MÁY TÍNH LƯỢNG TỬ, CƠ HỘI VÀ THÁCH THỨC ĐỐI VỚI AN TOÀN AN NINH

PGS.TS Phạm Thanh Giang

Viện Công nghệ Thông tin, Viện Hàn lâm Khoa học và Công nghệ Việt Nam

Công nghệ về máy tính lượng tử được dự báo sẽ tạo ra những thay đổi có tính cách mạng với các ngành công nghiệp hiện nay; đồng thời tác động đáng kể đến xã hội trải rộng trên nhiều lĩnh vực như trí tuệ nhân tạo, khám phá thuốc, tài chính, tối ưu hóa. Tuy nhiên, sức mạnh của máy tính lượng tử cũng dẫn đến các vấn đề của mật mã học. Nhiều thuật toán mã hóa hiện nay trở nên không đảm bảo an toàn với sự xuất hiện của máy tính lượng tử. Từ đó, một loạt vấn đề của hệ thống mật mã, chữ ký số sẽ phải được định hình lại.

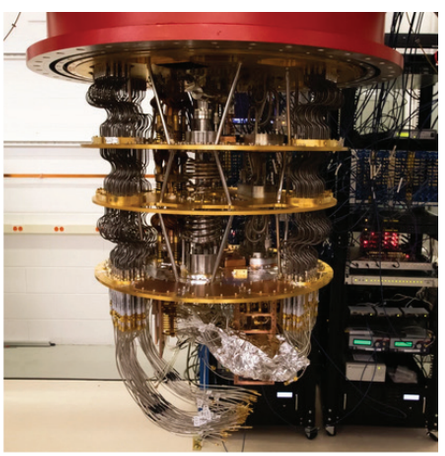
Tính chất của lượng tử

Hiện nay, lý thuyết cơ học lượng tử dẫn dắt bởi Bohr được coi là chính thống. Các nhà khoa học vẫn đang thúc đẩy nhiều nghiên cứu về lý thuyết cũng như thực nghiệm, nhằm bổ sung và đưa ra nhiều quan điểm mới về cơ học lượng tử. Dưới đây là một số đặc điểm độc đáo trong thế giới lượng tử và những "nghịch lý" mang tính triết học:

Nguyên lý siêu vị trí: Một hệ lượng tử có thể tồn tại trong nhiều trạng thái cùng một lúc. Vấn đề tính xác định của thế giới vật lý.

Nguyên lý rối lượng tử: Hai hoặc nhiều hạt lượng tử có thể trở nên rối với nhau, nghĩa là trạng thái của một hạt sẽ ảnh hưởng đến trạng thái của các hạt khác bất kể khoảng cách của chúng. Vấn đề tính nhân quả, thông tin có thể truyền nhanh hơn vận tốc ánh sáng.

IBM Q System One, máy tính lượng tử mang tính thương mại đầu tiên của IBM, 01/2019



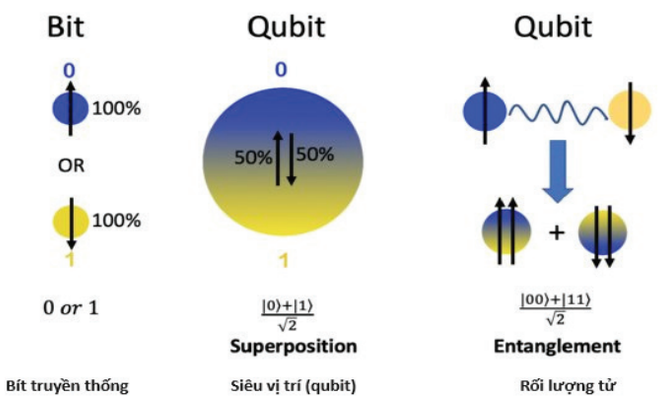
Google sycamore, máy tính lượng tử do Google sản xuất thành công năm 2019

Hai máy tính được IBM và Google giới thiệu gần đây.

Nguyên lý bất định Heisenberg: Không thể xác định đồng thời cả vị trí và động lượng của một hạt lượng tử với độ chính xác tuyệt đối. Vấn đề xác định bản chất của thực tại.

