Qin ZHOU

780 Acacia Walk Apt J, Goleta, California, U.S. 93117
qinzhou@cs.ucsb.edu, +1(805)-453-4657
http://cs.ucsb.edu/~qinzhou

EDUCATION: University of California, Santa Barbara — Santa Barbara, CA, U.S.
- PhD Student, Computer Science — *Sept. '2011 – Present*

Zhejiang University — Hangzhou, P.R.China
- College of Computer Science and Technology — *Sept. '2007 – Jun. '2011*
- Overall GPA: 3.91/4.0(88/100) Major GPA: 3.93/4.0(89/100) Rank: Top 10%

INTERNSHIP: **Microsoft Research Asia** — *Jan. '2011 – Jul. '2011*

Fulltime Research Intern, Software Analytics Group
- Develop Software Analysis Systems for operating system.

PROJECT EXPERIENCE:

4096-Bit RSA Hardware Implementation — *Mar. '2013 – Aug. '2013*
- Implemented 4096-Bit RSA encryption on Altera EP2C50 chip. Montgomery multiplication and Coarsely Integrated Operand Scanning (CIOS) were used to improve performance. Our goal is to build side channel attacks and counter measures on this project and publish several papers.

Parallelized Attacks to Elliptic Curve Discrete Logarithm Problem — *Jan. '2013 – Mar. '2013*
- Parallelized attacks to Elliptic Curve Discrete Logarithm Problem (ECDLP), in which I used Bruteforce Attack and Pollard Rho Attack.

Implementing AES-CCM ECC Cipher Suites for TLS — *Oct. '2012 – Dec. '2012*
- Implemented AES-CCM ECC Cipher Suites for TLS based on draft-mcgrew-tls-aes-ccm-ecc-02, which uses ECDHE-ECDSA for key exchange and AES-CCM for data transfer to build up a Transfer Layer Security. Involved approximately 3,000 lines of C code.

Stack Trace Mining based on Frequent Sequence Mining Algorithm — *Jan. '2011 – Jul. '2011*
- Done in Microsoft Research Asia. A distributed data mining system, which would divide a file into multiple partitions then loaded onto each machine, which would compute its share using multi-threads. I finished the trial of different partition scheduling methods. Involved approximately 30,000 lines, using HPC API and mainly in C#.

TEACHING EXPERIENCE:

CS178: Introduction to Cryptography, Instructed by Cetin Kaya Koc — *Winter. '2013*

CS170: Operating Systems, Instructed by Tao Yang, Christopher Kruegel — *Spring & Fall. '2012*

Served as teaching assistant. Tasks including holding discussion sections, office hours and grading.

COURSES: **Security Seminar: Hacking Night, Instructed by Richard A. Kemmerer** — *Winter. '2013*

Hacking Vortex (an online Wargame from OverTheWire), Learned a lot of different hacking methods.

Network Security, Instructed by Cetin Kaya Koc — *Fall. '2012*

Learned cryptography and network security protocols. Implemented AES-CCM ECC Cipher Suites for TLS.

SKILLS: Python, JAVA, C/C++/C#, Verilog HDL, PHP, HTML, CSS, JS, Linux, Cryptography, Security, Data Mining, Database, Algorithms, Writing, Translation