UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA

PEDRO HENRIQUE TÔRRES SANTOS
SERGIO TORRES TEIXEIRA FILHO

CRIPTOGRAFIA QUÂNTICA:
História, Técnicas e Desafios

RECIFE
2018

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA

PEDRO HENRIQUE TÔRRES SANTOS
SERGIO TORRES TEIXEIRA FILHO

CRIPTOGRAFIA QUÂNTICA:
História, Técnicas e Desafios

Monografia apresentada como requisito para aprovação na matéria de Metodologia e Expressão Técnico-Científica (IF676) no curso de Ciência da Computação, Centro de Informática (Cin) da Universidade Federal de Pernambuco (UFPE).

Orientador(a):
Patrícia Cabral de Azevedo Restelli Tedesco

RECIFE
2018

RESUMO

A Criptografia Quântica é uma área da Criptografia que faz uso das leis da Mecânica Quântica para garantir uma comunicação segura. A pesquisa na área vem crescendo de pouco em pouco, com os computadores quânticos se tornando uma possível ameaça aos sistemas de criptografia mais populares como o RSA que se baseiam em problemas muitos custosos para o computador comum. Essa pesquisa busca abordar um pouco da história da criptografia, quais técnicas são utilizadas para estabelecimento de uma comunicação segura, qual a importância da Mecânica Quântica para esse processo e os desafios na implementação da tecnologia.

Palavras-chave: criptografia, mecânica, informação, quântica, chave pública, segurança.

SUMÁRIO

1. INTRODUÇÃO

A humanidade sempre teve a necessidade de estabelecer alguma forma de comunicação entre seus membros, inicialmente via oral, posteriormente via escrita ou até digital. Entretanto algumas informações sensíveis compartilhadas podem cair nas mãos erradas, para prevenir isto o homem desenvolveu técnicas de proteção desta informação, permitindo que apenas o receptor desejado consiga decifrar a mensagem, o estudo destas técnicas é conhecido como Criptografia.

A importância da Criptografia sofreu um crescimento imensurável com o começo da Era da Informação, dados são enviados constantemente na internet e podem ser alvo de agentes maliciosos que farão mal uso dos mesmos. Nos últimos anos, um tipo específico de criptografia vem ganhando mais interesse, a Criptografia Quântica. O diferencial deste tipo de criptografia está principalmente na resistência a ataques mesmo que o intruso detenha de poder computacional ilimitado.

Este trabalho tem como objetivo apresentar a Criptografia Quântica, seu funcionamento e sua importância para o futuro. Para a exploração desse tema, alguns tópicos como Criptografia e Mecânica Quântica foram abordados, pois possuem conceitos base para o entendimento do tema.

A monografia em questão possui três capítulos. Começando com o capítulo 2, onde é apresentado o estudo da Criptografia, seus principais conceitos e as técnicas usadas atualmente. No capítulo 3 é apresentada a Mecânica Quântica, seus princípios físicos que permitem a existência da Criptografia Quântica e é desenvolvido o tema da Criptografia Quântica propriamente dita, demonstrando seus protocolos, sua fase de implementação e desafios para o futuro. Finalmente, a monografia termina com as conclusões extraídas deste trabalho.

2. CRIPTOGRAFIA

A Criptografia é o conjunto de técnicas e princípios para cifrar a escrita, permitindo que apenas os indivíduos possuidores de um conhecimento específico consigam fazer sentido da mesma. Com o avanço e disseminação da tecnologia, pessoas ao redor do mundo passaram a usar a internet constantemente como parte do seu cotidiano e para garantir a segurança e privacidade destes indivíduo no meio cibernético a criptografia moderna foi de extrema importância. A área de estudo da Criptografia não é apenas de caráter matemático, mas também de linguístico, além de refletir a capacidade do homem de desenvolver técnicas para se adaptar à situações adversas. Neste capítulo será apresentado a história da criptografia e os conceitos importantes da Criptografia Moderna.

2.1. HISTÓRIA

Antes de falar da história da Criptografia deve-se entender as motivações por trás de sua criação. Conforme o homem evolui, suas comunidades também, logo inevitavelmente surgem conflitos e disputas. Para estabelecer a comunicação segura entre dois aliados, foi bastante usada a Esteganografia que funciona como técnicas para "esconder" a escrita, sua primeira aparição na história foi registrada em 400 A.C. com a técnica de marcar a cabeça raspada do mensageiro, deixar o cabelo crescer e raspar quando chegar ao receptor desejado. Embora tenham existido técnicas sofisticadas de Esteganografia, o principal defeito deste tipo de prática se encontra na mensagem desprotegida, uma vez interceptada o indivíduo malicioso tem acesso pleno à mensagem.

