RETICULADOS

Problemas Hard e Técnicas Criptográficas

31 Janeiro 2013

PERTINÊNCIA

Criptografia Assimétrica

Criptografia Simétrica → Criptografia Assimétrica

Chave Comum

Chave Pública

Chave Privada

Derivar a chave privada a partir da chave pública é tão difícil quanto inverter uma função unidireccional.

PROBLEMAS HARD

Em Reticulados

VECTORES CURTOS

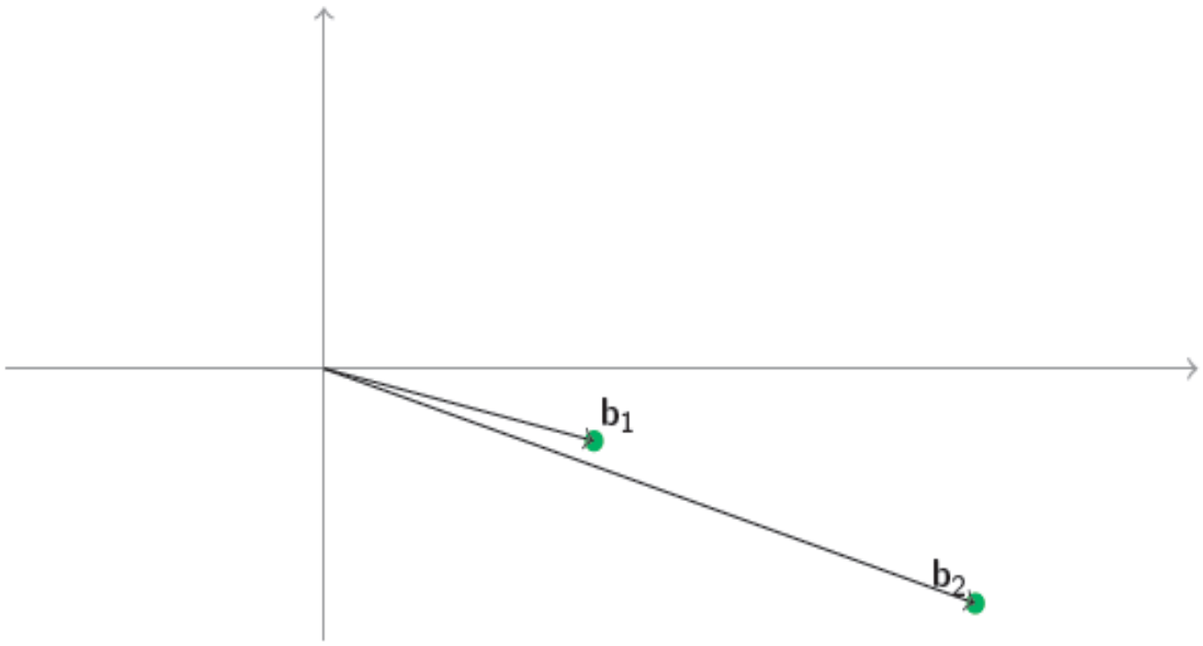
VECTORES PRÓXIMOS

PROBLEMAS HARD

Em Reticulados

VECTORES CURTOS

VECTORES PRÓXIMOS



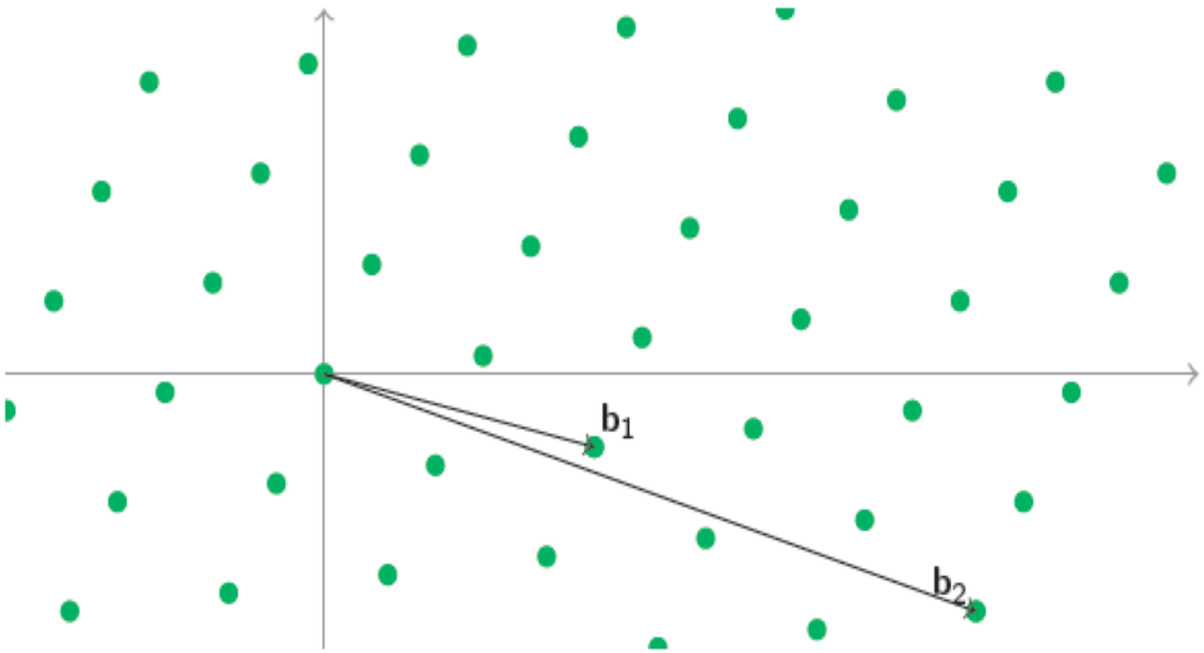
Shortest Vector Problem (SVP)

