Fundamentos de teoria quântica

Aula 9: Criptografia

Rafael Rabelo – rabelo@ifi.unicamp.br

Departamento de Física da Matéria Condensada
Instituto de Física "Gleb Wataghin"
Universidade Estadual de Campinas

Criptografia

Criptografia é a ciência e a arte de se armazenar e transmitir informação de forma segura.

Armazenamento seguro: funções hash

Uma *função hash criptográfica* é um algoritmo que mapeia dados de tamanho arbitrário em um *bit string* de tamanho fixo, tal que

- é determinística;
- é *one-way*, praticamente infactível de ser invertida;
- é infactível que duas mensagens gerem o mesmo hash;
- uma pequena mudança na mensagem deve gerar uma mudança extensa no hash.

Chaves públicas e chaves privadas

- Criptografia de chave pública: a chave para encriptação é disponibilizada publicamente. A chave para decriptação é conhecida somente pela parte recebedora. A segurança depende da dificuldade de resolução de problemas matemáticos.
- Criptografia de chave privada: As chaves criptográficas são conhecidas somente pelas partes legítimas. A segurança é incondicional. O maior desafio é a distribuição das chaves para as partes.

Criptografia de chave pública: RSA

O princípio básico por trás do algoritmo RSA é a observação de que é possível encontrar três inteiros positivos grandes e, d e n tais que, para todo $0 \leq m < n$:

$$(m^e)^d = m \mod n.$$

Algoritmo RSA

1. Escolha dois primos distintos p e q;
2. calcule $n = pq$;
3. calcule $\phi(n) = \phi(p)\,\phi(q) = (p-1)(q-1)$, onde

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

   é a *função totiente de Euler*, e p's são os fatores primos de n;
4. escolha um inteiro e tal que $\text{mdc}(e, \phi(n)) = 1$;
5. determine $d = e^{-1} \mod \phi(n)$.

Algoritmo RSA

A *chave pública* é o par (n, e), e a *chave privada* é o número d.

Na etapa de *encriptação*, calcula-se

$$c = m^e \mod n.$$

Na etapa de *decriptação*, calcula-se

$$c^d = (m^e)^d = m \mod n.$$

A segurança do protocolo se baseia na dificuldade de se calcular d, que é essencialmente a dificuldade de se calcular $\phi(n)$, que, por sua vez, se reduz à dificuldade de se fatorar n.

Criptografia de chave privada: one-time pad

- Suponha que Alice e Bob compartilham chaves criptográficas dadas por sequências de n bits perfeitamente correlacionadas

$$\mathbf{k}_A = \mathbf{k}_B = [k_1, \ldots, k_n] .$$

- Seja $\mathbf{m}$ a mensagem de Alice, codificada em n bits.
- Na etapa de encriptação, calcula-se

$$\mathbf{c} = \mathbf{m} \oplus \mathbf{k}_A .$$

- Na etapa de decriptação, calcula-se

$$\mathbf{c} \oplus \mathbf{k}_B = \mathbf{m} \oplus \mathbf{k}_A \oplus \mathbf{k}_B = \mathbf{m} .$$

Condições de segurança

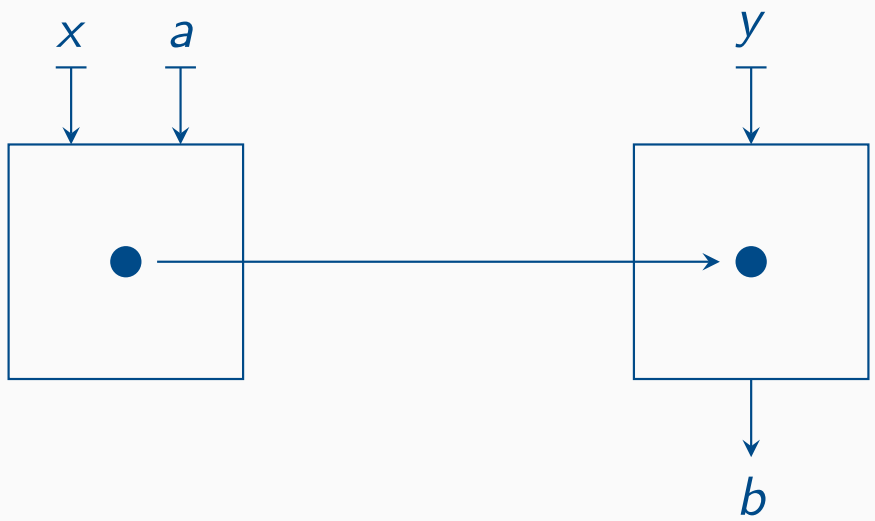
O protocolo *one-time pad* é incondicionalmente seguro se satisfeitas as seguintes condições:

- os elementos da chave devem ser gerados de forma aleatória e independente;
- a chave deve ser utilizada uma única vez.