Nguyên lý đo lường: Khi đo lường một trạng thái lượng tử, nó sẽ "sụp đổ" thành một trong những trạng thái có thể quan sát được. Vấn đề tính khách quan, thực tại phụ thuộc người quan sát.

Điện toán lượng tử là lĩnh vực nghiên cứu nhằm ứng dụng công nghệ máy tính dựa trên các đặc tính và hành vi của vật chất và năng lượng ở cấp độ lượng tử. Điện toán lượng tử được khởi đầu bởi Richard Feynman vào năm 1982, tuy nhiên, việc xây dựng các máy tính lượng tử là quá phức tạp ở thời điểm đó. Đến năm 1994, Peter Shor đề xuất thuật toán lượng tử để phân tích thừa có độ phức tạp đa thức. Thuật toán này vượt trội so với thuật toán có độ phức tạp hàm mũ hoạt động trên máy tính truyền thống, do đó thúc đẩy một loạt nghiên cứu và thực nghiệm trong việc chế tạo máy tính lượng tử và xây dựng các thuật toán lượng tử khác.



So sánh bit truyền thống và qubit.

Khác với máy tính cổ điển, bit sử dụng biểu diễn dữ liệu chỉ có một trạng thái duy nhất là 0 hoặc 1, máy tính lượng tử sử dụng qubit, trong đó qubit tồn tại ở trạng thái siêu vị trí. Điều đó có nghĩa là, qubit có thể đồng thời tồn tại trong trạng thái 0 hoặc trạng thái 1, hoặc bất kỳ tổ hợp nào của hai trạng thái. Đây là cơ sở cho khả năng tính toán song song của máy tính lượng tử. Khi hai qubit trở nên rối, trạng thái của qubit này sẽ ảnh hưởng đến trạng thái của qubit kia, bất kể khoảng cách giữa chúng. Rối lượng tử là cơ sở cho việc xây dựng bộ xử lý với các cổng chuyển trạng thái lượng tử hoặc truyền thông tin lượng tử với thời gian tức thời.

Tuy vậy, sự song song của tính toán lượng tử không giống với song song của máy tính truyền thống. Mặc dù, một qubit lượng tử có thể được đặt ở vô số trạng thái chồng chất, nhưng chỉ có thể trích xuất một trạng thái thông tin duy nhất khi thực hiện phép đo. Khi tiến hành đo, trạng thái chồng chất lượng tử sẽ "sụp đổ" thành một trạng thái duy nhất. Điều đó có nghĩa là tất cả các kết quả tính toán khác sẽ bị bỏ qua. Điều này khác với mô hình tính toán song song của máy tính truyền thống, có thể cho ra toàn bộ các kết quả đầu ra. Do vậy, máy tính lượng tử chỉ thực sự hiệu quả trong các thuật toán lượng tử phù hợp.

Cơ hội và thách thức với an toàn an ninh

Những tiến bộ trong công nghệ lượng tử có khả năng định hình lại các ngành công nghệ do khả năng tăng năng lực tính toán theo cấp số nhân với việc tăng tuyến tính kích thước hệ thống lượng tử. Máy tính lượng tử hứa hẹn cung cấp năng lực tính toán gấp hàng tỷ lần các siêu máy tính hiện nay. Nhờ đó, có thể giúp chúng ta có công cụ mạnh mẽ để giải quyết nhiều bài toán lớn như trí tuệ nhân tạo, dự báo thời tiết, các bài toán sinh học, vật liệu mới.

Cơ hội

Điện toán lượng tử: Cơ hội đầu tiên là máy tính lượng tử có thể vượt trội hơn các siêu máy tính cổ điển tiên tiến nhất trong việc giải quyết một vấn đề cụ thể. Điện toán lượng tử sẵn sàng đẩy nhanh những khám phá và đổi mới khoa học trong các lĩnh vực như khoa học vật liệu, khám phá thuốc và mô hình khí hậu.

