APJ 6 (4):50-56, Winter 2025

Arman Process Journal (APJ)

Arman Process Journal (APJ)

Homepage: https://www.armanprocessjournal.ir

Achievements of Quantum Computing in the Field of Information and Communication

R. Mohammadpoor [1]

[1] ***Department of Computer Engineering, Ma.C., Islamic Azad University, Mashhad , Iran***

RESEARCH PAPER

Received: 2025-9-15
Accepted: 2025-11-4

KEYWORDS:
Quantum Computing ,
Qubit ,
Cryptography,
Quantum Optimization,

ABSTRACT

Quantom computation is a new approach based on the principles of quantum mechanics to perform computations .Quantum computation uses unique behaviors of quantum physics to solve problems that are too complex for classical calculations .Theoretically , the connected inverters can use the interference between wave quantum states such as themselves for computations that may take millions of years .The potential use of these calculations is widespread and is used in areas such as cryptography , finance and drug discovery .With the implementation of quantum computing , several industries can be transformed . Although quantum computing can create a large transformation in the encryption and security system, they can be a threat to the privacy and digital information in the world .The reason for this is that quantum computers can easily break the toughest modern code .In this article, we intend to analyze and examine the new achievements of quantum computing in the field of information and communication technology, challenges and prospects.

[1] Corresponding author:
re.mohammadpoor@iau.ac.ir

نشریه تخصصی آرمان پردازش، دوره ۶، شماره ۴، سال ۱۴۰۴

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

فصلنامه تخصصی فناوری اطلاعات و ارتباطات
شماره مجوز: ۸۷۰۹۰

دستاوردهای نوین محاسبات کوانتمی در حوزه فناوری اطلاعات و ارتباطات

رضا محمدپور

گروه مهندسی برق و کامپیوتر ، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران

چکیده

مقاله پژوهشی

این نوع محاسبات یک رویکرد جدید بر اساس اصول مکانیک کوانتومی برای انجام محاسبات بنا شده است. این نوع محاسبات کوانتومی از رفتارهای منحصر به فرد فیزیک کوانتومی برای حل مسائلی استفاده می‌کند که برای محاسبات کلاسیک بسیار پیچیده هستند. از نظر تئوری، کیوبیت‌های متصل می‌توانند از تداخل بین حالت‌های کوانتومی موج مانند خود برای انجام محاسباتی استفاده کنند که ممکن است میلیون‌ها سال طول بکشد. اربردهای بالقوه این محا سبات گسترده ا ست و در زمینه‌هایی مانند: رمزنگاری، امور مالی و کشف دارو ا ستفاده می‌شود. با پیاده سازی محاسبات کوانتومی می‌توان چندین صنعت را متحول کرد. گرچه رایانش کوانتومی می‌تواند تحول بزرگی در سیستم رمزنگاری و امنیت ایجاد کند، وجود آن‌ها می‌تواند تهدیدی برای حریم خصوصی و اطلاعات دیجیتال جهان باشد. دلیل این موضوع آن است که کامپیوترهای کوانتومی به‌راحتی می‌توانند سخت‌ترین رمزهای امروزی را بشکنند. در این مقاله قصد داریم دستاوردهای نوین محاسبات کوانتمی در حوزه فناوری اطلاعات و ارتباطات و چالش ها و چشم اندازهای مرتبط را تحلیل و بررسی نمائیم.

