Revista de Sistemas de Informação da FSMA
n. 7 (2011) pp. 39-48

SISTEMAS DE INFORMAÇÃO
http://www.fsma.edu.br/si/sistemas.html

TUTORIAL

# Criptografia Quântica: Uma Abordagem Direta

A. J. B. Mendes, E. H. Paulicena, W. A. R de Souza

*Resumo*—**O presente trabalho tem por objetivo responder de forma direta a quatro questões atinentes ao conhecimento do que seja Criptografia Quântica. O texto se desenvolve através de um painel histórico da cifragem de mensagens, chegando até a criptografia assimétrica, enquanto solução para o problema da produção e distribuição de chaves. A seguir, inserido em um escopo quântico, conceitua e exemplifica protocolos de criptografia quântica, apresentando, em conclusão, as respostas pretendidas.**

*Index Terms*- **Criptografia Quântica, Distribuição Quântica de Chaves Secretas, BB84, Reconciliação de Informações, Amplificação de Privacidade.**

## INTRODUÇÃO

ESTE trabalho tem por propósito estabelecer um encadeamento sequencial, em linguagem acessível a quem não se dedica ao tema, sobre os limites e as possibilidades da Criptografia Quântica.

Faz-se necessário um esclarecimento inicial quanto à abrangência do que se pretende: o termo Criptografia Quântica, para os específicos fins do presente tutorial, será cingido, exclusivamente, ao conceito de Distribuição Quântica de Chaves Secretas.

Pretende-se, sem extravio dos nortes acadêmicos já estabelecidos ao assunto, trazê-lo a um nível de entendimento objetivo que permita entender os conceitos fundamentais e apresentar respostas a algumas perguntas relacionadas.

Para tanto, a Seção II aborda a questão fundamental da criptografia, qual seja, a garantia do segredo de uma mensagem. Através de um breve histórico é verificado de que forma algoritmo e chave se relacionam em sistemas criptográficos e a quais limites de segurança estão submetidos.

A Seção III apresenta algumas evidências da Mecânica Quântica que a diferenciam da Clássica, tornando uma hipótese possível a construção de um computador que tenha o seu processamento de cálculos baseado em estados quânticos.

Manuscript received march 25, 2011.

Alvaro Jorge Braga MENDES, Centro de Análises de Sistemas Navais – CASNAV. Rua da Ponte, Ed 23 do AMRJ, Ilha das Cobras, Centro, 20091-000 Rio de Janeiro, RJ, Brasil, alvaro@casnav.mar.mil.br

Edésio Hernane PAULICENA, Centro de Análises de Sistemas Navais – CASNAV. Rua da Ponte, Ed 23 do AMRJ, Ilha das Cobras, Centro, 20091-000 Rio de Janeiro, RJ, Brasil, edesio@casnav.mar.mil.br

William Augusto Rodrigues de SOUZA., Centro de Análises de Sistemas Navais – CASNAV. Rua da Ponte, Ed 23 do AMRJ, Ilha das Cobras, Centro, 20091-000 Rio de Janeiro, RJ, Brasil, william@casnav.mar.mil.br

A Seção IV, após observar a distinção entre Computação Quântica e Distribuição Quântica de Chaves Secretas, apresenta os procedimentos relativos ao Protocolo BB84, estabelecendo as conclusões pertinentes àquele procedimento.

A Seção V estabelece uma exemplificação teórica que atenda aos procedimentos de Reconciliação de Informação e Amplificação de Privacidade, conforme as suas definições acadêmicas originais e observa alguns comentários sobre o estado atual do assunto deste trabalho.

A Seção VI, que é a conclusão, apresenta resposta às seguintes perguntas:

a) a computação quântica é imprescindível para a Distribuição Quântica de Chaves Secretas?

b) a Distribuição Quântica de Chaves Secretas é um sistema autossuficiente para a cifragem e a decifragem de mensagens?

c) qual é o propósito da Distribuição Quântica de Chaves Secretas?

d) o que significa a afirmação de que a Distribuição Quântica de Chaves Secretas é 100% segura?

## CRIPTOGRAFIA CLÁSSICA

Três palavras são, usualmente, utilizadas no universo da cifragem e decifragem de mensagens: criptologia, criptografia e criptoanálise. Convém esclarecer e nada melhor do que usar a etimologia das palavras. *Cripto* é palavra de origem grega que significa segredo. *Logos* significa discurso, estudo. *Grafos* significa grafia, escrita. *Análise*, oposto a síntese, significa separação. Dito isto, torna-se simples prosseguir.

Criptologia é o estudo dos segredos, de forma ampla, compreendendo a criptografia e a criptoanálise; criptografia é a escrita dos segredos, aqui entendida pelos dois processos, o de cifragem de uma mensagem e o de decifragem; e criptoanálise é a separação dos segredos, ou seja, a busca de se obter, a partir de um texto cifrado, sem conhecimento prévio do segredo, qual mensagem original o originou, ou a obtenção da própria chave em si.

A arte de cifrar mensagens já era conhecida pelos antigos e a Cifra de Cesar [1], imperador romano, consistia em escrever a mensagem original, chamada de texto claro no contexto criptográfico, através de uma simples substituição de cada letra por outra letra três posições adiante. Assim, a letra “A” cifrada se tornava “D” e a palavra “CESAR” se transformava em “FHVDU”.

No século XX, máquinas eletromecânicas inicialmente e computadores logo a seguir deram grande avanço à criptografia, pelo enorme poder de modificação e embaralhamento de um texto claro.

É interessante observar que processos criptográficos habitualmente têm dois elementos fundamentais: algoritmo e chave. O algoritmo é o procedimento a ser usado na cifragem e a chave é uma especificação para aquele procedimento. Na Cifra de Cesar, por exemplo, o algoritmo é: "substitua pela letra que fica em alguma posição adiante". E a chave é "3 ou terceira posição". Note-se que conhecer, apenas, o algoritmo não resolve o problema, porque não se sabe em quantas posições adiante se deve parar. Para descobrir isso, deve-se entrar no campo da criptoanálise, com um procedimento chamado "força bruta", que consiste em testar todas as possibilidades de chave. Para um alfabeto de 26 letras, a Cifra de Cesar teria 25 chaves, já que uma delas não faria sentido por manter o texto claro na mesma posição do cifrado. Assim, com apenas 25 tentativas, no máximo, seríamos capazes de ter quebrado aquela cifra e descoberto o texto claro.

Esse pequeno exemplo só tem um propósito: mostrar o quão importante é a questão da chave criptográfica. Até porque, os algoritmos criptográficos normalmente utilizados têm seus códigos abertos e são de conhecimento público. Como se mantém o segredo então? Pela chave.

Tal fato já fora estabelecido, de forma explícita, por Auguste Kerckhoffs em 1873, em *La criptographie Militaire*, quando foi apresentado, propondo que a segurança de um sistema criptográfico deve residir unicamente no segredo da chave, e não no sigilo do algoritmo [2].

