On sharing private calendars and scheduling meetings

Daniel Bosk

School of Computer Science and Communication
KTH Royal Institute of Technology
dbosk@kth.se

6th May 2017

Abstract

Many are reluctant to sharing their calendars publicly, even just their free–busy times — it is a matter of privacy, with varying reasons. We want to solve the problem of scheduling meetings and leak as little information as possible in the process.

We analyse the privacy properties of two general classes of schemes for sharing calendars and computing intersections to schedule events. The two classes of constructions are (algebraically) multiplicative and additive schemes. The multiplicative schemes require all participants to be available in a timeslot for that timeslot to be selected (no known implementation). The additive schemes add all participants' preferences together to select the timeslot where most participants can participate (e.g. Doodle and Dudle).

In our analysis we assume that there is an ideal function — in the sense of secure multiparty computation (MPC) — and the results are thus valid for *any* provably secure scheme based on either of these structures. There are schemes that are provably secure (e.g. Dudle) — for a single run, standard MPC requirement. But we never schedule only one meeting, problems occur when we schedule several meetings. We analyse what can be inferred from the outputs of multiple runs and find that Eve can infer everyone's secret inputs in many cases. These results can then be used in the design of a multi-run secure scheme with the desired privacy properties.