Protocolo Híbrido para Autenticação Quântica de Mensagens Clássicas com uso do Gerador de Seqüências Pseudo-aleatórias Blum-Blum-Shub

Manoel Socorro Santos Azevedo

Dissertação de Mestrado submetida à Coordenadoria do Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande - Campus de Campina Grande como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências no Domínio da Engenharia Elétrica.

Área de Concentração: Comunicações

Francisco Marcos de Assis, Dr.
Orientador
Raimundo Carlos S. Freire, Dr.
Orientador

Campina Grande, Paraíba, Brasil

Protocolo Híbrido para Autenticação Quântica de Mensagens Clássicas com uso do Gerador de Seqüências Pseudo-aleatórias Blum-Blum-Shub

Manoel Socorro Santos Azevedo

Dissertação de Mestrado apresentada em Maio de 2006

Francisco Marcos de Assis, Dr.
Orientador
Raimundo Carlos S. Freire, Dr.
Orientador

Campina Grande, Paraíba, Brasil, Maio de 2006

A994p Azevedo, Manoel Socorro Santos
Protocolo hibrido para autenticacao quantica de mensagens classicas com uso do gerador de sequencias pseudo-aleatorias blum-blum-shub / Manoel Socorro Santos Azevedo. - Campina Grande, 2006.
45 f.

Dissertacao (Mestrado em Engenharia Eletrica) - Universidade Federal de Campina Grande, Centro de Engenharia Eletrica e Informatica.

1. Gerador de Sequencias Blum-Blum-Shub 2. Autenticacao Quantica I. Assis, Francisco Marcos de, Dr. II. Freire, Raimundo Carlos S., Dr. III. Universidade Federal de Campina Grande - Campina Grande (PB)

CDU 621.313.52(043)

PROTOCOLO HÍBRIDO PARA AUTENTICAÇÃO QUÂNTICA DE MENSAGENS CLÁSSICAS COM USO DO GERADOR DE SEQÜÊNCIAS PSEUDO-ALEATÓRIAS BLUM-BLUM-SHUB

MANOEL SOCORRO SANTOS AZEVEDO

Dissertação Aprovada em 04.05.2006

FRANCISCO MARCOS DE ASSIS, Dr., UFCG
Orientador

RAIMUNDO CARLOS SILVÉRIO FREIRE, Dr., UFCG
Orientador

AÉRCIO FERREIRA LIMA, Dr., UFCG
Componente da Banca

EDMAR CANDEIA GURJÃO, D.Sc., UFCG
Componente da Banca

CAMPINA GRANDE - PB
MAIO - 2006

Dedicatória

Este trabalho é dedicado a minha família, em especial aos meus pais, João e Iracy Azevedo, aos meus filhos Alysson e Andreza e a minha esposa Franciana, que sempre me apoiaram de forma incondicional.

Agradecimentos

Talvez, tão difícil quanto fazer esta dissertação é encontrar as palavras certas para agradecer a todos que tornaram mais simples e/ou mais produtiva a realização desta dissertação. Espero que nesses agradecimentos eu possa retribuir, ao menos, um pouco da atenção que me foi dada.

Aos meus orientadores Francisco Marcos de Assis e Raimundo Carlos Freire, pelas valiosas contribuições, apoio, paciência, sugestões, amizade e orientação segura.

Aos meus pais, João e Iracy, pelo amor e carinho. Eles souberam me incentivar bastante neste trabalho, mesmo estando à distância. Com certeza, aqui faltam palavras para expressar o meu agradecimento.

Aos meus amigos Bruno da Costa Bitencurt, Deusdete Brito, Francisco Ferreira, Will Ribamar, Rex Antônio da Costa Medeiros, e demais colegas do Laboratório de Instrumentação, Medição e Controle (LIMC) pela ajuda e discussões técnicas que elevaram o nível deste trabalho.

Ao Colega e também amigo Andrei Sidorenko, pela contribuição e respostas de emails, proporcionando a troca de experiências e valorizando este trabalho.

A Universidade do Estado do Amazonas (UEA) que proporcionou este mestrado.

A todos, a minha gratidão e muito obrigado.

Resumo

Na atualidade, quando a busca por segurança computacional e incondicional é uma realidade, tem-se feitos estudos e pesquisas para solucionar problemas relacionados à troca e autenticação de mensagens de maneira segura.

Sistemas criptográficos são estudados, avaliados e testados quanto à real segurança, permitindo a criptoanalistas usarem todo seu potencial para testes de segurança de tais sistemas. A criptografia quântica surge como um poderoso aliado para prover segurança incondicional.

A autenticação quântica de mensagens clássicas é uma realidade que pode ser colocada em prática em um tempo relativamente curto.

Propõe-se um protocolo hibrído de autenticação quântica de mensagens clássicas, usando o gerador de sequências pseudo-aleatórias BBS (Blum-Blum-Shub). A segurança do protocolo contra ataques individuais é avaliada formalmente.

Abstract

In the present time, when the search for computational and unconditional security is a reality, studies have been done to solve problems related to messages changes and authentication, in a safe way.

Cryptographic systems are studied, valued and tested for real safety, allowing the cryptoanalysts of such systems. The quantum cryptography appears as a powerful allied to provide unconditional security.

The quantum authentication of classic messages is a reality that can be put in practice in a relatively short time.

A hybrid protocol authentication of classic messages is considered, using the BBS(Blum-Blum-Shub), pseudo-random sequence generator. The protocol´s security against individual attacks is formally evaluated.

Lista de Símbolos e Abreviaturas

$\|\psi\rangle$	:	Estado quântico ou vetor de estado com rótulo ψ.
$\langle\psi\|$	:	Vetor dual ou conjugado Hermitiano de $\|\psi\rangle$.
$\langle\upsilon \mid \omega\rangle$	:	Produto interno entre os vetores $\|\upsilon\rangle$ e $\|\omega\rangle$.
$\|\upsilon\rangle\langle\omega\|$	:	Produto externo entre os vetores $\|\upsilon\rangle$ e $\|\omega\rangle$.
$\|\|\|\psi\rangle\|\|$	:	Norma do vetor $\|\psi\rangle$.
ρ	:	Operador de densidade.
δ_{ij}	:	Função delta. Assume o valor 1 se e somente se $i = j$. Caso contrário, $\delta_{ij} = 0$.
$A^\dagger$	:	Conjugado Hermitiano da matriz A.
U	:	Matriz unitária ou operador unitário.
I	:	Matriz identidade.
X, Y, Z	:	Matrizes de Pauli.
M_m	:	Operador de medição correspondente a saída m.
P_m	:	Projetor s/ o subespaço gerado p/ autovetores c/ autovalor m correspondente.
$p(m)$	:	Probabilidade de se obter a saída m em uma medição.
$\|\psi\rangle^{\otimes n}$	:	n produtos tensoriais do estado $\|\psi\rangle$.
$POVM$	:	*Positive Operator-Valued Measure*.
$\|M\|$	:	Cardinalidade do conjunto M.
$Gf(p)$	:	Campo de Galois formado pelos inteiros $\{0, 1, ..., p-1\}$
RQ_p	:	Conjunto dos resíduos quadráticos *módulo p*.
x_o, y_o	:	Sementes para um gerador de sequencias pseudo-aleatórias.
$x_o(n)$	:	n-ésima subsequência gerada a partir da semente x_o.
$h \in H$	:	função h pertencente a um conjunto H de funções *hash*.
$(0, N/2)$		Conj. de Inteiros $\{1, 2, ..., \lfloor N/2 \rfloor\}$
$Z_n^*(+1)$		Conj. dos Inteiros c/ Símbolo de Jacobi $+1$
$L[N]$		Complexidade da fatoração de N

Índice

Lista de Figuras

Capítulo 1

Introdução

A criptografia é considerada a principal tecnologia dos sistemas de segurança eletrônica. As técnicas modernas de criptografia têm muitas aplicações úteis, como assinatura digital de documentos, controle de acesso, implementação de dinheiro eletrônico e proteção de direitos autorais.(SIMON, 2001; DAVID, 1997; ALBRECHT, 1994).

Na computação, as principais técnicas conhecidas envolvem o conceito das chamadas "chaves criptográficas". Trata-se de um conjunto de bits baseado em um determinado algoritmo capaz de codificar e de decodificar informações. Se o receptor da mensagem usar uma chave incompatível com a chave do emissor, não conseguirá extrair a informação.

Um dos grandes problemas da comunicação é o ruído. Torna-se ruído da comunicação tudo aquilo que possa atrapalhar o entendimento da informação a ser transmitida, bem como, tudo que interfere na comunicação, prejudicando-a. Pode ser um som sem harmonia, um emissor ou receptor fora de sintonia, falta de empatia ou habilidade para colocar-se no lugar de terceiros, falta de atenção do receptor etc.

Os recursos usados para anular ruídos são:

- redundância: é todo o elemento da mensagem que não traz nenhuma informação nova. É um recurso utilizado para chamar à atenção e eliminar possíveis ruídos. Nesse sentido, deve-se repetir frases e informações julgadas essenciais à compreensão do receptor;

- *realimentação*: conjunto de sinais perceptíveis que permitem conhecer o resultado da mensagem; é o processo de se dizer a uma pessoa como uma pessoa se sente em função do que ela fez ou disse. Para isso, fazer perguntas e obter as respostas, a fim de verificar se a mensagem foi recebida ou não (SIMON, 2001; DAVID, 1997; ALBRECHT, 1994).

Muitas vezes, deseja-se transmitir uma informação de forma segura, ou seja, de forma que ela só possa ser decodificada por determinado receptor (ou receptores) autorizado

para isso. Isto é feito para evitar que receptores não autorizados possam interceptar a comunicação, decodificá-la e usá-la para fins indevidos, bem como atuar como transmissores de mensagens falsas recebidas por receptores verdadeiros, gerando interpretações equivocadas.

O termo Criptografia surgiu da fusão das palavras gregas "*Kryptós*" e "*gráphein*", que significam "oculto" e "escrever", respectivamente. Trata-se de um conjunto de conceitos e técnicas que visa codificar uma informação de forma que somente o emissor e o receptor possam acessá-la, evitando que um intruso consiga interpretá-la. Para isso, uma série de técnicas são usadas e muitas outras surgem com o passar do tempo(BALPARDA, 2001).

Na computação, as técnicas mais conhecidas envolvem o conceito de chaves, as chamadas "chaves criptográficas". Trata-se de um conjunto de bits baseado em um determinado algoritmo capaz de codificar e de decodificar informações. Se o receptor da mensagem usar uma chave incompatível com a chave do emissor, não conseguirá extrair a informação. Essas técnicas permitem transformar um texto claro para outra forma usando-se um procedimento só conhecido pelo transmissor e pelo receptor, mas para que haja total segurança, é necessário o mecanismo de chaves.

Com o uso de chaves, um emissor pode usar o mesmo algoritmo (o mesmo método) para vários receptores. Basta que cada um receba uma chave diferente. Além disso, caso um receptor perca ou exponha determinada chave, é possível trocá-la, mantendo-se o mesmo algoritmo.

Baseada em chaves, uma informação pode ser codificada por algum algoritmo de criptografia, de modo que, tendo conhecimento do algoritmo utilizado e da chave utilizada, é possível recuperar a informação original fazendo o percurso contrário da encriptação, a decriptação.

Os métodos que existem atualmente para se criptografar mensagens podem ser classificados em clássicos e quânticos. Este último ainda é objeto de estudo e não está sendo empregado na prática comercialmente.

Enquanto na criptografia clássica utilizam-se técnicas convencionais nos processos de ocultação da informação, através de procedimentos matemáticos, a criptografia quântica, que é baseada na teoria da mecânica quântica, a informação é protegida pelas leis da física.

Na criptografia clássica não se pode garantir uma segurança absoluta da informação, porque, sendo a informação interceptada, o receptor invasor pode sempre encontrar uma forma de decodificar a mensagem recebida e pode inclusive atuar como transmissor de mensagens falsas.

Nos algoritmos modernos, o segredo de uma mensagem encontra-se na chave, que é um parâmetro utilizado na cifragem e decifragem de uma mensagem. Quanto maior for

o tamanho da chave, espera-se que seja mais difícil quebrá-la.

Para melhor entendimento e seguindo a bibliografia especializada, chamaremos de Alice quem deseja enviar uma mensagem privada e Bob quem vai recebê-la. Denomina-se Eva, um intruso tentando ler esta mensagem secreta.

Na terminologia da Criptografia a mensagem original é chamada "texto claro", ou simplesmente "mensagem". O processo de embaralhar a mensagem de forma a ocultar seu conteúdo de outrem é denominado "cifragem", se constituindo-se de transformações matemáticas adequadas sobre a mensagem. A mensagem embaralhada, ou seja, cifrada, é denominada "texto cifrado" ou "criptograma". Deve-se fazer o processo inverso de recuperar a mensagem a partir do criptograma, e este processo é denominado "decifragem". Os processos de cifragem e decifragem se utilizam de um algoritmo (o processo de codificação/embaralhamento) e de um parâmetro de controle denominado "chave criptográfica", de forma que a decifragem, em princípio, somente é possível conhecendo-se a chave apropriada para decifrar, mesmo que se conheça o algoritmo utilizado.

Enquanto a Criptografia trata de manter mensagens secretas, por outro lado existe também a "Criptoanálise", que é a ação de "quebrar" os criptogramas, recuperando-se as mensagens, mesmo sem se conhecer a chave apropriada para a decifragem. Por isso, os algoritmos criptográficos devem satisfazer a uma série de critérios de forma a garantir, no maior grau possível, que seja impraticável quebrar o sistema.

