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), Secret Sharing Scheme (SSS), Information Rate, Rank.

بناء بنية وصول منظمة باستخدام هيئة الرؤوس المستقلة الصغيرة

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 وتوزيعها بين مجموعة من الأشخاص، وباختصار مجموعة جزئية مخدولة العدد مسبقا، تتمكن من استرجاع المفتاح الرئيس بعد ان يجمعوا حصصهم معا. لكن اية مجموعة بعدد أقل من العدد المحدد لايمكنها ذلك. العديد من التقنيات الرياضية تم توضيفها من أجل

https://doi.org/10.30684/etj.32.5B.13
2412-0758/University of Technology-Iraq, Baghdad, Iraq
This is an open access article under the CC BY 4.0 license http://creativecommons.org/licenses/by/4.0
INTRODUCTION

The information age brings some unique challenges to society. New technology and new application bring new threats and force us to invent new protection mechanism, which makes the computer security to be reinvented every few years. Due to the recent development of computers and communication networks, a huge amount of digital data can be easily transmitted or stored. The transmitting or storing data in computer networks may easily be eavesdropped or substituted if these data are not secured. Therefore, information security is one of the most important technologies in modern computerized society that founded to provide a protection to the transmitted data.

The public key encryption is a powerful mechanism for protecting the confidentiality of stored and transmitted information [1]. As most cipher are public knowledge; one can easily encrypt and decrypt any message if they know the key(s) used. Therefore, the security of data is fully dependent on the security of the key. For some highly confidential data, it is not always in the best interests to have a single person in control of the key, and thus, the security of the data. This has led to the need for new mechanism that allows keys to be distributed among a group of people according to some policy based on user’s credentials. Hence, the secure key management motivates Adi Shamir and George Blakley in 1979 [2, 3], to discover independently a new mechanism for this purpose called Secret Sharing Scheme (SSS). It is a method for distributing a secret among a set of participants, such that; when a group of \(t\) or more of them cooperate to pool their shares together, they can reconstruct the secret, but no less than \(t\) can do so. Hence, even if \(n-t\) shares are destroyed by enemies then \(K\) can be recovered from the remaining shares. Furthermore, even if an enemy steals \(t-1\) shares, any information about \(K\) does not leak out. This means that the secret sharing scheme is secure against both destruction and stealing.

The general security of the secret sharing scheme is measured by how much information about the secret is given by each of the shares. After the first kind of secret sharing scheme that introduced by Shamir and Blakley in 1979, a considerable attention was given to this subject later on, to propose an efficient secret sharing scheme that has high information rate, which is considered as a measure for the efficiency of such systems. Ito, Saito, and Nishizeki in 1987[4], described a more general method of secret sharing called an access structure. They gave a methodology to realize secret sharing schemes for arbitrary monotone access structure, and shown that the multiple assignment scheme can realize any access structure. At the same period, Benaloh and Leichter in 1988 [5], gave a simpler and more efficient way to realize secret sharing schemes, they proved that there exist an access structure, such that the share given to each participant is from a domain.
larger than the secret. Brickell [6-8], construct some ideal secret sharing scheme for more
general access structure, which included the multilevel access structure proposed by
Simmons. Stinson [9-12] has many contributions on a secret sharing scheme. Numerous
constructions are presented by him; one of them is the scheme that based on graphs ac-
cess structure. He also found their optimal information rate value. H. Sun and S. Shieh
[13-16] propose an efficient construction of perfect secret sharing schemes for the access
structures consisting of the closure of a graph where a vertex denotes a participant, and an
edge denotes a minimal qualified pair of participants.

Other general techniques handling arbitrary access structures are given by C. Blundo,
el. [12,17], M. Iwamoto [18] in 2003. In 2010 H. Sun, etl. in [19], describe a new de-
composition construction for perfect secret sharing schemes with graph access structures.
Recently, in 2012, Hui-Chuan Lu [20] study the access structures based on bipartite
graphs and determines the exact values of the optimal average information rate for some
infinite classes of them.

