Cryptology ePrint Archive: Report 2011/141

Fast and Private Computation of Set Intersection Cardinality

Emiliano De Cristofaro and Paolo Gasti and Gene Tsudik

Abstract: The use of sensitive electronic information has increased tremendously in recent years. In many realistic application scenarios, legitimate needs for sensitive information must be reconciled with privacy concerns. This has motivated various privacy-protecting cryptographic techniques, such as Private Set Intersection (PSI) and Private Set Union (PSU). Such techniques involve two parties – a client and a server – each holding a private data set: the client learns only the intersection (or union) of the two respective sets, while the server learns nothing. How- ever, it is often imprudent to use PSI and PSU protocols alone, since their use may offer little or no privacy for the server. Instead, prospective participants in PSI/PSU protocols should use their respective policies to decide whether or not to participate. Policies can be based on variables, such as the size of set intersection and its relationship to the entire set size. To enable policy considerations in advance of private set operations, we need a cryptographic primitive called Private Set Intersection Cardinality (PSI-CA), which yields only the size of set intersection. PSI-CA protocols are also particularly appealing in numerous realistic scenarios where it is crucial to obtain the magnitude – rather than the content – of the set intersection.

This paper motivates the need for PSI-CA and constructs a very efficient (i.e., linear-complexity) protocol. Efficiency claims are supported by experiments with prototype implementations. Finally, an extension to support authorization of client input is also sketched.

Category / Keywords: cryptographic protocols /

Date: received 21 Mar 2011, last revised 26 Jul 2011

Contact author: edecrist at uci edu