



Fundamentos de Criptografia Pós-Quântica

Prof. Bryan Kano



Bryan Kano

- Mestrado em Ciência da Computação (Criptografia e Segurança de Dados). Universidade de São Paulo (USP).
- MBA em Inteligência Artificial e Big Data. Universidade de São Paulo (USP).
- Especialização em Proteção de Dados. Universidade Presbiteriana Mackenzie (MACKENZIE).
- Bacharelado em Ciência da Computação. Universidade Presbiteriana Mackenzie (MACKENZIE).

bryan.ferreira@inteli.edu.br



Meta is getting ready for post-quantum cryptography

EPISODE 65
Getting Ready for Post-Quantum Cryptography

Pascal H.
Rafael M.

Meta Tech Podcast

Post-Quantum Cryptography

Bringing quantum-resistance to AWS services and customers

What is post-quantum cryptography at AWS?

The path to quantum-safe

Microsoft is working towards a quantum-safe future. This involves securing our products, services, customers, partners, and our entire supply chain. We are prioritizing cryptographic agility and hybrid solutions, integrating standardized post-quantum cryptographic algorithms, and enhancing security processes with dedicated services and training.

Microsoft's Quantum-Safe Program is helping Microsoft's customers and partners prepare.

Ensino contextualizado em Post-Quantum Cryptography

Análise e Desenvolvimento de Criptossistemas PQC

Principais agentes: meio acadêmico e entidades de padronização.

Descrição: criar e analisar minuciosamente propostas de algoritmos PQC candidatos (e.g. segurança, eficiência).

Considerações: atividade extremamente teórica e complexa. Difícil contribuição para iniciantes (e.g. o Brasil não tem contribuições significativas na área).

Implementação de módulos criptográficos para uso

Principal agentes: empresas especializadas em fornecimento de soluções em criptografia e setores específicos de Big Techs.

Descrição: implementações adequadas compatíveis para uso em determinados tipos de software, midwares e hardware.

Considerações: atividade extremamente sensível, necessidade de certificações.

Transição eficaz para PQC

Principais agentes: qualquer organização com ímpeto inovador.

Descrição: avaliação e adaptação de sistemas existentes para suportar algoritmos PQC, garantindo compatibilidade e segurança a longo prazo.

Considerações: substituição gradual dos algoritmos atuais e o treinamento de profissionais para lidar com os novos padrões e tecnologias.

Um pouco de storytelling

A criptografia é a joia dos mecanismos de segurança.

- A história das duas princesas:



1. As princesas constroem **muros enormes** que conectam os dois reinos para impedir que os capangas do rei capturem a mensagem. Porém, o príncipe envia soldados que encontram brechas, escalam ou cavam túneis no muro.
2. As princesas criam **rotas secretas** para os mensageiros e colocam **guardas para vigiar e defender o trajeto**. O príncipe rejeitado, astuto, envia espiões para descobrir as novas rotas e mercenários para neutralizar os soldados das princesas.

Um pouco de storytelling

A criptografia é a joia dos mecanismos de segurança.

- A história das duas princesas:



3. As princesas fornecem **melhores soldados, armaduras e armas para proteger os mensageiros** no caminho. Porém, o príncipe ainda consegue emboscar e capturar o mensageiro.
4. As princesas **colocam as cartas em baús trancados** para dificultar a vida do príncipe. Após forçar os mecanismos, os capangas conseguem quebrar a proteção externa.

O trunfo criptográfico

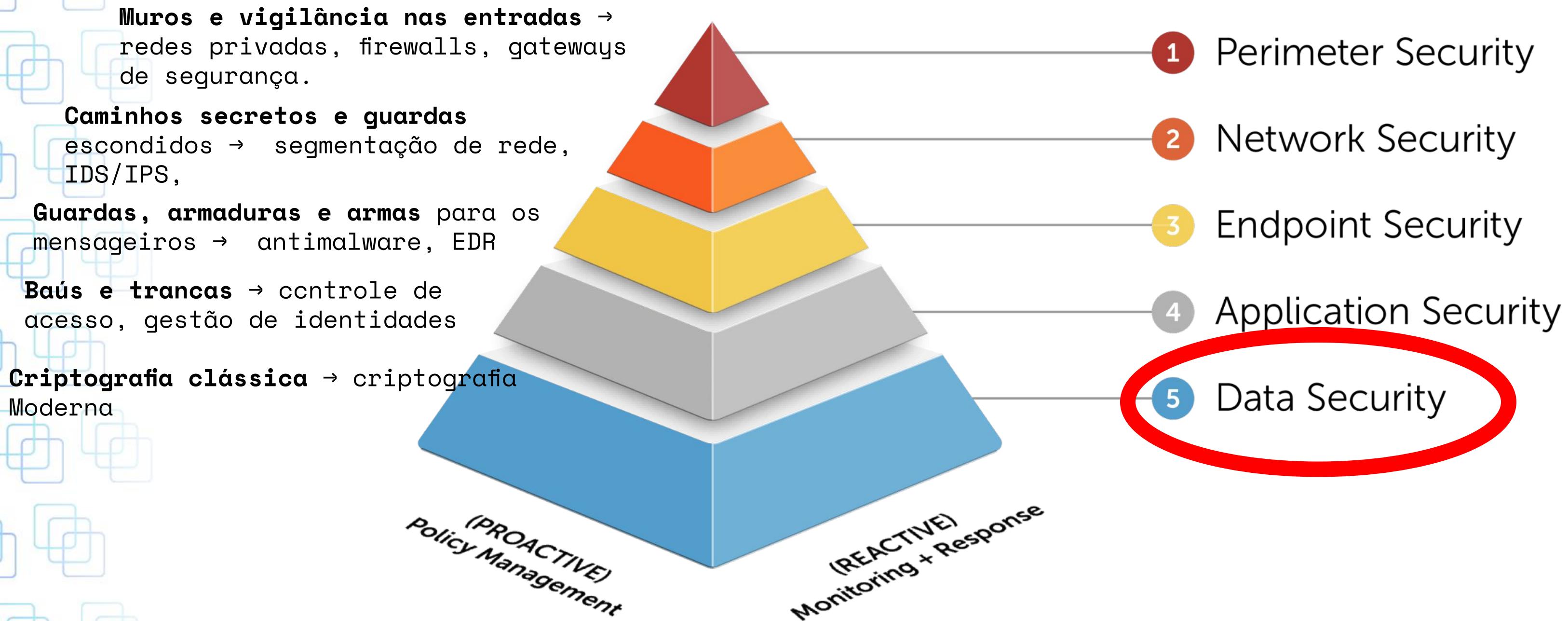
A criptografia é a joia dos mecanismos de segurança.

- A história das duas princesas:



?

Não estamos falando sobre muralhas, soldados e batalhas.



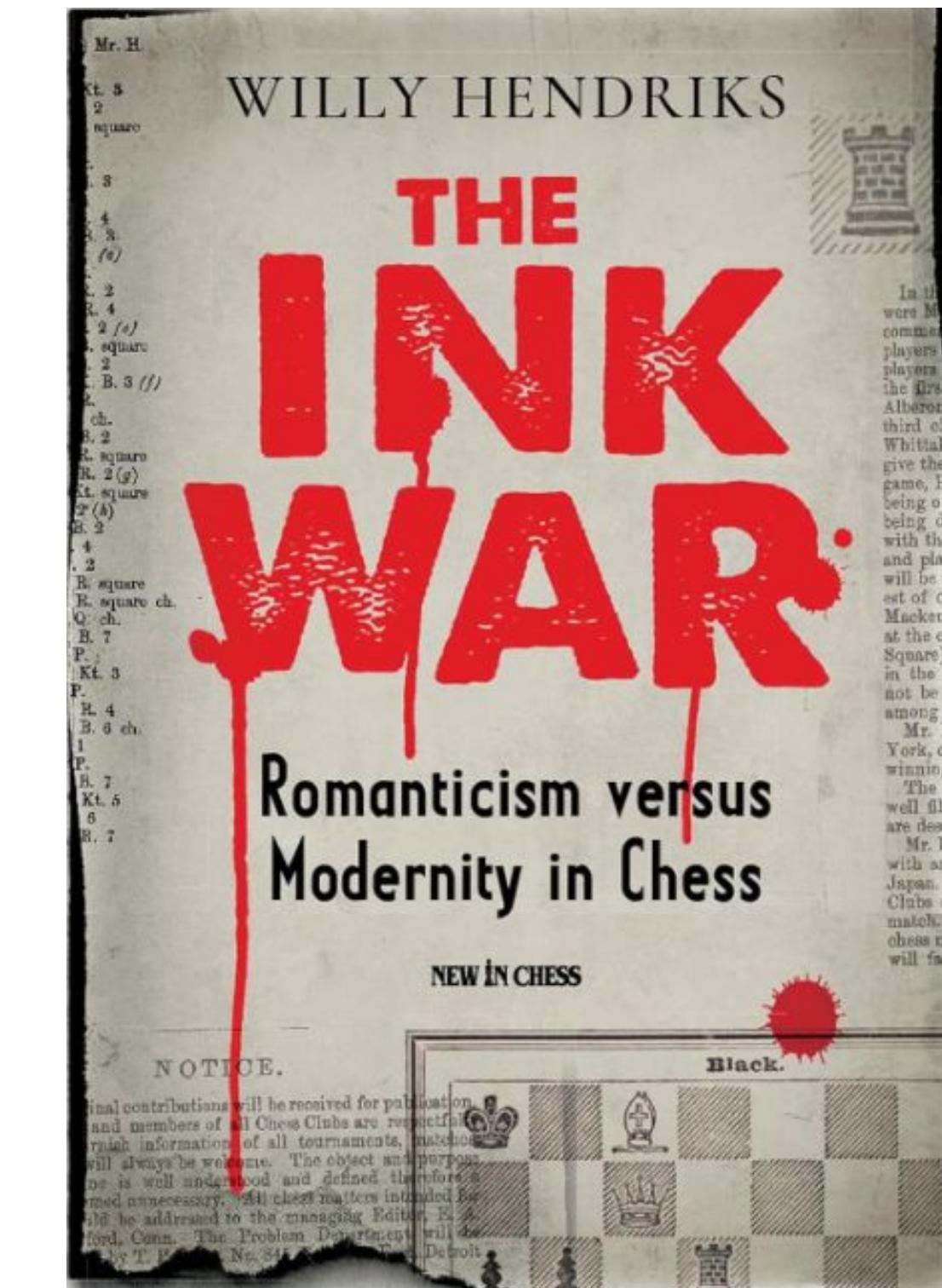
Criptografia Clássica X Criptografia Moderna



