RAFAEL TRAPANI POSSIGNOLO

**PROJETO DE UM COPROCESSADOR QUÂNTICO
PARA OTIMIZAÇÃO DE ALGORITMOS
CRIPTOGRÁFICOS**

Dissertação apresentada à Escola Politécnica
da Universidade de São Paulo para obtenção
do Título de Mestre em Ciências.

São Paulo
2012

RAFAEL TRAPANI POSSIGNOLO

**PROJETO DE UM COPROCESSADOR QUÂNTICO
PARA OTIMIZAÇÃO DE ALGORITMOS
CRIPTOGRÁFICOS**

Dissertação apresentada à Escola Politécnica
da Universidade de São Paulo para obtenção
do Título de Mestre em Ciências.

Área de Concentração:

Sistemas Digitais

Programa de Engenharia Elétrica

Orientador:

Prof.^a Dr.^a Cíntia Borges Margi

São Paulo
2012

Este exemplar foi revisado e alterado em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, 29 de agosto de 2012.

Assinatura do autor

Assinatura do orientador

FICHA CATALOGRÁFICA

Possignolo, Rafael Trapani

Projeto de um coprocessador quântico para otimização de algoritmos criptográficos/ R. T. Possignolo. – ed. rev. – São Paulo, 2012.
124 p.

Dissertação (Mestrado) — Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Computação e Sistemas Digitais.

1. Computação Quântica 2. Arquitetura e organização de computadores 3. Criptologia I. Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Computação e Sistemas Digitais II. t.

“Se você acha que entendeu alguma coisa sobre mecânica quântica, então você não entendeu nada.”

Richard Feynman

AGRADECIMENTOS

Agradeço inicialmente à minha orientadora, Prof.^a Cíntia Margi, por ter acreditado em meu potencial e ter aceito me orientar em um trabalho tão fora da sua área de atuação. Seus conselhos e ensinamentos foram, sem dúvida, essenciais para a realização deste trabalho. Seu empenho em buscar referências, se manter por dentro do trabalho e dar críticas a este foram fundamentais para a melhoria do trabalho. Sou especialmente grato pela abertura sempre existente para discutir qualquer assunto, desde pesquisa e ensino até àqueles não relacionados ao mestrado. Também não poderia deixar de citar toda a ajuda durante o processo seletivo para o doutorado, ou talvez devesse dizer, os processos seletivos, além é claro de todas as indicações e referências após minha aceitação. Espero ter correspondido a altura e ter preenchido as expectativas, no sentido intelectual e na dedicação.

Também agradeço ao Prof. Paulo Barreto, que desempenhou extra-oficialmente um papel de coorientação em meu trabalho. Agradeço inicialmente por ter indicado o tema e o problema a serem abordados. As discussões em diversos momentos ajudaram a sanar dúvidas e mostrar o caminho a ser seguido na execução deste trabalho.

Agradeço ao Laboratório de Arquitetura e Redes de Computadores, todos seus membros, e em especial ao Prof. Wilson Ruggiero, por ter me acolhido durante a realização do mestrado. Não apenas pelo apoio material recebido, mas especialmente pelo ótimo ambiente aqui encontrado. Hoje posso dizer que me sinto parte dessa grande família.

Gostaria de agradecer aos membros da banca Prof. José Roberto Piqueira e Dr. José Eduardo Moreira, que aceitaram participar de minha avaliação, agradeço por seus comentários que ajudaram a enriquecer este trabalho e diminuir suas falhas. Também, agradeço ao Prof. Carlos Molina Mendes pela revisão e pelos comentários que foram de grande utilidade para a melhora deste manuscrito.

Adicionalmente, gostaria de agradecer ao membros do SEMBEI, grupo de pesquisa do qual tenho a honra de fazer parte. Cada um dos membros contribuiu de alguma forma na realização deste trabalho, com cada um aprendi um pouco a ser um melhor pesquisador e uma melhor pessoa. Agradeço pelo agradável convívio que tivemos ao longo deste tempo e espero sinceramente que esta amizade ainda se mantenha por muito tempo.

Finalmente, agradeço a minha família, em especial meus pais, Luiz e Bernadete, meu irmão, André, e minha noiva, Gisele, por estarem presentes em cada dificuldade, por me motivarem quando as dificuldades apareceram e por entenderem as noites em claro e os momentos de ausência familiar tão comuns na vida de um estudante/pesquisador. Devo o que sou à presença destes em minha vida. Agradeço também é claro, aos tios e primos que sempre estiveram na torcida e com quem compartilho momentos únicos, o que torna as dificuldades da vida menos significantes.

RESUMO

A descoberta do algoritmo de Shor, para a fatoração de inteiros em tempo polinomial, motivou esforços rumo a implementação de um computador quântico. Ele é capaz de quebrar os principais criptossistemas de chave pública usados hoje (RSA e baseados em curvas elípticas). Estes fornecem diversos serviços de segurança, tais como confidencialidade e integridade dos dados e autenticação da fonte, além de possibilitar a distribuição de uma chave simétrica de sessão.

Para quebrar estes criptossistemas, um computador quântico grande (≈ 2000 *qubits*) é necessário. Todavia, alternativas começaram a ser investigadas. As primeiras respostas vieram da própria mecânica quântica. Apesar das propriedades interessantes encontradas na criptografia quântica, um criptossistema completo parece inatingível, principalmente devido as assinaturas digitais, essenciais para a autenticação.

Foram então propostos criptossistemas baseadas em problemas puramente clássicos que (acredita-se) não são tratáveis por computadores quânticos, que são chamadas de pós-quânticas. Estes sistemas ainda sofrem da falta de praticidade, seja devido ao tamanho das chaves ou ao tempo de processamento. Dentre os criptossistemas pós-quânticos, destacam-se o McEliece e o Niederreiter. Por si só, nenhum deles prevê assinaturas digitais, no entanto, as assinaturas CFS foram propostas, complementando-os.

Ainda que computadores quânticos de propósito geral estejam longe de nossa realidade, é possível imaginar um circuito quântico pequeno e dedicado. A melhoria trazida por ele seria a diferença necessária para tornar essas assinaturas práticas em um cenário legitimamente pós-quântico.

Neste trabalho, uma arquitetura híbrida quântica/clássica é proposta para acelerar algoritmos criptográficos pós-quânticos. Dois coprocessadores quânticos, implementando a busca de Grover, são propostos: um para auxiliar o processo de decodificação de códigos de Goppa, no contexto do criptossistema McEliece; outro para auxiliar na busca por síndromes decodificáveis, no contexto das assinaturas CFS.

Os resultados mostram que em alguns casos, o uso de um coprocessador quântico permite ganhos de até 99,7% no tamanho da chave e até 76,2% em tempo de processamento. Por se tratar de um circuito específico, realizando uma função bem específica, é possível manter um tamanho compacto (≈ 300 *qubits*, dependendo do que é acelerado), mostrando adicionalmente que, caso computadores quânticos venham a existir, eles viabilizarão os criptossistemas pós-quânticos antes de quebrar os criptossistemas pré-quânticos.

Adicionalmente, algumas tecnologias de implementação de computadores quânticos são estudadas, com especial enfoque na óptica linear e nas tecnologias baseadas em silício. Este estudo busca avaliar a viabilidade destas tecnologias como potenciais candidatas à construção de um computador quântico completo e de caráter pessoal.

ABSTRACT

The discovery of the Shor algorithm, which allows polynomial time factoring of integers, motivated efforts towards the implementation of a quantum computer. It is capable of breaking the main current public key cryptosystems used today (RSA and those based on elliptic curves). Those provide a set of security services, such as data confidentiality and integrity and source authentication, and also the distribution of a symmetric session key.

To break those cryptosystem, a large quantum computer (≈ 2000 *qubits*) is needed. Nevertheless, cryptographers have started to look for alternatives. Some of which came from quantum mechanics itself. Despite some interesting properties found on quantum cryptography, a complete cryptosystem seems intangible, specially because of digital signatures, necessary to achieve authentication.

Cryptosystems based on purely classical problems which are (believed) not treatable by quantum computers, called post-quantum, have them been proposed. Those systems still lacks of practicality, either because of the key size or the processing time. Among those post-quantum cryptosystems, specially the code based ones, the highlights are the McEliece and the Niederreiter cryptosystems. Per se, none of these provides digital signatures, but, the CFS signatures have been proposed, as a complement to them.

Even if general purpose quantum computers are still far from our reality, it is possible to imagine a small dedicated quantum circuit. The benefits brought by it could make the difference to allow those signatures, in a truly post-quantum scenario.

In this work, a quantum/classical hybrid architecture is proposed to accelerate post-quantum cryptographic algorithms. Two quantum coprocessors, implementing the Grover search, are proposed: one to assist the decoding process of Goppa codes, in the context of the McEliece and Niederreiter cryptosystems; another to assist the search for decodable syndromes, in the context of the CFS digital signatures.

The results show that, for some cases, the use of the quantum coprocessor allows up to 99,7% reduction in the key size and up to 76,2% acceleration in the processing time. As a specific circuit, dealing with a well defined function, it is possible to keep a small size (≈ 300 *qubits*), depending on what is accelerated), showing that, if quantum computers come to existence, they will make post-quantum cryptosystems practical before breaking the current cryptosystems.

Additionally, some implementation technologies of quantum computers are studied, in particular linear optics and silicon based technologies. This study aims to evaluate the feasibility of those technologies as potential candidates to the construction of a complete and personal quantum computer.

SUMÁRIO

Lista de Ilustrações

Lista de Tabelas

Lista de Abreviaturas e Siglas

1	Introdução	12
1.1	Justificativa	16
1.2	Objetivos	17
1.3	Métodos e Métricas	18
1.4	Contribuições Originais	19
1.5	Organização	20
2	Conceitos Preliminares	21
2.1	Complexidade Computacional	21
2.2	Aritmética em Corpos Finitos	22
2.3	Álgebra Linear	25
2.4	Sumário do Capítulo 2	29
3	Da Mecânica à Computação Quântica	30
3.1	Formulação de Dirac	30
3.2	Bases da Teoria Quântica	32

3.2.1	Superposição	33
3.2.2	Evolução Temporal	34
3.2.3	Medições	36
3.2.4	Sistemas Compostos e Emaranhado	37
3.3	Computação Quântica	38
3.3.1	Operadores Quânticos	39
3.3.2	Busca de Grover	42
3.4	Implementações Físicas de Computadores Quânticos	45
3.4.1	Requisitos Básicos para Computadores Quânticos	46
3.4.2	Tecnologias de Estado Sólido	48
3.4.2.1	Computação Quântica Baseada em Pontos Quânticos	48
3.4.2.2	Qubits Supercondutores com Junção de Josephson .	49
3.4.3	Óptica Linear	50
3.4.4	Ressonância Magnética Nuclear	51
3.4.5	Armadilhas de Íon	52
3.4.6	Outras Tecnologias	52
3.4.7	Tempo de decoerência e frequência de operação de diferentes tecnologias	53
3.5	Sumário do Capítulo 3	54
4	Criptografia Pós-Quântica	55
4.1	Introdução à Segurança da Informação	55

4.2	Criptografia Assimétrica	57
4.3	Motivação da Criptografia Pós-Quântica	59
4.4	Códigos Corretores de Erros	60
4.5	Criptossistemas McEliece e Niederreiter	62
4.6	Códigos de Goppa	63
4.6.1	Códigos de Goppa Quase-Diádicos	65
4.7	Assinaturas CFS	67
4.7.1	Assinaturas CFS Paralelas	68
4.8	Sumário do Capítulo 4	71
5	Assinaturas CFS Paralelas Assistidas por Computadores Quânticos	72
5.1	Oráculo para Encontrar Raízes de Polinômios	73
5.1.1	Resultados de Simulação	78
5.1.2	Resultados Obtidos e Análise	79
5.2	Oráculo para Decodificação de Síndromes	81
5.2.1	Aritmética em $\mathbb{F}_{p^m}$	83
5.2.2	Resultados Obtidos e Análise	89
5.3	Sumário do Capítulo 5	91
6	Arquitetura Híbrida	93
6.1	Trabalhos Relacionados	93
6.2	Coprocessador Quântico Implementando Grover	94
6.3	Implementação com Óptica Linear	97

6.4	Análise	99
6.5	Sumário do Capítulo 6	101
7	Análise de Tecnologias de Implementação de Computadores Quânticos	102
7.1	Requisitos para Computação Pessoal	103
7.1.1	Tamanho Físico Razoável	104
7.1.2	Baixo Custo de Energia	105
7.2	Análise das Tecnologias sob a Óptica da Computação Pessoal	105
7.3	Estudo de Viabilidade da Construção de Computadores Quânticos . .	109
7.3.1	Óptica Linear	109
7.3.2	Tecnologias Baseadas em Silício	110
7.3.3	Análise	111
7.4	Sumário do Capítulo 7	112
8	Considerações Finais	113
8.1	Trabalhos Futuros	114
8.2	Perspectivas do Campo	115
	Referências	116

LISTA DE ILUSTRAÇÕES

1	Operadores quânticos de um qubit.	40
2	Operadores quânticos de múltiplos qubits.	42
3	Operador de observação de um estado quântico.	42
4	Modelo de circuito da computação quântica para a busca de Grover. . .	44
5	Circuito quântico que verifica se X é raiz do polinômio $\sigma(X)$ em $\mathbb{F}_{2^4}$. .	77
6	Algoritmo quântico que calcula o polinômio localizador de erros. . . .	83
7	Circuito quântico que calcula $a \cdot b$ em $\mathbb{F}_{2^4}$	85
8	Circuito quântico que calcula a^{-1} em $\mathbb{F}_{2^4}$	87
9	Circuito quântico que calcula $\sqrt{a}$ em $\mathbb{F}_{2^4}$	88
10	Circuito quântico que calcula a^2 em $\mathbb{F}_{2^4}$	89
11	Arquitetura híbrida quântica/clássica.	96
12	Busca de Grover para encontrar raízes do polinômio σ	96
13	Implementação de busca de Grover em óptica linear.	99
14	A porta quântica CNOT implementada com óptica linear, conforme Okamoto (OKAMOTO <i>et al.</i> , 2005).	100
15	A porta Toffoli Sinal implementada por Ralph <i>et al.</i> (RALPH; RESCH; GILCHRIST, 2007).	100

LISTA DE TABELAS

1	Estimativas de tempo de decoerência (τ_Q), tempo de operação τ_{op} e número de operações $\eta_{op} = \lambda^{-1} = \tau_Q/\tau_{op}$ para alguns candidatos a qubits. A última coluna apresenta o número de operações estimado para cada tecnologia (NIELSEN; CHUANG, 2000).	54
2	Conjunto de parâmetros para CFS ((BARRETO <i>et al.</i> , 2010)).	68
3	Parâmetros para assinaturas CFS paralelas (BARRETO, 2011).	70
4	Resultado de simulação do oráculo pequeno. É exibido o número de acerto em 10 rodadas para cada $\sigma(X)$ possível para 1, 2, 3 e 4 ciclos de Grover.	78
5	Comparação da abordagem usando a busca de Grover contra o Micro-Eliece (EISENBARTH <i>et al.</i> , 2009).	80
6	Parâmetros para CFS Paralelo, com uso de computação quântica. . . .	90
7	Análise comparativa de três tecnologias de implementação de computadores quânticos.	106

LISTA DE ABREVIATURAS E SIGLAS

CCE	Criptografia baseada em Curvas Elípticas
CFS	Courtois-Finiasz-Sendrier - esquema de assinaturas digitais
CI	Circuito Integrado
DMA	Direct Memory Access (Acesso Direto à Memória) - esquema de transferência de dados para o processador
E/S	Entrada e Saída
GBA	Generalized Birthday Attack - ataque contra funções de hash criptográfico baseado no paradoxo generalizado do aniversário
GRS	Generalized Reed-Solomon code (código Reed-Solomon generalizado)
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
KiB	Kibibyte, 2^{10} bytes - unidade de informação IEC 60027-2
MiB	Mebibyte, 2^{20} bytes - unidade de informação IEC 60027-2
QD	Quase-Diádico
QKD	Quantum Key Distribution (Distribuição Quântica de Chaves)
RMN	Ressonância Magnética Nuclear
RSA	Rivest-Shamir-Adleman - criptossistema de chave pública
USP	Universidade de São Paulo
VLSI	Very-Large-Scale Integration - tecnologia de circuitos integrados com alta densidade

1 INTRODUÇÃO

Richard Feynman (1986) foi, provavelmente, o primeiro a sustentar a possibilidade de realizar computação com o uso da mecânica quântica. Desde então diversas hipóteses sobre como seria um computador quântico foram levantadas. Pode-se destacar o trabalho de David Deutsch (1985) que propôs uma extensão à famosa tese de Church-Turing sobre a computabilidade de funções, adequando-a a computadores quânticos.

Esse trabalho de David Deutsch foi um divisor de águas, na medida em que efetivamente sugeriu que computadores quânticos teriam um poder computacional maior que computadores não-quânticos (clássicos). Mais que isso, deixou claro que a capacidade computacional de uma máquina qualquer está intimamente ligada às leis da física, logo é plausível assumir que computadores baseados em teorias relativísticas ou mesmo em teoria das cordas tenham capacidade computacional diferente das presentes em computadores clássicos e quânticos, não necessariamente maiores.

No entanto, o impulso que realmente motivou a corrida por computadores quânticos partiu da publicação de dois algoritmos: o de Peter Shor (1994) para a fatoração de números inteiros e o de Lov Grover (1996) para busca em uma lista desordenada. Esses algoritmos foram os primeiros a trazer vantagens claras em problemas realmente interessantes sobre as contrapartes clássicas. Enquanto a busca de Grover permite a redução de complexidade de busca de tempo linear (busca exaustiva) para tempo subpolinomial ($O(\sqrt{N})$), a fatoração de Shor permite a redução de complexidade de ordem sub-exponencial para ordem polinomial. Ou seja, um problema tido como intratável

em computadores clássicos, passa a ter uma solução eficiente em computadores quânticos.

Benjamin Schumacher (1995) publicou estudos na área de informação quântica, fornecendo um análogo à teoria da informação desenvolvida por Claude Shannon (1956). Esse estudo na área de informação quântica possibilitou o entendimento de como conceitos da mecânica quântica se relacionam à teoria da informação e deu subsídios para a comunicação de informação quântica.

O otimismo com a computação quântica cresceu quando, em 2001, Isaac Chuang e alguns colaboradores (VANDERSYPEN *et al.*, 2001) relataram a execução com sucesso do algoritmo de Shor em um computador quântico baseado em Ressonância Magnética Nuclear (RMN).

Desde então, diversos mecanismos para a implementação física de computadores quânticos vem sendo propostos. Não existe ainda consenso sobre qual tecnologia será realmente usada, uma vez que cada uma delas ainda enfrenta diversos problemas para se viabilizar (DIVINCENZO, 2005).

Enquanto essas tecnologias não se viabilizam e um computador quântico em escala razoável não se torna real, alguns autores tem se dedicado a estudar novos algoritmos e o impacto daqueles já descobertos nas tecnologias existentes hoje. Um dos impactos mais citados é a quebra, pelo algoritmo de Shor, de sistemas criptográficos assimétricos atuais, como o RSA (RIVEST; SHAMIR; ADLEMAN, 1978) (nomeado após seus inventores Ronald Rivest, Adi Shamir e Leonard Adleman) e aqueles baseados em curvas elípticas (HANKERSON; MENEZES; VANSTONE, 2003).

Alternativas a esses criptossistemas passaram a ser buscadas desde então. A Distribuição Quântica de Chaves (BENNETT; BRASSARD, 1984) (QKD, em inglês) é um esquema para a transmissão de informação baseado em primitivas quânticas. As leis da física impossibilitam o “grampo” (escuta por uma terceira parte) de uma comunica-

ção desse tipo, de onde vem a segurança do mecanismo.

No entanto, esquemas baseados em mecânica quântica falharam em suprir outras necessidades básicas de segurança. É o caso das assinaturas digitais, que permitem a *autenticação* de um usuário, garantindo sua *irretratabilidade*. É sabido que uma assinatura digital puramente quântica não é possível (BARNUM *et al.*, 2002). Sem isso, em uma comunicação baseada no QKD é impossível saber (de fato) com quem se está trocando dados. Se a comunicação precisar de amparo jurídico, o problema se torna ainda mais complexo.

Face a esses problemas, criptógrafos criaram o conceito de criptografia pós-quântica (BERNSTEIN; BUCHMANN; DAHMEN, 2008), definida como criptografia clássica baseada em problemas computacionais que, acredita-se, não são resolvíveis eficientemente por computadores quânticos. Obviamente, não se sabe ao certo quais problemas matemáticos são tratáveis por computadores quânticos, logo o limite exato do que é pós-quântico é incerto.

Entre os algoritmos criptográficos pós-quânticos, pode-se identificar três classes (BERNSTEIN; BUCHMANN; DAHMEN, 2008): baseados em códigos corretores de erros, baseados em reticulados e baseados em sistemas multivariados quadráticos. Os sistemas baseados em códigos são os mais promissores para implementação prática de criptossistemas pós-quânticos. Entre eles podemos destacar os criptossistemas McEliece (MCELIECE, 1978) e Niederreiter (NIEDERREITER, 1986), ambos baseados na decodificação de síndromes.

Apesar de originalmente não existir a especificação de um código, os criptossistemas McEliece e Niederreiter tem sido tradicionalmente usados com códigos de Goppa (GOPPA, 1970). Em especial, códigos de Goppa Quase-Diádicos (QD) e Quase-Cíclicos (QC) vem sendo usados como forma de reduzir a chave criptográfica usada nesses criptossistemas (MISOCZKI; BARRETO, 2009).

Originalmente, McEliece e Niederreiter não apresentavam nenhum esquema de assinaturas digitais e, portanto, não seriam capazes de preencher os requisitos básicos de segurança. No entanto, recentemente foi proposto um esquema de assinaturas baseado no sistema Niederreiter. As assinaturas CFS (COURTOIS; FINIASZ; SENDRIER, 2001) (nomeadas após seus criadores) preenchem essa necessidade.

O grande problema ainda em aberto de criptossistemas pós-quânticos, em particular os baseados em códigos, é torná-los viáveis para uso prático. As soluções existentes variam entre chaves grandes ou tempos de processamento proibitivos, sendo chaves de 170 KiB ou tempos de processamento da ordem de 2^{50} passos computacionais para o nível de segurança de 80 (o mesmo nível pode ser obtido com 1024 bits e 2^{30} passos no RSA, no entanto o RSA pode ser quebrado em 2^{30} passos em um computador quântico) (BARRETO *et al.*, 2010). Diversos trabalhos vêm sendo feitos nesse caminho, mas uma solução final ainda inexiste.

É certo que esses criptossistemas pós-quânticos serão realmente necessários apenas caso computadores quânticos venham a existir, o que não quer dizer que não possam ser usados caso contrário. Dado o cenário da existência de computadores quânticos, é razoável assumir que esses computadores possam ser usados por um usuário legítimo para fins de criptografia. Em outras palavras, o computador quântico poderia auxiliar (e possivelmente acelerar) algoritmos criptográficos pós-quânticos (mas puramente clássicos do ponto de vista algorítmico).

O presente trabalho pretende analisar o impacto *positivo* do uso de primitivas quânticas em métodos criptográficos pós-quânticos. Em particular, nas assinaturas digitais CFS.

1.1 Justificativa

A busca por computadores quânticos é uma constante há algumas décadas. Essa busca se justifica principalmente na possibilidade de ganhos de capacidade computacional sobre os atuais computadores (DEUTSCH, 1985). No entanto, é importante destacar que mesmo antes de computadores quânticos perfeitamente funcionais existirem, já se pode observar diversos efeitos positivos das pesquisas nesta direção.

Alguns importantes resultados estão relacionados à área de complexidade computacional, onde novas classes de problemas foram criadas e sua relação com o espaço clássico da complexidade permitiu um melhor entendimento de como os problemas computacionais se organizam (WATROUS, 2008).

Em outra frente, a busca por computadores quânticos tem forçado físicos a desenvolver e testar novas tecnologia para a manipulação de estados quânticos. Com isso, novos resultados surgem e permitem a revisão, ou a confirmação de teorias para explicar o que se observa (CAVES; SCHUMAKER, 1985; SPEKKENS, 2007).

A criptografia é, provavelmente, o campo que mais irá mudar caso computadores quânticos de larga escala venham a existir. Por isso, a importância de pesquisas na direção de novos métodos criptográficos, resistentes a essa nova tecnologia (BERNSTEIN; BUCHMANN; DAHMEN, 2008).

Enquanto protocolos puramente quânticos são capazes de prover confidencialidade na comunicação, uma forma de prover autenticação de usuário é improvável (BARNUM *et al.*, 2002). Daí a necessidade de algoritmos clássicos para cumprir essa função, resistindo a ataques montados com computadores quânticos.

Tais algoritmos existem há algum tempo, no entanto, sua viabilidade prática ainda não foi atingida (MISOCZKI; BARRETO, 2009). Esse vem sendo o principal foco de pesquisa da criptografia pós-quântica. Uma possibilidade ainda não explorada nesse

cenário é o uso de tecnologias quânticas como forma de viabilizar esses algoritmos.

Essa abordagem é razoável se um cenário realmente pós-quântico for considerado. Além disso, os resultados encontrados até agora indicam que tal implementação necessitaria de um dispositivo quântico menor do que o necessário para a real quebra dos criptosistemas atuais, o que, se confirmado, indica que a transição seria possível mesmo antes de os sistemas atuais se tornarem obsoletos.

1.2 Objetivos

O principal objetivo do presente trabalho é um estudo de viabilidade sobre a construção física de computadores quânticos. Em especial busca-se analisar a possibilidade de implementação de um pequeno dispositivo capaz de realizar uma função previamente definida e delimitada. Para isso, escolheu-se uma tarefa simples, porém de aplicação prática clara.

A tarefa escolhida é a busca por síndromes decodificáveis em códigos de Goppa, etapa necessária para a implementação de assinaturas digitais CFS, baseadas no criptosistema McEliece. Foi escolhida a instância mais simples possível da tarefa, o que torna o código usado inseguro para aplicações criptográficas, mas serve como prova de conceito para a abordagem utilizada.

O algoritmo quântico de Grover será usado para a realização da tarefa apresentada, de forma que espera-se obter ganho de desempenho. A observância dos ganhos permite ao projetista de segurança modificar os parâmetros utilizados de forma a reduzir as chaves criptográficas.

O uso de técnicas de simulação permite verificar a funcionalidade da implementação. Além disso, possibilidades de implementação reais do algoritmo projetado devem ser levantadas, permitindo o estudo de viabilidade proposto.

1.3 Métodos e Métricas

Nesta seção, discute-se a metodologia adotada para a realização do projeto de pesquisa do mestrado e para alcançar os objetivos propostos, além das métricas usadas para avaliar os resultados obtidos.

Inicialmente uma revisão bibliográfica sobre computação quântica foi conduzida. Essa revisão teve por base livros texto sobre o assunto, tais quais o consagrado livro de Nielsen e Chuang (2000) e o mais atual por Colin Williams (2011). Essa revisão foi aprofundada através de artigos científicos em periódicos das diversas áreas que tangem a teoria quântica, entre eles pode-se destacar *Nature*, *Science*, *Physical Review A*, *B* e *Letters*, *Journal of Modern Physics*, *IEEE Transactions on Information Theory* e *on Computers*, além de conferências relevantes nessas áreas.

Em outra frente, uma revisão bibliográfica na área de criptografia, em especial baseada em códigos, foi realizada. Nesse caso as principais fontes foram conferências na área, destacam-se o *Crypto*, *Asiacrypt*, *Eurocrypt* e *PQCrypto*.

A partir desta análise, foi possível identificar problemas dentro da criptografia pós-quântica com potencial de melhoria com o uso de computadores quânticos. Nessa etapa boa parte do escopo final foi definido, uma vez que o problema a ser atacado impacta na maioria dos aspectos do projeto.

Além da definição do problema específico, optou-se por fixar os parâmetros utilizados, de forma a simplificar o projeto final, permitindo sua simulação e trazendo-o mais perto de uma possível implementação física.

A seguir uma solução para o problema, baseada em primitivas quânticas foi proposta, implementada em simulador e validada através de simulação. Paralelamente, um estudo sobre alternativas para a implementação física da solução proposta foi conduzido.

A definição de uma arquitetura computacional híbrida quântica/clássica, implementando a solução projetada como um coprocessador, foi proposta e analisada.

Finalmente os resultados obtidos, tanto do ponto de vista de desempenho, como do ponto de vista de custos, são analisados de acordo com 2 métricas principais: o número de *qubits* necessários para a implementação e o ganho em número de ciclos de processamento.

