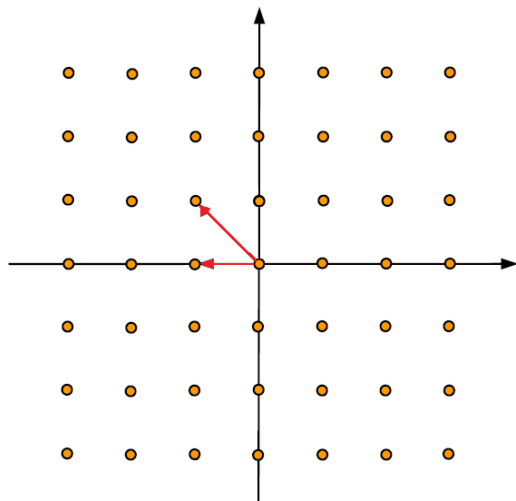
Reticulado $\mathbb{Z}^2$



$$B = \{(1, 0), (0, 1)\}$$



Reticulado $\mathbb{Z}^2$



$$B = \{(-1, 0), (-1, -1)\}$$

Definição

Um **empacotamento esférico** no $\mathbb{R}^n$ é uma distribuição de esferas de mesmo raio de forma que a intersecção de quaisquer duas esferas tenha no máximo um ponto.

Definição

Um **empacotamento esférico** no $\mathbb{R}^n$ é uma distribuição de esferas de mesmo raio de forma que a intersecção de quaisquer duas esferas tenha no máximo um ponto.

Definição

Um **empacotamento reticulado** é um empacotamento em que o conjunto dos centros das esferas formam um reticulado Λ do $\mathbb{R}^n$.

Definição

Dado um empacotamento no $\mathbb{R}^n$ associado a um reticulado Λ com base $B = \{v_1, \dots, v_n\}$, definimos a sua **densidade de empacotamento** como sendo a proporção do espaço $\mathbb{R}^n$ coberta pela união das esferas.

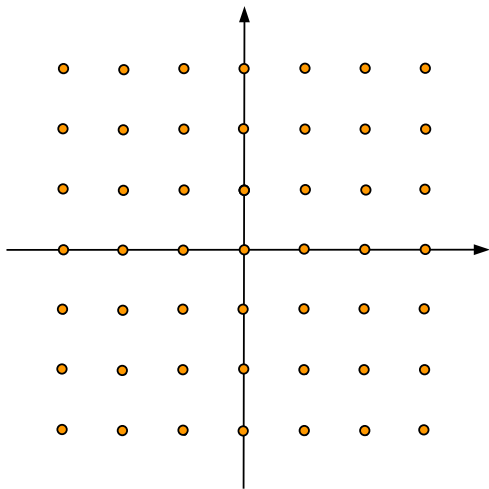
Definição

Dado um empacotamento no $\mathbb{R}^n$ associado a um reticulado Λ com base $B = \{v_1, \dots, v_n\}$, definimos a sua **densidade de empacotamento** como sendo a proporção do espaço $\mathbb{R}^n$ coberta pela união das esferas.

Definição

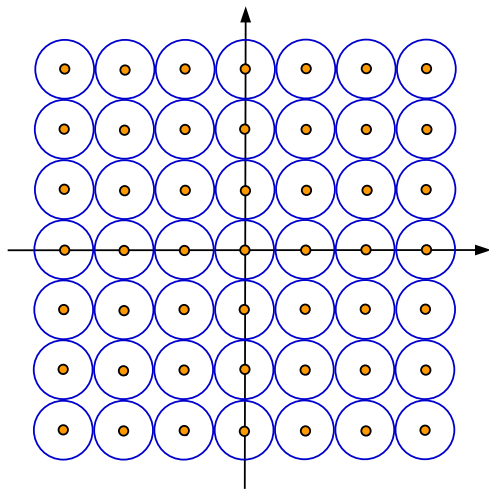
O **raio de empacotamento** de um reticulado Λ é o raio de qualquer uma das esferas do empacotamento.

