Journal of Information and communication Technology in policing (JICTP)
Journal Homepage: pitc.jrl.police.ir

Vol. 2, No.2 (6), Spring 2021

Smarting in cyberspace with quantum cloud computing

Received: 18 November 2021
Accepted: 15 January 2022
Article type: Research Article
PP: 1-11

DOI:
10.22034/pitc.2022.1265628.1099

Nasibollah Doustimotlagh
Supreme National Defense University
(Corresponding author)
doustimotlagh@chmail.ir

Abstract

Cloud computing and online storage of information is realized as an excellent replacement for hardware memory mostly because it is the transfer and use of information by cloud computing are less expensive, more practical, simpler, faster, and more accessible. However, some issues should be taken care of. One of these issues is cyber threats which are much greater than what we had in the past. The current technologies and even the most advanced computers and classical cryptography are not able to deal with cyber threats in this volume of information transfer and use. On the other hand, there is quantum computing which is the most advanced type of data transmission we know. It relies on the existence and presentation of quantum computers and will be the only way to smarten and provide cyber security in the future. Quantum computing focuses on building very fast computers using the concepts of quantum physics, and cloud computing allow this computing power to be provided as a service. Cloud-based quantum computing provides direct access to quantum simulators and processors, and this could revolutionize intelligence. With the advent of quantum computers, the security of today's cryptographic systems is compromised, since many of today's cryptocurrencies are based on the difficulty of calculating the prime factors of numbers, and the Shor's quantum algorithm can break these cryptographies. Grover's quantum algorithm can also make it easier for us to access passwords. In this article, we first briefly discuss the basics and concepts related to quantum cloud computing.

Keywords: Smartening, quantum computing, quantum cloud computing, quantum algorithm, quantum simulating, quantum cryptography

نشریه عملی "فناوری اطلاعات و ارتباطات انتظامی"

سامانه نشریات: pitc.jrl.police.ir

سال دوم- شماره چهارم(پیاپی ۸)– زمستان ۱۴۰۰

هوشمندسازی در فضای سایبری با استفاده از محاسبات ابری کوانتومی

دریافت: ۱۴۰۰/۰۷/۲۷

پذیرش: ۱۴۰۰/۱۰/۲۵

نوع مقاله: پژوهشی

صص: ۱۱-۱

شناسه دیجیتال(doi).

10.22034/pitc.2022.1265628.1099

سید نصیب اله دوستی مطلق

استادیار, پژوهشکده آماد، فناوری های دفاعی و پدافند غیرعامل- دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی- تهران- ایران

(نویسنده مسئول)

doustimotlagh@chmail.ir

چکیده

امروزه رایانش ابری و ذخیره آنلاین اطلاعات که جایگزین استفاده از حافظه‌های سخت افزاری شده است در دنیا همه‌گیر شده چراکه انتقال و استفاده از اطلاعات توسط رایانش ابری کم هزینه‌تر، کابردی‌تر، ساده‌تر، سریع‌تر و همچنین در دسترس‌ترین نوع انتقال می باشد؛ لذا خطرات و تهدیدات سایبری نیز چندین برابر گذشته بوده و فناوری‌های حال حاضر و حتی پیشرفته ترین رایانه ها و رمزنگاری های کلاسیک توان مقابله با تهدیدات سایبری در این حجم از انتقال و استفاده از اطلاعات را ندارند. از طرفی محاسبات کوانتومی یکی از پیشرفته ترین نوع انتقال اطلاعات در آینده است که نیازمند وجود و ارائه توسط کامپیوترهای کوانتومی می‌باشد و در آینده تنها راه هوشمندسازی و تامین امنیت سایبری خواهد شد. محاسبات کوانتومی بر ایجاد رایانه‌های بسیار سریع با استفاده از مفاهیم فیزیک کوانتومی متمرکز است، و محاسبات ابری این اجازه را می‌دهد تا این قدرت محاسباتی به عنوان یک سرویس ارائه شود. محاسبات کوانتومی مبتنی بر ابر دسترسی مستقیم به شبیه‌سازها و پردازنده‌های کوانتومی را فراهم می‌کند و این امر می تواند باعث انقلابی بزرگ در هوشمندسازی شود. با ظهور رایانه‌های کوانتومی امنیت سیستم‌های رمزنگاری امروزی به خطر می‌افتد، زیرا بسیاری از رمزنگاری‌های امروزی بر اساس سختی محاسبه عوامل اول اعداد کار می‌کنند و الگوریتم کوانتومی شور می‌تواند این رمزنگاری‌ها را بشکند. هم‌چنین الگوریتم کوانتومی گرور می‌تواند دستیابی به رمزهای عبور را برای ما تسهیل کند.

کلیدواژه‌ها: هوشمندسازی، محاسبات کوانتومی، محاسبات کوانتومی ابری، الگوریتم های کوانتومی، شبیه سازی کوانتومی، رمزنگاری کوانتومی

۱- مقدمه

طراحی و ساخت رایانه‌های کوانتومی بیشتر از حد تصورات امروزه حائز اهمیت هستند چرا که محاسبات کوانتومی یکی از پیشرفته‌ترین نوع انتقال اطلاعات در آینده است که نیازمند وجود و ارائه توسط کامپیوترهای کوانتومی است طور یکه شرکت‌هایی نظیر آی‌بی‌ام، گوگل، مایکروسافت و ... در حال تلاش برای عمومی کردن این تکنولوژی جدید در سریع‌ترین زمان ممکن هستند.

همچنین در چند سال اخیر پژوهشگران به نتایجی دست پیدا کرده‌اند که با استفاده از آن انتقال اطلاعات به شیوه جدید و کاربردی امکان‌پذیر باشد. این تحقیقات تحولی عظیم در امنیت سایبری ایجاد خواهد کرد و در آینده‌ای نه‌چندان دور شاهد این تکنولوژی در دسترس خیلی از کشورهای توسعه‌یافته خواهیم بود.

یکی از مشکلات و چالش‌های امروزه جوامع کاهش امنیت فضای مجازی است چرا که قسمت عمده اطلاعات شخصی و حقوقی مردم در فضای مجازی است که این موضوع در دوران شیوع پاندمی کرونا خود را با شدت بیشتری نشان داد؛ لذا چالش عمده جوامع عدم امنیت کامل فضای مجازی است که مأموریت پلیس فضای مجازی و سازمان‌های امنیتی را بیشتر تحت‌تأثیر قرار داده است. به طور مثال خیلی از سازمان‌ها با تهدیدهای بی‌سابقه‌ای روبه‌رو هستند و داده‌ها و اطلاعات آن‌ها در معرض خطر قرار می‌گیرد. شاید در آینده کاهش تهدیدات امنیت سایبری با موفقیت بیشتری رشد کند. امروزه رایانش ابری در دنیا بطور گسترده‌ای همه‌گیر شده است چراکه انتقال و استفاده از اطلاعات توسط رایانش ابری کم‌هزینه‌تر، سریع‌تر و همچنین در دسترس‌ترین نوع انتقال می‌باشد؛ لذا تهدیدات سایبری نیز چندین برابر گذشته خواهد بود و فناوری‌های حال حاضر توان مقابله با تهدیدات سایبری در این حجم از اطلاعات را ندارند و تنها محاسبات ابری کوانتومی می‌تواند در آینده، امنیت رایانش ابری و انواع دیگر انتقال اطلاعات مخصوصاً در نهادهای نظامی، انتظامی و امنیتی را تأمین کند. در آینده با روی کار آمدن اینترنت نسل پنجم و ششم و استفاده بیشتر جوامع از رایانش ابری و ذخیره آنلاین اطلاعات، بیگ دیتا و آنالیز پیشرفته اطلاعات ، هوش مصنوعی، ماشین لرنینگ، اینترنت اشیا، لباس‌های هوشمند و همکاری انسان و ربات‌ها، بلاک‌چین و تحولات تجاری آینده، واقعیت مجازی، سیستم‌عامل‌های دیجیتال، تکنولوژی الکترونیک بدون سیم و دوربرد و ... به طور خودکار تأمین امنیت سایبری را نیز می‌طلبد و چنین امکانی تاکنون توسط هیچ تکنولوژی خاصی فراهم و حتی پیش‌بینی هم نشده است. خوشبختانه استفاده از محاسبات ابری کوانتومی و رایانه‌های کوانتومی چنین امکانی را فراهم می‌آورد. به طور مثال در آینده انتقال انواع اطلاعات با سرعتی نزدیک به‌سرعت نور انجام خواهد شد و سازمان‌های نظامی و تجاری برای در امان ماندن از هک اطلاعات و تهدیدات سابیری ناگزیر به استفاده از محاسبات ابری کوانتومی خواهند شد چرا که اساس رایانه های کوانتومی می باشند و چنین تکنولوژی یارای مقابله با تهدیدات سایبری را خواهد داشت. لذا مقابله و هوشمند سازی سازمانها در آینده با کمک محاسبات و رایانه های کوانتومی فراهم خواهد شد.

