حمله‌های کوانتومی به سیستم‌های رمز متقارن

علی الماسی

۲۸ فروردین ۱۴۰۲

چکیده

مفهوم امنیت، و بالاخص امنیت محاسباتی، که تکیه‌ی آن بر محدودیت‌های محاسباتی یک مهاجم است، مفاهیمی بنیادی در نظریه‌ی رمزنگاری به شمار می‌روند. در رمزنگاری کلاسیک[۱]، مهاجم یک ماشین تورینگ احتمالاتی است که به انحاء مختلف برای حمله به یک سیستم رمز تلاش می‌کند و اگر تلاش‌هایش در زمان چندجمله‌ای منجر به آشکارشدن اطلاعاتی در مورد سیستم رمز شود، ممکن است امنیت سیستم به مخاطره افتد. با این همه، سال‌های پایانی قرن بیستم و ظهور نظریه‌ی محاسبات کوانتومی جامعه‌ی علمی را نسبت به این امر آگاه کرد که ضروری است حملات مهاجم‌هایی کوانتومی نیز، که لزوما معادل کلاسیک ندارند، در بررسی امنیت سیستم‌های رمزنگاری مورد بررسی قرار گیرد. مقاله‌ی تاثیرگذار پیتر شور[۲] که در آن الگوریتمی کوانتومی با زمان چندجمله‌ای برای حل مسأله‌های تجزیه‌ی اعداد و لگاریتم گسسته ارائه کرد، نشان داد که سیستم‌های نامتقارنی مانند RSA می‌توانند در حضور مهاجمان کوانتومی ناامن باشند؛ و بدین ترتیب عصری جدید در رمزنگاری آغاز شد که از آن، به عنوان رمزنگاری پساکوانتومی[۳] یاد می‌کنند.

گرچه تاثیرات الگوریتم‌های کوانتومی بر امنیت سیستم‌های نامتقارن موضوعی است که از اواخر دهه‌ی نود میلادی مورد توجه قرار گرفته است، بررسی سیستم‌های متقارن در حضور حملات کوانتومی موضوعی نسبتاً جدیدتر، و مربوط به دهه‌ی دوم قرن حاضر است. در این گزارش، اجمالاً به بیان دو الگوریتم شناخته‌شده‌ی کوانتومی، الگوریتم جست‌وجوی گروور[۴] و الگوریتم سایمون[۵]، خواهیم پرداخت و تاثیر این دو الگوریتم را بر امنیت برخی سیستم‌های متقارن، با توجه به منابع [۴، ۶، ۹، ۳۰، ۳۳] بیان خواهیم کرد.

فهرست مطالب

[۱] در اینجا کلاسیک را در مقابل پساکوانتومی به کار می‌بریم.

[2] Peter Shor
[3] post-quantum cryptography
[4] Grover's search algorithm
[5] Simon's algorithm

۱ مقدمه

۱.۱ گذری تاریخی بر محاسبات کوانتومی

بر کسی پوشیده نیست که بستر تاریخی قرن بیستم زمینه‌ای برای بسیاری از انقلاب‌های علمی و پیشرفت‌های تکنولوژی بوده است که زندگی و درک بشر از جهان را برای همیشه دگرگون کرده‌اند. از میان این تحولات، سه انقلاب مهم علمی را می‌توان زمینه‌ساز شکل‌گیری حوزه‌ای از دانش دانست که موضوع این گزارش را در بر می‌گیرد: نخست، پیدایش فیزیک کوانتوم در سه دهه‌ی آغازین این قرن؛ دوم، تلاش چرچ و تورینگ در دهه‌ی ۳۰ میلادی برای تعریف مفهوم الگوریتم و محاسبه‌پذیری؛ و سوم، مقاله‌ی انقلابی شانون در سال‌های پایانی نیمه‌ی اول قرن بیستم که منجر به پیدایش رمزنگاری نوین شد. گرچه امروزه برای ما روشن است که موارد فوق چگونه می‌توانند به یکدیگر مرتبط شوند، اما نباید فراموش کرد که این ارتباط تا نخستین سال‌های دهه‌ی هشتاد بر کسی روشن نبود.

از نظر تاریخی، اولین پیشنهاد برای ساختن ماشین محاسبه‌ای که بر اساس فیزیک کوانتوم کار می‌کند را می‌توان مربوط به پاول بنیوف[۶] دانست [۱۶]. با این وجود، معمولاً از ریچارد فاینمن[۷]، به عنوان آغازکننده‌ی راه محاسبات کوانتومی یاد می‌شود. در حقیقت فاینمن، در [۱۷] پیشنهاد داد که با توجه به این‌که شبیه‌سازی برخی پدیده‌های فیزیکی کوانتومی بر روی کامپیوترهای کلاسیک غیرممکن به نظر می‌رسد، از کامپیوترهایی که خود بر اساس فیزیک کوانتوم کار می‌کنند برای چنین شبیه‌سازی‌هایی استفاده شود. بدون شک دعوت فاینمن، که فیزیکدان برجسته و شناخته‌شده‌ای در آن زمان بود، در جلب توجه فیزیکدانان به این مسأله تأثیر زیادی داشت. از جمله‌ی این افراد، دیوید دویچ[۸] بود که سه سال پس از مقاله‌ی فاینمن، مدل محاسبه‌ی ماشین تورینگ کوانتومی[۹] را معرفی کرد [۱۸]. او همچنین در سال ۱۹۸۸ مدل محاسبات مداری کوانتومی[۱۰] را معرفی کرد؛ و به دنبال آن نشان داد گیت‌هایی جهانی[۱۱] برای محاسبات مداری کوانتومی وجود دارند [۱۹].

با وجود تلاش‌های فوق برای تعریف کردن مدل مناسبی برای محاسبات کوانتومی، تا سال ۱۹۹۳ هنوز بر کسی روشن نبود که محاسبات کوانتومی چه مزایایی بر محاسبات کلاسیک می‌تواند داشته باشد. بالاخص، در آن زمان پیاده‌سازی واقعی مدل‌های محاسبه‌ی کوانتومی بسیار دور از ذهن می‌نمود؛ و همین سبب شده بود که توجه کمتری به این حوزه جلب شود. در این سال، برنشتاین[۱۲] و وزیرانی[۱۳] نشان دادند که مدل محاسبات کوانتومی از منظر محاسبه‌پذیری، قدرت یکسانی با مدل کلاسیک تورینگ دارد [۲۰]. با این وجود، پیتر شور یک‌سال بعد نشان داد که گرچه طراحی الگوریتم‌هایی که بر اساس اصول موضوعه‌ی فیزیک کوانتومی کار می‌کنند بر قدرت محاسبه‌پذیری ما نمی‌افزاید؛ اما می‌تواند در حل برخی از مسائل مزیت‌هایی از نظر کارایی حل مسأله برای این الگوریتم‌ها نسبت به الگوریتم‌های کلاسیک ایجاد کنند. این مزیت، می‌تواند در قالب کاهش زمان اجرای الگوریتم، تعداد کوئری‌ها به اوراکل و یا تعداد ارتباطات لازم باشد. از اولین الگوریتم‌هایی که امکان وجود چنین مزیت‌هایی را نشان دادند، الگوریتم‌های ارائه شده توسط شور برای حل مسائل تجزیه‌ی اعداد و لگاریتم گسسته در زمان چندجمله‌ای بودند [۱۰]. با ارائه‌ی این الگوریتم‌ها، توجه جامعه‌ی علمی به قدرت و تاثیرات بالقوه‌ی محاسبات کوانتومی بر زمینه‌های متعددی از علوم کامپیوتر جلب شد. بالاخص که با پیاده‌سازی الگوریتم شور، شکستن برخی سیستم‌های رایج رمزنگاری همچون RSA، DH و ECC امکان‌پذیر می‌گردید؛ و همین مسأله لزوم توجه به خطر مهاجم‌های کوانتومی در تحلیل امنیت سیستم‌های رمزنگاری را مطرح کرد.

محاسبات کوانتومی از آن زمان تا کنون، در کمتر از چهل سال، رشد و پیشرفتی بسیار سریع داشته است. در هزاره‌ی جدید با پیشرفت تکنولوژی، قادر هستیم در عمل کامپیوترهای کوانتومی بسازیم و با آن‌ها محاسبه انجام دهیم. از سوی دیگر، امروزه به طور نظری، بسیاری از حوزه‌های علوم کامپیوتر همتای کوانتومی دارند و نتایج امیدبخشی در این حوزه‌ها به دست آمده است، که نویدبخش آن است که در آینده‌ای نه چندان دور، می‌توان از محاسبات کوانتومی به طور گسترده‌ای بهره گرفت؛ و همین سبب شده است که توجه ویژه‌ای از سوی بسیاری از دولت‌ها و سرمایه‌گذاران بخش خصوصی به توسعه‌ی فناوری‌ها و علوم کوانتومی روانه شود. به علاوه نتایجی همچون الگوریتم‌های شور، انگیزه‌بخش حوزه‌هایی همچون رمزنگاری برای وفق دادن خود با مخاطرات حملات مهاجم‌های کوانتومی بوده است؛ که منجر به آغاز عصری جدید در رمزنگاری شده است که از آن با عنوان رمزنگاری پساکوانتومی یاد می‌شود.

[6] Paul Benioff
[7] Richard Feynman
[8] David Deutsch
[9] quantum Turing machine
[10] quantum circuit model
[11] universal
[12] Ethan Bernstein
[13] Umesh Vazirani

شکل ۱: پیشگامان محاسبات کوانتومی؛ از راست به چپ: ریچارد فاینمن، دیوید دویچ و پیتر شور.

۲.۱ الگوریتم‌های کوانتومی در یک نگاه

پیش از آن‌که به طور دقیق مقصودمان از یک الگوریتم کوانتومی را بیان کنیم، خالی از لطف نیست که توصیفی غیر دقیق، اما شهودبخش، و بدون استفاده از جزئیات تکنیکی مکانیک کوانتوم، از یک الگوریتم کوانتومی داشته باشیم. این توضیحات، برگرفته از مرجع [۲۱] است.

یک الگوریتم را می‌توان یک سیستم دینامیکی با زمان گسسته دانست که فضای فاز آن نیز گسسته است. در واقع، فضای فاز چنین سیستم‌هایی عبارت است از مجموعه‌ای از رشته‌ها (در الفبایی دلخواه، که در ادامه برای راحتی فرض می‌کنیم مجموعه‌ی $\{۰,۱\}$ است) که کد شده‌ی پیکربندی ماشین محاسبه در هر لحظه هستند. قانون انتقال حالت این سیستم دینامیکی، به این صورت است که در گذر هر لحظه، به طور موضعی رشته‌ای که متناظر با حالت فعلی سیستم است را تغییر داده و آن را به رشته‌ای دیگر، متناظر با حالتی دیگر در فضای فاز، تبدیل می‌کند. در ادامه برای سادگی بیشتر، فرض کنید که اعضای فضای فاز همگی رشته‌هایی به طول n هستند[۱۴]. با چنین فرمالیسمی، محاسبه‌ی یک ورودی توسط یک ماشین محاسبه، در واقع معادل با یک مسیر[۱۵] در سیستم دینامیکی متناظر با آن است.

با داشتن این ایده در ذهن، انواع مختلف مدل‌های محاسبه را می‌توان به این صورت، معادل با انواع مختلفی از سیستم‌های دینامیکی دانست. برای مثال، یک مدل محاسباتی احتمالاتی، عملاً همان مدل فوق است؛ با این تفاوت که هر حالت سیستم متناظر با آن برابر است با یک بردار ۲^n تایی توزیع احتمال روی ۲^n عضو متمایز $\{۰,۱\}^n$؛ یا معادلاً، ترکیب محدبی مانند $\sum_{x\in\{۰,۱\}^n} p_x x$. قانون انتقال حالت سیستم نیز متشکل از اعمالی موضعی است که در طول زمان این بردار حالت‌ها را تغییر می‌دهند.

