Họ và tên: Trần Thị Kim Thoa

Số điện thoại:0918939942

Số tài khoản: 74210000200543 ngân hàng BIDV chi nhánh sóc trăng

CÔNG NGHỆ MÁY TÍNH LƯỢNG TỬ MỘT CÔNG NGHỆ CỦA TƯƠNG LAI MỐI ĐE DỌA CHO VẤN ĐỀ BẢO MẬT HIỆN TẠI.

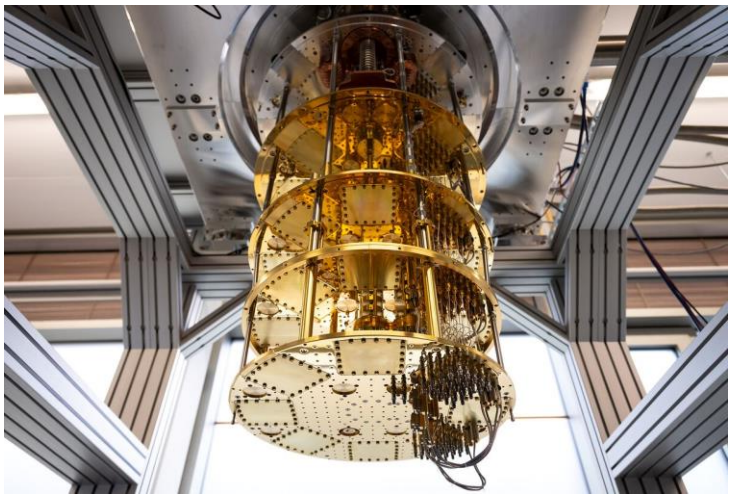
GV. Trần Thị Kim Thoa – Trường THPT Hoàng Diệu- Sóc Trăng.

Tóm tắt

Theo một báo cáo mới nhất của Công ty nghiên cứu công nghệ toàn cầu Forrester được công bố ngày 25/7/2024. Top 10 công nghệ mới nổi hàng đầu, xu hướng của tương lai mà các công ty cần phải quan tâm thì công nghệ lượng tử nằm trong xu hướng, giá trị kinh doanh mang lại lợi ích trung hạn *(Jr., 2024)*. Dự kiến trong thập kỷ tới, máy tính lượng tử sẽ được ra mắt và phá vỡ các thuật toán mật mã hiện tại. Cùng với sự trỗi dậy sắp tới của điện toán lượng tử sẽ đặt ra những tác động nghiêm trọng, đe dọa tới vấn đề an ninh mạng. Các siêu máy tính lượng tử quy mô lớn có thể xâm phạm vào các thuật toán mã hóa một cách công khai, vốn là nền tảng của nhiều biện pháp kiểm soát bảo mật phần mềm của chúng ta hiện nay và khiến chúng trở nên vô hiệu *(Andy Smith, 2024)*. Do đó, các tổ chức, công ty cũng nên có những bước tiến chủ động để chuẩn bị cho quá trình chuyển đổi mật mã hậu tương lai của công nghệ lượng tử.

1. Máy tính lượng tử là gì?

Với công nghệ hiện tại chúng ta đang sử dụng các siêu máy tính để tính toán. Về cơ bản các siêu máy tính này chính là những máy tính cổ điển, thường có hàng nhìn lõi CPU và GPU có khả năng chạy các phép tính toán rất lớn và trí tuệ nhân tạo tiên tiến.

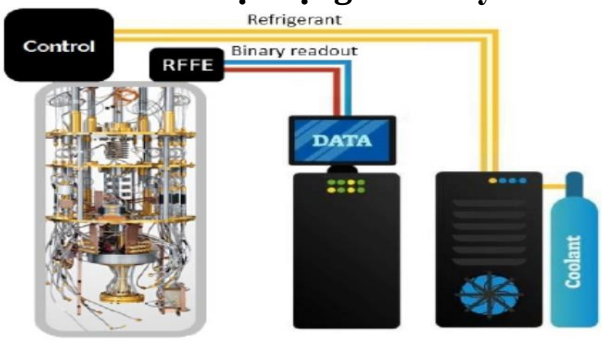


Hình 1 Một phần của máy tính lượng tử tại Trung tâm máy tính Leibniz ở Đức. Nguồn: Nhiếp ảnh gia: Sven Hoppe/picture alliance/Getty Images