As atuais chaves criptográficas costumam ter 128 ou 256 bits (sequências de zeros e uns). No caso de uma chave com 256 bits, isso significa $2^{256}$ possibilidades. Só para se ter uma ideia da ordem de grandeza desse número, deve-se imaginar o número 1 seguido de 77 zeros. Bem melhor do que as 25 tentativas da Cifra de Cesar, portanto.

A **Tabela 1** apresenta um exemplo do tempo médio exigido, para um ataque por força bruta executado em alguns algoritmos criptográficos, para busca completa da chave, a partir da realização de um número fixo de tarefas de decriptografia por unidade de tempo [1].

O resultado obtido na última coluna contempla a possibilidade de arquiteturas de sistemas de microprocessadores maciçamente paralelas.

Como comparação, é bom lembrar que se costuma atribuir a idade do universo -da explosão do Big Bang aos nossos dias- como sendo de $1{,}37 \times 10^{10}$ anos.

A criptografia simétrica, que se usa até hoje para garantir a confidencialidade das mensagens, é um procedimento algorítmico que utiliza uma única chave, tanto para cifrar quanto para decifrar. Dessa forma, em algum momento a chave usada pelo emissor para cifrar um texto claro tem que chegar às mãos do destinatário, para que ele possa decifrar o texto que foi cifrado. Os canais clássicos de transmissão da chave, a ser utilizada, vão desde a possibilidade oral até a transmissão telefônica ou por e-mail. Se por um lado, informar uma chave oral e pessoalmente tem um razoável critério de segurança, por outro turno, essa forma não produz a agilidade que se precisa. Já a informação de uma chave por um meio ágil de transmissão, como o e-mail, por exemplo, implica na possibilidade daquele meio ser invadido por um intruso e essa informação da chave ser copiada ou mesmo adulterada.

Essa é a questão central da criptografia: garantir que apenas partes autorizadas tenham acesso ao que se quer transmitir. A criptografia simétrica garante a segurança do texto claro com a utilização de uma chave de 128 ou 256 bits. Mas quem garante a segurança da chave?

Nas últimas décadas do século passado, essa questão foi resolvida pela criptografia assimétrica ou de chave pública. Como um ovo de Colombo, ela é simples depois que se conhece. A criptografia assimétrica também consiste em algoritmo e chave. Só que agora, duas chaves. Quando uma chave é usada para cifrar, só a outra chave, que lhe faz par, pode decifrar o texto.

Assim, se um usuário deseja receber mensagens criptografadas, basta ele informar, publicamente, qual é a chave que deve ser utilizada por quem quiser cifrar mensagens para ele. Esta chave é chamada de chave pública. Recebida a mensagem cifrada, o usuário usará para decifrá-la outra chave de conhecimento exclusivo dele, chamada chave privada. E apenas esta chave privada é capaz de decifrar a mensagem recebida. Dessa forma, cada usuário envolvido em um processo de transmissão criptográfica terá o seu próprio par de chaves; com a pública as mensagens são cifradas para aquele usuário e com a chave privada ele as decifra.

Tabela 1 - Tempo Médio de Busca de Chaves

| Tamanho da chave (bits) | Número de chaves possíveis | Tempo necessário para busca da chave, usando-se 1 decriptografia /µs | Tempo necessário para busca da chave, usando-se 1 milhão de decriptografias/ µs |
|---|---|---|---|
| 32 | $2^{32}=4{,}3 \times 10^{9}$ | 35,8 minutos | 2,15 milissegundos |
| 56 | $2^{56}=7{,}2 \times 10^{16}$ | 1.142 anos | 10,01 horas |
| 128 | $2^{128}=3{,}4 \times 10^{38}$ | $5{,}4 \times 10^{24}$ anos | $5{,}4 \times 10^{18}$ anos |
| 168 | $2^{168}=3{,}7 \times 10^{50}$ | $5{,}9 \times 10^{36}$ anos | $5{,}9 \times 10^{30}$ anos |

Alguns conceitos devem ficar bem claros:

a) O algoritmo assimétrico é estruturalmente diferente do simétrico. Os cálculos que suportam o assimétrico são baseados em funções matemáticas que exigem a utilização obrigatória de duas chaves, uma de entrada para cifrar e outra de saída para decifrar;
b) Qualquer usuário da transmissão pode calcular o seu

próprio par de chaves;

c) Calculado o par de chaves, o que foi cifrado com a pública só pode ser decifrado com a chave privada;
d) Não é exequível, exceto para quem calculou o seu próprio par de chaves, obter a chave privada, conhecendo-se apenas a chave pública, e vice-versa, se for o caso.

O que pode parecer estranho é como alguém é capaz de calcular as duas chaves, que são interligadas por uma função matemática, informar uma delas e não ser exequível para mais ninguém calcular a outra chave. A resposta disso é que a pessoa que calcula as duas chaves possui determinadas informações adicionais que não são repassadas em público. Sem essas informações, surge a inexequibilidade.

Em uma linguagem meramente ilustrativa pode-se pensar assim: existem algumas funções matemáticas em que é trivial fazer-se o caminho de ida (a cifragem), mas inexequivel fazer-se o caminho de volta (a decifragem). E como é feita a decifragem, então? Com um conhecimento adicional, por parte de quem cifrou, de um informação não repassada.

Serve de exemplo um sistema usualmente utilizado na criptografia assimétrica: o RSA [3]. Como existe uma dificuldade para se fatorar alguns números muito grandes, gerados pelo produto de dois números primos também grandes, a informação divulgada apenas do número que representa esse produto não é suficiente para que através de uma chave pública seja exequível se obter a chave privada correspondente. Contudo, à pessoa que conhece a fatoração daquele número, torna-se simples formar um par de chaves.

Esse modelo apresentado tinha tudo para substituir e expurgar a criptografia de uma só chave. Ocorre que os cálculos matemáticos dessa criptografia de chave pública são muito extensos e geram uma lentidão de processamento computacional, se comparados aos da simétrica. Assim, no lugar de se cifrar todo um extenso texto claro com a criptografia assimétrica, optou-se por cifrar apenas um texto pequeno, por exemplo de 128 ou 256 bits, que é o tamanho de uma chave a ser usada em criptografia simétrica. Implica dizer que, habitualmente, a criptografia assimétrica é utilizada para cifrar apenas a chave que vai ser usada. A cifragem de todo o texto claro é a criptografia simétrica quem vai fazer. Tal procedimento é, comumente, referenciado como sistema criptográfico híbrido.

Na verdade, a criptografia assimétrica desempenha outros papéis, como a assinatura digital. Só que para o escopo aqui traçado, a criptografia de chave pública será limitada à produção de chaves.

