

اعلام کرد. اگرچه این مجموعه از الگوریتم‌ها روز در برابر هم‌روش‌های رمزگشایی منتشر ششده نفوذناپذیر هستند، اما ممکن است یک یا چند مورد از آن‌ها در آینده آسیب‌پذیر شوند. چنین نگرانی‌هایی در پی تحقیقات جدیدی که نشان می‌دهد رمزگذاری عمومی ممکن است هرگز در برابر حملات کوانتومی کاملاً ایمن نباشد، فوریت بیشتری پیدا کرده‌است.

مانند سایر فناوری‌های جدید و قدرتمند، محاسبات کوانتومی هم حائز توان‌مان ویژگی‌های نویدبخش و خطرناک جدید است. رایانه‌های کوانتومی علاوه بر سرعت اطلاعات در مقیاس بزرگ، اختلالات اقتصادی و نقض اطلاعات می‌توانند برای اهداف مخربی مانند شبیه‌سازی و سنتز سلاح‌های شیمیایی یا بهینه‌سازی مسیر پرواز گروهی از پهپادها استفاده شوند. همانند هوش مصنوعی، احتمال سوءاستفاده از فناوری کوانتومی هم سبب ایجاد سؤالاتی درباره نهاد مسئول کنترل این خطرات ونحوه کاهش آن‌ها ایجاد کرده است.ت سیاست‌گذاران باید تعیین کنند که چگونه می‌توانند منافع اقتصادی و اجتماعی این فناوری را به حداکثر رسانده و درعین حال خطرات را حداقل کنند. یافتن بهترین راه‌ها برای دستیابی به این موازنه مستلزم یک بحث جدی در جامعه مدنی و درک عموم از دستاوردها و آسیب‌های بالقوه فناوری است. آینده‌های متعددی برای جهانی با رایانه‌های کوانتومی وجود دارد. در بهترین آن‌ها دموکراسی‌های لیبرال هم توسعه این فناوری و هم مدیریت جمعی آن را رهبری خواهند کرد. اما بدترین سناریو این است که ایالات متحده و شرکای بین‌المللی آن، با انفعال با اقدامات ناکافی، سلطه بر این فناوری جدید را به چین و دیگر کشورهای خودکامه واگذار می‌کنند.

جهش کوانتومی

تکمیل ساخت رایانه‌های کوانتومی یک پروژه جسورانه، جاه‌طلبانه و چندوجهی است و هیچ شرکت یا کشوری نمی‌تواند به‌تنهایی آن را انجام دهد. سیستم‌های اولیه امروزی به هزاران قطعه و ابزار تخصصی نیاز دارند. ساخت پیچیده و امکانات برودتی و تسلط در سطح جهانی در ده‌ها زمینه فنی که با میلیارد‌ها دلار سرمایه‌گذاری در تحقیق و توسعه پشتیبانی می‌شود. سیستم‌های نسل فردا به‌طرز محسوسی پیچیده‌تر خواهند بود. اگر ایالات متحده تمایل دارد پیش‌از این رقابت بوده و همراه با متحدان بین‌المللی خود، پیشرفته‌ترین سیستم‌های محاسباتی کوانتومی را بسازد، باید به فعالان حوزه کوانتومی اجازه دهد تا در سراسر بخش‌ها و مراکز با یکدیگر همکاری کنند. همکاری مؤثر می‌تواند به دموکراسی‌های لیبرال برتری قابل توجهی نسبت به کشورهای بسته‌تر و اقتدارگرا اعطا کند.

برای بسیاری از شرکت‌هایی که امروزه روی سیستم‌های کوانتومی کار می‌کنند، پردازنده‌های کوانتومی تاج مالکیت معنوی به شمارفته و به همین دلیل در کشوری که خود آن‌ها در آن تأسیس شده‌اند (و نه کشورهای دیگر) تولید می‌شوند: گوگل تراشه‌های کوانتومی را در ایالات متحده می‌سازد، مدارهای کوانتومی آکسفورد تراشه‌های کوانتومی را در انگلیس تولید می‌کنند، و آلیس و باب این کار را در فرانسه انجام می‌دهد. در تمامی موارد، این تراشه‌ها برای تحقیق و توسعه داخلی به کاررفته و فقط در برخی موارد، اشخاص ثالث اجازه دسترسی به نمونه‌های اولیه آن‌ها را دارند. همان‌طور که صنعت نیمه‌هادی نشان داده است حفظ مزیت تولید داخلی یک محصول راهبردی برای هر کشوری منافع ژئوپلیتیک دارد.

