PET seminar lecture on

Homomorphic operations over secret shares

Dor Bitan

I will talk about my research on algorithms for information theoretically secure homomorphic encryption and secret sharing. The main question that stands in the basis of the research concerns the possibility of modifying encrypted data obliviously. Oblivious modification of encrypted data is useful for various applications, e.g., multiparty computation, outsourcing of computations, and QKD.

I will present algorithms that consider the scenario in which a user wishes to outsource the storage and computation of confidential data to an untrusted server. The first two works consider the approach of employing multiple servers and distributing secret shares of the data among the servers. The first work introduces a method for evaluating quadratic functions over a dynamic database, with no communication between the servers. The second work allows communication and considers a method for homomorphic evaluation of polynomials of arbitrary degree over non-zero secret shares in a single round of communication. In particular, we suggest novel protocols that enable the evaluation of multivariate polynomials over shares of a non-zero secret without requiring a secret sharing phase invoked in an offline preprocessing phase, and deal with possibly-zero secrets in several ways.

The third work considers the approach of employing a single server. That work assumes that the user and server have quantum capabilities, and attempts to enable the homomorphic evaluation of encrypted classical data using quantum devices. The homomorphic encryption scheme presented in that work is used to construct a quantum key distribution (QKD) scheme resilient against weak measurements. Weak measurement based attacks over known QKD schemes are also introduced in the third work, along with the innovative concept of securing entanglement.