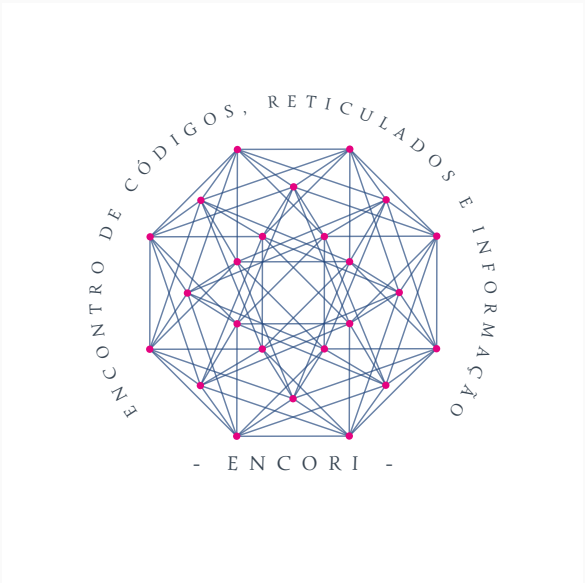
Número de condição e equivalência dos problemas Ring-LWE e Poly-LWE em corpos de números monogênicos

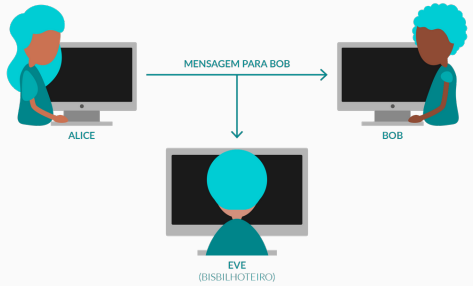


Junho de 2023 - IMECC/UNICAMP - Campinas-SP

Robson Ricardo de Araujo (IFSP/Catanduva)

Criptografia pós-quântica

- **Criptografia** é uma área que estuda e propõe técnicas que objetivam a confidencialidade, a integridade, a autenticação e a não repudiação de dados.



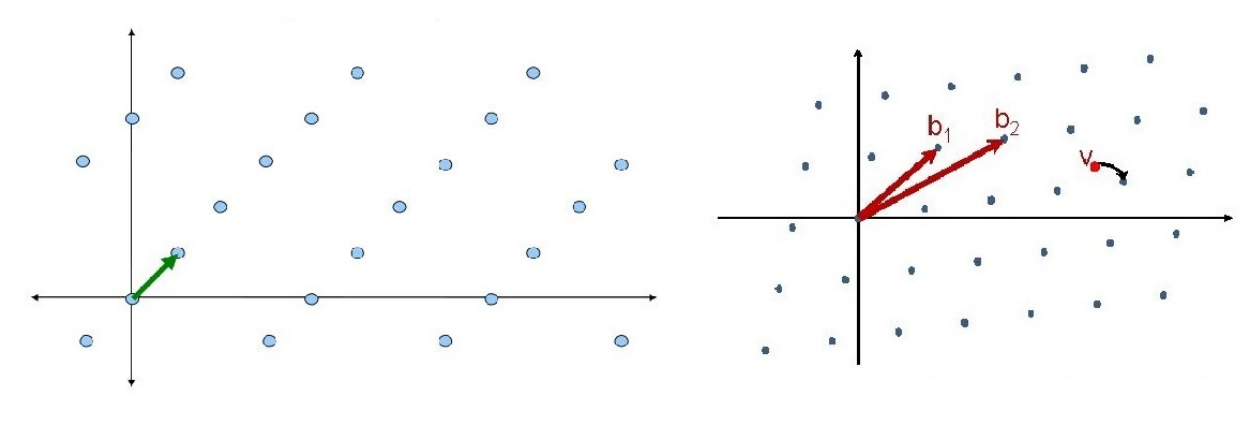
- Os sistemas criptográficos mais usados hoje (RSA e ECCs) não devem sobreviver aos computadores quânticos [Shor-94].
- A **criptografia pós-quântica** busca novos procotolos resistentes a ataques quânticos.
- Os protocolos pós-quânticos mais promissores até hoje são baseados em reticulados, códigos, funções Hash e isogenias super-singulares [NIST].