Reticulado $\mathbb{Z}^2$



$$B = \{(1, 0), (0, 1)\}$$

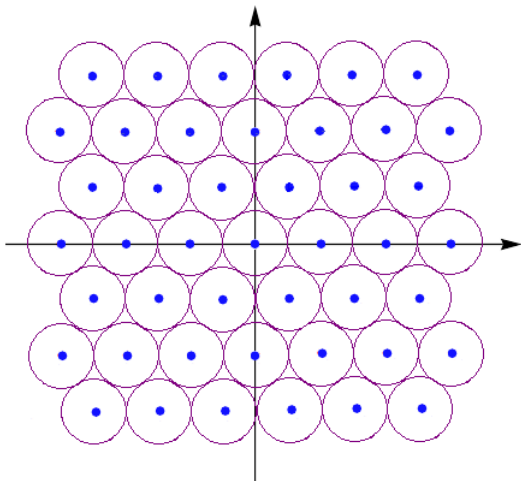
Reticulado $\mathbb{Z}^2$



$$B = \{(1, 0), (0, 1)\}$$

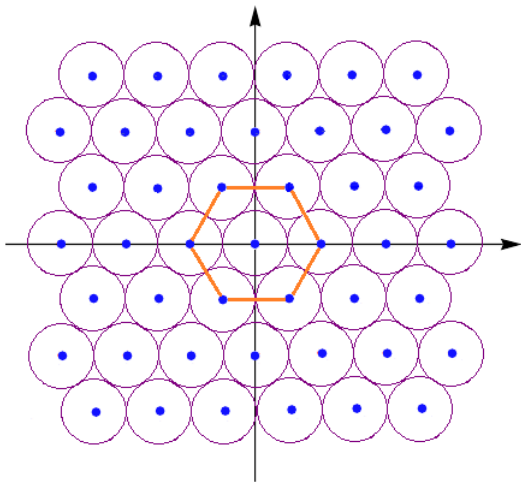


Reticulado Hexagonal



$$B = \{(1, 0), (1/2, \sqrt{3}/2)\}$$

Reticulado Hexagonal



$$B = \{(1, 0), (1/2, \sqrt{3}/2)\}$$

Definição

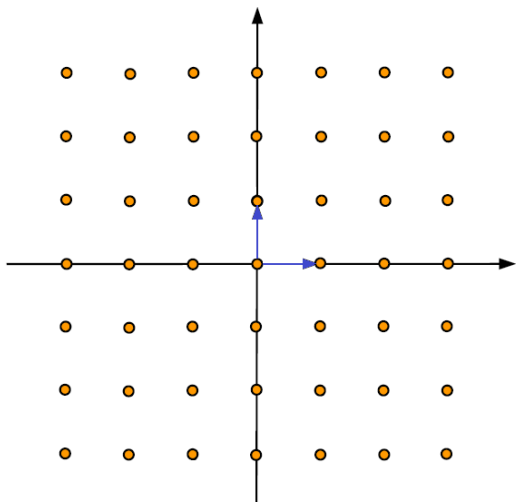
Seja M uma matriz geradora de um reticulado Λ . Um **sub-reticulado** de Λ é dado por

$$\Lambda' = \{xBM; x \in \mathbb{Z}^n\}$$

onde B é uma matriz de ordem n com entradas inteiras.

