ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA

COORDENADORIA ACADÊMICA

CURSO DE APERFEIÇOAMENTO DE OFICIAIS 1/2020

ALBERTO HIDEAKI **SAKAJIRI**, Cap Eng

Computação Quântica e a Criptografia na Força Aérea Brasileira

Rio de Janeiro

2020

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO DE APERFEIÇOAMENTO DE OFICIAIS 1/2020

ALBERTO HIDEAKI **SAKAJIRI**, Cap Eng

Computação Quântica e a Criptografia na Força Aérea Brasileira

Trabalho de conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica como requisito parcial para aprovação no Curso de MBA em Gestão Pública com ênfase em Gestão de Projetos e Processos.
Área de Concentração. Multidisciplinar
Orientador: Maj Int Rogério dos Santos Ferreira

Rio de Janeiro

2020

ALBERTO HIDEAKI **SAKAJIRI**, Cap Eng

Computação Quântica e a Criptografia na Força Aérea Brasileira

Trabalho de conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica.

Aprovado por:

_____

Rogério dos Santos Ferreira – Maj Int
EAOAR

_____

Thiago Diorgilis Ribeiro Daniel – Maj Av
EAOAR

_____

Daniel Rodrigues Figueiredo – Maj Av
EAOAR

Rio de Janeiro
Julho de 2020

RESUMO

A Computação Quântica irá tornar obsoleta a criptografia utilizada em sistemas de segurança da informação e pela Força Aérea Brasileira (FAB) em diversas Aplicações Operacionais. Por se tratar de uma tecnologia revolucionária e disruptiva, a FAB deve investir em linhas de pesquisa para o desenvolvimento de modelos próprios de Computação Quântica, podendo garantir ao Brasil independência tecnológica e a liderança em um setor estratégico, além de adquirir conhecimentos para a criação e emprego de novas técnicas criptográficas, resistentes e imunes a ataques cibernéticos de um eventual computador quântico inimigo. A pesquisa e desenvolvimento da computação quântica é fundamental para o futuro da segurança da informação da FAB e terá grandes reflexos na sociedade brasileira.

Palavras-chave: Computação quântica. Criptografia. Segurança da informação.

1 INTRODUÇÃO

O mundo está em guerra. Vivemos atualmente em uma guerra pela informação e seu maior campo de batalha é o meio digital, envolvendo computadores, celulares, redes de telecomunicações e a Internet. O principal meio de defesa em um ambiente de guerra de informação digital é a utilização de sistemas criptográficos, que compreendem técnicas e equipamentos para comunicação e armazenamento seguros de dados. Utilizando técnicas criptográficas assimétricas, estes sistemas eram considerados altamente seguros e inquebráveis. Porém em 1982, o físico Richard Feynman propôs um modelo inovador de computador que utiliza princípios da Mecânica Quântica para fazer sua capacidade computacional crescer exponencialmente. Um computador quântico, quando devidamente desenvolvido, será capaz de quebrar a maior parte dos sistemas criptográficos amplamente utilizados no mundo.

A Computação Quântica irá causar uma revolução na área da criptografia, pois as técnicas utilizadas atualmente se tornarão ineficazes em proteger dados sensíveis. Será uma ruptura dos padrões e tecnologias estabelecidas, sendo necessário a criação de técnicas inovadoras para enfrentar essa mudança de paradigma. Por se tratar de uma tecnologia revolucionária e disruptiva, a Força Aérea Brasileira (FAB) deve investir em linhas de pesquisa para o desenvolvimento de modelos próprios de Computação Quântica.

A computação quântica está em sua infância, uma vez que ainda não existe um computador quântico com grande poder computacional. A criptografia é uma área estratégica, porém grande parte da tecnologia criptográfica utilizada pela FAB atualmente, tanto em nível de *hardware* quanto de *software*, é de origem estrangeira. O desenvolvimento da computação quântica pela FAB pode garantir ao Brasil independência tecnológica e a liderança em um novo setor estratégico.

A FAB utiliza amplamente sistemas criptográficos em Aplicações Operacionais de Comando e Controle, Defesa Cibernética e Guerra Eletrônica. Após a revolução da computação quântica, será necessário empregar novos meios de defesa dos dados para que a FAB consiga cumprir sua missão. Pesquisar e desenvolver a computação quântica permite adquirir conhecimentos para a criação e emprego de novas técnicas criptográficas, resistentes e imunes a ataques cibernéticos de um eventual computador quântico inimigo.