O número de *qubits* fornece uma noção da dificuldade de implementar o circuito proposto e implica no custo deste. Já o ganho em número de ciclos permite avaliar o desempenho da solução proposta. Esse ganho é calculado em relação ao estado da arte de técnicas pós-quânticas no momento da realização do trabalho.

1.4 Contribuições Originais

Os capítulos a seguir contém as contribuições deste trabalho:

- Capítulo 5 - avaliação do impacto do uso do algoritmo quântico de Grover nas assinaturas CFS e na decodificação de síndrome de Goppa - artigo “Quantum Assisted CFS signatures” submetido ao periódico “Quantum Information and Computation”;
- Capítulo 6 - proposta de uma arquitetura híbrida, usando um coprocessador quântico - artigo “A quantum/classical hybrid architecture for security algorithm optimization” publicado nos anais da “11th International IEEE Conference on Trust, Security and Privacy in Computing and Communications” (POSSIGNOLO; MARGI, 2012);
- Capítulo 7 - estudo de viabilidade, sob a óptica da computação pessoal, da implementação de computadores quânticos usando as tecnologias baseadas em silício e em fotônica.

1.5 Organização

O restante deste documento é organizado da seguinte forma: no Capítulo 2 conceitos preliminares, necessários ao entendimento deste trabalho, são discutidos. Ele é especialmente útil para um leitor com pouca familiaridade com os temas ali tratados. A seguir, uma revisão bibliográfica sobre os dois principais temas deste trabalho é conduzida, os assuntos relativos à computação quântica são tratados no Capítulo 3 e os relativos à criptografia pós-quântica são discutidos no Capítulo 4.

As contribuições originais deste trabalho se encontram nos capítulos seguintes. No Capítulo 5, a aceleração de algoritmos criptográficos pós-quânticos com o uso de computadores quânticos é proposta. Os impactos desta aceleração também são discutidos neste capítulo. Já no Capítulo 6, uma arquitetura híbrida quântica/clássica, baseada no uso de um coprocessador quântico, é proposta, e algumas restrições e implicações deste coprocessador são discutidas. Finalmente, um estudo de viabilidade da implementação de computadores quânticos, usando diferentes tecnologias, é conduzido no Capítulo 7. Algumas considerações finais são levantadas no Capítulo 8 e indicações de possíveis trabalhos futuros são apresentadas.

2 CONCEITOS PRELIMINARES

Ao longo deste capítulo são apresentados conceitos em diversas áreas do conhecimento que dão suporte a este trabalho. A intenção aqui não é abordar as minúcias de cada uma destas áreas, mas apenas apresentar conceitos importantes para o entendimento do presente trabalho.

Um leitor interessado pode procurar qualquer das referências citadas, onde encontrará explicações mais completas a respeito de cada assunto.

2.1 Complexidade Computacional

Nesta seção algumas ideias básicas sobre complexidade computacional são apresentadas. Não se pretende aqui percorrer toda extensão desta área, apenas discutir conceitos que facilitem o entendimento deste trabalho.

O campo da complexidade computacional se interessa em estudar quais problemas podem ser resolvidos computacionalmente. Obviamente, um problema considerado “difícil” pode conter instâncias de fácil resolução, desta forma costuma-se separar problemas computacionais de acordo com classes de dificuldade (PAPADIMITRIOU, 1994).

Estas classes são definidas de acordo com a variação do número de ciclos computacionais em função do tamanho da entrada. A notação $O(\cdot)$ define o comportamento limite desta função quando o tamanho da entrada tende ao infinito (PAPADIMITRIOU,

1994), ou seja, do ponto de vista de complexidade, se interessa apenas pelo termo que cresce mais rápido da função que define o tempo de processamento de acordo com o tamanho da entrada.

Assim sendo, problemas classificados com “fáceis” ou “tratáveis” são aqueles que podem ser resolvidos com o uso de recursos (temporais e físicos) polinômiais no tamanho da entrada (BARRETO, 2011). Também costuma-se dizer que estes problemas podem ser resolvidos de maneira eficiente. Esta classe de problemas é chamada de P . Já a classe NP comporta problemas para os quais é possível verificar se um dado resultado é uma solução para o problema em questão de maneira eficiente (BARRETO, 2011). Cabe notar que $P \subseteq NP$, mas não se sabe se $P = NP$ ou $P \neq NP$.

Um abuso de nomenclatura é comum ao se referir a problemas que não podem ser resolvidos com o uso de recursos polinômiais, costuma-se dizer que tais problemas são *exponenciais*, mesmo quando o comportamento destes problemas é de natureza sub-exponencial (NIELSEN; CHUANG, 2000).

Finalmente, problemas pelo menos tão difíceis quanto os mais difíceis em NP pertencem à classe *NP-difícil* e problemas de decisão na classe *NP-difícil* são ditos *NP-completos* (BARRETO, 2011).

Adicionalmente, diz-se que um problema A pode ser *reduzido* a um outro problema B , caso uma instância qualquer do problema A possa ser transformada em uma instância do problema B com uma sobrecarga polinomial (NIELSEN; CHUANG, 2000).

2.2 Aritmética em Corpos Finitos

Esta seção dedica-se a discutir a aritmética em corpos matemáticos finitos. Callioli, Domingues Hygino e Costa (1998) definem um *corpo* de acordo com a Definição 1 e um *sub-corpo* de um corpo de acordo com a Definição 2.

Definição 1. Um corpo matemático, ou anel comutativo, é uma estrutura algébrica,

constituída de um conjunto de elementos e dois operadores binários (adição e multiplicação), cujos elementos não nulos formam um grupo comutativo para a multiplicação.

Definição 2. *Um subcorpo matemático S de um corpo K é um corpo matemático, tal que o conjunto de elementos de S esteja contido no conjunto de elementos de K , e S esteja munido dos operadores binários de K .*

Já um *corpo finito*, ou *corpo de Galois*, é um corpo com um número finito de elementos (LIDE; NIEDERREITER, 1997). Tais estruturas algébricas são especialmente úteis em criptografia, particularmente baseada em códigos corretores, e por isso são tratadas aqui. Corpos deste tipo possuem uma aritmética diferente da usual em corpos comuns.

Denota-se ao longo deste documento $\mathbb{F}_{p^m}$ um corpo finito de *ordem* (número de elementos) p^m , onde p é um número primo, chamado *característica* do corpo. A notação $\mathbb{F}_q$ também é usada, assumindo-se $q = p^m$. Além disso, elementos de $\mathbb{F}_{p^m}$ serão representados na forma polinomial: $a(z) \in \mathbb{F}_{p^m} = \sum_{i=0}^{m-1} a_i \cdot z^i$, onde a é um inteiro $\text{mod } p$ e z é a variável de interesse.

Devido à quantidade finita de elementos em $\mathbb{F}_{p^m}$ é preciso especial atenção na definição das duas operações básicas, para evitar que o resultado de uma operação seja externo ao corpo. Por isso, adição e, consequentemente, a subtração são definidas módulo a característica do corpo e a multiplicação e, consequentemente, a divisão são definidas módulo um elemento redutor irredutível (LIDE; NIEDERREITER, 1997).

O Pequeno Teorema de Fermat pode ser usado em corpos finitos (LIDE; NIEDERREITER, 1997), e de fato, seu uso pode simplificar alguns cálculos. O Pequeno Teorema de Fermat diz que:

Teorema 1. *Dado um primo p e um inteiro a :*

$$a^p = a \pmod{p} \quad (2.1)$$

Como acontece em corpos infinitos, é possível definir polinômios sobre um corpo finito $\mathbb{F}_{p^m}$ (LIDE; NIEDERREITER, 1997):

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, \quad (2.2)$$

onde n é um inteiro não negativo, os coeficientes a_i , com $0 \leq i \leq n$ são elementos de $\mathbb{F}_{p^m}$ e x é uma variável em $\mathbb{F}_{p^m}$. Note que neste caso a variável usada é denominada x , mas quando elementos de $\mathbb{F}_{p^m}$ são representados como polinômios a variável usada é z .

Define-se a soma de dois polinômios $f(x) = \sum_{i=0}^n a_i x^i$ e $g(x) = \sum_{i=0}^n b_i x^i$ sobre $\mathbb{F}_{p^m}$ como:

$$f(x) + g(x) = \sum_{i=0}^n (a_i + b_i) x^i. \quad (2.3)$$

Caso um dos polinômios tenha grau maior, o menor deve ser completados com zeros. De maneira equivalente, define-se o produto de $f(x) = \sum_{i=0}^n a_i x^i$ e $g(x) = \sum_{j=0}^m b_j x^j$ como:

$$f(x)g(x) = \sum_{i=0}^n \sum_{j=0}^m a_i b_j x^{i+j} \quad (2.4)$$

Com essas duas operações, o conjunto de polinômios sobre $\mathbb{F}_{p^m}$ define um *anel* algébrico. Este anel será denotado no restante deste trabalho $\mathbb{F}_{p^m}[X]$. Além disso, tomando $f \in \mathbb{F}_{p^m}[X]$ um polinômio irredutível sobre $\mathbb{F}_{p^m}$ o anel residual $\mathbb{F}_{p^m}[X]/(f)$ (conjunto de elementos de $\mathbb{F}_{p^m}[X]$ módulo f) é um corpo finito (LIDE; NIEDERREITER, 1997).

2.3 Álgebra Linear

Nesta seção, alguns conceitos úteis da álgebra linear são definidos. Todos os conceitos aqui abordados foram retirados do livro “Álgebra Linear e Aplicações” (CALLIOLI; DOMINGUES HYGINO; COSTA, 1998).

O objeto de estudo da álgebra linear são os espaços vetoriais (Definição 3), definidos sobre corpos matemáticos (também chamados de anéis comutativos), formalizados na Definição 1.

Definição 3. *Um espaço vetorial sobre um corpo $\mathbb{K}$ é constituído de um conjunto $V \neq \emptyset$ de elementos e dois operadores binários:*

1. *Uma adição $(u, v) \rightarrow u + v$ em V , com as seguintes propriedades:*

- $u + v = v + u, \forall u, v \in V$ (comutativa);
- $u + (v + w) = (u + v) + w, \forall u, v, w \in V$ (associativa);
- $\exists o \in V | u + o = u, \forall u \in V$ (elemento neutro);
- $\forall u \in V, \exists (-u) \in V | u + (-u) = o$ (oposto).

2. *Uma multiplicação de $\mathbb{K} \times V$ em V , ou seja, para cada par (a, u) de $\mathbb{K} \times V$ está associado um elemento único de V que se indica por au ou $a \cdot u$, com as seguintes propriedades:*

- $a \cdot (b \cdot u) = (a \cdot b) \cdot u, \forall a, b \in \mathbb{K}, u \in V$ (associatividade)
- $(a + b) \cdot u = a \cdot u + b \cdot u, \forall a, b \in \mathbb{K}, u \in V$ (distributiva em $\mathbb{K}$)
- $a \cdot (u + v) = a \cdot u + a \cdot v, \forall a \in \mathbb{K}, u, v \in V$ (distributiva em V)
- $1 \cdot u = u, \forall u \in V$ (elemento neutro)

Elementos de V são chamados vetores e elementos de $\mathbb{K}$ são chamados escalares.

Definição 4. Diz-se que um vetor v de V é uma combinação linear de um conjunto de vetores $\{s_1, \dots, s_n\}$, com $s_i \in V$ se existe um conjunto de escalares $\{a_1, \dots, a_n\}$, com $a_i \in \mathbb{K}$ para os quais $v = \sum_{i=1}^n a_i \cdot s_i$.

A partir do conceito de combinação linear (Definição 4), pode-se imaginar um sub-espço de V gerado com um pequeno conjunto de vetores. A este conjunto é dado o nome de *conjunto gerador* do espaço V . Esta relação é dada na Definição 5.

Definição 5. Chama-se de *espaço gerado* $[S]$ por um conjunto de vetores $S = \{s_1, \dots, s_n\}$, com $s_i \in V$, o espaço formado por todas as combinações lineares dos elementos de S , ou seja $[S] = \{a_1 s_1, \dots, a_n s_n \mid a_1, \dots, a_n \in \mathbb{K}\}$.

Definição 6. Um conjunto de vetores $C = \{v_1, v_2, \dots, v_n\}$, com $v_i \in V$ é dito linearmente dependente se existir um subconjunto de C e escalares $a_i \in \mathbb{K}$, não todos nulos, tais que $\sum_{v_i \in C} a_i \cdot v_i = 0$. Se diz que o conjunto de vetores é linearmente independente se tal condição não é satisfeita.

A partir da Definição 6 de dependência linear e da Definição 5 de espaço gerado por um conjunto de vetores, podemos definir uma base do espaço V .

Definição 7. Uma base do espaço V é um conjunto linearmente independente de vetores de V , cujo espaço gerado é o espaço V . Ao tamanho deste conjunto é dado o nome de *dimensão do espaço* V .

O elemento do espaço vetorial, ou vetor, é representado por uma n -upla de elementos de $\mathbb{K}$. Assim o vetor v pode ser escrito na forma $(a_1, a_2, \dots, a_n)$, com $a_1, \dots, a_n \in \mathbb{K}$. Essa representação depende de uma base escolhida. Se o vetor a é representado como $(a_0, \dots, a_n)$ para a base $B = (v_0, \dots, v_n)$ do espaço V , onde n é a dimensão de B , então $a = \sum_{i=0}^n (a_i \cdot v_i)$.

Para realizar a adição de dois vetores cada um dos termos do vetor é adicionado individualmente, em ordem: $(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$.

b_n). De forma análoga, a multiplicação por escalar é feita individualmente sobre cada um dos termos do vetor: $c \cdot (a_1, a_2, \dots, a_n) = (c \cdot a_1, c \cdot a_2, \dots, c \cdot a_n)$.

Uma transformação linear T do espaço V para o espaço U é uma operação que associa (ou mapeia) à cada elemento de V um elemento de U , denota-se $T : V \rightarrow U$. A linearidade de uma transformação é definida por:

Definição 8. Uma transformação T é dita linear, se dados $u, v \in V$ e $a, b \in \mathbb{K}$ a igualdade

$$T(a \cdot u + b \cdot v) = a \cdot T(u) + b \cdot T(v), \quad (2.5)$$

é válida.

Transformações lineares podem ser representadas por matrizes de elementos de $\mathbb{K}$. Uma transformação *em* um espaço V é uma transformação do tipo $T : V \rightarrow V$.

Espaços vetoriais podem ser dotados de *produtos internos*, definidos, para $\mathbb{K} = \mathbb{C}$, como (REED; SIMON, 1972):

Definição 9. Produto interno sobre um espaço vetorial V é uma aplicação que transforma o par ordenado $(u, v) \in V \times V$ em um elemento de $\mathbb{K}$, obedecendo às regras:

1. $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle, \forall u, v, w \in V$;
2. $\langle u, a \cdot v \rangle = a \langle u, v \rangle, \forall a \in \mathbb{K} \text{ e } \forall u, v \in V$;
3. $\langle u, v \rangle = \langle v, u \rangle^*, \forall u, v \in V$, onde a^* é o complexo conjugado de a e
4. $\langle u, u \rangle \geq 0, \forall u \in V \text{ e } \langle u, u \rangle = 0 \Leftrightarrow u = 0$

Uma nota adicional é que as condições 1, 2, 3 implicam também em $\langle u, a \cdot v + b \cdot w \rangle = a \langle u, v \rangle + b \langle u, w \rangle$ e que $\langle a \cdot u, v \rangle = a^* \langle u, v \rangle$. Também nota-se que alguns autores consideram o produto interno como linear no primeiro termo e não no segundo, ao contrário da condição 2 aqui apresentada (REED; SIMON, 1972). A condição 3 se torna uma simetria (*i.e.* $\langle u, v \rangle = \langle v, u \rangle$), se $\mathbb{K} = \mathbb{R}$.

O produto interno de um espaço vetorial pode ser usado para criar uma *norma*, dentro deste espaço (REED; SIMON, 1972). Desta forma, tem-se que:

Definição 10. A norma $\|u\|$ do vetor $u \in V$, associada ao produto interno $\langle \cdot, \cdot \rangle$, é dada por $\|u\| = \sqrt{\langle u, u \rangle}$.

Pode-se definir a métrica (Definição 11) $d(u, v) = \|u - v\|$ a partir da norma definida pelo produto interno.

Definição 11. Uma métrica é uma distância geométrica, i.e. uma função $d : V \times V \rightarrow \mathbb{K}$ que satisfaz as seguintes propriedades:

1. $d(x, y) \geq 0$ (positiva)
2. $d(x, u) = d(y, x)$ (simétrica)
3. $d(x, z) \leq d(x, y) + d(y, z)$ (desigualdade triangular)
4. $d(x, y) = 0 \Leftrightarrow x = y$

Diz-se que dois vetores são *ortogonais* se o produto interno entre eles é 0. Finalmente, uma base é dita *ortonormal* se ela é formada por *vetores unitários* ortogonais par a par.

Definição 12. Um vetor unitário é um vetor tal que $\|u\| = 1$.

Finalmente, um espaço vetorial especialmente útil na mecânica quântica é um espaço de Hilbert (Definição 15), que é definido a partir de um espaço completo (Definição 13).

Definição 13. Um espaço vetorial é dito completo se todas as Sequências de Cauchy convergem dentro do espaço.

Definição 14. Sequência de Cauchy é toda sequência cujos elementos se tornam arbitrariamente próximos conforme a sequência progride.

Definição 15. *Um espaço de Hilbert é um espaço vetorial completo e dotado de um produto interno.*

Espaços de Hilbert são vistos como uma generalização para dimensão infinita de espaços Euclidianos. Espaços de Hilbert também são geralmente vistos como espaços de funções.

2.4 Sumário do Capítulo 2

Neste capítulo foram introduzidos diversos conceitos em várias áreas do conhecimento. Tais conceitos, apesar de não serem tratados diretamente no escopo deste projeto de pesquisa, são úteis no entendimento do trabalho desenvolvido.

Nos próximos capítulos, uma revisão bibliográfica dos dois principais temas que abrangem este trabalho é conduzida, partindo-se destes conceitos.

3 DA MECÂNICA À COMPUTAÇÃO QUÂNTICA

Entende-se por computação quântica a utilização de primitivas da mecânica quântica para fins de computação (NIELSEN; CHUANG, 2000). Isso não fornece uma ideia precisa sobre o que exatamente é possível fazer com um computador quântico. De fato, esse é um problema em aberto na comunidade científica ainda hoje (BERNSTEIN; BUCHMANN; DAHMEN, 2008). É possível numerar algumas funções que um computador quântico é capaz de executar eficientemente, no entanto, não se conhece os limites dessa capacidade.

Neste capítulo são discutidas as formulações teóricas e as propriedades da mecânica quântica sobre as quais se apoiam a computação quântica, além disso, são apresentados os elementos básicos desta computação, bem como as principais tecnologias de construção de computadores quânticos, que estão sendo estudadas na comunidade acadêmica.

3.1 Formulação de Dirac

A mecânica quântica pode ser definida a partir da chamada formulação de Dirac (apesar de existirem outras formulações equivalentes), onde o estado de um sistema é representado por um vetor no espaço de Hilbert de dimensão N (PIQUEIRA, 2011).

Na notação de Dirac, um estado quântico é representado por um vetor coluna denominado “ket” ($|\cdot\rangle$) (Equação 3.1) (DIRAC, 1981). O dual de um “ket” é um “bra”, representado por $\langle\cdot|$ (Equação 3.2) e composto pelos complexos conjugados do “ket”

equivalente (NIELSEN; CHUANG, 2000), representados por $\cdot^*$. Vetores que diferem apenas de um fator de fase (*i.e.* $|\psi\rangle$ e $e^{i\theta}|\psi\rangle$) são vetores ditos *equivalentes*, ou seja, representam o mesmo estado quântico (NIELSEN; CHUANG, 2000), esse fator de fase pode ser chamado de fase global.

$$|\psi\rangle = \begin{bmatrix} \psi_0 \\ \psi_1 \\ \vdots \\ \psi_{N-1} \end{bmatrix} \quad (3.1)$$

$$\langle\psi| = \begin{bmatrix} \psi_0^* & \psi_1^* & \dots & \psi_{N-1}^* \end{bmatrix} \quad (3.2)$$

Todo espaço de Hilbert é dotado de um produto interno, conforme definido na Seção 2.3 (REED; SIMON, 1972), esse produto interno será denotado $\langle\cdot|\cdot\rangle$, no contexto de estados quânticos. Pode ser útil definir uma base $B = \{|\phi_0\rangle, |\phi_1\rangle, \dots, |\phi_{N-1}\rangle\}$ para o espaço em questão. A formulação apresentada até aqui é perfeitamente compatível com um número infinito de dimensões, mas neste trabalho apenas espaços com um número finito de dimensões é considerado. Logo, a não ser que mencionado explicitamente, quando estados quânticos são mencionado, fica implícito o uso de espaços de dimensões finitas.

Outras duas notações são importantes para o entendimento das propriedades da mecânica quântica: os produtos *externo* e *tensorial*. Produtos externos são usados para representar operadores (NIELSEN; CHUANG, 2000):

Definição 16. O produto externo de $|a\rangle = \sum_i a_i|i\rangle$ por $\langle b| = \sum_i b_i\langle i|$ é definido como:

$$|a\rangle\langle b| = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \begin{pmatrix} b_1 & \dots & b_n \end{pmatrix}$$

Já produtos tensoriais são usados para representar estados quânticos compostos de

mais de um sub-estado. Segundo Nielsen e Chuang (NIELSEN; CHUANG, 2000), eles são usados para formar espaços maiores a partir de espaços base.

Definição 17. *O produto tensorial entre uma matriz A $m \times n$ e uma matriz B $p \times q$ é*

$$\text{uma matriz } mp \times nq, \text{ na forma: } A \otimes B = \begin{pmatrix} a_{11} \cdot B & a_{12} \cdot B & \dots & a_{1n} \cdot B \\ a_{21} \cdot B & a_{22} \cdot B & \dots & a_{2n} \cdot B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} \cdot B & a_{m2} \cdot B & \dots & a_{mn} \cdot B \end{pmatrix}$$

A mesma definição pode ser aplicada para vetores, considerando-os como matrizes onde o número de linhas ou o número de colunas é 1. Ao longo deste documento as notações $|a\rangle \otimes |b\rangle$, $|a\rangle|b\rangle$ e $|ab\rangle$ serão usadas para representar produtos tensoriais entre os vetores $|a\rangle$ e $|b\rangle$.

Adicionalmente, denota-se $H_3 = H_1 \otimes H_2$ o produto tensorial dos espaços de Hilbert H_1 e H_2 . Este produto tensorial gera um novo espaço de Hilbert de dimensão $n_1 \times n_2$ onde n_1 é a dimensão de H_1 e n_2 a dimensão de H_2 (NIELSEN; CHUANG, 2000). Finalmente, uma base para H_3 pode ser encontrada através dos produtos tensoriais dos elementos das bases de H_1 e H_2 (NIELSEN; CHUANG, 2000).

3.2 Bases da Teoria Quântica

Nielsen e Chuang (2000) descrevem a mecânica quântica como um arcabouço matemático e conceitual para a elaboração de leis da física. Desta forma, a mecânica quântica não provê, por si só, leis que devem ser obedecidas por sistemas quânticos. No entanto, alguns postulados, ligados à esta concepção matemática, fazem parte da mecânica quântica. Esta seção dedica-se a apresentar estes postulados.

3.2.1 Superposição

O primeiro postulado da mecânica quântica (NIELSEN; CHUANG, 2000), para estados de dimensões finitas, diz que:

Postulado 1. *O estado $|\psi\rangle$ de um sistema quântico, descrito por um vetor em um espaço de Hilbert de dimensão finita, pode ser representado em um espaço de Hilbert por uma combinação linear de elementos de uma base ortonormal $B = \{|\phi_0\rangle, |\phi_1\rangle, \dots, |\phi_{n-1}\rangle\}$, dada por:*

$$|\psi\rangle = \sum_{i=0}^{N-1} \alpha_i \cdot |\phi_i\rangle \quad (3.3)$$

Com $\sum_{i=0}^{N-1} \alpha_i \cdot \alpha_i^* = 1$, ou de forma equivalente $\langle\psi|\psi\rangle = 1$.

Uma observação importante é que a mecânica quântica (assim como a definição de espaços de Hilbert) não se limita a espaços com um número finito de dimensões, no entanto, dentro do contexto deste trabalho o uso de um número finito de dimensões é suficiente.

Este postulado, em primeiro lugar, define que sistemas quânticos são representados em espaços de Hilbert (NIELSEN; CHUANG, 2000). Ele também enuncia que o estado de um sistema qualquer pode ser representado por uma combinação de elementos da base. Esta combinação pode ser representada pelo vetor unitário (conforme a Definição 12) por $|\psi\rangle = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$.

Do ponto de vista físico, a interpretação mais comum para esta combinação linear é a chamada *superposição* (PIQUEIRA, 2011). Não se pode dizer com precisão em qual estado da base encontra-se um estado superposto (NIELSEN; CHUANG, 2000). É comum dizer que um estado superposto encontra-se, simultaneamente, em todas as posições $|\phi_i\rangle$, até que uma medição seja feita, neste caso um dos estados $|\phi_i\rangle$ é obtido com probabilidade $\alpha_i \alpha_i^*$ e a superposição deixa de existir (PIQUEIRA, 2011).

Dirac (1981) caracteriza a *superposição* como uma combinação peculiar de estados para a formação de um novo estado que não pode ser entendida de maneira clássica. Ainda segundo Dirac, a representação de um estado resultante de uma superposição é um processo independente de qualquer referência física.

Para fins de computação, estados de dimensão dois são especialmente úteis. Ao longo deste documento, quando um estado deste tipo for mencionado, assume-se que uma base $B = \{|0\rangle, |1\rangle\}$, chamada de *base computacional*, que deve ser previamente definida para o sistema físico, está sendo usada. Tais sistemas são chamados de *qubits*, ou *bits quânticos* (PIQUEIRA, 2011), por se tratarem de um análogo aos *bits* de um computador clássico. Os estados da base $|0\rangle, |1\rangle$ são equivalentes aos valores clássicos de um bit 0, 1 (NIELSEN; CHUANG, 2000).

Esta definição não corresponde à definição de bit dada pela teoria da informação de Shannon, onde um bit é o quanta (menor unidade) de informação (SHANNON, 1956). Mesmo no caso da teoria quântica da informação, a definição de qubit é válida, mas também com uma interpretação distinta da aqui utilizada (SCHUMACHER, 1995).

Nota-se adicionalmente que para se representar um qubit seria necessária quantidade infinita de informação (coeficiente complexo de precisão arbitrária), no entanto apenas um bit (no sentido computacional) pode ser extraído dele após uma medição (NIELSEN; CHUANG, 2000).

3.2.2 Evolução Temporal

Uma transformação linear algébrica U pode ser definida como $U : H^n \rightarrow H^n$ (PIQUEIRA, 2011). Já um *operador unitário* é definido da seguinte forma (NIELSEN; CHUANG, 2000):

Definição 18. Operador unitário é todo aquele cuja matriz satisfaz: $O \cdot O^\dagger = O^\dagger \cdot O = \mathbb{I}$. Onde $O^\dagger$ é a transposta conjugada de O e $\mathbb{I}$ é a matriz identidade.

A dinâmica de sistemas quânticos é representada por transformações lineares no espaço de Hilbert, essas transformações são descritas por *operadores quânticos*. Esta dinâmica é modelada pelo segundo postulado da mecânica quântica (NIELSEN; CHUANG, 2000):

Postulado 2. *A evolução temporal de um sistema quântico fechado é descrito por uma transformação unitária. Ou seja, o estado $|\psi_1\rangle$ de um sistema no tempo t_1 se relaciona com o estado $|\psi_2\rangle$ do sistema no tempo t_2 por uma operação unitária linear U que depende de t_1 e t_2 :*

$$|\psi_2\rangle = U|\psi_1\rangle \quad (3.4)$$

O postulado, como aqui apresentado, é muito restrito, exigindo que o sistema seja *fechado*. Um sistema fechado é um sistema que não interage com nenhum sistema externo. Essa restrição não pode ser observado na prática, no entanto, para fins de computação costuma ser suficiente reduzir as principais fontes de interferência do sistema (NIELSEN; CHUANG, 2000), que passa a ser considerado fechado, mesmo que isso não seja absolutamente verdadeiro. De fato, um dos grandes desafios na implementação de computadores quânticos é a redução destas interferências, que acabam levando o sistema à chamada *perda de coerência* (DIVINCENZO, 2005). A perda de coerência, ou *decoerência*, é definida como a interferência de fontes externas sobre o estado quântico de interesse, causando a perda da informação quântica (BACON, 2003).

