ا رائه ساختار جدیدی برای رمزنگاری بلاکی مبتنی بر اتوماتای سلولی 3 بعدی

سید مرتضی حسینی[1] ، حسین کریمی[2] ، مجید وفایی جهان[3]

[1] کارشناس ارشد، دانشگاه آزاد سلامی،واحد مشهد، گروه کامپیوتر نرم افزار Seyedmorteza.hosseiny@gmail.com
[2] کارشناس ارشد، دانشگاه آزاد سلامی،واحد مشهد، گروه کامپیوتر نرم افزار Th.karimi@gmail.com
[3] استادیار، دانشگاه آزاد سلامی،واحد مشهد، گروه کامپیوتر نرم افزار VafaeiJahan@mshdiau.ac.ir

چکیده - اتوماتای سلولی ساختاری خودسازمانده با مجموعه ای از سلول‌هاست که در آن هر سلول بوسیله قوانین مشخصی آپدیت می‌شود که به تعداد محدودی از سلول‌های همسایه وابسته است. اتوماتای سلولی دارای خصوصیاتی از قبیل ارتباطات محلی ،رفتار تکاملی و پیچیده و انجام موازی عملیات است که این خصوصیات باعث کاربرد آن در تولید اعداد تصادفی، رمزنگاری اطلاعات و حل مسائل بهینه‌سازی شده است. در این مقاله یک متد جدیدی از رمزنگاری بلاکی مبتنی بر مد رمزنگاری *CBC* با استفاده از ترکیب اتوماتای سلولی 3 بعدی بازگشت پذیر با قابلیت برنامه‌ریزی و *S-box* مبتنی بر آن ارائه شده است. برمبنای این طرح 16 قانون بازگشتی ارائه شده است. در این طرح از بلاک و کلید 256 بیتی برای رمزنگاری و رمزگشایی استفاده می‌شود بطوریکه کلید رمزنگاری برای هر بلاک متفاوت از بلاک دیگر می‌باشد. در اتوماتای سلولی 3 بعدی هر بیت از متن ساده با شش بیت از کلید همسایه است و بر طبق مقادیر همسایه‌ها یکی از 16 قانون بر روی آن اعمال می‌شود. نتایج بدست آمده از تحلیل رمز طرح ارائه شده نشان می‌دهد که این الگوریتم در برابر بسیاری از حملات شناخته شده دارای مقاومت بالایی می‌باشد.

کلید واژه- اتوماتای سلولی، رمزنگاری بلاکی، S_box، مد رمزنگاری CBC، خاصیت بهمن گونه

1- مقدمه

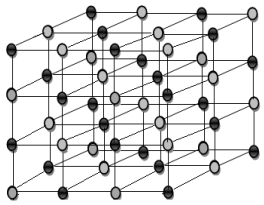
یکی از روش‌هایی که برای رمزنگاری اطلاعات مورد استفاده قرار می‌گیرد اتوماتای سلولی است. اتوماتای سلولی ساختار ساده؛ عملکردی تصادفی، رفتاری پیچیده و قابلیت موازی سازی بسیار بالا دارد[1,2]، که این خصوصیات کاربرد آنرا در رمزنگاری مطلوب کرده است. در سال 1986، ولفریم برای اولین بار از اتوماتای سلولی در رمزنگاری استفاده کرد، این کار توانایی اتوماتای سلولی را برای تولید بیت‌های تصادفی و همچنین رمزنگاری داده، آشکار کرد [3]. در سال 1994 نندی و همکاران اتوماتای سلولی قابل برنامه ریزی(PCA) را ارئه کرد که دریچه ای جدید برای رمزنگاری با اتوماتای سلولی شد. آنها استفاده از اتوماتای سلولی را در رمزگذاری جویباری و بلوکی، بررسی کرده‌اند و با استفاده از اتوماتای سلولی ترکیبی توانستند اعداد تصادفی با دنباله طولانی قابل قبولی تولید کنند و روشی برای رمزگذاری و رمزبرداری بلوکی با ارائه سخت‌افزار قابل برنامه‌ریزی ارائه دهند[4]. هاوارد گوتوویتز، اتوماتای سلولی بازگشتی (RCA) را ارائه کرد [5]که در آن متن با یک قانون رمز می‌شود و با قانون دیگر رمزگشایی می‌شود. به هر حال RCA نمی‌تواند فضای کلیدی بزرگی را در رمزنگاری پشتیبانی کند. در ادامه مطالعات بر روی RCA، در سال 2002 ، چانوو و همکاران یک متد جدیدی از رمزنگاری بر پایه RCA اراده دادند که فضای کلید بزرگی را شامل میشد[6]. در سال 2005، سردینسکی و بوری با استفاده از RCA یک رمزنگاری بلاکی را توسعه دادند[7]. در این مقاله سعی شده است که با استفاده از مد CBC، یک سیستم جدید رمزنگاری بلاکی مبتنی بر اتوماتای سلولی سه بعدی ارائه گردد. برای ایجاد کیفیت بهتر رمزنگاری یک ساختار جدیدی از S-box، مبتنی بر ساختار سه بعدی و شش همسایگی اتوماتای سلولی ارائه شده است که در هر دور از اجرا توسط کلید مقداردهی می‌شود. هر بلاک n دور رمز می‌شود و در هر دور کلید و مقدار بردار اولیه تغییر می‌یابند.

