N.M.G. Al-Saidi
Applied Sciences Dept.,
University of Technology,
Baghdad, Iraq.
nadiamg08@gmail.com

M.M. Abdulhadi
Applied Sciences Dept.,
University of Technology,
Baghdad, Iraq.
mohammedmuthna@gmail.com

Received on: 30/03/2016
Accepted on: 29/09/2016

E–Voting System based on Secret Sharing Scheme

Abstract- *The electoral process is considered as one of the important and sensitive operations that take place from time to time in all countries of the world and need to be protected. The importance of the electronic voting came because, it provides a maintaining for the secrecy of the vote, as well as, the speed, accuracy and credibility of the vote counts. This is due to the growing of the technology that always needs for electronic process and for new approaches to achieve high security. In this paper, a new E-voting system is designed based on secret sharing scheme. The new protocol is implemented to show its efficiency in terms of computational time and cost.*

Keywords- *E – voting; secret sharing scheme; uniform access structure; rank*

How to cite this article: N.M.G. Al-Saidi and M.M. Abdulhadi "E–Voting System based on Secret Sharing Scheme," *Engineering and Technology Journal*, Vol. 35, Part B, No. 1, pp. 13-18, 2017.

1. Introduction

Protecting the confidential data is a necessary aspect emerges nowadays with the growing needs for electronic process. Electronic- voting is one of the important processes that need to be protected. The distribution of shares and the computation of votes for each candidate are sensitive issue that needs to be secure in such a way that each casted vote can be modified and tracked by the particular candidate only, where the vote representation in the E-voting process is as bitwise pattern.

In this work, secret sharing scheme is used to design a secure E-voting system, such that, the voter's identity is protected, where each casted vote is divided into shares to be distributed to multiple parties. By using a secret sharing scheme that based on edge dominating set in a given graph, the random share given to each participant according to one of the elements in the minimum edge dominating set, and do not give any information about the voter, which resulted in a perfectly secure system.

The proposed secret sharing scheme that is based on minimum edge dominating set is applied for the E-voting system, such that, this system is represented as a regular graph where each candidate represents an edge in the graph.

To ensure secure data storage from eavesdropping and substituting, and to overcome the threats of destruction attack and troubles of storage devices is achieved by making as many copies of the secret as possible. Having many copies of the secret leads to leak out, which necessitate that, the number of the copies to be as small as possible. To achieve this goal, a new protocol is proposed independently in 1979 by Shamir [1] and Blakley [2] called secret sharing scheme. It is a method to split secret information S into n pieces called shares $y_1, \dots, y_n$, each of them has no information about the secret S, but collecting several numbers of them may reconstruct the secret S. It allows the secret S to be shared among a set of participants P [3]. A secret sharing scheme is called threshold scheme [1], if all groups of participants of at least some fixed size are qualified to reconstruct the secret. A special participant is called the dealer is responsible of choosing the secret S, he is also responsible for distributing the shares.

The collection of subsets of participants that used to reconstruct the secret is called access structure Γ. It is called monotone if for $A \in \Gamma$ and $A \subseteq B \subseteq P$ then $B \in \Gamma$. A minimal qualified subset $X \in \Gamma$ is a subset of participants such that $Y \notin \Gamma$ for all $Y \subseteq X, Y \neq X$. The basis of Γ denoted by Γ_0, is the family of all minimal qualified subset. Let 2^P denotes the collection of all subsets of P. For any $\Gamma_0 \subseteq \Gamma$, the closure of Γ_0 is defined as $cl(\Gamma_0) = \{X' : \exists X \in \Gamma_0, X \subseteq X' \subseteq P\}$. Therefore, an access structure Γ is the same as the closure of its basis Γ_0, $\left(cl(\Gamma_0)\right)$.

The important relation between an access structure and secret sharing scheme motivates many researchers to propose different approaches to use suitable access structure in order to obtain a perfect and an efficient secret sharing scheme (see, [4, 5, and 6]). The approach that investigates an access structure based on graph theory considered as an attractive; it is called graph access structure. In this approach, the vertices and the edges of the graph represent the participant, and the access structure (see, [5, 6, 7, and 8]), where the access structure Γ

https://doi.org/10.30684/etj.35.1B.3
2412-0758/University of Technology-Iraq, Baghdad, Iraq

of the graph G is decomposed into a number of subgraphs, in such a way that at least λ subgraphs of them should contain each edge of Γ. This idea is called λ-decomposition, it was introduced by Blundo *et al.* [5] and Brickell and Stinson [9]. It also leads to an increase in the number of subgraphs that increased with the increment of the number of vertices and edges (participants), which resulted in an exponential increment of the construction time.

