TẠP CHÍ PHÒNG CHÁY VÀ CHỮA CHÁY ĐIỆN TỬ
JOURNAL OF FIRE ONLINE
e-ISSN: 3093-3595
Ngày nhận bài: 19/11/2025; Ngày thẩm định: 09/01/2026; Ngày nhận đăng: 19/01/2026.

ỨNG DỤNG MÁY TÍNH LƯỢNG TỬ TRONG ĐÀO TẠO CÔNG AN NHÂN DÂN CƠ HỘI ĐỔI MỚI VÀ THÁCH THỨC AN NINH MẠNG

Thượng tá, TS NGUYỄN TÀI NĂNG LƯỢNG
Khoa Khoa học cơ bản và Ngoại Ngữ, Trường Đại học PCCC
*Tác giả liên hệ: Nguyễn Tài Năng Lượng (Email: tailuong2003@gmail.com)

***Tóm tắt**: Máy tính lượng tử đang được xem là một trong những thành tựu mang tính cách mạng của khoa học, công nghệ thế kỷ XXI. Khả năng xử lý dữ liệu vượt trội của công nghệ này hứa hẹn mang lại nhiều lợi ích trong công tác đào tạo Công an nhân dân, từ mô phỏng nghiệp vụ, hỗ trợ nghiên cứu khoa học đến quản trị thông minh. Tuy nhiên, sự phát triển nhanh chóng của các thuật toán lượng tử cũng đồng nghĩa với việc các cơ chế mật mã hiện hành có nguy cơ bị phá vỡ, tạo ra mối đe dọa đặc biệt nghiêm trọng đối với an toàn thông tin. Bài viết phân tích những cơ hội nổi bật mà máy tính lượng tử mang lại, đồng thời tập trung làm rõ các giải pháp an ninh mạng nhằm bảo vệ dữ liệu đào tạo trong lực lượng Công an, nhấn mạnh vai trò của mật mã hậu lượng tử, phân loại dữ liệu nhiều lớp và đào tạo nhân lực chuyên sâu.*

***Từ khoá**: máy tính lượng tử, mật mã hậu lượng tử, an ninh mạng, đào tạo, Công an nhân dân.*

***Abstract**: Quantum computing is widely regarded as one of the most revolutionary scientific and technological achievements of the 21st century. The superior data-processing capabilities of this technology promise to bring significant benefits for the training of the People's Public Security forces, ranging from professional simulations and support for scientific research to intelligent management. However, the rapid development of quantum algorithms also implies that existing cryptographic mechanisms may be compromised, posing a particularly serious threat to information security. This article analyzes the key opportunities offered by quantum computing, while focusing on cybersecurity solutions to protect training-related data within the Public Security forces, emphasizing the role of post-quantum cryptography, multi-level data classification, and the development of highly specialized human resources.*

***Keywords**: quantum computing, post-quantum cryptography, cybersecurity, training, People's Public Security.*

1. Cuộc Cách mạng công nghiệp 4.0 thúc đẩy mạnh mẽ việc ứng dụng các công nghệ tính toán tiên tiến trong giáo dục và đào tạo chuyên ngành. Máy tính lượng tử, dựa trên các nguyên lý chồng chập và vướng víu lượng tử, có khả năng xử lý song song khối lượng trạng thái khổng lồ, mở ra tiềm năng giải quyết các bài toán tối ưu hóa, mô phỏng và học máy với tốc độ vượt trội so với máy tính cổ điển [3].

Tuy nhiên, chính sức mạnh này khiến một số thuật toán lượng tử, đặc biệt là thuật toán Shor, thuật toán có khả năng phá vỡ các hệ mật mã công khai hiện nay như RSA và ECC. Trong môi trường đào tạo Công an nhân dân, nơi quản lý lượng dữ liệu lớn liên quan đến bí mật nhà nước và an ninh quốc gia, rủi ro này trở nên đặc biệt đáng lo ngại. Vì vậy, việc đánh giá cơ hội và đề xuất giải pháp an ninh thông

tin trong bối cảnh lượng tử là nhiệm vụ quan trọng và cấp thiết [1, 6].