A Criptografia trata não apenas dos problemas estritos de sigilo de mensagens, como também de problemas de autenticação, assinatura digital (eletrônica), dinheiro eletrônico, e outras aplicações.

Nos algoritmos simétricos, também conhecidos como algoritmos de chave privada, a mesma chave é utilizada tanto na cifragem como na decifragem. Desta forma, Alice e Bob precisam combinar uma chave previamente. Nas transações comerciais e bancárias realizadas através da internet, a utilização de apenas uma chave é impraticável, sendo necessário um algoritmo assimétrico ou de chave pública. Em um algoritmo assimétrico, a chave utilizada na cifragem é diferente daquela utilizada na decifragem. Desta forma, não há a necessidade de Alice e Bob combinarem uma chave previamente, eliminando o problema da distribuição de chaves. A segurança desse algoritmo é baseada em problemas computacionalmente difíceis, como a fatoração de um número razoavelmente grande em seus fatores primos, onde destacamos o algoritmo RSA, que é um dos mais utilizados na atualidade (BALPARDA, 2001; SALOMAA, 1996; STINSON, 1995; BURNETT; PAINE, 2002).

Na criptografia quântica existem mecanismos para que dois transmissores/receptores possam trocar uma chave de codificação, em um canal privado, com segurança completa de comunicação.

Baseando-se nos princípios da Mecânica Quântica, a grande vantagem deste método,

em relação aos outros, reside em sua segurança incondicional, ou seja, não apresenta falhas como os métodos criptográficos atuais e não pode ser quebrado, mesmo com recursos computacionais infinitos. Além do mais, é possível estabelecer protocolos de troca de chaves secretas sem comunicação secreta prévia, como acontece nos algoritmos simétricos.

A Criptografia Quântica se destaca em relação aos outros métodos criptográficos, pois não necessita segredo prévio, permite detectar um intruso pelo simples fato de ele tentar ler os fótons na distribuição de chaves e é incondicionalmente segura, mesmo que o intruso tenha poder computacional infinito. Apresenta um elevado custo de implementação, entretanto, com a evolução tecnológica, poderá ser usada em larga escala num futuro próximo, tanto para fins militares como comerciais (OLIVEIRA, 2004; H.; H, 1999; BENNETT et al., 1992; C.; G.; EKERT, 1992).

O primeiro protocolo de Criptografia Quântica foi proposto em 1984 por Bennett e Brassard (BB84)(BENNETT et al., 1992). Ele é utilizado para estabelecer uma chave entre Alice e Bob para ser usada em um protocolo de Criptografia Clássica, permitindo detectar se Eva está espionando a comunicação. Há dois canais utilizados: o quântico, onde serão transmitidos os fótons, e o público, onde será feito todo o resto da comunicação. E Eva pode estar monitorando os dois. Recentemente o protocolo proposto por Medeiros e Assis, em 2004, que aqui será denominado MA4 (MEDEIROS, 2004), o qual faz uso do gerador Blum-Micali (BM) destinado a distribuição de chaves para autenticação de mensagens clássicas. O tema, alvo escolhido para esta dissertação, é um protocolo híbrido para autenticação quântica de mensagens clássicas, usando o gerador de seqüências pseudo-aleatórias Blum-Blum-Shub(BBS), cujo resultado matemático é extraído do resíduo quadrático. Trata-se de um protocolo que apresenta segurança incondicional, mesmo quando Eva possui recursos computacionais quânticos e clássicos infinitos. Este protocolo é baseado no caráter unidirecional das funções *hash* fortemente universal-2 (CARTER; WEGMAN, 1979).

Este trabalho de dissertação aborda uma aplicação prática da criptografia quântica, que é a demonstração de que o protocolo para autenticação quântica de mensagens clássicas MA4, também pode ser usado com gerador de seqüências pseudo-aleatórias BBS. A principal contribuição é a prova de que nas mesmas condições do protocolo MA4, a segurança do protocolo proposto é mantida.

1.1 Organização do Trabalho

Este texto de dissertação de mestrado está dividido em 5 capítulos, sendo este o primeiro e os outros apresentados a seguir.

Capítulo 2: Algoritmos de autenticação clássica e quântica de mensagens.

Neste capítulo mostram-se as diferenças e técnicas significativas de utilização de sistemas de autenticação de mensagens e principalmente seus fundamentos matemáticos.

Capítulo 3: Algoritmo de autenticação híbrido (MA4)

Neste capítulo descrevem-se o algoritmo de autenticação híbrido e o uso do gerador de sequências pseudo-aleatório Blum-Micali.

Capítulo 4: Uso do BBS no protocolo de autenticação quântica de mensagens clássicas e uma prova de sua segurança. Neste capítulo apresenta-se uma alternativa ao protocolo MA4, seguindo-se de uma discussão sobre vulnerabilidades no protocolo, mecanismos de correções de erros e amplificação de privacidade.

Capítulo 5: Conclusões e Perspectivas.

Finalmente, neste capítulo apresentam-se as conclusões do trabalho desenvolvido, as linhas de pesquisas atuais e perspectivas em criptografia quântica.

Capítulo 2

Autenticação Clássica e Quântica de Mensagens Clássicas

2.1 Introdução

Um sistema de autenticação é um conjunto de procedimentos que permite o envio de mensagens através de um canal de comunicação não confiável, de tal forma que o destinatário Bob possa identificar a identidade da remetente Alice, garantindo ainda que a mensagem não foi modificada por uma terceira parte Eva.

Os códigos de autenticação de mensagens(MAC) são métodos para assegurar a Bob que a mensagem foi enviada por Alice ou alguém autorizado por ela, através de uma chave secreta compartilhada entre ambos, e constatar-se de que a mensagem não foi alterada.

Neste capítulo, é dada uma visão geral sobre autenticaçã o e sobre os protocolos presentes na bibliografia especializada, com ênfase para os protocolos de autenticação quântica de mensagens clássicas. Para melhor compreensão dos tópicos mencionados, será dada uma breve noção dos algoritmos de chave privada e de chave pública.

2.2 Algoritmos Criptográficos de chave pública e chave secreta

Existem duas classes de algoritmos criptográficos clássicos: simétricos (ou de chave secreta) e assimétricos (ou de chave pública). Os algoritmos simétricos utilizam uma mesma chave tanto para cifrar como para decifrar (ou pelo menos a chave de decifragem pode ser obtida trivialmente a partir da chave de cifragem), ou seja, a mesma chave utilizada para "fechar o cadeado" é utilizada para "abrir o cadeado". Nos algoritmos assimétricos temos chaves distintas, uma para cifrar e outra para decifrar e, além disso, a

chave de decifragem não pode ser obtida apenas pelo conhecimento da chave de cifragem. Aqui, uma chave é utilizada para "fechar" e outra chave, diferente, mas relacionada à primeira, deve ser utilizada para "abrir". Por isso, nos algoritmos assimétricos, as chaves são sempre geradas aos pares: uma para cifrar e a sua correspondente para decifrar.

Pela sua característica no uso da chave, os algoritmos simétricos exigem que a chave seja mantida secreta, do conhecimento exclusivo dos dois interlocutores. Este fato traz complexidade ao manuseio destas chaves, o que dificulta um pouco a utilização destes algoritmos isoladamente. É requerido um canal seguro que permita a um usuário transmitir a chave ao seu interlocutor (um canal seguro pode ser, por exemplo, uma pessoa de confiança). A figura 2.1 ilustra a forma de operação de uma algoritmo criptográfico simétrico, onde Alice envia uma mensagem cifrada para Bob, tendo antes que enviar a chave que vai utilizar, secretamente, para Bob.

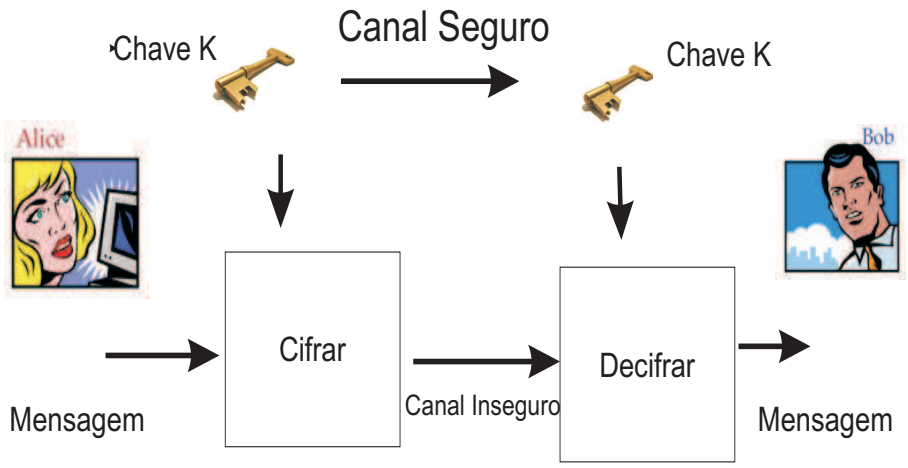

Figura 2.1: Uso de algoritmo criptográfico simétrico (chave secreta)

Os algoritmos assimétricos permitem que a chave de cifragem possa ser tornada pública, por exemplo, disponibilizando-a em um repositório de acesso público ("canal público"), e por isso denominada chave pública, retirando aquele problema existente nos algoritmos simétricos. Qualquer um pode cifrar mensagens com uma dada chave pública, contudo somente o destinatário, detentor da correspondente chave de decifragem (denominada chave privada, ou secreta), poderá decifrá-la. A chave privada não precisa e nem deve ser dada a conhecer a ninguém, devendo ser guardada em segredo apenas pelo seu detentor, que deve também ter sido o responsável pela geração do seu par de chaves, enquanto a chave-pública pode ser publicada livremente. Na figura 2.2 tem-se uma ilustração da operação de um algoritmo assimétrico. Aqui, Alice gera seu par de chaves, e envia (publica) sua chave pública para Bob. Este cifra a mensagem com a chave-pública de Alice KP(chave pública), a qual, e somente ela, será capaz de decifrá-la, utilizando sua chave-privada KS(chave secreta).

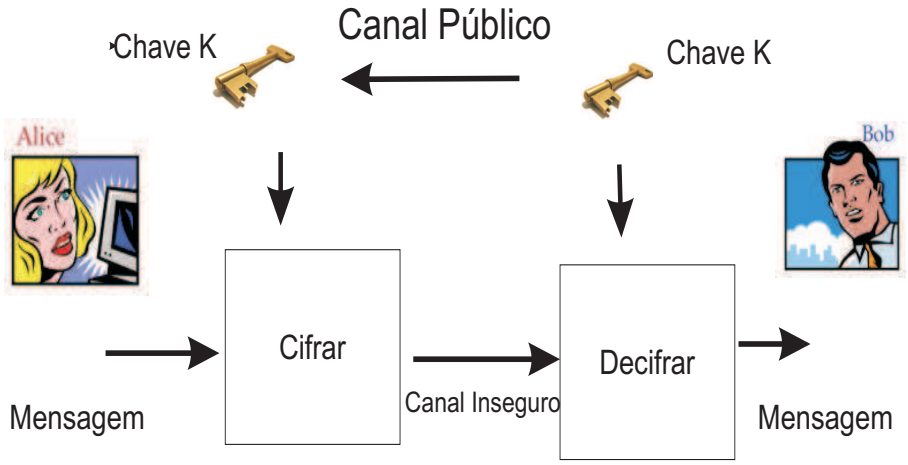

Figura 2.2: Uso de algoritmo criptográfico assimétrico (chave pública)

Geralmente os algoritmos simétricos são mais eficientes computacionalmente que os assimétricos, podendo ser bastante rápidos em sua execução, permitindo altas taxas de cifragem (até da ordem de gigabits/s – 10^9 bits/s). Os algoritmos assimétricos são geralmente menos eficientes, e normalmente a tendência é a utilização dos dois tipos de algoritmos em conjunto, tal que um algoritmo de chave pública é utilizado para cifrar uma chave criptográfica, gerada aleatoriamente, para ser então utilizada para cifrar a mensagem através de um algoritmo simétrico. O destinatário primeiro decifra a chave simétrica utilizando sua chave privada no sistema de chave pública, e após decifra a mensagem utilizando a chave recuperada no sistema simétrico. Desta forma não há o problema de "compartilhar o segredo da chave" com outras pessoas. A cada nova mensagem pode-se sempre repetir todo o processo. Nesta situação, se Alice deseja enviar uma mensagem para Bob, ele primeiro escolhe uma chave K, e a envia através do algoritmo de chave pública cifrada com a KP de Bob. Este recupera K decifrando o criptograma recebido com sua chave privada KS. Agora Alice pode enviar a mensagem real através do algoritmo simétrico mais eficiente, para isto cifrando-a com a chave K, que Bob já dispõe, e enviada a ela de forma segura.

2.3 Autenticação

Autenticação é um procedimento para reconhecer uma mensagem quanto a veracidade de seu conteúdo original. A criptografia clássica possui várias técnicas para implementar autenticação. Nesse contexto pode haver confusão entre os Códigos de Autenticação de Mensagens (MACs) e assinaturas digitais com a técnica de verificação de alguns protocolos (*checksums*). De fato, ambas as técnicas garantem a detecção de modificações da informação transmitida entre remetente e receptor. A diferença entre as duas técnicas

se apresenta quanto aos perigos possíveis que existem para modificar as mensagens. Um "*checksum*" típico é um mecanismo que tem como função encontrar erros que são resultados de ruídos ou outras fontes não intencionais. Por outro lado, uma assinatura digital ou MAC é um " *checksum*" criptográfico que é designado para detectar ataques iniciados por fontes intencionais ou acidentais. Há quatro tipos de MACs: incondicionalmente seguros, baseados em funções hash, baseados em fluxo de cifras e baseados em bloco de cifras (LABORATORIES, 2000).