In addition to this Section that emphasize on the defining the basic concepts for se-
cret sharing scheme, and presenting some of the previous related works, this paper is con-
stit to other 4Sections; they are outlined as follows: The concept of the dominated set in
graph,and an access structure; the most important mathematical models for secret sharing
schemes are reviewed in Section 2. Section 3, describes the proposed algorithm for the
constructions and reconstruction of SSS of rank 2 and 3with illustrated examples. Sec-
tion4, presents the program implementation and some of the experimental result of a se-
cret sharing scheme, in addition to the proving of its efficiency and security in terms of
time and number of vertices. Finally, the paper is concluded in Section 6.

THEORETICAL BACKGROUND

Some background for uniform access structure and domination in graph to unde-
stand the proposed method are given as follows. A more detailed review of the topics can
be found in [11,20-22].

Access Structure

A method of sharing a secret $K$ among a set of $n$ participants, such that, any $t$ of them
can reconstruct the secret $K$, but no group of $t - 1$ or less can do that is called
$(t, n)$-threshold scheme, for any two positive integers $t$ and $n$, where $t \leq n$. The set of all
subset of $P$ is denoted by $\Gamma, \Gamma \subseteq 2^P$. The set is desired to be qualified to compute the se-
cret. It is called an “access structure” or “qualified subsets” or “authorized subsets”. The
basis of $\Gamma$, denoted by $\Gamma_0$, is the family of all minimal qualified subsets. For any $\Gamma_0 \subseteq \Gamma$, the
closure of $\Gamma_0$ is defined as $cl(\Gamma_0) = \{X : \exists X \in \Gamma_0, X \subseteq X \subseteq P\}$. Therefore, an
access structure $\Gamma$ is the same as the closure of its basis $\Gamma_0$. For every $p \in P$, we denote by
$B$ the set of shares for the participantsin subset $B$, where $B \subseteq P$. Therefore, for the access
structure $\Gamma$, a secret sharing scheme is a method of sharing a secret $K$ among a set of $n$
participants in such a way that the following two properties hold [11]:

1. If $B \in \Gamma$, $B$ can compute the master key.
2. If $B \notin \Gamma$, $B$ can obtain no information.

It is clear from the definition that any qualified subset can recover the secret, whereas any
non-qualified subset $B$ has some uncertainty about the secret.

We see that a $(t, n) − threshold$ scheme has an access structure
\[ \Gamma = \{ B \subseteq P; |B| \geq t \} \] 

**Definition 1:** The maximum cardinality of a minimal qualified subset is called the rank of an access structure \( \Gamma \), it is denoted by \( R = |MID| \).

**Definition 2:** If every minimal qualified subset has the same cardinality, in this case an access structure is called uniform. Therefore, a graph-based access structure is a uniform access structure with constant rank.

**Domination in Graph**

For a graph \( G = (V, E) \), where \( V \) is the set of vertices, and \( E = \{(u, v); u, v \in V\} \) is the set of edges, the order of the graph \( G \) is the cardinality of \( V \). A set of vertices \( D \) is a dominating set of vertices in \( G \), if \( N[D] = V \), or equivalently, every vertex in \( V - D \) is adjacent to at least one vertex in \( D \), where \( N[v] = \{u \in V \{u, v\} \in E \} \cup \{v\} \), be an open neighborhood for any vertex \( v \in V \). A dominating set \( D \) is minimal if no proper subset of \( D \) is a dominating set.