واژگان کلیدی:
محاسبات کوانتمی،
کیوبیت،
رمزنگاری،
بهینه سازی کوانتمی،

مقدمه

در دهه‌های اخیر، فناوری اطلاعات به ستون فقرات جوامع مدرن تبدیل شده و پردازش داده‌های عظیم که پیش‌بینی می‌شود تا سال ۲۰۲۵ به ۱۸۱ زتابایت برسد و اجرای الگوریتم‌های پیچیده هوش مصنوعی را ممکن ساخته است [۱و۲]. با این حال، معماری سنتی فون‌نویمن در رایانه‌های کلاسیک با موانع فیزیکی و مفهومی اساسی مواجه شده است. کوچک‌سازی ترانزیستورها به ابعاد اتمی نزدیک شده و پدیده‌هایی نظیر تونل‌زنی کوانتومی، عملکرد پایدار آن‌ها را مختل می‌کند [۳]. از سوی دیگر، آموزش مدل‌های عظیم هوش مصنوعی با تریلیون‌ها پارامتر، نیازمند توان محاسباتی و انرژی نامتعارفی است که توسعه پایدار را با چالش مواجه می‌سازد. در این میان، محاسبات کوانتومی به عنوان یک انقلاب علمی و فناورانه ظهور کرده است. این فناوری با بهره‌گیری از اصول بنیادین مکانیک کوانتومی، به‌ویژه "برهم‌نهی و "درهم‌تنیدگی، از بیت‌های کوانتومی یا کیوبیت[1] استفاده می‌کند که برخلاف بیت‌های کلاسیک (صفر یا یک)، می‌توانند در ترکیبی خطی از هر دو حالت به طور هم‌زمان وجود داشته باشند [۴]. این ویژگی منحصربه‌فرد به رایانه‌های کوانتومی اجازه می‌دهد تا مسائل خاصی را با سرعتی نمایی بیش از قدرتمندترین ابررایانه‌های امروزی حل کنند [۵]. برای مثال، الگوریتم معروف شور[2] تهدیدی جدی برای زیرساخت‌های رمزنگاری کنونی است و الگوریتم گروور[3] می‌تواند جستجو در پایگاه‌های داده بدون ساختار را به طور چشمگیری تسریع بخشد [۶و۷].

اهمیت این فناوری برای حوزه فناوری اطلاعات از آنجا ناشی می‌شود که بسیاری از مسائل حل‌نشده در امنیت سایبری، تحلیل داده‌های کلان، بهینه‌سازی شبکه‌های پیچیده و توسعه هوش مصنوعی، ماهیتاً مسائلی با پیچیدگی محاسباتی بالا هستند که راه‌حل‌های کلاسیک برای آن‌ها ناکارآمد یا غیرممکن است [۸]. ازاین‌رو، هدف این مقاله پژوهشی-مروری، ارائه یک بررسی جامع و نظام‌مند از مبانی محاسبات کوانتومی، آخرین دستاوردهای آن در زمینه‌های کلیدی حوزه فناوری اطلاعات و نیز تحلیل چالش‌ها و ترسیم چشم‌انداز پیش روی این فناوری تحول‌آفرین است . این مطالعه به متخصصان و پژوهشگران حوزه فناوری اطلاعات کمک می‌کند تا با فرصت‌ها و تهدیدهای ناشی از ظهور عصر کوانتوم آشنا شوند.

تحقیقات مرتبط

توسعه محاسبات کوانتومی مرهون تلاش‌های نظری و عملی گسترده‌ای در چند دهه گذشته است. این بخش مروری بر مهم‌ترین تحقیقات و مقالات در زمینه مبانی، الگوریتم‌ها، کاربردها و چالش‌های این حوزه دارد. ایده اولیه استفاده از پدیده‌های کوانتومی برای پردازش اطلاعات به کارهای پیشگامانی چون پال بنیاف ، ریچارد فاینمن و دیوید دویچ در دهه ۱۹۸۰ بازمی‌گردد [۹]. فاینمن استدلال کرد که شبیه‌سازی سیستم‌های کوانتومی بر روی رایانه‌های کلاسیک به دلیل رشد نمایی فضای حالت، غیرممکن است و بنابراین، رایانه‌های کوانتومی برای غلبه بر این محدودیت ضروری هستند [۴]. در دهه ۱۹۹۰، ارائه الگوریتم‌های انقلابی شور برای تجزیه اعداد صحیح و گروور برای جستجوی پایگاه داده، قدرت بالقوه محاسبات کوانتومی را به طور عینی به نمایش گذاشت و زمینه‌ساز سرمایه‌گذاری‌های گسترده در این عرصه شد [۶و۷].