A Criptografia deve ter surgido pouco tempo depois da escrita, o primeiro possível registro são hieróglifos egípcios com alguma ordem fora do padrão, alterado pelo escriba. Alguns métodos notáveis na história da criptografia foram a Cifra de César, a Cifra de Veginère e o Enigma. Todos esses métodos usam da substituição de caracteres para cifrar a mensagem, mas posteriormente no começo da Era da Informação a Criptografia começou a se apoiar em conceitos matemáticos como fatoração de números primos e funções de mão única, já que a informação circulava de forma digital e letras e palavras não são nada mais que bits para um computador [De Souza, 2011].

Assim como a Química e Engenharia nuclear, a Criptografia teve seu desenvolvimento impulsionado pelos constantes conflitos históricos, este investimento militar contribuiu para a sofisticação de seus protocolos e técnicas. Em contrapartida, a Criptoanálise mostrou-se mais à frente da Criptografia em vários momentos na história, como na trágica execução da Maria da Escócia, prima da rainha inglesa Isabel I, quando teve suas cartas, que provam seu envolvimento com tentativa de golpe para tomar o trono Inglês, decriptadas [De Souza, 2011].

Figura 1 - Maria da Escócia

Fonte: Wikimedia Commons

Após a Segunda Guerra Mundial, a Criptografia teve avanços em descobertas como a Criptografia de Chave Pública e a Criptografia Quântica que ainda está em uma fase de desenvolvimento até o ano de 2018. Detalhes sobre a pesquisa atual no estado que se encontra a Criptografia Quântica será abordado no capítulo 4.

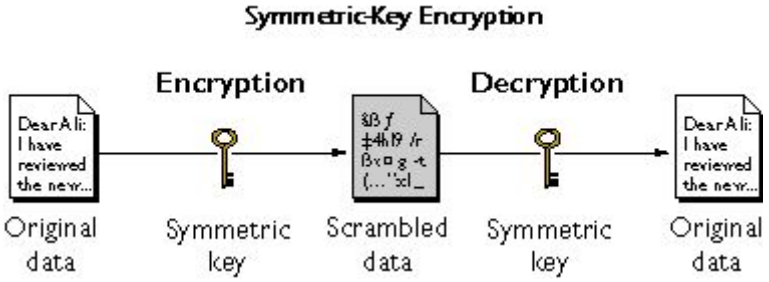
2.2. CONCEITOS CHAVE

Existem vários conceitos específicos dentro da Criptografia, mas serão apresentados os mais importantes e relevantes para o estudo e entendimento da Criptografia Quântica.

2.2.1. Criptografia de Chaves Simétricas

Neste tipo de Criptografia, a chave usada para cifrar a mensagem é a mesma usada para decifrá-la. Embora tenha um bom desempenho, requer um meio seguro de comunicação para transferência das chaves, pois caso o invasor tenha acesso a chave, todas as mensagens se tornam vulneráveis. Após estabelecidas a chave, pode-trocar mensagens com segurança, porém uma troca de chaves periódica é recomendada neste tipo de Criptografia [Stinson, 2006].

Figura 2 - Sistema de Encriptação Simétrica



Fonte: IBM

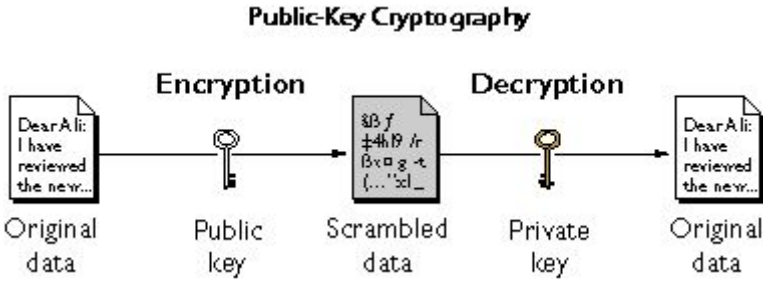
Alguns exemplos de cifras deste tipo são: o DES (Data Encryption Standard 1976-1999, hoje inseguro), o Triple-DES, o IDEA, o RC (Rivest Cipher - muito usado em e-mails), o Twofish, o Blowfish e o AES (Advanced Encryption Standard) [De Souza, 2011].

