Wenxing Duan

github.com/WenxingDuan wenxingduan.com linkedin.com/in/wenxingduan 0x.wenxingduan@gmail.com

Education

The Hong Kong Polytechnic University 09/2025 - Present
PhD in Blockchain, Cyber Security and Privacy

the University of Edinburgh 09/2023 - 12/2024
Master of Science in Cybersecurity, Privacy and Trust *Merit*

the University of Edinburgh 09/2019 - 06/2023
Bachelor of Science in Computer Science *First Class Honours*

Professional Experience

The Hong Kong Polytechnic University | *Teaching Assistant* 09/2025 - Present

- Delivered lectures and facilitated weekly tutorials to reinforce core concepts and problem-solving skills.
- Designed assignments and tutorial materials, including problem sets, grading rubrics, and solution outlines.
- Graded assignments and exams, provided detailed written feedback, and ensured consistent assessment standards.
- Held office hours and responded to student questions via in-person and online channels, offering timely academic support.

Story Protocol, Inc. | *Consultant Researcher* 12/2024 - Present

- Collaborate with engineering leads to identify and address opportunities for improvement across Story's blockchain stack.
- Propose and develop innovative research topics, strategies, and approaches.
- Lead the end-to-end cryptography workstream for Confidential Data Rails (CDR), owning protocol-level security design and cryptographic correctness (e.g., DKG/threshold decryption, encryption/authentication primitives, and threat-model-driven mitigations).
- Serve as the primary in-house cryptography researcher and security counterpart for engineering, providing design reviews, security proofs/arguments, and implementation guidance across confidential-computing and key-management components.
- Present findings and thought leadership on the latest blockchain developments through internal talks and external forums.
- Publish in-depth research reports on blockchain technology, cryptography, and decentralized systems.
- Design and implement proof-of-concept projects to validate research findings and explore new opportunities.

China Telecom Quantum Information Technology Group Co. | *Cryptography R&D Intern* 09/2024 - 11/2024

- Studied various side-channel attacks, including timing analysis, power analysis, and electromagnetic attacks.
- Utilized the ChipWhisperer platform to perform Differential Power Analysis (DPA) and Correlation Power Analysis (CPA) on chip-based RSA and AES algorithms.
- Replicated implementations of post-quantum cryptographic algorithms CRYSTALS-Dilithium and CRYSTALS-Kyber, and reproduced research on side-channel attacks against these algorithms.
- Gained understanding of common defense techniques against side-channel attacks, including masking and random delay techniques, and developed targeted attack strategies for these defenses.
- Contributed to the establishment of the company's Side-Channel Security Laboratory, completed industry research, and authored project reports.

Laboratory for Foundations of Computer Science | *Junior Research Assistant* 06/2023 - 08/2023

- 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.
- 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.

- 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.
- 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.

Nethermind | *Cryptography & Blockchain Research Intern* 06/2022 - 09/2022

- Participated in the protocol research of the next phase of the Lido project
- Studied and analysed current mainstream oracle protocols, including DECO, Town Crier, Chainlink, Provable, etc.
- 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.
- 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.
- Wrote a smart contract to measure the performance of ETH2.0 validators using the Provable oracle.
- Improved proficiency in Solidity; grasped the most advanced trustless oracle model in the industry, improved understanding of zero-knowledge proofs, and learn about the latest developments in the field of decentralized identity.

Huazhong University of Science and Technology | *Summer Research Intern* 06/2021 - 09/2021

- Participated in "China Software Cup" as a member of the Huazhong University of Science and Technology team
- Coordinated the 4-person team in the project "Hazardous Agricultural Pest Recognition System", which earned us National Second Prize
- Studied and researched the academic literature on cutting-edge research into fine-grained recognition with Associate Professor Tang He
- Developed an identification system of harmful agricultural pests based on fine-grained identification
- Responsible for back-end development and machine vision development
- Mastered knowledge of back-end development, improved knowledge of database SQLite, grasped the principles and applications of machine vision
- Utilized Python, TensorFlow, PyTorch, Recurrent Attention Convolutional Neural Network, SQLite

Shanghai Zhuofan Technology Co., Ltd. | *Backend Development Intern* 06/2020 - 09/2020

- Participated in the backend service and system maintenance of Xiangyang Municipal Affairs Service Network
- Assisted senior engineers in the development and maintenance of the "Hubei Government Affairs Approval Platform" project
- Assisted in testing a number of new functions including automatic query webpage generation, data transfer.
- Supported senior engineers by processing, analyzing, and cleaning platform data using Python script.
- Participated in testing the database of the Xiangyang government's mobile staff management app "Ehuiban"
- Improved understanding of the production and testing processes of regular software manufacturers an grasped the operating principles of numerous website backgrounds