با این مقدمه، محاسبات کوانتومی را می‌توان با استفاده از تعبیر سیستم دینامیکی فوق مورد بررسی قرار داد. در حقیقت، حالت سیستم در هر لحظه، برداری ۲^n تایی مانند $(\alpha_x)_{x\in\{۰,۱\}^n}$ است که هر درایه‌ی آن عددی مختلط است؛ و این بردار با نرم $L_۲$ برداری یکه است. حالت سیستم با استفاده از اعمالی موضعی تغییر می‌کند که نگاشت‌هایی خطی و یکانی روی بردار حالت اعمال می‌کنند. نهایتاً خروجی الگوریتم با *اندازه‌گیری* حالت سیستم مشخص می‌شود. برای سادگی فرض کنید نتیجه‌ی این اندازه‌گیری یک رشته‌ی n بیتی است. در این صورت نتیجه‌ی یک اندازه‌گیری به صورت کاملاً تصادفی یکی از رشته‌های $x\in\{۰,۱\}^n$ خواهد بود که با توزیع احتمال $(|\alpha_x|^۲)_{x\in\{۰,۱\}^n}$ مشخص می‌شود. به طور خلاصه، یک الگوریتم کوانتومی عبارت است از اعمال متناهی نگاشت موضعاً نابدیهی یکانی بر بردار اولیه‌ای واقع در کره‌ی واحد فضای $\mathbb{C}^{۲^n}$ که در پایان الگوریتم، با استفاده از اندازه‌گیری، به یک بردار توزیع احتمال تبدیل می‌شوند.

گرچه توضیحات نادقیق فوق، شهودی از کارکرد و ساختار یک الگوریتم کوانتومی در اختیار ما می‌گذارد، دور از انتظار نیست که در تعریف‌کردن یک «الگوریتم کوانتومی» به صورت دقیق، به همان اندازه که تعریف‌کردن دقیق مفهوم «الگوریتم» در حالت کلاسیک چالش‌برانگیز است، با مشکل مواجه شویم. در حقیقت، مدل‌های مختلف محاسبات کوانتومی، نظیر مدل ماشین تورینگ کوانتومی یا مدل محاسبات مداری کوانتومی، تعاریف متفاوتی از الگوریتم‌های کوانتومی را در اختیار ما قرار می‌دهند. در این گزارش، ما بر مدل محاسبات مداری کوانتومی تمرکز خواهیم کرد، و می‌توان نشان داد که با گذر از ماشین‌های تورینگ به مدل مداری، چیز زیادی را نیز از دست نخواهیم داد [۱۱]. در مدل مداری نیز، تعریف الگوریتم به انحاء مختلفی قابل انجام است. از میان روش‌های موجود، تعریف الگوریتم در چهارچوب پیچیدگی کوئری[۱۶] را برخواهیم گزید. با این همه، توجه خواننده را به این جلب می‌کنیم که بسیاری از الگوریتم‌های کوانتومی را می‌توان در چهارچوب‌های دیگری، مانند پیچیدگی محاسباتی[۱۷] یا پیچیدگی ارتباطاتی[۱۸] نیز بیان کرد. خواننده‌ی علاقه‌مند می‌تواند به مرجع [۲] مراجعه کند تا با تعاریف مختلف یک الگوریتم کوانتومی و مثال‌هایی از آن آشنایی یابد.

در چهارچوب پیچیدگی کوئری، ورودی یک مسأله عبارت است از تابعی مانند $f : S \to T$ که دسترسی به آن از طریق یک ساختار جعبه‌سیاه[۱۹] فراهم شده است؛ و هدف، یافتن ویژگی‌هایی از تابع f است. در حل مسأله، می‌توان کوئری‌هایی مانند q از جعبه‌سیاهی که f را

[۱۴] این فرض چندان دور از ذهن نیست. به عنوان مثال، سیستم دینامیکی متناظر با یک مدار محاسبه روی n بیت، مثالی از چنین سیستمی است.

[15] trajectory

[16] query complexity

[17] computational complexity

[18] communication complexity

[19] black box

تحقق می‌بخشد پرسید؛ به این معنی که این جعبه‌سیاه (یا اوراکل)، مقدار $f(q)$ را در اختیار ما قرار می‌دهد. پیچیدگی کوئری، چهارچوبی برای مطالعه‌ی حداقل تعداد کوئری‌های لازم برای حل مسأله‌هایی از این نوع است [۲].

۳.۱ ساختار گزارش

ما در این گزارش، توجه خود را به تهدیدهای مهاجم‌های کوانتومی برای سیستم‌های رمز متقارن معطوف خواهیم کرد. نخست، برخی پیش‌نیازها را از جبرخطی و مکانیک کوانتوم مرور می‌کنیم. سپس به معرفی دو الگوریتم شناخته‌شده‌ی کوانتومی، الگوریتم گروور و سایمون، خواهیم پرداخت و در هر مورد، به برخی کاربردهای آن در تهدید امنیت سیستم‌های رمز متقارن اشاره خواهیم کرد. در این گزارش سعی بر آن بوده است که از جزئیات تکنیکی و غیر ضروری (که برخی از آن‌ها بیش از آن‌که مرتبط با رمزنگاری باشند، ظرایفی در احتمال یا جبرخطی هستند) اجتناب شود؛ با این همه در مواردی که از توضیح دقیق این موارد خودداری شده، ارجاعاتی به مراجع مرتبط برای خواننده‌ی علاقه‌مند فراهم شده است.

۲ پیشنیازها

۱.۲ پیشنیازهای جبرخطی

نمادگذاری دیراک: بسیاری از افرادی که با پیش‌زمینه‌ی غیر فیزیکی، به مطالعه‌ی محاسبات کوانتومی مبادرت می‌ورزند، معمولاً نمادگذاری دیراک را دشوار می‌یابند و گمان می‌کنند این دشواری، بازتابی از دشواری مفاهیم و اصول مکانیک کوانتومی است [۲۳]. با این همه، نباید از یاد برد زمانی که پاول دیراک این نمادگذاری را در اثر درخشانش، «اصول مکانیک کوانتومی [۲۴]»، به کار برد، در پی آن بود که این فرمول‌بندی به عنوان جایگزینی ساده‌تر برای فرمول‌بندی‌های رایج در آن زمان، یعنی *مکانیک ماتریسی*[۲۰] و *توابع موج*[۲۱] در جامعه‌ی علمی رواج یابد. این نمادگذاری گرچه در آغاز ممکن است پیچیده به نظر بیاید، اما همان‌گونه که خواهیم دید «به ما اجازه می‌دهد که محاسباتی صوری انجام دهیم که خود به خود ما را به نتایج درست رهنمون می‌کنند [۲۲]»؛ و به همین دلیل است که امروزه به طور گسترده‌ای در ادبیات محاسبات کوانتومی به کار برده می‌شود.

پیش از معرفی این نمادگذاری، توجه کنید که در سراسر این گزارش، تمام فضاهای خطی روی میدان اعداد مختلط تعریف شده‌اند و متناهی‌البعد هستند، مگر آن‌که خلاف آن ذکر شود.

نمادگذاری ۱.۲ کت[۲۲] یک بردار: برای نمایش برداری مانند v که عضو فضایی خطی مانند V است، از نمادگذاری $|v\rangle$ استفاده می‌کنیم و آن را «کتِ بردار v» می‌خوانیم. □

نمادگذاری ۲.۲ برای[۲۳] یک بردار: اگر V یک فضای خطی ضرب داخلی و $|v\rangle$ برداری در این فضا باشد، $\langle v| : V \to \mathbb{C}$، که آن را «برای بردار v» می‌خوانیم، تابعکی خطی است که به صورت

$$\langle v|\left(|w\rangle\right) = \left(|v\rangle, |w\rangle\right) \qquad \forall |w\rangle \in V \tag{۱}$$

تعریف شده است و در آن، مقصود از $\left(|w\rangle, |v\rangle\right)$، ضرب داخلی بردارهای $|v\rangle$ و $|w\rangle$ است. □

یادداشت ۳.۲ چنانچه پایه‌ی $\{|v_۰\rangle, \ldots, |v_{n-۱}\rangle\}$ را برای فضای خطی V داشته باشیم، می‌دانیم هر بردار $|v\rangle \in V$ نمایش یکتایی به صورت

$$|v\rangle = \sum_{i=۰}^{n-۱} \alpha_i |v_i\rangle \tag{۲}$$

دارد. بردار $\begin{pmatrix}\alpha_۱ \cdots \alpha_{n-۱}\end{pmatrix}^t$ را *بردار مختصات*[۲۴] $|v\rangle$ در پایه‌ی داده‌شده می‌نامیم. به سادگی می‌توان دید که نگاشت

$$|v\rangle \mapsto \begin{pmatrix}\alpha_۱ \\ \vdots \\ \alpha_{n-۱}\end{pmatrix} \tag{۳}$$

[20] matrix Mechanics
[21] wave Functions
[24] coordinate vector

یک یکریختی بین V و $\mathbb{C}^n$ است. بنابراین هر بردار $|v\rangle$ در یک فضای خطی n بعدی در تناظر یک‌به‌یک با یک بردار ستونی $n \times 1$ با درایه‌های مختلط است. به طور مشابه، چنانچه پایه‌ی متعامد یکه‌ای مانند $\{|v_0\rangle, \ldots, |v_{n-1}\rangle\}$ برای فضای ضرب داخلی V موجود باشد، برای هر دو بردار دلخواه $|v\rangle = \sum_{i=0}^{n-1} \alpha_i |v_i\rangle$ و $|w\rangle = \sum_{i=0}^{n-1} \beta_i |v_i\rangle$، داریم:

$$(|v\rangle, |w\rangle) = \Big(\sum_{i=0}^{n-1} \alpha_i |v_i\rangle, \sum_{i=0}^{n-1} \beta_i |v_i\rangle\Big) \tag{۴}$$

$$= \sum_{i,j} \alpha_i^* \beta_j (|v_i\rangle, |v_j\rangle) \tag{۵}$$

$$= \sum_{i,j} \alpha_i^* \beta_j \delta_{i,j} \tag{۶}$$

$$= \begin{pmatrix} \alpha_0^* & \cdots & \alpha_{n-1}^* \end{pmatrix} \begin{pmatrix} \beta_0 \\ \vdots \\ \beta_{n-1} \end{pmatrix}. \tag{۷}$$

بنابراین، می‌توان نتیجه گرفت که برای هر بردار دلخواه $\langle v| = \sum_{i=0}^{n-1} \alpha_i |v_i\rangle$، $|v\rangle$ متناظر با یک بردار $n \times 1$ با درایه‌های مختلط است که همان ترانهاده مزدوج بردار مختصات $|v\rangle$ در آن پایه می‌باشد. با توجه به مطلب فوق، در ادامه‌ی این گزارش، به‌جای فضاهای خطی دلخواه، خود را به $\mathbb{C}^n$ محدود خواهیم کرد و تعبیرهای فوق را برای کت و برای یک بردار دلخواه به کار خواهیم گرفت. ◁

نمادگذاری ۴.۲ دیگر قراردادها در نمادگذاری دیراک:

۱. با توجه به تعریف برا و کت، واضح است که برای دو بردار دلخواه $|v\rangle, |w\rangle \in V$، $\langle v| |w\rangle$ برابر با ضرب داخلی آن‌هاست. در نمادگذاری دیراک، ضرب داخلی این دو بردار با $\langle v|w\rangle$ نمایش داده می‌شود.

۲. می‌دانیم برای هر نگاشت خطی $T : V \to V$، نگاشت الحاقی T که آن را با $T^\dagger : V \to V$ نمایش می‌دهیم، نگاشتی است با این ویژگی که برای هر $|v\rangle, |w\rangle \in V$،

$$(|v\rangle, T|w\rangle) = (L^\dagger |v\rangle, |w\rangle). \tag{۸}$$

در نمادگذاری دیراک برای هر $|v\rangle \in V$ و هر نگاشت خطی T روی فضای V تعریف می‌کنیم:

$$\langle v|^\dagger \stackrel{\text{def}}{=} |v\rangle, \tag{۹}$$

$$(T|v\rangle)^\dagger \stackrel{\text{def}}{=} \langle v| T^\dagger. \tag{۱۰}$$

۳. برای دو فضای خطی ضرب داخلی V و W و دو بردار دلخواه $|v\rangle \in V$ و $|w\rangle \in W$، نگاشت خطی $|v\rangle\langle w| : W \to V$ به صورت زیر تعریف می‌شود:

$$|v\rangle\langle w|(|u\rangle) \stackrel{\text{def}}{=} \langle w|u\rangle |v\rangle \qquad \forall |u\rangle \in W. \tag{۱۱}$$

به نگاشت فوق، ضرب خارجی[۲۵] دو بردار $|v\rangle$ و $|w\rangle$ گویند.

۴. پایه‌ی استاندارد $\mathbb{C}^n$، که متشکل از n بردار

$$|0\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |1\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \ldots, \quad |n-1\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \tag{۱۲}$$

است، پایه‌ی محاسباتی نامیده می‌شود.

[25] outer product

□

شایان ذکر است که علاقه‌مندان به آشنایی بیشتر با نمادگذاری دیراک می‌توانند به مرجع [۱۲] مراجعه کنند.

ضرب تنسوری: ضرب تنسوری[۲۶] یکی از مفاهیمی است که در حوزه‌های مختلف ریاضیات و فیزیک، و بالاخص مکانیک کوانتومی، به طور گسترده‌ای به کار گرفته می‌شود. در این قسمت، به معرفی این مفهوم، و بیان برخی ویژگی‌های آن خواهیم پرداخت.

تعریف ۵.۲ فرض کنید V و W دو فضای برداری و $\{|v_0\rangle, \dots, |v_{n-1}\rangle\}$ و $\{|w_0\rangle, \dots, |w_{m-1}\rangle\}$ به ترتیب پایه‌هایی برای آن‌ها باشند. **ضرب تنسوری دو فضای** V و W، که آن را با $V \otimes W$ نمایش می‌دهیم، یک فضای برداری با پایه‌ی صوری

$$\{|v_i\rangle \otimes |w_j\rangle \ : \ i = 0, 1, \dots, n-1,\ j = 0, 1, \dots, m-1\} \tag{۱۳}$$

(روی میدان $\mathbb{C}$) است. ▶

تعریف ۶.۲ برای دو فضای برداری V و W با پایه‌های $\{|v_0\rangle, \dots, |v_{n-1}\rangle\}$ و $\{|w_0\rangle, \dots, |w_{m-1}\rangle\}$، و دو بردار $|v\rangle = \sum_{i=0}^{n-1} \alpha_i |v_i\rangle$ و $|w\rangle = \sum_{j=0}^{m-1} \beta_j |w_j\rangle$، حاصلضرب تنسوری دو بردار $|v\rangle$ و $|w\rangle$، که آن را با $|v\rangle \otimes |w\rangle$ نمایش می‌دهیم، به صورت

$$|v\rangle \otimes |w\rangle = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \alpha_i \beta_i |v_i\rangle \otimes |w_j\rangle \tag{۱۴}$$

تعریف می‌شود. ▶

یادداشت ۷.۲ توجه کنید که در تعریف‌های فوق، ضرب تنسوری دو فضای برداری وابسته به پایه‌ای که برای دو فضا انتخاب می‌کنیم خواهد بود. شایان ذکر است که ضرب تنسوری را می‌توان به نحوی تعریف کرد که فضای $V \otimes W$ مستقل از انتخاب پایه باشد. خواننده‌ی علاقه‌مند می‌تواند برای آشنایی بیشتر با این تعریف، به مرجع [۲۵] مراجعه کند. ▷

یادداشت ۸.۲ از تعریف ۵.۲ روشن است که حاصلضرب تنسوری دو فضای n و m بعدی، فضایی nm بعدی است. بنابراین $\mathbb{C}^n \otimes \mathbb{C}^m \cong \mathbb{C}^{nm}$. به طور خاص، اگر $\{|i\rangle\}_{i=0}^{n-1}$ و $\{|j\rangle\}_{j=0}^{m-1}$ به ترتیب پایه‌های محاسباتی $\mathbb{C}^n$ و $\mathbb{C}^m$ باشند، نگاشت

$$|i\rangle \otimes |j\rangle \mapsto |mi + j\rangle \tag{۱۵}$$

یک یکریختی بین $\mathbb{C}^n \otimes \mathbb{C}^m$ و $\mathbb{C}^{nm}$ را مشخص می‌کند. در ادامه، ما نیز $|i\rangle \otimes |j\rangle$ و $|mi + j\rangle$ را یکی خواهیم گرفت. ▷

نمادگذاری ۹.۲ در نمادگذاری دیراک، $|v\rangle \otimes |w\rangle$ معمولا به صورت $|v\rangle |w\rangle$ یا $|vw\rangle$ خلاصه می‌شود. □

تعریف ۱۰.۲ مقصود از **ضرب تنسوری دو نگاشت خطی** $L_1 : V \to V'$ و $L_2 : W \to W'$، نگاشتی خطی مانند $L_1 \otimes L_2 : V \otimes W \to V' \otimes W'$ است که عمل آن روی پایه‌ی $\{|v_i\rangle \otimes |w_j\rangle\}_{i,j}$ به صورت

$$L \otimes L'(|v_i\rangle \otimes |w_j\rangle) = (L |v_i\rangle) \otimes (L' |w_j\rangle) \tag{۱۶}$$

تعریف شده است. ▶

همان‌گونه که در یادداشت ۳.۲ دیدیم، در بسیاری از موارد ترجیح می‌دهیم به جای بردارهای دلخواه در یک فضای برداری، با بردارهای مختصات آن‌ها (در پایه‌ای دلخواه) کار کنیم. به طور مشابه، گاهی کار با نمایش ماتریسی یک نگاشت خطی (در پایه‌ای دلخواه) را ترجیح می‌دهیم. در چنین مواردی، که فضاهای برداری را به $\mathbb{C}^n$ و نگاشت‌های خطی را به ماتریس‌هایی با درایه‌های مختلط تقلیل می‌دهیم، راحت‌تر است که ضرب تنسوری را با ضرب کرونکر[۲۷] که ساده‌تر، ولی معادل با آن است، جایگزین کنیم. در واقع، تعریف بعد، تعمیمی از یکریختی یادشده در یادداشت ۸.۲ را ارائه می‌دهد.

تعریف ۱۱.۲ ضرب کرونکر دو ماتریس $A_{m\times n}$ و $B_{p\times q}$، که آن را با $A \otimes B$ نمایش می‌دهیم، ماتریسی با ابعاد $(mp) \times (nq)$ است که به صورت زیر تعریف می‌شود:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix} \tag{۱۷}$$

[26] tensor product
[27] Kronecker product

▶

یادداشت ۱۲.۲ توجه کنید که اگر فضاهای V و W دو فضای ضرب داخلی باشند، فضای $V \otimes W$ را می‌توان به ضرب داخلی طبیعی

$$\left(\sum_i \alpha_i |v_i\rangle \otimes |w_i\rangle , \sum_j \beta_j |v_j\rangle \otimes |w_j\rangle\right) = \sum_{i,j} {\alpha_i}^* \beta_j \langle v_i|v_j\rangle \langle w_i|w_j\rangle \quad (۱۸)$$

مجهز کرد. در ادامه، مقصودمان از ضرب داخلی روی فضای ضرب تنسوری، ضرب داخلی کانونی فوق خواهد بود. ◁

نهایتا، این زیربخش را با گزاره‌ای به پایان خواهیم برد که برخی ویژگی‌های پرکاربرد ضرب تنسوری را بیان می‌کند.

گزاره ۱۳.۲ *فرض کنید V و W دو فضای ضرب داخلی هستند؛ $|v\rangle , |v'\rangle \in V$ و $|w\rangle , |w'\rangle \in W$؛ c یک عدد مختلط دلخواه است و L و L' دو نگاشت خطی هستند که به ترتیب روی V و W تعریف شده‌اند. در این صورت، تساوی‌های زیر برقرارند:*

۱. $(|v\rangle + |v'\rangle) \otimes |w\rangle = |vw\rangle + |v'w\rangle$

۲. $|v\rangle \otimes (|w\rangle + |w'\rangle) = |vw\rangle + |vw'\rangle$

۳. $c\,|vw\rangle = (c\,|v\rangle) \otimes |w\rangle = |v\rangle \otimes (c\,|w\rangle)$

۴. $(L \otimes L')^\dagger = L^\dagger \otimes {L'}^\dagger$

۵. $tr(L \otimes L') = tr(L)tr(L')$

۲.۲ پیشنیازهای مکانیک کوانتومی

مکانیک کوانتومی چهارچوبی ریاضی است که جهان فیزیکی، به طور خاص پدیده‌هایی فیزیکی که در سطح اتمی و زیراتمی رخ می‌دهند، را به نظریات ریاضی پیوند می‌دهد. از نظر تاریخی، پیدایش فیزیک کوانتوم را می‌توان مربوط به اولین سال‌های قرن بیستم و ناکامی فیزیک کلاسیک در توضیح تعدادی از نتایج آزمایشگاهی حاصل شده در آن زمان دانست. معرفی مفهوم بسته‌های انرژی توسط مکس پلانک [۲۶] که بعدها انیشتین آن را توسعه داد و اثر فوتوالکتریک را به کمک این مفهوم توضیح داد [۲۷]، معرفی مدل اتمی بور برای توصیف طیف اتم هیدروژن [۲۸]، توسعه‌ی مکانیک ماتریسی توسط هایزنبرگ و توابع موج توسط شرودینگر برای توصیف ریاضی پدیده‌های کوانتومی و ارائه‌ی اصول موضوعه‌ی مکانیک کوانتومی توسط فون نویمان [۲۹] از جمله مهم‌ترین گام‌هایی است که در سه دهه‌ی اول قرن بیستم رخ داده و منجر به ساخته شدن این نظریه‌ی ارزشمند، و البته غامض، شده‌اند. نظریه‌ای که تاثیرات شگرفی بر زندگی بشر در عصر حاضر گذاشته و انتظار می‌رود که به زودی، بسیار بیشتر از امروز، وجوه مختلف زندگی ما را متاثر کند.

در این زیربخش، بررسی خواهیم کرد که اصول موضوعه‌ی مکانیک کوانتومی چگونه فضای حالت و تحول زمانی سیستم‌های فیزیکی کوانتومی را فرمول‌بندی می‌کنند. هم‌چنین خواهیم دید که چگونه این فرمول‌بندی‌ها قابل تعمیم به سیستم‌هایی متشکل از زیرسیستم‌های کوچکتر است. علاوه بر این، در اصلی که مشابه آن در مکانیک کلاسیک وجود ندارد، خواهیم دید که اندازه‌گیری یک سیستم کوانتومی، یکی از مفاهیم مناقشه‌برانگیز فیزیک کوانتوم، چگونه صورت‌بندی می‌شود.

اصل ۱۴.۲ (فضای حالت) *به هر سیستم فیزیکی منزوی یک فضای هیلبرت نسبت داده می‌شود که به آن **فضای حالت** **سیستم**[a] می‌گویند. **بردار حالت**[b] سیستم (یا به طور خلاصه، **حالت** سیستم)، بردار یکه‌ای در فضای حالت آن است [۱۲].*

[a] State Space
[b] State Vector

تعریف ۱۵.۲ یک کیوبیت[۲۸]، یک سیستم کوانتومی است که فضای حالت آن، فضای هیلبرت دو بعدی $\mathbb{C}^2$ است. ▶

کیوبیت‌ها، همتای کوانتومی بیت‌های کلاسیک، اساسی‌ترین و ضروری‌ترین سیستم‌های فیزیکی هستند که در محاسبات و اطلاعات کوانتومی به کار گرفته می‌شوند. حالت یک کیوبیت می‌تواند به صورت

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \quad (۱۹)$$

[28] qubit

نوشته شود که در آن، $\alpha, \beta \in \mathbb{C}$، $|\alpha|^2 + |\beta|^2 = 1$، و $|0\rangle$ و $|1\rangle$ بردارهای $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ و $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ را مشخص می‌کنند.

برخلاف بیت‌های کلاسیک، که تنها می‌توانند یکی از دو مقدار ۰ یا ۱ را داشته باشند، یک کیوبیت می‌تواند (مانند معادله‌ی ۱۹) در یک *برهم‌نهی*[۲۹] از $|0\rangle$ و $|1\rangle$ قرار گیرد. این یکی از تفاوت‌های اساسی میان محاسبات کلاسیک و محاسبات کوانتومی است. تفاوتی که می‌تواند در امکان ساختن الگوریتم‌هایی کوانتومی که بسیار بهتر از الگوریتم‌های کلاسیک عمل می‌کنند، نقش داشته باشد.

در ادبیات محاسبات کوانتومی، نام‌های خاصی برای برخی حالت‌های یک کیوبیت وجود دارد. در نمادگذاری بعد، دو مورد از این حالات را معرفی می‌کنیم.

نمادگذاری ۱۶.۲ حالت‌های $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ و $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ به ترتیب با $|+\rangle$ و $|-\rangle$ نمایش داده می‌شوند. □

توجه کنید که $\{|+\rangle, |-\rangle\}$ پایه‌ای برای $\mathbb{C}^2$ است که به آن پایه‌ی X می‌گویند. همچنین پایه‌ی محاسباتی $\mathbb{C}^2$ پایه‌ی Z نامیده می‌شود.

اصل ۱۷.۲ (تحول زمانی سیستم) *این اصل را می‌توان به دو صورت متفاوت بیان کرد؛ و البته می‌توان نشان داد که این دو صورت با یکدیگر معادلند [۱۲]:*

- *حالت یک سیستم بسته‌ی کوانتومی مطابق با معادله‌ی شرودینگر تحول می‌یابد. معادله‌ی شرودینگر به صورت زیر است:*

$$i\hbar \frac{d|\psi(t)\rangle}{dt} = H|\psi(t)\rangle,$$

که در آن $\psi(t)$ حالت سیستم در لحظه‌ی t، H عملگری هرمیتی که به آن همیلتنی[a] سیستم می‌گویند، و $\hbar$ ثابت پلانک است.

- *اگر حالت یک سیستم بسته‌ی کوانتومی در لحظه‌ی t_1، $|\psi(t_1)\rangle$ باشد، حالت سیستم در لحظه‌ی $t_2 > t_1$ با*

$$|\psi(t_2)\rangle = U|\psi(t_1)\rangle$$

مشخص می‌شود که U نگاشتی یکانی است که تنها به $t_2 - t_1$ وابسته است.

[a] Hamiltonian

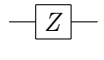
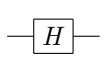
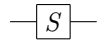
از این به بعد، اصطلاح «گیت کوانتومی» را برای اشاره به عملگرهای یکانی که تحول سیستم را مشخص می‌کنند، به کار خواهیم برد. با وجود این‌که تعداد گیت‌های کوانتومی که قابل اعمال بر یک کیوبیت هستند نامتناهی است، به دلایل متعددی تنها تعدادی متناهی از این گیت‌ها مورد علاقه‌ی ما هستند. جدول ۱ شامل لیست مختصری از تعدادی از این گیت‌های کوانتومی و نمایش گرافیکی و ماتریسی آن‌هاست.

LT

جدول ۱: برخی از مهم‌ترین گیت‌های تک‌کیوبیتی

نام گیت	نمایش ماتریسی	نمایش گرافیکی[۳۰]
Pauli-I	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$-\boxed{I}-$
Pauli-X	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$-\boxed{X}-$
Pauli-Y	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$-\boxed{Y}-$

[29] superposition

نام گیت	نمایش ماتریسی	نمایش گرافیکی
Pauli-Z	$\begin{pmatrix} ۱ & ۰ \\ ۰ & -۱ \end{pmatrix}$	
Hadamard	$\begin{pmatrix} \frac{۱}{\sqrt{۲}} & \frac{۱}{\sqrt{۲}} \\ \frac{۱}{\sqrt{۲}} & -\frac{۱}{\sqrt{۲}} \end{pmatrix}$	
T-gate	$\begin{pmatrix} ۱ & ۰ \\ ۰ & e^{\frac{i\pi}{۴}} \end{pmatrix}$	
Phase (S-gate)	$\begin{pmatrix} ۱ & ۰ \\ ۰ & i \end{pmatrix}$	
Relative Phase Rotation	$\begin{pmatrix} ۱ & ۰ \\ ۰ & e^{۲\pi i\theta} \end{pmatrix}$	

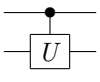
اصل ۱۸.۲ (سیستم‌های مرکب) *فضای حالت یک سیستم مرکب که متشکل از n زیرسیستم با فضاهای حالت $V_۱, \dots, V_n$ است، برابر است با $V_۱ \otimes \cdots \otimes V_n$. هم‌چنین اگر هر یک از زیرسیستم‌ها حالت $|v_i\rangle$ را داشته باشند، حالت سیستم مرکب برابر با $|v_۱\rangle \otimes \cdots \otimes |v_n\rangle$ خواهد بود [۱۲].*

با توجه به اصول ۱۷.۲ و ۱۸.۲، تحول زمانی یک سیستم مرکب کوانتومی که متشکل از دو زیرسیستم با فضاهای حالت V و W است، با نگاشت‌های یکانی روی فضای $V \otimes W$ مشخص می‌شود. توجه کنید که زیرمجموعه‌ای از چنین نگاشت‌هایی، به صورت $L \otimes L'$ هستند، که L و L' به ترتیب نگاشت‌هایی یکانی روی فضاهای V و W هستند. با این وجود، باید توجه شود که این زیرمجموعه، زیرمجموعه‌ای سره از همه‌ی نگاشت‌های یکانی روی $V \otimes W$ است.

بنا بر دلایلی، نظری و عملی، در محاسبات کوانتومی بیشتر علاقه‌مند به گیت‌هایی هستیم که حداکثر روی ۳ کیوبیت به طور نابدیهی عمل می‌کنند. جدول ۲ تعدادی از این گیت‌ها، که روی بیش از یک کیوبیت به طور نابدیهی عمل می‌کنند، نمایش ماتریسی و نمایش گرافیکی آن‌ها را لیست کرده است.

LT

جدول ۲: برخی از مهم‌ترین گیت‌های چند کیوبیتی

نام گیت	نمایش ماتریسی	نمایش گرافیکی
CNOT	$\begin{pmatrix} ۱ & ۰ & ۰ & ۰ \\ ۰ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۱ \\ ۰ & ۰ & ۱ & ۰ \end{pmatrix}$	
[۳۱]Controlled-U	$\begin{pmatrix} ۱ & ۰ & ۰ & ۰ \\ ۰ & ۱ & ۰ & ۰ \\ ۰ & ۰ & U_{۱۱} & U_{۱۲} \\ ۰ & ۰ & U_{۲۱} & U_{۲۲} \end{pmatrix}$	

[۳۰] سیم‌ها نمایانگر کیوبیت‌ها هستند.

نام گیت	نمایش ماتریسی	نمایش گرافیکی
Toffoli gate (CCNOT)	$\begin{pmatrix} ۱ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۱ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۰ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۱ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۰ & ۱ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۰ & ۰ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۱ \\ ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۱ & ۰ \end{pmatrix}$	

اصل ۱۹.۲ (اندازه‌گیری) *مقصود از یک اندازه‌گیری با m نتیجه‌ی ممکن روی یک سیستم کوانتومی، خانواده‌ای از عملگرها مانند $M = \{M_۱, \dots, M_m\}$ است (M_i متناظر با نتیجه‌ی i ام است) که روی فضای حالت آن سیستم عمل می‌کنند و شرط $\sum_{i=۱}^{m} M_i^\dagger M_i = I$ را نیز برآورده می‌کنند. هنگامی که این اندازه‌گیری روی سیستمی که در حالت $|\psi\rangle$ قرار دارد انجام می‌شود، نتیجه‌ی اندازه‌گیری با احتمال*

$$p(i) = \left\langle \psi \middle| M_i^\dagger M_i \middle| \psi \right\rangle,$$

برابر با i خواهد بود؛ و در این صورت، حالت سیستم به حالت

$$\frac{M_i|\psi\rangle}{\sqrt{\left\langle \psi \middle| M_i^\dagger M_i \middle| \psi \right\rangle}}$$

فرو خواهد ریخت [a] [۱۲].

[a] Collapse

در ادامه‌ی این گزارش، عموماً از حالت خاصی از اندازه‌گیری‌های معرفی شده در بالا استفاده خواهیم کرد که در ادامه معرفی می‌شوند.

تعریف ۲۰.۲ یک **اندازه‌گیری افکنشی** یک اندازه‌گیری کوانتومی است که متشکل است از عملگرهای افکنشی دو به دو متعامد. یک عملگر افکنشی عملگری مانند $P : \mathbb{C}^n \to \mathbb{C}^n$ است به طوری که $P^۲ = P$. به عبارت دیگر، یک اندازه‌گیری افکنشی خانواده‌ای مانند $M = \{P_۱, \dots, P_m\}$ است به طوری که:

۱. هر P_i یک عملگر افکنشی است.

۲. $\sum_{i=۱}^{m} P_i = I$

۳. $\forall i, j \in \{۱, \dots, m\}, \quad P_i P_j = \delta_{ij} P_i$

▶

همچنین ممکن است در ادامه‌ی این گزارش، از اصطلاح اندازه‌گیری در پایه‌ی $\{|v_۰\rangle, \dots, |v_{n-۱}\rangle\}$ استفاده کنیم. در چنین مواردی، مقصودمان یک اندازه‌گیری افکنشی با عملگرهای اندازه‌گیری $|v_i\rangle\langle v_i|$ خواهد بود.

نمادگذاری ۲۱.۲ در ادامه از نماد زیر برای نمایش گرافیکی اندازه‌گیری استفاده خواهیم کرد.

□

[۳۱] فرض کنید $U = \begin{pmatrix} U_{۱۱} & U_{۱۲} \\ U_{۲۱} & U_{۲۲} \end{pmatrix}$.

۳.۲ پیش‌نیازهای محاسبات کوانتومی

با مقدمه‌ای که در زیربخش‌های قبل بیان شد، اکنون می‌توانیم یک الگوریتم کوانتومی را در چهارچوب پیچیدگی کوئری تعریف کنیم.

تعریف ۲۲.۲ یک **مدار کوانتومی** روی n کیوبیت، عبارت است از یک رجیستر n کیوبیتی (که ورودی مدار در آن قرار می‌گیرد) به همراه یک رجیستر m کیوبیتی که به آن رجیستر کمکی[۳۲] می‌گوییم و معمولاً یک مقداردهی اولیه (مستقل از ورودی) دارد؛ به علاوه‌ی تعداد متناهی گیت‌های کوانتومی مانند

$$U_1, U_2, \ldots, U_t$$

که هر یک، روی فضای حالت $(\mathbb{C}^2)^{\otimes(n+m)}$ تعریف شده‌اند اما به طور نابدیهی روی $\mathcal{O}(1)$ کیوبیت عمل می‌کنند. ◄

با توجه به این‌که می‌خواهیم کوئری کردن از یک اوراکل را در مدل محاسبه‌مان وارد کنیم، این کار را با گیت‌های کوانتومی خاصی که در ادامه تعریف می‌شود، انجام می‌دهیم. شایان ذکر است که این گیت‌ها، گیت‌هایی نیستند که به طور موضعی نابدیهی عمل کنند؛ و نحوه‌ی ساخته‌شدنشان از گیت‌های ساده‌تر نیز مشخص نیست؛ که فرضی قابل قبول در مدل جعبه‌ی سیاه است.

تعریف ۲۳.۲ برای تابع $f : \{0,1\}^n \to \{0,1\}^m$، یک گیت fـکوئری، عبارت است از نگاشتی یکانی مانند $U_f : (\mathbb{C}^2)^{\otimes n} \otimes (\mathbb{C}^2)^{\otimes m} \to (\mathbb{C}^2)^{\otimes m} \otimes (\mathbb{C}^2)^{\otimes n}$ که روی یک رجیستر n کیوبیتی اصلی و یک رجیستر m کیوبیتی کمکی عمل می‌کند و عمل آن به صورت زیر تعریف شده است:

$$\forall |x\rangle \in (\mathbb{C}^2)^{\otimes n} \quad \forall |y\rangle \in (\mathbb{C}^2)^{\otimes m}, \qquad U_f(|x\rangle\,|y\rangle) = |x\rangle\,|y \oplus f(x)\rangle\,. \tag{۲۰}$$

►

نهایتاً می‌توانیم یک الگوریتم کوانتومی را در چهارچوب پیچیدگی کوئری توصیف کنیم.
فرض کنید که ورودی مسأله تابع $f : \{0,1\}^n \to \{0,1\}^m$ باشد؛ و مطلوب مسأله مشخص‌کردن ویژگی‌هایی از این تابع است. تابع f در ورودی، با جعبه‌ی سیاهی که آن را محقق می‌کند توصیف شده است (به عبارت دیگر، نگاشت U_f در اختیار ما قرار داده شده است.). یک الگوریتم کوانتومی که چنین مسأله‌ای را حل می‌کند عبارت است از یک مدار کوانتومی که از گیت‌های کوانتومی استاندارد و گیت fـکوئری تشکیل شده است؛ که بر رجیسترهای اصلی و کمکی (که هر دو با مقادیر مناسبی، مقداردهی اولیه شده‌اند) اعمال می‌شوند، و خروجی الگوریتم نیز با اندازه‌گیری برخی کیوبیت‌های خروجی مدار در یک پایه‌ی مناسب (که معمولاً پایه‌ی محاسباتی است) تعیین می‌گردد.
در چهارچوب پیچیدگی کوئری، مطالعه‌ی تعداد بارهایی که باید از گیت‌های کوئری استفاده شود، اهمیت می‌یابد [۲].
این بخش را با ذکر این نکته به پایان می‌رسانیم که در حملاتی که در ادامه می‌آید، فرض شده است مهاجم دسترسی به یک اوراکل کوانتومی دارد. مقصود از اوراکل کوانتومی، همان نگاشت یکانی U_f است که در بالا مطرح شده است؛ و می‌تواند از f سوالاتی به صورت برهم‌نهی بپرسد.

۳ الگوریتم جست‌وجوی گروور و کاربرد آن

۱.۳ الگوریتم گروور

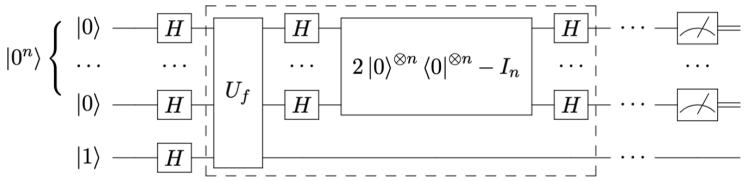
الگوریتم گروور، یکی از مشهورترین الگوریتم‌های کوانتومی (احتمالا بعد از الگوریتم شور) است. این الگوریتم در سال ۱۹۹۶ توسط لاو گروور[۳۳] در [۱۴] ارائه شد و بعدها نسخه‌های متنوع‌تری از آن نیز توسعه یافت [۱۳]. الگوریتم گرور، با وجود آن‌که برخلاف الگوریتم سایمون (که آن را در بخش بعد خواهیم دید) یک مسأله‌ی کلاس پیچیدگی نمایی را به چندجمله‌ای تبدیل نمی‌کند، از مهم‌ترین الگوریتم‌های کوانتومی به دست آمده تا امروز است؛ و دلیل آن مسأله‌ی مهم و پرکاربردی است که این الگوریتم حل می‌کند. این مسأله همان‌گونه که از عنوان این بخش بر می‌آید، مسأله‌ی جست‌وجو است.

مسأله‌ی جست‌وجوی بدون ساختار

ورودی: دسترسی اوراکلی به تابع $f : \{0,1\}^n \to \{0,1\}$ با این ویژگی که قرارداد شده است، تعداد اعضای مجموعه‌ی $\{x \in \{0,1\}^n \;:\; f(x) = 1\}$ برابر با t است.
خروجی: رشته‌ای مانند $x \in \{0,1\}^n$ چنانکه $f(x) = 1$.

[32] ancilla register
[33] Lov Grover

شکل ۲: شمایی از الگوریتم گروور. قسمتی که دور آن خط‌چین کشیده شده است، یک *تکرار گروور* نامیده می‌شود.



گروور الگوریتم زیر را برای حل مسأله‌ی فوق پیشنهاد داد. شکل ۲ پیاده‌سازی این الگوریتم را نمایش می‌دهد. (در ادامه فرض کنید $N = ۲^n$.)

الگوریتم

۱. با یک رجیستر n بیتی (رجیستر اول) و یک رجیستر ۱ بیتی (رجیستر دوم) شروع می‌کنیم که رجیستر اول در حالت $|۰\rangle^{\otimes n}$ و رجیستر دوم در حالت $|۱\rangle$ آماده‌سازی شده‌اند.

۲. نگاشت $H^{\otimes(n+۱)}$ را بر رجیستر اول و دوم اعمال می‌کنیم.

۳. (تکرار گروور) مراحل زیر را $\mathcal{O}\left(\sqrt{N}\right)$ بار تکرار می‌کنیم:

(آ) U_f را بر رجیستر اول و دوم اعمال می‌کنیم.

(ب) نگاشت $D = (D_{ij}) : \mathbb{C}^N \to \mathbb{C}^N$ را که به صورت زیر تعریف شده است بر رجیستر اول اعمال می‌کنیم.

$$D_{ij} = \begin{cases} \frac{۲}{N}, & \text{اگر} \quad i \neq j \\ -۱ + \frac{۲}{N} & \text{اگر} \quad i = j \end{cases} \qquad (۲۱)$$

۴. رجیستر اول را در پایه‌ی محاسباتی اندازه می‌گیریم.

آنالیز درستی الگوریتم فوق:

- نخست توجه کنید که پس از اعمال اولین مجموعه از گیت‌های هادامارد حالت سیستم برابر است با:

$$|\psi\rangle = |+\rangle^{\otimes n} |-\rangle = \frac{۱}{\sqrt{۲^n}} \sum_{x\in\{۰,۱\}^n} |x\rangle |-\rangle .$$

- از طرفی، برای هر $x \in \{۰,۱\}^n$ داریم:

$$\begin{aligned} U_f(|x\rangle |-\rangle) = \frac{۱}{\sqrt{۲}} U_f(|۰\rangle + |۱\rangle) = \frac{۱}{\sqrt{۲}} U_f(|x\rangle |۰\rangle + |x\rangle |۱\rangle) = |x\rangle \frac{۱}{\sqrt{۲}}(|f(x)\rangle - |f(x)\oplus ۱\rangle) \\ = (-۱)^{f(x)} |x\rangle |-\rangle \end{aligned}$$

بنابراین با اعمال گیت U_f بر حالت $|\psi\rangle$ خواهیم داشت:

$$U_f |\psi\rangle = \sum_{x\in\{۰,۱\}^n} (-۱)^{f(x)} |x\rangle |-\rangle \qquad (۲۲)$$

از اینجا به بعد، با توجه به این‌که حالت فعلی سیستم جداشدنی است (و با توجه به معادله‌ی فوق، با اعمال مجدد U_f جداشدنی باقی می‌ماند)، توجه خود را تنها به رجیستر اول معطوف خواهیم کرد. فرض کنید حالت رجیستر اول قبل از اولین تکرار گروور را $|\psi_۰\rangle$ بنامیم. بنابراین:

$$|\psi_۰\rangle = \frac{۱}{\sqrt{۲^n}} \sum_{x\in\{۰,۱\}^n} |x\rangle .$$

$|\psi_\circ\rangle$ را به صورت زیر بازنویسی می‌کنیم:

$$|\psi_\circ\rangle = \sqrt{\frac{t}{N}}(\frac{1}{\sqrt{t}}\sum_{x:f(x)=1}|x\rangle) + \sqrt{\frac{N-t}{N}}(\frac{1}{\sqrt{N-t}}\sum_{x:f(x)=\circ}|x\rangle),$$

اگر تعریف کنیم:

$$|G\rangle = \frac{1}{\sqrt{t}}\sum_{x:f(x)=1}|x\rangle\,,$$
$$|B\rangle = \frac{1}{\sqrt{N-t}}\sum_{x:f(x)=\circ}|x\rangle\,,$$
$$\sin\theta = \sqrt{\frac{t}{N}},$$

در این صورت $|\psi_\circ\rangle$ را می‌توان به صورت زیر بازنویسی کرد:

$$|\psi_\circ\rangle = \sin\theta\,|G\rangle + \cos\theta\,|B\rangle\,.$$

روشن است که $|\psi_\circ\rangle$ در صفحه‌ی تولید شده توسط بردارهای متعامد $|G\rangle$ و $|B\rangle$ قرار دارد.

- حال اگر به نگاشت U_f توجه کنیم، از معادله‌ی ۲۲ متوجه می‌شویم که $U_f|G\rangle|-\rangle = -|G\rangle|-\rangle$ و $U_f|B\rangle|-\rangle = |B\rangle|-\rangle$. بنابراین، اگر عمل نگاشت U_f روی رجیستر اول را در نظر بگیریم، به این صورت است که هر بردار در صفحه‌ی تولید شده توسط $|G\rangle$ و $|B\rangle$ را نسبت به بردار $|B\rangle$ بازتاب می‌کند.

- از طرفی به سادگی می‌توان دید که:

$$D = H^{\otimes n}(2\,|\circ^n\rangle\langle\circ^n| - I)H^{\otimes n} = 2\,|\psi_\circ\rangle\langle\psi_\circ| - I.$$

مشابه بند قبل، می‌توان دید که $2\,|\psi_\circ\rangle\langle\psi_\circ| - I$ یک بازتاب در صفحه‌ی دوبعدی تولیدشده توسط $|G\rangle$ و $|B\rangle$، حول بردار $|\psi_\circ\rangle$ را مشخص می‌کند.

- با توجه به دو بند قبل، می‌توان دید با هر بار اعمال یک تکرار گروور، زاویه‌ی بین بردار حاصل و بردار $|B\rangle$ به اندازه‌ی 2θ افزایش می‌یابد. به عبارت دیگر، پس از تکرار k ام گروور حالت رجیستر اول برابر است با:

$$|\psi_k\rangle = \sin(2k+1)\theta\,|G\rangle + \cos(2k+1)\theta\,|B\rangle\,.$$

بنابراین، چنانچه پس از تکرار k ام، حالت رجیستر اول را اندازه بگیریم، با احتمال $|\sin(2k+1)|^2$ حالت سیستم بعد از اندازه‌گیری برابر با $|z\rangle$ است که $f(z) = 1$.

- می‌توان نشان داد برای مقادیر کوچک t، با اعمال $\mathcal{O}\left(\sqrt{\frac{N}{t}}\right)$ بار تکرار گروور، با احتمال خطای کمی، حالت رجیستر اول بعد از اندازه‌گیری برابر است با $|z\rangle$ که $f(z) = 1$. در واقع کافی است k را نزدیک‌ترین عدد صحیح به $\frac{\pi}{4}\sqrt{\frac{2^n}{t}} - \frac{1}{2}$ قرار دهیم، در این صورت $\frac{t}{N}$ کران بالایی برای احتمال خطای الگوریتم خواهد بود، که برای t های به اندازه‌ی کافی کوچک، احتمال ناچیزی خواهد بود.

۲.۳ کاربرد الگوریتم گروور در حمله به رمزهای متقارن

همان‌گونه که از آنالیز فوق بر می‌آید، الگوریتم گروور پیچیدگی زمانی جست‌وجو را به صورت مربعی تسریع می‌کند. به عبارت دیگر، زمان لازم برای جست‌وجوی یک دیتابیس N عضوی را از $\mathcal{O}(N)$ به $\mathcal{O}\left(\sqrt{N}\right)$ کاهش می‌دهد. در ادامه خواهیم دید که چطور می‌توان از این تسریع مربعی در جهت حمله‌ی کاراتر به یک سیستم رمز قالبی بهره گرفت.
فرض کنید یک رمز قالبی داریم که تابع رمزگذاری آن E و طول قالب و کلید آن n است. فرض کنید مهاجم به یک زوج (P, C) دسترسی دارد که $C = E_{k_j}(P)$ و برای سادگی، فرض کنید k_j یکتاست. تابع $F : \{\circ,1\}^n \to \{\circ,1\}$ را به این صورت تعریف می‌کنیم:

$$F(k_i) = \begin{cases} 1 & \text{اگر} \quad E_{k_i}(P) = C \\ \circ & \text{اگر} \quad E_{k_i}(P) \neq C \end{cases}$$

در این صورت با به کار بردن الگوریتم گروور برای تابع فوق، می‌توان k_j را در $\mathcal{O}\left(\sqrt{۲^n}\right)$ پیدا کرد. با وجود این‌که در این روش، هزینه‌ی سرچ کاهش یافته است، اما روشن است که با دوبرابر کردن طول کلید می‌توان با این حمله مقابله کرد [۱۵]. با این وجود، [۳۰] ترکیبی از ایده‌های حمله‌های کلاسیک به رمزهای قالبی و استفاده از الگوریتم گروور را پیشنهاد می‌دهد؛ و نتیجه آن است که با کاهش فضای جست‌وجو، حمله‌ی گروور کاراتر خواهد شد.

۴ الگوریتم سایمون و کاربردهای آن

۱.۴ الگوریتم سایمون

در این بخش، به اختصار الگوریتم سایمون[۳۴] و مسأله‌ای که با این الگوریتم حل می‌شود را توضیح خواهیم داد. این الگوریتم نخستین‌بار توسط دانیل سایمون[۳۵] در [۱] ارائه شد. مسأله‌ای که الگوریتم سایمون آن را حل می‌کند به شرح زیر است:

مسأله‌ی سایمون [۱]

ورودی: دسترسی اوراکلی به تابع $f : \{۰,۱\}^n \to \{۰,۱\}^n$ با این ویژگی که قرارداد شده است که رشته‌ای مانند $s \in \{۰,۱\}^n$ وجود دارد به طوری که برای هر دو رشته‌ی $x, y \in \{۰,۱\}^n$، $f(x) = f(y)$ اگر و تنها اگر $x = y$ یا $x = y \oplus s$.

خروجی: رشته‌ی s.

سایمون الگوریتم زیر را برای حل مسأله‌ی فوق ارائه داد (ما در اینجا، الگوریتم را مطابق با [۴] ارائه خواهیم کرد):

الگوریتم

۱. با دو رجیستر n بیتی شروع می‌کنیم که هر یک در حالت $|۰\rangle^{\otimes n}$ آماده‌سازی شده‌اند. به علاوه، قرار می‌دهیم $Y = \varnothing$.

۲. مراحل زیر را $\mathcal{O}(n)$ بار تکرار می‌کنیم:

(آ) روی رجیستر اول تبدیل هادامارد $H^{\otimes n}$ را اعمال می‌کنیم.

(ب) نگاشت U_f را روی رجیستر اول و دوم اعمال می‌کنیم.

(ج) رجیستر دوم را در پایه‌ی محاسباتی اندازه‌گیری می‌کنیم.

(د) تبدیل هادامارد $H^{\otimes n}$ را روی رجیستر اول اعمال می‌کنیم.

(ه) رجیستر اول را اندازه می‌گیریم. فرض کنید حالت این رجیستر پس از اندازه‌گیری $|y\rangle$ باشد. در این صورت y را به Y اضافه می‌کنیم.

۳. اگر Y شامل n بردار مستقل‌خطی باشد، $s = ۰۰\cdots۰$.

۴. در غیر این صورت، اگر Y شامل $n-۱$ بردار مستقل‌خطی باشد، بردار s برداری است که بر اعضای Y عمود است. (با حل یک دستگاه خطی، s را می‌یابیم.)

۵. در غیر این صورت، خروجی می‌دهیم: «شکست!»

آنالیز درستی الگوریتم فوق:

- پس از اعمال اولین سری از گیت‌های هادامارد حالت سیستم برابر با $|\psi_۰\rangle = \frac{۱}{\sqrt{۲^n}} \sum_{x\in\{۰,۱\}^n} |x\rangle\,|۰^n\rangle$ است.

[34] Simon's algorithm
[35] Danial Simon

- سپس با اعمال گیت U_f، خواهیم داشت:

$$U_f(\frac{۱}{\sqrt{۲^n}}\sum_{x\in\{۰,۱\}^n}|x\rangle\,|۰^n\rangle)=\frac{۱}{\sqrt{۲^n}}\sum_{x\in\{۰,۱\}^n}|x\rangle\,|f(x)\rangle$$

- با اندازه‌گیری رجیستر دوم، حالت سیستم به حالت

$$\frac{۱}{\sqrt{۲}}(|z\rangle+|z\oplus s\rangle)\,|f(z)\rangle$$

فرو می‌ریزد.

- ابتدا توجه کنید که برای هر رشته‌ی $z\in\{۰,۱\}^n$،

$$H^{\otimes n}\,|z\rangle=\frac{۱}{\sqrt{۲^n}}\sum_{x\in\{۰,۱\}^n}(-۱)^{x\cdot z}\,|x\rangle\,.$$

با توجه به این مطلب، با اعمال سری دوم عملگرهای هادامارد بر رجیستر اول، حالت این رجیستر به صورت زیر خواهد بود:

$$\begin{aligned}H^{\otimes n}\frac{۱}{\sqrt{۲}}(|z\rangle+|z\oplus s\rangle)&=\frac{۱}{\sqrt{۲^{n+۱}}}\sum_{x\in\{۰,۱\}^n}((-۱)^{x\cdot z}+(-۱)^{x\cdot(z\oplus s)})\,|x\rangle\\&=\frac{۱}{\sqrt{۲^{n+۱}}}\sum_{x\in\{۰,۱\}^n}((-۱)^{x\cdot z}(۱+(-۱)^{x\cdot s}))\,|x\rangle\end{aligned}$$

با توجه به این معادله، احتمال این که حالت رجیستر اول پس از اندازه‌گیری $|y\rangle$ باشد، که $y\cdot s\neq ۰$، برابر با صفر است. بنابراین با اندازه‌گیری رجیستر اول، با احتمال ۱ حالت این رجیستر به $|y\rangle$ فرو می‌ریزد، به طوری‌که $y\cdot s=۰$.

- حال با پیدا کردن $n-۱$ بردار مستقل خطی مانند $y_۱,y_۲,\ldots,y_{n-۱}$، می‌توان بردار s را به نحوی یافت که بر این $n-۱$ بردار عمود باشد. به علاوه، به سادگی می‌توان نشان داد که به طور متوسط $\mathcal{O}(n)$ بار اجرای حلقه‌ی سایمون برای یافتن $n-۱$ بردار مستقل خطی کافی است.

شمایی از این الگوریتم در شکل ۳ نمایش داده شده است. روشن است که پیچیدگی زمانی اجرای الگوریتم سایمون چندجمله‌ای است. در این‌جا شایان ذکر است که الگوریتم‌های تصادفی کلاسیکی وجود دارند که مسأله‌ی سایمون را در $\mathcal{O}(\sqrt{۲^n})$ حل می‌کنند [۳]. با این وجود، سایمون در [۱] نشان داد که هر الگوریتم کلاسیکی که این مسأله را با احتمال بالا حل کند، نیاز به پرسیدن $\Omega(\sqrt{۲^n})$ کوئری دارد؛ و این در حالی است که الگوریتم سایمون مسأله را در زمان $\mathsf{poly}(n)$ حل می‌کند. بنابراین، الگوریتم سایمون نمونه‌ای از آن دسته از الگوریتم‌های کوانتومی است که به طور اثبات‌شده‌ای بر الگوریتم‌های کلاسیک برتری محاسباتی دارند.

یادداشت ۱.۴ توجه کنید که در تعریف مسأله‌ی سایمون، وجود s به عنوان یک ویژگی برای تابع ورودی قرارداد شده است. با این حال، ممکن است لزوما این شرط برآورده نشود. به این معنی که ممکن است $t\notin\{۰,s\}$ هایی موجود باشند که برای بعضی x ها، $f(x)=f(x\oplus t)$. در چنین حالاتی نیز الگوریتم سایمون به همان صورت ارائه شده در این زیربخش، کار می‌کند. کاپلان و همکاران در [۴] نشان دادند که اگر تابع f شرط

$$\max_{t\notin\{۰,s\}}\Pr_x[f(x\oplus t)=f(x)]\leq\frac{۱}{۲}$$

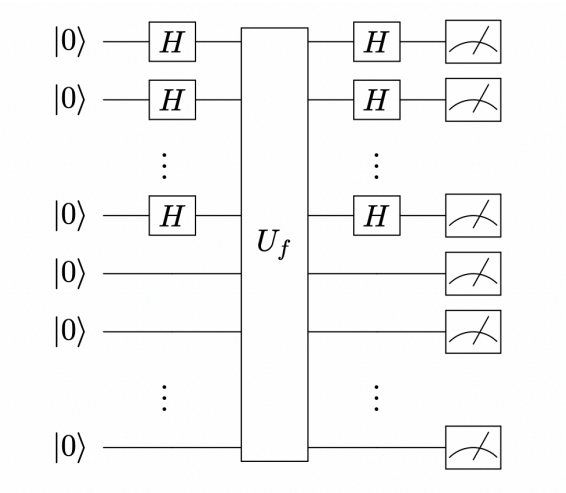
را برآورده کند، الگوریتم سایمون همچنان با $\mathcal{O}(n)$ بار تکرار حلقه، با احتمال خطایی که به صورت نمایی کاهش می‌یابد، s را خواهد یافت. ما در اینجا از بیان این جزئیات تکنیکی صرف‌نظر می‌کنیم و خواننده را برای جزئیات بیشتر به منبع مزبور ارجاع می‌دهیم. ◁

۲.۴ کاربرد در حمله به شبکه‌ی فایستل ۳-دوری

استفاده از شبکه‌های فایستل[۳۶] یکی از روش‌های رایج در رمزنگاری قالبی است. این شبکه‌ها روشی برای ساخت توابع وارون‌پذیر از روی مولفه‌های غیر وارون‌پذیر در اختیار ما می‌گذارند و از این جهت در رمزنگاری متقارن اهمیتی ویژه دارند [۵].

[36] Feistel networks

شکل ۳: شمایی از الگوریتم سایمون



یک شبکه‌ی فایستلی (شکل ۴) از تکرار r دور با ساختار یکسان تشکیل شده است. هر دور از یک تابع دور[۳۷] f_{k_i} و یک عملگر جابه‌جایی تشکیل شده است. در ابتدا ورودی (که یک رشته‌ی $۲n$ بیتی است) به دو زیررشته‌ی n بیتی $(L_۰, R_۰)$ جدا می‌شود و سپس برای هر $i \geq ۱$، خروجی دور iام شبکه‌ی فایستلی به شکل زیر صورت می‌گیرد:

$$L_i = R_{i-۱} \tag{۲۳}$$
$$R_i = L_{i-۱} \oplus f_{k_i}(R_{i-۱}) \tag{۲۴}$$

به سادگی می‌توان دید که یک شبکه‌ی فایستلی، فارغ از این‌که توابع دور جایگشت باشند یا نه، یک جایگشت را روی ورودی خود اعمال می‌کند.

تمایزناپذیری یک شبکه‌ی فایستلی از یک جایگشت تصادفی، موضوعی است که در آنالیز امنیت این رمزها اهمیت دارد. قضیه‌ی زیر از لوبی و راکوف نشان می‌دهد که برخی شبکه‌های فایستلی ۳ـدوری را با تعداد چندجمله‌ای کوئری از اوراکل آن نمی‌توان از یک جایگشت کاملا تصادفی تمییز داد.

تعریف ۲.۴ فرض کنید $F : \{۰,۱\}^* \times \{۰,۱\}^* \to \{۰,۱\}^*$ تابعی کارا و حافظ طول باشد؛ کارا به این معنی که $F(k,x)$ از روی ورودی‌های k و x در زمان چندجمله‌ای محاسبه شود؛ و حافظ طول به آن معنی که چنانچه (k,x) ورودی تابع باشند، طول k، x و $F(k,x)$ برابر باشد. علاوه بر این برای هر $k \in \{۰,۱\}^n$ تعریف کنید $F_k(\cdot) := F(k,\cdot)$. تابع F را شبه‌تصادفی نامیم هرگاه برای هر مهاجم چندجمله‌ای D، تابع ناچیز $\mathsf{negl}(n)$ موجود باشد چنانکه

$$\left|\Pr_{k\leftarrow\{۰,۱\}^n}\left[D^{F_k(\cdot)}(۱^n)=۱\right] - \Pr_{f\leftarrow \text{Func}_n}\left[D^{f(\cdot)}(۱^n)=۱\right]\right| \leq \mathsf{negl}(n), \tag{۲۵}$$

که در این‌جا مقصود از $D^{\mathcal{O}((\cdot)}$، این است که الگوریتم D دسترسی اوراکلی به تابع $\mathcal{O}(\cdot)$ دارد.

به طور مشابه با تابع شبه‌تصادفی، می‌توان جایگشت شبه‌تصادفی را نیز تعریف کرد. ◄

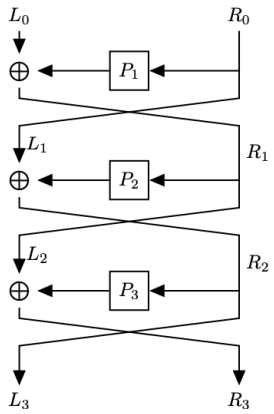
قضیه ۳.۴ (لوبی‌ـراکوف) *فرض کنید F تابعی شبه‌تصادفی است. در این صورت یک شبکه‌ی فایستل ۳ـدوری با توابع دور $f_{k_۱}$، $f_{k_۲}$ و $f_{k_۳}$ یک جایگشت شبه‌تصادفی از $۲n$ بیت است [۷].*

قضیه‌ی فوق نشان می‌دهد که با یک الگوریتم کلاسیک چندجمله‌ای که دسترسی اوراکلی به یک شبکه‌ی فایستل دارد، نمی‌توان آن را از یک جایگشت کاملا تصادفی تمایز داد. در ادامه نشان خواهیم داد که یک مهاجم کوانتومی با دسترسی اوراکلی به شبکه‌ی مزبور، می‌تواند بین آن و یک جایگشت کاملا تصادفی تمایز قائل شود. اثباتی که در این‌جا بیان می‌کنیم، مطابق [۶] است؛ که با فرض این‌که توابع دور جایگشت هستند این تمایزپذیری را نشان داده است. پس از بیان این اثبات، درباره‌ی حالت‌های کلی‌تر بحث خواهیم کرد.

قضیه ۴.۴ *الگوریتمی کوانتومی با زمان چندجمله‌ای برای تمایز دادن یک شبکه‌ی فایستل ۳ـدوری با توابع دور جایگشت از یک جایگشت تصادفی روی $۲n$ بیت وجود دارد [۶].*

[37] round function

شکل ۴: شمایی از یک شبکه‌ی فایستلی ۳ـدوری؛ تصویر برگرفته از مرجع [۹] است.



اثبات. فرض کنید جایگشت $\mathcal{V} : \{۰,۱\}^{۲n} \to \{۰,۱\}^{۲n}$ در دست است و مهاجم قصد دارد با دسترسی اوراکلی به این تابع، در زمان چندجمله‌ای تصمیم بگیرد که آیا این تابع مربوط به یک شبکه‌ی فایستلی است و یا یک جایگشت تصادفی است. تابع $\mathcal{W} : \{۰,۱\}^{۲n} \to \{۰,۱\}^{n}$ را به این صورت تعریف می‌کنیم که $\mathcal{W}(x)$ برابر با n بیت سمت چپ خروجی $\mathcal{V}(x)$ باشد. توجه کنید که اگر $\mathcal{V}$ تابع ورودی‌ـخروجی یک شبکه‌ی فایستلی ۳ـدوری باشد، در این صورت می‌توان گفت $\mathcal{W}(L_۰, R_۰) = L_۳$. هم‌چنین فرض کنید $\alpha_۰, \alpha_۱ \in \{۰,۱\}^{n}$ رشته‌هایی متمایز و n بیتی باشند. تابع $f : \{۰,۱\}^{n+۱} \to \{۰,۱\}^{n}$ را به صورت زیر تعریف می‌کنیم:

$$f(b, L_۰) = \mathcal{W}(L_۰, \alpha_b) \oplus \alpha_b \tag{۲۶}$$

تابع f به $\mathcal{W}$ (و در نتیجه به $\mathcal{V}$) وابسته است.

لم ۵.۴ *اگر $\mathcal{V}$ تابع ورودی‌ـخروجی یک شبکه‌ی فایستلی ۳ـدوری باشد، برای هر دو رشته‌ی $(b, L_۰) \neq (b', L'_۰)$ داریم:*

$$f(b, L_۰) = f(b', L'_۰) \iff b = b' \oplus ۱ \text{ و } L_۰ = L'_۰ \oplus f_{k_۱}(\alpha) \oplus f_{k_۱}(\beta) \tag{۲۷}$$

برای اثبات لم فوق، بنا به تقارن میان b و b'، کافی است تنها دو حالت زیر را در نظر بگیریم: نخست فرض کنید $b = b' = ۰$. در این صورت:

$$\begin{aligned} f(b, L_۰) = f(b', L'_۰) &\iff \mathcal{W}(L_۰, \alpha_۰) \oplus \alpha_۰ = \mathcal{W}(L_۰{}', \alpha_۰) \oplus \alpha_۰ \\ &\iff \alpha_۰ \oplus f_{k_۲}(L_۰ \oplus f_{k_۱}(\alpha_۰)) \oplus \alpha_۰ = \alpha_۰ \oplus f_{k_۲}(L_۰{}' \oplus f_{k_۱}(\alpha_۰)) \oplus \alpha_۰ \end{aligned}$$

که با توجه به این‌که f_{k_i} ها جایگشت هستند، نتیجه می‌شود $L_۰ = L_۰{}'$ که خلاف فرض است.
در حالت دیگر، فرض کنید $b = ۰$ و $b' = ۱$. در این حالت داریم:

$$\begin{aligned} f(b, L_۰) = f(b', L'_۰) &\iff \mathcal{W}(L_۰, \alpha_۰) \oplus \alpha_۰ = \mathcal{W}(L_۰{}', \alpha_۱) \oplus \alpha_۱ \\ &\iff \alpha_۰ \oplus f_{k_۲}(L_۰ \oplus f_{k_۱}(\alpha_۰)) \oplus \alpha_۰ = \alpha_۱ \oplus f_{k_۲}(L_۰{}' \oplus f_{k_۱}(\alpha_۱)) \oplus \alpha_۱ \\ &\iff L_۰{}' = L_۰ \oplus f_{k_۱}(\alpha_۰) \oplus f_{k_۱}(\alpha_۱) \end{aligned}$$

از لم ۵.۴ درمی‌یابیم که قراردادی مشابه با آن‌چه در مسأله‌ی سایمون قرارداد شده بود، اینجا نیز برقرار است. به عبارت دیگر، تابع f در قرارداد سایمون با $s = (۱, f_{k_۱}(\alpha_۰) \oplus f_{k_۱}(\alpha_۱)) \in \{۰,۱\}^{n+۱}$ صدق می‌کند. از سوی دیگر، چنانچه $\mathcal{V}$ تابع ورودی‌ـخروجی یک شبکه‌ی فایستلی ۳ـدوری نباشد، و یک جایگشت تصادفی باشد، با احتمال بالا $s \neq ۰$ وجود ندارد به نحوی که $\Pr_x[f(x \oplus s) = f(x)] > \frac{۱}{۲}$ [۸]. حال، الگوریتمی که مهاجم می‌تواند برای تمایز دادن یک شبکه‌ی فایستلی از یک جایگشت تصادفی به کار ببرد را ارائه می‌دهیم. فرض کنید که مهاجم دسترسی اوراکلی کوانتومی به تابع f دارد.

الگوریتم

۱. مقدار اولیه‌ی مجموعه‌ی χ را برابر با تهی قرار می‌دهیم.

۲. تا زمانی که χ دارای n بردار مستقل خطی شود مراحل زیر را تکرار می‌کنیم:

(آ) اگر $|\chi| \geq ۲n$، در این صورت خروجی می‌دهیم: «$\mathcal{V}$ یک شبکه‌ی فایستلی است.»

(ب) الگوریتم سایمون را برای تابع f اجرا می‌کنیم و خروجی الگوریتم (برداری مانند $y = (y_۰, y_۱, \ldots, y_n)$) را به χ می‌افزاییم.

۳. دستگاه معادلات خطی

$$\begin{pmatrix} & | & \\ y_۱ & \cdots & y_n \\ & | & \end{pmatrix} \begin{pmatrix} s_۱ \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} | \\ y_۰ \\ | \end{pmatrix} \qquad (۲۸)$$

را حل می‌کنیم و بردار $(s_۱, \ldots, s_n)$ را به دست می‌آوریم.

۴. به صورت تصادفی یک رشته‌ی $n+۱$ بیتی مانند u انتخاب می‌کنیم و $u' = u \oplus (۱, s_۱, s_۲, \ldots, s_n)$ را حساب می‌کنیم.

۵. $f(u)$ و $f(u')$ را حساب می‌کنیم. اگر با هم برابر بودند، خروجی می‌دهیم: «$\mathcal{V}$ یک شبکه‌ی فایستلی است.»؛ و اگر برابر نباشند خروجی می‌دهیم: «$\mathcal{V}$ یک جایگشت تصادفی است.»

با توضیحات بالا، روشن است که الگوریتم فوق، در حالتی که $\mathcal{V}$ یک شبکه‌ی فایستلی است، با احتمال ۱ جواب درست می‌دهد. به علاوه، می‌توان نشان داد در حالتی که $\mathcal{V}$ یک جایگشت کاملا تصادفی است، با احتمال ناچیزی پاسخ اشتباه خواهد داد. از طرفی توجه کنید که زمان الگوریتم فوق، چندجمله‌ای است و به این ترتیب، نتیجه می‌شود که قضیه‌ی لوبی-راکوف در حالتی که توابع دور جایگشت‌های شبه تصادفی باشند، برای یک مهاجم کوانتومی برقرار نخواهد ماند. □

یادداشت ۶.۴ سانتولی و شفنر در [۹] و کاپلان و همکاران در [۴] درستی قضیه‌ی ۴.۴ را در حالتی که توابع دور، توابع شبه‌تصادفی هستند نیز نشان داده‌اند. در حالتی که توابع دور جایگشت نباشند، در آنالیزی که در [۶] ارائه شده است مشکلی پیش می‌آید. مشکل این است که ممکن است قرارداد مسأله‌ی سایمون به‌طور کامل برقرار نشود؛ به این معنی که yهایی وجود داشته باشند به طوری که $f(x) = f(y)$ و $y \notin \{x, x \oplus s\}$ (اصطلاحا برخوردهای ناخواسته وجود داشته باشند). به عبارت دیگر، در حالتی که توابع دور، توابع شبه‌تصادفی باشند، جهت عکس حکم ۲۷ دیگر برقرار نیست. [۹] برای حل این مشکل، الگوریتم ارائه شده در [۶] را به صورتی که در اثبات فوق ارائه کردیم تغییر می‌دهد (با این وجود، تحلیل درستی الگوریتم کمی با آن‌چه در بالا گفتیم متفاوت است). در مقابل، [۴] برای حل مشکل، آنالیزی کلی‌تر از الگوریتم سایمون، مطابق آن‌چه در یادداشت ۱.۴ به آن اشاره کردیم ارائه می‌دهد؛ به این ترتیب که کران بالایی برای تعداد دفعات استفاده از مدار الگوریتم سایمون بر حسب تعداد برخوردهای ناخواسته می‌یابد و نشان می‌دهد الگوریتم سایمون همچنان با زمان چندجمله‌ای و احتمال خطای کم در این حالت قابل تطبیق خواهد بود. ▷

۳.۴ کاربرد در حمله به سیستم ایون-منصور

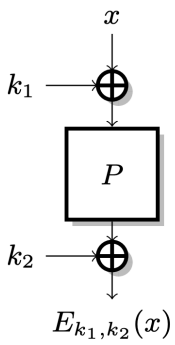
افزون بر آن‌چه که در بالا به آن اشاره کردیم، از الگوریتم سایمون می‌توان در حمله به سیستم‌های متقارن دیگری نیز بهره گرفت. به عنوان مثالی از چنین سیستم‌هایی، سیستم ایون-منصور[۳۸] (شکل ۵) را بررسی می‌کنیم.

یادآوری می‌کنیم که در سیستم ایون-منصور، برای رمز کردن یک پیام P، از یک تابع جایگشت تصادفی (در اختیار عموم) Π و کلیدهای $\frac{n}{۲}$ بیتی $k_۱$ و $k_۲$ استفاده می‌شود. فرض کنید $k = (k_۱, k_۲)$ و برای سادگی، طول k را برابر با n در نظر بگیرید. عمل رمزنگاری به صورت زیر است:

$$E_{k_۱,k_۲}(P) = \Pi(P \oplus k_۱) \oplus k_۲. \qquad (۲۹)$$

[38] Even-Mansour

شکل ۵: شمایی از یک رمز ایون-منصور؛ تصویر برگرفته از مرجع [۴] است.



امنیت این سیستم در [۳۱، ۳۲] مورد بررسی قرار گرفته است؛ و نشان داده شده است که شکستن آن به زمان $\mathcal{O}\left(۲^{\frac{n}{۲}}\right)$ نیاز دارد.