2.4 Autenticação clássica

Quando Bob recebe uma mensagem de correio eletrônico, como ele pode saber se é da pessoa que pretendeu enviá-la? Bob não sabe. É claro, a mensagem tem um cabeçalho, mas o cabeçalho pode ter sido falsificado. Isso é fácil para um intruso não tão habilidoso que deseja que sua mensagem venha de alguém que ele gosta e de qualquer lugar que ele gosta e faça isso tão bem que Bob seja enganado. Nunca é sábio acreditar completamente na linha de " *From*" de qualquer mensagem de e-mail.

Programas de segurança de e-mail podem garantir, ou autenticar, que uma certa mensagem é de fato de alguma pessoa de quem o nome aparece na linha de "*From*". Isto é algumas vezes conhecido como "autenticação de dados da origem" e é feito com alguma coisa chamada de assinatura digital. Antes de verificar ao equivalente digital, vamos olhar para as assinaturas manuscritas.

2.5 Princípios da criptografia quântica

A descoberta, bem como a formalização da mecânica quântica a partir do ano 2000, impulsionaram estudos no campo da ciência da computação e da teoria da informação. Efeitos como o emaranhamento e a descoberta dos pares EPR possibilitaram o teletransporte de estados quânticos. Para melhor entendimento, conceitua-se qubit da seguinte forma: O bit quântico ou qubit é representado por um sistema quântico de dois estados que é constituído por apenas uma partícula. Um sistema quântico de dois estados é descrito por um vetor unitário complexo no espaço de Hilbert de dimensão dois. O espaço de Hilbert é um espaço vetorial complexo. Os dois estados do sistema quântico são representados por: $|0\rangle$ e $|1\rangle$. O estado $|0\rangle$ é representado pelo vetor complexo $(1, 0)$ em C^2 enquanto que o estado $|1\rangle$ é representado pelo vetor $(0, 1)$. Os vetores $(1, 0)$ e $(0, 1)$ ou $|0\rangle$ e $|1\rangle$ constituem a base ortogonal no espaço de Hilbert(NIELSEN; CHUANG, 2005).

Alguns problemas computacionalmente intratáveis no universo clássico, como a fatoração, são resolvidos por algoritmos de ordem polinomial em um computador quântico

(NIELSEN; CHUANG, 2005). O desenvolvimento de tal tecnologia inviabilizaria, por exemplo, os sistemas de criptografia por chave pública, cuja segurança é baseada na eficiência dos algoritmos clássicos de fatoração de números grandes em produto de números primos. Uma das aplicações mais interessantes da teoria da informação quântica é a criptografia quântica. Em 1970, Wiesner mostrou que as propriedades da mecânica quântica poderiam ser usadas para tal fim, mas seu trabalho só foi publicado em 1983. No ano seguinte, (BENNETT; BRASSARD, 1984) descreveram um protocolo para distribuição de chave secreta usando um canal quântico, que ficou conhecido como BB84. Existem várias provas de que o BB84 é incondicionalmente seguro, mesmo quando sujeito a ataques coletivos (BIHAM; BOYER, 2001).

Até o final dos anos 90, a expressão "criptografia quântica" se referia basicamente aos protocolos para distribuição de chave secreta (QKD) usando um canal quântico. Recentemente, várias pesquisas vêm sendo feitas no sentido de explorar as propriedades da mecânica quântica na resolução de outros problemas ligados à segurança de dados. Os primeiros trabalhos nessa linha dizem respeito à verificação de chave secreta e à autenticação de usuários. A verificação de chave consiste em garantir a legitimidade das duas partes que compõe um sistema de distribuição de chave, e que a mesma é autêntica. A autenticação de usuário, conhecida também como identificação de usuário, permite que um sistema determine a identidade do usuário que deseja usá-lo.

Somente em 2001, foi descrito o primeiro protocolo para autenticação quântica de mensagens (CURTY; SANTOS, 2001). Tratava-se de um protocolo que permitia o envio, de forma autêntica de bits, e cuja segurança era garantida pelas leis da mecânica quântica. Em seguida, os mesmos autores propuseram um protocolo para autenticação de bits quânticos, que foi uma extensão natural do primeiro. Por último, Barnum et al. descreveu um protocolo que permitia a autenticação de mensagens quânticas de comprimento arbitrário.

2.6 Protocolos de Autenticação: Clássicos e Quânticos

São apresentados a seguir sistemas clássicos e quânticos.

2.6.1 Assinaturas Digitais

Uma assinatura digital é uma seqüência de bits adicionados à documentos digitais. Assim elas são feitas para que uma entidade possa, digitalmente "assinar" um documento. Espera-se que uma assinatura eletrônica tenha as mesmas características de uma assinatura do mundo real:

- Seja fácil de produzir para quem assina;

- Seja fácil de verificar por qualquer um;
- Seja muito difícil de ser falsificado;
- Tenha uma vida útil apropriada(de modo que quem assine não negar ter assinado).

Assinatura digital é uma outra aplicação de criptografia de chave pública. Qualquer um pode codificar mensagens com a chave pública de Bob, mas só Bob pode decifrar mensagens com a sua chave privada.

Existe outro procedimento que se pode fazer com criptografia de chave pública. Pode-se inverter os papéis da chave pública e privada. Alice poderia codificar a sua mensagem com a sua chave privada e poderia envia-la para Bob. Esta não é uma comunicação segura. Bob, ou qualquer um outro interessado, poderia decifrar a mensagem com a chave pública de Alice e poderia ler o conteúdo. Ninguém mais tem a chave privada de Alice, e não há possibilidade de uma entidade desconhecida ter codificado esta mensagem, e isto autentica a origem da mensagem.

As assinaturas digitais satisfazem os cinco critérios:

1. A assinatura não pode ser falsificada; só Alice conhece sua chave privada.

2. A assinatura é autêntica; quando Bob verifica a assinatura com a chave pública de Alice ele sabe que ela assinou (codificou) isto.

3. A assinatura não é reutilizável; a assinatura em um documento não pode ser transferida para qualquer outro documento.

4. O documento assinado é inalterável; qualquer alteração de um documento (se ele foi ou não codificado) e a assinatura não são mais válidas.

5. A assinatura não pode ser recusada. Bob não precisa da ajuda de Alice para verificar sua assinatura.

2.6.2 Algoritmos de Assinatura Digital

Em 1976, surgiu um novo conceito em criptografia: A criptografia de chave pública. Como muitas das inovações, esta surgiu para atender a uma nova necessidade. Até o surgimento dos meios de comunicação à distância, sempre se considerava que duas pessoas teriam que se encontrar para combinar uma chave a ser usada na comunicação criptográfica. Isto não seria problemático pois, sem comunicações à distância, não haveria outra opção. Com o avanço da tecnologia, duas pessoas em locais distantes poderiam ter motivos para trocar mensagens criptografadas, e, ao mesmo tempo, não terem a oportunidade(ou o tempo) de se encontrarem fisicamente.

Poderia-se argumentar que bastaria estas pessoas trocarem a chave através de um meio seguro. Só que, se as duas pessoas têm um meio seguro para trocar a chave, então

elas poderiam trocar a própria mensagem por este mesmo meio seguro! Éclaro que este raciocínio nem, sempre é válido, mas ele é ilustrativo das razões do surgimento dos algoritmos de chave pública. Além disso, o mundo de hoje se tonou muito mais dinâmico. Uma companhia pode querer comunicar-se com outra que está fisicamente distante e, além disso, querer se comunicar rapidamente, de maneira que não há tempo para trocas seguras de chaves. Considere-se também o problema de um conjunto de cem pessoas que queiram garantir comunicações seguras entre quaisquer duas entre elas. Utilizando a criptografia clássica necessitaria (100 x 99) /2 = 4.950 chaves diferentes (para algoritmos simétricos). O gerenciamento desta quantidade de chaves é problemático. Por exemplo, podemos destacar alguns algoritmos de chave pública, bem como:

- **PGP** (*Pretty Good Privacy* - Programa para a codificação mensagens de texto, inventado por Philip Zimmerman. (HOLSCHUH, 2003)) ou do PEM (*Privacy Enhanced Mail* - Um padrão de criptografia de mensagens e de autenticação dos remetentes (S., 1993)).

- **RSA** (Algoritmo de encriptação de chave pública, criado por Ron Rivest, Adi Shamir e Len Adleman e1977(LABORATORIES, 2000). Além de codificar chaves, o algoritmo de chave pública RSA pode ser também usado para gerar assinaturas digitais. A matemática é a mesma que se utiliza o RSA para administração de chaves ou assinaturas digitais: existe uma chave pública e uma privada, e a segurança do sistema está baseada na dificuldade de fatorar números grandes. Ambos PGP e PEM utilizam o RSA para assinaturas digitais.

- **DSA** (CERTICON, 1997, 1997):

  O DSA é um algoritmo de assinatura digital (*Digital Signature Algorithm*). (Também existe um Padrão de Assinatura Digital (*Digital Signature Standard*), ou DSS. O padrão implementa o algoritmo - realmente é só uma diferença na terminologia.) é um algoritmo de chave pública, mas só pode ser usado para assinaturas digitais.

- *Privacy-Enhanced Mail* - PEM - É um dos padrões da InterNet para o envio de mensagens de correio eletrônico criptografadas. Foi criada uma implementação utilizando a lógica do DES chamada de *Riodan's InterNet Privacy-Enhanced Mail* (RIPEM), criada pelo americano Mike Riordan.

  Um exemplo poderia tornar as coisas claras. Alice está usando PEM: MD5(do inglês *Message Digest Algorithm 5*) como uma função *hash* de uma só via e o RSA para assinaturas digitais. (Dar-se nesse ponto um pouco de como o MD5 trabalha.). Ela

quer enviar uma mensagem assinada para Bob. Estes são os passos que ela tem que seguir:

1. Alice escreve a mensagem.

2. Alice gera um função *hash* de uma só via da mensagem e usa uma função *hash* de uma só via, como o MD5.

3. Alice assina o valor *hash* com um algoritmo de assinatura digital de chave pública, como o RSA e a chave privada dela.

4. Alice concatena a mensagem e a assinatura para adquirir uma nova, assinada, mensagem.

5. Alice envia por e-mail esta mensagem assinada para Bob.

No lado de Bob, ele pode ler a mensagem sem fazer qualquer esforço. Mas ele quer verificar a assinatura de Alice. Estes são os passos ele tem que seguir (Figura 2.3(BALPARDA, 2001)):

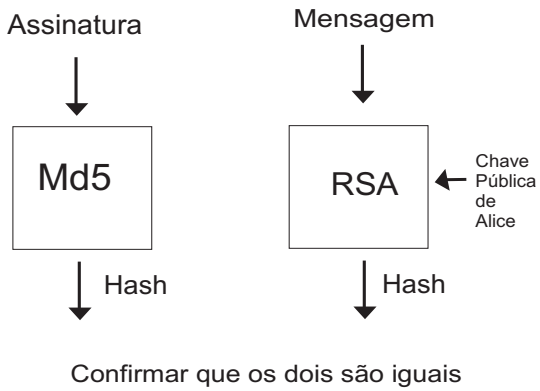

Figura 2.3: Verificando a assinatura de um correio eletrônico.

1. Bob separa a mensagem da assinatura.

2. Usando uma função de hash de uma só via, Bob computa o valor de hash da mensagem.

3. Bob adquire a chave pública de Alice.

4. Usando um algoritmo de assinatura digital de chave pública e a chave pública de Alice, Bob decifra a assinatura de Alice.

5. Bob compara a assinatura decifrada de Alice com o valor de hash da mensagem. Se eles são o mesmo, Bob verificou a assinatura de Alice e aceitou a mensagem como genuína. Se eles são diferentes, Bob rejeita a assinatura.

Eva não pode forjar a assinatura de Alice, pois ela não conhece a chave privada de Alice. Eva não pode pegar uma assinatura de uma mensagem válida assinada por Alice e anexá-la a uma nova mensagem; quando Bob tenta verificar a assinatura ele perceberá que os dois valores de *hash* são diferentes e assinatura não é válida.

2.6.3 Funções *hash* e funções *hash* fortemente universais-2

Uma função *hash* em autenticação foi introduzido inicialmente por (CARTER; WEGMAN, 1979). Funções "*hash*" são funções usadas para autenticar mensagens. Estas funções são diferentes das funções normais de encriptação, por não possuirem uma chave, e por serem irreversíveis. Daí vem o seu poder. As funções *hash* mapeiam domínios extensos em intervalos pequenos.

