هفتمین کنفرانس مهندسی برق ایران
مرکز تحقیقات مخابرات ایران
۲۷-۲۹ اردیبهشت ۱۳۷۸

اتوماتای سلولی و کاربرد آن در رمزنگاری

(بهبود مولد دنباله کلید با بکارگیری اتوماتای سلولی مشبک)

عباس قائمی بافقی محمد رضا میبدی بابک صادقیان

دانشگاه صنعتی امیر کبیر
دانشکده مهندسی کامپیوتر
g7631950@cic.aku.ac.ir

چکیده

دو ویژگی مهم دنباله کلید اجرایی در رمزنگاری ، دارابودن دوره تکرار[1] بزرگ و حصول ویژگی های آماری مناسب می باشد. ویژگی مهم دیگر در تولید کلید اجرایی بویژه در رمزنگاری دنباله ای، سرعت روند اجرای مولد می باشد. یک روش اولیه در تولید دنباله کلید با دوره تکرار بالا استفاده از ثبات های انتقال می باشد که علی رغم تولید حلقه های بزرگ، بعلت ترتیبی بودن ساختار و روند اجرایی آن، کارایی و سرعت نسبت به سیستم های موازی کمتر می باشد. در سال ۱۹۹۵ سیستم رمزی با ساختار شبه DES توسط تسالیدس و همکاران او با بکارگیری اتوماتای سلولی پیاده سازی شد ، که با بکارگیری روش موازی مربوطه روند اجرا سرعت داده شده است [۳] . در آن سیستم از اتوماتای خطی جهت عملیات رمز و تولید کلیداجرایی ز از روی کلید مخفی استفاده شده که دارای دوره تکرار کوچک است.

ما در این مقاله روش تولید کلید را ، با بکارگیری اتوماتای دو بعدی با بهنگام سازی خطی ، در سیستم رمز مربوطه بهبود بخشیده ایم. دنباله کلید تولید شده با این روش علاوه بر تولید حلقه های با طول بزرگ ، ویژگی های آماری مناسبی را از خود نشان داده است. در طرح اولیه با استفاده از اتوماتای خطی ۸ سلولی حداکثر طول حلقه ها برابر ۱۷ است ، که با طرح جدید با بکارگیری اتوماتای مشبک ۳×۳ به ۴۹۲ می رسد . همچنین دنباله های تولید شده با طول بزرگ در آزمون های تکرار ، توالی ، پوکر ، ران ، مشتق دودویی، همبستگی ، و پیچیدگی خطی قبول می گردند .

کلمات کلیدی : اتوماتای سلولی ، رمزنگاری ، ساختار رمز شبهDES ، مولد دنباله کلید اجرایی ، تمامیت .

۱- مقدمه

رمزنگاری عبارتست از تبدیل کردن اطلاعات مورد نظر به یک سری داده به ظاهر نامفهوم ، که تبدیل تحت یک دنباله دلخواه بنام کلید انجام می شود . بطوریکه کلید بطور مخفی بین فرستنده و گیرنده اطلاعات قرارداد می شود و تنها این دو فرد از آن با خبر می شوندو دنباله کلید اجرایی براساس کلید مخفی تولید می گردد. انجام عملیات رمز گشایی بدون داشتن کلید مخفی بسیار پیچیده و وقت گیر می باشد ، در حالیکه ترجمه رمز با داشتن کلید مخفی با سرعت و به سهولت امکانپذیر است [۲] .

از آنجا که ساختار رمز برای همگان معلوم و مشخص است و قوت سیستم رمز مبتنی بر پیچیدگی بین ورودی/خروجی و کلید می باشد، تولید دنباله کلید از روی کلید مخفی اهمیت قابل توجهی دارد. چند ویژگی لازم برای مولد دنباله کلید عبارتست از: تولید حلقه های با طول بزرگ و ارضای تست های آماری و نیز سرعت و کارایی بالا در تولید دنباله کلید [۱].

