Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.2 Year 2018
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

A New Electronic Voting Protocol Using Secret Sharing Based on Set of Path Domination

Samaa F. Ibraheem

Applied Sciences Department, University of Technology, Baghdad, Iraq

samaafuad@gmail.com

Recived : 24\12\2017 **Revised : 8\1\2018** **Accepted : 10\1\2018**

Available online : 17 /2/2018

DOI: 10.29304/jqcm.2018.10.2.362

Abstract

For secret electronic voting protocol we always need a secure system. Secret sharing scheme are proved to be safe guarding through distributing the input key to number of participants then reconstructing the shares through a secure process. In this paper, the set of dominating paths in special graph is used to share the votes among a set of candidates, such that, each candidate represents an edge in the graph. Based on this new technique, we have shown that it is secure and confidential. The efficiency of the new protocol is demonstrated in terms of time and cost.

Keywords: Electronic voting systems; secret sharing scheme; set of dominating path.

Mathematics subject classification: 94-xx, 05-xx.

1. Introduction

The theory of domination is considered as one of the major research area in graph theory. Historically, the first domination type problems came from chess. In 1958, Berge[1] was the first how introduced the concept of domination in graph. After that this concept takes high popularity by many mathematicians and scientists, and it is utilized in many applications. Various types of domination of a graph have been defined and studied by many researchers. In the appendix of Haynes [2] more than 75 models are listed.

Technical systems like computer communication network, radio station and traffic management system have a structure like a graph. These systems needs many requirements to achieve the security, speed, accuracy and privacy, for example, we need a minimum number of computers to control the communication network, these can be performed through the dominating set in grapg. Electronic voting system is one of the technical systems that required many efforts to minimize the cost and time while maintaining security and confidentiality, all these objective are achieved by secret sharing schemes (SSS).

Secret sharing was introduced in 1979 by Shamir [3] and Blakley [4], it has important applications in cryptography as a protocol. A secret sharing scheme is a method to keep safe a secret value (key) by partitioned it into shares and distributes it among several participants in such a way that only confirmed qualified subsets of participants can regain the secret by pooling their shares together. This distribution increases the safety, reliability, security and convenience.

In 1987, Benelux[5] was introduce the first E-voting system that based on secret sharing scheme. E-voting systems are fundamentally different but any system should guarantee the privacy and security to protect the confidential data. In other words, it must be guaranteed that no one can discover the identity of the voter .

During twenty years ago, various techniques are used in E-voting systems that based on multiple key cipher[6], secret sharing technique and zero knowledge protocol[7], publicly verifiable secret sharing scheme[8], chinese remainder theorem[9] and some other techniques. Recently, many researchers pay attention to E-voting systems that based on secret sharing scheme and discrete logarithm problem[10]. In 2014, Pan et al.[11] introduced an improved scheme in the same field with high privacy and confidentiality.

The classical approaches that based on graph theory used to consider the set of vertices in the graph as a set of participants. In 2016, Al saidi et al.[12] proposed a new system based on secret sharing scheme that depends on the edge dominating sets as an access structure by representing the participants as a set of edges in the graph.

In this work, secret sharing scheme that based on path dominating set in a given graph is used to design a new 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 and each vote is represented as bitwise pattern according to number of voters. The random share given to each participant according to one element in the minimum path dominating set, without giving any information about the personality of the voter, that resulted in a perfectly secure system. The proposed protocol of electric voting is based on secret sharing scheme depending on the set of minimum dominating paths, such that, this system is represented as a special graph (C_n) which is a cycle of order n, where each candidate (participant) represents an edge in the graph.

This paper includes four additional sections ordered as follows: section 2, contains basic concepts in graph theory and secret sharing scheme; in section 3, the proposed system is introduced; implementation and analysis is given in section 4; finally, our work is concluded in section 4.

2. Basic concepts

A major concepts regarding to topics presented in this work are abstracted as an overview in this section, for more details, we refer the reader to see [1, 13].

a) Graph theory

Let $G(V,E)$ be a finite, undirected, simple, connected graph. The order and the size of G is the number of vertices V (i.e. $|G|=n$), and the number of edges E respectively. The degree of a vertex v in G is the number of edges incident on v denoted by $deg(v)$. When all vertices of the graph has the same degree, it is called regular, otherwise it is irregular. An open neighbor set, $N(u)=\{v|(u,v)\in E\}$, is the set of vertices that are neighbor to u. A closed neighbor set, $N[u]=N(u)\cup\{u\}$, is the set of neighbors of u in addition to u itself. A path is an alternative sequence of vertices and edges, beginning at a vertex and ending at another one, and it doesn't visit any vertex more than one time. A cycle is just like a path except that is starts and ends at the same vertex. The length of a path (or cycle) is defined as the number of edges in it. A cycle graph with n vertices is a graph consists of a single cycle and denoted by C_n. A subset H of a graph G is denoted by $H\leq G$ with $V(H)\subseteq V(G)$ and $E(H)\subseteq E(G)$.

