Int. J. Nonlinear Anal. Appl. 12 (2021) No. 1, 821-829
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2021.4937

New formula to calculate the number of designs in RADG cryptosystem

Laith M Kadhum[a,1], Ahmad Firdaus[a,*], Mohamad Fadli Zolkipli[b], Luay Saferali[a,1], Mohd Faizal Ab Razak[a]

[a]*Faculty of Computing College of Computing and Applied Sciences, Universiti Malaysia Pahang 26600 Pekan, Pahang Darul Makmur*
[1]*University of Kufa, Najaf, Iraq*
[b]*School of Computing, UUM College Arts Sciences, Universiti Utara Malaysia, 06010 UUM Sintok, Kedah Darul Aman, Malaysia*

(Communicated by Madjid Eshaghi Gordji)

Abstract

Reaction automata direct graph (RADG) is a new technique that uses the automata direct graph method to represent a certain design for encryption and decryption. Jump states are available in the RADG design that enables the encipher to generate different ciphertexts each time from the same plaintext and wherein not a single ciphertext is related to a certain plaintext. This study created a matrix representation for RADG designs that allows the calculation of the number of cases (F_Q)mathematically possible for any design of the set Q. F_Q is an important part of the function $\mathrm{F(n, m, \lambda)}$ that calculates the total number of cases of a certain design for the values $Q, R, \sum, \psi, J$ and T. This paper produces a mathematical equation to calculate F_Q.

Keywords: RADG, Cryptography, Block Cipher, Keyless, Graph Theory

1. Introduction

Cryptography is the science of encryption and decryption and uses many mathematical concepts, such as algebra, number theory, graph theory and combinatorial mathematics [1]. Many relationships that exist between combinatorial mathematics and theoretical computer science enumerate and count

*Corresponding author
Email addresses: laithmr@uokufa.edu.iq (Laith M Kadhum[a,1]), firdausza@ump.edu.my (Ahmad Firdaus[a,]), m.fadli.zolkipli@uum.edu.my (Mohamad Fadli Zolkipli[b]), luaymr@uokufa.edu.iq (Luay Saferali[a,1]), faizalrazak@ump.edu.my (Mohd Faizal Ab Razak)

Received: October 2020 *Revised:* December 2020

with graph theory [2], [3]. Graph theory is involved in RADG algorithm (or method) [4],wherein its mathematical model is represented by a pair of objects that transfers between each other (object relation). The theory is based on combinatorial mathematics and its application is generally used in communication [5], [6]. This study treated the mathematical side of RADG algorithm. RADG algorithm is one of methods that minimizes ciphertext-breaking because of the random ciphertext [4]. The relation between the number of designs of the RADG and the random ciphertexts is trivial whenever many designs are involved. The first step in optimization is to find the function $F_Q(n,\,\lambda)$ for every $n > 3, \lambda > 1$, and the number of jump states is $1, 2$, or more[4].

Radi proposed new methods dependent on the RADG cryptosystem called BRADG (Block RADG) and RBC (Random Block Cipher) that use key block ciphers on the basis of the structure of unbalanced Fiestel and new S-boxes [7]. Alwan proposed a faster and changeable design that developed RADG by using multireaction states called MRADG [8]. Nathim solved the problem of transition states in the design by proposing a system dependent on the chaotic map equation (logistic map equation) called CRADG [9]. Mahdi use the RADG to develop the stream cipher automata algorithm [10].

2. Reaction Automata Direct Graph (RADG)

The mathematical model of RADG is affected by graph theory and is expressed by the sextuple $\{Q, R, \Sigma, \Psi, J, T\}$, where the function $F_Q(n, \lambda)$ is the number of cases that consist of the design of the set Q, which containsa jump state. The jump state in the set Q is represented by $|J| \leq \left|\frac{n}{2}\right|$ where $k = 1, \ldots, \left|\frac{n}{2}\right|$ and is expressed as follows [4]:

$$F_Q(n, \lambda) \leq n^{(n-k)(\lambda-1)}(n-1)^{(n-k)}, \text{ where k} = 1, \ldots, |\frac{n}{2}|, \, (n-k) \geq \lambda$$