[1] Period

روش اولیه در تولید دنباله کلید با دوره تکرار بالا استفاده از ثباتهای انتقال می باشد. این روش علی رغم تولید حلقه های بزرگ، بعلت ترتیبی بودن روند اجراء ، نسبت به سیستم های موازی کارایی و سرعت کمی دارد. اتوماتای سلولی یک ساختار موازی می باشد که می توان آنرا در پیاده سازی مولد دنباله کلید بکار گرفت. در سال ۱۹۹۵ سیستم رمزی با ساختار شبه DES با یک اتوماتای سلولی خطی پیشنهاد شد [۳] ، که البته دنباله های تولید شده برای کلید دارای دوره تکرار کوچک می باشد . ما در این مقاله ابتدا مولد کلید بکارگرفته در روش فوق را مورد ارزیابی قرار داده و سپس با بکارگیری توپولوژی مشبک در اتوماتای سلولی و بهنگام سازی خطی، آن را بهبود بخشیده ایم . این روش ضمن دارابودن ساختار موازی و کارایی بالا ، دنباله های بزرگ تولید کرده و ویژگی های آماری را نیز به خوبی ارضاء می کند .

در ادامه مقاله ، ابتدا ماشین اتوماتای سلولی را معرفی کرده و سپس سیستم رمز با ساختار شبه DES ، که با بکارگیری اتوماتای سلولی خطی در سال ۱۹۹۵ توسط تسالیدس و همکارانش انجام شده ، را بطور مختصر تشریح می نماییم. در انتها روشی برای بهبود مولد کلید ارائه کرده و دنباله های کلید تولید شده توسط این مولدهای بهبود یافته را به لحاظ طول دوره تکرار و ارضای تست های آماری مورد بررسی قرار می دهیم.

۲- معرفی ماشین اتوماتای سلولی (Cellular Automata Machines CAM)[۴]:

ماشین اتوماتای سلولی یک ساختار موازی هماهنگ[1] است بطوریکه :

(۱) فضا توسط یک سطح یکنواخت ارائه می شود.

(۲) هر سلول شامل تعدادی بیت داده است (وضعیت جاری سلول).

(۳) زمان[2] بصورت گسسته در نظر گرفته می شود.

(۴) وضعیت بعدی هر سلول با توجه به وضعیت فعلی آن و همسایه هایش تعیین می گردد.

(۵) قوانین حاکم بر سیستم محلی[3] و یکنواخت[4] می باشد.

در ماشین اتوماتی سلولی اولاً قوانین برای همه یکسان است و تنها در شرایط مرزی و شرایط محیط متفاوت می باشند (یکنواختی) و ثانیاً هر کس با توجه به خود و اطرافیان، نزدیکان و یا بعبارت دیگر همسایگانش برای آینده اش تصمیم می گیرد.

در نمونه های کاربردی اتوماتای سلولی اغلب دارای چندین میلیارد سلول (مثلاً 10^9) است ومقادیر (وضعیت) هر سلول ممکن است تا یک میلیون مرتبه بهنگام شود. این تعداد و تکرار زیاد در اتوماتای سلولی باعث نیاز به صرف وقت زیاد دارد. مجموعاً 10^{15} مرتبه بهنگام سازی لازم است. اگر بخواهیم از سیستم های ترتیبی استفاده نموده و سیستم را شبیه سازی نماییم چندین سال برای محاسبه اتوماتای سلولی فوق وقت نیاز خواهیم داشت. از طرفی اگر بخواهیم از سیستم های موازی همه منظوره (بطور مثال سیستم موازی PC) استفاده نمائیم، بعلت آنکه از امکانات در نظر گرفته شده در کامپیوترهای همه منظوره استفاده چندانی نمی شود، امکانات هدر می رود. لذا به طراحی سیستمی برای پردازش اتوماتای سلولی می پردازیم که ماشین فوق را CAM می نامیم.

۲-۱ ویژگی های ماشین اتوماتای سلولی (CAM)

اتوماتای سلولی را می توان از جهات مختلف دسته بندی ومقایسه کرد از جمله به لحاظ توپولوژی شبکه سلولی، همسایگان، وضعیت ها، و بهنگام سازی شبکه. از لحاظ توپولوژی شبکه سلولی می توان شکل و بعد شبکه را مد نظر داشت که به لحاظ شکل، شبکه سلولی می تواند مربع، چند ضلعی، ... و به لحاظ بعد می تواند دارای بعدهای متفاوت خطی، دو بعدی، سه بعدی و ... باشد.

