هفتمین کنفرانس بین المللی انجمن رمز ایران

۲۴ و ۲۵ شهریورماه ۱۳۸۹، دانشگاه صنعتی خواجه نصیرالدین طوسی

دانشگاه صنعتی خواجه نصیرالدین طوسی

انجمن رمزایران

طراحی S-Box با استفاده از الگوریتم ژنتیک

مریم مهرنژاد[۱]، مهسا گرائیلو تنها [۲]، احسان تورینی[۳]، دکتر عباس قائمی بافقی [۴]

دانشگاه فردوسی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر[۱و۲]

maryam.mehrnejad@gmail.com

mahsa_grailoo@yahoo.com

دانشگاه آزاد اسلامی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر[۳]

toreini@gmail.com

دانشگاه فردوسی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر[۴]

ghaemib@yahoo.com[2,3]

چکیده

در علم رمزشناسی S-Boxها یکی از اجزای مهم الگوریتم‌های رمزنگاری متقارن می‌باشند. در رمزنگاری قطعه‌ای S-Boxها به منظور مبهم کردن رابطه‌ی بین متن واضح و متن رمز بکار می‌روند. S-Boxهای غیرخطی و غیرهمبسته، امن‌ترین S-Boxها در مقابل حملات تحلیل خطی و تفاضلی می‌باشند. بدست آوردن S-Boxهایی 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 کاراتر می‌باشد.

واژه های کلیدی

الگوریتم ژنتیک میانگین رتبه، توازن[۱]، غیرخطی[۲]، خودهمبستگی[۳]، S-Box[۴].

[1] Balanced

[2] Non-Linear

[3] Auto Correlation

[4] Substitution Box

1- مقدمه

بر اساس نظریه شانون[1] درهم‌پیچیدگی[2] و پراکندگی[3] دو خاصیت رمزهای امن هستند. درهم‌پیچیدگی باعث می‌شود که رابطه‌ی متن رمزشده و کلید تا حد ممکن پیچیده شود و پراکندگی باعث می‌شود که رابطه‌ی بین متن رمزشده و متن واضح متناظرش تا حد ممکن کم شود. جایگزینی به عنوان مکانیزم اصلی درهم‌پیچیدگی شناخته شده است و در مقابل جایگشت[4] نیز یکی از تکنیک‌های پراکندگی می‌باشد. در رمزهای مدرن تکنیک‌های دیگری نظیر تبدیلات خطی[5] نیز برای پیچیده کردن هر چه بیشتر رمز به‌کار برده می‌شوند. دراین گونه رمزها مکانیزم‌های جانشینی و جایگشتی متناوبا به منظور درهم پیچیدگی و پراکندگی بیشتر رمز به کار می روند[1]. در واقع با طراحی S-Boxهای امن‌تر، رمزی با پیچیدگی بالاتر تولید می‌شود.

یک S-Box را می‌توان به طور ساده یک تابع بولی با n ورودی وm خروجی در نظر گرفت. در حال حاضر تلاش‌های محققان به سمت طراحی S-Boxهایی با حداکثر مقاومت در برابر حملاتی چون تحلیل خطی و تفاضلی می‌باشد. بدین منظور ویژگی‌های متفاوتی برای S-Boxها تعریف شده است. سه ویژگی منظم بودن، غیرخطی بودن و غیرهمبسته بودن، سه معیار مهم در طراحی S-Boxهای مقاوم می‌باشند.

در طراحی S-Box در این مقاله سه معیار فوق مدنظر می‌باشند. ثابت می‌شود که به دست آوردن S-Box هایی با این ویژگی‌ها در دسته‌ی مسائل NP-complete قرار می‌گیرد. بنابراین برای برآورده کردن این سه هدف به طور همزمان باید از روش‌های محاسبات تکاملی چندهدفه استفاده شود. در این مقاله با استفاده از الگوریتم ژنتیک میانگین رتبه به عنوان یکی از روش‌های حل مسائل چندهدفه به طراحی S-Box پرداخته شده است.

در بخش 2 این مقاله به معرفی کارهای مرتبط پرداخته می‌شود. در بخش 3 ابتدا S-Box ساده و سپس ویژگی‌های آن تعریف می‌شود. بخش 4 به تشریح الگوریتم ژنتیک میانگین رتبه می‌پردازد. در بخش 5 به مدل‌سازی مسئله در قالب الگوریتم ژنتیک پرداخته می‌شود. بخش 6 شامل نتایج بدست آمده می‌باشد. در فصل 7 مقایسه‌ای بین نتایج بدست آمده و کارهای مشابه پیشین به عمل می‌آید. فصل 8 خلاصه‌ای از آن‌چه در مقاله ارائه شده است را در بردارد.