اما برای ساخت پردازنده‌ها و ادغام کامل سیستم‌های رایانه‌ای بصورت محلی، استعدادهای لازم نیز باید در دسترس باشند. این امر مستلزم همکاری بین نهادهای دولتی، صنایع و مؤسسات تحقیقاتی و آموزشی است. شرکت‌های محاسبات کوانتومی می‌توانند با به اشتراک گذاشتن نیازهای نیروی کار پیش‌بینی‌شده خود و ارائه فرصت‌های آموزشی ضمن کار، از این فرایند پشتیبانی کنند. از آنجایی‌که مجموعه مهارت‌های مورد نیاز برای محاسبات کوانتومی بسیار تخصصی است، برای هر کشوری امکان‌پذیر نخواهد بود که تمام استعدادهای مورد نیاز در این مسیر را ایجاد کند - و حتی ممکن است برای هیچ کشوری امکان‌پذیر نباشد. کار خود ما در محاسبات کوانتومی شامل همکاری با بیش از ۱۰۰ مؤسسه دانشگاهی و شریک صنعتی در سراسر ایالات متحده، اروپا و آسیا و اقیانوسیه است. برای ایالات متحده و متحدان آن عاقلانه خواهد بود که سیاست‌های ویزا، مهاجرت و کنترل صادراتی را اجرائی کنند که به شرکت‌های این بخش حیاتی اجازه می‌دهد تا با استعدادترین دانشمندان، مهندسان و تکنسین‌ها را جذب خود کنند. در ماه سپتامبر، وزارت بازرگانی ایالات متحده و با اعلام قوانین جدیدی که شامل معافیت صادراتی تلقی می‌شود، گام مهمی برای تسهیل اشتغال کارگران بین‌المللی بسیار ماهر در ایالات متحده برداشت. واشنگتن و شرکای بین‌المللی‌اش همچنین باید زنجیره‌های تأمین قوی را برای همه زیرسیستم‌ها و اجزایی ایجاد کنند که در محاسبات کوانتومی مورد استفاده قرار می‌گیرند. بسیاری از اجزای ضروری برای این کار در کشور‌های متفاوت در سراسر جهان تولید می‌شوند و این روند ادامه خواهد داشت، برای مثال ساخت کیوبیت‌های ابررسانا به بسیاری از ابزارهای مشابهی نیاز دارد که در تأسیسات ساخت نیمه‌رساناهای پیشرفته متعلق به شرکت‌های مانند اینتل و TSMC هم استفاده می‌شوند. این ابزارها در فرانسه، آلمان، هلند و ایالات متحده و سایر کشورها تولید می‌شوند. یخچال‌های برودتی هم نیاز به تخصص‌هایی دارند که تنها تعداد انگشت‌شماری از شرکت‌ها از آن برخوردارند که اکثر آن‌ها در انگلیس و اتحادیه اروپا مستقرند. اجرای دیگر، مانند الکترونیک کنترل و سیم‌کشی، توسط شرکت‌های تخصصی در اسرائیل، ژاپن و تایوان و همچنین در ایالات متحده و اتحادیه اروپا طراحی شده‌اند. هر کشوری ممکن است بر نحوه ساخت قطعات مختلف تسلط پیدا کند، اما کشور‌های هم‌فکر باید با هم کار کنند تا باازل کامل را به دست آورند و این فناوری را دور از دسترس دولت‌های مستبد نگه دارند.

برای اینکه محاسبات کوانتومی به پتانسیل کامل خود دست یابند، ذهن خلاق بسیاری از رشته‌های مختلف برای توسعه کاربردهای این فناوری مورد نیاز است. چندین تلاش اولیه برای تقویت یک زیست‌بوم توسعه‌دهنده وجود دارد، از جمله برنامه سنجش کوانتومی دارپا که پیشرفت به سمت حوزه‌های کاربردی بالقوه را اندازه‌گیری می‌کند و XPRIZE Quantum Applications که یک رقابت بین‌المللی سه‌ساله به ارزش پنج میلیون دلار برای تولید الگوریتم‌های محاسبات کوانتومی جدید برای چالش‌های دنیای واقعی است. منافع حاصله ناشی از ایجاد رابط‌ها برای دسترسی مستقیم توسط توسعه‌دهندگان نرم‌افزار، استفاده از این رابط‌ها برای مشکلات بسیار حائز اهمیت از سوی دانشگاهیان و رهبران کسب‌وکار و ارائه درون‌داد در باره ارزشمندترین چیزها برای مصرف‌کنندگان و جامعه مدنی خواهد بود.

مانند مسابقه فرود انسان‌سان روی ماه یا توالی‌یابی تمام ژن‌های موجود در ژنوم انسان، توسعه موفقیت‌آمیز و ایمن محاسبات کوانتومی به‌تنهایی توسط دانشمندان امکان‌پذیر نیست. این امر مستلزم تعهد ارائه عمومی و خصوصی منابع درطول نسل‌ها و استعدادها و دیپلماسی بین‌المللی دوراندیش است. رایانه‌های کوانتومی فرصت‌های فوق‌العاده‌ای را برای ایالات متحده و بسیاری از کشورهای دیگر در سراسر جهان ایجاد خواهند کرد. آن‌ها همچنین خطرات جدیدی از جمله احتمال سوءاستفاده و شوک‌های احتمالی به نظم جهانی خواهند داشت. اگر بتوان این خطرات را مدیریت کرد، پتانسیل استفاده از محاسبات کوانتومی برای تسریع پیشرفت انسان وجود دارد.

