Tổng quan về phân phối khóa lượng tử (Quantum Key Distribution)

Nguyễn Cẩm Ly

Trung tâm nghiên cứu và phát triển Toshiba, Nhật Bản

TÓM TẮT:
Phân phối khóa lượng tử (Quantum Key Distribution - QKD) được kỳ vọng là phương pháp bảo mật an toàn tuyệt đối bất chấp sự tiến bộ của khoa học máy tính bao gồm sự ra đời của máy tính lượng tử. QKD được dùng để bảo vệ dữ liệu có độ nhạy cảm và tính quan trọng cao trong nhiều ngành công nghiệp như tài chính, quốc phòng, y tế. Bài viết này trước tiên giới thiệu sơ lược về QKD cũng như tầm quan trọng của nó, và giới thiệu thành tựu chính trong nghiên cứu thực nghiệm QKD những năm gần đây. Bên cạnh đó, bài viết giới thiệu các tổ chức ở Nhật Bản cũng như trên thế giới tham gia nghiên cứu và phát triển hệ thống QKD.

Từ khóa: *Phân phối khóa lượng tử, bảo mật, dữ liệu.*

1. Giới thiệu về phân phối khóa lượng tử

Những năm gần đây, khi hệ thống công nghệ thông tin và lượng dữ liệu phát triển nhanh chóng, một trong những thách thức lớn nhất là việc bảo mật dữ liệu. Việc ngày càng có nhiều dữ liệu quan trọng được lưu trữ trong các máy chủ từ xa, chẳng hạn như trên đám mây (cloud), khiến việc làm thế nào để truy cập dữ liệu một cách an toàn trở thành mối quan tâm hàng đầu. Trong các phương pháp bảo mật truyền thống, khóa mật mã được tạo ra dựa trên khả năng khó tính toán được của một số hàm số toán học. Tuy nhiên các phương pháp bảo mật này có khả năng bị tấn công, ví dụ khi máy tính lượng tử (quantum computer) được đưa vào sử dụng. Ngược lại, phân phối khóa lượng tử (quantum key distribution, viết tắt là QKD) [1], được đề xuất vào thập kỉ 80, được chứng minh trên lý thuyết là phương pháp bảo mật an toàn tuyệt đối. Do đó, QKD được dùng để bảo vệ dữ liệu có độ nhạy cảm và tính quan trọng cao trong nhiều ngành công nghiệp như tài chính, quốc phòng, tiện ích, y tế, cơ sở hạ tầng trong thành phố thông minh…

Bản chất của QKD là dựa vào việc mã hóa từng bit của khóa bảo mật bằng một hạt ánh sáng (photon) đơn lẻ truyền qua, ví dụ, một sợi quang thông thường. Khi hai người dùng (user) ở cách xa nhau và ban đầu không chia sẻ một khóa bí mật, QKD cho phép họ tạo ra một chuỗi bí mật ngẫu nhiên chung, hay còn gọi là khóa bí mật. Thông tin được mã hóa trong trạng thái chồng chất của các hạt tải điện vật lý ở mức lượng tử đơn. QKD sử dụng các photon, tức các qubit bay nhanh nhất bằng sức mạnh nội tại của chúng để tách rời và dễ kiểm soát. Bất kỳ cách nào nhằm đọc trộm các photon đều làm xáo trộn hệ thống nên người dùng có thể phát hiện được. Do đó, QKD đảm bảo bảo mật tuyệt đối ngay cả khi toán học và điện toán có những bước nhảy vọt, bao gồm cả khả năng xử lý của máy tính lượng tử.

