Criptografia Quântica

Gustavo Thebit Pfeiffer
Rodrigo Rodrigues Paim
Vinicius Neves Motta

Criptografia

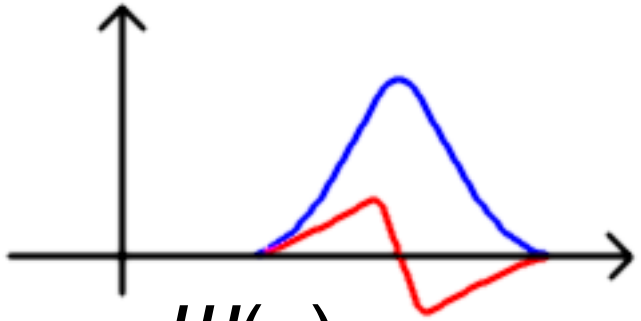
- Criptografia Simétrica
- Criptografia Assimétrica
  - RSA
- Função Resumo

Computação Quântica

Mecânica Clássica

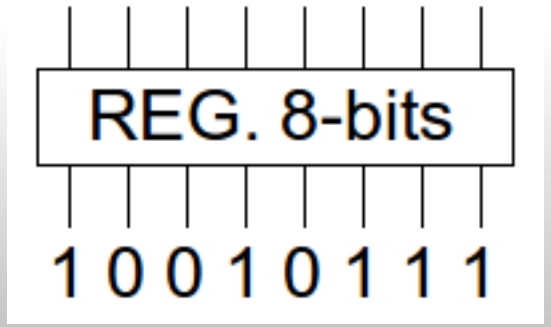
x = 53m

Mecânica Quântica



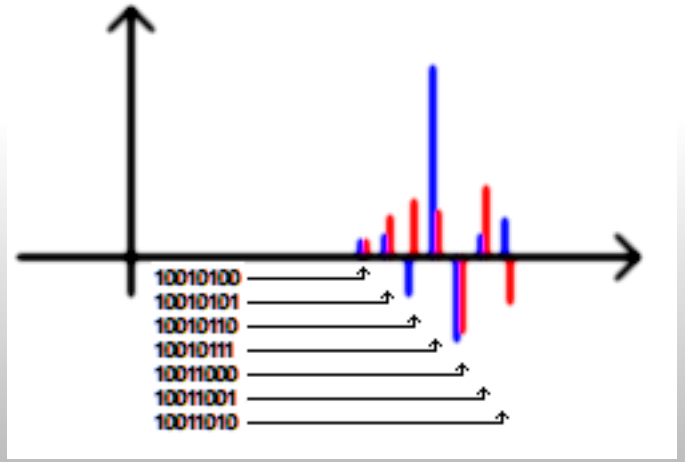
$\Psi(x)$ = ...

Computação Clássica



x = 10010111

Computação Quântica



$\Psi(x)$ = ...

Como funciona?

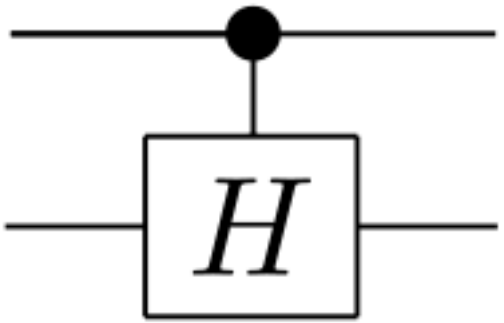
Computação Clássica

Porta Lógica

00	0
01	0
10	0
11	1

Tabela-verdade

Computação Quântica



Porta Quântica

$$\begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \end{array}$$

Matriz unitária

Alguns Princípios

- Operações reversíveis
- Impossibilidade de cópia (clonagem)

- Medida
  - Colapso da função de onda
  - Irreversível
  - Resultado Probabilístico

Futuro Distante?

