Comunicações Seguras - Criptografia Quântica

Os muitos métodos de cifragem, anunciados como detentores de alto grau de segurança para as comunicações, têm-se, ao longo da história, revelado de segurança relativa, já que acabaram por cair numa ou noutra circunstância; ao ponto de hoje em dia olharmos sempre com algumas reservas para os sistemas de cifragem de mensagens considerados altamente seguros. No entanto, são já comercializados sistemas, esses sim, determinantemente inquebráveis, baseados no comportamento quântico dos fotões. Neste artigo analisaremos a base de funcionamento desses sistemas.

Desde os primórdios da capacidade comunicativa humana, fosse em que forma fosse, a procura de métodos sustentadores de segredos portados nas mensagens fez-se incessantemente. Trate-se de segredos pessoais, militares ou comerciais, a importância da privacidade comunicativa é sem dúvida inquestionável. Muito embora filosoficamente a importância da capacidade reversa possa ser discutida e até provada, basta regredirmos até aos acontecimentos da segunda guerra mundial para constatarmos que a quebra das mensagens trocadas pelos Alemães com a sua máquina Enigma, por parte dos Aliados, foi essencial para a antecipação do término da guerra.

Ao longo da história múltiplos métodos de cifragem foram surgindo, alguns até apelidados como indecifráveis, mas que mais tarde ou mais cedo acabaram por ser quebrados.

Hoje em dia servimo-nos de métodos altamente seguros para realizar operações que já se tornaram quotidianas, como por exemplo o acesso às nossas contas bancárias através de páginas de Internet. Estamos a falar de métodos que se apoiam na dificuldade matemática de factorizar números à medida que o tamanho do número aumenta. O método de cifragem RSA, desenvolvido por Rivest, Shamir e Adleman nos finais da década de 70, serve-se deste pressuposto e é um dos mais usados actualmente. O comprimento numérico dos parâmetros RSA permite na prática, aos cifradores, estarem sempre à frente da capacidade computacional existente, mesmo da distribuída, no que refere à possibilidade de quebra em tempo útil. O insucesso que a procura de técnicas matemáticas, redutoras dos caminhos da factorização, tem sofrido também ajuda a

suportar o grau de segurança do método. Assim, parece que o eterno duelo entre cifradores e decifradores está a ser perdido por estes últimos.

Mas existe uma ameaça tecnológica com que se enfrentam os métodos de cifragem apoiados nas características da factorização com resolução temporal de ordem complexa. Essa tecnologia adquire forma nos chamados processadores quânticos. Estes conseguem por mecanismos quânticos bem conhecidos transformar problemas de custo temporal complexo em problemas de custo temporal simples. Isto significa que os métodos de cifragem actuais, como o RSA, deixariam de ter qualquer valor. Por exemplo, em 1994 um número de 129 dígitos, relativo ao RSA 129, levou 8 meses para ser factorizado por mais de 1000 computadores. Esse número, se fosse processado usando um único processador quântico, seria factorizado em apenas 10 segundos. Para já os processadores quânticos são apenas uma promessa tecnológica, porque estes processadores apresentam variadíssimos problemas de construção que os inibem de serem aproveitados para o inerente fim. Por outro lado, e também suportados por mecanismos quânticos, estão já a surgir no mercado mundial sistemas de cifragem que aos olhos da teoria quântica são determinantemente invioláveis. O princípio foi proposto no início dos anos 80 por Charles Bennett e por Giles Brassard e é relativamente simples de perceber.

Este tipo de cifragem está normalmente orientado para a troca de chaves secretas a serem usadas posteriormente num método clássico de cifragem que se mantém inquebrável desde que o comprimento da chave se aproxime do comprimento da mensagem a cifrar, desde que a chave seja aleatória e desde que a chave seja usada uma única vez. É o caso da cifra conhecida por *maço de cifras para uma só vez*.

A portação da informação, constituinte da chave, pode ser conseguida através da polarização de fotões de luz. São considerados dois estados possíveis de polarização correspondentes aos bits de informação 0 e 1. No entanto, estas polarizações vão estar condicionadas a dois referenciais distintos, o ortogonal e o diagonal. O ortogonal permite associar o estado 0 do bit com a polarização horizontal (H) e o estado 1 com a polarização vertical (V). O diagonal relaciona o estado 0 do bit com a polarização a 45º e o estado 1 com a polarização a -45º. Estes relacionamentos podem ser deduzidos na tabela seguinte:

Estado do Bit	Referencial Ortogonal	Referencial Diagonal
0	 (H)	 (45º)
1	 (V)	 (-45º)

Tabela 1

Tradicionalmente existem nos cenários da criptografia três personagens: a Alice, a Eve e o Bob. A Alice pretende passar uma mensagem, neste caso uma chave, ao Bob sem que a Eve a consiga interceptar.