2 DESENVOLVIMENTO

2.1 Computador quântico nacional

Uma das bases da criptografia moderna é a dificuldade de se realizar a fatoração de grandes números por meio de algoritmos computacionais. Um computador é capaz de realizar a multiplicação de dois números inteiros de forma muito rápida e eficiente, dando a resposta de forma quase instantânea. Porém o inverso, ou seja, dado um produto descobrir dois números primos que multiplicados resultam nesse produto, é um problema que só é resolvido com força bruta, testando cada combinação de números um a um. Mesmo utilizando um super computador, realizar a fatoração de um grande número, como por exemplo um número inteiro que possua 900 dígitos, demoraria dezenas de bilhões de anos, mais que a idade estimada de nosso universo (NIELSEN e CHUANG, 2011).

Utilizando estas características, os sistemas criptográficos assimétricos, também chamados tradicionalmente de chave pública, são usados como um método de garantir a confidencialidade, autenticidade e o não-repúdio de comunicações eletrônicas e de armazenamento de dados.

O que diferencia um computador quântico de um computador clássico é a utilização de fenômenos da Mecânica Quântica chamados Superposição e Entrelaçamento. Estes fenômenos permitem que as unidades básicas de informação utilizados por um computador quântico, os chamados bits quânticos ou *qubits*, possam estar nos estados ‘0’ e ‘1’ ao mesmo tempo. Isto possibilita que os computadores quânticos realizem múltiplos cálculos em paralelo, nos dando acesso a um poder computacional sem precedentes (AKAMA, 2019).

Em 1994, Peter Shor publicou um algoritmo que, utilizando um computador quântico com número suficiente de *qubits*, é capaz de fatorar grandes números em segundos (GERJUOY, 2004), provando que é possível quebrar a criptografia de chave pública. Os protocolos que utilizam esse tipo de criptografia incluem o RSA, HTTPS, TLS, SSH, PKI, DAS, ECC, além de serem utilizados em segurança de redes Wi-Fi, *smartcards,* autenticações em duas etapas e na maior parte das criptomoedas (GRIMES, 2020). Isso significa que grande parte da criptografia utilizada em segurança empresarial, na internet e em sistemas de defesa será quebrada.

As implicações do algoritmo de Shor para a FAB são muitas, pois ele atua diretamente em áreas vitais para a aplicação militar do Poder Aeroespacial. As comunicações de voz e dados, sistemas de Comando e Controle e Apoio à Decisão, sistemas de segurança da informação, sistemas de inteligência e integração de dados, sistemas de vigilância, sistemas IFF (*Identification Friend or Foe*) e sistemas satelitais estarão vulneráveis a ataques de um computador quântico. Ao fazer com que a criptografia atual se torne obsoleta, deter a tecnologia de um computador quântico provê uma grande vantagem estratégica. Muitos comparam essa situação com o fato dos Aliados terem quebrado os códigos Enigma alemães e os códigos navais japoneses durante a Segunda Guerra Mundial (MERMIN, 2006).

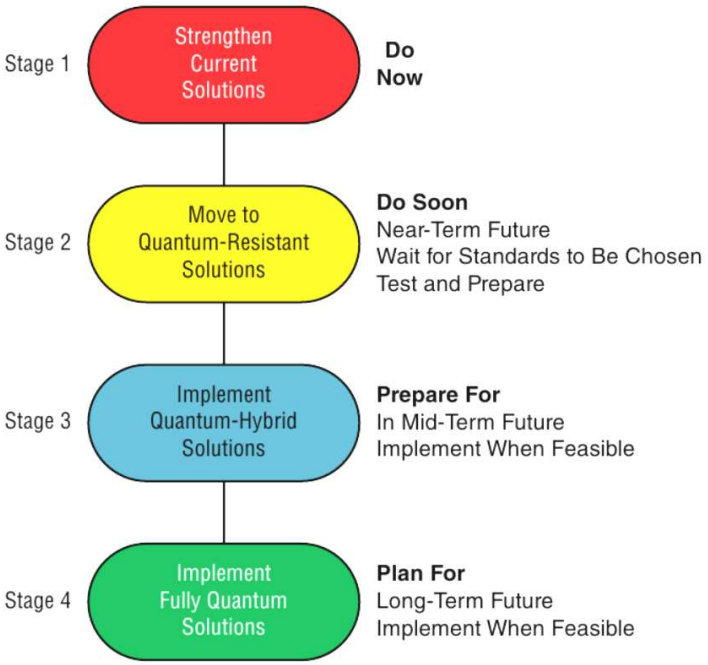
Existe hoje uma verdadeira corrida para o desenvolvimento de um computador quântico funcional em busca dessa vantagem. As máquinas que foram construídas até agora são grandes, com pouca capacidade computacional e não confiáveis (BERNHARDT, 2019). Porém, os investimentos na área são crescentes em todo o mundo, principalmente nos EUA e na China. A China atualmente é líder na pesquisa e desenvolvimento dessa tecnologia. Ela possui um satélite quântico em órbita, realizando comunicações quânticas em longas distâncias e, iniciou o projeto de um laboratório de ciências da informação quântica com investimento estimado em 10 bilhões de dólares (QUANTUM, 2019). Os Estados Unidos realizam grandes investimentos por parte de universidades e da Defesa americana, além de investimentos do setor privado por empresas como Google, Microsoft e Intel (QUANTUM, 2019).