A set of vertices in a graph is an independent set denoted by \( I \) if its vertices are adjacent, i.e., for every two vertices \( u \) and \( v \) in \( I \) there is no edge connecting them, whereat most one endpoint of each edge is belonging to \( I \). An independent set is called maximal independent set if adding any extra vertex to the set leads the set to contain an edge. The sets are closely related to independent sets is called dominating set, where an independent set is also a dominating set if and only if it is a maximal independent set. The size of the smallest maximal independent set is the size of the smallest independent dominating set. It is called the independent domination number of a graph \( G \). The minimum independent dominating set \( MID \) is a variation in which we need to find minimum dominating set whose vertices form an independent set. In this work, such type of dominating set is used in the construction for the secret sharing scheme.

**The proposed construction algorithm for rank 2, and 3**

A novel construction algorithm for a perfect secret sharing scheme with an access structure of rank 2 and 3 is proposed. It’s based on the same concepts given by H. Sun [16]. This algorithm consists of three parts as follows:

1. **The initialization phase:**
   (a) Given a simple, \( r - \) regular graph \( G = (V, E) \), with \( V = \{v_1, v_2, ..., v_n\} \). Let \( P = \{p_1, p_2, ..., p_n\} \) be the set of participants corresponding to the set of vertices \( V \).
   (b) Construct \( \Gamma_0 \) by computing all \( MID \) in \( G \), such that \( \Gamma_0 = \{MID; \forall \} \).
   (c) All the computation is done over \( GF(q) \), where \( q \) is a prime, \( R2 \), \( q \geq n \).
   (d) Let \( K \) be a secret, such that, \( K_i \) is taken randomly from \( GF(q^{\mid\text{MID}\mid}) \).

2. **The Construction Phase:**
   (a) Select a polynomial \( f(x) = (\sum_{j=0}^{\mid\text{MID}\mid-1} K_{j+1}x^j) \mod q \).
   (b) Select random numbers over \( GF(q) \).
Theorem 1: For any set of participant $H$, if $A \in H$ and $B \subseteq A \subseteq P$, then $B$ obtained no information regarding to the master key of the constructed secret sharing scheme for the access structure based on a graph $G$. In another word, any unqualified subset has no information about the secret.

Proof: Let $B \in H$ be a subset of participants, the proof contains two cases according to the rank, and as follows:

R2. $r_1, r_2, \ldots, r_n$.
R3. $r_1, r_2, \ldots, r_{2n}$.

c) Compute $y_i$, such that, $y_i = f(i) \bmod q, i = 1, 2, \ldots, n$.

d) R3 case,

- Decompose the graph $G$ into $n$ subgraphs $G_i$, where $V(G_i) = \{V \setminus N[v_i] : i = 1, 2, \ldots, n\}$.
- Assume that there exists a secret sharing scheme realizing $G_i$, in which the secret is $(r_i + y_i, r_{n+i} + y_{n+i})$ and the share of participant $p_j$ is $S_j(G_i)$.

The share of participant $p_i$, $i = 1, 2, \ldots, n$:

R2 $S_i = < a_{i_1}, \ldots, a_{i_t}, \ldots, a_{i_n} >$, Where,$1 \leq t \leq n$, and

- $a_{i_t} = r_i \bmod q = i$,
- $a_{i_t} = (r_i + y_i) \bmod q 
eq \text{iand}(P_i, P_t) \in \Gamma_0$, and
- $a_{i_t} = \text{isemptyift} \neq \text{iand}(P_i, P_t) \notin \Gamma_0$. 

R3 $S_i = < a_{i_1}, a_{i_2}, \ldots, a_{i_t}, \ldots, a_{i_n} >$, where $1 \leq t \leq n$,

- $a_{i_t} = S_i(G_i) \neq \text{iandp_i} \in V(G_t)$,
- $a_{i_t} = \text{isemptyotherwise}$. 

The secret can be reconstructed when the authorized participants pool their shares together. The reconstruction phase could be expressed as follow:

II. The reconstruction phase:

The secret can be reconstructed by getting $|\text{MID}|$ or more $y_i$’s. This can be done by combining their values together.