Tuy nhiên, những siêu máy tính này cũng là những cổ máy tính toán dựa trên mã nhị phân, dựa trên công nghệ bóng bán dẫn, chúng thường gặp khó khăn trong việc giải quyết một số vấn đề nhất định có mức độ phức tạp cao. Máy tính lượng tử sử dụng công nghệ chuyên dụng, bao gồm: phần cứng máy tính và thuật toán tận dụng cơ học lượng tử - để giải quyết các vấn đề phức tạp mà máy tính cổ điển hoặc siêu máy tính không thể giải quyết hoặc không thể giải quyết công việc đủ nhanh. Trong máy tính lượng tử sẽ thực hiện phép tính bằng cách sử dụng trạng thái lượng tử của bit lượng tử .Với cách thực hiện này cho phép

máy tính lượng tử giải quyết một số vấn đề lớn một cách hiệu quả mà thời gian tính toán chỉ trong vài ngày, trong khi đó nếu giải quyết trên máy tính cổ điển sẽ mất thời gian hàng trăm, hàng nghìn, thậm chí hàng triệu năm.

2. Cách thức hoạt động của máy tính lượng tử.



Hình 2. Sơ đồ miêu tả cấu trúc bậc cao của máy tính lượng tử IBM

Một máy tính lượng tử thực sự được cấu thành về mặt vật lý từ ba thành phần chính, gồm: *Thành phần thứ nhất*, là một máy tính thông thường và phần cứng hỗ trợ để thực hiện lập trình và truyền lệnh đến các qubit. *Thành phần thứ hai*, là một công nghệ kỹ thuật để gửi tín hiệu từ máy tính đến các qubit. *Thành phần cuối cùng*, các qubit phải được lưu trữ ở đâu đó. Một số yêu cầu hoặc điều kiện nhất định phải được đáp ứng, và đơn vị lưu trữ qubit này phải có khả năng ổn định các qubit. Nơi lưu trữ này cần phải đảm bảo các điều kiện như: vỏ buồng chân không hoặc yêu cầu nhiệt độ gần bằng không *(Prof. Hiral B. Patel, Sejal Mishra, Rahul Jain, Prof. Nirali Kansara, 2023).*

Để hiểu được cách thức hoạt động của máy tính lượng tử, trước tiên chúng ta tìm hiểu cách thức hoạt động của máy tính cổ điển. Cách thức mà máy tính cổ điển hoạt động dự vào bit, có thể biểu diễn 1 và 0 tương tự như trạng thái công tắc (bật/tắt). So sánh máy tính lượng tử với máy tính cổ điển, máy tính cổ điển thường xử lý các lệnh khác nhau. Điện toán lượng tử đo các electron hoặc photon. Các hạt hạ nguyên tử này được gọi là bit lượng tử hoặc ***"qubit".*** Trong khi máy tính lượng tử sử dụng qubit để truyền thông tin, máy tính truyền thống sử dụng bit nhị phân. Thành phần cơ bản của điện toán lượng tử là khả năng tồn tại của qubit trong trạng thái chồng chập, thể hiện sức mạnh phân tích cực lớn. Máy tính lượng tử hoạt động bằng cách sử dụng chồng chập, giao thoa và vướng víu để thực hiện các phép tính phức tạp, để chạy các thuật toán lượng tử đa chiều *(Ray, 2011/10/01)*. Khái niệm sự chồng chập là khả năng của một hệ lượng tử có thể tồn tại ở nhiều trạng thái cùng một lúc cho đến khi được đo lường, theo đó sự chồng chập của một qubit phụ thuộc vào qubit kia. Sự kết hợp chồng chập và vướng víu ***qubit*** này cho phép máy tính lượng tử khám phá một lượng lớn các khả năng đồng thời. Để có thể hiểu rõ hơn, chúng ta cứ tưởng tượng như đang chơi một trò chơi giải bài toán tìm kiếm lối ra trong mê cung: Có thể ví rằng, một máy tính cổ điển mỗi lần thực hiện sẽ khám phá từng đường dẫn một, trong khi một máy tính lượng tử có thể khám phá tất cả các đường dẫn cùng một lúc. Điều này cho phép chúng ta tăng tốc rất nhiều để giải được bài toán tìm lối ra trong mê cung.