Por ainda ser uma tecnologia que ainda está dando os primeiros passos no mundo, a FAB e o Brasil têm a oportunidade de investir em pesquisa e desenvolvimento de *hardware* e *software* para computação quântica, o que pode garantir ao Brasil a liderança e independência tecnológica em uma nova área estratégica. Em um mundo pós computador quântico, a FAB estará preparada para enfrentar as consequências dessa inovação tecnológica, sem depender de tecnologias estrangeiras. Diversos institutos da FAB têm potencial para realizar pesquisas nesse campo, entre eles o Instituto Tecnológico de Aeronáutica (ITA), o Instituto de Estudos Avançados (IEAv) e o Instituto de Aplicações Operacionais (IAOp).

2.2 Como a FAB pode se proteger

A Computação Quântica, e a consequente quebra da criptografia, está chegando, e em breve tornará obsoleta grande parte da criptografia de chave pública utilizada mundialmente. Ela é uma grande oportunidade, como visto acima, mas também uma grande ameaça para as comunicações e armazenamento de dados sensíveis. A FAB e a Defesa devem começar a se preparar hoje para mitigar os riscos de um eventual computador quântico inimigo. Grimes (2020) sugere que uma organização implemente um projeto de mitigação destes riscos com quatro estágios, conforme Figura 1.

Figura 1 – Estágios de um projeto de mitigação.



Fonte: Grimes (2020, p. 208).

No primeiro estágio, o “fazer agora”, Grimes (2020) indica que toda organização deve, o mais cedo possível, fortalecer e atualizar as soluções criptográficas utilizadas atualmente. As organizações devem, aonde possível, atualizar os sistemas criptográficos para soluções comprovadamente mais seguras. Como a evolução dos computadores quânticos é passo a passo, sistemas criptográficos que utilizam chaves menores serão quebrados primeiro. Com isso, faz se necessário utilizar as maiores chaves possíveis para cada aplicação. Para evitar

problemas operacionais e de performance, deve-se sempre realizar mudanças somente após rigorosos testes.

O segundo estágio, chamado de “fazer em breve” por Grimes (2020), consiste em testar, se preparar e implementar a utilização de Criptografia Resistente a ataques de um computador quântico. Criptografia resistente, também conhecida como Pós-Quântica, é uma evolução das técnicas criptográficas utilizadas atualmente, porém ainda não são imunes a ataques de um computador quântico, apenas dificultam os ataques. Bernstein *et al.* (2009) citam como exemplos a criptografia baseada em reticulados, a criptografia baseada em *hash* e a criptografia multivariada.

Como ainda não há uma padronização pelos órgãos regulatórios internacionais, as organizações ainda não podem migrar suas aplicações para esses tipos de criptografia resistente. Testes e projetos pilotos devem ser realizados pelos desenvolvedores e pesquisadores da organização, utilizando as ferramentas já disponíveis. Quando os órgãos regulatórios aprovarem os padrões oficiais deste tipo de criptografia, testes de viabilidade e performance devem ser realizados para cada aplicação. Em seguida deve-se fazer a migração gradual utilizando os padrões selecionados na fase de testes.

Grimes (2020) chama o terceiro estágio de “preparar para”, no qual a organização implementará sistemas criptográficos híbridos. Envolve a utilização de uma combinação de computação clássica e computação quântica em seus sistemas criptográficos. Por exemplo ao acrescentar nos sistemas resistentes, implantados no estágio 2, sistemas de Distribuição de Chave Quântica (QKD), no qual as chaves criptográficas quânticas são transmitidas por meios de comunicação clássicos (KABANOV *et al*., 2018). Adicionalmente pode-se também utilizar Geradores Quânticos de Números Aleatórios, que podem ser utilizados em sistemas criptográficos clássicos (STIPCEVIC, 2012).

No quarto e último estágio, chamado de “planejar para” por Grimes (2020), será implantado pela organização soluções puramente quânticas. Será a proteção definitiva contra ataques de computadores quânticos, utilizando Criptografia Quântica e Comunicação Quântica. Este tipo de sistema será imune a ataques de computadores quânticos (JONES e JAKSCH, 2012), eliminando os riscos dos sistemas resistentes implantados no segundo estágio.