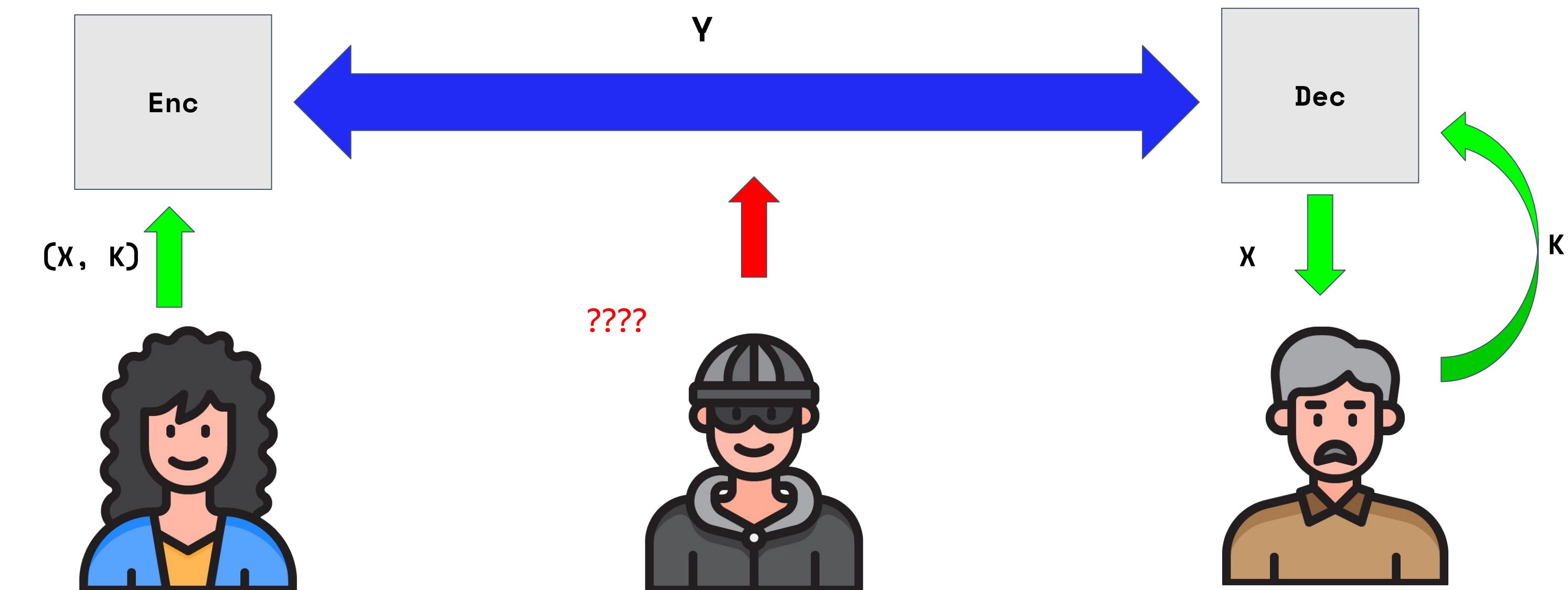
O Princípio de Kerckhoff afirma que a segurança de um criptosistema deve residir apenas na escolha de suas chaves; todo o resto (incluindo o próprio algoritmo) deve ser considerado de conhecimento público.

Substituição de caracteres por códigos (morse, bits).

Segurança matemática ao invés de criativa.



Criptografia Simétrica:



A limitação da Criptografia Simétrica (Only) em um mundo globalizado.

Como combinar a chave secreta?



New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Abstract—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a com-

1977 - um ano depois do DH fraco

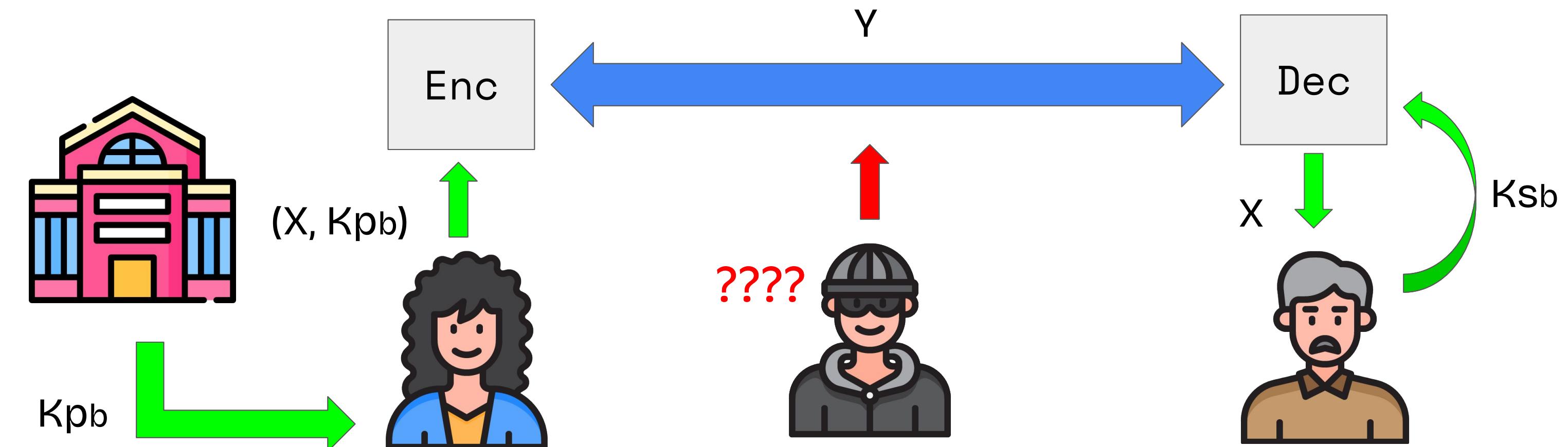
A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman*