In 2016, a new secret sharing scheme is proposed by Alsaidi et al. [10], it is based on dominating set of edges as an access structure. The classical approaches that based on graph theory used to consider the set of vertices in the graph as a set of participants. In [10], the set of participants $P = \{p_1, p_2, \dots, p_n\}$ corresponds to the set of edges of the graph $G, E = \{e_1, e_2, \dots, e_n\}$, and the minimum edge dominating set in G represent the minimum access structure Γ_0.

The current work is organized as follows: In Section 2, related work of E – voting is abstracted. In Section 3, two types of secret sharing scheme based on graph access structure is presented. The proposed E – voting system is presented in section 4. System implementation is given in section 5. The paper finally concluded in section 6.

2- Related work

The first E-voting system based on a secret sharing scheme was introduced by Benaloh [11] in 1987. A voting system based on multiple key ciphers was proposed by Boyd et al., in 1990 [12]. In 1992, Iverson and Kenneth [13] proposed a secure election system based on secret sharing technique and zero knowledge protocol. In 1993, Fujioka et al. [14] presented a practical secret voting scheme for large scale elections. In 1999, Schoenmakers [15] presented a secure E-voting system based on a publicly verifiable secret sharing scheme. In 2007, Iftene et al. [16] proposed a general secret sharing based on Chinese remainder theorem with application to e-voting. In 2010, Damagaard et al. [17] proposed a generalization of the Pailliar's cryptosystem and its application to the voting schemes. In 2014, Chen et al. [18] suggested a scheme based on discrete logarithm problem and secret sharing. In 2014, Pan et al. [19] introduced an improved scheme with high privacy and confidentiality.

3-Secret Sharing Scheme based on graph access structure

In this section, two types of secret sharing scheme based on graph access structure is presented, they are:

I.Sun et al. Scheme [20]

A new construction of a perfect secret sharing scheme of rank m is proposed, such that $P= \{p_1,p_2,\dots,p_n\}$ is a set of participants and Γ is a uniform access structure of rank m on those participants, where Γ_0 is the basis of Γ. The decomposition of Γ_0 is Γ_i's, for $1\leq i\leq n$ where $\Gamma_i = \{X: X \in \Gamma_0 \; and \; p_i \in X\}$.

Thus, $\Gamma = cl(\Gamma_0) = cl(\Gamma_1) \cup \dots \cup cl(\Gamma_n)$, then $\Gamma_i^* = \{X: X \cup \{p_i\} \in \Gamma_i\}$ id defined, where each $cl(\Gamma_i*)$ is a uniform access structure of rank m-1. The secret K=($k_1,k_2,\dots,k_m\}$, where each k_i, $1\leq i\leq m$ is taken randomly over $GF(q^{h(m-1)})$, which is considered as the space of the secret. A polynomial $f(x)$ of degree $m.h(m$-1)-1with coefficients K is selected by a dealer to compute y_i=$f(i$-1)mod q, for i=1,…$n.h(m$-1). Thus, the secret can be recovered if one can get $m.h(m$-1) or more y_i's. If one has no knowledge of any y_i, no information about the secret can be obtained. Random numbers $r_1,r_2,\dots,r_n$ are also selected by the dealer over $GF(q^{h(m-1)})$. They presumed that there exists a secret sharing scheme realizing $cl(\Gamma_i^*)$, such that, the secret is r_i+y_i and the share of participant p_j is $S_j(\Gamma_i^*)$, which is given by:

$$S_i = \langle R_i, S_i(\Gamma_1^*), \dots, S_i(\Gamma_{i-1}^*), S_i(\Gamma_{i+1}^*), \dots, S_i(\Gamma_n^*)\rangle.$$

The reconstruction of the secret is done when the authorized participants collect their share together.