A emissão de fotões é proporcionada por um Laser que fica colocado no lado da Alice. A Alice vai ter que escolher de forma aleatória, para cada bit a enviar, um dos dois referenciais. Assim como na recepção, o Bob vai ter que empregar um dos dois filtros detectores, associados a cada referencial de polarização, aleatoriamente para cada bit recebido (Tabela 2).

Quando, por coincidência, ambos usarem o mesmo referencial torna-se possível ao Bob perceber o bit exacto que Alice enviou, caso contrário os referenciais são distintos implicando incerteza no estado do bit observado por Bob. A aleatoriedade da escolha dos referenciais vai assim obrigar a que apenas 50% dos bits enviados por Alice sejam considerados por ambos. Para evitar

	Referencial Ortogonal	Referencial Diagonal
Detector usado na recepção		

Tabela 2

que o Bob considere os bits errados, o Bob, através de um canal de comunicação clássico, vai comunicar a Alice os referenciais que usou para receber cada um dos bits. Alice, por sua vez, vai anunciar a Bob quais os referenciais não coincidentes e que devem ser eliminados. Assim, apenas os bits que correspondem a referenciais

coincidentes serão considerados por ambos (Tabela 3). Note-se que unicamente a informação respeitante aos referenciais usados é passada através do canal de comunicação clássico; os bits em causa não são referidos durante o uso desse canal.

Bits enviados por Alice	0	1	1	0	1	0	0	1	1	0
Polarizações usadas por Alice	↗	↘	|	↗	|	↗	−	|	|	↗
Filtros usados por Bob	×	+	+	×	×	+	+	+	×	×
Bits observados por Bob	0	0	1	0	1	1	0	1	1	0
Coincidência de Referenciais	=	≠	=	=	≠	≠	=	=	≠	=
Bits a considerar	0	-	1	0	-	-	0	1	-	0

Tabela 3

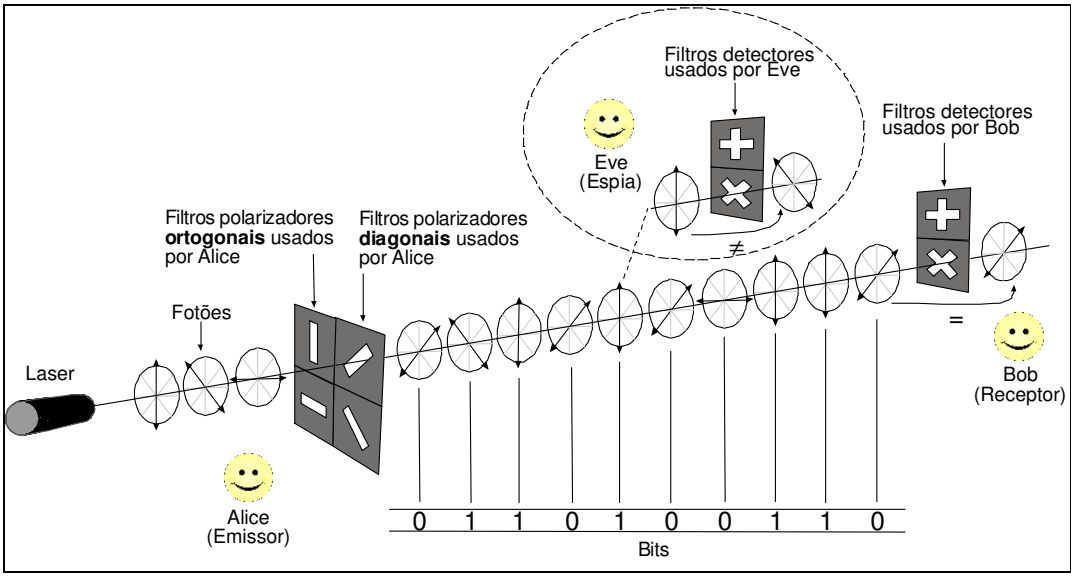

Ilustração 1

Na ilustração 1 são visíveis, em propagação, 10 fotões, situados entre os filtros polarizadores de Alice e os filtros detectores de Bob. Cada um dos fotões tem a sua polarização representada por uma direcção. O primeiro fotão enviado, agora prestes a ser observado pelo detector de Bob, encontra-se polarizado sob um referencial diagonal e o detector escolhido por Bob, nesse momento, pertence ao mesmo referencial possibilitando a correcta leitura do estado desse bit e que é 0. Já a Eve, que se encontra

aqui a tentar observar o estado do 5º fotão já enviado por Alice, vai fazê-lo usando o referencial errado. Por consequência, o bit observado poderá estar errado ou certo de acordo com um valor probabilístico de 0,5. Mais ainda, o fotão, depois de observado no filtro detector, altera a sua base de polarização para a base de polarização do detector.

