# Uso de Criptografia Pós-Quântica

Prof. Dr. Jean Everson Martina

jean.martina@ufsc.br

LabSEC/UFSC

Slides: Alexandre Giron

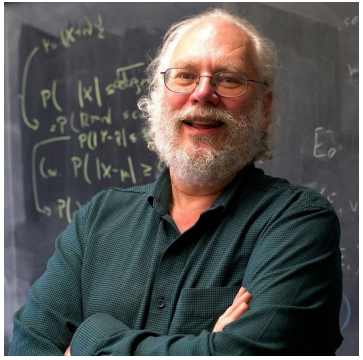

# O que é Criptografia Pós-Quântica?

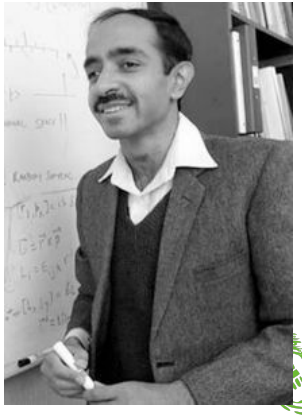
- *Post-Quantum Cryptography / Quantum-resistant / Quantum-safe*
- Criptografia resistente ao computador quântico
- Cenário da Criptografia Pós-Quântica
  - **Usuários** utilizando **computadores atuais** (arquiteturas convencionais); vs
  - **Adversários** utilizando **computadores quânticos**

**Criptografia Pós-Quântica ≠ Criptografia Quântica!**

# O surgimento da “ameaça quântica”

- Algoritmo “Quântico” de Peter Shor [SHO94]
  - Criptografia de chaves públicas mais usada é **vulnerável**!
  - Solução eficiente para o problema matemático no qual esquemas populares são baseados
  - Fatoração de Inteiros; Logaritmo Discreto
- Algoritmo “Quântico” de Busca de Lov Grover [GRO96]
  - Diminui a segurança da Criptografia Simétrica **pela metade**!
  - Impacto reduzido: “basta” dobrar os parâmetros de segurança