PROBLEMAS HARD

Em Reticulados

VECTORES CURTOS

VECTORES PRÓXIMOS



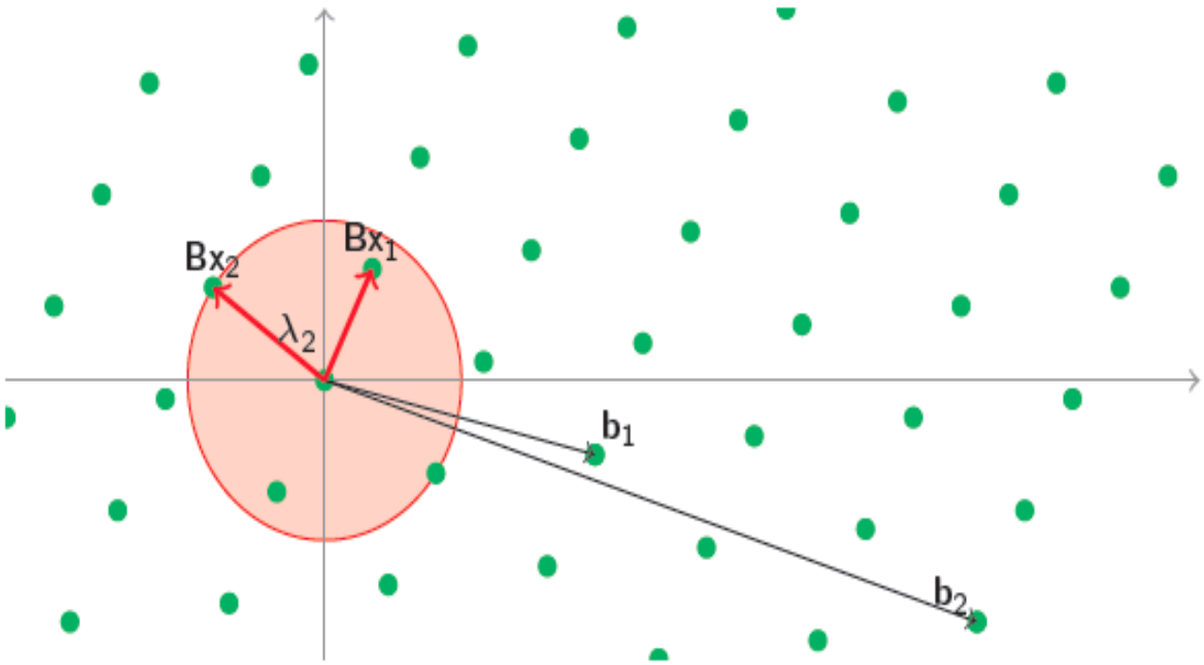
Shortest Vector Problem (SVP)