Criptografia baseada em reticulados

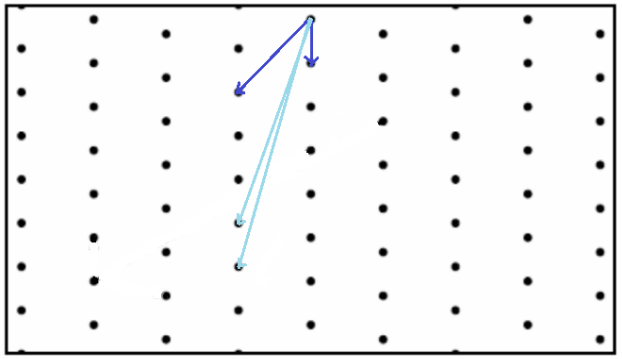
Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado.

SVP - Problema do vetor mais curto: encontrar um vetor $v \in \Lambda$ que tenha o menor comprimento ($\neq 0$) entre todos os vetores de Λ.

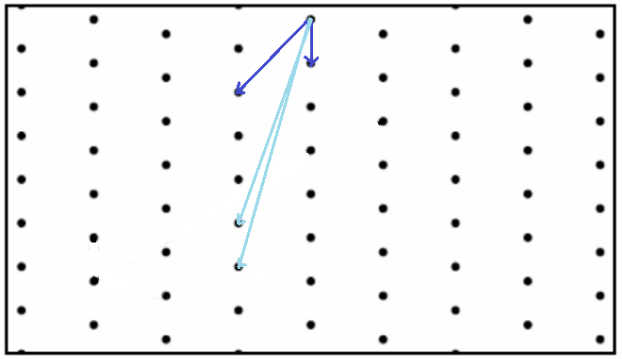
CVP - Problema do vetor mais próximo: dado $u \in \mathbb{R}^n$, encontrar o vetor $v \in \Lambda$ mais próximo de u.



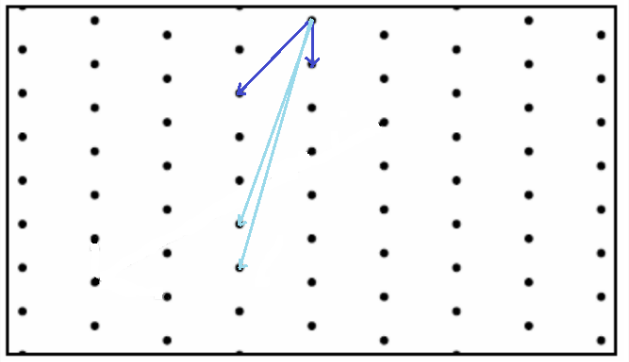
Sistemas criptográficos cuja segurança é baseada na dificuldade de solução de problemas como o SVP e o CVP constituem a chamada **criptografia baseada em reticulados**.



- A primeira proposta criptográfica baseada em reticulados foi proposta em 1996 - o NTRU [Ajtai-96].



- A primeira proposta criptográfica baseada em reticulados foi proposta em 1996 - o NTRU [Ajtai-96].
- Em 2005, O. Regev propôs o **LWE** (*Learning With Errors*), que foi aprimorado em 2010 por Lyubashevsky, Peikert e Regev para uma **versão algébrica Ring-LWE** [Regev-05, LPR-10].



- A primeira proposta criptográfica baseada em reticulados foi proposta em 1996 - o NTRU [Ajtai-96].
- Em 2005, O. Regev propôs o **LWE** (*Learning With Errors*), que foi aprimorado em 2010 por Lyubashevsky, Peikert e Regev para uma **versão algébrica** **Ring-LWE** [Regev-05, LPR-10].
- Outras versões algébricas mais práticas e/ou mais seguras teoricamente vieram depois: **Poly-LWE**, Module-LWE, Twisted Ring-LWE, entre outras [DD-12,LS-15,OAACD-21].

