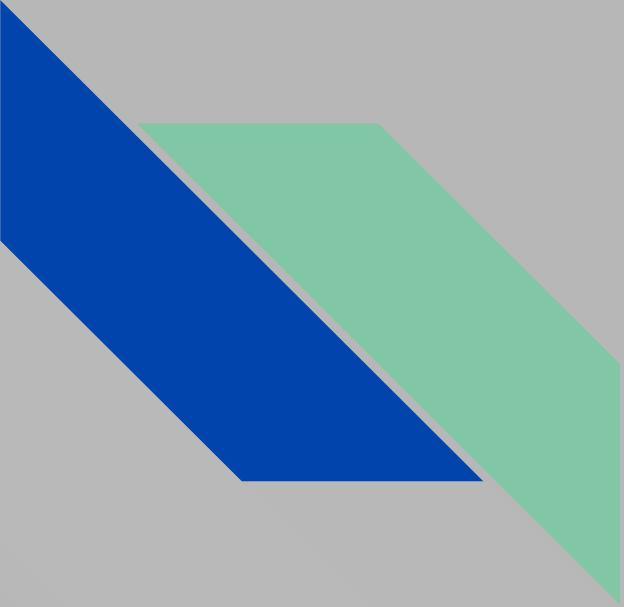




Criptografia

Segurança Digital



Sumário

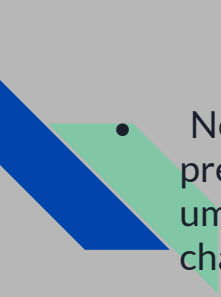
1. Introdução
4. Objetivo
6. Criptografia Quântica
7. Protocolo BB84
12. Interação com a sala



Criptografia

- Criptografia é a ciência da comunicação secreta, e está se tornando cada vez mais importante com o crescimento das redes de computadores e transações eletrônicas.
- Quando informações pessoais, financeiras e militares são transferidas, tornam-se vulneráveis a técnicas de monitoramento que potencialmente podem ter consequências. Estes problemas podem ser evitados através da encriptação da informação de forma que esta se torne ininteligível a todos, menos ao destinatário.
- Este objetivo pode ser atingido se o remetente e o destinatário possuírem uma chave, que pode ser usada para encriptação pelo remetente e deciptação pelo destinatário. A chave é portanto um material de grande valor apesar de não conter nenhuma informação em si. Contudo, o passo inicial da distribuição de chaves precisa ser completado com alta segurança de forma que nem mesmo informações parciais sejam comprometidas.

- 
- O objetivo da criptografia é transmitir informações de forma que o acesso seja restrito apenas ao destinatário pretendido. Originalmente a segurança de um criptograma dependia do segredo dos procedimentos de criptografia e decriptografia. Atualmente usamos codificadores para os quais os algoritmos de encriptar e decriptar podem ser revelados a qualquer um sem comprometer a segurança de um criptograma em particular.
 - Nesses codificadores um conjunto de parâmetros, chamados de chave, é fornecido junto com o texto não criptografado como entrada para o algoritmo de encriptação e com o criptograma para o algoritmo de decriptação. A segurança do criptograma depende inteiramente da segurança da chave, e esta precisa ser composta de uma sequência aleatória de bits. Uma vez que a chave é estabelecida, comunicações subseqüentes envolvem o envio de criptogramas através de um canal público, que é vulnerável à espionagem passiva total (por exemplo, um anúncio numa mídia de massa).
 - Contudo para estabelecer a chave, dois usuários (que não compartilham nenhuma informação secreta inicialmente) precisam, num certo estágio, usar um canal muito seguro e confiável. Como em teoria todo canal clássico de comunicação pode sempre ser monitorado, dois usuários legítimos podem sofrer espionagem passiva sem se darem conta. Matemáticos tentaram resolver o problema da distribuição de chaves.