PROBLEMAS HARD

Em Reticulados

VECTORES CURTOS

VECTORES PRÓXIMOS



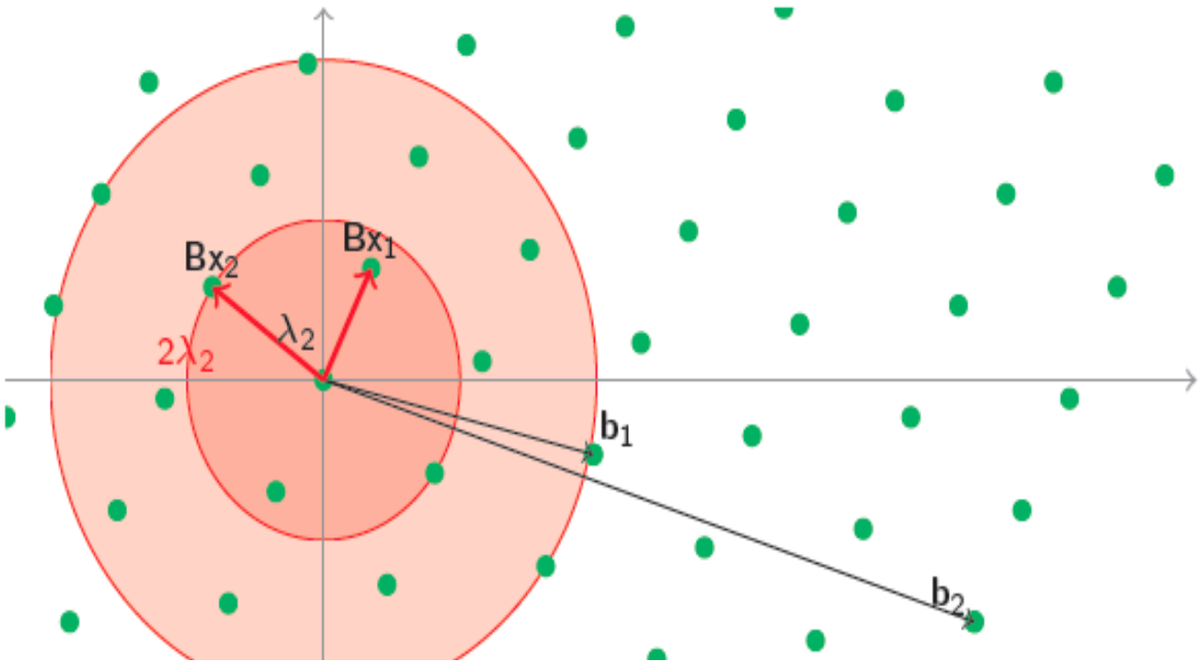
Shortest Vector Problem (SVP)

PROBLEMAS HARD

Em Reticulados

VECTORES CURTOS

VECTORES PRÓXIMOS



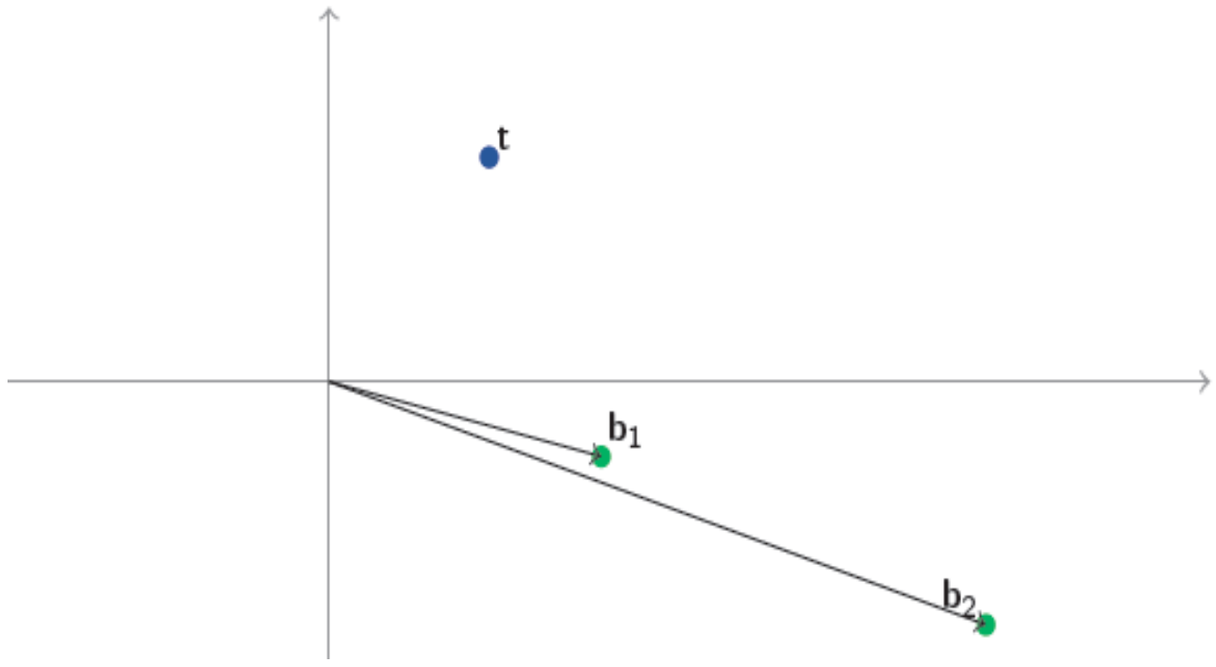
Approximate Shortest Vector Problem (SVP$_\gamma$)

