

برتری کوانتومی قرار است جهان را تغییر دهد!

چندین شرکت حوزه فناوری اقدام به ساخت رایانه‌های کوانتومی کرده‌اند اما این مدل‌های اولیه هنوز برتری کوانتومی را که توانایی پیشی گرفتن از ابررایانه‌های معمولی است، نشان نداده‌اند.



چندین شرکت حوزه فناوری اقدام به ساخت رایانه‌های کوانتومی کرده‌اند اما این مدل‌های اولیه هنوز برتری کوانتومی را که توانایی پیشی گرفتن از ابررایانه‌های معمولی است، نشان نداده‌اند. «دنیل لیدار» فیزیکدان آمریکایی در یک گزارش جدید توضیح داده است که برتری کوانتومی چگونه جهان را تغییر خواهد داد.

به گزارش ایسنا و به نقل از فست کمپانی، «برتری کوانتومی» (Quantum advantage) در حال حاضر یک نقطه عطف است که حوزه محاسبات کوانتومی به شدت با آن سر و کار دارد. یک رایانه کوانتومی می‌تواند مسائلی را حل کند که فراتر از توان قوی‌ترین رایانه‌های غیرکوانتومی یا کلاسیک هستند.

کوانتوم به مقیاس اتم‌ها و مولکول‌ها اشاره می‌کند. در این مقیاس، قوانین فیزیک شکسته می‌شوند و مجموعه متفاوتی از قوانین غیرمعمول اعمال می‌گردند. رایانه‌های کوانتومی از این رفتارهای عجیب برای حل مشکلات استفاده می‌کنند. مسئله‌های گوناگونی مانند شکستن الگوریتم‌های رمزگذاری پیشرفته وجود دارند که حل کردن آنها برای رایانه‌های کلاسیک عملی نیست. پژوهش‌های انجام شده در دهه‌های اخیر نشان داده‌اند که رایانه‌های کوانتومی، توانایی حل کردن برخی از این مشکلات را دارند. اگر بتوان یک رایانه کوانتومی ساخت که یکی از این مشکلات را حل کند، برتری کوانتومی ثابت خواهد شد. «دنیل لیدار» (Daniel Lidar) فیزیکدان و استاد مهندسی «دانشگاه کالیفرنیا جنوبی» (USC) است که پردازش اطلاعات کوانتومی و کنترل سیستم‌های کوانتومی را مطالعه می‌کند. او باور دارد که این مرز نوآوری در علم و فناوری نه تنها نویدبخش پیشرفت‌های پیشگامانه در محاسبات است، بلکه افزایش گسترده‌تر فناوری کوانتومی از جمله پیشرفت‌های قابل توجه در رمزنگاری کوانتومی و سنجش کوانتومی را به نمایش می‌گذارد.

لیدار در این گزارش توضیح داده است که چگونه برتری کوانتومی می‌تواند جهان را تغییر دهد.

منبع قدرت محاسبات کوانتومی

مرکز محاسبات کوانتومی، بیت کوانتومی یا کیوبیت است. برخلاف بیت‌های کلاسیک که فقط می‌توانند در حالت‌های صفر یا یک باشند، یک کیوبیت می‌تواند در هر حالتی از ترکیب صفر و یک باشد. این حالت که نه فقط یک و نه فقط صفر است، به عنوان «برهم نهی کوانتومی» شناخته می‌شود. با هر کیوبیت اضافی، تعداد حالت‌هایی که می‌توان با کیوبیت‌ها نشان داد دو برابر می‌شود.

این ویژگی اغلب با منبع قدرت محاسبات کوانتومی اشتباه گرفته می‌شود و در عوض، به یک فعل و انفعال پیچیده از برهم نهی، تداخل و درهم تنیدگی می‌رسد.

