Ho Kiu Gareth Ma

SH44.5 University of Warwick, Gibbet Hill Road, Coventry, CV4 7ES   ✉ Gareth.Ma@warwick.ac.uk

https://grhkm21.github.io   24 Jan 2005

EDUCATION

University of Warwick, Sep 2021 – Jun 2024

Bachelor of Science (with Honours) Mathematics

- Year 1 mark: **85.3**% (High First Class Honours)
- Year 1 optional modules: Discrete Mathematics 2, Programming in Java and Python, Probability A and B
- Year 2 optional modules: French Beginners Accel., Programming for Business Application, Formal Languages

PROJECTS

Personal Blog Oct 2021 – present

- Wrote article on key recovery attack on the CKKS scheme, widely shared in the cryptographic community
- An article on the Hardy-Littlewood Circle method is being written, partial progress found here
- Maintains personal blog using Hugo and Github Pages

Java Snake Game Mar 2021 – Jun 2021

- Recreated the classic Snake game in Java using Swing, and Git for collaboration.

Building Solar Unmanned Boat, *Leader of Software Team* Sep 2019 – Feb 2020

- Created a Python simulation program that models the trajectory of the boat under ocean currents
- Developed Arduino (C) program that controls the angle of rudders based on GPS and environment sensors data
- Reduced video streaming costs by detecting activities using motion sensors and incorporating video compression

ACHIEVEMENTS

Qualified for NWERC (ICPC Regionals), *UKIEPC 2021 & 2022* Nov 2022

- The ICPC is the largest competitive programming competition for colleges around the world
- The NWERC is a round before ICPC for north-western europe teams, where the top teams advance to the ICPC
- Final position: 33 / 141 (2022), 28 / 128 (2021), 1st within Warwick (2021 & 2022)

Junior Division Finalist (Top 20), *CODEGATE CTF* Feb 2022

- International security conference with a 12-hour CTF event for students under 19
- Solved problem on differential cryptanalysis on (modified) 8-round DES
- The finals event is hosted in Seoul in 7th - 8th November

12th Place (Top 0.029%), *CryptoHack*

- Platform with 50,000 registered users focused on exploiting poorly designed/implemented modern cryptography
- Techniques include differential-linear attack, LFSR algebraic attack, MOV attack and padding oracle attacks
- Currently tied first place solving all problems, and 12th when ordered by time spent

EXTRACURRICULAR ACTIVITIES

Black Bauhinia, *Cryptography & Reverse Engineering (CTF)* Apr 2021 – present

- Black Bauhinia is the current best Hong Kong CTF team
- Participated in TJCTF, CryptoCTF, SekaiCTF and more, all of which we came top 10

University of Warwick, *Maths Course Representative* Sep 2021 – present

- Met with department heads to discuss issues raised by students, such as assignments workload and wellbeing
- Wrote extra practice worksheets for modules with overall positive feedback

AI Safety Discussion Group, *Warwick AI Society* Oct 2021 – Dec 2021

- 8 week reading and discussion groups on essays and research about AI Safety
- Topics discussed include misalignment, threat models, training AGI by Iterated Amplification & Distillation, etc.

LANGUAGE

Mandarin (Native) • **Cantonese** (Native) • **English** (IELTS 7.5) • **French** (Beginner)