PRINCÍPIOS DE CRIPTOGRAFIA QUÂNTICA

Daniel Nobuo Uno (IC)
danieluno@yahoo.com.br

Antonio Cândido Faleiros (PQ)
faleiros@ief.ita.br

Instituto Tecnológico de Aeronáutica
Divisão de Ensino Fundamental
Praça Mal. Eduardo Gomes, nº 50, Vila das Acácias
CEP: 12228-900, São José dos Campos - SP

RESUMO

Neste artigo será apresentada a Criptografia Quântica, um método incondicionalmente seguro segundo as Leis da Mecânica Quântica. Também veremos uma breve introdução à Criptografia e alguns dos princípios físicos envolvidos, para melhor compreensão do assunto.

ABSTRACT

In this article we will present Quantum Cryptography, a unconditionally secure method according to Laws of Quantum Mechanics. We will also have a brief introduction to Cryptography and some related physical principles, for the better comprehension of the subject.

1. INTRODUÇÃO

A necessidade de troca de mensagens sigilosas e a possiblidade de ler informações inimigas, que podem determinar o vencedor numa guerra, impulsionaram a evolução dos métodos criptográficos. Hoje em dia, com o advento da internet, cresceu o interesse pela Criptografia, que tem por objetivo preservar o sigilo da correspondência num ambiente inseguro.

A segurança dos métodos atuais se baseia em problemas computacionalmente difíceis, proporcionando um bom nível de segurança. Todavia, caso haja um grande crescimento do poder computacional, onde destacamos pesquisas com Computadores Quânticos, poderão ocorrer brechas de segurança na correspondência criptografada pelos métodos usados na atualidade. Através dessa constatação, diversos centros de pesquisa vêm estudando métodos alternativos que possam, num futuro próximo, substituir as técnicas existentes atualmente, proporcionando uma segurança muito maior mesmo diante de um crescimento exponencial do poder de computação disponível. Uma técnica muito promissora é a Criptografia Quântica, como veremos adiante.

2. ALGORITMOS CRIPTOGRÁFICOS

Nos algoritmos modernos, o segredo de uma mensagem encontra-se na *chave*, que é um parâmetro utilizado na cifragem e decifragem de uma mensagem. Quanto maior for o tamanho da chave, espera-se que seja mais difícil quebrá-la.

Para melhor entendimento e seguindo a literatura, chamemos de *Alice* quem quer mandar uma mensagem privada e *Bob* quem vai recebê-la. E denominenos *Eva*, um intruso tentando ler esta mensagem secreta.

Nos *algoritmos simétricos,* também conhecidos como de *chave privada*, a mesma chave é utilizada tanto na cifragem como na decifragem. Desta forma, Alice e Bob precisam combinar uma chave previamente. Nas transações comerciais e bancárias realizadas através da internet, a utilização de apenas esta chave é impraticável, sendo necessário um *algoritmo assimétrico* ou de *chave pública*, como veremos adiante.

Exemplos de algoritmos de chave privada são o *One Time Pad* (uma cifra simples mas incondicionalmente segura, inventada em 1917 por Gilbert Vernam) e a cifra *DES* (Data Encryption Standard, adotada em 1976 e que continua sendo o padrão oficial americano para cifragem).

A cifra One Time Pad baseia-se na operação XOR (OU exclusivo), como indica a tabela abaixo. O processo de decifragem é análogo.

mensagem original	0	1	1	0	1
CHAVE	1	0	0	0	1
mensagem cifrada	1	1	1	0	0

Tabela 1. Cifra One Time Pad

Podemos utilizar uma chave de tamanho inferior ao da mensagem, pois será mais fácil distribuir uma chave quanto menor esta for. Mas isso deixará brechas para um criptoanalista experiente, que poderá decifrá-la. Caso a chave utilizada no One Time Pad seja aleatória e do tamanho da mensagem, temos uma *segurança incondicional*: prova-se que não há como decrifá-la de forma alguma. Mas o problema de distribuição de chaves permanece: para mandar uma mensagem de tamanho n com uma segurança incondicional, Alice e Bob precisam combinar previamente uma chave de tamanho n, o que é inviável para a maioria das aplicações, principalmente quando há um grande fluxo de mensagens.

