T.P.

19/04/2018

ASSINATURAS BASEADAS EM RETICULADOS

· Assinaturas digitais

Def Tripla de algoritmos { KEYGEN(λ); σ ← SIGN(M, SK); VERIF(σ, M, PK)

Fornecem Autenticidade, Integridade e Irretratabilidade.

· Noção de segurança é EXISTENTIAL UNforgeability under CHOSEN MESS. ATTACK (EU-CMA)

→ Um atacante que faz poly(λ) pedidos de assinatura não deve ser capaz de gerar uma nova assinatura.

· Esquemas de assinatura tradicionais (RSA-PSS, ECDSA) não resistem a criptanálise quântica.

RETICULADOS

Def: É um subgrupo discreto de $\mathbb{Z}^n$.

Form Sejam $b_1, b_2, \dots, b_n \in \mathbb{Z}^n$ linearmente independentes. Seja $B = [b_1 | \dots | b_n] \in \mathbb{Z}^{n \times n}$, Então o reticulado gerado por M é o conjunto

$$\Lambda = \mathcal{L}(B) = \{ Mx : x \in \mathbb{Z}^n \}.$$

· A base B não é única! Para qualquer matriz unimodular U ($\det(U) = \pm 1$)

$$\mathcal{L}(B) = \mathcal{L}(BU)$$

Há bases boas e bases ruins

+ ORTOGONAIS

- ORTOGONAIS

Problemas em Reticulados

- SVP (Shortest Vector Problem)

Dada uma base B, qual o menor vetor de $\mathcal{L}(B)$ (NP-completo na versão de decisão)

- CVP (Closest Vector Problem)

Dada uma base B e um vetor $t \in \mathbb{R}^n$, qual o vetor em $\mathcal{L}(B)$ mais próximo de t? (NP-completo decisão)

Em cripto se usa versões de aproximação: γ-SVP e γ-CVP

Para $\gamma = poly(n)$, melhores algs conhecidos levam tempo exponencial.

ASSINATURA GGH (Goldreich, Goldwasser, Halevi) Crypto '97

- Ideia: Tentar usar a dificuldade do CVP.

- KEYGEN: $R \in \{-4, -3, \ldots, 3, 4\}^{n \times n}$, secreta

colunas de S formam uma base boa.

$B = RU$, para alguma matriz unimodular U.

$(SK, PK) = (R, B)$

- SIGN: (m)

$m \in \mathbb{Z}^n$ é o hash da msg.

$$s = R\lceil R^{-1} m \rfloor$$

Extrai qual combinação linear é próxima de m

Intuição:

$$\begin{cases} m = \lfloor R(x) + \varepsilon \rceil \\ R^{-1}m = x + R^{-1}(\varepsilon) \end{cases} \quad x \in \mathbb{Z}^n \quad \varepsilon \in \mathbb{R}^n$$

$R^{-1}m = R^{-1}Rm$

- VERIFY:
  - Testa se $s \in \mathcal{L}(\widehat{B})$ (publica)
  - Testa se $\|m - s\| \leq \tau$

$$\tau = \rho_{max} \left\lfloor \log(2n/\varepsilon) \frac{\sqrt{n}}{2} \right\rfloor \quad (\varepsilon \approx 2^{-30})$$

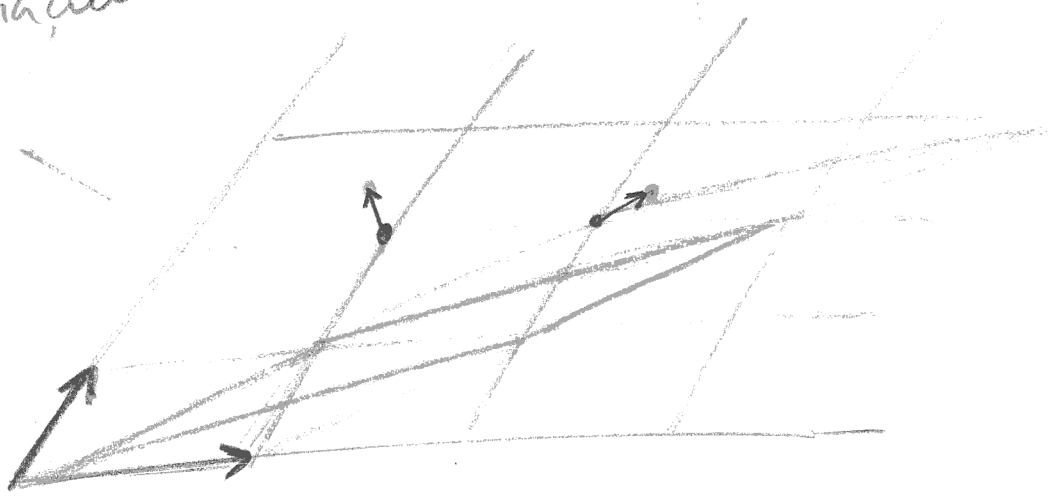
entrada máxima de R ($\ell = 4$)