محاسباتی موجود آن را روشن کرد. بااین حال با کمپیوترهای کوانتومی، محققان ممکن است قادر به انجام محاسبات دشوار لازم برای یادگیری مکانیسم واکنش FeMoco باشند؛ امری که امکان طراحی کاتالیزورهای الهام‌گرفته از FeMoco را فراهم می‌کند و می‌تواند موجب ذخیره مقادیر زیادی از انرژی شود. مانند دیگر در این زمینه داروها هستند که مستلزم تعامل مؤثر مولکول‌های دارو با مولکول‌های داخل بدن می‌باشند. برای شبیه‌سازی رفتار سیتوکروم P=۴۵۰ خانواده‌ای از آنزیم‌ها که عمدتاً مسئول متابولیسم دارو و بنابراین نحوه پاسخ بیماران به داروها هستند - رایانه‌های کلاسیک به مقادیر عظیمی از قدرت محاسباتی نیاز دارند. اما با رایانه‌های کوانتومی، می‌توان این کار را بسیار کارآمدتر انجام داد و به نوآوری‌های مهمی در مبارزه با بیماری‌ز نیز نایل شد. محاسبات کوانتومی در صنایع شیمیایی و مواد نیز می‌تواند به طراحی باتری‌های کارآمدتر برای خودروهای برقی و همچنین عناصر غیرخورنده برای کشتی‌ها کمک کند. رایانه‌های کوانتومی همچنین می‌توانند به حل مشکل تبدیل راکتورهای هسته‌ای صنعتی از منبع انرژی پایدار کمک کنند. یکی دیگر از زمینه‌های کاربردی امیدوارکننده، حوزه یادگیری ماشینی است. آموزش کامپیوترهای کلاسیک در زمینه داده‌های کوانتومی - اطلاعات الکترونیکی، مغناطیسی و سایر اطلاعاتی که رفتار یک سیستم کوانتومی را توصیف می‌کنند - به مقادیر زیادی داده زمان پردازش نیاز دارد. در مقابل همین نوع آموزش با استفاده از رایانه‌های کوانتومی به نمونه‌های کمتری برای کسب تسلط نیاز دارند. با چنین دستاوردهای عظیمی در کارایی می‌توان از این ماشین‌ها برای یادگیری و پیش‌بینی رفتار مواد شیمیایی و موادی شمار دیگری استفاده کرد. در حال حاضر مشخص نیست که آیا رایانه‌های کوانتومی در یادگیری از داده‌های کلاسیک مانند داده‌های متنی، صوتی و تصویری بر زیربنای سیستم‌های هوش مصنوعی امروزی مزیت خواهند داشت یا خیر. با این حال محاسبات کوانتومی از پیشرفت‌های هوش مصنوعی کلاسیک سود می‌برند؛ محققان از مدل‌های زبان بزرگ، مدل‌های ترانسفورماتور و دیگر معماری‌های هوش مصنوعی برای کمک به طراحی دستسنگ‌های کوانتومی، توسعه نرم‌افزار و بهبود نحوه تصحیح خطای کوانتومی استفاده می‌کنند.

البته منطقی است که رایانه‌های کوانتومی در کاربردهایی مزیت داشته باشند که خود مکانیک کوانتومی به شمار می‌روند، اما در این میان مسئله‌ای وجود دارد که کمتر به آن پرداخته شده‌است: اینکه رایانه‌های کوانتومی می‌توانند دستاوردهای چشمگیری در حل برخی از انواع مسائل مکانیکی غیرکوانتومی می‌سازد. توجه به این موضوع درواقع محققان و ریاضی‌دانان ۶۰ الگوریتم را کشف کرده‌اند که به رایانه‌های کوانتومی اجازه می‌دهد مسائل را بسیار سریع‌تر از نمونه‌های کلاسیک حل کنند. برخی از این افزایش هادر مقیاس بسیار چشمگیرند که در مثال‌های بالا به آن‌ها اشاره شد؛ برخی دیگر کمتر چشمگیر بوده اما همچنان نسبت به کامپیوترهای کلاسیک مزایای قابل توجهی دارند.

یکی از حوزه‌های جدی تحقیق، مطالعات مربوط به بهینه‌سازی است. با توجه به مجموعه‌ای متغیر، به بهینه‌سازی به دنبال یافتن کارآمدترین راه‌حل است. و توسط برنامه‌ریزان مالی، مدیران تدارکات و تحلیل‌گران مالیان و در زمینه دیگر از آن استفاده می‌شود. بهینه‌سازی نیز در سیستم‌های هوش مصنوعی نقش اساسی دارد. با توجه به اهمیت محاسبات بهینه‌سازی برای اقتصاد جهانی، اگر حتی کسری از آنها به‌بسیار سریع‌تر و ارزان‌تر و با انرژی بسیار کمتر اجرائی شوند، تأثیر این کار غیر قابل اندازه‌گیری خواهد بود.

ماشین‌های سریع‌تر، خطرات بزرگ‌تر

امکانات متنج از محاسبات کوانتومی الهام‌بخش بوده، اما محدودیت‌های فعلی این فناوری هم جدی‌اند. حرکت از وضعیت فعلی به سامانه‌های پیشرفته مورد نیاز برای اجرائی کردن برخی از امیدوارکننده‌ترین کاربردهای این فناوری، مستلزم ادغام اجزای بسیار پیچیده و غلبه بر چالش‌های بی‌شماری است. در نتیجه بسیاری از برنامه‌های پیش‌بینی شده ممکن است برای سال‌ها محقق نشوند. مثلاً بر اساس برآوردهای فعلی یک رایانه کوانتومی که قادر به شکستن کدشاد، به مقایسه با بهترین نمونه‌های فعلی، به حدود ۴۰ هزار برابر کیوبیت‌های فیزیکی و کاهش پنج برابری میزان خطای فیزیکی نیاز دارد. رایانه‌های کوانتومی هم که بتوانند محاسبات شیمی ساده‌ای را انجام دهند، تقریباً دو مرتبه کم‌زیر بهتر هستند، اما آن‌ها نیز به فناوری بسیار پیشرفته‌تری وابسته خواهند بود.