به موازات پیشرفت‌های نظری، رقابت فشرده‌ای برای پیاده‌سازی فیزیکی کیوبیت‌ها در جریان است. فناوری‌های پیشرو شامل مدارهای ابررسانا، یون‌های به دام افتاده ، کیوبیت‌های فوتونیکی و اتم‌های خنثی می‌شود [۱۰]. هر یک از این فناوری‌ها دارای مزایا و معایبی از نظر زمان همدوسی ، وفاداری گیت و پتانسیل مقیاس‌پذیری هستند. در حال حاضر، رایانه‌های کوانتومی در دوره "نویز و مقیاس متوسط به سر می‌برند؛ دستگاهی با ده‌ها تا صدها کیوبیت که به شدت تحت تأثیر نویز و خطاهای محاسباتی هستند. گزارش‌های فنی از شرکت‌هایی مانند IBMنشان‌دهنده پیشرفت مستمر در افزایش تعداد کیوبیت‌ها و بهبود کیفیت آن‌هاست، مانند پردازنده ۴۳۳ کیوبیتی [۱۱].

ادبیات پژوهشی اخیر به طور فزاینده‌ای بر کاربردهای خاص محاسبات کوانتومی در فناوری اطلاعات متمرکز شده است. مطالعه‌ای از ولفمایر و یوتپالا (۲۰۲۵) به بررسی چگونگی یکپارچه‌سازی محاسبات کوانتومی برای کاربردهای هوش مصنوعی در محیط‌های شبکه کلاسیک پرداخته و بر نیاز به ارتقای زیرساخت‌های شبکه برای پشتیبانی از الگوریتم‌های کوانتومی-هوش مصنوعی تأکید کرده است [۱۲و۱۳]. آن‌ها نشان دادند که معماری‌های شبکه امروزی باید برای تعامل با سیستم‌های کوانتومی و پردازش‌های بی‌درنگ تکامل یابند. همچنین، مقاله مروری جامعی در مجله Frontiers (2025) با بررسی پایه‌ها، الگوریتم‌ها و کاربردهای نوظهور محاسبات کوانتومی، به پتانسیل تحول‌آفرین این فناوری در حوزه‌هایی مانند رمزنگاری، بهینه‌سازی مالی، شیمی محاسباتی و یادگیری ماشین اشاره کرده است. [۱۴] این مطالعه نشان می‌دهد که علیرغم وعده‌های نظری، شکاف قابل‌توجهی بین مزیت کوانتومی نظری و امکان‌پذیری عملی وجود دارد که نیازمند طراحی همزمان سخت‌افزار و نرم‌افزار است.

[1] Qubit
[2] Shor's algorithm
[3] Grover's algorithm

جدول ۱: مقایسه تحقیقات مرتبط در حوزه محاسبات کوانتومی و فناوری اطلاعات

مرجع	محور اصلی تحقیق	نقاط قوت	محدودیت/شکاف پژوهشی	تمایز پژوهش حاضر
[۴و۹]	مبانی نظری و فیزیک کوانتوم	ارائه پایه‌های ریاضی و فیزیکی ضروری	عدم تمرکز بر کاربردهای عملی در فناوری اطلاعات	کاربردی‌سازی : تبدیل مبانی نظری به راهکارهای عملیاتی برای متخصصان IT
[۶و۷]	الگوریتم‌های بنیادین کوانتومی	اثبات ریاضی مزیت نمایی نسبت به الگوریتم‌های کلاسیک	عدم توجه به محدودیت‌های سخت‌افزاری عصر NISQ	تحلیل واقع‌بینانه : بررسی امکان‌پذیری اجرای این الگوریتم‌ها با فناوری امروز
[۱۱و۲۲]	چالش‌های سخت‌افزاری و برتری کوانتومی	تحلیل دقیق پدیده نویز و ارائه معیارهای سنجش پیشرفت	عدم ارائه نقشه راه جامع برای حوزه‌های نرم‌افزاری و امنیتی	دیدگاه کل‌نگر : ترکیب دیدگاه سخت‌افزاری، نرم‌افزاری و امنیت سایبری
[۴و۹]	یکپارچه‌سازی محاسبات کوانتومی و هوش مصنوعی	تمرکز بر ارتقای زیرساخت‌های شبکه برای پشتیبانی از QML	تمرکز محدود بر لایه شبکه و زیرساخت	پوشش جامع‌تر : بررسی سایر کاربردها نظیر رمزنگاری و بهینه‌سازی منابع
[۱۴]	مرور الگوریتم‌ها و کاربردهای نوظهور	پوشش گسترده الگوریتم‌ها و کاربردهای علمی (شیمی، داروسازی)	بررسی کلی و عدم تفکیک دقیق کاربردهای تخصصی فناوری اطلاعات	تمرکز تخصصی : دسته‌بندی اختصاصی دستاوردها برای سه حوزه کلیدی فناوری اطلاعات

