عنوان مقاله:

Ideal secret sharing schemes on graph-based ۳-homogeneous access structures

محل انتشار:

فصلنامه معادلات در ترکیبات, دوره 10, شماره 2 (سال: 1400)

تعداد صفحات اصل مقاله: 14

نویسندگان:

Shahrooz Janbaz - *Electrical and computer faculty, Malek Ashtar University of Technology, Tehran, Iran*

Bagher Bagherpour - *Department of Mathematics and Cryptography, Malek Ashtar University of Technology, Isfahan, Iran*

Ali Zaghian - *Department of Mathematics and Cryptography, Malek Ashtar University of Technology, Isfahan, Iran*

خلاصه مقاله:

The characterization of the ideal access structures is one of the main open problems in secret sharing and is important from both practical and theoretical points of views. A graph-based ۳-homogeneous access structure is an access structure in which the participants are the vertices of a connected graph and every subset of the vertices is a minimal qualified subset if it has three vertices and induces a connected graph. In this paper, we introduce the graph-based ۳-homogeneous access structures and characterize the ideal graph-based ۳-homogeneous access structures. We prove that for every non-ideal graph-based ۳-homogeneous access structure over the graph G with the maximum degree d there exists a secret sharing scheme with an information rate $\frac{۱}{d+۱}$. Furthermore, we mention three forbidden configurations that are useful in characterizing other families of ideal access structures.

کلمات کلیدی:

Cryptography, Secret sharing, Ideal access structures, Graph-based access structures, ۳-homogeneous access structures