Assim, com a criptografia assimétrica desempenhando o papel de fornecedora de chaves para a simétrica, os criptoanalistas desviaram o olhar da criptoanálise para outra possibilidade: em vez de aplicar a força bruta na procura da chave usando o texto cifrado, agora era possível, também, aplicar a força bruta no algoritmo assimétrico que produzia a chave, em consequência dos problemas matemáticos intrínsecos ao fato dos algoritmos não serem eficientemente resolvidos. Só que isso se verificou, igualmente, inexequível para os atuais padrões computacionais. Significa dizer que a partir dos dados contidos na chave pública, sem a solução eficiente dos algoritmos matemáticos, os mais avançados computadores de hoje levariam um tempo tão absurdamente grande para chegar à chave privada que tornariam essa possibilidade inexequível.

## COMPUTAÇÃO QUÂNTICA

**"O propósito final da computação quântica é construir um computador impensavelmente mais rápido do que os computadores que dispomos hoje em dia" [4].**

Os computadores clássicos utilizados no dia a dia podem ser imaginados, de forma bastante simplificada, como sendo máquinas capazes de ler entradas codificadas em zeros e uns, executar cálculos e gerar saídas também codificadas em zeros e uns. Tais zeros e uns podem ser representados, fisicamente, através de um estado de baixo potencial elétrico (o bit 0), ou de um estado de alto potencial elétrico (o bit 1). O fundamento que norteia a computação clássica é o que advém do senso comum: ou ocorre um estado de baixo potencial elétrico ou ocorre um de alto, significando que ou se tem o bit 0 ou se tem o bit 1. Nunca os dois ao mesmo tempo.

Dessa forma, a realização de duas operações consecutivas e independentes com esses bits acontecerá, normalmente, através de dois passos lógicos seguidos.

Ocorre que, em Mecânica Quântica, esse senso comum cai por terra. Não existem estados clássicos, mas estados quânticos, aos quais está associada uma distribuição de probabilidade. Essa distribuição indica a probabilidade de se encontrar cada valor possível de uma medição, que pode ser simbolizado pelo bit 0 ou pelo bit 1.

Em computação quântica o bit é substituído pelo *q-bit* e os valores 0 e 1 de um bit são substituídos por vetores, aqui representados em nomenclatura conhecida como notação de Dirac [5]:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Costuma-se, ainda, representar essa função de probabilidade de um *q-bit* genérico $|\psi\rangle$ como sendo uma combinação linear dos vetores $|0\rangle$ e $|1\rangle$, tal que [5]:

$|\psi\rangle = m\,|0\rangle + p\,|1\rangle$, onde m e p são números complexos.

O que interessa, diretamente, na interpretação física do *q-bit*, é o fato dele poder estar simultaneamente nos estados $|0\rangle$ e $|1\rangle$.

Este é o grande antagonismo: no mundo clássico, diferentes possibilidades não podem coexistir simultaneamente, mas no mundo quântico as diferentes possibilidades podem coexistir, chamando-se a isso de superposição. Portanto, aquelas operações independentes que tinham que ser feitas passo a passo na computação clássica, agora na quântica podem ser feitas ao mesmo tempo em um único passo, dentro daquele

estado quântico específico.

Uma analogia pode ser traçada [4]: imagine-se um carro andando e dispondo de duas possibilidades, uma delas continuar em linha reta e a outra virar na esquina. No mundo clássico, o carro não pode seguir reto e dobrar na esquina ao mesmo tempo. Já um hipotético "carro quântico" poderia, simultaneamente, seguir em frente e dobrar na esquina. Ainda no campo exclusivo da ilustração teórica, duas novas versões de "carros quânticos" teriam sido geradas nesse caso. Ocorre que cada uma das versões poderia, de novo, continuar reto ou virar na esquina, gerando mais duas versões e assim sucessivamente. A questão seguinte é: será que cada uma dessas versões de "carro quântico" poderia executar uma tarefa? A resposta que a computação quântica apresenta é que sim, é possível realizar, simultaneamente, uma quantidade exponencialmente grande de tarefas, ainda que não se obtenha o resultado de cada uma delas em separado.

Com isso, fica claro o propósito final da computação quântica enunciado anteriormente, qual seja: o de obter um computador "impensavelmente" mais rápido.

Porém, existem obstáculos a serem transpostos, que ainda fazem com que a computação quântica tenha muito caminho a percorrer. Como foi visto, existe uma realidade física nos fenômenos da mecânica clássica, intrínsecos a eles mesmos, independentes do observador. O que a mecânica quântica constata é o oposto disso. Não há uma realidade intrínseca no estado quântico. Ao invés, há uma superposição, uma coexistência de possibilidades que, quando são aferidas pela medição de um observador, terão o seu estado afetado, de modo a colapsar para uma daquelas possibilidades. Assim, após a execução dos cálculos simultâneos, na extração da informação desejada, a leitura de um resultado quântico carrega sempre uma probabilidade de que o resultado correto não seja obtido.

Com o avanço da nanotecnologia, a superação da fragilidade de sistemas a interferências externas e a descoberta de novos materiais e processos, aguarda-se, para o mais breve que a ciência permitir, a produção do computador quântico como artigo comercial.

## PROTOCOLO BB84

Diferentemente do que se possa imagina, a Distribuição Quântica de Chaves Secretas não é uma criptografia que deverá ser usada nos computadores quânticos.

Enquanto o computador quântico ainda não existe como produto comercial, a Distribuição Quântica de Chaves Secretas já estabeleceu os seus protocolos de comunicação e já foi utilizada publicamente.

Na verdade, a Distribuição Quântica de Chaves Secretas, como se a conhece hoje, prescinde do computador quântico. Ela se utiliza apenas de um canal quântico e de um canal clássico.

Por canal de comunicação quântica, entenda-se uma fibra ótica, por exemplo, que permite a transmissão de fótons, partículas que compõem a luz. E por canal clássico, entenda-se a comunicação por qualquer outro meio usual, como e-mail, ondas radiofônicas, etc.

Na Mecânica Quântica é possível estabelecer o conceito de polarização para um único fóton, em caráter binário. Assim, a polarização da luz pode ser entendida como sendo uma propriedade quântica que pode ser representada por um vetor em um espaço bidimensional, como mostram os eixos ortogonais da **Figura 1**.

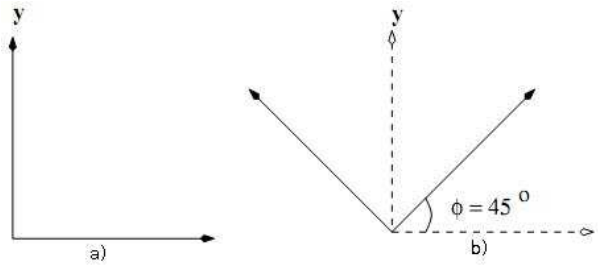


Figura 1 - Bases Ortogonais a) V-H b)D-C

Muito antes de artigos, relativamente, recentes sobre criptografia quântica, que apresentam o assunto de forma mais ampla, como em [6] e [7], na década 80 do século passado, surgiu o primeiro protocolo de Distribuição Quântica de Chaves Secretas, designado por BB84. As letras fazem referência aos nomes de Charles H. Bennett e Gilles Brassard e o número, ao ano de 1984 [8].