R2. There exists $p_i, p_j \in \Gamma_0, i \neq j$, participant $p_i$ owns $a_{i,i} = r_i$ and $a_{i,j} = r_i + y_j$, and participant $p_j$ owns $a_{j,i} = r_j$ and $a_{j,j} = r_j + y_i$. Thus, participant $p_i$ and participant $p_j$ recover $y_i$ and $y_j$, and recover $f(x)$ and the secret $K$.

R3. There exists $p_i, p_j, p_k \in \Gamma_0, i \neq j \neq k$, participant $p_i$ owns $r_i$, $r_{n+i}$, $S_i(G_j)$ and $S_i(G_k)$, participant $p_j$ owns $r_j$, $r_{n+j}$, $S_j(G_i)$ and $S_j(G_k)$, and participant $p_k$ owns $r_k$, $r_{n+k}$, $S_k(G_i)$ and $S_k(G_j)$. Therefore, from $S_j(G_i)$ and $S_k(G_i)$, they can recover $r_i + y_i, r_{n+i} + y_{n+i}$ because $(p_j, p_k)$ dominate the subgraph $G_i$. From $S_i(G_j)$ and $S_k(G_j)$, they can recover $r_j + y_j, r_{n+j} + y_{n+j}$ because $(p_i, p_k)$ dominate the subgraph $G_j$. Finally, from $S_i(G_k)$ and $S_j(G_k)$, they can recover $r_k + y_k, r_{n+k} + y_{n+k}$ because $(p_i, p_j)$ dominate the subgraph $G_k$. Thus, participants, $p_i, p_j$ and $p_k$ can recover $y_i, y_{n+i}, y_j, y_{n+j}, y_k$ and $y_{n+k}$, and can then recover $f(x)$ and secret $K$.

In other words, any set not belongs to MID can obtain no information about the secret key, as proved in the following theorem.
I. When the rank, \( R = |\text{MID}| = 2 \) for any pair of participants \( p_i, p_j \in B (i \neq j), (p_i, p_j) \notin \Gamma_0 \). \( B \) is assumed can recover \( y_i \). Therefore, there exists participant \( p_i \) owns \( a_{i,j} = r_i \) and participant \( p_j \) owns \( a_{j,i} = r_i + y_i \). Thus, \( (p_i, p_j) \in \Gamma_0 \). This is a contradiction to the condition \( (p_i, p_j) \notin \Gamma_0 \). Hence, \( B \) cannot recover any \( y_i \), or in other words, \( B \) obtains no information about secret \( K \).

II. When the rank, \( R = |\text{MID}| = 3 \), let \( B \notin \Gamma \) be a subset of participants. Therefore, there does not exist any three participants \( p_i, p_j, p_k \) in \( B \), such that \( \{p_i, p_j, p_k\} \in \Gamma_0 \). Assume that \( B \) can recover \( y_i \), hence there exists participant \( p_i \) that owns \( r_i \), and participants \( p_j \) and \( p_k \) that recover \( r_i + y_i \). Thus, \( (p_j, p_k) \) dominate the graph \( G_i \) and \( \{p_i, p_j, p_k\} \notin \Gamma_0 \). This is a contradiction of the condition \( \{p_i, p_j, p_k\} \notin \Gamma_0 \). Hence, \( B \) obtains no information about \( y_i \), for \( 1 \leq i \leq 2n \), and about secret \( K \).

To explain the algorithm we illustrate the following examples; the construction of perfect secret sharing scheme for uniform access structure of rank 2, and rank 3 respectively:

**Example 1:**

Let \( G \) be a simple, \( 2 - \)regular \( \) graph of order 6 as shown in Figure (1) such that the rank, \( R = |\text{MID}| = 2 \).