Suppose α denotes the number of data values in Q and $|\mathrm{Q}| = \mathrm{n}$ is the size of a nonempty finite set Q of standard states including jump states J, where the size of the non-empty finite set J is $|\mathrm{J}| = \mathrm{k}$, which is a subset of the set Q, where J is called a jump set and $n - 1 \geq \lambda$, where λ is the size of the set Σ, which is a non-empty finite set of an alphabet input data, then $\alpha = \lambda\tau$ and $\tau = \mathrm{n} - \mathrm{k}$,

3. Space of RADG Designs(SRDs)

For each collection of n, k and λ, a finite number of possible designs exists. Albermany gave an example on the design size [4]. If a system has a certain number of standard and jump states and data, then the existing finite number of possible designs can be described as a space of designs

Definition 3.1. *The space of all the RADG designs of n standard states, k jump states and λ data of each state is called a space of RADG designs(SRD), as denoted by $D^{\lambda}_{n,k}$*

$$\textit{where } n > 2, k < \left\lfloor \frac{n}{2} \right\rfloor \textit{ and } \lambda > 1 \ .$$

Definition 3.2. *The representation of the space of all the matrices of size $\alpha * n$ in a RADG design is called a space of RADG matrices (SRM), as denoted by $M^{\lambda}_{n,k}, \forall M \in M^{\lambda}_{n,k}$, such that $\mathrm{M} = [\mathrm{m_{ij}}]$, where $\mathrm{m_{ij}} = 1$ if a transition exists between the states S_a and S_b in $D^{\lambda}_{n,k}$ otherwise $\mathrm{m_{ij}} = 0$ in the following conditions:*

1- If S_b is a jump state, then $j > \tau, b = j$ and $a = \lfloor \frac{(i-1)}{\lambda} \rfloor$.

2- If $\mathrm{S_b}$ is a non-jump state, then $j \leq \tau, \mathrm{b} = \mathrm{j}$ and $a = \lfloor \frac{(i-1)}{\lambda} \rfloor$

Definition 3.3. *A map* H *from the finite* SRD $D^{\lambda}_{n,k}$ *to the* SRM $M^{\lambda}_{n,k}$ *is defined by* $\mathrm{H} : D^{\lambda}_{n,k} \to M^{\lambda}_{n,k}$ *and is called the matrix representation of RADG design.*

Definition 3.4. *The representation of the space of all the matrices of size* $\alpha * n$ *in a RADG design is called a space of standard RADG matrices* $(SSRM)$*, as denoted by* $M^{\lambda}_{n,k}$ *with the following conditions:*

1- $\sum_{j=1}^{n} m_{ij} = 1 \quad , i = 1, \cdots, \alpha, \forall M \in M^{\lambda}_{n,k}$*,(Only one transition exists from each data in each state)*

2- $m_{ij} = 0 \quad , \quad 1 \leq j \leq \tau$ *and* $i = \lambda(j-1)+1, \lambda(j-1)+2, \cdots, \lambda j, \forall M \in M^{\lambda}_{n,k}$ *(to eliminate the loops)*

3- $\sum_{i=1}^{\alpha} m_{ij} \geq 1, \quad j > \tau, \forall M \in M^{\lambda}_{n,k}$*. (Each jump state must be included in at least one path.)*

Example 3.5. *The matrix* M *belongs to* RADG *matrix space* $M^{2}_{7,3}$*, where* $\lambda = 2, k = 3$ *and* $n = 7$ *are the number of columns in matrix* M*, then* $\tau = 7 - 3 = 4$ *and* $\alpha = \lambda\tau = 8$ *are the number of rows in matrix* M*.*