یکی از معیارهای وضعیت فعلی توسعه کوانتومی را می‌توان از نقشه راهی که گوگل در سال ۲۰۱۸ منتشر کرد گرفت. این طرح شش نقطه عطف برای رایش‌بینی کرده است که برای دستیابی به یک رایانه کوانتومی در مقیاس کامل مورد نیاز است: نشان دادن اینکه یک پردازنده کوانتومی می‌تواند در اولین کار خود از پردازنده کلاسیک بهتر عمل کند؛ ساخت یک نمونه اولیه برای یک کیوبیت منطقی؛ نمایش یک کیوبیت منطقی واقعی؛ ساخت یک دروازه منطقی برای عملیات بین چند کیوبیت منطقی، تولید ۱۰۰ کیوبیت منطقی که نقطه شروعی برای شبیه‌سازی کوانتومی ساده در نظر گرفته می‌شود؛ تولید هزار کیوبیت منطقی برای شبیه‌سازی‌های پیچیده‌تر (یک کامپیوتر رمز شکن حتی به قابلیت‌های پیشرفته‌تری هم نیاز دارد). گوگل به دو نقطه عطف اول خود دست یافت و در دسامبر ۲۰۲۴ پردازنده کوانتومی جدیدی به نام Willow را معرفی کرد که قادر است در چند دقیقه الگوریتم معیاری را حل کند که حل آن توسط یکی از سریع‌ترین رایبرایانه‌های امروزی، ۱۰۲۵ سال طول می‌کشد. سازمان‌های دیگر - از جمله IBM، Q-ERA و IonQ - نقشه‌های راه خود را برای یک کامپیوتر کوانتومی عاری از خطا و در مقیاس بزرگ منتشر کرده‌اند. محققان چینی، به‌ویژه در دانشگاه علم و فناوری چین، به اولین نقطه عطف گوگل دست یافته‌اند و پردازنده‌هایی را با صداهای کیوبیت به‌نمایش گذاشته‌اند. مانند سایر بازیگران این عرصه، محققان چینی بدون شک پیشرفت‌های مهم دیگری هم دارند که هنوز به‌صورت عمومی منتشر نشده‌است.

برای ارزیابی وضعیت فعلی رقابت کوانتومی، سازوی تحقیقاتی وزارت دفاع ایالات متحده، آژانس پروژه‌های تحقیقاتی پیشرفته دفاعی یا «دارپا»، اخیراً یک ابتکار محاسبات کوانتومی را برای تعیین اینکه آیا ریزگرد محاسباتی کوانتومی می‌تواند تا سال ۲۰۳۳ به عملیاتی در مقیاس کاربردی دست یابد یا خیر، اعلام کرد. اگرچه پیش‌بینی سرعت دقیق نوآوری‌های آتی غیر ممکن است، اما کمپیوترهایی که احتمالاً از ۱۰ کیوبیت منطقی تشکیل شده‌اند، ممکن است تا پایان این دهه ساخته شوند، چنین شاخص‌اری، هم‌اکنون برای بهبود یافته تصحیح خطا را الگوریتم‌های کارآمدتر، جهان را به‌طرز وسوسه‌انگیزی به شبیه‌سازی کوانتومی نزدیک خواهد کرد. بر اساس برآوردهای کنونی، بعد است محققان تا اواخر ده ۲۰۳۰ به اولین ماشین رمزشکن کوانتومی واقعی دست یابند که رایانه کوانتومی با میلیون‌ها کیوبیت و تصحیح خطای کافی. حتی در آن زمان هم ساعت‌ها طول خواهد کشید تا چنین رایانه‌ای یک عدد بزرگ را فاکتورگیری کند. با این حال، برای ایالات متحده و شرکای بین‌المللی آن بسیار مهم است که از هم‌کنون برای چنین فناوری آماده شوند. این شبکه‌های لغم‌درمسترس بودن طولانی‌مدت، در پیاده‌سازی استانداردهای امنیتی جدید بسیار کند بوده‌اند. توسعه، آزمایش و اصلاح مجموعه‌ای از استانداردهای کوانتومی ام‌ن سال‌ها طول خواهد کشید. مؤسسه ملی استاندارد و فناوری ایالات متحده از سال ۲۰۱۶ تلاش‌هایی را برای توسعه استانداردهای رمزنگاری برای دنیای پساکوانتومی رهبری می‌کند. در آگوست ۲۰۲۴، این مؤسسه اولین مجموعه از سه الگوریتم رمزگذاری کلاسیک را به‌عنوان استانداردهای آماده‌برای استفاده فوری، همراه با دستورالعمل‌هایی برای ادغام آن‌ها در سامانه‌های رمزنگاری و سایر محصولات،

۱۹۸۰ هستند. قانون مور - که مطابق آن تعداد ترانزستورهای یک تراشه رایانه‌ای هر دو سال یکبار دو برابر می‌شود - علی‌رغم پیش‌بینی‌های متعدد مبنی بر کنار رفتن آن، همچنان در صنعت نیمه‌رساناها صادق است. به علاوه، بهترین ابررایانه‌های امروزی می‌توانند یک کوئینتیلیون - یعنی یک میلیارد میلیارد - عملیات را در ثانیه انجام دهند. با این حال، همان‌طور که این انقلاب به رشد خود ادامه می‌دهد، به‌طور فزاینده‌ای روشن شده‌است که برخی از محاسبات همچنان فراتر از بهترین رایانه‌های کلاسیک هستند و این‌گونه نیز خواهند ماند.