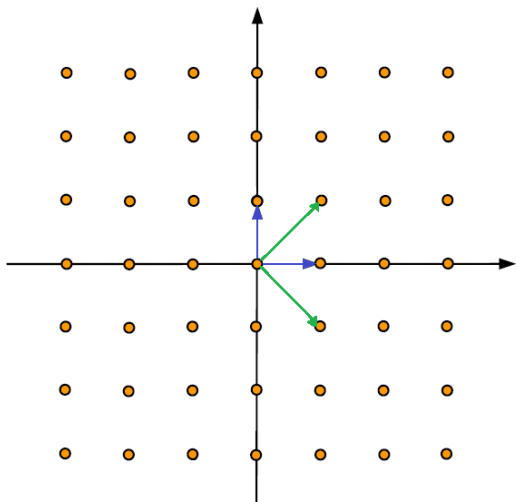


Reticulado $\mathbb{Z}^2$



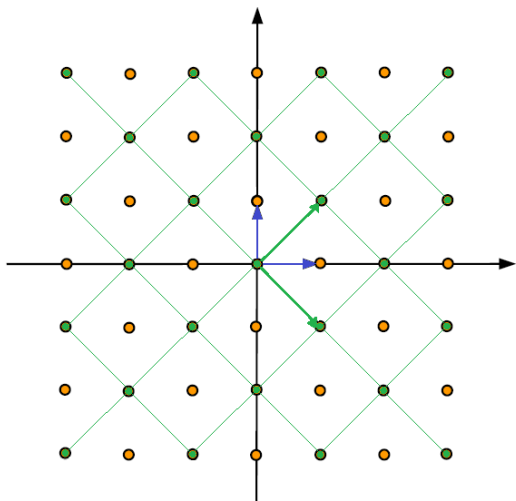
$$M = \{(1, 0), (0, 1)\}$$

Reticulado $\mathbb{Z}^2$



$$B = \{(1, 1), (1, -1)\}$$

Reticulado $\mathbb{Z}^2$



$$B = \{(1,1), (1,-1)\}$$



Reticulados

Problemas intratáveis em reticulados

Problemas intratáveis em reticulados

Shortest Vector Problem - SVP

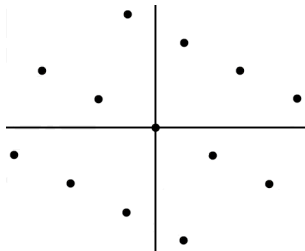
Dada uma base $B \in \mathbb{Z}^{m \times n}$, encontrar um vetor xB ($x \in \mathbb{Z}^m$) não nulo no reticulado gerado por B tal que

$$\|xB\| \leq \|yB\|, \forall y \in \mathbb{Z}^m - \{0\}.$$

Problemas intratáveis em reticulados

Shortest Vector Problem - SVP

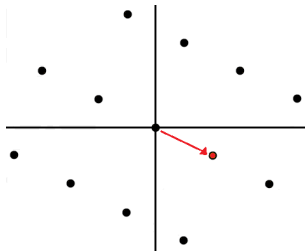
Dada uma base $B \in \mathbb{Z}^{m \times n}$, encontrar um vetor xB ($x \in \mathbb{Z}^m$) não nulo no reticulado gerado por B tal que $\|xB\| \leq \|yB\|, \forall y \in \mathbb{Z}^m - \{0\}$.



Problemas intratáveis em reticulados

Shortest Vector Problem - SVP

Dada uma base $B \in \mathbb{Z}^{m \times n}$, encontrar um vetor xB ($x \in \mathbb{Z}^m$) não nulo no reticulado gerado por B tal que $\|xB\| \leq \|yB\|, \forall y \in \mathbb{Z}^m - \{0\}$.





Reticulados

Problemas intratáveis em reticulados

Problemas intratáveis em reticulados

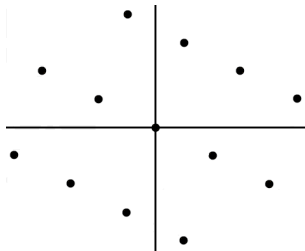
Closest Vector Problem - CVP

Dada uma base $B \in \mathbb{Z}^{m \times n}$ para um reticulado e um vetor-alvo $w \in \mathbb{R}^n$, encontrar um vetor xB ($x \in \mathbb{Z}^m$) mais próximo de w no reticulado gerado por B , isto é, $\|xB - w\| \leq \|yB - w\|, \forall y \in \mathbb{Z}^m$.