Học máy lượng tử: Điện toán lượng tử và trí tuệ nhân tạo cổ điển có thể hợp nhất để tạo ra các thuật toán học máy nâng cao lượng tử. Học máy lượng tử tận dụng tính song song và vướng víu lượng tử để xử lý và phân tích các tập dữ liệu phức tạp hiệu quả hơn. Các thuật toán lượng tử, chẳng hạn như Máy vectơ hỗ trợ lượng tử (QSVM) và Mạng thần kinh lượng tử (QNN), mang lại những lợi thế tiềm năng cho các nhiệm vụ như phân cụm dữ liệu, nhận dạng mẫu và tối ưu hóa. Học máy lượng tử hứa hẹn sẽ mở ra những hiểu biết sâu sắc từ dữ liệu lớn và thúc đẩy các ứng dụng trí tuệ nhân tạo trong nhiều lĩnh vực khác nhau.

Tối ưu hóa tài chính và đầu tư: Điện toán lượng tử có khả năng trong việc giải quyết các vấn đề tối ưu hóa phức tạp một cách hiệu quả. Điều này rất có ý nghĩa đối với việc quản lý chuỗi cung ứng, hậu cần và phân bổ nguồn lực. Điện toán lượng tử còn có thể biến đổi thế

giới tài chính bằng cách cung cấp các giải pháp nhanh hơn và chính xác hơn cho việc tối ưu hóa danh mục đầu tư và các mô hình tài chính phức tạp. Các thuật toán lượng tử, như ước tính biên độ lượng tử (Quantum Amplitude Estimation - QAE) và ước tính giá trị số ít lượng tử (Quantum Singular Value Estimation - QSVE), có thể được áp dụng cho các nhiệm vụ như phân tích rủi ro, định giá quyền chọn.

Thách thức

Tuy có nhiều ưu thế, nhưng hiện tại vẫn còn rất nhiều thách thức để máy tính lượng tử có thể thực sự được triển khai trong các bài toán thực tế.

Lỗi lượng tử: Máy tính lượng tử rất nhạy cảm với nhiệt độ, nhiễu và tương tác môi trường. Máy tính cổ điển dễ bị đảo bit (trạng thái 0 có thể trở thành 1 và ngược lại). Qubit không những bị đảo bit, mà còn có khả năng bị lỗi pha. Việc kiểm tra tại các khâu trung gian là rất khó khăn vì sẽ làm cho giá trị lượng tử bị sụp đổ hoặc bị chuyển trạng thái. Để có thể mở rộng bộ xử lý lượng tử, tăng số lượng qubit yêu cầu các kỹ thuật sửa lỗi lượng tử phức tạp. Khi số lượng qubit tăng lên, việc duy trì sự gắn kết lượng tử cũng đòi hỏi các kỹ thuật phức tạp. Để giữ được sự kết hợp lâu dài, các qubit không chỉ cần được cách ly mà còn phải được giữ ở gần nhiệt độ không tuyệt đối. Thuật toán sửa lỗi lượng tử tốt nhất hiện nay do Microsoft và Quantinuum công bố năm 2024, cho phép thu được khoảng 4 qubit tin cậy từ 30 qubit vật lý. Như vậy, chi phí về qubit sửa lỗi là rất lớn so với bit sửa lỗi truyền thống.

Kết nối lượng tử và mạng lượng tử: Kết nối các qubit trên khoảng cách xa trong khi vẫn giữ được sự vướng víu của chúng là một thách thức, yêu cầu các công nghệ, kỹ thuật phức tạp. Hiện nay, việc sử dụng kỹ thuật rối lượng tử để truyền khoảng các xa mới chỉ dừng ở mức thử nghiệm.

Thuật toán lượng tử: Để được hưởng lợi từ khả năng tính toán song song lượng tử, đòi hỏi phải có các thuật toán lượng tử phù hợp. Các thuật toán lượng tử bản chất phải hoạt động dựa trên tính xác suất. Tichy đã chỉ ra việc thử và sai để đo lường và xác minh câu trả lời đúng làm suy yếu lợi thế về tốc độ tính toán lượng tử (Tichy 2017).

