ANÁLISE DE PROVÁVEL CENÁRIO CRIPTOGRÁFICO PÓS COMPUTAÇÃO QUÂNTICA: VIABILIDADE QUANTO À SEGURANÇA DOS ALGORITMOS ASSIMÉTRICOS

https://doi.org/10.5281/zenodo.15558187

SALGADO, Rodrigo Lopes, Especialista*

*Faculdade de Tecnologia de Praia Grande
Departamento de Análise e Desenvolvimento de Sistemas
Praça 19 de Janeiro, 144, Boqueirão, Praia Grande/SP, CEP: 11700-100
Telefone (13) 3591-1303
rodrigo@fatecpg.com.br

RESUMO

O trabalho apresenta um possível cenário que se instaurará imediatamente após o advento da construção, para utilização em ambiente produtivo, de computadores baseados na arquitetura quântica. Discute-se a segurança dos algoritmos criptográficos assimétricos, baseados na teoria dos números ou em curvas elípticas, perante o alto poder de processamento proporcionado por este novo paradigma computacional. O momento analisado compreende o intervalo de tempo que se dará após a construção, de fato, do computador quântico. Provavelmente, será realizado por alguma superpotência econômica que hoje já investe no desenvolvimento do computador quântico, com custos de pesquisa e manutenção muito elevados para os padrões de países em desenvolvimento, tornando o uso da capacidade de processamento deste computador um excelente ponto forte alavancador de oportunidades.

PALAVRAS-CHAVE: computação quântica, criptografia, segurança.

ABSTRACT

The paper presents a possible scenario that would be established immediately after the advent of construction of commercial computers based on quantum architecture. It discusses the security of the asymmetric cryptographic algorithms based on number theory and

elliptic curves, before the high processing power provided by this new computing paradigm. The analysis includes the time interval that will occur after construction of the quantum computer. It will probably be done by some economic superpower which already invests in the development of quantum computer, which has very high research and maintenance costs by the standards of developing countries, making the use of processing capacity of this computer an excellent opportunity generator.

KEY-WORDS: *quantum computer, criptography, security.*

INTRODUÇÃO

A arquitetura e organização de computadores está vivenciando um momento de iminente avanço. A computação clássica, como se conhece desde a criação dos primeiros computadores, está próxima de conhecer comercialmente a computação quântica. Neste estudo será abordada a conceitualização de computação quântica, de criptografia e criptoanálise em um nível que permita ser vislumbrado um cenário em que exista um computador quântico com capacidade real de processamento que torne completamente obsoleto os métodos de segurança baseados na fatoração de números primos muito grandes.

1 COMPUTAÇÃO QUÂNTICA

Desde os anos 1940 a computação vem sendo desenvolvida, inicialmente patrocinada pelas nações que atuavam no esforço de guerra desprendido durante a Segunda Guerra Mundial. Muitos dos paradigmas e conceitos definidos àquela época ainda estão fortemente presentes na computação atual. A própria arquitetura do computador se manteve praticamente inalterada desde John von Neumann e Alan Turing iniciaram seus estudos. Após a invenção do transistor, nenhum outro componente criou tamanha revolução na computação a ponto de alterar o que os historiadores chamam de Geração de Computador.

Segundo Stallings (2010), todo computador ainda é composto pelas mesmas unidades que compunham um computador em 1950. Ainda utilizam a mesma macrotecnologia baseada na eletrônica utilizando transistores para a realização dos cálculos binários. O que houve desde então foi a crescente onda de miniaturização destes mesmos componentes, proporcionando reduções de escalas que passaram de milimétricas para micrométricas - nos anos 1970, e finalmente nanométricas em 1993. Os computadores atuais possuem transistores fabricados e manipulados a uma escala de 22 nm. Muitos físicos e estudiosos acreditam que esta distância entre componentes está muito próxima do limite para que um elétron não salte de um transistor para outro, causando assim curtos circuitos e falhas computacionais.

