# Some Words to Say :)

## Self Introduction

I am Tinghao (Vitus) Xie, a junior undergraduate student majoring in Computer Science and Technology at Zhejiang University (ZJU). My current research interest lies in the intersection of secure, efficient, robust AI and systems.

I've been studying and working around **systems** since my freshman year at ZJU. Guided by Prof. *Jianhai Chen*, I learned about **high-performance computing** and participated in related competitions as a member of ZJU Super Computing Team. Then I involved in the Student Training Research Program, conducting research on *SGX Security Protection Technology of Distributed Machine Learning under GPU Architecture* around **system-level security**, also advised by *Chen*. During the research, I lead a group of three undergraduates. The research topic was huge to us, leading to difficulties we had never imagined, various system and security terminologies as examples. Nevertheless, we overcame most obstacles and decided to focus on an achievable smaller part of the topic. Eventually, we shrank the topic to a protocol, **Enchecap**. Even though we were not comprehensively guided throughout the research program, I did benefit a lot from the groping process. In addition, I acquired some overview of system security. And I began to realize that such security and related overheads nowadays highly depend on hardware-level improvements, which are difficult to push forward individually.

Recently, I've realized some of my interest in **algorithm-level security**, especially for deep learning or generic AI. My interest in AI security might be sort of an extension of the system security knowledge (though not much) I've obtained earlier. Furthermore, I believe AI security is a promising area with a lot to be experimented with and discovered. As a result, I've recently started another research internship around AI security advised by Prof. *Shouling Ji* and *Xuhong Zhang* in NESA Lab. By now, I've read some papers around **adversarial learning** (image retrieval & ranking) and am trying to reproduce some of them.

I am planning to apply for the PhD/MS program after graduation and am hoping to obtain advanced academic guidance and related research experience. Looking even further, I want to work on the intersection of both efficiently robust AI and systems in the future, helping advance the current machine learning systems on different levels. I would be honored if I am offered the chance to visit SL2 Lab, which would get me closer to my pursuit.

I acquired strong coding/programming ability through the last 2 years in my university. Together with my understanding of systems and basic knowledge of AI security, I think I would be helpful to Secure Learning Lab at UIUC.

# My Proud Projects

## Enchecap

It's the product during my first research experience. Although it's not yet strong enough against most actual attacks, it makes some difference! More words are covered in my research summary.

## Tron

It's a project for Computer Graphics course, on which I cooperated closely with my friends. With half a month of hard work, we build the render engine and a fun demo from scratch. We arranged the code structure carefully and tried to make it practical for quick use. The demo can run on various platforms, both desktop and mobile.

## Research on the Texture Packing Problem

It's a research project for Advanced Data Structure & Algorithm course in my sophomore year. After an exciting meeting about it, we came up with the idea to solve the problem with not only the traditional approximation algorithms available on Wikipedia and other papers, but also novel ones -- the traditional algorithms mixed with the genetic algorithm. The idea significantly improved the approximation ratio.