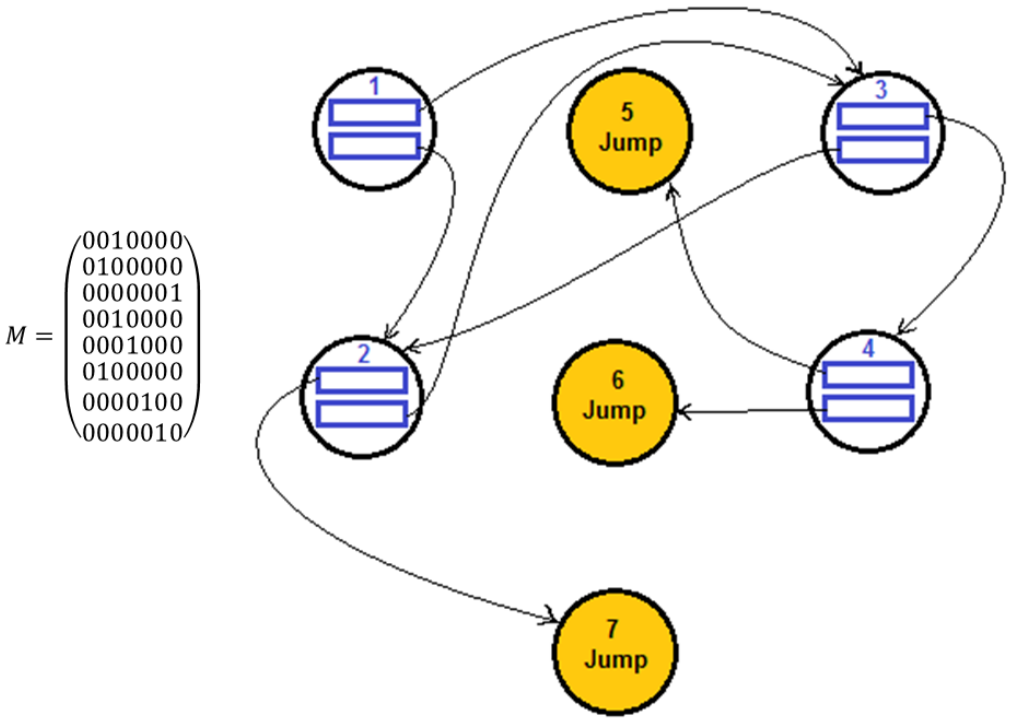

Figure 1: Standard RADG Matrix

Definition 3.6. *The summation of all the elements of* M *is called the norm of* M*, as denoted by* $\|\mathrm{M}\| \forall M \in M^{\lambda}_{n,k}$

Lemma 3.7.

$$\|M\| = \sum_{i=1}^{\alpha} \sum_{j=1}^{n} M_{ij} = \alpha \forall M \in M^{\lambda}_{n,k}$$

Proof . The proofis straightforward. □

Lemma 3.8. $\|\mathrm{A} \vee \mathrm{B}\| = \alpha$ *if and only if* $\mathrm{A} = \mathrm{B}$ $\forall A, B \in M^{\lambda}_{n,k}$, *where* V *is a logical* OR.

Proof . Since $A = B$, then $A \vee B = A = B$, which means $\|A \vee B\| = \alpha$ from Lemma(3.7). Suppose $A \neq B$, then $\exists aij \neq bij$ $\mathrm{i} = 1, 2, \ldots, \alpha$ and $\mathrm{j} = 1, 2, .., \mathrm{n}$ means that $aij \vee bij = 1$, then $\|A \vee B\| > \alpha$ but $\|A \vee B\| = \alpha$, then $A = B$. □

Lemma 3.9. *The size of* SRD $D^{\lambda}_{n,1}$ *is*

$$\left|D^{\lambda}_{n,1}\right| = \sum_{i=1}^{\alpha} (n-1)^{\alpha-i} * (n-2)^{i-1}$$

Proof . Every design belongs to the space $D^{\lambda}_{n,1}$ in the corresponding matrix that belongs to $\mathrm{M}^{\lambda}_{\mathrm{n,k}}$ because the map H of the matrix representation of RADG design is one to one on the map, where the number of matrices in the range of H is equivalent to the number of designs in domain of H, which means $\left|D^{\lambda}_{n,1}\right| = \left|M^{\lambda}_{n,1}\right|$, then suppose $M \in M^{\lambda}_{n,1}$, where

$$M = \left(\begin{array}{cccc|c} M_{11} & M_{12} & \cdots & M_{1(n-1)} & M_{1n} \\ M_{21} & M_{22} & \cdots & M_{2(n-1)} & M_{2n} \\ \vdots & \vdots & & \vdots & \vdots \\ M_{\alpha 1} & M_{\alpha 2} & \cdots & M_{\alpha(n-1)} & M_{\alpha n} \end{array}\right) \tag{3.1}$$