3. Công dụng và lợi ích của máy tính lượng tử

Máy tính lượng tử có tiềm năng và mang lại những lợi ích sau :

- Tốc độ - máy tính lượng tử cực kỳ nhanh so với máy tính cổ điển.
- Khả năng giải quyết các quy trình phức tạp. Máy tính lượng tử được thiết kế thực hiện nhiều phép tính phức tạp cùng lúc. Điều này có thể đặc biệt hữu ích cho các phép phân tích thừa số, có thể giúp phát triển các công nghệ giải mã.
- Mô phỏng - máy tính lượng tử có thể chạy các mô phỏng phức tạp so với máy tính cổ điển.
- Tối ưu hóa – với khả năng xử lý khối lượng lớn dữ liệu phức tạp của máy tính lượng tử, nó có tiềm năng chuyển đổi trí tuệ nhân tạo (AI) và máy học (ML).

4. Máy tính lượng tử tác động tới mật mã thế nào?

Hiện nay, bảo mật internet của chúng ta chủ yếu dựa vào lược đồ mã hóa RSA *(R. Rivest, A. Shamir, L. Adleman, 1978*). Cách thức bảo mật RSA sử dụng các phép tính số học phức tạp, được thực hiện bằng việc mã hóa một số lớn được tạo thành từ hai số nguyên tố lớn. Về cơ bản cách thức hoạt động của hệ mã hóa RSA gồm 3 bước: *Bước thứ nhất*, **Tạo khóa** – quá trình này sẽ tạo ra cặp khóa gồm khóa công khai (public key) và khóa bí mật (private key). *Bước thứ hai*, **Mã hóa** – để mã hóa một thông điệp, chia nó thành các khối nhỏ hơn bằng một công thức mã hóa. *Bước thứ ba*, **Giải mã** – dựa vào đoạn thông điệp mã hóa, để giải mã chúng ta phải sử dụng khóa bí mật và áp dụng công thức giải mã để cho ra kết quả là thông điệp gốc. Việc tìm ra khóa bí mật từ khóa công khai là một bài toán khó khăn, đảm bảo tính an toàn và bảo mật của hệ mã hóa RSA. Khóa RSA thường dài 1024 hoặc 2048 bit, nhưng các chuyên gia tin rằng khóa 1024 bit không còn hoàn toàn an toàn trước mọi cuộc tấn công nữa. Đây là lý do tại sao chính phủ và một số ngành công nghiệp đang chuyển sang độ dài khóa tối thiểu là 2048 bit.Với công nghệ siêu máy tính hiện tại, để hacker tìm được khóa bí mật và giải mã được hệ mã hóa RSA thì có thể mất thời gian hàng chục năm, hàng trăm năm, thậm chí hàng nghìn năm. Do đó, việc tìm ra các số nguyên tố lớn rất hữu ích để giải mã tin nhắn. Tuy nhiên, sự ra đời của máy tính lượng tử và *thuật toán **Shor** (P.W.Shor, 1999)* thì hệ mã hóa RSA không còn đảm bảo tính an toàn và bảo mật nữa. Theo một nghiên cứu, thử nghiệm của các nhà khoa học gần đây, mật mã cổ điển có thể bị lộ nếu sử dụng máy tính lượng tử, trong đó máy tính lượng tử nhanh hơn máy tính cổ điển nhiều năm tính toán *(Abushgra, 2023/07/15)*.

