Sanket Kanjalkar

Curriculum Vitae

508 E University Avenue
2412-D, 61820, Champaign IL
(217) 721 7898
sanket1729@gmail.com
sanket1729.github.io

Education

Aug 2018 – May 2020 **Masters with thesis**, *Computer Science*,
University of Illinois Urbana Champaign (UIUC) , GPA – 4.0/4.0 – **A+** in all courses.

July 2012– May 2016 **Bachelor of Technology and Honors**, *Computer Science and Engineering*,
Indian Institute of Technology(IIT) Bombay, GPA – 8.98/10.

Publication

Feb'2019 **I can't believe it's not stake**, ***Sanket K***, *J. Kuo, Y. Li, Andrew Miller*, Financial Crypto '19, pdf.

- Largest coordinated disclosure for resource exhuastion vulnerabilities affecting 26+ currencies having a total of **2.6 billion** USD market cap. Awarded a bug bounty of 15k$

Apr 2019– Feb 2020 **An Empirical Analysis of Privacy in the Lightning Network** ,
G Kappos, H Yousaf, A Piotrowska, ***Sanket K****, Sergi, A Milller, S Meiklejohn*, Fin Crypto '21, pdf.

- Empirical evaluation of the security and privacy of lightning network, an off-chain Layer-2 scaling solution for bitcoin with novel attacks and private channel analysis github

Feb 2020– Oct 2020 **Publicly Auditable MPC-as-a-Service with succinct verification and universal setup** ,
Sanket K*, Y Zhang, S Gandlur, A Milller*, pdf.

- Extends the Multi-Party Computation(MPC) state of the art to offer integrity guarantees even if all parties are corrupt. github
- Makes auditable MPC practical by removing expensive setup and improves the state of art in performance by a factor of three.

Current Employment: Blockstream Research

June 2020 – current **Simplicity: A new language for blockchains**,
Russell O Connor, Andrew Poelstra(Blockstream) *pdf*,
Design and implementation of simplicity – A new smart contract programming language for bitcoin like blockchains github.

Research Internship

May 2019–Aug 2019 **Research Intern**, *Dr. Pieter Wuille, Andrew Poelstra*, Blockstream research.

- Research and development of minisript, a language for writing (a subset of) Bitcoin Scripts in a structured way, enabling analysis, composition, generic signing github
- Currently maintaining a production ready implementation of open source library mini-script in rust.

Selected Course Projects

Spring 2019 **Formally verified secp256k1**,
Prof. Madhu Parthsarthy,
built a formally verified version of secp256k1 ecliptic curve library github.

Fall 2018 **SVM on bulletproofs**,
Prof. Andrew Miller,
A Zero Knowledge Proof where the prover can convince the verifier that the classifier classifies a known dataset with a certain accuracy without revealing any secret weights used in the classifier github.

July 2015– May 2016 **Undergraduate Dissertation**,
Prof. R K Shyamasundar, IIT Bombay,
Static Analysis of programs for checking malicious behavior using clustering techniques on program control flow graphs github.

Industry Experience

Samsung Electronics, S. Korea

Sept 2016– June 2018 **Associate**, *Security Part, Visual Display*.
Worked on design and development of Threat Intelligence System for Samsung Smart Tv's.

- Designing a system from scratch via ***Enterprise Architect***. Single-handedly responsible for implementation of distributed system across multiple machines with rpc support via ***rabbitMQ***, ***Spring*** framework for webservers, ***postgreSQL/hibernate*** for database and ***python3*** for data analytics using **TDD** approach
- Automated Weekly Security Status report generation based on analytics on TV security reports from tens of thousands of Smart TV's worldwide. Deployment and maintenance of the system in production environment

May 2015– July 2015 **Summer Intern**, *Security Part, Visual Display*, Performed qualitative research on methods to determine a trust metric for an IoT(Internet of Things) device in an IoT ecosystem. Built an online Machine learning model which takes various device attributes as input and outputs trust level .

CarSense Technologies

June 2016– Aug 2016 **Graduate Intern**, *Firmware team*.
Implemented logic for detecting vandalism, towing and gps location tracking on STM32 IC in ***low level C*** for an embedded device connected to OBD port of the car.

Achievements

2019 Recived a bounty of **15,000 USD** for responsible disclosure of bugs to open source cryptocurrencies

2018 Recieved full scholarship **(4000$)** to attend the workshop of **Programming Blockchain** by Jimmy Song in Chicago and successfully completed it

2016 - 2108 Co-organizer of Seoul Bitcoin Meetup with over 2200 members. Conducted tens of technical presentations on bitcoin and 1 hands on developer workshop about Bitcoin Scripts

2012 Secured All India Rank 29 in IIT-JEE

2015 Won chess, Coding and Logic General championship at IITB

2016 Awarded Hostel technical color for Hostel-2 in 2016

Teaching Assitantships

2018 Fall 2018 Teaching Assistant for CS101 Intro to Computing course at UIUC

2019 Fall 2019 Teaching Assistant for EE407 Cryptography course at UIUC

2016 Awarded TA of the month award for Introduction to Programming CS101 course amongst all TAs in computer science department IITB

Interests and Skills

Open Source bitcoin, rust-bitcoin ecosystem

Languages **C, C++, Java EE, Python, Latex, SQL, rust** *2 years industry + 4 years academic*

Framework **Spring, Hibernate, RabbitMQ, Enterprise Architect** *2 years industry experience*

Interests Bitcoin, Blockchain, Software design, Security and Applied Cryptography

Courses Computer Security, Applied Cryptography, Special topics in Cryptography, Consensus Algorithms, Formal Methods