PROBLEMAS HARD

Em Reticulados

VECTORES CURTOS

VECTORES PRÓXIMOS



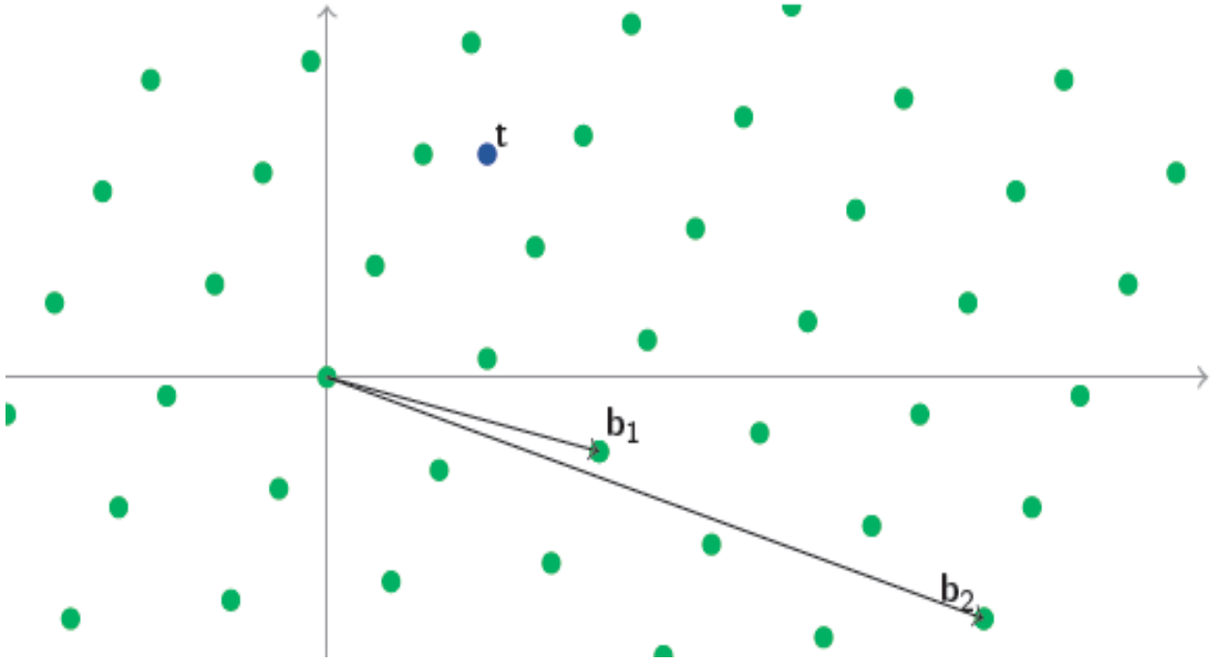
Closest Vector Problem (CVP)

PROBLEMAS HARD

Em Reticulados

VECTORES CURTOS

VECTORES PRÓXIMOS



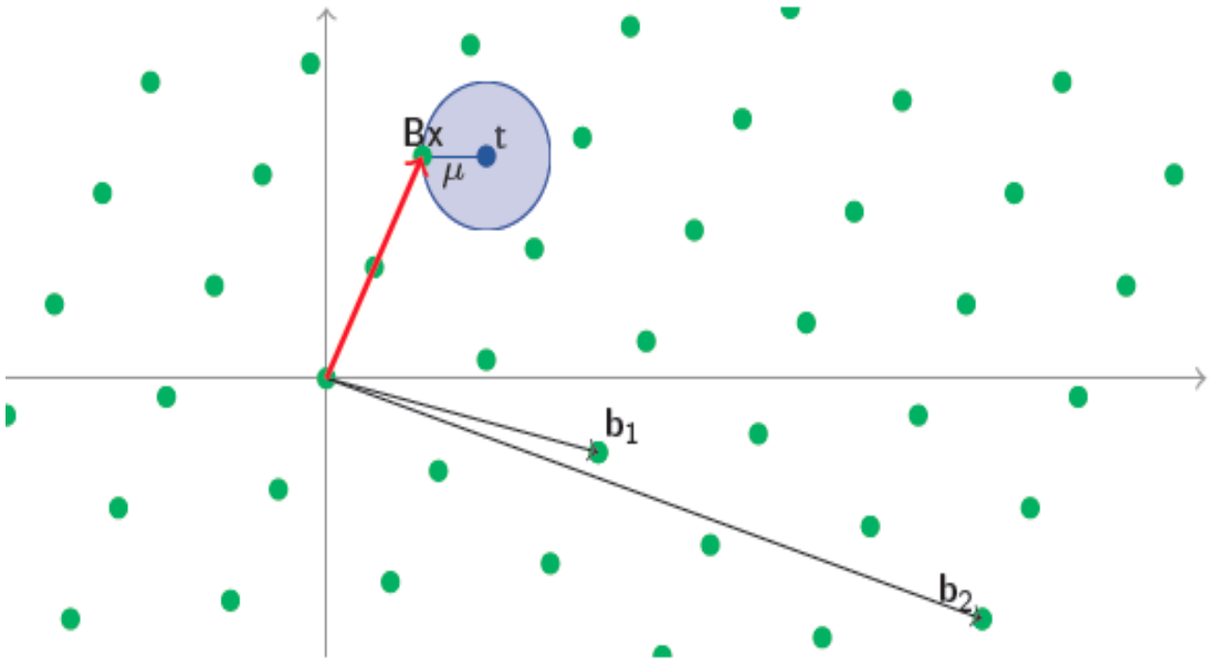
Closest Vector Problem (CVP)