- 
- Nos anos 70 houve a descoberta dos sistemas de chave pública. Nestes sistemas os usuários não precisam combinar uma chave secreta antes de enviar mensagens. Eles funcionam sobre o princípio de um cofre com duas chaves: uma pública para trancá-lo e outra privada para abrí-lo. Todos tem uma chave para trancar o cofre mas apenas um tem a chave que abre.
 - Estes sistemas exploram o fato de que certas operações matemáticas são mais fáceis de serem computadas em um sentido do que no outro. Eles evitam o problema da distribuição de chaves mas infelizmente sua segurança depende de uma hipótese matemática não provada, como a dificuldade de fatoração de grandes inteiros (RSA, o sistema de criptografia de chave pública mais comum baseia sua segurança nisso). Isto significa que se e quando matemáticos ou cientistas da computação desenvolverem procedimentos de fatoração mais rápidos toda a privacidade de sistemas de criptografia pública pode acabar do dia para a noite. De fato, trabalhos recentes na área da computação quântica mostram que com o auxílio destes é possível fatorar muito mais rápido do que com computadores clássicos.



Criptografia Quântica

- A criptografia quântica é baseada na incerteza natural do mundo quântico. Com ela você pode criar um canal de comunicação difícil de ser monitorado sem interferir na transmissão. As leis da física dão segurança a este canal mesmo que o observador possa fazer o que quiser, mesmo que ele tenha poder computacional infinito, mesmo que $P=NP$. O mundo quântico possui uma incerteza fundamental e não há maneira de evitá-la. Esta incerteza pode ser usada para gerar uma chave secreta.
- Na prática, a criptografia quântica foi demonstrada em laboratório pela IBM e outros, mas em distâncias relativamente curtas. Recentemente distâncias da ordem de 120 Km foram obtidas usando cabos de fibra óptica de alta pureza. Acima disso a taxa de erros de bit causados pelo princípio da incerteza de Heisenberg e por impurezas microscópicas na fibra tornam o sistema inviável. Aplicações práticas nos EUA desta tecnologia incluem um link dedicado entre a Casa Branca e o Pentágono em Washington e outros links entre bases militares importantes e laboratórios de pesquisa próximos.



Protocolo BB84

- Esse protocolo, foi originalmente descrito utilizando os estados de polarização dos fótons para transmitir a informação. Ao trocarem entre as suas várias posições possíveis, os fótons vibram e se, num grupo de fótons, todos vibram na mesma direção, então eles estão polarizados. Utilizando filtros polarizadores é possível restringir a passagem aos fótons polarizados numa determinada direção, bloqueando os restantes. Para medir a polarização de um fóton são utilizadas bases de medida, que são compostas por duas direções que façam um ângulo reto. Por exemplo: horizontal e vertical, ou diagonal à esquerda e à direita. No entanto, qualquer dois pares de variáveis conjugadas pode ser utilizado para o protocolo.
- Os estados de polarização mais utilizados são: a base retilínea com vertical (0°) e horizontal (90°), a base diagonal com os ângulos de 45° e 135° ou a base circular com a direita e esquerda.

- Exemplo:

1. Alice envia para Bob uma seqüência de fótons. Cada fóton é polarizado aleatoriamente em uma de quatro direções: horizontal, vertical, diagonal direita e diagonal esquerda. Por exemplo, Alice envia para Bob:



2. Bob tem um detector de polarização. Ele pode usar seu detector para medir polarização vertical e horizontal ou nas diagonais. Ele não pode medir ambas: a mecânica quântica não permite. Medir uma polarização destrói qualquer possibilidade de medir a outra. Então, ele seta seus detectores aleatoriamente, por exemplo:



Agora, quando Bob posiciona seu detector corretamente, ele descobre a polarização. Se ele coloca seu detector na base errada ele obtém um resultado aleatório. Bob não sabe quando acerta e quando erra. Neste exemplo, ele poderia obter como resultado:



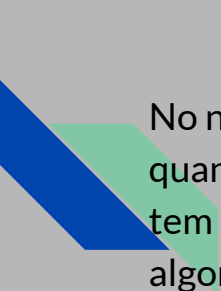
3. Bob diz a Alice, por um canal inseguro, como ele configurou seu detector.
4. Alice diz a Bob quais configurações estavam corretas. No nosso exemplo, o detector estava corretamente polarizado para os fótons 1, 4, 5, 7 e 9



5. Alice e Bob guardam apenas as polarizações que foram corretamente medidas. No nosso exemplo, eles guardaram:

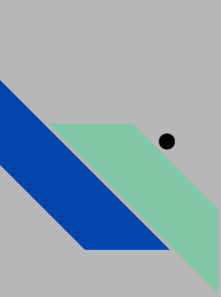


6. Usando um código pré-combinado, Alice e Bob traduzem estas medidas de polarização em bits. Por hipótese, horizontal e diagonal esquerda podem ser iguais a 0, e vertical e diagonal direita podem ser iguais a 1.



No nosso exemplo, eles obtiveram: 11001. Dessa forma, Alice e Bob geraram 5 bits. Eles podem gerar quantos bits quiserem usando este esquema. Em média, Bob acerta a polarização 50% do tempo, então Alice tem que enviar $2n$ fótons para gerar n bits. Estes bits podem ser usados como uma chave secreta para um algoritmo simétrico, ou podem garantir segurança perfeita gerando bits suficientes para um "one time pad" ou cifra de chave única. A parte mais interessante é que Eva não consegue espionar passivamente. Assim como Bob, ela tem que chutar qual polarização usar, e como Bob, metade dos chutes estarão errados. Como chutes errados trocam a polarização dos fótons, ela introduz erro na comunicação. Dessa forma Alice e Bob terminarão com strings de bits diferentes. Assim, Alice e Bob finalizam o protocolo da seguinte forma: 6. Alice e Bob comparam alguns bits em suas strings. Se houverem discrepâncias, eles sabem que estão sendo monitorados. Se não houverem, eles descartam estes bits usados para comparação e usam outros. Melhorias neste protocolo permitem que Alice e Bob usem seus bits mesmo na presença de Eva. Eles podem comparar apenas a paridade de grupos de bits. Depois, se não houverem discrepâncias, eles só tem que descartar um bit do grupo. Isto só detecta espionagem com uma probabilidade de 50%, mas se for repetido para n diferentes grupos a probabilidade de Eva espionar sem ser notada é de 1 em 2^n .

- **Não existe espionagem passiva no mundo quântico. Se Eva tentar receber todos os bits ela vai obrigatoriamente interferir nas comunicações.**

- 
- Assim como o protocolo BB84 a criptografia conta com mais três protocolos estes são:

- **Protocolo E91:** O protocolo de Ekert se baseia em duas propriedades do emaranhamento. Primeiro, os estados emaranhados estão perfeitamente correlacionados, de forma que, se Alice e Bob medirem se suas partículas tem polarização vertical e horizontal, eles sempre obterão a mesma resposta, com 100% de probabilidade. O mesmo é verdade se os dois medirem qualquer outro par de polarizações complementares (ortogonais). No entanto, os resultados particulares são completamente aleatórios; é impossível para Alice prever se ela (ou Bob) obterão polarização vertical ou horizontal. Segundo, qualquer tentativa de espionagem por parte de Eva irá destruir as correlações de forma que Alice e Bob poderão detectar sua presença.
- **Protocolo BBM92 e o B92:** Eles podem ser vistos como simplificações dos dois primeiros protocolos.

Hora de Criptografar...



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
V	}	\$	%	&	J	6	T	!	?	^	[	W	4	@	B	*	+	°	7	)	/	3	#	Ü	F

&W %)B[V° @) 7+!@ \$+!B7@6+VJ&W)WV J+V°&



EM DUPLAS OU TRIO CRIPTOGRAFEM UMA FRASE



PERGUNTAS POR FAVOR ENCAMINHAR A:

souza.joaopedro092@gmail.com

fabimellosanches@gmail.com

OBRIGADA!