با توجه به اینکه گفتیم تصمیم گیری آینده در هر سلول با توجه به وضعیت فعلی خودش و همسایگانش می باشد بایستی محدودهٔ همسایگان یک سلول را مشخص نمائیم. معمولاً شکل محدودهٔ همسایگان بصورت فاصله از یک سلول در نظر گرفته می شود یعنی سلولهایی که به یک فاصله معین (افقی، عمودی، مورب) از یک سلول قرار دارند همسایه آن سلول نامیده می شود. و به لحاظ مرزی برای سلولهایی که در مرز جامعه (شبکه) قرار دارند می توان همسایگی را بصورت دوری در نظر بگیریم که در این صورت دو سلول در دو انتهای مرزی همسایه یکدیگر می باشند و یا می توان مرز تهی در نظر بگیریم که در این صورت در شرایط مرزی وضعیت همسایگان سلول صفر منظور می شود.

---

[1] Synchron

[2] Clock

[3] Local

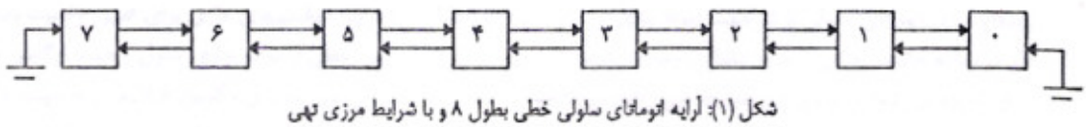
[4] Uniform

وضعیت جاری هر سلول را توسط متغیر محلی آن معین می نمائیم که وضعیت هر سلول ممکن است دو مقداری (مرگ و زندگی) یا چند مقداری باشد. که این بسته به مساله مورد بحث متفاوت است.

اتوماتای سلولی به لحاظ بهنگام سازی به چندین نوع تقسیم بندی می شود. اولا ٌ به لحاظ خود گردان بودن بهنگام سازی و ثانیاً به لحاظ نوع قوانین (خطی/ غیر خطی) حاکم بر اتوماتای سلولی که در ادامه پس از ارائه دو نمونه اتوماتای سلولی بیان و تشریح می شوند.

(الف) اتوماتای سلولی خطی :

شکل (۱) اتوماتای سلولی، با توپولوژی خطی بر شرایط مرزی تهی، دارای وضعیت دو مقداری و متأثر از دو همسایهٔ مجاورش (شعاع همسایگی یک) نشان داده شده است.



شکل (۱): آرایه اتوماتای سلولی خطی بطول ۸ و با شرایط مرزی تهی

در اتوماتای سلولی خطی هر سلول متأثراز تنها دو همسایه اش می باشد و داریم:

$$X_i(t+1) = f\left(X_{i-1}(t), X_i(t), X_{i+1}(t)\right)$$

که در آن $X_\alpha(\beta)$ وضعیت سلول α ام در زمان β ام می باشد. از آنجا که هر سلول دو وضعیت دارد سه سلول مجاور (سلول جاری و همسایگانش) $2^3 = 8$ ترکیب مختلف می تواند داشته باشد، که وضعیت سلول جاری با توجه به هریک از این ترکیبات در زمان بعدی متفاوت خواهد بود. با کنار هم قراردادن وضعیت بعدی سلول i ام به ازای ترکیبات مختلف ۱۱۱، ۱۱۰، ... ، ۰۰۰ (از چپ به راست) یک عدد دهدهی بدست می آید که شماره قانون حاکم بر اتوماتای سلولی است.

