

مقدمه‌ای بر ارتباطات کوانتومی

سرپرست مؤلفین:

سارا توفیقی

عضو هیئت علمی پژوهشگاه ارتباطات و فناوری اطلاعات

ویراستاران:

مریم افسری، سارا توفیقی

مؤلفین:

آزاده احمدیان، سید محمود اشرفی، مریم افسری، مرضیه‌السادات
بطحایی، نجمه تابع بردبار، سارا توفیقی، لیلا چهره‌قانی انزابی،
سروش خادمی، معصومه شیرچیان، فرناز فرمان، اعظم مانی،
مرتضی نیک‌آیین، مهدی هاشمی، منیره هوشمند

مقدمه‌ای بر ارتباطات کوانتومی

تألیف: سارا توفیقی (عضو هیئت علمی پژوهشگاه ارتباطات و فناوری اطلاعات)

ناشر: آتی‌نگر

چاپ اول: ۱۴۰۰

شمارندگان: ۵۰ نسخه

صفحه‌آرایی: ساغر حسابی

قیمت: ۲۴۰۰۰۰ تومان

شابک: ۹۷۸-۶۲۲-۷۵۷۱-۲۹-۵

نشانی مرکز پخش: میدان انقلاب، خیابان جمالزاده جنوبی، پلاک ۱۴۴، واحد ۹

انتشارات آوین قلم

تلفن: ۶۶۹۰۶۳۷۶ - ۹۳۶۴۳۷۹۴۲۷

"کلیه حقوق این اثر متعلق به پژوهشگاه ارتباطات و فن‌آوری اطلاعات می‌باشد."

در کانال تلگرامی ما عضو شوید: <https://t.me/ghanjinebook>

سرشناسه

عنوان و نام پدیدآور

مشخصات ناشر

مشخصات ظاهری

شابک

وضعیت فهرست‌نویسی

یادداشت

یادداشت

موضوع

موضوع

موضوع

موضوع

موضوع

موضوع

موضوع

موضوع

شناسه افزوده

شناسه افزوده

رده‌بندی کنگره

رده‌بندی دیویی

شماره کتابشناسی ملی

اطلاعات رکورد کتابشناسی

توفیقی، سارا. ۱۳۶۴-

: مقدمه‌ای بر ارتباطات کوانتومی / سرپرست مؤلفین سارا توفیقی؛ مؤلفین آزاده

احمدیان ... [و دیگران]؛ ویراستاران مریم افسری، سارا توفیقی.

: تهران، آتی‌نگر، ۱۴۰۰.

: [۷۰۹] ص: ۲۱/۵×۱۴/۵ س.م

: 978-622-7571-29-5

: فیبا

: مؤلفین آزاده احمدیان، سید محمود اشرفی، مریم افسری، مرضیه‌السادات

بطحایی، نجمه تابع‌بردبار، سارا توفیقی، لیلا چهره‌قانی انزایی، سروش خادمی،

معصومه شیرچیجان، فرناز فرمان، اعظم مانی، مرتضی نیک‌آیین، مهدی هاشمی،

منیره هوشمند.

: کتابنامه

: ارتباط کوانتومی

Quantum communication :

: کوانتوم

Quantum theory :

: کامپیوترهای کوانتومی

Quantum computers :

: نظریه اطلاعات

Quantum computers :

: احمدیان، آزاده، ۱۳۵۳-

: افسری، مریم، ۱۳۶۵؛ ویراستار

QC۱۷۴ :

: ۵۳۹

: ۸۵۰۷۲۴۷

: فیبا

فهرست مطالب

۱	پیشگفتار
۳	فصل اول- مقدمه
۵	۱- انقلاب کوانتومی
۶	۲- اهمیت و ضرورت فناوری های کوانتومی در حوزه فاوا
۱۰	۳- درخت فناوری ارتباطات و رمزنگاری کوانتومی
۱۰	۳-۱- توزیع کلید کوانتومی
۱۴	۳-۲- ارتباط امن کوانتومی
۱۵	۳-۳- گفتگو و گردهمایی کوانتومی
۱۵	۳-۴- تسهیم راز کوانتومی
۱۶	۳-۵- احراز اصالت کوانتومی
۱۶	۳-۶- امضای دیجیتال کوانتومی
۱۷	۳-۷- مزایده کوانتومی
۱۷	۳-۸- ارتباطات نیمه کوانتومی
۱۷	۳-۹- پنهان نگاری کوانتومی
۱۸	۳-۱۰- زنجیره بلوک کوانتومی
۱۸	۳-۱۱- فرابرد کوانتومی
۱۹	۳-۱۲- تدارک حالت کوانتومی از راه دور
۱۹	۳-۱۳- رمزگذاری هم ریخت کوانتومی
۲۰	۳-۱۴- شبکه های کوانتومی
۲۱	۳-۱۴-۱- شبکه های کوانتومی مبتنی بر گردهای قابل اعتماد
۲۲	۳-۱۴-۲- شبکه های کوانتومی مبتنی بر گردهای نسبتاً قابل اعتماد
۲۲	۳-۱۴-۳- شبکه ماهواره های کوانتومی
۲۴	۳-۱۴-۴- شبکه های کوانتومی مبتنی بر گردهای غیر قابل اعتماد (ایترنت کوانتومی)
۲۷	فصل دوم- مبانی مکانیک کوانتومی
۲۹	۱- مقدمه
۲۹	۲- تاریخچه مکانیک کوانتومی
۳۳	۳- مبانی ریاضی مکانیک کوانتومی
۳۳	۳-۱- فضای برداری
۳۳	۳-۱-۱- تعریف فضای برداری
۳۳	۳-۱-۲- ضرب داخلی
۳۳	۳-۱-۳- پایه ها و بعد فضای برداری
۳۴	۳-۲- فضای هیلبرت
۳۴	۳-۲-۱- نمادگذاری دیراک

فهرست مطالب

۳۵	 ۳-۳- عملگرهای خطی
۳۶	 ۱-۳-۳- جابه‌جایی عملگرها
۳۶	 ۲-۳-۳- ضرب خارجی
۳۷	 ۳-۳-۳- نمایش ماتریسی عملگرها
۳۷	 ۴-۳-۳- رد یک عملگر
۳۸	 ۵-۳-۳- ویژه‌بردارها و ویژه‌مقادیر عملگر
۳۸	 ۴-۳- عملگرهای پرکاربرد در مکانیک کوانتومی
۳۹	 ۱-۴-۳- عملگر هرمیتی
۳۹	 ۲-۴-۳- عملگر یکانی
۳۹	 ۵-۳- ضرب تانسوری فضاهای برداری
۴۱	 ۴- اصول موضوعه مکانیک کوانتومی
۴۱	 ۱-۴- حالت یک سامانه فیزیکی
۴۲	 ۱-۱-۴- نمایش‌های مختلف یک بردار از فضای هیلبرت
۴۲	 ۲-۱-۴- مفهوم فیزیکی بردار حالت
۴۲	 ۳-۱-۴- اصل برهم‌نهی
۴۳	 ۴-۱-۴- حالت خالص و آمیخته
۴۴	 ۵-۱-۴- هیبت کوانتومی (کیوبیت)
۴۶	 ۲-۴- مشاهده‌پذیرهای فیزیکی و عملگرها
۴۷	 ۳-۴- اندازه‌گیری کوانتومی و نتایج تصادفی
۴۸	 ۱-۳-۴- مشاهده‌پذیرهای گسسته و پیوسته
۴۸	 ۲-۳-۴- عملگرهای تصویر
۴۹	 ۳-۳-۴- مقدار انتظاری
۵۰	 ۴-۳-۴- اندازه‌گیری هم‌زمان مشاهده‌پذیرها
۵۱	 ۵-۳-۴- اصل عدم قطعیت
۵۱	 ۶-۳-۴- اندازه‌گیری سامانه کوانتومی با حالت آمیخته
۵۲	 ۷-۳-۴- اندازه‌گیری غیرمتعامد یا تعمیم‌یافته
۵۳	 ۸-۳-۴- اندازه‌گیری عام یا POVM
۵۵	 ۴-۴- تحول سامانه کوانتومی
۵۶	 ۱-۴-۴- تحول زمانی سامانه کوانتومی با حالت آمیخته
۵۶	 ۲-۴-۴- تصویر شرودینگر و هایزنبرگ
۵۷	 ۵-۴- سامانه‌های کوانتومی مرکب
۵۸	 ۱-۵-۴- درهم‌تنیدگی
۵۹	 ۲-۵-۴- حالات درهم‌تنیده بل
۶۰	 ۳-۵-۴- عملگر چگالی کاهش‌یافته

فهرست مطالب

۶۱	 ۴-۵-۴- قضیه کبی ممنوع
۶۲	 ۵- ایده‌های انقلابی مکانیک کوانتومی
۶۲	 ۵-۱- ویژگی تصادفی عملگر چگالی کاهش یافته
۶۲	 ۵-۲- عدم قطعیت
۶۳	 ۵-۳- کوانتش
۶۳	 ۵-۴- برهم‌نهی
۶۵	 ۵-۵- درهم‌تنیدگی
۶۷	 فصل سوم- مبانی اپتیک کوانتومی
۶۹	 ۱- مقدمه
۶۹	 ۲- تاریخچه
۷۱	 ۳- کوانتش میدان الکترومغناطیس
۷۴	 ۳-۱- چارک‌های میدان الکترومغناطیس
۷۵	 ۳-۲- حالت تعداد
۷۶	 ۳-۲-۱- افت‌وخیزهای میدان الکتریکی
۷۷	 ۳-۳- کوانتش میدان چند مودی
۷۹	 ۳-۴- حالت همدوس
۸۲	 ۳-۴-۱- تولید حالت همدوس
۸۴	 ۳-۵- حالت چلانده
۸۸	 ۳-۵-۱- تولد حالت چلانده
۸۹	 ۳-۶- حالت گرمایی
۹۱	 ۴- توابع همدوسی
۹۱	 ۴-۱- تابع همدوسی مرتبه اول
۹۴	 ۴-۲- تابع همدوسی مرتبه دوم
۹۵	 ۵- طبقه‌بندی آماری حالات کوانتومی نور
۹۶	 ۵-۱- آمار شمارش فوتون
۹۸	 ۵-۲- آمار فوتونی خوشه‌ای و پاد خوشه‌ای
۱۰۰	 ۵-۲-۱- حالت‌های نور کلاسیک
۱۰۱	 ۵-۲-۲- حالت‌های نور کوانتومی
۱۰۴	 ۶- نمایش‌های مختلف حالات کوانتومی نور
۱۰۵	 ۶-۱- بسط بر حسب حالات تعداد
۱۰۵	 ۶-۲- بسط بر حسب حالات همدوس
۱۰۵	 ۶-۲-۱- نمایش P
۱۰۷	 ۶-۲-۲- نمایش ویگنر
۱۰۹	 ۶-۲-۳- نمایش Q

فهرست مطالب

۱۱۳	فصل چهارم - مروری بر مفاهیم مخابرات از کلاسیک تا کوانتوم
۱۱۵	۱- مقدمه
۱۱۶	۲- مخابرات کلاسیک
۱۱۸	۳- گذار از سامانه‌های آنالوگ به دیجیتال
۱۱۹	۱-۳- قضیه نرخ نمونه‌برداری شانون
۱۲۰	۲-۳- انتقال اطلاعات از طریق مدولاسیون
۱۲۰	۱-۲-۳- مدولاسیون PAM
۱۲۰	۲-۲-۳- مدولاسیون PDM
۱۲۴	۳-۲-۳- مدولاسیون PPM
۱۲۴	۴- سامانه‌های دیجیتال
۱۲۴	۱-۴- کوانتیده کردن سیگنال در مخابرات کلاسیک
۱۲۶	۲-۴- کانال کلاسیک
۱۲۶	۱-۲-۴- کانال دودویی متقارن BSC
۱۲۷	۲-۲-۴- کانال دودویی پاک‌کننده BEC
۱۲۷	۳-۲-۴- کانال AWGN-BI
۱۲۸	۵- نظریه اطلاعات کلاسیک
۱۲۸	۱-۵- آنتروپی
۱۳۰	۲-۵- اطلاعات مشترک
۱۳۰	۳-۵- قضیه کدگذاری منبع شانون
۱۳۴	۴-۵- ظرفیت کانال کلاسیک
۱۳۷	۵-۵- قضیه کدگذاری کانال نویزدار شانون
۱۴۰	۶- مخابرات کوانتومی
۱۴۱	۱-۶- کانال‌های کوانتومی
۱۴۴	۱-۱-۶- کانال افت فاز
۱۴۵	۲-۱-۶- کانال افت دامنه
۱۴۶	۳-۱-۶- کانال نویز جمعی
۱۴۶	۴-۱-۶- کانال نویز پائولی
۱۴۷	۲-۶- ظرفیت کانال کوانتومی
۱۴۸	۱-۲-۶- کمیت هولوو
۱۴۸	۱-۱-۲-۶- کانال بدون نویز
۱۴۹	۲-۱-۲-۶- کانال نویزی
۱۵۰	۲-۲-۶- ظرفیت کلاسیک کانال کوانتومی
۱۵۴	۱-۲-۲-۶- خاصیت جمع‌پذیری
۱۵۵	۲-۲-۲-۶- ظرفیت هولوو-شوماخر-وستمورلند

فهرست مطالب

۱۵۷	 ۳-۲-۶ ظرفیت خصوصی کانال کوانتومی
۱۵۸	 ۴-۲-۶ ظرفیت با کمک درهم‌تنیدگی
۱۵۹	 ۱-۴-۲-۶ کدگذاری ابرچگال
۱۶۳	 فصل پنجم- مبانی توزیع کلید کوانتومی
۱۶۵	 ۱- مقدمه
۱۶۷	 ۲- مروری بر سامانه‌های رمزنگاری
۱۶۸	 ۱-۲- سامانه‌های رمزنگاری متقارن
۱۶۹	 ۲-۲- سامانه‌های رمزنگاری نامتقارن
۱۷۳	 ۳- سامانه‌های رمزنگاری کوانتومی
۱۷۴	 ۱-۳- مؤلفه‌های اصلی سامانه‌های رمزنگاری کوانتومی
۱۷۶	 ۲-۳- مراحل انجام پروتکل‌های توزیع کلید کوانتومی
۱۷۶	 ۱-۲-۳- تدارک و اندازه‌گیری
۱۷۸	 ۲-۲-۳- غربالگری
۱۷۸	 ۳-۲-۳- تخمین پارامتر
۱۷۸	 ۴-۲-۳- تصحیح خطا
۱۷۹	 ۵-۲-۳- تقویت حریم خصوصی
۱۷۹	 ۶-۲-۳- احراز اصالت
۱۸۱	 ۳-۳- جنبه‌های کوانتومی توزیع کلید به روش کوانتومی
۱۸۳	 ۴- انواع دسته‌بندی پروتکل‌های توزیع کلید کوانتومی
	 ۱-۴- دسته‌بندی پروتکل‌های توزیع کلید کوانتومی بر اساس دسترس‌پذیری ایو
۱۸۳	 به دستگاه‌های آلیس و باب
۱۸۳	 ۲-۴- دسته‌بندی پروتکل‌های توزیع کلید کوانتومی بر اساس نوع کدکردن
۱۸۳	 ۱-۲-۴- پروتکل‌های توزیع کلید کوانتومی با متغیرهای گسسته
۱۸۴	 ۲-۲-۴- پروتکل‌های توزیع کلید کوانتومی با متغیرهای گسسته
۱۸۴	 ۳-۲-۴- پروتکل‌های توزیع کلید کوانتومی مرجع فاز توزیع‌شده
۱۸۴	 ۵- پارامترهای عملکرد پروتکل‌های توزیع کلید کوانتومی
۱۸۵	 ۱-۵- نرخ خطای بیت کوانتومی
۱۸۵	 ۲-۵- نرخ توزیع کلید امن
۱۸۶	 ۳-۵- فاصله
۱۸۷	 ۴-۵- چالش‌های تجربی و پیاده‌سازی
۱۸۹	 ۶- حملات کوانتومی و امنیت پروتکل‌های توزیع کلید کوانتومی
۱۹۲	 ۱-۶- نمونه‌هایی از حملات انفرادی
۱۹۲	 ۱-۱-۶- حمله قطع و باز ارسال
۱۹۲	 ۲-۱-۶- حمله تمیز دادن غیرمهم حالات

پیشگفتار

پژوهشگاه ارتباطات و فناوری اطلاعات بر مبنای اهداف سند راهبردی برنامه ششم توسعه وزارت ارتباطات و فناوری اطلاعات در خصوص "رصد فناوری‌های پیشرفته و تولید محصولات بومی"، فعالیت پژوهشی در حوزه ارتباطات کوانتومی نوری را با توجه به اهمیت موضوع از اوایل سال ۱۳۹۴ در دستور کار خود قرار داد. در اواخر سال ۱۳۹۵، پروژه‌ی بنیادی^۱ در حوزه ارتباطات کوانتومی در این پژوهشگاه و با بهره‌گیری از توان علمی نخبگان دانشگاهی آغاز به کار کرد که در بهمن‌ماه ۱۳۹۶ به اتمام رسید. با توجه به ضرورت به‌کارگیری فناوری‌های کوانتومی در حوزه فضا و اهمیت استراتژیک آن‌ها برای کشور، پژوهشگاه ارتباطات و فناوری اطلاعات موضوع فناوری‌های کوانتومی کاربردیپذیر در حوزه فضا را از اوایل سال ۱۳۹۷ به‌عنوان یک موضوع محوری در دستور کار خود قرار داد. در همین راستا پروژه راهبردی تدوین نقشه راه فناوری‌های کوانتومی کاربردیپذیر در حوزه فضا^۲، در اواخر سال ۱۳۹۷ آغاز به کار کرد که در شهریورماه ۱۳۹۸ به اتمام رسید.

در حین اجرای این دو پروژه، سمینارها و کارگاه‌های متعددی از طرف اعضای گروه پروژه برگزار شد که با استقبال خوب دانشجویان و علاقه‌مندان به حوزه فناوری‌های کوانتومی مواجه شد. پیگیری‌ها و علاقه‌مندی مخاطبین برای دسترسی به مرجعی فارسی که مبانی ارتباطات کوانتومی را به زبانی ساده توضیح می‌دهد، ما را بر آن داشت تا خلاصه‌ای از فعالیت‌های انجام‌شده در حوزه ارتباطات کوانتومی در این دو پروژه را در قالب کتاب *مقدمه‌ای بر ارتباطات کوانتومی* در اختیار علاقه‌مندان قرار دهیم. هدف از تألیف این کتاب، معرفی اجمالی فناوری ارتباطات کوانتومی و جنبه‌های مختلف آن به زبانی ساده و قابل‌درک برای علاقه‌مندان از گرایش‌های مختلف است. بدین منظور فناوری ارتباطات و رمزنگاری کوانتومی در فصل یک معرفی می‌شود و ضرورت به‌کارگیری آن در حوزه فضا تبیین می‌شود. مبانی مکانیک کوانتومی و مبانی اپتیک کوانتومی موردنیاز در فصل ۲ و ۳ کتاب به‌اختصار بیان شده است. سپس در فصل ۴ نگاهی اجمالی به سیر تحولی مخابرات در دنیای کلاسیک و گذار آن به مکانیک کوانتومی بیان شده است.

^۱ کد پروژه: ۴۴۰۹۵۰۷۰۰

^۲ کد پروژه: ۴۴۰۹۷۱۰۱۰