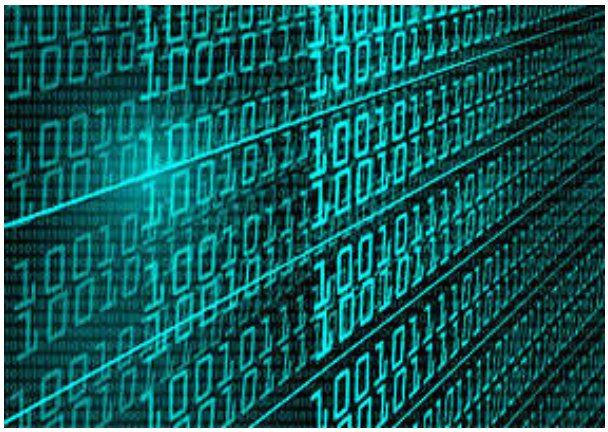
Pino Estrada: Computação quântica, qubits e a descriptografia

09/11/2022

Em outubro de 2019, segundo reportagem da *Financial Times*, o computador quântico do Google, o *Sycamore*, atingiu o estado "supremo", ou seja, o processador conseguiu calcular em 3 minutos e 20 segundos algo que o *Summit*, supercomputador mais avançado do mundo (da IBM), levaria quase 10 mil anos. O computador quântico do Google tem 53 qubits, que representam 9 bilhões de estados simultaneamente, ou seja, uma quantidade de arroz que soterraria a Torre Eiffel [1].

morgue



O que é computação quântica?
A computação quântica usa o *qubit*, que é a junção do "0 e 1" numa coisa só, diferente do "bit" do código binário (usado atualmente por todos os computadores), que usa "0 ou 1". O qubit é a unidade quântica, e cuja capacidade de processamento é muito assustadora.

A inteligência artificial (IA) em sua forma atual é inofensiva, mas isso não vai durar muito tempo. As máquinas estão ficando mais inteligentes e mais capazes a cada minuto, o que leva a preocupações de que a IA acabará se equiparando e depois excedendo os níveis humanos de inteligência uma possibilidade conhecida como superinteligência artificial (ASI na sigla em inglês).

O processador quântico chinês, batizado de *Jiuzhang*, é mais avançado que o *Sycamore* e que o *Summit*, pois executou cálculos que seriam "impossíveis" de serem realizados por um supercomputador em um tempo razoável. A equipe liderada por pesquisadores da Universidade de Ciência e Tecnologia da China também estima que seu protótipo processa 10 bilhões de vezes mais rápido do que o computador quântico de "só" 53 qubits do Google, segundo publicado na *Science*.

O *Jiuzhang* levou pouco mais de 3 minutos a completar uma tarefa que um supercomputador não conseguiria resolver em 600 milhões de anos, anunciaram cientistas chineses. A China gastou US$ 10 bilhões nos laboratórios [2]. As leis físicas da mecânica quântica permitem um método alternativo de como os computadores de hoje processam as informações. Enquanto os computadores tradicionais usam bits (0 ou 1) como um bloco de construção, os computadores quânticos empregam "bits quânticos", ou qubits, que podem ser ao mesmo tempo uma combinação de 0 e 1, como já foi dito anteriormente.

Em suma, os computadores quânticos têm uma vantagem de velocidade sobre os computadores clássicos para problemas selecionados e podem, portanto, realizar tipos de computação não disponíveis para os computadores clássicos atuais. Salienta-se que na computação quântica acontecem dois fenômenos interessantes que não acontecem na computação clássica ou binária:

a) A sobreposição, que é quando 0 e 1 se sobrepõem ou se juntam numa só unidade, que é o Qubit, que é a unidade quântica. Na computação clássica binária não existe isso, pois o bit (que é a unidade binária) só pode ser 0 ou 1, nunca os dois ao mesmo tempo como acontece na computação quântica.

b) O emaranhamento ou entrelaçamento quântico, que é quando todos os qubits utilizados para o processamento de dados trabalham juntos ao mesmo tempo, fazendo que quando são usados mais qubits o nível de processamento aumenta exponencialmente.

Isso não acontece na computação binária ou clássica usando os bits, os bits não se juntam para trabalharem juntos ao mesmo tempo. Salientando que este emaranhamento ou entrelaçamento quântico é comum e natural entre os qubits, é como se fossem irmãos gêmeos.

O que é um qubit?
Também conhecido como qubit ou simplesmente *qbit*, o bit quântico também assume valores 0 ou 1, mas ao contrário do bit comum, suas informações podem ser sobrepostas umas às outras. O bit é a menor unidade de informação que pode ser armazenada ou transmitida, usada na computação e na teoria da informação. Um bit pode assumir somente dois valores: 0 ou 1, é o famoso "dígito binário". Enquanto a base binária soma a informação de cada bit, uma sobreposição de qubits resulta na multiplicação de suas possibilidades.