2. Tổng quan về sự phát triển những năm gần đây

Sau ba thập kỷ kể từ thử nghiệm QKD đầu tiên năm 1989 được tiến hành với khoảng là 32 cm [2], thế giới đã ghi nhận nhiều thành tựu

Tác giả: TS. Nguyễn Cẩm Ly

Đơn vị công tác: Trung tâm nghiên cứu và phát triển Toshiba, Nhật Bản

Email: camly268@gmail.com

Tiến sỹ Nguyễn Cẩm Ly tốt nghiệp Đại học Osaka, chuyên ngành Khoa học máy tính năm 2010. Chị lấy bằng Thạc Sỹ và bằng Tiến Sỹ Đại học Tokyo, chuyên ngành Công nghệ Thông tin lần lượt vào các năm 2012 và 2019. Từ năm 2012 đến nay, chị làm việc ở Trung tâm nghiên cứu và phát triển Toshiba (Toshiba R&D), thuộc tập đoàn Toshiba. Chuyên môn của chị bao gồm truyền thông không dây, tối ưu hóa, học máy. Chị là tác giả hoặc đồng tác giả của hơn 10 bài báo trên các tạp chí, hội nghị Quốc tế uy tín, và nộp hơn 10 bằng sáng chế.

https://doi.org/10.15625/vap.2021.0009

to lớn trong việc phát triển hệ thống QKD. Chương này tóm tắt các tiến bộ trên mặt thực nghiệm những năm gần đây cũng như các hệ thống QKD thương mại.

2.1. Sự phát triển trên mặt thực nghiệm

Năm 2004, Toshiba là công ty đầu tiên thử nghiệm thành công việc truyền QKD trên 100 km sợi quang [3]. Tiếp đó, khoảng cách đã được đẩy lên 500 km [4]. Ngoài khoảng cách xa, tốc độ truyền QKD cao rất quan trọng đối với các ứng dụng thực tế. Toshiba tiếp tục tiên phong trong việc sở hữu tốc độ truyền QKD trên 100 km là 1 Mbit/giây vào năm 2010, và 10 Mbit/giây vào năm 2017 [5].

Ngoài các thành tựu truyền QKD bằng sợi quang, truyền khóa lượng tử qua vệ tinh cũng đạt được nhiều bước tiến quan trọng. Thí nghiệm QKD vệ tinh lượng tử vào năm 2017 trên 1200 km của Trung Quốc [6] và 7600 km vào năm 2018 giữa Trung Quốc và Áo [7] được coi là bước ngoặt lớn trong những năm gần đây. Ngoài ra, thế giới ghi nhận những nỗ lực truyền khóa lượng tử thông qua vệ tinh của Châu Âu, Hoa Kỳ, Canada, Nhật Bản và Singapore [8].

2.2. Các hệ thống QKD thương mại

Hiện nay, một số công ty như tập đoàn Toshiba, ID Quantique, Quantum CTek, Qasky đã thương mại hóa các hệ thống QKD. Ví dụ Toshiba cung cấp hệ thống QKD đa kênh (multiplexed QKD system) có tốc độ 40 kbit/giây, và khoảng cách truyền tối đa là 70 km và hệ thống QKD đường dài (long distance QKD system) có tốc độ 300 kbit/giây, và khoảng cách truyền tối đa là 120 km [9].

Năm 2020, Trung Quốc đã hoàn thành tuyến đường trục cáp quang dài 2000 km giữa Bắc Kinh đến Thượng Hải [10]. Vương quốc Anh đã khởi động dự án Trung tâm Truyền thông Lượng tử nhằm mục đích xây dựng các mạng lượng tử ở Anh [11]. Hoa Kỳ đang triển khai mạng lượng tử sợi tối đầu tiên của họ kết nối Washington DC với Boston trên 800 km [12]. Ngoài ra, QKD đã được ứng dụng trong thực tế [13], như QKD được sử dụng để mã hóa thông tin liên lạc bảo mật trong cuộc bầu cử Thụy Sĩ năm 2007 và World Cup 2010. Tại Trung Quốc, QKD đang được sử dụng rộng rãi để đảm bảo an ninh lâu dài cho nhiều người dùng trong chính phủ, ngành tài chính và năng lượng [10], bao gồm Ngân hàng Nhân dân Trung Quốc, Ủy ban Điều tiết Ngân hàng Trung Quốc và Công nghiệp và Ngân hàng Thương mại Trung Quốc.