![Figure (1) 2-regular simple graph of order 6.](image)

Let \( P = \{p_1, p_2, p_3, p_4, p_5, p_6\} \) be the set of participants corresponding to the vertices of the graph \( G \), where \( \Gamma_0 = \{(p_1, p_6), (p_2, p_5), (p_3, p_4)\} \), and the master key of the secret sharing scheme for the access structure based on the graph \( G \) given by \( K = (K_1, K_2) = (12, 27) \) that are randomly selected over \( GF(q^2) \), where \( q \) is a prime and \( q \geq n \). Let \( q = 7 \), so \( K_1 \) and \( K_2 \) is taken randomly over \( GF(49) \).

\[
f(x) = \sum_{i=0}^{1} (K_i x^{i-1}) \mod q = (K_1 + K_2 x) \mod q = (12 + 27x) \mod 7.
\]

\[
y_i = f(i) \mod q, \text{ for } i = 1, \ldots, 6.
\]

\[
y_1 = f(1) \mod 7 = (12 + 27(1)) \mod 7 = 4,
\]

\[
y_2 = f(2) \mod 7 = (12 + 27(2)) \mod 7 = 3,
\]

\[
.\]

\[
y_6 = f(6) \mod 7 = (12 + 27(6)) \mod 7 = 6.
\]

Such that \( y_i = \{4, 3, 2, 1, 0, 6\} \).

The dealer selects 6 random numbers, \( r_1, \ldots, r_6 \), over \( GF(7) \), let \( r = \{5, 3, 6, 2, 1, 4\} \). The share of participant \( p_i \) is given by:

\[
S_i = <a_{i,1}, \ldots, a_{i,t}, \ldots, a_{i,n}>, \text{ Where } 1 \leq t \leq n, \quad a_{i,t} = r_i \mod q, t = i,
\]
\[ a_{i,t} = (r_t + y_t) \mod q_i \text{ if } i \neq t \text{ and } (P_i, P_t) \in \Gamma_0, \text{ and} \]
\[ a_{i,t} \text{ is empty if } i \neq t \text{ and } (P_i, P_t) \notin \Gamma_0. \] ... (2)

Now, applying equations (2) to obtain:

\[ S_1 = \langle a_{1,1}, a_{1,2}, ..., a_{1,6} \rangle = \langle r_1, r_2, r_3, r_4, r_5, y_6 \rangle. \]
\[ S_2 = \langle a_{2,1}, a_{2,2}, ..., a_{2,6} \rangle = \langle r_2, r_3, r_4, r_5, r_6, y_5 \rangle. \]
\[ S_6 = \langle a_{6,1}, a_{6,2}, ..., a_{6,6} \rangle = \langle r_1 + y_1, r_2, r_3, r_4, r_5, r_6 \rangle. \]

Such that the share for each participant \( p_i, i = 1, 2, ..., 6 \); is
\[ \langle 5, r_2, r_3, r_4, r_5, 10 \rangle, \langle r_1, 3, r_4, r_5, 1, 6 \rangle, \langle r_6, r_2, 2, 1, 6, 1 \rangle, \langle 9, r_3, 1, 6, 4 \rangle, \text{ respectively}. \]

The secret can be reconstructed when the authorized participants pool their share together, let \( A = \{p_2, p_5\} \), where \( p_2 \) and \( p_5 \) corresponding to the vertices in \( G \) forms a minimum independent dominating set, it is clearly that \( A \subseteq \Gamma_0 \subseteq P \) can reconstruct the secret as follows:

Since \( p_2 \) owns \( r_2 = 3 \) and \( y_5 = 1 \), \( p_5 \) owns \( r_5 = 1 \) and \( y_2 = 6 \), then, when they pool their shares together they can reconstruct \( y_2 = 3 \) and \( y_5 = 0 \). Now, using Lagrange interpolation polynomial [22], to find \( f(x) = 12 + 27x \), and the master secret key is \( K = (K_1, K_2) = (12, 27) \).

The construction of perfect secret sharing scheme for uniform access structure of rank 3 based on a simple, \( r- \) regular graph \( G \), illustrated in the following example:

**Example 2:**
Let \( G \) be a simple, 3-regular graph of order \( n = 12 \), such that rank, \( R = |\text{MID}| = 3 \).