Isso faz que um computador quântico processe muitas informações ao mesmo tempo e esta capacidade de processar informações ao mesmo tempo aumenta quando são usados mais qubits. Enquanto a informação total armazenadas pelos bits é igual à soma direta deles (1 + 1 + 1 + … = n), já a informação armazenada por um conjunto de qubits cresce exponencialmente (2 x 2 x 2 … = 2^n). Cada bit adiciona uma única informação ao conjunto, já um único qubit dobra a capacidade de informações do mesmo.

Para entender melhor a noção gigantesca de um qubit em comparação ao bit é importante ver a tabela a seguir:

Unidades

1 bit = 0 ou 1

1 byte = 8 *bits*

1 kilobyte (kB) = 1024 *bytes*

1 megabyte (MB) = 1024 *kilobytes*

1 gigabyte (GB) = 1024 *megabytes*

1 terabyte (TB) = 1000 gigabytes ou 1 milhão de megabytes

1 petabyte = 1000 terabytes, que são 1 milhão de gigabytes e 1 bilhão de megabytes

50 qubits = 16 petabytes

A partir de 230 qubits, está se tratando de uma quantidade equivalente a todos os átomos do universo visível. Com um computador quântico, quebrar códigos criptográficos, usados para a segurança de operações bancárias, pode deixar de ser um desafio. A nanotecnologia e a pesquisa de novos materiais também devem ser beneficiadas, assim como o setor financeiro. A computação quântica pode ser usada para a análise de carteiras de investimento e o comportamento de ações de empresas nas bolsas de valores ao longo do tempo [3].

Descriptografia quântica e a proteção de dados
Existem muitas razões pelas quais a computação quântica pode ter implicações significativas para a proteção de dados em termos de segurança de dados e confidencialidade das comunicações. Um dos motivos é a capacidade de quebrar a criptografia, ou seja, "descriptografar", pois enquanto a criptografia vira dados documentos em bits, a descriptografia é o oposto, quer dizer, virar documentos em bits em documentos legíveis.

A computação quântica pode descriptografar muitas das criptografias clássicas de hoje e, como tal, prejudicar gravemente a segurança de tecnologia da informação. O risco se estende aos principais protocolos de segurança da Internet. Quase todos os sistemas atuais que exigem segurança, privacidade ou confiança seriam afetados.

Salienta-se que a palavra "cripto" é de origem grega e significa "segredo". É interessante notar que a Criptologia atual está amparada na Matemática mas com a introdução desse conceito de mensagens criptografadas por chaves quânticas a ciência da Física passou a ter importância primordial no tema. A criptografia quântica é baseada na incerteza natural do mundo quântico. Com ela é possível criar um canal de comunicação impossível de ser monitorado sem interferir na transmissão. As leis da física dão segurança a este canal, mesmo que o observador possa fazer o que quiser, mesmo que ele tenha poder computacional infinito.

O surgimento da criptografia quântica remonta uma curiosa ideia de 1960 com um artigo não publicado de Stephen Wiesner, da Universidade de Columbia (EUA): trava-se do Dinheiro Quântico, que propunha a criação de notas monetárias a prova de fraudes. Desacreditado por ser uma ideia vanguardista para a época, levou-a em 1980 para seu amigo e pesquisador da IBM, Charles H. Bennett que mostrou interesse e juntamente com outro pesquisador Gilles

Brassard debateram as várias ideias sobre o artigo de Wiesner, percebendo que poderia haver alguma aplicação prática dentro da criptologia quântica.

A segurança da criptografia quântica se baseia na incerteza natural do mundo microscópico. Aproveitando-se deste estado de instabilidade que as partículas sofrem ao serem perturbadas no sistema de processamento quântico, seria possível a transmissão de dados de forma segura por um canal óptico denominado de meio quântico, onde esta partícula de luz (fóton) não poder ser "capturada" por uma atacante, porque um sinal interceptado (entenda-se perturbado) afetará o resultado ou representação binária do conteúdo. Esta incerteza pode ser usada para gerar uma chave secreta, pois enquanto viajam pelo meio óptico, os fótons vibram em algum sentido e direção angular, dando a conotação representativa de um bit clássico.

Assim, a ideia central da criptografia quântica trata do envio de fótons polarizados emitidos por um laser via um meio óptico e não da cifragem de texto a ser protegido. Ou seja, é o processo que trata da distribuição quântica das chaves de forma segura e inviolável, que utilizam técnicas de comunicação e princípios de física quântica para troca chaves (cadeia de qubits) entre emissor e receptor sem o prévio conhecimento do meio compartilhado, onde um interveniente possa enviar uma chave via um canal público seguramente, graças a "Incerteza Fundamental do Mundo Quântico" que mitiga ataques de interceptação (espionagem) [4].

A computação quântica também é considerada capaz de lidar com outros problemas matemáticos que os computadores clássicos não podem resolver rapidamente. No âmbito do Direito, imagine-se no âmbito da proteção de dados pessoais, sensíveis e metadados, bitcoins com as suas chaves privadas, um computador quântico poderá descriptografar facilmente informações criptografadas ou dados sigilosos criptografados.

