NAN CHENG

Phd Student

nan.cheng@unisg.ch (+41) 0795576571 St. Gallen, Switzerland https://nancheng.me
https://github.com/nann-cheng

WORK EXPERIENCE

Game Client Engineer

Shanghai Joywhale Technology Co., Ltd.

March 2014 – November 2015 Shanghai, China

Full development of a 2D Side-Scrolling Strategic Fighting Mobile Game. (C++, Lua, Java)

Software Engineer

Shanghai Bloks Technology Group Co., Ltd.

December 2015 – May 2017 Shanghai, China

Full development of a Motion-Sensing Mobile Game, foundational back-end infrastructure development. (C++, Unity3D, Lua, D, Object-c)

Technical Manager

Shanghai Votance Intelligent Technology Co., Ltd.

December 2017 – July 2018 Shanghai, China

Team management & technical solution implementation for an unattended vending machine product, encompassing software and hardware development, as well as core AI algorithm creation.

EDUCATION

Doctoral Researcher — University of St. Gallen

St. Gallen, Switzerland October 2021 – June 2025 (expected)

Cryptography, M.S.E — Fudan University

Shanghai, China September 2018 – July 2021

Computer Science, B.E. — Jiangxi Agricultural University

Nanchang, China September 2008 – July 2012

ACADEMIC ENRICHMENT

Summer School on PPML — Technical University of Denmark

Copenhagen, Denmark Aug.01 – Aug.04 2022

Summer School on Privacy-Preserving Cryptography — CISPA

Saarbrücken, Germany Jul.29 – Jul.31 2024

Visiting Research on PCG and HSS — Aarhus University

Aarhus, Denmark Oct.01 – Nov.30 2024

TEACHING/TUTORING

TA, Discrete Mathematics

Fudan University

Sep 2019 – Jan 2020

TA, Cyber Security and Cryptography

University of St. Gallen

Sep 2021 – Jan 2025

Co-supervision on a Master thesis: "Practical Secure Inference via Function Secret Sharing"

University of St. Gallen

March 2023 – June 2024

SKILLS

C++ Rust Python Lua Java
Cryptographic Engineering
Software Development

PUBLICATIONS

- Efficient Three-party Boolean to Arithmetic Share Conversion [PST 2023] (Link)
- Constant-Round Private Decision Tree Evaluation for Secret Shared Data [*PoPETS 2024, CORE Rank A*] (Link)
- Nomadic: Normalising Maliciously-Secure Distance with Cosine Similarity for Two-Party Biometric Authentication [*AsiaCCS 2024, CORE Rank A*] (Link)
- Efficient Two-Party Secure Aggregation via Incremental Distributed Point Function [*Euro S&P 2024, CORE Rank A*] (Link)
- A post-quantum Distributed OPRF from the Legendre PRF (ePrint)

RESEARCH INTERESTS

Privacy-Enhancing Technologies
Privacy-Preserving Cryptography
Zero Knowledge Proof System
Provable Security