به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

رمزنگاری کاملاً همریخت و کاربرد آن در پروتکل بازیابی اطلاعات محرمانه

Fully homomorphic encryption system and its application in private information retrieval protocol

محمد مختاری

زمان: شنبه ۱۳ اسفندماه ۱۳۹۲ ساعت ۳ عصر

مکان: دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه چهارم، سالن ۴۰۴

Suppose that we want to delegate the ability to process encrypted data, without giving away access to it. The fully homomorphic encryption scheme maintains data private, but allows a worker that does not have the secret decryption key to compute any (still encrypted) result of the data, even when the function of the data is very complex. Fully homomorphic encryption has numerous applications. For example, it enables private queries to a search engine - the user submits an encrypted query and the search engine computes a succinct encrypted answer without ever looking at the query in the clear.

The purpose of this presentation is the present of homomorphic encryption systems and its application on private information retrieval (PIR) protocol. At first, we introduce the integers based homomorphic encryption system where the second homomorphic encryption system. The purpose of this cryptosystem is understanding homomorphic encryption. In the following, LWE cryptography system is introduced where improves previous scheme from various aspects. Finally, PIR protocol is expressed and the development of this protocol is reviewed. We also have a comparison between some kinds of this protocol.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.