در حالی که تحقیقات پیشین عمدتاً بر مبانی نظری یا الگوریتم‌های خاص متمرکز بوده‌اند، نیاز به یک بررسی ساختاریافته و به‌روز که به طور خاص دستاوردهای ملموس محاسبات کوانتومی را برای متخصصان حوزه فناوری اطلاعات تشریح کرده و چالش‌های عملی پیش روی پذیرش این فناوری را تحلیل کند، احساس می‌شود .نوآوری این پژوهش در تمرکز ویژه بر ترسیم یک نقشه راه از کاربردهای عملیاتی‌شده یا در شرف عملیاتی‌شدن در حوزه فناوری اطلاعات و ارائه یک تحلیل واقع‌بینانه از چشم‌انداز آینده با توجه به محدودیت‌های عصر NISQ است.

محاسبات کوانتومی، ویژگی‌ها و دستاوردها

محاسبات کوانتومی بر پایه دستکاری حالت‌های سیستم‌های کوانتومی بنا شده است. در قلب این فناوری، "کیوبیت" قرار دارد. همان‌طور که در مقدمه ذکر شد، یک کیوبیت می‌تواند در حالت برهم‌نهی از $|۰\rangle$ و $|۱\rangle$ به صورت $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ قرار گیرد، جایی که α و β اعداد مختلطی هستند که احتمال مشاهده هر یک از حالات پایه را تعیین می‌کنند. این ویژگی، پردازش موازی انبوهی از اطلاعات را ممکن می‌سازد. علاوه بر برهم‌نهی، پدیده "درهم‌تنیدگی" کوانتومی نیز حیاتی است. دو یا چند کیوبیت درهم‌تنیده، چنان همبستگی غیرکلاسیکی با یکدیگر پیدا می‌کنند که حالت هر یک به‌طور آنی به حالت دیگری وابسته است، صرف‌نظر از فاصله فیزیکی بین آن‌ها [۴].

این ویژگی‌ها به الگوریتم‌های کوانتومی اجازه می‌دهند تا بر محدودیت‌های کلاسیک غلبه کنند. برای پیاده‌سازی این الگوریتم‌ها، از "مدارهای کوانتومی "استفاده می‌شود که از دنباله‌ای از گیت‌های منطقی کوانتومی تشکیل شده‌اند. این گیت‌ها، عملگرهای ریاضی هستند که حالت کیوبیت‌ها را تغییر می‌دهند. به دلیل ماهیت کوانتومی، محاسبات تا زمان "اندازه‌گیری در حالت احتمالاتی باقی می‌مانند و عمل اندازه‌گیری، حالت برهم‌نهی را به یکی از حالات پایه فرومی‌ریزد.

از منظر سخت‌افزاری، چالش اصلی، حفظ همدوسی کوانتومی است. کیوبیت‌های فیزیکی به شدت نسبت به نویز محیطی حساس هستند و پدیده واگدوسی باعث از دست رفتن اطلاعات کوانتومی می‌شود [۱۱]. برای مقابله با این مشکل، تکنیک‌های تصحیح خطای کوانتومی توسعه یافته‌اند که با استفاده از چندین کیوبیت فیزیکی برای نمایش یک "کیوبیت منطقی" بی‌نقص، پایداری محاسبات را افزایش می‌دهند. این امر مستلزم سربار بسیار بالایی است و تحقق یک رایانه کوانتومی مقیاس‌پذیر و مقاوم در برابر خطا را به یک چالش مهندسی بزرگ تبدیل کرده است [۱۴].

علیرغم چالش‌های فنی، محاسبات کوانتومی دستاوردهای نظری و عملی قابل‌توجهی در حوزه فناوری اطلاعات داشته است که در سه محور اصلی قابل دسته‌بندی است: امنیت سایبری، هوش مصنوعی و خدمات مالی. در ادامه این ابعاد را با جزئیات بررسی خواهیم کرد.