PROBLEMAS HARD

Em Reticulados

VECTORES CURTOS

VECTORES PRÓXIMOS



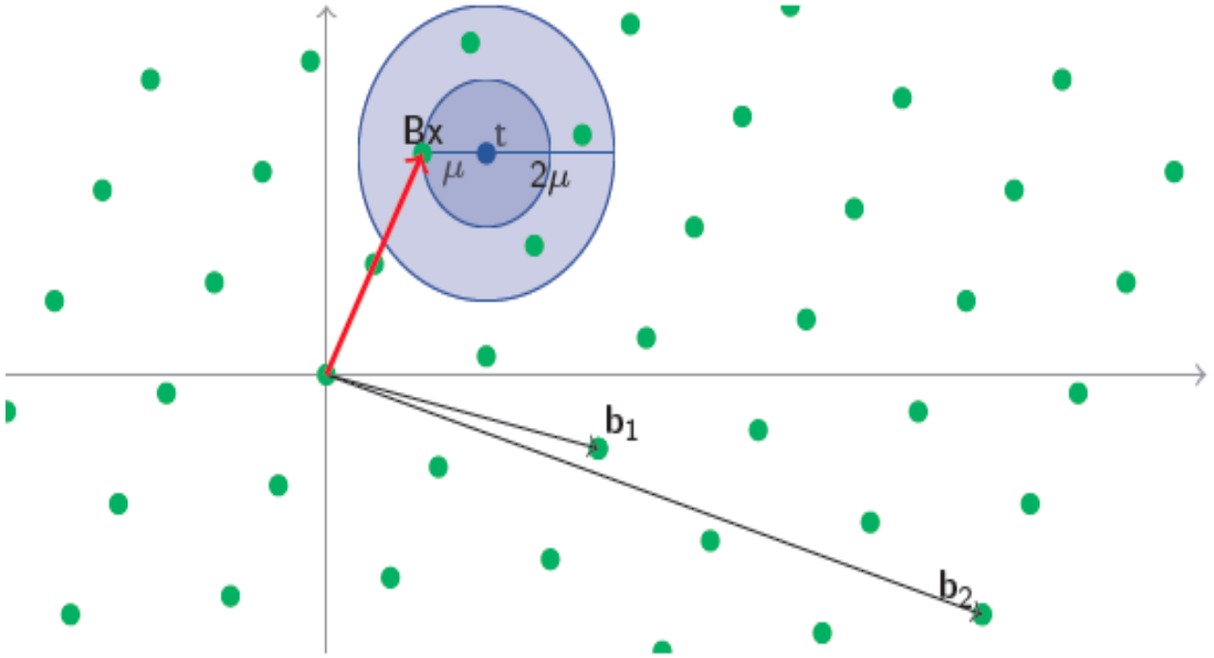
Closest Vector Problem (CVP)

PROBLEMAS HARD

Em Reticulados

VECTORES CURTOS

VECTORES PRÓXIMOS



Approximate Closest Vector Problem (CVPγ)

TÉCNICAS CRIPTOGRÁFICAS

Esquemas de Criptografia de Chave Pública

EMISSOR

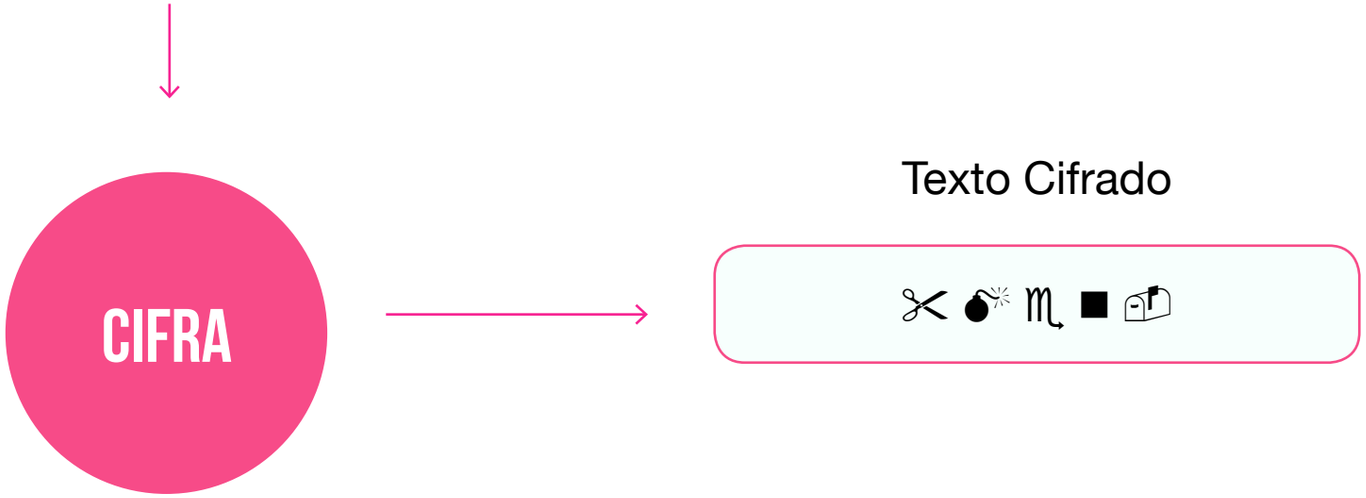
"Mensagem"