Definição 1 *Uma classe H de funções hash $A \rightarrow B$ é universal-2 se para quaisquer a_1 e $a_2 \in A$, $a_1 \neq a_2$. A probabilidade de se ter $f(a_1) = f(a_2\ )$ é, no máximo $\frac{1}{|B|}$, quando f é escolhida do conjunto H de maneira aleatória e uniforme.*

Exemplos de funções *hash* fortemente universal-2.
Classe Universal de funções *hash*. [Carter-Wegman 1980s]
Para todo par de elementos $a_1, a_2 \in A,\ p_{a \in A}\ [\ f(a_1) = f(a_2\ )] \leq \frac{1}{|B|}$
Pode ser selecionado aleatório h eficientemente.
Pode ser computado h(x) eficientemente. É interessante observar dois exemplos abaixo:
Exemplo 1:
Sejam A = $\{a,\ b,\ c,\ d,\ e,\ f\}$, B= $\{0, 1\ \}$

	a	b	c	d	e	f
$h_1(x)$	0	1	0	1	0	1
$h_2(x)$	0	0	0	1	1	1

$H = \{h_1, h_2\}$
$p_{h \in H}\ [h_1(a) = h_2(b)] = \frac{1}{2}$
$p_{h \in H}\ [h_1(a) = h_2(c)] = 1$
$p_{h \in H}\ [h_1(a) = h_2(d)] = 0$
O exemplo acima é considerado não-universal-2, pois, como a cardinalidade de B é 2, a probabilidade da igualdade de h_1 e h_2 é no máximo $\frac{1}{2}$.

Exemplo 2:

	a	b	c	d	e	f
h_1	0	1	0	1	0	1
h_2	0	0	0	1	1	1
h_3	0	0	1	0	1	1
h_4	1	0	0	1	1	0

$H = \{h_1, h_2, h_3, h_4\}$
$p_{h\in H}\ [h_1(a) = h_2(b)] = \frac{1}{2}$
$p_{h\in H}\ [h_1(a) = h_2(c)] = \frac{1}{2}$
$p_{h\in H}\ [h_1(a) = h_2(d)] = \frac{1}{2}$
$p_{h\in H}\ [h_1(a) = h_2(e)] = \frac{1}{2}$
$p_{h\in H}\ [h_1(a) = h_2(f)] = 0$

O exemplo acima é considerado uma função hash fortemente universal-2, pois, satisfaz a exigência da definição.

Um outro exemplo apresentado por Carter e Wegman é o da classe de todas as funções lineares de $\{0,1\}^n \rightarrow \{0,1\}^r$. Estas funções podem ser descritas por matrizes M de dimensões $r \times n$ sobre $GF(2)$, ou seja rn bits. A classe de funções *hash* fortemente universais-2 definida no lema a seguir é baseada no corpo algébrico $GF(2^n)$.

Lema 2 *(CARTER; WEGMAN, 1979) Seja a um elemento de $GF(2^n)$. Considere a função $\{0,1\}^n \rightarrow \{0,1\}^r$, atribuindo a um argumento $x \in GF(2^n)$ os r primeiros bits do elemento $ax \in GF(2^n)$. A classe de todas as funções para $a \in GF(2^n)$ é uma classe universal$_2$ de funções para $1 \leq r \leq n$.*

A classe de funções descrita no lema acima necessita de apenas n bits para especificar qualquer função que pertença a mesma.

Definição 3 *(CARTER; WEGMAN, 1979) Suponha que H é um conjunto de funções hash, em que cada elemento de H é uma função mapeia um elemento de A em um elemento de B. É dito que H é fortemente universal$_n$ se, dados n elementos distintos de A, $a_1,...,a_n$, e n elementos de B, $b_1,...,b_n$, então $\frac{|H|}{|B|^n}$ funções devem levar a_1 em b_1, a_2 em b_2, etc.*

Uma diferença entre algoritmos de cifragem e funções de *hash* de uma só via é que as funções *hash* de uma só via não têm uma chave (veja a Figura 2.4). Nenhum segredo é envolvido na função *hash* de uma só via; a segurança está na falta da habilidade de ir ou voltar para outro modo. Esta propriedade faz disso uma maneira útil para identificar uma mensagem.

Seja uma função *hash* de uma só via como uma impressão digital. Da mesma maneira que uma impressão digital identifica exclusivamente um indivíduo, uma função de *hash* de uma só via pode identificar uma mensagem de tamanho arbitrário.

Figura 2.4: Função *hash* de uma só via.

Valores *hash* de uma só via são normalmente pequenos: 16 ou 20 *bytes*. As mensagens podem ser grandes, muito grandes. Mas vale ressaltar que a chance de duas mensagens quaisquer resultem um *hash* do mesmo valor é muito pequeno e pode ser considerada desprezível. São projetadas funções de *hash* de uma só via de forma que seja praticamente impossível criar uma mensagem que resulte um *hash* de um valor particular, ou criar duas mensagens diferentes que resultem um *hash* de um mesmo valor.

Podem-se destacar alguns algoritmos de funções *hash*:

- SHA (*Secure Hash Algorithm*):

  O algoritmo SHA produz uma compilação de mensagem de 160 bits, uma função de *hash* de uma só via inventado no *National Security Agency* (NSA). Ele produz um valor de *hash* de 160-bit de um tamanho arbitrário da mensagem.

  Os funcionamentos internos do SHA são bem parecidos aos do MD4, indicando que os criptógrafos do NSA analisaram o algoritmo MD4 como base e melhoraram a sua segurança. De fato, a fraqueza na parte do algoritmo MD5(sucessor direto do MD4), descoberta depois que o SHA foi proposto, não funciona contra o SHA.

  Atualmente, não existe alguma forma conhecida de ataque criptoanalítico clássico contra o SHA com exceção do ataque de força bruta. E seu valor de 160-bit faz do ataque de força bruta ineficiente. É claro que não existe alguma prova que alguém não possa entender como quebrar o SHA num futuro próximo.

- **MD2 e MD4** (RIVEST, 1992):

  O MD2 é uma função de *hash* de uma só via simplificada e produz um hash de 128-bit. É uma opção no PEM; Não é recomendado usá-lo porque geralmente acredita-se que não é muito seguro.

O MD4 é o precursor do MD5 e também foi inventado por Ron Rivest. Depois que algumas fraquezas de segurança foram descobertas no MD4, Rivest escreveu o MD5. O MD4 foi parte das especificações originais do PEM, mas já não é mais usado.

Na subsecção seguinte apresenta-se um dos protocolos para autenticação quântica de mensagens clássicas, ressaltando que o princípio é o mesmo visto na autenticação clássica, ou seja, autenticar uma mensagem. A diferença básica é o processo do envio da etiqueta nos canais inseguros. Na criptografia quântica, a etiqueta é enviada através de procedimentos quânticos.

2.6.4 O Protocolo de Curty e Santos para Autenticação Quântica de Mensagens Clássicas

O primeiro protocolo encontrado na bibliografia especializada para autenticação quântica de mensagens clássicas foi descrito pelos espanhóis Curty e Santos (CURTY; SANTOS, 2001) . Mais especificamente, os autores propuseram um protocolo capaz de autenticar mensagens clássicas de comprimento unitário, ou seja, um bit. Esta seção visa descrever e analisar, em detalhes, o funcionamento de tal protocolo.

Supõe-se que Alice deseja enviar para Bob, por meio de um canal quântico, uma mensagem clássica certificada. Supondo que a mensagem é binária de comprimento unitário, existirão somente duas mensagens possíveis, "0" e "1", que são associadas a dois estados quânticos $|\phi_0\rangle$ e $|\phi_1\rangle$, respectivamente. Para que Bob consiga distinguir perfeitamente entre esses dois estados, eles necessitam ser ortogonais, i.e., $\langle\phi_i \mid \phi_j\rangle = \delta_{ij}$, com i, $j \in \{0, 1\}$. Esses estados devem conter, como qualquer outro sistema de autenticação, alguma etiqueta que permita a Bob checar a autenticidade da mensagem. Considera-se que os estados $|\phi_i\rangle$ pertencem a um espaço de estado de dois qubits (um espaço de Hilbert de dimensão quatro) H, em que o primeiro qubit transporta informação sobre a mensagem e o segundo sobre a etiqueta.

A chave secreta consiste de um estado quântico de dois qubits emaranhados, a serem compartilhados por Alice e Bob. Dessa forma, Alice guarda o primeiro qubit do estado $|\psi\rangle_{AB}$ e Bob o segundo qubit, em que

$$|\psi\rangle_{AB} = \frac{|01\rangle_{AB} - |10\rangle_{AB}}{\sqrt{2}}. \tag{2.1}$$

O procedimento de autenticação é descrito a seguir. Quando Alice deseja enviar um bit certificado i, ela prepara dois qubits no estado $|\phi_i\rangle$ (é importante lembrar de que já é um estado quântico de dois qubits) e aplica a operação de codificação

$$E_{AH} = |0\rangle\langle 0|_A I_H + |1\rangle\langle 1|_A U_H. \tag{2.2}$$

na sua parte de $|\psi\rangle_{AB}$ e na mensagem, em que U_H é um operador unitário. Basicamente, o resultado desta operação de codificação é criar um estado de superposição, no qual o operador unitário U_H é aplicado no estado $|\phi_i\rangle$ [segundo termo da Equação 2.2] ou não [primeiro termo da Equação 2.2], dependendo do estado do qubit da chave de Alice.

2.6.5 Autenticação de um Qubit

Em 2002, Curty, Santos *et al.* propuseram um protocolo para autenticação de mensagens quânticas (CURTY; SANTOS, 2001; CURTY; SANTOS; PERE, 2002). O esquema é capaz de identificar um único qubit descrito por um operador de densidade ρ_M, pertencente a um espaço de mensagens M de dimensão dois. A diferença fundamental em relação ao caso clá ssico é que a etiqueta agora é dada por um operador densidade ρ_T, de algum espaço de etiquetas T. A mensagem e a etiqueta são descritas por um operador de densidade $\rho_H = \rho_M \otimes \rho_T$, em que $\otimes$ representa simbolicamente o produto tensorial, que atua no espaço de estado $H = M \otimes T$. No caso em que o canal quânticoé perfeito, T é o espaço de Hilbert de dimensão dois e $\rho_T = |0\rangle \langle 0|_T$.

Da mesma forma que no protocolo anterior, o par EPR $|\psi\rangle_{AB}$ é usado como chave secreta quando Alice deseja enviar para Bob uma mensagem ρ_M. O estado do sistema global (chave, mensagem e etiqueta) é dado por

$$\rho_{ABH} = |\psi\rangle \langle\psi|_{AB} \otimes \rho_H = |\psi\rangle \langle\psi|_{AB} \otimes \rho_M \otimes |0\rangle \langle 0|_T . \tag{2.3}$$

Em seguida, Alice realiza uma operação de codificação, descrita pelo operador E_{AH}, na sua parte da chave, na mensagem e na etiqueta, em que

$$E_{AH} = |0\rangle \langle 0|_A \otimes I_H + |1\rangle \langle 1|_A \otimes U_H \tag{2.4}$$

em que U_H é algum operador unitário em H. Se ρ^e_{ABH} é o operador densidade que descreve o estado do sistema global após a codificação, i.e., $\rho^e_{ABH} = E_{AH}\rho_{ABH}E^\dagger_{AH}$, então o estado da mensagem que Alice envia a Bob através do canal quântico é dado por $\rho^e_H =$tr$_{AB}(\rho^e_{ABH})$, em que ρ^e_{ABH} pode ser descrito como

$$\begin{aligned} \rho^e_{ABH} &= \frac{1}{2}\left(|01\rangle \langle 01|_{AB} \otimes \rho_H + |10\rangle \langle 10|_{AB} \otimes U_H\rho_H U^\dagger_H \right. \\ &\quad \left. - |01\rangle \langle 10|_{AB} \otimes \rho_H U^\dagger_H - |10\rangle \langle 01|_{AB} \otimes U_H\rho_H\right). \end{aligned} \tag{2.5}$$

Assim,

$$\rho^e_H = \frac{1}{2}(\rho_H + U_H\rho_H U^\dagger_H). \tag{2.6}$$

No lado da recepção, Bob decodifica a informação enviada por Alice aplicando a operação unitária

$$D_{BH} = |0\rangle \langle 0|_B U_H^\dagger + |1\rangle \langle 1|_B I_H \tag{2.7}$$

ao seu qubit da chave secreta e à mensagem autenticada recebida, obtendo $\rho^d_{ABH} = D_{BH}\rho^e_{ABH}D^\dagger_{BH}$. Finalmente, Bob verifica o estado da etiqueta através de uma medição ortogonal $\{|0\rangle \langle 0|_T, |1\rangle \langle 1|_T\}$ sobre a porção da etiqueta de $\rho^d_H = \mathrm{tr}_{AB}(\rho^d_{ABH})$, em que $|1\rangle_T$ é o estado em T ortogonal a $|0\rangle_T$. Se o resultado desta medição for $|0\rangle_T$, Bob deve assumir que o estado quântico recebido é autêntico. Caso contrário, ele o descarta.

2.6.6 Outros Protocolos

Em virtude de ser uma área de pesquisa relativamente recente, são poucos os trabalhos na área de autenticação quântica. Somente três protocolos foram descritos neste trabalho diferentes para esse fim: o já descrito protocolo de Curty e Santos, uma generalização deste protocolo para autenticação de qubits (mensagens quânticas representadas por vetores em um espaço de Hilbert de dimensão dois) e, por último, um protocolo para autenticação de mensagens quânticas de comprimento arbitrário (BARNUM et al., 2002).

Os protocolos destinados à autenticação de mensagens quânticas devem utilizar uma quantidade maior de recursos para serem implementados, visto que Alice e Bob manipulam, ao invés de um simples conjunto de estados quânticos ortogonais, estados quânticos genéricos a serem transmitidos de forma autêntica por meio de um canal quântico. Como o objetivo deste trabalho de dissertação é descrever um protocolo de autenticação quântica de mensagens clássicas que utilize o mínimo possível de recursos, os protocolos de autenticação de mensagens quânticas mencionados acima serão descritos de forma breve nas próximas subseções. Caso se tenha interesse, são disponibilizadas da bibliografia especializada conceitos ou recursos usados em cada protocolo.