Num *algoritmo assimétrico*, a chave utilizada na cifragem é diferente daquela utilizada na decifragem. Desta forma, não há a necessidade de Alice e Bob combinarem uma chave previamente, eliminando o problema da distribuição de chaves. A segurança desse algoritmo se baseia em problemas computacionalmente difíceis, como a fatoração de um número razoavelmente grande em seus fatores primos, onde destacamos o algoritmo RSA, que é um dos mais utilizados na atualidade.

Caso haja um grande crescimento do poder computacional, onde destacamos pesquisas com Computadores Quânticos, estes algoritmos não serão mais seguros. Um computador pessoal dos dias atuais demoraria 100 mil bilhões de anos para fatorar um número de 600 dígitos decimais, o que seria realizado em poucos minutos num computador quântico, caso possa ser construído.

3. CRIPTOGRAFIA QUÂNTICA

Baseando-se nos princípios da Mecânica Quântica, a grande vantagem deste método em relação aos outros reside em sua segurança incondicional, ou seja, não apresenta falhas como os métodos criptográficos atuais e não pode ser quebrado, mesmo com poderosos computadores, como veremos adiante. Além do mais, é possível estabelecer protocolos de troca de chaves secretas sem comunicação secreta prévia como acontece nos algoritmos simétricos.

3.1 Princípios de Mecânica Quântica

A Mecânica Quântica nos diz que a luz apresenta tanto uma natureza corpuscular como ondulatória. Experimentos como o *Efeito Fotoelétrico* (Einstein) e a *Radiação Térmica do Corpo Negro* (Planck) mostram a natureza corpuscular da luz, nos dizendo que é a luz é formada por fótons, partículas elementares *indivisíveis*, cuja massa é igual a zero. Além disso, vejamos a *Polarização*, fenômeno utilizado na Criptografia Quântica.

» Polarização

Uma onda luminosa consiste de dois campos perpendiculares e que variam no tempo: o campo elétrico *E* e o campo magnético *B*. O *plano de polarização* é definido como o plano que contém *E* e a direção de propagação da onda. Desta forma podemos atribuir uma polarização (qualquer medida em graus) a um fóton. Por exemplo, polarizações de 0º, 45º, 90º e 135º de um fóton são ilustradas abaixo.

Figura 1. Diferentes planos de polarização de um fóton

Dado um fóton, podemos mudar sua polarização com a utilização de polarizadores, como cristais de calcita e óculos de sol. Filtros polaróides deixam passar fótons cujo plano de polarização seja igual ao da "fenda" do filtro e absorvem os fóton cujo plano de polarização seja perpendicular a essa.

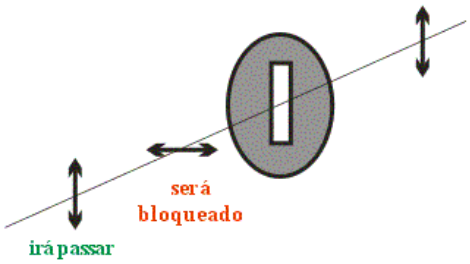


Figura 2. Filtro polaróide

Caso o fóton apresente uma polarização genérica θ em relação à fenda do polarizador, a probabilidade do fóton passar é $\boldsymbol{P = cos^2\ \theta}$, expressão conhecida como *Postulado de Redução de Von Newman*. E caso ele passe, sua polarização será a mesma do polarizador. Por exemplo, caso θ = 45º, a probabilidade será de 50% do fóton passar e adquirir polarização igual à da fenda do polarizador.