II.Alsaidi et al. Scheme [21]

Another secret sharing scheme is proposed by represented the set of participants by the set of vertices in graph G, but the minimum access structure is represented by the minimum dominating set of vertices (*MID)*. The scheme is summarized as follows:

The set of vertices V=$\{v_1,v_2,\dots,v_n\}$ corresponds to the set of participants P=$\{p_1,p_2,\dots,p_n\}$, and the set of all *MID* in *G* is corresponds to the minimum access structure Γ_0. They decomposed the graph *G* into n– subgraphs $G_i = (V_i, E_i)$, i=1,2,…,n, in such a way that $V_i = \{V \backslash N[v_i]\}$. The set Γ_0 is also decomposed into $n \; \Gamma_i's$ where $\Gamma_i = \{MID \in \Gamma_0,$ $where \; p_i \in MID\}$ They defined $\Gamma_i^* = \{X: X \cup \{p_i\} \in \Gamma_i\}$.

The coefficients of the polynomial *f(x)* are chosen randomly over $GF(q^{(m-1)!})$ and used to represent the secret K=($k_1,k_2,\dots,k_m\}$. Hence, $f(x) = (k_1 x^{m-1} + k_2 x^{m-2} + \cdots + k_m)$. The secret K can be reconstructed by getting m or more y_i*'s,* where y_i*'s* are computed using y_i=$f(i)$ mod q, i=1,2,…,n, and the share for each participant p_i is calculated after selecting r random numbers $r_1,r_2,\dots,r_n$ by the dealer such that:

$S_i = \langle r_i, S_i(\Gamma_1^*), \ldots, S_i(\Gamma_{i-1}^*), S_i(\Gamma_{i+1}^*), \ldots, S_i(\Gamma_n^*)\rangle$.
When the authorized participants pool their share together, the secret can be reconstructed.

```
E-voting algorithm
Input: $M$, the number of candidates
$N$, number of voters
$K \in GF(q^2)$
Output: number of votes for each candidate
Set $CC(M), Y, V = 0$
  for $i = 1\ To\ M$
    for $j = 1\ To\ N$
        $b = \left|\frac{ln(N)}{ln(2)}\right| + 1$
        $Y = K * i + 2^{b(V-1)}$
    End $j$
  end $i$
Calculate $\Gamma_0$    % using Gama 0 algorithm given in [10]
Let e $\in \Gamma_0$
Let $A = 0$
      for $i = 1\ To\ |\varpi|$
    $Eu = 1$ , $Ed = 1$
  $j = 1$  while $j < G$ do
    if $j \neq i$ then $Eu = Eu * e(j)$
    $Ed = Ed * (e(i) - e(j))$
    $j = j + 1$
    end
      $A = A + CC(e(i)) * \frac{Eu}{Ed}$
      end $i$
  for $i = M$ down to 2
    set $AT, V(M) = 0$
    $AT = \left\lceil\frac{A}{2^{b(i-1)}}\right\rceil$
    $V(i) = AT$
    $A = A - AT * 2^{b(i-1)}$
  end $i$
$V(1) = A$
   end
```

4- The Proposed E – Voting system

In traditional elections, there are things that must be present, such as democracy, privacy and so on, which ensures free elections and a safe. For this, we need to use the electronic voting, because it ensures all of the above**.** The electoral process is considered as one of the important and sensitive operations that attract many researchers to work on. The importance of the electronic voting came because, it provides what we have mentioned earlier in terms of maintaining the secrecy of the vote, as well as, the speed, accuracy and simplicity of the vote counts. This is due to the growing needs for technology that need for new approaches to achieve high security. In the proposed algorithm for E-voting, a secret sharing scheme that based on minimum edge dominating set of a graph is used for this purpose. It is explained in the following algorithm:

This algorithm can be illustrated through the following three phases:

I.Key generation phase

In this phase, we choose the number of candidate M and the number of voters N and then use the edge dominating algorithm given in [10] to find Γ_0.

II.The decomposition phase (encoding)

To encoding the votes, we first choose a value of k over $GF(q^2)$ where $q \geq m, m$ is the number of edges, construct the polynomial $f(x) = kx + v_i$, where v_i is the value of the vote, such that; the value of v_i depends on the number of voters and the number of candidates.

III.The reconstruction phase (decoding)

For each voter, the share for all candidates is computed by $y_{ij} = f(j)$, then the share is sent to the collection center (CC), after that the shares of each candidate are summed in the collection center.

In the construction part, we use the sum in the collection center and applied the Lagrange interpolation formula to obtain the polynomial *f(x)*, and finally, from its constant term, the number of votes for each candidate is found.