Se Eve tentar interceptar a mensagem vai ter dois problemas. O primeiro resulta do uso aleatório do filtro observador do estado da polarização do fotão. Como não conhece qual a sequência de referenciais usados pela Alice, aplicará os órgãos detectores com o referencial errado em 50% dos casos. Traduzindo-se isto na obtenção, por Eve, de uma chave com 25% dos bits errados. Repare-se que, apesar de 50% dos referenciais não coincidirem, teremos apenas 25% dos bits errados. Metade dos bits observados, por coincidência de referenciais, vai estar toda correcta. A outra metade, a dos referenciais não coincidentes, porque o deslocamento angular entre referenciais é de 45º, manterá 50% dos bits no seu estado correcto e outros 50% no estado errado. Estes 50% parciais correspondem logicamente a 25% dos bits originais.

Mesmo que Eve tenha escutado as validações de referenciais feitas pelo Bob e pela Alice através do canal clássico, os seus bits observados continuarão a conter erros, uma vez que os filtros usados, por inerência aleatória, não coincidirão com os usados pelo Bob. Pelo menos para um certo comprimento de bits a possibilidade de coincidência é ínfima.

O segundo problema que afectará o intuito de Eve está relacionado com uma característica quântica que faz com que a polarização adquirida pelo fotão após uma observação fique associada ao referencial do filtro usado.

De facto, devido a isto, Eve não conseguirá copiar a totalidade dos fotões originais enviados por Alice sem adulterar o seu estado e assim enviá-los para Bob. Isto introduzirá erros em 25% dos bits recebidos pelo Bob, apesar de este ter validado aqueles referenciais. Reservando, para teste, alguns dos bits recebidos, Bob e Alice podem compará-los e se algum, ou alguns, não coincidirem, então existirá um motivo provável para isso: a Eve, ou alguém, tentou escutar a mensagem.

Apenas existe uma possibilidade deste método ser quebrável: é a de que a teoria quântica actual contenha erros ou omissões, mas trata-se da teoria física mais experimentada com sucesso até hoje, o que torna esta possibilidade remota.

Nos últimos tempos têm surgido empresas, como a MagiQ Technologies, a comercializarem estes sistemas por centenas de milhares de Euros; as primeiras

experiências realizadas por Charles Bennett e por Giles Brassard, em 1989, estavam limitadas a uma distância de 32cm. Os sistemas actuais conseguem atingir a centena de quilómetros. Estas limitações encontram-se fundamentalmente relacionadas com a dificuldade de se conseguir distinguir um erro introduzido pelas fontes de fotões, polarizadores e detectores, derivado das imperfeições destes mecanismos, de um erro introduzido por um espia.

Existem também desenvolvimentos feitos em comunicações em espaço livre com o objectivo final de criar uma rede de satélites de baixa altitude para suportarem comunicações cifradas quanticamente. É o caso da equipa liderada por Richard Hughes que em Los Alamos tem conseguido obter bons resultados em distâncias de algumas dezenas de quilómetros.

No entanto a impenetrabilidade trazida por estes sistemas, apesar de em certas circunstâncias ser indubitavelmente útil, nas mãos erradas pode transformar-se numa ferramenta perigosa, ameaçadora da segurança das nações, das empresas e dos indivíduos. A invulnerabilidade na segurança das comunicações de grupos terroristas preocupa as entidades estatais que se dedicam à decifragem dessas mensagens. A instituição Norte Americana NSA (National Security Angency), que por curiosidade é a instituição mundial que mais matemáticos agrega e onde se desenvolvem métodos de vanguarda tanto a nível de cifragem como de decifragem, poderá vir a ter que redireccionar muito do trabalho que desenvolve.

No passado, uma empresa suíça, que comercializava um software de cifragem com algoritmos dificílimos de quebrar, fez um acordo com o governo dos Estados Unidos em que se obrigava a incluir no seu software acessos escondidos (Back-doors) que permitiam aos EUA decifrar sem problemas as mensagens originárias de outras nações que tinham adquirido o software. Poderá vir a acontecer algo semelhante com os sistemas de criptografia quântica?

Bibliografia:

An introduction to quantum computing for non-physicists. Eleanor Riefell e Wolfgang Polak. arxive.org, quant-ph/9809016 v2, Janeiro de 2002.

Best-Kept Secrets. Gary Stix.

Scientific American, Vol. 292, No. 1, 65-69, Janeiro 2005.

O livro dos Códigos. Simon Singh.
Temas e Debates, Outubro de 2001.

Practical free-space quantum key distribution over 10 km in daylight and at night.
Richard J Hughes et al.
New Journal of Physics 4 43.1-43-14, Julho de 2002.

The New Quantum Universe. Tony Hey e Patrick Walters.
Cambridge-University Press, 2003.

Apontadores:

www.magiqtech.com

http://quantum.lanl.gov/hughes.shtml