3. Các mạng lưới nghiên cứu QKD ở Nhật Bản và trên thế giới

3.1. Mạng lưới nghiên cứu ở Nhật Bản

Mạng QKD Tokyo, được khánh thành vào ngày năm 2010 [14], bao gồm sự hợp tác quốc tế giữa bốn đối tác từ Nhật Bản là các công ty NEC, Mitsubishi Electric, NTT và Viện Công nghệ Thông tin và Truyền thông Quốc gia (NICT), và ba đối tác của Châu Âu là Toshiba Research Europe Ltd. (Anh), Id Quantique (Thụy Sĩ) và All Vienna (Áo).

Có ba mục tiêu chính trong mạng lưới QKD Tokyo. Mục tiêu đầu tiên sẽ là phát triển hệ thống QKD cho các mạng IP đô thị trong phạm vi 50 km với tốc độ phát chính tối thiểu là 1 Mbit/giây. Mục tiêu thứ hai là xây dựng một hệ thống QKD vượt quá phạm vi 100 km với tốc độ tạo chính là 10 kbit/giây trở lên. Mục tiêu thứ ba là phát triển phần cứng cơ bản cho bộ lặp lượng tử.

3.2. Mạng lưới nghiên cứu trên thế giới

Mạng DARPA (DARPA quantum network) (2002–2007) [15], mạng lưới QKD đầu tiên trên thế giới, được phát triển bởi BBN Technologies, Đại học Harvard, Đại học Boston, với sự hợp tác từ IBM Research, Viện Tiêu chuẩn và Công nghệ Quốc gia, và QinetiQ. DARPA hỗ trợ một mạng máy tính Internet dựa trên tiêu chuẩn được bảo vệ bởi phân phối khóa lượng tử. DARPA phân phối khóa lượng tử chạy liên tục trong 4 năm, 24 giờ mỗi ngày, từ năm 2004 đến năm 2007 tại Massachusetts, Hoa Kỳ.

Mạng SECOQC (truyền thông an toàn dựa trên mật mã lượng tử) [16], mạng máy tính đầu tiên trên thế giới được bảo vệ bằng QKD, được triển khai vào năm 2008, tại Vienna, Áo. Mạng lưới này đã sử dụng 200 km cáp quang tiêu chuẩn để kết nối sáu địa điểm trên khắp Vienna và thị trấn St Poelten.

Mạng SwissQuantum [17] được lắp đặt tại Geneva, Thụy Sĩ vào năm 2009. Mục tiêu chính của dự là xác nhận độ tin cậy và độ bền bỉ của QKD trong môi trường thực địa. Lớp lượng tử hoạt động trong gần 2 năm cho đến khi dự án ngừng hoạt động vào năm 2011.

Mạng Trung Quốc [18] là mạng lượng tử phân cấp được kiểm chứng tại Vu Hồ, Trung Quốc vào năm 2009. Mạng phân cấp bao gồm một mạng xương sống gồm bốn nút kết nối một số mạng con. Các nút xương sống được kết nối thông qua một bộ định tuyến lượng tử chuyển mạch quang. Thí nghiệm lượng tử ở quy mô không gian (QUESS) [19] được khởi động vào năm 2016. QUESS đã tạo ra một kênh QKD quốc tế giữa Trung Quốc và Viện Quang học Lượng tử và Thông tin Lượng tử ở Vienna, Áo với khoảng cách mặt đất là 7500 km. Nó cho phép cuộc gọi video lượng tử an toàn liên lục địa đầu tiên. Năm 2017, một tuyến cáp quang dài 2000 km đã đi vào hoạt động giữa Bắc Kinh, Tế Nam, Hợp Phì và Thượng Hải. Chúng tạo thành mạng lượng tử mặt đất không gian đầu tiên trên thế giới.