Problemas intratáveis em reticulados

Closest Vector Problem - CVP

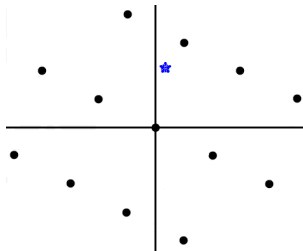
Dada uma base $B \in \mathbb{Z}^{m \times n}$ para um reticulado e um vetor-alvo $w \in \mathbb{R}^n$, encontrar um vetor xB ($x \in \mathbb{Z}^m$) mais próximo de w no reticulado gerado por B , isto é, $\|xB - w\| \leq \|yB - w\|, \forall y \in \mathbb{Z}^m$.



Problemas intratáveis em reticulados

Closest Vector Problem - CVP

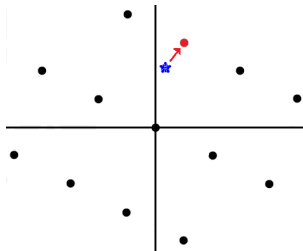
Dada uma base $B \in \mathbb{Z}^{m \times n}$ para um reticulado e um vetor-alvo $w \in \mathbb{R}^n$, encontrar um vetor xB ($x \in \mathbb{Z}^m$) mais próximo de w no reticulado gerado por B , isto é, $\|xB - w\| \leq \|yB - w\|, \forall y \in \mathbb{Z}^m$.



Problemas intratáveis em reticulados

Closest Vector Problem - CVP

Dada uma base $B \in \mathbb{Z}^{m \times n}$ para um reticulado e um vetor-alvo $w \in \mathbb{R}^n$, encontrar um vetor xB ($x \in \mathbb{Z}^m$) mais próximo de w no reticulado gerado por B , isto é, $\|xB - w\| \leq \|yB - w\|, \forall y \in \mathbb{Z}^m$.





Tópicos

- Criptografia clássica - RSA
- Criptografia Pós-Quântica - Motivação
- Criptografia Pós-Quântica - Criptossistemas robustos
- Reticulados - Conceitos básicos
- Criptossistema baseado em reticulados
- Área de pesquisa
- Referências



Criptossistema baseado em reticulados



Alice



Bob

Criptossistema baseado em reticulados

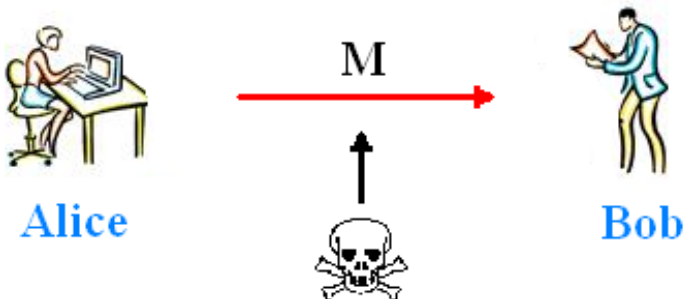


Alice



Bob

Criptossistema baseado em reticulados



Criptossistema baseado em reticulados

Geração de chaves

Bob (destinatário) gera um par de chaves da seguinte maneira:

1— Escolhe um reticulado Λ com matriz geradora M , $n \times n$, $n \geq 500$, raio de empacotamento r , na qual ele conhece um algoritmo eficiente de decodificação.

2— Escolhe uma matriz S , matriz randômica inversível com entradas inteiras.

3— Computa $A = SM$.

Chave Pública: (A, r)

Chave Privada: (S^{-1}, M^{-1})

Criptossistema baseado em reticulados

Encriptação

Alice deseja enviar uma mensagem m para Bob usando a **Chave Pública** (A, r) , e segue os seguintes passos:

1— Codifica a mensagem m como um vetor

$$x = (x_1, x_2, \dots, x_n), x_j \in \mathbb{Z}.$$

2— Computa um vetor $c' = xA$.

3— Computa um vetor erro e tal que $\|e\| < r$.

4— Envia o texto cifrado $c = c' + e = xA + e$.

5— De posse de c , um invasor não consegue descobrir c' (CVP).