این امر به این دلیل است که فناوری‌های رایانه‌ای موجود توسط فرضیه اصلی که بر اساس آن کار می‌کنند، محدود شده‌اند. همه اشکال محاسبات کلاسیک، اعم از چرتکه، لپ‌تاپ شخصی، یا مجموعه‌ای از ماشین‌های با کارایی بالا در یک مرکز امنیتی، از چیزی پیروی می‌کنند که محققان منطق بولی می‌نامند. در این سیستم، واحد اصلی اطلاعات بیت است، که می‌تواند یکی از دو حالتی را که معمولاً ۰ یا ۱ نامیده می‌شود، به خود بگیرد. اگرچه این سیستم برای بسیاری از انواع محاسبات بسیار کارآمد بوده است، اما نمی‌تواند محاسباتی با پیچیدگی بیش از حد را انجام دهد؛ محاسباتی مانند فاکتورگیری یک عدد هزار رقمی، محاسبه دینامیک واکنش یک مولکول با صداهاتم یا حل انواع خاصی از مسائل مربوط به بهینه‌سازی که در بسیاری از رشته‌ها رایج هستند.

در مقابل، محاسبات کوانتومی به دلیل استفاده از مکانیک کوانتومی محدودیت‌های یکسانی ندارد. یک درس فیزیک کوانتومی - که شکفت‌انگیز و غیرقابل درک است - این است که ذرات می‌توانند در ترکیبی از چندین حالت وجود داشته باشند. بر این اساس، محاسبات کوانتومی به جای استفاده از بیت‌هایی که از منطق مبنی بر «یا این یا آن» استفاده می‌کنند، از بیت کوانتومی یا کیوبیت بهره‌می‌جویند که می‌تواند هم‌زمان در حالت‌های ۰ و ۱ باشد. این توانایی هم‌زمان که به‌عنوان «برهم‌نهی» شناخته می‌شود، دارای مزیت محاسباتی عظیمی است که وقتی کیوبیت‌های بیشتری با هم کار می‌کنند، افزایش هم می‌یابد. در حالی که یک کامپیوتر کلاسیک باید یک حالت را به صورت متوالی پردازش کند، یک کامپیوتر کوانتومی می‌تواند بسیاری از احتمالات را به‌صورت موازی کشف کند. به تلاش برای یافتن مسیر صحیح از داخل یک هزارتو (ماز) فکر کنید؛ یک رایانه کلاسیک باید هر مسیر را یکی یکی امتحان کند؛ اما یک کامپیوتر کوانتومی می‌تواند چندین مسیر را به‌طور هم‌زمان کاوش کند؛ امری که به‌مقدار بسیار بسیار زیادی کارکرد این رایانه‌ها را برای بعضی از امور تسریع می‌سازد. توجه به این نکته مهم است که برخلاف ساده‌سازی رایج، یک کامپیوتر کوانتومی صرفاً مجموعه عظیمی از کامپیوترهای کلاسیک نیست که به‌صورت موازی کار می‌کنند. اگرچه به صورت تصاعدی پاسخ‌های احتمالی زیادی وجود دارد که می‌توان آن‌ها را از طریق یک پردازنده کوانتومی بررسی کرد، اما در نهایت تنها یک ترکیب را می‌توان سنجش کرد. بنابراین استخراج یک راه حل از یک کامپیوتر کوانتومی نیازمند برنامه‌نویسی هوشمندانه است که نل به پاسخ صحیح را تقویت کند.

یک چالش بزرگ این است که به‌فهمیم چگونه پردازنده‌های کوانتومی بسازیم که به اندازه کافی بزرگ و پایدار باشند تا نتایج ثابتی برای مسائل مختلف ایجاد کنند. چنین پردازنده‌هایی نسبت به محیط خود بسیار حساس هستند و به راحتی می‌توانند تحت تأثیر تغییرات دم‌ا، ارتعاشات و سایر اختلالات قرار گیرند؛ امری که می‌تواند منجر به خطاهای مختلف در سیستم شود. از آنجایی که وفاداری محاسباتی به حفظ انسجام کیوبیت‌ها متکی است، محققان سر مایه‌گذاری زیادی روی روش‌هایی برای بهبود کیفیت کیوبیت انجام داده‌اند که از جمله طرح‌های جدید، فرایندهای ساخت تراشه و تکنیک‌های برای تصحیح خطای کیوبیت است.

در حال حاضر، طیف گسترده‌ای از رویکردهای طراحی کیوبیت‌ها وجود دارد که هر کدام مزایا و معایب خاص خود را دارند. هر یک نظام مکانیکی کوانتومی - اتم‌ها، مولکول‌ها، یون‌ها، فوتون‌ها - می‌توانند به صورت کیوبیت درآیند. در عمل، عواملی مانند قابلیت ساخت، کنترل‌پذیری، عملکرد و سرعت محاسباتی عملی مسیرهای ریزش را دیکته می‌کنند. تلاش‌های پیشرو امروزی در این عرصه شامل ابررسانایی، اتم خنثی، فوتونیک و نلته بولی است. البته اکنون مشخص نیست که این تلاش‌ها به موفقیت خواهند رسید یا خیر. در کنار ساخت پردازنده، چالش‌های دیگری هم وجود دارند که شامل نحوه سته‌بندی کیوبیت‌ها، انتقال سیگنال‌های آن‌ها و اجزای برنامه‌هاست. محققان باید از یخچال‌های برودتی استفاده کنند که می‌توانند کیوبیت‌های ابررسانا را از چند هزار درجه بالا صفر مطلق خنک کنند تا محیطی فوق‌العاده سرد، تاریک و آرام را برای این کار فراهم کنند. تخصص‌های مربوط به اجزای مختلف این فرایند وابسته به کشورهای مختلفی هستند.

ماشین پاسخگوی جدید

رقابت برای رسیدن به یک رایانه کوانتومی در مقیاس کامل با انگیزه‌های مختلفی انجام می‌شود. اساساً محاسبات کوانتومی نوید پاسخ به مشکلاتی را می‌دهند که قبلاً غیرقابل حل تصور می‌شدند - مسائلی که چندین سال طول می‌کشد تا از سوی بهترین رایانه‌های کلاسیک پاسخ داده شوند.

شناخته‌شده‌ترین مشکل از این نوع فاکتورسازی ساده‌ای با شکستن یک عدد به‌عنوان حاصل ضرب چند عدد کوچک‌تر است. حتی سریع‌ترین ابررایانه‌ها نیز قادر به فاکتورگیری اعداد بسیار بزرگ نیستند. این امر بدان معناست که پیشرفته‌ترین شکل‌های رمزنگاری - که مبنی بر فاکتورگیری اند- اکنون نمی‌توانند شکسته شوند، اما رایانه‌های کوانتومی ممکن است این وضعیت را تغییر دهند.

در سال ۱۹۹۴ یک دانشمند رایانه به نام پیتر شواب ثابت کرد که یک کامپیوتر کوانتومی قادر به فاکتورگیری اعداد بسیار بزرگ است. در آن زمان، ساخت چنین رایانه‌ای کاملاً در قلمرو تئوری (و دور به دور از عمل) بود، اما با شروع توسعه این فناوری این نگرانی به عرصه وجود آمد که پردازنده‌های کوانتومی ممکن است روزی قادر به شکستن پیشرفته‌ترین رمزگذاری‌ها باشند. امروزه، کارشناسان امنیت ملی معتقد هستند که بازیگران دولتی و خصوصی متخاصم در حال جمع‌آوری اطلاعات رمزگذاری‌شده و در انتظار این فناوری جدید هستند، ریزگری که به‌عنوان حمله «اکنون ذخیره کن، بعداً رمزگشایی کن» شناخته می‌شود. اما رمزگشایی تنها یکی از کاربردهای ممکن برای کامپیوترهای کوانتومی است و احتمالاً بیش از یک‌دهه یا به‌کارگیری آن فاصله داریم. همان‌طور که فاینمن می‌دانست، کاربردهای واضح‌تر برای محاسبات مبتنی بر کوانتوم به شبیه‌سازی کوانتومی - توانایی انجام محاسبات دقیق سیستم‌های کوانتومی مانند الکترون می‌دهد، مولکول‌ها و مواد- مربوط می‌شود و این کاربردها می‌توانند زودتر مورد استفاده قرار گیرند.

پردازنده‌های کوانتومی در حال حاضر به اکتشافات در تعدادی از زمینه‌های بسیار تخصصی در فیزیک کمک می‌کنند - از جمله مهندسی شیب‌هزات، دینامیک بدنه‌های متعد، انتقال اسپین، انتقال فلز، کریستال‌های زمان، دینامیک کرم‌چاله و مغناطیس‌سازی. با یک رایانه کوانتومی در مقیاس کامل و با قابلیت کامل، احتمالات ممکن خیره‌کننده‌اند، مثلاً کدهای کاشوری را در نظر بگیرید.

در حال حاضر تثبیت نیتروژن - فرایند شیمیایی مورد نیاز برای تولید آمونیاک از گاز نیتروژن - بسیار انرژی‌بر است و ۲ درصد از بودجه سالانه انرژی جهان را به خود اختصاص می‌دهد، زیرا کاتالیزورهای صنعتی مورد استفاده در این واکنش بسیار ناکارآمد هستند. در واقع مولکول FeMoco به‌طور طبیعی وجود دارد و یک کاتالیزور برای تثبیت نیولوژیکی نیتروژن به‌شمار می‌رود و برای این کار بسیار کارآمدتر است، اما هنوز نمی‌توان آن را به‌صورت شیمیایی سنتز کرد یا در مقادیر صنعتی جدا نمود؛ به علاوه مکانیسم عمل آن بسیار چالش‌برانگیزتر از آن است که بتوان آن فناوری