Um fato notável e que exemplifica o *Princípio da Incerteza de Heisenberg* é a impossibilidade da determinação exata da polarização de um fóton. Para obtermos alguma informação sobre sua polarização, precisamos de um filtro polarizador. Caso o fóton não passe por este, apenas podemos concluir que ele não foi polarizado paralelamente à fenda do polarizador. E caso ele passe, apenas concluímos que não foi polarizado perpendicularmente à fenda, pois senão ele não iria passar. Com qualquer outra polarização há uma probabilidade do fóton passar.

O Princípio da Incerteza de Heisenberg, de uma forma geral, afirma que não podemos obter todas as informações que descrevem uma partícula subatômica, não sendo possível determinar a polarização exata de um fóton específico (observação causa perturbação).

3.2 Protocolos Quânticos

Os protocolos quânticos utilizam dois canais: um público e um quântico. A idéia principal destes protocolos é a combinação de uma chave secreta *K* entre os personagens Alice e Bob. Com essa chave, cujo tamanho espera-se ser igual ao da mensagem, Alice e Bob podem se comunicar com segurança: Alice pode enviar, pelo canal público, uma mensagem cifrada pelo One Time Pad utilizando a chave *K* e, dessa forma, apenas Bob será capaz de decrifá-la.

Esses protocolos servem apenas para a combinação de chaves criptográficas, não servindo para a transmissão da mensagem, como veremos. A seguir, detalharemos um protocolo quântico.

» Protocolo de Bases Conjugadas

Este protocolo, também conhecido como BB84 e criado pelos pioneiros no assunto C. H. Bennett e G. Brassard em 1984, foi o primeiro protocolo quântico que surgiu e também foi o primeiro a ser implementado.

Vejamos de um modo geral o BB84: pelo canal quântico, Alice envia fótons polarizados para Bob, que os mede segundo um polarizador. E pelo canal público, eles publicam mensagens necessárias para a determinação da chave, sendo que estas mensagens podem ser lidas por um espião qualquer sem afetar a segurança do protocolo. Utilizam-se quatro polarizações: 0º, 45º (representando o bit 0), 90º, 135º (representando o bit 1), conforme indicado pela figura abaixo.

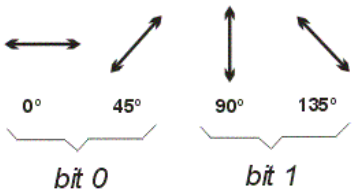


Figura 3. Polarizações referentes ao BB84

Vejamos:

►Alice envia uma seqüência aleatória de fótons com as polarizações da figura 5, mantendo em segredo as polarições utilizadas

►Bob, para a leitura de cada fóton enviado por Alice, escolhe aleatoriamente o tipo de medição que vai fazer: com a fenda do polarizador a 45º ou 90º

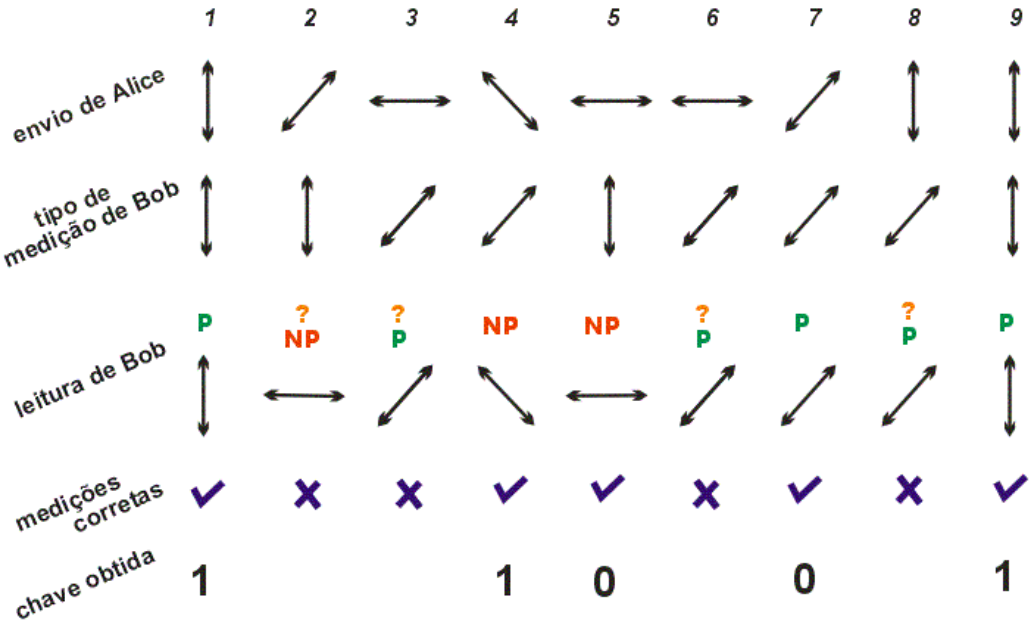
►Bob guarda o resultado das medições em segredo