حوزه امنیت سایبری بیش از همه تحت تأثیر محاسبات کوانتومی قرار گرفته است. الگوریتم شور تهدیدی وجودی برای سیستم‌های رمزنگاری کلید عمومی رایج مانند RSA و ECC است که امنیت ارتباطات اینترنتی امروز بر پایه آن‌ها استوار است [۶]. این تهدید منجر به ظهور حوزه جدیدی به نام رمزنگاری پسا-کوانتومی شده که هدف آن توسعه الگوریتم‌های مقاوم در برابر حملات رایانه‌های کوانتومی است. از سوی دیگر، توزیع کلید کوانتومی روشی برای تبادل امن کلید رمزنگاری با استفاده از اصول مکانیک کوانتومی (مانند قضیه عدم-شبیه‌سازی) است که امنیت اطلاعات را در سطح فیزیکی تضمین می‌کند [۱۳]. شبکه‌های QKDدر مقیاس شهری و حتی بین‌قاره‌ای (با استفاده از ماهواره) با موفقیت آزمایش شده‌اند و گامی بلند به سوی شبکه‌های ارتباطی غیرقابل‌نفوذ محسوب می‌شوند [۱۵].

از سوی دیگر، محاسبات کوانتومی به طور بالقوه فرصت‌های جدیدی را در هوش مصنوعی باز می‌کند، که اغلب شامل پردازش ترکیبی مقادیر بسیار زیادی از داده‌ها به منظور پیش‌بینی و تصمیم‌گیری بهتر است (به تشخیص چهره یا تشخیص تقلب فکر کنید). یک زمینه تحقیقاتی رو به رشد در یادگیری ماشین کوانتومی راه‌هایی را شناسایی می‌کند که الگوریتم‌های کوانتومی می‌توانند هوش مصنوعی سریع‌تری را فعال کنند. محدودیت‌های فعلی بر روی فناوری و نرم‌افزار، هوش عمومی مصنوعی کوانتومی را به یک امکان نسبتاً دور تبدیل می‌کند – اما مطمئناً ماشین‌های فکری را بیش از موضوعی برای داستان‌های علمی تخیلی تبدیل می‌کند. همگرایی محاسبات کوانتومی و هوش مصنوعی یکی از هیجان‌انگیزترین مرزهای پژوهشی است . الگوریتم‌های یادگیری ماشین کوانتومی نظیر ماشین‌های بردار پشتیبان کوانتومی و شبکه‌های عصبی کوانتومی وعده تسریع نمایی در آموزش مدل‌ها و بهبود دقت پیش‌بینی را می‌دهند [۱۶]. در سال‌های اخیر، پیشرفت‌های عملی قابل‌توجهی حاصل شده است. به عنوان مثال، مدل‌های QML در تحلیل تصاویر پزشکی برای تشخیص زودهنگام بیماری‌ها دقت بالاتری نسبت به همتایان کلاسیک خود نشان داده‌اند . همچنین، محاسبات مخزنی کوانتومی به عنوان یک رویکرد کارآمد برای تحلیل سری‌های زمانی و پیش‌بینی ترافیک شبکه در زیرساخت‌های IT مطرح شده است [۱۳].

امور مالی نیز یکی از اولین حوزه هایی بود که کلان داده را پذیرفت. و بسیاری از علم پشت قیمت گذاری دارایی های پیچیده - مانند گزینه های سهام - شامل محاسبه ترکیبی است. برای مثال، وقتی گلدمن ساکس، مشتقات قیمت‌ها را محاسبه می‌کند، یک محاسبات بسیار محاسباتی به نام شبیه‌سازی مونت کارلو را اعمال می‌کند که پیش‌بینی‌هایی را بر اساس حرکات شبیه‌سازی شده بازار انجام می‌دهد. سرعت محاسبات مدت‌هاست که منبع مزیتی در بازارهای مالی بوده است) جایی که صندوق‌های تامینی برای به دست آوردن مزایای میلی‌ثانیه‌ای در به دست آوردن اطلاعات قیمت با هم رقابت می‌کنند). الگوریتم های کوانتومی می توانند سرعت یک مجموعه مهم از محاسبات مالی را افزایش دهند. بعلاوه، رایانه‌های کوانتومی می‌توانند در جمع‌آوری مجموعه‌های بزرگ داده‌های تولیدی در مورد خرابی‌های عملیاتی و ترجمه آن‌ها به چالش‌های ترکیبی استفاده شوند که وقتی با یک الگوریتم الهام‌گرفته از کوانتومی جفت می‌شوند، می‌توانند تشخیص دهند که کدام بخش از یک فرآیند تولید پیچیده در حوادث خرابی محصول نقش داشته است. برای محصولاتی مانند ریزتراشه ها که این فرآیند تولید می تواند هزاران مرحله داشته باشد، کوانتوم می تواند به کاهش خرابی های پرهزینه کمک کند.