2- طرح پیشنهادی برای رمزنگاری

2-1- ساختار اتوماتای سلولی بکارگیری شده و نحوه رمزنگاری و رمزگشایی از طریق آن

در این طرح از یک اتوماتای سلولی 3 بعدی غیریکنواخت و با شرط مرزی چرخشی با ابعاد 4 × 8 × 8 استفاده شده است. این اتوماتای سلولی شامل 256 سلول است که 128 سلول آن شامل کلید و 128 سلول دیگر شامل بیت‌های متن اصلی است. هر سلول شامل بیت متن اصلی با شش سلول شامل بیت‌های کلید همسایه است و هر سلول شامل کلید نیز با شش سلول شامل بیت متن

اصلی همسایه است. شکل 1 نمایانگر بخشی از اتوماتای سه بعدی است که در آن سلول‌های پررنگ نمایانگر بیت‌های‌هایهای کلید و سلول‌های کمرنگ نمایانگر بیت‌های متن اصلی است.



شکل 1 : نمایی از ساختار یک اتوماتای سه بعدی $3 \times 4 \times 4$

2-1-1- رمزنگاری و اعمال قوانین در اتوماتای سلولی

در این طرح از شانزده قانون بنیادی اتوماتای سلولی (که بر یک اتوماتای سلولی یک بعدی باشعاع همسایگی 1 اعمال می‌شود و شامل 256 قانون می‌باشد) برای اعمال بر یک سلول شامل متن اصلی استفاده شده است. 16 قانون انتخاب شده در جدول 1 آمده است. علت انتخاب این 16 قانون این است که باید قوانینی انتخاب شوند که با دانستن مقادیر همسایه‌های یک سلول، آن قوانین بازگشت پذیر باشند که در بخش 3.1.2 به طور کامل توضیح داده شده است. اگر مختصات یک بیت از داده را $[x,y,z]$ بدانیم بیت‌های $[x,y,z-1]$ ، $[x,y-,[x,y,z+1]$ ، $[x,y+1,z]$ ، $[x+1,y,z]$ و $[x-1,y,z]$ به ترتیب یک شش بیتی را تشکیل می‌دهند که یک عدد از صفر تا 63 را تولید می‌کنند. باقیمانده این عدد بر شانزده یک عدد بین صفر تا پانزده تولید می‌کند که شماره قانون انتخابی برای آن سلول شامل داده ورودی خواهد بود. برای یک سلول شامل یک بیت از متن اصلی با مختصات $[x,y,z]$ سه دسته همسایگی مختلف تعریف شده است: 1- سلول‌های‌ $[x,y,z+1]$ و $[x,y,z-1]$، 2- سلول‌های $[x,y+1,z]$ و $[x,y-1,z]$ 3- سلول‌های $[x+1,y,z]$ و $[x-1,y,z]$. ابتدا قانون انتخابی بر اساس همسایه‌های اول بر روی سلول اجرا می‌شود، سپس همان قانون بر اساس همسایگی‌های دوم و نتیجه اعمال قانون در مرحله اول انجام می‌شود و سر انجام قانون بر اساس همسایگی‌های سوم و نتیجه اعمال قانون در مرحله دوم انجام می‌شود. همسایه‌های نوع اول، دوم یا سوم با سلول مورد نظر یک سه بیتی را تولید می‌کنند که یک عدد بین 0 تا 7 را تولید می‌کنند. برای اعمال قانون بر سلول با همسایگی مشخص، بیت با عدد مشخص شده توسط این سلول و همسایه‌های معینش، از نمایش بیتی آن قانون، جایگزین آن سلول می‌شود. به طور مثال اگر قانون انتخابی برابر قانون 108 باشد و مقدار یک سلول برابر 0 باشد و مقدار همسایه‌های نوع اول آن برابر 1 باشند، آنگاه عدد انتخابی برابر $(101)_2 = 5$ خواهد بود. پس با اعمال قانون 108 بر این سلول با همسایگی نوع اول، مقدار آن سلول برابر 1 می‌شود.