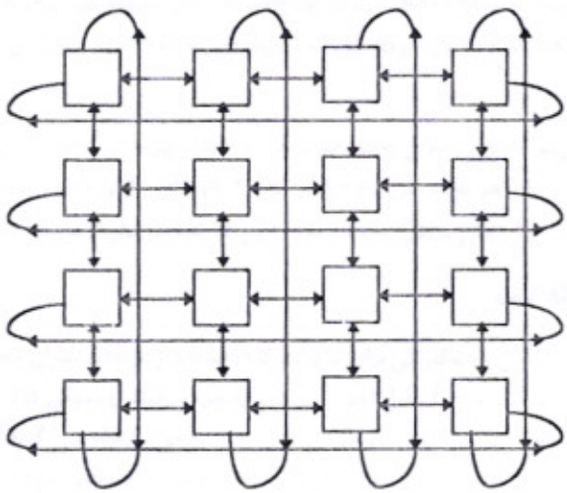
مثال: قانون ۹۰ در اتوماتای سلولی خطی بصورت زیر می باشد.

حالت فعلی	۰۰۰	۰۰۱	۰۱۰	۰۱۱	۱۰۰	۱۰۱	۱۱۰	۱۱۱
حالت بعدی	۰	۱	۰	۱	۱	۰	۱	۰

که : $(۰۱۰۱۱۰۱۰)_۲ = (۹۰)_{۱۰}$

ب) اتوماتای سلولی مشبک (دو بعدی):

در این ماشین اتوماتای سلولی، سلولها در یک توپولوژی مشبک به هم متصل می باشند. اگر شعاع همسایگی را یک در نظر بگیریم هر سلول داخلی دارای ۸ همسایه، هر یک از سلولهای مرزی دارای ۵ همسایه و سلولهای گوشه هر یک دارای ۳ همسایه خواهند بود. در این ساختار نیز می توان شبکه را دوری در نظر گرفت که در این صورت تمامی سلولهای اتوماتای سلولی حاصل هر یک دارای ۸ همسایه خواهند بود. در شکل (۲) یک اتوماتای سلولی دوری ۴ × ۴ نشان داده شده است.



شکل(۲) : اتوماتای سلولی مشبک ۴ × ۴ با شرایط مرزی دوری

در اتوماتای مشبک نیز می توان وضعیت بعدی هر سلول را با توجه به وضعیت فعلی خودش و وضعیت همسایگانش تحت یک قانون تعیین کـرد. این قانون را می توان بطور مشابه اتوماتای خطی بدست آورد که توسط یک عدد دهدهی در فاصلهٔ $[0,2^{512}]=[0,2^{512}]$ نشان داده مـی شـود. از آنجا که این عدد بزرگ می باشد قوانین خطی را می توان با یک عدد دهدهی در فاصله $[0,2^{9}]$ نشان داد که اگر آنرا بصورت دودویی در نظـر بگیریم ضرایب معادله حالت سلول خواهند بود. یعنی اگر قانون بصورت $(a_0,a_1,a_2,\ldots,a_8)_2$ باشد معادلـه حـالت سـلول X_{ij} بصـورت زیـر است.

$$X_{ij}(t+1)=\sum_{k=0}^{8} a_k \; X_{i+k \bmod 3, j+\lfloor k/3 \rfloor}$$

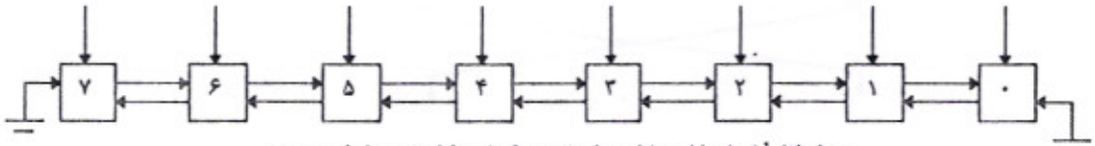
۲-۲ انواع بهنگام سازی

بهنگام سازی اتوماتای سلولی از دو جهت دسته بندی می شود . اولاً به لحاظ نحوه ترکیب وضعیتهای جاری برای تعیین وضعیت بعدی ماشین که اگر در معادله حالت، وضعیت بعدی سلول باتوجه به وضعیت جاری سیستم تنها ترکیب خطی از مقدار جاری سلول و همسـایگانش باشـد، قـانون خطی نامیده می شود و در غیر این صورت غیر خطی خواهد بود. ثانیاً اگر برای تعیین وضعیت بعـدی ماشـین عـلاوه بـر وضعیـت جـاری آن یـک ورودی از خارج نیز دریافت نماییم بهنگام سازی غیر خودگردان خواهد بود. در این صورت وضعیت بعدی آنرا با توجـه بـه مقـدار ورودی و وضعیـت جاری اتوماتای سلولی معین می سازیم یعنی :

$$S(t+1)=T_R.s(t)+K(t)$$

که در آن T_R ماتریس اتوماتای سلولی و $k(t)$ ورودی در لحظه t ام است.