If k = 1, then one state exist in the set J represented by the column n in matrix M and is denoted on the matrix of one column by $\mathrm{K} = [\mathrm{k_{ij}}]$, where the size of K is $\alpha * 1$ and

$$k_{\mathrm{in}} = \begin{cases} 0 & \text{,if there is no edge from state } [i/\lambda \mid \text{ to jump state n} \\ 1 & \text{,if there is edge from state } [i/\lambda \text{ to jump state n} \end{cases}$$

Several probable cases are available for connecting the single jump state with the other states in the set Q by one edge.From the summation of each required status, then
First status:
In this case $K = \begin{bmatrix} 1 \\ x \\ \vdots \\ x \end{bmatrix}$, where $\mathrm{k_{1n}} = 1$ and $k_{\mathrm{in}} = x, 1 < \mathrm{i} \leq \alpha.(\mathrm{x} = 1 \text{ or } 0)$
The element $\mathrm{k_{1n}}$ (in the last column of matrix M) is equal to 1 , and the other elements in K is equal to 0 or 1 and denoted by x, such that $(n-1)$ cases for each row have 1 (each row from 2 to α has only one element of value 1), then in each row of M (from row 2 to row α) except the first row are connected with the other $n-1$ cases, such that the number of all cases is $(n-1)^{\alpha-1}$ cases in the first status.
Second status:
In this case $K = \begin{bmatrix} 0 \\ 1 \\ x \\ \vdots \\ x \end{bmatrix}$, where $\mathrm{k_{1n}} = 0, k_{2n} = 1$ and $k_{\mathrm{in}} = x, 2 < \mathrm{i} \leq \alpha.(x = 1 \text{ or } 0)$
In this case, changing the value of element $\mathrm{k_{1n}} = 0$ is forbidden, and the value $k_{2n} = 1$ in the column

K will replace the value of x to 1 or 0, then each case in the second status by the number of cases in the first row of M is calculated byn -2, and each row from the third row to α 'th row is $(n-1)$, then the number of all the cases in the second status is $(n-1)^{\alpha-2}(n-2)$.
r -th status:

In this case the column $K = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ x \\ \vdots \\ x \end{bmatrix}$, where $k_{\text{in}} = 0$ for $1 \leq \text{i} < r, k_{rn} = 1$ and $k_{\text{in}} = x, \text{r} < \text{i} \leq \alpha.(x = 1 \text{ or } 0)$, then the number of all cases in $\text{r} - th$ status is $(n-1)^{\alpha-r}(n-2)^{r-1}$

The last status of column K is $K = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$, then the number of all the cases in this status is $(n-2)^{\alpha-1}$

and by the summation of each of the above statuses with all the cases. This proof is done. □

Lemma 3.10. *The size* $\text{SRD}D^{\lambda}_{n,2}$ *is*

$$\left|D^{\lambda}_{n,2}\right| = 2\sum_{i=1}^{\alpha}(n-1)^{\alpha-i} * (n-3)^{i-1}$$

Proof . The same as the proof given above with k = 2, and $\forall M \in M^{\lambda}_{n,2}$, then

$$M = \left(\begin{array}{cccc|cc} M_{11} & M_{12} & \cdots & M_{1(n-2)} & M_{1(n-1)} & M_{1n} \\ M_{21} & M_{22} & \cdots & M_{2(n-2)} & M_{2(n-1)} & M_{2n} \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ M_{\alpha 1} & M_{\alpha 2} & \cdots & M_{\alpha(n-2)} & M_{\alpha(n-1)} & M_{\alpha n} \end{array}\right) \tag{3.2}$$

A total of two states exist in the jump set J represented by the matrix $\text{K} = [\text{k}_{\text{ij}}]$, where the last two columns in the matrix M with the size of K is $\alpha * 2$ and the same previous statuses in lemma (3), but each status has two parts with the first part to the first column of K and the other to the second column of K. The first status is

$$K = \begin{bmatrix} 0 & 1 \\ x & x \\ \vdots & \vdots \\ x & x \end{bmatrix} \text{ or } K = \begin{bmatrix} 1 & 0 \\ x & x \\ \vdots & \vdots \\ x & x \end{bmatrix}$$

where $k_{1(n-1)} = 0, k_{1n} = 1$ for the first part and $k_{1(n-1)} = 1, k_{1n} = 0$ for the second part. If $k_{ij} = x, 2 < \text{i} \leq \alpha.j = 1, 2$ and $x = 1$ or 0, then the number of all the cases in first status is $2(n-1)^{\alpha-1}$.
The second status is

$$K = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ x & x \\ \vdots & \vdots \\ x & x \end{bmatrix} \text{ or } K = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ x & x \\ \vdots & \vdots \\ x & x \end{bmatrix}$$

where $k_{2(n-1)} = 0, k_{2n} = 1$ for first part and $k_{2(n-1)} = 1, k_{2n} = 0$ for the second part. If $k_{ij} = 0, \mathrm{i} = 1, j = 1, 2, k_{ij} = x, 3 < \mathrm{i} \leq \alpha, j = 1, 2$ and $x = 1$ or 0, then the number of all the cases in the second status is $2(n-1)^{\alpha-2}(n-3)$.
The r -th status is

$$K = \begin{bmatrix} 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \\ 0 & 1 \\ x & x \\ \vdots & \vdots \\ x & x \end{bmatrix} \text{ or } K = \begin{bmatrix} 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \\ 1 & 0 \\ x & x \\ \vdots & \vdots \\ x & x \end{bmatrix}.$$

where $\mathrm{k_{r(n-1)}} = 0, k_{rn} = 1$ for the first part and $\mathrm{k_{r(n-1)}} = 1, k_{rn} = 0$ for the second part. If

$$k_{ij} = 0, i = 1, \ldots, r-1, j = 1, 2, k_{ij} = x, r+1 < i \leq \alpha, j = 1, 2 \text{ and } x = 1 \text{ or } 0$$

then the number of all cases in the r-th status is $2(n-1)^{\alpha-r}(n-3)^{r-1}$
The last status of matrix K is

$$K = \begin{bmatrix} 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \\ 0 & 1 \end{bmatrix} \text{ or } K = \begin{bmatrix} 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \\ 1 & 0 \end{bmatrix}$$

then the number of all the cases in this status is $2(n-3)^{\alpha-1}$ and by the summation of each of the above statuses with all cases. This proof is done.

From above, α for $k = 1$ is denoted by α_1, where $\alpha_1 = \lambda\tau_1$ and $\tau_1 = n-1, k = 2$ is denoted by α_2, where $\alpha_2 = \lambda\tau_2$ and $\tau_2 = n-2$, in general, for $k = r$

$$\alpha_r = \lambda\tau_r and \tau_r = n - r, where\ r \geq 1 \tag{3.3}$$

□

Lemma 3.11.

$$\alpha_{r+1} = \alpha - \lambda\ and\ \tau_{r+1} = \tau_r\ where\ r \geq 1 \tag{3.4}$$

where $\tau_1 = n-1$ *and* $\alpha_1 = \lambda\tau_1$

Proof . If $\alpha_{r+1} = \lambda\tau_{r+1}$ and $\tau_{r+1} = n-(r+1)$ from Equation(3.3), then $\tau_{r+1} = n-(r+1) = (n-r)-1$
If $\tau_r = n-r$, then $\tau_{r+1} = \tau_{r-1}, \alpha_{r+1} = \lambda\tau_{r+1=} = \lambda(\tau_r - 1) = \lambda\tau_r - \lambda = \alpha_r - \lambda$ □

Theorem 3.12. *The size of* SRD $D^{\lambda}_{n,k}$ *is*

$$F_Q = k\sum_{i=1}^{\alpha}(n-1)^{\alpha-i} * (\tau-1)^{i-1}\ , where\ \tau = n-k \tag{3.5}$$

Proof . The proof of the theorem by mathematical induction is as follows. Let S_k be the statement of Equation(3.5). The proof will now proceed in the following steps: the basis and the inductive steps.

Basis Step: If k = 1 or k = 2, then S_1 and S_2 is true, then they satisfy theorem (3.12) by using lemmas (3.9) and (3.10).
Inductive Step: The inductive assumption assumes that S_r is true, where $k = r \geq 1$and proves that S_{r+1} is true for $k = r + 1$
Suppose

$$S_r = \sum_{i=1}^{u_r} C_i$$

in lemma(3.8).Let C_i be denoted in the r -th status (inside of the proof in lemma(3.10)) as

$$C_i = r(n-1)^{\propto_r - 1} * (n - r - 1)^{i-1}$$

and from lemma(3.11), then

$$C_i = r(n-1)^{\propto_r - 1} * (\tau_r - 1)^{i-1}$$

If $A_r \in M^{\lambda}_{n,r}$ and $A_{(r+1)} \in M^{\lambda}_{n,(r+1)}$, then the size of matrix A_r is $\alpha_r \times n$ and the size of matrix $A_{(r+1)}$. is $\alpha_{r+1} \times n$, then two differences exist between the matrices A_r and $A_{(r+1)}$. The number of rows in $A_{(r+1)}$. is the number rows in A_r minus λ, and the column number of the jump states in $A_{(r+1)}$. is the column number of the jump states in A_r plus one.

From the above difference between matrices A_r and $A_{(r+1)}$, we calculate C_i of matrix $A_{(r+1)}$· and for each of the rows in $A_{(r+1)}$ for r-times plus one.

$$(n-1)^{\alpha_r - 1 - \lambda} * (\tau_r - 2)^{i-1} + (n-1)^{\alpha_r - 1 - \lambda} * (\tau_r - 2)^{i-1} + \ldots + (n-1)^{\propto_r - 1 - \lambda} * (\tau_r - 2)^{i-1}$$

$= (\mathrm{r}+1)(n-1)^{\alpha_r - \lambda - 1} * (\tau_r - 1 - 1)^{i-1} = (\mathrm{r}+1)(n-1)^{\alpha_{r+1} - 1} * (\tau_{r+1} - 1)^{i-1}$
and

$$C_i = (r+1)(n-1)^{\propto_{r+1} - 1} * (\tau_{r+1} - 1)^{i-1}$$

then
$S_{r+1} = \sum_{i=1}^{\alpha_{r+1}} (r+1)(n-1)^{\alpha_{r+1} - 1} * (\tau_{r+1} - 1)^{i-1}$, the proof is done □

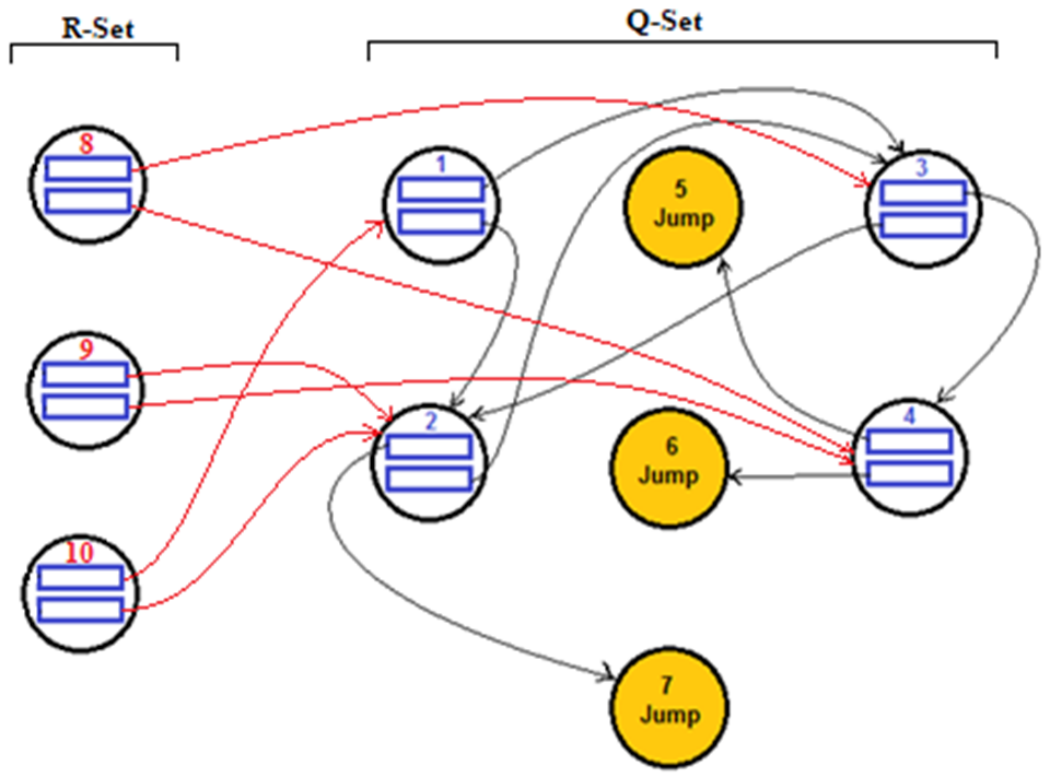

Figure 2: Typical RADG design with $(m = 3, n = 7, k = 3, \lambda = 2)$

Example 3.13. *For the RADG design in figure* 2, *where* $n = 7, k = 3$ *and* $\lambda = 2$, *then* $\tau = n - k = 4, \alpha = \lambda\tau = 8$RQ *can be calculated due to theorem 1 as follows*

$$F_Q = k \sum_{i=1}^{\alpha} (n-1)^{\alpha-i} * (\tau-1)^{i-1}$$
$$F_Q = 3 * \sum_{i=1}^{8} (7-1)^{8-i} * (4-1)^{i-1} = 3 * 557685 = 1,673,055$$

4. Conclusion

An inequality formula for F_Q produced by Albermany and Safdar to show out that a huge number of possible designs exist for a certain combination of n, mand λ, but they could not calculate the exact number of possible designs .The use of a matrix representation simplified the process of expressing the relations and conditions and by using the mathematical induction, that could be stated as a new equality formula to accurately calculate F_Q. Not all the possible designs are acceptable. The acceptable designs are called 'standard RADG designs', which are represented by the SRM and its space is denoted by SSRM. The matrix representation allows us to identify the conditions easily. Hence, we can similarly state the conditions that identify the set of optimum designs.
A matrix representation development may be done in future, so that each element (mi, j) in the matrix M can represent the state address of the transition destination and create another matrix to represent the output data from each state due to the input data.
Depending on the matrix representation, mathematical conditions can be formulated to identify the optimal desig.

5. Acknowledgement

This study thanked to Sysarmy Sdn Bhd and Universiti Malaysia Pahang (UMP), with grant number of UIC190807.

References

[1] G. Baumslag, B. Fine, M. Kreuzer and G. Rosenberger, *A course in mathematical cryptography,* De Gruyter, 2015.

[2] L. MAO, *Mathematics after CC conjecture-combinatorial notions and achievements,*. Int. J. Math. Comb. 2 (2015) 1–31.

[3] S. Lovett, *Additive combinatorics and its applications in theoretical computer science,* Theory Comput. (2016) 1–53.

[4] S. A. Albermany and G. A. Safdar, *Keyless security in wireless networks,* Wirel. Pers. Commun. 79(3) (2014) 1713–1731.

[5] J. L. Gross and J. Yellen, *Handbook of graph theory,* CRC Boca Raton, Florida, 2004.

[6] I. Anderson and R. Diestel, *Graph theory,* 85(502) (2001).

[7] S. Albermany, F. Radi Hamade and G. A. Safdar, *New random block cipher algorithm,* International Conference on Current Research in Computer Science and Information Technology (ICCIT), 2017.

[8] S. A. Albermany and A. H. Alwan, *RADG design On elliptic curve cryptography,* ICCIIDT 2016 London - UK Proceedings.

[9] S. Albermany, M. Nathim and Z. M. Hussain, *"CRADG: A chaotic RADG security system,* J. Eng. Appl. Sci. 12 (2017) 4118–4122.

[10] A. Salah, D. Amer and S. Kamal, *S-RADG: A stream cipher RADG cryptography,* J. Eng. Appl. Sci. 13 (2018) 2317–2321.