Construction of a Uniform Access Structure Using Minimum Independent Dominating Vertices

Kadhim A. Kadhim
Branch of Applied Mathematics, University of Technology/Baghdad
Email:kadhum.technology@gmail.com
Dr. Nadia M. G. Al-Saidi
Applied Science Department, University of Technology/Baghdad
Dr.Nuha A. Rajab
Applied Science Department, University of Technology/Baghdad

Received on: 7/11/2013 & Accepted on: 24/3/2013

ABSTRACT

The most important technologies in modern society are the information security; it is founded to provide a protection to the transmitted data. Secret sharing scheme is one of the methods designated to protect the secret data. It is a method that allows a secret to be shared among a set of participants in such a way that only qualified subsets of them can recover the secret by pooling their share together, but no less sets can do that. Many mathematical structures are used to create a secret sharing scheme; the one that based on graph access structure is the most widely used structure. In this paper, a new horizon for the construction of the perfect secret sharing schemes of rank 2 and 3 is opened by proposing of a new algorithm to construct a uniform access structure in a connected, simple, undirected, r-regular graph G.This has been done by introducing for the first time the minimum independent dominating set of vertices in a graph. The efficiency of this method is deduced to prove that the proposed method has an improvement over other previous methods.

Keywords: Uniform Access Structure, Minimum Independent Dominating Set (MID), Se Cret Sharing Scheme (SSS), Information Rate, Rank.

بناء بنية وصول منتظمة باستخدام هيمنة الرؤوس المستقلة الصغرى

الخلاصة

تعتبر امن البيانات من اهم التقنيات في المجتمعات الحديثة، لقد وجدت لتوفير الحماية للبيانات المتبادلة. تعتبر برامج مشاركة السرية احد الطرق المصممة لهذا الغرض، حيث يتم من خلالها تقسيم المفتاح الرئيسي الى مجموعة من الاجزاء و توزيعها بين مجموعة من الاشخاص، وباجتماع مجموعة جزيئة مخولة محددة العدد مسبقا، تتمكن من استرجاع المفتاح الرئيس بعد ان يجمعوا حصصهم معا. لكن اية مجموعة بعدد اقل من العدد المحدد لايمكنها ذلك.العديد من التقنيات الرياضية تم توضيفها من اجل تكوين برامج مشاركة السرية، وتعتبر الطرق التي تستند على نظرية البيانات هي اكثر الطرق المعتمدة والاوسع استخداما.

في هذا البحث تم فتح افاق جديدة في بناء برامج مشاركة السرية من الرتبة 2 و3. حيث تم تصميم خوارزميات جديدة لكلا الرتبتين لبناء بنية وصول منتظمة في البيانات المتصلة البسيطةالمنتظمة وغير الموجهه، وذلك من خلال استخدام ولاول مرة خاصية الهيمنة على روؤس البيان. لقد تم تنفيذ الخوارزميات المقترحة، حيث اثبتت النتائج العملية ان الطريقة المقترحة كفوءة واعطت نتائج محسنة نسبة للطرق السابقة المعروفة.