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

Dear Sir/Madam,

I am a Ph.D. student at HSG, supervised by Prof. Katerina Mitrokotsa, and I expect to graduate this coming June. I am writing to express my interest in working at Ompex. With over six years of experience in applied cryptography research and a robust background in software engineering, I am confident that my academic training and technical skills make me well-suited to contribute effectively to the team at Ompex.

I have authored several top publications in applied cryptography conferences. In these works, I developed efficient multiparty computation (MPC) protocols with provable security guarantees, targeting specific circuits and reducing the communication complexity of the corresponding protocols through innovative techniques and optimizations. With the exception of my publication at PoPETS, I led both the design and implementation of all other protocols, utilizing programming languages such as Python, C/C++, and Rust. Beyond my primary focus, I have a broad interest and skill set in other areas as well. I have systematically followed developments in zero-knowledge proofs (ZKPs). Motivated to construct private cryptographic primitives, I attended the Privacy-Preserving Applied Cryptography Summer School organized by CISPA, which concentrated on anonymous credentials. This experience provided me with a fundamental understanding of blind signatures, including their development, various variants, underlying cryptographic assumptions, potential attacks, and their relationship with ZKPs. Cryptographic primitives are not standalone entities; rather, they exhibit intricate relationships and dependencies. Concepts from one area can often be applied across the broader cryptographic landscape. Similarly, I believe my experience in applied cryptography research, coupled with my commitment to seeking innovative ideas and solving complex problems, will be an invaluable asset in any future role. Given the urgent need for data protection in smart grids, I hope my background of data security could foster useful ideas for the development of Ompex.

My diverse experience in software engineering has equipped me with a wide range of skills, including proficiency in programming languages such as C/C++, Python, and Rust. This background has also instilled disciplined programming habits, such as clear module design prior to coding, effective class and function abstraction, robust coding practices, and scalable interface design for future use. Furthermore, these experiences have enhanced my patience in tackling challenging problems and provided me with a clearer approach to navigating complex systems, along with the ability to adapt quickly to effective teamwork.

Over these years of teaching and research, I have particularly enjoyed interacting with students and preparing slides for seminars, whether discussing my own work or presenting other researchers' work. I take pride in my ability to simplify complex cryptographic concepts through clear explanations and engaging illustrations, to make a deeper understanding among my audience. Thus, I believe these experience would make me a fit for consulting work as well.

Thank you for considering my application. I look forward to the opportunity to speak with you.

Nan Cheng
Email: nan.cheng@unisg.ch
Date: 17.01.2025