2. Máy tính lượng tử nếu được ứng dụng phù hợp sẽ không chỉ là công cụ tính toán cao cấp mà còn là động lực đổi mới toàn diện cho phương pháp đào tạo và năng lực nghiên cứu trong hệ thống Công an nhân dân. Ở tầng vĩ mô, định hướng phát triển đại học số và chuyển đổi số đã được Nhà nước và Bộ Công an xác định rõ, tạo hành lang chính sách để các học viện và trường triển khai thí điểm các công nghệ mới; điều này là tiền đề quan trọng để xem xét việc tích hợp những công nghệ tiên tiến như: mô phỏng lượng tử, AI tăng tốc và phân tích dữ liệu lớn vào chương trình đào tạo. Tài liệu về "Phát triển mô hình đại học số" nêu rõ việc đầu tư hạ tầng, phát triển kho học liệu số và phòng thí nghiệm ảo là ba trụ cột để chuyển đổi, do đó việc đưa ứng dụng lượng tử vào trước hết cần đặt trong khung hạ tầng đã được hoạch định sẵn.

Ở cấp độ giảng dạy và huấn luyện nghiệp vụ, công nghệ lượng tử (khi kết hợp với mô phỏng cao cấp và thực tế ảo/thực tế tăng cường) có thể tạo ra các tình huống giả lập nhiều biến số, phức tạp về tương tác vật lý và mạng, mà kỹ thuật mô phỏng cổ điển khó làm được. Điều này cho phép thiết kế bài tập tình huống sát thực tế hơn, rèn phản ứng của học viên trong môi trường có nhiều nguồn rủi ro cùng lúc - từ thao tác điều tra hiện trường đến xử lý sự cố an ninh mạng trong mạng lưới phân tán. Tài liệu về AI và dữ liệu lớn cũng đã chỉ ra rằng "phân tích dữ liệu trong đào tạo" và mô phỏng nâng cao sẽ giúp cá nhân hoá lộ trình học tập, nhận diện sớm học viên yếu kém và tối ưu hoá nội dung đào tạo; nếu bổ sung thêm mô-đun lượng tử tăng cường, chất lượng mô phỏng và độ chính xác mô hình hoá sẽ được nâng cao.

Ở góc độ nghiên cứu khoa học và ứng dụng, khả năng tính toán nhanh hơn cho các bài toán tối ưu hoá, mô phỏng vật lý - phân tử hay các mô hình học máy lớn sẽ rút ngắn chu kỳ nghiên cứu, tạo điều kiện cho các đề tài cấp ngành có bước tiến nhanh hơn. Các tài liệu nội bộ cho thấy các trường Công an đang khuyến khích nghiên cứu ứng dụng AI và Big Data (dữ liệu lớn) vào PCCC, cứu nạn và quản lý đào tạo; lượng tử có thể đóng vai trò gia tốc, nhưng cần lồng trong chương trình thí nghiệm có kiểm soát để đánh giá hiệu quả thực tế trước khi mở rộng.