2.2.2. Criptografia de Chaves Assimétricas

Também chamada de Criptografia de chave pública, é um modelo de criptografia que busca resolver o problema da distribuição de chaves, famoso na área de Criptografia. O problema consiste na necessidade de um meio de comunicação seguro para distribuição das chaves criptográficas. A primeira abordagem desse tipo de técnica foi proposta por Whitfield Diffie e Martin Hellman, em 1976 [Singh, 1999].

O grande diferencial deste modelo de criptografia é a existência de um par de chaves criptográficas, a chave pública e a privada. Como o próprio nome diz a chave pública pode ser anunciada sem risco de fragilidade na segurança do algoritmo, já a chave privada deve ser guardada em segredo. Quem deseja enviar uma mensagem para determinado receptor deve usar a chave pública do destinatário para encriptar a mensagem, e o receptor deve usar a sua chave privada para decriptar a mensagem recebida. Dessa maneira apenas os receptores adequados tem acesso às suas mensagens sem precisar de um meio de comunicação seguro para troca de chaves criptográficas [Stallings, 2016].

Figura 3 - Sistema de Criptografia de Chave Pública



Fonte: IBM

Os algoritmos usados neste tipo de criptografia se baseiam em funções matemáticas chamadas de funções de mão única, nestas funções a engenharia reversa é impraticável de ser feita, usualmente devido ao custo computacional necessário. Logo mesmo sabendo-se a saída e a função, não se consegue obter a entrada usada.

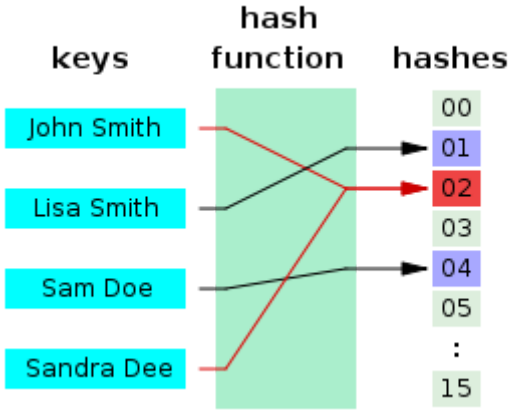
As cifras mais famosas deste tipo de Criptografia são a RSA e o El Gamal, ambos fazem uso de números primos muito grandes para garantir sua segurança [De Souza, 2011].

2.2.3. Criptografia de Hash

A Criptografia de Hash faz uso das funções de hash, que são funções que convertem um dado para outro dado, com menos memória(bits de informação). Como é o conjunto de entrada é maior que o de saída, já que o número de bits diminui, entradas diferentes podem ter a mesma saída, isso é o que chamamos de colisões. Uma boa função de hash deve ser difícil de encontrar colisões e caso ocorra uma leve modificação na entrada a saída deve ser bastante diferente [Stallings, 2016].

Quanto mais antigo e testado mais seguro o algoritmo de Hash, não é recomendado o uso de algoritmos relativamente novos, pois vulnerabilidades podem tomar tempo para serem descobertas. As funções de Hash podem ser usadas para verificar a integridade de arquivos na internet e também para melhorar o desempenho de busca de dados, com estruturas de dados baseadas em Hash(como a Tabela de Hash).

