

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.

¹Variational Quantum Algorithms

²Noisy Intermediate Scale Quantum Device

³Symmetric-Key Cryptography

قسمت ۲

اهداف

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

قسمت ۵

روش و فنون پژوهش

قسمت ۶

زمانبندی پیشنهادی

زمانبندی پیشنهادی

جدول ۱: زمانبندی پیشنهادی برای پژوهش

مرحله	بازه زمانی	شرح کامل فعالیت ها
مرحله اول	فرایند مارکوف	زنجیره مارکوف
مرحله دوم	فرایند مارکوف وضعیت پیوسته	زنجیره مارکوف وضعیت پیوسته

قسمت ۷

پیشینه پژوهش

قسمت ۸

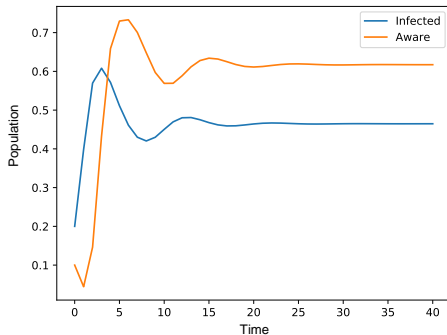
منابع و مراجع

- [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.

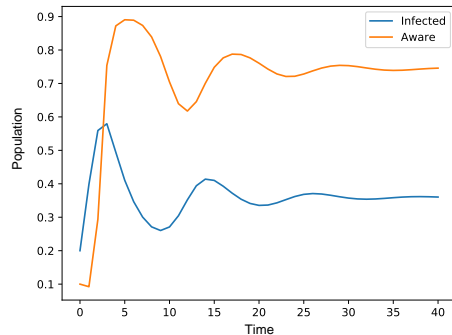
- [7] Moon, Sifat Afroj, Sahneh, Faryad Darabi, and Scoglio, Caterina.
Group-based general epidemic modeling for spreading processes on networks: Groupgem.
IEEE Transactions on Network Science and Engineering, pp. 1–1, 2020.
- [8] Abhishek, Vishal and Srivastava, Vaibhav.
Sis epidemic model under mobility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

نتیاج شبیه سازی آماری



(ب) یادگیری = ۰.۵ و فراموشی = ۰.۷۵



(آ) یادگیری = ۰.۷۵ و فراموشی = ۰.۵

شکل ۱: نتیجه اجرای شبیه سازی آماری در دو حالت