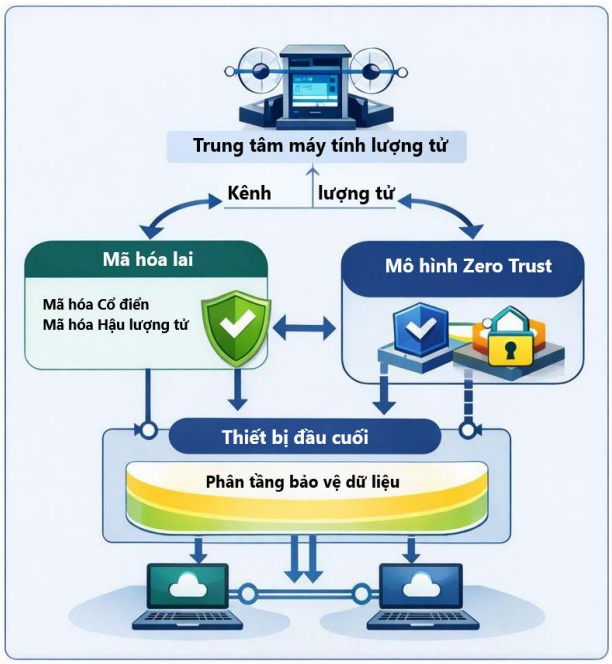
Cuối cùng, ở mảng quản trị đào tạo, máy tính lượng tử kết hợp AI có thể hỗ trợ phân tích khối hồ sơ học viên, dự báo nhu cầu nhân lực, tối ưu hoá phân tuyến lịch thực hành và tự động hoá một số quy trình quản trị. Tuy nhiên, chính đặc thù "dữ liệu phải tuyệt đối chính xác và bảo mật nghiêm ngặt" của ngành Công an được nhấn mạnh trong tài liệu nội bộ; do đó mọi lợi ích quản trị phải đi đôi với giải pháp an ninh tương ứng để tránh tạo thêm rủi ro không đáng có.

3. Trước hết, mọi giải pháp kỹ thuật phải được triển khai trong khuôn khổ quản trị dữ liệu chặt chẽ: tài sản số cần được lập bản đồ, phân loại theo mức nhạy cảm và "tuổi thọ bảo mật" rồi xác định ưu tiên bảo vệ. Điều này phù hợp hoàn toàn với khuyến nghị trong tài liệu "An ninh mạng và bảo mật thông tin trong chuyển đổi số giáo dục ngành Công an", trong đó nêu rõ phân loại dữ liệu nhiều lớp là bước nền tảng để áp dụng các biện pháp kỹ thuật và vật lý phù hợp. Việc thực hiện bước này trước khi thử nghiệm công nghệ lượng tử sẽ giúp tránh lãng phí nguồn lực và bảo vệ tốt hơn các tài liệu có giá trị chiến lược [5].

Về mặt công nghệ bảo mật, bên cạnh việc lập kế hoạch cho chuyển đổi mật mã hậu lượng tử (PQC) ở tầm vĩ mô, các trường cần bắt đầu bằng các chiến lược thực dụng: xây dựng một môi trường thử nghiệm được cách ly khỏi hệ thống chính, dùng để kiểm tra và đánh giá các thuật toán mật mã hậu lượng tử trên các luồng dữ liệu không thuộc diện ưu tiên bảo vệ cao, áp dụng chiến lược mã hóa lai (kết hợp thuật toán cổ điển và PQC) trên các tuyến truyền quan trọng, đồng thời chuẩn hoá quy trình quản lý khoá và vòng đời chứng chỉ. Về an ninh mạng nội bộ khuyến nghị tiếp cận theo lộ trình: Thí điểm → Triển khai mã hóa lai → mở rộng triển khai và nhấn mạnh tầm quan trọng của việc phối hợp với nhà cung cấp phần mềm/hạ tầng để đảm bảo khả năng tương thích [3].

Các giải pháp kiến trúc mạng và vận hành cần được củng cố ngay song song với thử nghiệm PQC. Mô hình Zero Trust nên được triển khai theo lộ trình kết hợp phân đoạn mạng, kiểm soát truy cập theo ngữ cảnh, xác thực đa yếu tố và giám sát tập trung bằng

SIEM/EDR. Hiện nay nhiều trường hiện vẫn dựa chủ yếu vào tường lửa và phần mềm chống virus; để bảo đảm an toàn trong bối cảnh nguy cơ lượng tử, cần nâng cấp lên các lớp bảo vệ hiện đại hơn, giảm phụ thuộc vào một cơ chế mã hoá đơn lẻ, và tăng cường khả năng phát hiện - phản ứng với các sự cố trong hệ thống [4].