Ring-LWE

Considere:

- $\mathbb{K}$ um corpo de números de grau n
- $R = \mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$
- $q \geq 2$ um número primo
- $R_q = R/qR$

Ring-LWE

Considere:

- $\mathbb{K}$ um corpo de números de grau n
- $R = \mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$
- $q \geq 2$ um número primo
- $R_q = R/qR$
- $\sigma : \mathbb{K} \longrightarrow \mathbb{R}^n$ o **mergulho canônico** de $\mathbb{K}$, dado por

$$\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), Re(\sigma_{r+1}(\alpha)), Im(\sigma_{r+1}(\alpha)), \ldots, Re(\sigma_{r+s}(\alpha)), Im(\sigma_{r+s}(\alpha)))$$

em que $\sigma_1, \ldots, \sigma_r$ são os monomorfismos reais de $\mathbb{K}$ em $\mathbb{C}$ e $\sigma_{r+1}, \ldots, \sigma_{r+s}$ os monomorfismos complexos de $\mathbb{K}$ em $\mathbb{C}$ não conjugados entre si (assim, $n = r + 2s$).

Ring-LWE

Considere:

- $\mathbb{K}$ um corpo de números de grau n
- $R = \mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$
- $q \geq 2$ um número primo
- $R_q = R/qR$
- $\sigma : \mathbb{K} \longrightarrow \mathbb{R}^n$ o **mergulho canônico** de $\mathbb{K}$, dado por

$$\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), Re(\sigma_{r+1}(\alpha)), Im(\sigma_{r+1}(\alpha)), \ldots, Re(\sigma_{r+s}(\alpha)), Im(\sigma_{r+s}(\alpha)))$$

  em que $\sigma_1, \ldots, \sigma_r$ são os monomorfismos reais de $\mathbb{K}$ em $\mathbb{C}$ e $\sigma_{r+1}, \ldots, \sigma_{r+s}$ os monomorfismos complexos de $\mathbb{K}$ em $\mathbb{C}$ não conjugados entre si (assim, $n = r + 2s$).
- $\|\alpha\| = \|\sigma(\alpha)\|$, para todo $\alpha \in R$.

Definição (distribuição Ring-LWE)

Sejam $s \in R_q$ (segredo) e χ uma distribuição gaussiana em R_q. Uma **distribuição Ring-LWE** $\mathcal{A}_{s,\chi}$ é aquela que **retorna pares ordenados** (a, b), em que:

- $a \in R_q$ é amostrado pela distribuição uniforme.
- $b = a \cdot s + e \in R_q$, em que $e \in R_q$ é amostrado por χ.

Definição (distribuição Ring-LWE)

Sejam $s \in R_q$ (segredo) e χ uma distribuição gaussiana em R_q. Uma **distribuição Ring-LWE** $\mathcal{A}_{s,\chi}$ é aquela que **retorna pares ordenados** (a, b), em que:

- $a \in R_q$ é amostrado pela distribuição uniforme.
- $b = a \cdot s + e \in R_q$, em que $e \in R_q$ é amostrado por χ.

Problema de busca Ring-LWE

Dada uma amostra $\{(a_i, b_i)\}_{i=1}^{m}$ vinda de uma distribuição Ring-LWE $\mathcal{A}_{s,\chi}$, o **problema de busca Ring-LWE** consiste em descobrir s.