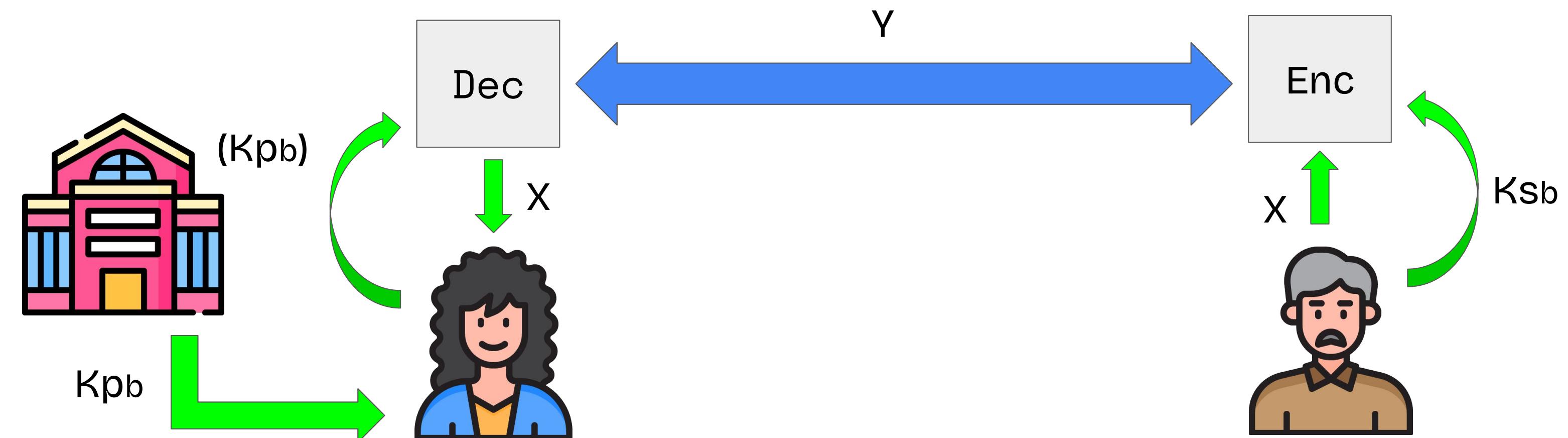
Abstract

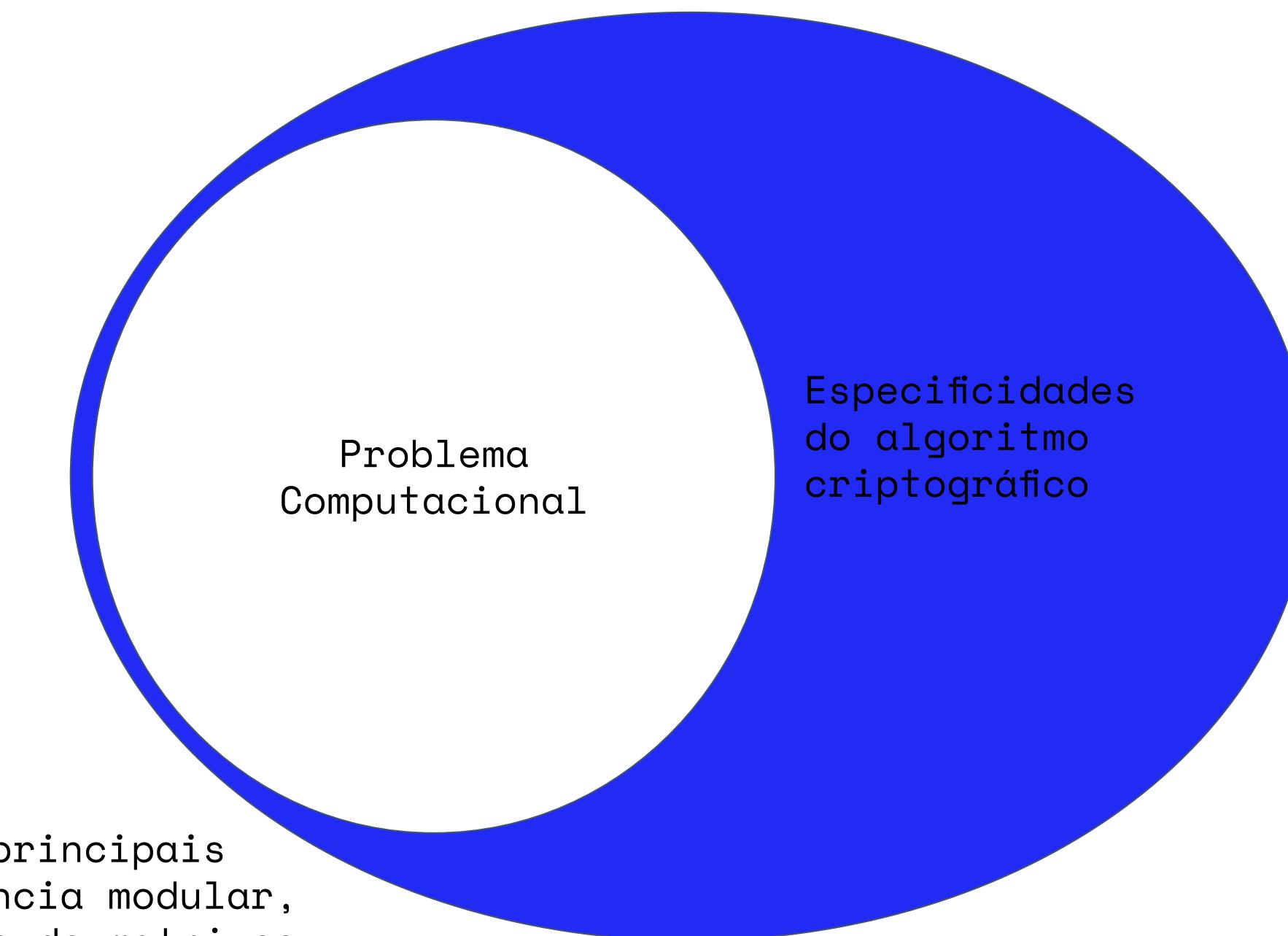
An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

Criptografia Assimétrica:



Invertendo o esquema, conseguimos prover um serviço diferente (Assinatura Digital):





As operações principais envolvem potência modular, multiplicações de matrizes ou operações sobre curvas elípticas, que são mais custosas em tempo e espaço em comparação com os algoritmos simétricos.

A criptografia assimétrica requer, por design, um **problema computacional** considerado difícil para garantir que a chave pública seja derivada da chave privada de forma que o processo inverso seja computacionalmente impraticável. Isso assegura que, mesmo com a chave pública exposta, a chave privada permaneça segura e inacessível.

Fatoração de Inteiros (Primos):

Dado um número N , encontrar seus fatores primos. Exemplo: para $N = 15$, os fatores são 3 e 5.

A dificuldade cresce na medida do tamanho do número primo. Um número grande como N perto de 10^{300} . Um quatrilhonésimo de trecentilhões de trecentilhões de trecentilhões de trecentilhões.

Sem algoritmos quânticos, levaria milhares/milhões de anos para um computador clássico fatorar esse número

Logaritmo Discreto:

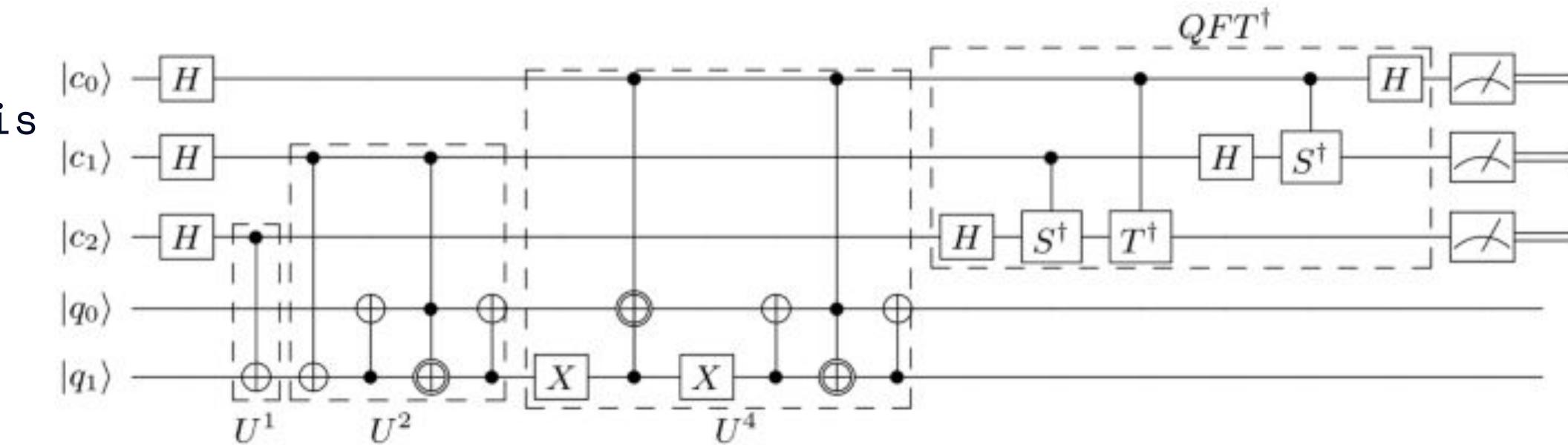
Dado um número dado g , h , e p , encontrar x tal que $g^x \equiv h \pmod{p}$.

Exemplo: tomamos o grupo \mathbb{Z}_7 (números inteiros módulo 7), onde $g = 3$, $h = 5$ e queremos encontrar x tal que $3^x \equiv 5 \pmod{7}$. Vamos testando os valores de x , até $x = 5$ que é a solução, já que $3^5 = 243$, $243 \pmod{7} = 5$ e $5 \pmod{7} = 5$. Assim $3^5 \equiv 5 \pmod{7}$.

Para grupos enormes, isso é completamente inviável de uma perspectiva computacional clássica.