O protocolo BB84 parte do pressuposto de que um emissor transmite, em um canal quântico, fótons polarizados para um receptor. Além disso, serão utilizadas para a emissão e recepção desses fótons as duas bases ortogonais estabelecidas na **Figura 1**, quais sejam V-H (vertical/horizontal) e D-C (diagonal/contradiagonal).

Com o propósito de facilidade de entendimento, mas sem perda de exatidão, será utilizada uma simbologia gráfica para a designação das possibilidades de polarização do fóton, em substituição à clássica notação de Dirac. Trata-se de simbologia gráfica semelhante à utilizada por Brassard e Bennett. Da mesma forma, dentro do escopo do presente trabalho, fóton polarizado e *q-bit* significarão o mesmo.

Com a utilização da base V-H, há duas polarizações (ou *q-bits*) possíveis: → ↑

A primeira delas define direção estabelecida fazendo-se $\phi = 0$; e a segunda, $\phi = \pi/2$

Com a utilização da base D-C, há duas polarizações (ou *q-bits*) possíveis: ↗ ↖

A primeira delas define direção estabelecida fazendo-se $\phi = \pi/4$; e a segunda, $\phi = 3\pi/4$.

Pode-se resumir, então, as seguintes constatações verificadas a partir de uma comunicação em canal quântico:

1. Emissor consegue polarizar um fóton, a partir das bases V-H e D-C, em quatro diferentes posições:

↑ → ↗ ↖

2. Receptor, para captar o fóton, utiliza uma das seguintes bases:
   - (V-H)
   - (D-C)
3. Se o receptor utilizar a base V-H, há quatro possibilidades:
   a) Se o fóton polarizado for ↑ , ele é captado exatamente como ↑;
   b) Se o fóton polarizado for → , ele é captado exatamente como →;
   c) Se o fóton polarizado for ↗ , essa informação é perdida e o fóton é captado como ↑ ou → , com probabilidade de ½ para a captação ↑ e ½ para a captação →;
   d) Se o fóton polarizado for ↖ , essa informação é perdida e o fóton é captado como ↑ ou → , com probabilidade de ½ para a captação ↑ e ½ para a captação →.
4. Se o receptor utilizar a base D-C há quatro possibilidades:
   a) Se o fóton polarizado for ↗ , ele é captado exatamente como ↗;
   b) Se o fóton polarizado for ↖ , ele é captado exatamente como ↖;
   c) Se o fóton polarizado for ↑ , essa informação é perdida e o fóton é captado como ↗ ou ↖ , com probabilidade de ½ para a captação ↗ e ½ para ↖;
   d) Se o fóton polarizado for → , essa informação é perdida e o fóton é captado como ↗ ou ↖ , com probabilidade de ½ para a captação ↗ e ½ para ↖.

Deve-se ressaltar que a escolha de duas bases ortogonais, sendo tais que, D-C esteja rotacionada em exatos $\pi/4$ em relação a V-H, assegura a probabilidade de ½ para cada uma das captações obtidas com a base não adequada (itens 3.c, 3.d, 4.c e 4.d).

Em prosseguimento ao protocolo, emissor e receptor devem estabelecer uma convenção binária. A **TABELA 2** ilustra o fato:

TABELA 2 - CONVENÇÃO BINÁRIA

| BASE | 0 | 1 |
|---|---|---|
| V-H | ↑ | → |
| D-C | ↗ | ↖ |

Assim, pode-se imaginar uma situação hipotética que resultará nos seguintes passos do protocolo BB84:

**1a. parte**: Protocolo BB84 – Canal quântico

a) Emissor deseja encaminhar a mensagem:

**0 1 1 0 1 0 0 1**

b) Emissor escolhe aleatoriamente 8 bases para proceder a emissão dos fótons polarizados:

**V-H V-H D-C V-H D-C D-C D-C V-H**

c) A polarização gera 8 *q-bits*, que são encaminhados para o receptor:

↑ → ↖ ↑ ↖ ↗ ↗ →

d) Receptor, para captar os *q-bits*, escolhe aleatoriamente uma seqüência de bases:

**V-H D-C D-C D-C V-H D-C V-H V-H**

e) Um exemplo de leitura do receptor (captação dos fótons polarizados) pode ser a seguinte:

| 1º | 2º | 3º | 4º | 5º | 6º | 7º | 8º |
|---|---|---|---|---|---|---|---|
| ↑ | ↖ | ↖ | ↗ | → | ↗ | ↑ | → |

- É importante observar que os 1º, 3º, 6º, e 8º *q-bits* **obrigatoriamente** serão captados daquela forma, porque as bases do emissor e do receptor são iguais;
- O 2º q-bit poderia ter sido captado como ↖ ou ↗ (½ de probabilidade para cada um);
- O 4º q-bit poderia ter sido captado como ↖ ou ↗ (½ de probabilidade para cada um);
- O 5º q-bit poderia ter sido captado como ↑ ou → (½ de probabilidade para cada um);
- O 7º q-bit poderia ter sido captado como ↑ ou → (½ de probabilidade para cada um);

**2a. parte:** Protocolo BB84 – Canal clássico

a) Por um canal clássico, emissor e receptor informam a sequência de bases que utilizaram, de tal forma que a segunda linha apresenta as bases utilizadas pelo emissor e a terceira linha as do receptor.

| 1ª | 2ª | 3ª | 4ª | 5ª | 6ª | 7ª | 8ª |
|---|---|---|---|---|---|---|---|
| V-H | V-H | D-C | V-H | D-C | D-C | D-C | V-H |
| V-H | D-C | D-C | D-C | V-H | D-C | V-H | V-H |

b) Só serão considerados os *q-bits* oriundos das posições onde houve coincidência de base, ou seja, 1ª, 3ª, 6ª, e 8ª posições:

↑ ↖ ↗ →

c) Que pela convenção binária acarreta na seguinte seqüência de bits:

**0 1 0 1**

A obtenção da seqüência de bits (no exemplo acima: 0101) encerra o protocolo BB84.