2- کارهای مرتبط

روش‌های مختلفی برای ساختن S-Box وجود دارد که در دو دسته‌ی کلی روش‌های ریاضی و روش‌های تصادفی جای می‌گیرند. روش‌های ریاضی دارای این مزیت می‌باشند که ویژگی‌های لازم برای یک رمز خوب را در S-Boxها، تا حد خوبی فراهم می‌کنند[2]. به طور مثال الگوریتم رایندال[6] در رمز AES، S-Boxهایی می‌سازد که در مقابل حملات تحلیل تفاضلی و خطی کاملا امن می‌باشند[1]. اما S-Boxهایی که با روش‌های ریاضی ساخته می‌شوند در مقابل حمله‌ی جبری آسیب‌پذیر می‌باشند. روش‌های تصادفی از این بابت دارای قابلیت اعتماد بیشتری هستند.

یکی از این روش‌ها این است که به تصادف یک S-Box تولید شود و سپس میزان خوب بودن آن اندازه‌گیری شود که این روش بسیار ناکارا و زمان‌بر است. یکی دیگر از روش‌های تصادفی این است که S-Box های جدید بر مبنای یک سری S-Boxهای خوب و معروف ساخته شوند. مثلا S-Box رمز سرپنت[7] بر مبنای S-Boxهای رمز DES ساخته‌شده است. روشی دیگر، استفاده از الگوریتم‌های محاسبات نرم از قبیل الگوریتم تبریدسازی[8]، ژنتیک، بهینه‌سازی ازدحام ذرات[9] می‌باشد. در بیشتر مقالات معمولا یکی از ویژگی‌های لازم برای طراحی یک S-Box خوب مورد توجه قرار گرفته است. بنابراین در تمامی آن‌ها از الگوریتم‌های تکاملی ساده برای بهینه‌سازی استفاده شده است. در [3] از الگوریتم تبریدسازی برای بهینه‌سازی ویژگی غیرخطی بودن در S-Box استفاده شده است. در [4] نیز نویسندگان از الگوریتم بهینه‌سازی ازدحام ذرات برای S-Boxهای مطلوب استفاده کرده‌اند. همچنین در مقالات متعددی از الگوریتم ژنتیک برای طراحی S-Box استفاده شده است. در این مقالات ویژگی‌های متعددی برای s-Boxها مورد بهینه‌سازی قرار گرفته‌اند. مثلا در [2] نویسندگان سعی کرده‌اند با استفاده از الگوریتم ژنتیک S-Boxهای 8*8 بهینه تولید کنند. همچنین در [5] سعی شده است با استفاده از الگوریتم ژنتیک و الگوریتم تپه‌نوردی[10] S-Boxهایی با بیشترین میزان غیرخطی بودن ارائه شود. همچنین در [6] با بهره‌گیری از تئوری بازی‌های نش[7] و استفاده از مفاهیم الگوریتم ژنتیک، به طراحی S-Boxهایی 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-Boxهایی با همین سه ویژگی پرداخته شده است. نتایج بدست آمده در این مقاله با نتایج سه مقاله‌ی اخیر مقایسه می‌شود.

۳- S-box

S-Boxها نقش بسیار مهمی را در بسیاری از رمزهای قطعه‌ای مدرن دارند. در رمزنگاری بلوکی S-Boxها به منظور مبهم کردن

[1] Shanon Theory
[2] Confusion
[3] Diffusion
[4] Permutation
[5] Linear Transformation

[6] Rijndael
[7] Serpent
[8] Simulated Annealing (SA)
[9] Particle Swarm Optimization (PSO)
[10] Hill Climbing (HC)

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.

تعریف‌ها:

تعریف1. یک S-Box ساده، یک تابع بولی است که به صورت زیر تعریف می‌شود:

$$S: B^n \mapsto B \qquad (1)$$

تعریف2. یک S-Box خطی L به صورت زیر تعریف می‌شود:

$$L_\beta(x) = \oplus_{i=0}^{i=m} \beta_i L(x_i) \qquad (2)$$

تعریف3. پلاریته یک S-Box ساده به صورت زیر تعریف می‌شود:

$$\hat{S}(x) = (-1)^{S(x)} \qquad (3)$$

تعریف4. فاکتور غیرهمبستگی دو S-Box ساده‌ی S و S’ به صورت زیر تعریف می‌شود:

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

تعریف5. دو S-Box ساده‌ی S و S’ غیرهمبسته گفته می‌شوند، اگر و تنها اگر: $U_{s,s'} = 0$

تعریف6. میزان غیرخطی بودن S-Box ساده‌ی S توسط فاکتور غیرهمبستگی آن با تمام S-Boxهای ساده‌ی خطی ممکن آن اندازه‌گرفته می‌شود و به صورت زیر تعریف می‌شود:

$$\mathcal{N}_s = \frac{1}{2}\left(2^n - \max_{\alpha \in B^n} |\mathcal{U}_{s,x}|\right) \qquad (5)$$

تعریف7. میزان خودهمبستگی S-Box ساده‌ی S توسط فاکتور همبستگی‌اش با مشتقات D(x) آن به صورت زیر تعریف می‌شود:

$$A_s = \max_{\alpha \in B^n \setminus \{0^n\}} |\mathcal{U}_{s,D}| \qquad (6)$$

که در آن: $D(x) = S(x) \oplus \alpha$

برای همه‌ی $\alpha \in B^n \setminus \{0^n\}$

تعریف8. S-Box ساده‌ی S متوازن نامیده می‌شود اگر و تنها اگر تعداد ترکیبات $x \in B^n$ که به ازای آن‌ها $S(x) = 0$ است، برابر تعداد ترکیبات $y \in B^n$ باشد که با ازای آن‌ها $S(y) = 1$. میزان توازن S-Box ساده‌ی S توسط وزن همینگ آن و به صورت زیر تعریف می‌شود:

$$\mathcal{W}_s = \frac{1}{2}(2^n - \sum_{x \in B^n} \hat{S}(x)) \qquad (7)$$

تعریف9. یک S-Box، یک تابع بولی است که به صورت زیر تعریف می‌شود:

$$S: B^n \mapsto B^m \qquad (8)$$

تعریف10. S-Box تعریف شده‌ی S در بالا، الحاقی از m تا S-Box ساده‌ی S_i است که $1 \le i \le m$ و به صورت زیر نمایش داده می‌شود:

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

تعریف11. میزان غیرخطی بودن S-Box غیرساده‌ی S به صورت زیر محاسبه می‌شود:

$$\mathcal{N}_S = \min_{\beta \in B^m \setminus \{0^m\}} \mathcal{N}_{S_\beta(x)} \qquad (10)$$

که در آن:

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

تعریف12. میزان خودهمبستگی S-Box غیرساده‌ی S به صورت زیر محاسبه می‌شود:

$$\mathcal{A}_S = \max_{\beta \in B^m \setminus \{0^m\}} \mathcal{A}_{S_\beta(x)} \qquad (11)$$

تعریف13. به S-Box غیرساده‌ی S منظم گفته می‌شود اگر و تنها اگر به ازای هر $W \in B^m$، همان تعداد $x \in B^n$ وجود داشته باشد که $S(x) = W$. میزان منظم بودن یک S-Box به صورت زیر محاسبه می‌شود:

$$\mathcal{W}_S = \max_{\beta \in B^m \setminus \{0^m\}} |\mathcal{W}_{S_\beta(x)}| \qquad (12)$$

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

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

4- الگوریتم ژنتیک میانگین رتبه

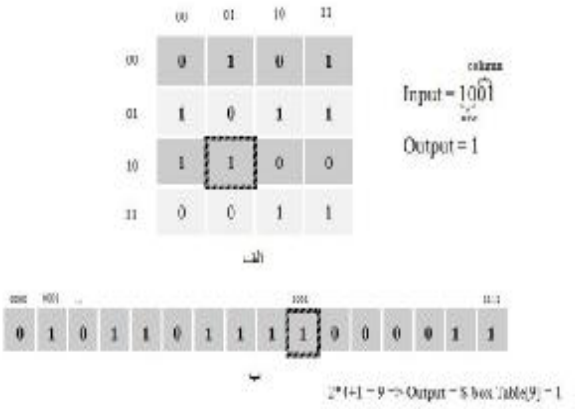
یکی از روش‌های حل مسائل چندهدفه در قالب الگوریتم ژنتیک، استفاده از الگوریتم ژنتیک میانگین رتبه می‌باشد. این روش یکی از روش‌های مبتنی بر جمعیت است[10]. در این الگوریتم، در پایان هر نسل، تمامی افراد جمعیت بر اساس هر کدام از معیارها به طور جداگانه رتبه‌بندی می‌شوند. به طور مثال در مسئله‌ی طراحی S-Box در 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.

5- مدل‌سازی مسئله در قالب الگوریتم ژنتیک

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

5-1- ساختار کروموزوم

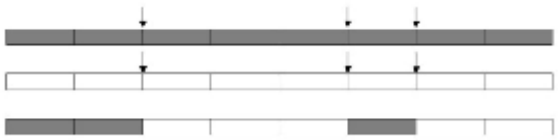
بطور ساده در این مسئله برای ساختن کرموزوم یعنی تبدیل فنوتایپ[11] به ژنوتایپ[12]، از یک آرایه‌ی بیتی استفاده شده است. هر S-Box دارای تعدادی بیت ورودی و تعدادی بیت خروجی است که تعداد بیت‌های ورودی و خروجی الزاما برابر هم نمی‌باشند. در این پیاده سازی تعداد بیت‌های ورودی ثابت و مساوی 8 بیت و تعداد بیت‌های 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 درکنارهم 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.



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

5-2- عملگرهای ژنتیکی

عملگر تقاطع ابتدا چندین نقطه به طور تصادفی در طول دو آرایه‌ی کرموزوم‌های 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 خانه های آرایه می باشند. شکل 2 نحوه‌ی اعمال عملگر تقاطع را نمایش می‌دهد.



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:

- ü حداکثر کردن میزان منظم بودن
- ü حداکثر کردن میزان غیرخطی بودن
- ü حداقل کردن میزان خود همبستگی

یعنی:

$$\begin{cases} \max\limits_{S} W_S^* \\ \max\limits_{S} N_S^* \\ \max\limits_{S} \left|\rho_S^2\right| \end{cases}$$

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 می شود 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 می آید.

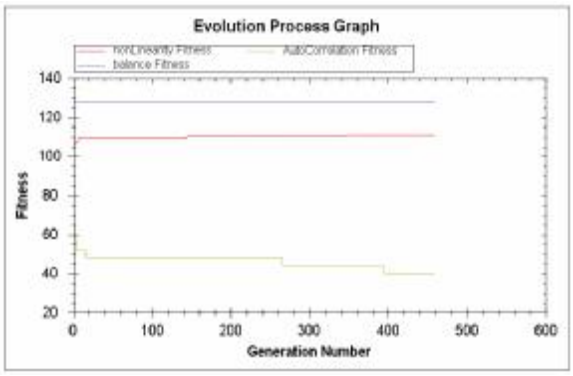
5-4- نحوه‌ی انتخاب

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

6- نتایج

برنامه در محیط 2008 net. 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.

[11] Phenotype
[12] Genotype
[13] Roulette Wheels



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

همان‌طور که مشاهده می‌شود با صعودی بودن نمودار دو ویژگی منظم بودن و غیرخطی بودن و نزولی بودن نمودار خودهمبستگی، همگرایی الگوریتم ژنتیک تضمین می‌شود.

جدول شماره‌ی 1 نتایج بدست آمده از روش پیشنهاد شده را نمایش می‌دهد.

جدول(1). نتایج

تعداد بیت‌های 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 جمع‌بندی

جدول 2 به مقایسه‌ی نتایج به‌دست آمده در این مقاله و کارهای مشابه پرداخته است.

همان‌طور که مشاهده می‌شود پیاده‌سازی این کار در مقایسه با کارهای انجام شده توسط ندجاه[6]، کلارک[8] و برنرت[9] نتایج بهتری داشته است. یعنی S-Boxهایی که از روش پیشنهاد شده بدست آمده‌اند غیرخطی‌تر و دارای همبستگی کمتری می‌باشند. 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 می‌باشد، رسیده‌اند و این نتیجه در تمامی کارها به طور مشابه به‌دست آمده است.

جدول(2).مقایسه

	نتایج برنرت		نتایج کلارک		نتایج ندجاه		نتایج کار ما	
	میزان غیرخطی بودن	میزان غیرهمبستگی بودن	میزان غیرخطی بودن	میزان غیرهمبستگی بودن	میزان غیرخطی بودن	میزان غیرهمبستگی بودن	میزان غیرخطی بودن	میزان غیرهمبستگی بودن
۵	۱۰۲	۷۲	۱۰۸	۵۶	۱۱۰	۵۶	۱۰۷	۵۶
۶	۱۰۰	۸۰	۱۰۶	۶۴	۱۰۶	۶۲	۱۰۷	۶۰
۷	۹۸	۸۰	۱۰۴	۷۲	۱۰۳	۷۰	۱۰۶	۵۶
۸	–	–	–	–	–	–	۱۰۷	۶۴

8- نتیجه‌گیری

در این مقاله یک الگوریتم ژنتیک مناسب برای حل مسائل چندهدفه به نام الگوریتم ژنتیک میانگین رتبه برای حل مسئله‌ی 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 رضایت‌بخش‌تر می‌باشد. بدین ترتیب، به عنوان کارهای آینده می‌توان این الگوریتم را روی S-Boxهایی با ویژگی‌های بیشتر و همچنین S-Boxهای بزرگتر (یعنی با تعداد بیت‌های ورودی و خروجی بیشتر) گسترش داد. همین‌طور می‌توان از روش‌های دیگر محاسبات تکاملی مثل SA و PSO یا روش‌های دیگر الگوریتم ژنتیک برای حل مسائل چندهدفه از قبیل روش‌های 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

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.