A Equação 3.4 mostra a evolução de um estado quântico em passos discretos, ou seja, uma operação por vez. Essa descrição da dinâmica do sistema é suficiente para a computação, mas incompleta do ponto de vista físico. Uma modelagem completa do sistema pode ser obtida com o uso da *equação de Schrödinger* (NIELSEN; CHUANG, 2000), no entanto, este uso está fora do escopo deste trabalho.

3.2.3 Medições

Se um sistema *fechado* evolui no tempo de acordo com transformações lineares, ao entrar em contato com o mundo externo (seja de forma voluntária ou não) essa evolução não é mais unitária (NIELSEN; CHUANG, 2000). Interferências voluntárias no sistema acontecem quando o controlador do sistema precisa saber o que se passa nele, ou medi-lo, essas operações também são chamadas de *observações*.

Elas são descritas por um conjunto de *operadores de observação* M_m , onde o índice m se refere à saída da operação de observação. Dado o estado anterior à medição $|\psi\rangle$, a probabilidade do evento m acontecer é $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$. Esse conjunto de operadores de observação satisfazem a condição $\sum_m M_m^\dagger M_m = I$, o que significa que a probabilidade total de observação deve ser 1 (NIELSEN; CHUANG, 2000).

Uma vez que uma observação corresponde a uma leitura sobre um estado físico, é evidente que esse tipo de operação tem a restrição adicional de resultar em um número real (DIRAC, 1981). Uma outra característica importante sobre o comportamento destes operadores é que eles não são comutativos, ou seja, a ordem em que eles são aplicados muda o resultado da medição (DIRAC, 1981), isso se explica pelo fato da medição destruir o estado quântico existente antes do processo de medida ser realizado.

Um conjunto especialmente útil de operadores de observação é conjunto da base computacional $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$. Supondo o estado $|\psi\rangle = a|0\rangle + b|1\rangle$, tem-se que $p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = |a|^2$. Analogamente $p(1) = |b|^2$.

Segundo Nielsen e Chuang (2000) existe grande discussão na comunidade acerca do Postulado 2. Argumenta-se que, considerando o aparato de medição como parte do sistema, deveria ser possível descrever o sistema através de operadores unitários, o que ainda não foi provado. Essa discussão, no entanto, não será explorada neste trabalho.

3.2.4 Sistemas Compostos e Emaranhado

Dados os estados $|\psi_1\rangle \in H_1$ e $|\psi_2\rangle \in H_2$ de dois sistemas quânticos distintos, o estado do sistema composto por estes sistemas pode ser representado por $|\psi_3\rangle \in H_3$, onde $H_3 = H_1 \otimes H_2$ (NIELSEN; CHUANG, 2000). Ou seja, o estado de sistemas compostos podem ser representados no espaço obtido através do produto tensorial dos espaços nos quais se encontram os elementos da composição.

Dada esta formulação, pode-se definir um estado *emaranhado*, ou *entrelaçado*, como qualquer estado com mais de um sub-sistema cujo estado não pode ser expresso através de um produto tensorial (WILLIAMS, 2011). Exemplos disto são os estados de Bell. Tomando o primeiro estado de Bell $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ que pertence a $H^{2 \times 2}$, pode-se mostrar que é impossível escrevê-lo como produto tensorial de dois vetores em H^2 , logo o primeiro estado de Bell é emaranhado (PIQUEIRA, 2011).

Já estados não emaranhados podem ser escritos como produto tensorial dos estados base diretamente, por exemplo, o estado $|\psi_{AB}\rangle = \frac{1}{2} \cdot (|0_A 0_B\rangle + |0_A 1_B\rangle + |1_A 0_B\rangle + |1_A 1_B\rangle)$ pode ser escrito como produto tensorial dos estados $|\psi_A\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle + |1_A\rangle)$ e $|\psi_B\rangle = \frac{1}{\sqrt{2}}(|0_B\rangle + |1_B\rangle)$. Note que os índices A e B são usados para identificar sub-sistemas diferentes.

De um ponto de vista prático, o emaranhado quântico pode ser visto como uma forma de interação “forte” entre estados quânticos. Ao se realizar uma observação sobre um dos sub-sistemas emaranhados é possível saber qual será o resultado da medição sobre o outro sub-sistema (PIQUEIRA, 2011). O emaranhado quântico não depende da distância e, por isso, seu uso foi proposto para a comunicação (NIELSEN; CHUANG, 2000).

Novamente, destaca-se que o formalismo físico por trás do emaranhado é muito discutido na literatura. Piqueira (2011) destaca que Einstein não aceitava a mecânica quântica como uma descrição completa da realidade devido justamente ao emara-

nhado. O chamado paradoxo EPR (Einstein, Podolsky e Rosen) (EINSTEIN; PODOLSKY; ROSEN, 1935) está relacionado ao emaranhado quântico. Einstein argumentava que a mecânica quântica não poderia ser uma descrição completa da realidade, uma vez que implicaria em informação viajando com velocidade infinita, devendo haver alguma “variável escondida”. Já Bell argumentava que nenhuma explicação de variável escondida local seria suficiente para explicar o que se observa em mecânica quântica, propondo, então, que a mecânica quântica seria “não-local” (ASPECT; DALIBARD; ROGER, 1982; BELL, 1966). No entanto, está fora do escopo deste trabalho discutir cada uma destas vertentes.

3.3 Computação Quântica

A computação quântica é mais comumente modelada na literatura através de uma série de operadores quânticos, como definido na Seção 3.3.1 (NIELSEN; CHUANG, 2000). No contexto de computação quântica a aplicação destes operadores é chamada de *portas (lógicas) quânticas* e o modelo computacional é chamado de *modelo de circuito*, apesar de não se tratar de um circuito no sentido elétrico. A representação destas portas quânticas ao longo do tempo remete a diagramas de portas lógicas em circuitos clássicos (WILLIAMS, 2011).

Um requisito importante para que a computação seja bem sucedida é que estas transições ocorram de forma *coerente*, *i.e.* que elas não destruam o estado quântico existente. Essa exigência é mapeada diretamente na necessidade de operadores unitários. Operadores unitários são necessariamente reversíveis e por isso, a computação quântica se desenvolveu a partir de modelos de computação reversível já existentes (FREDKIN; TOFFOLI, 1982).

Nesta seção o modelo de circuito da computação quântica será tratado, inicialmente apresentando as principais portas lógicas, ou operadores, quânticos, chegando

ao algoritmo de Grover, usado ao longo do trabalho.

3.3.1 Operadores Quânticos

Nesta seção apresentaremos os principais operadores quânticos relacionados à computação presentes na literatura, definindo alguns conjuntos universais. Uma explicação completa e mais detalhada dessas portas pode ser encontrada nos livros de Nielsen e Chuang (2000) ou Williams (2011).

Por conjunto universal entende-se um conjunto de operadores com o qual é possível modelar um operador arbitrário (DIVINCENZO, 2005; NIELSEN; CHUANG, 2000). No entanto, como existe um número infinito de estados – e, portanto, de operadores – exige-se apenas uma modelagem aproximada (DIVINCENZO, 2005). Diversos operadores, ou portas lógicas, quânticos existem na literatura. Em geral, busca-se agrupá-los de forma a se obter um conjunto universal de operadores, suficiente para a realização de qualquer tarefa computacional.

Inicialmente, destaca-se os operadores quânticos de um qubit. Na Figura 1 as portas quânticas de um qubit são representadas. A porta de *Hadamard* (Figura 1-a) leva o estado $|0\rangle$ à superposição $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ e o estado $|1\rangle$ à superposição $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, podendo ser representado pela matriz:

$$H = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (3.5)$$

A porta de Pauli-X também é vista como a porta clássica inversora, pois mapeia o estado $|0\rangle$ no estado $|1\rangle$ e vice versa. Sua matriz é exibida na Equação 3.6. Já a porta Pauli-Y transforma o estado $|0\rangle$ no estado $i|1\rangle$ e o estado $|1\rangle$ no estado $-i|0\rangle$, sua matriz é apresentada na Equação 3.7. Finalmente, a porta Pauli-Z mantém o estado $|0\rangle$ inalterado, invertendo o sinal do estado $|1\rangle$, a matriz da porta Pauli-Z é exibida na

Equação 3.8.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (3.6)$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad (3.7)$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (3.8)$$

Figura 1: Operadores quânticos de um qubit.

Já as portas de *Mudança de Fase* levam o estado $\alpha \cdot |0\rangle + \beta \cdot |1\rangle$ para o estado $\alpha \cdot |0\rangle + e^{i\theta} \cdot \beta \cdot |1\rangle$, onde θ é a fase aplicada. Uma representação matricial para esta porta é fornecida na Equação 3.9. É importante destacar que uma implementação desta porta irá aplicar uma mudança no estado quântico, ao contrário da aplicação de uma fase global (ver Seção 3.1).

$$R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \quad (3.9)$$

Além dos operadores com um qubit, pode-se destacar alguns operadores com mais qubits. A porta *CNOT* ou “Inversor Controlado” é a principal delas, ela inverte o segundo qubit quando o primeiro é $|1\rangle$. De certa forma, essa porta pode ser vista como uma operação de “Ou-Exclusivo” (representado por $\cdot \oplus \cdot$) pois mapeia o estado $|a\rangle \otimes |b\rangle$

em $|a\rangle \otimes |a \oplus b\rangle$. A porta *CNOT* pode ser vista matricialmente na Equação 3.10.

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (3.10)$$

Portas de um qubit e a porta *CNOT* formam um conjunto universal (DEUTSCH; BARENCO; EKERT, 1995), no entanto, por facilidade, algumas outras portas são definidas. Entre elas pode-se destacar as portas de Toffoli e a porta *SWAP*. A primeira pode ser vista como uma porta inversora duplamente controlada, ou seja, ela inverte o qubit alvo caso dois qubits de controle sejam $|1\rangle$, e é, portanto, uma porta de três qubits. Já a segunda troca os valores de dois qubits, ou seja, realiza a operação $|a\rangle \otimes |b\rangle \rightarrow |b\rangle \otimes |a\rangle$. A porta de Toffoli é representada matricialmente na Equação 3.11 e a porta *SWAP* na Equação 3.12.

$$\text{Toffoli} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (3.11)$$

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (3.12)$$

Na Figura 2 as representações dessas três portas no modelo de circuitos quânticos são apresentadas.

Figura 2: Operadores quânticos de múltiplos qubits. $|C\rangle$, $|C1\rangle$, $|C2\rangle$ são qubits de controle e $|T\rangle$ é o alvo da operação, o índice $_o$ indica valores de saída e A e B são estados arbitrários.

Finalmente, uma operação de observação será representada genericamente pelo desenho mostrado na Figura 3. A não ser que especificado de maneira contrária, a medição terá como referência a base computacional, ou seja, espera-se como saída um vetor binário. A linha dupla será usada para representar estados clássicos obtidos após as medições.

Figura 3: Operador de observação de um estado quântico. A linha dupla representa um estado clássico, obtido após a observação.

3.3.2 Busca de Grover

Antes de tratar da Busca de Grover propriamente dita, é interessante definir um problema de busca e explicar como este problema é resolvido em computadores clássicos. Neste trabalho, quando o termo “desordenado” for usado, o sentido pretendido é o de uma lista em que a ordem importa, mas os termos não se encontram ordenados de alguma maneira peculiar (crescente, decrescente, alfabética, etc.).

Em um problema de busca em uma lista desordenada L com N elementos, pretende-se encontrar uma solução ou um conjunto de soluções S de M elementos, não necessariamente iguais. A busca estará concluída quando:

- um dos elementos de S for encontrado, neste caso o índice do elemento será devolvido;

- nenhum elemento de S estiver presente na lista L .

Em um computador clássico, a maneira mais eficiente de se resolver esse problema é com uma busca exaustiva ou incremental. Ou seja, os elementos de L são comparados um a um com os elementos de S até que algum elemento de S seja encontrado, quando a busca para. No pior caso, todos os elementos de L devem ser visitados, o que leva tempo de $O(M \cdot N)$.

O algoritmo de Busca de Grover (GROVER, 1996; NIELSEN; CHUANG, 2000) é um dos mais importantes algoritmos quânticos já descobertos. Ele permite uma busca em uma lista desordenada, de maneira mais eficiente que a busca clássica. A busca de Grover tem complexidade $O(\sqrt{\frac{N}{M'}})$. Onde M' é o número de elementos de S efetivamente presentes em L .

O algoritmo de Grover, como boa parte dos algoritmos quânticos, é probabilístico, ou seja, tem uma chance não nula de falhar. Ao final do algoritmo sempre haverá uma leitura de posição, que deve então ser verificada:

- caso haja uma solução na posição indicada, a busca acaba;
- caso contrário, ela deve ser refeita para diminuir a probabilidade que uma solução existente em L não seja encontrada.

A probabilidade de falha é de aproximadamente $\frac{M'}{N}$ para cada vez que o algoritmo é rodado (NIELSEN; CHUANG, 2000), note que M' em geral é desconhecido. Cabe ao projetista estimar M' e decidir quantas rodadas serão necessárias para decidir que uma solução não existe. A probabilidade de falha ao final de k rodadas da busca de Grover é dada pela Equação 3.13. Um não determinismo adicional existe quando o conjunto M' é maior que 1, neste caso, diferentes rodadas da busca podem apontar para diferentes

soluções (GROVER, 1996).

$$P_G = \left(\frac{M'}{N} \right)^k \quad (3.13)$$

O algoritmo consiste na aplicação iterativa de um oráculo e um operador de difusão, a esse conjunto é dado o nome de *iteração de Grover*. São necessárias aproximadamente $\frac{\pi}{4} \cdot \sqrt{\frac{N}{M'}}$ iterações, assumindo $M' \ll N$ (NIELSEN; CHUANG, 2000). Na Figura 4, o modelo de circuito para a busca de Grover é esboçado, o eixo horizontal denota a passagem do tempo e cada linha representa um estado quântico (também chamado de *registrador quântico* no contexto de computação), $n_1 = \log_2 N$ e n_2 depende da busca. O espaço de Grover é o espaço dos endereços, ou índices da busca, já o espaço de busca está relacionado à busca específica que se pretende calcular, em geral, uma consulta a uma lista e comparação com os valores procurados.

Figura 4: Modelo de circuito da computação quântica para a busca de Grover. O eixo horizontal representa o tempo e as linhas representam os operadores quânticos. $H^{\otimes n}$ representa a aplicação da porta de Hadamard para cada um dos n estados e G é a iteração de Grover.

O oráculo da iteração de Grover é o operador responsável por verificar se a posição x aponta para uma solução da busca (*i.e.* um elemento de M). O oráculo deverá inverter o sinal dos coeficientes dos estados x que apontam para uma solução da busca, comportamento descrito pela Equação 3.14, tomando $f(x) = 1$ se x aponta para uma solução e $f(x) = 0$, caso contrário. Fica claro que este oráculo depende da instância

específica do problema de busca e deve ser definido pelo projetista.

$$|x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle. \quad (3.14)$$

Já o operador de difusão se encarrega de aumentar ligeiramente o coeficiente das posições que apontam para os resultados da busca (que foram marcados pelo oráculo com o sinal negativo). O operador de difusão pode ser expresso como $D = 2|\psi\rangle\langle\psi| - I$, onde I é a identidade e $|\psi\rangle$ é uma superposição de estados de igual peso (NIELSEN; CHUANG, 2000). A aplicação do operador de difusão sobre um estado genérico $|a\rangle = \sum_k a_k|k\rangle$ irá resultar em $\sum_k [-a_k + \hat{a}]|k\rangle$, onde $\hat{a} = \sum_k a_k/N$ é a média dos coeficientes a_k (GROVER, 1996). Para uma prova mais formal do funcionamento da busca de Grover, bem como das probabilidades e número de iterações, recomenda-se o livro de Nielsen e Chuang (2000).

3.4 Implementações Físicas de Computadores Quânticos

Nesta seção são discutidas implementações de computadores quânticos, iniciando em alguns requisitos básicos, amplamente aceitos na comunidade e chegando à algumas propostas de implementação mais relevantes. Nota-se que não foi feita uma lista exaustiva destas propostas, mas buscou-se identificar as mais aceitas e com resultados mais maduros na presente data.

As quatro tecnologias abordadas são: as de estado sólido, pois acredita-se serem as únicas escaláveis (SHERWIN; IMAMOGLU; MONTROY, 1999); a baseada em óptica linear, que pode ser operada em temperatura ambiente (KNILL; LAFLAMME; MILBURN, 2001); as armadilhas de íon, que possibilitam maior número de operações (NIELSEN; CHUANG, 2000) e a Ressonância Magnética Nuclear, que resultou na primeira implementação do algoritmo de Shor (VANDERSYPEN *et al.*, 2001).

3.4.1 Requisitos Básicos para Computadores Quânticos

Os requisitos aqui discutidos foram inicialmente introduzidos por David Divincenzo (2005), como um guia para se buscar implementações possíveis. Eles tratam da possibilidade de efetuar cálculos com o uso da mecânica quântica, mas não de sua viabilidade, logo essas características são necessárias, mas não suficientes para uma solução definitiva.

Ao todo sete requisitos são introduzidos, cinco visando a computação puramente e outros dois visando a comunicação.

1. Um sistema físico escalável com qubits bem determinados: em outras palavras, um sistema físico onde se conheça bem o estado quântico usado para a codificação do qubit, evitando confusão com demais estados, e que possa ser escalado para um número razoável de qubits. Qubits bem determinados são aqueles que possuem características físicas conhecidas e baixa probabilidade de passar para outros níveis de energia além dos determinados.

2. A habilidade de inicializar o estado para um estado simples e conhecido: exatamente como no caso clássico, a capacidade de inicializar o estado a ser usado para um valor conhecido (uma operação de *reset*) é necessária. Essa operação deve ser independente do estado inicial (normalmente desconhecido).

3. Tempos de decoerência longos, muito maiores que o tempo de aplicação de uma operação: como já foi discutido, a *decoerência* ocorre devido à interferência externa. Quando ela ocorre toda a computação em curso é perdida, por isso é necessário que tudo seja feito antes que a decoerência ocorra. É impossível isolar totalmente um sistema quântico, no entanto, medidas para reduzir interferências são possíveis. O que se deseja aqui é que se possa realizar um número grande de operações (todo um algoritmo), antes que o sistema perca sua coerência.

4. Um conjunto universal de portas quânticas: um conjunto universal é neces-

sário para tirar proveito completo da computação quântica. A disponibilidade de um conjunto maior que um conjunto universal mínimo é desejável, mas não necessária. Felizmente, diversos conjuntos universais existem e é possível reduzir qualquer porta com três ou mais entradas para combinações de portas de uma e duas entradas (DIVINCENZO, 1995), simplificando essa necessidade.

5. A capacidade de realizar uma medição em um qubit arbitrário: nenhum cálculo é útil, a não ser que se possa extrair seu resultado. Por isso a necessidade de se medir o valor de um qubit. Também é necessário que essa medição não interfira no estado do resto do computador, causando perda de coerência. A forma como essa medição é feita depende da tecnologia usada e do grau de liberdade usado para codificar o qubit.

Os próximos dois requisitos estão ligados à comunicação, sendo também úteis para a computação distribuída. No entanto, eles não são necessários caso se deseje apenas realizar todos cálculos localmente.

6. A habilidade de converter qubits “estacionários” em “voadores”¹: na computação clássica, bits são armazenados em registradores e “passam” por portas lógicas. Em tecnologias como RMN, armadilha de íons e as baseadas em silício essa lógica se inverte: os qubits são estacionários e as operações são aplicadas a eles. Ou seja, o qubit encontra-se confinado em um espaço restrito. Nesses casos, a habilidade de transformá-los em algo que possa ser enviado é essencial. Essa conversão deve preservar o estado. Mesmo no caso onde as operações são aplicadas a qubits “voadores”, como óptica linear, esse requisito é necessário para possibilitar o armazenamento do estado quântico.

7. Capacidade de transmissão fiel de qubits “voadores” entre localidades específicas: a transmissão fiel de estados quânticos é necessária para a comunicação.

¹O termo “flying qubits” se tornou popular na literatura para identificar estados quânticos presentes em partículas que se deslocam espacialmente (em geral fótons, mas possivelmente elétrons) (DIVINCENZO, 2005).

Também é importantes que essa transmissão alcance grandes distâncias. Essa capacidade deve estar associada à anterior, ou seja, deve ser possível transformar um qubit “estacionário” em um qubit “voador” que possa ser transmitido.

3.4.2 Tecnologias de Estado Sólido

É amplamente aceito que as tecnologias de estado sólido serão as únicas capazes de atingir um grande número ($\approx 10^3$) de qubits (SHERWIN; IMAMOGLU; MONTROY, 1999), o que as torna especialmente interessantes. Dentre as tecnologias de estado sólido, as baseadas em silício tem grande apelo, devido ao parque industrial de produção de semicondutores, já instalado, e ao conhecimento técnico adquirido na fabricação destes dispositivos. Dentro desse grupo destacam-se as tecnologias baseadas em junções de Josephson e os pontos quânticos, que serão discutidas a seguir.

3.4.2.1 Computação Quântica Baseada em Pontos Quânticos

Pontos quânticos (LOSS; DIVINCENZO, 1998) são pequenos dispositivos feitos de semicondutores que operam baseados no bloqueio de Coloumb, com portadores de carga confinados nas três dimensões do espaço. Pontos quânticos se comportam de maneira similar a átomos artificiais devido a seu espectro de energia discreto (KOUWENHOVEN; AUSTING; TARUCHA, 2001).

Para atingir o bloqueio de Coloumb, a temperatura do sistema deve ser extremamente baixa. As implementações usando arseneto de gálio (GaAs), por exemplo, devem ser resfriadas abaixo de 1K (HANSON *et al.*, 2007).

Duas codificações de qubits em pontos quânticos foram propostas, uma usando o estado fundamental e o primeiro estado excitado como base computacional ($|0\rangle$ e $|1\rangle$) (BARENCO *et al.*, 1995), e outra usando o *spin* dos elétrons contidos no ponto como qubits (BURKARD; LOSS; DIVINCENZO, 1999).

A implementação baseada no *spin* eletrônico apresenta algumas vantagens sobre a primeira: apenas as duas dimensões usadas como base computacional existem, o que impede que o qubit assuma um valor estranho ao convencionado. Além disso, o tempo de perda de fase do *spin* em GaAs pode ser da ordem de milissegundos (KIKAWA; AWSCHALOM, 1998), enquanto que o tempo de uma operação é da ordem de $10^{-9}s$ (NIELSEN; CHUANG, 2000).

Uma das grandes vantagens do uso de pontos quânticos é que o controle de estados, operadores e medições são feitos através de sinais elétricos, tecnologia já comum em computadores clássicos, logo, circuitos desse tipo poderiam ser integrados sem grandes dificuldades nos computadores tradicionais. Além disso, a fabricação desses dispositivos poderia usar as plantas industriais já instaladas para a fabricação de circuitos integrados (CIs).

3.4.2.2 Qubits Supercondutores com Junção de Josephson

Uma junção de Josephson é um sistema de três camadas, sendo que as duas externas são supercondutoras, enquanto a central é um isolante (MAKHLIN; SCHÖN; SHNIRMAN, 2001). Uma ou mais junções são então ligadas e colocadas em um circuito elétrico, formando os qubits (MAKHLIN; SCHÖN; SHNIRMAN, 2001; MARTINIS *et al.*, 2002).

Dois grupos de implementações podem ser distinguidos: *qubit carga* e *qubit fluxo* (MAKHLIN; SCHÖN; SHNIRMAN, 2001). No caso do qubit carga, a carga da capacitância da junção é usada como grau de liberdade para a codificação do estado computacional, já no segundo essa codificação é feita através do fluxo magnético em um anel que contém a junção. O segundo também é chamado na literatura de qubit fase, pois o fluxo também é visto como fase do anel.

Duas grandes vantagens desses sistemas são a simplicidade do controle, que permite uma manipulação precisa do estado (MAKHLIN; SCHÖN; SHNIRMAN, 2001) e a

habilidade de redução de fontes de decoerência, possibilitando o aumento no tempo de decoerência (MARTINIS *et al.*, 2002). O controle do estado pode ser feito com correntes, indução magnética ou tensões elétricas (MAKHLIN; SCHÖN; SHNIRMAN, 2001; HARRIS *et al.*, 2010). Para haver manipulação coerente do estado do sistema, parâmetros de acoplamento devem ser devidamente regulados (MARTINIS *et al.*, 2002) e a temperatura de operação deve ser baixa ($\approx$ dezenas mK) (MAKHLIN; SCHÖN; SHNIRMAN, 2001).

3.4.3 Óptica Linear

O uso de óptica linear é outro esquema promissor para a implementação de computadores quânticos (KNILL; LAFLAMME; MILBURN, 2001). Os operadores quânticos são implementados através de lentes e espelhos especiais, chamados *divisores de feixe* e *deslocadores de fase*, e os estados computacionais podem ser representados pelo caminho seguido pelos fótons, por sua polarização ou pelo momento angular.

A maior vantagem na adoção das tecnologias de implementação baseadas em óptica linear é a possibilidade de operação em temperatura ambiente, ao contrário das demais tecnologias. Outra vantagem é que fótons parecem não sofrer perda de coerência, o que torna essas tecnologias extremamente interessantes (KOK *et al.*, 2007).

Finalmente, o uso de fótons é até hoje a única proposta realista para a implementação de comunicação de estados quânticos para longas distâncias (KNILL; LAFLAMME; MILBURN, 2001), o que simplificaria a interface comunicação/computação.

Uma dificuldade nesse caso é a falta de um mecanismo eficiente para o controle do estado. A escolha da ordem de aplicação de portas é feita *a priori*, dada a dificuldade de posicionar os elementos ópticos com precisão em tempo hábil. Isso limita a quantidade de operações que um determinado *hardware* é capaz de realizar, ao contrário do que aconteceria em outras tecnologias. No entanto, operações podem ser realizadas rapidamente, na ordem de uma operação a cada $10^{-14}s$ (NIELSEN; CHUANG, 2000).

Um outro problema é que os operadores ópticos tem grande probabilidade de falha (KOK *et al.*, 2007), logo a operação precisa ser repetida diversas vezes para minimizar a probabilidade de erro.

3.4.4 Ressonância Magnética Nuclear

A primeira implementação de um algoritmo quântico, o de Shor, foi realizada em RMN, por isso, essa tecnologia despertou grande interesse na comunidade (VANDERSYPEN *et al.*, 2001). Computadores quânticos baseados em RMN usam moléculas inteiras para armazenar os estados quânticos. Para possibilitar a observação desses estados um grande número de moléculas idênticas devem ser usadas, isso pois o sinal de momento magnético nuclear de uma única molécula é fraco para leitura (NIELSEN; CHUANG, 2000).

Em geral, elementos no estado líquido são usados para a computação. Como cada estado quântico é armazenado no momento de um núcleo, um número de núcleos é igual ao número de qubits. Por isso, grandes moléculas tem sido sintetizadas para permitir um número razoável de qubits. Essa abordagem, no entanto, leva a sinais de medição cada vez mais fracos (WARREN, 1997).

A grande vantagem no uso dessa técnica é que seus conceitos são muito bem conhecidos, com equipamentos robustos e maduros, o que elimina dificuldades relacionadas à preparação dos experimentos (NIELSEN; CHUANG, 2000). Além disso, esse tipo de tecnologia é o que se mostrou melhor em termos de número de operações antes da decoerência, permitindo frequências entre 10^3 e 10^6 Hz (NIELSEN; CHUANG, 2000). Com uso desta técnica, computadores de até sete qubits já foram implementados (NIELSEN; CHUANG, 2000). No entanto, diversos autores acreditam que tal solução não será usada na prática devido à sua falta de escalabilidade (WARREN, 1997).

As operações são feitas através da aplicação de fluxos eletromagnéticos sobre o conjunto de moléculas. Para a inicialização do estado, em geral é necessário o res-

friamento do conjunto para que os momentos magnéticos se alinhem. Finalmente, as medições são feitas através do sinal elétrico induzido pelo momento magnético.

3.4.5 Armadilhas de Íon

Armadilhas de íon são assim chamadas pois, literalmente, confinam íons nas três dimensões do espaço. A informação é então armazenada nos *spins* eletrônicos. Para isso é necessário que os íons sejam resfriados, de forma a reduzir sua energia cinética a níveis menores do que a energia dos *spins*, permitindo assim sua leitura e controle (NIELSEN; CHUANG, 2000). A armadilha é feita de forma eletromagnética, enquanto que o resfriamento é normalmente feito com lasers nas três dimensões (CIRAC; ZOLLER, 1995).

