QIYUAN XU

(+65) 8044 9201 ⋄ xu@qiyuan.me ⋄ qiyuan.xu@ntu.edu.sg

EDUCATION

Zhejiang U. Chu Kochen Honors College B.E. in Computer Science *Sep.2013 - Jun.2017*
Zhejiang U. Master in Cyber Security *Sep.2017 - Jun.2020*
Nanyang Technological U. PhD candidate, supervised by Conrad Watt *Aug.2022 - Now*

Awards
Second-Class Scholarship for Elite Students in Basic Science, Zhejiang U.
Scholarship for Excellence in Research and Innovation, Zhejiang U.
Academic Scholarship, Zhejiang U.

PUBLICATION

- Generically Automating Separation Logic by Functors, Homomorphisms and Modules.
  Qiyuan Xu, David Sanan, Zhe Hou, Xiaokun Luan, Conrad Watt, Yang Liu.
  POPL'25, CORE ranking **A***, CCF ranking **A**
- Why the Proof Fails in Different Versions of Theorem Provers: An Empirical Study of Compatibility Issues in Isabelle. Xiaokun Luan, David Sanan, Hou Zhe, **Qiyuan Xu**, Chengwei Liu, Yufan Cai, Yang Liu and Meng Sun. Accepted by FSE'25, CORE ranking **A***, CCF ranking **A**

REMARKABLE EVENT

As a key member in the team, established a new **world record** on 3KW Linpack testing, during the ASC Student Supercomputer Challenge 2016 [1].

COMPETITION HONORS

ASC15 (ASC Student Supercomputer Challenge 2015) First Prize
ASC16 First Class Award ASC16 Highest LINPACK

PATENTS

- coinventor, CN109753288A, *Intelligent contract compiling method suitable for formal verification*
- coinventor, CN109918375A, *Large text storage, indexing and retrieval method based on block chain and distributed storage*
- coinventor, CN111679809A, *Noesis logic-based program development and verification method and system*
- coinventor, CN111562906A, *Smart contract development and verification method based on Noesia logic*
- coinventor, CN111311255A, *Intelligent contract formal verification and error correction method based on oracle machine*

ENGINEERING & RESEARCH EXPERIENCE

Research Associate & PhD student in **Nanyang Technology University** *2022 - now.*
Supervisor: Conrad Watt, assistant professor, NTU, conrad.watt@ntu.edu.sg

Project: *Phi-System*, a certified programming language & program verification framework built on top of Isabelle/HOL. It is based on a first-order fictional separation logic, equipped with an algebra-based generic automation mechanism and a symbolic execution engine for assisting certified programming. The system supports verifying a quasi C language and an LLVM subset.

[1] This is reported by an official media https://www.zju.edu.cn/english/2016/0505/c19573a811355/page.htm

Senior engineer in **Hangzhou Yunphant Network Technology Co.,Ltd** *2020 - 2022.*
Director: Dr. Butian Huang, founder & CEO, Yunphant Co.,Ltd, hr@yunphant.com

Project 1: *Prototype Phi-System*, a verification system aiming for generating certified smart contracts

- Formulated the operational semantics of LLVM on the HOL4 interactive theorem prover and Isabelle/HOL prover.
- Proposed and implemented a refinement calculus, *ν-type*, to reduce the complication during the development on this LLVM semantics.
- Designed and implemented the code extractor with extremely tiny trust base, generating LLVM-IR suitable for resource limited situations including embedded smart contract platform.

Project 2: Blockchain-based Manufacturing Service Supply and Demand Matching Platform ‖ Group member.
Key R&D Program of Zhejiang Province, No. 2021C01116
Advisor: Dr. Zhenguang Liu, Zhejiang U.

- Audited key smart contracts, and found several deficiencies including a critical re-entry vulnerability resulting in stealing of total assets potentially.

Graduate student in **the lab of Very Large Information System, Zhejiang U.** *2017-2020*
Advisor: Dr. Liang Cai, Vice Dean of the Software College, Zhejiang U., leoncai@zju.edu.cn.
Project: GPU based implementation of SM2 cyptographic algorithm.

- Implemented finite group operations of elliptical curves on the CUDA device, with hotpot written in manually optimized PTX assemble code.
- The work has been applied in the industrial product of Hyperchain (a blockchain platform raised in this laboratory), and its productive distribution for the Shanghai Stock Exchange.

Key member in **Supercomupting Team of Zhejiang University** *2014 - 2017.*
Advisor: Associate Prof. Jianhai Chen, Zhejiang U., chenjh919@zju.edu.cn.
Project 1: Parallel optimization – MASNUM (marine science and numerical modeling) ‖ Project Leader

- Implemented the first GPU-accelerated version of the MASNUM software, during the ASC16. The optimized software reached the theoretical performance peak of the GPU device, Nvidia Tesla K40.
- The final benchmark of the optimization in the ASC16 competition exceeded that of the opponents by more than 10 times.

Project 2: SKA (Square Kilometer Array telescope) data processing application Gridding ‖ Project Leader

- Implemented a CPU-based cluster-scale parallel version of the hotpot of the SKA-Gridding, which is a 2-dim convolution, based on the MPI and OpenMP, specified for Intel Many Integrated Core.

CONTRIBUTION TO SOFTWARE COMMUNITIES

- Isabelle REPL, a basic infrastructure for AI-based theorem proving, allowing machine learning systems to connect the Isabelle theorem prover. https://github.com/xqyww123/Isa-REPL.
- Isabelle Proof Shell, a minimal proof abstraction layer integrating the full power of Isabelle's automation, designed for machine learning. https://github.com/xqyww123/Isa-Proof-Shell.
- Verification for Uniswap v3, a partial verification for the core functions of the famous smart contract Uniswap v3. https://github.com/xqyww123/Uniswap_v.
- I am also a contributor of the Crystal programming language (https://github.com/crystal-lang/crystal)