Preparado para o futuro

a jornada rumo à segurança quântica

Relatório Vanguard

abril de 2022

Encomendado por

IBM

451 Research

S&P Global
Market Intelligence

Sobre o autor

John Abbott

Analista-chefe de Pesquisa, 4SIGHT

John Abbott cobre temas relacionados a sistemas, armazenamento e infraestrutura de software para a 451 Research, parte da S&P Global Market Intelligence. Ao longo de uma carreira de mais de 30 anos, ele foi pioneiro na cobertura de tecnologia especializada em áreas como Unix, supercomputação, arquitetura de sistemas, desenvolvimento de software e armazenamento.

Um dos cofundadores da empresa The 451 Group em outubro de 1999, John dirigiu operações dos analistas na sede da empresa em São Francisco. É um dos principais autores de muitos relatórios especiais da 451 Research, incluindo aqueles sobre virtualização de armazenamento e servidores blade – as primeiras pesquisas abrangentes sobre esses assuntos a serem publicadas. Mais recentemente, John concentrou-se em temas como infraestrutura convergente, novas arquiteturas de sistemas, IA e aceleradores de deep learning. Ele ajudou a fundar a 4SIGHT, a inovadora estrutura da 451 Research dedicada às tecnologias emergentes a longo prazo.

John começou a cobrir o setor de tecnologia em 1984, com base em sua experiência anterior como autor técnico e em seu envolvimento direto utilizando mainframes, os primeiros PCs e estações de trabalho Unix. Como jornalista freelancer, ele contribuiu para publicações como *Computing*, *Computer Weekly*, *The Financial Times* e *The Times*. Em 1987, ele foi nomeado editor da Unigram.X, a newsletter semanal dedicada ao Unix da ComputerWire, e posteriormente tornou-se editor do serviço diário da Computergram International, primeiro em Londres e depois em São Francisco. Abriu o escritório da 451 Research em São Francisco e morou lá por mais de uma década.

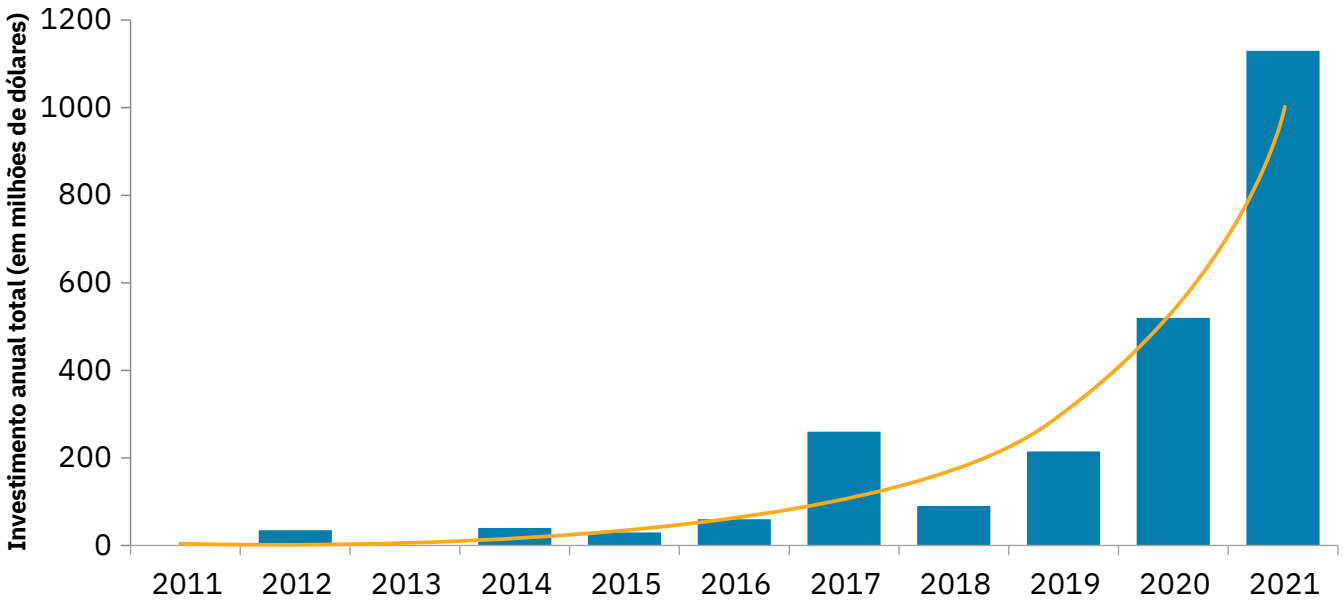
John estudou música na Universidade de Keele e tem um mestrado em literatura inglesa moderna pela Universidade de Londres.