para prob de falha menor que ε

- Note que $\tau = O(n^{\frac{1}{2}})$, então está na zona difícil do CVP

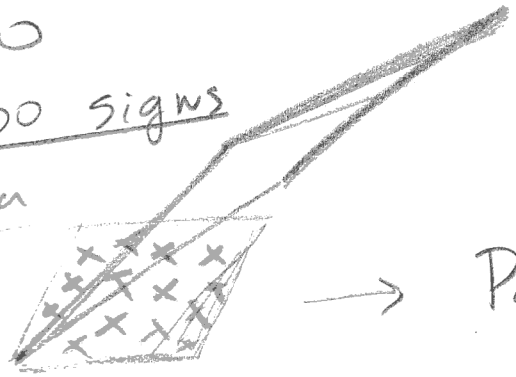
CRIPTANÁLISE DO GGH

- Todo par assinatura - msg vaza informação sobre R.



- $n = 200$

$\Rightarrow$ 20000 signs recupera

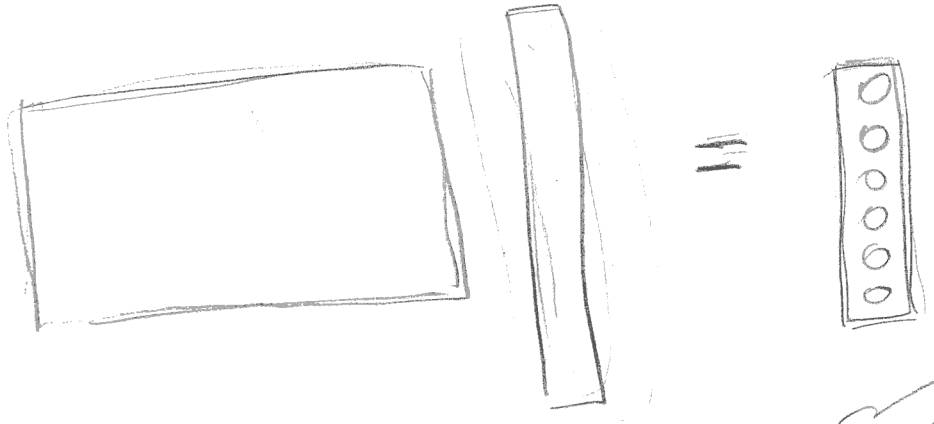


→ Parabolic prédor escondido

· BLISS (OBTENDO ESQUEMAS SEGUROS)

· O PROBLEMA SIS (Short Integer Solution)

$l_2\text{-}SIS_{q,n,m,\beta}$ Dada uma matriz aleatória $A \in \mathbb{Z}_q^{n \times m}$, encontre $v \in \mathbb{Z}^m$ - {0} tal que $Av = 0 \bmod q$ e $\|v\| \leq \beta$



entropia

Lema Se $\beta \geq \sqrt{m}\, q^{\frac{n}{m}}$, então

$SIS_{q,n,m,\beta}$ tem ao menos uma sol.

z ($Az \equiv 0 \mod q$ e $\|z\| \leq \beta$.

Dem Seja S o conjunto de vetores m-dimensionais com coordenadas menores ou iguais a $\lceil q^{\frac{n}{m}} \rceil$. Então

$$|S| = \left(q^{\frac{n}{m}} + 1\right)^m > q^n.$$

$0, 1, 2, \ldots \lceil q^{\frac{n}{m}} \rceil$ — possíveis z — possíveis Az

$\exists\, z_1 \neq z_2$ tais que $Az_1 = Az_2$

$\Rightarrow A(z_1 - z_2) = 0$

E $\|z_1 - z_2\| \leq \sqrt[2]{(q^{\frac{n}{m}})^2 m} = q^{\frac{n}{m}} \sqrt{m}$.

$x, y \in \{0, 1, \ldots, k\} \Rightarrow |x - y| \in \{0, 1, \ldots, k\}$.

. Conexão com Reticulados

$$\Lambda^{\perp}(A) = \{ z \in \mathbb{Z}^m : Az = 0 \}$$

SIS $\approx$ SVP no reticulado Dual.

Esquema de Assinatura Baseado no SIS

(Tentativa 1)

$\beta = O(n \log n)$

. KeyGen

. $S \xleftarrow{\$} \{-d, \dots, 0, \dots, d\}^{m \times k}$

. $A \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$

. $T = AS \in \mathbb{Z}_q^{n \times k}$

Quem consegue encontrar S a partir de S e T, consegue resolver o SIS!