تداخل شامل دستکاری کیوبیت‌ها به گونه‌ای است که حالت‌های آنها در طول محاسبات، به طور سازنده برای تقویت راه حل‌های درست و به طور مخرب برای سرکوب پاسخ‌های اشتباه ترکیب شوند. تداخل سازنده زمانی اتفاق می‌افتد که قله‌های دو موج مانند امواج صوتی یا امواج اقیانوس، برای ایجاد یک قله بالاتر با هم ترکیب شوند. تداخل مخرب زمانی اتفاق می‌افتد که یک قله و یک فرورفتگی موج با هم ترکیب شوند و یکدیگر را خنثی کنند. الگوریتم‌های کوانتومی که ابداع کردن آنها کم و دشوار است، دنباله‌ای از الگوهای تداخلی را تنظیم می‌کنند که پاسخ درست را به یک مسئله می‌دهند.

درهم تنیدگی، یک همبستگی کوانتومی منحصربه‌فرد را بین کیوبیت‌ها ایجاد می‌کند که در آن، حالت یکی را نمی‌توان مستقل از بقیه توصیف کرد؛ مهم نیست کیوبیت‌ها چقدر از هم دور باشند. این همان چیزی است که «آلبرت اینشتین» آن را «کنش ترسناک از راه دور» نامید. رفتار جمعی درهم تنیدگی که از طریق یک رایانه کوانتومی تنظیم شده، افزایش سرعت محاسباتی را امکان‌پذیر می‌کند که خارج از دسترس رایانه‌های کلاسیک است.

کاربرد محاسبات کوانتومی

محاسبات کوانتومی، طیف گسترده‌ای از کاربردهای احتمالی را دارند که می‌توانند بهتر از کاربرد رایانه‌های کلاسیک باشند. در رمزنگاری، رایانه‌های کوانتومی هم یک فرصت و هم یک چالش هستند. معروف‌تر از همه این است که آنها پتانسیل رمزگشایی الگوریتم‌های رمزگذاری کنونی مانند «آراس‌ای» (RSA) را دارند.

یکی از پیامدهای این امر این است که پروتکل‌های رمزگذاری امروزی باید دوباره مهندسی شوند تا در برابر حملات کوانتومی آینده مقاوم باشند. این شناخت، به شکل‌گیری حوزه روبه‌رشد «رمزنگاری پساکوانتوم» منجر شده است. پس از یک فرآیند طولانی، «موسسه ملی فناوری و استانداردهای آمریکا» (NIST) اخیراً چهار الگوریتم مقاوم در برابر کوانتوم را انتخاب کرده و فرآیند آماده‌سازی الگوریتم‌ها را آغاز کرده است تا سازمان‌های سراسر جهان بتوانند از آنها در فناوری رمزگذاری خود استفاده کنند.

علاوه بر این، محاسبات کوانتومی می‌توانند سرعت شبیه‌سازی کوانتومی را به طور چشمگیری افزایش دهند. شبیه‌سازی کوانتومی، توانایی پیش‌بینی کردن نتیجه آزمایش‌هایی است که در قلمرو کوانتوم عمل می‌کنند. «ریچارد فاینمن» (Richard Feynman) فیزیک‌دان مشهور آمریکایی، بیش از ۴۰ سال پیش این امکان را تصور کرد. شبیه‌سازی کوانتومی، پتانسیل پیشرفت

های قابل توجهی را در علم شیمی و مواد ارائه می دهد و در زمینه هایی مانند مدل سازی پیچیده ساختارهای مولکولی برای کشف دارو و امکان کشف یا ایجاد مواد با خواص جدید کمک می کند.

یکی دیگر از کاربردهای فناوری اطلاعات کوانتومی، سنجش کوانتومی است. سنجش کوانتومی، به تشخیص و بررسی خواص فیزیکی مانند انرژی الکترومغناطیسی، گرانش، فشار و دما با حساسیت و دقت بیشتر نسبت به تجهیزات غیرکوانتومی گفته می شود. سنجش کوانتومی، کاربردهای بی شماری را در زمینه هایی مانند بررسی محیطی، اکتشافات زمین شناسی، تصویربرداری پزشکی و نظارت دارد.