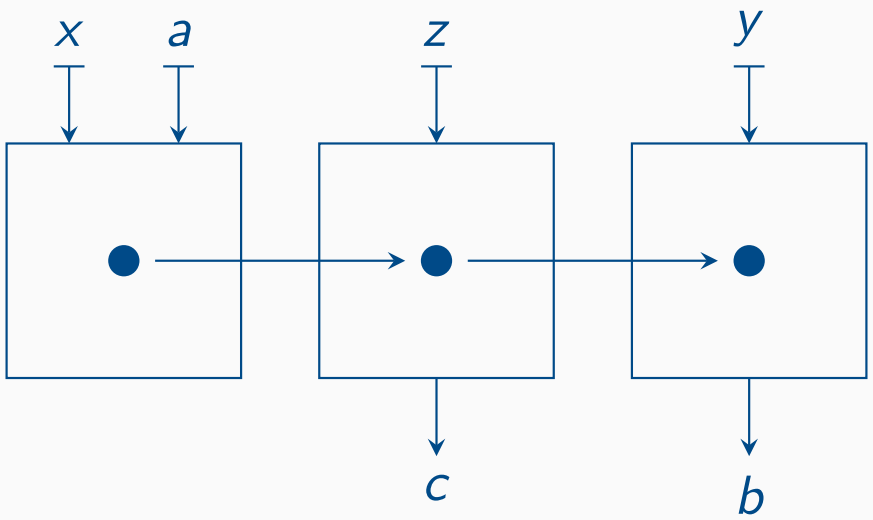
Distribuição quântica de chaves (QKD)

Os processos de *distribuição quântica de chaves* são algoritmos de processamento de informação quântica para a distribuição segura de chaves criptográficas privadas, que podem ser posteriormente utilizadas para comunicação segura por meio de *one-time pad*.

Cenário prepare-and-measure



Eva



O protocolo BB84 (Bennett-Brassard 1984)

1. Alice sorteia bits x e a, e prepara o sistema no estado $\left|\psi_{a|x}\right\rangle$, onde

$$\left|\psi_{0|0}\right\rangle = |0\rangle\,, \quad \left|\psi_{0|1}\right\rangle = |+\rangle\,,$$
$$\left|\psi_{1|0}\right\rangle = |1\rangle\,, \quad \left|\psi_{1|1}\right\rangle = |-\rangle\,.$$

2. Ao receber o sistema, Bob sorteia o bit y, e realiza a medição projetiva $\left\{\left|\psi_{b|y}\right\rangle\!\left\langle\psi_{b|y}\right|\right\}_{b=0,1}$.
3. Se $x = y$, então $a = b$ com probabilidade 1;
   se $x \neq y$, então $a = b$ com probabilidade $1/2$.
4. Ao fim de n rodadas, Alice e Bob anunciam publicamente os bit strings $\mathbf{x}$ e $\mathbf{y}$, e descartam todos os bits a_i e b_i para os quais, na i-ésima rodada, $x_i \neq y_i$.

Segurança

- Suponha que Eva intercepta o sistema quântico, com a intenção de aprender alguma informação da chave em distribuição.
- O teorema da não-clonagem garante que Eva não pode determinar $\left|\psi_{a|x}\right\rangle$, e, portanto, não pode aprender o valor de a.
- Mas Eva pode realizar medições sobre o sistema. Suponha que Eva pode realizar as mesmas medições que Bob.
- Se $x = y = z$, então $a = b = c$, e Eva aprende sobre a chave.
- Se $x = y \neq z$, Eva não aprenderá sobre a chave, e ainda preparará o sistema na base errada; com probabilidade $1/2$, $a \neq b$.

Segurança

- Alice e Bob podem sacrificar parte da chave para avaliar a segurança do protocolo: eles anunciam publicamente alguns valores de a e b, para que possam compará-los.
- Se não há erros ou interferências, $a = b$ em todas as rodadas.
- Se a fração de bits discordantes for maior que um limite acordado, a chave é considerada comprometida e o protocolo é abortado.
- Em média, Eva aprenderá $1/2$ dos bits da chave, e introduzirá erros em $1/4$ dos bits restantes.