فرصت محاسبات کوانتومی برای حل سریع‌تر و ارزان‌تر مسائل ترکیبی در مقیاس بزرگ، میلیاردها دلار سرمایه‌گذاری را در سال‌های اخیر تشویق کرده است. بزرگترین فرصت ممکن است در یافتن برنامه های کاربردی جدید بیشتر باشد که از راه حل های ارائه شده از طریق کوانتوم سود می برند. همانطور که پروفسور و کارآفرین Alan Aspuru-Guzik گفت، "نقشی برای تخیل، شهود و ماجراجویی وجود دارد. شاید این مهم نیست که چند کیوبیت داریم. شاید این مربوط به تعداد هکرهای ما باشد".

همچنین بسیاری از مسائل کلیدی در مدیریت فناوری اطلاعات، مانند مسیریابی در شبکه، تخصیص منابع در مراکز داده، زمان‌بندی وظایف و کشف ناهنجاری در امنیت شبکه، در دسته مسائل بهینه‌سازی ترکیبیاتی با پیچیدگی NP-hard قرار می‌گیرند. الگوریتم‌های کوانتومی مانند بازپخت کوانتومی و الگوریتم بهینه‌سازی تقریبی کوانتومی (QAOA)برای مقابله با این دسته از مسائل بسیار امیدوارکننده هستند [۱۷]. برای نمونه، تحقیقات نشان داده است که بازپخت کوانتومی می‌تواند راه‌حل‌های بهینه‌تری برای مسئله معروف "فروشنده دوره‌گرد و کاربردهای آن در بهینه‌سازی مسیرهای لجستیک و شبکه‌های مخابراتی ارائه دهد. در حوزه مالی نیز، الگوریتم‌های کوانتومی برای بهینه‌سازی سبد سرمایه‌گذاری با در نظر گرفتن تعداد زیادی متغیر و محدودیت، کارایی خود را نشان داده‌اند [۱۴].

چالش‌ها و چشم‌اندازها

با وجود پتانسیل عظیم، مسیر رسیدن به "برتری کوانتومی" عملی و گسترده با چالش‌های مهندسی و بنیادین متعددی همراه است. در حال حاضر، رایانه‌های کوانتومی در عصر NISQ قرار دارند [۱۱]. کیوبیت‌های این دستگاه‌ها ناپایدار بوده و زمان همدوسی آن‌ها (مدت زمانی که می‌توانند حالت کوانتومی خود را حفظ کنند) بسیار کوتاه و در حد میکروثانیه است . .علاوه بر این، گیت‌های کوانتومی با نرخ خطای نسبتاً بالایی (بیش از 10^{-3}) عمل می‌کنند که این امر عمق مدارهای قابل‌اجرا را به شدت محدود می‌سازد . برای غلبه بر این مشکل، پیاده‌سازی کامل روش‌های تصحیح خطای کوانتومی ضروری

است که به نوبه خود نیازمند میلیون‌ها کیوبیت فیزیکی برای ساخت یک کیوبیت منطقی پایدار است. همچنین، چالش توسعه نرم‌افزار و الگوریتم‌های کارآمد که با محدودیت‌های سخت‌افزارهای NISQ سازگار باشند، پابرجاست [۱۹].

با این وجود، چشم‌انداز آینده همچنان روشن است. پیش‌بینی می‌شود که در دهه آینده، رویکرد غالب، سیستم‌های هیبریدی کلاسیک-کوانتومی باشد [۲۰]. در این معماری، رایانه‌های کلاسیک بخش‌های اصلی برنامه را اجرا می‌کنند و تنها زیرمسائل بسیار پیچیده را برای حل به پردازنده کوانتومی (QPUs)ارسال می‌نمایند. این رویکرد بهره‌برداری از مزایای محاسبات کوانتومی را در کوتاه‌مدت و پیش از رسیدن به رایانه‌های کوانتومی کامل و بی‌نقص ممکن می‌سازد [۸]. شرکت‌های بزرگ فناوری و استارتاپ‌های متعددی به طور فعال در حال سرمایه‌گذاری در این زمینه هستند و نقشه‌های راه آن‌ها حکایت از افزایش مداوم تعداد کیوبیت‌ها و بهبود کیفیت آن‌ها دارد [۱۲]. از سوی دیگر، همکاری‌های بین‌المللی برای توسعه استانداردهای جدید رمزنگاری پسا-کوانتومی (PQC) توسط موسساتی مانند NIST در حال نهایی شدن است [۲۱].