Introdução

A melhor definição de computação quântica hoje em dia é que se trata de um investimento de alto risco e alto retorno. Não há garantias de que algum dia um computador quântico universal e prático seja viável enquanto estivermos por aqui. Mas os laboratórios de pesquisa – e, cada vez mais, as empresas privadas do setor tecnológico – estão quebrando barreiras a cada dia e inovando na vanguarda da ciência. E a recompensa poderia ser colossal, resolvendo problemas que atualmente estão além da capacidade de qualquer supercomputador (clássico). Isso explica por que tanto os vendedores quanto os usuários estão se arriscando em tecnologias potencialmente disruptivas. Os dados da S&P Capital IP Pro (Figura 1) mostram que as startups quânticas conseguiram US$ 2,4 bilhões em investimentos durante a última década. Em 2021, vimos um grande aumento de interesse, com US$ 1,1 bilhão de investimento em empresas quânticas. E esses dados não incluem os investimentos substanciais feitos por empresas de TI já estabelecidas, como IBM, Amazon, Google e Honeywell.

Junto com a oportunidade surgem algumas grandes preocupações. Talvez a mais premente seja a ameaça às práticas de segurança atuais. Armados com computação quântica, os indivíduos mal-intencionados seriam capazes de forjar assinaturas digitais e decifrar os níveis atuais de criptografia e encriptação, incluindo a infraestrutura de chave pública que agora está profundamente incorporada aos sistemas de TI em todo o mundo. E o que é ainda mais grave, mesmo os dados criptografados que estão atualmente protegidos podem ser armazenados para posterior decodificação quando a computação quântica for viável na prática. Este é um problema que não pode ser adiado. Quanto mais tempo esperarmos, maior será a quantidade de dados gerados que estarão em risco.

Figura 1: Investimento em startups de computação quântica



Fonte: S&P Capital IQ Pro

The 451 Take

Não é possível prever exatamente quando um computador quântico que possa rodar efetivamente o algoritmo de Shor se tornará acessível de tal forma que um indivíduo mal-intencionado possa ter acesso a ele. Até agora, nenhum fornecedor de TI apresentou um cronograma definido de quando a computação quântica terá um desempenho significativamente superior ao dos computadores convencionais. Mas os rápidos avanços tecnológicos nos últimos cinco anos, juntamente com os investimentos significativos agora em curso, sugerem que esse dia chegará, talvez até o final dessa década. Quando isso acontecer, todas as informações atualmente protegidas por algoritmos de chave pública serão ameaçadas de exposição. Para as agências de defesa e inteligência governamentais, e para os provedores de serviços de nuvem e fornecedores de sistemas cujos clientes estão nas indústrias regulamentadas, o risco já é muito alto para ser ignorado. Apesar dos falsos alarmes do passado (pense no Y2K, ou "bug do milênio", quando um atalho de programação de computador amplamente utilizado ameaçou causar estragos com a mudança do ano de 1999 para 2000) e das incógnitas do futuro, uma coisa é certa: o perigo dos ciberataques é um problema enorme atualmente, e a natureza das ameaças e vulnerabilidades está em constante evolução. As políticas de segurança precisam de revisão e atualização contínuas, e as tecnologias criptográficas de segurança quântica, juntamente com a implementação de agilidade criptográfica e um inventário criptográfico, são agora uma parte vital da equação.

