Teaching Statement

DONGHOON CHANG
Associate Professor, Computer Science and Engineering & Applied Math, IIIT Delhi, India
Cryptographic Technology Group, Computer Security Division, NIST, USA

Since 2012, I have been serving students as a course instructor for the last seven years. Let me first share my past experience and teaching philosophy. As we have done for IIIT Delhi students (mentioned in below), I would like to bring the learning culture to a renowned university in USA.

1. 1-1 Biweekly Meetings with students (by creating Mentoring based course structures)

For crypto-related courses, my PhD students are involved to mentor each student. Every week each student had to meet his/her mentor and meet me bi-weekly and they are supposed to show their progress of learning. I have applied this strategy for more than five years in IIIT Delhi. I can also teach practical security systems such as crypto currency, block-chains, biometric security system etc.

For teaching discrete mathematics, I usually prepare all the lecture notes in advance by using various color pens. It is effective to deliver the concept of mathematics to students. Especially, in order to create lecture notes, I had to read several books and resources from the Internet. In this way, I want to teach discrete mathematics to students so that they might not lose a desire of learning but may actively participate in classes and improve their learning and understanding throughout the semester.

2. Motivating Undergraduate students to do research

In 2016, two undergraduate students, Akshima and Aarush Goel, under my supervision for their research, got direct PhD admission with full scholarship from renowned US universities. Akshima has got admission from Rutgers University and her supervisor is now Dr. David Cash. Aarushi got admission from Johns Hopkins University and her supervisor is Dr. Abhishek Jain. Currently, they are doing research on cryptography actively to build their own career. Likewise, my teaching philosophy is that an instructor should not teach only inside classrooms but also encourage and help students to do more practical research or internship through company projects for their career building.

3. Active Collaboration with other universities or organizations to provide opportunities to students

During the last five years, my crypto group has been collaborating with security division of NIST (National Institute of Standards and Technology), USA. For example, Monika and Sweta (supervised under my guidance) have been working with NIST by participating in NIST projects. By the end of 2019, two more PhD students, Jinkeon Kang and Munawar Hasan, are expected to join NIST. NIST fully supports my group members to do research on computer security with NIST researchers.

Arpan and Naina, PhD students under my guidance, were doing research in NTU in Singapore for six months. Surabhi Garg, a PhD student under my guidance, visited Germany for three months for research collaboration on biometric security. In this way, I try to help our students to grow as security experts and professionals through the collaboration with worldwide renowned universities.

In order to bring collaboration between the universities of two nations, India and Korea, I visited four major universities in Korea and incubation centers. Due to such effort, Game development workshop could be held in February 2019 in IIIT Delhi. The workshop was conducted by Prof. Kim of Sangmyung University, Korea, for 4 days. More than 60 IIIT Delhi students registered and two of them were finally selected for the Summer internship (with full support) starting from June 25, 2019. And MoUs were established between IIIT Delhi and Sangmyung University and between Centre for Design and New Media (CDNM) and College of Convergence Engineering. Korea is strong in Game development. I hope that IIIT Delhi may grow in Game development through the collaboration with Universities in Korea.

In 2019, Double PhD degree program between IIIT Delhi and the graduate school of cyber security (GSCS) of Korea University was established under the approval of both universities. Through this program, the collaboration in various security-related R&D would be possible by exchanging PhD students of both universities.

4. Active Collaboration with companies to provide internship opportunities to students inside the campus

In January 2016, R&D center for a Korean IT company, Irisys, was established inside IIIT Delhi campus. Through this, more than 10 students could have the internship opportunities. Two graduated bachelor students and two master students are currently working in the R&D center of Irisys, and at the same time, they are doing research with other professors in their interesting research field for their higher education and career building. Through this kind of collaboration, students can learn more practical knowledge and skills.

