Verifiable Delegation of Computation on Outsourced Data

Dario Fiore – Instituto Imdea Software

Viernes 23 de Mayo, 10:30. Salón de grados. Departamental II.

We address the problem in which a client stores a large amount of data with an untrusted server in such a way that, at any moment, the client can ask the server to compute a function on some portion of its outsourced data. In this scenario, the client must be able to efficiently verify the correctness of the result despite no longer knowing the inputs of the delegated computation, it must be able to keep adding elements to its remote storage, and it does not have to fix in advance (i.e., at data outsourcing time) the functions that it will delegate. Even more ambitiously, clients should be able to verify in time independent of the input-size -- a very appealing property for computations over huge amounts of data.

In this talk I will present novel cryptographic techniques that solve the above problem for the class of computations which can be expressed by arithmetic circuits of bounded degree. In particular I will discuss an efficient solution for the case of quadratic polynomials over a large number of variables. This class covers a wide range of significant arithmetic computations -- notably, many important statistics. To confirm the efficiency of our solution, we show encouraging performance results, e.g., correctness proofs have size below 1 kB and are verifiable by clients in less than 10 milliseconds.

Universidad Rey Juan Carlos

CÁTEDRA I4S-URJC DE INNOVACIÓN EN SEGURIDAD DE LA INFORMACIÓN, PREVENCIÓN DEL FRAUDE Y GESTIÓN DEL RIESGO TECNOLÓGICO