Zero-Knowledge Proof Workshop 2019

The Zero-Knowledge Proof Workshop 2019 was organized April 10.-12. 2019 in Berkeley, USA. This was the second workshop in the series, started in Boston, USA in May 2018. The workshop aims to bring together mathematicians, computer scientists and entrepreneurs working on zero-knowledge proofs, to join people working both from a theoretical and practical view with this technology. Zero-knowledge proofs (ZKP) was first described in 1989, and there's been a lot of theoretical development since then. However, in the last few years, we've seen a lot more traction when it comes to implement this into real world system, partly because of the rapid increase of people working on blockchain and privacy focused technology.

You can find information about the workshop on zkproof.org/workshop2/main.

Zero Knowledge Proofs were first introduced by Goldwasser, Micali and Rackoff in the late 80's. They created a new proving procedure for communicating a proof, or in modern terms, an efficient interactive proof system. An interactive proof is a process in which a prover probabilistically convinces a verifier of the correctness of a mathematical proposition. In 2012, Shafi and Silvio received the A.M. Turing Award "for transformative work that laid the complexity-theoretic foundations for the science of cryptography".

Surprisingly, they show how to make any proving system in NP zero knowledge, meaning that the verifier learns nothing but the correctness of the proposition. Zero Knowledge Proofs therefore provide complete privacy to the prover while convincing the verifier. Further research resulted in the study of non-interactive zero knowledge proofs (NIZKs), a variant that does not require interaction between the prover and the verifier. Building on top of these, modern NIZK systems have become more efficient, including succinct proofs, sub-linear verifiers and highly efficient provers.

The workshop included an industry day with showcases from real world applications, for how ZKPs are used in consumer communication, banking industry, online privacy applications and blockchains. The second and third day

had a more theoretical focus, in addition to focusing on how the ZKP technology can be standardized, so that it more easily can be implemented and used across different platforms. Some of the inventors and greatest researchers in the development of ZKP gave talks during the workshop, including Shafi Goldwasser, Jens Groth, Amit Sahai, Yael Kalai, Alessandro Chiesa and Dan Boneh. The talks are available on YouTube: s.ntnu.no/zkp.

Figure 1: Group photo of all participants

I had a great time at the workshop, and I got to meet several prominent researchers over the three days. Thank you Coins, for giving me the chance to attend the Zero Knowledge Proof Workshop 2019.

May 13, 2019
Tjerand Silde
tjerandsilde.org