Multiparty Data Sharing and Computation using Privacy preserving Data Sharing with Anonymous ID Assignment

Abstract:
An algorithm for anonymous sharing of private data among N parties is developed. This technique is used iteratively to assign these nodes ID numbers ranging from 1 to N. This assignment is anonymous in that the identities received are unknown to the other members of the group. Resistance to collusion among other members is verified in an information theoretic sense when private communication channels are used. This paper builds an algorithm for sharing simple integer data on top of secure sum. A secure sum algorithm allows the sum to be collected with some guarantees of anonymity. Secure computation function is popular in data mining applications and also helps characterize the complexities of the secure multiparty computation.

Data encryption is an anonymisation technique that replaces sensitive data with encrypted data.

The process provides effective data confidentiality. An algorithm for distributed solution of certain polynomials over finite fields enhances the scalability of the algorithms. Markov chain representations are used to find statistics on the number of iterations required, and computer algebra gives closed form results for the completion rates.