Etapas de QKD

1. Distribuição da chave *crua*.
2. *Reconciliação de informação*: Alice e Bob se comunicam de forma a detectar e corrigir erros nas chaves, às custas de vazar informação sobre elas. Como provado por Shannon, a fração de bits completamente correlacionados que podem ser extraídos das chaves cruas é
$$I(A:B) = H(A) + H(B) - H(A,B).$$
3. *Amplificação de privacidade*: Alice e Bob aplicam uma função hash nas chaves; as chaves finais serão completamente desconhecidas por Eva, a menos que ela tenha uma versão idêntica da chave crua. A maior fração secreta de bits é
$$r = I(A:B) - \min(I_{EA}, I_{EB}).$$

Tipos de ataque

- Ataques individuais: Eva ataca cada um dos sistemas independentemente e usando a mesma estratégia, e deve medir seus sistemas auxiliares antes do pós-processamento clássico. A cota de segurança é a *cota de Csiszár-Körner*:

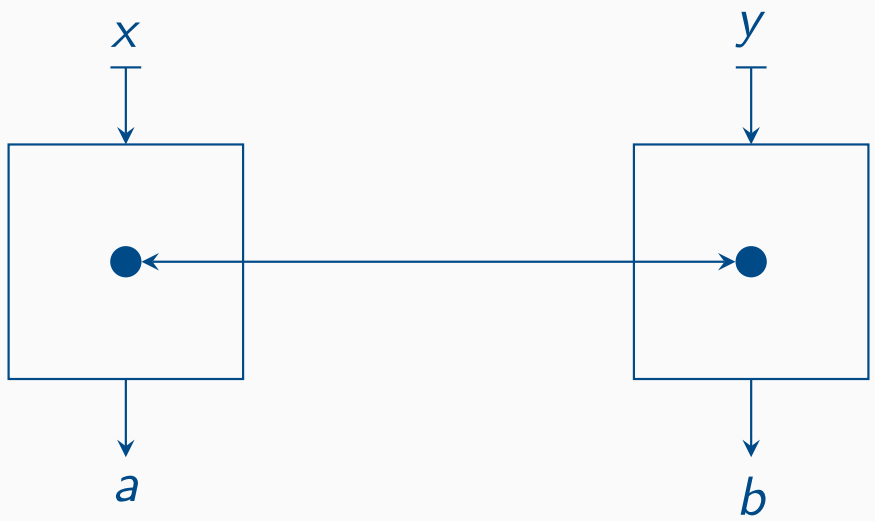
$$I_{EA} = \max_{\text{Eva}} I\left(A : E\right).$$

- Ataques coletivos: Eva ataca cada um dos sistemas independentemente e usando a mesma estratégia, e pode medir seus sistemas auxiliares quando for conveniente. A cota de segurança é a *cota de Devetak-Winter*:

$$I_{EA} = \max_{\text{Eva}} \chi\left(A : E\right),$$

onde $\chi\left(A : E\right)$ é a *quantidade de Holevo*.

Cenário baseados em emaranhamento



Cenário baseados em emaranhamento

Suponha que o estado compartilhado entre Alice e Bob é

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right),$$

e as medições de Alice e Bob são $\left\{\left|\psi_{a|x}\right\rangle\!\left\langle\psi_{a|x}\right|\right\}$ e $\left\{\left|\psi_{b|y}\right\rangle\!\left\langle\psi_{b|y}\right|\right\}$, respectivamente, onde

$$\left|\psi_{0|0}\right\rangle = |0\rangle, \quad \left|\psi_{0|1}\right\rangle = |+\rangle,$$
$$\left|\psi_{1|0}\right\rangle = |1\rangle, \quad \left|\psi_{1|1}\right\rangle = |-\rangle.$$

Então, uma implementação direta e equivalente de BB84 pode ser feita neste cenário.

Os dispositivos

As provas de segurança de protocolos de QKD se baseiam na completa caracterização dos dispositivos: os sistemas sendo preparados e as medições realizadas.

Suponha que os dispositivos sejam descaracterizados, mas que um comportamento 'ideal' seja observado:

$$p\left(a = b|x = y\right) = 1; \quad p\left(a = b|x \neq y\right) = 1/2.$$

Dispositivos descaracterizados

Este comportamento pode ser realizado se o estado do sistema é

$$\rho_{AB} = \frac{1}{4}\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right) \otimes \left(|{+}{+}\rangle\langle {+}{+}| + |{-}{-}\rangle\langle {-}{-}|\right).$$

Os qubits 1 e 3 são de Alice, e os qubits 2 e 4, de Bob, e as medições $x, y = 0$ são realizadas nos primeiros qubits, e as medições $x, y = 1$ são realizadas nos segundos qubits de cada parte.

O estado ρ_{AB} é separável, e Eva pode correlacionar seu sistema perfeitamente com ele sem ser notada. Uma chave secreta não pode ser obtida neste cenário.

