

Secure Coprocessor-based Private Information Retrieval without Periodical Preprocessing

October 13, 2009

Abstract

First works on Private Information Retrieval (PIR) focused on minimizing the necessary communication overhead. They seemed to achieve this goal but at the expense of query response time. To remove this weakness, protocols with secure coprocessors were introduced. They achieve optimal communication complexity and better online processing complexity. Unfortunately, all secure coprocessor-based PIR protocols require heavy periodical preprocessing computation. In this paper, we propose a new protocol, which is free from the periodical preprocessing computation while offering the optimal communication complexity and almost optimal online processing complexity. The proposed protocol is proven to be secure.

Keywords. Private information retrieval, secure coprocessor.