

Criptografia Quântica ¹

**Anderson Barnabé
Claudemberg Ferreira
Luciana Carreiro Albuquerque
Ronny Raupp ²**

Resumo

Neste trabalho será avaliado o comportamento de uma tecnologia emergente perante premissas básicas de funcionamento e segurança, onde computadores quânticos com seu processamento paralelo teriam condições de violar, em questão de horas, a segurança dos modelos criptográficos atualmente utilizados. Essa nova tecnologia é conhecida como Criptografia Quântica ou pela sigla QKD (Quantum Key Distribution – Distribuição Quântica de Chaves). Por fim, são discutidas as atuais limitações técnicas da tecnologia, sua vulnerabilidade a ataques clássicos e seu desempenho no atendimento a premissas básicas de segurança.

Palavras-Chave

Criptografia Quântica; Distribuição Quântica de Chaves (QKD).

Quantum Cryptography ¹

Summary

In this paper the behavior of an emergent technology will be evaluated before basic premises of operation and security, where quantum computers with yours parallel processing would have conditions of violating, in few hours, the safety of the cryptographics models now used. This new technology is known as Quantum Cryptography or for the acronym QKD (Quantum Key Distribution). Finally, the current technical limitations of the technology are discussed, your vulnerability to classics attacks and your performance in the attendance to security basic premises.

Keywords

Quantum Cryptography; Quantum Key Distribution (QKD).

1 Trabalho desenvolvido na Disciplina Segurança da Informação do MBA em Gestão de Sistemas de Informação da Universidade Católica de Brasília - UCB / 1º semestre de 2005.

2 Os autores são alunos do MBA em Gestão de Sistemas de Informação da UCB.

1. Introdução

Os sistemas de criptografia baseados em problemas matemáticos e computacionais conseguiram um nível de sigilo tão aceitável que o custo da decifragem ultrapassa, na maioria dos casos, o valor da informação a ser descoberta. Porém, da forma como foram concebidos, estão prestes a se tornarem obsoletos por novas tecnologias com base na teoria quântica.

Os princípios da teoria quântica nos mostram que somente o fato de observarmos um objeto já é suficiente para modificar o seu estado, e assim as suas características. Isso nos traz a segurança de ser sempre notificados toda vez que uma pessoa não autorizada interfira em uma comunicação quântica.

Apesar do nome Criptografia Quântica já ter se tornado comum no meio científico, na realidade ela engloba apenas a troca segura de chaves, utilizando para isso princípios da Mecânica Quântica, mais precisamente a natureza quântica dos fótons. É preciso, portanto, utilizar métodos clássicos para a troca da mensagem propriamente dita. Devido a isso, a Criptografia Quântica também é conhecida como Distribuição Quântica de Chaves ou QKD (Quantum Key Distribution).

Utilizando-se fótons, a Criptografia Quântica permite que duas pessoas escolham uma chave secreta que, em teoria, não pode ser quebrada por qualquer algoritmo, pois não é gerada matematicamente, mesmo utilizando-se um canal público e inseguro para a comunicação. É interessante notar a mudança que se processará nos métodos criptográficos, que atualmente estão amparados na Matemática mas, com a introdução desse conceito de mensagens criptografadas por chaves quânticas, passam a ter na Física sua referência.

2. Conceitos Iniciais

2.1. A Sobreposição (O Gato de Schrödinger)

De forma ilustrativa pode-se dizer que ao jogar uma “moeda quântica” para cima, o resultado poderia ser cara, coroa ou qualquer sobreposição destes estados; ou seja, a moeda poderia cair com as duas faces para cima. Um fóton, por exemplo, pode ter uma sobreposição de estados de sua polaridade (vertical, horizontal, oblíqua, etc).

No entanto, se um determinado objeto quântico estiver em mais de um estado simultaneamente, ao medi-lo ele irá colapsar em um dos seus estados sobrepostos e permanecer neste estado medido. Por exemplo, se um fóton estiver num estado sobreposto em que possui polaridade vertical e horizontal ao mesmo tempo, ao medi-lo ele colapsaria em uma das duas polarizações. Ou seja, não é possível conhecer todos os estados sobrepostos.

