

# ZITAO CHEN

X410C, ICICS, University of British Columbia, BC, Canada  
+1 778-316-8835 ✦ zitaoc@ece.ubc.ca

## EDUCATION

---

1. Bachelor of Engineering in Information Security Sept. 2014 - Jun. 2018  
School of Computer Science, **China University of Geosciences (Wuhan)**  
GPA: 87.67/100  
GRE: V158 Q168 AW:3.5
2. Master of Applied Science in Electrical and Computer Engineering Sept. 2018 - May 2020 (**Expected**)  
**The University of British Columbia**  
**Supervisor:** Prof. Karthik Pattabiraman

## RESEARCH EXPERIENCE

---

### **Wearable Computing Security** Undergraduate research

- Lightweight and real-time key establishment scheme for wearable embedded devices.
- Sensing user real-time motion to secure communication between body-worn devices.
- Key establishment scheme leveraging original sensory data.
- I independently proceeded the project under minimal supervision.

### **Reliability in Machine Learning Systems** Graduate Research

- *Research question:* How to identify the critical bits in ML systems under the presence of transient hardware faults.
- We analyze the mathematical properties of common ML systems, and find many of them exhibit monotonicity, which constraints the fault propagation behaviors.
- We design a binary-search like fault injector to identify these critical bits, *without* resorting to doing fault injection (FI) on every state space.
- Our approach can identify over 99.54% of critical bits with significantly lower overhead than doing FI on every state space, which is the only other way to find these critical bits.
- Code: <https://github.com/DependableSystemsLab/TensorFI-BinaryFI>
- *Ongoing research:* Designing detection&protection techniques for enhancing the reliability and security (due to hardware faults) of ML systems.

## PUBLICATION

---

- [SC'19] [Zitao Chen](#), Guanpeng Li, Karthik Pattabiraman, Nathan DeBardeleben "BinFI: An Efficient Fault Injector for Safety-Critical Machine Learning Systems", *In Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*, **AR: 20.9% (72/344) direct acceptance rate for regular papers.**
- [FGCS] [Zitao Chen](#), Wei Ren, Yi Ren and Kim-Kwang Raymond Choo, "LiReK: A Lightweight and Real-time Key Establishment Scheme for Wearable Embedded Devices by Gestures or Motions", *Future Generation Computer Systems* (2018): 84, 126-138, [2018 Impact Factor: 5.768]

## COMPUTER SKILLS

---

Programming Language	Python, C, Java, C++
Operation System	Linux, Windows

## AWARD

---

Graduate Student Initiative: \$4000

2019