Figura 4 - Tabela de Hash



Fonte: Wiki Commons

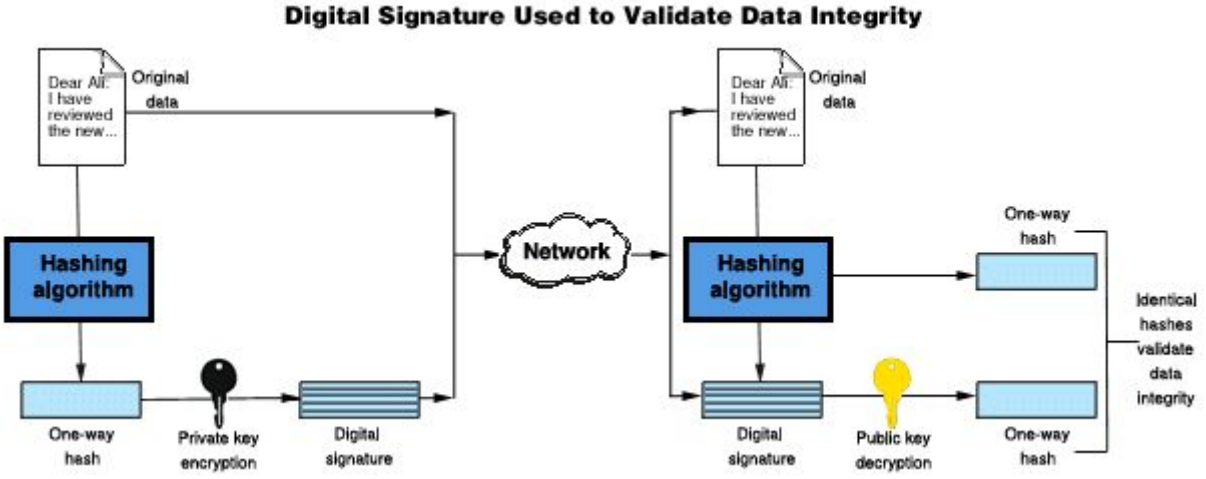
Existem várias funções de Hash, mas dentre elas podemos destacar a SHA(Secure Hash System) e a MD(Message Digest Algorithm) [De Souza, 2011].

2.2.4. Criptografia de Assinaturas Digitais

No mundo digital, foram desenvolvidas técnicas para garantir a autenticidade de arquivos, mensagens e outras coisas. A assinatura criptográfica é normalmente utilizada incluindo o Hash da mensagem, ou arquivo, encriptado pela chave privada do assinante nele

mesmo, desta maneira qualquer indivíduo pode verificar a autenticidade e integridade calculando o Hash e o comparando com o Hash contido no arquivo ou mensagem após ser decriptado pela chave pública(a qual todos têm acesso).

Figura 5 - Sistema de Assinatura Digital para Integridade de Dados



Fonte: IBM

2.3. CONSIDERAÇÕES DO CAPÍTULO

Neste capítulo foram apresentadas a história e origem da criptografia, mostrando que sua importância para a sociedade não começou apenas na Era da Informação e revelando a necessidade do homem moderno de Segurança de Informação. Também foram apresentados os conceitos chave da Criptografia Moderna, como a Criptografia de Chave Pública que foi uma grande descoberta para a área já que solucionava o Problema da Distribuição de Chaves. A Criptografia sempre esteve alinhada à segurança, embora nos tempos modernos ela está sendo utilizada para garantir a privacidade do homem no meio digital.

3. CRIPTOGRAFIA QUÂNTICA

Neste capítulo vamos explicar brevemente os conceitos básicos da Mecânica Quântica para conseguir mostrar como algumas propriedades podem ser usadas para criar protocolos de Criptografia e também apresentar protocolos de Criptografia Quântica existentes.

3.1. MECÂNICA QUÂNTICA

A Mecânica Quântica é o ramo da Física que estuda sistemas físicos com dimensões quase atômicas ou menores como moléculas e átomos, vamos entender como esses sistemas podem nos ajudar a estabelecer uma comunicação segura.

3.1.1. Dualidade da Luz

Uma descoberta importante para a Física Quântica foi o comportamento onda-partícula da Luz, revelando que um raio de Luz consistia de inúmeras partículas com propriedades parecidas com o de onda, chamadas Fótons. Após a descoberta, a tecnologia moderna permitiu que físicos usassem filamentos para a transferência de Fótons individuais em sequência na tentativa de entender melhor seu comportamento. Os resultados obtidos desafiavam as Leis Clássicas da Física e necessitavam de novas teorias para explicar o fenômeno [Singh, 1999].

3.1.2. Sobreposição Quântica

O conceito de Sobreposição na Mecânica Quântica procura explicar o comportamento de certas partículas quando não se sabe o que ela está fazendo agora, assumindo que ela pode estar fazendo todas as possibilidades simultaneamente. Se cada possibilidade for considerada um estado então existe uma sobreposição de estados. A explicação pode parecer infantil, mas justifica os resultados obtidos no experimento descrito acima e é aceita por uma boa proporção de cientistas [Nielsen e Chuang, 2010].