Isso levou Erwin Schrödinger, o físico que vislumbrou a equação central da mecânica quântica, a questionar essa teoria elaborando um exercício mental para mostrar que a teoria quântica estava incompleta. Neste experimento, um gato é colocado em uma caixa lacrada, juntamente com um dispositivo que contém uma pequena quantidade de substância radioativa. Há 50% de chance que um dos átomos da substância decaia em uma hora. Se um átomo decair, o dispositivo faz com que se

quebre um frasco contendo substância venenosa, matando o gato. Se o átomo não decair, o gato permanece vivo. Aplicando as leis da mecânica quântica ao gato, sem abrir a caixa, ele estaria não morto ou vivo, mas numa sobreposição destes estados: morto e vivo, ao mesmo tempo. Somente quando a caixa fosse aberta, e a situação do gato fosse medida, é que seu estado se colapsaria em "morto" ou "vivo".

O que ele queria mostrar é que não deveriam existir os estados sobrepostos, apenas uma probabilidade de eles ocorrerem. No entanto, um time liderado por Lukens e Friedman, físicos da State University of New York, conseguiram comprovar com um experimento a existência de dois estados quânticos sobrepostos, sem medi-los. A sobreposição é uma das responsáveis pelo paralelismo dos computadores quânticos.

2.2. O Emaranhamento (e o Paradoxo EPR)

Einstein o chamou de "ação fantasmagórica à distância" quando publicou com Podolsky e Rosen um trabalho no qual procuravam demonstrar que a mecânica quântica era uma teoria incompleta. Esse trabalho ficou conhecido como Paradoxo EPR (das iniciais Einstein, Podolsky e Rosen).

Segundo Einstein, nada pode viajar mais rápido que a velocidade da luz, inclusive informação. Mas se Alice e Bob estiverem suficientemente distantes um do outro, a informação viajaria, sim, mais rápido que a luz, pois seria instantânea. No entanto, com o emaranhamento, sistemas quânticos estão envolvidos de uma forma diferente, e a restrição da velocidade da luz não se aplica. Os mecanismos de como um sistema afeta o outro ainda é desconhecido.

No dia 21 de abril de 2004, em Viena, Áustria, um grupo da Universidade de Viena liderado pelo professor Zeilinger demonstrou comunicação com fótons emaranhados através de fibra óptica. Eles fizeram a primeira transação bancária da história usando esta tecnologia.

A comunicação foi feita sobre um link óptico de 1,45 km, especialmente instalada dentro do sistema de esgotos de Viena e utilizando uma bomba de laser violeta que gerava 8200 pares de fótons emaranhados por segundo. Além disso, utilizaram a criptografia quântica como meio de segurança.

Quando duas partículas estão em um estado dito emaranhado, qualquer medição em uma delas afetará instantaneamente a medição da outra, não importando a distância entre elas. Uma vez estabelecido um canal quântico entre duas partes, uma mudança de estado de uma das partículas emaranhadas muda instantaneamente o estado da outra partícula.

2.3. A Computação Quântica

A computação quântica é baseada em fenômenos da Mecânica Quântica. Enquanto nos computadores clássicos os bits são a unidade de informação, podendo assumir um dos valores 0 ou 1, na computação quântica temos os equivalentes qubits, que podem assumir valores 0, 1 ou a sobreposição destes estados (ou seja, 0's e 1's ao mesmo tempo).

É importante observar que a computação quântica, antes de surgir qualquer implementação física, é uma teoria como a de Alan Turing (computação clássica). Assim como ele previu diversos problemas que poderiam ser calculados com sua máquina, conhecemos hoje diversos algoritmos e soluções para problemas que seriam possíveis de serem resolvidos em um computador quântico.

Um computador quântico é qualquer "aparelho" capaz de efetuar operações segundo a teoria de computação quântica. Atualmente, o computador quântico mais desenvolvido foi implementado na IBM por um grupo de pesquisadores liderados por Isaac Chuang, do MIT. O computador possui 7 átomos: cinco de flúor e dois de carbono, inseridos em uma molécula mais complexa. Com ele foi possível fatorar o número 15 utilizando-se o algoritmo de Shor. Para isso, utilizaram um frasco contendo 1018 dessas moléculas, que tiveram o movimento controlado por ondas de rádio. O computador quântico chegou aos números 3 e 5.

