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

۱. پیاده‌سازی الگوریتم حمله در محیط **پنی‌لین**[9]، و در صورت امکان دستگاه واقعی
۲. حمله به نسخه‌های ساده‌شده **بلوک‌رمزها**[10] برای تحلیل نتایج اولیه و استخراج زمان‌های همگرایی
۳. 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

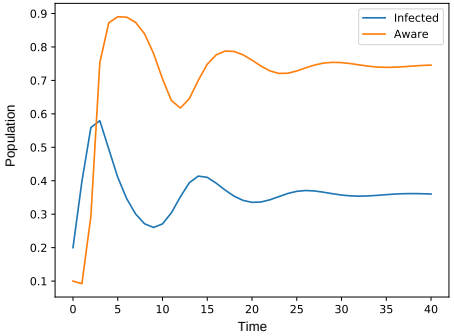
جدول ۱: زمانبندی پیشنهادی برای پژوهش

مرحله	بازه زمانی	شرح کامل فعالیت‌ها
مرحله اول	ماه اول	زنجیره مارکوف
مرحله دوم	ماه اول و دوم	زنجیره مارکوف وضعیت پیوسته
مرحله سوم	ماه سوم	زنجیره مارکوف وضعیت پیوسته
مرحله چهارم	ماه سوم و چهارم	زنجیره مارکوف وضعیت پیوسته
مرحله پنجم	ماه پنجم	زنجیره مارکوف وضعیت پیوسته

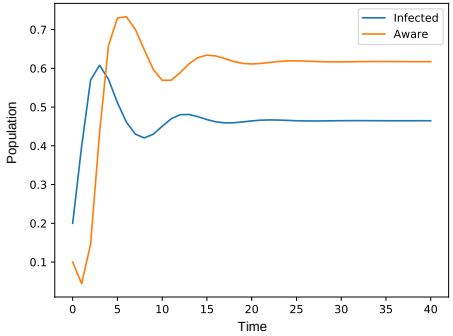
قسمت ۷

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

[1] Chen, Yi-Cheng, Lu, Ping-En, Chang, Cheng-Shang, and Liu, Tzu-Hsuan.
A time-dependent sir model for covid-19 with undetectable infected persons.
IEEE Transactions on Network Science and Engineering, 7(4):3279–3294, 2020.

[2] Wang, Wei, Liu, Quan-Hui, Liang, Junhao, Hu, Yanqing, and Zhou, Tao.
Coevolution spreading in complex networks.
Physics Reports, 820:1–51, 2019.

[3] Estrada, Ernesto.
Covid-19 and sars-cov-2. modeling the present, looking at the future.
Physics Reports, 2020.

[4] Vizuete, Renato, Frasca, Paolo, and Garin, Federica.
Graphon-based sensitivity analysis of sis epidemics.
IEEE Control Systems Letters, 4(3):542–547, 2020.

[5] Khanjanianpak, Mozhgan, Azimi-Tafreshi, Nahid, and Castellano, Claudio.
Competition between vaccination and disease spreading.
Physical Review E, 101(6):062306, 2020.

[6] Efimov, Denis and Ushirobira, Rosane.
On interval prediction of covid-19 development in france based on a seir epidemic model.
in *2020 59th IEEE Conference on Decision and Control (CDC)*, pp. 3883–3888. IEEE, 2020.

[7] Moon, Sifat Afroj, Sahneh, Faryad Darabi, and Scoglio, Caterina.
Group-based general epidemic modeling for spreading processes on networks: Groupgem.
IEEE Transactions on Network Science and Engineering, pp. 1–1, 2020.

[8] Abhishek, Vishal and Srivastava, Vaibhav.
Sis epidemic model under mobility on multi-layer networks.
in *2020 American Control Conference (ACC)*, pp. 3743–3748. IEEE, 2020.

[9] Huang, D. W., Yang, L. X., Li, P., Yang, X., and Tang, Y. Y.
Developing cost-effective rumor-refuting strategy through game-theoretic approach.
IEEE Systems Journal, pp. 1–12, 2020.

[10] Bolzern, P., Colaneri, P., and De Nicolao, G.
Opinion dynamics in social networks: The effect of centralized interaction tuning on emerging behaviors.
IEEE Transactions on Computational Social Systems, 7(2):362–372, 2020.

[11] Nettasinghe, Buddhika, Krishnamurthy, Vikram, and Lerman, Kristina.
Diffusion in social networks: Effects of monophilic contagion, friendship paradox, and reactive networks.
IEEE Transactions on Network Science and Engineering, 7(3):1121–1132, 2019.

[12] Cinelli, Matteo, Quattrociocchi, Walter, Galeazzi, Alessandro, Valensise, Carlo Michele, Brugnoli, Emanuele, Schmidt, Ana Lucia, Zola, Paola, Zollo, Fabiana, and Scala, Antonio.
The covid-19 social media infodemic.
Scientific Reports, 10(1):1–10, 2020.

[13] Li, Zhixun, Hong, Jie, Kim, Jonghyuk, and Yu, Changbin.
Control design and analysis of an epidemic seiv model upon adaptive network.
in *2019 18th European Control Conference (ECC)*, pp. 2492–2497. IEEE, 2019.

[14] Bhowmick, Sourav and Panja, Surajit.
Influence of opinion dynamics to inhibit epidemic spreading over multiplex network.
IEEE Control Systems Letters, 5(4):1327–1332, 2020.

[15] Sahneh, F. D., Vajdi, A., Melander, J., and Scoglio, C. M.
Contact adaption during epidemics: A multilayer network formulation approach.
IEEE Transactions on Network Science and Engineering, 6(1):16–30, 2019.