4. Giới thiệu các tổ chức nghiên cứu QKD ở Nhật Bản

4.1. Trung tâm nghiên cứu và phát triển Toshiba (Toshiba R&D)

Website: https://www.toshiba.co.jp/qkd/en/index.htm

Tầm nhìn của Toshiba là phát triển hệ thống QKD để bảo vệ thông tin liên lạc của thế giới khỏi các mối đe dọa do những tiến bộ trong máy tính và toán học tạo ra. Toshiba nghiên cứu hệ thống vật lý mạng để bảo vệ thông tin cá nhân của công dân và công ty. Toshiba áp dụng các quy luật cơ bản của Vật lý lượng tử trong dịch vụ QKD để bảo mật thông tin. Cách tiếp cận của Toshiba là cung cấp cho các tổ chức khả năng cách mạng hóa cơ sở hạ tầng công nghệ thông tin của họ với các phương tiện truyền thông an toàn nhất hiện nay.

4.2. Trung tâm phát triển ứng dụng công nghệ thông tin lượng tử NICT (Quantum ICT Advanced Development Center)

Website:
https://www.nict.go.jp/en/quantum/index.html
Director: Masahiro Takeoka

Mục tiêu của NICT là cung cấp máy dò photon đơn siêu dẫn (superconducting single photon detector, SSPD) và kết hợp tất cả các công nghệ có sẵn để hiện thực hóa mạng QKD. NICT đang nghiên cứu mạch quang lượng tử để điều khiển thống nhất các biến rời rạc và liên tục, sử dụng trạng thái ép, đếm photon và đồng phân. NICT áp dụng các thành quả nghiên cứu trên cho việc xử lý thông tin lượng tử tại các nút mạng quang, để ước lượng dung lượng của các kênh quang.

Ngoài ra, NICT thúc đẩy phát triển hệ thống phân phối khóa lượng tử (QKD) và các công nghệ cơ bản liên quan, bằng cách tài trợ cho các tổ chức nghiên cứu khác.

4.3. Phòng nghiên cứu cơ bản NTT (NTT Basic Research Laboratory)

Website: http://www.brl.ntt.co.jp/e/
Director: Dr. Hideki Gotoh

NTT tham gia nghiên cứu quang học lượng tử, là lĩnh vực cơ bản của công nghệ truyền thông và thông tin lượng tử (Quantum ICT). NTT tham gia nghiên cứu cả thực nghiệm và lý thuyết liên quan đến QKD. Trong thực nghiệm, ví dụ, NTT kết hợp với đại học Stanford thực nghiệm protocol BB84 QKD sử dụng bộ phát photon đơn với một chấm lượng tử. Trong lý thuyết, ví dụ, NTT và Đại học Stanford đề xuất giao thức QKD mới rất đơn giản và có thể áp dụng được với tốc độ xung nhịp cao và có khả năng chịu đựng tốt đối với cuộc tấn công phân tách số photon.

Ngoài ra, NTT cũng đang phát triển máy dò photon đơn (single-photon detector, SPD) với nhiều cải tiến. Ví dụ, NTT đã phát triển và một hệ thống SPD chuyển đổi tần số bằng cách tăng tần số photon. Đặc biệt, NTT đã dẫn đầu trong việc tạo cặp photon vướng víu băng tần viễn thông và các ứng dụng QKD của nó.

Trong tương lai, NTT theo đuổi nghiên cứu và phát triển các bộ lặp lượng tử và kết nối các máy tính lượng tử từ xa để đạt được mạng lượng tử phát triển cao.

4.4. Các tổ chức nghiên cứu khác

Ngoài các tổ chức nghiên cứu đã giới thiệu ở trên, Nhật Bản còn có các công ty, trường đại học hoạt động sôi nổi trong nghiên cứu về QKD như NEC, Mitsubishi Electric Co Ltd, Đại học Tokyo (the University of Tokyo), Viện Tin học Quốc gia (National Institute of Informatics), Viện Vật liệu Quốc gia Khoa học (National Institute of Materials Science) và Đại học Nippon (University Nippon)