Hình 1. Sơ đồ kiến trúc an ninh mạng lượng tử.

Sơ đồ minh họa một kiến trúc an ninh mạng trong bối cảnh ứng dụng máy tính lượng tử (hình 1), được thiết kế theo mô hình bảo vệ nhiều lớp nhằm bảo đảm an toàn dữ liệu đào tạo và quản lý. Trung tâm máy tính lượng tử đóng vai trò hạt nhân xử lý các bài toán mô phỏng và phân tích nâng cao, kết nối với hệ thống thông qua kênh lượng tử bảo mật. Dữ liệu trao đổi được bảo vệ bằng cơ chế mã hóa lai, kết hợp giữa các thuật toán mật mã cổ điển và mật mã hậu lượng tử, nhằm duy trì khả năng tương thích trong giai đoạn chuyển đổi đồng thời giảm thiểu rủi ro trước sự phát triển của năng lực tấn công lượng tử. Song song với đó, mô hình Zero Trust được áp dụng để kiểm soát chặt chẽ mọi truy cập, yêu cầu xác thực và phân quyền liên tục đối với người dùng và thiết bị. Ở tầng thiết bị đầu cuối và lưu trữ, dữ liệu được phân tầng bảo vệ theo mức độ nhạy cảm, kết hợp các biện pháp kỹ thuật và quản trị, qua đó hình thành một hệ thống phòng thủ tổng thể, bảo đảm an toàn thông tin xuyên suốt từ người dùng đến hạ tầng trung tâm.

Về lưu trữ và sao lưu dữ liệu nhạy cảm, tài liệu ngành khuyến cáo áp dụng lưu trữ tách biệt và biện pháp vật lý bổ sung cho các tập tin tối mật; những hồ sơ có "tuổi thọ bảo mật" dài nên được lưu ở hệ thống cách ly và không kết nối với hệ thống bên ngoài, kèm chính sách mã hoá mạnh (ưu tiên AES-256 cho dữ liệu cực kỳ nhạy cảm) và quản lý khoá nghiêm ngặt. Đồng thời cần cơ chế kiểm soát truy cập chặt chẽ, ghi nhật ký chi tiết và chính sách lưu trữ/làm mới khoá theo chu kỳ đã được chuẩn hoá. Những nội dung này phù hợp với khuyến nghị về phân loại dữ liệu và an toàn thông tin trong các tài liệu nội bộ.

Con người và đào tạo là lõi sống còn của mọi chuyển đổi kỹ thuật. Tài liệu "Phát triển mô hình đại học số" và báo cáo an ninh mạng đều nêu rõ cần đầu tư mạnh mẽ cho năng lực nhân lực: xây dựng chương trình đào tạo PQC cho chuyên viên công nghệ thông tin, module cơ bản về an toàn thông tin cho lãnh đạo và giảng viên, các khóa thực hành về phản ứng sự cố và diễn tập tình huống liên quan đến rủi ro "thu hoạch nay giải mã sau". Trên thực tế, khuyến nghị là kết hợp ba lớp đào tạo: lãnh đạo (chiến lược), chuyên viên (triển khai kỹ thuật) và người dùng cuối (nhận thức, quy trình xử lý dữ liệu) [2].

Về quản trị và chính sách, các đơn vị cần sớm xây dựng chính sách chuyển đổi mật mã, quy chế quản lý dữ liệu, khung kiểm thử an ninh và yêu cầu nhà cung cấp phải có lộ trình hỗ trợ PQC/Mã hóa lai. Tài liệu nội bộ nhấn mạnh rằng khung pháp lý và quy chuẩn kỹ thuật của Bộ Công an (ví dụ các quyết định quy hoạch chuyển đổi số) là nền tảng để triển khai đồng bộ; mọi kế hoạch ở trường, học viện nên tương thích với định hướng, quy chuẩn ngành để dễ dàng được phê duyệt và nhận hỗ trợ.

