



## طراحی S-Box با استفاده از الگوریتم ژنتیک

مریم مهرنژاد<sup>۱</sup>، مهسا گرائیلو تنها<sup>۲</sup>، احسان تورینی<sup>۳</sup>، دکتر عباس قائمی بافقی<sup>۴</sup>

دانشگاه فردوسی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر<sup>۱</sup>

maryam.mehrnejad@gmail.com

mahsa\_grailoo@yahoo.com

دانشگاه آزاد اسلامی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر<sup>۳</sup>

toreini@gmail.com

دانشگاه فردوسی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر<sup>۴</sup>

ghaemib@yahoo.com<sup>2,3</sup>

### چکیده

در علم رمزشناسی S-Box ها یکی از اجزای مهم الگوریتم‌های رمزنگاری متقارن می‌باشند. در رمزنگاری قطعه‌ای S-Box ها به منظور مبهم کردن رابطه‌ی بین متن واضح و متن رمز بکار می‌روند. S-Box های غیرخطی و غیرهمبسته، امن‌ترین S-Box ها در مقابل حملات تحلیل خطی و تفاضلی می‌باشند. بدست آوردن S-Box هایی با حداکثر میزان غیر خطی بودن و به طور همزمان با حداقل میزان همبسته بودن کار بسیار دشواری است و در دسته‌ی مسائل NP-complete قرار می‌گیرد. یکی از روش‌های حل مسائل چندهدفه در قالب الگوریتم ژنتیک، استفاده از الگوریتم ژنتیک میانگین‌رتبه می‌باشد. در این مقاله با استفاده از این الگوریتم به طراحی S-Box پرداخته شده است. سه ویژگی غیرخطی بودن، غیرهمبستگی و منظم بودن اهداف مسئله برای بهینه‌سازی می‌باشند. نتایج بدست آمده از روش پیشنهاد شده نسبت به کارهای قبلی کارا تر می‌باشد.

### واژه های کلیدی

الگوریتم ژنتیک میانگین رتبه، توازن<sup>۱</sup>، غیرخطی<sup>۲</sup>، خودهمبستگی<sup>۳</sup>، S-Box<sup>۴</sup>.

<sup>1</sup> Balanced

<sup>2</sup> Non-Linear

<sup>3</sup> Auto Correlation

<sup>4</sup> Substitution Box

## 1- مقدمه

بر اساس نظریه شانون<sup>1</sup> درهم پیچیدگی<sup>2</sup> و پراکندگی<sup>3</sup> دو خاصیت رمزهای امن هستند. درهم پیچیدگی باعث می شود که رابطه ی متن رمز شده و کلید تا حد ممکن پیچیده شود و پراکندگی باعث می شود که رابطه ی بین متن رمز شده و متن واضح متناظرش تا حد ممکن کم شود. جایگزینی به عنوان مکانیزم اصلی درهم پیچیدگی شناخته شده است و در مقابل جایگشت<sup>4</sup> نیز یکی از تکنیک های پراکندگی می باشد. در رمزهای مدرن تکنیک های دیگری نظیر تبدیلات خطی<sup>5</sup> نیز برای پیچیده کردن هر چه بیشتر رمز به کار برده می شوند. در این گونه رمزها مکانیزم های جانشینی و جایگشتی متناوبا به منظور درهم پیچیدگی و پراکندگی بیشتر رمز به کار می روند [1]. در واقع با طراحی S-Box های امن تر، رمز ی با پیچیدگی بالاتر تولید می شود.

یک S-Box را می توان به طور ساده یک تابع بولی با  $n$  ورودی و  $m$  خروجی در نظر گرفت. در حال حاضر تلاش های محققان به سمت طراحی S-Box هایی با حداکثر مقاومت در برابر حملاتی چون تحلیل خطی و تفاضلی می باشد. بدین منظور ویژگی های متفاوتی برای S-Box ها تعریف شده است. سه ویژگی منظم بودن، غیرخطی بودن و غیرهمبسته بودن، سه معیار مهم در طراحی S-Box های مقاوم می باشند.

در طراحی S-Box در این مقاله سه معیار فوق مدنظر می باشند. ثابت می شود که به دست آوردن S-Box هایی با این ویژگی ها در دسته ی مسائل NP-complete قرار می گیرد. بنابراین برای برآورده کردن این سه هدف به طور همزمان باید از روش های محاسبات تکاملی چندهدفه استفاده شود. در این مقاله با استفاده از الگوریتم ژنتیک میانگین رتبه به عنوان یکی از روش های حل مسائل چندهدفه به طراحی S-Box پرداخته شده است.