A subset D of vertices in a graph G is a dominating set if every vertex not in D has a neighbor in D. if the subgraph induced by D is connected, then D is called a connected dominating set. A path P is called dominating path if every vertex outside P has a neighbor in P. There is an efficient algorithm for finding the set of dominating paths in a graph [14].

b) Secret sharing scheme

In secret sharing scheme the secret information is distributed and shared among the participants in such a way that only appointed sets of participants can reconstructed the secret, besides that, no one of them has any information about the secret S. For more details see [15].

In the domain of secret sharing scheme that based on graph access structure we'll introduce two types which are:

i. Sun et al. Scheme [16]: It is summarized as follows:

1) Let $P=\{p_1,p_2,\ldots,p_n\}$ be 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.

2) The decomposition of Γ_0 is Γi's, for $1\leq i\leq n$, where $\boldsymbol{\Gamma_i=\{X: X\in \Gamma_0 \text{ and } p_i\in X\}}$. Thus, $\boldsymbol{\Gamma = cl(\Gamma_0)=cl(\Gamma_1)\cup\ldots\cup cl(\Gamma_n)}$, then $\boldsymbol{\Gamma_i^*=\{X: X\cup\{p_i\}\in\Gamma_i\}}$ is defined, where each cl(Γi*) is a uniform access structure of rank m -1. The secret $K=(k_1,k_2,\ldots,k_m)$, 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.

3) A polynomial f(x) of degree m.h(m -1)-1 with coefficients K is selected by a dealer to compute $y_i=f(i-1) \bmod q$, for $i=1,\ldots n.h(m-1)$. If one has no knowledge of any y_i, no information about the secret can be obtained.

4) Random numbers $r_1, r_2, \ldots, r_n$ 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: $S_i = \langle R_i, S_i(\Gamma_1^*), \ldots, S_i(\Gamma_{i-1}^*), S_i(\Gamma_{i+1}^*), \ldots, S_i(\Gamma_n^*)\rangle$. The reconstruction of the secret is done when the authorized participants collect their share together.

ii. Al saidi et al. Scheme[17, 18]: It is summarized as follows:

1) The set of vertices $V=\{v_1,v_2,\ldots,v_n\}$ in graph G corresponds to the set of participants $P=\{p_1,p_2,\ldots,p_n\}$, while minimum access structure Γ_0 is represented by the minimum dominating set of vertices (*MID)*
2) The graph G is decomposed into n–subgraphs $G_i = (V_i, E_i)$, i=1,2,…,n, where $V_i = \{V \backslash N[v_i]\}$. The set Γ_0 is also decomposed into n $\Gamma_i's$ where $\Gamma_i = \{MID \in \Gamma_0,\ where\ p_i \in MID\}$ and the set $\Gamma_i^* = \{X: X \cup \{p_i\} \in \Gamma_i\}$.
3) The coefficients of the polynomial $f(x) = (k_1x^{m-1} + k_2x^{m-2} + \cdots + k_m)$ are chosen randomly over $GF(q^{(m-1)!})$ and used to represent the secret $K=(k_1,k_2,\ldots,k_m\}$.
4) 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 $r_1,r_2,\ldots,r_n$ 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.

Fuad et al. [14] proposed an optimal scheme based on minimum set of dominating path in cycle graph C_n. That scheme represented the minimum access structure Γ_0 by the minimum set of dominating paths in C_n. Based on this contribution, an efficient electronic voting protocol is proposed in this work.

3. E – Voting system

The electoral process is considered as one of the important and sensitive operations that attract many researchers to work on. The proposed system for E-voting focus on choosing the access structure Γ_0 to achieve high security. For this purpose, a secret sharing scheme based on minimum path dominating set of a graph C_n is used, and an algorithm that works for m candidate and n voters is designed also which is works on a bitwise-pattern representation votes.

The access structure Γ_0 is a set consist of n dominating paths each of length (n-3) for more details see [14]. The electoral process using the proposed system can be summarized in the following algorithm in three steps:

Algorithm 1: The proposed E-voting system

Input: m=the number of candidates, n=the number of voters, Input $k \in GF(p^2)$

Output: The number of votes for each candidate

Step1: key generation:

1-Take the number of candidates m and the number of voters n

2- Find Γ_0 directly using theorem 2 in [14] after representing each candidate as a vertex in graph C_m, so we have m sets each has (m-3) candidates.