$AS_i = 0$

- SIGN (μ, A, S)

$y \xleftarrow{\$} D_\sigma^m$ = Normal discreta m-dimensional sobre $\mathbb{Z}^m$

$c \leftarrow H(Ay, \mu)$ | impede que μ interaja com a chave

hash que devolve $v \in \{-1, 0, 1\}^k$, $\|v\| \leq k$

$z \leftarrow Sc + y$

pequeno

$\sigma = (z, c)$

- Verify: Aceita se

$\|z\| \leq 2\sigma\sqrt{m}$ e

$c = H(Az - Tc, \mu)$

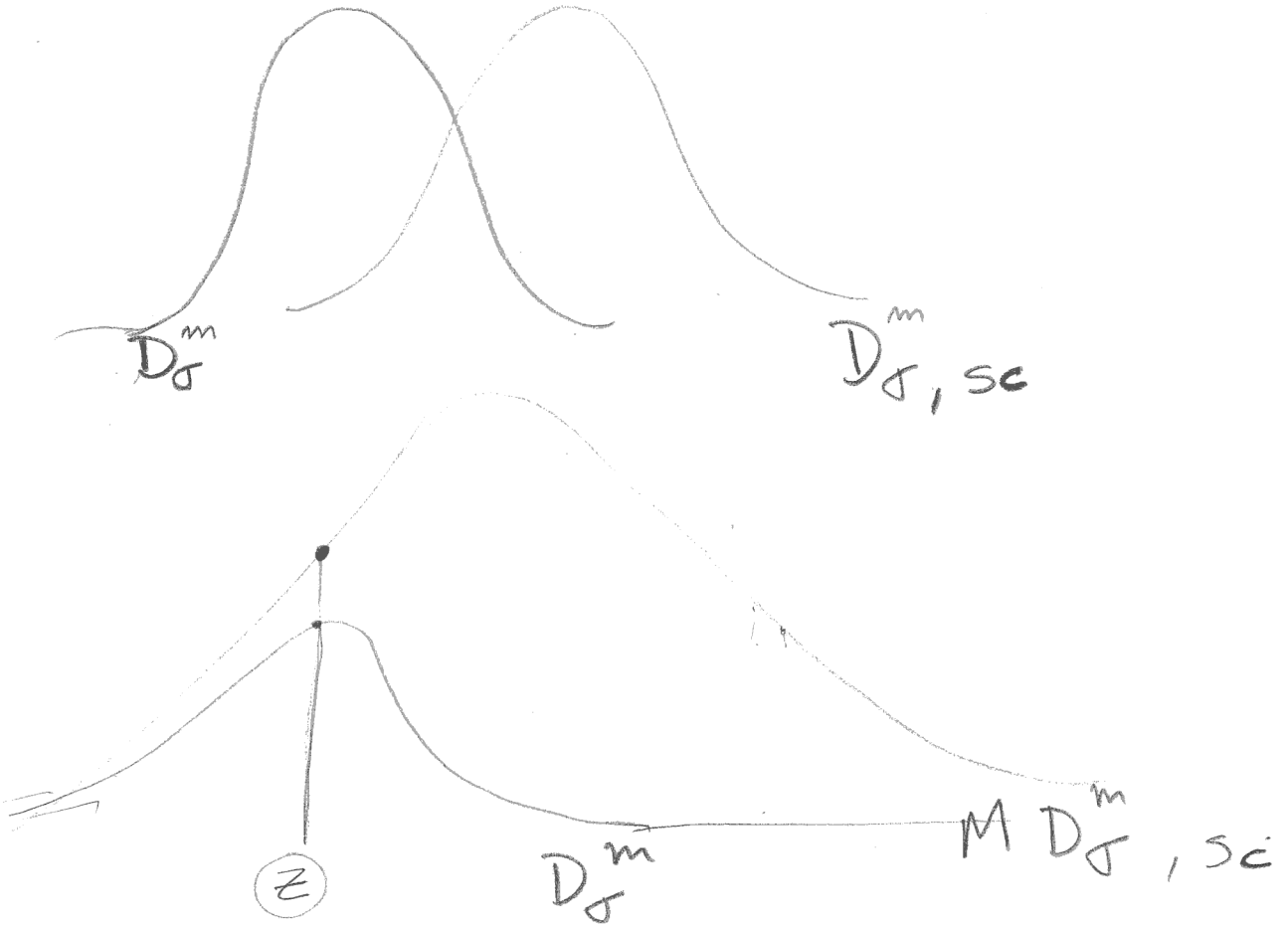
Problema: z vaza informação sobre S.

Como resolver? Rejection sampling

para deixar z independente de S.

Para corrigir a falha

- Rejection sampling



Aceita z com probabilidade

$$\min\left(\frac{D_\sigma^m(z)}{M D_{sc,\sigma}^m(z)}, 1\right)$$

Dist $\sim 2^{-100}$