![Figure (2,a) 3-regular simple graph of order 12.](image-url)

Let \( \Gamma_0 = \{(p_1, p_5, p_9), (p_2, p_6, p_{10}), (p_3, p_7, p_{11}), (p_4, p_8, p_{12})\} \). Define \( G_i \), for \( 1 \leq i \leq n \), as the graph with vertices \( V(G_i) \) and edges \( E(G_i) \), such that \( V(G_i) = \{V \setminus N[v_i] ; i = 1, 2, ..., n\} \) and \( E(G_i) = \{E \setminus \{(v_i, v_j) ; i = 1, 2, ..., n\} \}. \)

![Figure (2,b) Decomposition graph of order 12.](image-url)
Let $P = \{p_1, p_2, ..., p_{12}\}$ be the set of participants corresponding to the vertices of a graph $G$. Let the master key of the secret sharing scheme for the access structure based on the graph $G$ is given by $K = (K_1, K_2, ..., K_6) = (12, 27, 33, 21, 57, 9)$ that are randomly selected over $GF(q^6)$, where $q$ is a prime s.t. $q \geq 2n$. Let $q = 27$, so $K$ is taken randomly over $GF(27^6)$.

$$f(x) = \left( \sum_{i=0}^{5} K_{i+1}x^i \right) \mod q = (12 + 27x + 33x^2 + 21x^3 + 57x^4 + 9x^5) \mod 27$$

$$y_i = f(i) \mod q, \text{ for } i = 1, \ldots, 24.$$  
$$y_1 = f(1) \mod 27 = 24,$$  
$$y_2 = f(2) \mod 27 = 0,$$  
$$y_{24} = f(24) \mod 27 = 12.$$  
Such that $y_1 = \{24, 0, 12, 15, 9, 12, 16, 18, 12, 24, 0, 12, 15, 9, 12, 16, 18, 12, 24, 0, 12, 15, 9, 12\}$. 

The dealer selects $2n$ random numbers, $r_1, \ldots, r_{2n}$, over $GF(q)$. Let the random numbers are $\{5, 13, 26, 19, 12, 24, 0, 12, 15, 2, 17, 22, 14, 6, 3, 16, 11, 1, 24, 4, 8, 17\}$. 

Since the secret sharing scheme that realizing $G_i$ is of rank 2, the dealer gives $(r_i + y_i, r_{n+i} + y_{n+i})$ to the dominated vertices in $G_i$. 

So, 

$$S_1 = < r_1, r_{13}, a_{1,1}, a_{1,2}, a_{1,3}, a_{1,4}, a_{1,5}, a_{1,6}, a_{1,7}, a_{1,8}, a_{1,9}, a_{1,10}, a_{1,11}, a_{1,12} >$$  
$$S_2 = < r_2, r_{14}, a_{2,1}, a_{2,2}, a_{2,3}, a_{2,4}, a_{2,5}, a_{2,6}, a_{2,7}, a_{2,8}, a_{2,9}, a_{2,10}, a_{2,11}, a_{2,12} >$$  
$$\vdots$$  
$$S_{12} = < r_{12}, r_{24}, a_{12,1}, a_{12,2}, a_{12,3}, a_{12,4}, a_{12,5}, a_{12,6}, a_{12,7}, a_{12,8}, a_{12,9}, a_{12,10}, a_{12,11}, a_{12,12} >$$  