All computation is done over $GF(p)$, where p is a prime, $p \geq m$

Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.2 Year 2018
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

Step2: The decomposition:

1- Construct the code for each candidate, which is represented as bitwise pattern according to the number of voters and the number of candidates.
2- Chose a value of k over $GF(p^2)$ to encoding the votes.
3- Construct the polynomial $f(x) = kx + v_i$, where v_i is the value of the vote.

Step3: The reconstruction:

1- Compute the shares for all candidates by $y_{ij}=f(j)$ for each voter, then send them to the collection center (CC).
2- Find the sum SCC_j of collection center, then apply Lagrange interpolation on any dominating set belongs to Γ_0 to obtain $f(x)$.
3- The number of votes for each candidate is founded from the constant term of the polynomial $f(x)$.

Example:

Let m=5 and n=7 so the related graph will be C_5 shown in Figure 1, then apply path dominating algorithm to find $P_1=\{e_1,e_2\}$, $P_2=\{e_2,e_3\}$, $P_3=\{e_3,e_4\}$, $P_4=\{e_4,e_5\}$, $P_5=\{e_5,e_6\}$

Hence $\Gamma_0 = =\{P_1,P_2,\dots,P_5\}$

Figure 1: The cycle Graph C_5

Let $k = 13 \in GF(p^2)$, where $p \geq m$. $f(x) = kx + v_i = 13x + v_i$, where v_i is the value of the vote for candidate i. Since we have 7 candidates, then we need at least 3 bit to represent code for each candidate. The 21 bit vote pattern $a_{20}a_{19}a_{18} \dots a_3a_2a_1a_0$ is initially set to 0. When a voter votes for candidate 1, bit a_0 is set to 1, similarly for candidate 2, bit a_3 is set to 1 and so on for candidate 7, bit a_{18} is set to 1.

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

Now if the first voter votes for candidate 1, then $v_1 = 1$.

$$y_{1,1} = f(1) = 13(1) + 1 = 14 \Rightarrow CC_1 = 14.$$

$$y_{1,2} = f(2) = 13(2) + 1 = 27 \Rightarrow CC_2 = 27.$$

$$y_{1,3} = f(3) = 13(3) + 1 = 40 \Rightarrow CC_3 = 40.$$

$$y_{1,4} = f(4) = 13(4) + 1 = 53 \Rightarrow CC_4 = 53.$$

$$y_{1,5} = f(5) = 13(5) + 1 = 66 \Rightarrow CC_5 = 66.$$

If voter 2 votes for candidate 3, then $v_2 = 64$, and $y_{2,1}$ to $y_{2,5}$ are computed

If voter 3 votes for candidate 1, then $v_3 = 1$, and, $y_{3,1}$ to $y_{3,5}$ are computed.

If voter 4 votes for candidate 2, then $v_4 = 8$, and $y_{4,1}$ to $y_{4,5}$ are computed.

If voter 5 votes for candidate 3, then $v_5 = 64$, and $y_{5,1}$ to $y_{5,5}$ are computed.

If voter 6 votes for candidate 3, then $v_6 = 64$, and $y_{6,1}$ to $y_{6,5}$ are computed.

If voter 7 votes for candidate 4, then $v_7 = 512$, and $y_{7,1}$ to $y_{7,5}$ are computed.

Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.2 Year 2018
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

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

$SCC_1 = 805$, $SCC_2 = 896$, $SCC_3 = 987$, $SCC_4 = 1078$, $SCC_5 = 1169$.

Let, the qualified subset from Γ_0 is $A = \{e_1, e_2\}$. Then by applying Lagrange interpolation on the set A, we have the following polynomial

$$f(x) = \frac{805(x-2)}{(1-2)} + \frac{896(x-1)}{(2-1)}$$
$$= 91x + 714$$

Decoding the constant term 714 in binary, we obtain, 000 001 011 001 010. Each 3 bit represents the vote's number for the candidates respectively.