Algoritmo de SHOR

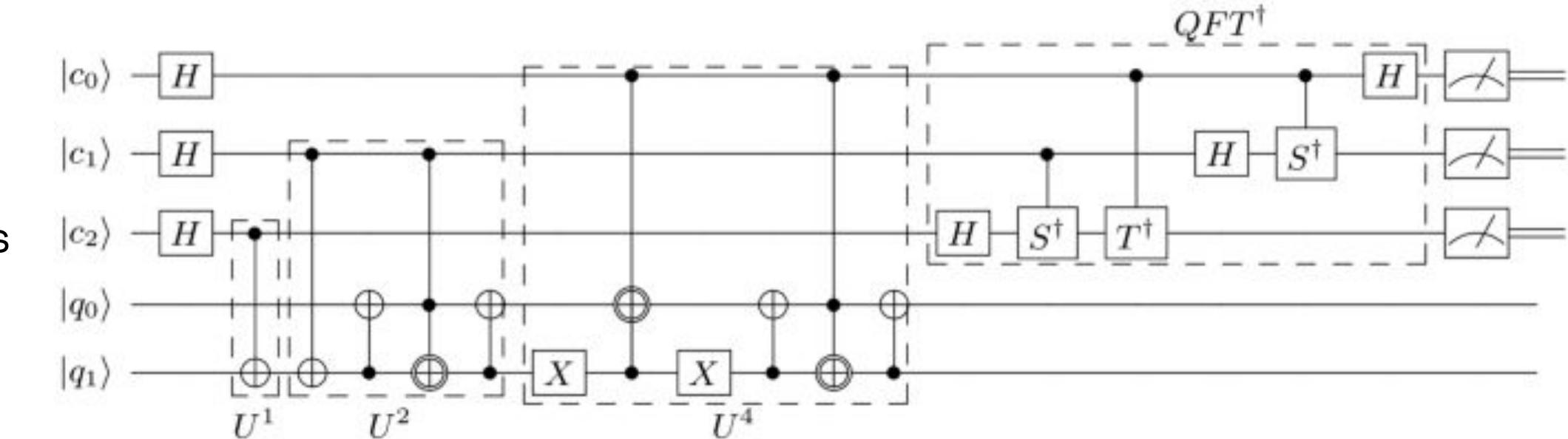
1. O algoritmo de Shor inicia criando uma **superposição quântica** de todos os possíveis estados do sistema, **representando diferentes candidatos para a fatoração**, isso permite explorar múltiplas soluções simultaneamente.



2. No coração do algoritmo está a tarefa de encontrar o período de uma função relacionada ao número que queremos fatorar. Para isso, o algoritmo realiza uma série de operações aritméticas no registrador quântico. Aqui, o **emaranhamento começa a ser introduzido**. Quando o algoritmo quântico aplica essas operações a um registrador quântico, ele emaranha os qubits desse registrador com o valor do número sendo fatorado. Isso cria uma **dependência entre os qubits**, de forma que o estado de um qubit influencia os outros.

Algoritmo de SHOR

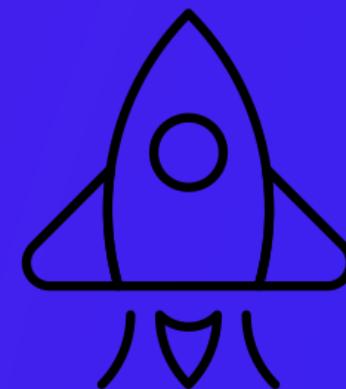
3. Após essa fase de computação, os qubits estão emaranhados de tal forma que as informações sobre a periodicidade estão distribuídas pelos diferentes qubits. Quando o sistema é medido, os qubits colapsam para um único estado, mas o emaranhamento garante que a medição de um conjunto de qubits reflete a informação global do sistema, relacionada ao período da função.



A transformada de Fourier quântica (que é crucial no algoritmo) funciona mais eficientemente devido ao emaranhamento, pois ela correlaciona os qubits de maneira que a periodicidade desejada pode ser extraída com precisão.

Computação Clássica X Computação Quântica

300 trilhões de anos



Fatoração de inteiro de 2048 bits. Algoritmo General Number Field Sieve (GNFS) X Algoritmo de Shor
(em um idealizado computador quântico de 20 milhões de qubits). - Quantum Safe

Tempo polinomial.

8 a 24 horas

CRIPTOGRAFIA PÓS-QUÂNTICA

Desmistificando e simplificando:

Criptografia Quântica

NÃO é =

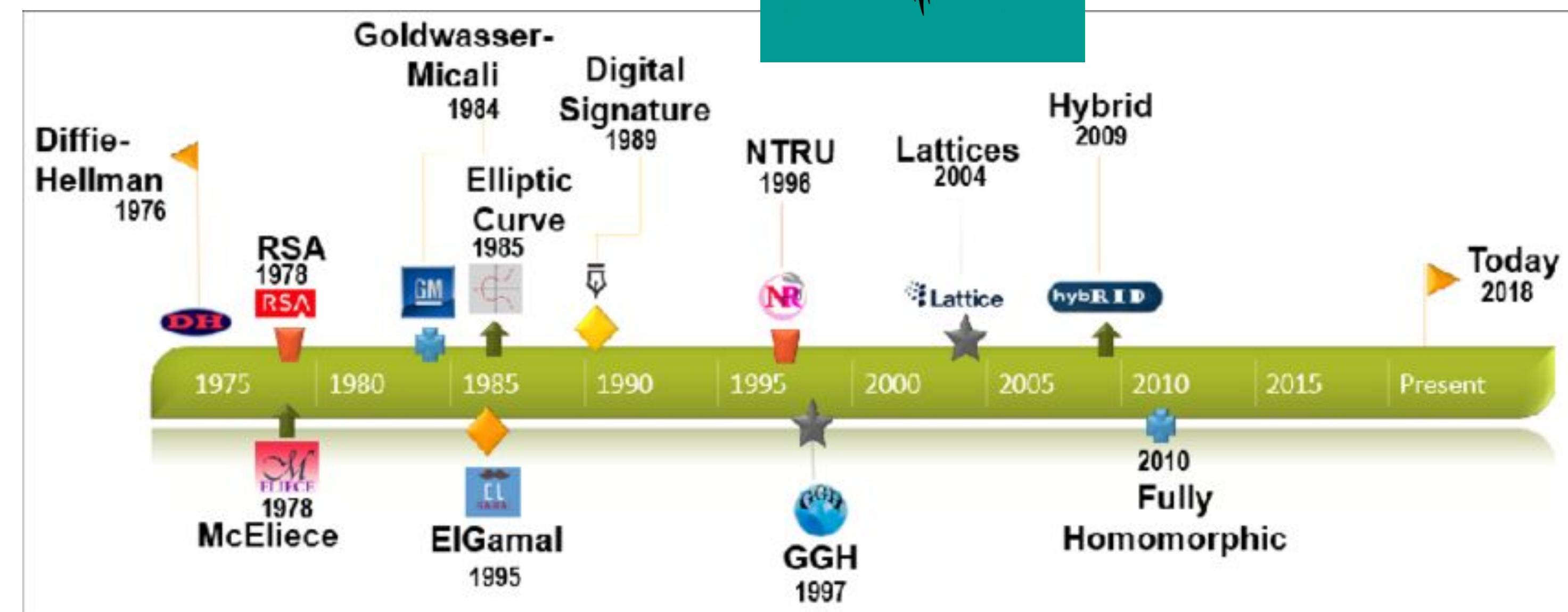
Criptografia Pós-Quântica

Desmistificando e simplificando:

Criptografia Pós-Quântica (atualmente)

é =

Criptografia assimétrica não baseada em
fatoração de números primos, logaritmo discreto
e variações



Problemas de Redes (Lattices)

Uma **rede** é um conjunto de pontos em um espaço n-dimensional que segue padrões matemáticos regulares. Esses pontos são formados por combinações lineares de vetores base.

- **Problema do Vetor Mais Curto (SVP - Shortest Vector Problem):**

Dada uma rede, o desafio é encontrar o vetor mais curto que pertence a ela, exceto o vetor nulo. Resolver isso é difícil porque, em redes de alta dimensão, os pontos estão próximos uns dos outros, dificultando identificar qual é realmente o mais curto.