5. Kết luận

Ngày nay, khi việc bảo vệ quyền riêng tư của dữ liệu ngày càng thiết yếu, sự bảo mật tuyệt đối mà phân phối khóa lượng tử(QKD) mang lại thực sự hấp dẫn. Tuy nhiên hiện nay còn tồn tại nhiều vấn đề cần giải quyết trong nghiên cứu và phát triển hệ thống QKD, cũng như trong việc áp dụng vào trong thực tế. Ví dụ, để tạo ra một hệ thống QKD chạy ổn định trong thời gian dài với hiệu suất lớn, giữa hai người dùng cách xa nhau là một trong những thách thức lớn. Các tổ chức nghiên cứu đã và đang chung tay nỗ lực giải quyết các vấn đề tồn đọng. Bài viết này trước tiên giới thiệu sơ lược về QKD cũng như tầm quan trọng của nó, và giới thiệu thành tựu chính trong nghiên cứu thực nghiệm QKD những năm gần đây. Bên cạnh đó, bài viết giới thiệu các tổ chức ở Nhật Bản cũng như trên thế giới tham gia nghiên cứu và phát triển hệ thống QKD.

Lời cảm ơn

Bài viết này này được tài trợ bởi Tập đoàn Vingroup – Công ty CP và hỗ trợ bởi Quỹ Đổi mới sáng tạo Vingroup (VINIF) trong Dự án mã số VINIF.2020.DA09.

Tài liệu tham khảo

[1] Bennett, C. H. & Brassard, G. Quantum, “Cryptography: public key distribution and coin tossing”, *Int. Conf. on Computers, Systems & Signal Processing* 175–179 (1984).

[2] Bennett, C. H. & Brassard, G., “Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental

prototype is working!", *Sigact News* 20, 78–80 (1989).
[3] https://www.toshiba.co.jp/qkd/en/why.htm
[4] Fang, X.-T., P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, et al. (2019), arXiv:1908.01271
[5] https://www.toshiba.co.jp/about/press/2017_09/pr1501.htm
[6] Liao, Sheng-Kai, et al. "Satellite-to-ground quantum key distribution." *Nature* 549.7670 (2017): 43-47.
[7] Liao, Sheng-Kai, et al. "Satellite-relayed intercontinental quantum network." *Physical review letters* 120.3 (2018): 030501.
[8] Joshi, Siddarth Koduru, et al. "Space QUEST mission proposal: experimentally testing decoherence due to gravity." *New Journal of Physics* 20.6 (2018): 063016.
[9] https://www.toshiba.co.jp/qkd/en/products.htm
[10] Liu, L. -zheng, Zhang, Y. -zhe, Da Li, Z. -, Zhang, R., Yin, X. -fei, Fei, Y. -yang, Li, L., Le Liu, N. -, Xu, F., Chen, Y. -A. & Pan, J. -W. *Distributed quantum phase estimation with entangled photons.* Nature Photonics 4-11 (2020)
[11] https://www.quantumcommshub.net/
[12] https://techcrunch.com/2018/10/25/new-plans-aim-to-deploy-the-firstu-s-quantum-network-from-boston-to-washington-dc/
[13] Qiu, Jane. "Quantum communications leap out of the lab." *Nat.* 508.7497 (2014): 441-442.
[14] http://www.uqcc2010.org/highlights/index.html
[15] Knight, Will. "Quantum cryptography network gets wireless link". Retrieved 18 August 2016.
[16] "'Unbreakable' encryption unveiled". 9 October 2008. Retrieved 18 August 2016 – via bbc.co.uk.
[17] https://web.archive.org/web/20150228080058/http://swissquantum.idquantique.com/
[18] Xu, FangXing, et al. "Field experiment on a robust hierarchical metropolitan quantum cryptography network." *Chinese Science Bulletin* 54.17 (2009): 2991-2997.
[19] Koushik, C. S. N., et al. "A Literature Review on Quantum Experiments at Space Scale—QUESS Satellite." *Innovations in Electronics and Communication Engineering. Springer, Singapore, 2020. 13-25.*