

شکستن پروتکل‌های رمزنگاری با استفاده از حملات کوانتومی سازگارپذیر پیشرفته

محمدعلی خواجه‌نیا

استاد راهنما: زهرا شاطرزاده‌یزدی
دانشکده علوم مهندسی / دانشگاه تهران

۲۸ اردیبهشت ۱۴۰۴



فهرست

- ۱ تعریف مسئله
- ۲ اهداف
- ۳ ضرورت انجام پژوهش
- ۴ پرسش های پژوهش
- ۵ روش و فنون پژوهش
 - بخش تئوری
 - بخش پیاده سازی
- ۶ زمانبندی پیشنهادی
- ۷ پیشینه پژوهش
- ۸ منابع و مراجع

۱ تعریف مسئله

۴ پرسش های پژوهش

۲ اهداف

۵ روش و فنون پژوهش

۳ ضرورت انجام پژوهش

۶ زمانبندی پیشنهادی

۷ پیشینه پژوهش

۸ منابع و مراجع

قسمت ۱

تعریف مسئله

تعریف مسئله

الگوریتم های کوانتومی سازگارپذیر^۱ که از ترکیب پردازش کلاسیک و کوانتومی استفاده می کنند، گزینه ای مناسب برای رایانه های کوانتومی اندازه میانی پراختلال^۲ هستند. این پژوهش کارایی الگوریتم های کوانتومی سازگارپذیر را در شکستن رمزنگاری یکسان کلید^۳ و بهینه سازی این حمله ها بررسی می کند. [۱]

¹Variational Quantum Algorithms

²Noisy Intermediate Scale Quantum Device

³Symmetric-Key Cryptography

قسمت ۲

اهداف

اهداف پژوهش

اهداف اصلی این پروژه به شرح زیر هستند:

- ۱ طراحی و پیاده سازی نسخه های بهینه شده از الگوریتم های کوانتومی سازگارپذیر جهت کاهش زمان اجرا و افزایش دقت
- ۲ کاهش تعداد کیوبیت های مورد نیاز از طریق به کارگیری کدگذاری غیرمتعامد^۴
- ۳ ارائه الگوریتمی کارا برای استفاده روی پلتفرم های رایانه های کوانتومی اندازه میانی پراختلال با قابلیت حمل به دستگاه های کوانتومی پیشرفته تر در آینده

⁴Non-Orthogonal Encoding

اهداف پژوهش

اهداف اصلی این پروژه به شرح زیر هستند:

- ۴ ارائه الگوریتمی کارا برای استفاده روی پلتفرم های رایانه های کوانتومی اندازه میانی پراختلال با قابلیت حمل به دستگاه های کوانتومی پیشرفته تر در آینده
- ۵ مقایسه عملکرد الگوریتم طراحی شده با الگوریتم های بی رویه^۵ کلاسیک و الگوریتم گروور^۶ از نظر سرعت، دقت و منابع مصرفی
- ۶ ارزیابی مقاومت پروتکل های رمزنگاری یکسان کلید در برابر حملات مبتنی بر الگوریتم های کوانتومی سازگارپذیر

^۵Brute-Force

^۶Grover's Algorithm

قسمت ۳

ضرورت انجام پژوهش

ضرورت انجام پژوهش

این پژوهش با هدف بررسی عملی و نظری این حملات در شرایط واقعی، کمک می کند تا پیش از رسیدن رایانه های کوانتومی قدرتمند، آمادگی لازم برای حفاظت از زیرساخت های امنیتی فراهم گردد.