2.6.7 Autenticação de Mensagens Quânticas de Comprimento Arbitrário

Recentemente, Barnum *et al.* descreveram um esquema não interativo para autenticação de mensagens quânticas de comprimento m (BARNUM et al., 2002). O protocolo faz uso de códigos estabilizadores para codificar a mensagem na qual são usados $m + O(s)$ qubits, em que a probabilidade de falha de autenticação decresce exponencialmente com o

parâmetro de segurança s. O protocolo requer a criação de pares EPR por Alice e o envio de uma das metades a Bob. Foi demonstrado também que, para alcançar tal segurança, Alice e Bob devem compartilhar uma chave secreta clássica de comprimento maior ou igual a $2m$ bits, para cada mensagem quântica de comprimento m. Este protocolo requer circuitos quânticos para codificação e decodificação das mensagens.

Devido a quantidade e a complexidade de conceitos envolvidos, foi descartada a descrição detalhada deste protocolo, pois, foge ao escopo deste trabalho.

2.6.8 Segurança Computacional e Incondicional

Muitos aplicativos transmitem dados confidenciais entre as camadas de aplicativo, do servidor de banco de dados para o navegador e vice-versa. Exemplos de dados confidenciais incluem detalhes de contas bancárias, números de cartão de crédito, dados de folha de pagamento etc. Além disso, os aplicativos devem proteger as credenciais de autenticação local(*logon*) à medida que elas são passadas pela rede.

Definição 4 (Segurança computacional) *(CANETTI; GOLDWASSER; MICALI, 2000; BELLARE; GOLDWASSER; MICALI, 2001)(CANETTI; GOLDWASSER; MICALI, 2000, pág.04) Um esquema de criptografia ou autenticação é dito possuir segurança computacional quando a segurança do sistema depende de limitações de tempo e de recursos computacionais, que inviabilizam a resolução de uma determinada classe de problemas.*

Os sistemas de criptografia e autenticação que apresentam segurança computacional são utilizados nas mais diversas aplicações. Os mais conhecidos são os sistemas de criptografia por chave pública, a exemplo dos algoritmos RSA, MD5 e, mais recentemente, os algoritmos SHA-1 e HMAC. Suas aplicações incluem transações financeiras, comerciais, militares, autenticação de usuários e sistemas, proteção de arquivos, transmissão segura de dados, etc. A segurança desses esquemas de criptografia e autenticação é baseada na Teoria dos números que são atualmente intratáveis via algoritmos clássicos, como a fatoração de números em produto de primos, o problema do logaritmo discreto e o problema dos resíduos quadráticos. Esses problemas serão discutidos com mais detalhes no próximo capítulo.

Com relação aos sistemas de criptografia e autenticação por chave pública, o seguinte resultado pode ser provado:

Teorema 5 *Todo sistema de criptografia por chave pública apresenta segurança computacional. Isto é, desde que Eva disponha de recursos computacionalmente ilimitados, as mensagens podem ser forjadas.*

(WEGMAN; CARTER, 1981)

Definição 6 (Segurança incondicional) *Um esquema de criptografia ou autenticação é dito possuir segurança incondicional quando a segurança do sistema independe do poder computacional de criptoanalistas.*

O exemplo mais conhecido de sistemas que apresentam segurança incondicional é a cifra de Vernam (ALBRECHT, 1994) . A cifra pode ser sucintamente descrita como

$$C_i = b_i \oplus k_i, \tag{2.8}$$

em que C_i representa o bit criptografado, b_i o bit em claro (a ser criptografado), $\oplus$ é a operação ou-exclusivo e é o bit de chave secreta compartilhado entre as duas partes, que deve ser escolhido de forma aleatória, uniforme e independente do bit b_i. Além disso, para cada bit de mensagem b_i, um bit de chave k_i deve ser usado e descartado em seguida. Se uma mensagem binária de comprimento n é criptografada usando a cifra de Vernam, é fácil verificar que a probabilidade de um criptoanalista decifrá-la é 2^{-n}, independentemente do poder computacional que ele possua.

2.6.9 Códigos de Autenticação de Mensagens

Um código de autenticação de mensagens, ou código MAC, é considerado uma técnica de autenticação que envolve o uso de uma chave secreta para gerar um bloco pequeno de tamanho fixo, conhecido como etiqueta MAC, que é concatenado a mensagem a ser enviada por um canal inseguro. Na recepção, é gerada uma segunda etiqueta, que é função da mensagem recebida e da chave secreta. As duas etiquetas são comparadas e a mensagem é considerada autêntica se as etiquetas coincidirem. Caso contrário, a mensagem é descartada.

Existem diversos códigos MAC cada um apresentando um determinado nível de segurança. É possível projetar um esquema MAC que alcance segurança incondicional, de tal forma que uma terceira parte (Eva) tenha uma probabilidade arbitrariamente pequena de criar uma mensagem que o destinatário aceitaria como autêntica.

Um código de autenticação de mensagens pode ser formalizado como segue. Seja M como sendo o conjunto de mensagens possíveis e T como sendo o conjunto de etiquetas de autenticação possíveis. É definido também um conjunto de funções F, publicamente conhecido, em que cada função em F mapeia uma mensagem de M em uma etiqueta de T. Para usar o sistema, Alice e Bob devem compartilhar uma chave secreta que especifica

uma função $f \in$ F. Para transmitir uma determinada mensagem $m \in$ M, Alice calcula a função f na mensagem m, e concatena o resultado a mensagem, transmitindo ambos em seguida. Na recepção, Bob aplica a mesma função f na mensagem recebida com a etiqueta recebida. Etiquetas idênticas indicam que a mensagem é autêntica. Neste esquema, a probabilidade de Eva encontrar a função f, conhecendo apenas a mensagem e a etiqueta, deve ser arbitrariamente pequena.

Wegman e Carter provaram que, dada uma chave secreta compartilhada entre Alice e Bob, qualquer esquema de autenticação incondicionalmente seguro pode ser usado somente um número finito de vezes, e tal número depende do tamanho da chave secreta e da probabilidade que um adversário qualquer possui de inferir a função de geração da etiqueta.

Definição 7 *Um código de autenticação de mensagens é incondicionalmente seguro com probabilidade p se, dadas uma mensagem m e a etiqueta correspondente $f(m)$, a probabilidade de se encontrar uma mensagem diferente m' tal que $f(m') = f(m)$ é sempre menor do que p.*

O que a definição afirma é que a segurança do esquema de autenticação é condicionada somente a manutenção em segredo da chave secreta por Alice e Bob. Gilbert et al. propuseram um código MAC considerando as premissas acima. A dificuldade de utilizar tal esquema reside no tamanho da chave secreta, que deveria ter comprimento mínimo igual ao tamanho da mensagem a ser enviada. Outro problema é que a chave secreta poderia ser usada para criar uma única etiqueta, devendo ser descartada em seguida.

2.6.10 A utilização Geradores de Números Pseudo-Aleató rios em protocolos de autenticação clásssicos e quânticos

A geração de números aleatórios desempenha um papel fundamental em praticamente todas as áreas da criptografia e segurança de dados em geral. Idealmente, é desejável que um gerador de seqüências pseudo-aleatórias rapidamente produza seqüências longas de bits a partir de uma seqüência curta e pré-determinada, de forma que os bits gerados, de todas as formas, aparentem ter sido obtidos aleatoriamente.

Obviamente, a idéia de tal mecanismo determinístico gerando seqüências de comportamento aleatório parece ser contraditório. Observam-se que diversas de suas saídas deve ser possíveis, pelo menos em princípio, determinar seus parâmetros de forma a simular o gerador.

A solução usual é projetar o gerador de tal forma que as seqüências produzidas não sejam reprovadas por um conjunto de testes estatísticos. Esses testes incluem o cálculo da freqüência de zeros e uns, comprimento de surtos e distribuição dos bits na seqüência. Existem testes para determinar se uma seqüência segue uma determinada distribuição, incluindo a uniforme, mas não existe nenhum teste que prove a independência entre os bits da mesma. Ao contrário, existem testes que podem ser aplicados para demonstrar que a seqüência não possui independência.

Uma característica importante dos geradores de seqüências pseudo-aleatórias é a imprevisibilidade computacional, essencial para a maioria das aplicações em criptografia clássica.

Definição 8 *Um gerador de seqüências pseudo-aleatória é* ***imprevisível em tempo polinomial*** *(imprevisível à esquerda e imprevisível à direita), ou computacionalmente imprevisível, se e somente se as seqüências geradas não são previsíveis (à esquerda e à direita) em tempo polinomial. Isto é, dada uma seqüência finita produzida pelo gerador, x_k, x_{k+1}, ... , x_{n-1}, x_n, o melhor algoritmo que determina, em tempo polinomial, o termo anterior à seqüência, x_{k-1}, ou o termo posterior, x_{n+1}, consegue fazê-lo somente com uma probabilidade arbitrariamente pequena, do que se os termos fossem obtidos a partir de lançamentos sucessivos de uma moeda não viciada.*

A definição menciona que as seqüências produzidas por geradores que satisfazem os requisitos da Definição 2.4 resistem a todos os testes estatísticos em tempo polinomial, ou seja, essas seqüências não podem ser distinguidas por nenhum teste estatístico em tempo polinomial, com uma probabilidade arbitrariamente pequena, de seqüências produzidas por lançamentos sucessivos de uma moeda não viciada.

A segurança dos geradores computacionalmente seguros é geralmente baseada em problemas computacionalmente intratáveis da teoria dos números e por isso são utilizados para proporcionar maior segurança aos protocolos de autenticação quântica. Na seção seguinte sáo apresentado os geradores Blum-Micali (usado no protocolo MA4), que aqui será denominado simplesmente por BM e o Blum-Blum-Shub (que é utilizado no protocolo descrito) que será denominado simplesmente por BBS, bem como os fundamentos em que a sua segurança é baseada. Também é apresentado a descrição do protocolo MA4.

2.7 Conclusão

Neste capítulo foram apresentados os protocolos clássicos e quânticos presentes na bibliografia atual. Os protocolos clássicos são importantes na medida em que os quânticos tornam-se mais rápidos e eficientes.

No próximo capítulo, sao feitas as descrições dos Geradores pseudo-aleatórios BM e BBS e também o protocolo de autenticacação quântica de mensagens clássicas propostos por Medeiros e Assis (MA4) (MEDEIROS, 2004).

Capítulo 3

Os Geradores BM e BBS e o algoritmo de autenticação híbrido (MA4)

3.1 Introdução

São apresentados os geradores de seqüências pseudo-aleatórios e suas particularidades. Também são feitas comparações entre os geradores apresentados.

3.1.1 O Gerador de sequências pseudo-aleatório Blum e Micali (BM)

O gerador de Blum-Micali (M.BLUM; MICALI, 1984) (BM) é um gerador simples, porém eficiente na sua função de gerar seqüências pseudo-aleatórias, que é baseado na intratabilidade computacional (clássica) do problema do logaritmo discreto. Dada pela equação

$$y = g^x \ mod \ p, \tag{3.1}$$

em que p é um primo, g é um gerador g para $GF(p)$ e $x \in GF(p)$. Dados g, x e p, o cálculo de y é direto. Entretanto, dados y, g e p, o problema de encontrar x, que é o logaritmo discreto de y módulo p na base g, é considerado computacionalmente intratável. Acredita-se que a dificuldade de calcular o logaritmo discreto é da mesma ordem de magnitude da fatoração em produtos de primos. Formalmente, o problema do logaritmo discreto é resumido como segue:

O problema do logaritmo discreto (M.BLUM; MICALI, 1984). Seja p um número primo e seja g um gerador para o grupo $(Z_p^*, \cdot)$. A função $f_{g,p} : Z_p^* \rightarrow Z_p^*$ definida por $f_{b,p} = b^x \bmod p$ é uma permutação de Z_p^* calculada em tempo $O(|p|^3)$. O problema do logaritmo discreto com parâmetros g e p consiste em encontrar, para cada $y \in Z_p^*$, o índice

$x \in Z_p^*$ tal que $g^x modp = y$. Um algortimo probabilístico $\mathbf{P}[g, p, y]$ resolve o problema do logaritmo discreto se para todo primo p, para todos os geradores g de Z_p^* e para todo $y \in Z_p^*$, $\mathbf{P}[g,p,\ y] = x$, $x \in Z_p^*$ tal que $g^x modp = y$. O problema do logaritmo discreto é comumente chamado de problema de encontrar o índice.

O problema do logaritmo é considerado intratável em tempo polinomial. Isto porque ainda não foi descrito um algoritmo clássico que resolva tal problema eficientemente.

Consideração acerca do problema do logaritmo discreto (M.BLUM; MICALI, 1984): Afirma que existe uma fração fixa de tempo em que o problema do logaritmo discreto não pode ser resolvido eficientemente. Seja $\mathbf{P}[g,p,y]$ um procedimento probabilístico para resolver o problema do logaritmo discreto, que executado em um computador clássico. Seja $0 \leq \epsilon \leq 1$ uma constante fixa e *poly* um polinômio também fixo.

Então, para todo número n suficientemente grande e para todos, com exceção de uma fração ϵ, dos números primos p de n bits, para todos os geradores g de Z_p^* e para pelo menos uma fração ϵ de números $y \in Z_p^*$, $\mathbf{P}[g,p,y]$ gasta um tempo (esperado) maior do que $poly(n)$ para calcular um elemento particular x tal que $g^x \ mod \ p = y$.