Algumas considerações se fazem fundamentais para o devido esclarecimento dos limites de competência e de propósito da Distribuição Quântica de Chaves Secretas:

a) A Distribuição Quântica de Chaves Secretas não prescinde da existência de um canal clássico de comunicação, para a troca de informações sobre as bases utilizadas.

b) Na Distribuição Quântica de Chaves Secretas não há texto claro, original, a ser transmitido e, posteriormente, recebido e recuperado integralmente pela decifragem. Portanto, enquanto restrita ao canal quântico, não se oferece, nem se pretende oferecer, o serviço tradicional de privacidade ou confidencialidade, aqui bem entendido, como a "manutenção do segredo da informação para todos exceto para quem é autorizado a ter a informação" [9].

c) Recomenda-se a Distribuição Quântica de Chaves Secretas, portanto, para se promover uma distribuição de chave (0101, no exemplo dado), a ser utilizada em criptografia simétrica.

d) Como a probabilidade do receptor usar a base certa na recepção de um fóton é 1/2, é conveniente transmitir um número de fótons polarizados que seja, no mínimo, o dobro do tamanho da *string* que originará a chave que se queira.

e) Ainda que no canal público ocorra o vazamento das bases usadas por emissor e receptor, essa informação, por si só, de nada adiantará ao interceptador, uma vez que para cada par de bases coincidentes haverá duas possibilidades de fótons polarizados e, consequentemente, sempre duas possibilidades de bits, 0 ou 1.

f) A Distribuição Quântica de Chaves Secretas é concorrente, portanto, da criptografia assimétrica, quando esta se propõe a promover um acordo de chave a ser utilizada na cifragem convencional feita pela criptografia simétrica.

g) Princípios da mecânica quântica asseguram que sempre ocorre interferência quando há observação em um estado quântico. Significa dizer que o invasor de um canal quântico fica restrito a uma probabilidade matemática de utilizar todas as bases certas para a "captação perfeita". Em uma transmissão de 256 fótons polarizados, a probabilidade seria $1/2^{256}$. Diferentemente da criptografia assimétrica, na qual a criptoanálise pode incidir na função matemática que origina a chave, na Distribuição Quântica de Chaves Secretas a criptoanálise se reduz a uma probabilidade tão pequena quanto se queira.

h) Estados quânticos, conforme demonstrado em [10] e [11], não podem ser clonados, a partir de uma emissão original, o que inviabiliza a figura de uma cópia de segurança quântica.

A questão seguinte a ser analisada é a eventual interceptação da mensagem, em canal quântico, por parte de um invasor. Pelos princípios da mecânica quântica, o fato acarretará, com alta probabilidade, na alteração da mensagem encaminhada.

Como apenas os *q-bits* oriundos dos pares de bases coincidentes entre emissor e receptor é que vão interessar para a criação da chave, somente os *q-bits* relativos às posições de tais bases coincidentes é que serão relevantes para a análise.

Analisando-se os fótons polarizados obtidos a partir das posições de bases coincidentes entre emissor e receptor, e supondo que houve intromissão de um invasor no canal quântico, que esteja usando o mesmo protocolo de bases ortogonais da transmissão, a probabilidade da intromissão não ter alterado o q-bit captado pelo receptor é, para cada fóton em análise, de ¾, ou seja, 75%, já que:

a) Se o invasor usou a mesma base do fóton polarizado que o emissor usou, nada será alterado e a intromissão não será percebida (½ de probabilidade);

b) Se o invasor usou outra base diferente da usada pelo emissor (½ de probabilidade), ele alterará a recepção do fóton; ocorre que mesmo esse fóton alterado, ao ser captado pela base do receptor (que por hipótese é a mesma do emissor), tem ½ de chance de retorná-lo à posição do q-bit original e, com isso, a intromissão não ser detectada (½ de ½ = ¼).

c) Ao todo, ½ + ¼ = ¾ de probabilidade de permanecer o mesmo q-bit, apesar da intromissão.

Cumpre destacar que quanto maior for o número de *q-bits* postos em análise tão menor será a probabilidade de não ocorrer alteração pela intromissão do invasor.

A **TABELA 3** a seguir mostra a probabilidade de não ocorrer alteração na informação encaminhada:

TABELA 3 - PROBABILIDADE DE NÃO OCORRÊNCIA DE ALTERAÇÃO

| Bits | Probabilidade (unitária) | | Probabilidade (%) |
|---|---|---|---|
| 1 | $(3/4)^1$ | ¾ | 75% |
| 2 | $(3/4)^2$ | 9/16 | 56% |
| 3 | $(3/4)^3$ | 27/64 | 42% |
| 4 | $(3/4)^4$ | 81/256 | 32% |
| 8 | $(3/4)^8$ | $10^{-1}$ | 10% |
| 16 | $(3/4)^{16}$ | $10^{-2}$ | 1% |
| 32 | $(3/4)^{32}$ | $10^{-4}$ | 0,01% |
| 64 | $(3/4)^{64}$ | $10^{-8}$ | $10^{-6}$ % |
| 128 | $(3/4)^{128}$ | $10^{-16}$ | $10^{-14}$ % |
| 256 | $(3/4)^{256}$ | $10^{-32}$ | $10^{-30}$ % |

A Tabela 4 mostra uma hipotética transmissão quântica com intromissão de invasor.

Os fótons polarizados que são captados pelo invasor são, a seguir, encaminhados para o receptor.

TABELA 4 - TRANSMISSÃO QUÂNTICA COM INTERCEPTAÇÃO

| Posição | 1º. | 2º. | 3º | 4º | 5º | 6º | 7º | 8º |
|---|---|---|---|---|---|---|---|---|
| Bits | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
| Base do emissor | V-H | V-H | D-C | V-H | D-C | D-C | D-C | V-H |
| Fótons polarizados | ↑ | → | ↖ | ↑ | ↖ | ↗ | ↗ | → |
| Base do invasor | D-C | D-C | V-H | V-H | D-C | D-C | V-H | V-H |
| Fótons captados pelo invasor | ↖ | ↗ | → | ↑ | ↖ | ↗ | → | → |
| Base do receptor | V-H | D-C | D-C | D-C | V-H | D-C | V-H | V-H |
| Fótons captados pelo receptor | → | ↗ | ↖ | ↗ | ↑ | ↗ | ↑ | → |
| Bits após comparação de bases do emissor com o receptor | 1 | | 1 | | | 0 | | 1 |

Note que as bases do emissor e do receptor, informadas em canal clássico, só apresentam coincidência na 1ª, 3ª, 6ª e 8ª posições. Só essas posições serão analisadas.

Nas 6ª e 8ª posições, como a base do invasor é igual à do emissor, não há alteração na captação do receptor.

Nas 1ª e 3ª posições, como a base do invasor é diferente da do emissor, pode haver alteração na recepção, com probabilidade de haver de ½ por fóton polarizado.

Emissor e receptor só poderão descobrir a invasão através de checagem de dados em canal clássico.

Assim, para verificar se houve intromissão, após a verificação de que as 1ª, 3ª, 6ª e 8ª posições são as de bases coincidentes, emissor e receptor informam, também por canal clássico, quais são os seus bits nessas posições, que são comparados entre si:

Emissor: 0 1 0 1

Receptor: 1 1 0 1

A diferença entre os bits da 1ª posição assegura que houve erro (intromissão ou ruído no canal quântico).