4. Implementation and analysis

The implementation of the algorithm is done in matlab. A flowchart for algorithm 1 is introduced in Figure 2. Table 1 gives some details about the construction of the code for each candidate and the calculation of theirs values v_i. Table 2 shows the shares generation for each voter. All results are based on example 1. In Table 3, shows comparison explains the running time required to election with different number of voters and same number of candidates:

Table 1: Representation of votes

Candidate	**Candidate's code (Bitwise representation)**	**Vote's value (v_i)**
1	000 000 000 000 001	2^0=1
2	000 000 000 001 000	2^3=8
3	000 000 001 000 000	2^6=64
4	000 001 000 000 000	2^9=512
5	001 000 000 000 000	2^{12}=4096

Table 2: Share Generation

Collection center	*CC 1*	*CC 2*	*CC 3*	*CC4*	*CC5*
Voter1	14	27	40	53	66
Voter2	77	90	103	116	129
Voter3	14	27	40	53	66
Voter4	21	34	47	60	73
Voter5	77	90	103	116	129
Voter6	77	90	103	116	129
Voter7	525	538	551	564	577
SCC	805	896	987	1078	1169

Table 3: Running time (1)

candidates	voters	Running time
5	7	0:0:001
5	10	0:0:001
5	50	0:0:002
5	100	0:0:002

Table 3: Running time (2)

candidates	voters	Running time
5	50	0:0:001
10	50	0:0:001
20	50	0:0:002
30	50	

Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.2 Year 2018
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

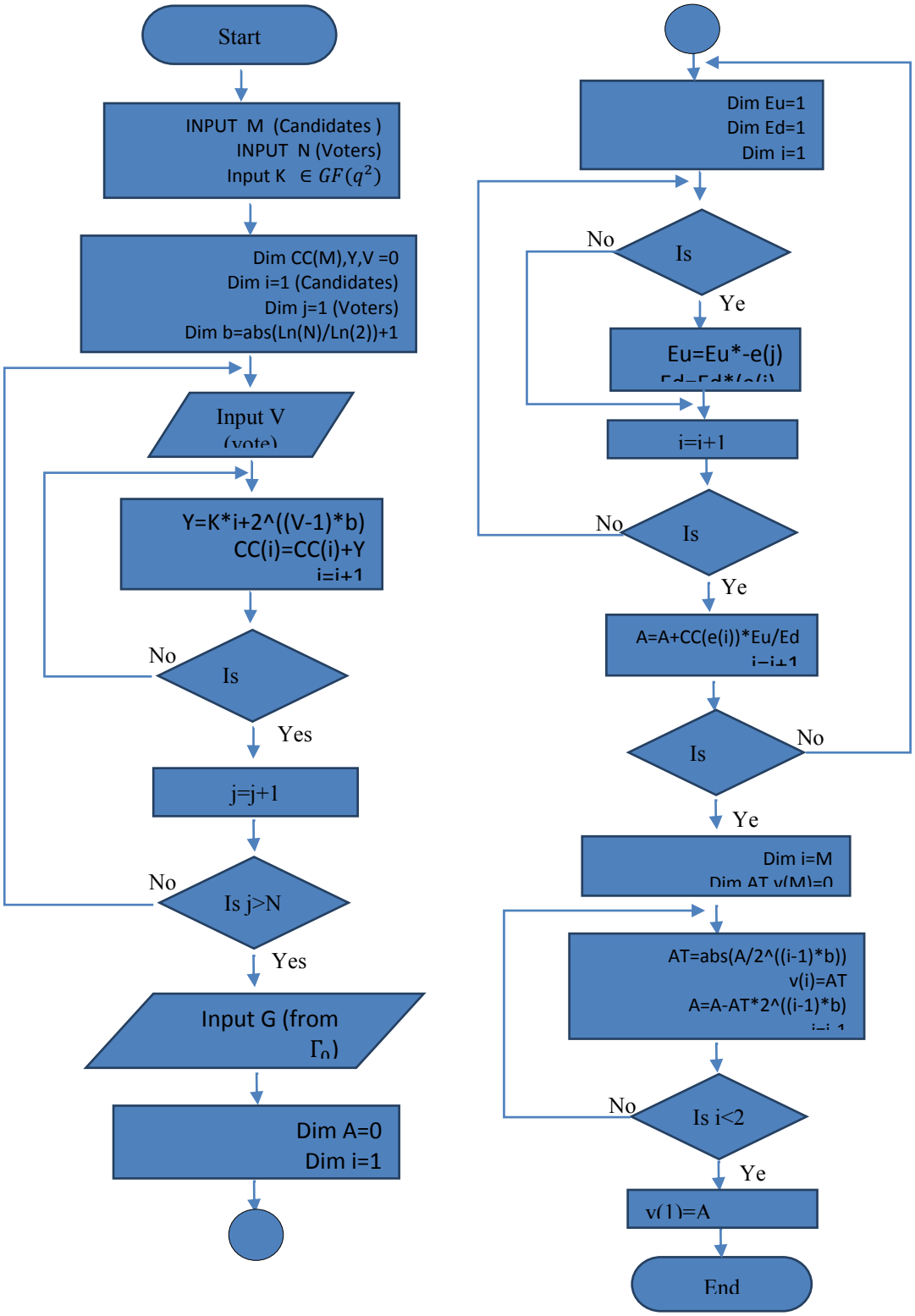

Figure 2: E-voting flowchart

5. Conclusion

In this paper the new E- voting system depends on secret sharing scheme is proposed, where a set of dominating paths in special graph is used to share the votes among a set of candidates. The efficiency of the system depends on the number of voters, as well as, it is active when the number of candidates is not large that decrease the running time and cost. To provide more security, the shares can be sent to the collection center using different secure channels.