جدول 1: 16 قانون اعمال شده در اتوماتای سلولی

شماره قانون	نمایش باینری قانون	نمایش دهدهی	شماره قانون	نمایش باینری قانون	نمایش دهدهی
0	11001100	204	**8**	11001001	201
1	01101100	108	**9**	01101001	105
2	10011100	156	**10**	10011001	153
3	00111100	60	**11**	00111001	57
4	11000110	198	**12**	11000011	195
5	01100110	102	**13**	01100011	99
6	10010110	150	**14**	10010011	147
7	00110110	54	**15**	00110011	51

2-1-2 رمزگشایی بوسیله قوانین در اتوماتای سلولی

در این روش برای اینکه یک قانون قابلیت بازگشت داشته باشد، باید بیت‌های (0,2) ، (1,3) ، (4,6) ، (5,7) در آن قانون با هم متفاوت باشند. تعداد حالات ایجاد شده برای قوانین برابر 16 قانون است که در جدول 1 نشان داده شده است. علت این تفاوت این است که در بازگردان متن، آنچه مجهول است مقدار سلول در مرحله t ام است و قانون اعمال شده و همسایه‌های آن سلول و مقدار آن در زمان t+1 ام در دسترس است. با دانستن همسایگی‌ها 4 حالت بوجود می‌آید(0?0)، (0?1)، (1?0) ، (1?1) که هر حالت خود شامل دو حالت دیگر است. به طور مثال با داشتن همسایگی‌های 0، دو حالت (010)، (000) بوجود می‌آید. حال با دانستن مقدار در مرحله t+1 ام اگر مقدار بیت‌های با شماره حاصله از هر حالت در قانون با هم متفاوت باشند، به راحتی مقدار مرحله t ام بدست می‌آید.

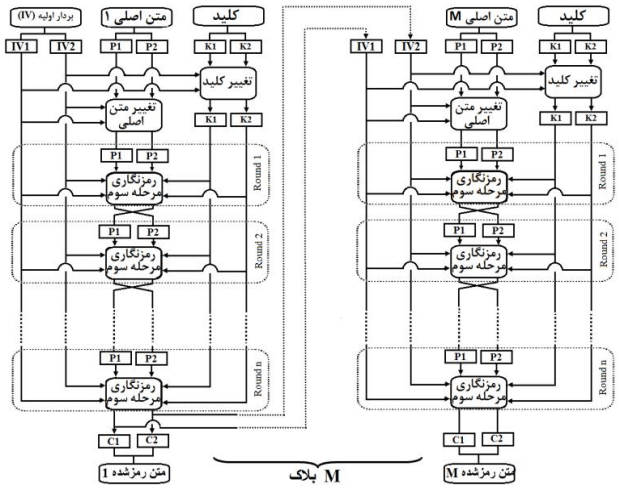
2-2- رمزنگاری و رمزگشایی از طریق s-box

در رمزنگاری، s-box (جدول جاینشینی) یک جزء اصلی در رمزنگاری کلید خصوصی است که عمل جانشینی را انجام می‌دهد. به طور کلی s-box شامل تعدادی بیت ورودی(m) و سپس تبدیل

