Chapter 6
Secure Computation of Private Set Intersection Cardinality With Linear Complexity

Sumit Kumar Debnath
National Institute of Technology Jamshedpur, India

ABSTRACT

PSI and its variants play a major role when the participants want to perform secret operations on their private data sets. The importance of this chapter is twofold. In the first phase, the author presents a size-hiding PSI-CA protocol followed by its authorized variant, APSI-CA, utilizing Bloom filter. All these constructions are proven to be secure in standard model with linear complexity. In the second phase, the author employs Bloom filter to design an efficient mPSI-CA protocol. It achieves fairness using offline semi-trusted third party (arbiter) unlike the most efficient existing protocols. The arbiter is semi-trusted in the sense that he does not have access to the private information of the entities while he will follow the protocol honestly. Proposed mPSI-CA is proven to be secure against malicious adversaries in the random oracle model (ROM) under the decisional Diffie-Hellman (DDH) assumption. It achieves linear complexity.

INTRODUCTION

At present, sharing of electronic information among mutually unreliable entities increases rapidly. Consequently, there is a strong need of cryptographically secure techniques, that allows sharing of electronic information. Private Set Intersection (PSI) is one such technique that allows two parties to secretly determine the

DOI: 10.4018/978-1-5225-5742-5.ch006

intersection of their respective private sets without revealing any additional information. Depending on the functionality, PSI is of two kinds: (i) one-way PSI which enables either of the two parties to receive the output (intersection), while the other does not get any information and (ii) two-way PSI or mutual PSI (mPSI), whereby both the parties receive the intersection. In DNA matching, two entities may wish to determine private computation of Hamming Distance between two strings on an arbitrarily large alphabet by considering each symbol in the alphabet along with its position in the string as a unique set element. Private Set Intersection Cardinality (PSI-CA) is an appropriate cryptographic technique for this kind of real-life scenarios as it allows the entities to execute the cardinality, instead of any content of the intersection. Similar to PSI, PSI-CA is of two kinds: one-way PSI-CA and two-way PSI-CA or mutual PSI-CA (mPSI-CA). Another variant of PSI or PSI-CA, where the client's set needs to be authorized by a certifying authority before the communications between client and server, is known as Authorized PSI (APSI) or Authorized PSI-CA (APSI-CA). In the recent research community, PSI and its variants have gained considerable attention due to their broad applications. Privacy preserving data mining, location-based services, social networks, testing of fully sequenced human genomes, are a few to name. Let us consider some real-life scenarios where private data needs to be shared:

1. Program chairs of a conference want to make sure that none of the submitted manuscripts are also under review in any other journal or conference, while they have to preserve the privacy of the contents of the submitted manuscript.
2. A social network user, say Bob would like to discover a nearby match from a group of users by determining the number of standard connections.
3. Two NGOs may wish to determine the total number of ordinary villagers, affected by a disease in a village. While none of them are allowed to reveal their list of suspects as revealing that list may create an impact on a patient's mind.

In any real-life application of PSI-CA or its variants, the user's privacy can be preserved using the Internet of things (IoT). For instance, in the case of the aforementioned social networking example, Bob cannot reveal its privacy as that may cause a threat to him. Thus, user's privacy needs to be preserved in PSI-CA and its variants, and in order to do that IoT is required.

Results

In this chapter, the author is mainly interested to design PSI-CA, APSI-CA and $mPSI$ -CA protocols utilizing the Bloom filter. The importance of the work is