Null e Lobur (2010) concordam com o posicionamento de Stallings (2010) e apresentam algumas opções de arquiteturas computacionais possíveis, porém nem um pouco economicamente viáveis em termos de custo benefícios. Uma das opções seria a computação ótica ou fotônica, onde se utiliza fótons de luz laser ao invés de elétrons para realização da lógica e armazenamento do estado binário. Em termos de desempenho, a velocidade da luz em circuitos fotônicos aproxima-se muito da velocidade da luz no vácuo além de poderem trafegar em paralelo sem que haja interferência entre os fótons, situação que merece mais cuidado com taxas de velocidade e blindagens no caso dos circuitos elétricos. Existem também computadores biológicos construídos com organismos vivos ao invés de silício inorgânico. Um exemplo clássico é o computador criado por cientistas americanos que utiliza neurônios de sanguessugas - projeto *"leech-ulator"*, como publicado por Sharma e Bhardwaj em outubro de 1999.

Por fim, tem-se a computação quântica como uma nova arquitetura. Esta baseia-se na mecânica quântica. Enquanto um elétron armazena apenas um bit, podendo estar ligado ou desligado, computadores quânticos utilizam *quantum bits (qubits)* que podem assumir diversos estados simultaneamente.

Explicar mecânica quântica é uma tarefa árdua. Entender tende a ser muito mais complexo. Os princípios mecânicos da física clássica não se aplicam à mecânica quântica, e propriedades como uma partícula estar ao mesmo tempo em vários lugares, superposicionando-se, mantendo ao mesmo tempo ambos os estados binários

(ligado e desligado) torna-se difícil de ser aceito. Mas isto ocorre na mecânica quântica.

1.1 *QUBITS*, BITS E FORÇA BRUTA

Um computador quântico com apenas três *qubits* pode armazenar, ao mesmo tempo, os estados ligado (1) e desligado (0) em cada um dos três *qubits*, gerando as oito combinações possíveis. Um computador clássico só consegue manter uma das oito combinações por vez. Portanto, só consegue executar cálculos com uma das combinações por vez, também. Já no computador quântico, é possível que os oito cálculos sejam realizados simultaneamente.

Um computador quântico com apenas 600 (seiscentos) *qubits* teria um poder de processamento impossível de ser simulado em uma arquitetura clássica.

Null e Lobur (2010) ainda apontam outra questão a favor da arquitetura quântica: ela é cerca de um bilhão de vezes mais rápida que componentes fabricados em silício e podem, teoricamente, funcionar sem consumo de energia.

Em vista do exposto, percebe-se que a arquitetura quântica é muito mais poderosa em termos de capacidade de processamento pelo fato de realizar simultaneamente cálculos com todas as combinações possíveis de variáveis (booleanas). Sendo assim, um computador quântico mostra sua superioridade quando o paralelismo quântico se torna necessário, como por exemplo testar todas as senhas de acesso possíveis de um usuário de computador, ou testar todas as combinações possíveis de chaves de criptografia utilizados por uma instituição bancária em uma transação eletrônica.

O "testar todas as combinações possíveis" tecnicamente é definido como um ataque por Força Bruta. Apesar de sucesso óbvio, testar todas as possíveis combinações não é tão simples como parece. No sistema binário (e o computador quântico também é binário) a quantidade de combinações possíveis se dá na ordem de 2^n, onde n é a quantidade de dígitos binários. Assim, numa chave criptográfica composta por apenas 3 bits, tem-se $2^3 = 8$ combinações de valores.

Sendo elas:

0 0 0
0 0 1
0 1 0
0 1 1
1 0 0
1 0 1
1 1 0
1 1 1

Hoje, algoritmos simétricos como o AES utilizam chaves de no mínimo 128 bits, ou seja, existem 2^{128} combinações possíveis de chaves para se testar ($2^{128} = 3{,}4x10^{38} = 340.282.366.920.938.463.463.374.607.431.768.211.456$). Um supercomputador consegue "testar" cerca de 1 bilhão de chaves por segundo. Supondo que exista 1 bilhão destes supercomputadores trabalhando juntos para testar estas chaves, ainda assim seria necessário $1x10^{20}$ segundos, ou pouco mais de 5 trilhões de anos, segundo Singh (2010).