در بخش 2 این مقاله به معرفی کارهای مرتبط پرداخته می شود. در بخش 3 ابتدا S-Box ساده و سپس ویژگی های آن تعریف می شود. بخش 4 به تشریح الگوریتم ژنتیک میانگین رتبه می پردازد. در بخش 5 به مدل سازی مسئله در قالب الگوریتم ژنتیک پرداخته می شود. بخش 6 شامل نتایج بدست آمده می باشد. در فصل 7 مقایسه ای بین نتایج بدست آمده و کارهای مشابه پیشین به عمل می آید. فصل 8 خلاصه ای از آنچه در مقاله ارائه شده است را در بردارد.

## 2- کارهای مرتبط

روش های مختلفی برای ساختن S-Box وجود دارد که در دو دسته ی کلی روش های ریاضی و روش های تصادفی جای می گیرند.

روش های ریاضی دارای این مزیت می باشند که ویژگی های لازم برای یک رمز خوب را در S-Box ها، تا حد خوبی فراهم می کنند [2]. به طور مثال الگوریتم رایندال<sup>6</sup> در رمز AES، S-Box هایی می سازد که در مقابل حملات تحلیل تفاضلی و خطی کاملا امن می باشند [1]. اما S-Box هایی که با روش های ریاضی ساخته می شوند در مقابل حمله ی جبری آسیب پذیر می باشند. روش های تصادفی از این بابت دارای قابلیت اعتماد بیشتری هستند.

یکی از این روش ها این است که به تصادف یک S-Box تولید شود و سپس میزان خوب بودن آن اندازه گیری شود که این روش بسیار ناکار و زمان بر است. یکی دیگر از روش های تصادفی این است که S-Box های جدید بر مبنای یک سری S-Box های خوب و معروف ساخته شوند. مثلا S-Box رمز سرپنت<sup>7</sup> بر مبنای S-Box های رمز DES ساخته شده است. روشی دیگر، استفاده از الگوریتم های محاسبات نرم از قبیل الگوریتم تبریدسازی<sup>8</sup>، ژنتیک، بهینه سازی ازدحام ذرات<sup>9</sup> می باشد. در بیشتر مقالات معمولا یکی از ویژگی های لازم برای طراحی یک S-Box خوب مورد توجه قرار گرفته است. بنابراین در تمامی آن ها از الگوریتم های تکاملی ساده برای بهینه سازی استفاده شده است. در [3] از الگوریتم تبریدسازی برای بهینه سازی ویژگی غیرخطی بودن در S-Box استفاده شده است. در [4] نیز نویسندگان از الگوریتم بهینه سازی ازدحام ذرات برای S-Box های مطلوب استفاده کرده اند. همچنین در مقالات متعددی از الگوریتم ژنتیک برای طراحی S-Box استفاده شده است. در این مقالات ویژگی های متعددی برای S-Box ها مورد بهینه سازی قرار گرفته اند. مثلا در [2] نویسندگان سعی کرده اند با استفاده از الگوریتم ژنتیک S-Box های  $8 \times 8$  بهینه تولید کنند. همچنین در [5] سعی شده است با استفاده از الگوریتم ژنتیک و الگوریتم تپه نوردی<sup>10</sup> S-Box هایی با بیشترین میزان غیرخطی بودن ارائه شود. همچنین در [6] با بهره گیری از تئوری بازی های نش [7] و استفاده از مفاهیم الگوریتم ژنتیک، به طراحی S-Box هایی با سه ویژگی منظم بودن، غیرخطی بودن و غیرهمبسته بودن پرداخته شده است. در [8] و [9] نیز با استفاده از الگوریتم ژنتیک به طراحی S-Box هایی با همین سه ویژگی پرداخته شده است. نتایج بدست آمده در این مقاله با نتایج سه مقاله ی اخیر مقایسه می شود.