A grande vantagem dessa abordagem é que teoricamente um grande número de operações pode ser realizado antes da perda de coerência ($\approx 10^{13}$) (NIELSEN; CHUANG, 2000). Isso se deve em parte ao relativamente longo tempo de decoerência ($\approx 10^{-1}s$), mas principalmente à velocidade com que as operações podem ser realizadas ($10^{-14}s$). As operações são rápidas uma vez que são realizadas com pulsos de laser e medidas através de fotodetectores (CIRAC; ZOLLER, 1995).

Finalmente, a grande desvantagem do uso de armadilhas de íon é a dificuldade em se preparar o estado inicial, o processo de prender os íons na armadilha e resfriá-los é delicado e instável (NIELSEN; CHUANG, 2000).

3.4.6 Outras Tecnologias

Outras tecnologias foram teorizadas ou testadas na prática, cada uma com suas vantagens e desvantagens. Podemos destacar as Cavidades Eletrodinâmicas Quânticas, que também usam o fóton como portador do estado quântico, mas nesse caso a luz encontra-se em uma cavidade formada por espelhos e lentes (PELLIZZARI *et al.*, 1995). Como no caso de óptica linear, as operações são realizadas através de lentes e espelhos

especiais (RAIMOND; BRUNE; HAROCHE, 2001). A grande dificuldade dessa abordagem é emaranhar estados, o que é feito com a ajuda de átomos fora da cavidade (NIELSEN; CHUANG, 2000).

Uma alternativa ainda menos aceita, mas que tem resultados recentes interessantes é o uso de vagos de nitrogênio em diamantes (JELEZKO *et al.*, 2004). Nessa abordagem, elétrons localizados na impureza dos diamantes são usados para codificar o qubit. O grande interesse por trás dessa tecnologia é o bom isolamento provido pelo diamante, que permite uma operação com baixa decoerência. Resultados mais recentes (SAR *et al.*, 2012) incluem a execução do algoritmo de Grover e de portas de múltiplos qubits com fidelidade de mais de 90%.

Além dessas, outras tecnologias podem ser citadas, tais como reticulados ópticos (BLOCH, 2005), *spin* nuclear em silício (KANE, 1998), entre outros. No entanto, não é intuito deste trabalho fazer uma revisão completa de todas as tecnologias propostas, apenas as mais relevantes na literatura foram brevemente discutidas.

Recentemente, uma técnica ligada à comunicação (e não à computação propriamente) foi proposta (RITTER *et al.*, 2012). Nessa abordagem átomos de rubídio são colocados em uma cavidade ressonante, que é associada a uma cavidade eletrodinâmica quântica. É possível interconverter estados quânticos de uma cavidade para outra e da cavidade eletrodinâmica o estado pode ser enviado para outro ponto da rede via fibra óptica. A fidelidade alcançada é da ordem de 85%, número razoável em tecnologias quânticas. Para se tornar realmente prático, o esquema precisaria ser acoplado a um esquema de computação.

3.4.7 Tempo de decoerência e frequência de operação de diferentes tecnologias

Um dos fatores mais importantes para comparar as tecnologias de implementação é o número de operações que se pode realizar, em média, antes que a perda da coerência

ocorra. Nielsen e Chuang (2000) fazem uma síntese interessante desta métrica para diversas tecnologias, tendo por base o tempo médio de para perda de coerência e o tempo médio de uma operação. Esta síntese é apresentada, conforme o livro de Nielsen e Chuang, na Tabela 1.

Tabela 1: Estimativas de tempo de decoerência (τ_Q), tempo de operação τ_{op} e número de operações $\eta_{op} = \lambda^{-1} = \tau_Q/\tau_{op}$ para alguns candidatos a qubits. A última coluna apresenta o número de operações estimado para cada tecnologia (NIELSEN; CHUANG, 2000).

Tecnologia	τ_Q (s)	τ_{op} (s)	$\eta_{op} = \lambda^{-1}$
Spin Nuclear	$10^{-2} - 10^8$	$10^{-3} - 10^{-6}$	$10^5 - 10^{14}$
Spin Eletrônico	10^{-3}	10^{-7}	10^4
Armadilhas de Íon	10^{-1}	10^{-14}	10^{13}
Elétron - Au	10^{-8}	10^{-14}	10^6
Elétron - GaAs	10^{-10}	10^{-13}	10^3
Pontos Quânticos	10^{-6}	10^{-9}	10^3
Cavidades Ópticas	10^{-5}	10^{-14}	10^9
Cavidades Microondas	10^0	10^{-4}	10^4

3.5 Sumário do Capítulo 3

Neste capítulo, uma formulação sobre a qual é possível desenvolver a mecânica quântica foi apresentada e as principais características da teoria quântica bem como seus postulados foram discutidos. Foram tratado os conceitos relativos ao modelo de circuito da computação quântica bem como o algoritmo de busca de Grover, especialmente útil neste trabalho. Finalmente algumas tecnologias de implementação de computadores quânticos foram discutidas.

No próximo capítulo é realizada uma revisão bibliográfica sobre a criptografia pós-quântica, outro tema de grande importância neste trabalho.

4 CRIPTOGRAFIA PÓS-QUÂNTICA

Neste capítulo, os conceitos de segurança da informação e os principais métodos criptográficos assimétricos, também chamados de criptografia de chave pública, são apresentados. A seguir, discute-se a criptografia pós-quântica, dando especial atenção aos criptosistemas baseados em códigos corretores de erros e às assinaturas CFS.

4.1 Introdução à Segurança da Informação

Nesta seção, uma revisão dos serviços e mecanismos básicos de segurança da informação é feita. Essa revisão visa clarificar o que está compreendido na expressão “segurança da informação”, para que se possa entender que tipos de problemas precisam ser resolvidos. A partir desse entendimento, é possível discutir os impactos que terão os computadores quânticos sobre a segurança da informação.

John Howard (1998) define a segurança da informação como “prevenir adversários de atingir seus objetivos através de acesso ou uso não autorizados de computadores ou redes”. Essa definição é útil como um primeiro entendimento, mas incompleta no sentido que não provê subsídios para a implementação de técnicas de segurança.

A segurança também pode ser definida como (BISHOP, 2002; STALLINGS, 2010) um conjunto de medidas preventivas factíveis dentro de um processo. Ou seja, a segurança deve ser parte do que se pode exigir de um sistema e não pode ser vista como um produto final. Também é necessário ressaltar que essas medidas visam adversários específicos, no sentido que dependem de seu poder de ataque. Não existe solução

perfeita de segurança.

Na literatura (STALLINGS, 2010), a segurança costuma ser caracterizada por cinco serviços: confidencialidade, integridade, autenticidade, irretratabilidade e disponibilidade. Essa separação permite, finalmente, a escolha de métodos e algoritmos para a implementação prática de um sistema de segurança.

1. Confidencialidade: é a garantia que nenhuma informação será revelada, acessada ou manipulada por um usuário não autorizado. Algumas sutilezas residem no termo “nenhuma”: um sistema que vise a confidencialidade deve ocultar repetições ao longo de uma mensagem, ou mesmo, não deve ser possível observar que duas mensagens idênticas foram enviadas em momentos distintos.

2. Integridade: é a garantia que nenhuma alteração passará despercebida pelos usuários. Nota-se que não há garantia que nenhuma alteração ocorrerá, no entanto, num sistema que garanta a integridade da mensagem será possível detectar essa alteração.

3. Autenticidade: visa impedir que um atacante personifique um usuário legítimo. Em um sistema com serviço de autenticidade é possível detectar que um usuário não legítimo está mandando mensagens como se fosse um usuário legítimo.

4. Irretratabilidade: é a capacidade de provar para terceiros que uma comunicação entre duas partes ocorreu. O receptor pode provar que o emissor enviou a mensagem e o emissor pode provar que o receptor a recebeu.

5. Disponibilidade: é a garantia que um serviço ou recurso não será negado a um usuário legítimo. Nota-se que este serviço não depende exclusivamente de algoritmos, é necessário garantir disponibilidade nos níveis de *hardware* e rede, com uso de redundância. Alguns autores (STALLINGS, 2010) sequer consideram disponibilidade como um serviço de segurança.

4.2 Criptografia Assimétrica

Para prover os serviços mencionados na Seção 4.1, diversos algoritmos são utilizados em conjunto. Os algoritmos podem ser agrupados em algumas classes, dependendo de sua função (BISHOP, 2002).

Duas grandes classes de algoritmos criptográficos têm especial importância: a dos algoritmos simétricos e a dos algoritmos assimétricos. Algoritmos simétricos dependem de uma informação secreta compartilhada (normalmente denominada chave de sessão) e algoritmos assimétricos dependem de uma informação pública confiável (certificada por alguma autoridade confiável, ou que possa ser conferida via algum canal seguro) (STALLINGS, 2010).

A existência destas classes tem uma explicação prática: algoritmos simétricos dependem de um acordo da chave de sessão (que não pode ser usada por muito tempo), enquanto que algoritmos assimétricos são ineficientes do ponto de vista de tempo de cálculo (STALLINGS, 2010).

O foco deste trabalho são os métodos assimétricos. Uma cifração assimétrica é feita com o uso de uma chave pública, apenas o usuário que conheça a chave privada correspondente é capaz de decifrar o criptograma. Além da cifra assimétrica, as assinaturas digitais são métodos assimétricos. Uma assinatura é feita com a chave privada e pode ser verificada com o uso da chave pública equivalente, dessa forma o usuário gerando a assinatura prova ter posse da chave privada (STALLINGS, 2010).

A segurança de um criptossistema é associada ao número de passos computacionais necessários para quebrá-lo, sem o conhecimento da chave privada, usando o melhor ataque conhecido. De maneira quantitativa, define-se o nível de segurança como o $\log_2$ de número de passos. Ou seja, no nível de segurança de 80, são necessários 2^{80} passos para se quebrar o sistema (aproximadamente 9 milhões de anos em um computador a 4 GHz) (STALLINGS, 2010). Para critérios de comparação, o nível

de segurança de 80 é considerado obsoleto para contratos com o governo americano, desde 2010 (BARKER *et al.*, 2007).

Entre os principais criptossistemas assimétricos, podemos destacar o RSA (RIVEST; SHAMIR; ADLEMAN, 1978) e aqueles baseados em curvas elípticas (CCE) (HANKERSON; MENEZES; VANSTONE, 2003). A segurança do RSA é baseada no problema da fatoração de números, a chave privada é um fator primo da chave pública, no entanto encontrar esse fator é um problema difícil (da ordem de $O(e^{\sqrt[3]{\ln N (\ln \ln N)^2}})$, onde N é o número de bits do número em questão) para chaves grandes (o RSA usa chaves de 2048 bits para o nível de segurança 96). Já sistemas baseados em curvas elípticas usam problemas inerentes a essas estruturas matemáticas para a realização da criptografia. No entanto, quebrar estes sistemas é uma tarefa que pode ser reduzida ao problema do logaritmo discreto, por sua vez redutível ao problema de fatoração.

A definição de nível de segurança abstrai a informação de que tipo de computador está sendo usado para o ataque. Se apenas computadores clássicos estão sendo usados, é evidente que um computador duas vezes mais poderoso será capaz de quebrar o criptossistema em questão duas vezes mais rápido. No entanto, caso um novo algoritmo de ataque seja descoberto o número de passos necessários pode mudar. A redução do número de passos necessários para quebrar um criptossistema para um valor menor do que o que ele foi projetado é chamado de quebra do criptossistema. Isso acontece quando se considera computadores quânticos. O algoritmo de Shor é capaz de resolver o problema da fatoração de números em N^3 passos, onde N é o tamanho do número que se deseja fatorar. No caso do RSA 2048, $2048^3 = 2^{33}$ passos são necessários (e não 2^{96} , como projetado), caracterizando uma quebra deste criptossistema.

Uma *assinatura digital*, seja RSA ou CCE, é uma *tag* adicionada à mensagem. Essa *tag* depende do conteúdo da mensagem e da chave privada, podendo ser verificada com a chave pública. Uma assinatura digital é uma prova matemática da posse da chave privada. Com uma assinatura digital pode-se fornecer os serviços de

autenticidade, irretratibilidade e integridade.

4.3 Motivação da Criptografia Pós-Quântica

O algoritmo quântico de Shor (SHOR, 1997) é capaz de fatorar números inteiros, ou resolver o problema do logaritmo discreto, em tempo $O((\log N)^3)$, ameaçando criptossistemas de chave pública atuais (RSA e CCE), cuja segurança é baseada nestes problemas. Por exemplo, a quebra do RSA 1024, com uso de um computador quântico, se daria em $1024^3 = 2^{30}$ passos ao invés de 2^{80} passos para os quais ele foi projetado.

Em vista disso, criptógrafos deram início a uma busca por soluções de segurança alternativas às existentes (BERNSTEIN; BUCHMANN; DAHMEN, 2008). Algumas dessas alternativas vieram da própria mecânica quântica, o protocolo de distribuição quântica de chaves (QKD, em inglês) (BENNETT; BRASSARD, 1984; EKERT, 1991) foi uma delas.

O QKD permite a distribuição fisicamente segura de uma chave de sessão, tendo como base os princípios quânticos (emaranhado e superposição). Esse esquema tem a grande vantagem de impossibilitar fisicamente a espionagem da informação por um terceiro (BENNETT; BRASSARD, 1984), o que o torna, sem dúvidas, muito atrativo. O grande problema com este método é que ele não permite a autenticação dos usuários, ou seja, não é possível saber, com certeza, com quem se está trocando informação (BERNSTEIN; BUCHMANN; DAHMEN, 2008).

De fato, nenhum método puramente quântico capaz de fornecer a totalidade dos serviços de segurança foi descoberto (BERNSTEIN; BUCHMANN; DAHMEN, 2008). Em especial, pode-se citar os serviços de autenticação e irretratibilidade, classicamente implementados através das assinaturas digitais. Não existe, até a presente data, e parece difícil (BARNUM *et al.*, 2002), criar assinaturas digitais puramente quânticas. Alguns esquemas de autenticação foram propostos, mas nenhum satisfazendo as ne-

cessidades de segurança cumpridas hoje pelas assinaturas (BARNUM *et al.*, 2002).

Dado este cenário, criptógrafos passaram a buscar algoritmos clássicos baseados em problemas que não podem ser eficientemente resolvidos com computadores quânticos, a esses algoritmos deu-se o nome de pós-quânticos (BERNSTEIN; BUCHMANN; DAHMEN, 2008). Em especial, dentre os métodos pós-quânticos, pode-se destacar três grupos: códigos corretores de erros, reticulados e sistemas multi-variados quadráticos.

O foco deste trabalho são os criptossistemas baseados em códigos corretores de erros, em especial nos criptossistemas McEliece e Niederreiter, que têm grande destaque entre os criptossistemas pós-quânticos.

4.4 Códigos Corretores de Erros

Em teoria dos códigos, códigos corretores de erros são códigos capazes de identificar a presença de, e em alguns casos corrigir, um determinado número de erros em uma palavra. Um código é definido como um conjunto de palavras possíveis. Esse tipo de código foi inicialmente motivado para as aplicações de comunicação, onde erros de transmissão são comuns e em geral o custo de retransmissão é alto. Códigos corretores funcionam com o uso de redundância, que pode ser maior ou menor, melhorando ou piorando a capacidade de correção de um código. A Definição 19 formaliza o conceito de códigos (HUFFMAN; PLESS, 2003).

Definição 19. *Um código $\mathbb{C}(n, M)$ sobre $\mathbb{F}_q$ é um subconjunto de $\mathbb{F}_q^n$ de tamanho M . Onde $\mathbb{F}_q^n$ denota n -uplas de elementos de $\mathbb{F}_q$. Os elementos de $\mathbb{C}$ são chamados palavras de código.*

Códigos especialmente úteis no contexto deste trabalho são códigos lineares. Um código linear $\mathbb{C}$ de dimensão k é um sub-espço de $\mathbb{F}_q^n$, chamado código linear $[n, k]$ sobre $\mathbb{F}_q$. Este código linear possui q^k palavras de código (HUFFMAN; PLESS, 2003). Um código linear pode ser representado por sua matriz geradora G , ou de maneira

equivalente por sua matriz verificadora de paridade H . Uma matriz geradora de um código linear $\mathbb{C}[n, k]$ é qualquer matriz $k \times n$, cujas linhas de G formem uma base para $\mathbb{C}$ (HUFFMAN; PLESS, 2003). Em geral, é possível definir uma diversidade de matrizes geradoras para um dado código.

Já uma matriz verificadora de paridade é uma matriz que multiplica uma palavra do código, resultando no vetor nulo. Ou seja, uma matriz de verificadora de paridade $H (n - k) \times n$ define um código linear $\mathbb{C}[n, k]$ como $\mathbb{C} = \{x \in \mathbb{F}_q^n | Hx^T = 0\}$. Da mesma forma que para a matriz geradora, podem existir diversas matrizes verificadoras de paridade para um mesmo código (HUFFMAN; PLESS, 2003).

Uma família de códigos bem interessantes é a família Reed-Solomon Generalizada. Barreto (2011) define códigos Reed-Solomon Generalizados como:

Definição 20. *Dada uma sequência $L = (L_0, \dots, L_{n-1}) \in \mathbb{F}_q^n$ (chamada o suporte) de elementos distintos e uma sequência $D = (D_0, \dots, D_{n-1}) \in \mathbb{F}_q^n$ de elementos não nulos, o código Reed-Solomon Generalizado $\text{GRS}_t(L, D)$ é o código $[n, k, t+1]$ linear corretor de erros definido pela matriz de paridade*

$$H = \text{vdm}(t, L) \cdot \text{diag}(D) \in \mathbb{F}_q^{t \times n}.$$

Onde $\text{vdm}(t, L)$ é a matriz de Vandermonde com t linhas e com os elementos de L como componentes e $\text{diag}(D)$ é uma matriz diagonal formada pelos elementos de D . A distância de um código¹ GRS é, portanto, pelo menos $t + 1$ onde t é o número de linhas da matriz de paridade (BARRETO, 2011). Uma outra família de interesse neste trabalho é a de códigos *alternantes*, conforme a Definição 22, eles se baseiam no conceito de *subcódigo*, mostrado na Definição 21.

Definição 21. *Um subcódigo SC de um código C , definido sobre um corpo K , é um código definido sobre um subcorpo S de K .*

¹A distância de um código é dada pela menor *distância de Hamming* (i.e. o número de coordenadas em que dois vetores divergem), entre cada par de vetores descrita pelo código.

Definição 22. *Um código alternante é um subcódigo de subcorpo de um código Reed-Solomon Generalizado.*

O uso de códigos corretores de erro para fins criptográficos foi proposto por McEliece (1978). A ideia por trás desse uso é a inserção voluntária de erros, que só podem ser corrigidos por um usuário que conheça o código.

4.5 Criptossistemas McEliece e Niederreiter

McEliece (1978) e Niederreiter (1986) são dois dos criptossistemas mais antigos conhecidos, não foram adotados à época devido aos tamanhos de chaves necessários (da ordem de 262 Kbits para um nível de segurança de aproximadamente 65 (MCELIECE, 1978), no caso do McEliece, por exemplo).

Ambos são baseados no problema da decodificação de síndromes em códigos corretores de erros. A princípio, não existe uma definição sobre qual código deve ser usado. No entanto alguns códigos apresentam melhores resultados, como é o caso de códigos de Goppa (GOPPA, 1970) apresentado na Seção 4.6 deste documento.

A geração de chaves, em ambos os casos, consiste na criação do código base, ou seja, na escolha de uma matriz geradora de palavras de código G (no caso do McEliece (MCELIECE, 1978)), ou de forma equivalente, de uma matriz verificadora de paridade H (no caso do Niederreiter (NIEDERREITER, 1986)). Essa matriz é, a seguir, “camuflada”, de maneira que a estrutura do código seja preservada. A matriz camuflada é usada como chave pública, enquanto a estrutura do código é usada como chave privada.

A estrutura do código permite a decodificação eficiente de uma síndrome, logo apenas um usuário em posse dessa estrutura é capaz de realizar a decifração. Esse processo depende do código usado, cada código possui um método próprio de decodificação.

Já o processo de cifração se resume a criação de uma palavra de código (multiplicação pela matriz geradora) e adição de um número pré-definido de erros (número ligado à capacidade de correção do código) (MCELIECE, 1978; NIEDERREITER, 1986). É fácil notar que tal método não apresenta segurança semântica, ou seja, um texto cifrado difere do texto claro original em alguns bits apenas. Logo se o texto claro fosse um texto em linguagem natural, seria trivial encontrar o texto claro. Por esse motivo os sistemas McEliece e Niederreiter são usados para cifração de chaves de sessão (totalmente aleatórias), dificultando sua recuperação semântica.

4.6 Códigos de Goppa

A família de códigos de Goppa (GOPPA, 1970) é uma das mais importantes para fins criptográficos. Códigos de Goppa vem sendo amplamente usados em conjunto com os criptossistemas McEliece e Niederreiter (BERNSTEIN, 2008; FINIASZ; SENDRIER, 2009; EISENBARTH *et al.*, 2009; MISOCZKI; BARRETO, 2009). A Definição 23 formula um código de Goppa.

Definição 23. *Dado um primo p , $q = p^m$ com $m > 0$, uma sequência $L = (L_0, \dots, L_{n-1}) \in \mathbb{F}_q$ de elementos distintos, e um polinômio mônico irreduzível $g(x) \in \mathbb{F}_q[X]$ de grau t (polinômio gerador) tal que $g(L_i) \neq 0$ para $0 \leq i < n$, o código de Goppa $\Gamma(L, g)$ é o código $\mathbb{F}_p$ -correspondente alternante a $\text{GRS}_t(L, D)$ sobre $\mathbb{F}_q$, onde $D = (g(L_0)^{-1}, \dots, g(L_{n-1})^{-1})$.*

A distância de um código de Goppa é pelo menos $2t + 1$ (GOPPA, 1970); logo, um código de Goppa binário (sobre $\mathbb{F}_2$) pode corrigir até t erros, usando o algoritmo de Patterson (PATTERSON, 1975) (descrito a seguir).

Na Definição 25 apresenta-se uma definição alternativa para códigos de Goppa, por sua função de síndrome, para isso a definição de síndrome é apresentada na Definição 24, como uma função linear de e (BARRETO, 2011).

Definição 24. A síndrome de Goppa é definida como qualquer palavra $e \in \mathbb{F}_{p^n}$ escrita de maneira polinomial $s_e \in \mathbb{F}_q[X]$ como

$$s_e(x) = \sum_{i=0}^{n-1} \frac{e_i}{x - L_i} \mod g(x). \quad (4.1)$$

Definição 25. O $[n, n - mt]$ código de Goppa, definido sobre $\mathbb{F}_p$ com suporte L e polinômio gerador g , é o núcleo da função síndrome (Equação 4.1), i.e. o conjunto $\Gamma(L, g) := \{e \in \mathbb{F}_{p^n} \mid s_e \equiv 0 \mod g\}$.

Escrevendo $s_e(x) := \sum_i s_i x^i$ para algum $s \in \mathbb{F}_{q^n}$, pode-se mostrar que $s^T = He^T$, com:

$$H = \begin{bmatrix} g_t & 0 & \dots & 0 \\ g_{t-1} & g_t & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_1 & g_2 & \dots & g_t \end{bmatrix} \cdot \begin{bmatrix} 1 & \dots & 1 \\ L_0 & \dots & L_{n-1} \\ L_0^2 & \dots & L_{n-1}^2 \\ \vdots & \ddots & \vdots \\ L_0^{t-1} & \dots & L_{n-1}^{t-1} \end{bmatrix} \cdot \begin{bmatrix} d_0 & 0 & \dots & 0 \\ 0 & d_1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_{n-1} \end{bmatrix} \quad (4.2)$$

A decodificação de códigos de Goppa é feita através do algoritmo de Patterson (PATTERSON, 1975), apresentado no Algoritmo 1 (BARRETO, 2011). O objetivo do algoritmo é encontrar um padrão de erros e dada sua síndrome $s(x)$ e o código de Goppa, representado por seu polinômio g e pelo suporte L . O algoritmo é baseado no algoritmo estendido de Euclides, aplicado a corpos finitos.

O padrão de erros consiste de um vetor do tamanho da palavra que se quer corrigir, as posições que contém erro na palavra são marcadas com um bit 1 no vetor padrão de erros. Na primeira parte do algoritmo (linhas 1 a 10) é feita a montagem do *polinômio localizador de erros* $\sigma(x)$, cujas raízes indicam as posições com erro. Na segunda parte (linhas 14 a 20), as raízes desse polinômio são encontradas. A saída “INDECODIFICÁVEL” significa que a síndrome não pode ser decodificada, isso ocorre quando o número de

erros é maior do que o código é capaz de corrigir, o que pode acontecer por erros de transmissão ou tentativa de fraude.

Algoritmo 1 Decodificador de Patterson para um código binário de Goppa

Entrada: Polinômio de Goppa g , suporte L , matriz de paridade H .

Entrada: Síndrome s em forma polinomial.

Saída: Padrão de erros e tal que $s = eH^T$

```

1:  $v \leftarrow \sqrt{x+1/s} \bmod g$ 
2:  $F \leftarrow v, G \leftarrow g, B \leftarrow 1, C \leftarrow 0, t \leftarrow \deg(g)$ 
3: while  $\deg(G) > \lfloor t/2 \rfloor$  do
4:    $F \leftrightarrow G, B \leftrightarrow C$ 
5:   while  $\deg(F) \geq \deg(G)$  do
6:      $j \leftarrow \deg(F) - \deg(G), h \leftarrow F_{\deg(F)} / G_{\deg(G)}$ 
7:      $F \leftarrow F - hx^j G, B \leftarrow B - hx^j C$ 
8:   end while
9: end while
10:  $\sigma \leftarrow G^2 + xC^2$ 
11: if  $x^{2^m} + x \bmod \sigma \neq 0$  then
12:   return “INDECODIFICÁVEL” – (raízes fora do corpo base  $\mathbb{F}_{2^m}$ )
13: end if
14: for  $i = 0 \rightarrow 2^m - 1$  do
15:   if  $\sigma(i) = 0$  then
16:      $e[i] := 1$ 
17:   else
18:      $e[i] := 0$ 
19:   end if
20: end for
21: Calcule a síndrome  $s^* \leftarrow eH^T$ 
22: if  $s^* \neq s$  then
23:   return “INDECODIFICÁVEL”
24: end if
25: return  $e$ 

```

Para uma prova formal do funcionamento do algoritmo, a leitura do artigo original do decodificador (PATTERSON, 1975) é recomendada.

4.6.1 Códigos de Goppa Quase-Diádicos

O uso de códigos de Goppa QD foi proposto (MISOCZKI; BARRETO, 2009) como forma de reduzir o tamanho das chaves. Códigos QD são apresentados na Definição 26.

Definição 26. *Um código corretor linear quase-diádico é um código com uma matriz*

geradora (ou verificadora de paridade) quase-diádica (i.e. uma matriz composta por blocos diádicos).

Uma matriz diádica pode ser recursivamente definida (MISOCZKI; BARRETO, 2009): toda matriz 1×1 é diádica, e para $k > 0$, toda matriz diádica tem dimensão $2^k \times 2^k$ e a forma mostrada na Equação 4.3, onde A e B são matrizes diádicas de dimensão $2^{k-1} \times 2^{k-1}$.

$$M = \begin{bmatrix} A & B \\ B & A \end{bmatrix}$$

O Teorema 2 caracteriza todas as matrizes que são simultaneamente diádicas e de Cauchy, condição necessária para construir códigos binários de Goppa com matrizes verificadoras de paridade diádicas (MISOCZKI; BARRETO, 2009).

Teorema 2. *Seja $H \in \mathbb{F}_q^{n \times n}$, com $n > 1$, uma matriz simultaneamente diádica, $H = \Delta(h)$ para algum $h \in \mathbb{F}_{q^n}$, e de Cauchy, $H = C(z, L)$ para duas sequências disjuntas $z \in \mathbb{F}_{q^n}$ e $L \in \mathbb{F}_{q^n}$ de elementos distintos. Então, $\mathbb{F}_q$ tem característica 2, h satisfaz*

$$\frac{1}{h_{i \oplus j}} = \frac{1}{h_i} + \frac{1}{h_j} + \frac{1}{h_0}, \quad (4.3)$$

e $z_i = 1/h_i + \omega$, $L_j = 1/h_j + 1/h_0 + \omega$ para algum $\omega \in \mathbb{F}_q$.

Dado que esta limitação constitui um sub-conjunto dos códigos de Goppa, nenhuma alteração nos algoritmos (exceto pela geração de matrizes) se faz necessária. Logo pode-se prosseguir com a decodificação em códigos de Goppa QD da mesma forma que se faria em códigos de Goppa.