2 CRIPTOGRAFIA E CRIPTOANÁLISE

Segundo Stallings (2008), o processo de reverter um texto cifrado em texto claro, sem que se conheça a chave e/ou segredo utilizado para criptografá-lo, é chamado de criptoanálise. A ciência que estuda tanto a criptografia quanto a criptoanálise é chamada de criptologia. A criptoanálise coexiste com a criptografia. Historicamente criptógrafos e criptoanalistas se alternaram quanto a quem detinha o melhor método. Desde os anos de 1970 os criptógrafos possuem deveras vantagem sobre os criptoanalistas, visto que a definição dos algoritmos criptográficos assimétricos se deu neste período e que até hoje não se publicou método matemático que reverta um texto cifrado assimetricamente para a forma clara.

Porém, o que se discute no cenário criptológico é que um computador quântico poderia por força bruta testar todas as chaves possíveis (e em tempo hábil) dando vantagem novamente aos criptoanalistas. Discute-se também o ambiente "conspiratório" que sempre permeou

o mundo criptológico. No decorrer da história muitos métodos criptográficos foram criptoanalisados e apenas décadas depois é que se tornaram públicos, gerando assim uma enorme vantagem competitiva ao detentor deste conhecimento. Superpotências sempre estiveram à frente destas descobertas e usufruíram muito desta vantagem, tanto militarmente quanto no âmbito corporativo.

Sendo assim, existindo altos investimentos na construção de um computador quântico, não é difícil conectar uma das aplicações deste computador (ou até mesmo protótipo) com a tarefa de criptoanalisar as atuais mensagens criptográficas. Neste ponto, tanto Stallings (2008) quanto Singh (2010) concordam na plausibilidade desta questão bem como na alta probabilidade disto ocorrer, ou até mesmo, já estar ocorrendo.

2.1 SEGURANÇA MATEMÁTICA

No que diz respeito às famílias de algoritmos criptográficos, Misoczki (2009) aponta a existência de dois grandes grupos. O primeiro baseado na problemática relacionada à teoria dos números, e tendo a fatoração de números inteiros em primos como principal elemento complicador matemático, como por exemplo o RSA. O segundo grupo utiliza-se dos logaritmos discretos, sendo amplamente representado pelos algoritmos de criptografia baseados em curvas elípticas, o ECDSA (*Elliptic Curve Digital Signature Algorithm*) é um exemplo.

Atente-se ao fato de que a Agência Nacional de Segurança dos Estados Unidos da América - NSA (*National Security Agency*), considerada a maior autoridade de segurança e inteligência do governo dos EUA, adota como protocolo de segurança soluções criptográficas baseada nos princípios matemáticos descritos anteriormente. Ambos os métodos apresentados são sistemas criptográficos assimétricos, onde existe um par de chaves (uma pública e outra privada) responsáveis pela cifragem e decifragem. Portanto, torna-se evidente que a problemática da fatoração de inteiros em primos e a dificuldade em se resolver o problema de um logaritmo discreto para um grupo de uma curva elíptica sobre alguns corpos finitos são, atualmente, os elementos matemáticos que garantem a segurança da informação, seja ela armazenada ou trafegando em redes de telecomunicações.

2.2 ALGORITMO DE SHOR

Em 1994, Peter Shor, professor americano de matemática aplicada do MIT (*Massachusetts Institute of Technology*), publicou um trabalho que mudou a forma de observação e aplicação da computação quântica. Ele criou um algoritmo quântico (que necessariamente depende de um computador quântico para funcionar) capaz de fatorar números inteiros: dado um número inteiro G o algoritmo descobre seus fatores primos. Esta tarefa, que até então era impraticável, torna-se viável (desde que se construa um computador quântico com certa quantidade de *qubits*).

A Tabela 1 ilustra esta situação, que segundo Costa (2008) exibe um comparativo de quebra do algoritmo criptográfico RSA através da fatoração do número inteiro *G* nos primos *p* e *q* (onde G = p.q). Foram utilizados três métodos para efeito de comparação: Força Bruta, Melhor Algoritmo Clássico e algoritmo de Shor. Neste cenário foi considerado que tanto o computador quântico quanto o clássico realizassem 10^{12} (um trilhão) operações por segundo.