اگر تصمیم گیری وضعیت آینده ماشین تنها با توجه به وضعیت جاری آن و مستقل از عوامل خارجی صـورت پذیـرد بهنگـام سـازی را خودگـردان می گوئیم. می توان اتوماتای سلولی خودگردان را نوع خاصی از اتوماتای سلولی غیرخودگردان در نظر گرفت که مقدار ورودی تمامی زمانها برابـر صفر است. اتوماتای معرفی شده در شکل (۱) یک اتوماتای سلولی خودگردان است. نمونه غیرخودگردان این اتوماتا در شکل (۳) آمده است.



شکل (۳): آرایه اتوماتای سلولی خطی غیر خودگردان بطول ۸ و شرایط مرزی تهی

۳- پیاده سازی الگوریتم رمز شبهDES با بکارگیری اتوماتای سلولی

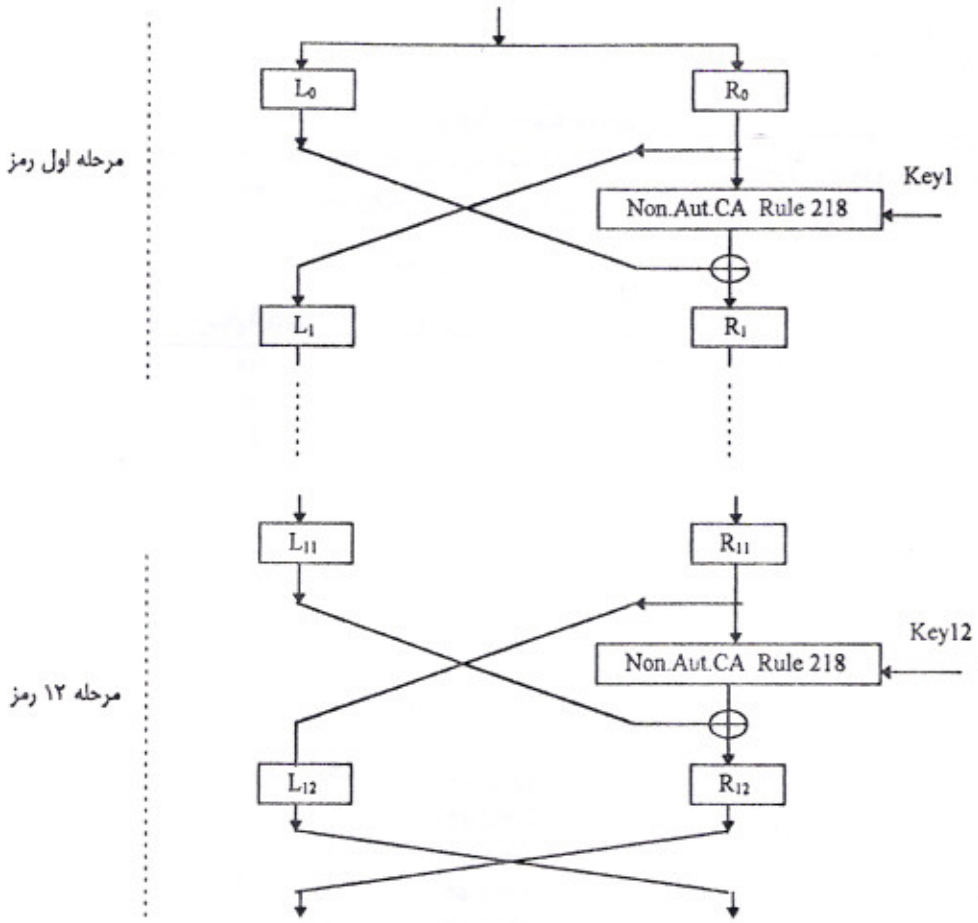
تسالیدس و همکارانش در سال ۱۹۹۵ سیستم رمزی با ساختار شبه DES با ۱۲ مرتبه تکرار را با بکارگیری اتوماتای سلولی غـیر خودگـردان پیـاده سازی کردند . آنها در هر مرحله به جای تابع f یک اتوماتای سلولی غیرخودگردان خطی ۸ سلولی با قانون ۲۱۸ بعنوان نمونه بکار بردند[۳] . نحوه عملکرد اتوماتای سلولی مانند شکل (۳) است بطوریکه ۸ بیت کلید رمزنگاری در ۱۲ مرحله متوالی ساختار با برچسب Key1 تـا Key12 در شـکل (۴) بیان شده است.