5. System Implementation

In the following we explain how the process of voting is implemented and we compute the votes for each candidate. Let the number of voters equal 10 and the number of candidates 10, to find the votes of each candidate, we apply algorithm 1. Since we have 10 candidates, then a graph of regular two with 10 edges is constructed as shown in Figure 1, the rank of the graph is 4 and the minimum edge dominating set Γ_0 is:

$$\Gamma_0 = \left\{ \begin{array}{c} (e_1, e_3, e_5, e_8), (e_1, e_3, e_6, e_8), (e_1, e_3, e_6, e_9), (e_1, e_4, e_6, e_8), \\ (e_1, e_4, e_6, e_9), (e_1, e_4, e_7, e_9), (e_2, e_4, e_6, e_9), (e_2, e_4, e_7, e_9), \\ (e_2, e_4, e_7, e_{10}), (e_2, e_5, e_7, e_9), (e_2, e_5, e_7, e_{10}), (e_2, e_5, e_8, e_{10}), \\ (e_3, e_5, e_7, e_{10}), (e_3, e_5, e_8, e_{10}), (e_3, e_6, e_8, e_{10}) \end{array} \right\}$$

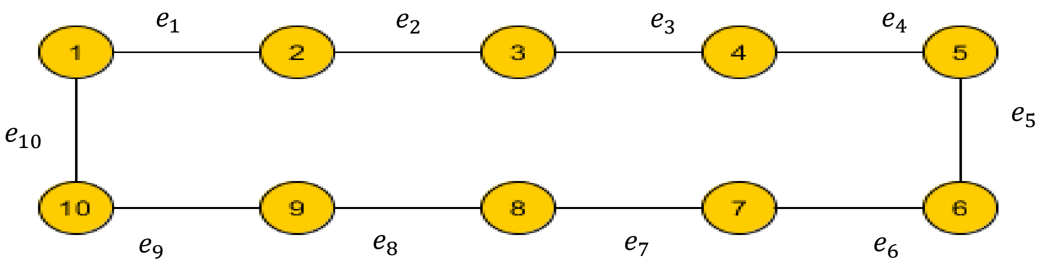
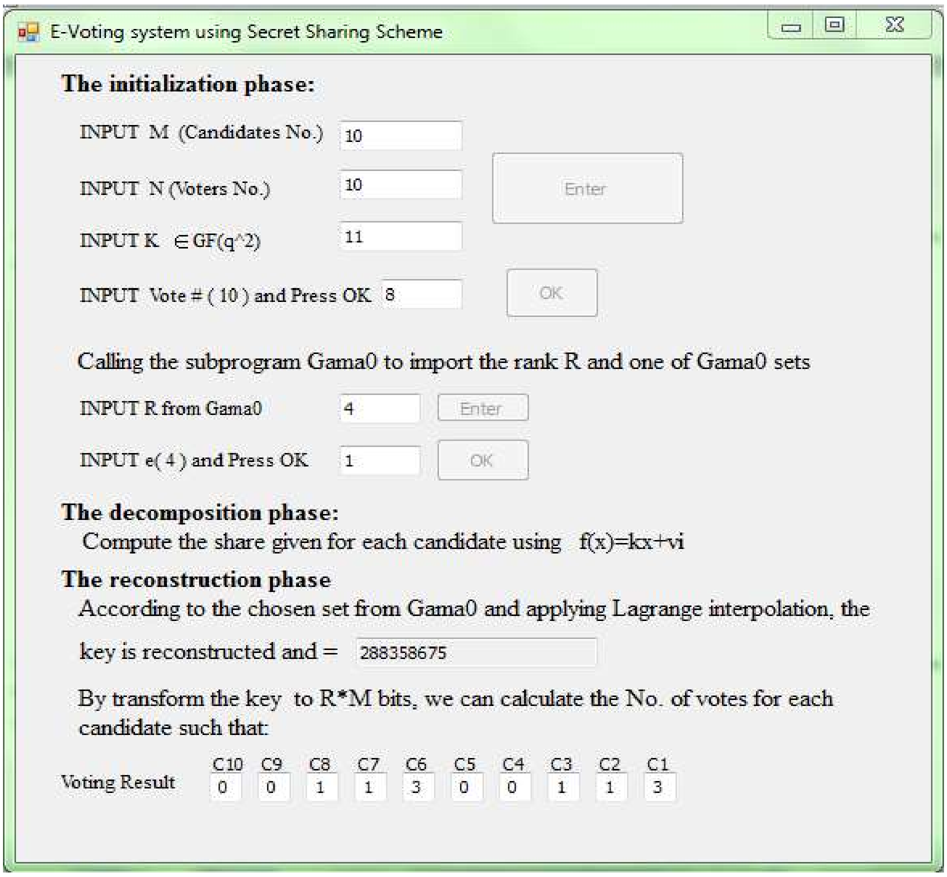