Poly-LWE

Considere:

- $f(x) \in \mathbb{Z}[x]$ um polinômio mônico irredutível de grau n
- $q \geq 2$ um número primo
- $R = \mathbb{Z}[x]/(f(x))$
- $R_q = R/qR = \mathbb{F}_q[x]/(f(x))$

Poly-LWE

Considere:

- $f(x) \in \mathbb{Z}[x]$ um polinômio mônico irredutível de grau n
- $q \geq 2$ um número primo
- $R = \mathbb{Z}[x]/(f(x))$
- $R_q = R/qR = \mathbb{F}_q[x]/(f(x))$
- $\psi : R \longrightarrow \mathbb{R}^n$ o **mergulho por coeficientes** de R, dado por

$$\psi\left(\sum_{i=0}^{n-1} a_i \overline{x}^i\right) = (a_0, a_1, \ldots, a_{n-1})$$

onde $a_i \in \mathbb{Z}$ e $\overline{x}$ denota a classe de x módulo $(f(x))$.

Poly-LWE

Considere:

- $f(x) \in \mathbb{Z}[x]$ um polinômio mônico irredutível de grau n
- $q \geq 2$ um número primo
- $R = \mathbb{Z}[x]/(f(x))$
- $R_q = R/qR = \mathbb{F}_q[x]/(f(x))$
- $\psi : R \longrightarrow \mathbb{R}^n$ o **mergulho por coeficientes** de R, dado por

$$\psi\left(\sum_{i=0}^{n-1} a_i \overline{x}^i\right) = (a_0, a_1, \ldots, a_{n-1})$$

  onde $a_i \in \mathbb{Z}$ e $\overline{x}$ denota a classe de x módulo $(f(x))$.
- $\|\alpha(x)\| = \|\psi(\alpha(x))\|$, para todo $\alpha(x) \in R$.

Definição (distribuição Poly-LWE)

Sejam $s(x) \in R_q$ (segredo) e χ uma distribuição gaussiana em R_q. Uma **distribuição Poly-LWE** $\mathcal{A}_{s,\chi}$ é aquela que **retorna pares ordenados** (a, b), em que:

- $a(x) \in R_q$ é amostrado pela distribuição uniforme.
- $b(x) = a(x) \cdot s(x) + e(x) \in R_q$, em que $e(x) \in R_q$ é amostrado por χ.

Definição (distribuição Poly-LWE)

Sejam $s(x) \in R_q$ (segredo) e χ uma distribuição gaussiana em R_q. Uma **distribuição Poly-LWE** $\mathcal{A}_{s,\chi}$ é aquela que **retorna pares ordenados** (a, b), em que:

- $a(x) \in R_q$ é amostrado pela distribuição uniforme.
- $b(x) = a(x) \cdot s(x) + e(x) \in R_q$, em que $e(x) \in R_q$ é amostrado por χ.

Problema de busca Poly-LWE

Dada uma amostra $\{(a_i(x), b_i(x))\}_{i=1}^{m}$ vinda de uma distribuição Poly-LWE $\mathcal{A}_{s,\chi}$, o **problema de busca Poly-LWE** consiste em descobrir $s(x)$.

- Considerando a semelhança das definições dos problemas Ring-LWE e Poly-LWE, **quando eles são equivalentes**?

- Considerando a semelhança das definições dos problemas Ring-LWE e Poly-LWE, **quando eles são equivalentes**?
- Elias, Lauter, Ozman e Stange, em 2015, mostraram que sob certas condições é possível **reduzir** o problema Ring-LWE ao problema Poly-LWE (para fins de criptoanálise) [ELOS-15].

- Considerando a semelhança das definições dos problemas Ring-LWE e Poly-LWE, **quando eles são equivalentes**?
- Elias, Lauter, Ozman e Stange, em 2015, mostraram que sob certas condições é possível **reduzir** o problema Ring-LWE ao problema Poly-LWE (para fins de criptoanálise) [ELOS-15].
- Uma dessas condições (algébrica) pede que o corpo de números $\mathbb{K}$ utilizado no problema Ring-LWE seja **monogênico**, isto é, seja isomorfo a um anel de polinômios $\mathbb{Z}[x]/(f(x))$.

