Cryptology ePrint Archive: Report 2011/446

Private Information Extraction over Online Social Networks

Huang Lin and Yuguang Fang and Zhenfu Cao

Abstract: Due to the popularity of online social networks (OSNs), various online surveys have been done over OSNs to help researchers extract information of human behaviors on various aspects, ranging from online purchasing to disease epidemic patterns. Since online surveys usually attempt to extract the statistical features over a large population, the more participants respond, the more accurate the results will be, and hence the greater the social utility of such survey will be. Despite the growing importance of online surveys in modern social life, people are generally reluctant to respond to an online survey due to the possible privacy leakage especially when the questionnaire in the survey is related to sensitive personal information such as the health related issues, or even if they choose to respond to the survey, people might deliberately twist their responses to protect their privacy. On the other hand, low response rate of online surveys will lead to biased or even unqualified results. How to find an effective way to increase the response rate while preserving responders' privacy to some extent is a challenging problem. In this paper, we design two privacy-preserving online survey protocols which enable the inquirer to extract two most important statistical data: the intersection and the union information of responders' choices. The intersection information implies the common choice selected by all the responders while the union information corresponds to the preference of each choice in the survey. We formally prove that the proposed schemes are secure. We have also carried out extensive study and shown that the proposed schemes are more efficient than the related works. Moreover, we also discuss how to make the two basic schemes accommodate dynamic group formation and extend our schemes without central key authority.

Category / Keywords:

Date: received 15 Aug 2011

Contact author: huanglin at ufl edu