Segundo Stallings (1998) (STALLINGS, 2005), o algoritmo mais eficiente para calcular o logaritmo discreto módulo um primo p tem ordem

$$e^{\left((\ln p)^{(1/3)} \ln(\ln p)\right)^{2/3}}, \tag{3.2}$$

que é inviável para primos grandes.

3.1.2 Gerador de Sequências pseudo-aleatórias Blum-Blum-Shub (BBS)

Nesta seção, é apresentado o gerador PRBG Blum-Blum-Shub, que foi descrito inicialmente por (BLUM; BLUM; SHUB, 1983). Primeiramente, é dado algum fundamento da Teoria dos números para se compreender as fundamentações (SIDORENKO; SHOENMARKERS, 2005) que estiverem sendo usadas neste trabalho.

Em primeiro lugar, vale recordar o Teorema dos Restos Chinês(CRT), em que, são especificados as transformações uma a uma entre os elementos $a \in Z_m$, onde, $m = m_1 \cdot m_2 \cdot ... \cdot m_k$ e listas de resíduos $(r_1,r_2, ..., r_k)$, quando o módulo de $m_1, m_2, ..., m_k$ são termos relativamente primos. Recorre-se à lista $(r_1,r_2, ..., r_k)$ como a transformada-CRT de a.

As duas principais propriedades interessantes desta transformação são as seguintes:

- Primeiro, a transformada-CRT do produto de dois números a_1 e a_2 em Z_m é o produto da transformada-CRT de a_1 e a_2;

- Segundo, a é um elemento inversível em Z_m se e somente se os módulos r_i são elementos inversíveis de Z_m para todo $1 \leq i \leq k$ respectivamente.

Agora, apresentam-se os conceitos de resíduos quadráticos e do símbolo de Legendre: $\mathbb{N}$

Definição 9 (Resíduo Quadrático) *Seja $n \in \mathbb{N}$. Então $a \in Z_n^*$ é chamado resíduo quadrático modulo n se existe $b \in Z_n^*$ tal que*

$$a \equiv b^2 \ (mod\ n)$$

O conjunto dos resíduos quadráticos módulo n é denotado por QR_n. Além disso,

$$QNR_n := Z_n^* \backslash QR_n$$

é chamado o conjunto de resíduos não quadráticos.

O método BBS, proposto inicialmente por L. Blum, M. Blum e M. Shub (BLUM; BLUM; SHUB, 1999), propõe que a partir do produto (N) de dois grandes números primos especiais tais que $p \equiv q \equiv 3 \ \ mod \ \ 4$, e de uma semente inicial escolhida aleatoriamente (x) pode-se obter uma seqüência de números aleatórios com a seguinte lei de formação:

$$S_o = x^2 \ mod \ N \tag{3.3}$$

e

$$S_{i+1} = S_i^2 \ mod \ N, \tag{3.4}$$

A exigência de que p e q devem ser primos especiais está presente no artigo original, citado, e, aparentemente, garante maior controle sobre o ciclo do sistema, mas essa exigência tem sido ignorada ultimamente. Mais recentemente, Sidorenko (SIDORENKO; SHOENMARKERS, 2005) propõe uma nova concepção para o gerador BBS, proporcionando maior segurança ao gerador como será visto a seguir.

Sejam $N = p.q$ em que p e q são números primos conguêntes a 3 módulo 4, i.é, $p \equiv q \equiv 3 \ \ mod \ \ 4$. O algoritmo a seguir descreve o Gerador de Sequências Pseudo-aleatórias (PRBG)- Blum-Blum-Shub:

Entrada: Semente $x_0 \in Z_N(+1) \cap (0, N/2)$ escolhida de forma aleatória.

Saída: Uma sequência binária $\{b_1 \ b_2 \ b_3 \ ... \ b_M\}$ de comprimento $M = jk$.

Inicialização:

$x_1 := x_0$;

Iteração:
para $i = 1, ..., k$ faça
para $r = 1, ..., j$ faça

$$b_{(i-1)j+r} = l_{j-r+1}(x_i) \tag{3.5}$$

$$x_{i+1} = E_N(x_i) = x_i^2 mod N \tag{3.6}$$

Exemplo: Dados, $N = 133$, $x_0 = 4$, $r = 1, ..., 3$, $i = 1, ..., 4$, teremos:

$i = 1$		$i = 2$	
$r = 1$	$b_1 = l_3(x_1) = 0$	$r = 1$	$b_4 = l_3(x_2) = 0$
$r = 2$	$b_2 = l_2(x_1) = 0$	$r = 2$	$b_5 = l_2(x_2) = 0$
$r = 3$	$b_3 = l_1(x_1) = 1$	$r = 3$	$b_6 = l_1(x_2) = 0$
$i = 3$		$i = 4$	
$r = 1$	$b_7 = l_3(x_1) = 1$	$r = 1$	$b_{10} = l_3(x_2) = 0$
$r = 2$	$b_8 = l_2(x_1) = 1$	$r = 2$	$b_{11} = l_2(x_2) = 1$
$r = 3$	$b_9 = l_1(x_1) = 1$	$r = 3$	$b_{12} = l_1(x_2) = 1$

Assim, continuando até a $i = 4$ iteração, obtêm-se a seqüência:
$\{b_1 b_2 b_3 ... b_{12}\} = 001000111011$

3.1.3 Análise da segurança computacional clássica do BBS.

É analisada a segurança computacional do BBS partindo do princípio de que sua segurança é baseada na dificuldade de encontrar a diferença de sequências pseudo-aleatórias de sequências verdadeiramente aleatórias (SIDORENKO; SHOENMARKERS, 2005).

A segurança criptográfica do PRBG de Blum-Blum-Shub é assegurada pela Teoria dos números, que é chamada de problemas dos resíduos quadráticos, na qual são alguns definidos conceitos preliminares para a análise desses problemas. Estas definições são encontradas em (JUNOD, 1999).

Em (SIDORENKO; SHOENMARKERS, 2005) é usada a definição padrão de segurança de um gerador, isto é, o gerador pseudo-aleatório é denominado $(T_A, \varepsilon) - seguro$ se nenhum inimigo pode distinguir sequências verdadeiramente aleatórias em tempo T_A com probabilidade $1/2 + \varepsilon$. Ainda em (SIDORENKO; SHOENMARKERS, 2005), é provado que o BBS é $(T_A, \varepsilon) - seguro$ se

$$T_A \leq \frac{L(N)}{36n(\log_2 n)\delta^{-2}} - 2^{2j+9}n\delta^{-4} \tag{3.7}$$

onde,

$$\delta = (2^j - 1)^{-1}M^{-1}\varepsilon. \tag{3.8}$$

Na próxima subseção é feita uma comparação entre os geradores BM e BBS.

3.1.4 Comparação entre o BM e o BBS.

O gerador BM que é baseado na intratabilidade computacional (clássica) do problema do logaritmo discreto, tem como saída apenas um bit por cada iteração.

O gerador BBS (BLUM; BLUM; SHUB, 1999) também é baseado na intratabilidade computacional , dada pela equação

$$y = x^2 \ mod \ N \tag{3.9}$$

em que $N = p.q$ e p e q são ambos congruêntes a 3 *módulo* 4, este é reduzido ao problema clássico da busca de um algoritmo eficiente de fatoração, que é considerado computacionalmente intratável. É assegurada pelo corolário abaixo , encontrada em (SIDORENKO; SCHOENMAKERS, 2005).

Corolário 10 *Supõem-se que o gerador pseudo-aleatório BBS é vulnerável contra ataques de recuperação de A com* (T_A, ε)*. Então existe um algoritmo F que fatora o módulo N em tempo esperado*

$$T_F \leq 36n(\log_2 n)\delta^{-2}(T_A + 2^{2j+9}n\delta^{-4}) \tag{3.10}$$

onde,

$$\delta = (2^j - 1)^{-1}M^{-1}\varepsilon \tag{3.11}$$

Além disso, o BBS produz log(n) bits por 1 quadrado modular, enquanto o gerador BM produz um só bit por exponenciação modular (SIDORENKO; SCHOENMAKERS, 2005).

O protocolo apresentado por Medeiros e Assis (MA4) é uma extensão do protocolo de Brassard, este último apresentando somente segurança computacional. Quando é usado o PRBG Blum-Micali, usado no esquema de Brassard, o algorítmo clássico atinge limites infinitos e eficientes capazes de resolver o problema do logaritmo discreto, o que seria suficiente para que Eva pudesse falsificar uma mensagem e enganar Bob.

A seguir é apresentado a descrição do protocolo MA4, baseado na teoria da mecânica quântica, no protocolo de Brassard e na eficiência do gerador de Blum e Micali.

3.2 A descrição do Protocolo MA4

O protocolo MA4 (MEDEIROS, 2004) possui as propriedades da mecânica quântica para "mascarar" a seqüência pseudo-aleatória de bits enviados por Alice para Bob de forma que Eva, mesmo possuindo recursos computacionais clássicos e quânticos infinitos, não consiga distinguir uma seqüência falsa de uma seqüência verdadeiramente aleatória. O protocolo faz uso de uma função *hash* fortemente universal$_2$ (CARTER; WEGMAN, 1979), de forma que Eva, até mesmo com poder computacional infinito, não possa forjar ou mesmo modificar uma mensagem sem ser descoberta. Além disso, o protocolo faz uso de um gerador de seqüências pseudo-aleatórias, descrito por Blum e Micali(M.BLUM; MICALI, 1984), que é imprevisível em tempo polinomial, considerado intratável porque é baseado no problema do logaritmo discreto.

O protocolo descrito aqui utiliza outra chave secreta y_o, que é uma semente para o mesmo gerador de seqüências pseudo-aleatórias. Quando Alice deseja enviar uma mensagem certificada para Bob, ela realiza todos os passos descritos pelo protocolo de Brassard. Considerando que Alice e Bob compartilham uma chave secreta que consiste de uma função *hash* particular $h \in H$ e duas sementes x_o e y_o. Mais detalhes deste protocolo será apresentado no próximo capítulo, fazendo uso do gerador BBS.

3.3 Conclusão

Neste capítulo, foi apresentado um resumo da descrição do protocolo descrito por Medeiros e Assis (MEDEIROS, 2004), no qual, é apresentado, em seus originais, uma prova formal quanto à segurança desse protocolo quando se utiliza do gerador de Blum-Micali no protocolo de Brassard. O protocolo apresentado apresenta várias vantagens quando comparados a outros protocolos apresentados na bibliogafia atual.

No proxímo capítulo, é apresentado um novo esquema de autenticação quântica de mensagens clássicas utilizando o PRBG Blum-Blum-Shub (BBS). O esquema apresenta uma segurança incondicional, mesmo quando Eva possui computadores quânticos e clássicos, sem restrição de tempo de processamento.

Capítulo 4

Protocolo de Autenticação Quântica de mensagens clássicas com uso do BBS.

4.1 Introdução

O protocolo que é apresentado é uma variação do protocolo proposto por (MEDEIROS, 2004), que por sua vez é baseado no protocolo de Brassard, em que o gerador BM é substituído pelo gerador BBS.

A seguir é apresentada a descrição do protocolo, baseada na teoria da mecânica quântica, no protocolo MA4 e na eficiência do gerador de Blum-Blum-Shub.

O protocolo proposto por Brassard e, posteriormente, aperfeiçoado por Medeiross e Assis (MEDEIROS, 2004), será novamente aperfeiçoado com a substituição do gerador BM pelo gerador BBS e, também, serão utilizadas as propriedades da mecânica quântica para "mascarar" a seqüência pseudo-aleatória de bits enviados por Alice para Bob de forma que, Eva não consiga distinguir uma seqüência falsa de uma seqüência verdadeiramente aleatória. Assim como o MA4, o protocolo faz uso de uma função *hash* fortemente universal-2 (CARTER; WEGMAN, 1979), de forma que Eva, até mesmo com poder computacional infinito, não possa forjar ou mesmo modificar uma mensagem sem ser descoberta. Além disso, o protocolo faz uso de um gerador de seqüências pseudo-aleatórias,o BBS, que é imprevisível em tempo polinomial, considerado um dos problemas intratáveis (SIDORENKO; SHOENMARKERS, 2005).

Neste trabalho se utiliza outra chave secreta y_o, que é uma semente para o mesmo gerador de seqüências pseudo-aleatórias BBS. Quando Alice deseja enviar uma mensagem certificada para Bob, ela realiza todos os passos descritos pelo protocolo de Brassard. Considerando que Alice e Bob compartilham uma chave secreta que consiste de uma função *hash* particular $h \in H$ e duas sementes x_o e y_o. Para a n-ésima mensagem $m \in M$ a ser enviada, Alice prepara uma etiqueta $a(m, n)$ de k bits, dada pela equação

$$a_B(m,n) = h(m_B) \oplus x_o(n), \tag{4.1}$$

em que $x_o(n) = x_o[(n-1)k+1, ..., nk]$. Alice cria k qubits nas bases ortogonais Z ou X, dependendo da etiqueta $a(m,n)$ e da seqüência $y_o(n)$. Ela envia os qubits através de um canal quântico perfeito. A mensagem é enviada por um canal inseguro, podendo ser clássico ou quântico. Em seguida Bob escolhe as bases (conjuntos POVMs) usadas na medição de acordo com a seqüência pseudo-aleatória $y_o(n)$. Como resultado, ele obtém uma seqüência de k bits, $a_B(m,n)$. Agora Bob calcula uma etiqueta local $a'_B(m,n)$, baseado na mensagem recebida e na seqüência $x_o(n)$, que é comparada com $a_B(m,n)$. Se as etiquetas são idênticas, Bob considera que a mensagem é autêntica, caso contrário, ele a rejeita.