Criptossistema baseado em reticulados

Encrytação

Alice deseja enviar uma mensagem m para Bob usando a **Chave Pública** (A, r) , e segue os seguintes passos:

1— Codifica a mensagem m como um vetor

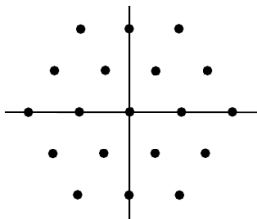
$$x = (x_1, x_2, \dots, x_n), x_j \in \mathbb{Z}.$$

2— Computa um vetor $c' = xA$.

3— Computa um vetor erro e tal que $\|e\| < r$.

4— Envia o texto cifrado $c = c' + e = xA + e$.

5— De posse de c , um invasor não consegue descobrir c' (CVP).



Criptossistema baseado em reticulados

Encrytação

Alice deseja enviar uma mensagem m para Bob usando a **Chave Pública** (A, r) , e segue os seguintes passos:

1— Codifica a mensagem m como um vetor

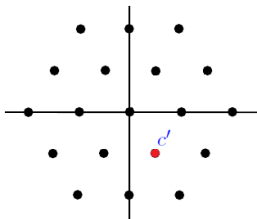
$$x = (x_1, x_2, \dots, x_n), x_j \in \mathbb{Z}.$$

2— Computa um vetor $c' = xA$.

3— Computa um vetor erro e tal que $\|e\| < r$.

4— Envia o texto cifrado $c = c' + e = xA + e$.

5— De posse de c , um invasor não consegue descobrir c' (CVP).



Criptossistema baseado em reticulados

Encrytação

Alice deseja enviar uma mensagem m para Bob usando a **Chave Pública** (A, r) , e segue os seguintes passos:

1— Codifica a mensagem m como um vetor

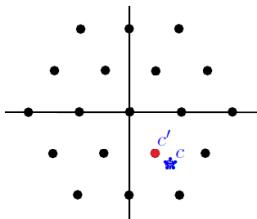
$$x = (x_1, x_2, \dots, x_n), x_j \in \mathbb{Z}.$$

2— Computa um vetor $c' = xA$.

3— Computa um vetor erro e tal que $\|e\| < r$.

4— Envia o texto cifrado $c = c' + e = xA + e$.

5— De posse de c , um invasor não consegue descobrir c' (CVP).



Criptografia baseada em reticulados

Deciptação

Bob recebe o texto cifrado c e segue os seguintes passos:

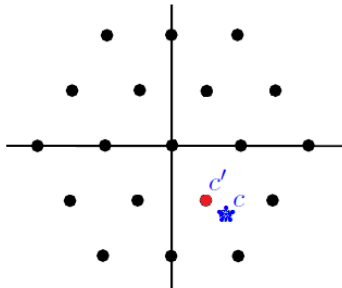
- 1— Usa o algoritmo de decodificação para o reticulado Λ para decodificar $c = xSM + e = \hat{x}M + e$ em $\hat{c} = \hat{x}M$, onde $\hat{x} = xS$.
- 2— Usa a chave privada e faz $\hat{c}M^{-1}S^{-1} = xSM M^{-1}S^{-1} = x$.

Criptografia baseada em reticulados

Deciptação

Bob recebe o texto cifrado c e segue os seguintes passos:

- 1— Usa o algoritmo de decodificação para o reticulado Λ para decodificar $c = xSM + e = \hat{x}M + e$ em $\hat{c} = \hat{x}M$, onde $\hat{x} = xS$.
- 2— Usa a chave privada e faz $\hat{c}M^{-1}S^{-1} = xSM M^{-1}S^{-1} = x$.



