فصلنامه علمی علوم حیاتی و عرصه های نوپدید، سال اول، شماره اول، تابستان ۱۴۰۲

علوم و فناوری‌های کوانتومی زمینه‌ساز شکوفایی علمی و حوزه‌ای کلیدی برای ایفای نقش حداکثری در هندسه نظم جدید جهانی

سید نصیب الله دوستی مطلق[1]

تاریخ دریافت: ۱۴۰۲/۰۳/۱۲ تاریخ پذیرش:۱۴۰۲/۰۶/۲۵

چکیده:

ما در میانه «انقلاب دوم کوانتومی» قرار داریم؛ انقلابی که به فناوری‌های برهم زنی امکان بروز می‌دهد که از توانایی تغییر پویایی‌های بلندمدت در حوزه‌های تجارت، امور نظامی و توازن و برابری راهبردی قدرت برخوردار هستند. در آینده نزدیک، تحقق محاسبات کوانتومی منجر به انقلابی در قدرت محاسباتی، همراه با تحولات وسیع برنامه‌های کاربردی خواهد شد، که فضای سایبر جدیدی را پایه‌ریزی خواهد کرد. با ناتوانی فیزیک کلاسیک برای توصیف برخی پدیده‌ها در اوایل قرن بیستم، نظریه کوانتوم به وجود آمد، که محققان این ظهور را انقلاب کوانتومی اول می‌نامند (نظریه کوانتوم منجر به ۳ انقلاب شد: انقلاب اول منجر به ایجاد نظریه کوانتومی شد و درواقع تحول در دنیای ماده بود، انقلاب دوم ورد نظریه کوانتوم به دنیای محاسبات، اطلاعات، ارتباطات و اندازه‌گیری است و منجر به تحول این حوزه‌ها شد و انقلاب سوم ورود نظریه کوانتوم به دنیای علوم انسانی و اجتماعی است). امروزه نظریه کوانتوم دیگر مختص فیزیک و شیمی نیست و از زیست‌شناسی کوانتومی، بیوانفورماتیک کوانتومی، مغز کوانتومی، شناختی کوانتومی و حتی مدیریت و علوم اجتماعی الهام گرفته از نظریه کوانتوم صحبت می‌شود. کشورهای دنیا برای به سرانجام رساندن علوم و فناوری‌های کوانتومی سرمایه گزاری های زیادی انجام داده‌اند. در این مقاله بر آنیم تا با استفاده از روش توصیفی –تحلیلی و با ابزار کتابخانه‌ای و گردآوری اطلاعات از منابع مختلف و نیز مصاحبه خبرگانی نقش علوم و فناوری‌های کوانتومی را به‌عنوان حوزه‌ای کلیدی در هندسه نظم جدید جهانی بررسی نماییم.

واژگان کلیدی: علوم و فناوری‌های کوانتومی، نظم جدید جهانی، درهم‌تنیدگی، محاسبات کوانتومی.

[1] استادیار، گروه پژوهشی سایبر الکترونیک، دانشگاه عالی دفاعی ملی doustimotlagh@chmail.ir

۱. مقدمه

ما در میانه «انقلاب دوم کوانتومی» قرار داریم؛ انقلابی که به فنّاوری‌های برهم زن امکان بروز می‌دهد که از توانایی تغییر پویایی‌های بلندمدت در حوزه‌هایی همچون تجارت، امور نظامی و توازن و برابری راهبردی قدرت برخوردار هستند. در آینده نزدیک، تحقق محاسبات کوانتومی منجر به انقلابی در قدرت محاسباتی، همراه با تحولات وسیع برنامه‌های کاربردی خواهد شد، که فضای سایبر جدیدی را پایه‌ریزی خواهد کرد(quantum h, 2018)

با ناتوانی فیزیک کلاسیک (فیزیک نیوتنی، ترمودینامیک، مکانیک آماری و الکترومغناطیس) برای توصیف برخی پدیده‌ها در اوایل قرن بیستم ، نظریه کوانتوم به وجود آمد، که محققان این ظهور را انقلاب کوانتومی اول می‌نامند(dousti, 1401). انقلاب کوانتومی اول درواقع همان بنیان‌های فیزیکی برای پیشرفت‌های عظیمی مانند چیپ‌های کامپیوتری، لیزرها، تصویربرداری رزونانسی مغناطیسی (MRI)، فنّاوری‌های ارتباطی مدرن، فیزیک اتمی، فیزیک هسته‌ای، فیزیک مولکولی، نانو و .... است (quantum h, 2018). اما چیزی که به‌عنوان انقلاب کوانتومی دوم شناخته می‌شود، درواقع استفاده از مزایای پدیده ***درهم تنیدگی*** کوانتومی است. درهم تنیدگی یک پدیده طبیعی است که محققان در اوایل دهه ۱۹۳۰، آن را شناسایی کرده‌اند و امروزه ، پایه و اساس کاربردهای جدیدی مانند ارتباطات کوانتومی، سنجش کوانتومی، شبیه‌سازی کوانتومی، محاسبات کوانتومی و ... به‌حساب می‌آید. انقلاب کوانتومی دوم ، به معنای درک و کاربرد این امکانات جدید است، که منجر به فضای سایبر جدیدی بنام فضای سایبر کوانتومی می‌شود و همچنین یک همگرایی بی‌نظیری را که احتمالاً QMBIC[1] است را رقم خواهد زد، که بدون شک، علوم و فناوری‌های همگرای QMBIC یکی از برترسازهایی است، که سکان هدایت بیشتر در دهه‌های آینده خواهد بود[۲]. همگرایی علوم و

[1] کوانتوم، ماده، زیست فناوری، فناوری اطلاعات، علوم شناختی

[۲] البته باید دقت شود که مدل‌های همگرایی زیادی وجود دارد و برخی از کشورها و حتی برخی از کشورها مدل‌های همگرایی خاص خود را دارا می‌باشند. مثل ناتو ۶ نوع همگرایی را بعنوان چالش‌های امنیت فناوری ۲۰۲۰ تا ۲۰۴۰ خود

فناوری‌ها، یکی از مهم‌ترین و بهترین راه‌حل ارائه‌شده برای تسریع درروند توسعه فناوری‌های موردنیاز در آینده و رهایی جامعه بشری از مشکلات عدیده‌ای است که با آن دست‌وپنجه نرم می‌کند. علاوه بر این موارد، تبعات و پیامدهای فناوری‌های همگرای QMBIC بر تأمین امنیت ملی، امنیت زیرساخت‌های اطلاعاتی و صیانت از زیرساخت‌های حیاتی کشور و همچنین، پیامدهای ناشی از غافلگیر شدن کشور از این فناوری‌ها، اهمیت بررسی حوزه فناوری‌های همگرای QMBIC و برنامه‌ریزی راهبردی جهت دستیابی به علوم و فناوری‌های این حوزه را بیش‌ازپیش مشخص می‌کند(dousti, 1401). اهمیت این موضوع تا جایی است که تن کیو[1] یک از محققان دانشگاه ارتش آمریکا در سال ۲۰۱۵، مدل ارتش جدیدی را به ایالات‌متحده پیشنهاد داد، که مدل "سه‌گانه " نامیده شد (than, 2017) و در این مدل چهار نیروی دریایی، هوایی، فضایی و زمینی آمریکا را در یک‌طرف، سایبر کلاسیک را یک‌طرف و سایبر کوانتومی را در طرف دیگر قرار می‌دهد و بیان می‌کند که کشوری که بتواند بخش سایبر خود را با فناوری‌های کوانتومی مجهز کند در ارتقاء بازدارندگی، حکم کشوری را دارد که اولین بار به فنّاوری بمب هسته‌ای دست پیداکرده است. در دنیای امروز دیگر نظریه کوانتوم مختص فیزیک و شیمی نیست و در مجامع علمی امروزی از زیست‌شناسی کوانتومی، بیوانفرماتیک کوانتومی، مغز کوانتومی، شناختی کوانتومی و حتی مدیریت و علوم اجتماعی الهام گرفته از نظریه کوانتوم صحبت می‌شود. کشورهای دنیا برای به سرانجام رساندن علوم و فناوری‌های کوانتومی سرمایه گزاری های بسیار زیادی را انجام داده‌اند. چین یک پروژه ۱۰ ساله چهارده و نیم میلیارد داری تعریف کرده است و چندین مرکز مهم در حوزه‌های مختلف علوم و فناوری‌های کوانتومی تأسیس کرده است(quantum h, 2018).

۲. مبانی نظری و پیشینه

معرفی کرده است. روسیه مدل همگرایی خاصی را تعریف کرده مرکزیت آن با پزشکی است. سازمان ملل نیز مدل هگرایی دیگری بنام DAME را مطرح کرده است و ...