Cenários de resistência quântica (quantum-resistant) e segurança quântica (quantum-safe)

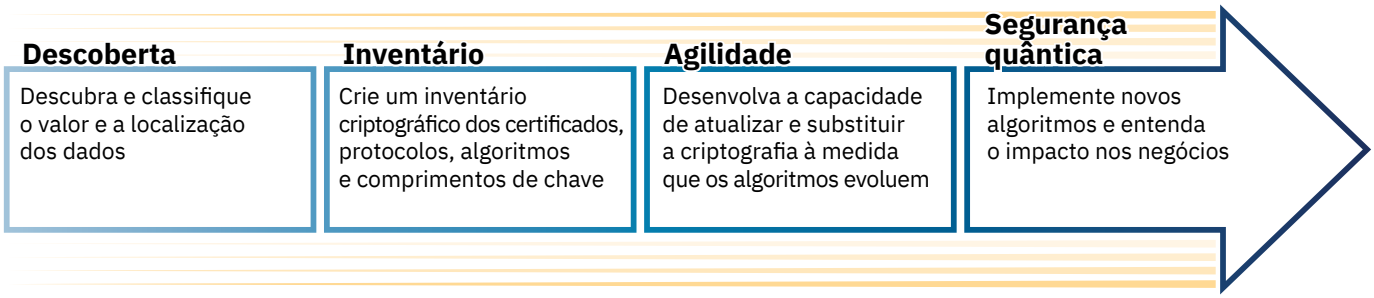
O problema é o seguinte: **a geração atual de algoritmos de segurança amplamente utilizados se baseia em complicados problemas matemáticos, difíceis demais para serem resolvidos por computadores convencionais.** Mas esses problemas poderiam ser facilmente resolvidos por um computador quântico com potência suficiente, uma premissa que tem sido amplamente aceita desde 1994, quando o matemático americano Peter Shor descobriu o algoritmo de tempo polinomial agora conhecido como algoritmo de Shor. O primeiro computador quântico foi construído três anos depois. O desenvolvimento de algoritmos com segurança quântica tem progredido bem ao longo da última década. Mas a conversão dos sistemas de criptografia de chave pública, amplamente utilizados pelo governo e pela indústria atualmente, para um novo conjunto de algoritmos pode levar décadas.

É por isso que organizações como o Instituto Nacional de Padrões e Tecnologia (NIST, National Institute of Standards and Technology) e o Departamento de Segurança Interna dos Estados Unidos têm trabalhado tanto no processo de padronização dos próprios algoritmos quanto em recomendações, para ajudar as empresas a se prepararem para a transição para a criptografia pós-quântica. Esse trabalho levou a um memorando da Casa Branca, em janeiro, determinando que os serviços de defesa e inteligência do governo começassem a fazer a transição.

Decifrar um inteiro composto de 2.048 bits (encontrando os fatores primos) nos computadores mais potentes disponíveis atualmente levaria milhões de anos. Em um computador quântico, essa tarefa poderia teoricamente ser concluída em várias horas. Os esquemas atuais de chave pública decifrados pelo algoritmo de Shor incluem o venerável algoritmo RSA – agora com 45 anos, mas ainda utilizado em quase todas as transações realizadas pela internet –, assim como o Data Security Standard, o sistema criptográfico Paillier, o algoritmo de assinatura digital de curva elíptica, a curva elíptica Diffie-Hellman e a criptografia ElGamal. Uma longa lista de normas estabelecidas pelo NIST, ISO/IEC, ETSI e IETF são afetadas, o que indica que o problema é de caráter internacional: o algoritmo de assinatura digital chinês SM2 e o padrão nacional de criptografia SM9 também foram decifrados.

O processo de normas do NIST, iniciado em 2016 com um chamado para apresentação de propostas, identificou um novo conjunto de candidatos com resistência quântica (quantum-resistant). Agrupados em uma série de abordagens – tais como a criptografia reticulada, multivariada, e baseada em hash ou em código – eles incluem o mecanismo de encapsulamento de chave (KEM) CRYSTALS-Kyber, McEliece (KEM baseado em código), e os esquemas de assinatura pós-quântica Falcon (baseado em reticulada) e Rainbow (multivariada). Estes e outros finalistas estão se preparando para o esboço da padronização após terem concluído a terceira rodada da competição. A quarta rodada, incluindo algoritmos alternativos e um chamado para esquemas de assinatura adicionais, começa este ano e será concluída até o final de 2024.