Then, 

$$S_1 = < r_1, r_{13}, \ldots, S_1(G_3), S_1(G_4), S_1(G_5), S_1(G_6), \ldots, S_1(G_8), S_1(G_9), S_1(G_{10}), S_1(G_{11}), \ldots >$$  
$$S_2 = < r_2, r_{14}, \ldots, S_2(G_4), S_2(G_5), S_2(G_6), S_2(G_7), \ldots, S_2(G_9), S_2(G_{10}), S_2(G_{11}), S_2(G_{12}) >$$  
$$\vdots$$  
$$S_{12} = < r_{12}, r_{24}, \ldots, S_{12}(G_2), S_{12}(G_3), S_{12}(G_4), S_{12}(G_5), \ldots, S_{12}(G_7), S_{12}(G_8), S_{12}(G_9), S_{12}(G_{10}), \ldots >$$  

The secret can be reconstructed when the authorized participants pool their share together. Let $A = \{p_2, p_6, p_{10}\}$, it is clearly that $A \subseteq \Gamma_0 \subseteq P$ can reconstruct the secret as follows:

Since $p_2$ owns $r_2, r_{14}$, $S_2(G_6)$ and $S_2(G_{10})$, $p_6$ owns $r_{18}$, $S_6(G_2)$ and $S_6(G_{10})$, and $p_{10}$ owns $r_{10}, r_{22}$, $S_{10}(G_2)$ and $S_{10}(G_6)$. Hence, from $S_6(G_2)$ and $S_{10}(G_2)$, they can recover $(r_2 + y_2, r_{14} + y_{14})$, because $p_6$ and $p_{10}$ dominate the subgraph $G_2$. From $S_2(G_6)$ and
Construction of a Uniform Access Structure Using Minimum Independent Dominating Vertices

$S_{10}(G_6)$ they can recover $(r_6 + y_6, r_{18} + y_{18})$, because $p_2$ and $p_{10}$ dominate the subgraph $G_6$. Finally from $S_2(G_{10})$ and $S_6(G_{10})$ they can recover $(r_{10} + y_{10}, r_{22} + y_{22})$, because $p_2$ and $p_6$ are dominate the subgraph $G_{10}$. Therefore,

$r_2 + y_2 = 13 \Rightarrow y_2 = 0$

$r_6 + y_6 = 35 \Rightarrow y_6 = 12$

$r_{10} + y_{10} = 45 \Rightarrow y_{10} = 24$

$r_{14} + y_{14} = 31 \Rightarrow y_{14} = 9$

$r_{18} + y_{18} = 28 \Rightarrow y_{18} = 12$

$r_{22} + y_{22} = 10 \Rightarrow y_{22} = 15$

By using Lagrange’s interpolation polynomial method [23], $f(x)$ and secret $K$ can be recovered.

1-Implementation and analysis

This section describes the implemented of the proposed scheme. Some experimental results are presented and analyzed also. The proposed scheme was implemented by a computer with the specification, CPU CORi5 with 4 GB Ram under the operating system Windows 8 using Visual Basic.NET 2008. Two user interfaces have been built, one for construction and the other for reconstruction for both rank 2&3. Some samples of user interfaces windows are shown in Figures 3-6. After input the number of participants and the secret key, the values $K_i$, $q$, $y_i$ and $r_i$, is computed, where each participant got his/her own share after inputting the dominating matrix, as illustrated in Figure 4. In the reconstruction face, when we want to reconstruct the key, when the participants input their indexes, the program asks about their shares, whereas, if the participants input wrong authorized number, then the program is terminated with error sentence. Finally, when the authorized participants pool their shares together, the program computes the secret key.

Figure (3) Construction of proposed S.S.S of rank 2.

Figure (4) Construction of proposed S.S.S of rank 3.
Experimental results

Applying the program on some graphs using H. Sun method and our proposed method, some experimental results for rank 2 and 3 is obtained. These values are compared to prove the efficiency in terms of execution time as shown in table 1 and 2. These tables show that our proposed method is more efficient than H. Sun method, that proved previously to be an efficient method and has improvement upon Stinson’s methods. The tables are drawn as charts Figure (7-10) to show the differences in a more clarified way. This big different in time because of the reducing in $\Gamma_0$ that is directly proportional with the increase in the number of vertices, that lead to a reduction in the number of shares distributed to each participant. From Figures 6 and 7 it is obvious that the differences between our proposed method and H. Sun method for construction and reconstruction phases are very small, whereas, Figures 9 and 10 shows big differences for rank 3. After implementing of our method and H. Sun method under the same environment, we conclude that the execution time taken in all phases is better than H. Sun as have been shown in Tables (1, 2) and Figures (7 to 10).
For rank 2:

Table (1)  Construction and reconstruction times in a millisecond (Rank2).