References

1- C. J. Berge, "Theory of Graphs and its Applications", Methuen, London, 1962.
2- T. W. Haynes, S. T. Hedetniemi and P. J. Slater, "Fundamentals of Domination in Graphs", Marcel Dekker, Inc., New York, 1998.
3- A. Shamir, "How to Share a Secret", Communications of the ACM, Vol. 22, No. 11, pp. 612-613, 1979.
4- G. R. Blakley, "Safeguarding Cryptographic Keys", In Proceedings of American Federation of Information Processing Societies, National Computer Conference, Vol. 48, pp. 313-317, 1979.
5- J. C. Benaloh, "Verifiable Secret-ballot Elections", PhD Thesis, Yale University, USA, 1987.
6- C. Boyd, "A new multiple key cipher and an improved voting scheme". In Advances in CryptologyEUROCRYPT89. pp. 617–625. Springer, 1990.
7- K. R. Iversen, "A cryptographic scheme for computerized general elections", In Advances in CryptologyCRYPTO91. pp. 405–419. Springer, 1992.
8- B. Schoenmakers. "A simple publicly verifiable secret sharing scheme and its application to electronic voting", In Advances in Cryptology—CRYPTO '99, Lecture Notes in Computer Science, Springer-Verlag, Vol. 1666, pp. 148-164, 1999.
9- S. Iftene, "General secret sharing based on the Chinese remainder theorem with applications in e-voting", Electronic Notes in Theoretical Computer Science, Vol. 186: pp. 67–84, 2007.
10- C. L. Chen, Y. Y. Chen, J. K. Jan, and C. C. Chen, "A secure anonymous e-voting system based on discrete logarithm problem", Applied Mathematics & Information Sciences, Vol.8, No.5, 2014.
11- H. Pan, E. Hou and N. 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.
12- 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.
13- F. Harary. "Graph theory". Addison-Wesley Publishing Co., Reading Mass.-Menlo Park, Calif.-London, 1969.
14- S. F. Ibraheem, S. S. Hasan and N. M. Al-Saidi, "Optimal Secret Sharing Scheme via path Domination Sets". The 23rd Scientific Specialist Conference of Education al-Mustansiriya, Iraq, pp. 237-242, 2017
15- M. Ito, A. Saito, and T. Nishizeki, "Secret Sharing Scheme Realizing General Access Structure", Proc. IEEE Globecom, Vol. 87, pp. 99–102, 1987.

16- H. Sun and S. Shieh, "Recursive constructions for perfect secret sharing schemes", Comput. Math. Appl. Vol. 37, pp. 87–96, 1999.
17- 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, pp.1755-1763, 2015.
18- N. M. Al-Saidi, N.A. Rajab, and K.A. Kadhim. "Construction of a Uniform Access Structure Using Minimum Independent Dominating Vertices", Engineering and Technology Journal, Vol.32, Part (B), No. 5, pp.966-979, 2014.

بروتوكول تصويت الكتروني جديد باستخدام نظام مشاركة السرية بالاعتماد على مجموعة الدروب المهيمنة

سماء فؤاد ابراهيم
قسم العلوم التطبيقية ـ الجامعة التكنولوجية
samaafuad@gmail.com

المستخلص :

في بروتوكولات التصويت الإلكتروني السري نحن دائما بحاجة إلى نظام آمن. وقد ثبت أن نظام مشاركة السرية يوفر حماية جيدة من خلال توزيع مفتاح الإدخال على عدد من المشاركين ثم إعادة بناءه من خلال عملية آمنة. في هذا البحث تم استخدام مجموعة الدروب المهيمنة في بيان معين لمشاركة الأصوات بين مجموعة من المرشحين، بحيث يمثل كل مرشح حافة في ذلك البيان. استناداً على هذا البروتوكول الجديد برهنّا انه مأمون وسري. وقد تم اثبات كفاءة البروتوكول الجديد من خلال عامل الوقت والكلفة.

الكلمات المفتاحية: انظمة التصويت الألكتروني . نظام مشاركة السرية ، مجموعة الدروب المهيمنة.