Figura 2: Marcos de maturidade rumo à segurança quântica



Fonte: 451 Research

O caminho para a criptografia de segurança quântica

Que providências as organizações devem tomar agora para se prepararem para a incorporação da criptografia de segurança quântica em suas arquiteturas de segurança da informação ao longo da próxima década? O primeiro passo, já em andamento, é participar do processo de padronização. É importante que qualquer organização interessada em prevenir a autenticação fraudulenta, proteger a integridade da criptografia e evitar o comprometimento da assinatura digital atue proativamente para garantir que seus requisitos sejam cumpridos pela lista aprovada de algoritmos, processadores e ferramentas finais. Apesar dos bons avanços dos órgãos de padronização, é uma tarefa contínua: serão necessários mais algoritmos. Além disso, os seguintes marcos de maturidade levam à segurança quântica.

- **Descoberta e classificação dos dados:** fazer um inventário dos dados críticos. Qual deles tem o maior valor? Onde estão os dados? Quais são as exigências de conformidade? Entender isso é crítico porque muitas organizações não estarão plenamente conscientes do que possuem ou de seu valor. Sem esse conhecimento, elas não podem identificar suas vulnerabilidades mais graves. Elas devem criar e gerenciar um inventário de dados com propriedade definida.
- **Inventário criptográfico:** um inventário criptográfico detalha onde e como a criptografia de chave pública está sendo usada, e contém detalhes como certificados, protocolos de criptografia, algoritmos e comprimentos de chave. O inventário deve ser gerenciado para cobrir todo o ciclo de vida dos certificados e chaves de criptografia.
- **Agilidade criptográfica**: dentro dos planos e processos de transição, as organizações precisam considerar a agilidade criptográfica para que possam fazer ajustes com menos desconforto à medida que a tecnologia evoluir e as circunstâncias mudarem. Elas devem projetar e implantar processos para que possam atualizar ou substituir a criptografia de geração atual – e depois testá-la – mais facilmente dentro de prazos de entrega bem definidos.
- **Segurança quântica**: as organizações devem implementar novos algoritmos com consciência do possível impacto no desempenho provocado pela criptografia de segurança quântica nos negócios.

Cada organização é diferente, e nem todas as organizações estarão em posição (ou terão uma mentalidade) de mudar tudo, por exemplo, devido aos custos ou aos problemas de gerenciamento do ciclo de vida. Porém, projetar prevendo a capacidade de atualizar ou substituir protocolos de segurança é crucial tanto a curto quanto a longo prazo. Por estar intimamente relacionada à infraestrutura do sistema, alcançar a agilidade criptográfica exigirá a cooperação de criadores de sistemas, desenvolvedores de aplicações e especialistas em segurança. Atualmente, há uma escassez de ferramentas disponíveis para ajudar nesse processo.

As organizações usarão uma variedade de fatores para priorizar a substituição criptográfica de segurança quântica: o valor dos ativos protegidos; a vulnerabilidade do que está sendo protegido (ou seja, armazenamento de chaves e senhas); quais sistemas conectados poderiam ser afetados (ou seja, compartilhamento de informações com entidades externas, incluindo agências federais); e por quanto tempo os dados precisam ser protegidos. Os esquemas híbridos, que combinam algoritmos clássicos e de segurança quântica, serão necessários durante o longo período de transição.

Implementação, motivação e condutores da transição

Os fornecedores de sistemas e os grandes provedores de serviços em nuvem cujos equipamentos e infraestrutura hospedam cargas de trabalho empresariais de missão crítica não podem se dar ao luxo de esperar que os padrões de criptografia de segurança quântica sejam totalmente finalizados. Eles vêm trabalhando neste problema há vários anos e têm contribuído para as opções de algoritmos e protocolos que estão entre os primeiros colocados para compor a lista final de padrões em 2024. Vários serviços de gerenciamento de chaves baseados em nuvem já têm compatibilidade com os algoritmos da segunda e terceira rodadas. Os clientes estão começando a usar esses serviços para medir os possíveis impactos no desempenho de suas aplicações a partir da provável sobrecarga adicional na utilização e latência da largura de banda, e também para mitigar as prováveis falhas de conexão nas camadas proxy de Segurança de Nível de Transporte. Mas todos concordam que a transição para a segurança quântica será uma jornada de vários anos à medida que os padrões e a tecnologia evoluírem, e que a jornada começa por garantir a infraestrutura central.