Mật mã và an ninh mạng

Năng lực tính toán vượt trội của máy tính lượng tử cũng là áp lực ngược lại cho các hệ thống an toàn bảo mật hiện nay, khi độ an toàn chủ yếu dựa trên sự hạn chế năng lực tính toán của hệ thống máy tính hiện tại. Phần lớn các hệ mật mã, chữ ký số hiện nay phát triển trên nền tảng thuật toán RSA (Rivest - Shamir - Adleman) hoặc mật mã đường cong Elliptic (ECC), trong đó độ an toàn dựa trên sự phức tạp hàm mũ của bài toán phân tích thừa số nguyên tố lớn. Tuy nhiên, thuật toán lượng tử Shor cho khả năng giải bài toán phân tích thừa số với độ phức tạp đa thức. Điều đó dẫn đến máy tính lượng tử có khả năng phá vỡ các hệ thống mã hóa truyền thống, gây ra lo ngại về tính bảo mật của dữ liệu nhạy cảm. Việc đảm bảo các thuật toán mã hóa an toàn trước kỷ nguyên lượng tử là rất quan trọng đối với vấn đề an toàn thông tin liên lạc, bảo vệ thông tin cá nhân.

Ngoài ra, khi điện toán lượng tử phát triển, có nguy cơ mở rộng khoảng cách công nghệ giữa các quốc gia và tổ chức. Việc tiếp cận các công nghệ lượng tử tiên tiến và khả năng khai thác năng lực lượng tử cho các ứng dụng khác nhau có thể trở thành vấn đề có ý nghĩa kinh tế và địa chính trị.

Một số đề xuất và kiến nghị đối với Việt Nam

Lập kế hoạch chuyển đổi tiêu chuẩn mã hóa hậu lượng tử

Nguy cơ tấn công "thu thập ngay, giải mã sau" ("harvest now, decrypt later") là hiện hữu khi kỷ nguyên máy tính lượng tử đang đến gần. Ngày 21/08/2023, Cơ quan An ninh Quốc gia (NSA) và Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) đã ra thông cáo kêu gọi các tổ chức, đặc biệt là những tổ chức quản lý cơ sở hạ tầng quan trọng cần sớm lập kế hoạch cho việc chuyển đổi sang các tiêu chuẩn mật mã hậu lượng tử. Hiện nay, ở châu Âu, Trung Quốc, Singapore... đang lên kế hoạch xây dựng hạ tầng công nghệ thông tin có khả năng kháng lượng tử. Để tránh việc tin tặc thu thập dữ liệu mã hóa và giải mã trong tương lai, Việt Nam cũng cần sớm lên kế hoạch cho việc chuyển đổi và áp dụng các tiêu chuẩn mã hóa hậu lượng tử.

Khuyến khích doanh nghiệp áp dụng mã hóa hậu lượng tử

Ở Việt Nam, một số đơn vị đã áp dụng giải pháp sử dụng mật mã kháng lượng tử như Trios. Trios là hệ thống cung cấp dịch vụ mã hóa E2EE (End to End Encryption) cho các loại dữ liệu tin nhắn, file, thoại. Hệ thống được thiết kế để có thể triển khai giao thức PQXDH (Post Quantum Extended Diffie Hellman). Tương tự X25519Kyber768, giao thức PQXDH tạo ra một khóa chung dựa trên sự kết hợp của cả hai khóa đường cong elliptic X25519 và mã

hậu lượng tử được đề xuất của NIST hoặc NTRU (Nth degree truncated polynomial ring units) cho phép bảo vệ trước các cuộc tấn công của cả máy tính lượng tử và máy tính truyền thống.

Hiện nay, ở Việt Nam không nhiều cơ quan, đơn vị quan tâm đến việc tích hợp mã hóa hậu lượng tử do việc phức tạp và chưa phổ biến về công nghệ. Do đó, Việt Nam cần có chính sách khuyến khích, hỗ trợ các doanh nghiệp, đơn vị ứng dụng mã hóa hậu lượng tử trong các sản phẩm an toàn, bảo mật.

Đầu tư cho nghiên cứu về máy tính lượng tử

Nhiều quốc gia trên thế giới, các tập đoàn công nghệ đang bước vào cuộc đua để dành ưu thế trong kỷ nguyên máy tính lượng tử. Tham gia vào cuộc đua chế tạo máy tính lượng tử có lẽ là vượt quá khả năng về nguồn lực tài chính và trình độ nhân lực, nền tảng công nghệ hiện tại của Việt Nam. Tuy nhiên, chúng ta có thể tham gia vào các công đoạn trong việc hình thành và triển khai máy tính lượng tử.