O protocolo Ekert91

1. O sistema conjunto é preparado no estado

$$|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}.$$

2. Alice sorteia um trit x, e mede o observável A_x, onde

$$A_0 = \sigma_x, \quad A_1 = \sigma_z, \quad A_2 = (\sigma_x + \sigma_z)/\sqrt{2}.$$

3. Bob sorteia um trit y, e mede o observável B_y, onde

$$B_0 = (\sigma_x + \sigma_z)/\sqrt{2}, \quad B_1 = (\sigma_x - \sigma_z)/\sqrt{2}, \quad B_2 = \sigma_x.$$

4. Nas rodadas nas quais $(x, y) \in \{0, 1\}^2$, os resultados são utilizados para testar CHSH.
5. Nas rodadas nas quais $(x = 0, y = 2)$, ou $(x = 2, y = 0)$, então $a = b$ com probabilidade 1, gerando a chave.

Segurança

A segurança do protocolo Ekert91 depende da violação da desigualdade CHSH: se há violação, então não é possível existir informação sobre os resultados das medições antes que elas sejam realizadas.

Apesar da falta de uma demonstração rigorosa de segurança, era apresentada ali a principal idéia por trás da *distribuição quântica de chaves independente de dispositivos*.

O protocolo de AGM06 (Acín-Gisin-Masanes 2006)

DIQKD com segurança baseada em violação da desigualdade CHSH, certificada contra ataques individuais de Eva, que é limitada por recursos não-locais não-sinalizantes.

Se Alice e Bob observam uma violação S, então a fração secreta de bits é

$$r \geq I(A:B) - I_{EA} = \frac{S}{4} - h\left(\frac{4-S}{8}\right).$$

Esta quantidade é positiva para $S > 2.636$.

O protocolo de PABGMS09

DIQKD com segurança baseada em violação da desigualdade CHSH, certificada contra ataques coletivos de Eva, que é limitada por recursos quânticos.

Se Alice e Bob observam uma violação S, então a fração secreta de bits é

$$r \geq I(A:B) - I_{EA} = 1 - h\left(\frac{1+\sqrt{(S/2)^2-1}}{2}\right).$$

Esta quantidade é positiva para $S > 2$.

Testes experimentais de não-localidade: loopholes

Loopholes são brechas experimentais das quais um sistema local poderia, a princípio, se aproveitar para emular um comportamento não-local.

Loophole de localidade

O *loophole de localidade* é aberto quando os eventos de medições nas diferentes partes não são espacialmente separados, e, a princípio, informação sobre a escolha de medição de uma das partes está disponível para que as demais ajustem o resultado de suas medições de acordo com esta informação.

Este loophole pode ser fechado para canais de comunicação conhecidos, mas descartar possíveis canais desconhecidos é impossível.

Loophole de detecção

O *loophole de detecção* tem um alto caráter conspiracional, e é especialmente relevante em experimentos fotônicos, onde a eficiência de um detector pode não ser tão alta. Em linhas gerais, está relacionado à possibilidade de um sistema local permitir ser detectado apenas nas rodadas que lhe forem convenientes, de forma que a subestatística gerada nestes eventos selecionados seja não-local, mesmo que a estatística total, que inclui as não-detecções, seja local.

Este loophole pode ser fechado exigindo-se que resultados sejam dados em todas as rodadas, mesmo naquelas em que não há detecção.

Loophole de independência de medições

O *loophole de independência de medições* é aberto se o sistema compartilhado pode ter informação prévia sobre as medições que serão realizadas. Assim, um sistema local poderia, a princípio, se preparar adequadamente para emular um comportamento não-local.

Este loophole não pode ser fechado incondicionalmente, mas apenas com hipóteses razoáveis sobre as escolhas de medições realizadas em cada rodada.

Loopholes desconhecidos e ceticismo

Não-localidade é um fenômeno escrutinado com enorme rigor, muito maior que o exigido de outras áreas da Física. Céticos, porém, continuam apresentando 'falhas' no Teorema de Bell, em geral através de argumentos super complexos.

Testes experimentais importantes

- Freedman e Clauser (1972);
- Aspect, Dalibard e Roger (1982);
- Ou e Mandel (1988);
- Weihs *et al.* (1998);
- Rowe *et al.* (2001);
- Giustina *et al.* (2015);
- Shalm *et al.* (2015);
- Hensen *et al.* (2015).

Interpretando não-localidade

Não-localidade é o fenômeno físico que, possivelmente, exige mais esforço por parte das diferentes interpretações da teoria quântica. Na classificação de Scarani, elas se encaixam, em geral, em 4 grupos:

- Grupo 1: variáveis ocultas não-locais.
- Grupo 2: superdeterminismo e amigos.
- Grupo 3: restrição epistêmica.
- Grupo 4: teoria de colapso.