چگونه انقلاب کوانتومی، اقتصاد جهانی را متحول کرده است و امنیت ملی را واژگون خواهد ساخت

سجاد عطا‌زاده
مترجم

چارناچو (مدیرعامل گوگل کوانتوم و هوش مصنوعی)، جیمز مانیکا (معاون ارشد گوگل و مدیر تحقیق، فناوری و جامعه این شرکت) و هارتموت نون (معاون مهندسی گوگل و رئیس گوگل کوانتوم و هوش مصنوعی) در مقاله «رقابت برای رهبری آینده کوانتوم، چگونه انقلاب محاسباتی آینده، اقتصاد جهانی را متحول کرده و امنیت ملی را واژگون خواهد ساخت» که در شماره ژانویه /فوریه نشر به‌فان‌افرنشر شده است، به‌بررسی تاریخچه و کاربردهای کوانتوم، به‌عنوان یکی از حوزه‌های نو ظهور فناوری، پرداخته و معتقدند که تکامل این فناوری سبب تحولات بسیاری در مباحث مربوط به اقتصاد و امنیت جهانی خواهد شد. در ادامه ترجمه این مقاله را از نظر می‌گذرانید.

=====

در طول چند سال گذشته و هم‌زمان با توجه گسترده افکار عمومی به پیشرفت‌های سریع انجام گرفته در هوش مصنوعی و بررسی دقیق این تحولات، پیشرفت‌های یک فناوری حیاتی دیگر تا حد زیادی از دید عموم پنهان مانده است. محاسبات کوانتومی که زمانی محدود به نظریه انتزاعی بود، در پی استفاده از عملیات‌های مبتنی بر مکانیک کوانتومی برای حل مسائل محاسباتی است که قبلاً غیر قابل حل تلقی می‌شدند. اگرچه این فناوری هنوز در مراحل ابتدایی خود به سر می‌برد، اما از هم‌اکنون واضح است که محاسبات کوانتومی می‌تواند پیامدهای عمیقی برای امنیت ملی و اقتصاد جهانی در دهه‌های آینده داشته باشد.

از اواخر دهه ۲۰۱۰، ایالات متحده و بسیاری از کشورهای پیشرفته دیگر به‌طور فزاینده‌ای درگیر رقابت برهبری علم و فناوری اطلاعات کوانتومی شده‌اند؛ حوزه‌ای که محاسبات کوانتومی، ارتباطات کوانتومی و سنجش کوانتومی را در بر می‌گیرد. در طول دهه گذشته، دولت‌های ۲۰ کشور سرمایه‌گذاری‌های خود در توسعه کوانتومی به ارزش بیش از ۴ میلیارد دلار را اعلام کرده‌اند. چین به تنهایی متعهد شده است که در طول پنج سال ۱۵٫۳ میلیارد دلار در این حوزه هزینه کند. در سال ۲۰۱۶، پکن توسعه فناوری‌های کوانتومی را به عنوان یک اولویت ملی برای خود تعیین کرد و هاب‌های پیشرفته‌ای را هم در این زمینه ایجاد کرد. ایالات متحده در سال ۲۰۱۸، قانون ملی کوانتوم را با هدف حفظ برتری فنی و علمی این کشور در اطلاعات کوانتومی و کاربردهای آن وضع کرد. دولت ایالات متحده ۳٫۷ میلیارد دلار بودجه طبقه‌بندی نشده به اضافه بودجه‌م‌ها به‌بیشتر برای تحقیق و توسعه دفاعی را اعلام کرده است. علاوه بر ابتکارات تحت رهبری دولت، تلاش‌های تحقیق و توسعه متعددی هم در بخش خصوصی و دانشگاه در حال انجام است.

اگرچه این سرمایه‌گذاری‌ها هنوز در برابر بودجه اختصاص داده‌شده از سوی ایالات متحده و بودجه‌های بین‌المللی برای هوش مصنوعی کم‌رنگ است، اما ظهور فناوری کوانتومی از هم‌اکنون سیاست‌های بین‌المللی مختص به خود را ایجاد کرده است. در سال ۲۰۱۹، ایالات متحده یک «بیانیه دو جانبه درباره همکاری کوانتومی» را به همراه ژاپن اعلام کرد که واشنگتن در سال ۲۰۲۳ دست به تقویت آن نیز زد. در سال ۲۰۲۴ هم آمریکا یک ابتکار چند جانبه به نام گروه توسعه کوانتومی را برای هماهنگ کردن راهبردهای پیشرفت و مدیریت این فناوری جدید اعلام کرد. ایالات متحده همچنین مسائل مربوط به کوانتوم را در مجامع مختلف اقتصادی و امنیتی، از جمله آکس - پیمان دفاعی سه‌جانبه بین اسرائیل، بریتانیا و ایالات متحده - کوارد - مشکل از استرالیا، هند، ژاپن و ایالات متحده - و شورای تجارت و فناوری ایالات متحده و اتحادیه اروپا به بحث گذاشته است. یکی از تحلیلگران مرکز امنیت جدید آمریکا در نوامبر و پس از انتخابات ریاست جمهوری، با تأکید بر نگرانی‌های فزاینده در مورد این فناوری در واشنگتن، اظهار داشت که دولت آینده باید تا ۱۰۰ روز اول به سرعت برای تقویت رقابت‌پذیری کوانتومی آمریکا عمل کند.