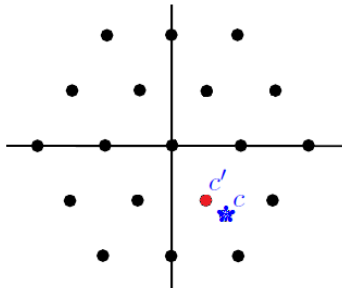
Matriz A

Criptografia baseada em reticulados

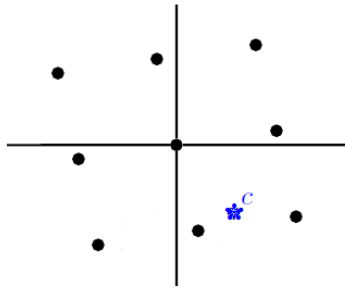
Deciptação

Bob recebe o texto cifrado c e segue os seguintes passos:

- 1— Usa o algoritmo de decodificação para o reticulado Λ para decodificar $c = xSM + e = \hat{x}M + e$ em $\hat{c} = \hat{x}M$, onde $\hat{x} = xS$.
- 2— Usa a chave privada e faz $\hat{c}M^{-1}S^{-1} = xSM M^{-1}S^{-1} = x$.



Matriz A



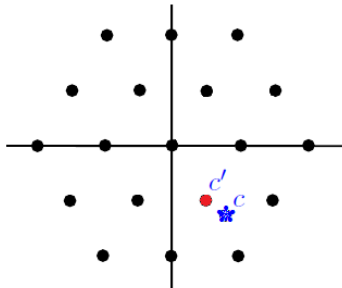
Matriz M

Criptografia baseada em reticulados

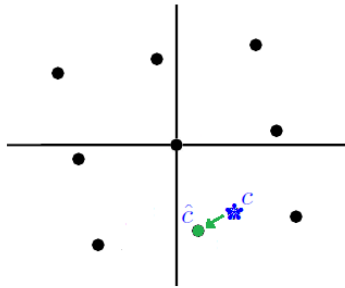
Deciptação

Bob recebe o texto cifrado c e segue os seguintes passos:

- 1— Usa o algoritmo de decodificação para o reticulado Λ para decodificar $c = xSM + e = \hat{x}M + e$ em $\hat{c} = \hat{x}M$, onde $\hat{x} = xS$.
- 2— Usa a chave privada e faz $\hat{c}M^{-1}S^{-1} = xSM M^{-1}S^{-1} = x$.



Matriz A



Matriz M



Criptografia baseada em reticulados

Dificuldades

- 1- Reticulado em dimensão alta com algoritmo de decodificação eficiente.



Criptografia baseada em reticulados

Dificuldades

1- Reticulado em dimensão alta com algoritmo de decodificação eficiente.

- Reticulados gerados por códigos corretores de erros.



Criptografia baseada em reticulados

Dificuldades

1- Reticulado em dimensão alta com algoritmo de decodificação eficiente.

- Reticulados gerados por códigos corretores de erros.
- Treliça minimal de reticulados.



Criptografia baseada em reticulados

Dificuldades

2- Tamanho das chaves: A , S^{-1} , M^{-1} .

Dificuldades

2- Tamanho das chaves: A , S^{-1} , M^{-1} .

- Matrizes geradoras triangulares (Forma Normal de Hermite).

Criptografia baseada em reticulados

Dificuldades

2- Tamanho das chaves: A , S^{-1} , M^{-1} .

- Matrizes geradoras triangulares (Forma Normal de Hermite).
- Matrizes geradores de reticulados cíclicos.



Criptografia baseada em reticulados

Matrizes geradoras triangulares (Forma Normal de Hermite)

Criptografia baseada em reticulados

Matrizes geradoras triangulares (Forma Normal de Hermite)

Forma Normal de Hermite

Dada uma matriz M com entradas inteiras, existe uma matriz unimodular U tal que $A = UM$, com A triangular superior e entradas inteiras.

Criptografia baseada em reticulados

Matrizes geradoras triangulares (Forma Normal de Hermite)

Forma Normal de Hermite

Dada uma matriz M com entradas inteiras, existe uma matriz unimodular U tal que $A = UM$, com A triangular superior e entradas inteiras.