TÉCNICAS CRIPTOGRÁFICAS

Esquemas de Criptografia de Chave Pública

EMISSOR

"Mensagem"



Chave Pública

TÉCNICAS CRIPTOGRÁFICAS

Esquemas de Criptografia de Chave Pública

EMISSOR

"Mensagem"

RECEPTOR

"Mensagem"

CIFRA

Texto Cifrado

DECIFRA

Chave Pública

Chave Privada

ESQUEMAS DE CRIPTOGRAFIA DE CHAVE PÚBLICA

Criptosistema de Ajtai-Dwork

 Chave Privada	Vector $\mathbf{u}$ escolhido aleatoriamente da esfera $\mathcal{S}_n$ $$\mathcal{S}_n = \{x \in \mathbb{R}^n : \|x\| \leqslant n^{-c}\}$$
 Chave Pública	$n+m$ vectores $\mathbf{w_1}, ..., \mathbf{w_n}, \mathbf{v_1}, ..., \mathbf{v_m}$ retirados de $\mathcal{H}_u$

ESQUEMAS DE CRIPTOGRAFIA DE CHAVE PÚBLICA

Criptosistema de Ajtai-Dwork

Chave Pública

$n + m$ vectores $\mathbf{w_1}, \ldots, \mathbf{w_n}, \mathbf{v_1}, \ldots, \mathbf{v_m}$ retirados de $\mathcal{H}_u$

$$\mathbf{m} = (1,0,1,1,1,1,1,0,1) \longrightarrow$$

CIFRA

Bit a Bit

$$\mathbf{c} = ((9.986,3.746,-2.791),(1.365,1.417,-3.108),(-16.955,-1.992,9.227),$$
$$(-5.223,-1.139,1.278),(5.590,-3.151,-6.728),(-7.319,9.134,17.364),$$
$$(-3.014,3.752,2.509),(-9.874,4.964,7.645),(-9.039,4.727,5.035)).$$

ESQUEMAS DE CRIPTOGRAFIA DE CHAVE PÚBLICA

Criptosistema de Ajtai-Dwork

Chave Privada

Vector $\mathbf{u}$ escolhido aleatoriamente da esfera $\mathcal{S}_n$

$$\mathcal{S}_n = \{x \in \mathbb{R}^n : \|x\| \leqslant n^{-c}\}$$

DECIFRA

Bit a Bit

$\mathbf{c_i}$	$\langle \mathbf{c_i}, \mathbf{u} \rangle$
$\mathbf{c_1}$	3.994
$\mathbf{c_2}$	1.000
$\mathbf{c_3}$	-11.08
$\mathbf{c_4}$	2.519
$\mathbf{c_5}$	7.316
$\mathbf{c_6}$	-15.76
$\mathbf{c_7}$	-4.777
$\mathbf{c_8}$	-10.99
$\mathbf{c_9}$	-9.458

$\mathbf{m'} = (0,0,0,1,0,0,0,0,1)$ X

ESQUEMAS DE CRIPTOGRAFIA DE CHAVE PÚBLICA

Criptosistema GGH

 Chave Privada	Matriz secreta $\mathcal{R}$
 Chave Pública	Matriz $\mathcal{B}$ gerada aleatoriamente a partir de $\mathcal{R}$

ESQUEMAS DE CRIPTOGRAFIA DE CHAVE PÚBLICA

Criptosistema GGH

Chave Pública

Matriz $\mathcal{B}$ gerada aleatoriamente a partir de $\mathcal{R}$

$\mathbf{m} = (-2,0,-4,-1)$ ⟶ CIFRA

Vector de Erro

$\mathbf{c} = \mathcal{B}\mathbf{m} + \mathbf{e} = (-3,1,-3,-1438)$

ESQUEMAS DE CRIPTOGRAFIA DE CHAVE PÚBLICA

Criptosistema GGH

Chave Privada

Matriz secreta $\mathcal{R}$

DECIFRA

CVP

Método de Babai

$$\mathbf{m} = (\text{-}2,0,\text{-}4,\text{-}1)$$

ESQUEMAS DE CRIPTOGRAFIA DE CHAVE PÚBLICA

Criptosistema NTRU

Chave Privada

Dados dois polinómios f e g, considerar a multiplicação matricial $[\mathcal{C}^*\mathbf{f}]\mathbf{g}$ equivalente ao produto da convolução dos polinómios $f * g$. Sendo $\mathbf{f}$ e $\mathbf{g}$ os vectores coeficiente dos polinómios, a chave pri vada corresponde ao vector curto $(\mathbf{f},\mathbf{g})$.