4.7 Assinaturas CFS

Nos esquemas McEliece e Niederreiter originais não existia uma previsão para assinaturas digitais. No entanto Matthieu Courtouis, Matthieu Finiasz e Nicolas Sendrier propuseram um esquema de assinaturas digitais baseado no sistema Niederreiter e que pode servir como um complemento para aqueles (COURTOIS; FINIASZ; SENDRIER, 2001). As assinaturas CFS são tidas como as mais promissoras para a implementação de assinaturas digitais pós-quânticas. Também para esse esquema foi proposto o uso de códigos de Goppa QD, uma vez que o problema de tamanho extensivos de chaves é ainda mais crítico nesse caso (BARRETO *et al.*, 2010).

Assinar uma mensagem implica em calcular um *hash criptográfico* na forma de uma síndrome, que é então decodificado, resultando em um vetor de erros. O problema é que nem todas as síndromes são decodificáveis, logo um número aleatório (na prática, incremental) entra no cálculo do *hash* até que uma síndrome decodificável seja encontrada.

Fica claro que a dificuldade computacional deste problema resume-se em encontrar um valor do contador que gera uma síndrome decodificável. O número total de síndromes decodificáveis é $\binom{n}{t}$ (vetores de n bits com t bits iguais a ‘1’), o número total de vetores é 2^{mt} (vetores de mt bits), para simplificar $n \approx 2^m$, logo a densidade de síndromes decodificáveis é dada pela Equação 4.4.

$$\frac{\binom{n}{t}}{2^{mt}} \approx \frac{\frac{n^t}{t!}}{2^{mt}} \approx \frac{\frac{n^t}{t!}}{n^t} \approx \frac{1}{t!} \quad (4.4)$$

Logo, a dificuldade para se encontrar um síndrome decodificável é da ordem de $O(t!)$. Pode-se concluir trivialmente que esse resultado limita o valor de t (número de erros que podem ser corrigidos).

Como acontece com outros métodos pós-quânticos, as assinaturas CFS sofrem de

falta de praticidade. Trabalhos recentes (BARRETO *et al.*, 2010) chegaram aos resultados (usando $p = 2$ e matrizes QD) mostrados na Tabela 2.

Tabela 2: Conjunto de parâmetros para CFS ((BARRETO *et al.*, 2010)).

Nível de Segurança	m	t	Esforço para assinar	Tamanho da chave (KiB)
80	15	12	2^{29}	169
100	20	12	2^{29}	7248
120	25	12	2^{29}	289956

A limitação no tamanho do parâmetro t ajuda ataques baseados no paradoxo generalizado do aniversário² (*Generalized Birthday Attack, GBA*) (FINIASZ, 2010), reduzindo o nível de segurança desse esquema.

Um outro problema com o esquema CFS é que para ser totalmente seguro, é preciso que o código de Goppa usado seja indistinguível de um código binário aleatório (DALLOT, 2008). Como consequência, os parâmetros do código precisam ser aumentados, fazendo com que cresça o tamanho das chaves e o tempo para gerar uma assinatura, saindo dos limites práticos.

4.7.1 Assinaturas CFS Paralelas

O esquema CFS paralelo (FINIASZ, 2010) foi proposto como uma alternativa ao esquema anterior. Nesse novo esquema, são aceitos um total de $t + \delta$ erros no vetor de erro, além disso σ assinaturas são geradas em paralelo. O uso de múltiplas assinaturas em paralelo fortifica o esquema contra ataques do tipo GBA.

A grande dificuldade nesse caso, é que o código de Goppa usado não é capaz de corrigir todos os erros introduzidos, logo uma estratégia adicional deve ser usada. O esquema propõe a correção desses erros adicionais de forma intrínseca (tentativa e

²O paradoxo do aniversário concerne a probabilidade de, ao se sortear ao acaso n pessoas, pelo menos duas possuírem a mesma data de aniversário. É evidente que para se ter certeza que tal fato ocorrerá, é necessário um conjunto de 366 pessoas (excluindo 29 de fevereiro), o paradoxo vem do fato que para uma probabilidade de 99% apenas 57 pessoas são necessárias (BORJA; HAIGH, 2007). Com esse paradoxo é possível reduzir a complexidade de se atacar funções de *hash*.

erro), aleatoriamente, ou sequencialmente. O procedimento consiste em tentar “corrigir” os primeiros δ erros e então tentar decodificar o resultado, caso este não seja decodificável, outros δ erros são tentados.

Se assinar uma mensagem no esquema CFS simples pode ser reduzido ao problema de encontrar síndromes decodificáveis por amostragem aleatória, no esquema CFS paralelo a densidade de síndromes decodificáveis é 100% (graças aos δ erros), mas nem todas as combinações de δ erros resultam em vetores decodificáveis. A explicação para isto é que ao se escolher aleatoriamente δ posições no vetor, algumas delas podem corresponder a posições que não possuíam erros e, ao invés de corrigir erros existentes, acaba-se por adicionar novos erros. Logo, torna-se necessário encontrar uma combinação adequada. Isso é feito através de busca exaustiva, em geral, incremental. Desta busca resulta a complexidade da assinatura.

Existem $\binom{n}{\delta}$ vetores de erro com δ erros, mas existem $\binom{t+\delta}{\delta}$ formas de se corrigir δ em $t + \delta$ erros dados. Em média, existem $\binom{n}{t+\delta}/2^{mt}$ vetores de erro por síndrome. A densidade de vetores de erro decodificável é dada pela Equação 4.5.

$$\frac{\binom{t+\delta}{\delta} \cdot \binom{n}{t+\delta} / 2^{mt}}{\binom{n}{\delta}} = \frac{\binom{n-\delta}{t}}{2^{mt}} \approx \frac{1}{t!} \quad (4.5)$$

O esforço computacional para se encontrar uma combinação adequada é da ordem do inverso da densidade, ou seja, $O(t!)$. Logo, no esquema paralelo, nenhum esforço adicional (além do fator multiplicativo σ) é necessário, mas a segurança é aumentada. O esquema é composto de 3 algoritmos, *GerarChaves*, *Assinar* e *Verificar*.

- **GerarChaves.** Dado o nível de segurança λ , escolher um primo p (em geral $p = 2$), um corpo finito $\mathbb{F}_q$ com $q = p^m$, $m > 0$, e um código de Goppa $\Gamma(L, g)$ com suporte $L = (L_0, \dots, L_{n-1}) \in (\mathbb{F}_q)^n$ (de elementos distintos) e um polinômio gerador $g \in \mathbb{F}_q[x]$ de grau t sem raízes duplas, que satisfaça $g(L_j) \neq 0$, $0 \leq j < n$. Seja $k = n - mt$. As escolhas são feitas de maneira que o custo para

decodificar o código $[n, k, 2t + 1]$ seja ao menos 2^λ passos computacionais. Uma matriz verificadora de paridade sistemática $\hat{H}$, de forma que exista uma matriz escalonada de H e $(H, \hat{H}) \in \mathbb{F}_{p^{mt \times n}}$ para $\Gamma(L, g)$, *i.e.* $\hat{H} = [M \mid I_{mt}]$ para alguma matriz $M \in \mathbb{F}_{p^{mt \times k}}$, onde I_{mt} é a matriz identidade de ordem mt . Finalmente, como parâmetros públicos, uma função de posto de permutação $\phi : \mathcal{B}(n, t + \delta) \rightarrow \mathbb{Z}/\binom{n}{t+\delta}\mathbb{Z}$ e σ oráculos aleatórios $\mathcal{H}_i : \{0, 1\}^* \rightarrow \mathbb{Z}/\binom{n}{t}\mathbb{Z}$ são escolhidos. A chave privada é $sk := (L, g)$, e a chave pública é $pk := (M, t, \delta, \phi, \sigma, \mathcal{H}_0, \dots, \mathcal{H}_{\sigma-1})$.

- **Assinar.** Dada a mensagem $d \in \{0, 1\}^*$ que se deseja assinar e $i \in \mathbb{N}$ um índice, tal que $0 \leq i < \sigma$. Cada $s_i \leftarrow \mathcal{H}_i(d)$ é uma síndrome decodificável. Usando L e g , calcular cada $e_i \in \mathbb{F}_{q^n}$ com peso $\text{wt}(e_i) \leq t + \delta$ tal que $He_i^T = s_i^T$. A assinatura é $(\phi(e_0), \dots, \phi(e_{\sigma-1})) \in \mathbb{Z}/\binom{n}{t+\delta}\mathbb{Z}$.
- **Verificar.** Seja $(\phi(e_0), \dots, \phi(e_{\sigma-1})) \in \mathbb{Z}/\binom{n}{t+\delta}\mathbb{Z}$ um conjunto suposto de assinaturas σ para a mensagem $d \in \{0, 1\}^*$ e $i \in \mathbb{N}$ um índice tal que $0 \leq i < \sigma$. Calcular $s_i \leftarrow \mathcal{H}_i(d)$, e aceitar cada assinatura se, e somente se, $\text{wt}(e_i) \leq t + \delta$ e $\hat{H}e_i^T = s_i^T$.

Tabela 3: Parâmetros para assinaturas CFS paralelas (BARRETO, 2011).

Nível de segurança	m	t	σ	δ	Esforço para assinar	Tamanho da chave
80	20	8	3	2	16,8	2560 KiB
80	17	9	4	2	17,3	idem
80	16	10	3	3	23,4	639 KiB
80	15	11	3	3	26,8	idem
80	14	12	3	4	30,4	84 KiB
112	27	8	4	1	17,3	432 MiB
112	22	10	4	2	23,8	55 MiB
112	21	11	3	2	26,8	idem
112	19	12	3	3	30,4	3.5 MiB
128	23	11	4	2	27,3	252 MiB
128	22	12	3	3	30,4	33 MiB

Os tempos de cálculo passam a ser multiplicados por σ , mas dado que com o aumento na segurança, pode ser realizada uma redução nos parâmetros, o tempo final diminui. A escolha de σ deve levar em conta a densidade de vetores de erro por sín-

dromes decodificáveis (definida acima), que deve ser maior que um, e a probabilidade de não existir uma assinatura, dada pela Equação 4.6.

$$P_{noCFS} = 1 - \left(1 - \left(1 - \frac{1}{p^{mt}} \right)^{\binom{n}{t+\delta}} \right)^{\sigma} \quad (4.6)$$

Não há uma prova de segurança formal para o esquema CFS paralelo, no entanto, para os ataques conhecidos ele se mostra mais seguro que o esquema simples (FINIASZ, 2010). Um conjunto de parâmetros com os respectivos tamanhos de chaves e tempo de processamento para assinaturas CFS paralelas com uso de chaves quase-diádicas é exibido na Tabela 3 (BARRETO, 2011), onde o esforço para assinar é dado pelo $\log_2$ do número de passos computacionais necessários para calcular a assinatura.

4.8 Sumário do Capítulo 4

Este capítulo discutiu a criptografia pós-quântica e em especial os criptossistemas McEliece e Niederreiter. As assinaturas CFS, complemento a estes criptossistemas, foram apresentadas.

No próximo capítulo os impactos do uso de computadores quânticos para auxiliar o cálculo de assinaturas CFS são analisados.

5 ASSINATURAS CFS PARALELAS ASSISTIDAS POR COMPUTADORES QUÂNTICOS

Como visto no Capítulo 4, as assinaturas CFS e CFS paralelas são pouco práticas, seja pelo tamanho das chaves envolvidas, seja pelo tempo de processamento. Neste capítulo, estuda-se o impacto do uso de computadores quânticos para acelerar métodos criptográficos assimétricos. Essa constitui a primeira contribuição original do presente trabalho.

Duas possibilidades foram consideradas, a primeira é genérica para códigos de Goppa, já a segunda é específica para assinaturas CFS paralelas. No caso da primeira, é preciso entender a segunda parte do algoritmo de decodificação de Patterson (Algoritmo 1, linhas 14 a 20) como um problema de busca por raízes do polinômio localizador de erros. No caso da segunda, é preciso notar que as tentativas de correção de δ erros podem ser vistas como um problema de busca.

Nas próximas duas seções, discute-se a construção de dois oráculos de Grover, para a resolução destes problemas de busca. O primeiro oráculo (Seção 5.1), para a busca de raízes do polinômio localizador de erros, também será chamado de *oráculo pequeno*, uma vez que tem um escopo restrito. O oráculo pequeno será então usado dentro do *oráculo grande*, permitindo acelerar o processo de decodificação, necessário para verificar se uma síndrome é decodificável.

5.1 Oráculo para Encontrar Raízes de Polinômios

A parte mais crítica do processo de decodificação de síndrome é encontrar as raízes do polinômio localizador de erros $\sigma \in \mathbb{F}_{p^m}[X]$, que pode ser vista no Algoritmo 1 (linhas 14 a 20). A proposta apresentada nesta seção é a de acelerar essa busca com o uso do algoritmo de busca de Grover.

Classicamente, essa busca é implementada de maneira incremental sobre os elementos do suporte, e portanto o tempo de busca nesse caso é da ordem de $O(n) \approx O(2^{mt})$. Nesta seção, constrói-se um oráculo de Grover, chamado *oráculo pequeno*, capaz de verificar se um elemento $X \in \mathbb{F}_{p^m}$ é raiz de um polinômio $\sigma \in \mathbb{F}_{p^m}[X]$. Com o uso do oráculo pequeno, a busca de Grover encontrará as raízes do polinômio $\sigma(X)$, e essa busca passa a ter complexidade $O(2^{\frac{mt}{2}})$.

Como explicado na Seção 3.3.2, a busca de Grover é probabilística. Ela pode resultar em valores incorretos e, quando correta, resultará a cada rodada em raízes diferentes. Desta forma, o número de rodadas de busca necessárias para encontrar todas as raízes será maior que o grau do polinômio. O Algoritmo 2 apresenta este processo.

Algoritmo 2 Busca de Grover para encontrar raízes de polinômios em $\mathbb{F}_{p^m}$

Entrada: Polinômio $\sigma(X) \in \mathbb{F}_{p^m}[X]$

Saída: Raízes $x_i \in \mathbb{F}_{p^m}$ de σ

```

1: repeat
2:   Preparar  $X$  em uma superposição de estado com igual probabilidade
3:    $i := 0$ 
4:   for  $i = 0$  to  $\lceil \pi \frac{\sqrt{t}}{4} \rceil$  do // laço de Grover
5:      $O(X, \sigma)$  // Aplicar o oráculo pequeno
6:      $D(X)$  // Aplicar o operador de difusão
7:   end for
8:   Medir  $X$ 
9:   if  $X$  é solução (i.e. se  $X$  é raiz de  $\sigma$ ) then
10:     $x_i = X$ ;  $\sigma := \sigma / (x - x_i)$ ;  $i := i + 1$ 
11:   end if
12: until Todas raízes encontradas

```

Para completar o algoritmo, resta apenas projetar o oráculo. O oráculo deve ser

capaz de verificar se um dado X é raiz do polinômio σ . Classicamente, esse tipo de função é implementada com o pré-cálculo da aritmética e uso de tabelas de logaritmos e exponenciais (BARRETO, 2011). Nesta abordagem multiplicações e divisões são calculadas primeiro transformadas em somas e subtrações (com uso de tabelas de logaritmo) e depois remetidas aos valores finais (com uso de tabelas de exponenciação).

No entanto, esse tipo de abordagem não é possível no modelo de circuito da computação quântica. Por isso, neste trabalho, a aritmética é feita manualmente, gerando um circuito quântico ao final. Para isso, é necessário fixar os parâmetros a serem usados. Além disso, é necessário considerar a limitação do número de qubits na simulação. Por isso, deve-se escolher um tamanho fixo e pequeno de polinômio, que resultará em um código pequeno, portanto inseguro, mas suficiente como demonstração da abordagem. A construção é feita para os parâmetros $p = 2, m = 4, t = 1$, no entanto a abordagem usada é geral. Um elemento redutor, irredutível, sobre $\mathbb{F}_{2^4}$ é necessário, neste trabalho, utiliza-se $R(z) = z^4 + z + 1$ ¹.

Com esses parâmetros, o que se busca são as raízes do polinômio $\sigma \in \mathbb{F}_{p^m}[X]$, mostrado na Equação 5.1, onde $\sigma_i, X \in \mathbb{F}_{p^m}$, com $0 \leq i < t$. A partir de então, uma série de manipulações aritméticas é necessária, com o intuito de encontrar um valor de X em função dos valores σ_i de forma que o polinômio σ se torne 0.

Para isso, denota-se $\sigma_i \in \mathbb{F}_{p^m}$ como um polinômio em z , o produto $\sigma_1 \cdot X$ é mostrado na Equação 5.2. Note que para os parâmetros escolhidos, o polinômio localizador de erros se torna $\sigma = \sigma_1 X + \sigma_0$.

$$\sigma(X) = \sigma_0 + \sigma_1 \cdot X + \sigma_2 \cdot X^2 + \cdots + \sigma_t \cdot X^t \quad (5.1)$$

¹Neste caso, o polinômio $R(z)$ é uma representação de um elemento de $\mathbb{F}_{2^4}$ e é usado para reduzir os elementos deste corpo. Não deve ser confundido com os polinômios em $\mathbb{F}_{p^m}[X]$. A variável z é usada para evitar a confusão.

$$\begin{aligned}
\sigma_1 \cdot X &= (\sigma_{1,0} + \sigma_{1,1}z + \sigma_{1,2}z^2 + \sigma_{1,3}z^3) \cdot (x_0 + x_1z + x_2z^2 + x_3z^3) \\
&= \sigma_{1,0}x_0 + z(\sigma_{1,0}x_1 + \sigma_{1,1}x_0) + z^2(\sigma_{1,0}x_2 + \sigma_{1,1}x_1 + \sigma_{1,2}x_0) \\
&\quad + z^3(\sigma_{1,0}x_3 + \sigma_{1,1}x_2 + \sigma_{1,2}x_1 + \sigma_{1,3}x_0) \\
&\quad + z^4(\sigma_{1,1}x_3 + \sigma_{1,2}x_2 + \sigma_{1,3}x_1) + z^5(\sigma_{1,2}x_3 + \sigma_{1,3}x_2) + z^6(\sigma_{1,3}x_3) \quad (5.2)
\end{aligned}$$

A seguir, calcula-se $\sigma_1 \cdot X \bmod R(z)$. Em geral, esse processo pode ser feito de maneira iterativa, mas como este caso é simples, pode-se observar que a redução é feita através de $\sigma_1 \cdot X - (\sigma_{1,3}x_3z^2 + (\sigma_{1,2}x_3 + \sigma_{1,3}x_2)z + (\sigma_{1,1}x_3 + \sigma_{1,2}x_2 + \sigma_{1,3}x_1))R(z)$. Mas, em característica 2², $a + b = a - b$, logo a subtração pode ser substituída por uma adição, resultando em:

$$\begin{aligned}
\sigma_1 \cdot X \bmod R(X) &= (\sigma_{1,0}x_0 + \sigma_{1,1}x_3 + \sigma_{1,2}x_2 + \sigma_{1,3}x_1) \\
&\quad + z(\sigma_{1,0}x_1 + \sigma_{1,1}x_0 + \sigma_{1,1}x_3 + \sigma_{1,2}x_3 + \sigma_{1,2}x_2 + \sigma_{1,3}x_2 + \sigma_{1,3}x_1) \\
&\quad + z^2(\sigma_{1,0}x_2 + \sigma_{1,1}x_1 + \sigma_{1,2}x_0 + \sigma_{1,2}x_3 + \sigma_{1,3}x_3 + \sigma_{1,3}x_2) \\
&\quad + z^3(\sigma_{1,0}x_3 + \sigma_{1,1}x_2 + \sigma_{1,2}x_1 + \sigma_{1,3}x_0 + \sigma_{1,3}x_3) \quad (5.3)
\end{aligned}$$

Finalmente, pode-se retornar ao polinômio completo somando $\sigma_0 = \sigma_{0,0} + \sigma_{0,1}z + \sigma_{0,2}z^2 + \sigma_{0,3}z^3$, chegando à Equação 5.4.

$$\begin{aligned}
\sigma(X) &= (\sigma_{1,0}x_0 + \sigma_{1,1}x_3 + \sigma_{1,2}x_2 + \sigma_{1,3}x_1 + \sigma_{0,0}) \\
&\quad + z(\sigma_{1,0}x_1 + \sigma_{1,1}x_0 + \sigma_{1,1}x_3 + \sigma_{1,2}x_3 + \sigma_{1,2}x_2 + \sigma_{1,3}x_2 + \sigma_{1,3}x_1 + \sigma_{0,1}) \\
&\quad + z^2(\sigma_{1,0}x_2 + \sigma_{1,1}x_1 + \sigma_{1,2}x_0 + \sigma_{1,2}x_3 + \sigma_{1,3}x_3 + \sigma_{1,3}x_2 + \sigma_{0,2}) \\
&\quad + z^3(\sigma_{1,0}x_3 + \sigma_{1,1}x_2 + \sigma_{1,2}x_1 + \sigma_{1,3}x_0 + \sigma_{1,3}x_3 + \sigma_{0,3}) \quad (5.4)
\end{aligned}$$

²Todas operações calculadas $\bmod 2$.

O objetivo é encontrar X , raiz de $\sigma, \forall z$. Isso implica que todos os coeficientes devem ser iguais a 0, gerando as 4 condições mostradas na Equação 5.5.

$$\begin{aligned}
 (\sigma_{1,0}x_0 + \sigma_{1,1}x_3 + \sigma_{1,2}x_2 + \sigma_{1,3}x_1 + \sigma_{0,0}) &= 0 \\
 (\sigma_{1,0}x_1 + \sigma_{1,1}x_0 + \sigma_{1,1}x_3 + \sigma_{1,2}x_3 + \sigma_{1,2}x_2 + \sigma_{1,3}x_2 + \sigma_{1,3}x_1 + \sigma_{0,1}) &= 0 \\
 (\sigma_{1,0}x_2 + \sigma_{1,1}x_1 + \sigma_{1,2}x_0 + \sigma_{1,2}x_3 + \sigma_{1,3}x_3 + \sigma_{1,3}x_2 + \sigma_{0,2}) &= 0 \\
 (\sigma_{1,0}x_3 + \sigma_{1,1}x_2 + \sigma_{1,2}x_1 + \sigma_{1,3}x_0 + \sigma_{1,3}x_3 + \sigma_{0,3}) &= 0 \quad (5.5)
 \end{aligned}$$

Resta reescrever a Equação 5.5, trocando as operações aritméticas em corpos finitos por seus equivalentes lógicos. Multiplicações em característica 2 se tornam portas lógica E , representadas como $a \cdot b$ ou simplesmente ab , e adições se tornam portas lógicas XOR^3 :

$$\begin{aligned}
 (\sigma_{1,0}x_0 \oplus \sigma_{1,1}x_3 \oplus \sigma_{1,2}x_2 \oplus \sigma_{1,3}x_1 \oplus \sigma_{0,0}) &= 0 \\
 (\sigma_{1,0}x_1 \oplus \sigma_{1,1}(x_0 \oplus x_3) \oplus \sigma_{1,2}(x_3 \oplus x_2) \oplus \sigma_{1,3}(x_2 \oplus x_1) \oplus \sigma_{0,1}) &= 0 \\
 (\sigma_{1,0}x_2 \oplus \sigma_{1,1}x_1 \oplus \sigma_{1,2}(x_0 \oplus x_3) \oplus \sigma_{1,3}(x_3 \oplus x_2) \oplus \sigma_{0,2}) &= 0 \\
 (\sigma_{1,0}x_3 \oplus \sigma_{1,1}x_2 \oplus \sigma_{1,2}x_1 \oplus \sigma_{1,3}(x_3 \oplus x_0) \oplus \sigma_{0,3}) &= 0 \quad (5.6)
 \end{aligned}$$

Pode-se também concatenar as 4 expressões da Equação 5.7 em uma única com o uso de portas lógica OU , criando uma única condição:

³Operação lógica ou-exclusivo, representadas pelo operador $\oplus$.

$$\begin{aligned}
& (\sigma_{1,0}x_0 \oplus \sigma_{1,1}x_3 \oplus \sigma_{1,2}x_2 \oplus \sigma_{1,3}x_1 \oplus \sigma_{0,0}) + \\
& (\sigma_{1,0}x_1 \oplus \sigma_{1,1}(x_0 \oplus x_3) \oplus \sigma_{1,2}(x_3 \oplus x_2) \oplus \sigma_{1,3}(x_2 \oplus x_1) \oplus \sigma_{0,1}) + \\
& (\sigma_{1,0}x_2 \oplus \sigma_{1,1}x_1 \oplus \sigma_{1,2}(x_0 \oplus x_3) \oplus \sigma_{1,3}(x_3 \oplus x_2) \oplus \sigma_{0,2}) + \\
& (\sigma_{1,0}x_3 \oplus \sigma_{1,1}x_2 \oplus \sigma_{1,2}x_1 \oplus \sigma_{1,3}(x_3 \oplus x_0) \oplus \sigma_{0,3}) = 0 \quad (5.7)
\end{aligned}$$

O circuito final do oráculo é mostrado na Figura 5. O circuito irá inverter o último qubit quando X for raiz do polinômio $\sigma(X)$. Sozinho ele é capaz de acelerar o processo de decodificação de códigos de Goppa, seja no contexto das assinaturas CFS ou no contexto mais geral dos criptossistemas McEliece e Niederreiter.

Figura 5: Circuito quântico que verifica se X é raiz do polinômio $\sigma(X)$ em $\mathbb{F}_{2^4}$.

5.1.1 Resultados de Simulação

A validação da abordagem proposta foi feita com a implementação dos algoritmos na versão 0.6.3 do simulador QCL (ÖMER, 2009), em uma máquina Fedora 14, rodando sobre um Intel Core i5, 2GiB de memória RAM. O simulador permite a descrição de circuitos quânticos através de uma linguagem de programação estilo C, onde os operadores básicos são disponíveis na forma de função. A simulação permite a validação funcional do algoritmo, no entanto, nenhum parâmetro de tempo é fornecido, uma vez que esse tipo de informação dependeria da tecnologia utilizada. Simulações quânticas levam tempo exponencial no número de qubits usados (ÖMER, 2009), o que limita o tamanho do código que pode ser simulado. Essa limitação guiou a escolha dos parâmetros de simulação usados.

A simulação foi feita com o circuito apresentado nesta seção, ou seja, com $p = 2, m = 4, t = 1$. Com esses parâmetros, espera-se que o algoritmo de Grover convirja com $n \approx \frac{\pi}{4} \cdot \sqrt{2^4} \approx 3$ ciclos. A simulação foi efetuada 10 vezes para cada uma das combinações de valores de σ_0 e σ_1 , para observar o efeito estatístico da busca de Grover. Para confirmar que o número de ciclos esperado é o que apresenta maior probabilidade de acerto, a simulação foi rodada com 1, 2, 3 e 4 ciclos de Grover. O número de acertos médio entre os diversos $\sigma(X)$ para 10 rodadas de simulação para cada número de ciclos é apresentado na Tabela 4.

Tabela 4: Resultado de simulação do oráculo pequeno. É exibido o número de acerto em 10 rodadas para cada $\sigma(X)$ possível para 1, 2, 3 e 4 ciclos de Grover.

Ciclos de Grover	Número médio de Acertos	Desvio padrão
1	6,12	1,64
2	9,02	0,93
3	9,64	0,62
4	6,12	1,64

A partir da análise dos valores da Tabela 4 pode-se observar que o valor ótimo para o número de iterações se encontra entre 2 e 3 neste caso, tendendo a 3, como previsto

teoricamente.

5.1.2 Resultados Obtidos e Análise

Para avaliar os resultados obtidos com a aceleração na busca pela raízes, realiza-se comparação com a implementação MicroEliece do McEliece (EISENBARTH *et al.*, 2009). O MicroEliece é uma implementação leve do McEliece para sistemas embarcados. Os resultados do MicroEliece são interessantes pois estão separados por tarefas, permitindo uma comparação mais precisa. Duas comparações são feitas: a primeira leva em conta apenas a tarefa de encontrar as raízes, já a segunda considera que todos os outros resultados permanecem constante, com a busca por raízes acelerada.

Para alcançar alguma ideia quantitativa do ganho no desempenho, algumas considerações são feitas. A primeira é que o computador quântico executa um ciclo enquanto o computador clássico executa 20, como foi observado na Tabela 1 o tempo de operação em computadores quânticos pode variar muito (de 1 KHz a 100 THz), mas um valor foi fixado para simplificar as comparações. Também considera-se que a busca de Grover tem sucesso uma vez a cada 3 rodadas, em média. De fato, esse último parâmetro pode ser visto como uma grande desvantagem para a busca quântica, se observada a Tabela 4, mas as implementações de computadores quânticos diminuem a fidelidade e a probabilidade de acerto dos resultados.