قسمت ۴

پرسش های پژوهش

پرسش های پژوهش

- ۱ کدام بهینه سازی ها در طراحی حدس مسئله، تابع هزینه و نحوه نمونه گیری، به افزایش دقت حمله کمک می کنند؟
- ۲ چه تکنیک هایی برای کاهش مصرف کیوبیت مؤثر هستند و آیا می توان بدون کاهش دقت از کدگذاری غیرمتعامد استفاده کرد؟
- ۳ چگونه می توان این الگوریتم را در چارچوب رایانه های کوانتومی اندازه میانی پراختلال به طور عملی پیاده سازی کرد؟

قسمت ۵

روش و فنون پژوهش

- ۱ بررسی مفاهیم پایه رمزنگاری متقارن و مبانی رایانش کوانتومی
- ۲ بررسی الگوریتم های کوانتومی سازگارپذیر مانند الگوریتم تعیین مقدارویژه^۷ و الگوریتم بهینه سازی تقریبی کوانتومی^۸
- ۳ مدلسازی حمله به صورت یک مسئله بهینه سازی، تعریف تابع هزینه

⁷Quantum Eigen Solver

⁸Quantum Approximation Optimization Algorithm

بخش پیاده سازی

- ۱ پیاده سازی الگوریتم حمله در محیط پنی لین^۹، و در صورت امکان دستگاه واقعی
- ۲ حمله به نسخه های ساده شده بلوک رمزها^{۱۰} برای تحلیل نتایج اولیه و استخراج زمان های همگرایی
- ۳ به کارگیری کدگذاری غیرمتعامد و بررسی تأثیر آن در کاهش منابع موردنیاز (تعداد کیوبیت و عمق مدار)

⁹PennyLane¹⁰Cipher Blocks

- ۴ پیاده سازی ساختارهای بهینه در فضای پارامترها مانند استفاده از **مختصات ابرکروی^{۱۱}** برای افزایش سرعت همگرایی
- ۵ تحلیل نتایج به دست آمده و مقایسه با الگوریتم گروور و بی رویه کلاسیک

¹¹Hyperspherical Coordinates

قسمت ۶

زمانبندی پیشنهادی

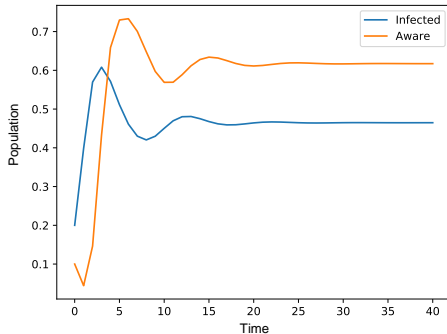
زمانبندی پیشنهادی

جدول ۱: زمانبندی پیشنهادی برای پژوهش

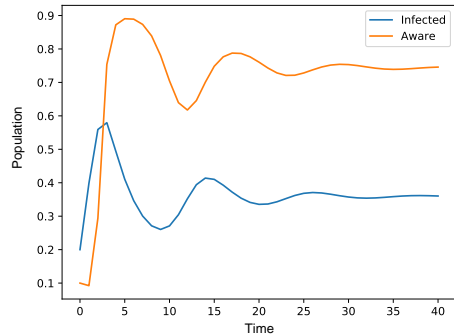
مرحله	زمان	فعالیت ها
اول	ماه اول	مطالعه منابع پایه رمزنگاری و الگوریتم های کوانتومی
دوم	ماه اول و دوم	مدل سازی الگوریتم ها به صورت مسئله بهینه سازی
سوم	ماه سوم	پیاده سازی حمله روی نسخه های ساده شده
چهارم	ماه سوم و چهارم	پیاده سازی حمله روی نسخه اصلی
پنجم	ماه پنجم	تحلیل نتایج و نگارش مقاله

قسمت ۷

پیشینه پژوهش



(ب) یادگیری=0.5 و فراموشی=0.75



(آ) یادگیری=0.75 و فراموشی=0.5

شکل ۱: نتیجه اجرای شبیه سازی آماری در دو حالت

قسمت ۸

منابع و مراجع

- [1] Zhang, J., Liu, W., Zheng, S., and et al.
Variational quantum attacks threaten advanced encryption standard based symmetric cryptography.
Science China, 2022.