Tabela 1 - Comparativo entre métodos de fatoração.

Método	Chave 128 bits	Chave 1024bits
Força Bruta	210 dias	4 x 10^{134} anos
Melhor Algoritmo Clássico	0,0006 segundos	11,3 anos
Algoritmo de Shor	0,002 segundos	0,01 segundos

Fonte: Costa (2008).

A Tabela 1, de Costa (2008), evidencia o que Misoczki e Barreto (2009) afirmam a respeito das implicâncias da construção do computador quântico quanto à segurança dos atuais algoritmos criptográficos, como o RSA, onde todos os algoritmos baseados na fatoração de inteiros primos e logaritmos discretos estão vulneráveis ao algoritmo de Shor.

2.3 COMPUTADOR QUÂNTICO NA CRIPTOANÁLISE

Alguns protótipos funcionais de computadores quânticos já foram construídos e operam com um número ainda muito reduzido de bits quânticos, na ordem de 2 a 4 qubits.

Segundo Lucero (2012) e Xu (2013) computadores quânticos tem quebrado recordes na resolução de fatoração de primos. Ainda que pequenos primos, como o número quinze, vinte e um no ano de 2012. E o número primo 143 (cento e quarenta e três) no ano de 2013.

Ainda que o número primo 143 aparente ser muito pequeno em termos de segurança criptográfica (e de fato é), o que a comunidade de cientistas quânticos destaca neste projeto é a técnica de processamento utilizada, que difere do que se tinha utilizado até então. As técnicas mais pesquisadas de computação quântica são baseadas em condensados de Bose-Einstein e, mais recentemente, em dispositivos de estado sólido, incluindo semicondutores e diamante. Porém, neste projeto utilizou-se o processo em um experimento que se dá em fase líquida, chamado "computação adiabática em fase líquida", segundo Xu (2013).

Percebe-se assim que, independentemente do mérito, tipo ou técnica de construção do computador quântico, cientistas tem construído e publicado trabalhos acerca de computadores quânticos com capacidades teóricas de serem escalonados para que possam fatorar números muito maiores. Ainda há muita dúvida se isto é possível, seja na técnica A, B ou C.

2.3.1 Computador quântico *D-WAVE TWO*™

Em maio de 2013 o diretor de engenharia da Google, Hartmut Neven, anunciou oficialmente a parceria entre Google e NASA na construção do Laboratório de Inteligência Quântica Artificial no Vale do Silício, na Califórnia. E de fato, após este anúncio foi publicada a aquisição do computador quântico chamado D-Wave™, produzido pela D-Wave Systems, uma empresa fundada em 1999 e que em 2004 começou a pesquisar a produção de computadores quânticos. A D-Wave Systems lançou comercialmente o primeiro computador quântico em 2010 (D-Wave One™) e em 2013 apresentou o D-Wave Two™, com 512 qubits (Figura 1).

Figura 1 - Computador Quântico D-WAVE TWO
Fonte: D-Wave Systems (2014)

Passado algumas semanas do anúncio feito por Neven muitas controvérsias foram levantadas por toda a comunidade cientistas quânticos, questionando se, de fato, o D-Wave é um computador quântico. A maioria dos pesquisadores não tem acesso ao sistema proprietário da D-Wave, sendo assim eles não podem sequer examinar as especificações HRUSKA (2014).

Ainda segundo Hruska, o que muito se discute quanto ao D-Wave ser classificado ou não como um computador quântico, é a postura quanto à organização e arquitetura do computador.