O primeiro estágio deste projeto deve ser acompanhado de ampla divulgação da evolução da computação quântica e suas consequências para a criptografia. As autoridades do Comando da Aeronáutica devem ser informadas e sensibilizadas sobre o assunto, de forma a possibilitar o sucesso desse estágio. Será necessário também realizar um levantamento de dados de todos os serviços e equipamentos que utilizam criptografia, classificando sua criticidade.

Para uma efetiva implantação dos estágios 2 a 4 deste projeto de mitigação, será necessário que pesquisadores e desenvolvedores tenham conhecimento profundo do funcionamento de um computador quântico. A pesquisa e desenvolvimento de *hardware* e *software* para computação quântica é a forma ideal para adquirir este conhecimento, além de possibilitar o desenvolvimento nacional de técnicas criptográficas resistentes e da criptografia quântica.

3 CONSIDERAÇÕES FINAIS

A Computação Quântica irá tornar obsoleta a criptografia utilizada pela FAB em suas Aplicações Operacionais. Esse fato influenciará diretamente no cumprimento de sua missão associada ao Poder Aeroespacial. Um computador quântico modificará rapidamente o equilíbrio geoestratégico mundial, pois garante grande vantagem estratégica para quem possuí-lo. Para que a FAB consiga controlar, defender e integrar o país, deve-se investir em linhas de pesquisa para o desenvolvimento de modelos próprios de Computação Quântica.

Sem a pretensão de analisar o tema deste trabalho em profundidade, a proposta aqui é uma reflexão sobre o futuro da criptografia em um mundo com computadores quânticos. A criptografia de chave pública é uma peça fundamental na segurança da informação atualmente, porém a computação quântica irá mudar esse paradigma. Esse é só o cenário mais otimista, pois a computação quântica irá avançar mais e mais a cada dia, com a evolução do poder de processamento dos computadores quânticos e o desenvolvimento de novos algoritmos e técnicas. O parecer final deste trabalho é que a pesquisa e desenvolvimento da computação quântica é fundamental para o futuro da segurança da informação da FAB e terá grandes reflexos na sociedade brasileira.

REFERÊNCIAS

AKAMA, S. **Elements of Quantum Computing. History, Theories and Engineering Applications.** 1ª Edição. Londres, Springer, 2015.

BERNHARDT, C. **Quantum Computing for everyone**. 1ª Edição. Cambridge: The MIT Press, 2019.

BERNSTEIN, D. J.; BUCHMANN J.; DAHMEN E. **Post-Quantum Cryptography**. 1ª Edição. Berlin: Springer, 2009.

FEYNMAN, R. **Simulating Physics with Computers.** International Journal of Theoretical Physics, 1982.

GERJUOY, E. **Shor's Factoring Algorithm and Modern Cryptography.** An Illustration of the Capabilities Inherent in Quantum Computers. University of Pittsburgh, 2004. Disponível em: https://arxiv.org/pdf/quant-ph/0411184.pdf. Acesso em: 18 fev. 2020.

GRIMES, R. **Cryptography Apocalypse.** Preparing for the Day when Quantum Computing Breaks Today's Crypto. 1ª Edição. Hoboken: John Wyley & Sons, Inc, 2020.

JONES, J. A.; JAKSCH, D. **Quantum Information, Computation and Communication**. 1ª Edição. Cambridge: Cambridge University Press, 2012.

KABANOV, I. S.; YUNUSOV, R. R.; KUROCHKIN, Y. V.; FEDOROV, A. K. **Practical Cryptographic Strategies in the Post-Quantum Era**. AIP Conference Proceedings, 2018. Disponível em: https://arxiv.org/pdf/1703.04285.pdf. Acesso em: 24 mar. 2020.

MERMIN, D. **Breaking RSA Encryption with a Quantum Computer:** Shor's Factoring Algorithm. Cornell University, Physics p. 481-486, 2006. Disponível em: https://web.archive.org/web/20121115112940/http://people.ccmr.cornell.edu/~mermin/qcomp/chap3.pdf. Acesso em: 10 mar. 2020.

NIELSEN, M. A.; CHUANG, I. L. **Quantum Computation and Quantum Information**. 10th Anniversary Edition. Cambridge: Cambridge University Press, 2011.

QUANTUM Computing and Defense. **The MIlitary Balance 2019**, Abingdon, ed. 2019, cap. 1, p. 18-20, 2019.

STIPCEVIC, M. **Quantum random number generators and their use in cryptography**. SPIE Defense, Security and Sensing, 2012. Disponível em: https://arxiv.org/ftp/arxiv/papers/1103/1103.4381.pdf. Acesso em 24 mar. 2020.