Exemplo

$$\underbrace{\begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 6 \end{pmatrix}}_A = \underbrace{\begin{pmatrix} 4 & -4 & -2 & -1 \\ 3 & -3 & -2 & -1 \\ 5 & -5 & -3 & -1 \\ 6 & -5 & -2 & -1 \end{pmatrix}}_U \cdot \underbrace{\begin{pmatrix} -2 & 1 & -1 & 3 \\ -3 & 2 & -1 & 2 \\ 2 & -1 & -1 & 1 \\ -1 & -2 & 1 & 0 \end{pmatrix}}_M$$

Criptografia baseada em reticulados

Matrizes geradoras triangulares (Forma Normal de Hermite)

Forma Normal de Hermite

Dada uma matriz M com entradas inteiras, existe uma matriz unimodular U tal que $A = UM$, com A triangular superior e entradas inteiras.

Exemplo

$$\underbrace{\begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 6 \end{pmatrix}}_A = \underbrace{\begin{pmatrix} 4 & -4 & -2 & -1 \\ 3 & -3 & -2 & -1 \\ 5 & -5 & -3 & -1 \\ 6 & -5 & -2 & -1 \end{pmatrix}}_U \cdot \underbrace{\begin{pmatrix} -2 & 1 & -1 & 3 \\ -3 & 2 & -1 & 2 \\ 2 & -1 & -1 & 1 \\ -1 & -2 & 1 & 0 \end{pmatrix}}_M$$



Criptografia baseada em reticulados

Matrizes geradores de reticulados cíclicos

Reticulados cíclicos

Um reticulado Λ é dito **cíclico** se dado um vetor $(a_1, a_2, \dots, a_n) \in \Lambda$, então $(a_2, a_3, \dots, a_n, a_1) \in \Lambda$.

Criptografia baseada em reticulados

Matrizes geradores de reticulados cíclicos

Reticulados cíclicos

Um reticulado Λ é dito **cíclico** se dado um vetor $(a_1, a_2, \dots, a_n) \in \Lambda$, então $(a_2, a_3, \dots, a_n, a_1) \in \Lambda$.

Exemplo

$$\underbrace{\begin{pmatrix} 1 & 0 & 3 & -14 \\ 0 & 1 & 2 & 7 \\ 0 & 0 & 4 & -4 \\ 0 & 0 & 0 & 38 \end{pmatrix}}_A = \underbrace{\begin{pmatrix} -4 & 4 & -1 & 0 \\ 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 11 & -9 & 1 & 1 \end{pmatrix}}_U \cdot \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{pmatrix}}_M$$

Criptografia baseada em reticulados

Matrizes geradores de reticulados cíclicos

Reticulados cíclicos

Um reticulado Λ é dito **cíclico** se dado um vetor $(a_1, a_2, \dots, a_n) \in \Lambda$, então $(a_2, a_3, \dots, a_n, a_1) \in \Lambda$.

Exemplo

$$\underbrace{\begin{pmatrix} 1 & 0 & 3 & -14 \\ 0 & 1 & 2 & 7 \\ 0 & 0 & 4 & -4 \\ 0 & 0 & 0 & 38 \end{pmatrix}}_A = \underbrace{\begin{pmatrix} -4 & 4 & -1 & 0 \\ 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 11 & -9 & 1 & 1 \end{pmatrix}}_U \cdot \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{pmatrix}}_M$$

Referencias

-  D. J. Bernstein, J. Buchmann, E. Dahmen, *Post-Quantum Cryptography, Hardcover, 2009.*
-  J. H. Conway, N. J. A. Sloane, *Sphere Packings, Lattices and Groups, Springer-Verlag, New York, 1998.*
-  G. D. Forney Jr., *Final report on a coding system design for advanced solar missions, Contract NAS2-3637, NASA Ames Research Center. Moffet Field, CA, Dec 1967.*
-  A.H. Banihashemi and I.F. Blake, *Trellis complexity and minimal trellis of lattices, IEEE Trans. Inform. Theory, vol IT-44, n 5, pp. 1829-1847, Sep. 1998.*