




# Wenxing Duan

 [github.com/WenxingDuan](https://github.com/WenxingDuan)  [wenxingduan.com](https://wenxingduan.com)  [linkedin.com/in/wenxingduan](https://linkedin.com/in/wenxingduan)  [0x.wenxingduan@gmail.com](mailto:0x.wenxingduan@gmail.com)

## EDUCATION

<b>the University of Edinburgh</b> <i>Master of Science in Cybersecurity, Privacy and Trust</i>	09/2023 - 12/2024 <i>Merit</i>
<b>the University of Edinburgh</b> <i>Bachelor of Science in Computer Science</i>	09/2019 - 06/2023 <i>First Class Honours</i>

## PROFESSIONAL EXPERIENCE

<b>Story Protocol, Inc.</b>   <i>Research Fellow</i>	12/2024 - 04/2025
<ul style="list-style-type: none"><li>Collaborate with engineering leads to identify and address opportunities for improvement across Story's blockchain stack.</li><li>Propose and develop innovative research topics, strategies, and approaches.</li><li>Present findings and thought leadership on the latest blockchain developments through internal talks and external forums.</li><li>Publish in-depth research reports on blockchain technology, cryptography, and decentralized systems.</li><li>Design and implement proof-of-concept projects to validate research findings and explore new opportunities.</li></ul>	
<b>China Telecom Quantum Information Technology Group Co.</b>   <i>Cryptography R&amp;D Intern</i>	09/2024 - 11/2024
<ul style="list-style-type: none"><li>Studied various side-channel attacks, including timing analysis, power analysis, and electromagnetic attacks.</li><li>Utilized the ChipWhisperer platform to perform Differential Power Analysis (DPA) and Correlation Power Analysis (CPA) on chip-based RSA and AES algorithms.</li><li>Replicated implementations of post-quantum cryptographic algorithms CRYSTALS-Dilithium and CRYSTALS-Kyber, and reproduced research on side-channel attacks against these algorithms.</li><li>Gained understanding of common defense techniques against side-channel attacks, including masking and random delay techniques, and developed targeted attack strategies for these defenses.</li><li>Contributed to the establishment of the company's Side-Channel Security Laboratory, completed industry research, and authored project reports.</li></ul>	
<b>Laboratory for Foundations of Computer Science</b>   <i>Junior Research Assistant</i>	06/2023 - 08/2023
<ul style="list-style-type: none"><li>Conducted a comprehensive analysis of quantum computing, building on previous dissertation work. This research focused on examining experimental data from Google's Sycamore 53-qubit quantum computer, aiming to provide deeper insights.</li><li>Identified significant patterns and anomalies in Fourier weight outputs during the initial phase of the research, which highlighted potential discrepancies in large qubit analysis and indicated areas that warranted further exploration.</li><li>In a subsequent study, delved deeper into these anomalies to understand the underlying causes and their implications. The effort involved rigorous data analysis, which led to pivotal observations for the field of quantum computing.</li><li>Further developed analytical methods, refining those used in the initial dissertation. This advanced stage of research aimed to establish relationships between quantum system dynamics and specific parameters, enhancing the depth and applicability of the findings. These results are poised to be published in an upcoming paper.</li></ul>	
<b>Nethermind</b>   <i>Cryptography &amp; Blockchain Research Intern</i>	06/2022 - 09/2022
<ul style="list-style-type: none"><li>Participated in the protocol research of the next phase of the Lido project</li><li>Studied and analysed current mainstream oracle protocols, including DECO, Town Crier, Chainlink, Provable, etc.</li><li>Participated in the research of decentralized identity (Decentralized Identity), and learned and analyzed other feasible solutions for on-chain identity, including CanDID, soulbound token, verifiable credentials, etc.</li><li>Learned the relevant knowledge of zero-knowledge proof and participated in the formulation of the trustless verification framework scheme for the next stage of Lido.</li><li>Wrote a smart contract to measure the performance of ETH2.0 validators using the Provable oracle.</li></ul>	

Language	Percentage
Python	~85%
Solidity	~75%
Java	~70%
Cairo	~65%
C	~45%

## ACADEMIC AWARDS

---

- **Outstanding Undergraduate Thesis** 05/2023  
The University of Edinburgh
- **China Software Cup** | *Second Prize* 09/2021  
Ministry of Industry and Information Technology
- **Canadian Computing Competition** | *Certificate of Distinction* 03/2019  
University of Waterloo
- **Euclid Mathematics Contest** | *Certificate of Distinction* 03/2019  
University of Waterloo
- **Australian Mathematics Competition** | *Certificate of Distinction* 11/2018  
Australian Maths Trust
- **Hypatia Mathematics Contest** | *Certificate of Distinction* 03/2018  
University of Waterloo
- **Galois Mathematics Contest** | *Certificate of Distinction* 03/2017  
University of Waterloo
- **Xiangyang Science and Technology Competition** | *Science and Technology Innovation Practice Award* 09/2016  
Xiangyang Science and Technology Bureau
- **The 17th "China Mobile 'He Education' Cup"** | *Second Prize* 07/2016  
National Center for Educational Technology
- **National Youth Robot Competition** | *Third Prize* 09/2015  
China Association For Science And Technology
- **Xiangyang Youth Science and Technology Festival** | *First Prize* 01/2015  
Xiangyang Association For Science And Technology
- **Hubei Adolescents Science & Technology Innovation Contest** | *First Prize* 06/2014  
Hubei Association For Science And Technology