یک رایانه کوانتومی از پدیده‌ها و قوانین مکانیک کوانتوم مانند برهم‌نهی و درهم‌تنیدگی برای انجام محاسباتش استفاده می‌کند و قدرتی فراتر از رایانه‌های کلاسیک دارد[۱]. ریچارد فاینمن برای نخستین بار، در سال ۱۹۸۲ پیشنهاد کرد که باید محاسبات را از دنیای دیجیتال وارد دنیای جدیدی به نام کوانتوم کرد. محاسبات کوانتومی می‌تواند پیامدهای بسیار شگرفی در هر چیز دنیای دیجیتال امروز از هوش مصنوعی گرفته تا توسعه داروها داشته باشد.

یک رایانه کوانتومی می‌تواند به‌راحتی از برخی از ابررایانه‌های برتر جهان پیشی بگیرد و این قدرت پردازش ناشی از وجود کیوبیت‌ها است. در پردازش کوانتومی یک کیوبیت یا بیت کوانتومی واحد پایه‌ای پردازش کوانتومی بوده و مشابه بیت در رایانه‌های کلاسیک می‌باشد که کوچک‌ترین واحد ذخیره اطلاعات است. از نظر فیزیکی، کیوبیت یک سامانه کوانتومی دو حالتی است، یعنی سیستمی که توسط مکانیک کوانتومی به درستی قابل توصیف است و هنگام اندازه‌گیری یکی از دو حالت ممکن خود را اختیار می‌کند. مانند قطبش یک فوتون که در اینجا، جهتِ قطبشِ عمودی و جهتِ قطبشِ افقی دو حالت ممکن برای سامانه هستند. در یک سامانه کلاسیک، هر بیت در هر لحظه یا در حالت صفر و یا در حالت یک است، اما اصل‌های مکانیک کوانتومی به کیوبیت اجازه می‌دهند که در همان حال، حالتی را برابر با برهم‌نهی دو حالت اصلی نیز اختیار کند، یک ویژگی که در پردازش کوانتومی بنیادی است. به عبارتی، یک کیوبیت هم ممکن است در حالت‌های کلاسیک صفر و یک وجود داشته باشد و هم می‌تواند در حالت ترکیب این دو قرار گیرد (هم‌زمان دارای هر دو حالت صفر و یک باشد). در واقع همین پدیده، تفاوت اصلی بین بیت‌های کلاسیک و کیوبیت‌ها است[۲]. رایانه‌های کوانتومی بیشتر در زمینه‌هایی نظیر هواشناسی، مدل‌سازی شیمی و فیزیک و رمزنگاری کاربرد دارند. مسئله مهمی که در زمینه امنیت داده‌ها وجود دارد این است که امروزه اطلاعات به‌صورت رمزنگاری شده مخابره می‌شوند تا امنیت آن‌ها حفظ شود. رایانه‌های کوانتومی باتوجه‌به قدرت محاسباتی بالای خود می‌توانند این رمزنگاری‌ها را شکسته و امنیت اطلاعات را به خطر بیندازند. این رایانه‌ها از الگوریتم‌های کوانتومی برای این کار بهره می‌گیرند. کاربردی که محاسبات ابری کوانتومی در زمینه امنیت داده‌ها دارد این است که تا زمانی که رایانه‌های کوانتومی که در اختیار عموم قرار گیرد، ساخته نشده‌اند، می‌توان با بهره‌گیری از سخت‌افزارها و نرم‌افزارهای موجود که شرکت‌های پیشرو در این زمینه، از طریق فضای ابری (اینترنت) در اختیار ما قرار می‌دهند، به محاسبات کوانتومی و اجرای الگوریتم‌های کوانتومی پرداخت و خود را برای مواجهه با تهدید امنیتی رایانه‌های کوانتومی آماده کرد. در بخش دوم این مقاله

تاریخچه‌ای از محاسبات ابری کوانتومی بیان شده است، موضوع محاسبات کوانتومی به تفسیر در بخش سوم توضیح داده شده، در بخش چهارم مقاله اختراع‌های ثبت شده در زمینه محاسبات ابری کوانتومی (بخش چهارم به بعد در این مقاله روش پیشنهادی است)، محاسبات ابری کوانتومی و نتایج نرم‌افزارهای آفلاین برای محاسبات کوانتومی به ترتیب در بخش پنجم و ششم آورده شده است و نهایتاً در بخش هفتم نتایج مقاله بیان شده است.

۲- تاریخچه محاسبات ابری کوانتومی

آغاز رسمی محاسبات کوانتومی در سال ۱۹۸۰ بود. جایی که بنیوف[1] در کار خود نشان داد که تبدیل‌های یکانی معادل با همان گیت‌های[2] منطقی مورد استفاده در محاسبات است و می‌توان محاسبات را با استفاده از این تبدیل‌ها انجام داد [۳]. در سال ۱۹۸۵، دیوید دویچ[3] با استفاده از توازی[4] کوانتومی، الگوریتمی را برای تعیین توابع ثابت و متوازن معرفی کرد [۴]. پس از آن، او به همراه جوزا[5] این روش را توسعه داده و توانستند این خصوصیت را برای توابع با ورودی بیشتر هم به کار ببرند [۵]. در سال ۱۹۸۲ فاینمن پیشنهاد ورود به دنیای کوانتوم و رایانه کوانتومی را مطرح کرد [۶].

پیتر شور در سال ۱۹۹۴ الگوریتمی کوانتومی، برای تجزیه عددها به عوامل اول اختراع کرد [۷]. پس از او، لو گرور[6] الگوریتمی را معرفی کرد که از رایانه‌های کوانتومی برای جستجو در پایگاه داده‌های نامرتب استفاده می‌کند. در راستای پیشرفت در زمینه محاسبات کوانتومی و در سال ۲۰۰۱، پژوهشگران شرکت آی‌بی‌ام توانستند عدد ۱۵ را به عوامل اول آن یعنی ۳ و ۵ تجزیه کنند [۸]. در همین سال رابرت راساندورف و هانس جی بریگل[7] پیشنهاد محاسبات کوانتومی مبتنی بر اندازه‌گیری را دادند [۹]. در سال ۲۰۰۴، اولین درهم‌تنیدگی پنج فوتون توسط گروه جیان وی پان[8] در دانشگاه علم و صنعت چین، نشان داده شد [۱۰]. چندین سال بعد و در سال ۲۰۰۹، اولین پردازنده کوانتومی الکترونیکی ایجاد شد[۱۱].. در همین سال، نزدیک‌ترین مورد به یک رایانه کوانتومی، یعنی ترانزیستور نوری ساخته شده از یک تک مولکول، ارائه شد [۱۲]. یک سال بعد و در سال ۲۰۱۰، محققان توانستند با استفاده از رایانه کوانتومی نوری، با سه کیوبیت طیف انرژی هیدروژن مولکولی را بادقت بالا محاسبه کنند [۱۳].