A Tabela 5 apresenta os resultados da comparação da abordagem usando a busca de Grover e as implementações do MicroEliece, tanto em software como em FPGA. A versão em software foi testada no ATxMega 192 μC , e a versão em FPGA foi testada na Spartan-3AN 1400.

A melhora na busca por raízes foi significativa em ambos os casos; se comparado com a versão em software (*ATxMega*), ela é de 5 ordens de grandeza. A implementação em FPGA já é uma versão otimizada; ainda assim, a abordagem usando Grover permite

Tabela 5: Comparação da abordagem usando a busca de Grover contra o MicroEliece (EISENBARTH *et al.*, 2009).

	μ Eliece Software (ciclos)	μ Eliece FPGA (ciclos)	Grover (ciclos)	Ganho (%) Software	Ganho (%) FPGA
Busca por raízes	$15 \cdot 10^6$	$312 \cdot 10^3$	$51.8 \cdot 10^3$ ($4.7 \cdot 10^6$)	99.7	83.4
Decodificação	$20 \cdot 10^6$	$1.7 \cdot 10^6$	or $1.4 \cdot 10^6$) ⁴	76.2 ⁵	15.2 ⁵

uma melhora de mais de 95%.

Considerando todo o processo de decodificação, os resultados são menos expressivos. Há uma melhora considerável se considerada a versão em software ($\approx 75\%$), mas a melhora contra a versão em FPGA é pequena ($\approx 15\%$). Para melhorar o desempenho contra a implementação em FPGA, outras tarefas deveriam também ser aceleradas, mas isso levaria a um circuito mais complexo, não havendo, a princípio, garantias de ganhos.

Finalmente, resta estimar o número de qubits desta abordagem. Essa estimativa é feita extrapolando o circuito gerado. Este número é estimado como $O(m \cdot t)$ no espaço do oráculo, mais $O(m)$ no espaço de Grover (índice da busca). O número estimado de qubits é $n_{qubits} = m \cdot t + m$. Alguns qubits adicionais podem ser necessários, como variáveis temporárias, eles são chamados na literatura de *ancilas* e são tradicionalmente deixados fora da conta.

Tomando o código proposto no MicroEliece, $m = 11$, $t = 27$ (nível de segurança de 80 (EISENBARTH *et al.*, 2009)), um total de aproximadamente 308 qubits é necessário. Esse número é maior que o atual estado da arte em implementações quânticas, ainda assim é menor que o número necessário para quebrar os criptossistemas de chave pública atuais. Além disso, computadores quânticos com centenas de qubits já se encontram na fase de projeto (OSKIN; CHONG; CHUANG, 2002).

⁴Dependendo de como os demais módulos são implementados (ATxMega ou FPGA).

⁵Considerando que as demais tarefas permanecem constantes.

5.2 Oráculo para Decodificação de Síndromes

Dado o oráculo pequeno, usado para encontrar raízes do polinômio localizador de erros $\sigma(X)$, nesta seção, um novo oráculo é construído. Como já foi discutido, o processo de assinatura CFS paralela também pode ser reduzido a um problema de busca e é neste nível que o novo oráculo atua.

Este novo oráculo, chamado de *oráculo grande*, deve verificar se um vetor qualquer é uma palavra de códigos, ao menos de $t + \delta$ erros, onde t é o número de erros que o código é capaz de corrigir e δ é o número de erros que deve ser corrigido via tentativa e erro. Essa verificação é feita através do processo de decodificação, caso o vetor não seja decodificável o processo irá alertar isso.

Seguindo a estratégia clássica, onde tenta-se adivinhar δ erros, e os demais t são decodificados, o problema de busca reduz-se a encontrar δ posições que contenham, de fato, erros. Como a minoria das posições do vetor contém erros, em geral o processo de tentativa e erros falha, adicionando novos erros ao invés de corrigir os existentes. Uma abordagem inicial consiste na aplicação da busca de Grover sobre todo o espaço de busca, de tamanho $\binom{n}{t+\delta}$ (vetores de n bits com δ bit com valor ‘1’). Apesar de funcional, essa abordagem é mais demorada do que a estratégia clássica, uma vez que o algoritmo clássico irá parar quando encontrar um resultado, o que não é possível no algoritmo de Grover.

A estratégia aqui proposta é a de sub-amostragem do espaço, tomando sub-espacos de tamanho $t!$. Como foi mostrado na Seção 4.7.1 a densidade de acertos no espaço de “tentativas” é $\frac{1}{t!}$, logo em um sub-espaco de tamanho $t!$ espera-se que exista exatamente uma solução.

Essa sub-amostragem permite reduzir o tamanho do circuito quântico, bem como o tempo de processamento. No entanto, é evidente que não existem garantias que haja uma solução no sub-espaco escolhido, criando um indeterminismo adicional na busca.

Mas a redução da complexidade justifica a aplicação de algumas buscas adicionais em espaços reduzidos. O algoritmo final de busca, implementando o que foi descrito até aqui, é mostrado no Algoritmo 3, onde a função Φ^{-1} é a função inversa do posto de permutação, ou seja, dado um índice i a função $\Phi^{-1}(i)$ devolverá o i -ésimo elemento da permutação correspondente. A permutação escolhida é variável e é definida como um dos parâmetros públicos das assinaturas CFS.

Algoritmo 3 Busca de Grover para encontrar síndromes decodificáveis

```

1: Selecionar um sub-conjunto aleatório  $R$  de tamanho  $t!$  de vetores de peso  $\delta$ , tomar
    $C$  de tamanho  $\log_2(t!)$ , um ponteiro neste espaço
2: repeat
3:   repeat
4:      $H(C)$  // Superposição do ponteiro para todos os elementos
5:      $e = \Phi^{-1}(C)$ 
6:     for  $i = 0$  to  $\lceil \pi \frac{\sqrt{t!}}{4} \rceil$  do // laço de Grover
7:       Aplicar o oráculo decodificador para uma palavra de código  $m$  de um
       código de Goppa com  $t + \delta$  erros
8:       Operador de difusão de Grover
9:     end for
10:    Medir  $e$ 
11:    Verificar se  $e$  é solução (i.e. verificar se  $m \oplus e$  é decodificável)
12:  until Encontrar solução ou  $P_G(R) > \rho$ 
13:  Selecionar um novo sub-conjunto aleatório  $R$  de tamanho  $t!$ 
14: until Encontrar Solução

```

O polinômio localizador de erros pode ser encontrado com o algoritmo quântico apresentado na Figura 6, derivado do Algoritmo 3. Após esta etapa resta encontrar as raízes do polinômio localizador de erros, o que pode ser feito através de uma busca de Grover, usando o oráculo definido na seção anterior. Resta implementar cada uma das caixas do algoritmo quântico da Figura 6.

Tendo em vista o mesmo tipo de limitação existente na construção do oráculo pequeno, o código usado continua sendo sobre o corpo $\mathbb{F}_{2^4}$, com polinômio redutor $R(z) = z^4 + z + 1$. Vale lembrar que esse tamanho de código é inseguro para fins criptográficos, mas serve para a demonstração de princípio pretendida aqui, sendo a metodologia usada perfeitamente aplicável para qualquer tamanho de código.

Os parâmetros escolhidos permitem algumas simplificações no algoritmo mostrado na Figura 6. Especificamente, os laços não são mais necessários, tampouco os acumuladores B e C (os valores podem ser obtidos diretamente a partir de f_n/g_n). Novamente, as operações aritméticas serão calculadas manualmente, com posterior transformação em circuitos lógicos quânticos. Os cálculos para $\mathbb{F}_{2^4}$ são realizados explicitamente, enquanto os cálculos para o corpo genérico $\mathbb{F}_{p^m}$ são indicados.

Figura 6: Algoritmo quântico que calcula o polinômio localizador de erros a partir da síndrome em $\mathbb{F}_{2^m}$, onde f_n e g_n denota o coeficiente do termo mais significativo de f e g .

5.2.1 Aritmética em $\mathbb{F}_{p^m}$

Nesta sub-seção, a aritmética em $\mathbb{F}_{2^m}$, em particular com $m = 4$, é definida e implementada com o uso de operações lógicas. A metodologia utilizada segue a linha do que foi feito para a implementação do oráculo pequeno.

Como explicado na Seção 2.2, adições e subtrações em $\mathbb{F}_{p^m}$ são realizadas módulo p , e no caso $p = 2$ adições e subtrações são equivalentes e iguais a uma operação lógica de ou-exclusivo (como desenvolvido na Seção 5.1). Já multiplicações (e operações dela derivadas) devem ser calculadas e reduzidas módulo um elemento irredutível $R(z)$. No caso de operações de exponenciação, ou afins, o uso do Pequeno Teorema de Fermat, apresentado na Seção 2.2, é especialmente útil.

Multiplicação

A primeira operação a ser calculada é justamente a multiplicação. O raciocínio usado para a redução modular no caso da multiplicação será transposto para outras operações. Dados $a, b \in \mathbb{F}_{2^4}$, adota-se a noção polinomial para elementos de $\mathbb{F}_{2^4}$, onde $a = a_3 \cdot z^3 + a_2 \cdot z^2 + a_1 \cdot z + a_0$ e $b = b_3 \cdot z^3 + b_2 \cdot z^2 + b_1 \cdot z + b_0$, para $a_i \in \{0, 1\}$, $0 \leq i \leq 3$. O produto de a por b pode ser calculado da seguinte maneira:

$$\begin{aligned}
 a \cdot b &= (a_3 \cdot z^3 + a_2 \cdot z^2 + a_1 \cdot z + a_0) \times (b_3 \cdot z^3 + b_2 \cdot z^2 + b_1 \cdot z + b_0) \\
 &= a_3 b_3 \cdot z^6 + (a_3 b_2 + a_2 b_3) \cdot z^5 + (a_3 b_1 + a_2 b_2 + a_1 b_3) \cdot z^4 \\
 &\quad + (a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3) \cdot z^3 + (a_2 b_0 + a_1 b_1 + a_0 b_2) \cdot z^2 \\
 &\quad + (a_1 b_0 + a_0 b_1) \cdot z + (a_0 b_0)
 \end{aligned} \tag{5.8}$$

A seguir, o resultado é reduzido módulo $R(z)$, essa redução é feita tomando o resto da divisão de $a \cdot b$ por $R(z)$:

$$\begin{aligned}
 a \cdot b \bmod R(z) &= z^3 \cdot (a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3 + a_3 b_3) \\
 &\quad + z^2 \cdot (a_2 b_0 + a_1 b_1 + a_0 b_2 + a_3 b_3 + a_3 b_2 + a_2 b_3) \\
 &\quad + z \cdot (a_1 b_0 + a_0 b_1 + a_3 b_2 + a_2 b_3 + a_3 b_1 + a_1 b_3 + a_2 b_2) \\
 &\quad + (a_0 b_0 + a_3 b_1 + a_1 b_3 + a_2 b_2)
 \end{aligned} \tag{5.9}$$

Inversa Modular

A operação de inversão modular é desenvolvida a partir do Pequeno Teorema de Fermat, ela será útil no calculo da divisão. A Equação 5.10 mostra o cálculo feito a partir do Pequeno Teorema de Fermat, onde $a \in \mathbb{F}_{p^m}$. Ao se adotar $m = 4$, obtém-se a

Figura 7: Circuito quântico que calcula $a \cdot b$ em $\mathbb{F}_{2^4}$.

Equação 5.11.

$$a^{-1} = a^{p-2} \pmod{p} \text{ ou } a^{-1} = a^{2^m-2} \pmod{p^m} \in \mathbb{F}_{p^m} \quad (5.10)$$

$$a^{-1} = a^{14} \in \mathbb{F}_{2^4} \quad (5.11)$$

Logo, o cálculo de a^{-1} equivale ao cálculo de $a^{14} \pmod{R(z)}$ em $\mathbb{F}_{2^4}$. Para esse cálculo adota-se a seguinte estratégia: $a^{14} = a^8 \times a^4 \times a^2$. Usando o triângulo de Pascal binário⁶, pode-se obter as expressões mostradas na Equação 5.12 de potências parciais, de onde se calcula o valor de a^{14} , mostrado na Equação 5.13.

$$\begin{aligned} a^8 &= (a_3 \cdot z^3 + a_2 \cdot z^2 + a_1 \cdot z + a_0)^8 = a_3 \cdot z^{24} + a_2 \cdot z^{16} + a_1 \cdot z^8 + a_0 \\ a^4 &= (a_3 \cdot z^3 + a_2 \cdot z^2 + a_1 \cdot z + a_0)^4 = a_3 \cdot z^{12} + a_2 \cdot z^8 + a_1 \cdot z^4 + a_0 \\ a^2 &= (a_3 \cdot z^3 + a_2 \cdot z^2 + a_1 \cdot z + a_0)^2 = a_3 \cdot z^6 + a_2 \cdot z^4 + a_1 \cdot z^2 + a_0 \end{aligned} \quad (5.12)$$

⁶Triângulo de Pascal onde cada elemento é calculado mod 2.

$$\begin{aligned}
a^{14} &= (a_3 \cdot z^{24} + a_2 \cdot z^{16} + a_1 \cdot z^8 + a_0) \times (a_3 \cdot z^{12} + a_2 \cdot z^8 + a_1 \cdot z^4 + a_0) \\
&\quad \times (a_3 \cdot z^6 + a_2 \cdot z^4 + a_1 \cdot z^2 + a_0) \\
&= z^{42}(a_3) + z^{40}(a_3.a_2) + z^{38}(a_3.a_1 + a_3.a_2) + z^{36}(a_3.a_0 + a_3.a_2) \\
&\quad + z^{34}(a_3.a_2.a_1 + a_3.a_2 + a_3.a_1) + z^{32}(a_3.a_2.a_0 + a_3.a_2.a_1 + a_3.a_2) \\
&\quad + z^{30}(a_3.a_1 + a_3.a_0 + a_3.a_2.a_1 + a_3.a_2) \\
&\quad + z^{28}(a_3.a_1.a_0 + a_3.a_2.a_0 + a_3.a_2.a_1 + a_2) \\
&\quad + z^{26}(a_3.a_1.a_0 + a_2.a_1 + a_3.a_2.a_1 + a_3.a_1) \\
&\quad + z^{24}(a_3.a_0 + a_2.a_0 + a_2.a_1 + a_3.a_2.a_1) \\
&\quad + z^{22}(a_2.a_1 + a_3.a_2.a_0 + a_3.a_1 + a_3.a_2.a_1) \\
&\quad + z^{20}(a_2.a_1.a_0 + a_2.a_0 + a_3.a_1.a_0 + a_2.a_1) \\
&\quad + z^{18}(a_2.a_1.a_0 + a_2.a_1 + a_3.a_1 + a_3.a_0) \\
&\quad + z^{16}(a_2.a_0 + a_2.a_1.a_0 + a_2.a_1 + a_3.a_2.a_0) \\
&\quad + z^{14}(a_1 + a_3.a_1.a_0 + a_3.a_1.a_0 + a_3.a_2.a_0) \\
&\quad + z^{12}(a_1.a_0 + a_3.a_1.a_0 + a_3.a_0 + a_2.a_0) \\
&\quad + z^{10}(a_1.a_0 + a_2.a_1.a_0 + a_3.a_1.a_0) \\
&\quad + z^8(a_1.a_0 + a_2.a_0 + a_2.a_1.a_0) + z^6(a_1.a_0 + a_3.a_0) \\
&\quad + z^4(a_1.a_0 + a_2.a_0) + z^2(a_1.a_0) + z^0(a_0)
\end{aligned} \tag{5.13}$$

Resta calcular $a^{14} \bmod R(z)$:

$$\begin{aligned}
a^{14} \bmod R(z) &= z^3(a_1 + a_2 + a_3 + a_3.a_0 + a_3.a_1 + a_3.a_2 + a_3.a_2.a_1) \\
&+ z^2(a_1.a_0 + a_2 + a_2.a_0 + a_3 + a_3.a_0 + a_3.a_2.a_0) \\
&+ z^1(a_1.a_0 + a_2.a_0 + a_2.a_1 + a_3 + a_3.a_1 + a_3.a_1.a_0) \\
&+ z^0(a_0 + a_1 + a_2 + a_2.a_0 + a_2.a_1 + a_2.a_1.a_0 + a_3 + a_3.a_2.a_1) \quad (5.14)
\end{aligned}$$

O circuito que calcula a^{-1} é mostrado na Figura 8.

Figura 8: Circuito quântico que calcula a^{-1} em $\mathbb{F}_{2^4}$.

Divisão

A partir da inversa e da multiplicação, pode-se calcular a divisão, na forma $\frac{a}{b} = a \times b^{-1}$. Logo, nenhum circuito adicional é necessário.

Raíz quadrada

A próxima função a ser calculada é a raíz quadrada modular, também a partir do Pequeno Teorema de Fermat:

$$a^{1/2} = (a^p)^{1/2} \pmod{p} \text{ or } (a^{2^{m-1}}) \pmod{2^m} \text{ or } (a^8) \pmod{2^4} \quad (5.15)$$

Logo, em $\mathbb{F}_{2^4}$, tem-se que $\sqrt{a} = a^8$. O cálculo de a^8 é linear em característica 2:

$$a^8 = (a_3 \cdot z^{24} + a_2 \cdot z^{16} + a_1 \cdot z^8 + a_0) \quad (5.16)$$

Que pode ser reduzido como:

$$a^8 \bmod R(z) = z^3 \cdot (a_3) + z^2 \cdot (a_1) + z^1 \cdot (a_2 + a_3) + z^0 \cdot (a_0 + a_1) \quad (5.17)$$

A Figura 9 mostra o circuito quântico que calcula a raiz quadrada de a em $\mathbb{F}_{2^4}$.

Figura 9: Circuito quântico que calcula $\sqrt{a}$ em $\mathbb{F}_{2^4}$.

Quadrado

O cálculo do quadrado de um elemento em $\mathbb{F}_{2^m}$ é feito simplesmente por:

$$\begin{aligned} a^2 \bmod R(z) &= (a_3 \cdot z^3 + a_2 \cdot z^2 + a_1 \cdot z^1 + a_0)^2 \\ &= (a_3 \cdot z^6 + a_2 \cdot z^4 + a_1 \cdot z^2 + a_0) \\ &= (a_3 \cdot z^3 + (a_3 + a_1) \cdot z^2 + a_2 \cdot z^1 + (a_0 + a_2)) \end{aligned} \quad (5.18)$$

Esta função é calculada pelo circuito quântico mostrado na Figura 10.

Figura 10: Circuito quântico que calcula a^2 em $\mathbb{F}_{2^4}$.

5.2.2 Resultados Obtidos e Análise

Os resultados serão analisados para 4 parâmetros: tamanho de chaves (em bits), esforço para assinar (número de passos computacionais), esforço para quebrar o sistema (nível de segurança) e número de qubits necessários. Esses parâmetros permitem uma ideia global da solução em termos de desempenho e custo. Diversas configurações de parâmetros são testadas, permitindo uma ideia do tipo de balanço que pode ser feito com estes.

A chave consiste de uma matriz geradora de $t \times n$ elementos em $\mathbb{F}_{p^m}$, com $n \approx 2^m$. A adoção de matrizes quase-diádicas permite que apenas uma linha da matriz seja pública (BARRETO *et al.*, 2010). Desta forma, o tamanho de chaves é dado pela Equação 5.19, onde $maxpow$ é a maior potência de p que divide exatamente t .

$$key_{size} = \left\lceil \log_2(p) \cdot \left(\frac{m \cdot t \cdot (n - mt)}{maxpow(p, t)} \right) \right\rceil \quad (5.19)$$

Como discutido na Seção 4.7.1, o número de passos computacionais necessários para assinar uma mensagem é da ordem de $\sqrt{t!}$, o esforço computacional para realizar uma assinatura é calculado aqui como $\log_2(\sqrt{t!})$.

Finalmente, uma estimativa do custo computacional para atacar o esquema é feito tomando por base os ataques conhecidos, sabendo que não existem garantias que ataques melhores não serão descobertos. O melhor ataque contra o esquema de assinatu-

ras CFS Paralelo é descrito por Finiasz e Sendrier (FINIASZ; SENDRIER, 2009), e tem custo de (FINIASZ, 2010):

$$WF_{FS} = L \log(L) \text{ with } L = \min \left(\frac{2^{mt}}{\binom{n}{t-\lfloor t/3 \rfloor}}, \sqrt{\frac{2^{mt}}{\binom{n}{n/3}}} \right) \quad (5.20)$$

A partir desta formulação, é possível estimar os valores de custo de assinatura, tamanho de chave e custo do ataque (nível de segurança) para uma série de parâmetros, essas estimativas são mostradas na Tabela 6. Também, pode-se estimar, analisando os circuitos gerados, o número de qubits necessários para a implementação do oráculo. O número de qubits necessários no espaço do oráculo (*i.e.* para fazer os cálculos) é da ordem de $O(m \cdot t)$, e o número de qubits necessários no espaço de Grover (*i.e.* para endereçar cada solução) é da ordem de $O(\log_2(t!))$. O número final de qubits estimado será dado por $\#_{qubits} = \lceil 6m \cdot t + \log_2(t!) \rceil$. O fator multiplicativo 6 foi escolhido devido aos 6 registradores presentes no algoritmo (F, G, B, C, t, s), vale ressaltar que neste trabalho g é puramente clássico.

Tabela 6: Parâmetros para CFS Paralelo, com estimativas de custo, tamanho de chave, nível de segurança e número de qubits.

Nível de Segurança	m	t	σ	δ	Tamanho da Chave (KiB)	Esforço para Assinar	Esforço para Atacar	$\approx \#Qubits$
80	20	8	3	2	2560	8.89	80.62	963
80	16	10	3	3	639	12.13	81.75	964
80	14	12	3	4	84	15.67	85.82	1011
80	12	16	2	7	6	22.86	89.64	1156
112	27	8	4	1	442368	9.30	113.22	1299
112	22	10	4	2	56317	12.55	112.96	1324
112	19	12	3	3	3647	15.66	114.72	1372
112	15	16	3	6	60	23.37	117.70	1444
128	22	12	3	3	33790	15.65	129.55	1588
128	16	16	4	5	128	23.78	129.95	1540

Neste cenário seria possível, por exemplo, gerar uma assinatura com $m = 14$, $t = 12$ e $\delta = 3$, nível de segurança de 80, em menos de 53000 passos. Num computador clássico, a mesma assinatura levaria mais do que um bilhão de passos (conforme

Tabela 3), o que representa mais do que 99,99% de aceleração. Neste exemplo a chave possui o menor valor encontrado na literatura para este nível de segurança, conforme visto na Tabela 3.

Mesmo que os níveis de segurança mais elevados ainda apresentem baixa eficiência, eles já poderiam ser considerados práticos, em um cenário carente de outras alternativas. No nível de segurança 80, uma chave de 6 KiB é possível, valor razoavelmente próximo do atual RSA (1024 bits), sendo mais lento que o último exemplo, no entanto. Nos demais níveis, chaves de algumas dezenas de MiB se apresentam, apesar de tal faixa não ser ótima, ela está dentro do que se pode considerar plausível em um sistema computacional atual.

Já em relação ao número de qubits, a observação inicial é que esse número é bem maior que o encontrado implementando-se apenas o oráculo pequeno, no entanto, continua válida a comparação contra o número de qubits necessários para quebrar o RSA. Mesmo neste cenário, onde a busca por padrões de erros é implementada de maneira completa, é necessário um número menor de qubits do que o necessário para quebrar o RSA em cada nível de segurança.

5.3 Sumário do Capítulo 5

Neste capítulo duas propostas de otimização para criptossistemas pós-quânticos foram apresentadas. Em uma delas a otimização se dá no nível do decodificador de Patterson para códigos de Goppa. Neste caso a busca de Grover é usada para acelerar a busca por raízes de polinômios em $\mathbb{F}_{p^m}$. A outra otimização se dá no nível das assinaturas CFS paralelas, em específico a busca de Grover é usada para acelerar a procura por combinações de erros que gerem síndromes de Goppa decodificáveis. Os resultados obtidos apontam para otimizações interessantes, que permitem, para alguns conjuntos de parâmetros, a implementação prática destes criptossistemas.

No próximo capítulo será apresentada uma arquitetura híbrida, com um coprocessador quântico implementando a busca de Grover com o oráculo pequeno. Este coprocessador permite a implementação dos algoritmos propostos, mesmo sem o total desenvolvimento da computação quântica.

6 ARQUITETURA HÍBRIDA

Nas seções anteriores, foram revisados os criptossistemas McEliece e Niederreiter com códigos de Goppa, bem como a busca quântica de Grover, também discutiu-se uma forma de usar estes para melhorar o desempenho daqueles. Neste capítulo, discute-se a criação de um coprocessador quântico, capaz de executar a busca de Grover.

A ideia aqui é a construção de um dispositivo quântico pequeno, capaz de executar uma única tarefa, bem específica. Esse circuito seria associado a um computador clássico, onde seria implementado o restante do processo de decodificação (seja com ou sem aceleração em hardware). Essa abordagem permite a máxima redução do circuito quântico. Ainda assim, os resultados mostrados no Capítulo 5 mostram que esse pequeno circuito é capaz de melhorar consideravelmente o desempenho de criptossistemas pós-quânticos.

6.1 Trabalhos Relacionados

Nesta seção, algumas propostas de arquitetura para computadores quânticos são discutidas. Essa discussão tem o objetivo de posicionar melhor a contribuição específica deste capítulo com outros trabalhos presentes na literatura.

Oskin, Chong e Chuang (2002) propõem uma arquitetura para um computador puramente quântico. Essa arquitetura é projetada para um computador de propósito geral, possuindo um conjunto universal de portas. Ela inclui uma Unidade Lógica Aritmé-

tica, memória e registradores quânticos. Visivelmente, a arquitetura lembra a organização de um computador clássico, com a adição de elementos próprios da computação quântica, como por exemplo codificadores e decodificadores para códigos quânticos corretores de erros. Os autores propõem também um esquema de comunicação baseada na teleportação de estado quânticos. Em comparação com este trabalho, a arquitetura proposta pode ser vista como uma solução final para a computação quântica, enquanto aqui, propõe-se uma solução intermediária, anterior ao desenvolvimento completo da computação quântica.

Um outro trabalho, propõe uma arquitetura de programação quântica (BETTELLI; CALARCO; SERAFINI, 2003). Neste caso, a proposta é o uso de um circuito quântico como um periférico a um computador clássico. A implementação de uma linguagem de programação quântica é discutida, desde aspectos relacionados a registradores até a composição de diversos operadores, na forma de um algoritmo. O resultado é um esquema flexível para controlar um dispositivo quântico através de um computador clássico. Nesta solução *drivers* para o computador clássico seriam necessários para permitir o controle da operação.

6.2 Coprocessador Quântico Implementando Grover

Antes de dar início a discussão de como esse circuito quântico é realmente especificado, o levantamento de alguns requisitos para ele se faz necessário. Do ponto de vista do processador, seria interessante que não fossem necessárias mudanças significativas. Idealmente, o núcleo sequer tomaria conhecimento que o dispositivo é quântico. A descrição em forma de coprocessador preenche esse requisito. Desta forma, nenhuma mudança no núcleo é necessária, a resposta viria em um conjunto de endereços pré-definidos, assim como é usualmente feito com dispositivos de *entrada e saída* (E/S).

O resultado da operação deve ser escrito diretamente na memória, seguindo o esquema de *Acesso Direto à Memória* (DMA, em inglês), uma interrupção no processador permite informá-lo que a operação foi concluída e o resultado se encontra no local especificado da memória. Esse protocolo tem a vantagem de não travar o processador enquanto o cálculo é realizado, permitindo que o processador continue a executar outras tarefas enquanto espera os resultados do circuito quântico.

Uma restrição desejável é usar apenas tecnologias já existentes. Isso exclui algumas primitivas computacionais clássicas, como memórias. Apesar da demonstração experimental do armazenamento durante um certo tempo de estados quânticos, a implementação de memórias, no sentido computacional, ainda encontra-se distante (SIMON *et al.*, 2010).

O uso de um controlador permite a implementação do protocolo de comunicação com o processador de maneira isolada da lógica de operação da função. Este controlador também fica responsável pela operação do circuito quântico, como preparação do estado inicial, execução das operações lógicas e leitura de resultados. Ele fica responsável por verificar se o resultado encontrado na busca é correto e se todos os resultados foram encontrados, ou ainda se a busca deve ser repetida para obtenção de novos resultados. Isso restringe a quantidade de lógica a ser implementada no coprocessador, permitindo que ele seja realmente especificado para a tarefa de busca.