نتیجه‌گیری و راهکارهای آتی

محاسبات کوانتومی در آستانه تبدیل شدن از یک کنجکاوی علمی به یک فناوری راهبردی و تحول‌آفرین در حوزه فناوری اطلاعات است. این مقاله نشان داد که این فناوری با بهره‌گیری از پدیده‌های کوانتومی، توانایی حل مسائلی را دارد که فراتر از توان محاسباتی رایانه‌های کلاسیک است. دستاوردهای کلیدی آن در حوزه‌های **امنیت سایبری**)ظهور رمزنگاری پسا-کوانتومی و شبکه‌های(QKD ، هوش مصنوعی (توسعه الگوریتم‌های یادگیری ماشین کوانتومی با دقت و سرعت بالاتر) و بهینه‌سازی سیستم‌ها (ارائه راه‌حل‌های نوین برای مسائل پیچیده شبکه و تخصیص منابع) نویدبخش یک تحول بنیادین است. با این حال، مسیر پیش رو بدون چالش نیست. محدودیت‌های جدی سخت‌افزارهای کنونی در عصرNISQ ، به‌ویژه ناپایداری کیوبیت‌ها و نرخ بالای خطا، مهم‌ترین موانع در راه تحقق پتانسیل کامل این فناوری هستند .

بر اساس یافته‌های این مطالعه، راهکارهای زیر برای جامعه علمی و صنعتی ایران پیشنهاد می‌شود:

- سرمایه‌گذاری هدفمند در آموزش و پژوهش : با توجه به ماهیت میان‌رشته‌ای این حوزه، تربیت نیروی انسانی متخصص در تقاطع فیزیک کوانتوم، علوم کامپیوتر و مهندسی برق از بالاترین اولویت‌هاست.
- توسعه سیستم‌های هیبریدی : تمرکز بر توسعه الگوریتم‌ها و نرم‌افزارهای کاربردی برای معماری‌های هیبریدی کلاسیک-کوانتومی که در کوتاه‌مدت و با زیرساخت‌های موجود نیز قابل بهره‌برداری هستند.[20]
- آمادگی برای مهاجرت به رمزنگاری پسا-کوانتومی : سازمان‌ها و نهادهای حساس باید از هم‌اکنون برنامه‌ریزی برای ارزیابی و جایگزینی الگوریتم‌های رمزنگاری آسیب‌پذیر با استانداردهای PQC را آغاز کنند.[21]
- توسعه زیرساخت‌های آزمون و ارزیابی : ایجاد بسترهای آزمایشی برای توسعه‌دهندگان نرم‌افزار و پژوهشگران به‌منظور آزمایش الگوریتم‌های کوانتومی بر روی سخت‌افزارهای واقعی یا شبیه‌سازهای قدرتمند ضروری است.

در نهایت، اگرچه تحقق رایانه‌های کوانتومی جهانی و بی‌نقص ممکن است یک دهه یا بیشتر زمان ببرد، اما تأثیرات عمیق آن بر فناوری اطلاعات و جامعه از هم‌اکنون آغاز شده و نادیده گرفتن آن یک خطای استراتژیک خواهد بود. عصر کوانتوم فرا رسیده است و آمادگی برای آن نیازمند عزم ملی و همکاری نزدیک دانشگاه، صنعت و دولت است.

تعارض منافع

هیچ‌گونه تعارض منافع توسط نویسندگان بیان نشده است.