Constatada a invasão, toda aquela transmissão é descartada e inicia-se outra.

É evidente que ao fazer a conferência dos próprios bits (0 e 1) pelo canal clássico, as partes expõem aquela *string* de bits. Portanto, a conferência pelo canal clássico será feita apenas com uma parte da *string* de bits obtida no canal quântico. Se os parâmetros de conferência resultarem em conclusão de não invasão ou não ruído significativo, somente aquela parte da *string* de bits é descartada e todo o restante da *string* (que não foi submetido ao canal clássico) é aproveitada para a criação da chave.

Assim, pôde-se observar que o protocolo de Distribuição Quântica de Chaves Secretas tem como propósito final a obtenção de duas *strings* de bits que deem origem a uma chave comum a ser usada em criptografia simétrica.

Os princípios da mecânica quântica asseguram que qualquer interferência de um invasor no canal quântico será muito provavelmente percebida pelas partes da comunicação.

Diferentemente da criptografia assimétrica que, ao cuidar da distribuição de chaves, tem um arcabouço matemático por trás que lhe dá sustentação, mas pode ser objeto de quebra em algum momento, a Distribuição Quântica de Chaves Secretas assegura a possibilidade de uma distribuição inquebrável de chaves, restritas ao conhecimento, apenas, das duas partes envolvidas.

Assim, obtida pelas partes a chave quântica, não restará ao criptoanalista outra alternativa que o método da força bruta a incidir no próprio texto cifrado por criptografia simétrica, o que significa, portanto, ter-se obtido segurança máxima no processo de fornecimento de chaves.

Deve ser mencionado, ainda, que o protocolo simétrico clássico, usado nos protocolos quânticos, é aquele que utiliza tamanhos de chave e mensagem idênticos, denominado *"one-time-pad"*.

## RECONCILIAÇÃO DE INFORMAÇÕES E AMPLIFICAÇÃO DE PRIVACIDADE

Qualquer que seja o canal quântico utilizado para a criação da chave, ele não será perfeito. Ruídos, necessariamente, farão as partes obterem resultados diferentes [12].

Suponha os seguintes fatos que propiciarão um protocolo de reconciliação, a saber, um procedimento que tem por propósito, através de uma sequência de passos, conseguir a identificação e correção de erros ocorridos durante a transmissão quântica.

a) A transmissão quântica já ocorreu;

b) A comparação de bases já foi feita em canal clássico;

c) Existe a *string* S(e) de bits do emissor e foi obtida uma *string* S(r) de bits pelo receptor.

A questão que se coloca é: como, a partir de S(e) e S(r), pode-se chegar a uma *string* final Sf(e) do emissor que tenha uma máxima probabilidade de ser igual à *string* final Sf(r) do receptor, corrigindo os eventuais ruídos de transmissão?

Um protocolo de reconciliação foi apresentado por G. Brassard e L. Salvail, em [13]. Conhecido como *Cascade Protocol*, trata-se de um procedimento verificado em canal clássico, que dá prosseguimento ao "Experimento de Distribuição Quântica de Chaves" [14].

A seguir está delineado um exemplo de procedimento, meramente teórico, que tem como propósito uma simples visualização lógica do que se pretende:

1.Por canal clássico, emissor e receptor trocam as seguintes informações:

a)*k* e *i*, tamanho e posição, respectivamente, de um bloco de bits das *strings S(e)* e *S(r)* que será analisado;

b) Os bits desse bloco.

Assim, supondo-se uma *string S* de 1000 bits, e um tamanho *k* = 100, analisado a partir da posição *i* = 145, são informados pelo canal clássico os 100 bits consecutivos a partir da posição 145, inclusive.

2.Emissor e receptor concluem, então, qual é o percentual *p* de erros daquele bloco analisado, fazendo:

a)*p* = número de bits que diferem / tamanho do bloco;

b) Suponha-se que sejam encontrados 10 erros. Nesse caso *p* = 10/100 =1/10;

3.O bloco analisado é inteiramente descartado, restando uma nova *string S'*. A nova *string S'* considerada é formada pelos 144 bits anteriores à posição 145 e por todos os bits posteriores à posição 245, inclusive. (245 = 145 + 100). Claro está que o emissor terá uma nova *string S'(e)* e o receptor terá também uma nova *string S'(r)*;

4.O propósito da obtenção de *p* é saber em quantos blocos a *string* S' será dividida de tal forma que, ***provavelmente***, permaneça um erro por bloco. Podem ser executadas recomendações que ampliem em um determinado percentual o tamanho do bloco Ko. Uma usual é:

- *Ko* = 1/p + 1/4p, o que nada mais é do que aumentar o tamanho do bloco em 25%.
- Para as novas *strings* S'(e) e S'(r), os blocos *Ko* seriam, portanto, do tamanho:
- *Ko* = 1 / (1/10) + 1 / (4/10) = 10 + 2,5 = 12,5.

5.O passo seguinte é o emissor dividir a sua *string S'(e)* em blocos de tamanho *Ko* (no nosso exemplo em tamanho de 12 ou 13 bits) e verificar a paridade dos bits para cada bloco. Isso significa fazer uma operação XOR (operação de soma, módulo 2) entre os bits de cada bloco e obter um bit de paridade.

6.Por canal público esses bits de paridade (e apenas esses) são passados do emissor para o receptor que faz a conferência, ordenadamente, com os blocos obtidos a partir da sua *string S'(r).*

7.A conferência é feita pelo receptor, que também divide a sua *string S'(r)* em blocos de tamanho Ko e, analogamente, realiza uma operação XOR em cada bloco, conferindo o resultado da operação no bloco com o bit de paridade recebido do emissor.

8.Por canal clássico, o receptor informa ao emissor quais bits de paridade foram os não coincidentes. Com essa informação, o emissor sabe quais blocos contêm erro e subdivide cada um desses blocos em duas metades de bloco, fazendo, para cada metade, nova operação XOR e obtendo, assim, novos bits de paridade, que são informados ao receptor, outra vez, por canal clássico.

9.O processo é repetido até restar em uma metade de bloco um único bit, que será o erro identificado e corrigido. Fica claro agora o porquê do tamanho Ko inicial do bloco ser obtido através do percentual de erros encontrado na amostra. É, apenas, para se assegurar que, provavelmente, haja um erro por bloco de tamanho Ko e, assim, possa ele ser isolado ao final do processo de subdivisões e, então, corrigido.

10. Como toda a troca de informações dos bits de paridade foi pública através do canal clássico, o protocolo recomenda que seja descartado o último bit de cada bloco analisado.

11. Ao fim do procedimento, emissor e receptor têm as suas respectivas *strings* formadas por blocos com idêntica paridade.