می توان رمزنگاری را بصورت Pipeline انجام دهیم در این صورت هنگامی که پیام اول در مرحله اول رمـز شـده و آمـاده ارسـال بـه مرحلـه دوم می شود با پالس بعدی، یک پیام جدید وارد مرحله اول شده و پیام قبلی به مرحله دوم منتقل می شود. لذا بطور متوسط در ۱۲ پالس سـاعت ۱۹۲ = ۱۶ × ۱۲ بیت رمز می شود.

بعلت با قاعدگی بالا الگوریتم حاصل در مقابل تحلیل آسیب پذیر می باشد. پیچیدگی الگوریتم رمز را می توان با مدیریت کلید بصورت کارآ و نـیز استفاده از کلیدهای متفاوت برای هر بلوک متن پیام افزایش داد. یک اتوماتای سلولی خطی ۹۶ بیت خودگردان برای تولید رشته کلید رمز اسـتفاده می نمائیم. این اتوماتا را می توان بطور منطقی بصورت یک ماتریچ ۱۲ × ۸ در نظر گرفت که کلید ۱۲ مرحله رمز را تأمین می‌کند[۳].

۴- بهبود مولد دنباله کلید

روش بکار گرفته توسط تسالیدس و همکارانش برای مدیریت کلید، استفاده از اتوماتای سلولی خطی است. اما از آنجا که در اتوماتای سلولی خطی وضعیت جدید هر سلول تنها به وضعیت ۳ سلول (خودش و همسایه چپ و راستش) بستگی دارد، لذا تمامیت در تابع مولد دنباله کلید کاهش یافته و در نتیجه هم طول دوره تکرار کم می شود و هم ویژگی های آماری به خوبی ارضاء نمی گردد [۱]. البته بررسی جـامع عملـی انجـام شـده روی چند اتوماتای سلولی خطی مؤید همین مدعا می باشد. همانطور که در جدول(۱) دیده می شود در اتوماتای سلولی خطی ۸ تایی طـول بلنـد تریـن حلقه دنباله کلید ۱۷ است . در حالیکه فضای مورد بررسی دارای $۲^۸ = ۲۵۶$ وضعیت است .



شکل (۴): الگوریتم رمز شبه DES مبتنی بر اتوماتای سلولی غیر خودگردان

جدول(۱) :

طول بزرگترین حلقه دنباله	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷
تعداد قوانین	۱۸۰	۳۹	۱۱	۲	۱	۳	۰	۲	۰	۰	۰	۳	۰	۱۱	۰	۲	۲

برای بهبود مولد دنباله کلید وابستگی بین بیتهای دنباله کلید را افزایش دادیم. بعبارت دیگر سعی نمودیم تابع انتقال اتوماتای سلولی به ویژگی تمامیت[1] نزدیک باشد. تابع $f:\{0,1\}^n \to \{0,1\}^m$ را تمام گوئیم هر گاه تمامی بیتهای خروجی Y به تمامی بیتهای ورودی X وابسته باشد. برای این منظور اولین راه حلی که بنظر می رسد افزایش شعاع همسایگی است یعنی به جای در نظر گرفتن شعاع همسایگی یک(روش ارائه شده در بخش قبل) شعاع همسایگی ۲ و یا بیشتر در نظر بگیریم. اگر چه این روش مفید خواهد بود اما بعلت آنکه تبادل اطلاعات بین دو سلول غیر مجاور نیاز به صرف وقت بیشتری است و از طرفی تردد اطلاعات درشبکه افزایش می یابد، عملاً این بهبود باعث کاهش کارایی و سرعت در ماشین اتوماتای سلولی خواهد شد که مطلوب نظر ما نیست.