Figure 1: The 2 – regular graph



E-Voting system using Secret Sharing Scheme

The initialization phase:

INPUT M (Candidates No.) 10

INPUT N (Voters No.) 10

INPUT K ∈GF(q^2) 11

Enter

INPUT Vote # (10) and Press OK 8

OK

Calling the subprogram Gama0 to import the rank R and one of Gama0 sets

INPUT R from Gama0 4 Enter

INPUT e(4) and Press OK 1 OK

The decomposition phase:

Compute the share given for each candidate using f(x)=kx+vi

The reconstruction phase

According to the chosen set from Gama0 and applying Lagrange interpolation, the key is reconstructed and = 288358675

By transform the key to R*M bits, we can calculate the No. of votes for each candidate such that:

	C10	C9	C8	C7	C6	C5	C4	C3	C2	C1
Voting Result	0	0	1	1	3	0	0	1	1	3

Figure 1: The user interface of the proposed E – voting system

Therefore, $\mathrm{m} = 10$ (the number of candidates) and $\mathrm{n} = 10$ (the number of voters). Let $\mathrm{k} = 11 \in \mathrm{GF}(\mathrm{q}^2)$, where $\mathrm{q} \geq 2\mathrm{m}$.

$\mathrm{f(x)} = \mathrm{kx} + \mathrm{v_i} = 11\mathrm{x} + \mathrm{v_i}$, where $\mathrm{v_i}$ is the value of vote for candidate i

The 40 bit vote pattern $\mathrm{b_{39}b_{38}b_{37}b_{36} \dots b_3b_2b_1b_0}$ is initially set to 0. When a voter votes for candidate 1, bit $\mathrm{b_0}$ is set to 1, similarly for candidate 2, bit $\mathrm{b_4}$ is set to 1 and so on for candidate 10, bit $\mathrm{b_{36}}$ is set to 1.

$\mathrm{y_{i,j}} = \mathrm{f(j)}$, $\mathrm{CC_j} = \mathrm{y_{ij}}$.

The first voter votes for candidate 1, then $\mathrm{v_1} = 1$.

$\mathrm{y_{1,1}} = \mathrm{f(1)} = 11(1) + 1 = 12 \Rightarrow \mathrm{CC_1} = 12.$

$\mathrm{y_{1,2}} = \mathrm{f(2)} = 11(2) + 1 = 23 \Rightarrow \mathrm{CC_2} = 23.$

$\mathrm{y_{1,3}} = \mathrm{f(3)} = 11(3) + 1 = 34 \Rightarrow \mathrm{CC_3} = 34.$

$\mathrm{y_{1,4}} = \mathrm{f(4)} = 11(4) + 1 = 45 \Rightarrow \mathrm{CC_4} = 45.$

$\mathrm{y_{1,5}} = \mathrm{f(5)} = 11(5) + 1 = 56 \Rightarrow \mathrm{CC_5} = 56.$

$\mathrm{y_{1,6}} = \mathrm{f(6)} = 11(6) + 1 = 67 \Rightarrow \mathrm{CC_6} = 67.$

$\mathrm{y_{1,7}} = \mathrm{f(7)} = 11(7) + 1 = 78 \Rightarrow \mathrm{CC_7} = 78.$

$\mathrm{y_{1,8}} = \mathrm{f(8)} = 11(8) + 1 = 89 \Rightarrow \mathrm{CC_8} = 89.$

$\mathrm{y_{1,9}} = \mathrm{f(9)} = 11(9) + 1 = 100 \Rightarrow \mathrm{CC_9} = 100.$

$\mathrm{y_{1,10}} = \mathrm{f(10)} = 11(10) + 1 = 111 \Rightarrow \mathrm{CC_{10}} = 111.$

If voter 2 votes for candidate 3, then $v_2 = 256$, and $y_{2,1}$ to $y_{2,10}$ are computed following the same calculation doing above for the first voter.