Em 1933, o físico austríaco Erwin Schrödinger ganhou o prêmio Nobel de Física por ter inventado uma parábola conhecida como "Gato de Schrödinger", constantemente usada para explicar melhor o conceito de Sobreposição Quântica. Imagine um gato em uma caixa, sabemos que o gato está vivo pois podemos vê-lo, colocamos um frasco de cianeto dentro da caixa e a fechamos. Nesse momento, entramos em um período de ignorância já que o gato pode estar tanto vivo como morto e não conseguimos observá-lo, dessa maneira a teoria quântica nos permite afirmar que o gato está tanto vivo quanto morto, satisfazendo todas as possibilidades. Se abrirmos a caixa o gato estará em um estado apenas, ou vivo ou morto.

Figura 6 - Erwin Schrödinger em 1933

Fonte: Wikimedia Commons

3.2. PROTOCOLOS DE CRIPTOGRAFIA QUÂNTICA

Enquanto Criptoanalistas esperam a chegada de computadores quânticos, Criptógrafos estão trabalhando em técnicas que são resistentes a ataques dos mesmos. Uma grande escolha para enfrentar esta ameaça foi a de combater fogo com fogo, porque não utilizar dos mesmos princípios da Mecânica Quântica para confrontar o Computador Quântico [Rigolin e Rieznik, 2005].

3.2.1. Protocolo BB84

Em 1984, Charles Bennett e Gilles Brassard desenvolveram o que seria o primeiro protocolo de Criptografia Quântica da história, o BB84 resolve o famoso problema de distribuição de chaves da Criptografia fazendo uso de propriedades quânticas do Fóton. Uma solução alternativa aos protocolos de Criptografia Assimétrica discutidos anteriormente já que muitos deles estão ameaçados pelo desenvolvimento dos Computadores Quânticos, máquinas com poder computacional muito superior aos atuais computadores.

Por ser um protocolo simples e preciso, é bastante recomendado para iniciantes ao tema de Criptografia Quântica. É o protocolo de distribuição quântica de chaves mais bem sucedido do mercado.

Para transferir a chave são usados Fótons, cada Fóton representando um bit. Para saber se o Fóton representa um '1' ou um '0' a sua polarização seria medida em quatro direções distintas. Para a medição eram usadas as bases Retangular, onde os Fótons estavam com polarização ou na horizontal ou na vertical, e Diagonal, onde os Fótons estavam com polarização nas diagonais principal e secundária. Usando estas bases, os bits são definidos de acordo com a orientação obtida.

O protocolo funciona da seguinte forma: Primeiro Alice seleciona uma cadeia de bits aleatórios para enviar, depois escolhe aleatoriamente uma base para medir cada bit, alice gera os Fótons com os estados correspondentes aos bits de acordo com cada base escolhida individualmente. Finalizada essa parte, Alice transmite os Fótons um a um na rede. Para cada Fóton Bob escolhe aleatoriamente uma das bases para medir a polarização de um Fóton por vez, após esse processo Bob revela quais bases usou para cada Fóton, Alice lhe diz quais ele mediu com a base certa e usa apenas os bits corretos para gerar uma chave criptográfica [Bennet e Brassard, 1984].

Além de garantir a transmissão de chaves em segurança, esse protocolo também detecta se existe alguém escutando a rede, pois quando os Fótons tem sua polarização medida a sua orientação pode ser alterada. Para detectar Bob revela alguns dos bits da chave, e após confirmação os exclui na chave.

Figura 7 - Tabela do Protocolo BB84

QUANTUM TRANSMISSION															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕	⤡	⤢	⤢	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

Fonte: Bennet e Brassard(1984)

O protocolo foi posto em prática pela primeira vez em 1989 no Centro de Pesquisas Thomas J. Watson da IBM, por Charles H. Bennett e John A. Smolin.

