

شکستن پروتکل‌های رمزنگاری با استفاده از حملات کوانتومی سازگارپذیر پیشرفته

محمدعلی خواجه‌ئیان

استاد راهنما: زهرا شاطرزاده‌یزدی
دانشکده‌های فنی / دانشگاه تهران

۱۰ خرداد ۱۴۰۴



فهرست

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

فهرست

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

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، ۲، ۳]

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 [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 [۵، ۶]
- 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

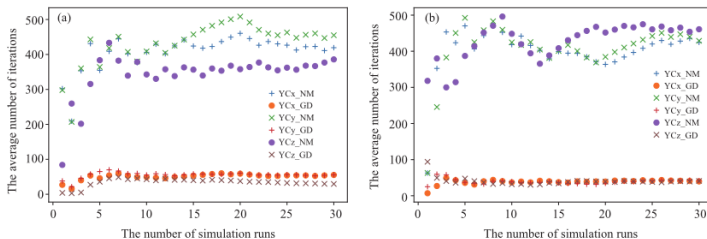
پرسش های پژوهش

- 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

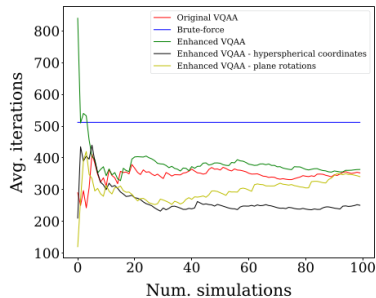
پیشینه پژوهش

► در [۸] از الگوریتم گروور برای جستجوی کلید در بلوک رمز استفاده می‌کند. نویسندگان یک سیستم کوانتومی با حداقل تعداد کیوبیت‌ها (۱۹ کیوبیت) طراحی کردند که می‌تواند کلید بلوک رمز را تنها با یک جفت متن اصلی و متن رمز شده پیدا کند.



شکل ۱: نمودار میانگین تعداد تکرار نسبت به تعداد اجرای شبیه‌سازی

▶ در [۱] یک روش کوانتومی متغیر برای حمله به رمزهای متقارن مبتنی بر بلوک رمز یکسان کلید ارائه می دهد. آن ها نشان دادند که این روش می تواند در برخی موارد حتی از الگوریتم گروور سریع تر عمل کند و کلید را با موفقیت بازیابی نماید.



شکل ۲: نمودار میانگین تعداد تکرار نسبت به تعداد اجرای شبیه سازی

قسمت ۶

روش و فنون پژوهش

- ۱ بررسی مفاهیم پایه رمزنگاری متقارن و مبانی رایانش کوانتومی [۳، ۶]
- ۲ بررسی الگوریتم های کوانتومی سازگارپذیر مانند الگوریتم تعیین مقدارویژه^۷ و الگوریتم بهینه سازی تقریبی کوانتومی^۸ [۲]
- ۳ مدلسازی حمله به صورت یک مسئله بهینه سازی، تعریف تابع هزینه

⁷Quantum Eigen Solver

⁸Quantum Approximation Optimization Algorithm

- ❶ پیاده سازی الگوریتم حمله در محیط پنی لین^۹، و در صورت امکان دستگاه واقعی
- ❷ حمله به نسخه های ساده شده بلوک رمزها^{۱۰} برای تحلیل نتایج اولیه و استخراج زمان های همگرایی [۶]
- ❸ به کارگیری کدگذاری غیرمتعامد و بررسی تأثیر آن در کاهش منابع موردنیاز (تعداد کیوبیت و عمق مدار)

⁹PennyLane

¹⁰Cipher Blocks

- ۴ پیاده سازی ساختارهای بهینه در فضای پارامترها مانند استفاده از **مختصات ابرکروی^{۱۱}** برای افزایش سرعت همگرایی [۷]
- ۵ تحلیل نتایج به دست آمده و مقایسه با الگوریتم گروور و بی رویه کلاسیک

¹¹Hyperspherical Coordinates

قسمت ۷

زمانبندی پیشنهادی

جدول ۱: زمانبندی پیشنهادی برای پژوهش

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

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.
- [2] Cerezo, M., Arrasmith, A., and et al.
Variational quantum algorithms.
Nature Reviews Physics, 2021.
- [3] Nielsen, M. A. and Chuang, I. L.
Quantum Computation and Quantum Information.
Cambridge University Press, 2010.
- [4] García-Bermejo, P. and Orús, Román.
Variational quantum non-orthogonal optimization.
Scientific Reports, 13(1), Jun 2023.
- [5] Grover, Lov K.
A fast quantum mechanical algorithm for database search.
in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, STOC '96, pp. 212–219,
Philadelphia, Pennsylvania, USA, 07-01 1996. Association for Computing Machinery.
- [6] Hoffstein, Jeffrey, Pipher, Jill, and Silverman, Joseph H.
An Introduction to Mathematical Cryptography.
Springer-Verlag New York Inc, Erscheinungsort Nicht Ermittlbar, 2014.

- [7] Bermejo, P., Aizpurua, Borja, and Orús, Román.
Improving gradient methods via coordinate transformations: Applications to quantum machine learning.
Physical Review Research, 6(2), Apr 2024.
- [8] Denisenko, D. V. and Nikitenkova, M. V.
Application of grover's quantum algorithm for SDES key searching.
Journal of Experimental and Theoretical Physics, 128(1):25–44, Jan 2019.