O primeiro fóton, θ = 0º (lembrando que θ é a diferença de ângulo entre a polarização do fóton e a fenda), irá passar pelo polarizador com certeza (indicado por **P**), e dessa forma, Bob concluirá que o fóton tinha uma polarização igual à da fenda (no caso, 90º).

Para o segundo fóton, θ = 45º, o fóton pode ou não passar pelo polarizador, com chance de 50% (como não há certeza do que irá ocorrer, foi indicado por **?**). Supondo que não passe (**NP**), Bob concluirá que o fóton tinha uma polarização ortogonal à da fenda.

No terceiro fóton, θ = 45º, ocorre algo similar ao segundo fóton, mas supomos que o fóton passe (**P**). Conclui-se que sua polarização é igual à da fenda. No quarto fóton, θ = 90º, logo não irá passar pelo polarizador (**NP**), sendo classificado com uma polarização ortogonal à fenda. E continua-se a leitura dos outros fótons. Percebemos que Bob faz a leitura dos fótons de forma errônea quando θ = 45º. Por isso, pelo canal público, ocorre o processo de reconciliação.

►Bob anuncia pelo meio público os tipos de medições que fez para cada fóton (45º ou 90º) e Alice diz quais medições foram corretas



Para o fóton 1 no caso acima, Bob diz para Alice: "medição com fenda a 90º". Como Alice sabe a polarização de cada fóton que enviou, ela diz a Bob que a medição foi correta para este fóton (***V***). Já para o fóton 2, Bob realizou uma medição com a fenda a 90º, e como o fóton original apresenta um desvio de 45º em relação à fenda, a medição foi errada (***X***): a polarização de 45º foi medida como 0º. Alice, sabendo que θ = 45º neste caso, diz para Bob que a medição está errada. Esse processo de reconciliação ocorre para toda a seqüência.

Para os fótons cuja medição foi correta (metade da seqüência), Alice e Bob convertem as respectivas polarizações em bits, como indicado pela figura 5, obtendo uma chave. Neste caso ilustrativo com poucos fótons, a chave obtida foi **11001**: essa chave claramente irá ser igual para os dois, caso não haja erros de transmissão ou um intruso. Os erros de transmissão costumam ser baixos (inferiores a 3%) e são causados por ruídos no canal quântico ou pelo desalinhamento dos polarizadores.

» A presença de um intruso

Caso Eva tente ler os fótons que Alice enviou, ela não conseguirá ler todos os fótons corretamente: ela apenas sabe que foi enviado fótons com polarizacões de 0º, 45º (bit 0), 90º e 135º (bit 1). Utilizando um polarizador, ela irá conseguir ter uma leitura correta de no máximo 75% dos bits enviados – alguns tipos de ataque estão especificados em [1], p. 28-33. Desta forma ela terá que reenviar fótons para Bob, e 25% da leitura dos bits de Bob irão diferir da de Alice.

