# شکستن پروتکل‌های رمزنگاری با استفاده از حملات کوانتومی سازگارپذیر پیشرفته

محمدعلی خواجه‌ئیان

استاد راهنما: زهرا شاطرزاده‌یزدی
دانشکدگان فنی / دانشگاه تهران

۱۰ خرداد 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. [۱، ۲، ۳]

[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] [۴]
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 [۵، ۶]

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

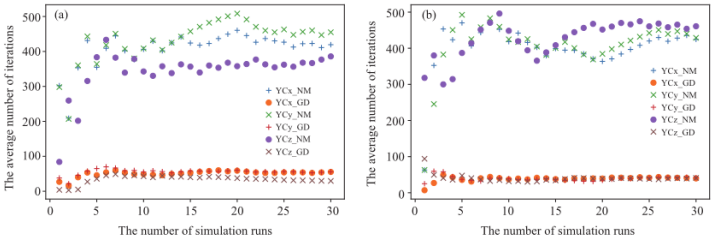
۱. کدام بهینه‌سازی‌ها در طراحی حدس مسئله، تابع هزینه و نحوه نمونه‌گیری، به افزایش دقت حمله کمک می‌کنند؟
۲. چه تکنیک‌هایی برای کاهش مصرف کیوبیت مؤثر هستند و آیا می‌توان بدون کاهش دقت از کدگذاری غیرمتعامد استفاده کرد؟
۳. چگونه می‌توان این الگوریتم را در چارچوب رایانه‌های کوانتومی اندازه‌میانی پراختلال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

قسمت ۵

# پیشینه پژوهش

## پیشینه پژوهش

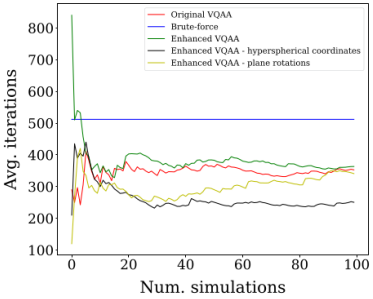
- در [۸] از الگوریتم گروور برای جستجوی کلید در بلوک‌رمز استفاده می‌کند. نویسندگان یک سیستم کوانتومی با حداقل تعداد کیوبیت‌ها (۱۹ کیوبیت) طراحی کردند که می‌تواند کلید بلوک‌رمز را تنها با یک جفت متن اصلی و متن رمز شده پیدا کند.




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

## پیشینه پژوهش

- در [۱] یک روش کوانتومی متغیر برای حمله به رمزهای متقارن مبتنی بر بلوک‌رمز یکسان‌کلید ارائه می‌دهد. آن‌ها نشان دادند که این روش می‌تواند در برخی موارد حتی از الگوریتم گروور سریع‌تر عمل کند و کلید را با موفقیت بازیابی نماید.




شکل ۲: نمودار میانگین تعداد تکرار نسبت به تعداد اجرای شبیه‌سازی

قسمت ۶

# روش و فنون پژوهش

1. بررسی مفاهیم پایه رمزنگاری متقارن و مبانی رایانش کوانتومی [۳، ۶]
2. بررسی الگوریتم‌های کوانتومی سازگارپذیر مانند **الگوریتم تعیین مقدارویژه**[۷] و **الگوریتم بهینه‌سازی تقریبی کوانتومی**[۸] [۲]
3. مدلسازی حمله به‌صورت یک مسئله بهینه‌سازی، تعریف تابع هزینه

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

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 [۶]
3. به‌کارگیری کدگذاری غیرمتعامد و بررسی تأثیر آن در کاهش منابع موردنیاز (تعداد کیوبیت و عمق مدار)

[9] PennyLane
[10] Cipher Blocks

## بخش پیاده‌سازی

۴ پیاده‌سازی ساختارهای بهینه در فضای پارامترها مانند استفاده از **مختصات ابرکروی**[11] برای افزایش سرعت همگرایی [۷]

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

[11] Hyperspherical Coordinates

قسمت ۷

# 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 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 Ermittelbar, 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.