Em um recente estudo realizado em janeiro de 2014 por Umesh Vazirani, diretor do Berkeley Quantum Computation Center, da Universidade de Berkeley, nos Estados Unidos, aponta os problemas quanto a técnica utilizada na máquina D-WAVE. Vazirani analisou o D-WAVE One, de 108 qubits, e constatou que a utilização de uma técnica chamada "*quantum simulated annealing*". Ele criou um modelo com 99% de similaridade com o D-WAVE One e analisou sua performance. Foi constatado que não houve o rendimento de desempenho esperado na resolução de problemas de 108 bits no qual poderia haver uma

"explosão" na análise combinatória teorizada pelos sistemas quânticos. Vazirani sugere mais estudos com modelos com mais qubits. Portanto, o D-WAVE apesar de utilizar qubits, foi organizado numa arquitetura que não garante nem de perto o desempenho esperado de um computador quântico. Mas ainda assim, por se tratar de uma tecnologia muito recente, mostra-se muito promissor.

Segundo Sebastian Anthony, em 2012 a IBM também já estava com o projeto de desenvolvimento do seu computador quântico em fase bastante avançada.

Após todas estas situações fica evidente que, havendo ou não questionamentos por parte dos cientistas, há claros progressos a respeito das pesquisas e do desenvolvimento comercial do computador quântico.

Caso se analise este cenário sob um hipotético aspecto conspiratório (envolvendo gigantes do mundo privado e governos com PIBs trilhonários) é, no mínimo plausível, assumir que está próximo o dia em que o homem terá criado um computador quântico realmente capaz de processar números da ordem de 1024 bits. Muitos cientistas afirmam que em 20 ou 30 anos o processador quântico estará em operação.

A questão que se levanta então é: depois de inventado o computador quântico, o anúncio público será imediato? Ou haverá uma utilização secreta e privilegiada de tamanho poder de processamento?

3 ALGORITMOS PÓS QUÂNTICOS

Tendo em vista todas as considerações acerca da evolução na pesquisa e desenvolvimento do computador quântico, muitos matemáticos trabalham há tempos em algoritmos capazes de suportar a criptoanálise advinda de uma grande quantidade de processamento. Em 2009, Misoczki e Barreto sugeriram a utilização do Sistema Criptográfico McEliece, que utiliza-se de problemas pertinentes à teoria da codificação, mais precisamente de decodificação de mensagens com erros aleatórios. Segundo os autores, esta abordagem mostra-se segura no cenário apresentado já que até então não se conhece nenhum algoritmo, quântico ou clássico, que resolva tais problemas em tempo polinomial.

O sistema criptográfico pós-quântico McEliece utiliza um paradigma diferente dos algoritmos criptográficos atuais. Ao invés de basear-se na teoria dos números ele utiliza a teoria da codificação utilizando métodos de correções de erros, decodificação de síndromes e Códigos de Goppa. Evidentemente que não é foco deste trabalho apresentar toda a conceitualização matemática deste sistema algorítmico. O que deve-se atentar é o fato de existirem outros paradigmas criptográficos como opção, que hoje não são utilizados por questões de performance, mas que, em um cenário crítico onde a segurança dos algoritmos baseados na fatoração de números gigantes esteja ameaçada, faz-se bastante pertinente.

CONSIDERAÇÕES FINAIS

O presente trabalho ilustrou os avanços ocorridos nos últimos cinco anos quanto à pesquisa e desenvolvimento dos computadores quânticos. Apesar de ainda ser temática bastante discutida perante a comunidade de cientistas quânticos fica evidente que as discussões agora estão acerca de uma máquina ser ou não ser considerada um computador quântico. O próprio tema desta discussão já permite assumir que o assunto "computador quântico" está bastante avançado, ainda mais quando se argumenta sobre uma máquina comercial, com gigantes do mercado de tecnologia e de governo investindo alto.

Como o título do trabalho aponta, em um cenário hipotético, porém provável, constrói-se um ambiente conspiratório que garante amplo poder de processamento a poucos devido ao acesso a máquinas com gigantesco poder de processamento, tornando muitos mecanismos de seguranças atuais completamente obsoletos.

Confirma-se que neste cenário hipotético, de fato, todos os sistemas criptográficos baseados na fatoração de grandes números primos estaria comprometido. Também haveria grande prejuízo e impacto ao tornar pública a informação da existência de uma máquina que pudesse processar com capacidade exponencialmente mais do que as atuais máquinas. Todos os sistemas de segurança deveriam ser alterados em escala global.