- Considerando a semelhança das definições dos problemas Ring-LWE e Poly-LWE, **quando eles são equivalentes**?
- Elias, Lauter, Ozman e Stange, em 2015, mostraram que sob certas condições é possível **reduzir** o problema Ring-LWE ao problema Poly-LWE (para fins de criptoanálise) [ELOS-15].
- Uma dessas condições (algébrica) pede que o corpo de números $\mathbb{K}$ utilizado no problema Ring-LWE seja **monogênico**, isto é, seja isomorfo a um anel de polinômios $\mathbb{Z}[x]/(f(x))$.
- Outra condição (probabilística) resume-se em pedir que o **número de condição** da matriz associada ao isomorfismo entre o anel de polinômios e o anel de inteiros seja de ordem polinomial (detalhes a seguir!).

Monogênse de corpos de números

Definição

Dizemos que um corpo de números $\mathbb{K}$ é **monogênico** se $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\beta]$, ou, equivalentemente, se $\mathcal{O}_{\mathbb{K}} \cong \mathbb{Z}[x]/(f(x))$.

Monogênse de corpos de números

Definição

Dizemos que um corpo de números $\mathbb{K}$ é **monogênico** se $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\beta]$, ou, equivalentemente, se $\mathcal{O}_{\mathbb{K}} \cong \mathbb{Z}[x]/(f(x))$.

- Os corpos quadráticos $\mathbb{Q}(\sqrt{d})$ e os corpos ciclotômicos $\mathbb{Q}(\zeta_n)$ são monogênicos.

Monogênse de corpos de números

Definição

Dizemos que um corpo de números $\mathbb{K}$ é **monogênico** se $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\beta]$, ou, equivalentemente, se $\mathcal{O}_{\mathbb{K}} \cong \mathbb{Z}[x]/(f(x))$.

- Os corpos quadráticos $\mathbb{Q}(\sqrt{d})$ e os corpos ciclotômicos $\mathbb{Q}(\zeta_n)$ são monogênicos.
- Os subcorpos ciclotômicos maximais reais $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ são monogênicos.

Monogênse de corpos de números

Definição

Dizemos que um corpo de números $\mathbb{K}$ é **monogênico** se $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\beta]$, ou, equivalentemente, se $\mathcal{O}_{\mathbb{K}} \cong \mathbb{Z}[x]/(f(x))$.

- Os corpos quadráticos $\mathbb{Q}(\sqrt{d})$ e os corpos ciclotômicos $\mathbb{Q}(\zeta_n)$ são monogênicos.
- Os subcorpos ciclotômicos maximais reais $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ são monogênicos.
- Exceto pelos corpos maximais reais, todo corpo de números cíclico de grau primo $p \geq 5$ não é monogênico [Gras-86].

Monogênse de corpos de números

Definição

Dizemos que um corpo de números $\mathbb{K}$ é **monogênico** se $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\beta]$, ou, equivalentemente, se $\mathcal{O}_{\mathbb{K}} \cong \mathbb{Z}[x]/(f(x))$.

- Os corpos quadráticos $\mathbb{Q}(\sqrt{d})$ e os corpos ciclotômicos $\mathbb{Q}(\zeta_n)$ são monogênicos.
- Os subcorpos ciclotômicos maximais reais $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ são monogênicos.
- Exceto pelos corpos maximais reais, todo corpo de números cíclico de grau primo $p \geq 5$ não é monogênico [Gras-86].
- Para cada n não divisível por 2 nem por 3, há finitos corpos de números abelianos de grau n que são monogênicos [Gras-84].

Número de condição

Dada uma matriz $A \in M_{n\times n}(\mathbb{C})$, denote por A^* sua conjugada transposta.

A **norma de Frobenius** de A é definida por

$$\|A\| = \sqrt{Tr(AA^*)} = \sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n} |a_{ij}|^2}.$$

Número de condição

Dada uma matriz $A \in M_{n\times n}(\mathbb{C})$, denote por A^* sua conjugada transposta.