شده آنها به تعدادی بیت خروجی (n) است. در بعضی از الگوریتم‌ها از s-box های ثابت (ایستا) استفاده می‌شود که در طول رمزنگاری تغییری نمی‌کنند، همانند des، ولی در بعضی از الگوریتم‌های دیگر از s-box های متغییر (دینامیک) استفاده می‌کنند که از طریق کلید ساخته می‌شوند، مانند الگوریتم‌های رمزنگاری Blowfish و Twofish . در این مقاله یک s-box 1 × 6 دینامیک جدید بر پایه اتوماتای سلولی سه بعدی ارائه می‌شود که بوسیله کلید در هر راند از اجرای الگوریتم مقداردهی می‌شود. در هر دور از اجرای الگوریتم این s-box بوسیله 64 بیت از کلید مقدار دهی می‌شود. اگر مقدار بیت برابر صفر باشد از عین مقادیر s- box برای جاینشینی استفاده می‌شود و اگر برابر یک باشد از عکس مقادیر s-box برای جاینشینی استفاده می‌شود. نحوه جاینشینی به این صورت است که همسایه‌های بالا، راست، جلو از یک سلول (با فرض مختصات $[x,y,z]$ برای سلول ، همسایه‌های $[x+1,y,z]$، $[x,y+1,z]$ و $[x,y,z+1]$) یک سه بیتی را تشکیل می‌دهند که مشخص کننده ستون در s-box است و همسایه‌های پایین، چپ، عقب (همسایه‌های $[x-1,y,z]$، $[x,y-1,z]$ و $[x,y,z-1]$) یک سه بیتی دیگر را تشکیل می‌دهند که مشخص کننده سطر در s-box است. سپس با استفاده از این مقادیر یک بیت از s-box مشخص می‌شود که باید جانشین مقدار سلول در مختصات $[x,y,z]$ شود. اگر مقدار سلول در این مختصات برابر صفر بود، همان مقدار بیت انتخاب شده در s-box با این بیت جایگزین می‌شود وگرنه عکس این مقدار جانشین آن خواهد شد. در رمزگشایی متن رمزشده بوسیله s-box، مقادیر s-box (بخش‌هایی از کلید)، مقدار رمزشده بیت (مقدار بیت در مرحله t+1 ام)و مقادیر همسایه‌های آن بیت(بخش‌هایی از کلید یا بردار IV) مشخص است. بوسیله همسایه‌های بیت رمزشده، همانطور که در بالا توضیح داده شد، سطر و ستون و در نتیجه مقدار بیت جایگزین شده در s-box مشخص می‌شود. حال اگر مقدار بیت انتخاب شده در s-box برابر با مقدار بیت در مرحله t+1 ام برابر باشد، پس مقدار بیت در مرحله t ام برابر 0 بوده است و گرنه مقدار بیت برابر 1 بوده است. به این ترتیب تمامی مقادیر رمز شده بوسیله s-box رمز گشایی خواهند شد.

3-2- طرح کلی پیشنهادی برای رمزنگاری

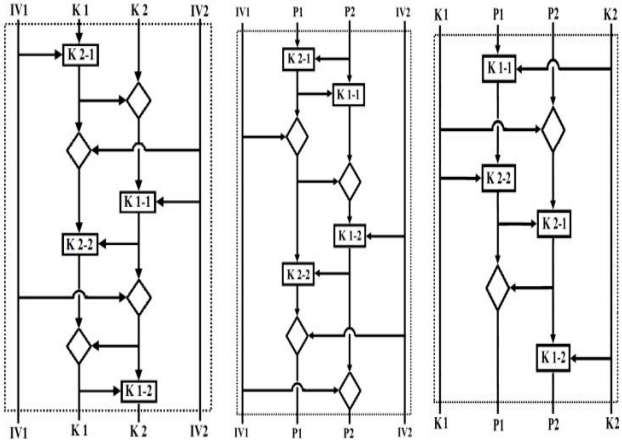
طرح کلی رمزنگاری در شکل 2 نشان داده شده است.اندازه کلید(k)، اندازه هر بلاک و اندازه برادر IV (بردار اولیه در مد CBC) برابر 256 بیت می‌باشد. در ابتدا متن ورودی (p)، به بلاک‌های 256 بیتی می‌شکند. سپس مقادیر P , IV , k به دو بخش 128 بیتی تقسیم می‌شوند، بطوریکه k1, IV1, p1 برابر 128 بیت ابتدایی از بردارهای k, IV, p می‌باشند و k2, v2, p2 برابر 128 بیت انتهایی آنها می‌باشند. رمزنگاری هر بلاک شامل سه مرحله کلی می‌باشد. در مرحله اول، مقادیر کلید توسط بردار IV و با استفاده از اتوماتای سلولی سه بعدی و s-box تغییر می‌یابند. شکل (a)3 نشان دهنده بخش اول(چگونگی تغییر کلید) می‌باشد.