Pesquisou-se também opções de segurança como solução para tal cenário e alguns artigos apontam uma área inteira da matemática (baseada em correção de erros) que torna inviável a tentativa de criptoanálise por força bruta mesmo em um computador quântico.

Portanto, o único cenário sem impactos e o cenário em que não existe o computador quântico com capacidade de processamento como teoriza-se. Todos os outros cenários, públicos ou secretos, implicam em severos impactos aos sistemas criptográficos amplamente utilizados no mundo nas mais diversas áreas, desde propósitos militares, diplomáticos e governamentais até os sistemas financeiros e empresariais.

REFERÊNCIAS

ANTHONY, Sebastian. ***IBM shows off quantum computing advances, says practical qubit computers are close.*** Extreme Tech. Ziff Davis, LLC. PCMag Digital Group, 2012.

BRYNER, Jeanna. ***Google and NASA Team Up to Study Artificial Intelligence.*** LiveScience, 2013.

COSTA, Carlos H. **Criptografia Quântica em Redes de Informação Crítica - Aplicação a Telecomunicações Aeronáuticas.** Universidade de São Paulo. São Paulo: Departamento de Engenharia de Computação e Sistemas Digitais, 2008.

HRUSKA, Joel. ***New benchmarks raise doubt over D-Wave's 'quantum computer,' but Google is optimistic long-term.*** Extreme Tech. Ziff Davis, LLC. PCMag Digital Group, 2014.

KLARREICH, Erica. ***Is That Quantum Computer for Real? There May Finally Be a Test.*** Quanta Magazine. Simons Foundation. New York, 2013.

LUCERO, Erik, et al. ***Computing prime factors with a Josephson phase qubit quantum processor.*** DOI: 10.1038/nphys 2385. Nature Physics 8, 2012

METZ, Cade. ***Google's Quantum Computer Proven To Be Real Thing (Almost).*** Wired Magazine. Condé Nast, 2013;

MISOCZKI, Rafael; BARRETO, Paulo S. L. M. **Criptografia Pós-Quântica com Códigos Corretores de Erros.** Universidade de São Paulo, REIC - Revista Eletrônica de Iniciação Científica, Ano IX, 2009.

NEVEN, Hartmut. ***Launching the Quantum Artificial Intelliegence Lab.*** Official Google Research Blog, 2013.

NSA - US National Security Agency. **Suite B Implementer's Guide to FIPS 186-3 (ECDSA)**, 2010. Disponível em http://www.nsa.gov. Acesso em: 20/01/2014.

NULL, Linda; LOBUR, Julia. **Princípios Básicos de Arquitetura e Organização de Computadores.** Bookman, 2010.

OLIVEIRA, Ivan S. **Física Moderna para iniciados, interessados e aficcionados.** Livraria da Física, 2005.

SHARMA, Saurabh; BHARDWAJ, Mili. **Competition Science Vision - out/1999**. Nova Déli: Mahendra Jain, 1999.

SHOR, Peter. **Algorithms for Quantum Computation: Discrete Logarithms and Factoring**. 35th Annual Symposium on Foundations of Computer. IEEE Comput. Soc. Press, 1994.

SINGH, Simon. **O Livro dos Códigos.** Record, 2010.

STALLINGS, William. **Arquitetura e Organização de Computadores** - 8ª Edição. São Paulo: Pearson Prentice Hall, 2010.

STALLINGS, William. **Criptografia e Segurança de Redes - Princípios e Práticas** - 4ª Edição. Pearson Prentice Hall, 2008.

VAZIRANI, Umesh, et al. ***How Quantum is the D-Wave Machine?*** Computer Science Division, UC Berkeley, USA. IBM T.J. Watson Research Center, Yorktown Heights, NY 10598, USA, 2014. Disponível em: http://arxiv.org/pdf/1401.7087v1.pdf. Acesso em 22/01/2014.

XU, Nanyang, et al. ***Quantum Factorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance System***, volume 108, DOI 10.1103/PhysRevLett.108.130501, Physical Review Letters, 2013.