در همین سال، اولین رایانه ۱۲۸ کیوبیتی تجاری(D-wave one) ساخته شد [۱۴]. سپس پیش از پایان سال ۲۰۱۲ تلاش برای ساخت رایانه کوانتومی ۵۱۲ کیوبیتی تجاری (D- wave two) آغاز شد و در سال ۲۰۱۳ این رایانه ساخته شد [۱۵]. هم چنین در سال ۲۰۱۲، فیزیکدانان استرالیایی و آمریکایی یک ترانزیستور کارا، از تک اتم فسفر که در یک کریستال سیلیکون قرار داشت، ساختند [۱۶]. در سال ۲۰۱۴ اتفاقی بزرگ در محاسبات کوانتومی رخ داد و آن تجزیه عدد ۵۶۱۵۳ به عوامل اولش بود [۱۷]. توسعه گیت منطقی سیلیکونی دوکیوبیتی در سال ۲۰۱۵ [۱۸] ساخت رایانه کوانتومی ۱۷ کیوبیتی در سال ۲۰۱۷ توسط شرکت آی‌بی‌ام [۱۹] ز جمله کارهای ارزشمند جدیدی است که در سال‌های اخیر انجام گرفته است. در تاریخ ۵ مارس ۲۰۱۸ میلادی، گردهمایی جامعه فیزیک آمریکا شاهد رونمایی از آخرین دستاورد فیزیکدانان گوگل بود: تراشه‌ای به نام «بریستلکون» که می‌تواند محاسبات کوانتومی را با پردازش ۷۲ کیوبیت انجام دهد. در حال حاضر علاوه بر دانشگاه‌ها و مراکز تحقیقاتی، شرکت‌های مختلفی مانند آی‌بی‌ام، مایکروسافت، اینتل و ... به پژوهش در حوزه محاسبات کوانتومی مشغولند. در سال ۲۰۱۸، خدمات ابری جدیدی مبتنی بر رزونانس مغناطیسی هسته[9] معرفی شد. این سرویس آنلاین به محققان اجازه می‌دهد تا به قدرت پردازش ۴ کیوبیت دسترسی داشته باشند [۲۰]. در همین سال، یک کار بسیار بزرگ و ارزشمند با استفاده از رایانه‌های کوانتومی در دسترس شرکت های آی‌بی‌ام و ریجتی صورت پذیرفت و آن محاسبات کوانتومی ابری یک هسته اتمی بود. در واقع یک شبیه‌سازی کوانتومی از انرژی بستگی دوترون انجام شد و نتایج به‌دست‌آمده بسیار نزدیک به نتایج نظری بودند [۲۱]. پس از آن، یک شبیه‌سازی از مدار کوانتومی ۶۴ کیوبیتی انجام شد. این کار امکان شبیه‌سازی کیوبیت‌های بیشتر با بار سخت‌افزاری کمتر را فراهم می‌کند و چشم‌انداز جدیدی را برای شبیه سازی‌های کلاسیک ترسیم می‌کند [۲۲]. در سال ۲۰۱۹، شبیه‌سازی سیستم‌های کوانتومی بس-ذره‌ای با استفاده از خدمات ابری شرکت آمازون مورد بررسی قرار گرفت. روش پیشنهادی باعث کاهش زمان محاسبه و میزان حافظه مورد استفاده می‌شود [۲۳]. در همین سال محققان گوگل ادعا کردند که با استفاده از یک پردازنده کوانتومی ۵۳ کیوبیتی توانستند برتری کوانتومی را به نمایش بگذارند و مسئله‌ای را که با استفاده از یک رایانه کلاسیک ده‌هزار سال طول می‌کشد تا بتوان آن را حل نمود، تنها در حدود ۲۰۰ ثانیه حل کردند [۲۴]. تولید اعداد تصادفی با استفاده از پردازنده کوانتومی ۲۰ کیوبیتی شرکت آی‌بی‌ام نیز از دیگر کارهای انجام شده در این سال است [۲۵]. در یکی از کارهای اخیر، توصیف کاملی از گیت‌های کوانتومی که به طور مستقیم قابل‌اجرا در پردازنده‌های کوانتومی آی‌بی‌ام هستند، صورت پذیرفته است [۲۶]. باتوجه‌به سرعت بالای پیشرفت در حوزه محاسبات ابری کوانتومی، امید است که به‌زودی رایانه‌های کوانتومی با تعداد کیوبیت بیشتر برای انجام تحقیقات در حوزه شبیه‌سازی و ساخت دارو و رمزنگاری ساخته شوند.

[1] Benioff
[2] Gate
[3] D. Deutsch
[4] Parallelism
[5] Jozsa
[6] Lov Grover
[7] Robert Raussendorf and Hans J. Briegel
[8] Jian-Wei Pan
[9] NMR

۳- محاسبات کوانتومی

محاسبات کوانتومی به بررسی الگوریتم‌ها و سخت‌افزارهای کوانتومی موردنیاز برای پیاده‌سازی عملی آن‌ها می‌پردازد. یک بیت، واحد بنیادی اطلاعات در رایانه‌های کوانتومی است. یک کیوبیت به بیت کلاسیک شباهت هایی دارد، اما در کل بسیار متفاوت است. اختلاف این است که درحالی‌که یک بیت کلاسیکی باید در هر لحظه یا در حالت صفر یا در حالت یک باشد، یک کیوبیت می‌تواند در حالت صفر، یک یا ترکیب خطی صفر و یک نیز قرار گیرد. دو حالتی که در آن مقدار یک کیوبیت ممکن است اندازه‌گیری شود، حالت‌های پایه (بردارهای پایه) نامیده می‌شوند. حالت‌های کوانتومی را، همانند حالت‌های کیوبیت‌ها، با نمادگذاری برا-کت دیراک [1] نمایش می‌دهند. یعنی دو حالت پایه محاسباتی به صورت $|0\rangle$ و $|1\rangle$ نوشته می‌شوند که کتِ یک و کتِ صفر خوانده می‌شود. حالت یک کیوبیت خالص، برهم نهی خطی دو حالت پایه است؛ یعنی یک کیوبیت می‌تواند به صورت برهم‌نهی خطی $|0\rangle$ و $|1\rangle$ نمایش داده شود:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (۱)$$

۳-۱- مدارهای کوانتومی

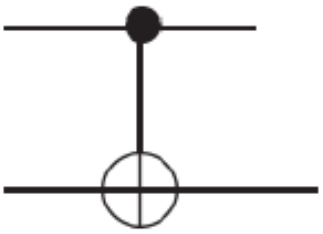
مدار کوانتومی مدلی برای محاسبات کوانتومی است که در آن، از کنار هم قراردادن گیت‌های کوانتومی برای انجام محاسبات استفاده می‌شود. گیت‌های کوانتومی، تبدیلات یکانی هستند که روی تعداد کمی کیوبیت عمل می‌کنند. مهم‌ترین گیت‌های کوانتومی در زیر معرفی شده‌اند:[2]

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad (۲)$$

دسته دیگری از گیت‌های کوانتومی گیت‌های کنترلی هستند. یکی از مهم‌ترین این گیت‌ها، گیت **CNOT** است که دو کیوبیت ورودی دارد که یکی کیوبیت کنترل و دیگری کیوبیت هدف است. عملیاتی که گیت **CNOT** انجام می‌دهد را می‌توان به‌صورت/ نوشت که اگر کیوبیت کنترل / باشد کیوبیت هدف تغییر می‌کند و در غیر اینصورت تغییری صورت نمی‌گیرد. یک ماتریس / است:

$$CNOT = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix} \qquad (۳)$$

در مدارها این گیت به صورت زیر نمایش داده می‌شود که در آن، کیوبیت بالایی، کیوبیت کنترل و پایینی کیوبیت هدف است.



شکل (۱): گیت CNOT

۳-۲-الگوریتم‌های کوانتومی

الگوریتم کوانتومی الگوریتمی است که روی مدلی واقعی از یک رایانه کوانتومی اجرا می‌شود. مسئله‌های غیر قابل‌حل با الگوریتم‌های کلاسیک همچنان با الگوریتم کوانتومی غیر قابل‌حل است، اما مزیت الگوریتم کوانتومی این است که مسئله‌های قابل‌حل با زمان کمتری حل می‌شوند. از معروف‌ترین الگوریتم‌های کوانتومی می‌توان الگوریتم شور[2] برای تجزیه اعداد به عوامل اول و الگوریتم گرور[3] برای جستجو در یک پایگاه‌داده نامرتب را نام برد.