Informação pode ser teleportada de um local a outro. Isto é, uma determinada informação é produzida de um lado e transmitida a outro sem que haja o tráfego através de um canal físico. Por exemplo, Alice digita sua senha e o código simplesmente "aparece" no banco. Mais ainda: Alice pode estar na Terra e o banco, teoricamente, em qualquer ponto do universo.

Um registrador clássico de 8 bits pode armazenar um número de 0 a 255. Um registrador de 8 qubits (o bit quântico) não só pode armazenar os mesmos números de 0 a 255, mas todos eles simultaneamente. Ou seja, um registrador de n qubits pode armazenar 2^n valores distintos. Essa característica, conhecida como paralelismo quântico, mostra que a memória de um computador quântico é exponencialmente maior que sua memória física. Isso sugere um possível ganho exponencial de velocidade dos computadores quânticos sobre os clássicos.

Algoritmos quânticos são executados de forma trivialmente paralela. Basta imaginar, como exemplo, a varredura de uma árvore binária a partir da raiz e o deslocamento simultâneo em direção às folhas. Ou mais, simular um autômato não determinístico sem necessidade de backtracking. Alguns algoritmos conhecidos são o algoritmo de Shor, que fatora números primos em tempo polinomial, e o algoritmo de Grover, que pesquisa uma lista não ordenada em tempo \sqrt{N} .

3. Ameaça e Oportunidade para a Criptografia

O surgimento de computadores quânticos é uma ameaça para os algoritmos tradicionais, que se baseiam na dificuldade computacional de se quebrar as chaves criadas. A criptografia mais conhecida e confiável atualmente é a RSA, que utiliza como base a dificuldade de se fatorar números primos grandes em computadores convencionais.

O algoritmo de Shor quebra essas criptografias tradicionais em tempo polinomialmente proporcional ao número de bits da chave. Vejamos a comparação entre o tempo de algoritmos convencionais e o algoritmo de Shor, na tabela a seguir:

O fator crítico da criptografia tradicional é a transmissão da chave. Tendo como objetivo impossibilitar espões de terem acesso à chave durante sua transmissão foi desenvolvido o protocolo RPS para distribuição de chave e pacotes de dados usando

elementos quânticos. O ponto principal para a garantia de segurança está no fato de que uma simples leitura não autorizada por um intruso bastaria para causar erros detectáveis na transmissão dos dados. Neste caso, o protocolo simplesmente invalida a chave e reinicia o processo até que uma chave válida seja enviada com segurança.

Comprimento do número a ser fatorado (em bits)	Tempo (algoritmo clássico)	Tempo (Shor)
512	4 dias	34 s.
1024	100 mil anos	4,5 min.
2048	100 mil bilhões de anos	36 min.

4. A Distribuição Quântica de Chaves (QKD)

Uma das propriedades mais importantes da Mecânica Quântica é a impossibilidade de cópia da informação (estado) quântica, segundo o teorema da Não-Clonagem. Por outro lado, não se pode medir ou obter informação de um estado quântico genérico, do qual não se tenha conhecimento a priori, sem que se perturbe o sistema. A idéia da Criptografia Quântica está justamente na utilização destas propriedades quânticas. Desse modo, se algum espião tentar ler (medir) a informação que está sendo enviada através de um canal quântico, irá modificá-la, sendo possível perceber sua presença.

A informação quântica é representada pelo qubit (quantum bit), em oposição ao bit clássico. Um exemplo de realização física de um qubit é o spin-1/2 de uma partícula quântica, que pode estar no estado para cima (spin-up), representando o 1, ou para baixo (spin-down), representando o 0. Outro exemplo de realização para um qubit é o estado de polarização de um fóton. Os fótons podem estar polarizados verticalmente, representando o 1, ou horizontalmente, representando o 0.

