# Eurocrypt 2019

**19-23 May**

**Mayank Raikwar**
Norwegian University of Science and Technology

## 1 Introduction

I am grateful to COINS to support me for attending Eurocrypt 2019, which held in Darmstadt, Germany. The conference had parallel sessions each day, and this year, there were many interesting papers on Blockchain as well. There were also the Distinguished lecture, Rump sessions, and IACR meeting. For me, It was the first time to attend a conference during the start of Ph.D. and Thanks to COINS to make it possible. It was an excellent learning and enjoyable experience attending the event with my friends from NTNU NaCl group. It was a nice venue to meet many researchers from different universities, industries and to make new connections. On the first day of my arrival there, I met with my Master's friends after a long time and through him, I got to know about his collaborators and colleagues, and we had few discussions about recent works in the blockchain field. I also got a chance to discuss different perspectives of Blockchain and use of cryptography in it with many researchers which aligns with my Ph.D. research topic.

## 2 Conference

As there were parallel sessions, I got to choose among the sessions. However, sometimes, it was difficult to choose as both of the sessions were equally interesting. I enjoyed most of the talks, especially the talks on Blockchain. I also experienced what happens in Rump session, which was amazingly refreshing, knowledgeable, and entertaining at the same time. Few of the talks I liked are as following :

- *Proof-of-Stake Protocols for Privacy-Aware Blockchains* (Chaya Ganesh, Claudio Orlandi, and Daniel Tschudi) : I have been interested in consensus mechanisms of different blockchains and *Proof-of-Stake* is one of these. In this paper, they showed how to achieve privacy of stake value as well as stakeholder in consensus protocol.
- *Reversible Proofs of Sequential Work* (Hamza Abusalah, Chethan Kamath, Karen Klein, Krzysztof Pietrzak, and Michael Walter) : The work from IST Austria group was really wonderful. They created a new efficient PoSW in the random permutation model based on skip lists. I got the chance to meet them and discuss more about it.

- *Founding Secure Computation on Blockchains* (Arka Rai Choudhuri , Vipul Goyal, and Abhishek Jain) : In this work, they used blockchain as a bookkeeping and used it to construct Zero-Knowledge and secure computation protocol. This work gives a direction to build different cryptographic concepts using blockchain.
- *Efficient Verifiable Delay Functions* (Benjamin Wesolowski) This paper won the Best Young Researcher Paper, and the talk by Benjamin was fascinating and easy to follow. He explained his construction of VDF, which is super nice and can be applied in the construction of randomness beacons and leader election in consensus protocols. This talk motivated me to do more research and exploration in this field.

## 3 Conclusion

Meeting with new researchers and making new connections was a pleasant experience. I gathered a lot of new information and found many interesting topics to do more research during my Ph.D. I also explored the beautiful city of Darmstadt as well as Frankfurt. So Overall it was an excellent and satisfactory experience attending Eurocrypt 2019.