Chave Pública

$$[\mathcal{C}^*\mathbf{f}]\mathbf{h} \equiv p\mathbf{g} \pmod{q} \Rightarrow \mathbf{h} = p[\mathcal{C}^*\mathbf{f}]^{-1}\mathbf{g} \bmod q$$

ESQUEMAS DE CRIPTOGRAFIA DE CHAVE PÚBLICA

Criptosistema NTRU

Chave Pública

$$[\mathcal{C}^*\mathbf{f}]\mathbf{h} \equiv p\mathbf{g} \pmod{q} \Rightarrow \mathbf{h} = p[\mathcal{C}^*\mathbf{f}]^{-1}\mathbf{g} \bmod q$$

$$\mathbf{m} = (0,\text{-}1,1,\text{-}1,1,0,\text{-}1) \longrightarrow$$

CIFRA

Blinding Factor

$$c = [\mathcal{C}^*\mathbf{h}]\mathbf{r} + \mathbf{m} \equiv (11, 2, 14, 30, 29, 25, 16) \pmod{q}$$

ESQUEMAS DE CRIPTOGRAFIA DE CHAVE PÚBLICA

Criptosistema NTRU

Chave Privada

Dados dois polinómios f e g, considerar a multiplicação matricial $[\mathcal{C}^*\mathrm{f}]\mathrm{g}$ equivalente ao produto da convolução dos polinómios $f * g$. Sendo f e g os vectores coeficiente dos polinómios, a chave pri vada corresponde ao vector curto (f,g).