A **norma de Frobenius** de A é definida por

$$\|A\| = \sqrt{Tr(AA^*)} = \sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n} |a_{ij}|^2}.$$

Definição (número de condição)

O **número de condição** de uma matriz invertível $A \in M_{n\times n}(\mathbb{C})$ é o valor

$$Cond(A) = \|A\| \cdot \|A^{-1}\|.$$

Seja $\mathbb{K}$ um corpo de números monogênico de grau n.
Considere $\mathcal{O}_{\mathbb{K}} \cong \mathbb{Z}[x]/(f(x))$ e uma bijeção

$$T_f : \mathbb{Z}[x]/(f(x)) \longrightarrow \sigma(\mathcal{O}_{\mathbb{K}})$$

onde σ denota o mergulho canônico de $\mathbb{K}$.

Seja $\mathbb{K}$ um corpo de números monogênico de grau n.
Considere $\mathcal{O}_{\mathbb{K}} \cong \mathbb{Z}[x]/(f(x))$ e uma bijeção

$$T_f : \mathbb{Z}[x]/(f(x)) \longrightarrow \sigma(\mathcal{O}_{\mathbb{K}})$$

onde σ denota o mergulho canônico de $\mathbb{K}$.

Compreende-se que o **número de condição da matriz associada a T_f** quantifica *quanto há de distorção* entre a imagem do mergulho por coeficientes associado a $f(x)$ e a imagem do mergulho canônico associado a $\mathbb{K}$ [RSW-18]. Assim:

Seja $\mathbb{K}$ um corpo de números monogênico de grau n.
Considere $\mathcal{O}_{\mathbb{K}} \cong \mathbb{Z}[x]/(f(x))$ e uma bijeção

$$T_f : \mathbb{Z}[x]/(f(x)) \longrightarrow \sigma(\mathcal{O}_{\mathbb{K}})$$

onde σ denota o mergulho canônico de $\mathbb{K}$.

Compreende-se que o **número de condição da matriz associada a T_f** quantifica *quanto há de distorção* entre a imagem do mergulho por coeficientes associado a $f(x)$ e a imagem do mergulho canônico associado a $\mathbb{K}$ [RSW-18]. Assim:

Equivalência Ring-LWE/Poly-LWE

O problema Ring-LWE sobre $\mathbb{K}$ e o problema Poly-LWE sobre $\mathbb{Z}[x]/(f(x))$ são **equivalentes** se $Cond(T_f) = O(n^r)$, com r independente de n.

Alguns fatos atuais sobre o assunto:

- Em [RSW-18] são estudados resultados genéricos sobre a redução Ring-LWE/Poly-LWE, incluindo casos não-monogênicos, e mostra-se a redução no caso particular em que $f(x) = x^n + xP(x) - a$, onde $grau(P) < n/2$ e a é um primo numa determinada faixa em função de n e de $P(x)$.

Alguns fatos atuais sobre o assunto:

- Em [RSW-18] são estudados resultados genéricos sobre a redução Ring-LWE/Poly-LWE, incluindo casos não-monogênicos, e mostra-se a redução no caso particular em que $f(x) = x^n + xP(x) - a$, onde $grau(P) < n/2$ e a é um primo numa determinada faixa em função de n e de $P(x)$.
- Em [CL-21], que generaliza [C-22], é mostrada a equivalência Ring-LWE/Poly-LWE em **corpos maximais reais de condutor** 2^r**,**$2^r p$ **e** $2^r pq$, em que p e q são primos ímpares e $r \geq 2$.

Alguns fatos atuais sobre o assunto:

- Em [RSW-18] são estudados resultados genéricos sobre a redução Ring-LWE/Poly-LWE, incluindo casos não-monogênicos, e mostra-se a redução no caso particular em que $f(x) = x^n + xP(x) - a$, onde $grau(P) < n/2$ e a é um primo numa determinada faixa em função de n e de $P(x)$.
- Em [CL-21], que generaliza [C-22], é mostrada a equivalência Ring-LWE/Poly-LWE em **corpos maximais reais de condutor** 2^r,$2^r p$ **e** $2^r pq$, em que p e q são primos ímpares e $r \geq 2$.
- Em [C-20] é mostrada a equvailência Ring-LWE/Poly-LWE em certas famílias de **corpos ciclotômicos, tais como aqueles cujo condutor é divisível por, no máximo, três primos distintos**.