A especificação realizada é compatível com um coprocessador. O uso do controlador, apesar de não ser usual em coprocessadores, permite a transparência em relação ao fato do componente ser quântico. A Figura 11 mostra como o coprocessador se acoplaria a uma arquitetura genérica de processador. Todas as conexões mostradas na figura são clássicas (inclusive a que liga o controlador ao coprocessador), só há manipulação de informação quântica dentro do coprocessador. Isso traz algumas vantagens, pois todos os sinais no processador continuam clássicos, logo não há necessidade de mudar o tratamento dado à informação nele. Uma outra vantagem é que o tempo de co-

erência da informação quântica necessário é reduzido, uma vez que o estado quântico é preparado no instante em que for ser usado

Figura 11: Arquitetura híbrida quântica/clássica, todas as conexões mostradas na figura são clássicas (inclusive a que liga o controlador ao coprocessador).

Os sinais de dados irão impactar na preparação do estado inicial apenas. No caso deste trabalho, o dado que representa o polinômio σ é estritamente clássico, ou seja, não existe emaranhado ou superposição entre os diversos componentes do polinômio, isso pois, procura-se raízes de um polinômio fixo e constante, definido pelo código em uso. O único dado quântico é o valor de X , que será avaliado para o polinômio. O registrador de X se inicia no estado *terra* (ou seja, zerado) e será colocado em um superposição completa de estados, como representado na Figura 12.

Figura 12: Uso de busca de Grover com um oráculo verificador de raíz, para encontrar raízes do polinômio σ .

As operações efetuadas após a preparação do estado inicial dependem apenas do algoritmo, e portanto são específicas para uma tarefa dada (NIELSEN; CHUANG, 2000). A forma como essas operações são implementadas dependem da tecnologia física do

computador quântico. Na Seção 6.3, a implementação usando fotônica é discutida.

Outras tecnologias existem, como RNM, armadilha de íons, dispositivo supercondutores, por exemplo, mas não são discutidas neste trabalho. Divincenzo (2005) apresenta uma lista mais completa de tecnologias de implementação. Na Seção 3.4, referências específicas para cada tecnologia são indicadas.

Para qualquer dos oráculos, as portas usadas no coprocessador são as portas CNOT, Toffoli e Pauli-X, além do arcabouço da busca de Grover. Em algumas tecnologias de implementação, tais como RMN, armadilhas de íons, pontos quânticos, entre outros, a aplicação de portas lógicas se resume a aplicação de pulsos eletromagnéticos ou ópticos. Logo, não há necessidade de implementação específica de uma porta física para cada instância lógica dela. Isso reduz o tamanho do hardware necessário. Já no caso onde este re-uso não é trivial, como em óptica linear, a implementação com múltiplas instâncias de cada porta é mais simples, porém implica em custos maiores de hardware.

6.3 Implementação com Óptica Linear

O uso de óptica linear é um esquema promissor para a implementação de computação quântica (KNILL; LAFLAMME; MILBURN, 2001). Na óptica linear, operações quânticas são realizadas através de lentes e espelhos especiais chamados de *separadores de raio* e *deslocadores de fase* (KOK *et al.*, 2007) e os estados quânticos são representados através do caminho seguido por fótons individuais. Para que seja possível é necessário o uso de fontes e detectores de um único fóton.

Dois fatores contam a favor da óptica linear: o fato desse esquema ser o único a ter possibilitado comunicação na prática e o fato dele permitir a operação a temperaturas ambiente (a maior parte dos esquemas necessita de resfriamento próximo a 0K) (NIELSEN; CHUANG, 2000; DIVINCENZO, 2005). O primeiro desses fatores pode

ser determinante para o uso da óptica, mesmo caso alguma outra tecnologia venha a ser usada para a computação.

Dentre os desafios enfrentados pela tecnologia para sua viabilização pode-se destacar a dificuldade para emaranhar um grande número de estados e a construção de boas fontes e detectores de um fóton (NIELSEN; CHUANG, 2000). A primeira dificuldade pode determinar a inabilidade desta tecnologia para o uso prático em computação, uma vez que para se tirar benefício completo de um computador quântico a capacidade de emaranhar estados é fundamental (SHOR, 1997).

Vantagens e desvantagens a parte, nota-se que um conjunto universal de portas usando óptica linear já foi provado experimentalmente (KOK *et al.*, 2007) assim como a busca de Grover (KWIAT *et al.*, 2000). Em especial, as portas usadas nos oráculos propostos neste trabalho também foram implementadas, o que permite o uso desta tecnologia para o circuito aqui proposto.

A implementação da busca de Grover com óptica linear é mostrada na Figura 13. Dentre os componentes usados, destacam-se as lâminas de meia-onda (indicados por *HWP*, do inglês *half wave plate*), que alteram a polarização do feixe luminoso, os atrasos de fase representados por ângulos anotados ao lado das caixas, os divisores de feixe polarizadores (indicados por *PBS*, do inglês *polarizing beam split*), que separam os feixes de acordo com sua polarização. Finalmente *H* representa a fonte luminosa e 1 – 4 os detectores. O resultado da operação é definido pelo detector em que o fóton foi recebido, e os estados parciais são representados pelo caminho seguido pelo feixe.

O oráculo indefinido da figura deve ser substituído pelo oráculo específico da função, no caso os especificados na Figura 5 e na Figura 6 do Capítulo 5, de forma que a busca retornará raízes para o polinômio, ou padrões de erros decodificáveis (dependendo de qual oráculo foi escolhido). É importante observar que, dependendo de qual oráculo for escolhido, a implementação do controlador será diferente. Caso o oráculo pequeno seja escolhido, todas as raízes do polinômio localizador precisam ser encon-

Figura 14: A porta quântica CNOT implementada com óptica linear, conforme Okamoto (OKAMOTO *et al.*, 2005).

Figura 15: A porta Toffoli Sinal implementada por Ralph *et al.* (RALPH; RESCH; GILCHRIST, 2007). A porta de Toffoli pode ser obtida através da porta Toffoli Sinal e da adição de dois divisores de feixes, um antes e um depois da Toffoli Sinal.

encontram-se no Capítulo 5, podendo chegar à 24 ordens de grandeza em alguns casos, o que pode representar a viabilidade de tais técnicas pós-quânticas num cenário verdadeiramente quântico.

Por outro lado, apenas o gargalo dos algoritmos é implementado com o uso de tecnologia quântica, o que permite um hardware reduzido, mas certamente reduzindo o ganho que seria possível. O número de qubits necessários (ver Seção 5.1) ainda é superior ao estado da arte em qualquer tecnologia, o que pode ser, a primeira vista, desanimador. Entretanto, ressalta-se que este número é menor que o número necessário para realizar a quebra efetiva dos criptossistemas de chave pública atuais.

Finalmente, pode-se destacar que a técnica apresentada é viável, no sentido que todos os componentes necessários já foram implementados e testados. O uso do coprocessador traz diversas vantagens práticas, entre elas a ausência de memórias, a preparação do estado quântico no momento do uso, o pequeno tempo de processamento de informação quântica (em relação ao tempo total do algoritmo) e o pequeno hardware. Além disso, a adoção de um controlador, permite a redução da complexidade do circuito quântico a ser implementado, deixando toda a lógica de controle dentro de um contexto clássico.

6.5 Sumário do Capítulo 6

Neste capítulo foi apresentada uma arquitetura híbrida quântica/clássica, usando um coprocessador quântico capaz de acelerar uma tarefa específica, no caso apresentado, a busca por raízes do polinômio localizador de erros em códigos de Goppa. Adicionalmente, a implementação deste coprocessador com óptica linear foi discutida.

No próximo capítulo, um estudo de viabilidade da implementação de computadores quânticos, com diferentes tecnologias, é conduzido. Este estudo visa a possibilidade de construção, no escopo deste trabalho, do coprocessador apresentado. Adicionalmente, a viabilidade destas tecnologias é analisada sob a óptica da computação pessoal.

7 ANÁLISE DE TECNOLOGIAS DE IMPLEMENTAÇÃO DE COMPUTADORES QUÂNTICOS

No Capítulo 5, discutiu-se a utilização do algoritmo de Grover para aceleração das assinaturas CFS. A seguir, no Capítulo 6, uma arquitetura usando um coprocessador quântico que implementa o algoritmo de Grover foi apresentada. Neste capítulo, algumas tecnologias de implementação de computadores quânticos são estudadas com maior profundidade. A ideia deste estudo é analisar a viabilidade da implementação de computadores quânticos sob duas ópticas: a da computação pessoal e a de sua construção no contexto deste trabalho.

A primeira visa preencher o que parece ser uma falha na comunidade acadêmica. Os trabalhos na área de computação quântica visam apenas a implementação de dispositivos capazes de computar e pouco foi discutido no que tange a viabilidade de usar esses dispositivos em um contexto exterior a um laboratório especializado de pesquisa.

Já a segunda tem como objetivo dar uma direção futura ao presente trabalho. Busca-se, portanto, identificar como os circuitos propostos ao longo deste trabalho poderiam ser implementados na prática, dentro do Departamento de Engenharia de Computação e Sistemas Digitais da EPUSP.

As tecnologias escolhidas para análise foram as baseadas em silício (pontos quânticos e junções de Josephson) e as baseadas em fotônica (óptica). As tecnologias baseadas em silício possuem forte apelo do mercado, uma vez que poderiam tirar proveito

do parque industrial de semicondutores já instalado ao redor do mundo. As tecnologias baseadas em óptica são as mais interessantes do ponto de vista da comunicação, uma vez que elas permitem a transmissão de informação quântica, o que não foi viabilizado com outras tecnologias ainda.

Para a primeira óptica de análise, propõe-se aqui, duas características necessárias para a computação pessoal. A seguir, as tecnologias escolhidas serão confrontadas com estes requisitos e com aqueles propostos para a computação e comunicação quântica.

A segunda análise levanta os materiais necessários para a realização de cada uma das tecnologias estudadas. Além disso, busca-se identificar o conhecimento e as técnicas que precisam ser dominadas para a implementação destas.

7.1 Requisitos para Computação Pessoal

Antes de iniciar a análise das tecnologias escolhidas, nesta seção são propostos alguns requisitos específicos para a computação pessoal. Eles devem ser vistos como um complemento aos requisitos à computação quântica, já amplamente aceitos pela comunidade, apresentados na Seção 3.4.1 e aqui recordados:

1. sistema físico escalável com qubits bem determinados;
2. habilidade de inicializar o estado para um estado simples e conhecido;
3. tempos de decoerência muito maiores que o tempo de uma operação;
4. conjunto universal de portas quânticas;
5. capacidade de medição em um qubit arbitrário;
6. habilidade de converter qubits estacionário/voadores;
7. capacidade de transmissão fiel de um qubit voador.

Esses requisitos adicionais, aqui propostos, não estão relacionados à tecnologia quântica em si, mas podem ser aplicadas a ela, sendo necessários para habilitar a computação pessoal.

No contexto deste trabalho, a expressão “computação pessoal” é usada com o sentido de uma máquina operada por uma única pessoa, dentro de sua rotina diária. Ele se opõe aos primeiros computadores que ocupavam salas inteiras, consumindo grande quantidade de energia e precisavam de grande número de especialistas para serem usados (PRESS, 1993). Essa segunda visão é a que mais se aproxima dos computadores quânticos hoje, com características proibitivas para um pequeno escritório ou para uma residência.

7.1.1 Tamanho Físico Razoável

A adoção de computadores cada vez menores é definitivamente uma tendência (AGAR, 2005). A descoberta do transistor e os avanços na miniaturização dos componentes eletrônicos (CHAU *et al.*, 2010) permitiram a popularização de tecnologias como *desktops*, *notebooks*, *smartphones*, e mais recentemente *tablets* (PRESS, 1993). Logo, é natural a comparação do desenvolvimento da computação pessoal com a computação quântica, criando expectativas relativas a um computador quântico pessoal.

Enquanto os requisitos propostos por DiVincenzo (Seção 3.4.1) são suficientes para permitir a realização de cálculos e comunicação com uso de computadores quânticos, a existência de dispositivos “pequenos” é uma necessidade para a computação pessoal. Dentro deste requisito duas análises são necessárias: o tamanho do dispositivo de cálculo em si e o tamanho dos periféricos necessários. Nesta segunda conta devem ser inclusos equipamento para resfriamento, aparatos de controle de pulsos, vibração, armaduras para isolamento do sistema contra interferências externas, entre outros. É claro que nem todas as tecnologias usam todos esses equipamentos, mas o importante é considerar o conjunto e não apenas o circuito quântico.

7.1.2 Baixo Custo de Energia

É comum encontrar referências na literatura argumentando que a computação quântica conserva energia (exceto pelas observações). Essa observação é válida do ponto de vista da entropia, uma vez que portas quânticas são reversíveis, não havendo perda de informação, tampouco energia associada a elas (NIELSEN; CHUANG, 2000). No entanto, fica de fora desta conta os mecanismos de controle e resfriamento necessários para colocar e manter o sistema quântico no estado de operação. Também não são considerados os custos energéticos para a geração dos estados, seja uma fonte de fótons ou síntese de moléculas.

Novamente, essa lista não é plenamente aplicável a cada uma das tecnologias de implementação, mas ao menos um desses gastos é necessário para cada tecnologia. Esse custo colateral de energia precisa ser considerado para a escala industrial da computação quântica. O que se defende aqui não é que um computador quântico tenha consumo energético compatível a um *desktop* atual, mas que a demanda energética daquele não seja grande se comparado ao consumo médio de um eletrodoméstico. Mais do que isso, caso a portabilidade seja desejada, os custos energéticos devem ser compatíveis com a capacidade de uma bateria.

7.2 Análise das Tecnologias sob a Óptica da Computação Pessoal

Nesta seção, é apresentada uma análise de tecnologias de implementação de computadores quânticos de acordo com os sete requisitos para computação e comunicação quânticas apontados na Seção 3.4.1 e de acordo com os dois requisitos apontados para a computação pessoal quântica, apresentados na Seção 7.1. As tecnologias escolhidas para esta análise foram as baseadas em silício e a baseada em óptica linear. A escolha destas tecnologias se deve a sua maturidade e grande possibilidade que elas apresentam

de serem adotadas, no caso do silício para a computação e no caso da óptica para a comunicação. Um resumo dessa comparação é feito na Tabela 7, os próximos parágrafos se dedicam a explicar as entradas dessa tabela.

Tabela 7: Análise comparativa de três tecnologias de implementação de computadores quânticos, usando como base 5 requisitos para a computação, 2 para a comunicação e 2 para a computação pessoal. Numeração usada segue a listagem da Seção 7.1, 8 foi atribuído para tamanho razoável e 9 para baixo custo de energia.

Tecnologia	Requisitos para computação quântica					Requisitos para comunicação		Requisitos para computação pessoal	
	1	2	3	4	5	6	7	8	9
Pontos Quânticos	Em Teoria	Sim	Sim (em GaAs)	Sim	Sim	Talvez	Sem proposta	Não ¹	Não ¹
Qubits supercondutores	Em Teoria	Sim	Em alguns casos	Sim	Sim	Talvez	Talvez	Não ¹	Não ¹
Óptica linear	Não	Sim	Sim	Sim	Sim	Talvez	Sim	Talvez	Sim

É amplamente aceito que tecnologias de estado sólido (tais quais as duas baseadas em silício, aqui discutidas) serão as únicas a permitir um grande número de qubits ($\geq 10^3$) (SHERWIN; IMAMOGLU; MONTROY, 1999). Essas tecnologias de estado sólido já avançaram nesse caminho, mas para preencher realmente o que se espera, resta muito por fazer. As implementações feitas até hoje possuem apenas um pequeno número de qubits, e apesar de se considerar que dispositivos na escala de algumas centenas de qubits encontram-se em projeto (OSKIN; CHONG; CHUANG, 2002), não se sabe se eles irão funcionar. Por isso, considera-se que essas tecnologias podem ser escaladas em teoria. Já no caso da óptica, não se acredita que essa escalabilidade possa ser atingida (SHERWIN; IMAMOGLU; MONTROY, 1999).

O tempo de decoerência pode ser considerado atingido para as três tecnologias (NIELSEN; CHUANG, 2000). No caso de junções de Josephson, o cumprimento deste requi-

¹Não é possível devido à restrição de temperatura.

sito é possível para alguns conjuntos de parâmetros (MARTINIS *et al.*, 2002; MAKHLIN; SCHÖN; SHNIRMAN, 2001), já no caso dos pontos quânticos, ele é possível com o uso de GaAs (KIKKAWA; AWSCHALOM, 1998). Além disso, nos casos das tecnologias de silício, a possibilidade de um grande número de qubits permite o uso de técnicas de correção de erros, diminuindo o impacto da decoerência (SVORE; TERHAL; DIVINCENZO, 2005).

Os outros requisitos para a computação foram demonstrados, de alguma forma. Inicialização, conjunto universal de porta e medições foram todas demonstradas com sucesso: junções de Josephson (NAKAMURA; PASHKIN; TSAI, 1999; CHIORESCU *et al.*, 2003; HARRIS *et al.*, 2010), pontos quântico (HANSON *et al.*, 2007) e óptica linear (KOK *et al.*, 2007; KNILL; LAFLAMME; MILBURN, 2001; KWIAT *et al.*, 2000).

Considerando que a escalabilidade venha a ser atingida nas tecnologias baseadas em silício, os cinco requisitos básicos ficam demonstrados para essas tecnologias. O mesmo não é válido, e provavelmente não será verdade (SHERWIN; IMAMOGLU; MONTROY, 1999), para as tecnologias baseadas em óptica. O próximo quesito a ser analisado é a comunicação. Nesse aspecto duas possibilidades devem ser consideradas. No caso do silício o armazenamento é trivial, então é necessário um mecanismo de comunicação, seja através de conversão para outra tecnologia, ou através de algum método direto. Já no caso da óptica, o problema é o contrário, a comunicação é trivial (os fótons já estão viajando pelo espaço), é necessário então encontrar uma forma de armazenar os qubits localmente, em um esquema de memória ou registrador.

É justamente nesse ponto que começam os grandes desafios. O teorema da impossibilidade de cópia (NIELSEN; CHUANG, 2000) impede a conversão via cópia direta de um estado voador em um estado estacionário. A interconexão entre tecnologias baseadas em silício e tecnologias baseadas em fotônica foi proposta, mas ainda não foi provada prática (TIAN *et al.*, 2004). Isso responde pelas entradas “Talvez” na Tabela 7. Uma outra possibilidade é a comunicação direta com junções de Josephson (ROMITO;

FAZIO; BRUDER, 2005), mas não existe prova prática de que tal esquema funcione, tampouco se sabe as distâncias em que essa abordagem seria prática. Como mencionado, em uma tecnologia óptica, a comunicação é trivial. No entanto, técnicas para guardar estados quânticos para uso posterior (sejam memórias ou registradores) são necessárias. Até a presente data, diversas propostas se apresentaram mas nenhuma proposta se mostrou convincente sobre todos os aspectos necessários (fidelidade, desempenho, tempo de vida) (LVOVSKY; SANDERS; TITTEL, 2009).

Finalmente, quando considerados os aspectos de praticidade, o cenário é ainda pior. No caso das soluções baseadas em silício, tanto Josephson como pontos quânticos, necessitam de temperaturas de operação extremamente baixas ($< 1\text{K}$). Não é razoável pensar que tais temperaturas podem ser consideradas práticas em um ambiente doméstico ou comercial. O aparato de resfriamento para essas temperatura possui tamanho desencorajante e consomem quantidade proibitiva de energia para um *desktop*. Pode-se argumentar que as tecnologias de supercondutores de altas temperaturas poderia viabilizar as junções de Josephson, no entanto, para que os tempos de decoerência longos, temperaturas baixas ainda seriam necessárias.

Já no caso de óptica a temperatura não é um problema. Dispositivos ópticos quânticos operam em temperatura ambiente sem perdas de desempenho. O desafio, neste caso, está relacionado ao tamanho. Componentes ópticos, tais como lentes e espelhos, mesmo que possam ser reduzidos são discretos, ou seja devem ser montados em uma estrutura maior, limitando a possibilidade de miniaturização.

Obviamente, essas limitações não são apontadas com o intuito de desencorajar o uso destas tecnologias, mas servem como um conjunto de desafios de pesquisa que precisam ser vencidos para permitir a implementação prática desses esquemas. No pior caso, ou seja, caso esses desafios não venham a ser vencidos, um estudo deste tipo possibilitará entender em que situações cada tecnologia pode ser usada.

7.3 Estudo de Viabilidade da Construção de Computadores Quânticos

Nesta seção, examina-se quais os materiais necessários para a construção de computadores quânticos, usando cada uma das três tecnologias propostas no início deste capítulo. As técnicas de pontos quânticos e junções de Josephson foram agrupadas dentro deste análise, uma vez que suas necessidades são similares. Adicionalmente, procura-se identificar quais técnicas precisam ser dominadas para a implementação destas tecnologias.

7.3.1 Óptica Linear

As primeiras propostas de implementações de computadores quânticos baseadas em fótons dependiam do uso de óptica não-linear (NIELSEN; CHUANG, 2000). Essa necessidade era a principal desvantagem destas implementações, uma vez que a construção de elementos ópticos não-lineares não é trivial (NIELSEN; CHUANG, 2000).

No entanto, Knill, Laflamme e Milburn (2001) provaram que é possível a construção de um computador quântico com o uso apenas de elementos ópticos lineares, usando realimentação. Esse resultado simplifica as necessidades materiais para a construção de um dispositivo quântico baseado em fótons.

Segundo Kok *et al.* (2007), os elementos necessários para a computação quântica com óptica linear são alguns tipos de lentes especiais: divisores de feixe, lâminas de meia e quarto de onda e deslocadores de fase. Adicionalmente, fontes e detectores de um fóton são necessários para geração de estados e medições (KNILL; LAFLAMME; MILBURN, 2001). Apesar de não mencionados, espelhos costumam ser usados para a mudança da direção dos feixes luminosos, no entanto, não há nenhuma necessidade especial sobre estes elementos.

Os elementos passivos (lentes e espelhos), apesar de suas peculiaridades, não são

um grande problema. Esse tipo de material pode ser comprado em lojas especializadas, sem grandes dificuldades, além, é claro, de sua correta especificação.

O maior problema nesse tipo de construção são as fontes e os detectores de um fóton. O modelo proposto por Knill, Laflamme e Milburn (2001) usa o modelo de qubit bosônico, *i.e.* o valor do qubit está relacionado ao número de fótons em cada modo óptico, ou seja, contado por cada detector. Apesar de diversos avanços na área, a construção de fonte e detectores de um fóton de alta precisão ainda é um problema de pesquisa (JENNEWEIN; BARBIERI; WHITE, 2011).

Para a operação de tais dispositivos, a leitura simultânea de diversos eventos em diferentes detectores é necessária (KOK *et al.*, 2007), esse tipo de trabalho exige um grande controle do sistema, em geral obtido com auxílio computacional. Essa necessidade representa um grande trabalho inicial para a realização da montagem do sistema, de forma que todos os componentes funcionem adequadamente.

Finalmente, a montagem destes elementos ópticos exige uma mesa de montagem, que para o número de elementos propostos deve possuir grandes dimensões ($\approx 20m^2$). Esse tipo de equipamento pode ser encontrado por exemplo na Lambda Scientific Systems (SCIENTIFIC, 2012).

7.3.2 Tecnologias Baseadas em Silício

Nesta seção são analisadas duas tecnologias baseadas em silício: pontos quânticos e junções de Josephson. Vale ressaltar que existem propostas de implementações baseadas em pontos quânticos com outros substratos, tal como o grafeno (TRAUZETTEL *et al.*, 2007), mas a análise aqui conduzida não é válida para essas outras tecnologias.

Duas necessidades emergem das discussões apresentadas nas Seções 3.4.2 e 7.2: dopagem de silício e temperaturas na ordem de mK. O aparato necessário para a dopagem de silício é extremamente conhecido e as técnicas utilizadas são bem dominadas.

Além disso, as implementações, usando essas tecnologias, colocadas na prática até hoje não usam o estado da arte na produção desses elementos, bastando alguns microns (SHERWIN; IMAMOGLU; MONTROY, 1999; BURKARD; LOSS; DIVINCENZO, 1999; PLOURDE *et al.*, 2004), o que, sem dúvida, facilita o processo. Além disso, processos de resfriamento a baixíssimas temperaturas são bem conhecidos e suficientemente dominados. No entanto, esses dois aparatos são custosos e volumosos.

Um outro problema está relacionado a operação dos dispositivos. Tanto no caso de pontos quânticos como no caso de junções supercondutoras os pulsos eletromagnéticos e as tensões aplicadas deve ser suficientemente precisas e, no caso de operadores de mais de um qubit, sincronizadas para a manipulação correta dos estados (MARTINIS *et al.*, 2002; PLOEG *et al.*, 2007; HARRIS *et al.*, 2010).

Esses requisitos demandam um grande conhecimento dos sistemas e de sua operação e em geral devem ser controlados por um grupo grande de pessoas, o que dificulta sua adoção num contexto de não especialistas nessas tecnologias.

7.3.3 Análise

Nesta seção foram discutidos os principais requisitos práticos para a construção de computadores quânticos usando óptica linear e tecnologias baseadas em silício. Essa discussão buscou observar os aspectos mais pragmáticos dessa construção, deixando de lado as vantagens ou desvantagens, ou mesmo as teorias físicas suportando destas tecnologias.

O maior problema relacionado às tecnologias de silício está na disponibilidade de fábricas de supercondutores, praticamente inexistentes no país. A fabricação dos semicondutores é obrigatória, uma vez que o projeto usado na construção de junções de Josephson ou de pontos quânticos é diferente do usado em semicondutores de mercado existentes hoje. Uma outra necessidade é o treinamento de pessoal para a operação dos circuitos fabricados, que está longe de ser uma tarefa trivial.

Já no caso da óptica, a compra de componentes de prateleira é possível, mesmo no caso das fontes e detectores de um fóton. No caso destes, equipamentos de baixa precisão são suficientes para testes iniciais, apesar de não serem ideias para uso prático. Além disso, a possibilidade de operação em temperatura ambiente é uma grande vantagem nessa tecnologia. Tendo em vista essas vantagens, a escolha de uma solução baseada em óptica parece mais razoável.

7.4 Sumário do Capítulo 7

Neste capítulo foram analisadas três tecnologias de implementação de computadores quânticos sob a óptica da computação pessoal. As tecnologias baseadas em silício e em óptica foram analisadas contra três conjuntos de requisitos: requisitos para a computação quântica, requisitos para a comunicação e requisitos para a computação pessoal. A escolha destas tecnologias se deve ao fato de serem promissoras, seja para fins de computação ou para fins de comunicação. Essas tecnologias também foram analisadas sob o ponto de vista de implementação como continuidade a este trabalho, seja pelo autor ou por qualquer interessado. Nesse quesito, foram considerados aspectos pragmáticos, como a compra de equipamentos necessário, espaço físico e temperatura de operação.

O próximo capítulo conclui esta dissertação. Os objetivos do trabalho propostos no início desse texto são retomados sob a luz do que foi feito ao longo deste trabalho. As principais contribuições são lembradas e um caminho a seguir é proposto.

8 CONSIDERAÇÕES FINAIS

O principal objetivo de pesquisa deste trabalho foi o estudo de viabilidade da construção física de um computador quântico. Dentro deste objetivo, optou-se por restringir o escopo a uma única aplicação, bem definida e simples.

A tarefa escolhida, a busca de síndromes decodificáveis de Goppa, foi definida no Capítulo 4 e a metodologia de execução da tarefa foi desenvolvida no Capítulo 5. Ficou mostrado então, neste capítulo, que a metodologia proposta é capaz de acelerar o processo de busca por síndromes decodificáveis, dentro do contexto das assinaturas CFS paralelas. Todo o processo foi validado com a simulação do circuito no simulador de computadores quânticos QCL.

A seguir, no Capítulo 6, um circuito quântico, na forma de coprocessador e capaz de executar a tarefa proposta, foi definido. A forma de coprocessador para um dispositivo quântico traz diversas vantagens, como a preparação do estado quântico apenas no momento em que será usado. Além disso, a adoção de um controlador permite a abstração, no contexto do núcleo de processamento, de que se trata de um circuito quântico.

Finalmente, o estudo de viabilidade da implementação foi realizado ao longo do Capítulo 7. Três tecnologias de implementação foram consideradas: óptica linear, pontos quânticos e junções de Josephson. Essas tecnologias foram analisadas sob um total de nove requisitos, agrupados em três grupos: requisitos para a computação quântica, requisitos para a comunicação e requisitos para a computação pessoal. Essas tecno-

logias também foram analisadas com ênfase na viabilidade de sua construção como continuação a este trabalho, no contexto do Departamento de Engenharia de Computação e Sistemas Digitais da EPUSP.

