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)

Game Client Engineer

Shanghai Putao Technology Co., Ltd

December 2015 – May 2017 Shanghai, China

- Full development of a Motion-Sensing Mobile Game, as well as partial of back-end technical support. (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.

PUBLICATIONS

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

PREPRINT

- (ePrint) A post-quantum Distributed OPRF from the Legendre PRF

RESEARCH INTERESTS

- Privacy-preserving Technology
- Zero knowledge proof System
- Optimization of cryptographic engineering

EDUCATION

Doctoral student

University of St. Gallen

St. Gallen, Switzerland

October 2021 – September 2025 (expected)

Software Engineering, M.S.E

Fudan University Shanghai, China

September 2018 – July 2021

Computer science and technology, B.E.

Jiangxi Agricultural University

NanChang, China

September 2008 – July 2012

VISITING RESEARCH

Visiting research at Aarhus Crypto Group

Aarhus University Aarhus, Denmark

Oct.01 – Nov.30 2024

TEACHING

TA in Cyber security and Cryptography

University of St. Gallen

St. Gallen, Switzerland

Sep – Feb 2022-2024

SUPERVISION

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

University of St. Gallen

St. Gallen, Switzerland

March 2023 – June 2024

SKILLS

C++ Python Lua Rust Java