ابتکاراتی مانند توسعه اینترنت کوانتومی که رایانه های کوانتومی را به هم متصل می کند، گام های مهمی در جهت ایجاد پل ارتباطی بین دنیای محاسبات کوانتومی و کلاسیک هستند. این شبکه را می توان با استفاده از پروتکل های رمزنگاری کوانتومی مانند «توزیع کلید کوانتومی» (QKD) ایمن سازی کرد که کانال های ارتباطی فوق العاده ایمن را فعال می سازند تا در برابر حملات محاسباتی محافظت شوند.

به رغم وجود داشتن یک مجموعه کاربردی روبه رشد برای محاسبات کوانتومی، توسعه الگوریتم های جدید که از برتری کوانتومی به ویژه در یادگیری ماشینی به طور کامل استفاده می کنند، یک حوزه حیاتی از پژوهش های در حال انجام شدن است.

منسجم ماندن و غلبه کردن بر خطاها

حوزه محاسبات کوانتومی با موانع قابل توجهی در توسعه سخت افزار و نرم افزار روبرو است. رایانه های کوانتومی نسبت به هرگونه تعامل ناخواسته با محیط خود بسیار حساس هستند. این امر به بروز پدیده ناپیوستگی منجر می شود که در آن، کیوبیت ها به سرعت به حالت صفر یا یک بیت های کلاسیک تنزل می یابند.

ساختن سیستم های محاسبات کوانتومی در مقیاس بزرگ که قادر به فراهم کردن افزایش سرعت کوانتومی باشند، نیازمند غلبه بر عدم پیوستگی است. راه حل کلیدی، توسعه روش های مؤثر برای سرکوب و تصحیح خطاهای کوانتومی است و تحقیقات دنیل لیدار روی همین حوزه متمرکز شده اند.

در راستای بررسی این چالش ها، استارت آپ های سخت افزاری و نرم افزاری کوانتومی متعددی در کنار غول های فناوری مانند «گوگل» و «آی بی ام» (IBM) ظهور کرده اند. این علاقه صنعتی همراه با سرمایه گذاری قابل توجه دولت های سراسر جهان، بر شناخت جمعی در مورد پتانسیل تحول آفرین فناوری کوانتومی تأکید می کند. این ابتکارات، یک اکوسیستم غنی را تقویت می کنند که در آن دانشگاه و صنعت با یکدیگر همکاری دارند و پیشرفت در این زمینه را سرعت می بخشند.

برتری کوانتومی در حال نشان دادن خود است

محاسبات کوانتومی ممکن است روزی به اندازه ورود «هوش مصنوعی مولد» مخرب باشند. در حال حاضر، توسعه فناوری محاسبات کوانتومی در یک مقطع حیاتی قرار دارد. این حوزه قیلا نشانه های اولیه دستیابی به یک برتری کوانتومی تخصصی را نشان داده است. پژوهشگران گوگل و سپس گروهی از پژوهشگران چین، برتری کوانتومی را برای تولید فهرستی از اعداد تصادفی با ویژگی های خاص نشان دادند. گروه پژوهشی لیدار نیز سرعت کوانتومی را برای یک بازی حدس زدن اعداد تصادفی نشان داد.

از سوی دیگر، در صورتی که نتایج عملی در کوتاه مدت محقق نشوند، خطر ملموسی را برای ورود به «زمستان کوانتومی» به همراه خواهند داشت که یک دوره از کاهش سرمایه گذاری است.

در حالی که صنعت برای ارائه کردن برتری کوانتومی در محصولات و خدمات در کوتاه مدت تلاش می کند، پژوهش های آکادمیک همچنان بر بررسی اصول زیربنای این مفهوم متمرکز هستند. این پژوهش های بنیادی مستمر که مشتاقانه توسط دانشجویان جدید و باهوش انجام می شوند، تضمین می کنند که این حوزه به پیشرفت خود ادامه خواهد داد.