Além desse objetivo geral, algumas contribuições originais de pesquisa foram alcançadas. No Capítulo 5 é proposta a utilização de algoritmos quânticos para a aceleração de métodos de criptografia puramente clássicos, uma abordagem nova na literatura. Neste mesmo capítulo, demonstra-se que, caso computadores quânticos grandes venham a se tornar estáveis, eles viabilizarão a criptografia pós-quântica com um número menor de qubits do que o necessário para quebrar a atual criptografia assimétrica.

Uma outra contribuição interessante é a proposta de uma arquitetura híbrida no Capítulo 6, tendo um processador tradicional clássico e um coprocessador quântico. Essa abordagem pode ser vista como uma transição entre os atuais computadores e computadores puramente quânticos. Possibilitando a utilização das vantagens já conhecidas da computação quântica antes da viabilização de um computador 100% quântico. Finalmente, no Capítulo 7 são propostos dois requisitos para a computação pessoal, gerais, mas que podem ser aplicados ao caso particular da computação quântica. Além disso, três tecnologias são analisadas sob diversos requisitos, gerando uma lista de desafios de pesquisa a serem vencidos por elas.

8.1 Trabalhos Futuros

A continuação óbvia deste trabalho é a construção física do circuito quântico proposto. Caso a tecnologia escolhida seja óptica, todos os elementos básicos são dados ao longo deste texto. Se uma outra tecnologia for escolhida, alguns elementos adicionais precisarão ser escolhidos.

Uma outra possibilidade de continuação é otimizar ainda mais o processo de decodificação de Patterson para códigos de Goppa, ou ainda estender o trabalho para outros

métodos pós-quânticos (todo o criptossistema McEliece/Niederreiter, outros códigos, ou até mesmo reticulados e sistemas multivariados). Para isso seria necessário, inicialmente, identificar em quais partes do método escolhido a computação quântica poderia ser útil.

8.2 Perspectivas do Campo

A área da computação quântica é ainda muito nova e imatura em diversos aspectos. A começar pelo pequeno número de algoritmos existentes, que sem dúvida levantam questionamentos sobre a utilidade real de tais dispositivos. A grande quantidade de tecnologias de implementação, cada uma com suas vantagens e falhas também é um indicador desta imaturidade. Mais que isso, ao se observar os trabalhos em andamento, tem-se a impressão que as tecnologias existentes pouco evoluem e novas tecnologias surgem.

Ao mesmo tempo que tal imaturidade levanta questionamentos sobre a capacidade dos pesquisadores da área para viabilizar tal tecnologia, ela garante a qualquer pesquisador interessado um vasto e fértil campo de pesquisa.

Neste trabalho, buscou-se abordar algumas das questões que ainda parecem abertas, como por exemplo, como se dará a transição dos computadores atuais para computadores quânticos. Outra questão importante aqui levantada diz respeito à existência de computadores quânticos pessoais.

Mas a questão fundamental a ser respondida permanece: serão estes computadores possíveis em alguma escala em um futuro próximo?

REFERÊNCIAS

AGAR, J. *Constant Touch : A Global History of the Mobile Phone*. Minneapolis: Totem Books, 2005. Paperback. ISBN 1840465417.

ASPECT, A.; DALIBARD, J.; ROGER, G. Experimental test of bell's inequalities using time- varying analyzers. *Phys. Rev. Lett.*, American Physical Society, v. 49, p. 1804–1807, Dec 1982. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevLett.49.1804>>.

BACON, D. Decoherence, control, and symmetry in quantum computers. *Control*, p. 261, 2003. Disponível em: <<http://arxiv.org/abs/quant-ph/0305025>>. Acesso em: 29 de agosto de 2012.

BARENCO, A.; DEUTSCH, D.; EKERT, A.; JOZSA, R. Conditional quantum dynamics and logic gates. *Phys. Rev. Lett.*, American Physical Society, v. 74, p. 4083–4086, May 1995. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevLett.74.4083>>. Acesso em: 29 de agosto de 2012.

BARKER, E.; BARKER, W.; BURR, W.; POLK, W.; SMID, M. *Recommendation for Key Management - Part 1: General (Revised)*. Washington, mar. 2007. Disponível em: <<http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf>>. Acesso em 29 de agosto de 2012.

BARNUM, H.; CREPEAU, C.; GOTTESMAN, D.; SMITH, A.; TAPP, A. Authentication of quantum messages. *Proc. of 43rd Annual IEEE Symposium on the Foundations of Computers*, v. 02, p. 449, 2002.

BARRETO, P. *Construção de parâmetros e algoritmos eficientes para criptossistemas pós-quânticos baseados em teoria dos códigos*. Outubro 2011. Tese (Livre Docência) - Escola Politécnica da USP, São Paulo, SP, Brasil, 2011.

BARRETO, P. S. L. M.; CAYREL, P.-L.; MISOCZKI, R.; NIEBUHR, R. Quasi-dyadic CFS signatures. In: *International Conference on Information Security and Cryptology – Inscrypt 2010*. Shanghai, China: Springer, 2010. (Lecture Notes in Computer Science, v. 6584).

BELL, J. S. On the problem of hidden variables in quantum mechanics. *Rev. Mod. Phys.*, American Physical Society, v. 38, p. 447–452, Jul 1966. Disponível em: <<http://link.aps.org/doi/10.1103/RevModPhys.38.447>>.

BENNETT, C. H.; BRASSARD, G. Quantum cryptography : Public key distribution and coin tossing. *Proc. of IEEE Int. Conf. on Computers, Systems and Signal Processing*, 1984. Disponível em: <<http://ci.nii.ac.jp/naid/10016853803/en/>>. Acesso em: 29 de agosto de 2012.

BERNSTEIN, D. J. *List decoding for binary Goppa codes*. 2008. Unpublished manuscript. Disponível em: <<http://cr.yp.to/papers.html>>. Acesso em: 29 de agosto de 2012.

BERNSTEIN, D. J.; BUCHMANN, J.; DAHMEN, E. *Post-Quantum Cryptography*. Heidelberg, Deutschland: Springer, 2008.

BETTELLI, S.; CALARCO, T.; SERAFINI, L. Toward an architecture for quantum programming. *The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics*, Springer Berlin / Heidelberg, v. 25, p. 181–200, 2003. ISSN 1434-6060. 10.1140/epjd/e2003-00242-2. Disponível em: <<http://dx.doi.org/10.1140/epjd/e2003-00242-2>>.

BISHOP, M. *Computer Security: Art and Science*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2002. Hardcover. ISBN 0201440997.

BLOCH, I. Ultracold quantum gases in optical lattices. *Nat Phys*, v. 1, n. 1, p. 23–30, out. 2005. ISSN 1745-2473. Disponível em: <<http://dx.doi.org/10.1038/nphys138>>. Acesso em: 29 de agosto de 2012.

BORJA, M. C.; HAIGH, J. The birthday problem. *Significance*, Blackwell Publishing Ltd, v. 4, n. 3, p. 124–127, 2007. ISSN 1740-9713. Disponível em: <<http://dx.doi.org/10.1111/j.1740-9713.2007.00246.x>>. Acesso em: 29 de agosto de 2012.

BURKARD, G.; LOSS, D.; DIVINCENZO, D. P. Coupled quantum dots as quantum gates. *Phys. Rev. B*, American Physical Society, v. 59, p. 2070–2078, Jan 1999. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevB.59.2070>>. Acesso em: 29 de agosto de 2012.

CALLIOLI, C. A.; DOMINGUES HYGINO, H.; COSTA, R. C. F. *Álgebra Linear e Aplicações*. São Paulo: Editora Atual, 1998. Paperback. ISBN 85-7056.297-7.

CAVES, C. M.; SCHUMAKER, B. L. New formalism for two-photon quantum optics. I. Quadrature phases and squeezed states. *Phys. Rev. A*, American Physical Society, v. 31, p. 3068–3092, May 1985. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevA.31.3068>>. Acesso em: 29 de agosto de 2012.

CHAU, R.; DOCZY, M.; DOYLE, B.; DATTA, S.; DEWEY, G.; KAVALIEROS, J.; JIN, B.; METZ, M.; CMOS, H.-p. S. Advanced CMOS transistors in the nanotechnology era for high-performance , low-power logic applications. *Film, Ieee*, v. 1, p. 26–30, 2010.

CHIORESCU, I.; NAKAMURA, Y.; HARMANS, C. J. P. M.; MOOIJ, J. E. Coherent Quantum Dynamics of a Superconducting Flux Qubit. *Science*, v. 299, p. 1869–1872, mar. 2003.

CIRAC, J. I.; ZOLLER, P. Quantum computations with cold trapped ions. *Phys. Rev. Lett.*, American Physical Society, v. 74, p. 4091–4094, May 1995. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevLett.74.4091>>.

COURTOIS, N.; FINIASZ, M.; SENDRIER, N. How to achieve a McEliece-based digital signature scheme. In: *Advances in Cryptology – Asiacrypt 2001*. Gold Coast, Australia: Springer, 2001. (Lecture Notes in Computer Science, v. 2248), p. 157–174.

DALLOT, L. Research in cryptology. In: *Research in Cryptology*. Berlin, Heidelberg: Springer-Verlag, 2008. cap. Towards a Concrete Security Proof of Courtois, Finiasz and Sendrier Signature Scheme, p. 65–77. ISBN 978-3-540-88352-4. Disponível em: <http://dx.doi.org/10.1007/978-3-540-88353-1_6>. Acesso em: 29 de agosto de 2012.

DEUTSCH, D. Quantum theory, the Church-Turing principle and the universal quantum computer. In: ROYAL SOCIETY. *Proceedings of the Royal Society of London. Series A*. London, 1985. v. 400, n. 1818, p. 97–117.

DEUTSCH, D.; BARENCO, A.; EKERT, A. Universality in Quantum Computation. *Royal Society of London Proceedings Series A*, v. 449, p. 669–677, jun. 1995.

DIRAC, P. *The Principles of Quantum Mechanics*. Oxford: Clarendon Press, 1981. (International Series of Monographs on Physics). ISBN 9780198520115.

DIVINCENZO, D. P. Two-bit gates are universal for quantum computation. *Phys. Rev. A*, American Physical Society, v. 51, p. 1015–1022, Feb 1995. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevA.51.1015>>. Acesso em: 29 de agosto de 2012.

_____. The physical implementation of quantum computation. In: _____. *Scalable Quantum Computers*. Berlin: Wiley-VCH Verlag GmbH & Co. KGaA, 2005. p. 1–13. ISBN 9783527603183.

EINSTEIN, A.; PODOLSKY, B.; ROSEN, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, American Physical Society, v. 47, p. 777–780, May 1935. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRev.47.777>>. Acesso em: 29 de agosto de 2012.

EISENBARTH, T.; GÜNEYSU, T.; HEYSE, S.; PAAR, C. MicroEliece: McEliece for embedded devices. In: *Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems*. Berlin, Heidelberg: Springer-Verlag, 2009. (CHES '09), p. 49–64. ISBN 978-3-642-04137-2.

EKERT, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, American Physical Society, v. 67, p. 661–663, Aug 1991. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevLett.67.661>>. Acesso em: 29 de agosto de 2012.

FEYNMAN, R. Quantum mechanical computers. *Foundations of Physics*, Springer Netherlands, v. 16, p. 507–531, 1986. ISSN 0015-9018. 10.1007/BF01886518.

FINIASZ, M. Parallel-CFS: Strengthening the CFS McEliece-based signature scheme. In: BIRYUKOV, A.; GONG, G.; STINSON, D. (Ed.). *Workshop on Selected Areas in Cryptography – SAC 2010*. Berlin: Springer, 2010. (Lecture Notes in Computer Science, v. 6544), p. 161–172.

FINIASZ, M.; SENDRIER, N. Security bounds for the design of code-based cryptosystems. In: MATSUI, M. (Ed.). *Asiacrypt 2009*. Berlin: Springer, 2009. (Lecture Notes in Computer Science, v. 5912), p. 88–105.

FREDKIN, E.; TOFFOLI, T. Conservative logic. *International Journal of Theoretical Physics*, Springer Netherlands, v. 21, p. 219–253, 1982. ISSN 0020-7748. Disponível em: <<http://dx.doi.org/10.1007/BF01857727>>. Acesso em: 29 de agosto de 2012.

GOPPA, V. D. A new class of linear error correcting codes. *Problemy Peredachi Informatsii*, v. 6, p. 24–30, 1970.

GROVER, L. K. A fast quantum mechanical algorithm for database search. In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. New York, NY, USA: ACM, 1996. (STOC '96), p. 212–219. ISBN 0-89791-785-5.

HANKERSON, D.; MENEZES, A. J.; VANSTONE, S. *Guide to Elliptic Curve Cryptography*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003. ISBN 038795273X.

HANSON, R.; KOUWENHOVEN, L. P.; PETTA, J. R.; TARUCHA, S.; VANDERSYPEN, L. M. K. Spins in few-electron quantum dots. *Rev. Mod. Phys.*, American Physical Society, v. 79, p. 1217–1265, Oct 2007. Disponível em: <<http://link.aps.org/doi/10.1103/RevModPhys.79.1217>>. Acesso em: 29 de agosto de 2012.

HARRIS, R.; JOHANSSON, J.; BERKLEY, A. J.; JOHNSON, M. W.; LANTING, T.; HAN, S.; BUNYK, P.; LADIZINSKY, E.; OH, T.; PERMINOV, I.; TOLKACHEVA, E.; UCHAIKIN, S.; CHAPPLE, E. M.; ENDERUD, C.; RICH, C.; THOM, M.; WANG, J.; WILSON, B.; ROSE, G. Experimental demonstration of a robust and scalable flux qubit. *Phys. Rev. B*, American Physical Society, v. 81, p. 134510, Apr 2010. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevB.81.134510>>. Acesso em: 29 de agosto de 2012.

HOWARD, J. D. *An analysis of security incidents on the Internet 1989-1995*. Tese (Doutorado) — Carnegie Mellon University, Pittsburgh, PA, USA, 1998. UMI Order No. GAX98-02539.

HUFFMAN, W.; PLESS, V. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003. ISBN 9780521782807. Disponível em: <<http://books.google.com.br/books?id=RAsjychHkLYC>>.

JELEZKO, F.; GAEBEL, T.; POPA, I.; DOMHAN, M.; GRUBER, A.; WRACHTRUP, J. Observation of coherent oscillation of a single nuclear spin and realization of a two-qubit conditional quantum gate. *Phys. Rev. Lett.*, American Physical Society, v. 93, p. 130501, Sep 2004. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevLett.93.130501>>. Acesso em: 29 de agosto de 2012.

JENNEWEIN, T.; BARBIERI, M.; WHITE, A. G. Single-photon device requirements for operating linear optics quantum computing outside the post-selection basis. *Journal of Modern Optics*, v. 58, n. 3-4, p. 276–287, 2011.

KANE, B. E. A silicon-based nuclear spin quantum computer. *Nature*, v. 393, n. 6681, p. 133–137, maio 1998. ISSN 0028-0836. Disponível em: <<http://dx.doi.org/10.1038/30156>>. Acesso em: 29 de agosto de 2012.

KIKKAWA, J. M.; AWSCHALOM, D. D. Resonant spin amplification in *n*-type GaAs. *Phys. Rev. Lett.*, American Physical Society, v. 80, p. 4313–4316, May 1998. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevLett.80.4313>>. Acesso em: 29 de agosto de 2012.

KNILL, E.; LAFLAMME, R.; MILBURN, G. J. A scheme for efficient quantum computation with linear optics. *Nature*, v. 409, p. 46–52, jan. 2001.

KOK, P.; MUNRO, W. J.; NEMOTO, K.; RALPH, T. C.; DOWLING, J. P.; MILBURN, G. J. Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.*, American Physical Society, v. 79, p. 135–174, Jan 2007. Disponível em: <<http://link.aps.org/doi/10.1103/RevModPhys.79.135>>. Acesso em: 29 de agosto de 2012.

KOUWENHOVEN, L. P.; AUSTING, D. G.; TARUCHA, S. Few-electron quantum dots. *Reports on Progress in Physics*, v. 64, n. 6, p. 701, 2001. Disponível em: <<http://stacks.iop.org/0034-4885/64/i=6/a=201>>. Acesso em: 29 de agosto de 2012.

KWIAT, P. G.; MITCHELL, J. R.; SCHWINDT, P. D. D.; White, A. G. Grover's search algorithm: an optical approach. *Journal of Modern Optics*, v. 47, p. 257–266, fev. 2000.

LIDE, R.; NIEDERREITER, H. *Finite fields*. New York, NY, USA: Cambridge University Press, 1997. ISBN 0-521-39231-4.

LOSS, D.; DIVINCENZO, D. P. Quantum computation with quantum dots. *Physical Review A*, American Physical Society, v. 57, p. 120–126, jan. 1998. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevA.57.120>>. Acesso em: 29 de agosto de 2012.

LVOVSKY, A. I.; SANDERS, B. C.; TITTEL, W. Optical quantum memory. *Nat Photon*, Nature Publishing Group, v. 3, n. 12, p. 706–714, dez. 2009. ISSN 1749-4885. Disponível em: <<http://dx.doi.org/10.1038/nphoton.2009.231>>.

MAKHLIN, Y.; SCHÖN, G.; SHNIRMAN, A. Quantum-state engineering with Josephson-junction devices. *Rev. Mod. Phys.*, American Physical Society, v. 73, p. 357–400, May 2001. Disponível em: <<http://link.aps.org/doi/10.1103/RevModPhys.73.357>>. Acesso em: 29 de agosto de 2012.

MARTINIS, J. M.; NAM, S.; AUMENTADO, J.; URBINA, C. Rabi oscillations in a large Josephson-junction qubit. *Phys. Rev. Lett.*, American Physical Society, v. 89, p. 117901, Aug 2002. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevLett.89.117901>>. Acesso em: 29 de agosto de 2012.

MCELIECE, R. A *Public-Key Cryptosystem Based On Algebraic Coding Theory*. 1978. 114–116 p. The Deep Space Network Progress Report, DSN PR 42–44. Disponível em: <http://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF>. Acesso em: 29 de agosto de 2012.

ÖMER, B. *Structured Quantum Programming*. Tese (Doutorado) — Institute for Theoretical Physics - Vienna University of Technology, 2009. Disponível em: <<http://portal.acm.org/citation.cfm?id=264393.264406>>. Acesso em: 29 de agosto de 2012.

MISOCZKI, R.; BARRETO, P. Compact McEliece keys from Goppa codes. In: JACOBSON, M.; RIJMEN, V.; SAFAVI-NAINI, R. (Ed.). *Selected Areas in Cryptography*. Berlin / Heidelberg: Springer, 2009, (Lecture Notes in Computer Science, v. 5867). p. 376–392. ISBN 978-3-642-05443-3. Disponível em: <http://dx.doi.org/10.1007/978-3-642-05445-7_24>. Acesso em: 29 de agosto de 2012.

NAKAMURA, Y.; PASHKIN, Y.; TSAI, J. S. Coherent control of macroscopic quantum states in a single-Cooper-pair box. *Nature*, Nature Publishing Group, v. 398, n. 6730, p. 786–788, abr. 1999. ISSN 0028-0836. Disponível em: <<http://dx.doi.org/10.1038/19718>>.

NIEDERREITER, H. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, v. 15, n. 2, p. 159–166, 1986.

NIELSEN, M. A.; CHUANG, I. L. Book. *Quantum computation and quantum information*. Cambridge, UK: Cambridge University Press, 2000. 700p p. ISBN 0521632358.

OKAMOTO, R.; HOFMANN, H. F.; TAKEUCHI, S.; SASAKI, K. Demonstration of an optical quantum controlled-not gate without path interference. *Phys. Rev. Lett.*, American Physical Society, v. 95, p. 210506, Nov 2005.

OSKIN, M.; CHONG, F.; CHUANG, I. A practical architecture for reliable quantum computers. *Computer*, v. 35, n. 1, p. 79–87, jan 2002. ISSN 0018-9162.

PAPADIMITRIOU, C. H. Computational complexity. In: *Encyclopedia of Computer Science*. Chichester, UK: John Wiley and Sons Ltd., 1994. p. 260–265. ISBN 0-470-86412-5. Disponível em: <<http://dl.acm.org/citation.cfm?id=1074100.1074233>>. Acesso em: 29 de agosto de 2012.

PATTERSON, N. J. The algebraic decoding of Goppa codes. *IEEE Transactions on Information Theory*, IEEE, v. 21, n. 2, p. 203–207, 1975.

PELLIZZARI, T.; GARDINER, S. A.; CIRAC, J. I.; ZOLLER, P. Decoherence, continuous observation, and quantum computing: A cavity qed model. *Phys. Rev. Lett.*, American Physical Society, v. 75, p. 3788–3791, Nov 1995.

PIQUEIRA, J. R. C. Teoria quântica da informação: impossibilidade de cópia, entrelaçamento e teletransporte. *Revista Brasileira de Ensino de Física*, scielo, v. 33, p. 4303 – 4303, 12 2011. ISSN 1806-1117. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1806-111720110004000003&nrm=iso>. Acesso em: 29 de agosto de 2012.

PLOEG, S. H. W. van der; IZMALKOV, A.; BRINK, A. M. van den; HÜBNER, U.; GRAJCAR, M.; IL'ICHEV, E.; MEYER, H.-G.; ZAGOSKIN, A. M. Controllable coupling of superconducting flux qubits. *Phys. Rev. Lett.*, American Physical Society, v. 98, p. 057004, Feb 2007. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevLett.98.057004>>.

PLOURDE, B. L. T.; ZHANG, J.; WHALEY, K. B.; WILHELM, F. K.; ROBERTSON, T. L.; HIME, T.; LINZEN, S.; REICHARDT, P. A.; WU, C.-E.; CLARKE, J. Entangling flux qubits with a bipolar dynamic inductance. *Phys. Rev. B*, American Physical Society, v. 70, p. 140501, Oct 2004. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevB.70.140501>>.

POSSIGNOLO, R. T.; MARGI, C. B. A quantum/classical hybrid architecture for security algorithms acceleration. In: *Proceedings of the 11th International IEEE Conference on Trust, Security and Privacy in Computing and Communications*. Liverpool, UK: IEE, 2012. (TrustCom '12), p. 1032–1037. ISBN 978-0-7695-4745-9/12.

PRESS, L. Before the Altair: the history of personal computing. *Commun. ACM*, ACM, New York, NY, USA, v. 36, p. 27–33, September 1993. ISSN 0001-0782. Disponível em: <<http://doi.acm.org/10.1145/162685.162697>>.

RAIMOND, J. M.; BRUNE, M.; HAROCHE, S. Manipulating quantum entanglement with atoms and photons in a cavity. *Rev. Mod. Phys.*, American Physical Society, v. 73, p. 565–582, Aug 2001. Disponível em: <<http://link.aps.org/doi/10.1103/RevModPhys.73.565>>.

RALPH, T. C.; RESCH, K. J.; GILCHRIST, A. Efficient toffoli gates using qudits. *Phys. Rev. A*, American Physical Society, v. 75, p. 022313, Feb 2007.

REED, M.; SIMON, B. *Methods of Modern Mathematical Physics: Fourier analysis, self-adjointness*. New York: Academic Press, 1972. (Methods of Modern Mathematical Physics). ISBN 9780125850506.

RITTER, S.; NOLLEKE, C.; HAHN, C.; REISERER, A.; NEUZNER, A.; UPHOFF, M.; MUCKE, M.; FIGUEROA, E.; BOCHMANN, J.; REMPE, G. An elementary quantum network of single atoms in optical cavities. *Nature*, Nature Publishing Group, a division of Macmillan Publishers Limited. All Rights Reserved., v. 484, n. 7393, p. 195–200, abr. 2012. ISSN 0028-0836. Disponível em: <<http://dx.doi.org/10.1038/nature11023>>.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. M. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, v. 21, p. 120–126, 1978.

ROMITO, A.; FAZIO, R.; BRUDER, C. Solid-state quantum communication with josephson arrays. *Phys. Rev. B*, American Physical Society, v. 71, p. 100501, Mar 2005. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevB.71.100501>>.

SAR, T. van der; WANG, Z. H.; BLOK, M. S.; BERNIEN, H.; TAMINIAU, T. H.; TOYLI, D. M.; LIDAR, D. A.; AWSCHALOM, D. D.; HANSON, R.; DOBROWITSKI, V. V. Decoherence-protected quantum gates for a hybrid solid-state spin register. *Nature*, Nature Publishing Group, a division of Macmillan Publishers Limited. All Rights Reserved., v. 484, n. 7392, p. 82–86, abr. 2012. ISSN 0028-0836. Disponível em: <<http://dx.doi.org/10.1038/nature10900>>.

SCHUMACHER, B. Quantum coding. *Phys. Rev. A*, American Physical Society, v. 51, p. 2738–2747, Apr 1995. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevA.51.2738>>. Acesso em: 29 de agosto de 2012.

SCIENTIFIC, L. *Lambda Scientific Systems, Inc.* 2012. Disponível em <http://www.lambdasys.com>. Acesso em 29 de agosto de 2012.

SHANNON, C. The zero error capacity of a noisy channel. *Information Theory, IRE Transactions on*, v. 2, n. 3, p. 8–19, september 1956. ISSN 0096-1000.

SHERWIN, M. S.; IMAMOGLU, A.; MONTROY, T. Quantum computation with quantum dots and terahertz cavity quantum electrodynamics. *Phys. Rev. A*, American Physical Society, v. 60, p. 3508–3514, Nov 1999. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevA.60.3508>>. Acesso em: 29 de agosto de 2012.

SHOR, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In: *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*. [S.l.: s.n.], 1994. p. 124–134.

_____. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, v. 26, p. 1484–1509, October 1997. ISSN 0097-5397. Disponível em: <<http://portal.acm.org/citation.cfm?id=264393.264406>>. Acesso em: 29 de agosto de 2012.

SIMON, C.; AFZELIUS, M.; APPEL, J.; GIRODAY, A. Boyer de la; DEWHURST, S. J.; GISIN, N.; HU, C. Y.; JELEZKO, F.; KRÖLL, S.; MÜLLER, J. H.; NUNN, J.; POLZIK, E. S.; RARITY, J. G.; RIEDMATTEN, H. D.; ROSENFELD, W.; SHIELDS, A. J.; SKÖLD, N.; STEVENSON, R. M.; THEW, R.; WALMSLEY, I. A.; WEBER, M. C.; WEINFURTER, H.; WRACHTRUP, J.; YOUNG, R. J. Quantum memories. *The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics*, Springer Berlin / Heidelberg, v. 58, p. 1–22, 2010. ISSN 1434-6060. 10.1140/epjd/e2010-00103-y. Disponível em: <<http://dx.doi.org/10.1140/epjd/e2010-00103-y>>.

SPEKKENS, R. W. Evidence for the epistemic view of quantum states: A toy theory. *Phys. Rev. A*, American Physical Society, v. 75, p. 032110, Mar 2007. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevA.75.032110>>. Acesso em: 29 de agosto de 2012.

STALLINGS, W. *Cryptography and Network Security: Principles and Practice*. 5th. ed. Upper Saddle River, NJ, USA: Prentice Hall Press, 2010. ISBN 0136097049, 9780136097044.

SVORE, K. M.; TERHAL, B. M.; DIVINCENZO, D. P. Local fault-tolerant quantum computation. *Phys. Rev. A*, American Physical Society, v. 72, p. 022317, Aug 2005. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevA.72.022317>>.

TIAN, L.; RABL, P.; BLATT, R.; ZOLLER, P. Interfacing quantum-optical and solid-state qubits. *Phys. Rev. Lett.*, American Physical Society, v. 92, p. 247902, Jun 2004. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevLett.92.247902>>.

TRAUZETTEL, B.; BULAEV, D. V.; LOSS, D.; BURKARD, G. Spin qubits in graphene quantum dots. *Nat Phys*, v. 3, n. 3, p. 192–196, mar. 2007. ISSN 1745-2473.

VANDERSYPEN, L. M. K.; STEFFEN, M.; BREYTA, G.; YANNONI, C. S.; SHERWOOD, M. H.; CHUANG, I. L. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, v. 414, n. 6866, p. 883–887, dez. 2001. ISSN 0028-0836. Disponível em: <<http://dx.doi.org/10.1038/414883a>>. Acesso em: 29 de agosto de 2012.

WARREN, W. S. The usefulness of NMR quantum computing. *Science*, v. 277, n. 5332, p. 1688–1690, 1997. Disponível em: <<http://www.sciencemag.org/content/277/5332/1688.short>>. Acesso em: 29 de agosto de 2012.

WATROUS, J. Quantum Computational Complexity. abr. 2008. Disponível em: <<http://arxiv.org/abs/0804.3401v1>>. Acesso em: 29 de agosto de 2012.

WILLIAMS, C. P. *Explorations in Quantum Computing*. London, UK: Springer-Verlag, 2011. ISBN 978-1-84628-886-9.