A segurança do protocolo é assegurada pelo gerador de seqüências pseudo-aleatórias (PRBG), o BBS, que já foi descrito anteriormente.

A descrição mais detalhada do protocolo é vista como segue: considera-se que Alice e Bob combinam de usar duas bases ortonormais para o espaço de Hilbert de dimensão dois, compartilhando de uma chave secreta que consiste de uma função hash particular $h \in H$ e duas sementes x_o e y_o o protocolo para autenticação quântica de mensagens clássicas pode ser resumido como segue:

Para a n-ésima mensagem $m \in M$, Alice gera uma etiqueta dada por $a(m,n) = h(n) \oplus x_0(n)$ de k bits. Em seguida vem a parte quântica do protocolo.

Considere que Alice e Bob combinem de usar duas bases ortonormais para o espaço de Hilbert de dimensão dois,

$$Z = \{|0\rangle, |1\rangle\} \tag{4.2}$$

$$X = \{|+\rangle, |-\rangle\}, \tag{4.3}$$

em que

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ e } |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{4.4}$$

Estas são as mesmas bases ortonormais usadas para criar os quatro estados quânticos no protocolo BB84 (C.; G.; EKERT, 1992). Para cada bit de $a(m,n)$, Alice prepara um estado quântico não emaranhado $\left|\Psi_{n_j}\right\rangle$, que é baseado no bit correspondente emitido pelo gerador BBS com semente y_o. Dessa forma, se o j-ésimo bit de $y_o(n)$ é zero, Alice prepara $\left|\Psi_{n_j}\right\rangle$ usando a base Z da seguinte maneira:

$$\left|\Psi_{n_j}\right\rangle = \begin{cases} |0\rangle & \text{se o } j-\acute{e}simo \text{ bit de } a(m,n) \text{ é } 0 \\ |1\rangle & \text{se o } j-\acute{e}simo \text{ bit de } a(m,n) \text{ é } 1 \end{cases} \tag{4.5}$$

Analogamente, se o j-ésimo bit de $y_o(n)$ é 1, Alice prepara $\left|\psi_{n_j}\right\rangle$ usando a base X, em que

$$\left|\psi_{n_j}\right\rangle = \begin{cases} |+\rangle & \text{se o } j-\acute{e}simo \text{ bit de } a(m,n) \text{ é } 0 \\ |-\rangle & \text{se o } j-\acute{e}simo \text{ bit de } a(m,n) \text{ é } 1 \end{cases} \tag{4.6}$$

Após a geração dos qubits, Alice envia o estado $\left|\psi_{n_j}\right\rangle^{\otimes k}$ para Bob usando um canal quântico sem ruído. A mensagem m pode ser enviada usando um canal inseguro, seja ele clássico ou quântico.

Na recepção, Bob realiza medições POVMs nas bases Z e X, definidas pelos seguintes conjuntos

$$E_Z = \{E_o = |0\rangle\langle 0|, E_1 = |1\rangle\langle 1|\} \tag{4.7}$$

$$E_X = \{E_+ = |+\rangle\langle +|, E_- = |-\rangle\langle -|\}. \tag{4.8}$$

Para o j-ésimo qubit $\left|\psi_{n_j}\right\rangle$ recebido, Bob realiza uma medição usando o conjunto E_Z ou E_X, dependendo se o j-ésimo bit de $y_o(n)$ é 0 ou 1, respectivamente. Dessa forma, Bob considera que o j-ésimo bit da etiqueta de Alice é 0 quando ele obtém as saídas E_o ou E_+. Se a saída for E_1 ou E_-, Bob considera que o bit j de $a(m,n)$ é 1. Ao final de k medições, Bob dispõe de uma seqüência $a_B(m,n)$ de k bits clássicos. Além disso, Bob dispõe também da mensagem recebida, denotada por m_B que pode estar modificada ou não.

O próximo passo de Bob é calcular uma etiqueta local baseado na função *hash* e na seqüência gerada pela semente x_o, obtendo $a'_B(m,n) = h(m_B) \oplus x_o(n)$. Como o canal quântico é perfeito, Bob considera que a mensagem é autêntica se $a_B(m,n) = a'_B(m,n)$. Caso contrário, ele descarta a mensagem recebida. Este esquema é ilustrado na Figura 4.1.

A afirmação acima pode ser feita porque no caso em que Eva não interfere na transmissão quântica da etiqueta, Bob obterá na medição a mesma etiqueta enviada por Alice, ou seja, $a_B(m,n) = a(m,n)$. Isto porque o gerador cuja semente é y_o indica em qual das bases Alice deve criar os qubits, ao mesmo tempo em que diz a Bob qual dos conjuntos

POVMs ele deve escolher para medi-los. Se a medição é feita sempre na mesma base em que os qubits são criados, Bob sempre interpreta corretamente o bit enviado por Alice.

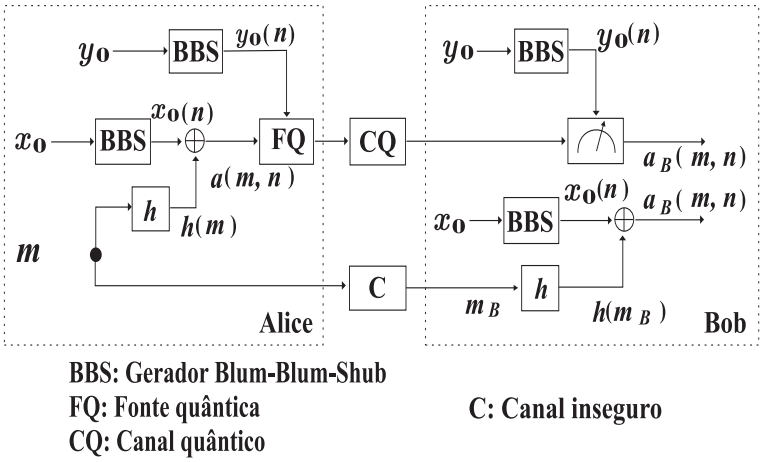

Figura 4.1: Diagrama em blocos do esquema proposto usando o BBS

4.1.1 Resumo do protocolo

- Alice e Bob compartilham a mesma chave secreta (x_0, y_0, h).
- Para a n-ésima mensagem $m \in M$ a ser enviada, Alice prepara uma etiqueta $a(m, n)$ de k bits, dada pela equação:

$$a_B(m, n) = h(m_B) \oplus x_o(n) \tag{4.9}$$

- Alice cria k qubits nas bases Z ou X, dependendo da etiqueta $a(m, n)$ e da seqüência $y_o(n)$. Ela envia os qubits através de um canal quântico perfeito
- Bob escolhe as bases (conjuntos POVMs) usadas na medição de acordo com a seqüência pseudo-aleatória $y_o(n)$.
- Bob calcula uma etiqueta local $a'_B(m, n)$ baseado na fun ção *hash* e na seqüência gerada pela semente x_o , que é comparada com a etiqueta $a_B(m, n)$. Como o canal quântico é perfeito e se as etiquetas forem identicas, Bob considera que a mensagem é autêntica . Caso contrário, ele descarta a mensagem recebida

4.1.2 Exemplo do uso do protocolo

Considera-se que Alice e Bob compartilham uma chave secreta composta por : (x_0 , y_0, h).

- Considere ainda que as mensagens são de comprimento 32 *bits*, e as etiquetas de comprimento 8;
- Alice deseja enviar a mensagem $n = 1$ dada por $m = FA\ 16\ AB\ C8$ (em hexadecimal);
- a função h mapeia (secretamente) $h(m) = 10011010$;
- o gerador BBS fornece $x_0(1) = 11101001$ e $y_0(1)$=11001100.
- Tanto Alice quanto Bob são capazes de gerar as seqüências $x_0(1)$ e $y_0(1)$.
- Inicialmente, Alice cria a etiqueta, fazendo uma operação ou-exclusivo entre $h(m)$ e $x_0(1)$:
- $a(m, n) = (10011010) \oplus (11101001) = 01110011$.

- Alice então usa os bits de $a(m, 1)$, em conjunto com os bits de $y_0(1)$, para criar os qubits a serem enviados pelo canal quântico

Alice → Bob

$y_0(1)$	1	1	0	0	1	1	0	0
$Bases$	X	X	Z	Z	X	X	Z	Z
$a(m,1)$	0	1	1	1	0	1	1	1
$\lvert\psi_{n_j}\rangle^{\otimes 8}$	$\lvert+\rangle$	$\lvert-\rangle$	$\lvert 1\rangle$	$\lvert 1\rangle$	$\lvert+\rangle$	$\lvert-\rangle$	$\lvert 1\rangle$	$\lvert 1\rangle$

Na recepção, Bob usa a sequência para decidir em que base ele deve fazer a medição de cada qubit

$y_0(1)$	1	1	0	0	1	1	0	0
$POVM$	E_X	E_X	E_Z	E_Z	E_X	E_X	E_Z	E_Z
$\lvert\psi_{n_j}\rangle^{\otimes 8}$	$\lvert+\rangle$	$\lvert-\rangle$	$\lvert 1\rangle$	$\lvert 1\rangle$	$\lvert+\rangle$	$\lvert-\rangle$	$\lvert 1\rangle$	$\lvert 1\rangle$

Um cálculo simples mostra que, neste caso, Bob obterá na medição a seqüência binária $a\,(m, n)$ =0111 0111. Para ver isso, considere as medições do primeiro e do segundo qubit, $|\psi_{i_1}\rangle$e $|\psi_{i_2}\rangle$, respectivamente.

Na medição do primeiro qubit, usando o $POVM$, Bob tem as seguintes probabilidades de medição:

$$p(E_+) = tr(E_+ |+\rangle \langle +|) = tr\left(\tfrac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\tfrac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\right) = 1$$

$$p(E_+) = tr(E_- |+\rangle \langle +|) = tr\left(\tfrac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}\tfrac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\right) = 0$$

Isto significa que Bob irá obter na medição com probabilidade máxima. Logo ele interpreta que o primeiro bit da etiqueta enviada por Alice é 0.

Analogamente, para o segundo qubit e usando a mesma base, Bob terá as seguintes probabilidades de leitura:

$$p(E_+) = tr(E_+ |-\rangle \langle -|) = tr\left(\tfrac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\tfrac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}\right) = 0$$

$$p(E_-) = tr(E_- |-\rangle \langle -|) = tr\left(\tfrac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}\tfrac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}\right) = 1$$

Pela sistemática adotada, Bob conclui que o segundo bit da etiqueta de Alice é 1. Após 8 medições, Bob obtém a seqüência $a_B(m,1) = 01110011$.

O próximo passo é criar uma etiqueta local $a_B^{'}(m,1)$, baseada na mensagem recebida m_B e na seqüência $x_0(1)$ que é gerada localmente. Considerando-se que a mensagem não foi modificada, tem-se que

$a_B^{'}(m,1) = 01110011$

Por último, Bob testa se a etiqueta enviada por Alice pelo canal quântico, $a_B(m,1)$, é igual a etiqueta gerada a partir da mensagem recebida, $a_B^{'}(m,1)$. Neste caso, tem-se que $a_B(m,1) = a_B^{'}(m,1)$ e Bob conclui que a mensagem é autêntica.

4.2 Demonstração da Segurança do Protocolo quando é usado o BBS (Ataques de Medição).

Está claro nesse ponto que a segurança do esquema proposto depende da segurança do gerador BBS. É investigado como Eva faz uso de recursos quânticos para predizer tal gerador. Neste trabalho, é provado o resultado seguinte relativo ao BBS, em que os parâmetros, p e q são números primos tais que $p \equiv q \equiv 3 \ mod\ 4$, e x_o é uma semente secreta escolhida de Z_n^*, tendo representação de l bits.

Lema 11 *Sejam $b_{i+1},...,b_{i+k}$ uma seqüência de bits da seqüência gerada pelo PRBG-BBS. O melhor algoritmo probabilístico $A_{BBS}(p, q,\ b_{i+1},...,b_{i+k})$ para predizer uma seqüência inteira para trás (e para frente) precisa de pelo menos $k = l$ bits para que*

$$Prob[A_{BBS}((p, q, b_{i+1}, ..., b_{i+k}) = b_i] = 1 \tag{4.10}$$

Prova: O lema é provado observando que o problema é equivalente ao problema de calcular o bit de paridade, que por sua vez pode ser reduzido ao problema de encontrar a raiz quadrada módulo N(SIDORENKO; SHOENMARKERS, 2005).

Seja então $A_{RQ}(p, q, x_{i+1})$, o algoritmo capaz de resolver a raiz quadrada de $x_i \; modN$ em que $b_i = paridade(x_i)$ em um computador quântico.

O resultado segue por contradição. Suponha que tal algoritmo $A_{BBS}(.,.)$ exista. Então deve existir uma função $f(b_{i+1}, ..., b_{i+k})$ tal que

$$x_{i+1} = f(b_{i+1}, ..., b_{i+k}), k < l \tag{4.11}$$

e

$$x_i = A_{RQ}(p, q, x_{i+1}) \tag{4.12}$$

$$b_i = paridade(x_i) \tag{4.13}$$

Mas tal função não existe, pois, a cardinalidade do domínio é (2^k) é menor que a cardinalidade do contradomínio que é (2^l), o que é uma contradição.

