PRIVATE SET INTERSECTION: THE PROBLEM, SOME SOLUTIONS, AND WHAT TO DO IF SIZE MATTERS

MARÍA ISABEL GONZÁLEZ VASCO

ABSTRACT. The Private Set Intersection (PSI) problem deals which a situation in which two mutually distrusting parties, each holding a set of inputs from a fixed ground set, wish to jointly compute the intersection of their sets without leaking any additional information. Typically, cryptographic solutions to PSI allow interaction between a Server S and Client C, with respective private input sets $\mathcal{C} = \{c_1, \ldots, c_v\}$, $\mathcal{S} = \{s_1, \ldots, s_w\}$, both drawn from a ground set $\mathcal{U}$. At the end of the interaction, C learns $\mathcal{S} \cap \mathcal{C}$ and $|\mathcal{S}|$, while S learns nothing beyond $|\mathcal{C}|$. Over the last few years, the research community has devised a number of PSI techniques under different security models. In this talk, we will revise these solutions and direct our attention to those who exhibit the extra feature of keeping the size of the input sets secret; we will in particular focus on recent results which are part of a joint work with Paolo D'Arco, Angel L. Pérez del Pozo and Claudio Soriente.

Dept. de Matemática Aplicada. Universidad Rey Juan Carlos
E-mail address: mariaisabel.vasco@urjc.es