A preocupação é tanta que a (NSA), que é a Agência de Segurança Nacional dos EUA está aconselhando as agências e empresas norte-americanas a se prepararem para um futuro não muito distante, quando a criptografia que protege praticamente todos os e-mails, registros médicos e financeiros e transações online se tornar obsoleta pela computação quântica, sendo descriptografados facilmente por algoritmos quânticos.

Os computadores quânticos têm recursos que podem arruinar todos os sistemas criptográficos de chave pública atualmente em uso. Essas capacidades, que não estão presentes nos computadores clássicos de hoje, incluem a habilidade de encontrar quase instantaneamente os fatores primos de números extremamente grandes, usando um método chamado algoritmo de Shor, que na verdade é um algoritmo quântico, que funciona em um modelo realístico de computação quântica, que utiliza as propriedades da computação quântica, como a sobreposição quântica ou entrelaçamento quântico, que é quando os qubits trabalham juntos ao mesmo tempo ao processarem os dados como já foi dito [5].

Como ficam as leis de proteção de dados?
E os segredos de Estado, dos presidentes, reis, rainhas, dados confidenciais das empresas, de cada governador de Estado, de cada parlamentar no mundo, de todas as pessoas no mundo? Se tudo isso já é possível com a computação clássica que temos atualmente, imagine-se com a computação quântica, a diferença está em que a criptografia binária não vai ser mais páreo

para a criptografia quântica no momento da proteção de dados, especificamente no momento da descriptografia.

É preciso usar formas de proteção da privacidade e intimidade que protejam as pessoas de um tipo de computação que poderá muito em breve descriptografar tudo, como já foi dito anteriormente. Em 2020 vários tribunais superiores, e autarquias federais e até o Ministério Público foram hackeados pegando dados de milhares de pessoas, fora outras entidades que tiveram os dados de milhões de brasileiros vazados justamente por falta de um sistema de proteção que consiga evitar isso.

Então, perante o citado anteriormente, é importante perguntar-se sobre como fica a Lei Geral de Proteção de Dados Brasileira (LGPD)? Como fica a Regulamentação Geral de Proteção de Dados Europeia (GDPR)? E as leis existentes no mundo a respeito de proteção de dados perante a computação e a descriptografia quântica? Até a NSA (Agência de Segurança Nacional dos EUA) e a própria NASA já demonstraram muita preocupação sobre esse assunto que já está batendo na porta.

A questão está em criar políticas de "cibersegurança nacional" para os cidadãos, a exemplo da China (com certas ressalvas), que criou uma lei a respeito disso, cujo escopo é amplo e inclui dados armazenados e tratados dentro das fronteiras chinesas, bem como informações no exterior que podem afetar a segurança nacional chinesa ou os direitos dos chineses, que é a Lei de Proteção de Informações Pessoais da China ou *Personal Information Protection Law* (PIPL), que entrou em vigor em 1º de novembro de 2021 [6].

Referências

BRASIL ESCOLA. Criptografia quântica. Disponível em: https://meuartigo.brasilescola.uol.com.br/informatica/criptografia-quantica.htm

MURGIA, Madhumita. *Google claims to have reached quantum supremacy.* Disponível em: https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17

PIVETTA, Marcos. A nova onda dos qubits. Disponível em: https://revistapesquisa.fapesp.br/a-nova-onda-dos-qubits/

SHOR, Peter W. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* Disponível em: https://arxiv.org/abs/quant-ph/9508027

ZHANG, Zhihao. Quantum computer created. https://www.chinadaily.com.cn/a/202012/05/WS5fcac383a31024ad0ba99e88.html

ZHOU Yuexin. Proteção cibernética de informações pessoais em um sistema multidimensional. Disponível em: https://cdn-conjur.s3.amazonaws.com/uploads/2022/11/ProtecCCA7aCC83o-ciberneCC81tica-de-informacCCA7oCC83es.pdf

[1] MURGIA, Madhumita. Google claims to have reached quantum supremacy. Disponível em: https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17 Acesso em 14 out. 2022.

[2]ZHANG, Zhihao. Quantum computer created. https://www.chinadaily.com.cn/a/202012/05/WS5fcac383a31024ad0ba99e88.html Acesso em 15 out. 2022.

[3] PIVETTA, Marcos. A nova onda dos qubits. Disponível em: https://revistapesquisa.fapesp.br/a-nova-onda-dos-qubits/ Acesso em 16 out. 2022.

[4] BRASIL ESCOLA. Criptografia quântica. Disponível em: https://meuartigo.brasilescola.uol.com.br/informatica/criptografia-quantica.htm Acesso em 22 out. 2022.

[5] SHOR, Peter W. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* Disponível em: https://arxiv.org/abs/quant-ph/9508027 Acesso em 18 out. 2022.

[6]ZHOU Yuexin. Proteção cibernética de informações pessoais em um sistema multidimensional. Disponível em: https://cdn-conjur.s3.amazonaws.com/uploads/2022/11/ProtecCCA7aCC83o-ciberneCC81tica-de-informacCCA7oCC83es.pdf Acesso em 28 out. 2022.