۳-۲-۱-تبدیل فوریه[4]

یکی از راه‌های مناسب برای حل مسائل در ریاضیات و علوم رایانه این است که آن را به یک مسئله دیگر تبدیل کنیم که برای آن یک راه‌حل شناخته‌شده وجود دارد [۲]. دستاورد بزرگ محاسبات کوانتومی این بوده است که برخی از چنین تبدیلاتی را می‌توان بسیار سریع‌تر از یک رایانه کلاسیک روی یک رایانه کوانتومی محاسبه کرد. یکی از این تبدیلات، تبدیل گسسته فوریه است. تبدیل گسسته فوریه به‌عنوان ورودی یک بردار از اعداد مختلط را می‌گیرد، که طول N بردار یک پارامتر ثابت است. داده‌های $x_0,...,x_{N-1}$ تبدیل شده را به‌عنوان خروجی می‌دهد که یک بردار شامل اعداد مختلط $y_0,...,y_{N-1}$ است. تعریف آن به‌صورت زیر است:

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N} \qquad (۴)$$

تبدیل فوریه کوانتومی دقیقا همین تبدیل است. اگر چه نماد متعارف برای تبدیل فوریه کوانتومی تا حدودی متفاوت است. تبدیل فوریه کوانتومی روی پایه‌هایی که همه آن‌ها بردارهای واحد هستند و به هم عمود می‌باشند، $|0\rangle,...,|N-1\rangle$ به این صورت تعریف می‌شود که یک عملگر خطی روی حالت‌های پایه به صورت زیر می باشد:

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle \qquad (۵)$$

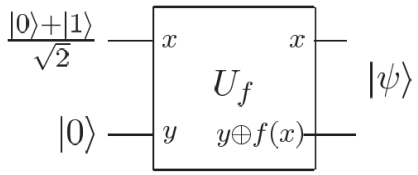
از جمله الگوریتم‌هایی که از تبدیل فوریه بهره می‌گیرند، تخمین فاز کوانتومی و الگوریتم شور را می‌توان نام برد.

[1] Dirac

[2] Shor's algorithm
[3] Grover's algorithm
[4] Fourier transform

۳-۲-۲-توازی کوانتومی

توازی کوانتومی یکی از ویژگی‌های اساسی بسیاری از الگوریتم‌های کوانتومی است [۲]. این ویژگی به رایانه‌های کوانتومی اجازه می‌دهد که تابع $f(x)$ را برای بسیاری از مقادیر مختلف x به طور هم‌زمان تعیین کنند. فرض کنید که تابع $f(x)$ یک تابع تک‌بیتی به‌صورت $f(x):\{0,1\}\to\{0,1\}$ باشد. یک روش مناسب برای محاسبه این تابع در یک رایانه کوانتومی، درنظرگرفتن یک رایانه کوانتومی دو کیوبیتی است که در شروع در حالت $|x,y\rangle$ قرار دارد. با یک ترتیب مناسب از گیت‌های منطقی، این حالت را می‌توان به حالت $|x,y\oplus f(x)\rangle$ تبدیل کرد. اولین رجیستر، رجیستر داده و دومین رجیستر، رجیستر هدف نام دارد. در واقع رجیستر کوانتومی سیستمی متشکل از چند کیوبیت است. ما این تبدیل را که به‌وسیله نگاشت $|x,y\rangle\to|x,y\oplus f(x)\rangle$ تعریف می‌شود، به نام U_f نام‌گذاری می‌کنیم. اگر $y=0$ باشد، حالت نهایی دومین کیوبیت فقط مقدار $f(x)$ خواهد بود.



شکل (۲): مدار کوانتومی برای محاسبه هم‌زمان $f(0)$ و $f(1)$

مدار نشان‌داده‌شده در شکل بالا را در نظر بگیرید. رجیستر داده‌ها در حالت برهم‌نهی یعنی حالت $|0\rangle+|1\rangle/\sqrt{2}$ آماده شده است که می‌تواند توسط اعمال یک گیت هادامارد روی $|0\rangle$ ایجاد شود. سپس ما U_f را اعمال می‌کنیم. نتیجه به صورت زیر خواهد بود:

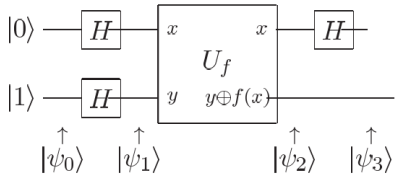
$$\frac{|0,f(0)\rangle+|1,f(1)\rangle}{\sqrt{2}} \qquad (۶)$$

این یک حالت جالب توجه است. جملات مختلف شامل اطلاعاتی درباره هر دوی $f(0)$ و $f(1)$می‌باشد. این‌گونه به نظر می‌رسد که ما $f(x)$ را به ازای دو مقدار x به طور همزمان تعیین کرده‌ایم. این ویژگی تحت عنوان توازی کوانتومی شناخته می‌شود.

۳-۳-۳-الگوریتم دویچ[1]

دویچ نشان داد وقتی می‌خواهیم بفهمیم که آیا تابع داده شده یک تابع ثابت است و یا متوازن(منظور از تابع ثابت، تابعی است که خروجی‌اش همواره یک مقدار ثابت و مستقل از ورودی است و منظور از تابع متوازن، تابعی است که خروجی‌اش به‌ازای نیمی از ورودی‌ها برابر با ۰ و به‌ازای نیمی دیگر برابر با ۱ است) می‌توان این مسئله را با الگوریتم کوانتومی تنها با یک‌بار فراخوانی حل کرد. روش کار این الگوریتم به‌صورت زیر است:

از گیت هادامارد برای آماده‌سازی کیوبیت اول در یک حالت برهم‌نهی ($|0\rangle+|1\rangle/\sqrt{2}$) استفاده می‌کنیم [۴و۲]. کیوبیت دوم یعنی yرا در حالت برهم‌نهی ($|0\rangle-|1\rangle/\sqrt{2}$) با اعمال گیت هادامارد روی حالت $|1\rangle$ آماده می‌کنیم. مدار کوانتومی که الگوریتم دویچ را پیاده‌سازی می‌کند در شکل زیر نشان داده شده است:



شکل (۳): مدار کوانتومی که الگوریتم دویچ را اجرا می‌کند.

حالت ورودی به صورت زیر می باشد:

$$|\psi_0\rangle=|01\rangle \qquad (۷)$$

پس از تاثیر دو گیت هادامارد، حالت زیر را خواهیم داشت:

$$|\psi_1\rangle=\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \qquad (۸)$$

در صورت تاثیر U_f بر حالت $|x\rangle\left(|0\rangle-|1\rangle\right)/\sqrt{2}$، حالت زیر را به دست می‌آوریم:

$$(-1)^{f(x)}|x\rangle\left(|0\rangle-|1\rangle\right)/\sqrt{2} \qquad (۹)$$

بنابراین تاثیر U_f بر حالت $|\psi_1\rangle$ یکی از دو احتمال زیر را به دست می دهد:

(۱۰)

$$|\psi_2\rangle=\begin{cases}\pm\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & if\ \ f(0)=f(1)\\ \pm\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & if\ \ f(0)\neq f(1)\end{cases}$$

اعمال گیت هادامارد نهایی روی کیوبیت اول، حالت نهایی زیر را به ما می دهد:

$$|\psi_3\rangle=\begin{cases}\pm|0\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & if\ \ f(0)=f(1)\\ \pm|1\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & if\ \ f(0)\neq f(1)\end{cases} \qquad (۱۱)$$

می‌توانیم این نتیجه را به صورت خلاصه به شکل زیر بنویسیم:

$$|\psi_3\rangle=\pm|f(0)\oplus f(1)\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right], \qquad (۱۲)$$

بنابراین با اندازه‌گیری کیوبیت اول ما می‌توانیم مقدار

[1] Deutsch's algorithm

$f(0) \oplus f(1)$ را تعیین کنیم. این مسئله بسیار جالب‌توجه است. در واقع مدار کوانتومی امکان تعیین یک ویژگی سراسری از $f(x)$ را که $f(0) \oplus f(1)$ است، برای ما فراهم می‌کند (آن هم تنها با استفاده از یک بار ارزیابی $f(x)$).