4.1. O Protocolo BB84

O primeiro protocolo de Criptografia Quântica foi proposto em 1984 por Bennett e Brassard [BB84]. Ele é utilizado para estabelecer uma chave entre Alice e Bob para ser usada em um protocolo de Criptografia Clássica, permitindo detectar se Eva está espionando a comunicação. Há dois canais utilizados: o quântico, onde serão transmitidos os fótons, e o público, onde será feito todo o resto da comunicação. E Eva pode estar monitorando os dois.

Inicialmente, Alice e Bob escolhem dois alfabetos para representar os bits 0 e 1, que são duas bases: a retilínea e a diagonal. O protocolo parte do princípio que o canal público é autenticado: cada um dos envolvidos sabe e tem garantia da identidade do outro.

A base retilínea $\begin{array}{|c|c|} \hline \square & \square \\ \hline \end{array}$ consiste nos estados de polarização horizontal (0° , representado por $|\rightarrow\rangle$) e vertical (90° , representado por $|\uparrow\rangle$), valores de 0 e 1, respectivamente. Assim, se Alice deseja enviar um "0" a Bob, ela envia um fóton no estado polarizado $|\rightarrow\rangle$, se deseja enviar um "1", envia o estado $|\uparrow\rangle$.

A base diagonal \boxtimes consiste também em dois estados ortogonais sendo um estado polarizado em 45° (representado por $|\nearrow\rangle$) e o outro polarizado em 135° (representado por $|\searrow\rangle$), valendo 0 e 1 respectivamente. Assim, se Alice deseja enviar um "0" a Bob, ela envia um fóton no estado polarizado $|\searrow\rangle$ e se deseja enviar um "1", envia o estado $|\nearrow\rangle$.

4.2. Envio de Fótons

Na primeira parte do protocolo, Alice deve enviar uma seqüência aleatória de bits para Bob através do canal quântico. Para isso:

1. Alice gera uma seqüência aleatória de bits que será usada para construir a chave secreta entre ela e Bob.

2. Para cada bit da seqüência gerada

Alice	1	0	0	1	1	0	0	1	0	1
	\boxplus	\boxtimes	\boxtimes	\boxtimes	\boxplus	\boxtimes	\boxplus	\boxtimes	\boxplus	\boxtimes
	\uparrow	\nearrow	\nearrow	\searrow	\uparrow	\nearrow	\rightarrow	\searrow	\rightarrow	\searrow

no passo 1, Alice escolhe aleatoriamente entre as duas bases do alfabeto. Assim, ela gera os fótons polarizados de acordo com sua seqüência de bits e de bases, e os envia a Bob.

3. Ao receber os fótons de Alice, Bob não sabe quais as bases ela escolheu para gerá-los. Assim, ele gera uma seqüência aleatória de bases escolhendo entre as duas do alfabeto.

Bob	\boxtimes	\boxtimes	\boxplus	\boxtimes	\boxplus	\boxtimes	\boxplus	\boxplus	\boxplus	\boxplus
	1	0	1	1	1	0	0	0	0	0

4. Bob utiliza essas bases para medir os fótons recebidos. Ao medi-los, Bob nem sempre obtém a informação correta, isto é, se a base que ele escolheu coincidir com a de Alice, ele obtém o valor correto do bit, caso contrário, ele obterá um bit de valor aleatório. Na média, em 50% das vezes, Bob vai errar. No final da medição, Bob e Alice terão, cada um, uma seqüência de bits.

4.3. A Chave Inicial

O canal de comunicação a partir de agora é o canal público, e nessa segunda parte do protocolo, Alice e Bob irão extrair uma chave inicial:

1. Bob comunica a Alice as bases que ele usou para fazer a medição dos fótons.

2. Alice então, as compara com as bases que ela utilizou, e diz a Bob quais as bases que ele usou corretamente, isto é, quais medições coincidiram.

3. Ambos eliminam os bits para os quais eles usaram bases incompatíveis, resultando então numa chave inicial, comumente chamada raw key.

Alice	1	0	0	1	1	0	0	1	0	1
	↑	↗	↗	↖	↑	↗	→	↖	→	↖
Bob										
	1	0	1	1	1	0	0	0	0	0
Bases divergentes	*		*					*		*
Chave inicial (raw key)		0		1	1	0	0		0	

As seqüências obtidas por cada um devem coincidir em 100%, a menos que a Eva tenha tentado escutar a comunicação realizada no canal quântico ou o mesmo seja ruidoso. Assumiremos que o canal não introduz ruído, logo toda perturbação será causada devido à presença de um espião.