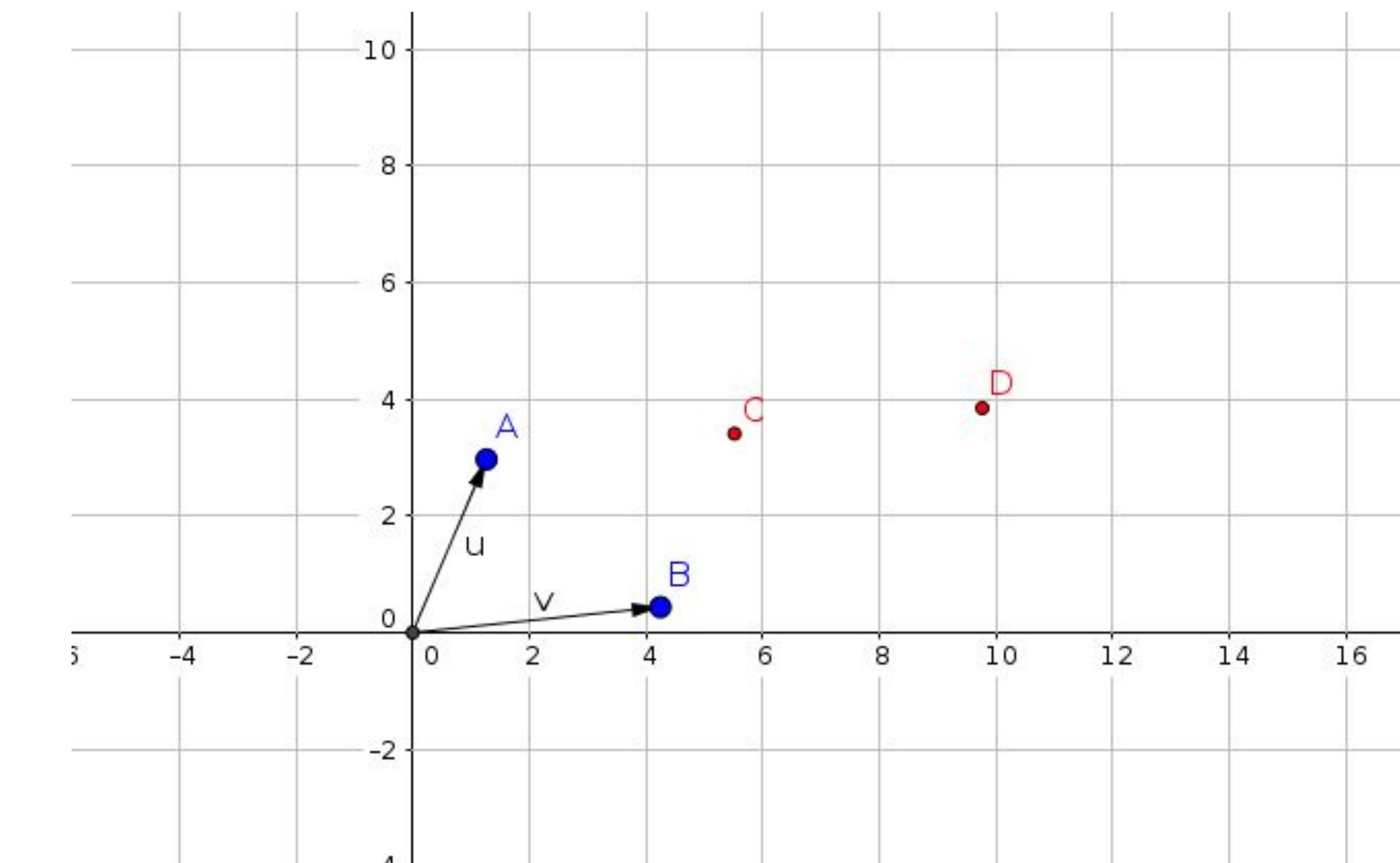
- **Problema do Vetor Mais Próximo (CVP - Closest Vector Problem):**

Dado um ponto qualquer no espaço e uma rede, o objetivo é encontrar o ponto da rede mais próximo ao ponto dado. Isso é computacionalmente difícil porque há muitas possibilidades para verificar.

- **Problema de Aprendizado com Erros (LWE - Learning with Errors):**

Dado um sistema de equações lineares onde pequenas quantidades de erro (ou ruído) foram adicionadas às respostas, o problema é determinar os valores originais antes do erro. A dificuldade vem do fato de que o ruído complica a identificação de soluções únicas.

(Kyber, Dilithium, NTRU)



Problemas de Códigos Corretores de Erros

Códigos corretores de erros adicionam redundância a mensagens para protegê-las contra ruídos. A dificuldade aqui está em reconstruir a mensagem original sem conhecer os detalhes do código usado.

- **Problema de Decodificação (Decoding Problem):**

Dado um vetor codificado que contém erros e uma matriz pública associada ao código, o objetivo é determinar a mensagem original. Sem a matriz secreta que descreve o código, encontrar a mensagem correta é extremamente difícil.

- **Códigos Goppa:**

Esses são códigos corretores de erros específicos que adicionam mais estrutura matemática, dificultando ainda mais a resolução do problema de decodificação sem o conhecimento da matriz secreta.

(McEliece, Niederreiter)

Problemas de Funções de Hash

Funções de hash transformam dados de qualquer tamanho em um valor fixo. A segurança delas está na dificuldade de realizar operações inversas.

- **Problema de Colisão:**

Encontrar duas entradas diferentes que produzam o mesmo hash. Funções hash seguras tornam isso impraticável porque o espaço de possíveis entradas é enorme.

- **Problema de Pré-Imagem:**

Dado um hash, encontrar uma entrada que o gere. Isso é difícil porque funções de hash criptográficas são projetadas para serem irreversíveis.

(SPHINCS+, Lamport One-Time Signatures)

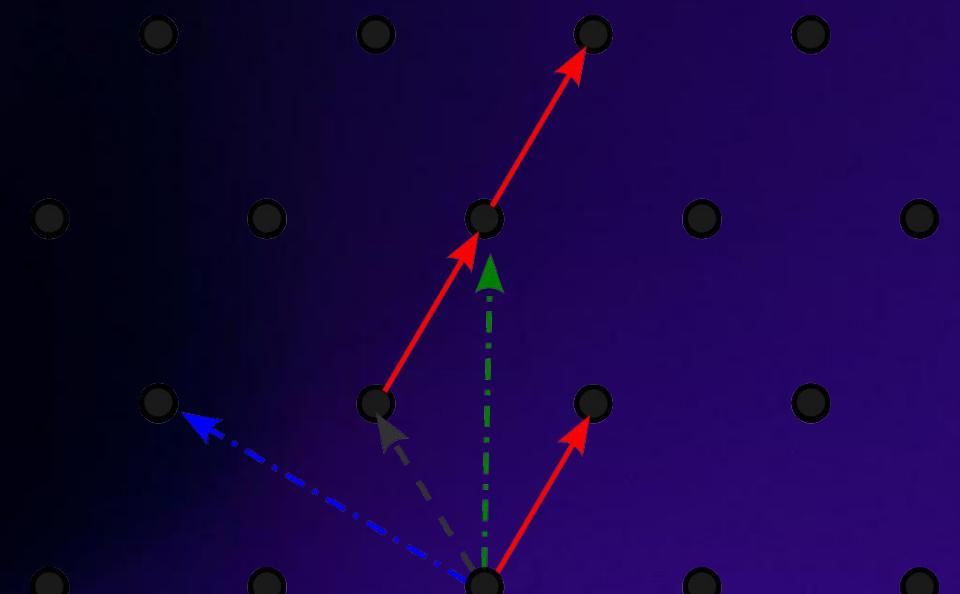
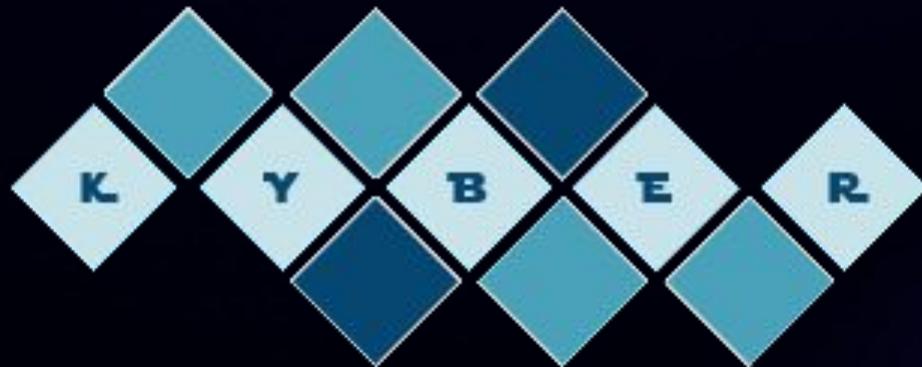
PRINCIPAIS ALGORITMOS PQC

KYBER

//Campeão PQC de KEM

Lattices (ou redes euclidianas) são estruturas matemáticas que consistem em arranjos regulares de pontos no espaço, formados por combinações lineares de vetores. Em termos simples, é como uma grade tridimensional onde cada ponto é uma combinação de vetores base.

FIPS 203



Na criptografia, os problemas associados a encontrar vetores curtos ou soluções em uma lattice são extremamente difíceis de resolver, o que torna essas estruturas úteis para criar algoritmos seguros contra ataques de computadores quânticos.