[1] Than kywe

با ظهور تناقضات آشکار در توجیه رفتار ذرات در مقیاس زیر اتمی با نظریات کلاسیک محققان و دانشمندان فیزیک نظری بر آن شدند اصول جدیدی از علم فیزیک را توسعه دهند که بتواند پاسخ گوی رفتار این ذرات باشد. کوانتوم شاخه از فیزیک است که در ابتدای قرن بیستم با ارائه چند اصل فیزیکی توانست بسیاری از مسائل پیشروی دانشمندان آن زمان را توجیه کند. اصول استخراج‌شده از این علوم باعث شد تا کاربرد فیزیک در زندگی روزمره نقش بسزایی داشته باشد. اولین انقلاب کوانتومی باعث اختراعاتی مانند لیزر و ترانزیستور، (بلوک اصلی ساخت رایانه) را امکان‌پذیر کرد، هنگامی‌که دانشمندان قوانین مکانیک کوانتومی را فهمیدند و دستگاه‌هایی ساختند که از آن قوانین پیروی کنند؛ اما با پیشرفت علم کوانتوم و ایده بهره‌مندی از این قوانین در افزایش کارایی سایر عرصه‌های نظامی، اجتماعی، بهداشت، امنیتی و ثروت آفرینی باعث شد تا فعالان این حوزه‌ها علاقه‌مند به سرمایه‌گذاری در فناوری‌های مرتبط به کوانتوم شوند(Hughes, 2021).

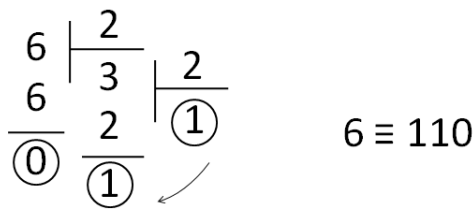
ازاین‌رو کشورها و شرکت‌های پیشرو در فناوری بر آن شدن برنامه‌هایی را برای بهره‌مندی از فناوری‌های کوانتومی تدوین کنند. برنامه ملی فناوری‌های کوانتومی بریتانیا که توسط دولت انگلستان در سال ۲۰۱٤ باهدف تبدیل زبان علمی مکانیک کوانتوم به خدمات و محصولات جدید تهیه‌شده است. طول مدت این سند ۱۰ سال در نظر گرفته‌شده است (Knight, 2019). شورای علوم و فناوری ملی کاخ سفید در حقیقت بازوی اجرایی برای هماهنگی سیاست‌های علوم و فناوری در میان سازمان‌های گوناگونی است که درزمینه تحقیقات و توسعه فدرالی فعالیت می‌کنند. این نهاد در سال ۲۰۱۸ برنامه را باهدف رهبری آمریکا در زمینه علم اطلاعات کوانتوم در دهه آینده برنامه‌ای را تدوین کرده است. محدوده زمانی این برنامه برای بخش‌های مختلف متفاوت است اما برای بخش دفاعی تا بیست سال برنامه در نظر گرفته‌شده است (Raymer, 2019). شورای تحقیقات دولت استرالیا با مأموریت مهندسی آینده کوانتوم برنامه را در سال ۲۰۱۸ تدوین کرده است. مدت این برنامه ۲ سال در نظر گفته‌شده است(EQUS, 2018).پژوهشگاه تحقیقات ملی هلند که متولی توسعه علوم در هلند است باهدف توسعه فناوری‌های کوانتومی سندی در سال ۲۰۱۹ تدوین کرده است. بازه زمانی این سند ۵ ساله خواهد بود. (Informatica, 2019).کشور چین در راستای

رسیدن به جایگاه رهبری جهان در عرصه نوآوری هزینه‌های سنگینی را انجام داده است و تدوین برنامه‌های در این زمینه سرمایه‌های زیادی را سرمایه‌گذاری و جذب کرده‌اند. به دلیل عدم شفافیت در اطلاعات منتشرشده توسط دولت چین بازه زمانی برنامه مشخص نیست ولی دست‌کم چین قصد دارد تا سال ۲۰۲۱ چین بزرگ‌ترین مرکز تحقیقاتی کوانتومی جهان را در استان آنهویی بسازد(USTC, 2016).دولت روسیه برای توزیع مسئولیت‌های لازم برای توسعه طیف گسترده‌ای از فناوری‌ها ، چندین توافق‌نامه با چندین شرکت دولتی امضا کرده است. و برنامه‌هایی را برای هریک از این شرکت‌ها تعریف کرده است در سال ۲۰۱۹ کشور روسیه اهداف زیر را برای ۵ سال آینده مشخص کرده است. (center, 2018) کشور ژاپن برنامه‌های ملی زیادی از سال‌های ۱۹۸۵ تا به امروز برای دستیابی به فناوری‌های کوانتومی اجرا کرده است این برنامه‌ها به‌صورت دوره‌ای تمدیدشده و تا سال ۲۰۲۶ برای این منظور این برنامه‌ها ادامه خواهد داشت(Iopscience, 2019). در مسابقه جهانی برای باز کردن پتانسیل‌های فناوری‌های کوانتومی و پیشرفت‌های تحول آمیز در علم ، صنعت و جامعه ، اروپا باید یک پایگاه صنعتی محکم ایجاد کند که از رهبری علمی آن استفاده کند. بدین منظور اهدافی و اسنادی را تعیین کرده است. این برنامه از سال ۲۰۱۶ شروع‌شده و تا سال ۲۰۲۱ ادامه خواهد داشت. (Commission, 2019). ناتو باهدف بررسی تهدیدات آینده امنیت روابط بین‌الملل که متأثر از فناوری پردازنده‌های کوانتومی است راهبرد دفاع سایبری ناتو در فناوری‌های کوانتومی را در سال ۲۰۱۶ تدوین کرده است. بخش هوش مصنوعی شرکت گوگل تلاش می‌کند تا در زمینه ساخت پردازنده‌های کوانتومی و توسعه الگوریتم‌های کوانتوم توسعه چشمگیری داشته باشد.شاخه رایانش ابری شرکت علی‌بابا با امضای یک تفاهم‌نامه با آکادمی علوم چین برنامه را در جهت استفاده از علوم کوانتومی در زمینه محاسبات و امنیت اطلاعات تدوین کرده است. شرکت آی بی ام یکی از بزرگ‌ترین شرکت‌های خدمات فناوری اطلاعات در جهان است که در ۱۷۰ کشور دنیا شعبه دارد این شرکت با سرمایه‌گذاری عظیم بر روی علوم فناوری‌های کوانتومی یکی از پیشتازان این فناوری محسوب می‌شود (IBM, 2017).واحد تحقیقات شرکت

مایکروسافت در تلاش است بتواند در عرصه محاسبات کوانتومی نقش یک رهبر انقلاب را بازی کند و بدین منظور چشم‌انداز و اهداف ویژه دارد (Microsoft, 2018).

۱-۲ شیوه‌های پردازش اطلاعات

به لحاظ شیوه‌های پردازش اطلاعات، نظریهٔ اطلاعات به دودسته تقسیم می‌شود: اطلاعات کلاسیک و اطلاعات کوانتومی. شاید بتوان اساسی‌ترین تفاوت را در این دو نظریه، عنصر بنیادی حافظه دانست که در اطلاعات کلاسیک به آن بیت و در اطلاعات کوانتومی به آن کیو بیت (بیت کوانتومی) می‌گویند. در اطلاعات کلاسیک، یک بیت را می‌توان نمایش جواب «آری» یا «خیر» به یک سؤال دانست. به لحاظ ریاضی، یک بیت کلاسیک یک سیستم دوحالته است که فقط دو مقدار صفر و یک را می‌پذیرد و اطلاعات را بر مبنای عدد ۲ یا سیستم دو–دویی نمایش می‌دهد. به‌عنوان‌مثال، برای نمایش یک عدد در مبنای ۲ کافی است یک عدد را بر عدد ۲ تقسیم کرده و سپس خارج‌قسمت را مجدداً بر ۲ تقسیم کنیم و این کار را تا زمانی که خارج‌قسمت از ۲ کمتر می‌شود ادامه دهیم. در پایان آخرین خارج‌قسمت و باقیمانده‌ها در کنار هم، نمایش دو–دویی عدد مذکور خواهند بود. مثلاً عدد ٦ در مبنای ۲ برابر با ۱۱۰ است(Nielsen, 200).



نمایش عدد ٦ در مبنای ۲

برای نمایش عدد ٦ به سه بیت نیازمندیم. به لحاظ فیزیکی می‌توان یک بیت را به‌صورت یک مدار الکتریکی طراحی کرد که یا در ولتاژ صفر (معادل عدد صفر) یا در ولتاژی غیر از صفر مثلاً «۵+» ولت (معادل عدد یک) باشد. با قرار دادن هر بیت در دو وضعیت مذکور می‌توان اطلاعات را

به‌صورت سیستم دو-دویی ذخیره کرد. با اطلاق یک عدد به هر حرف از حروف الفبا می‌توان آن‌ها را نیز در مبنای دو-دویی نمایش داد و ذخیره کرد. به‌طور کل برای ذخیره و نمایش اطلاعات (مثلاً یک عدد) به چند بیت نیاز است؟ فرض کنید کمیتی خاص می‌تواند بین صفرتا حالت خاص را به خود بگیرد. تعداد بیت لازم برای نمایش این کمیت از رابطه زیر به دست می‌آید:

(۱)

$$2^n \geq m,$$

که در آن n حداقل تعداد بیت است. مثلاً برای نمایش اعداد صفرتا ۷، ۸ تا عدد داریم. بنابراین حداقل به ۳ بیت نیاز داریم تا اعداد صفرتا ۷ را نشان دهیم.

جدول (۱): نمایش دودویی اعداد صفرتا ۷

عدد	0	1	2	3	4	5	6	7
نمایش دودویی	000	001	010	011	100	101	110	111

حال که می‌توانیم اطلاعات را کدگذاری کنیم، می‌خواهیم بدانیم که یک پیام حاوی چه میزان اطلاعات است. با در نظر گرفتن معادله (۱) و گرفتن لگاریتم در مبنای ۲ از طرفین معادله خواهیم داشت:

(۲)

$$n = \log_2^m,$$

بر مبنای رابطه بالا، n بیت می‌تواند m پیام مختلف را ذخیره کند. به‌عنوان‌مثال واحد اطلاعات در رایانه که بایت نامیده می‌شود شامل ۸ بیت به هم متصل است. بنابراین یک بایت می‌تواند ۲۵۶ پیام مختلف را ذخیره کند، چراکه $\log_2^{256} = 8$.

۲-۲ قانون کوانتومی نِون در برابر قانون کلاسیکی مور

در سال۱۹٦۵ مور (پایه‌گذار شرکت اینتل) مشاهده کرد که تعداد ترانزیستورهای موجود در چیپ‌های رایانه تقریباً هر 18ماه دو برابر می‌شود. این موضوع بیانگر رشدی نمایی در چگالی (تعداد در واحد سطح) ترانزیستورها در مدارهای الکترونیکی است. این کشف موسوم به قانون مور است و درواقع نتیجه پیشرفت سریع فناوری نیمه‌رساناهاست (بعدها این قانون اندکی اصلاح شد، به صورتی که هر دو سال تعداد ترانزیستورها دو برابر می‌شود). از دیدگاه فیزیک، بیان قانون مور به‌صورت تعداد اتم‌های لازم برای نمایش یک بیت اطلاعات در رایانه‌هاست. در کامپیوترهای مدرن امروزی برای بیان یک بیت از اطلاعات، حدوداً چند صد اتم لازم است. طبق پیش‌بینی قانون مور در سال 2020 یک بیت می‌تواند توسط یک اتم نمایش داده شود! این در حالی است که می‌دانیم رفتار تک اتم‌ها از قوانین مکانیک کوانتومی تبعیت می‌کند(dousti, 1401).

در دسامبر سال ۲۰۱۸، دانشمندان گوگل محاسبه‌ای بر روی بهترین پردازنده کوانتومی گوگل انجام دادند. آن‌ها توانستند با استفاده از یک لپ‌تاپ معمولی محاسبات انجام‌شده در پردازندهٔ

کوانتومی خود را تأیید کنند. سپس در ژانویه، آزمایش مشابهی را روی نسخه ارتقاء یافتهٔ تراشه کوانتومی خود انجام دادند. این بار به‌منظور شبیه‌سازی تأیید نتیجه مجبور بودند از یک رایانه رومیزی قدرتمند استفاده کنند. تا فوریه، دیگر رایانه‌ای کلاسیک در ساختمان وجود نداشت که بتوانند برنامه اجراشده بر روی پردازنده کوانتومی خود را با استفاده از آن شبیه‌سازی و نتیجه به‌دست‌آمده از آن را تأیید کنند.

این پیشرفت سریع منجر به قانونی شد که موسوم به "قانون نِون[1]" است که یک قانون جدید برای توصیف سرعت ارتقاء رایانه‌های کوانتومی نسبت به رایانه‌های کلاسیک است. بر مبنای این قانون رایانه‌های کوانتومی نسبت به انواع رایج کلاسیکی توان محاسباتی بالاتر، در حد نمایی دوگانه (یعنی یک سرعت ارتقایی بسیار بالاتر از قانون کلاسیکی مورا!) دارند. قانون مور بیان می‌کند (تقریباً) قدرت محاسبات هر دو سال یک‌بار دو برابر می‌شود و نمایی به‌صورت $2^1, 2^2, 2^3, \ldots$ است. اما رشد نمایی دوگانه بسیار چشمگیرتر است. یعنی به‌جای افزایش با توان ۲، مقادیر با قدرت‌های $2^{2^1}, 2^{2^2}, 2^{2^3}, \ldots$ رشد می‌کنند.

این رشد نماییِ دوگانه چنان بی‌همتا است که یافتن نظیر آن در جهان واقعی بسیار دشوار است. این میزان پیشرفت در محاسبات کوانتومی ممکن است اولین رتبه را داشته باشد. نرخ رشد نمایی دوگانه که طبق گفته نون در ارتقاء رایانه‌های کوانتومی وجود دارد، نتیجه‌ای از دو عامل نمایی است که با یکدیگر ترکیب‌شده‌اند. عامل اول این است که رایانه‌های کوانتومی یک مزیت نمایی ذاتی نسبت به انواع کلاسیکی دارند: اگر یک مدار کوانتومی دارای چهار کیو بیت باشد ، به یک مدار کلاسیک با ۱۶ بیت معمولی برای دستیابی به همان قدرت محاسباتی نیاز است. حتی اگر فناوری کوانتومی هرگز بهبود نمی‌یافت، بازهم این نتیجه صادق بود. دومین عامل ناشی از رشد سریع پردازنده‌های کوانتومی است. تراشه‌های کوانتومی با سرعت نمایی بهبود می‌یابند. طبق گفته نون این پیشرفت سریع با کاهش میزان خطا در مدارهای کوانتومی انجام‌شده است. کاهش میزان خطا به مهندسان این امکان را می‌دهد که پردازنده‌های کوانتومی بزرگ‌تری بسازند. اگر رایانه‌های کلاسیکی توان محاسباتی بیشتری برای شبیه‌سازی پردازنده‌های کوانتومی نیاز داشته باشند و پردازنده‌های

[1] Neven

کوانتومی باگذشت زمان ازنظر ظاهری قدرتمندتر شوند، تازه به این رابطه نمایی دوگانه بین ماشین‌های کوانتومی و کلاسیک می‌رسیم(dousti, 1400).

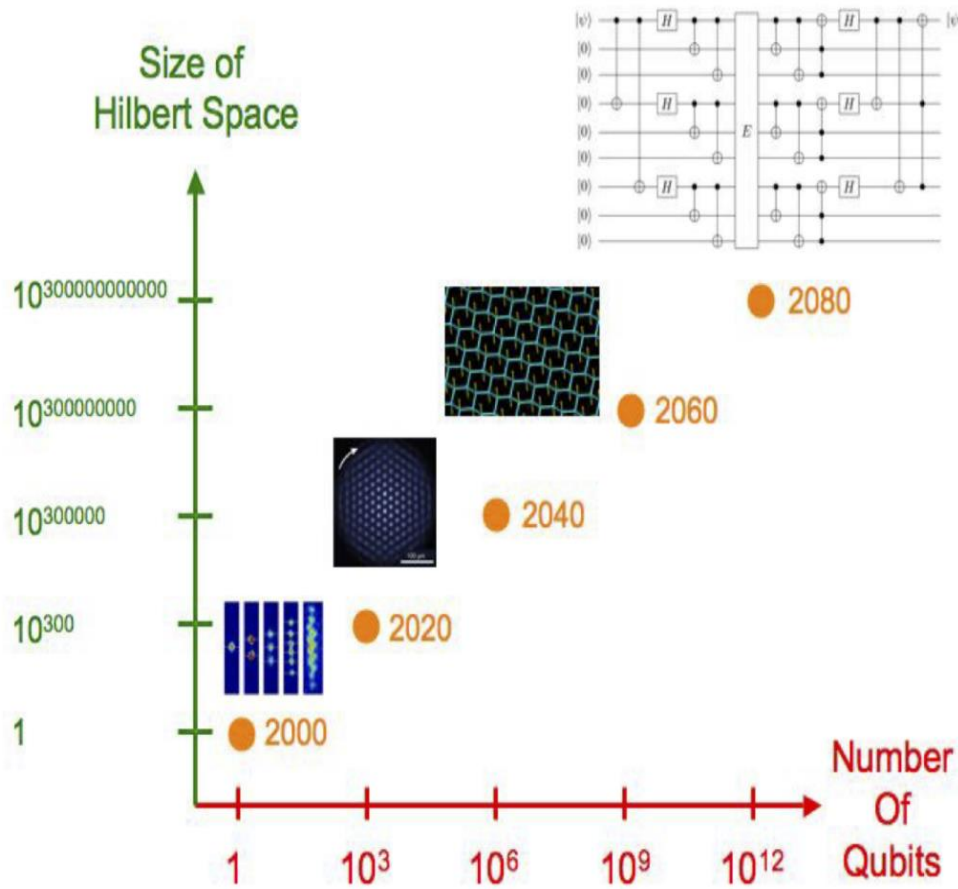
درهم‌تنیدگی کوانتومی

آیا این امکان دارد که اتفاق افتادن چیزی در اینجا، بلافاصله باعث روی دادن چیزی در مکانی دورتر شود؟ آیا ممکن است که در همان لحظه رویدادی مشابه ده کیلومتر دورتر یا آن‌سوی کیهان اتفاق بیفتد؟ پاسخ این سؤال مثبت است. این پدیده را درهم‌تنیدگی گویند. پدیده‌ای که در آن دو موجود صرف‌نظر از آن‌که چقدر از هم دور باشند، به‌شدت به هم مرتبط هستند. اتفاق جالب دیگری که در مورد درهم‌تنیدگی می‌افتد، مربوط به درهم‌تنیدگی بیش از دو ذره است(dousti, 1396).

اگر ذرات A و B درهم‌تنیده و ذرات C و D نیز باهم درهم‌تنیده باشند، آن‌وقت می‌توان با عبور دادن B و C از دستگاهی که این دو را درهم‌تنیده می‌کنند، ذرات جدا از هم یعنی A و D را نیز درهم‌تنیده نمود. با استفاده از درهم‌تنیدگی، حالت یک‌ذره را می‌توان به مقصدی معین دور فرستی یا تله پورت نمود.

قبل از پرداختن به موضوع درهم‌تنیدگی لازم است که در مورد اصل برهم‌نهی صحبت کنیم زیرا که ایده درهم‌تنیدگی در دل اصل برهم‌نهی نهفته است. اصل برهم‌نهی می‌گوید که یک حالت جدید از یک سامانه ممکن است از دو یا چند حالت ساخته‌شده باشد به شکلی که حالت جدید از هر یک از حالت‌های ترکیب‌شده، بخشی را سهم می‌برد. اگر A و B به دو ویژگی مختلف از یک‌ذره، همچون بودن در دو مکان مختلف، نسبت داده شوند، آن‌وقت برهم‌نهی حالت‌ها که به شکل A+B نوشته می‌شود هم باحالت A و هم باحالت B در چیزی مشترک است. مانند کیو بیت که به‌صورت $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ در رابطه (۳) نشان داده‌ایم.

کیو بیت یک ترکیب خطی از حالت‌های $|0\rangle$ و $|1\rangle$ است که درواقع کیو بیت در برهم‌نهی از دو حالت $|0\rangle$ و $|1\rangle$ قرار دارد(Nielsen, 200).



شکل (۱): فضای هیلبرت قابل دسترس در پنجاه سال آینده. مقیاس افقی قانون نون را برای پردازنده‌های کوانتومی با تعداد کیوبیت‌ها در پردازنده نشان می‌دهد که به دنبال آن هر چند سال یکبار تعداد کیوبیت‌های قابل کنترل به طور نمایی دو برابر می‌شود. از آنجایی که ابعاد فضای هیلبرت بار دیگر با تعداد کیوبیت‌ها به صورت نمایی مقیاس می‌شود، شاهد رشد نمایی دوگانه در راستای محور عمودی هستیم. زیرشکل (سمت چپ پایین) یک رایانه کوانتومی تله یونی با یک ، دو ، سه، شش و ده کیوبیت را نشان می‌دهد. شکل گرافیکی دوم تله یون NIST است که ممکن است در سال ۲۰۲۲، هزار کیوبیت درهمتنیده را پوشش دهد. شکل گرافیکی سوم طرحواره‌ای از ساختار گرافن است که ممکن است دارای 10^6 کیوبیت درهمتنیده باشد. شکل گرافیکی آخر (بالا سمت راست) الگوریتم شور است که بر روی یک رایانه‌ای کوانتومی حاوی یک تیلیارد کیوبیت اجرا خواهد شد. این نمودار حاکی از آن است که در پنجاه سال آینده، 3×10^{11} مرتبه بزرگی از فضای هیلبرت قابل دسترس خواهد بود.

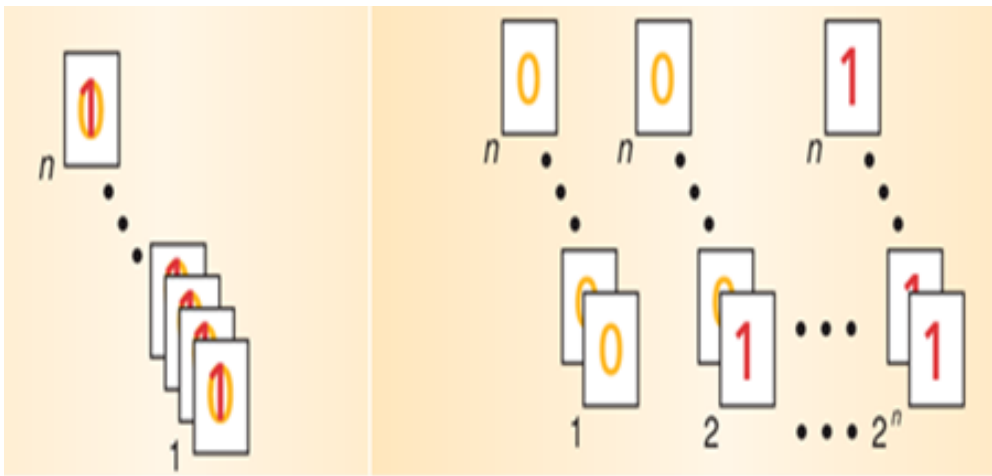
۲-۶ توازی کوانتومی

اولین تفاوت مهم رایانه کوانتومی با رایانه کلاسیک این است که یک حافظه کوانتومی می‌تواند درآن‌واحد در تمام حالت‌های بالقوه خود قرار بگیرد. این خصلت ناشی از برهم‌نهی حالت‌های کوانتومی است و اصطلاحاً توازی کوانتومی خوانده می‌شود. هرگاه هر حالت $|s_0,s_1,\cdots,s_{n-1}\rangle$ را برای کد کردن عددِ nبیتی $s=(s_0,s_1,\cdots,s_{n-1})$ به کار ببریم، درکلی‌ترین حالت، حالتی مثل،

$$|\psi\rangle=\sum_{s=0}^{2^n-1}\alpha_s|s\rangle$$

حالتِ توصیف‌کننده یک حافظه n بیتی است. بنابراین هرگاه حافظه را در حالت $|\psi\rangle$ قرار دهیم، مثل این است که هم‌زمان آن را در تمام حالت‌های $|s\rangle$ قرار داده‌ایم. البته واضح است که هرگاه حافظه را در پایه محاسباتی یعنی همان پایه sها (متشکل از 0ها و 1ها) اندازه‌گیری کنیم، تنها یکی از مقادیر s با احتمال $|\alpha_s|^2$ به دست خواهد آمد (که مقداری کلاسیکی است). در اصطلاح می‌گوییم اندازه‌گیری امری برگشت‌ناپذیر است که یک حالت برهم‌نهی را به یک حالت کلاسیک تصویر می‌کند(Nielsen, 200)..

بنابراین توازی کوانتومی اگرچه یک خاصیت مهم حافظه است ولی این خاصیت را می‌بایست باظرافت مورد بهره‌برداری قرار داد. درواقع می‌توان یک بیت کلاسیک را مشاهده کرد و از این طریق از خطای ایجادشده در آن آگاهی یافت ولی یک بیت کوانتومی را به‌راحتی نمی‌توان مشاهده کرد، زیرا مشاهده آن منجر به فرو کاهش و از بین رفتن حالت اولیه می‌شود(dousti, 1400).



شکل (۲): توازی کلاسیکی در برابر توازی کوانتومی: به منظور دستیابی به قدرت محاسباتی ناشی از توازی کوانتومی در 300 پردازشگر کوانتومی به 2^{300} پردازشگر کلاسیکی نیاز داریم. از آنجایی که این عدد از تعداد ذرات درون کیهان نیز بیشتر است بعضاً گفته می‌شود که رایانش کوانتومی باعث افزایش اختر‌فیزیکیِ قدرت محاسباتی خواهد شد.

۲-۷ الگوریتم کوانتومی

الگوریتم کوانتومی در ساده‌ترین شکل آن به مجموعه‌ای از گیت‌های کوانتومی متوالی گفته می‌شود که بر روی یک حالت معین اولیه اثر می‌کنند و چنان تنظیم‌شده‌اند که حالت نهایی چنان باشد که پس از اندازه‌گیری‌های سنجیده‌ای روی آن، جواب یک مسئله معین را با احتمال بسیار خوب در برداشته باشد. درواقع یک الگوریتم کوانتومی درست مانند یک الگوریتم کلاسیک است که می‌توان با استفاده از آن مجموعه‌ای از تصمیم‌گیری‌های مختلف را به رایانه کوانتومی فهماند و یک مسئله **الگوریتم پذیر** را با بهره بردن از مزیت‌های دنیای کوانتوم حل کرد. مزیت الگوریتم کوانتومی

این است که مسئله‌های قابل‌حل (الگوریتم پذیر) در زمان کمتری نسبت به هر الگوریتم کلاسیک، حل می‌شوند(dousti, 1400).

با توجه به اصل توازی که در بالا به آن اشاره شد و همچنین ویژگی درهم‌تنیدگی که یک خاصیت غیرموضعی و خاصه کوانتومی است، رایانه کوانتومی می‌تواند یک تابع را برای تعداد نمایی از متغیرها محاسبه کند؛ به‌عبارت‌دیگر ازنقطه‌نظر تئوریِ پیچیدگی[۱]، یک مسئله در کلاس NP را به مسئله‌ای در کلاس P تبدیل کند[۲]. همچنین یک گیت کوانتومی را به‌طور هم‌زمان بر روی تمامی ورودی‌هایی که در حالت برهم‌نهی[۳] قرار دارند، بزند. بنابراین یک محاسبه را به‌طور هم‌زمان و غیرموضعی[۴] بر روی تمامیِ داده‌های ورودی انجام دهد. برای مثال مسئله بهینه‌سازی و یافتن کمینه جهانی[۵] یک تابع را در نظر بگیرید. ازآنجایی‌که رایانه کوانتومی می‌تواند یک محاسبه را به‌طور هم‌زمان بر روی تمام داده‌های ورودی انجام دهد، بر مبنای الگوریتم کمینه‌سازی دور–هویر[۶] (که تعمیمی از الگوریتم جستجوی گرور[۷] است) می‌توان اکسترمم جهانی را به‌طور مستقیم (و نه با مقایسه اکسترمم‌های موضعی[۸]) پیدا کرد(dousti, 1400). برخی از الگوریتم‌های کوانتومی معروف و پیچیدگی زمانی آن‌ها در **Error! Reference source not found.** لیست شده‌اند.

[1] Complexity theory

[۲] البته رایانه کوانتومی همیشه در این کار موفق نیست. مثلاً در مسئله یافتن زیرگروه‌های پنهانِ غیرآبلی تنها در چند گروه خاص غیرآبلی این اتفاق رخ می‌دهد. بنابراین نمی‌توان ادعا کرد که در رایانش کوانتومی P=NP است.

[3] Superposition

[4] Non-local

[5] Global

[6] Durr-Hoyer

[7] Grover

[8] Local

جدول(۲): برخی از الگوریتم‌های کوانتومی معروف به همراه مقایسه پیچیدگی زمانی حل آن‌ها به روش کلاسیکی و کوانتومی

الگوریتم کوانتومی	پیچیدگی زمانی کلاسیکی	پیچیدگی زمانی کوانتومی[1]
جستجو در یک مجموعه نامنظم	N	$\sqrt{N}$
تجزیه یک عدد به عوامل اول	$e^{1.9N^{\frac{1}{3}}(\log N)}$	N^{3}
لگاریتم گسسته	$e^{O(\log N)}$	$(\log N)^3$
معادلهٔ پل	----------	$poly(N)$
تصدیق ضرب ماتریسی	N^{2}	$N^{\frac{5}{3}}$
مسئله جمع زیرمجموعه‌ها	$2^{0.291N}$	$2^{0.241N}$
مسئله زیرگروه‌های پنهان آبلی	N	$\log N$
مسئله زیرگروه پنهانِ غیر آبلی	N	$\log N$
حل دستگاه معادلات خطی[2]	$\sqrt{N\kappa}$	$\sqrt{(\log N)\kappa}$
جابجایی ماتریس‌ها[3]	KN^{2}	$K^{4/5}N^{9/5}$

[1] در اینجا بیشتر به بحث پیچیدگی زمانی توجه می‌کنیم. پیچیدگی‌های دیگری نیز وجود دارند. مثلاً با چند کیوبیت و چند گیت می‌توان یک الگوریتم کوانتومی را اجرا کرد. این نوع از پیچیدگی‌ها با معرفی الگوریتم‌های جدیدتر و هوشمندانه‌تر به طور روزانه در حال تغییر و به روزرسانی هستند.

[2] در اینجا κ تفاوت بین بزرگ‌ترین ویژه‌مقدار با کوچک‌ترین ویژه‌مقدار در یک ماتریس هرمیتی $N \times N$ است. هر چه این عدد بزرگ‌تر باشد مرحله معکوس کردن ماتریس در حل معادلات خطی دشوارتر می‌شود. زیرا در κهای بزرگ به تعداد بیشتری ویژه‌مقدار نزدیک به صفر نیاز خواهیم داشت.

[3] در اینجا K تعداد ماتریس‌های جابه‌جاشونده (یعنی $[A,B]=0$) می‌باشد.

جابجایی گروه‌ها	N	$N^{\frac{2}{3}}$
تبدیل فوریه	$N\,2^N$	$\log N$

۲–۸ نظم نوین جهانی

فشردگی زمانی و مکانی ایجادشده به برکت علوم و فناوری‌های جدید و برهم زن، پروسه جهانی‌شدن را سرعت بخشیده و جهان شبکه‌ای شده و درهم‌تنیده گونه‌های نوین از تأثیرگذاری و تأثیرپذیری را در قالب شبکه‌های بزرگ و جهانی اجتماعی، اقتصادی، سیاسی، نظامی و فرهنگی ممکن نموده است. تحولات فناورانه همگام با تحول سیستم روابط بین‌الملل به سمت پیچیدگی و آشوب ایده ضرورت تحقق نظم جدید جهانی را قوت بخشید (shelton, 1999). به‌طوری‌که می‌توان گفت نوعی از کنترل اجتماعی جدید که این بار در آن اجتماع مفهومی جهانی می‌یابد و امنیت بشری در آن مفهومی موسع خواهد داشت محقق و اعمال خواهد شد. کنترل اجتماعی به ابزارها و روش‌هایی اطلاق می‌گردد که برای وادار کردن فرد به انطباق با انتظارات گروه معینی یا «کل جامعه» به کار می‌رود (کوئن،۱۳۷۹).

با توجه به رفتار دولت ایالات‌متحده که همچنان یکجانبِ گرایی و نظام تک‌قطبی در آن مشهود است طبیعتاً نظم آتی مدنظر این کشور و متحدین نیز می‌بایست مطلوب رشد سیستمی همان تمدن و تأمین‌کننده منافع راهبردی این کشور باشد. لذا هرگونه رفتار غیرهمسو در دوره گذار به سمت نظم جدید جهانی به‌شدت مورد تازش ترکیبی این کشور و هم‌پیمانان آن در ناتو قرار می‌گیرد. در نظم جدید جهانی علوم و فناوری‌های قدرت ساز نقش بی‌بدیلی برای ارتقاء قدرت و تاب‌آوری را خواهند داشت. یک از حوزه‌های بسیار مهم در تعیین زیست‌بوم علوم و فناوری‌های جهانی، علوم و فناوری‌های کوانتومی است. علوم و فناوری‌های کوانتومی توسط رهبران بسیاری از کشورها مورد استقبال قرارگرفته است. رهبران چین، روسیه، ایالات‌متحده آمریکا، کانادا، انگلستان، اتحادیه اروپا و .. در بالاترین سطح، به پتانسیل راهبردی علوم و فناوری کوانتومی برای ارتقا ابعاد اقتصادی و نظامی قدرت ملی پی برده‌اند. یکی از کشورهایی که می‌توان گفت بیشترین حجم سرمایه گزاری را روی علوم و فناوری‌های کوانتومی انجام داده است چین است(quantum h, 2018).

این جاه‌طلبی‌های کوانتومی با اهداف راهبردی چین در ارتباط است، که تبدیل به یک ابرقدرت علمی و فناوری شود. به‌جای جذب فناوری‌های خارجی در دستیابی به نوآوری بومی، قصد دارد نوآوری‌های تحول‌آفرین، حتی نوآوری "رادیکال" را در فن‌آوری‌های نوظهور راهبردی نظیر هوش مصنوعی یا بیوتکنولوژی به دست بیاورد. همان‌طور که چین در حال پیشرفت یک استراتژی ملی برای تلفیق فناوری‌های نظامی–ملی است ، این فن‌آوری‌های حیاتی همچنین برای طیف وسیعی از کاربردهای دفاعی استفاده می‌شود. درحالی‌که همکاری‌های بین‌المللی می‌تواند سبب پیش بردن پیشرفت‌های علمی جهانی باشد، حساسیت و اهداف راهبردی مرتبط با این فناوری‌ها در چین می‌تواند در بدترین شرایط این تعهدات را تضعیف کند، به‌گونه‌ای که در آینده چنین نوآوری‌های به وجود آمده در چین، منحصر به چین شود. چین به‌طور واضح خواستار رهبری "انقلاب کوانتومی دوم" است که با ظهور این فناوری‌های جدید اتفاق می‌افتد. چین به‌طور گسترده رمزنگاری کوانتومی قابل‌اعتماد و ارتباطات کوانتومی را برای ایجاد شبکه‌های جدید که حداقل به‌طور نظری، "غیرقابل نفوذ" خواهد بود، به کار می‌برد.

در دهه‌های آینده، تحقق محاسبات کوانتومی، قابلیت‌های محاسباتی بی‌نظیر با کاربردهای قابل‌توجه که شامل شکستن انواع سیستم‌های رمزگذاری است، ایجاد می‌کند. اگرچه چین نسبتاً دیر وارد مسابقه شد، اما این‌یک مسابقه ماراتن خواهد بود نه مسابقه سرعت، که در دهه‌های آینده ادامه خواهد داشت و دانشمندان چینی که منابع تقریباً نامحدود دریافت می‌کنند، و اخیراً یک رکورد جهانی برای بیت‌های کوانتومی درهم‌تنیده (qubits) ثبت کردند، در بلندمدت به بقیه رقبا خواهند رسید. پیشرفت‌های چین در علوم کوانتومی می‌تواند بر تعادل نظامی و استراتژیک آینده تأثیر بگذارد و حتی از فناوری‌های معمول نظامی ایالات‌متحده نیز پیشی بگیرد. اگرچه پیش‌بینی مسیرها و زمان‌بندی‌ها برای تحقق آن دشوار است، این فناوری‌های دوگانه کوانتومی می‌تواند ستون‌های کلیدی قدرت نظامی ایالات‌متحده را خنثی کند و به‌طور بالقوه مزایای تکنیکی مرتبط با روش‌های اطلاعات محور برای جنگ را که به‌وسیله مدل ایالات‌متحده شکل می‌گیرد، تضعیف کند. همان‌طور که چین حساس‌ترین ارتباطات نظامی، دولتی و تجاری خود را به شبکه‌های کوانتومی تغییر می‌دهد، این انتقال می‌تواند امنیت اطلاعات را ارتقا دهد، شاید جاسوسی سایبری و توانایی‌های اطلاعاتی ایالات‌متحده را خنثی نماید. درعین‌حال، این انتقال ملی به رمزنگاری کوانتومی می‌تواند اطمینان حاصل کند که چین در برابر تهدیدهای آینده، ایمن خواهد بود، تهدیدهایی که یک کامپیوتر

کوانتومی در آینده می‌تواند با شکستن انواع مختلف رمزنگاری توسط الگوریتم شور ایجاد نماید . در مقابل، ایالات‌متحده هنوز در پیاده‌سازی این‌چنین راه‌حل‌ها، یا جایگزین‌هایی از رمزنگاری پسا کوانتومی به این اندازه پیشرفت نکرده است(quantum h, 2018).

۱. روش‌شناسی

در پژوهش حاضر از روش تحقیق توصیفی-تحلیلی از نوع پیمایشی استفاده‌شده است. در این پژوهش، گردآوری اطلاعات به دو صورت انجام پذیرفته‌شده است:

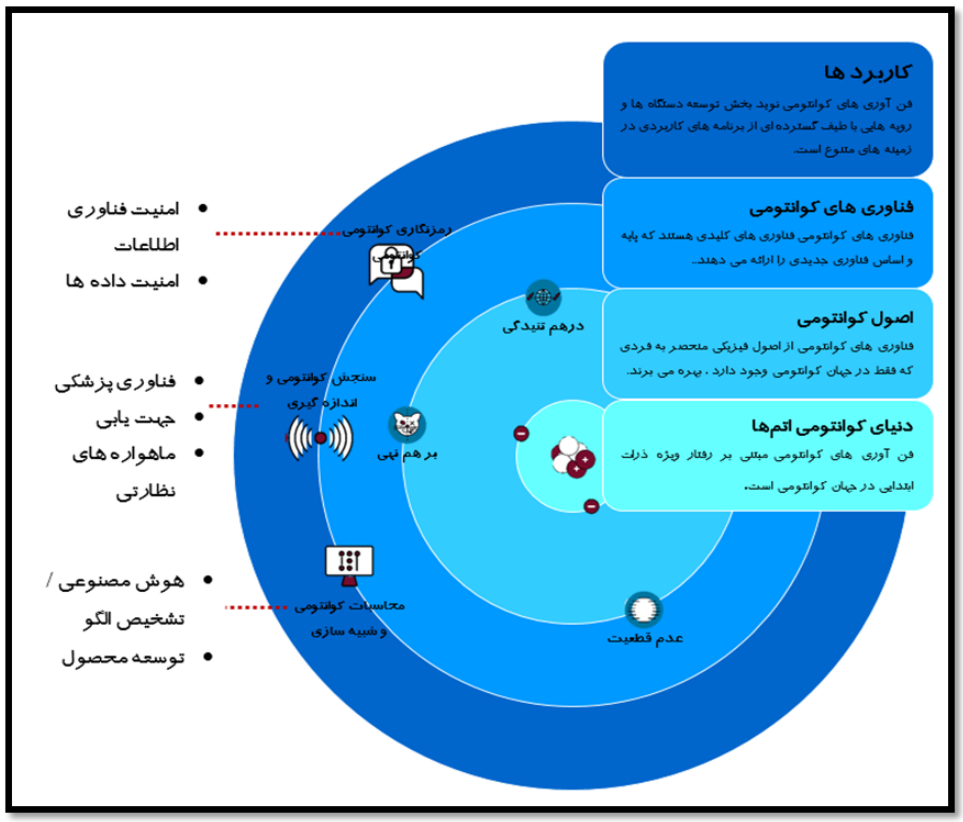
۱- اسناد، مدارک، مطالعات علمی و کتاب‌ها و مقاله‌های مرتبط: منابع اصلی این تحقیق، کتاب‌ها، مقالات و اسناد مرتبط با موضوع می‌باشند.

۲- نظرسنجی از نخبگان: از نخبگان با تحصیلات مرتبط در انجام تحقیق و پر کردن پرسشنامه‌ها و همچنین برگزاری جلسات مشترک کمک گرفته‌شده است.

نوع تحقیق: این تحقیق از نوع کاربردی-توسعه‌ای است.

۲. یافته‌ها و تحلیل داده‌ها

بر اساس موارد ذکرشده می‌توان این‌گونه ادعا نمود که نظم نوین جهانی در بسترهای مختلف متأثر از حوزه‌های مختلف علوم و فناوری‌های کوانتومی و همگرایی این حوزه با سایر حوزه‌ها و مخصوصاً فضای سایبری خواهد بود، که با ایجاد برتری کوانتومی برای صاحبان این حوزه ، منجر به نبردهای کوانتومی و درنهایت راهبری هوشمند در مسیر ایجاد نظم جدید جهانی خواهد گردید و امتی که بتواند هوشیارانه سراغ این حوزه برود حتماً به برکات بی‌نظیری دسترسی پیدا خواهد کرد. درشکه (۳) تأثیر علوم و فناوری‌های کوانتومی و کاربردهای آن در سایر فناوری‌ها بررسی‌شده است.



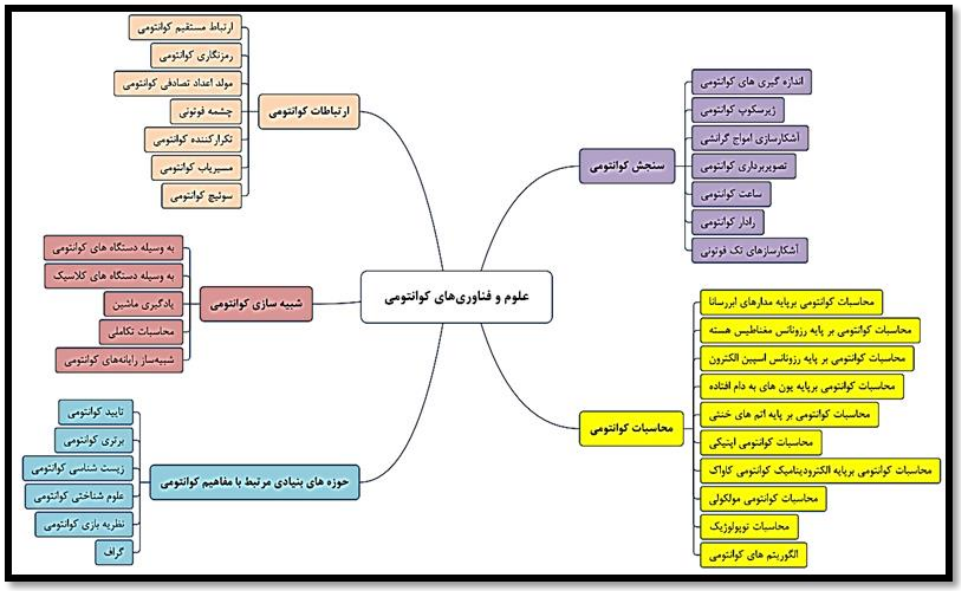
شکل(۳): تأثیر علوم و فناوری‌های کوانتومی و کاربردهای آن در سایر فناوری‌ها

با توجه به اینکه علوم و فناوری‌های کوانتومی یک حوزه زیربنایی است که به واسطه‌های کارکردهای متنوع خود، عرصه‌های مختلفی را تحت‌الشعاع قرار می‌دهد، لذا درخت علوم و فناوری‌های کوانتومی موردمطالعه و بررسی قرار گرفت که به ۵ دسته زیر تقسیم‌بندی شد:

- **محاسبات کوانتومی**
- **شبیه‌سازی کوانتومی**
- **سنجش کوانتومی**
- **ارتباطات کوانتومی**
- **حوزه‌های بنیادی مرتبط با مفاهیم کوانتومی**

و درخت فناوری‌های کوانتومی تا سطح ۳ ترسم گردید که در شکل (٤) قابل‌مشاهده است(dousti , 1401).

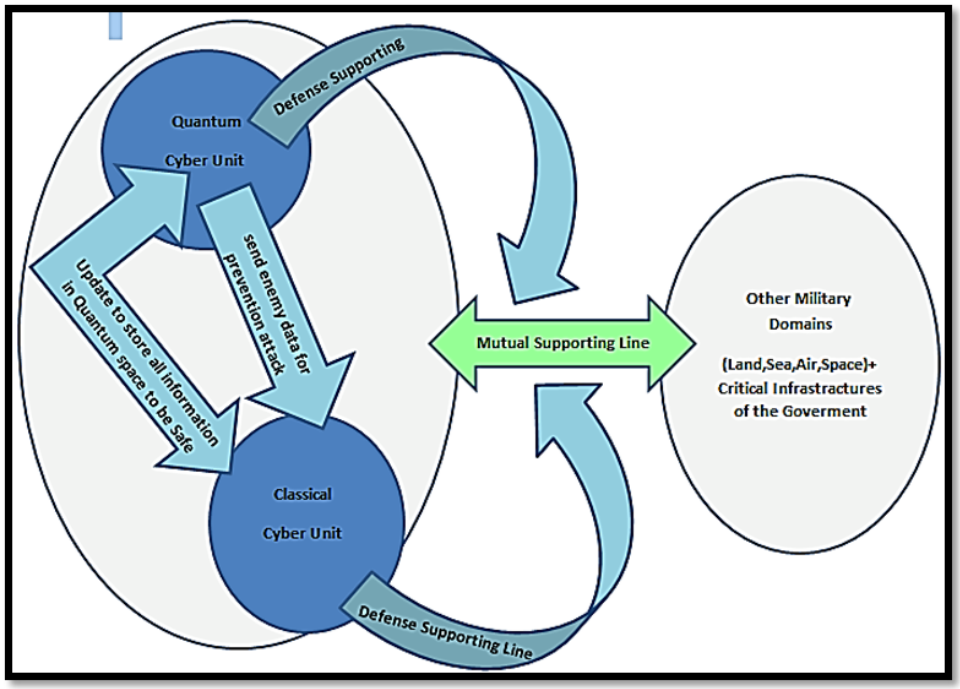
شکل (٤): درخت فناوری‌های کوانتومی تا سطح سوم



برای فضای سایبر دو رویکرد وجود دارد که عبارت‌اند از رویکرد کوانتومی و رویکرد کلاسیک، که در شکل (۵) ترسیم‌شده است. همان‌طور که در شکل (۵) قابل‌مشاهده است، در رویکردهای ارائه‌شده ما ۵ فضای نبرد زمین ، هوا ، دریا ، فضا و فضای سایبر به همراه بستر ارتباطی MSL را برای ارتباطات نرم‌افزاری و سخت‌افزاری بین ٤ عرصه دیگر با فضای سایبر ، بین تجهیزات سایبری و فرماندهی و کنترل نظارت خودشان همانند C4ISR را داریم که در جنگ مهم‌ترین نقش را دارد و چنانچه توسط دشمن منهدم یا در اختیار گرفته شود عملکرد و واکنش سایر حوزه نیز مختل می‌شود و منجر به شکست خواهد شد (همانند حمله اسراییل به نیروگاه اتمی سوریه که ابتدا خطوط راداری را مختل کرد سپس هم‌زمان در گام بعدی جنگنده‌های آن اقدام به بمب باران و انهدام نیروگاه کردن) لذا حیاتی‌ترین، آسیب‌پذیرترین و

اثرگذارترین وظیفه حفاظت از MSL است. فضای سایبر کلاسیک قادر به حافظت از MSL و داده‌های حیاتی (مربوط به زیرساخت‌های حیاتی و نظامی در حوزه آفند و پدافند و..) نخواهد بود چرا که بیشتر دولت‌های ملی به خاطر تئوری انتخاب منطقی مایل به نادیده گرفتن قوانین بین‌المللی سایبری بوده و معتقدند که اطاعت از قواعد بین‌المللی در جنگ سایبری مزایای کمتری نسبت به هزینه دارد بنابراین از آن تبعیت نمی‌کنند (همانند حمله روسیه به استونی) درنتیجه بسیاری از کشورها در معرض جنگ سایبری هستند و امنیت جهانی اینترنت در شرایط سختی است (than, 2017).

شکل (۵): رویکرد کوانتومی برای فضای سایبری



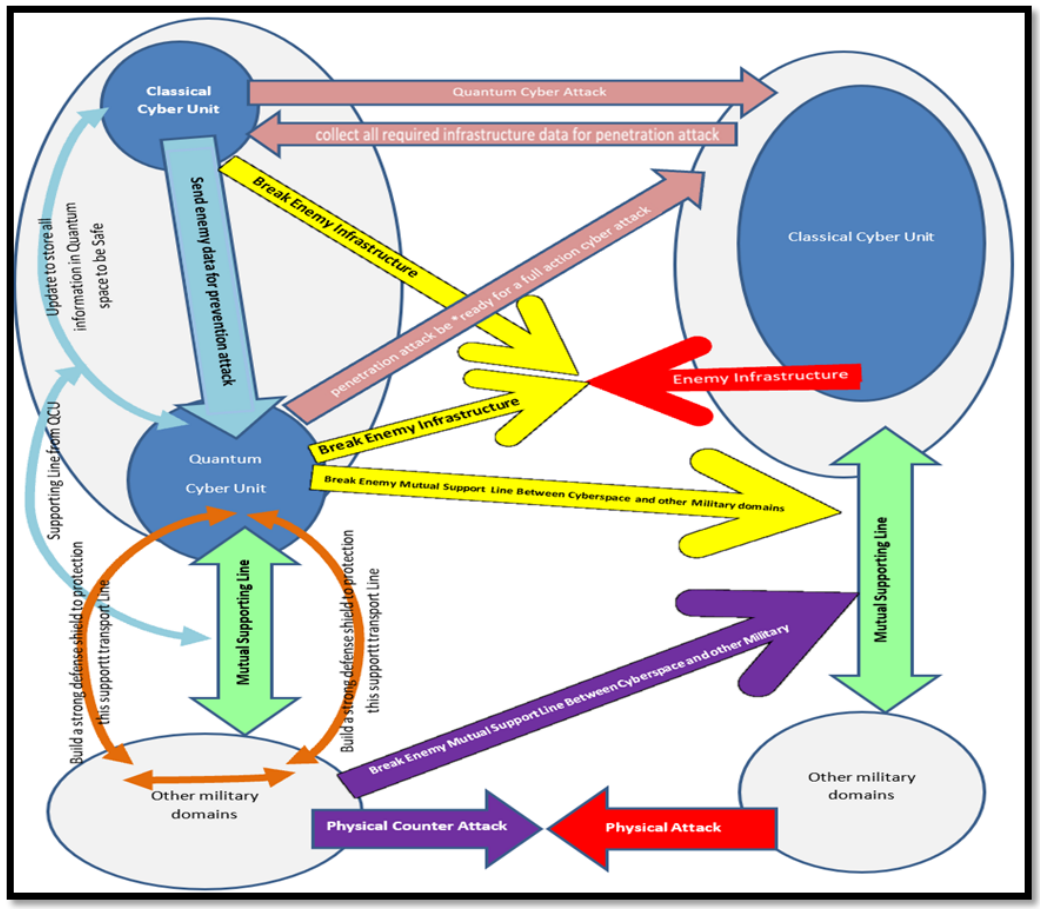
بعلاوه، از سوی دیگر در بررسی‌های علمی کلید اصلی موفقیت علیه جنگ سایبری بستگی به شکستن خط امنیتی فضای سایبری دشمن دارد لذا چنانچه دشمن دارای واحد سایبر کوانتومی QCU باشد قادر است این قابلیت را کسب نماید(کما اینکه قابلیت‌های الگوریتم‌های کوانتومی

همانند Shor (Hughes, 2021) و گرور قادرند الگوریتم‌های رمزنگاری سایبری کلاسیک را به‌آسانی بشکنند) و از سوی دیگر عکس قضیه نیز صادق است یعنی چنانچه از الگوریتم‌های کوانتومی برای رمزنگاری استفاده شود امکان شکستن فعلاً در زمان مؤثر میسر نیست(than, 2017).

درنتیجه هر کشوری برای حفظ امنیت خود و تأمین امنیت ملی‌اش باید به QCU دست یابد.

درصورتی‌که بین دو کشور جنگ شکل بگیرید و یک کشور فقط فضای سایبر کلاسیکی داشته باشد (Hughes, 2021) و کشور دیگر فضای سایبر تلفیقی کلاسیک و کوانتوم داشته باشد کشوری که دارای فضای سایبر تلفیقی است دست برتر را خواه داشت، که در شکل (٦) صفحه بعد قابل‌مشاهده است.

شکل (٦): نبردهای سایبری با محوریت کوانتوم



در مدل ارائه‌شده ۳ وظیفه اصلی بر عهده QCU و CCU قرار دارد.

الف)

۱. ارائه اطلاعات هوشمند برای استفاده در حملات پیرامون دفاع و مقابله بانفوذ دشمنان به CCUو زیرساخت‌های حیاتی که در این بخش QCUو CCU باهم دفاع می‌کنند.

۲. شکستن و آسیب زدن و در تعاقب در اختیار گرفتن MSL دشمن (شامل قطع ارتباط ،رمزگشایی و در اختیار گرفتن کنترل آن ، سرقت اطلاعات و....)

-عملکرد ما در حالت پدافندی

در این وضعیت همان‌طور که در مدل ترسیم‌شده دشمن با استفاده از زیرساخت‌های و سلاح‌های سایبری (فعلاً کلاسیک)خود به‌منظور نفوذ، سرقت اطلاعات، ایجاد اختلال یا انهدام زیرساخت‌های حیاتی سایبری به‌ویژهMSL و داده‌ها اقدام به حمله می‌کند در این حالت واحد سایبر کلاسیک ما به کمک واحد سایبر کوانتومی اقدام به دفاع و محافظت از سرمایه‌های حیاتی سایبری و MSL می‌کند.

-عملکرد ما در حالت آفندی در حین حمله دشمن و به عبارتی دفاع فعال (Proactive Defence)

در حین حمله دشمن با استفاده از هر دو فضا کلاسیک و کوانتومی اقدام به رمزگشایی رمزنگاری دشمن کرده و در مقابل حمله سایبری به زیرساخت‌های سایبری و خطوط MSL دشمن می‌کند(than, 2017).

ب)

۱.انتقال اطلاعات حساس از CCU به QCU و محافظت از آن‌ها با رمزنگاری کوانتومی از آن‌ها توسط QCU

۲. محافظت از MSL خودی باز از طریق رمزنگاری و همچنین رمزگشایی و مقابله با سایر حملات همانند حمله DDos از سوی دشمن

عملکرد در این حالت حوزه پدافندی است. در مدل این حوزه وظیفه محافظت از داده با انتقال از بخش کلاسیک به بخش کوانتومی و رمزنگاری کوانتومی بر روی آن‌ها صورت می‌دهد همچنین ارتباطات را با انتقال کوانتومی و رمزنگاری داده‌های در حال انتقال محافظت اصلی از زیرساخت‌ها و داده‌های حیاتی و MSL را به عمل می‌آید.

ج) حمله سایبری ،جاسوسی (کسب اطلاعات حیاتی) و نفوذ در مخالفان سایبری

عملکرد در این حوزه آفندی است. در مدل این حوزه وظیفه آفند(نفوذ،جمع‌آوری داده‌های حیاتی ،سرقت،رمزگشایی و...) از طریق فضای سایبر کلاسیک و به‌صورت ویژه‌فضای کوانتومی که از مزیت پردازش قوی،رمزگشایی و جمع‌آوری صورت می‌گیرد.

همچنین در خصوص حملات سایر حوزه‌های نظامی

۱. پاسخ متقابل به حملات فیزیکی
۲. شکستن و آسیب زدن به MSL دشمن

۳. بحث؛ نتیجه‌گیری و پیشنهادها

اگر چین موفق به پیشتازی در محاسبات کوانتومی شود، آنگاه بهره‌برداری از چنین قابلیت‌های محاسباتی قدرتمندی می‌تواند مزیت راهبردی را به ارمغان بیاورد و سیستم‌های اطلاعاتی حساس آمریکا را در معرض خطر جدی قرار می‌دهد. در همین حال، ظهور ناوبری کوانتومی ممکن است به استقلال بیشتری از سیستم‌های مبتنی بر فضا منجر گردد، و تحقق رادار کوانتومی، تصویربرداری و سنجش، دامنه هوشیاری و هدف‌گیری را افزایش خواهد داد، که به‌طور بالقوه سرمایه‌گذاری‌های ایالات‌متحده در زمینه فناوری‌های پنهان‌کار (رادار گریز) را تضعیف کرده و حتی منجر به ره‌گیری زیردریایی‌ها خواهد شد. درمجموع، این پیشرفت‌ها می‌تواند ادامه حضور ارتش چین (PLA) را به‌عنوان یک رقیب واقعی در این حوزه‌های فناورانه جدید قدرت نظامی پشتیبانی کند.

ایالات‌متحده باید مسیر پیشرفت‌های چین در این فناوری‌ها و وعده کاربردهای بالقوه نظامی و تجاری آن‌ها را تشخیص دهد. در پاسخ، ایالات‌متحده باید بر تلاش‌های موجود و افزودن بر آن‌ها تکیه کند تا بتواند به‌عنوان رهبر یا حداقل یک مدعی اصلی، در عرصه توسعه فناوری‌های کوانتومی از طریق تقویت اکوسیستم نوآوری خود باقی بماند. ایالات‌متحده باید اطمینان حاصل کند که تحقیقات و توسعه‌های علمی و کاربردی در زمینه علوم و فنون کوانتومی، بودجه کافی و پایدار دریافت می‌نماید. در این فرآیند، بررسی پارادایم‌های جدید برای مشارکت عمومی و خصوصی نیز حیاتی خواهد بود. در حینی که به بررسی گزینه‌های رمزنگاری پساکوانتومی می‌پردازد، دولت ایالات‌متحده باید شروع به ارزیابی هزینه‌ها و زمان‌بندی‌های مرتبط با انتقال گسترده نظامی و دولتی

از اشکال شایع امروزی رمزگذاری به یک رژیم جدید نماید، که ممکن است نیاز به تغییرات قابل‌توجهی در زیرساخت‌های اطلاعاتی اساسی داشته باشد. هرچند که تأثیر کامل این انقلاب کوانتومی دوم در آینده مشخص خواهد شد و شک و تردیدهایی نیز در این زمینه است، ایالات‌متحده باید از طریق استفاده از مزایای موجود در نوآوری، ریسک‌های طولانی‌مدت غافلگیری فنّاورانه در این حوزه را کاهش دهد.

٤. منابع و مآخذ

١. دوستی مطلق، نصیب الله.(١٣٩٦). **اولین قدم برای یادگیری فیزیک کوانتوم** ،چاپ اول، تهران، برتراندیشان.

٢. دوستی مطلق، نصیب الله، کریمی، محمد.(١٤٠١). **مقدمه‌ای بر محاسبات ابری کوانتومی** ،چاپ اول، تهران، دانشگاه عالی دفاع ملی.

٣. دوستی مطلق، نصیب الله، جادریان، مرتضی، دیوبند، اشکان.(١٤٠١). **درخت فناوری‌های کوانتومی: حوزه‌های بنیادی مرتبط با مفاهیم کوانتومی** ،چاپ اول، تهران، دانشگاه عالی دفاع ملی.

٤. کانیا، السا، کاستلو،جان.(١٤٠١). **هژمونی کوانتومی: بلندپروازی‌های چین و چالش رهبری نوآوری ایالات‌متحده**، ترجمه دوستی مطلق، نصیب الله ، چاپ اول، تهران، موسسه فرهنگی و هنری عصر اطلاعات.

٥. اسکوایزر، یوئن.(١٣٩٤). **اسرار جهان کوانتومی**، ترجمه کمالدین سید یعقوبی، چاپ چهارم، تهران، سروش.

1. M. A. Nielsen, Isaac L. Chuang(2000), Quantum Computation and Quantum Information, Cambridge University Press.
2. Knight, P., & Walmsley, I. (2019). UK national quantum technology programme. *Quantum Science and Technology*, *4*(4), 040502.
3. Kywe, Than (2017). Modern Military Model: The Quantum Cyber Unit: A Tripartite Model Of The Military System

4. Raymer, M. G., & Monroe, C. (2019). The US National Quantum Initiative. *Quantum Science and Technology*, *4*(2), 020504.
5. EQUS. (2018). Australian research council center of excellence for engineered quantum systems.
6. Informatica, C. W. (2019). Quantum strategic plan.
7. USTC. (2016). quantum project. *University of Science and Technology of China*.
8. center, R. q. (2018). Quantum technologies in Russia.
9. Iopscience. (2019). Quantum information science and technology in Japan.
10. Commission, E. (2019). Quantum Technologies FET Flagship.
11. IBM. (2017). Theory of quantum computing and information group IBM.
12. Microsoft. (2018). Microsoft Research – Emerging Technology, Computer, and Software Research.
13. Shelton, C. (1999). Quantum leaps: 7 skills for workplace recreation. Routledge.

Hughes-Castleberry,k(2021). **Quantum Warfare.** **https://thequantuminsider.com/2021/08/07/quantum-warfare/**