If voter 3 votes for candidate 1, then $v_3 = 1$, and, $y_{3,1}$ to $y_{3,10}$ are computed.

If voter 4 votes for candidate 2, then $v_4 = 16$, and $y_{4,1}$ to $y_{4,10}$ are computed.

If voter 5 votes for candidate 1, then $v_5 = 1$, and $y_{5,1}$ to $y_{5,10}$ are computed.

If voter 6 votes for candidate 6, then $v_6 = 1048576$, and $y_{6,1}$ to $y_{6,10}$ are computed.

If voter 7 votes for candidate 8, then $v_7 = 268435456$, and $y_{7,1}$ to $y_{7,10}$ are computed.

If voter 8 votes for candidate 6, then $v_8 = 1048576$, and $y_{8,1}$ to $y_{8,10}$ are computed.

If voter 9 votes for candidate 7, then $v_9 = 16777216$, and $y_{9,1}$ to $y_{9,10}$ are computed.

If voter 10 votes for candidate 6, then $v_{10} = 1048576$, and $y_{10,1}$ to $y_{10,10}$ are computed.

Now, to find the sum of all collection centers which is denoted by SCC_j, we have :

$\mathrm{SCC_1} = 288358785$, $\mathrm{SCC_2} = 288358895$, $\mathrm{SCC_3} = 288359005$, $\mathrm{SCC_4} = 288359115$, $\mathrm{SCC_5} = 288359225$,$\mathrm{SCC_6} = 288359335$, $\mathrm{SCC_7} = 288359445$, $\mathrm{SCC_8} = 288359555$, $\mathrm{SCC_9} = 288359665$, $\mathrm{SCC_{10}} = 288359775$.

Let, the qualified subset from Γ_0 is $\mathrm{A} = \{\mathrm{e_1}, \mathrm{e_3}, \mathrm{e_5}, \mathrm{e_8}\}$. Then by applying Lagrange interpolation on the set A, we have the following polynomial

$$\mathrm{f(x)} = \frac{288358785(\mathrm{x}-3)(\mathrm{x}-5)(\mathrm{x}-8)}{(1-3)(1-5)(1-8)} + \frac{288359005(\mathrm{x}-1)(\mathrm{x}-5)(\mathrm{x}-8)}{(3-1)(3-5)(3-8)} + \frac{288359225(\mathrm{x}-1)(\mathrm{x}-3)(\mathrm{x}-8)}{(5-1)(5-3)(5-8)} + \frac{288359555(\mathrm{x}-1)(\mathrm{x}-3)(\mathrm{x}-5)}{(8-1)(8-3)(8-5)}$$

$$= \frac{288358785(\mathrm{x}^3 - 3\mathrm{x}^2 - 5\mathrm{x}^2 + 15\mathrm{x} - 8\mathrm{x}^2 + 24\mathrm{x} + 40\mathrm{x} - 120)}{-56} + \frac{288359005(\mathrm{x}^3 - \mathrm{x}^2 - 5\mathrm{x}^2 + 5\mathrm{x} - 8\mathrm{x}^2 + 8\mathrm{x} + 40\mathrm{x} - 40)}{20} + \frac{288359225(\mathrm{x}^3 - \mathrm{x}^2 - 3\mathrm{x}^2 + 3\mathrm{x} - 8\mathrm{x}^2 + 8\mathrm{x} + 24\mathrm{x} - 24)}{-48} + \frac{288359555(\mathrm{x}^3 - \mathrm{x}^2 - 3\mathrm{x}^2 + 3\mathrm{x} - 5\mathrm{x}^2 + 5\mathrm{x} + 15\mathrm{x} - 15)}{105}$$

$$= 0\mathrm{x}^3 + 0\mathrm{x}^2 + 110\mathrm{x} + 288358675$$

Decoding the constant term 288358675 we obtain,

0000 0000 0001 0001 0011 0000 0000 0001 0001 0011

Each 4 bit represents the vote's number for the candidates respectively.

6- Conclusion

The voting scheme in this paper is a new method that serves to compute the individual vote for each candidate. It provides good security and efficiency when the number of voters is small. The property of the graph theory called edge domination is used to compute the access structure which represents the minimum edge dominating set in the graph; it is used to compute the number of vote for each candidate.