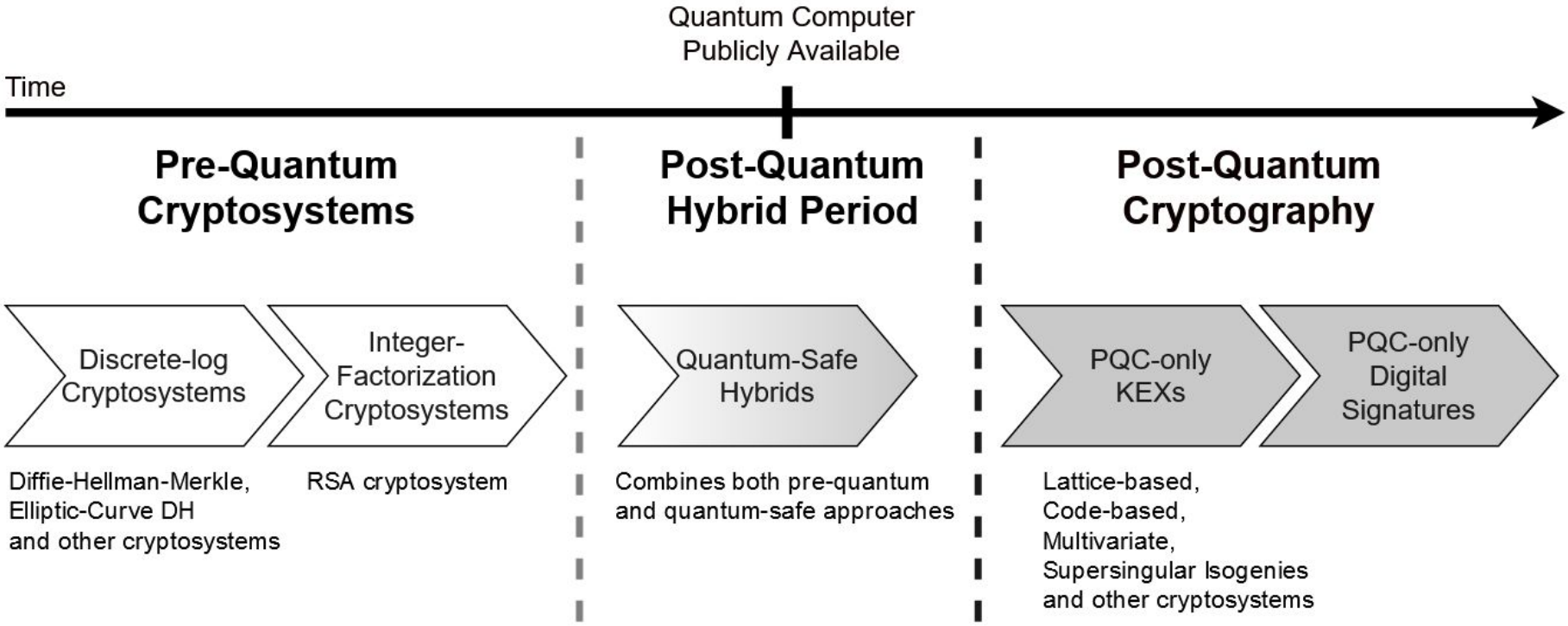


UNIVERSIDADE FEDERAL DE SANTA CATARINA

# Quais algoritmos mais ameaçados

- Algoritmos de Chave Pública “Quebrados”
  - RSA, DSA, ECDSA
  - Curvas Elípticas em geral
- Algoritmos impactados pelo algoritmo de busca de Grover:
  - Algoritmos de Hash (Hashes Criptográficos) em geral (exemplo: SHA256)
  - Algoritmos de Chave Simétrica em geral (exemplo: AES)

# Uma visão de transição (simplificada)



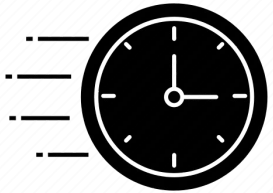

UNIVERSIDADE FEDERAL
DE SANTA CATARINA

# Ameaça do computador quântico: Quando?

- O que diz a NSA (*National Security Agency*) sobre isso:
  - *"NSA does not know **when** or **even if** a quantum computer of sufficient size and power to exploit public key cryptography (...) **will exist**."*[1]
- *Survey* de especialistas [MOS20]:
  - Quando um computador quântico ameaçará <u>concretamente</u> a criptografia de chaves públicas?
    - Pouco acima de **50%** das opiniões: **até 2035**
    - **86%** acreditam que isso ocorrerá **até 2040**

[1] https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF

# Há urgência para essa transição?



- Então temos tempo.... Temos?
- Possível ataque? À **autenticidade** das informações
  - Não é possível "se passar por alguém" retroativamente no tempo
  - Porém assinaturas digitais em documentos (de "longo prazo") podem perder a confiança
- Possível ataque: À **confidencialidade** das informações
  - Conhecido como *record-now-decrypt-later*
  - Alguém *poderia* decifrar, no futuro, as comunicações trocadas hoje!
  - Maior urgência nesse caso

# Quais são os algoritmos existentes?

- Classificação baseada no tipo do problema matemático
  a. *Lattice-based Cryptography*: "reticulados"
  b. *Code-based Cryptography*: códigos de correção de erro
  c. *Multivariate Cryptography:* equações polinomiais multivariadas
  d. Outros: *Hash-based Cryptography, Elliptic Curve Supersingular Isogenies*
- Classificação do tipo do esquema criptográfico (NIST)
  a. Mecanismo de Encapsulamento de Chaves
  b. Esquema de Assinatura Digital

# Encapsulamento de Chaves e Assinatura Digital

- ***Key-Encapsulation Mechanisms* (KEM)**:
  - Kyber, Saber, NTRU: 3 algoritmos do tipo *lattice-based*
  - Classic McEliece: algoritmo *code-based*. Obs: surgiu em 1978
- **Assinatura Digital**
  - Dilithium, Falcon: 2 algoritmos do tipo *lattice-based*
  - Rainbow: algoritmo do tipo *multivariate-cryptography*

Estes são os finalistas do Round 3 do processo do NIST

Nota: Assinaturas *Hash-based* são padronizadas separadamente

# Comparando as soluções existentes

## Tamanho de chaves públicas

- Elliptic-Curve Diffie-Hellman prime256v1 (**não é pós-quântico!**): 64 +1 Bytes
- Classic McEliece [STE16]: 261,120 Bytes
  - Pode chegar a ~**1,36 MB!**
- LightSaber [STE16]: 672 Bytes

