Cryptology ePrint Archive: Report 2011/267

Mutual Private Set Intersection with Linear Complexity

Myungsun Kim and Hyung Tae Lee and Jung Hee Cheon

Abstract: A private set intersection (PSI) protocol allows players to obtain the intersection of their inputs. While in its unilateral version only the client can obtain the intersection, the mutual PSI protocol enables all players to get the desired result. In this work, we construct a mutual PSI protocol that is significantly more efficient than the state-of- the-art in the computation overhead. To the best of our knowledge, our construction is the \emph{first} result with linear computational complexity in the semi-honest model. For that, we come up with an efficient data representation technique, called \emph{prime representation}.

Category / Keywords: Mutual Private Set Intersection, Prime Representation

Publication Info: To be appeared at WISA 2011

Date: received 25 May 2011, last revised 25 Dec 2011

Contact author: msunkim (at) snu (dot) ac (dot) kr

Available formats: PDF | BibTeX Citation

Version: 20111226:012330 (All versions of this report)

Discussion forum: Show discussion | Start new discussion