شکل 2 : ساختار کلی رمزنگاری با m بلاک و n دور رمز در هر بلاک

که در آن، شکل ◇ نمایانگر عملیات رمزنگاری بوسیله اتوماتای سلولی می‌باشد و شکل $K_{i,j}$ نمایانگر عملیات رمزنگاری بوسیله s-box می‌باشد که بخش j ام از زیر کلید iام، نشان دهنده مقادیر آن می‌باشد. به طور مثال k1,2 نشان دهنده این است که s-box بوسیله 64 بیت انتهایی (127-64) زیر کلید 128 بیتی k1 مقدار دهی شده است. **مرحله اول** شامل 8 قسمت می‌باشد: 1- اتوماتای سلولی بوسیله k1 و IV1 مقداردهی می‌شود بطوریکه هر بیت از k1 با شش بیت از IV1 همسایه باشد. سپس s-box بوسیله 64 بیت ابتدایی از زیرکلید k2 مقدار دهی می‌شود. سپس هر بیت از k1 با استفاده از همسایگانش همانطور که در بخش 2-2 توضیح داده شده است، با یک بیت از s-box جایگزین می‌شود. 2 - اتوماتای سلولی بوسیله k2 و مقدارk1 بدست آمده از قسمت قبل مقداردهی می‌شود، بطوریکه هر بیت از k2 با شش بیت از k1

همسایه می‌باشد، یعنی k2 بعنوان متن اصلی باشد و k1 بعنوان کلید رمزنگاری باشد. سپس قوانین معرفی شده در جدول 1، همانطور که در بخش 2-1 توضیح داده شده است بر روی مقادیر k2 اعمال می‌شوند. 3-اتوماتای سلولی بوسیله مقدارk1 بدست آمده از قسمت 1 و IV2 مقداردهی می‌شود بطوریکه هر بیت از k1 با شش بیت از IV2 همسایه باشد. سپس قوانین معرفی شده در جدول 1، همانطور که در بخش 2-1 توضیح داده شده است بر روی مقادیر k1 اعمال می‌شوند. - اتوماتای سلولی بوسیله مقدارk2 بدست آمده از قسمت 2 و IV2 مقداردهی می‌شود، بطوریکه هر بیت از k2 با شش بیت از IV2 همسایه باشد. سپس s-box بوسیله 64 بیت ابتدایی از زیرکلید k1 مقدار دهی می‌شود. 4 سپس هر بیت از k2 با استفاده از همسایگانش همانطور که در بخش 2-2 توضیح داده شده است، با یک بیت از s-box جایگزین می‌شود.



(a) مراحل و ساختار تغییر کلید توسط بردار اولیه در ابتدای هر بلاک

(b) مراحل و ساختار تغییر متن توسط بردار اولیه در ابتدای هر بلاک

(c) مراحل و ساختار تغییر متن توسط کلید (n بار در هر بلاک)