No caso acima, não havia espião, então a chave inicial não contém erro. Suponha então que Eva estivesse no canal, e interceptasse os fótons que Alice enviou, medindo-os e depois enviando-os a Bob. Como ela também não saberia quais bases Alice utilizou, ela iria escolher suas bases também aleatoriamente, acertando-as 50% das vezes. Logo, quando Bob fosse medir os fótons, ele também iria introduzir erro, e por fim, o erro introduzido pelo espião seria de 25%.

4.4. Estimativa de Erro

De posse da chave inicial, Alice e Bob devem calcular a taxa de erro da comunicação para saber se Eva está ou não espionando.

Para calcular a taxa de erro R , eles comparam pequenos trechos de suas chaves, por exemplo, eles retiram das suas chaves os bits das posições pares formando um bloco para comparação, e anunciam esses bits publicamente. No final da comparação, eles obtêm a taxa de erro R como sendo a proporção entre os erros encontrados e o tamanho do bloco.

Assim, se essa taxa R ultrapassar a taxa de erro máxima R_{max} , estipulada por eles como sendo o nível de segurança requerido, a comunicação não é segura e Eva está espionando o canal. Eles devem então, reiniciar o protocolo, com Alice enviando novos fótons a Bob.

De posse de uma chave secreta, eles podem iniciar agora um algoritmo clássico de troca de mensagens e conseguem, teoricamente, uma comunicação 100% segura na troca de mensagens, dado que suas chaves compartilhadas são secretas.

5. Conclusão

Com os primeiros avanços em direção ao Computador Quântico, os métodos mais eficientes de criptografia utilizados atualmente perderão a eficácia. A fatoração de números primos girantes (algoritmos RSA) poderá ser feita em minutos, inviabilizando os atuais algoritmos com base matemática.

A Criptografia Quântica surge como solução possível, e já disponível no mercado, através das empresas ID Quantique e MagiQ. São produtos que podem ser implementados, mas com diversas limitações técnicas: apenas para comunicação ponto-a-ponto, e para distâncias não superiores a 100 km. O custo elevado, entre U\$ 70.000,00 e U\$ 100.000,00, parece não inibir investimentos no que tem sido visto por muitos especialistas como a última palavra em Segurança de Dados.

A solução se destaca em relação aos outros métodos criptográficos, pois não necessita do segredo prévio, permite a detecção de leitores intrusos e é incondicionalmente segura, mesmo que o intruso tenha poder computacional ilimitado. Por apresentar um elevado custo de implantação, ainda não é um padrão adotado de segurança nas comunicações, mas o desenvolvimento tecnológico poderá torná-la acessível a todas as aplicações militares, comerciais e de fins civis em geral.

Quando falamos de segurança incondicional, nos baseamos nos conhecimentos atuais de nossa ciência e, se porventura, for encontrada uma brecha no método, preceitos fundamentais da Física também serão abalados e uma revisão na Teoria Quântica precisará ser feita. É interessante notar que é esta mesma teoria que, ao criar o computador quântico que virá a abalar a segurança das atuais chaves públicas e algoritmos RSA nos dará uma ferramenta ainda mais segura para comunicação de dados em segredo.

Referências

- [MAGIQ, 05] MagiQ Technologies, Inc. <http://www.magiqtech.com/> consulta em 19 de junho 2005.
- [IDQUANTIQUE, 05] ID Quantique SA. <http://www.idquantique.com/>, consulta em 19 de junho 2005.
- [CQC, 05] Centre for Quantum Computation. <http://www.qubit.org/>, consulta em 19 de junho 2005.
- [LEYDEN, 05] Leyden, John. “Quantum Crypto moves out of the lab”. The Register, http://www.theregister.co.uk/2005/04/28/quantum_crypto/print.html, consulta em 19 de junho 2005.
- [STIX, 05] Stix, Gary. “Os Segredos Mais Bem Guardados”. Scientific American Brasil, n. 33, fev. 2005, p. 39-45.