Algumas questões de interesse para pesquisa:

Algumas questões de interesse para pesquisa:

- Há famílias interessantes de polinômios $f(x)$ de grau alto (de interesse criptográfico) tais que o corpo de números $\mathbb{K} \cong \mathbb{Q}[x]/(f(x))$ seja monogênico? (Ex.: trinômios ou quadrinômios.)

Algumas questões de interesse para pesquisa:

- Há famílias interessantes de polinômios $f(x)$ de grau alto (de interesse criptográfico) tais que o corpo de números $\mathbb{K} \cong \mathbb{Q}[x]/(f(x))$ seja monogênico? (Ex.: trinômios ou quadrinômios.)
- Há equivalência Ring-LWE/Poly-LWE para corpos ciclotômicos quaisquer, subcorpos ciclotômicos maximais reais quaisquer ou outras famílias de corpos de números interessantes?

Algumas questões de interesse para pesquisa:

- Há famílias interessantes de polinômios $f(x)$ de grau alto (de interesse criptográfico) tais que o corpo de números $\mathbb{K} \cong \mathbb{Q}[x]/(f(x))$ seja monogênico? (Ex.: trinômios ou quadrinômios.)
- Há equivalência Ring-LWE/Poly-LWE para corpos ciclotômicos quaisquer, subcorpos ciclotômicos maximais reais quaisquer ou outras famílias de corpos de números interessantes?
- Mesmo que não seja monogênico, há como verificar se há equivalência Ring-LWE/Poly-LWE entre corpos de números cíclicos de grau primo $p \geq 5$?

Referências

- [Shor-94] Shor, P. W., **Algorithms for quantum computation: discrete logarithms and factoring**. Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, USA, 1994, pp. 124-134.
- [NIST] National Institute of Standards and Technology. Post-Quantum Cryptography. 2017. Available online: https://csrc.nist.gov/ Projects/post-quantum-cryptography/post-quantum-cryptography-standardization.
- [Ajtai-96] Ajtai, M. **Generating Hard Instances of Lattice Problems** (Extended Abstract). In Proceedings of the STOC '96. ACM: New York, NY, USA, 1996; pp. 99–108.

- [Regev-05] Regev, O. **On Lattices, Learning with Errors, Random Linear Codes, and Cryptography**. In Proce. of the STOC '05, ACM: New York, USA, 2005; pp. 84–93.
- [LPR-10] Lyubashevsky, V., Peikert, C., Regev, O. **On Ideal Lattices and Learning with Errors over Rings**. Advances in Cryptology, EUROCRYPT 2010.
- [LS-15] Langlois, A.; Stehlé, D. **Worst-case to average-case reductions for module lattices**. Des. Codes Cryptogr. 2015, 75, 565–599.
- [DD-12] Ducas, L., Durmus, A. **Ring-LWE in polynomial rings**. Proceedings of the 15th international conference on Practice and Theory in Public Key Cryptography, 2012.

[OAACD-21] Ortiz, J.N., de Araujo, R.R., Aranha, D.F., Costa, S.I.R., Dahab, R. **The Ring-LWE Problem in Lattice-Based Cryptography: The Case of Twisted Embeddings**. Entropy, 2021.