No mundo dos sistemas, os mainframes ainda são amplamente utilizados como infraestrutura central de grande disponibilidade e segurança para os maiores bancos, seguradoras, empresas de telecomunicações, de varejo e de transporte – uma posição que eles mantêm há mais de meio século. A mais nova geração de mainframes virá equipada com módulos de segurança de hardware que contarão com segurança quântica, trabalhando em conjunto com componentes atualizados do sistema operacional, APIs de gerenciamento de chaves e suporte para um conjunto de algoritmos emergentes com resistência quântica. A tecnologia de inicialização de segurança quântica com uma raiz de confiança baseada em hardware será usada para proteger a integridade do firmware de inicialização do sistema, e mecanismos de segurança quântica para a troca segura de chaves criptográficas com parceiros comerciais serão fornecidos por meio de interfaces de programação de aplicações.

Os provedores e fornecedores de serviços em nuvem devem desempenhar um papel significativo para ajudar seus clientes a fazer a transição para a criptografia de segurança quântica. Os pronunciamentos regulamentares por si só não são suficientes, em parte porque normalmente não são suficientemente prescritivos para fornecer diretrizes claras para as organizações de usuários que não tenham muita experiência própria. Os fornecedores que já estão no centro da infraestrutura de missão crítica podem facilitar o processo, fornecendo proteção ao sistema central do negócio sem mudanças adicionais no nível do sistema para habilitação. Eles também podem fornecer ferramentas de descoberta indispensáveis para a análise da aplicação criptográfica. As organizações responsáveis pelos dados precisam assegurar que eles sejam protegidos durante todo o seu ciclo de vida – hoje e no futuro – porque os dados criptografados que usam algoritmos convencionais hoje podem ser descriptografados por um computador quântico avançado no futuro. Se esses dados precisam ser protegidos por 20 anos, então estamos falando daqui até meados de 2040. Até os céticos, que acreditam que uma computação quântica viável ainda está a muitos anos de distância, devem reconhecer que, dado o ritmo do progresso atual, a probabilidade de esse momento chegar está aumentando significativamente.

Conclusões

Há muitas possibilidades de se aplicar a computação quântica nos negócios: um computador quântico totalmente desenvolvido permitiria oportunidades de avanço em química, aprendizagem de máquina, finanças, transporte, saúde e muito mais. Os computadores quânticos acelerariam exponencialmente o processamento de equações cuja execução é impraticável nos computadores clássicos e determistas usados atualmente.

Concomitantemente, está o efeito que a computação quântica poderia ter sobre a já crescente ameaça à proteção de dados e à privacidade decorrente de um ciberataque. À medida que o valor de negócio dos dados aumenta, também aumentam a escala e o custo dos requisitos de proteção de dados. E como o valor dos dados é duradouro, a crescente probabilidade de que a computação quântica se torne uma realidade praticável num futuro previsível deve ser levada em conta. Agir o quanto antes resultaria em uma evolução mais segura e controlada em direção a uma infraestrutura central de segurança quântica, à implementação de ferramentas capazes de descobrir as vulnerabilidades da camada de aplicação atuais, à proteção dos principais sistemas de intercâmbio utilizados nas organizações e à proteção contínua dos sigilos permanentes mantidos nos dados.

[1] O IBM z16 com a placa Crypto Express 8S fornece APIs de segurança quântica com acesso a algoritmos de segurança quântica que foram selecionados como finalistas durante o processo de padronização do PQC conduzido pelo NIST. https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions. A criptografia com segurança quântica refere-se aos esforços para identificar algoritmos que são resistentes a ataques tanto de computadores clássicos quanto quânticos, para manter os ativos de informação seguros mesmo após a criação de um computador quântico de grande escala. Fonte: https://www.etsi.org/technologies/quantum-safe-cryptography. Estes algoritmos são usados para ajudar a garantir a integridade de uma série de firmware e processos de inicialização.

CONTATO

Américas
+1 877 863 1306
market.intelligence@spglobal.com

Europa, Oriente Médio e África
+44 20 7176 1234
market.intelligence@spglobal.com

Ásia-Pacífico
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence