

---

# آشنایی با کامپیوترهای کوانتومی

دیوید مک ماهون

دکتر داریوش شیری

نیاز دانش

سرشناسه	: مک ماهون، دیوید ام. (David M.) McMahon
عنوان و نام پدیدآور	: <b>آشنایی با کامپیوترهای کوانتومی</b> / دیوید مک ماهون؛ [مترجم] داریوش شیری.
مشخصات نشر	: تهران: نیاز دانش، ۱۳۹۶
شابک	: ۹۷۸-۶۰۰-۷۷۲۴-۸۵-۹
مشخصات ظاهری	: ۳۳۶ ص.: مصور، جدول، نمودار.
وضعیت فهرست نویسی	: فیپا
یادداشت	: عنوان اصلی: Quantum computing explained, c2008.
موضوع	: کامپیوترهای کوانتومی Quantum computers
شناسه افزوده	: شیری، داریوش، ۱۳۵۴ - مترجم
رده بندی کنگره	: ۱۳۹۶ م/۷۷۵/۸۸۹/۸۷۶ QAY۶
رده بندی دیویی	: ۰۰۴/۱
شماره کتابشناسی ملی	: ۴۷۹۱۵۹۸



نام کتاب	: <b>آشنایی با کامپیوترهای کوانتومی</b>
نویسنده	: دیوید مک ماهون
مترجم	: دکتر داریوش شیری
مدیر اجرایی - ناظر بر چاپ	: حمیدرضا محمد شیرازی - محمد شمس
ناشر	: نیاز دانش
صفحه آرا	: واحد تولید انتشارات نیاز دانش
نوبت چاپ	: اول - ۱۳۹۶
شمارگان	: ۱۰۰ نسخه
قیمت	: ۲۸۰۰۰۰ ریال

ISBN:978-600-7724-85-9

شابک: ۹۷۸-۶۰۰-۷۷۲۴-۸۵-۹

هرگونه چاپ و تکثیر (اعم از زیراکس، بازنویسی، ضبط کامپیوتری و تهیهی CD) از محتویات این اثر بدون اجازه کتبی ناشر ممنوع است، متخلفان به موجب بند ۵ از ماده ۲ قانون حمایت از مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

کلیه حقوق این اثر برای ناشر محفوظ است.

آدرس انتشارات: تهران، میدان انقلاب، خیابان ۱۲ فروردین، تقاطع وحید نظری، پلاک ۲۵۵، طبقه ۱، واحد ۲

۰۲۱-۶۶۴۷۸۱۰۶-۶۶۴۷۸۱۰۸-۰۹۱۲۷۰۷۳۹۳۵

[www.Niye-Danesh.com](http://www.Niye-Danesh.com)

مشاوره جهت نشر: ۲۱۰۶۷۰۹ - ۰۹۱۲

## فهرست مطالب

خلاصه	۴۴
تمرین‌ها	۴۴

### فصل ۳

ماتریس‌ها و آپراتورها	۴۷
مشاهده‌پذیرها	۴۸
آپراتورهای پاولی	۴۸
ضرب‌های خارجی	۴۹
روابط بسته بودن	۵۰
نمایش آپراتورها با ماتریس	۵۰
ضرب‌های خارجی و نمایش ماتریسی آنها	۵۱
نمایش ماتریسی آپراتورها در فضای دو بعدی	۵۱
تعریف: ماتریس‌های پاولی	۵۲
آپراتورهای هرمیتی، یکانی و نُرمال	۵۳
تعریف: آپراتور هرمیتی	۵۵
تعریف: آپراتور یکانی	۵۵
تعریف: آپراتور نُرمال	۵۵
مقادیر ویژه و بردارهای ویژه	۵۶
معادلهٔ مشخصه	۵۶
تجزیه طیفی	۶۰

### فصل ۱

درآمدی کوتاه بر نظریهٔ اطلاعات	۱۳
اطلاعات کلاسیک	۱۳
محتوای اطلاعاتی یک سیگنال	۱۵
آنتروپی و نظریهٔ اطلاعات شانون	۱۵
مبانی احتمالات	۱۸
تمرین‌ها	۲۰

### فصل ۲

کیوبیت و حالت‌های کوانتومی	۲۱
کیوبیت	۲۱
فضاهای برداری	۲۴
ترکیب خطی بردارها	۲۶
یکتایی مجموعهٔ پرکننده (پایه)	۲۸
پایه و بُعد	۲۹
ضرب‌های داخلی	۳۰
ارتونرمال بودن	۳۳
متعامدسازی گرام - اشمیت	۳۵
فرمالیزم برا - کت	۳۷
نابرابری کوشی - شوارتز و نابرابری مثلثی	۴۰

تعریف: یافتن مقدار چشم داشتی با اپراتور چگالی.....	۶۱
ویژگی‌های مهم رد.....	۶۳
مقدار چشم‌داشتی یک اپراتور.....	۶۴
تابع اپراتورها.....	۶۶
تبدیلات یکانی.....	۶۷
اپراتورهای تصویر.....	۶۹
اپراتورهای مثبت.....	۷۲
جبر جابجا کننده‌ها (کموتاتورها).....	۷۳
اصل عدم قطعیت هایزنبرگ.....	۷۵
تجزیه قطبی و مقادیر تکین.....	۷۵
اصول موضوع مکانیک کوانتومی.....	۷۶
گزاره ۱: حالت یک سیستم.....	۷۷
گزاره ۲: کمیت‌های مشاهده پذیر که با اپراتور نشان داده می‌شوند.....	۷۷
گزاره ۳: اندازه‌گیری.....	۷۷
گزاره ۴: روند زمانی یک سیستم.....	۷۷
تمرین‌ها.....	۷۸

### فصل ۶

نظریه اندازه‌گیری کوانتومی.....	۱۲۹
تمایز حالت‌های کوانتومی و اندازه‌گیری.....	۱۲۹
اندازه‌گیری‌های نگاشتی.....	۱۳۱
اندازه‌گیری سیستم‌های مختلط.....	۱۴۰
اندازه‌گیری‌های تعمیم یافته.....	۱۴۶
اندازه‌های مثبت با مقدار اپراتوری.....	۱۴۸
تمرین‌ها.....	۱۵۲

### فصل ۷

درهم تافتگی.....	۱۵۵
قضیه بل.....	۱۵۹
سیستم‌های دو بخشی و پایه بل.....	۱۶۴
چه وقت یک حالت درهم تافته است؟.....	۱۶۶
نمایش پاولی.....	۱۷۰

### فصل ۴

ضرب تانسوری.....	۸۱
نمایش حالت‌های ترکیبی در مکانیک کوانتومی.....	۸۱
محاسبه ضرب‌های داخلی.....	۸۳
ضرب تانسوری بردارهای ستونی.....	۸۵
اپراتورها و ضرب تانسوری.....	۸۶
ضرب تانسوری ماتریس‌ها.....	۹۰
تمرین‌ها.....	۹۱

### فصل ۵

اپراتور چگالی.....	۹۳
اپراتور چگالی برای حالت سره.....	۹۴
تعریف: اپراتور چگالی برای حالت سره.....	۹۵

## فصل ۱۰

کاربردهای درهم تافتگی	۲۳۳	همان‌دهی درهم تافتگی	۱۷۴
ترارسانی و کدینگ ابرفشرده	۲۳۳	نمایش اپراتور چگالی با حالت‌های بل	۱۷۵
ترارسانی	۲۳۳	تجزیه آشمت	۱۷۶
شرط پرز برای ترانهادگی پاره‌ای	۲۳۷	پالایش	۱۷۸
جابه‌جا کردن درهم تافتگی	۲۴۲	تمرین‌ها	۱۷۸
کدینگ ابرفشرده (چگال)	۲۴۴		
تمرین‌ها	۲۴۶		

## فصل ۱۱

رمزنگاری کوانتومی	۲۴۷	گیت‌ها و مدارهای کوانتومی	۱۸۱
مرور کوتاهی بر رمزنگاری RSA	۲۴۸	گیت‌های منطقی کلاسیک	۱۸۱
رمزنگاری کوانتومی پایه	۲۵۱	گیت‌های یک کیوبیتی	۱۸۴
یک مثال از حمله: حمله با NOT کنترل شده	۲۵۴	انواع دیگر از گیت‌های تک کیوبیتی	۱۸۷
پروتکل B92	۲۵۵	تابع نمایی	۱۹۰
پروتکل E91	۲۵۶	تجزیه Z-Y	۱۹۲
تمرین‌ها	۲۵۷	نمودار مدارهای ساده کوانتومی	۱۹۲
		گیت‌های کنترل شونده	۱۹۳
		تجزیه گیت‌ها	۱۹۹
		تمرین‌ها	۲۰۲

## فصل ۱۲

نویز کوانتومی و اصلاح خطا	۲۵۹	گیت‌های هادامارد	۲۰۵
خطاهای تک کیوبیت	۲۵۹	گیت فاز	۲۰۶
عملیات کوانتومی و اپراتور کراوس	۲۶۱	نمایش ماتریسی عملیات سری و موازی	۲۰۹
کانال یاد قطبیده	۲۶۸	تداخل کوانتومی	۲۱۰
کانال‌های وارونش بیت و وارونش فاز	۲۶۹	موازی بودن کوانتومی و ارزیابی تابع	۲۱۱
افت دامنه	۲۷۰	الگوریتم دوچ - جوزا	۲۱۴
افت فاز	۲۷۷	تبدیل فوری کوانتومی	۲۱۸
اصلاح خطای کوانتومی	۲۷۹	تخمین فاز	۲۲۱
تمرین‌ها	۲۸۴	الگوریتم شر	۲۲۳

## فصل ۱۳

ابزارهای نظریه اطلاعات کوانتومی	۲۸۷	جستجوی کوانتومی و الگوریتم گراور	۲۲۶
قضیه منع همانند سازی	۲۸۷	تمرین‌ها	۲۲۹

## فصل ۸

گیت‌ها و مدارهای کوانتومی	۱۸۱
گیت‌های منطقی کلاسیک	۱۸۱
گیت‌های یک کیوبیتی	۱۸۴
انواع دیگر از گیت‌های تک کیوبیتی	۱۸۷
تابع نمایی	۱۹۰
تجزیه Z-Y	۱۹۲
نمودار مدارهای ساده کوانتومی	۱۹۲
گیت‌های کنترل شونده	۱۹۳
تجزیه گیت‌ها	۱۹۹
تمرین‌ها	۲۰۲

## فصل ۹

الگوریتم‌های کوانتومی	۲۰۵
گیت‌های هادامارد	۲۰۶
گیت فاز	۲۰۹
نمایش ماتریسی عملیات سری و موازی	۲۰۹
تداخل کوانتومی	۲۱۰
موازی بودن کوانتومی و ارزیابی تابع	۲۱۱
الگوریتم دوچ - جوزا	۲۱۴
تبدیل فوری کوانتومی	۲۱۸
تخمین فاز	۲۲۱
الگوریتم شر	۲۲۳
جستجوی کوانتومی و الگوریتم گراور	۲۲۶
تمرین‌ها	۲۲۹

## فصل ۱۵

محاسبه کوانتومی با حالت‌های خوشه‌ای ..	۳۲۱
حالت‌های خوشه‌ای ..	۳۲۲
آماده کردن حالت خوشه‌ای ..	۳۲۲
ماتریس‌های همسایگی ..	۳۲۵
حالت‌های پایدار ساز ..	۳۲۵
پیوست: شاهد (معیار) درهم‌تافتگی ..	۳۲۸
پردازش حالت خوشه‌ای ..	۳۲۹
تمرین‌ها ..	۳۳۲

فاصله رد ..	۲۸۸
همان‌دهی ..	۲۹۳
درهم‌تافتگی تشکیل و Concurrence ..	۲۹۷
محتوای اطلاعاتی و آنتروپی ..	۳۰۲
تمرین‌ها ..	۳۰۹

## فصل ۱۴

کامپیوترهای کوانتومی آدیباتیک ..	۳۱۱
فرآیندهای آدیباتیک ..	۳۱۴
محاسبه کوانتومی آدیباتیک ..	۳۱۵
تمرین‌ها ..	۳۱۸

## پیشگفتار نویسنده

منطقی است که یکی از مهمترین پیشرفت‌های دانش و مهندسی نتیجه‌ی پژوهش‌های میان رشته‌ای در "قرن بیست و یکم" باشد. یکی از جالب‌ترین و مهیج‌ترین این پیشرفت‌ها که به زودی شاهد پیاده‌سازی آن خواهیم بود کامپیوتر کوانتومی است. محاسبه (رایانش) کوانتومی که آمیزه‌ی دانش فیزیک و کامپیوتر است از این مکتب فکری سرچشمه می‌گیرد که می‌گوید اطلاعات ماهیت فیزیکی دارد یعنی اطلاعات را نمی‌توان بدون یک محیط (رسانه‌ی) مادی بوجود آورد یا پردازش کرد.

کامپیوترهای کوانتومی از نظر تئوری نشان داده‌اند که می‌توانند در بسیاری از موارد از کامپیوترهای کلاسیک سریع‌تر باشند. برای مثال الگوریتم تجزیه‌ی اعداد به عامل‌های اول آن، یعنی الگوریتم Shor را می‌توان روی کامپیوترهای کوانتومی طوری پیاده کرد که به سرعت کد اطلاعات رمز شده را بازگشایی کنند. سیستم‌های پردازش داده‌ی کوانتومی، می‌توانند کارهایی انجام دهند که از عهده‌ی کامپیوترهای کلاسیک خارج است، مثلاً تراسپورت (teleportation) حالت یک ذره از یک مکان به مکان دیگر و نیز ساختن رمزهای غیرقابل شکستن برای سیستم‌های رمزنگاری داده.

روش ارائه مطلب در این کتاب به دلایل زیر جزئی و عمیق نیست. این کتاب برای دو دسته از خوانندگان نوشته شده است. گروه نخست دانشجویان دوره‌ی کارشناسی فیزیک، ریاضی و علوم کامپیوتر هستند. بیشتر کتاب‌هایی که درباره‌ی کامپیوترها و نظریه‌ی اطلاعات کوانتومی نگاشته شده‌اند برای این دسته از خوانندگان دشوار هستند. این کتاب خلأ موجود را با ارائه یک متن ساده پر می‌کند و کمک می‌کند تا این دانشجویان مفاهیم اساسی دانش اطلاعات کوانتومی را فراگیرند.

در درجه‌ی دوم برای خوانندگانی نوشته شده است که در رشته‌های دیگر تخصص دارند مثلاً مهندسان، شیمی‌دانان و زیست‌شناسان. این خوانندگان ممکن است به اندازه‌ی متخصصان کامپیوترهای کوانتومی، در فیزیک کوانتومی و ریاضی پیش‌زمینه‌ی کافی نداشته باشند. این کتاب به اصطلاح "دست خواننده را می‌گیرد" تا علاوه بر مفاهیم پایه‌ای، مقداری هم محاسبه‌ی تئوری انجام دهد.

سرانجام این که کتاب برای دانشجویان تحصیلات تکمیلی فیزیک و کامپیوتر که درس کامپیوترهای کوانتومی می‌گذرانند، می‌تواند یک مرجع کمکی با مثال‌های عددی فراوان باشد در کنار متن اصلی و جزوه‌ی درسی‌شان.

هدف این کتاب بازکردن موضوع و آشنا کردن خواننده‌ی غیرمتخصص با کامپیوترهای کوانتومی است. بنابراین سطح آن ساده‌تر از کتاب‌های استاندارد موجود در بازار است. نحوه‌ی ارائه مطالب هم، نحوه‌ی مرسوم آن نیست، برای این که خواننده با مفاهیم پایه‌ای آشنا شود و آن‌ها را با حل مثال‌های عددی فرا گیرد. بعضی از موضوعات را در این کتاب نگنجانده‌ام یا خیلی عمیق بررسی نکرده‌ام، چون فرض شده که خواننده می‌تواند آن‌ها را در کتاب‌های سطح کارشناسی ارشد پیدا کند. مثلاً بررسی دقیق کامپیوترهای کوانتومی بی‌دررو (adiabatic) و حالت خوشه‌ای (cluster state) فراتر از سطح این کتاب است. بنابراین نمی‌توان گفت که کتاب از هر جهت کامل است. ولی به خوانندگانی که به تازگی وارد این رشته شده‌اند به اندازه‌ی کافی اطلاعات و [انگیزه] می‌دهد که بر پایه‌ی آن مطالعات خود را ادامه بدهند.

گرچه تلاش شده که کتاب زمینه‌ی وسیعی را دربرگیرد ولی نحوه‌ی ارائه کمی گرایش فیزیکی دارد.

دیوید مک ماهون

آزمایشگاه‌های ملی سندیا- نیو مکزیکو



## پیشگفتار مترجم

کتاب‌های بسیاری دربارهٔ محاسبات و پردازش اطلاعات کوانتومی نوشته شده‌اند که دارای درجات مختلف پیچیدگی هستند و بسته به این که تخصص نویسنده چیست، به زمینه خاصی از این رشته تأکید دارند. نویسنده کتابی که در دست دارید<sup>1</sup> فرض کرده که خواننده پیش زمینهٔ کافی دربارهٔ مکانیک کوانتومی (جبر دیراک و مکانیک ماتریسی) و نظریهٔ اطلاعات ندارد. به همین دلیل با زبانی ساده و با تمرین‌ها و مثال‌های گوناگون خواننده را با مفاهیمی مثل فضای هیلبرت، برهم نهی، ضرب تانسوری، ماتریس چگالی، درهم تافتگی و آنتروپی آشنا می‌کند و پس از آن خواننده را به دنیای گیت‌های کوانتومی، الگوریتم‌های کوانتومی، رمزنگاری، اصلاح خطا و نویز کوانتومی رهنمون می‌شود. از این رو این کتاب را برای ترجمه برگزیدم تا دانشجویان و مهندسان برق و کامپیوتر و حتی دانش‌آموزان علاقه‌مند دبیرستانی هم بتوانند با این رشته به صورت خودآموز آشنا شوند و چه بسا با ادامهٔ مطالعه به فکر کار و پژوهش در این رشته بیفتند.

هنگام ترجمه متوجه چند اشتباه تایپی در فرمول‌های اصل کتاب شدم که آنها را اصلاح کرده‌ام. هر جا که احساس کردم جمله‌بندی کتاب به اندازهٔ کافی ساده یا رسا نیست، توضیحاتی را در [ ] افزوده‌ام یا در پاورقی نوشته‌ام. اگرچه سعی کرده‌ام برای واژگان تخصصی این رشته معادل فارسی پیدا کنم ولی در اولین برخورد با واژه در متن، معادل انگلیسی را در ( ) آورده‌ام تا بدانید اصل واژه چه بوده است و اگر خواستید بیشتر بدانید، آنها را در جستجوگرهای اینترنتی پیدا کنید. اگر معادل فارسی

<sup>1</sup> David McMahon, Quantum Computing Explained, Wiley-IEEE Computer Society Press, 2008

را نمی‌پسندید به کتاب واژگان فیزیک مرکز نشر دانشگاهی و یا جزوه‌های درسی استادان این رشته در ایران مراجعه کنید.

به خواننده گرامی توصیه می‌کنم با شکیبایی و علاقه فصل ۱ تا ۸ را بخواند و مثال‌ها و تمرین‌های کتاب را خودش با مداد و کاغذ حل کند. به قول ریچارد فاینمن (Richard Feynman)، فیزیکدان و معلم افسانه‌ای فیزیک، هیچ چیز جای مسأله حل کردن را برای یادگیری نمی‌گیرد. بعد از فصل ۸ می‌توانید تصمیم بگیرید که به کدام کاربرد پردازش اطلاعات کوانتومی علاقه دارید و از میان فصل‌های ۹ تا ۱۵ هر کدام را دوست داشتید برگزینید.

اگر هم با احتمالی اندک بعد از خواندن این کتاب دریافتید که به "کامپیوتر کوانتومی" علاقه‌ای ندارید، نه تنها چیزی را از دست نداده‌اید بلکه مقدار زیادی مبانی مکانیک کوانتومی، نظریه اطلاعات و رمزنگاری فرا گرفته‌اید که می‌توانید از آن به عنوان پیش‌نیاز یا شروع برای زمینه‌های دیگر بهره ببرید. برای مثال مفهوم درهم تافتگی و حالت‌های خوشه‌ای را برای حل مسائل سیستم‌های بس ذره‌ای در فیزیک ماده چگال بکار ببرید یا رمزنگاری کلاسیک را دنبال کنید و یا کاربرد مفهوم ضرب تانسوری را در مسائل ریاضی کاربردی جستجو کنید.

درضمن، دیوید مک ماهون کتاب‌های دیگری هم به زبان ساده و با مثال‌های فراوان در زمینه مکانیک کوانتومی و نظریه میدان‌های کوانتومی نگاشته است که آنها هم شروع خوبی برای مطالعه جدی در نظریه کوانتومی هستند.

می‌توانید کتاب‌های پیشرفته‌تر زیر را هم بخوانید، مثل کتاب دانش کامپیوتر کوانتومی نوشته دیوید مرمین<sup>۱</sup>، کتاب درسی نیلسن و چوانگ<sup>۲</sup> و اگر می‌خواهید روش ساخت و پیاده‌سازی گیت‌ها و مدارهای کوانتومی را ببینید به کتاب ناکاهارا و اُمی<sup>۳</sup> نگاه کنید.

ترجمه این کتاب سال ۲۰۱۳ انجام شد و پس از آن در جستجوی ناشری بودم تا اینکه همکار پیشین بنده، خانم مهندس سیده مهتا جنابی از شرکت کاوش کام آسیا، انتشارات نیاز دانش را به بنده معرفی کردند. بعد از تماس با این انتشارات، مدیریت محترم آن جناب آقای مهندس حمیدرضا شیرازی به گرمی پذیرای چاپ کتاب شدند و با تلاش همکاران گرامی ایشان کتاب به سرعت آماده چاپ شد.

از همگی این بزرگواران نامبرده سپاسگزارم. از پدر و مادر، همسر و برادرانم که مشوق و پیگیر روند ترجمه و انتشار این کتاب بودند سپاسگزارم. از پروفیسور جان مارتینیس (John Martinis)، از دانشگاه کالیفرنیا در سانتا باربارا که اجازه دادند شکل تراشه پردازنده چهار کیوبیتی آزمایشگاه ایشان را

<sup>1</sup> Quantum Computer Science, N. David Mermin, 1<sup>st</sup> Edition, Cambridge University Press, 2007

<sup>2</sup> Quantum Computation and Quantum Information, 10<sup>th</sup> Edition, Michael A. Nielsen, Isaac L. Chuang, Cambridge University Press, 2010

<sup>3</sup> Quantum Computing: From Linear Algebra to Physical Realizations, Mikio Nakahara, Tetsuo Ohmi, CRC Press, 2008

برای طرح روی جلد بکار ببرم نیز سپاسگزارم. در پایان این ترجمه را تقدیم می‌کنم به همه دانش‌آموزان و دانش‌جویان امیدوار ایران زمین که سرمایه‌ای جز توکل به خدا و اعتماد به نفس، و تفریحی جز کتاب و کتابخوانی ندارند.

داریوش شیری  
بهار ۱۳۹۶ - سوئد