5. Motivating Undergraduate or Postgraduate students to do their own startup

As a foreigner in India, there are many limitations for me to get government projects or funds. However, through struggling by bringing projects and funds from other places and sources, my R&D capabilities and networking could have been much improved. For example, I have started to do research with Indian security experts and Indian companies such as Transech (www.tresea.com) as well as Korean companies, Korean governments, and Korean R&D institutes such as ETRI (https://www.etri.re.kr/eng/main/main.etri). Actually, Transech was established by my students in 2016, Munawar Hasan and Ajit Pratap Singh, and the company has been growing through various collaboration with Korean side. In this way, I would like to make Transech like Infosys or TCS, which is my vision. Also I try to encourage and support our students to open their own security companies.

6. Courses I can teach:

(1) **Programming Languages:** C, C++
(2) **CS courses:** Computer Architecture, Algorithms, Theory of Computation
(3) **Security-related Courses:** Network security, Applied Cryptography, Computer Security, Blockchain
(4) **Mathematics Courses:** Algebra, Discrete Mathematics, Combinatorics, Calculus, Probability, Statistics, Number Theory

7. Graduated PhD Students (for the last three years)

(1) **Jayaprakash Govindraj**, Thesis title: "Forensics enabled secure mobile computing system for enterprises". His PhD degree was awarded in Dec 2018. I am a co-guide with supervisor Dr. Gaurav Gupta. He is currently working in McAfee.
(2) **Robin Kumar Verma**, Thesis title: "Digital Forensics 2.0: an automated, efficient, and privacy preserving digital forensic investigation framework". His PhD degree was awarded in Oct 2018. I am a co-guide with supervisor Dr. Gaurav Gupta. He is currently doing Postdoc at The University of Texas at San Antonio, USA.
(3) **Sweta Mishra**, Thesis title: "Design and Analysis of Password-based Authentication Systems". Her PhD degree was awarded in Jan 2018. I am a supervisor with co-supervisor Dr. Somitra Sanadhya. From February 2018 to June 2019, she had been doing post doc in Computer Security Group, NIST, USA. Currently, she is working as an assistant professor at CSE department of Shiv Nadar University, India.
(4) **Tarun Kumar Bansal**, Thesis title: "Designing Generic Asymmetric Key Cryptosystem with Message Paddings". His PhD degree was awarded in April 2018. He is the first PhD through IIITD-QUT collaborative PhD program. I am his supervisor with co-supervisor Dr. Somitra Sanadhya. Currently, he is working as a senior specialist at Bosch in Bangalore, India.
(5) **Mohona Ghosh**, Thesis title: "Cryptanalysis of Block Cipher Constructions", Thesis submitted in Jan 2016. I am a co-supervisor with Dr. Somitra Sanadhya. She had done research with Prof. Thomas Peyrin at NTU Singapore as a post-doctorate from April 2016 to March 2017. She was an assistant professor at (IIITDM) Jabalpur from June 2017 to May 2018. Since May 2018, She has been working as an assistant professor of Department of IT of Indira Gandhi Delhi Technical University, New Delhi.

8. Current PhD Student

(1) Megha Agrawal
(2) Monika Singh
(3) Surabhi Garg
(4) Arpan Jati
(5) Jinkeon Kang
(6) Ajit Pratap Singh
(7) Munawar Hasan

9. Thesis Guidance for the 3rd or 4th year undergraduate students

(1) Purusharth Dwivedi, Security evaluation and Implementation of Face Recognition Algorithms
(2) Tanya Chowdhury, Cryptanalysis of Lightweight Block Ciphers against Zero Correlation & Division Attacks

10. Guidance for Research/Independent Study/Independent Project for 3rd or 4th year Undergraduate and graduate students (Master)

(1) Himanshu Punetha, Analysis of Haraka v2
(2) Shubham Singhal, IS, Study on Mediblock
(3) Nitin Jain, Mtech Minor Project, Tampering Proof Digital Certificate using Blockchain
(4) Shubham Singhal, Mtech Minor Project, Quantum blockchain
(5) Pranav Jain, Btech Project, Application of H-Technique for the Security Proofs of Symmetric-key Ciphers
(6) Sameer Khurana, Mtech Minor Project, Cryptanalysis of OCB2