12. Ocorre que a idêntica paridade dos blocos não assegura que eles sejam exatamente iguais (0110 e 1001 são blocos diferentes, mas que oferecem um mesmo resultado de operação XOR quando os seus bits são operados: 0 xor 1 xor 1 xor 0 = 0; da mesma forma que 1 xor 0 xor 0 xor 1 = 0). Assim, a reconciliação pode prosseguir da seguinte maneira:

a)Escolhe-se um tamanho de bloco *K1* que seja o dobro do *Ko* inicial e se faz todo o mesmo processo anterior com *K1*;

b) Escolhe-se um tamanho de bloco *K2* que seja o dobro de *K1* e repete-se o processo;

c)Prossegue-se assim até se obter um bloco *Kn* que seja maior do que ¼ da *string S'* e repete-se o processo.

d) Duas rodadas adicionais com tamanhos aproximados de ¼ da *string* podem ser recomendadas para finalizar o procedimento.

Como o processo de reconciliação de informações é todo feito em canal clássico, que é público, muitas dessas informações sobre os bits de paridade podem ter sido capturadas por um invasor. Dessa forma, o invasor pode ter uma quantidade grande de informações sobre a transmissão.

Existem algoritmos conhecidos como funções de *Hash* [9]. Essas funções se caracterizam por gerar um pequeno resumo de tamanho fixo (*hash value*, *message digest*, *digital fingerprint*), a partir de mensagens de qualquer tamanho. Por

isso, são conhecidas como funções compressoras ou condensadoras. Tais funções devem atender, entre outros, a dois princípios básicos:

a) Resistência à pré-imagem, que significa que a partir do *hash value* não é exeqüível encontrar a mensagem original.

b) Não-colisão, que significa que não é exeqüível encontrar duas mensagens que originem o mesmo *hash value*.

A amplificação de privacidade exposta em [15] e [16] propõe que se aplique, quando necessário, uma função de *Hash* [17] que transforme a *string* final obtida após a reconciliação em uma nova *string*, que será o *hash value* daquela transformação, de tal forma que o *hash value* do emissor (hv(e)) seja o mesmo obtido pelo receptor (hv(r)).

Com isso, pretende-se amplificar a privacidade das partes envolvidas na comunicação e expurgar o conhecimento que um eventual invasor tenha obtido por ocasião do procedimento de reconciliação.

O esquema a seguir, extraído e adaptado de [18] e mostrado na **Figura 2**, apresenta um processo completo de comunicação em que se utiliza a Distribuição Quântica de Chaves Secretas como forma de distribuição de chaves.

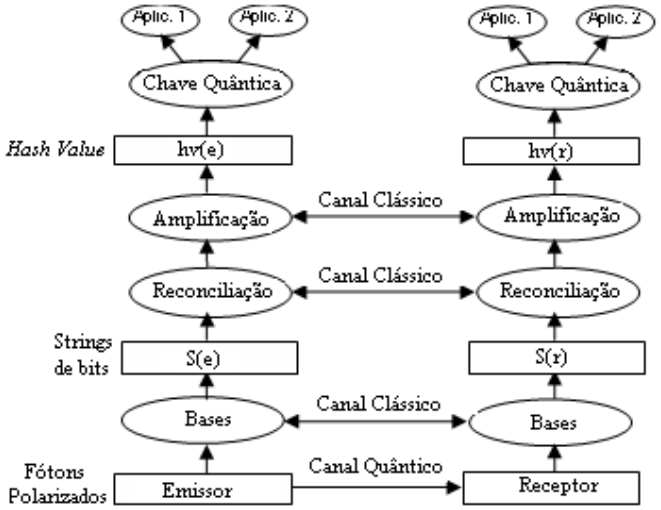


Figura 2 - Processo completo de Distribuição Quântica de Chaves Secretas.

Merece ainda alguns comentários o estado atual do presente assunto.

Se por um lado verifica-se que a computação quântica não apresentou, ainda, o seu produto comercial - um computador quântico -, estando em fase de estudos e pesquisas, o mesmo não acontece com a Distribuição Quântica de Chaves Secretas. Existem produtos comerciais que já se encontram disponíveis para venda a usuários [19].

Atualmente, o oferecimento a interessados é o de uma máquina que estabelece um processo de Distribuição Quântica de Chaves Secretas (*QKD – Quantum Key Distribution*), a ser usado conjuntamente com sistemas de cifragem simétricos.

Tais produtos se propõem a oferecer soluções em um raio de comunicação em fibra ótica de cerca de 100 km.

## CONCLUSÃO

Ainda que possa ser considerada incipiente, tão mais se comparada à idade da criptografia clássica, a utilização dos princípios quânticos assegura e permite a resolução de dois problemas cruciais na questão da comunicação secreta entre partes.

O primeiro deles diz respeito à invasão de partes não autorizadas ao acesso de uma transmissão.

Como saber se uma troca de chaves não está sendo interceptada e com isso descoberta? Qual ambiente pode assegurar que uma chave, informada oralmente, através de carta, telefone, telégrafo, e-mail, ondas de radiofrequência, ou seja lá qual for o meio, não pode ser objeto de uma interceptação não percebida pelas partes?

A criptografia assimétrica apresentou a sua solução para esse problema: a existência de duas chaves, de tal forma que quando uma delas cifra, só a outra pode decifrar. Tudo informado explicitamente, sem que se importe por quais ambientes. Nesse caso, o interceptador pode ter acesso à toda a informação que é pública e, mesmo assim, não conseguirá chegar à chave privada. Mas por quanto tempo isso permanecerá? A criação de um computador quântico poderá fazer com que a descoberta dessa chave privada se torne uma tarefa rápida e fácil, na medida em que torne exequíveis procedimentos, hoje, considerados inexequíveis.

Princípios de Mecânica Quântica asseguram que qualquer observação em um estado quântico obrigatoriamente interferirá nesse estado. Dessa forma, transmissões efetuadas em canais quânticos não podem ser passivamente observadas sem que ocorram interferências perceptíveis às partes legítimas da transmissão.

Assim, fica criado um canal de comunicação quântico que, se por um lado, não assegura a sua inviolabilidade, por outro, assegura a certeza quanto à eventual violação.

O segundo problema se refere à questão da distribuição de chaves criptográficas entre as partes envolvidas legitimamente na transmissão. O mesmo canal quântico, que informa a intromissão, é também capaz de propiciar elementos necessários para o estabelecimento de um protocolo de geração de chaves criptográficas.

Dessa forma, diante de todo o exposto no presente trabalho, pode-se responder às seguintes questões:

a) A computação quântica é imprescindível para a Distribuição Quântica de Chaves Secretas?

Não. Enquanto a primeira não apresentou, ainda, o seu exemplar comercial – um computador quântico – a segunda já existe em escala comercial.

b) A Distribuição Quântica de Chaves Secretas é um sistema autossuficiente para a cifragem e a decifragem de mensagens?

