Eurocrypt 2018

Andrea Tenti's report for COINS research School

Tel-Aviv. April, 29 2018 - May, 03 2018

Between the 29th of April and the 3rd of May I took part at the Eurocrypt conference held in Tel-Aviv, together with two colleagues, supported by COINS as well. Eurocrypt is an annual conference and is one of the flagship conferences of the *International Association for Cryptology Research*. The complete program description together with the abstracts of all the papers can be found at https://eurocrypt.iacr.org/2018/program.html. Due to the large amount of papers submitted the conference had, most of the time, two parallel sessions. I tended to attend the most mathematical related talks, but it should be noticed that many presentations about implementation, blockchain and more practical topics played a key role in the conference.

Among the topics in cryptology I was less familiar with, two of them got quite some attention at Eurocrypt 2018, giving me the chance to get up to date with the current "hot topics" in the field. Those were Multiparty computations and Zero-knowledge protocols.

I do believe, overall, that the presentation that I was the most interested in and that held up to my expectations was Henry Corrigan-Gibbs' and Dmitry Kogan's paper, *The Discrete-Logarithm Problem with Preprocessing*, which got awarded with the Best Young Researcher Award by the committee. Indeed, my current research problem has, as main motivation, the DLP in the group of points on elliptic curves. Having a general result as the one provided by the authors has been of great interest to me for it gave a deeper understanding of the intrinsic properties of the objects we are working with.

More in details, Henry Corrigan-Gibbs (the speaker) reminded the reasons for which we believe that, in general, the DLP is a hard problem, especially on Elliptic curves. Indeed, there is a lower bound on the number of operations that any generic algorithm that succeeds with at least $1/2$ probability has to perform. This amount is exponential and, so far, no dedicated algorithm that are faster than generic ones are known for elliptic curve cryptography.

In general, those, the existing lower bounds for generic algorithm do not account for preprocessing. In the paper they show how one can perform an attack with preprocessing in $\mathcal{O}(N^{1/3})$ operations against the known bound for algorithms without preprocessing, requiring $\mathcal{O}(N^{1/2})$ operations. The most interesting result, though, is that in order to perform such attack, it is necessary that the preprocessing time complexity is $\mathcal{O}(N^{2/3})$. More generally, the preprocessing time P must satisfy the relation $PT + T^2 = \mathcal{O}(\epsilon N)$,

where T is the time of the attack (after preprocessing) and ϵ is the success probability.

Worth of mention were also two of the invited talks. The first one was *Desperately seeking S-Boxes* by Anne Canteaut. She gave a really well explained presentation about the property that S-boxes should possess in order for them to be secure against differential attacks. I was already familiar with the topic, but her talk provided me with a global understanding of the subject. The second one was *Thirty years of Digital Currency: From DigiCash to the Blockchain* by Matthew Green. The reasons for which I appreciated it are similar to the ones for Anne Canteaut's paper and I, therefore, believe, that the committee has done an amazing job in choosing the invited speakers.

For what concerns the regular talks, I think that the session about lattices (first day, in parallel with "Foundations") was the richest in terms of compelling talks for me. I am not working on lattices, but among the post-quantum cryptosystems, it is the family I am most interested into. Worth of mention, among the talks in the session, was the presentation of the paper *On the Ring-LWE and Polynomial-LWE problems*, by Miruna Rosca Damien Stehlé Alexandre Wallet.

The experience has been, overall, of key relevance for my growth as a researcher, both for the talks and for the inspiration that the participants provoked in me. I am, therefore, grateful to COINS for having allowed my presence there through financial support.