- IBM (Final do Século Passado)
  - 2, 3 e 5 Q-bits
- Yale
  - 2 Q-bits, em estado sólido
- IBM (2001)
  - 7 Q-bits
  - Algoritmo de Shor: Número 15
- D-Wave One (2011) (duvidável)
  - 128 Q-bits, programável
  - Dedicado a algoritmos de otimização

Criptografia Quântica

- Criptografia que utiliza fenômenos quânticos
- *Quantum Key Distribution*
  - Geração de uma chave secreta
- *Quantum coin-tossing* e *Oblivious Transfer*
  - Utilizado em situações em que os dois lados da comunicação não se confiam

QKD: Protocolo BB84

- A e B desejam criar uma chave secreta.
- A gera uma sequência de bits (0 ou 1) e bases (retilínea ou diagonal)

A	
↕	1
⤨	1
⤨	0
↕	1
⤨	0
↕	0
⤨	0
↕	1

QKD: Protocolo BB84

- B tenta detectar os bits sem saber a base.
- Se a base for a mesma, o bit é lido corretamente, senão, há 50% de chance de acerto.

A		B	
+	1	×	0
×	1	×	1
×	0	+	0
+	1	+	1
×	0	+	1
+	0	+	0
×	0	×	0
+	1	×	1

QKD: Protocolo BB84

- Após a comunicação, A e B anunciam as bases utilizadas. Quando as bases forem diferentes, o resultado é descartado.

A		B		A	B	chave
↕	1	⤨	0	↕	⤨	
⤨	1	⤨	1	⤨	⤨	1
⤨	0	↕	0	⤨	↕	
↕	1	↕	1	↕	↕	1
⤨	0	↕	1	⤨	↕	
↕	0	↕	0	↕	↕	0
⤨	0	⤨	0	⤨	⤨	0
↕	1	⤨	1	↕	⤨	

Ataques possíveis ao BB84?

- Interceptação do canal quântico?
- Interceptação das bases?
- Homem do meio?

A		B		A	B	chave
↕	1	⤨	0	↕	⤨	
⤨	1	⤨	1	⤨	⤨	1
⤨	0	↕	0	⤨	↕	
↕	1	↕	1	↕	↕	1
⤨	0	↕	1	⤨	↕	
↕	0	↕	0	↕	↕	0
⤨	0	⤨	0	⤨	⤨	0
↕	1	⤨	1	↕	⤨	

QKD: Protocolo B92

- A e B geram suas sequências aleatórias
- A envia conforme '0' = vertical e '1' = diagonal +45º
- B tenta detectar '0' = diagonal -45º e '1' = horizontal
- B diz em quais posições o bit foi detectado

A	B	A	B	resultado	chave
0	1	↕	↔	não detecta	
0	1	↕	↔	não detecta	
1	1	↗	↔	não detecta	
0	0	↕	↖	detecta	0
1	1	↗	↔	detecta	1
1	0	↗	↖	não detecta	
0	0	↕	↖	não detecta	
1	0	↗	↖	não detecta	

Ataques possíveis ao B92?

- Interceptação do canal quântico?
- Interceptação do resultados enviados por B?
- Homem do meio?

A	B	A	B	resultado	chave
0	1	↕	↔	não detecta	
0	1	↕	↔	não detecta	
1	1	↗	↔	não detecta	
0	0	↕	↖	detecta	0
1	1	↗	↔	detecta	1
1	0	↗	↖	não detecta	
0	0	↕	↖	não detecta	
1	0	↗	↖	não detecta	

Quantum Coin-Tossing

- Definição:
  - "Cara ou Coroa" à distância entre duas pessoas A e B
  - Ausência de um mediador

- Protocolo:
  - Codificação de bits em fótons por A;
  - Detecção dos fótons por B;
  - B opina qual base de polarização foi utilizada para codificar os bits;
  - A diz se ele acertou ou não e manda os bits usados por ele para B, para que B comprove que não houve trapaças;

Quantum Coin-Tossing

- Ataques:
  - EPR
    - Definição
    - Aplicação para ataque
- Aplicações:
  - "Poker Mental"
  - Certificação de e-mail