Trong nhiều năm, các chuyên gia an ninh mạng và các tổ chức của họ đã nhận ra rằng mối đe dọa của điện toán lượng tử là có thật và mối quan ngại này chỉ mang tính lý thuyết. Giờ đây, mối quan ngại đã được nâng lên thành việc chờ đợi những chiếc máy tính lượng tử vật lý đầu tiên. Cho đến ngày nay, vẫn chưa có tiêu chí thực sự nào để đo lường các yếu tố rủi ro khi sử dụng máy tính lượng tử. Tuy nhiên, dựa trên các thí nghiệm về thuật toán lượng tử, kỳ vọng gây ra nhiều thiệt hại là có thể xảy ra. Khi một số nền tảng công nghệ bắt đầu tỏa sáng, chẳng hạn như Học máy, Trí tuệ nhân tạo và Chuỗi khối, sức mạnh của điện toán lượng tử có thể dẫn đến lỗ hổng lớn trong hệ thống. Gần đây, ChatGPT đã thu hút được rất nhiều sự chú ý từ các cá nhân và tổ chức,

thậm chí cả chính phủ. Khả năng lập bản đồ một lượng lớn dữ liệu được thu thập liên quan đến việc thực thi thời gian chạy có thể khiến chúng ta phải kinh ngạc nếu nền tảng này chạy trên một hệ thống lượng tử.

Trong một cuộc thảo luận nhóm tại Diễn đàn kinh tế Thé giới năm 2024, các nhà lãnh đạo IBM đã cảnh báo rằng máy tính lượng tử có thể tạo ra môi trường "ngày tận thế an ninh mạng" trong những năm tới *(Isabella Ward and Brad Stone, 2024)*. Với các máy tính lượng tử quy mô lớn có khả năng trực tuyến sớm nhất là vào năm 2030, Cơ quan An ninh Quốc gia, Cơ quan An ninh Cơ sở hạ tầng và An ninh mạng NIST của Hoa Kỳ đã ban hành một khuyến cáo vào tháng 8 năm 2023 kêu gọi các tổ chức bắt đầu phát triển lộ trình sẵn sàng lượng tử, tiến hành kiểm kê, áp dụng đánh giá phân tích rủi ro và thuê các nhà cung cấp để xây dựng các hệ thống có khả năng chống lại các mối đe dọa lượng tử trong tương lai. Máy tính lượng tử sẽ có thể phá vỡ các phương pháp mã hóa thông thường với tốc độ nhanh chóng. Các công cụ mã hóa hiện đang được sử dụng để bảo vệ mọi thứ từ giao dịch ngân hàng, dữ liệu kinh doanh, tài liệu và chữ ký số có thể nhanh chóng trở nên vô hiệu. Các cuộc tấn công sử dụng phương pháp "thu hoạch ngay, giải mã sau" có thể cho phép hacker đánh cắp các tệp tin được mã hóa và lưu trữ chúng cho đến khi các máy tính lượng tử tiên tiến xuất hiện để giải mã. Vì vậy, dữ liệu có giá trị lâu dài, như: dữ liệu sức khỏe, hồ sơ tài chính, hồ sơ chính phủ, tài liệu kinh doanh của các công ty sẽ lập tức được những kẻ xấu quan tâm.

Tài liệu tham khảo

Abushgra, A. (2023/07/15). *How Quantum Computing Impacts Cyber Security.* https://doi.org/10.1109/IMSA58542.2023.10217756

Andy Smith, S. I. (2024, August 02). *https://www.techtarget.com/searchsecurity/post/How-to-prepare-for-a-secure-post-quantum-future*.

Isabella Ward and Brad Stone. (2024, January 17). *https://www.bloomberg.com/news/articles/2024-01-17/quantum-computing-to-spark-cybersecurity-armageddon-ibm-says?embedded-checkout=true*.

Jr., B. J. (2024, june 25). *https://www.technewsworld.com/story/ai-iot-quantum-security-among-top-10-emerging-technologies-forrester-179253.html*.

P.W.Shor. (1999). Polynomial-time algorithms for prime factorization and. *SIAM review, 41*, 303-332.

Prof. Hiral B. Patel, Sejal Mishra, Rahul Jain, Prof. Nirali Kansara. (2023, 11 21). The Future of Quantum Computing and its Potential Applications. *23*, 513-519.

R. Rivest, A. Shamir, L. Adleman. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM, 21*, 120-126.

Ray, I. (2011/10/01). *Quantum Computing.* https://doi.org/10.13140/2.1.1021.7286