Về hợp tác nghiên cứu - văn bản nội bộ khuyến nghị các học viện chủ động liên kết với viện nghiên cứu, doanh nghiệp và diễn đàn quốc tế để tham gia các dự án thí điểm. Việc này vừa giúp cập nhật tiến bộ kỹ thuật (ví dụ PQC, phương pháp mô phỏng lượng tử), vừa tận dụng nguồn lực bên ngoài để giảm chi phí thử nghiệm, đồng thời tạo điều kiện cho sinh viên, học viên tham gia nghiên cứu thực tế; đây là con đường thực tế để vừa phát triển năng lực, vừa chuyển giao công nghệ an toàn.

Từ các giải pháp trên tác giả bài báo xin đề xuất lộ trình ứng dụng máy tính lượng tử trong đào tạo Công an nhân dân được đề xuất theo ba giai đoạn kế tiếp nhau, bảo đảm tính khả thi và an toàn trong triển khai. Trong giai đoạn thứ nhất, từ năm 2025 đến 2027, trọng tâm là công tác chuẩn bị và thí điểm, bao gồm nâng cao nhận thức cho đội ngũ lãnh đạo và giảng viên, xây dựng các phòng thí nghiệm mô phỏng phục vụ nghiên cứu lượng tử và an ninh mạng, đồng thời thử nghiệm các thuật toán mật mã hậu lượng tử trong môi trường thử nghiệm cách ly với các tập dữ liệu không nhạy cảm. Sang giai đoạn thứ hai, từ năm 2027 đến 2030, các ứng dụng được triển khai có kiểm soát, trong đó mã hóa lai được áp dụng cho các hệ thống đào tạo quan trọng, các mô hình mô phỏng lượng tử từng bước được tích hợp vào một số học phần nghiệp vụ và an ninh mạng, song song với việc đào tạo chuyên sâu đội ngũ cán bộ kỹ thuật về mật mã hậu lượng tử và năng lực phát hiện, phản ứng sự cố. Trên cơ sở đó, giai đoạn sau năm 2030 hướng tới mở rộng và tối ưu, với việc chuẩn hóa các giải pháp mật mã hậu lượng tử theo tiêu chuẩn ngành, tăng cường hợp tác nghiên cứu và đào tạo ở phạm vi quốc tế, đồng thời từng bước tích hợp các ứng dụng tính toán lượng tử vào hoạt động nghiên cứu khoa học và công tác quản trị đào tạo ở quy mô lớn.

4. Máy tính lượng tử vừa mở ra cơ hội nâng cao chất lượng đào tạo, vừa đặt ra thách thức to lớn về an toàn thông tin. Với môi trường đặc thù của Công an nhân dân, nơi dữ liệu đào tạo gắn liền với bí mật Nhà nước và an ninh quốc gia, việc chuẩn bị sớm các giải pháp là yêu cầu cấp thiết. Nghiên cứu và triển khai mật mã hậu lượng tử, áp dụng cơ chế phân loại dữ liệu nhiều lớp, đào tạo nhân lực chuyên sâu và tăng cường hợp tác nghiên cứu sẽ là những bước đi quan trọng nhằm bảo vệ an toàn thông tin trong kỷ nguyên lượng tử [4]. Đây cũng là cách để vừa tận dụng được cơ hội mà công nghệ mới mang lại, vừa bảo vệ vững chắc nền tảng an ninh mạng quốc gia.■

TÀI LIỆU THAM KHẢO

1. Craig Gidney, Martin Ekerå (2019), *How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits*. Quantum / arXiv.

2. Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen (2009), *Post-Quantum Cryptography*, Springer.

3. John Preskill (2018) "*Quantum computing in the NISQ era and beyond.*" Quantum.

4. Microsoft Security (2023), *Preparing for Quantum-Safe Cryptography: A Strategic Guide.*

5. NIST (2022), *Post-Quantum Cryptography Standardization Project – Finalists and Selected Algorithms*.

6. Peter W. Shor (1996), *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM Journal on Computing.