

Haofan Zheng

hzheng6@ucsc.edu

<https://haofan.me/>

<https://github.com/zhenghaven>

Education

Doctoral Program in Computer Science

09/2017 - 12/2024 (*Anticipated*)

University of California, Santa Cruz

Research Area: Trusted Computing

Research Thesis: Decent Framework

A distributed application framework using **secure enclaves**, a type of **Trusted Execution Environment (TEE)**.

Decent enables **decentralized** mutual attestation between enclaves, allowing microservice orchestration among a large number of components.

By integrating Decent with **blockchain** and **smart contracts**, Decent can provide highly available **Pub-Sub** system for data dissemination among components.

Meanwhile, **Service Level Agreement (SLA)** enforced by the smart contract adds the **availability** guarantee to enclave applications.

Bachelor of Science in Computer Science, *summa cum laude*

08/2013 - 05/2017

West Virginia University

GPA: 3.95

Honors

Ralph M. Barnes Senior Scholastic Achievement Award

For full-time students who graduated with the highest GPA during the junior and senior years
Benjamin M. Statler College, West Virginia University, Morgantown, 2017 Spring

President's List, West Virginia University

For students who enrolled 12 units of ABC grading courses and obtained a 4.0 GPA
Morgantown, 2014 Spring (~7.9%), 2014 Fall (~7.9%), 2015 Spring (~8.2%), 2015 Fall (~8.5%), 2016 Spring (~8.2%)

Blue & Gold Level 2 Scholarship

West Virginia University, Morgantown, 2013 - 2017

Publication

Payment Channels Under Network Congestion

ICBC'22, 05/2022

Tuan Tran, **Haofan Zheng**, Peter Alvaro, Owen Arden

A novel construction of payment channels that mitigate execution fork attack under network congestion
<https://doi.org/10.1109/ICBC54727.2022.9805547>

Secure Distributed Applications the Decent Way

ASSS'21, 06/2021

Haofan Zheng, Owen Arden

A framework for building secure decentralized applications with trusted execution environments and remote attestation
<https://doi.org/10.1145/3457340.3458304>

Total Eclipse of the Enclave: Detecting Eclipse Attacks from Inside TEEs

ICBC'21, 05/2021

Haofan Zheng, Tuan Tran, Owen Arden

Using difficulty monitoring to reliably detect extended eclipse attacks, even when the adversary controls all network connectivity
<https://doi.org/10.1109/ICBC51069.2021.9461081>

Experience - Industry

Facebook

PhD Software Engineer Intern

06/2021 - 09/2021

Implemented Intel Multi-package DCAP support for Facebook's **foundational** remote attestation (RA) framework, used by all Intel SGX applications at Facebook
Implemented AMD SEV RA protocol ensuring the genuineness of applications running on AMD SEV virtual machines
Integrated AMD SEV RA into Facebook's **foundational RA infrastructure**, enabling AMD SEV support for the existing RA framework
Implemented an **automated** process to build virtual machine **images for AMD SEV**, allowing **quick deployment** of applications on AMD SEV

ByteDance

PhD Software Engineer Intern

06/2020 - 09/2020

Researched and Analyzed the characteristics of **AMD SEV** and **Intel SGX**
Evaluated the **security guarantees** offered by AMD SEV RA in terms of confidentiality and integrity
Realized and demonstrated AMD SEV Remote Attestation (RA) protocol
Reported **precautions** and **potential vulnerabilities** in the current version of AMD SEV softwares
Revised **OVMF**, **QEMU**, and **linux kernel** to achieve a secure RA protocol

IstoVisio, Inc. (syGlass)

Software Engineer

05/2015 - 05/2017

syGlass is a 3D Virtual Reality **Scientific Visualization System**, and it was presented at the 2016 Society for Neuroscience
Led the development of the early version of syGlass on **Unreal Engine**
Experienced programming in **C\C++** with OpenGL, GLFW, GLM, OpenVR, Boost, curl, and more
Integrated CMU Sphinx **voice recognition** and **VR headsets**

Experience - Academia

Languages, Systems, and Data Lab, University of California, Santa Cruz

Graduate Student Researcher

09/2017 - present

Advisor: Professor Owen Arden
Implemented enclave applications using Intel SGX in **C\C++**
Implemented smart contracts in **Solidity**
Analyzed the performance of components of Decent framework in **Python**
Implemented dynamic typing system in C++ header-only library with zero 3rd party dependency
Implemented parsers for **JSON** and **RLP** in C++ header-only library with zero 3rd party dependency

University of California, Santa Cruz

Teaching Assistant, CSE 16 Applied Discrete Mathematics

01/2024 - 03/2024

Instructor: Professor Owen Arden
Discrete mathematics including propositional logic, predicate logic, etc.

Teaching Assistant, CSE 114A Foundations of Programming Languages

09/2023 - 12/2023

Instructor: Professor Owen Arden
Programming language theory including **lambda calculus**, **type system**, etc.
Programming in **Haskell**, a functional programming language

Teaching Assistant, CSE 30 Programming Abstractions Python

01/2023 - 03/2023

Instructor: Professor Kishore Pusukuri
Advanced programming techniques in **Python**
Data analysis and visualization using **pandas** and **matplotlib**
Graph algorithms including DAG, topological sort, etc.

Teaching Assistant, CSE 30 Programming Abstractions Python

04/2022 - 06/2022

Instructor: Professor Larissa Munishkina
Data processing using **numpy** and **pandas**

Teaching Assistant, CSE 111 Advanced Programming

04/2021 - 06/2021

Instructor: Professor Wesley Mackey
C++ Programming for **C** programmers
Graph algorithms including **Dijkstra's algorithm**, **Red-black tree**, etc.

Teaching Assistant, CMPS 109 Advanced Programming

09/2017 - 12/2017

Instructor: Professor Ira Pohl
Graph algorithms including **Minimax**, **Alpha-Beta**, **Monte Carlo**, etc.

Paper Review

5th International Congress on Blockchain and Applications
BLOCKCHAIN'23; Conference

05/2023

3rd International Symposium on Advanced Security on Software and Systems
ASSS'23; Conference

04/2023

4th International Congress on Blockchain and Applications
BLOCKCHAIN'22; Conference

05/2022

IEEE Transactions on Dependable and Secure Computing
TDSC; Journal

09/2021

Skill

Chinese (Native), English (Fluent)

C, C++, Python, Solidity, Haskell, Java, \LaTeX , SQL, HTML, PHP, CSS