Bob, sem saber que Eva leu e reenviou os fótons, faz a leitura dos fótons e o processo de reconciliação normalmente, obtendo uma chave que difere em 25% dos bits de Alice. Desta forma, Alice e Bob anunciam publicamente alguns bits da chave, para conferi-los. Caso haja uma taxa de erros relativamente alta, provavelmente há um intruso. Caso os erros sejam baixíssimos, eles descartam da chave os bits que foram anunciados publicamente.

Pode ser que uma baixíssima porcentagem da chave esteja incorreta devido aos erros de transmissão e há procedimentos matemáticos para corrigi-los. Há outros procedimentos utilizados na amplificação da privacidade da chave, como pode ser visto em [1], p. 24-27. Dessa forma Alice e Bob partilham de uma chave com privacidade.

3.3 Dificuldades da utilização da Criptografia Quântica

Um problema de sua implementação é taxa de erros na transmissão dos fótons, seja por via aérea ou fibra óptica. Consegue-se uma maior distância na transmissão de fótons por fibra óptica, sendo que tal distância está limitada atualmente em 70 km utilizando fibras óticas de alta pureza (elevadíssimo custo). Acima dessa distância, a taxa de erros torna-se inviável atualmente. Tecnologias para um perfeito alinhamento dos polarizadores, fibras ópticas mais apropriadas e amplificadores quânticos de sinais estão em desenvolvimento para ampliar a distância de transmissão. Por via aérea, tal distância limita-se a centenas de metros, mostrando-se menos viável atualmente.

Em [6d] podem-se ver áreas em pesquisa sobre Criptografia Quântica. Acredita-se que nos Estados Unidos há um link quântico dedicado entre a Casa Branca e o Pentágono, além de outros links entre algumas bases militares e laboratórios de pesquisa. Uma empresa Suíça, iD Quantique [6e], lançou aparelhos de Criptografia Quântica, mostrando que a utilização desses protocolos em larga escala está se tornando cada vez mais plausível.

4. CONCLUSÃO

A Criptografia Quântica se destaca em relação aos outros métodos criptográficos, pois não necessita segredo prévio, permite detectar um intruso pelo simples fato de ele tentar ler os fótons na distribuição de chaves e é incondicionalmente segura, mesmo que o intruso tenha poder computacional infinito. Apresenta um elevado custo de implementação, entretanto, com a evolução tecnológica, poderá ser usada em larga escala num futuro próximo, tanto para fins militares como comerciais.

AGRADECIMENTOS

Os autores agradecem aos pesquisadores que de alguma forma ajudaram na coleta de materiais, desde pequenos textos sobre o assunto até teses de Mestrado, assim como o apoio financeiro do CNPq através do Programa Institucional de Bolsas de Iniciação Científica – PIBIC.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Kowada, Luis Antonio Brasil; *Comparação entre os Principais Protocolos para Combinação de Chaves Criptográficas Quânticas*; IME, Universidade de São Paulo; tese de Mestrado; 1999

[2] Brylevski, Alexei; *Quantum key distribution: Real-time compensation of interferometer phase drift*; NTNU, Noruega; tese de Mestrado; 2001

[3] Singh, Simon; *O Livro dos Códigos (The Code Book)*; Editora Record; 2002

[4] Bennett, C. H.; Brassard, G.; Ekert, A. K.; *Quantum Cryptography*; Scientific American, Outubro 1992; p. 26 – 33

[5] Gisin, Nicolas; Ribordy, Grégoire; Tittel, Wolfgang; Zbinden, Hugo; *Quantum Cryptography*; Reviews of Modern Physics; 2002; v.74

[6] Internet

a. Quantum Cryptography in Norway, http://www.vad1.com/qcr/
b. Informação Quântica, pesquisas, http://www.phy.hw.ac.uk/resrev/EQUIS/
c. iD Quantique, http://www.idquantique.com
d. Bibliografia de Criptografia Quântica, http://www.cs.mcgill.ca/~crepeau/CRYPTO/Biblio-QC.html
e. Princípios de Criptografia e Computação Quânticas, http://www.mundoquantico.hpg.com.br