## 3- S-box

S-Box ها نقش بسیار مهمی را در بسیاری از رمزهای قطعه ای مدرن دارند. در رمزنگاری بلوکی S-Box ها به منظور مبهم کردن

<sup>6</sup> Rijndael

<sup>7</sup> Serpent

<sup>8</sup> Simulated Annealing (SA)

<sup>9</sup> Particle Swarm Optimization (PSO)

<sup>10</sup> Hill Climbing (HC)

<sup>1</sup> Shannon Theory

<sup>2</sup> Confusion

<sup>3</sup> Diffusion

<sup>4</sup> Permutation

<sup>5</sup> Linear Transformation

تعریف 9. یک S-Box، یک تابع بولی است که به صورت زیر تعریف می‌شود:

$$S: \mathbb{B}^m \mapsto \mathbb{B}^n \quad (8)$$

تعریف 10. S-Box تعریف شده‌ی S در بالا، الحاقی از m تا S-Box ساده‌ی  $S_i$  است که  $1 \leq i \leq m$  و به صورت زیر نمایش داده می‌شود:

$$S(x) = S_1(x) S_2(x) \dots S_m(x) \quad (9)$$

تعریف 11. میزان غیرخطی بودن S-Box غیرساده‌ی S به صورت زیر محاسبه می‌شود:

$$\mathcal{N}_S^* = \min_{\beta \in \mathbb{B}^n \setminus \{0\}} \mathcal{N}_{S\beta}(x) \quad (10)$$

که در آن:

$$S_{\beta}(x) = \bigoplus_{i=0}^{i=m} \beta_i S_i(x)$$

تعریف 12. میزان خودهمبستگی S-Box غیرساده‌ی S به صورت زیر محاسبه می‌شود:

$$\mathcal{A}_S^* = \max_{\beta \in \mathbb{B}^n \setminus \{0\}} \mathcal{A}_{S\beta}(x) \quad (11)$$

تعریف 13. به S-Box غیرساده‌ی S منظم گفته می‌شود اگر و تنها اگر به ازای هر  $W \in \mathbb{B}^m$ ، همان تعداد  $x \in \mathbb{B}^n$  وجود داشته باشد که  $S(x) = W$  می‌شود:

$$\mathcal{W}_S^* = \max_{W \in \mathbb{B}^n \setminus \{0\}} |\mathcal{W}_{S\beta}^*(x)| \quad (12)$$

همانطور که نتیجه می‌شود، S-Box منظم S-Box ای است که:

$$\mathcal{W}_S^* = 2^{n-1} \quad (13)$$

#### 4- الگوریتم ژنتیک میانگین رتبه

یکی از روش‌های حل مسائل چندهدفه در قالب الگوریتم ژنتیک، استفاده از الگوریتم ژنتیک میانگین رتبه می‌باشد. این روش یکی از روش‌های مبتنی بر جمعیت است [10]. در این الگوریتم، در پایان هر نسل، تمامی افراد جمعیت بر اساس هر کدام از معیارها به طور جداگانه رتبه‌بندی می‌شوند. به طور مثال در مسئله‌ی طراحی S-Box در پایان نسل t، یک بار افراد هر نسل بر اساس ویژگی توازن، یک بار بر اساس میزان غیرخطی بودن و یک بار هم بر اساس میزان غیرخودهمبسته بودن در مقایسه با بقیه افراد جمعیت رتبه‌بندی می‌شوند. میزان برازندگی نهایی هر فرد از میانگین رتبه‌های هر فرد در معیارهای مختلف بدست می‌آید.

رابطه‌ی بین متن واضح و متن رمز بکار می‌روند. یک S-Box را می‌توان به طور ساده، یک تابع بولی با n بیت ورودی و m بیت خروجی در نظر گرفت. ویژگی‌های متفاوتی برای یک S-Box تعریف شده است. سه ویژگی‌ای که در این مقاله مدنظر می‌باشد عبارت است از: منظم بودن، غیرخطی بودن و غیرهمبسته بودن که در زیر تعریف می‌شوند.

تعریف 1. یک S-Box ساده، یک تابع بولی است که به صورت زیر تعریف می‌شود:

$$S: \mathbb{B}^n \mapsto \mathbb{B} \quad (1)$$

تعریف 2. یک S-Box خطی L به صورت زیر تعریف می‌شود:

$$\mathcal{L}_n(x) = \bigoplus_{i=0}^{i=m} \beta_i \mathcal{L}(x_i) \quad (2)$$

تعریف 3. پلاریته یک S-Box ساده به صورت زیر تعریف می‌شود:

$$\mathcal{S}(x) = (-1)^{s(x)} \quad (3)$$

تعریف 4. فاکتور غیرهمبستگی دو S-Box ساده‌ی S و S' به صورت زیر تعریف می‌شود:

$$\mathcal{U}_{S,S'} = \sum_{x \in \mathbb{B}^n} \mathcal{S}(x) \times \mathcal{S}'(x) \quad (4)$$

تعریف 5. دو S-Box ساده‌ی S و S' غیرهمبسته گفته می‌شوند، اگر و تنها اگر:  $\mathcal{U}_{S,S'} = 0$

تعریف 6. میزان غیرخطی بودن S-Box ساده‌ی S توسط فاکتور غیرهمبستگی آن با تمام S-Box های ساده‌ی خطی ممکن آن اندازه گرفته می‌شود و به صورت زیر تعریف می‌شود:

$$\mathcal{N}_S^* = \frac{1}{2} \left( 2^n - \max_{\alpha \in \mathbb{B}^n} |\mathcal{U}_{S,\alpha}| \right) \quad (5)$$

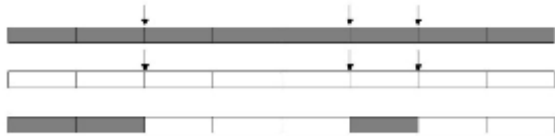
تعریف 7. میزان خودهمبستگی S-Box ساده‌ی S توسط فاکتور همبستگی‌اش با مشتقات D(x) آن به صورت زیر تعریف می‌شود:

$$\mathcal{A}_S = \max_{\alpha \in \mathbb{B}^n \setminus \{0\}} |\mathcal{U}_{S,D}| \quad (6)$$

$$D(x) = S(x) \oplus \alpha \quad \alpha \in \mathbb{B}^n \setminus \{0\}$$

تعریف 8. S-Box ساده‌ی S متوازن نامیده می‌شود اگر و تنها اگر تعداد ترکیبات  $x \in \mathbb{B}^n$  که به ازای آن‌ها  $S(x) = 0$  است، برابر تعداد ترکیبات  $y \in \mathbb{B}^n$  باشد که با ازای آن‌ها  $S(y) = 1$  است. میزان توازن S-Box ساده‌ی S توسط وزن همینگ آن و به صورت زیر تعریف می‌شود:

$$\mathcal{W}_S = \frac{1}{2} \left( 2^n - \sum_{\alpha \in \mathbb{B}^n} \mathcal{S}(x) \right) \quad (7)$$



شکل (2). تقاطع

عملگر جهش نیز با احتمال مشخص شده به عنوان میزان جهش، هر بیت را متمم می‌کند.

### 5-3- میزان برازندگی

برای محاسبه ی میزان برازندگی در هر فرد، باید به نحوی هر سه هدف را مد نظر قرار داد. اهداف در این مسئله به صورت زیر می‌باشند:

- $\bar{u}$  حداکثر کردن میزان منظم بودن
- $\bar{u}$  حداکثر کردن میزان غیرخطی بودن
- $\bar{u}$  حداقل کردن میزان خود همبستگی

یعنی:

$$\begin{cases} \max_{\xi} W_{\xi}^* \\ \max_{\xi} N_{\xi}^* \\ \max_{\xi} s/\xi^* \end{cases}$$

که هر کدام در بخش قبلی بطور کامل تشریح شده است.

پس از اتمام هر نسل بر اساس فرمول‌های فوق، میزان برازندگی هر یک از افراد به طور جداگانه محاسبه می‌شود و رتبه‌ی هر فرد در هر یک از معیارها نسبت به افراد دیگر جمعیت محاسبه می‌شود. میزان برازندگی نهایی هر کروموزوم از میانگین رتبه‌های آن در معیارهای مختلف بدست می‌آید.

### 5-4- نحوه‌ی انتخاب

برای انتخاب والدین جهت انجام عملیات ژنتیکی بر روی آنها و انتقال به نسل بعدی از الگوریتم معروف چرخ رولت<sup>13</sup> استفاده می‌شود.

### 6- نتایج

برنامه در محیط net 2008 و به زبان C# نوشته شده است. برای اجرای سریع‌تر برنامه قسمت‌های سنگین محاسباتی آن در محیط C++ نوشته و به برنامه لینک شده است. برنامه قابلیت تنظیم پارامترهای مختلفی از قبیل تعداد بیت‌های خروجی S-Box، تعداد حداکثر نسل‌ها، میزان تقاطع و جهش را دارد. شکل 3 نمایی از پیشرفت نتایج را در طول نسل‌ها نمایش می‌دهد.

## 5- مدل‌سازی مسئله در قالب الگوریتم ژنتیک

برای مدل‌سازی مسائل در الگوریتم ژنتیک، چندین مسئله باید مورد توجه قرار گیرد؛ ساختن افراد (کروموزوم‌ها)، عملگرهای ژنتیکی (تقاطع و جهش)، میزان برازندگی و نحوه‌ی انتخاب.

### 5-1- ساختار کروموزوم

بطور ساده در این مسئله برای ساختن کروموزوم یعنی تبدیل فنوتایپ<sup>11</sup> به ژنوتایپ<sup>12</sup>، از یک آرایه‌ی بیتی استفاده شده است. هر S-Box دارای تعدادی بیت ورودی و تعدادی بیت خروجی است که تعداد بیت‌های ورودی و خروجی الزاماً برابر هم نمی‌باشند. در این پیاده‌سازی تعداد بیت‌های ورودی ثابت و مساوی 8 بیت و تعداد بیت‌های خروجی از 5 تا 8 بیت تغییر کرده است. از آنجایی که تعداد بیت‌های ورودی 8 می‌باشد، هر S-Box ساده دارای 256 خانه است که در هر خانه‌ی آن اعداد 0 یا 1 به عنوان خروجی قرار گرفته‌اند. با در کنارهم قرار دادن این S-box های ساده می‌توان S-Box هایی با تعداد بیت‌های دلخواه خروجی را تولید کرد. شکل 1 نحوه‌ی کد کردن یک S-Box ساده با دو بیت ورودی را نشان می‌دهد.

	00	01	10	11
00	0	1	0	1
01	1	0	1	1
10	1	1	0	0
11	0	0	1	1

الف

0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0	1	0	1	1	0	1	1	1	1	1	0	0	0	0	1

ب

شکل (1): نحوه نگاشت ورودی به خروجی در S-Box ساده. (الف):

(ب) Phenotype (ج) Genotype

### 5-2- عملگرهای ژنتیکی

عملگر تقاطع ابتدا چندین نقطه به طور تصادفی در طول دو آرایه‌ی کروموزوم‌های والد را انتخاب می‌کند، سپس به طور یکی درمیان رشته‌های بیتی بین دو نقطه را به کروموزوم فرزند منتقل می‌کند. به این نوع تقاطع، تقاطع یکنواخت گفته می‌شود. تعداد نقاط انتخابی در برنامه قابل تنظیم از یک تا حداکثر تعداد خانه‌های آرایه می‌باشند. شکل 2 نحوه‌ی اعمال عملگر تقاطع را نمایش می‌دهد.

<sup>13</sup> Roulette Wheels

<sup>11</sup> Phenotype

<sup>12</sup> Genotype

جدول (2). مقایسه

تعداد بیت خروجی	نتایج برنت		نتایج کلارک		نتایج ندجه		نتایج لاسکری	
	میان	حداکثر	میان	حداکثر	میان	حداکثر	میان	حداکثر
5	102	72	108	56	110	56	107	56
6	100	80	106	64	106	62	107	60
7	98	80	104	72	104	70	106	56
8	-	-	-	-	-	-	107	64

### 8- نتیجه گیری

در این مقاله یک الگوریتم ژنتیک مناسب برای حل مسائل چندهدفه به نام الگوریتم ژنتیک میانگین رتبه برای حل مسئله طراحی S-Boxهایی که دارای حداکثر میزان منظم بودن، حداکثر میزان غیرخطی بودن و حداقل میزان خودهمبستگی باشند، ارائه شده است.

نتایج بدست آمده در این روش نسبت به کارهای قبلی به مراتب رضایت بخش تر می باشد. بدین ترتیب، به عنوان کارهای آینده می توان این الگوریتم را روی S-Boxهایی با ویژگی های بیشتر و همچنین S-Boxهای بزرگتر (یعنی با تعداد بیت های ورودی و خروجی بیشتر) گسترش داد. همین طور می توان از روش های دیگر محاسبات تکاملی مثل SA و PSO یا روش های دیگر الگوریتم ژنتیک برای حل مسائل چندهدفه از قبیل روش های پرتو [11]، [10] استفاده کرد.

### مراجع

[1] J. Daemen and V. Rijmen, "The design of rijndael: Aes—the advanced encryption standard", Springer-Verlag, 2002.

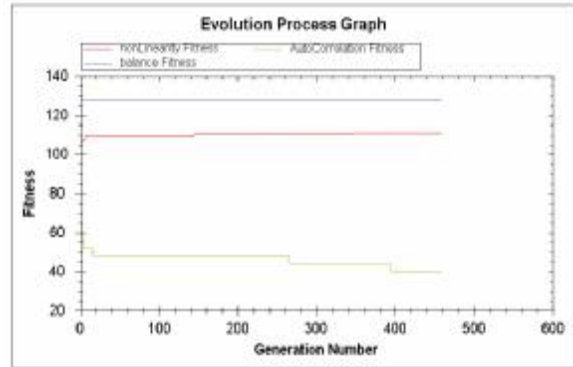
[2] H. Chen, D. Feng, "An effective evolutionary strategy for bijective S-boxes", In Proc. The 2004 IEEE Congress on Evolutionary Computation (CEC'04), Portland, Oregon, USA, Volume: 2, Date: 19-23 June 2004.

[3] J. Clark, Jeremy L. Jacob, Susan tepney, "The Design of S-Boxes by Simulated Annealing", In Proc. The 2004 IEEE Congress on Evolutionary Computation (CEC'04), Portland, Oregon, USA, Volume: 2, page(s): 1533- 1537, Date: 19-23 June 2004.

[4] E. Laskari, G. Meletiou, M. Vrahatis, "Utilizing Evolutionary Computation Methods for the Design of S-Boxes", In Proc. The 2006 IEEE International Conference on Computational Intelligence and Security, Volume: 2, On page(s): 1299-1302, 3-6 Nov. 2006.

[5] A. Dimovski, D. Gligoroski, "Generating highly nonlinear Boolean functions using a genetic algorithm", in Proc. Of 1 Balcan Conference on Informatics, Thessaloniki, Greece, November 2003.

[6] N. Nedjah, L. Mourelle, "Evolutionary Resilient Substitution Boxes for Secure Cryptography Using Nash equilibrium", In Proc. The 2006 IEEE International



شکل (3). نمودار خروجی برنامه برای S-Boxی با 7 بیت خروجی

همان طور که مشاهده می شود با صعودی بودن نمودار دو ویژگی منظم بودن و غیرخطی بودن و نزولی بودن نمودار خودهمبستگی، همگرایی الگوریتم ژنتیک تضمین می شود.

جدول شماره 1 نتایج بدست آمده از روش پیشنهاد شده را نمایش می دهد.

جدول (1). نتایج

تعداد بیت های خروجی	میزان غیرخطی	میزان غیرهمبستگی
5	107	56
6	107	60
7	106	56
8	107	64

پارامترهای الگوریتم ژنتیک در اجرا به صورت زیر تنظیم شده اند: تعداد افراد جمعیت: 100، تعداد نسل: 500، ضریب تقاطع: 80%، ضریب جهش: 5%. همچنین جواب به طور متوسط در کمتر از 200 نسل بدست آمده اند.

### 7- مقایسه و جمع بندی

جدول 2 به مقایسه نتایج بدست آمده در این مقاله و کارهای مشابه پرداخته است.

همان طور که مشاهده می شود پیاده سازی این کار در مقایسه با کارهای انجام شده توسط ندجه [6]، کلارک [8] و برنت [9] نتایج بهتری داشته است. یعنی S-Boxهایی که از روش پیشنهاد شده بدست آمده اند غیرخطی تر و دارای همبستگی کمتری می باشند. در تمامی کارهای انجام شده میزان منظم بودن S-Boxها گزارش نشده است. علت این است که S-Boxهای بهینه همگی به حداکثر میزان منظم بودن خود که 128 می باشد، رسیده اند و این نتیجه در تمامی کارها به طور مشابه بدست آمده است.

Conference on Computational Intelligence and Security, Volume: 2, On page(s): 1295-1298, 3-6 Nov. 2006.

[7] J. Nash, "Equilibrium points in n-person games", Proceedings of the National Academy of Sciences, 36:48-49, 1950.

[8] J. Clark, "The design of s-boxes by simulated annealing", New Generation Computing, 23(3):219-231, 2005.

[9] L. Burnett, "Evolutionary heuristics for finding cryptographically strong s-boxes", Lecture Notes in Computer Science, 1726:263-274, 1999.

[10] K. Tav, E. Khor, T. Lee, "Multiobjective Evolutionary algorithms and applications", page 20, Springer Verlag, 2005.

[11] A. Konak, D. Coit, A. Smith, "Multi-objective optimization using genetic algorithms: A tutorial", Reliability Engineering and System, Elsevier Journal, 2006.