منابع

[1] Reinsel D, Gantz J, Rydning J. The digitization of the world: from edge to core. IDC White Paper. 2018; US44413318. doi: 10.25607/IDC-2018-11

[2] Thompson NC, Greenewald K, Lee K, Manso GF. The computational limits of deep learning. arXiv. 2020; arXiv:2007.05558. doi: 10.48550/arXiv.2007.05558

[3] Powell JR. The quantum limit to Moore's law. Proceedings of the IEEE. 2008; 96(8): 1247-1248. doi: 10.1109/JPROC.2008.925411

[4] Feynman RP. Simulating physics with computers. International Journal of Theoretical Physics. 1982; 21(6/7): 467-488. doi: 10.1007/BF02650179

[5] Nielsen MA, Chuang IL. Quantum computation and quantum information: 10th anniversary edition. Cambridge: Cambridge University Press; 2010. doi: 10.1017/CBO9780511976667

[6] Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing. 1997; 26(5): 1484-1509. doi: 10.1137/S0097539795293172

[7] Grover LK. A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing; 1996 May; Philadelphia, USA. p. 212-219. doi: 10.1145/237814.237866

[8] Dalzell AM, McArdle S, Berta M, Bienias P, Chen CF, Gilyén A, et al. Quantum algorithms:

A survey of applications and end-to-end complexities. arXiv. 2023; arXiv:2310.03011. doi: 10.48550/arXiv.2310.03011

[9] Benioff P. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. Journal of Statistical Physics. 1980; 22(5): 563-591. doi: 10.1007/BF01011339

[10] Chae E, Choi J, Kim J. An overview of qubit technologies: Superconducting, trapped ions, and photonic quantum computing. Electronics. 2024; 13(3): 522. doi: 10.3390/electronics13030522

[11] Preskill J. Quantum Computing in the NISQ era and beyond. Quantum. 2018; 2: 79. doi: 10.22331/q-2018-08-06-79

[12] Gambetta J. IBM Quantum Roadmap: 2025 Update. IBM Quantum Blog. 2025. Available from: https://www.ibm.com/quantum/blog/quantum-roadmap-2025 [Accessed 18th April 2026].

[13] Wolfmayr M, Uthpala LM. The Utilization of Quantum Computing for AI Applications in Classical IT Network Environments [thesis]. Finland: Metropolia University of Applied Sciences; 2025. Available from: https://www.theseus.fi/handle/10024/896664

[14] Grigoryan H, Petrosyan L, Hakobyan S. Quantum computing: foundations, algorithms, and emerging applications. Frontiers in Quantum Science and Technology. 2025; 4:1723319. doi: 10.3389/frqst.2025.1723319

[15] Liao SK, Cai WQ, Liu WY, Zhang L, Li Y, Ren JG, et al. Satellite-to-ground quantum key distribution. Nature. 2017; 549(7670): 43-47. doi: 10.1038/nature23655

[16] Biamonte J, Wittek P, Pancotti N, Rebentrost P, Wiebe N, Lloyd S. Quantum machine learning. Nature. 2017; 549(7671): 195-202. doi: 10.1038/nature24274

[17] Farhi E, Goldstone J, Gutmann S. A quantum approximate optimization algorithm. arXiv. 2014; arXiv:1411.4028. doi: 10.48550/arXiv.1411.4028

[18] Campbell ET, Terhal BM, Vuillot C. Roads towards fault-tolerant universal quantum computation. Nature. 2017; 549(7671): 172-179. doi: 10.1038/nature23460

[19] Zhao J, Kumar S. Quantum software engineering: Landscape, challenges, and opportunities. ACM Transactions on Software Engineering and Methodology. 2024; 33(1): 1-38. doi: 10.1145/3625295

[20] McCaskey A, Dumitrescu E, Liakh D, Chen M, Feng W, Humble T. Hybrid programming for near-term quantum computing systems. 2018 IEEE International Conference on Rebooting Computing (ICRC); 2018 Nov; Tysons, VA, USA. IEEE; 2018. p. 1-8. doi: 10.1109/ICRC.2018.8638598

[21] Alagic G, Alperin-Sheriff J, Apon D, Cooper D, Dang Q, Kelsey J, et al. Status report on the third round of the NIST post-quantum cryptography standardization process. NIST Interagency Report. 2022; NIST IR 8413-upd1. doi: 10.6028/NIST.IR.8413-upd1

[22] Arute F, Arya K, Babbush R, Bacon D, Bardin JC, Barends R, et al. Quantum supremacy using a programmable superconducting processor. Nature. 2019; 574(7779): 505-510. doi: 10.1038/s41586-019-1666-5