Oblivious Transfer

- Definição:
  - Troca de mensagens de forma discreta.
  - Ausência de um mediador
- Protocolo:
  - Codificação de um bit em dois fótons;
  - Uma pessoa A envia os fótons para uma pessoa B;
  - Detecção de fótons por B
  - Caso não consiga detectar, A reenvia os fótons
- Ataques:
  - EPR
- Aplicação:
  - Resolver um objetivo comum sem revelar informações desnecessárias

Avanços Recentes

- Implementação física de CQ:
  - Tecnologias Atuais
  - Limitações

- Implementação futura:
  - "Retransmissor Quântico"
  - Necessidade de armazenar fóton por um período de tempo

Criptoanálise Quântica

- Criptoanálise que utiliza computação quântica

- Amplificação de Amplitude
  - Problemas combinatoriais
    - Clássico: $O(N)$
      - Testar todas as possibilidades
    - Quântico: $O(\sqrt{N})$
      - Baseado em autovalores

Criptoanálise Quântica

- Algoritmo de Shor
  - Fatoração da chave RSA
    - Descobrir p e q tal que $p \cdot q = n$
  - Custo polinomial!
    - $O((\log(n))^2.(\log(\log(n)).(\log(\log(\log(n)))))$
  - Tenta descobrir $\phi(n)$ analisando o período da função a^x mod n
  - Isso é otimizado através da Transformada de Fourier Quântica
    - QFT: $O(\log(n)\ \log(\log(n)))$ -> polinomial
    - FFT: $O(n\ \log(n))$ -> exponencial

Algoritmo de Shor e QFT

- Exemplo: período = 4, #amostras = 8

a^x \ x	0	1	2	3	4	5	6	7
0	$\frac{1}{\sqrt{8}}$	$\frac{1}{\sqrt{8}}$	$\frac{1}{\sqrt{8}}$	$\frac{1}{\sqrt{8}}$	$\frac{1}{\sqrt{8}}$	$\frac{1}{\sqrt{8}}$	$\frac{1}{\sqrt{8}}$	$\frac{1}{\sqrt{8}}$
1								
2								
3								
4								
5								
6								
7								

3 Q-bits para x

3 Q-bits para a^x

x: dist. unif.

$a^x = 0$

Algoritmo de Shor e QFT

- Computamos a^x mod n

a^x \ x	0	1	2	3	4	5	6	7
0								
1	$\frac{1}{\sqrt{8}}$				$\frac{1}{\sqrt{8}}$			
2								
3				$\frac{1}{\sqrt{8}}$				$\frac{1}{\sqrt{8}}$
4		$\frac{1}{\sqrt{8}}$				$\frac{1}{\sqrt{8}}$		
5			$\frac{1}{\sqrt{8}}$				$\frac{1}{\sqrt{8}}$	
6								
7								

x e a^x estão emaranhados

Algoritmo de Shor e QFT

- Em seguida aplicamos QFT em x

a^x \ f	0	1/8	2/8	3/8	4/8	5/8	6/8	7/8
0								
1	$\frac{1}{4}$		$\frac{1}{4}$		$\frac{1}{4}$		$\frac{1}{4}$	
2								
3	$\frac{1}{4}$		$\frac{i}{4}$		$\frac{-1}{4}$		$\frac{-i}{4}$	
4	$\frac{1}{4}$		$\frac{-i}{4}$		$\frac{-1}{4}$		$\frac{i}{4}$	
5	$\frac{1}{4}$		$\frac{-1}{4}$		$\frac{1}{4}$		$\frac{-1}{4}$	
6								
7								

Frequências múltiplas de 1/período

Criptografia Pós-Quântica

- Criptografia "à prova de" criptoanálise quântica
- Utiliza computação clássica
  - Criptografia baseada em Hash
    - Algoritmo de Lamport-Diffie
    - Árvore de Merkle
  - Criptografia baseada em código
    - Sistema McEliece
  - Criptografia baseada em látice

Algoritmo de Lamport-Diffie

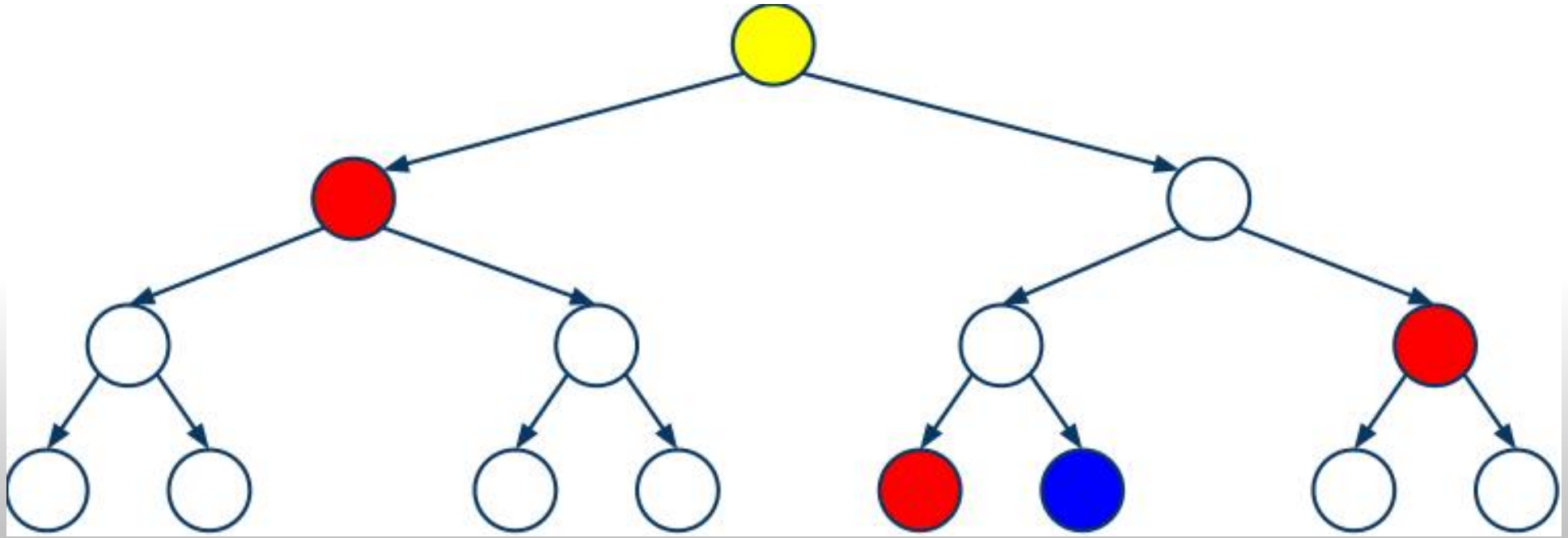
- Usado para autenticação
- Par de chaves (A, B) de 2^n bits
- Usados n^2 efetivamente
  - Escolha: função resumo g de n bits
- Função resumo f: $B_i = f(A_i)$
- Entidade emissora: possui A, B
- Entidade receptora: possui B
- Par de chaves descartável: uso único
- Curiosidade: passando B para o receptor

Árvore de Merkle

- Árvore cheia de altura *h*
  - Folha (2^h - 1): par de chaves (*A*, *B*)
- Função resumo *g*: Nó = *g*(filho esquerdo | filho direito)
  - Raiz: Chave Pública
- Autenticação: Escolhe uma folha e repete o procedimento de Lamport-Diffie
  - Envia caminho + posição da folha + chave privada (de Lamport-Diffie)
  - Usuário repete o procedimento de Lamport-Diffie e percorre a árvore até a raiz

Árvore de Merkle

- Pode ser usado, no mínimo, 2^h vezes
  - Pior caso: descobre sempre o "valor completo" da folha em 2 tentativas