تاکنون، ظهور فناوری کوانتوم تا حد زیادی به عنوان یک موضوع امنیت ملی تلقی شده است. از دهه ۱۹۹۰، محققان دریافته‌اند که یکی از بزرگ‌ترین تهدیدات رایانه‌های کوانتومی قدرتمند، پتانسیل این رایانه‌ها به عنوان ابزاری برای رمزگشایی است که به آن‌ها امکان می‌دهد به رمزگزارای مورد استفاده در پیشرفته‌ترین سامانه‌های ارتباطی و شبکه‌های دیجیتال سراسر جهان نفوذ کنند. این نگرانی، دولت ایالات متحده را به توسعه و حمایت از اتخاذ رمزنگاری مقاوم در برابر کوانتوم، تقویت کنترل‌های صادرات برای روی فناوری‌های کوانتومی و به‌صورت مرتبط و ایجاد مشارکت‌های عمل محور، با صنعت دانشگاه دولتی‌های محلی در حوزه کوانتوم کرده‌است. اما تمرکز بر شکستن کد، سیاست‌گذاران را به ناهماهنگ رفتن سایر کاربردهای مهم فناوری کوانتومی سوق داده‌است. ماشین‌های کوانتومی پیش از این که قادر باشند سامانه‌های رمزنگاری پیشرفته را بشکنند - قابلیت‌ی که حتی پس از توسعه این فناوری به قدرت محاسباتی عظیمی نیاز دارد - می‌توانند در بسیاری از بخش‌های اقتصاد، از جمله انرژی و داروسازی، اثر دگرگونی‌ساز داشته باشند. فناوری‌های کوانتومی اگر به‌طور مؤثری مورد استفاده قرار بگیرند، می‌توانند سبب نوآوری، اکتشاف علمی، رشد اقتصادی و تحرک فرصت‌ها شوند. از نظر تأثیر انسانی، برخی از پیشرفت‌هایی که می‌توانند توسط ماشین‌های کوانتومی ایجاد شوند، رقیب آن‌هایی به شمار می‌روند که انتظار می‌رود از هوش مصنوعی حاصل شوند. به همین دلیل، بسیار مهم است که این فناوری در جوامع باز، با نرده‌های محافظ شفاف برای اطمینان از استفاده آن‌ها در مسیر اهداف خیرخواهانه، توسعه یابد.

برنده شدن در رقابت کوانتومی آسان نخواهد بود. چین هم‌اکنون در برخی زمینه‌ها مانند ارتباطات کوانتومی پیش‌از است و به همین دلیل نوآوری ورهبری متمرکز آمریکا برای حفظ رقابت‌پذیری ایالات متحده در سال‌های آینده حیاتی خواهد بود. ایالات متحده و شرکای بین‌المللی آن باید منابع بسیار بیشتری را برای به‌ثمر رساندن پروژه‌های کوانتومی خود اختصاص داد و صنایع کوانتومی و همچنین یک زیرساخت تأمین کوانتومی قوی را برای حمایت از این پروژه‌ها توسعه دهند. اگر واشنگتن و متحدان آن نتوانند این تلاش‌ها را به یک هدف راهبردی مرکزی و اولویت سیاست‌گذاری برای خود تبدیل کنند، ممکن است نفوذ دیپلماتیک، قدرت نظامی و توانایی نظارت بر یک فناوری جدید قدرتمند را از دست بدهند. آن‌ها همچنین شاید یک فرصت جدید برای نیل به پیشرفت اقتصادی و اجتماعی را نیز از دست بدهند.

به یکباره در همه جا

مفهوم رایانه کوانتومی برای اولین بار توسط فیزیکدان نظری و برنده جایزه نوبل، ریچارد فاینمن، در سال ۱۹۸۱ مطرح شد. فاینمن در عصر طلوع مکانیک کوانتومی رشد کرد؛ زمانی که دانشمندان متوجه شدند که اتم‌ها، الکترون‌ها و نور و دیگر اجرام زیر مقیاس نانو - بلوک‌های سازنده هر چیزی که در جهان موجود است - متفاوت از قوانین اساسی زندگی روزانه هستند. مثلاً بر خلاف یک توپ که از قوانین مستقیم مکانیک کلاسیک پیروی می‌کند، الکترون‌ها به‌طور هم‌زمان به عنوان ذرات و امواج رفتار می‌کنند و مکان آن‌ها را نمی‌توان دقیقاً تعریف کرد. پیش فاینمن این بود که برای درک واقعی جهان مکانیک کوانتومی - و عملکرد کلی بخش کیهان - لازم است رایانه‌ای بسازیم که طبق قوانین مشابه عمل کند. او گفت: «طبیعت کلاسیک نیست و اگر می‌خواهید طبیعت را شبیه‌سازی کنید، بهتر است این کار را به صورت مکانیکی - کوانتومی انجام دهید.»

پیش فاینمن درست از آب درآمده‌است. در طول بیش از چهار دهه پس از او، رایانه‌هایی که از طراحی کلاسیک پیروی می‌کنند، کوه زمین را کاملاً متحول کرده‌اند؛ تلفن‌های همراه جیبی امروز میلیون‌ها برابر قدرتمندتر از رایانه‌های شخصی روزمیزی عظیم‌ه