شکل 3 : سه بخش اصلی رمزنگاری

5- اتوماتای سلولی بوسیله مقدارk1 بدست آمده از قسمت 3 و مقدار k2 بدست آمده از قسمت قبل مقداردهی می‌شود، بطوریکه هر بیت از k1 با شش بیت ازk2 همسایه باشد. سپس s-box بوسیله 64 بیت انتهایی از زیرکلید k2 مقدار دهی می‌شود. سپس هر بیت از k1 با استفاده از همسایگانش همانطور که در بخش 2-2 توضیح داده شده است، با یک بیت از s-box جایگزین می‌شود. 6- اتوماتای سلولی بوسیله مقدارk2 بدست آمده از قسمت4 و IV1 مقداردهی می‌شود بطوریکه هر بیت از k2 با شش بیت از IV1 همسایه باشد. سپس قوانین معرفی شده در جدول 1، همانطور که در بخش 2-1 توضیح داده شده است بر روی مقادیر k2 اعمال می‌شوند. 7- اتوماتای سلولی بوسیله مقدارk1 بدست آمده از قسمت 5 و مقدارk2 بدست آمده از قسمت قبل مقداردهی می‌شود بطوریکه هر بیت از k1 با شش بیت از k2 همسایه باشد. سپس قوانین معرفی شده در جدول 1، همانطور که در بخش 2-1 توضیح داده شده است بر روی مقادیر k1 اعمال می‌شوند. 8-اتوماتای سلولی بوسیله مقدارk2 بدست آمده از قسمت6 و مقدارk1 بدست آمده از قسمت قبل مقداردهی می‌شود بطوریکه هر بیت از k2 با شش بیت از k1 همسایه باشد. سپس s-box بوسیله 64 بیت انتهایی از زیرکلید k1 مقدار دهی می‌شود. سپس هر بیت از k2 با استفاده از همسایگانش همانطور که در بخش 2-2 توضیح داده شده است، با یک بیت از s-box جایگزین می‌شود. در **مرحله دوم** مقادیر متن ورودی با استفاده از بردار IV تغییر می‌یابند. این مرحله نیز شامل 8 قسمت می‌باشد و اساس کار آن مشابه با مرحله اول می‌باشد. شکل (b)3 نشان دهنده ساختار تغییر متن بوسیله بردار IV می‌باشد. **مرحله سوم** شامل تغییر مقادیر متن ورودی با استفاده از کلید می‌باشد. چگونگی انجام این کار در شکل (c)3 نشان داده شده است. این مرحله شامل 6 قسمت می‌باشد و اساس کار آن مشابه با مرحله اول و دوم می‌باشد. مرحله سوم به اندازه n بار تکرار می‌شود و در هر دور همانطور که در شکل2 مشخص است، مقادیر P1 و P2 عوض می‌شوند. سر انجام پس از n راند، متن رمزشده بلاک اول تولید می‌شود و این متن که شامل 256 بیت می‌باشد، بعنوان بردار IV در بلاک بعدی مورد استفاده قرار می‌گیرد.

3- تحلیل رمز

تحلیل رمز هنر و علم شکستن رمز برای آشکارسازی یک متن اصلی مشخص یا کلید مخفی[8] می باشد. این تحلیل می تواند در هر دو نوع خطی یا تفاضلی باشد. حمله کننده معمولا از ارتباط بین متن ورودی و متن رمزشده برای بدست آوردن کلید استفاده می کند. در رمزنگاری بلاکی از دو مشخصه برای ارزیابی میزان و چگونگی ارتباط بین متن اصلی و رمزشده استفاده می شود: خاصیت بهمن گونه و خاصیت کامل بودن[9]. مفهوم خاصیت بهمن گونه و کامل بودن توسط وبستر و توارس ترکیب شدند. آنها خاصیت اکیدا بهمن گونه (SAC) را تعریف کردند. بر طبق این خاصیت، هر بیت از متن رمز شده باید با احتمال 50 درصد وقتی

که یک بیت از متن اصلی تغییر کرد، تغییر کند. اگر الگوریتمی دارای خاصیت sac باشد بدست آوردن ارتباط بین متن اصلی و متن رمزشده و تشخیص کلید به علت رفتار رندم گونه و بسیارپیچیده آن بسیار مشکل می باشد و در برابر اکثر حملات معروف تحلیل رمز مقاومت خواهد کرد. بدین منظور در این مقاله از روشی که در [10] بیان شد برای تست این خاصیت بر روی طرح ارائه شده استفاده می‌شود: این آزمون با بررسی تاثیر تغییر یک بیت ورودی در بیتهای خروجی انجام می‌شود و نحوه پیاده سازی آن بصورت زیر می‌باشد: اگر تعداد بیت‌های ورودی تابع، برابر n و تعداد بیت‌های خروجی، برابر m باشد، ابتدا یک ماتریس (ماتریس SAC)، با ابعاد $n \times m$که تمام مقادیر آن صفر است، در نظر گرفته می‌شود. سپس یک داده ورودی به صورت تصادفی تولید شده و خروجی محاسبه می‌گردد. بیت iام $(0 < i \leq n)$ از داده ورودی معکوس شده و خروجی دوباره محاسبه می‌شود. در نهایت، دو خروجی با یکدیگر XOR شده و با مقادیر سطر iام از ماتریس SAC جمع می‌گردد. به عبارت دیگر، اگر در بیت jام، دو خروجی یکسان نباشد، به مقدار عنصر (i,j)ام از ماتریس، یک واحد افزوده می‌شود. این کار برای 2^{20} بار تکرار می‌شود. بنابراین، ارزش مورد انتظار از هر یک از ورودی‌های ماتریس، در حدود 2^{19} است و توزیع ارزش ماتریس باید یک توزیع نرمال را دنبال کند. بعد از انجام تست، برای ارزیابی ماتریس SAC، ، از آزمونx^2 متناسب با مقادیر مورد انتظار داده شده در جدول (1) استفاده می‌شود[10]. هدف این روش بررسی توزیع کلی داده‌ها است.. اگر در ماتریس، یک مقدار p-value کمتر از 0.01 وجود داشته باشد، تابع غیر تصادفی خواهد بود.