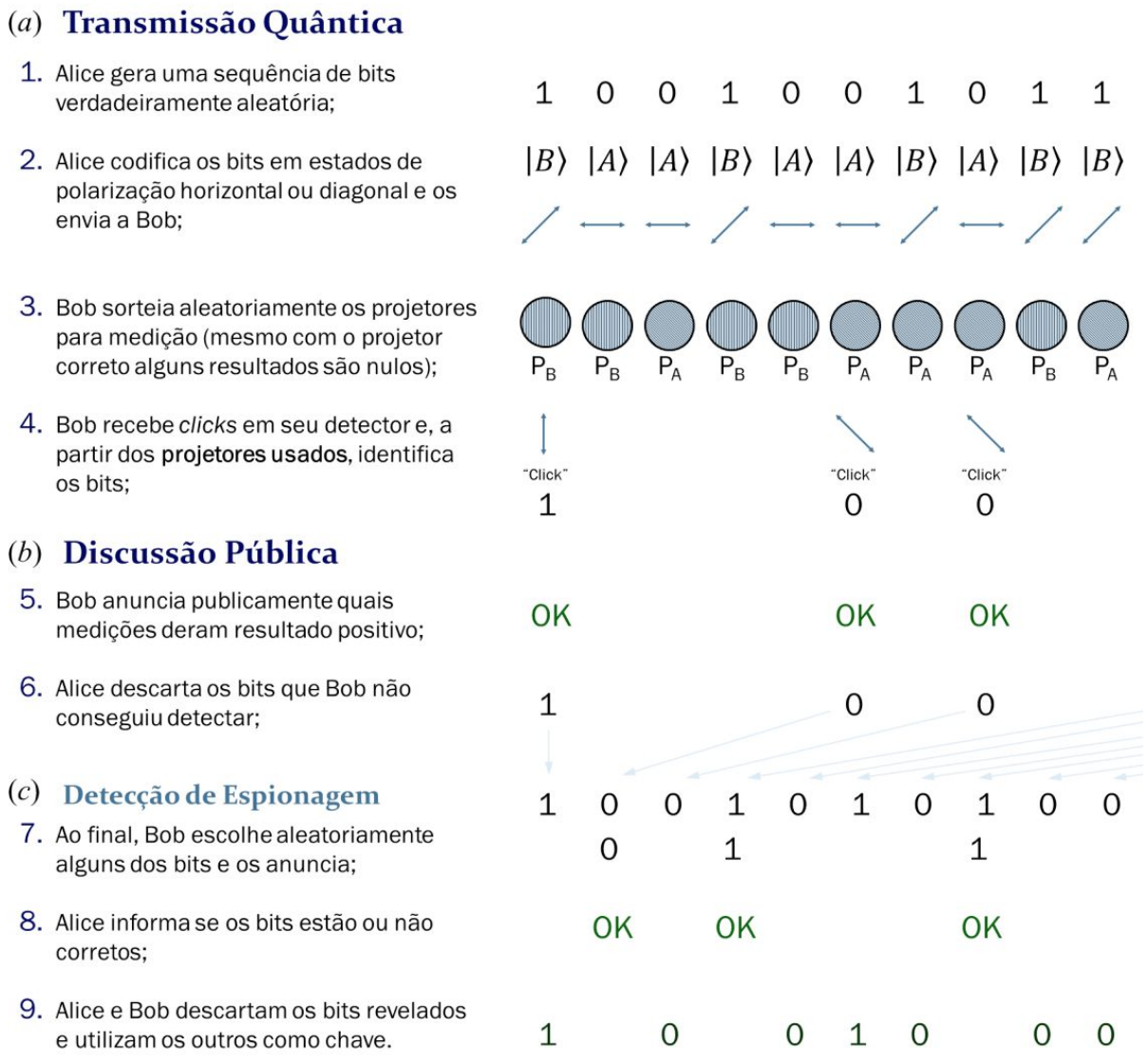
3.2.2. Protocolo B92

Em 1992, Charles Bennett não satisfeito com o protocolo BB84 desenvolveu outro protocolo de Criptografia Quântica abordando o problema de troca de chaves, embora muito semelhante ao BB84 faz uso de projetores para medição do Fóton.

A grande vantagem desse uso de projetores é que permite o uso apenas de dois estados não-ortogonais, logo sempre que for usado o medidor com base errada o resultado será nulo e quando certo tem chance de retornar algum resultado.

Feito o procedimento similar ao protocolo BB84, só que no nesse caso o receptor só teria acesso aos bits medidos corretamente, logo gerando uma chave que possibilita comunicação segura. É um protocolo de difícil implementação, mas é de fato uma evolução desejada em comparação ao BB84.

Figura 8 - Protocolo B92



Fonte: De Souza(2011)

3.3. CONSIDERAÇÕES DO CAPÍTULO

Neste capítulo, introduzimos a engenhosa Criptografia Quântica e o benefício que a Mecânica Quântica pode trazer para a Segurança da Informação nos tempos que estão por vir, onde o poder computacional será abundante. Foram discutidos dois importantes protocolos de Criptografia Quântica, o BB84 e o B92, não só o seu funcionamento mas também seu objetivo como ferramenta de segurança. Além de brevemente explicar alguns conceitos da Mecânica Quântica que permitem a existência desses protocolos.

5. CONCLUSÃO

Ao longo da história da humanidade a comunicação sempre teve um papel importante na sociedade, essa forma de troca de informações tornou-se a base de nossa sociedade tecnológica da Era Digital. A Criptografia, sempre presente nos maiores conflitos da humanidade, foi desenvolvida para garantir que essa comunicação seja feita de uma maneira segura, sem comprometer dados sensíveis.

O estudo na área da Criptografia foi cada vez mais aprimorado assim como na Computação Quântica, essa última área que está ameaçando grande parte dos protocolos de Criptografias atuais. Nesta monografia você conheceu um pouco da história da Criptografia, os conceitos da Criptografia moderna, conceitos da Mecânica Quântica e como eles podem ser usados para a criação de protocolos de Criptografia ainda mais seguros. Esses protocolos de Criptografia Quântica ainda não são utilizados amplamente pelo mercado, até pela complexidade técnica de sua implementação.

O dois protocolos discutidos são ótimos para introduzir novatos ao tema da Criptografia Quântica pois sua explicação teórica pode ser bastante simplificada. Embora os computadores quânticos ainda não estejam em fase de pesquisa muito avançada, é incrível notar que medidas contra essa possível ameaça já estão sendo providenciadas.

Existem muitas barreiras pela frente antes que a Criptografia Quântica seja amplamente utilizada na indústria, mas conforme foi exposto nesta monografia, o benefício que esta pesquisa pode trazer é imenso.

REFERÊNCIAS BIBLIOGRÁFICAS

RIGOLIN, Gustavo; RIEZNIK, Andrés Anibal. Introdução à Computação Quântica. **Revista Brasileira de Ensino de Física**, Campinas, v. 27, n. 4, p.517-526, 6 out. 2005.

NIELSEN, Michael A.; CHUANG, Isaac L.. **Quantum Computation and Quantum Information.** Cambridge: Cambridge University Press, 2010.

NOVAES, Marcel; STUDART, Nelson. **Mecânica Quântica Básica.** São Paulo: Livraria da Física, 2016.

SINGH, Simon. **The Code Book:** The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Londres: Fourth Estate, 1999.

GRIFFITHS, David. **Introduction to Quantum Mechanics.** New Jersey: Prentice Hall, 1995.

SCARANI, Valerio et al. The security of practical quantum key distribution. **Reviews Of Modern Physics**, [s.l.], v. 81, n. 3, p.1301-1350, 29 set. 2009.

GOEL, Rajni; GARUBA, Moses; GIRMA, Anteneh. Research Directions in Quantum Cryptography. **Fourth International Conference On Information Technology**, [s.l.], p.779-784, abr. 2007.

EKERT, Artur K.. Quantum cryptography based on Bell's theorem. **Physical Review Letters**, [s.l.], v. 67, n. 6, p.661-663, 5 ago. 1991. American Physical Society (APS).

ELBOUKHARI, Mohamed; AZIZI, Abdelmalek; AZIZI, Mostafa. Quantum Key Distribution in practice: The state of art. **2010 5th International Symposium On I/v Communications And Mobile Network**, [s.l.], p.1-4, set. 2010.

STALLINGS, William. **Cryptography and Network Security.** 7. ed. New Jersey: Pearson, 2016.

STINSON, Douglas R.. **Cryptography: Theory and Practice.** Boca Raton: Chapman & Hall/crc, 2006.

NIEMIEC, Marcin; PACH, Andrzej R.. The measure of security in quantum cryptography. **2012 Ieee Global Communications Conference (globecom)**, Anaheim, Ca, p.967-972, dez. 2012.

BENNETT, Charles H.; BRASSARD, Gilles. Quantum cryptography: Public key distribution and coin tossing. **Theoretical Computer Science**, [s.l.], p.7-11, set. 2011.

DE SOUZA, Douglas Delgado. **Criptografia Quântica com Estados Comprimidos da Luz**. Campinas: [s.n.], 2011. 1 p. Disponível em: <http://repositorio.unicamp.br/bitstream/REPOSIP/277397/1/Souza_DouglasDelgadode_M.pdf>.