Baseado em estruturas matemáticas chamadas redes euclidianas (lattices). O problema computacional que sustenta a segurança do **Kyber** é o **Problema de Vetor Curto (SVP - Shortest Vector Problem)** e, mais especificamente, uma variante chamada **LWE (Learning with Errors)**, que se baseia na dificuldade de resolver sistemas lineares com pequenos erros em redes euclidianas. Embora sistemas lineares sem erro sejam facilmente solucionáveis, a presença desses pequenos erros torna o problema extremamente difícil de resolver.

A segurança do Kyber está associada à dificuldade de inverter esse processo, ou seja, de recuperar a chave secreta a partir da chave pública gerada com base em operações do tipo LWE.

Temos dois, sendo duas abordagens diferentes.

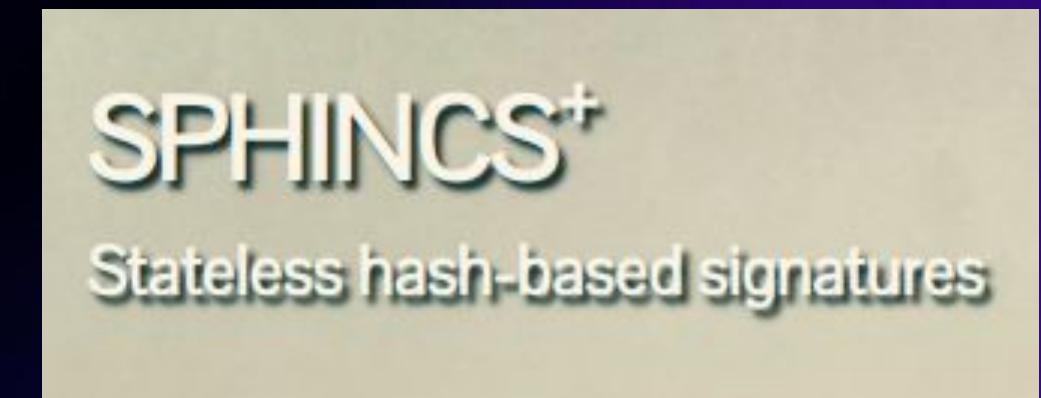
Campeões PQC de Assinatura Digital

FIPS 204



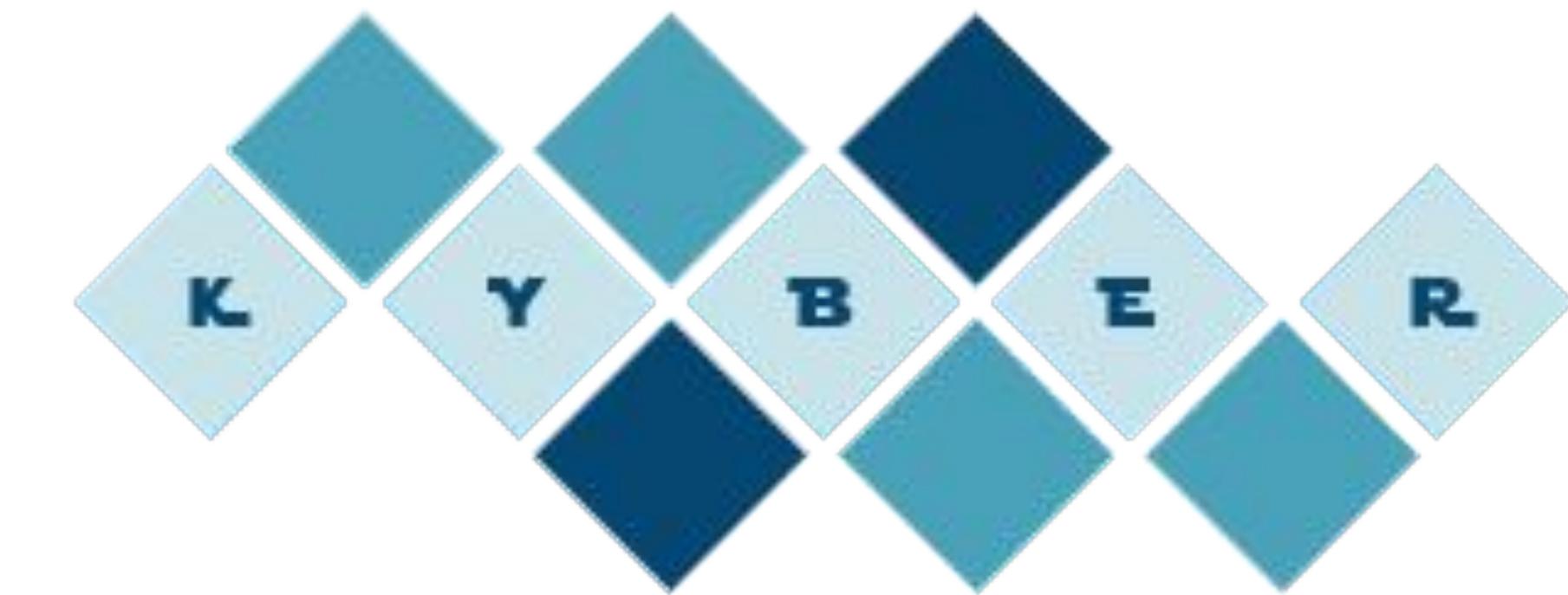
Também baseado em Lattices e no LWE, o problema específico do **Dilithium** é o problema SIS (Short Integer Solution) que envolve encontrar uma combinação linear de vetores inteiros com coeficientes pequenos que resulta em um vetor zero em uma rede. A dificuldade de resolver este problema aumenta com o tamanho da rede e é considerado computacionalmente intratável, mesmo para computadores quânticos.

FIPS 205



SPHINCS+ se baseia na dificuldade de inverter funções hash criptográficas. A segurança do algoritmo deriva da intractabilidade de encontrar colisões ou pré-imagens para funções hash seguras. O SPHINCS+ é projetado para ser seguro contra ataques quânticos, uma vez que a complexidade de ataques quânticos, como o de Grover, ainda não é suficiente para quebrar eficientemente funções hash.

ML - KEM



Fases gerais:

1. Alice gera suas chaves públicas e privadas.
2. Bob encapsula a chave secreta (k) e envia para Alice.
3. Alice decapsula e recupera a chave secreta (k).

Neste exemplo, estou usando vetores de inteiros ao invés de vetores de polinômios, para ilustrar de forma mais fácil.

Alice gera as chaves públicas e privadas:

$q = 17$: Módulo para as operações (um número primo pequeno neste exemplo).

Vetor polinômio $a = [7, 4]$: Um valor público conhecido usado para geração de chaves.

Vetor secreto de Alice (s) = $[3, 5]$: Chave privada de Alice.

Vetor de erro (e) = $[1, 2]$: Um ruído pequeno para segurança.

Alice gera as chaves públicas e privadas:

Alice calcula sua chave pública b usando a fórmula:

$$b = a \cdot s + e \pmod{q}$$

Ex. Para os elementos de b :

$$b[0] = (7 \cdot 3 + 1) \pmod{17} = 22 \pmod{17} = 5$$

$$b[1] = (4 \cdot 5 + 2) \pmod{17} = 22 \pmod{17} = 5$$

Chave pública de Alice (b): [5,5]

Chave privada de Alice (s): [3,5]

Bob encapsula a chave secreta

Vetor secreto de Bob (r) = [2,3]: Escolhido aleatoriamente.

Vetores de erro ($e1$) = [1,2], ($e2$) = [3,1]: Pequenos ruidos aleatórios.

Bob encapsula a chave secreta

Cálculo de $c1$:

$$c1 = a \cdot r + e1 \pmod{q}$$

$$c1[0] = (7 \cdot 2 + 1) \pmod{17} = 15 \pmod{17} = 15$$

$$c1[1] = (4 \cdot 3 + 2) \pmod{17} = 14 \pmod{17} = 14$$

$$c1 = [15, 14]$$

Geração da chave secreta k :

Bob usa uma função hash para derivar k a partir de r :

$$k = \text{Hash}(r) = [7, 7]$$

Bob encapsula a chave secreta

Cálculo de $c2$:

$$c2 = b \cdot r + e2 + k \pmod{q}$$

$$c2[0] = (5 \cdot 2 + 3 + 7) \pmod{17} = 20 \pmod{17} = 3$$

$$c2[1] = (5 \cdot 3 + 1 + 7) \pmod{17} = 23 \pmod{17} = 6$$

Bob envia $c1=[15, 14]$ e $c2=[3, 6]$ para Alice.

Alice decapsula e recupera a chave secreta

Alice usa $c1$, $c2$, e sua chave privada $s=[3, 5]$ para recuperar k .