۳-۳-۴-الگوریتم شور

پیتر شور در سال ۱۹۹۴ الگوریتمی کوانتومی، برای تجزیه عددها به عوامل اول اختراع کرد. روش شور قادر است در زمانی از مرتبه چندجمله‌ای، یک عدد را به عوامل اول تجزیه کند. در رایانه‌های کلاسیک اعتقاد بر این است که تجزیه به عوامل اول کاری سخت است و تجزیه اعداد بزرگ روی یک رایانه کلاسیک می‌تواند چندین سال طول بکشد، درحالی‌که روی یک رایانه کوانتومی، می‌تواند در چند دقیقه انجام شود. این موضوع زمانی اهمیت بیشتری می‌یابد که بدانیم بسیاری از الگوریتم‌های رمزنگاری امروزی از جمله RSA ، بر اساس سختی محاسبه عوامل اول کار می‌کند. در صورت ساخت رایانه کوانتومی، این‌گونه رمزنگاری‌ها در مدت زمانی کوتاه شکسته خواهند شد. در واقع، شور توانست از توازی موجود در رایانه‌های کوانتومی به‌منظور عامل‌یابی اعداد استفاده کند. این الگوریتم، عملاً بسیار ساده بود [۲۷]. یک عدد برای عامل‌یابی دریافت می‌شود (N). مقداری کمتر از N برای a انتخاب می‌شود. با فرض اینکه N، **حاصل‌ضرب** دو عدد اول است، a باید نسبت به N نیز اول باشد. به‌ازای مقادیر مختلف x، تابع $f(x) = (a^x \bmod N)$ محاسبه می‌شود. تمام این عملیات با توان محاسباتی کوانتومی می‌تواند در واحد زمان انجام شود. یک الگوی تکرار، در نتایج تابع وجود دارد که دوره این تکرار را باید پیدا کرد. دوره با r نشان داده می‌شود. سپس مقادیر $\gcd(a^{r/2}+1, N)$ و $\gcd(a^{r/2}-1, N)$ محاسبه می‌شوند. حداقل یکی از این مقادیر باید عاملی از N باشد که این فرضیه به دلیل برقراری تساوی $a^r = (1 \bmod N)$ امکان‌پذیر بوده و طی رابطه زیر نشان‌داده‌شده است:

$$a^r - 1 = (a^{r/2}-1).(a^{r/2}+1) = 0 \bmod N \qquad (۱۳)$$

به این صورت، $(a^{r/2}-1).(a^{r/2}+1)$ مضرب صحیحی از N است.

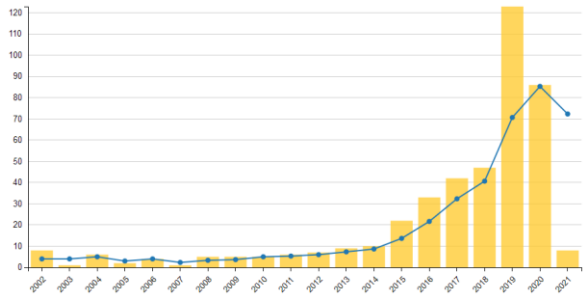
۳-۳-۵- الگوریتم گرور

صورت یک مسئله جستجو را می‌توان به این شکل بیان کرد. مجموعه/ شامل N شی است. تابعی مثل/ روی این مجموعه تعریف شده است. می دانیم که مقدار تابع f تنها روی یکی از عناصر این مجموعه که آن را با w نشان می‌دهیم برابر یک است و روی عناصر دیگر این مجموعه مقدار تابع برابر صفر است. w یکی از/هاست، ولی نمی‌دانیم که کدام یک از آنهاست. در غیاب هر نوع اطلاعات اضافه‌ای، تنها کاری که باید بکنیم این است که /های مختلف را یک به یک به تابع بدهیم و خروجی تابع را نگاه کنیم. هرگاه خروجی تابع f برابر با یک شد می‌فهمیم که عنصر داده شده به تابع w بوده است.

الگوریتم جستجوی گرور نشان می‌دهد که چگونه ویژگی‌های سیستم‌های کوانتومی را می‌توان برای بهبود محدوده زمان اجرا پایین‌تر از الگوریتم‌های کلاسیک به کار گرفت[28]. این الگوریتم کوانتومی برای اولین بار توسط گرور ارائه شد[29]. این الگوریتم در $O(\sqrt{N})$ مرحله به جستجوی یک حالت از N حالت می‌پردازد و از الگوریتم متعارف کلاسیکی که در $O(N)$ مرحله به جواب می‌رسد سریعتر است.

۴- اختراع‌های ثبت شده در زمینه محاسبات ابری کوانتومی

در این بخش به بررسی ثبت اختراع‌های صورت‌گرفته در حوزه محاسبات ابری کوانتومی می‌پردازیم. ابتدا به تحلیل اختراع‌های ثبت شده در حوزه سخت‌افزار کوانتومی می‌پردازیم. این کار با جستجوی کلیدواژه سخت‌افزار کوانتومی[1] در تاریخ ۶ اسفند ۱۳۹۹ در وب‌سایت patentinspiration انجام شده است.



شکل (۱۳): ثبت اختراع‌های صورت‌گرفته در حوزه سخت‌افزار کوانتومی

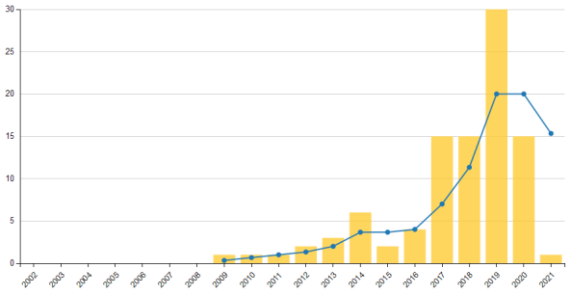
مشاهده می‌کنیم که از سال ۲۰۱۴ به بعد سیری صعودی در حوزه سخت‌افزار کوانتومی شکل‌گرفته که در سال ۲۰۱۹ تعداد پتنت‌ها به شکل قابل‌توجهی افزایش پیدا کرده است.

شکل (۱۴): کشورهای ارائه‌دهنده پتنت در زمینه سخت‌افزار کوانتومی

با توجه به شکل (۱۴) مشاهده می‌کنیم که کشورهای آمریکا و چین بیشترین سهم را در این زمینه دارند.

[1] Quantum hardware

در ادامه، با استفاده از کلیدواژه محاسبات ابری کوانتومی، به تحلیل اختراع‌های ثبت شده در این زمینه می‌پردازیم.



شکل (۱۵): ثبت اختراع‌های صورت گرفته در حوزه محاسبات ابری کوانتومی

شکل (۱۶): کشورها و شرکت‌های ارائه‌دهنده پتنت درزمینه‌ی محاسبات ابری کوانتومی

در حوزه محاسبات ابری کوانتومی نیز کشورهای آمریکا و چین بیشترین تعداد ثبت اختراع را دارند.

۵-محاسبات ابری کوانتومی

محاسبات ابری کوانتومی این اجازه را به فرد می‌دهد تا بدون این‌که به منابع سخت‌افزاری و نرم‌افزاری گران‌قیمت دسترسی داشته باشد، بتواند به محاسبات کوانتومی موردنظر خود بپردازد. در این بخش مهم‌ترین سرویس‌های آنلاین و نرم‌افزارهای آفلاین در دسترس برای انجام محاسبات کوانتومی را معرفی می‌کنیم.

۵-۱-محاسبات ابری شرکت ریجتی[1]

خدمات ابری ارائه شده توسط شرکت ریجتی(به نام فارست[2]) شامل مجموعه ابزاری برای محاسبات کوانتومی است. پایکیول[3] بخشی از مجموعه ابزار شرکت ریجتی برای برنامه‌نویسی کوانتومی در فضای ابری است. در واقع، کتابخانه پایتون منبع بازی است که در محاسبات ریجتی طراحی شده است که برنامه‌هایی را برای رایانه‌های کوانتومی ایجاد می‌کند [۳۰].