References

[1] Shamir. "How to Share a Secret". Communications of the ACM, Vol. 22, No. 11, pp. 612-613, 1979.

[2] G. R. Blakley. "Safeguarding Cryptographic Keys". In Proceedings of American Federation of Information Processing Societies 1979 National Computer Conference, Vol. 48, pp. 313-317, 1979.

[3] E.F Brickell and D.M. Davenport. "On the Classification of Ideal Secret Sharing Schemes". J. Cryptology, Vol.4, pp. 123-134, 1991.

[4] Beimel, T. Tassa, and E. Weinreb," Characterizing ideal weighted threshold secret sharing ", SIAM J. Discrete Math, Vol. 22, pp. 360–397, 2008.

[5] Blundo, A. De Santis, D.R. Stinson, and U. Vaccaro, "Graph Decomposition and Secret Sharing Schemes", J. Cryptol., Vol. 8, No. 1, pp. 39–64, 1995.

[6] G. Di Crescenzo and C. Galdi," Hypergraph Decomposition and Secret Sharing", Discrete Appl. Math., Vol. 157, pp. 928–946, 2009.

[7] M. Ito, A. Saito, and T. Nishizeki, "Secret Sharing Scheme Realizing General Access Structure", Proc. IEEE Globecom, Vol. 87, pp. 99–102, 1987.

[8] M. Liu, L. Xiao, and Z. Zhang, "Multiplicative Linear Secret Sharing Schemes Based

on Connectivity of Graphs", IEEE Trans. Inform. Theory, Vol. 53, pp. 3973–3978, 2007.

[9] E.F. Brickell and D.R. Stinson," Some Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes", J. Cryptol., Vol. 5, pp. 153–166, 1992.

[10] N. M. G. Al-Saidi, M. Muthna, and Mustafa Saed. Secret Sharing Scheme Based on Edge Dominating Set. The 2016 International Conference on Security and Management (SAM'16), July 25-27, 2016.

[11] J. Benaloh,: Verifiable Secret-ballot Elections", PhD Thesis, Yale University, 1987.

[12] C. Boyd, "A New Multiple Key Cipher and an Improved Voting Scheme", In Advances in Cryptology Eurocrypt 89, Vol. 434, pp. 617–625, Springer, 1990.

[13] R. Kenneth Iversen," A Cryptographic Scheme for Computerized General Elections", In Advances in Cryptology CRYPTO91, Vol. 576, pp. 405–419. Springer, 1992.

[14] Fujioka, Tatsuaki Okamoto and Kazuo Ohta, "A Practical Secret Voting Scheme for Large Scale Elections", In Advances in Cryptology Auscrypt'92,Vol. 718, pp. 244–251. Springer, 1993.

[15] Schoenmakers, "A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting", In Advances in Cryptology CRYPTO 99, Vol. 1666, pp. 148–164. Springer, 1999.

[16] S. Iftene, "General Secret Sharing based on the Chinese Remainder Theorem with Applications in Evoting", Electronic Notes in Theoretical Computer Science, Vol. 186, pp. 67–84, 2007.

[17] Ivan Damgard, Mads Jurik and Jesper Buus Nielsen, A Generalization of Pailliers Public-key System with Applications to Electronic Voting, International Journal of Information Security, Vol. 9, No.6, pp. 371–385, 2010.

[18] Chin-Ling Chen, Yu-Yi Chen, Jinn-Ke Jan and Chih-Cheng Chen, A Secure Anonymous E-voting System based on Discrete Logarithm Problem, Applied Mathematics & Information Sciences, vol. Vol. 8, No.5, 2014.

[19] H. Pan, Edwin Hou and Nirwan Ansari, "Enhanced Name and Vote Separated E-voting System: An E-voting System that Ensures Voter Confidentiality and Candidate Privacy", Security and Communication Networks, Vol. 7. pp. 2335 – 2344, 2014.

[20] N. M. Al – Saidi , N.A. Rajab, M. R. Md. Said and K.A. Kadhim. "Perfect Secret Sharing Scheme Based on Vertex Domination Set ". International Journal of Computer Mathematics. Vol. 92, No. 9, 2015.

[21] H. Sun and S. Shieh, "Recursive constructions for perfect secret sharing schemes", Comput. Math. Appl. Vol. 37, pp. 87–96, 1999.