<table>
<thead>
<tr>
<th>No. Vertices</th>
<th>Construction time (\textit{ms})</th>
<th>Reconstruction time (\textit{ms})</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>H. Sun</td>
<td>Our</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>2950.044</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15.78</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>3132.103</td>
</tr>
<tr>
<td></td>
<td></td>
<td>18.55</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>3240.064</td>
</tr>
<tr>
<td></td>
<td></td>
<td>21.63</td>
</tr>
</tbody>
</table>

Table (2)  Construction and reconstruction times in a millisecond (Rank3).

<table>
<thead>
<tr>
<th>No. Vertices</th>
<th>Construction time (\textit{ms})</th>
<th>Reconstruction time (\textit{ms})</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>H. Sun</td>
<td>Our</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>6731.323</td>
</tr>
<tr>
<td></td>
<td></td>
<td>721.780</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>6952.413</td>
</tr>
<tr>
<td></td>
<td></td>
<td>728.334</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>7247.175</td>
</tr>
<tr>
<td></td>
<td></td>
<td>736.638</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>7685.332</td>
</tr>
<tr>
<td></td>
<td></td>
<td>745.550</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>8101.432</td>
</tr>
<tr>
<td></td>
<td></td>
<td>755.812</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>8841.156</td>
</tr>
<tr>
<td></td>
<td></td>
<td>767.798</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>9643.667</td>
</tr>
<tr>
<td></td>
<td></td>
<td>770.009</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>10055.791</td>
</tr>
<tr>
<td></td>
<td></td>
<td>784.561</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>11056.052</td>
</tr>
<tr>
<td></td>
<td></td>
<td>799.335</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>12060.564</td>
</tr>
<tr>
<td></td>
<td></td>
<td>815.498</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>13071.334</td>
</tr>
<tr>
<td></td>
<td></td>
<td>831.701</td>
</tr>
<tr>
<td></td>
<td>18</td>
<td>14082.423</td>
</tr>
<tr>
<td></td>
<td></td>
<td>852.669</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td>15094.001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>877.478</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>17000.452</td>
</tr>
<tr>
<td></td>
<td></td>
<td>900.880</td>
</tr>
</tbody>
</table>

Figure (7) Construction phase for rank 2.
Construction of a Uniform Access Structure Using Minimum Independent Dominating Vertices

Figure (8) Reconstruction phase for rank 2.

Figure (9) Construction phase for rank 3.

Figure (10) Reconstruction phase for rank 3.
CONCLUSIONS
This paper has focused on an important cryptographic primitive called a secret sharing scheme. Our main contribution is obtained by using for the first time the independent dominating set of vertices in a regular graph. Satisfactory results have been obtained upon applying these new techniques; some useful features are pointed out, such as; the construction of a secret sharing scheme is possible, and has an improvement over other classical methods. In most of the previous proposed decomposition construction, the minimum authorized subset is constructed by a set of edges in a graph $G$, which is considered as small share in the construction of large schemes, whereas, in our scheme, the minimum authorized subset represents the minimum independent dominating set of vertices in the graph $G$.The constructed secret sharing scheme is perfect, where the set of vertices of the graph represents the set of participants.An algorithm for the construction and reconstruction phase for ranks 2&3 is constructed and implemented, where the experimental result is drawn to prove the efficiency of this method over other previous methods in terms of the time complexity factor.

REFERENCES