این یک شبیه‌سازی کلاسیک از یک پردازنده کوانتومی است که می‌تواند عملیات کیوبیتی مختلف را شبیه‌سازی کند. تنظیمات پیش‌فرض به ما اجازه دسترسی به ۲۶ کیوبیت برای اجرای شبیه‌سازی‌هایمان را می‌دهد. پایکیول همچنین شامل برخی ارتباطات ویژه است که اجازه می‌دهد تا آزمایش‌های خود را روی پردازنده‌های کوانتومی ابررسانای ریجتی انجام دهیم. برای مثال، برنامه‌ای که تأثیر ماتریس واحد روی حالت $|0\rangle$ را نشان می‌دهد به‌صورت زیر نوشته می‌شود:

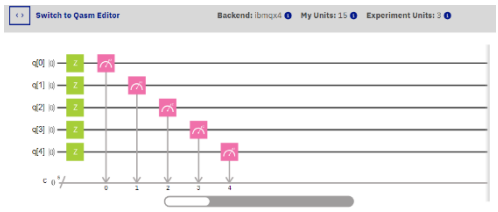
```
from pyquil.quil import Program
from pyquil.api import QVMConnection
from pyquil.gates import I
qvm = QVMConnection()
p = Program(I(0))
wf = qvm.wavefunction(p)
print(wf)
(1+0j)|0>                                    (۱۴)
```

ملاحظه می‌شود که تاثیر این ماتریس واحد روی حالت $|0\rangle$ این است که آن را بدون تغییر باقی می‌گذارد.

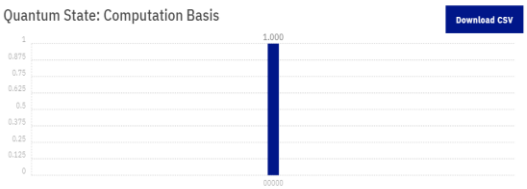
۵-۲-محاسبات ابری شرکت آی‌بی‌ام

خدمات ابری ارائه‌شده توسط شرکت آی‌بی‌ام(تجربه کوانتوم) شامل یک شبیه‌ساز و پردازنده ۵ یا ۱۶ یا ۲۰ کیوبیتی است. کاربران می‌توانند از طریق مدل مداری محاسبات با پردازنده کوانتومی تعامل داشته باشند و همچنین گیت‌های کوانتومی را روی کیوبیت‌ها تأثیر دهند و کدهای زبان اسمبلی کوانتومی را بنویسند. البته شرکت آی‌بی‌ام اعلام کرده به‌زودی امکان دسترسی کاربران و مشتریان به رایانه کوانتومی (۵۰ کیوبیتی) خود را از طریق فضای ابری میسر خواهد کرد و محققان و دانشجویان از سراسر دنیا می‌توانند با استفاده از ابزار قدرتمند جدید، پروژه‌های متنوعی را انجام دهند. این خدمات ابری قسمت‌های مختلفی را شامل می‌شود. زبان اسمبلی کوانتومی به نام OpenQasm برای برنامه‌نویسی مورداستفاده قرار می‌گیرد. این امکان برای ما وجود دارد تا گیت‌های مختلف را روی ۵ کیوبیت که در حالت اولیه صفر قرار دارند اثر دهیم و حالت نهایی سیستم را به دست آوریم. همچنین می‌توان با استفاده از این امکان، الگوریتم‌های کوانتومی را پیاده‌سازی کرد [۳۱]. شکل زیر مثالی است که در آن، گیت Z را روی تمامی ۵ کیوبیت اولیه اثر داده‌ایم. حالت نهایی سیستم به‌صورت زیر به دست می‌آید:

[1] Rigetti
[2] Forest
[3] pyQuil



شکل (۴): تاثیر گیت Z روی ۵ کیوبیت



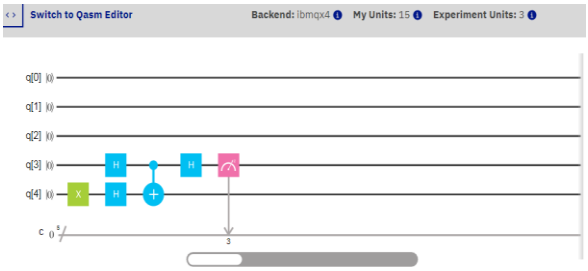
شکل (۵):حالت نهایی سیستم بعد از تاثیر گیت Z روی ۵ کیوبیت

این تاثیر در OpenQasm به‌صورت زیر نوشته می‌شود:

```
include "qelib1.inc";
qreg q[5];
creg c[5];
z q[0];
z q[1];
z q[2];
z q[3];
z q[4];
measure q[0] -> c[0];
measure q[1] -> c[1];
measure q[2] -> c[2];
measure q[3] -> c[3];
measure q[4] -> c[4] ;
```
(۱۵)

۵-۲-۱-اجرای الگوریتم دویچ روی رایانه کوانتومی آی-بی‌ام

همان‌طور که گفتیم، دویچ نشان داد که تنها با یک‌بار فراخوانی تابع می‌توان نشان داد که تابع داده شده یک تابع ثابت است یا متوازن؟ حال می‌خواهیم این الگوریتم را با استفاده از دو کیوبیت برای $f(x)=x$ اجرا کنیم. مدار کوانتومی که اجرای این الگوریتم را نشان می‌دهد به‌صورت زیر است:

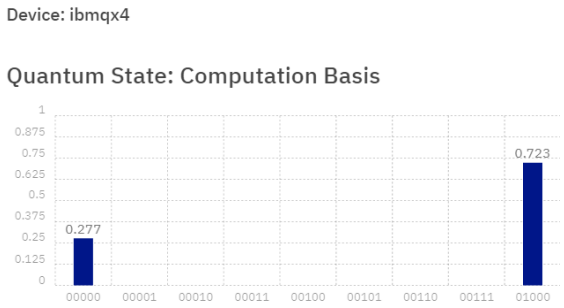


شکل (۶): مدار کوانتومی که الگوریتم دویچ را اجرا می‌کند.

این که چرا این مدار به‌صورت بالا است، علتش این است که در الگوریتم دویچ می‌بایست در ابتدا کیوبیت اول در حالت صفر و کیوبیت دوم در حالت یک باشند. تأثیر گیت X روی کیوبیت دوم آن را از حالت صفر به حالت یک می‌برد. سپس با تأثیر گیت هادامارد روی هر دو کیوبیت، حالت سیستم به‌صورت زیر خواهد بود:

$$|\psi_1\rangle=\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \quad (۱۶)$$

باتوجه‌به اینکه تأثیر U_f به‌صورت $|x,y\rangle\rightarrow|x,y\oplus f(x)\rangle$ است و اینکه داریم: $f(x)=x$ در نتیجه این تأثیر با استفاده از گیت CNOT اعمال می‌شود. با اعمال گیت هادامارد نهایی روی کیوبیت اول و سپس اندازه‌گیری آن، می‌توانیم مقدار $f(0)\oplus f(1)$ را تعیین کنیم. پس از اندازه‌گیری داریم:



شکل (۷): نتیجه اندازه‌گیری روی کیوبیت اول در الگوریتم دویچ

با توجه به نتیجه اندازه‌گیری، حالت {01000}با بیشترین دامنه احتمال ظاهر شده است، در نتیجه می‌توان گفت که $f(0)\oplus f(1)$ برابر با یک است و یا به‌عبارت‌دیگر $f(0)\neq f(1)$ هست و بنابراین تابع f یک تابع متوازن است.