Código Linear

- Código $C(n, k, d)$:
  - Palavras de código de n bits
  - Representa valores de k bits
  - Distância de Hamming d:
    - Corrige até $d / 2 + 1$ erros
- Palavras de código: Combinação Linear da matriz geradora
- Exemplo: Código Goppa

Sistema de McEliece

- Usado para troca de mensagens

- Matriz Geradora G: k x n
- Matriz Inversível S: k x k
- Matriz de Permutação P: n x n

- Chave Pública = ($G' = SGP$, quantidade de erros)
- Chave Privada = (P^{-1}, G, S^{-1})

- Problema: Chaves muito grandes (~ 64 kB)

Sistema de McEliece

- Encriptação:
  - Divisão em blocos de tamanho *k*

Criação de perturbação aleatória de *t* erros

  - Mensagem Encriptada = bloco *x* *G′* + vetor de erros
- Decriptação:
  - Aplicação de P^{-1}
  - Correção do valor gerado
  - Multiplicação por P^{-1}
- Robustez: Dificuldade em recuperar *S*, *G*, *P* a partir de *G*', ou de fazer a detecção de erro utilizando apenas *G*'.

Conclusões

- Criptografia quântica
  - Mais segura que a clássica
    - Interceptação
- Criptoanálise quântica
  - Quebra o RSA
  - "Força bruta" quebra chaves com pelo menos o dobro do tamanho
- Criptografia pós-quântica
  - Ainda há esperança!
  - Algoritmos clássicos ainda resistentes

Antes de passar para as 5 perguntas...

Dúvidas?

Perguntas

1) Por que a computação quântica ameaça os sistemas criptográficos atuais?

Perguntas

1) Por que a computação quântica ameaça os sistemas criptográficos atuais?

R: Porque o algoritmo de Shor torna vulneráveis os protocolos cuja segurança é baseada em fatoração de números inteiros (como RSA) e logaritmo modular (como Diffie-Hellman)

Perguntas

2) Em que fenômeno quântico se baseia a segurança dos protocolos QKD em geral?

Perguntas

2) Em que fenômeno quântico se baseia a segurança dos protocolos QKD em geral?

R: Impossibilidade de copiar (clonar) ou medir integralmente a função de estado de uma partícula.

Perguntas

3) Cite e explique um tipo de ataque ao qual o protocolos QDK são vulneráveis.

Perguntas

3) Cite e explique um tipo de ataque ao qual o protocolos QDK são vulneráveis.

R: Ataque do homem do meio. Quando não há autenticação, um terceiro pode se passar por A e por B, interrompendo e modificando as comunicações tanto no canal quântico quanto no digital.

Perguntas

4) Por que o par de chaves usados no algoritmo de Lamport-Diffie é de uso único?

Perguntas

4) Por que o par de chaves usados no algoritmo de Lamport-Diffie é de uso único?

R: Pois para as duas chaves criptográficas usadas no algoritmo, cada uma das *n* strings pode assumir apenas dois valores. A opção é feita com base na aplicação da função resumo sobre a mensagem: os *n* bits do resultado identificarão a permutação de valores das chaves. Portanto, a geração de duas mensagens tais que a aplicação de hash nelas gere sequências de bits complementares permitirá que um usuário mal-intencionado saiba o resultado da chave de assinatura e use esta informação para fins não-ortodoxos.

Perguntas

5) Qual é o ataque que é efetivo para os protocolos de Cara ou Coroa e Transferência Inconsciente? É possível implementá-lo, por que?

Perguntas

5) Qual é o ataque que é efetivo para os protocolos de Cara ou Coroa e Transferência Inconsciente? É possível implementá-lo, por que?

R: O efeito Einstein-Podolsky-Rosen (EPR). Não, não é possível implementá-lo, pois a tecnologia atual não é suficientemente desenvolvida para isso (na computação quântica).

Mais dúvidas?

Obrigado!