DOI: 10.20472/IAC.2017.33.043

BO-RONG LIN

National Chiao Tung University, Taiwan

HUI-CHUAN LU

National United University, Taiwan

HSIN-HAN TUNG

National United University, Taiwan

A CONSTRUCTION OF PERFECT SECRET-SHARING SCHEMES FOR THE ACCESS STRUCTURES BASED ON AN INFINITE CLASS OF GRAPHS WITH LOW INFORMATION RATIO

Abstract:

Secret-sharing is an interesting branch of modern cryptography. It is crucial in the security of information storage and has found numerous applications in many fields. In a secret-sharing scheme, there is a dealer who has a secret key, a finite set P of participants and a collection Γ of subsets of P called the access structure. Each subset in Γ is a qualified subset. A secret-sharing scheme is a method by which the dealer distributes a secret key among the participants in P such that only the participants in a qualified subset can recover the secret from the shares they received. If, in addition, the shares given to the participants in any unqualified subset reveal no information about the secret, then this secret-sharing scheme is called perfect. The information ratio of a perfect secret-sharing scheme is a measurement of the efficiency of the scheme. It is defined as the ratio of the maximum length (in bits) of the share given to a participant to the length of the secret. Since this ratio represents the maximum bits a participant has to remember for each bit of the secret, it is expected to be as low as possible. Constructing secret-sharing schemes with the lowest ratio becomes an important task to achieve. Given an access structure Γ, the infimum of the information ratio of all possible perfect secret-sharing schemes realizing this access structure is referred to as the optimal information ratio of Γ. In this paper, we consider graph-based access structures. Given a simple graph G, let each vertex of G represents a participant and each edge of G represents a minimal qualified subset. The optimal information ratio of G is the infimum of the information ratio over all possible perfect secret-sharing schemes on G. Determining the exact value of the optimal information ratio is challenging. Most results give bounds on it. In this paper, we introduce an infinite class of graphs G(n,k) whose optimal information ratio has been shown to be at least 2-2^(-n+1). Subsequently, we propose our construction of a perfect secret-sharing scheme on each G(n,k) whose information ratio is 2. Therefore, the optimal information ratio of G(n,k) lies between 2 and 2-2^(-n+1). This bound is very good when n is sufficiently large, which also means the perfect secret-sharing schemes we construct are in fact quite efficient

Keywords:

perfect secret-sharing scheme, information ratio, graph-based access structure, vector space