۵-۲-۲-اجرای الگوریتم گرور روی رایانه کوانتومی آی-بی‌ام

می‌دانیم که در الگوریتم گرور مقدار تابع f تنها روی یکی از عناصر این مجموعه که آن را با w نشان می‌دهیم برابر یک است و روی عناصر دیگر این مجموعه مقدار تابع برابر صفر است. هرگاه خروجی تابع f برابر با یک شد می فهمیم که عنصر داده شده به تابع w بوده است. در الگوریتم گرور، یک عملگر یکانی U_w داریم که به صورت زیر اثر می‌کند:

$$\begin{aligned} U_w|x\rangle &= -|x\rangle, \text{ for } x=w, \text{ if } f(x)=1 \\ U_w|x\rangle &= |x\rangle, \text{ for } x\neq w, \text{ if } f(x)=0 \end{aligned} \quad (۱۷)$$

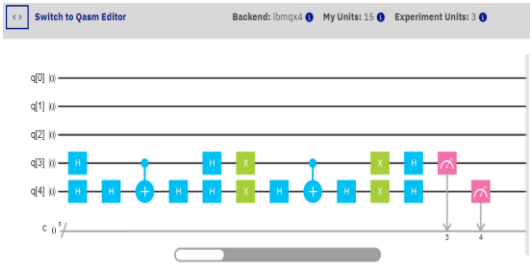
مراحل این الگوریتم عبارت‌اند از:

۱- قرار دادن سیستم در حالت اولیه $|s\rangle=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$

۲- تاثیر عملگر U_w و سپس تاثیر عملگر $U_s=2|s\rangle\langle s|-I$

۳- انجام اندازه‌گیری

کوچکترین مدار کوانتومی که اجرای این الگوریتم را نشان می‌دهد به‌صورت زیر است:



شکل (۸): مدار کوانتومی که الگوریتم گرور را اجرا می‌کند.

بخش اول این مدار برهم‌نهی ایجاد می‌کند. بخش دوم تاثیر U_w را نشان می‌دهد و بخش نهایی مدار، U_s را اجرا می‌کند. برای مثال فرض کنید که ما به دنبال حالت $\{1, 1\}$ هستیم. با انجام اندازه‌گیری نتیجه به‌صورت جدول (۱) به دست می‌آید:

جدول (۱): نتیجه اندازه‌گیری حالت های کوانتومی در الگوریتم گرور

حالت کوانتومی	دامنه احتمال وجود
$\|0,0\rangle$	0.055
$\|0,1\rangle$	0.125
$\|1,0\rangle$	0.223
$\|1,1\rangle$	0.598

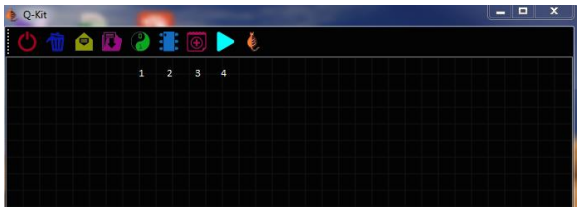
این اجرا روی رایانه کوانتومی واقعی ۵ کیوبیتی آی‌بی‌ام انجام گرفته است. نتیجه این‌که حالت $\{1, 1\}$ با بیشترین دامنه احتمال به‌دست آمده است.

۶-نتایج نرم‌افزارهای آفلاین برای محاسبات کوانتومی

علاوه بر خدمات ابری ارائه‌شده توسط شرکت‌های پیشرو در زمینه محاسبات ابری کوانتومی، تعدادی نرم‌افزار آفلاین برای انجام محاسبات کوانتومی و پیاده‌سازی الگوریتم‌های کوانتومی وجود دارند که در این‌جا به بررسی آن‌ها می‌پردازیم.

۶-۱-کیت کوانتوم

کیت کوانتوم [1] یک شبیه‌ساز مدار کوانتومی گرافیکی است و امکان ساخت و طراحی مدارهای کوانتومی را فراهم می‌کند [۳۲]. برای اهداف آموزشی و پژوهشی مناسب است و به‌صورت رایگان در دسترس است. در حال حاضر می‌تواند تا ۲۰ کیوبیت (بیش از یک میلیون حالت کوانتومی در حالت برهم‌نهی) را شبیه‌سازی کند. مهم‌ترین ویژگی آن، این است که می‌توان آن را روی رایانه شخصی نصب نمود و به انجام محاسبات کوانتومی موردنظر پرداخت. با استفاده از این نرم‌افزار می‌توان الگوریتم‌های کوانتومی را پیاده‌سازی کرد و با استفاده از ترکیب چند گیت، گیت موردنظر خود را ساخت. حالت نهایی سیستم را هم به‌صورت نموداری و هم متنی در اختیار می‌گذارد. یکی دیگر از ویژگی‌های منحصربه‌فرد آن این است که U_f مربوط به الگوریتم‌هایی چون دویچ را به‌صورت آماده در خود دارد و نیاز نیست که کاربر خود به تعریف آن‌ها بپردازد. شکل زیر محیط این نرم‌افزار را نشان می‌دهد:



شکل (۹): محیط Q-kit

مهم‌ترین قسمت‌های آن در شکل با اعداد مشخص شده‌اند.

۱: با استفاده از آن می‌توان تعداد کیوبیت‌ها را افزایش داد و کیوبیت‌های جدیدی را به مدار کوانتومی اضافه کرد. این افزایش تعداد کیوبیت‌ها تا ۲۰ کیوبیت امکان‌پذیر است.

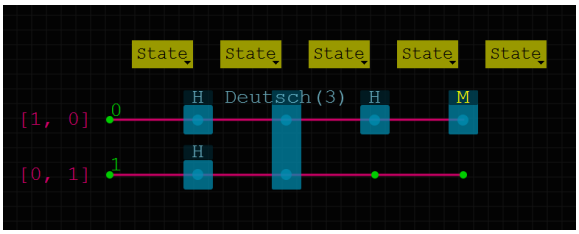
۲: از این قسمت گیت‌های کوانتومی، U_f و QFT را می‌توان انتخاب نمود و روی کیوبیت‌ها اثر داد.

۳: وقتی که تعداد گیت‌های کوانتومی که روی کیوبیت‌ها اثر می‌کنند افزایش می‌یابد، می‌بایست گره‌های جدیدی را به مدار کوانتومی اضافه کرد و در معنای عامیانه باید طول آن را افزایش داد، با استفاده از این قسمت این کار صورت می‌گیرد.

۴: این قسمت به اجرای عملیات موردنظر ما می‌پردازد.

۶-۱-۱- اجرای الگوریتم دویچ با استفاده از کیت کوانتوم

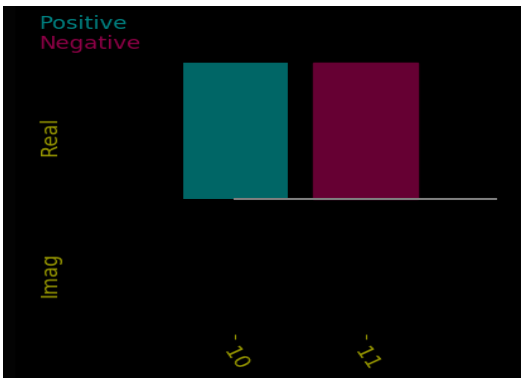
باتوجه‌به این که جزئیات چگونگی اجرای الگوریتم دویچ در بخش‌های قبل آمده است، در این جا فقط به اجرای این الگوریتم پرداخته و از بیان مراحل آن صرف‌نظر می‌کنیم. این الگوریتم در کیت کوانتوم به این صورت اجرا می‌شود:



شکل (۱۰): مداری که الگوریتم دویچ را اجرا می‌کند.

[1] Quantum-Kit

با استفاده از Deutsch(3) ثابت یا متوازن بودن تابع $f(x)=x$ بررسی می‌شود. پس از اجرا حالت سیستم به‌صورت زیر به دست می‌آید:



شکل (۱۱): نتیجه اندازه‌گیری در الگوریتم دویچ

باتوجه‌به نتیجه اندازه‌گیری روی کیوبیت اول، نتیجه می‌گیریم که $f(0)\oplus f(1)$ برابر با یک است و تابع ما یک تابع متوازن است.

