Report about Asiacrypt 2019

Shuang Wu

April 22, 2020

1 Overview

Asiacrypt 2019, the 25th Annual International Conference on the Theory and Application of Cryptology and Information Security, was hold in Kobe, Japan on December 8-12, 2019. It is organized by the International Association for Cryptologic Research (IACR) in cooperation with the technical group on Information Security(ISEC) of Institute of Electronics, Information and Communication Engineers(IEICE).

2 Interesting talks

The first day, the invited speaker Krzysztof Pietrzak gave a talk about a new proof technique for blockchain, called proofs of space and verifiable delay functions. Compared to proof of work, proof of space consumes less energy, thus more sustainable and environmental friendly.The main idea is instead of dedicate a significant amount of computation, a service requestor must dedicate a significant amount of disk space. It requires the prover to store large amount of data, while the verifier will ask some specific position of the data, the prover needs to reply quickly. Thus the construction also involves the verifiable delay function.

One talk I was interested is about 'Dual-Mode NIZKs from Obfuscation' from Bogdan Ursu, they provide a generic construction of dual-mode NIZK systems for all of NP. Dual-mode NIZK systems is a non-interactive zero-knowledge scheme which can provide soundness or zero-knowledge to unbounded adversaries dynamically and adaptively as the prover desired (only choose one of these two properties).

Another talk about 'The Broadcast Message Complexity of Secure Multiparty Computation' I found is also very good, They study the broadcast message complexity of secure multiparty computation, the total number of messages that are required for securely computing any functionality in the broadcast model of communication.

The talk I like most is 'Shorter Pairing-Based Arguments Under Standard Assumptions'. It talked about an sufficient non-interactive arguments for correct evaluation of a arithmetic and boolean circuits with proof size $O(d)$,where d is

the multiplicative depth of the circuit, under falsifiable assumptions. It drove me to dig more about the falsifiable assumption and other SNARKs algorithm. Even though the proof size is less than Groth's construction, but their technique 'argument of knowledge transfer,'combining techniques from SNARKs and QA-NIZK arguments of membership in linear spaces is quite interesting.

3 My experience and opinions

The conference is organized very well, the talks are interesting. The organization serves delicious Japanese food and sweets during coffee breaks. The banquet on the third evening was pretty good, there were some shows during the banquet, with traditional Japanese music and dancing. For the reputation of Japanese politeness and Japanese cuisine, I would recommend to join Asiacrypt if this would be hold in Japan again.

My research field is blockchain, even though the conference has only 4 talks about blockchain, but there are a lot interesting talks about multiparty computation and zero-knowledge, which is quite good and actually helpful for my research. Apart from the interesting talks, I gained a lot with respect of the PhD networking. I met and made friends with three speakers during the conference, we discussed the talks and our researches, they are doing PhD in India, Switzerland and America respectively. They are mainly doing multiparty computation and functional encryption. We also traveled together after the conference.