Research Works

Story Network Confidential Data Rails (CDR) 2025/2 - Present

- This work proposes and formalizes Confidential Data Rails (CDR) for Story: a protocol stack for secure, confidential, and programmable storage and transfer of sensitive data in on-chain workflows. CDR is executed by a decentralized committee of opt-in participants running a dedicated kernel inside Trusted Execution Environments (TEEs), orchestrated by core Story smart contracts, to jointly perform Distributed Key Generation (DKG) and threshold decryption. This design enables conditional decryption and automated delivery without any single party holding the full decryption key. The protocol adopts a client-side encryption model: bulk ciphertext is uploaded to an arbitrary data availability layer, while only the threshold-encrypted data key and on-chain access conditions are committed to CDR, achieving scalability and cost efficiency without relying on privacy guarantees from the storage layer. From a cryptographic engineering perspective, CDR adapts TDH2 by replacing hash+XOR with AES-GCM and binding a unique identifier as AAD to mitigate replay-style attacks. System-wise, it incorporates epoch-based kernel rotation and proactive secret refresh, remote attestation, and staking/slashing incentives to reduce key-share exposure under TEE vulnerabilities, side-channel leakage, and committee collusion, and it discusses mitigations for adversarial-committee and chosen-ciphertext threats. A primary instantiation of CDR is IP Vault, which binds confidential artifacts to on-chain IP assets and supports permissioned, condition-triggered disclosure (e.g., time locks, role/condition-based access, and environment-constrained release) with protocol-enforced automated delivery to license holders.

DECentralized Oracles (DECO): Extensions and Applications 2024/05 - 2024/08

- This is a master's thesis project that I proposed and completed under the supervision of Professor Markulf Kohlweiss, which was recognized as one of the Outstanding Postgraduate Thesis of the year. The thesis focuses on a blockchain oracle protocol based on cryptography, the TLS protocol, and zero-knowledge proofs—Decentralized Oracles (DECO). The project provides a detailed analysis of DECO's operational mechanisms, identifying its shortcomings and potential privacy risks. In response to these privacy concerns, and without altering the server-side TLS protocol, this paper profoundly modifies the DECO protocol based on a deep understanding of AES, HMAC, Merkle trees, and TLS, integrating zero-knowledge proof technology to achieve enhanced privacy performance. The project elucidates the operational principles and processes of these methods. It offers an extensive comparison and analysis of the advantages and disadvantages of each method and demonstrates their effectiveness through code verification. Additionally, the paper formally defines the security attributes of the enhanced protocol and provides a cryptographic proof of its privacy.

Testing the assumptions of recent quantum supremacy experiments 2022/09 - 2023/05

- This is an undergraduate thesis project that was recognized as one of the Outstanding Undergraduate Thesis of the year. In my thesis, I primarily focused on analyzing Google's quantum random circuit sampling experiment to evaluate their claims of quantum supremacy. I employed Fourier analysis to study the relationship between the experimental outcomes and the number of qubits, thus comprehensively assessing the strength of Google's quantum supremacy claim. During the research, I encountered an interesting phenomenon. Contrary to expectations, my experimental results demonstrated that the correlator values from Google's experiment were higher than those of a theoretical noise-free ideal circuit. This discrepancy led me to conduct extensive data analysis to determine the underlying reasons, which I ultimately attributed to an insufficient number of samples. Furthermore, it was discovered that the noise levels in the system significantly affected the results for different sample sizes. Therefore, determining the optimal sample size needed to achieve correlator values close to the true values has become an important research question worthy of further investigation.

Skills

Professional Skills: Python, Solidity, C, Java, Cairo, SNARK/STARK, Chainlink, Provable, Flask, Springboot, LaTeX, Haskell
Languages: English, Chinese
Interests: Cryptography, Blockchain, ZKP, Ethereum/EVM, Quantum Computing, Deep Learning, NLP, AIGC, Archery

Academic Awards

- **Hong Kong PhD Fellowship Scheme (HKPFS)** 04/2025
  Hong Kong Research Grants Council (RGC)
- **Research Excellence Scholarship** 03/2025
  The Hong Kong Polytechnic University
- **Outstanding Postgraduate Thesis** 10/2024
  The University of Edinburgh
- **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