۶-۲-QCAD

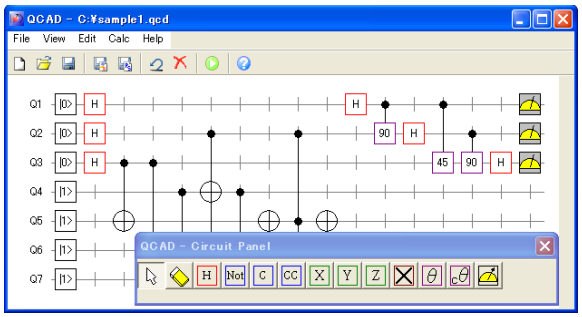
QCAD یک محیط مبتنی بر ویندوز برای شبیه‌سازی محاسبات کوانتومی است که به طراحی مدارها و شبیه‌سازی آن‌ها کمک می‌کند.

از مهم‌ترین ویژگی‌های آن می‌توان موارد زیر را نام برد:

۱- برای اجرای آن نیاز به اتصال به اینترنت نمی‌باشد و مبتنی بر ویندوز است.

۲- می‌توان حالت اولیه کیوبیت را $|0\rangle$ یا $|1\rangle$ انتخاب کرد.

۳- می‌توان به تعداد دلخواهی از کیوبیت‌ها دسترسی داشت.



شکل (۱۲): نمایی از محیط QCAD

۷- نتیجه‌گیری

ما در زمان حاضر به رایانه‌های کوانتومی که در اختیار همگان باشد، دسترسی نداریم و امکان استفاده از آن‌ها با تعداد کیوبیت محدود می‌تواند ما را برای رویارویی با این دستگاه‌های کوانتومی همگانی آماده کند. یک رایانه کوانتومی به‌خاطر بهره‌بردن از اصول کوانتومی مانند برهم‌نهی و توازی کوانتومی، می‌تواند محاسبات را به طور موازی انجام دهد و سرعت محاسبات در مقایسه با عملکرد یک رایانه کلاسیک بسیار بیشتر خواهد بود. مهم‌ترین کاربرد رایانه‌های کوانتومی در دسترس از طریق فضای ابری، پیاده‌سازی الگوریتم‌های کوانتومی همانند الگوریتم شور و گرور است. الگوریتم گرور می‌تواند دستیابی به کلمات عبور را بسیار آسان کند و الگوریتم شور می‌تواند تمامی رمزنگاری‌هایی که با مسئله تجزیه به عوامل اول در ارتباط هستند را بشکند. این الگوریتم‌ها روی رایانه‌های کوانتومی در دسترس از طریق فضای ابری پیاده‌سازی می‌شوند و این مسئله باعث می‌شود تا بتوان قبل از ظهور رایانه‌های کوانتومی با تعداد کیوبیت بالا خود را برای این تهدیدهای امنیتی آماده کرد. در این مقاله، تلاش شده است تا با معرفی خدمات ابری ارائه شده توسط شرکت‌های ریجتی و آی‌بی‌ام که دو شرکت پیشرو در این حوزه هستند و پیاده‌سازی الگوریتم‌های کوانتومی روی رایانه کوانتومی شرکت آی‌بی‌ام، گامی در جهت شناساندن ظرفیت‌های حوزه محاسبات ابری کوانتومی برداشته شود. همچنین نتایج حاصل از بررسی تعداد اختراع‌های ثبت شده در این زمینه نشانگر توجه روزافزون کشورها و شرکت‌های پیشرو در حوزه علم و فناوری به محاسبات ابری کوانتومی و انجام سرمایه‌گذاری‌های وسیع در این حوزه است.

۸- مراجع

[1] N. Gershenfeld, I. Chuang, “Quantum computing with molecules”, Scientific American 278.6,1998.

[2] I. Chuang, M. Nielsen, “Quantum computation and quantum information”, Cambridge, Cambridge University Press, 2010.

[3] P. Benioff, “The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines”, *Journal of Statistical Physics*, Vol. 29, No.5, 1980.

[4] D. Deutsch, “Quantum theory, the Church–Turing principle and the universal quantum computer”, Proc. R. Soc. Lond, Vol.400, No.1818, 1985.

[5] D. Deutsch, R. Jozsa, “Rapid solution of problems by quantum computation”, Proc. R. Soc. Lond, Vol.439, No.1907, 1992.

[6] R. Feynman, “Simulating physics with computers”, International journal of theoretical physics, Vol. 21, No. 6-7, 1982.

[7] P. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring”, *35th Annual Symposium on Foundations of Computer Science*, 1994.

[8] L. Vandersypen, et al, “Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance”, Nature, Vol. 414, No. 6866, 2001.

[9] R. Raussendorf, J. Briegel, “A one-way quantum computer”, *Physical Review Letters*, *86*(22), 5188,

[21] E. Dumitrescu, et al, "Cloud quantum computing of an atomic nucleus", *Physical review letters*, *120*(21), 210501, 2018.
[22] Z. Chen, et al, "64-qubit quantum circuit simulation", *Science Bulletin*, *63*(15), 964-971, 2018.
[23] J. Reyes, et al, "Simulation of Quantum Many-Body Systems on Amazon Cloud", *arXiv preprint arXiv:1908.08553*, 2019.
[24] F. Arute, et al, "Quantum supremacy using a programmablesuperconductingprocessor", *Nature*, *574*(7779), 505-510, 2019.
[25] K. Tamura, Y. Shikano, "Quantum random numbers generated by the cloud superconducting quantum computer", *arXiv preprint arXiv:1906.04410*, 2019.
[26] A. Shukla, et al, "Complete characterization of the directly implementable quantum gates used in the IBM quantum processors", *Physics Letters A*, 126387, 2020.
[27] M. Hayward, "Quantum computing and shor's algorithm", Sydney: Macquarie University Mathematics Department, 2008.
[28] E. Strubell, "An introduction to quantum algorithms", COS498 Chawathe Spring, 13, 19, 2011.
[29] L. Grover, "A fast quantum mechanical algorithm for database search", Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. ACM, 1996.
[30] Rigetti, https://www.rigetti.com/forest, 2018.
[31] M. Prigg, "IBM reveals record-breaking 'quantum chandelier' in race to revolutionise computing", http://www.dailymail.co.uk/sciencetech/article-5071659/IBM-reveals-quantum-computing-breakthrough.html, 2017.
[32] Q-kit, https://sites.google.com/view/quantum-kit/home, 2017.
2001.
[10] Z. Zhao, et al, "Experimental demonstration of five-photon entanglement and open-destination teleportation", Nature, Vol. 430, No. 6995, 2004.
[11] L. DiCarlo, et al, "Demonstration of two-qubit algorithms with a superconducting quantum processor", *Nature*, *460*(7252), 240-244, 2009.
[12] D. Borghino, "Quantum computer closer: Optical transistor made from single molecule", https://newatlas.com/optical-transistor-made-from-single-molecule/12157/, 2009.
[13] C. Petit, "Quantum computer simulates hydrogen moleculejustright",https://www.wired.com/2010/01/quantum-computer-hydrogen-simulation/, 2010.
[14] M. Johnson, et al, "Quantum annealing with manufactured spins", Nature, Vol. 473, No. 7346, 2011.
[15] N. Rockel, "The black box that could change the world",https://www.theglobeandmail.com/report-on-business/economy/canada-competes/the-black-box-that-could-change-the-world/article5327613/?page=1, 2012.
[16] M. Fuechsle, et al, "A single-atom transistor", Nature nanotechnology, Vol. 7, No. 4, 2012.
[17] L. Zyga, "New largest number factored on a quantum device is 56,153", https://phys.org/news/2014-11-largest-factored-quantum-device.html, 2014.
[18] W. Da silva, "Crucial hurdle overcome in quantum computing", http://newsroom.unsw.edu.au/news/science-tech/crucial-hurdle-overcome-quantum-computing, 2015.
[19] A. Dalton, "IBM unveils its most powerful quantum processoryet", https://www.engadget.com/2017/05/17/ibm-quantum-q-experience-qubits-most-powerful-processor-yet/, 2017.
[20] T. Xin, et al, "NMRCloudQ: a quantum cloud experience on a nuclear magnetic resonance quantum computer", *Science Bulletin*, *63*(1), 2018.