## Tamanhos nos algoritmos de assinatura

- Falcon-512 [STE16]: 897 Bytes de chave pública; 690 Bytes da assinatura digital
- Dilithium2 [STE16]: 1312 Bytes de chave pública; 2420 Bytes da assinatura digital
- RSA-2048 (**não é pós-quântico!**): 256 Bytes para chave e assinatura

UNIVERSIDADE FEDERAL DE SANTA CATARINA

# Como usar a Criptografia Pós-Quântica?

- *Disclaimer*: não há um padrão (ainda)
  - Exceto para *hash-based signatures* (RFC 8391, RFC 8554) e NTRU (IEEE 1363.1)
- **Confiança** na segurança de algoritmos e implementações em uso hoje
  - Diffie-Hellman, RSA: década de 70
    - Tempo para pesquisa, provas de segurança, análise de implementações
  - Criptografia pós-quântica não teve o mesmo tempo de análise e pesquisa
  - Uma recomendação: **Criptografia Pós-Quântica Híbrida**

**Criptografia "Clássica"** → **Modo Híbrido** → **Criptografia Pós-Quântica**

# Uma palavra sobre o modo “Híbrido”

- Qual é o propósito do híbrido?
  - Combinar dois (ou mais) algoritmos: ex. um pré e outro pós-quântico
  - A segurança permanece enquanto ao menos um não foi quebrado
- Lembrar que o atacante “quântico” não é o único atacante...
- Pontos **Positivos**:
  - Transição não-disruptiva
  - Confiança na criptografia atual
  - Nível de escrutínio de softwares
  - Regulações e conformidade
- Pontos **Negativos**:
  - Custo computacional (ex: +1 algoritmo)
  - Como combinar de maneira segura
  - Transmissão de mais objetos criptográficos (chaves públicas, etc)

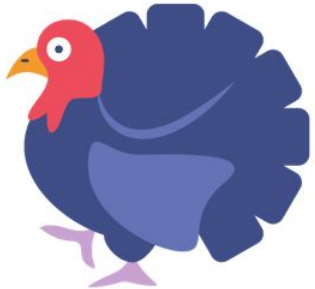
# Mais uma palavra sobre o modo “Híbrido”

- Exemplos de uso do Híbrido?
  - Experimento da Cloudflare[1]:

    TLS

- Outra possibilidade para o Híbrido
  - Combinar criptografia clássica, pós-quântica e criptografia **quântica** [DOW20]

CECPQ2 = HRSS + X25519



CECPQ2b = SIKE + X25519

https://blog.cloudflare.com/the-tls-post-quantum-experiment/

# Concluindo...

- Diversas possibilidades e espaço para contribuições
  - Analisar a segurança dos algoritmos, implementações, protocolos, aplicações...
  - Desempenho da criptografia pós-quântica
  - Projetar/colocar criptografia pós-quântica em novos ambientes de computação (*Blockchains, Internet-of-Things, 5G Networks*....)
- Transição para a **Criptografia Pós-Quântica**
  - Mundo pré-quântico para o pós-quântico
  - Modo **híbrido** para "suavizar" a transição

UNIVERSIDADE FEDERAL DE SANTA CATARINA

# Referências


- Peter W Shor,Algorithms for quantum computation: discrete logarithms and factoring, Proceedings 35th annual symposium on foundations of computer science, Ieee, 1994, pp. 124–134
- Lov K Grover,A fast quantum mechanical algorithm for database search,Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 1996, pp. 212–219.
- Bernstein, Daniel J., Buchmann, Johannes and Dahmen, Erik. Post-Quantum Cryptography. Springer-Verlag Berlim Heilderberg, 2009 (pp 147-187).
- Michele Mosca and Marco Piani. Quantum threat timeline report 2020. Available at: https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/
- Douglas Stebila and Michele Mosca,Post-quantum key exchange for the internet and the open quantum safe project, International Conference on Selected Areas in Cryptography, Springer, 2016, pp. 14–37.
- Processo de Padronização do NIST: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization
- Dowling B., Hansen T.B., Paterson K.G. (2020) Many a Mickle Makes a Muckle: A Framework for Provably Quantum-Secure Hybrid Key Exchange. In: Ding J., Tillich JP. (eds) Post-Quantum Cryptography. PQCrypto 2020. Lecture Notes in Computer Science, vol 12100. Springer, Cham. https://doi.org/10.1007/978-3-030-44223-1_26