DECIFRA

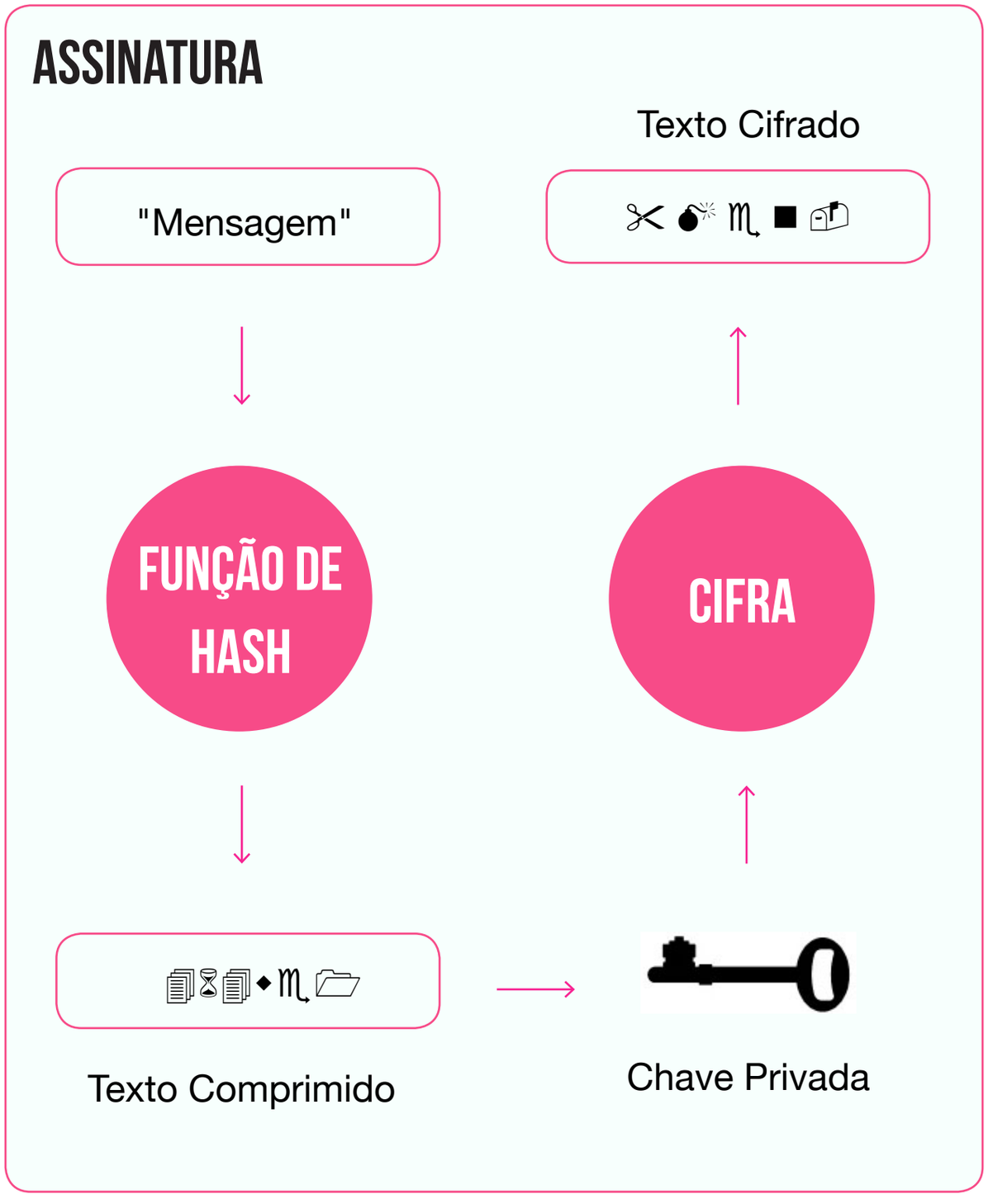
Redução mod q

$$[\mathcal{C}^*\mathrm{f}]\mathbf{c} \equiv (4,4,-4,1,-7,-4,5) \pmod{q}$$

$$[\mathcal{C}^*\mathrm{f}]_p^{-1} \cdot (4,4,-4,1--7,-4,5) \equiv (0,-1,1,-1,1,0,-1)(mod\mathrm{p}) = \mathbf{m}$$

TÉCNICAS CRIPTOGRÁFICAS

Esquemas de Assinatura Digital



TÉCNICAS CRIPTOGRÁFICAS

Esquemas de Assinatura Digital

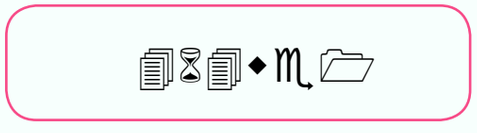
ASSINATURA

"Mensagem"

↓

FUNÇÃO DE HASH

↓



Texto Comprimido

→

Chave Privada

↑

CIFRA

↑

Texto Cifrado

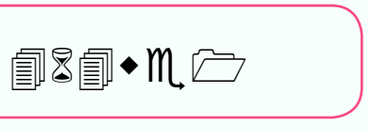
VERIFICAÇÃO

Chave Pública

↓

DECIFRA

↓



Texto Comprimido

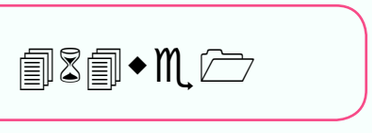
=

"Mensagem"

↓

FUNÇÃO DE HASH

↓



Texto Comprimido

TÉCNICAS CRIPTOGRÁFICAS

Esquemas de Assinatura Digital

SEGURANÇA

A probabilidade de um qualquer *forger* $\mathcal{F}$, após visualizar assinaturas de mensagens à sua escolha, conseguir assinar uma mensagem cuja assina tura ainda não tenha visto é desprezável.

TÉCNICAS CRIPTOGRÁFICAS

Esquemas de Assinatura Digital

SEGURANÇA

A probabilidade de um qualquer *forger* $\mathcal{F}$, após visualizar assinaturas de mensagens à sua escolha, conseguir assinar uma mensagem cuja assina tura ainda não tenha visto é desprezável.

STRONG UNFORGEABILITY

Um *forger* $\mathcal{F}$ não é capaz de apresentar uma assinatura diferente para u ma mensagem de cuja assinatura este já tenha tido conhecimento.

TÉCNICAS CRIPTOGRÁFICAS

Esquemas de Assinatura Digital

SEGURANÇA

A probabilidade de um qualquer *forger* $\mathcal{F}$, após visualizar assinaturas de mensagens à sua escolha, conseguir assinar uma mensagem cuja assina tura ainda não tenha visto é desprezável.

STRONG UNFORGEABILITY

Um *forger* $\mathcal{F}$ não é capaz de apresentar uma assinatura diferente para u ma mensagem de cuja assinatura este já tenha tido conhecimento.

Autenticação

Integridade

Não repudiação

TÉCNICAS CRIPTOGRÁFICAS

Esquemas de Assinatura Digital

LYUBASHEVSKY

Esquema de Identificação

Esquema de Assinatura

TÉCNICAS CRIPTOGRÁFICAS

Esquemas de Assinatura Digital

LYUBASHEVSKY

Esquema de Identificação

↓

FIAT-SHAMIR

↓

Esquema de Assinatura

LYUBASHEVSKY E MICCIANCIO

Esquema de Assinatura One-time

↓

FFT

↓

Esquema de Assinatura

CONCLUSÕES

- As construções criptográficas baseadas em reticulados constituem uma promessa na área da Criptografia Pós-Quântica;

- Nas situações em que o adversário é não passivo, a noção de segurança dos sistemas apresentados não é suficientemente robusta;

- Os esquemas de assinatura baseados em reticulados não atingiram ainda o nível de desenvolvimento das restantes construções criptográficas.