A seguir são apresentados algumas justificativas para a segurança do protocolo aqui descrito.

4.3 A presença de Eva no canal quântico

O problema de se tratar matemáticamente os ataques realizados por Eva, de uma forma geral, é extremamamente complicado. Normalmente, algumas premissas são tomadas para realizar a análise. É rapidamente entendido que embora os sistemas físicos sejam desprovidos de falhas, o protocolo ora proposto é absolutamente seguro, dado que ele é baseado nas leis da mecânica quântica que com a prova feita, com Eva fazendo ataques de medição, não apresenta falhas.

Para o caso de sistemas reais que possuem falhas, a situação não é tão simples e a prova de segurança é extremamente complexa.

Apesar de parecer absurdo, em alguns casos será assumido que Eva tem acesso à tecnologia ainda inexistente. Por exemplo, o computador quântico, sendo na verdade somente limitada pelas leis da mecância quântica. Existem dois tipos de ataques, os incoerentes ou individuais e os coerentes.

Os ataques incoerentes podem ser realizados com a tecnologia atual, isto é, Eva utiliza os mesmos equipamentos que Alice e Bob. Para os ataques coerentes e PNS(do inglês *photon number splitting*-divisão do número de fótons) é necessário que Eva tenha acesso a um computador quântico e memória quântica.

Neste momento são analisados ambos os casos.

A segurança do protocolo será verificada para duas situações (tipos de ataques) que registram a presença de Eva no canal quântico:

1. Eva não tem o computador quântico.
2. Eva tem o computador quântico.

4.3.1 Eva não tem o computador quântico (ataques incoerentes)

Os Ataques incoerente são os ataques mais simples e a idéia é que Eva intercepte os fótons individualmente, meça-os numa base escolhida aleatoriamente entre as duas preparadas por Alice e retransmita os fótons para Bob de acordo com o resultado obtido por ela. Nesse caso mais simples, e assumindo que os fótons enviados por Alice no canal quântico, ela obtém 0.5 bit de informação para cada bit na *sifted key* e infere uma taxa de erro realística da chave filtrada (QBER) de 25% (GISIN; RIBORDY; ZBINDEN, 2001).

Pulsos contendo mais de um fóton não estão mais incluídos nessa primeira análise. Na realidade, para uma QBER próxima de 25% conseguimos detectar a presença de Eva, mas será possível tornar a chave segura utilizando os procedimentos clássicos de correção de erro e amplificação da privacidade? A resposta é não. Para que isso seja possível a QBER na verdade tem que ser menor do que aproximadamente 15% (GISIN; RIBORDY; ZBINDEN, 2001). Caso isso não ocorra, eles sabem que Eva está presente mas não podem utilizar a chave pois não conseguirão torná-la segura. Nesse caso eles possuem três opções em teoria: tentam uma nova transmissão (em princípio eles não sabem se a QBER elevada é devido a Eva ou alguma perda no sistema devido a efeitos adversos), tentam outro canal ou recorrem a algoritmos quânticos para amplificação da privacidade e correção de erro, requerendo um computador quântico, indisponível num futuro próximo.

Uma falha de segurança grave corresponde à existência de pulsos contendo multi-fótons abrindo caminho para ataques PNS. Nesse tipo de ataque, Eva mede todos os pulsos que Alice envia pelo canal quântico. Todos os pulsos que contêm um fóton são bloqueados por Eva. Para os pulsos contendo dois fótons ou mais ela guarda um para si enquanto envia o outro para Bob sem nenhuma perturbação. Note que Bob não tem como saber quantos fótons o pulso continha na saída de Alice. É verdade que Bob pode notar uma diminuição na taxa de bits que irão formar a chave secreta (R_{raw}) de *qubits* que ele recebe, afinal todos os bits que contém 1 fóton (em geral a maioria) está sendo bloqueada por Eva.

Para evitar isso, ela tem que substituir o canal que liga a Bob por um mais transparente, ou seja com menos perdas. Felizmente para nós Eva está com um grande problema nas mãos. Como diminuir as perdas do canal se as atuais fibras ópticas já estão próximas do limite mínimo para atenuação dada pelo espalhamento Rayleigh? A primeira saída seria Eva utilizar um canal mais curto possível. A outra saída é teleportação, pois com isso as perdas do canal passariam a zero (assumindo teleportação perfeita), já que o *qubit* seria transportado através através de um canal clássico. Assumindo então que Eva conseguiu a façanha de adquirir um canal mais transparente, Bob não irá detectar a sua presença. Assumindo BB84 e caso ela tenha acesso a um meio de guardar os *qubits* indefinidamente (salvar os *qubits* em uma memória quântica ou utilizar um *loop* de fibra sem perdas), ela pode simplesmente esperar a reconciliação de bases para assim realizar as medidas em seus *qubits* de forma determinística.

Devido aos ataques PNS, é muito importante para a segurança dos sistemas de QKD que o valor médio μ de fótons por pulso seja menor do que 1 (ao se utilizar fontes poissonianas). Quanto menor for μ, mais pulsos Eva será obrigada a bloquear e conseqüentemente, mais difícil será mascarar a sua presença.

Uma outra situação de ataque é denominado: Ataque de pulsos de um único fóton, concluindo que a melhor medida que Eva pode realizar é usar a base de Breibard (NIELSEN et al., 2001), dada por:

$$|\varphi_1\rangle = \cos(\pi/8)\,|0\rangle + sen(\pi/8)\,|1\rangle \tag{4.14}$$

$$|\varphi_2\rangle = sen(\pi/8)\,|0\rangle + \cos(\pi/8)\,|1\rangle \tag{4.15}$$

Isso dá uma suposição ao bit enviado por Alice que está correto com probabilidade $p = \cos^2(\pi/8) \approx 0,85$, e conduz a uma taxa de erro para Bob de pelo menos $0,25$. Chamaremos isto de "Ataque único de interceptação e reenvio".

4.3.2 Eva tem o computador quântico (Ataques coerentes)

Neste momento, são destacadas situações possíveis da presença de Eva no canal quântico de posse do computador quântico.

Esse tipo de ataque é subdividido em dois tipos: ataques conjuntos (*joint attacks*), em que Eva mede e processa vários *qubits* de forma coerente simultaneamente; ataques coletivos (*collective attacks*), em que Eva acopla sondas (*probes*) em *qubits* individuais como nos ataques incoerentes, mas processa todas essas sondas de forma simultânea como nos ataques coerentes.

Para ambos os ataques coerentes o procedimento é usualmente o mesmo: Eva espera que o processo de reconciliação termine para medir as sondas cuidadosamente armazenadas em uma memória quântica. Os ataques coerentes também introduzem erros no sistema. No entanto, o limite de *QBER* para que ainda seja possível realizar correção de erro e amplificação da privacidade clássicos cai para 11% (GISIN; RIBORDY; ZBINDEN, 2001).

Capítulo 5

Conclusões e propostas para trabalhos futuros

Este trabalho abordou a questão da autenticação quântica de mensagens clássicas, usando o gerador de sequências pseudo-aleatório BBS.

É extremamente relevante, em questões de segurança, ter a certeza de que qualquer escuta indevida sobre o canal de comunicação seja imediatamente identificada pelas partes. No caso da criptografia quântica, isso pode ser feito por meio de medições estatísticas no nível quântico ou por outras alternativas não mencionadas neste trabalho.

Na abordagem deste trabalho, foi visto que o protocolo de autenticação quântica de mensagens clássicas, usando o gerador de sequências pseudo-aleatório BBS, utiliza a transmissão de uma etiqueta, de forma que Eva não consegue distinguir a seqüência falsa de uma seqüência verdadeiramente aleatória. Nos ataques de medições foi apresentado uma prova para sua segurança.

No protocolo ora mencionado neste trabalho, observou-se ainda que se Eva tiver ou não o computador quântico, ainda assim o protocolo apresenta uma alta segurança computacional.

5.1 Trabalhos futuros

Como proposta para trabalhos futuros, apresenta-se o seguinte problema: fazer uma análise sobre ataques coletivos e uma maior precisão na prova de segurança diante da disponibilidade de computação quântica.

Uma busca por outros geradores mais eficientes para assegurar uma segurança computacional eficaz, mesmo na presença dos computadores quânticos.

Referências Bibliográficas

ALBRECHT, B. Cryptology. *Washington D. C.: Mathematical Association of America*, p. 12, 1994.

BALPARDA, C. D. *Segurança de dados com criptografia: métodos e algoritmos*. [S.l.]: Editora Book Express, 2001. 230 p. ISBN 85-868-4691-0.

BARNUM, H. et al. Authentication of quantum messages. *43RD ANNUAL IEEE SYMPOSIUM ON THE FOUNDATIONS OF COMPUTER S 02 449 (2002)*, p. 20, 2002.

BELLARE, M.; GOLDWASSER, M. F. e S.; MICALI, S. Identification protocols secure against rese attacks. *Eurocrypt*, p. 34, 2001.

BENNETT, C. H. et al. Experimental quantum cryptography. *Journal of Cryptology*, p. 35, 1992.

BENNETT, C. H.; BRASSARD, G. Quantum cryptography: public-key distribution and coin tossing. *In procedings of IEEE international conference on Computers, systems, and Signal Procecssing, Bangalore*, p. 175–179, 1984.

BIHAM, E.; BOYER, M. A proof of the security of quantum key distribution. *arXiv.org:quant-ph/0107017*, p. 55, 2001.

BLUM, L.; BLUM, M.; SHUB, M. Comparison of two pseudo-random number generators. *Proc. CRYPTO 82*, p. 25, 1983.

BLUM, L.; BLUM, M.; SHUB, M. Cryptographic secure pseudo-random bits generation: The blum-blum-shub generator. *SIAM J. Comput.*, p. 35, 1999.

BURNETT, S.; PAINE, S. *Criptografia e seguranca: o guia oficial*. [S.l.]: Editora Record, 2002. 367 p. ISBN 85-352-1009-1.

C., B.; G., B.; EKERT. Quantum cryptography. *Scientific American*, p. 41, 1992.

CANETTI, R.; GOLDWASSER, S.; MICALI, S. Resetable zero-knowledge. *STOC*, p. 21, 2000.

CARTER, J.; WEGMAN, M. N. New hash functions and their use in authentication and set equality. *J. Comput. Syst*, p. 10, 1979.

CERTICON. Current public-key cryptographic systems. *www.certicom.com*, p. 125, 1997.

CERTICON. Remarks on the security of the elliptic curve cryptosystem. *www.certicom.com*, p. 21, 1997.

CURTY, M.; SANTOS, D. J. Quantum authentication of classical messages. *Phys. Rev. A*, p. 23, 2001.

CURTY, M.; SANTOS, D. J.; PERE, E. Qubit authentication. *Phys. Rev. A*, p. 18, 2002.

DAVID, N. E. encyclopedia of cryptology. *Santa Barbara, CA: ABC-Clio*, p. 20, 1997.

GISIN, N.; RIBORDY, G.; ZBINDEN, H. Quantum cryptography. *Reviews of Modern Physics*, p. 20, 2001.

H., C.; H, L. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, p. 2050–2056, 1999.

HOLSCHUH, H. Pgp. *http://www.dca.fee.unicamp.br/pgp/*, n. 32, 2003.

JUNOD, P. Cryptographic secure pseudo-random bits generation: The blum-blum-shub generator. *url = "http://www.citeseer.ist.psu.edu/junod99cryptographic.html*, p. 16, 1999.

LABORATORIES, R. Frequently asked questions about today's cryptography. *Rsa Security Inc*, p. 20, 2000.

M.BLUM; MICALI, S. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM J. Comput.*, p. 30, 1984.

MEDEIROS, R. A. Protocolo para autenticação quântica de mensagens clássicas. *Dissertação de mestrado-UFCG*, p. 90, 2004.

NIELSEN, M. A.; CHUANG, I. L. *Computação Quântica e Informação Quântica*. 1. ed. [S.l.]: 03 / 07 / 2005, 2005. ISBN 8536305541.

NIELSEN, P. et al. Experimental quantum key distribution with proven security against realistic attacks. *Institute of Physics and Astronomy, University of Aarhus*, p. 29, 2001.

OLIVEIRA, A. G. Criptografia usando protocolos quânticos. *Universidade Federal de Lavras*, p. 36, 2004.

RIVEST, R. The md4 message digest algorithm. *RFC 1320, MIT and RSA Data Security*, p. 45, 1992.

S., K. Privacy enhancement for internet electronic mail. *RFC 1422*, p. 31, 1993.

SALOMAA, A. Public-key cryptography. *Springer-Verlag*, p. 21, 1996.

SIDORENKO, A.; SCHOENMAKERS, B. State recovery attacks on pseudorandom generators. *10th IMA International Conference*, p. 32, 2005.

SIDORENKO, A.; SHOENMARKERS, B. Concrete security of the blum-blum-shub pseudorandom generator. *10th IMA International Conference*, p. 17, 2005.

SIMON, S. *O livro dos codigos*. [S.l.]: Editora Record, 2001. 512 p. ISBN 8501055980.

STALLINGS, W. *Cryptography and Network Security*. [S.l.]: Prentice Hall; 4 edition, 2005. 592 p. ISBN 0131873164.

STINSON, D. R. Cryptography: Theory and pratice. *CRC Press*, 1995.

WEGMAN, M.; CARTER, J. New hash functions and their use in authentication and set equality. *J. comput. Syst*, p. 30, 1981.