Title: Constant Communication Oblivious RAM

Tarik Moataz, Colorado State University, USA

Oblivious RAM is a cryptographic primitive that hides the access pattern made by a trusted CPU to an untrusted memory. Recent techniques reduce ORAM communication complexity down to constant in the number of blocks N. One of the most successful has been Onion ORAM, however, it has two main drawbacks. It requires a large block size while it requires expensive polylogarithmic computation based on homomorphic multiplications. In this talk, I present C-ORAM where we address these drawbacks: we reduce the required block size and remove most of the homomorphic multiplications while maintaining a constant communication complexity.

For the second part of this talk, I will introduce CNE-ORAM, a constant communication ORAM without homomorphic encryption. CNE-ORAM is an information-theoretically secure ORAM which, at the expense of requiring multiple servers, allows for substantially reduced client and server computation. In essence, our idea is to combine ORAM with Private Information Storage. By assuming a small number of non-colluding servers, we show how homomorphic encryption can be replaced with much simpler XOR operations. This leads to an ORAM which is extremely lightweight and suitable for deployment even on resource-constrained devices.