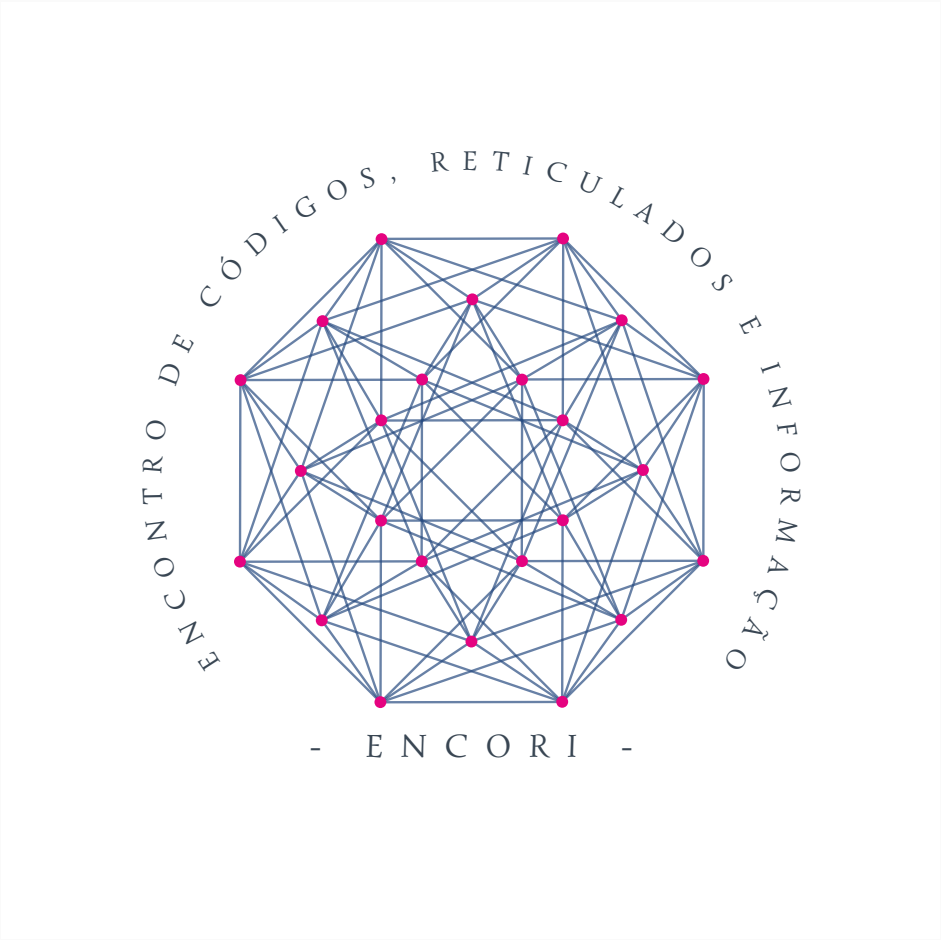
[ELOS-15] Elias, Y.; Lauter, K.E.; Ozman, E.; Stange, K.E. **Provably Weak Instances of Ring-LWE**. In Advances in Cryptology, Proc. of the CRYPTO 2015; Springer: Berlin/Heidelberg, Germany, 2015; pp. 63–92.

[Gras-84] Gras, M.-N. **Condition necessaire de monogeneite de l'anneau des entiers d'une extension abelienne de Q**, Seminare de theorie des nombres (Paris, 1984/1985), Prog. in Math, Birkhauser.

[Gras-86] Gras, M.-N. **Non monogeneite de l'anneau des entiers des extensions cycliques de Q de degre premier** $\ell \geq 5$, J. Number Theory 23(1986), no. 3, p. 347-353.

- [RSW-18] Rosca, M., Stehlé, D., Wallet, A. **On the ring-LWE and polynomial-LWE problems**. Advances in Cryptology EUROCRYPT 2018. Lecture Notes in Computer Science, vol. 10820. Springer, Berlin, 2018.
- [CL-21] Blanco-Chacón, I. **RLWE/PLWE equivalence for totally real cyclotomic subextensions via quasi-Vandermonde matrices**. Journal of Algebra and its Applications, 2021.
- [CL-20] Blanco-Chacón, I. **On the RLWE/PLWE equivalence for cyclotomic number fields**. AAECC 33, 53–71 (2022).

Muito obrigado!



robson.ricardo@ifsp.edu.br