شکستن پروتکل‌های رمزنگاری با استفاده از حملات کوانتومی سازگارپذیر پیشرفته

محمدعلی خواجه‌ئیان

استاد راهنما: زهرا شاطرزاده‌یزدی
دانشکدهٔ علوم مهندسی / دانشگاه تهران

۲۸ اردیبهشت ۱۴۰۴

فهرست

فهرست

قسمت ۱

تعریف مسئله

تعریف مسئله

الگوریتم های کوانتومی سازگارپذیر[1] که از ترکیب پردازش کلاسیک و کوانتومی استفاده می‌کنند، گزینه‌ای مناسب برای **رایانه‌های کوانتومی اندازه‌میانی پراختلال**[2] هستند. این پژوهش کارایی الگوریتم های کوانتومی سازگارپذیر را در شکستن **رمزنگاری یکسان‌کلید**[3] و بهینه‌سازی این حمله‌ها بررسی می‌کند.

[1] Variational Quantum Algorithms
[2] Noisy Intermediate Scale Quantum Device
[3] Symmetric-Key Cryptography

قسمت ۲

اهداف

اهداف پژوهش

اهداف اصلی این پروژه به شرح زیر هستند:

1. طراحی و پیاده‌سازی نسخه‌های بهینه‌شده از الگوریتم های کوانتومی سازگارپذیر جهت کاهش زمان اجرا و افزایش دقت
2. کاهش تعداد کیوبیت‌های موردنیاز از طریق به‌کارگیری **کدگذاری غیرمتعامد**[4]
3. ارائه الگوریتمی کارا برای استفاده روی پلتفرم‌های رایانه‌های کوانتومی اندازه‌میانی پراختلال با قابلیت حمل به دستگاه‌های کوانتومی پیشرفته‌تر در آینده

[4] Non-Orthogonal Encoding

اهداف پژوهش

اهداف اصلی این پروژه به شرح زیر هستند:

۴. ارائه الگوریتمی کارا برای استفاده روی پلتفرم‌های رایانه‌های کوانتومی اندازه‌میانی پراختلال با قابلیت حمل به دستگاه‌های کوانتومی پیشرفته‌تر در آینده

۵. مقایسه عملکرد الگوریتم طراحی‌شده با الگوریتم‌های **بی‌رویه**[5] کلاسیک و الگوریتم **گروور**[6] از نظر سرعت، دقت و منابع مصرفی

۶. ارزیابی مقاومت پروتکل‌های رمزنگاری یکسان‌کلید در برابر حملات مبتنی بر الگوریتم‌های کوانتومی سازگارپذیر

[5] Brute-Force
[6] Groverś Algorithm

قسمت ۳

ضرورت انجام پژوهش

ضرورت انجام پژوهش

این پژوهش با هدف بررسی عملی و نظری این حملات در شرایط واقعی، کمک می‌کند تا پیش از رسیدن رایانه‌های کوانتومی قدرتمند، آمادگی لازم برای حفاظت از زیرساخت‌های امنیتی فراهم گردد.

قسمت ۴

پرسش های پژوهش

پرسش های پژوهش

۱. کدام بهینه‌سازی‌ها در طراحی حدس مسئله، تابع هزینه و نحوه نمونه‌گیری، به افزایش دقت حمله کمک می‌کنند؟
۲. چه تکنیک‌هایی برای کاهش مصرف کیوبیت مؤثر هستند و آیا می‌توان بدون کاهش دقت از کدگذاری غیرمتعامد استفاده کرد؟
۳. چگونه می‌توان این الگوریتم را در چارچوب رایانه‌های کوانتومی اندازه‌میانی پراختلال به‌طور عملی پیاده‌سازی کرد؟

قسمت ۵

روش و فنون پژوهش

1. بررسی مفاهیم پایه رمزنگاری متقارن و مبانی رایانش کوانتومی
2. بررسی الگوریتم‌های کوانتومی سازگارپذیر مانند **الگوریتم تعیین مقدارویژه**[7] و **الگوریتم بهینه‌سازی تقریبی کوانتومی**[8]
3. مدلسازی حمله به‌صورت یک مسئله بهینه‌سازی، تعریف تابع هزینه

[7] Quantum Eigen Solver
[8] Quantum Approximation Optimization Algorithm

بخش پیاده‌سازی

1. پیاده‌سازی الگوریتم حمله در محیط **پنی‌لین**[9]، و در صورت امکان دستگاه واقعی
2. حمله به نسخه‌های ساده‌شده **بلوک‌رمزها**[10] برای تحلیل نتایج اولیه و استخراج زمان‌های همگرایی
3. به‌کارگیری کدگذاری غیرمتعامد و بررسی تأثیر آن در کاهش منابع موردنیاز (تعداد کیوبیت و عمق مدار)

[9] PennyLane
[10] Cipher Blocks

۴ پیاده‌سازی ساختارهای بهینه در فضای پارامترها مانند استفاده از **مختصات ابرکروی**[11] برای افزایش سرعت همگرایی

۵ تحلیل نتایج به‌دست‌آمده و مقایسه با الگوریتم گروور و بی رویه کلاسیک

[11] Hyperspherical Coordinates

قسمت ۶

زمانبدی پیشنهادی

زمانبندی پیشنهادی

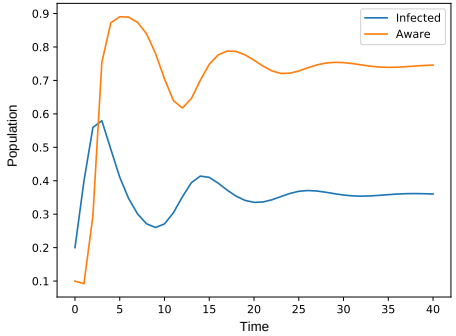
جدول ۱: زمانبندی پیشنهادی برای پژوهش

مرحله	زمان	فعالیت‌ها
اول	ماه اول	مطالعه منابع پایه رمزنگاری و الگوریتم‌های کوانتومی
دوم	ماه اول و دوم	مدل‌سازی الگوریتم‌ها به‌صورت مسئله بهینه‌سازی
سوم	ماه سوم	پیاده‌سازی حمله روی نسخه‌های ساده شده
چهارم	ماه سوم و چهارم	پیاده‌سازی حمله روی نسخه اصلی
پنجم	ماه پنجم	تحلیل نتایج و نگارش مقاله

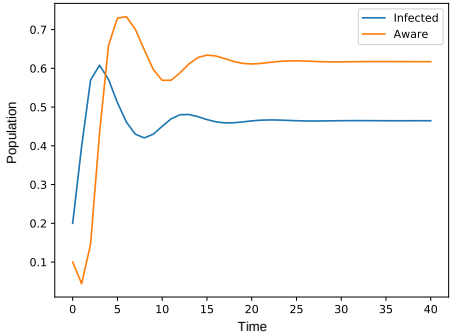
قسمت ۷

پیشینه پژوهش

پیشینه پژوهش



(آ) یادگیری=۰.۷۵ و فراموشی=۰.۵



(ب) یادگیری=۰.۵ و فراموشی ۰.۷۵

شکل ۱: نتیجهٔ اجرای شبیه‌سازی آماری در دو حالت

قسمت ۸

منابع و مراجع