جدول 2: محدوده‌ها و احتمالات آزمون SAC برای 2^{20} بار

Bin	Range	Probability
1	0-523857	0.200224
2	523858-524158	0.199937
3	524159-524417	0.199677
4	524418-524718	0.199937
5	524719-1048576	0.200224

در طرح ارائه شده، ماتریس sac برابر [0.2703,0.1267,0.1565,0.1433,0.3032] بدست آمده است که همانطور که مشاهده می‌شود تمامی مقادیر آن بالاتر از 0.01 می باشد و این نشانگر این موضوع می باشد که این الگوریتم دارای خاصیت sac میباشد. بنابراین حمله کننده با داشتن n جفت متن اصلی و متن رمز شده نخواهد توانست به کلید یا بخشی از آن دست یابد و برای آشکار سازی کلید باید فضایی جستجویی تقریبا برابر با فضای جستجوی کلید را بررسی کند.

4- نتیجه

در این مقاله سعی شد که روش نوینی برای رمزنگاری بلاکی با استفاده از اتوماتای سلولی سه بعدی بر مبنای مد رمزنگاری CBC ارائه شود. علاوه بر این از s-box برای نامفهوم کردن ارتباط بین کلید و متن رمزشده و همچنین مقاومت در برابر حملات رمزگشایی استفاده شده است. برای رمزنگاری بر پایه اتوماتی سلولی 3 بعدی، 16 قانون با قابلیت بازگشتی ارائه شده است که عملیات رمزنگاری و رمزگشایی با اتوماتای سلولی برپایه این قوانین می‌باشد. برای هر سلول، با استفاده از مقادیر آن سلول و همسایگانش یکی از 16 قانون انتخاب می‌شود. در هر دور از رمزنگاری ابتدا با استفاده از بردار اولیه، کلید و متن اصلی رمز می-شود و سپس برای n دور، متن اصلی توسط کلید رمز میشود. نتایج تحلیل رمز نشان دهنده مقاومت بالای این الگوریتم در برابر حملات شناخته شده می باشد.

مراجع

[1] L.chen, R.zhang, “A Fast Encryption Mode for Block Cipher with Integrity Authentication” , ieee, 2008.

[2] S. Wolfram, "Theory and Applications of Cellular Automata" , River Edge, NJ: World Scientific, pp: 1983–1986, 1986.

[3] S. Wolfram, “Cryptography with cellular automata,” in Proc. CRTPTO 85—Advances in Cryptography, vol. 218, pp: 429–432, 1985.

[4] S. Nandi, B. K. Kar, and P. P. Chaudhuri, “Theory and applications of cellular automata in cryptography,” IEEE Transactions on Computers, Vol. 43, pp:1346–1357, 1994.

[5] H.Gutowitz,” Cryptography with Dynamical Systems”, Internet:, http:// www.santafe.edu /~hag /crypto /crypto /crypto.html , 1996.

[6] Z.Chuanwu, P.Qicong, L.Yubo,“encryption based on reversible cellular automata “, communications, Circuits and systems and West Sino Expositions, IEEE 2002 international conference, Vol.2, pp. 1223-1226, 2002.

[7] M.Seredynski, P.Bouvary,”Block Cipher Based on Reversible Cellular Automata”, New Generation Computing, Vol.23, pp.245–258, 2005.

[8] Bruce Schneiner, “Applied Cryptography: Protocols, Algorithms and Source Code in C”, Wiley, New York, pp. 13, 1996.

[9] J. B. Kam and G. I. David, “Structured Design of Substitution-Permutation Encryption Networks”, IEEE Trans. on Computers, vol. 28, pp.747-753, 1979

[10] B.EGE , “Structural Testting of Block Ciphers and Hash Function”, the Degree of Master of Science, 2010: http:// www3.iam.metu.edu.tr /iam /images /8 /8e /Barisege.pdf.