Não. E nem pretende ser. A Distribuição Quântica de Chaves Secretas para acontecer exige um meio quântico de comunicação *pari passu* com outro canal de comunicação qualquer.

Apesar da maior parte das pesquisas ocorrer na distribuição das chaves, há estudos em criptografia quântica sobre cifragem de mensagens e autenticação quântica.

c) Qual é o propósito da Distribuição Quântica de Chaves Secretas?

Estabelecer uma distribuição de chaves confiável entre as partes legítimas de uma comunicação. A Distribuição Quântica de Chaves Secretas se propõe a oferecer os bits de uma chave a ser usada em uma criptografia simétrica convencional.

d) O que significa a afirmação de que a Distribuição Quântica de Chaves Secretas é 100% segura?

Significa, basicamente, duas possibilidades: a primeira, de que existe um meio de comunicação seguro contra a invasão e a espionagem, que é o canal quântico; a segunda é que, com a utilização desse meio, é possível produzir chaves criptográficas seguras. O ponto seguinte é a quantificação dessa segurança. A questão quântica é, em essência, uma questão de probabilidade. Assim, a expressão "100% de segurança" significa que se tenha uma probabilidade de segurança tão alta quanto se queira.

Complementando, apenas como facilitação de raciocínio hipotético, uma chave criptográfica, com o tamanho de um bit (0 ou 1) tem um grau de segurança, em termos de ataque por força-bruta, de ½.: 50% seguro, querendo isto dizer que a probabilidade de se descobrir o segredo é de ½. Em, no máximo, duas tentativas o segredo seria revelado. Como para cada tentativa haveria um tempo de execução, em, no máximo, duas unidades de tempo iguais àquela o segredo seria descoberto.

Daí a necessidade de chaves maiores. Conhecido o tempo de processamento e execução de cada tentativa do ataque por força-bruta, pode-se estabelecer um tamanho de chave que poderá ser considerada 100% segura.

Assim, como de hábito acontece com a evolução científica, a questão do conhecimento é, necessariamente, adstrita a uma época, à qual referencia os seus resultados em função das certezas de que se dispõem naquele momento.

Procurou-se, portanto, neste trabalho abordar alguns aspectos da Distribuição Quântica de Chaves Secretas de uma forma objetiva e clara em seus limites e possibilidades. Com isso, espera-se fazer motivar o espírito científico que investiga, pesquisa e transforma.

## REFERÊNCIAS


[1] W. Stallings, "Criptografia e segurança de redes – Princípios e práticas", Pearson Brasil, 4ª edição, pp 21, 2008.

[2] Auguste Kerckhoffs, "La cryptographie militaire," Journal des sciences militaires, vol. IX, pp. 5–83, Jan. 1883, pp. 161–191, Feb. 1883.

[3] Rivest, R; Shamir, A; e Adleman, L. "A method for obtaining digital signatures and public key cryptosystems". Communications of ACM, fevereiro de 1978.

[4] R. Portugal, "Computação quântica - III Ciclo de Estudos Desafios da Física para o Século XXI: o admirável e o desafiador mundo das nanotecnologias". Disponível em http://www.ihuonline.unisinos.br/index.php?option=com_content&view=article&id=1309&secao=235., Acesso em Março de 2011.

[5] R. Portugal, Uma Introdução à Computação Quântica - São Carlos, SP: SBMAC, 2004.

[6] G. Rigolin, A. A. Rieznik, "Introdução à criptografia quântica". In Revista Brasileira de Ensino de Física, vol. 27, n. 4, p. 517 - 526, 2005.

[7] N. Gisin et al, "Quantum Cryptography", Rev. Mod. Phys, 74, 145, (2002).

[8] C. H. Bennett, G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossin". In International Conference on Computers, Systems & Signal Processing. December, 1984.

[9] A. J. Menezes, P. C. V. Oorschot, S. A. V. "Handbook of Applied Cryptography", CRC Press, Boca Raton, 1996.

[10] W.K. Wootters and W.H. Zurek, A Single Quantum Cannot be Cloned, Nature 299, pp. 802–803, 1982.

[11] D. Dieks, Communication by EPR devices, Physics Letters A, vol. 92(6), pp. 271–272, 1982.

[12] G. V. Assche, J. Cardinal, J. Nicolas, "Reconciliation of a Quantum-Distributed Guassian Key", In proceedings of IEEE Transactions on Information Theory, vol. 50, no. 2, p. 394, 2004.

[13] G. Brassard, L. Salvail. "Secret-key reconciliation by public discussion".In Advances in Cryptology — Eurocrypt 93, Ed. Berlin, Germany: Springer-Verlag, pp 411-423, 1993.

[14] C. H. Bennet, F, Bessete, G. Brassard, L. salvail, J. Smolin, "Experimental Quantum Cryptography". In Journal of Cryptology, Vol. 5, no 3, 1992.

[15] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, Generalized privacy amplification,IEEE Transactions on Information Theory, vol. 41, pp. 1915–1923, November, 1995.

[16] C. H. Bennett, G. Brassard; J. M. Robert. "Privacy amplification by public discussion", SIAM J. Comput., vol. 17, no. 2, pp 210-229, 1988.

[17] J. L. Carter, M. N. Wegman. "Universal classes of hash functions", Journal of Compuier and System Sciences, Vol. 18, 1979, pp. 143-154.

[18] A. Mink, S. Frankel and R. Perlner. "Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration". In International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2, 2009.

[19] Idquantique. "A fast and secure solution: high speed encryption combined with quantum key distribution". Disponível em www.idquantique.com, acesso em março de 2011.



**Alvaro Jorge Braga Mendes** possui graduação em Matemática pela Faculdade de Filosofia, Ciências e Letras Anderson e especialização em Matemática pela Universidade Federal Fluminense - UFF. Atualmente é Tecnologista no Centro de Análise de Sistemas Navais, onde atua na Divisão de Criptologia. Tem experiência na área de Matemática Aplicada, atuando principalmente nos seguintes temas: Criptografia e Matemática Financeira.

**Edésio Hernane Paulicena** possui graduação em Ciência da Computação pela Universidade Federal de Goiás e mestrado em Engenharia Eletrônica e Computação pelo Instituto Tecnológico de Aeronáutica. É doutorando na área de Telecomunicações pelo ITA. Atualmente é Tecnologista no Centro de Análise de Sistemas Navais, onde atua na Divisão de Criptologia. Tem experiência na área de Engenharia Elétrica, com ênfase em Redes de Computadores, Criptografia e Segurança da Informação.

**William Augusto Rodrigues de Souza** possui mestrado em Sistemas e Computação pelo Instituto Militar de Engenharia (2007) e doutorando em Engenharia de Sistemas e Computação pela COPPE-UFRJ. Atualmente é Chefe da Divisão de Criptologia do Centro de Análises de Sistemas Navais. Tem experiência na área de Ciência da Computação e Matemática Aplicada.