برای شکستن این سیستم با استفاده از الگوریتم سایمون، مشابه با حمله‌ای که در بخش قبل مطرح کردیم، کافی است تابع f را طوری تعریف کنیم که در قرارداد سایمون صدق کند و دوره‌ی تناوب آن، اطلاعاتی در مورد کلید در اختیار ما قرار دهد. سپس با استفاده از الگوریتم سایمون، دوره‌ی تناوب را در زمان چندجمله‌ای به دست آوریم. فرض کنید تابع $f : \{۰,۱\}^{\frac{n}{۲}} \to \{۰,۱\}^{\frac{n}{۲}}$ به صورت زیر تعریف شده است:

$$f(x) = E_k(x) \oplus \Pi(x) \tag{۳۰}$$

در این صورت داریم:

$$\begin{aligned} f(x \oplus k_۱) &= E_k(x \oplus k_۱) \oplus \Pi(x \oplus k_۱) \\ &= (\Pi(x \oplus k_۱ \oplus k_۱) \oplus k_۲) \oplus \Pi(x \oplus k_۱) \\ &= \Pi(x) \oplus (\Pi(x \oplus k_۱) \oplus k_۲) \\ &= f(x) \end{aligned}$$

بنابراین با استفاده از الگوریتم سایمون می‌توان $k_۱$ را به دست آورد. پس از به دست آوردن $k_۱$، با انتخاب تصادفی یک $x \in \{۰,۱\}^{\frac{n}{۲}}$، مقدار $k_۲$ از رابطه‌ی

$$k_۲ = f(x) \oplus \Pi(x) \oplus \Pi(x \oplus k_۱)$$

به دست می‌آید.

یادداشت ۷.۴ حمله‌ی کوانتومی به رمز ایون-منصور برای اولین‌بار در [۳۳] مطرح شده است. نکته‌ای که باید به آن توجه کرد ولی در [۳۳] مغفول مانده است، این است که مشابه شبکه‌های فایستلی، در رمز ایون-منصور نیز ممکن است وجود برخوردهای ناخواسته، موجب شود قرارداد الگوریتم سایمون به طور کامل برقرار نشود. با توجه به یادداشت ۱.۴ می‌توان نشان داد که در حضور چنین برخوردهای ناخواسته‌ای، اگر

$$\max_{t \notin \{۰,s\}} \Pr_x[f(x \oplus t) = f(x)] \leq \frac{۱}{۲},$$

باز هم الگوریتم سایمون قابل استفاده است. کاپلان و همکاران در [۴] در حالتی که شرط فوق برقرار نشود، یک حمله‌ی کلاسیک پیشنهاد داده‌اند که خواننده‌ی علاقه‌مند می‌تواند به آن مراجعه کند. ◁

در پایان، شایان ذکر است که کاربرد الگوریتم سایمون، تنها محدود به موارد فوق نیست. سانتولی و شفنر در [۹] و کاپلان و همکاران در [۴]، کاربردهای دیگری از الگوریتم سایمون در حمله به ساختارهای LRW و کدهای اصالت‌سنجی پیام که مبتنی بر رمزهای قالبی هستند ارائه می‌دهند. همچنین در مقاله‌ی اخیر نشان داده شده است که الگوریتم سایمون می‌تواند منجر به تسریعی نمایی در نوعی از حمله‌های کلاسیک به رمزهای قالبی، که به حمله‌های لغزشی[۳۹] مشهورند [۳۴]، شود.

[39] slide attacks

۵ جمع‌بندی و نتیجه‌گیری

در این گزارش، ابتدا به بررسی تاریخی برخی رخدادهایی که در توسعه‌ی محاسبات کوانتومی نقش جدی داشتند، پرداختیم و سپس وجوهی از اهمیت بررسی الگوریتم‌های کوانتومی برای آنالیز امنیت سیستم‌های رمزنگاری را بیان کردیم. در ادامه، پس از یادآوری برخی پیشنیازهای ضروری در جبرخطی و مکانیک کوانتومی، تصریح کردیم که در ادامه‌ی بحث، مقصودمان از یک الگوریتم کوانتومی چیست.
با این مقدمات، به سراغ دو الگوریتم کوانتومی رفته و تلاش کردیم برخی تاثیرات وجود چنین الگوریتم‌هایی را بر امنیت سیستم‌های رمزنگاری مطالعه کنیم. الگوریتم نخست، الگوریتم جست‌وجوی گروور بود. دیدیم که گرچه این الگوریتم مسأله‌ای بسیار پرکاربرد را حل می‌کند، اما در حمله به سیستم‌های رمزنگاری چندان راهگشا نیست؛ و دلیل هم آن است که این الگوریتم، حداکثر یک تسریع مربعی برای حل مسأله خواهد داشت؛ و در نتیجه‌ی آن تهدید یک مهاجم گروور، به راحتی با دوبرابر کردن طول کلید قابل دفع است.
در ادامه،به عنوان دومین الگوریتم کوانتومی، الگوریتم سایمون را معرفی کردیم و نشان دادیم که با استفاده از این الگوریتم، یک مهاجم می‌تواند در زمان چندجمله‌ای یک شبکه‌ی فایستل ۳ـدوری با توابع دور جایگشت را از یک جایگشت تصادفی تمییز دهد؛ نتیجه‌ای که در حالت کلاسیک برقرار نیست. به طور مشابهی دیدیم که الگوریتم سایمون می‌تواند در حمله به سیستم ایون–منصور نیز موثر واقع شود. در واقع، ایده‌ی استفاده از الگوریتم سایمون به این صورت است که تابع مناسبی که در قرارداد سایمون صدق می‌کند، تعریف می‌شود که تابعی متناوب است؛ و دوره‌ی تناوب آن می‌تواند اطلاعاتی را در مورد سیستم رمزنگاری یا کلید آشکار کند. در این‌جاست که الگوریتم سایمون می‌تواند برای یافتن دوره‌ی تناوب تابع مزبور در زمان چندجمله‌ای به ما کمک کند.
آن‌چه که در گزارش فوق درباره‌ی آن بحث کردیم، از جهات مختلفی اهمیت دارد: از یک سو نشان دهنده‌ی این است که بسیاری از ساختارهایی که به طور گسترده در سیستم‌های متقارن کلاسیک مورد استفاده قرار می‌گیرند، ممکن است در حضور مهاجم‌های کوانتومی امن نباشند. این مسأله ما را به اهمیت روش‌های رمزنگاری پساکوانتومی رهنمون می‌کند. از سوی دیگر، بررسی کاربردهای الگوریتم سایمون در حمله به رمزهای متقارن، منجر به آنالیز دقیق‌تری از الگوریتم سایمون در حالت‌های تعمیم‌یافته شده است؛ که این مسأله در حوزه‌ی طراحی الگوریتم‌های کوانتومی اهمیت می‌یابد.

مراجع

References

[1] D. R. Simon, “On the power of quantum computation,” *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 116–123, 1994.

[2] R. Cleve, “An introduction to quantum complexity theory,” in *Quantum Computation and Quantum Information Theory*. WORLD SCIENTIFIC, Jan. 2001, pp. 103–127. [Online]. Available: https://doi.org/10.1142/9789810248185_0004

[3] R. de Wolf, “Quantum computing: Lecture notes,” *CoRR*, vol. abs/1907.09415, 2019. [Online]. Available: http://arxiv.org/abs/1907.09415

[4] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, “Breaking symmetric cryptosystems using quantum period finding,” in *Advances in Cryptology – CRYPTO 2016*, M. Robshaw and J. Katz, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 207–237.

[5] J. Katz and Y. Lindell, *Introduction to Modern Cryptography, Second Edition*, 2nd ed. Chapman Hall/CRC, 2014.

[6] H. Kuwakado and M. Morii, “Quantum distinguisher between the 3-round feistel cipher and the random permutation,” in *2010 IEEE International Symposium on Information Theory*, 2010, pp. 2682–2685.

[7] M. Luby and C. Rackoff, “How to construct pseudorandom permutations from pseudorandom functions,” *SIAM Journal on Computing*, vol. 17, no. 2, pp. 373–386, 1988. [Online]. Available: https://doi.org/10.1137/0217022

[8] J. Daemen and V. Rijmen, "Probability distributions of correlation and differentials in block ciphers," *Journal of Mathematical Cryptology*, vol. 1, no. 3, pp. 221–242, 2007. [Online]. Available: https://doi.org/10.1515/JMC.2007.011

[9] T. Santoli and C. Schaffner, "Using simon's algorithm to attack symmetric-key cryptographic primitives," *Quantum Info. Comput.*, vol. 17, no. 1–2, p. 65–78, feb 2017.

[10] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997. [Online]. Available: https://doi.org/10.1137/S0097539795293172

[11] A. Chi-Chih Yao, "Quantum circuit complexity," in *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*, 1993, pp. 352–361.

[12] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information: 10th anniversary edition*. Cambridge University Press, 2010.

[13] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, "Tight bounds on quantum searching," *Fortschritte der Physik*, vol. 46, no. 4-5, pp. 493–505, jun 1998. [Online]. Available: https://doi.org/10.1002%2F%28sici%291521-3978%28199806%2946%3A4%2F5%3C493%3A%3Aaid-prop493%3E3.0.co%3B2-p

[14] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, ser. STOC '96. New York, NY, USA: Association for Computing Machinery, 1996, p. 212–219. [Online]. Available: https://doi.org/10.1145/237814.237866

[15] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post Quantum Cryptography*, 1st ed. Springer Publishing Company, Incorporated, 2008.

[16] 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. 22, pp. 563–591, 1980.

[17] R. P. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, no. 6, pp. 467–488, 1982.

[18] D. Deutsch and R. Penrose, "Quantum theory, the church–turing principle and the universal quantum computer," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 400, no. 1818, pp. 97–117, 1985. [Online]. Available: https://royalsocietypublishing.org/doi/abs/10.1098/rspa.1985.0070

[19] D. Deutsch, "Quantum computational networks," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 425, pp. 73 – 90, 1989.

[20] E. Bernstein and U. Vazirani, "Quantum complexity theory," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1411–1473, 1997. [Online]. Available: https://doi.org/10.1137/S0097539796300921

[21] A. Wigderson, *Mathematics and Computation: A Theory Revolutionizing Technology and Science*. Princeton University Press, 2019. [Online]. Available: http://www.jstor.org/stable/j.ctvckq7xb

[22] F. Gieres, "Mathematical surprises and dirac's formalism in quantum mechanics," *Reports on Progress in Physics*, vol. 63, no. 12, pp. 1893–1931, nov 2000. [Online]. Available: https://doi.org/10.1088%2F0034-4885%2F63%2F12%2F201

[23] L. Fortnow, "One complexity theorist's view of quantum computing," *arXiv*, 2000.

[24] P. A. M. Dirac, *The Principles of Quantum Mechanics*, reprint, revised ed. Clarendon Press, 1981.

[25] H. Guo, *What Are Tensors Exactly?* World Scientific, 2021. [Online]. Available: https://www.worldscientific.com/doi/abs/10.1142/12388

[26] M. Planck, "Ueber das gesetz der energieverteilung im normalspectrum," *Annalen der Physik*, vol. 309, no. 3, pp. 553–563, 1901. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/andp.19013090310

[27] A. Einstein, "Concerning an heuristic point of view toward the emission and transformation of light," *Annalen Phys.*, vol. 17, pp. 132–148, 1905.

[28] N. B. D. phil., "I. on the constitution of atoms and molecules," *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, vol. 26, no. 151, pp. 1–25, 1913. [Online]. Available: https://doi.org/10.1080/14786441308634955

[29] J. Von Neumann, *Mathematische grundlagen der quantenmechanik*, ser. Die grundlehren der mathematischen wissenschaften in einzeldarstellungen... bd. XXXVIII. J. Springer, 1932. [Online]. Available: https://books.google.com/books?id=uqvQAAAAMAAJ

[30] A. Yamamura and H. Ishizuka, "Quantum cryptanalysis of block ciphers (algebraic systems, formal languages and computations)," , vol. 1166, pp. 235–243, 2000.

[31] S. Even and Y. Mansour, "A construction of a cipher from a single pseudorandom permutation," *Journal of Cryptology*, vol. 10, pp. 151–161, 1997.

[32] J. Daemen, "Limitations of the even-mansour construction," in *Advances in Cryptology - ASIACRYPT '91, International Conference on the Theory and Applications of Cryptology, Fujiyoshida, Japan, November 11-14, 1991, Proceedings*, ser. Lecture Notes in Computer Science, vol. 739. Springer, 1991, pp. 495–498.

[33] H. Kuwakado and M. Morii, "Security on the quantum-type even-mansour cipher," in *2012 International Symposium on Information Theory and its Applications*, 2012, pp. 312–316.

[34] A. Biryukov and D. Wagner, "Slide attacks," in *Fast Software Encryption: 6th International Workshop, FSE'99 Rome, Italy, March 24–26, 1999 Proceedings 6.* Springer, 1999, pp. 245–259.