Thứ nhất, nghiên cứu để giải quyết các bài toán về vật lý lượng tử. Vật lý lượng tử có cơ sở là vật lý lý thuyết với các mô hình toán học hoàn toàn phù hợp với năng lực và nguồn lực nghiên cứu của Việt Nam. Hiện có khá nhiều nhóm nghiên cứu mạnh đang tham gia lĩnh vực này.

Thứ hai, nghiên cứu về các thuật toán lượng tử. Máy tính lượng tử chỉ phát huy được sức mạnh khi có các thuật toán lượng tử phù hợp. Hiện nay, vẫn chưa có nhiều thuật toán chứng minh được khả năng vượt trội như thuật toán Shor. Con người Việt Nam với nền tảng tốt về toán học và tin học, hoàn toàn đủ khả năng tham gia nghiên cứu phát triển các thuật toán lượng tử trong tương lai.

Đào tạo nguồn nhân lực

Máy tính lượng tử đòi hỏi việc thay đổi về tư duy lập trình, kiến trúc hệ thống so với máy tính truyền thống. Hiện một số đơn vị nghiên cứu, trường đại học của Việt Nam có tổ chức một số khóa đào tạo ngắn hạn về lập trình lượng tử dựa trên nền tảng IBM quantum computing, sử dụng ngôn ngữ lập trình lượng tử Qiskit (IBM 2024) hoặc Google Cirq. Tuy các nền tảng này còn nhiều hạn chế như sai số và số lượng qubit nhỏ nhưng qua đó người học có thể hiểu về nguyên lý máy tính lượng tử và thử nghiệm các bài toán dựa trên các thuật toán lượng tử. Để Việt Nam có thể sẵn sàng nguồn nhân lực cho kỷ nguyên máy tính lượng tử, tăng khả năng trong việc nắm bắt các cơ hội và cũng như đối mặt với các thách thức khi máy tính lượng tử trở nên hiện thực, chúng ta cần xây dựng hệ thống đào tạo bài bản hơn về cả phần cứng và phần mềm lượng tử như là một môn học hay ngành học trong trường đại học.

*
* *

Điện toán lượng tử sẽ mang đến các cơ hội khám phá khoa học, quản lý tài nguyên được tối ưu hóa và xử lý dữ liệu nâng cao, đồng thời cũng đặt ra những cân nhắc về mặt đạo đức đòi hỏi phải xem xét cẩn thận và phát triển có trách nhiệm. Bên cạnh đó, điện toán lượng tử cũng mang đến những thách thức lớn về an toàn, an ninh thông tin, đặc biệt gây ảnh hưởng đến hệ thống chữ ký số quốc gia. Do đó, đòi hỏi việc nghiên cứu và chuyển dịch sang mật mã hậu lượng tử cần có sự quan tâm ở mức độ quốc gia. Khi chúng ta hướng tới một tương lai máy tính lượng tử, nỗ lực hợp tác giữa các nhà nghiên cứu, nhà hoạch định chính sách, ngành công nghiệp và công chúng là quan trọng để đảm bảo sự phát triển và sử dụng công nghệ lượng tử một cách có trách nhiệm và công bằng ✍

TÀI LIỆU THAM KHẢO

1. C.H. Bennett, G. Brassard (1984), "Quantum cryptography: Public key distribution, and coin-tossing", *1984 IEEE International Conference on Computers*, *Systems, and Signal Processing*, **560**, pp.175-179.

2. L.K. Grover (1996), "A fast quantum mechanical algorithm for database search", *STOC '96: Proceedings of The Twenty-Eighth Annual ACM Symposium on Theory of Computing,* pp.212-219, DOI: 10.1145/237814.237866.

3. S. Gill, S. Singh, A. Kumar, el al. (2022), "Quantum computing: A taxonomy, systematic review and future directions", *Software: Practice and Experience*, **52**, DOI: 10.1002/SPE.3039ISBN: 0038-0644.

4. Chrome Platform Status (2023), *Feature: X25519Kyber768 Key Encapsulation for TLS,* https://chromestatus.com/feature/5257822742249472, truy cập ngày 20/07/2024.

5. E. Kret, R. Schmidt (2024), "The PQXDH key agreement protocol", https://signal.org/docs/specifications/pqxdh/pqxdh.pdf, truy cập ngày 20/07/2024.