Alice usa a fórmula:

$$k = c2 - s \cdot c1 \pmod{q}$$

Alice decapsula e recupera a chave secreta

$$k[0] = (3 - (3 \cdot 15)) \bmod 17 = (3 - 45) \bmod 17 = -42 \bmod 17 = 9$$

$$k[1] = 6 - (5 \cdot 14) \bmod 17 = k[1] = 6 - 70 \bmod 17 = -64 \bmod 17 = 4$$

$$k = [9, 4]$$

Lembrando que esse exemplo é um cenário reduzido, na prática usariamos polinômios. Deixei um exemplo mais completo no rep.

Transicionando para PQC

//Conscientização

CURTO PRAZO

A responsabilidade primária de trazer a questão da transição PQC para a empresa é do CISO (Chief Information Security Officer).



Se a questão não for levantada pelo CISO, colaboradores do departamento podem e devem levantar a questão, respeitando a cultura e dinâmica hierárquica da organização.

Dica: Ao abordar o assunto, é essencial reforçar que a transição para a PQC não é uma escolha opcional ou uma mera melhoria de tecnologia que pode ser negligenciada. Trata-se de uma necessidade inevitável que todas as organizações, sem exceção, terão que enfrentar. A questão não é se a transição será feita, mas como ela será conduzida: de maneira planejada e estratégica ou de forma reativa e potencialmente prejudicial.

CURTO PRAZO

Transicionando para PQC

//Conscientização

O CISO, em conjunto com o CTO (Chief Technology Officer) e colaboradores designados devem buscar educação no tema e elaborar um roadmap inicial da transição, juntamente com um levantamento e apresentação da questão, dos impactos e de oportunidades.

O conselho deve ser informado o mais breve possível da questão, a transição não precisa e não deve ser apenas um fator de sobrevivência. Uma boa preparação para a transição pode trazer benefícios e oportunidades para organização.

CURTO PRAZO

Transicionando para PQC

//Profissionais e Qualificação

Estabelecida a vontade da transição, deve-se designar colaboradores capacitados para o projeto. Nesta etapa, a organização precisará investir em contratações de especialistas em criptografia ou na qualificação profissional de seus colaboradores, como a disponibilizada pelo Inteli.

É preciso entender que especialistas em cibersegurança não são, necessariamente, qualificados no tópico criptografia.

Organizações que investirem na educação dos seus colaboradores, estarão criando capital humano valioso. Empresas que não se preparam antecipadamente encontrarão dificuldades para contratação.



CURTO PRAZO

Transicionando para PQC

// Mapeamento de Dependência
Criptográficas

O primeiro passo concreto, descrito pelo NIST é a identificação de onde e para quê propósito, a criptografia de chave pública está sendo usada na organização.

Porém, podemos expandir essa atividade que será necessária a todas as organizações e transformá-la em uma oportunidade de amadurecimento e implementação da chamada **Cryptographic Agility**, que vai além da transição objetiva. Transformando essa tarefa em uma mapeamento completo de todos os módulos criptográficos utilizados e levantando informações não só necessárias para o início da adaptação para PQC, mas também, para a implementação de um gerenciamento ágil de criptografia.



CURTO PRAZO

Transicionando para PQC

// Mapeamento de Dependência
Criptográficas

Transição PQC

Utilizamos o mapeamento para verificar quais módulos criptográficos precisarão ser trocados para PQC e o que está sendo protegido por cada um deles.

Implementação Agility

Utilizamos o mapeamento para verificar se os algoritmos criptográficos usados estão implementados de forma modularizada (fácil de trocar), se estão implementados corretamente, se as soluções utilizadas continuam atualizadas e possuem preparação Quantum Safe.

Transicionando



para PQC

//Priorização de ativos

CURTO PRAZO

O próximo objetivo do projeto é classificar os componentes que precisam ser considerados primeiro na migração usando uma metodologia de gestão de risco já adotada pela organização que analise a sensibilidade e criticidade da informação.

Neste ponto é importante notar o tempo de vida útil do dado, por exemplo, um ativo que é crítico hoje pode não ser tão relevante até a concretização de uma ameaça quântica.

- Ativos críticos com um longo tempo de vida devem ser priorizados.

Esse processo deve ser feito em conjunto com o time de análise de riscos.

Transicionando para PQC

//Priorização de ativos

CURTO PRAZO

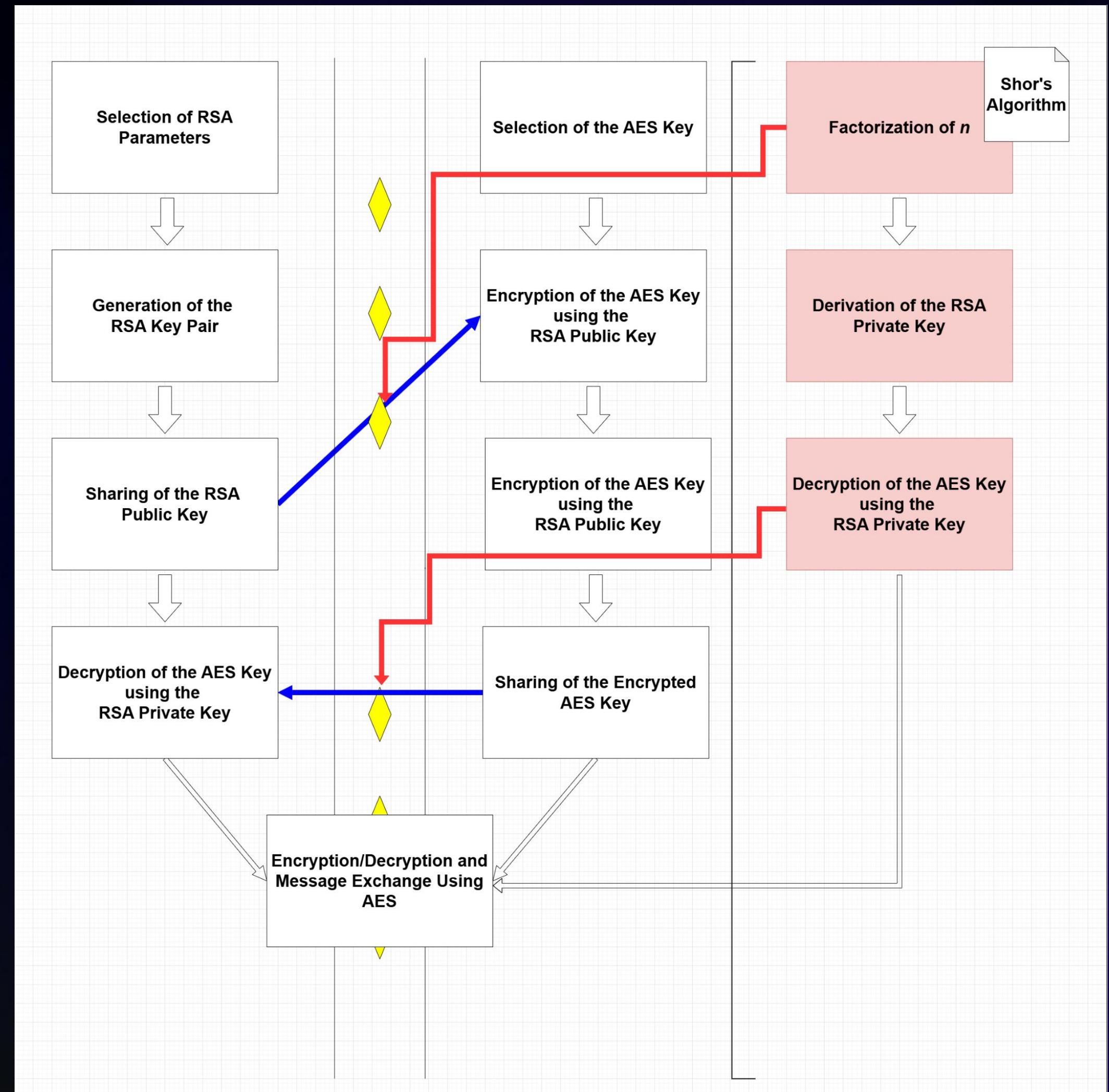


Mas qual o sentido de priorizar se todos os módulos vão precisar serem substituídos?

Ataque Colha Agora, Espere Amadurecer - Store (Harvest) Now, Decrypt Later (SNDL).



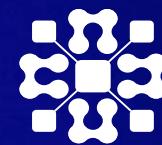
- As informações de hoje serão descriptadas amanhã. Atividade cibercriminosa atual com objetivo à longo prazo.



Transicionando para PQC

//Familiarização com soluções

CURTO PRAZO



Simultaneamente, é preciso que a equipe comece a se familiarizar com possíveis soluções de implementações futuras através de pequenos **toy examples**. Uma boa prática é manter um repositório atualizado com considerações e aprendizados sobre cada solução.

- Exemplos de bibliotecas candidatas:

Open Quantum Safe (liboqs)

OpenSSL com suporte ao OQS

Bouncy Castle (BCPQ)

PQClean



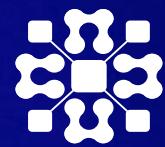
Transicionando para PQC

//Avaliação de dependência de

terceiros

(Supply-Chain)

CURTO PRAZO



Nem todos os fornecedores estarão no mesmo ritmo de adaptação à PQC. Isso pode gerar um ponto fraco, uma vez que fornecedores lentos na adaptação deixam a cadeia de suprimentos vulnerável. A gestão de risco deve incluir um plano para identificar e mitigar atrasos de fornecedores cruciais.

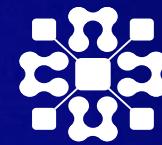
Converse com seus representantes, informe a necessidade da questão. Troque se for necessário.



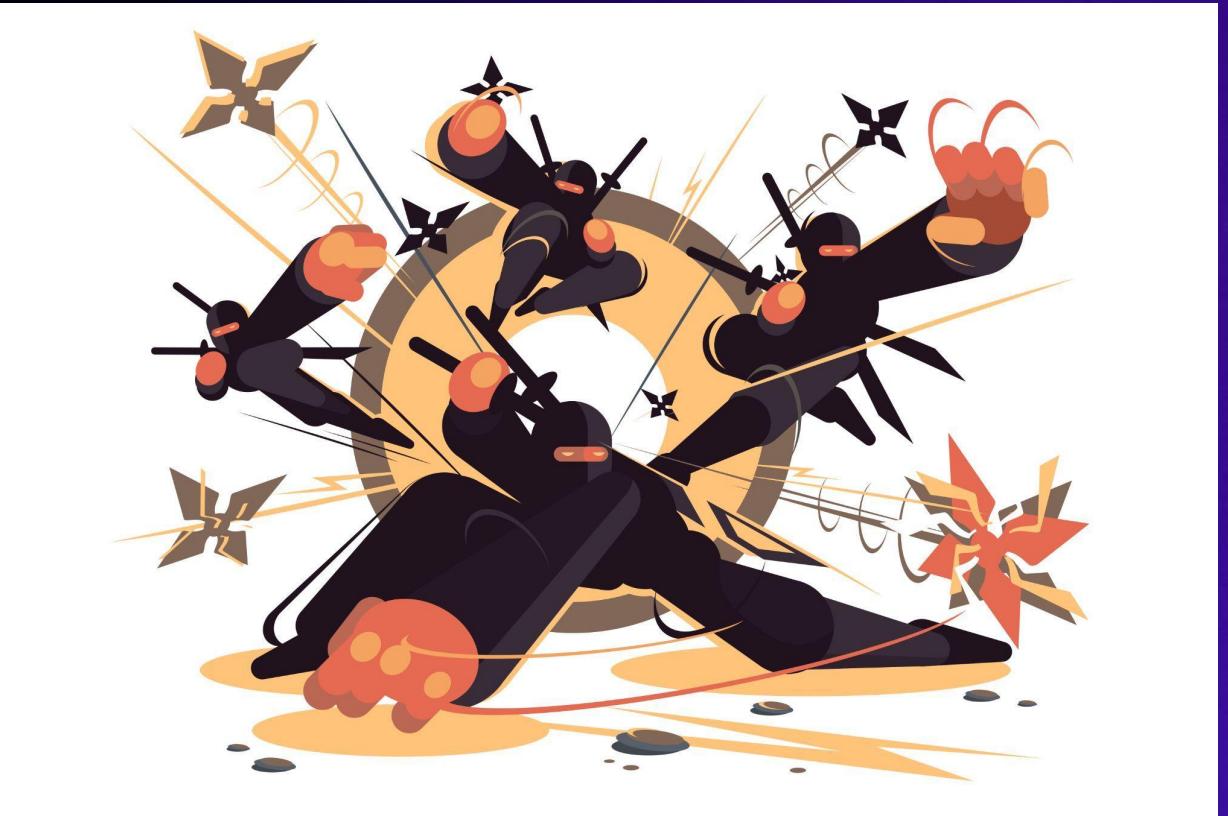
CURTO PRAZO

Transicionando para PQC

// Implementação do Cryptographic
Agility



- Modularidade
- Independência de algoritmos
- Verificação da conformidade com padrões abertos
- Automatização consciente de atualizações
- Gestão de chaves robusta
- Avaliação contínua
- Associação com fornecedores maduros



Transicionando para PQC

CURTO PRAZO

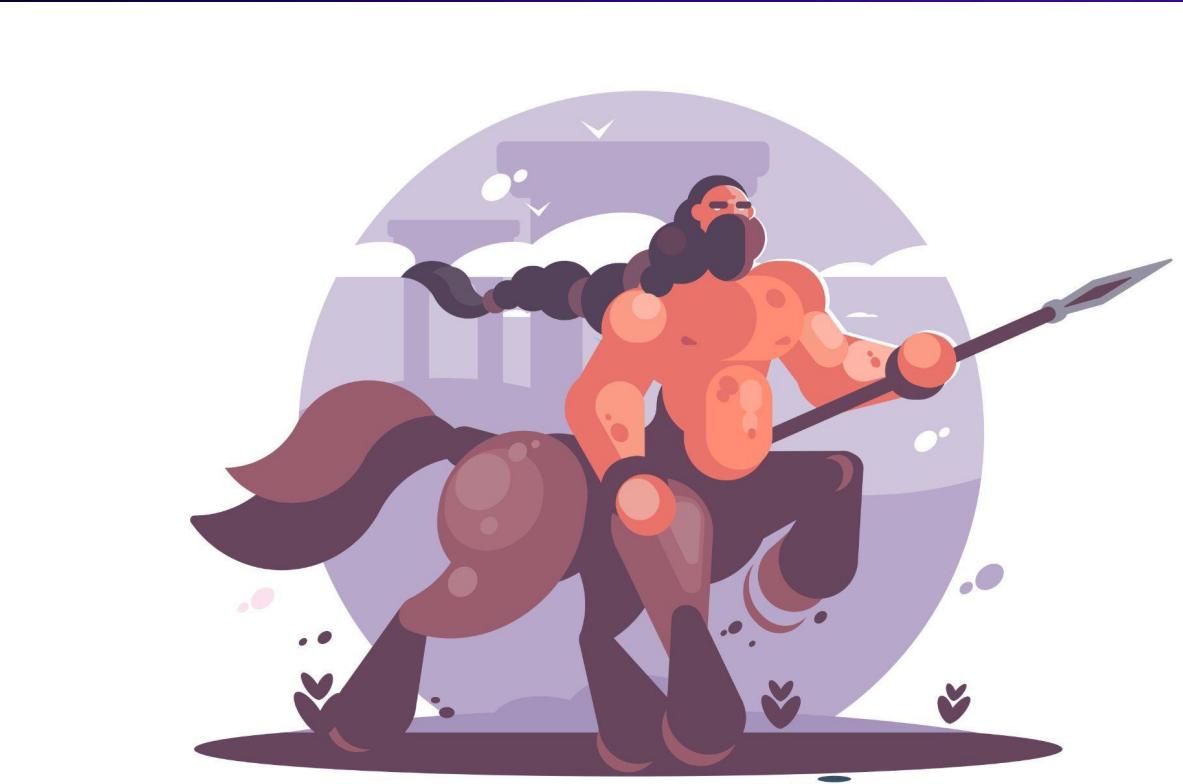
// Implementação de Criptografia Híbrida
Estrita em ativos prioritários

Ainda estamos em um período de desenvolvimento de implementações dos algoritmos padronizados e nenhuma solução ainda foi certificada e é considerada segura para uso.

Porém devido a criticidade de certos ativos e a possibilidade de uma coleta atual para execução do ataque SNLD, uma abordagem já adotada é o duplo uso criptográfico de o esquema padrão já utilizado com uma camada adicional de com um esquema PQC.

Há um claro trade-off entre segurança e eficiência, que deverá ser considerado.

As implementações PQC atuais ainda não devem ser utilizadas sozinhas.



Transicionando para PQC

// Implementação de Criptografia

MÉDIO PRAZO

Híbrida Flexível

Implementação de criptografia híbrida flexível em todos os módulos criptográficos vulneráveis, essa abordagem possibilita utilizar um esquema (PQC ou não) quando o outro não está disponível ou quando é mais eficiente, alternando conforme as necessidades ou limitações do ambiente.

Nessa etapa, a preparação principal da organização para a transição está pronta, porém os padrões não PQC continuam operando na comunicação com partes terceiras ainda não preparadas.

Timing para oportunidades com atrasados.



Transicionando para PQC

//Transição Total - Criptografia PQC
Estrita

LONGO PRAZO

- Considerando um tempo de precaução determinado pela equipe de análise de riscos em consideração a iminente futura viabilização da ameaça quântica, conclui-se a transição e todos os módulos criptográficos baseados no problema da fatoração e no problema do logaritmo discreto são desligados e substituídos pelos novos padrões pós-quânticos.

EMPREENDER EM CRIPTOGRAFIA PÓS-QUÂNTICA?