Perfect secret sharing scheme based on vertex domination set

ABSTRACT

Due to the fast development in data communication systems and computer networks in recent years, the necessity to protect the secret data has become extremely imperative. Several methods have been proposed to protect the secret data; one of them is the secret sharing scheme. It is a method of distributing a secret K among a finite set of participants, in such a way that only predefined subset of participant is enabled to reconstruct a secret from their shares. A secret sharing scheme realizing uniform access structure described by a graph has received a considerable attention. In this scheme, each vertex represents a participant and each edge represents a minimum authorized subset. In this paper, an independent dominating set of vertices in a graph G is introduced and applied as a novel idea to construct a secret sharing scheme such that the vertices of the graph represent the participants and the dominating set of vertices in G represents the minimal authorized set. While most of the previous schemes were based on the principle of adjacent vertices, the proposed scheme is based upon the principle of non-adjacent vertices. We prove that the scheme is perfect, and the lower bound of the information rate of this new construction is improved when compared to some well-known previous constructions. We include an experiment involving security threats to demonstrate the effectiveness of the proposed scheme.

Keyword: Secret sharing scheme; Independent dominating set; Information rate; Uniform access structure; Rank