راه حل دیگر که می تواند به افزایش تمامیت تابع انتقال کمک کند استفاده از توپولوژی های با اتصال بالاتر است. در این روش در ضمن آنکه وابستگی بین بیتهای دنباله کلید افزایش یافته است، کارایی تغییری نکرده و سرعت اجرا و تولید کلید همان مقدار قبلی باقی مانده است. البته سخت افزار سیستم پیچیده تر می شود. با بکارگیری یک ابر مکعب درجه n می توان برای هر سلول 2^n همسایه درنظر گرفت.

ما در بررسی خود توپولوژی ساده تری بصورت مشبک دو بعدی در نظر گرفتیم که وضعیت جدید هر سلول از روی وضعیت فعلی ۹ سلول تعیین می گردد. از طرفی با افزایش اتصال در توپولوژی، تعداد قوانینی که می توان در بهنگام سازی ماشین اتوماتای سلولی استفاده کرد نیز افزایش

[1] Completeness

می یابد. در اتوماتای سلولی مشبک دو بعدی $2^{2^9} = 2^{512}$ قانون وجود دارد در حالیکه در یک اتوماتای خطی $2^{2^3} = 2^8$ قانون متفاوت می توان داشت.

در بررسی عملی یک مشبک ۳ ×۳ را برای تولید دنباله کلید بکار گرفتیم و تنها قوانین خطی را مورد بررسی قرار دادیم. نتایج حاصله بسیار مطلوب و قابل توجه بود . چنانچه در جدول (۲) ملاحظه می شود در چندین مورد دوره تکرار بسیار خوب می باشد (کل وضعیتهای ممکن در این نمونه اتوماتای سلولی $2^9 = 512$ حالت است). این مولد دنباله کلید با سیکل بیش از ۳۶۰۰ = ۴۰۰ ×۹ بیت تولید می کند.

جدول (۲)

طول بزرگترین حلقه دنباله	تعداد قوانین
۱ تا ۱۰	۲۸۲
۱۱ تا ۲۰	۶۳
۲۱ تا ۳۰	۳۵
۳۱ تا ۴۰	۱۶
۴۱ تا ۵۰	۱۱
۵۱ تا ۶۰	۱۰
۶۱ تا ۷۰	۱۴
۷۱ تا ۸۰	۸
۸۱ تا ۹۰	۹
۹۱ تا ۱۰۰	۸
۱۰۱ تا ۱۵۰	۲۱
۱۵۱ تا ۲۰۰	۱۲
۲۰۱ تا ۲۵۰	۸
۲۵۱ تا ۳۰۰	۵
۳۰۱ تا ۳۵۰	۲
۳۵۱ تا ۴۰۰	۳
۴۰۱ تا ۴۵۰	۳
۴۵۰ تا ۵۰۰	۱

در زیر نمونه ای از خروجی این اتوماتای سلولی دیده می شود که قانون خطی ۲۲۶ در آن بکار رفته و بلندترین دنباله را به طول ۴۹۲ تولید می نماید.

(0) : 1

(140 ,202 ,144 ,238 ,402 ,306) : 6

(3 , 18, 154, 75, 19, 129, 152, 52, 430, 234, 438, 48, 336, 270, 340, 496, 176, 456, 479, 268, 354, 87, 237, 411, 352, 413, 342, 454, 461, 397, 453, 452, 507, 14, 100, 373, 233, 447, 98, 359, 104, 337, 491, 157, 102, 323, 362, 30 , 247, 339, 505, 28 , 193, 208, 166, 403, 297, 95 , 164, 421, 170, 510, 49 437, 57, 508, 7 , 54 , 408, 260, 299, 77 , 37 , 258, 313, 204, 130, 145, 11, 91 , 128, 395, 499, 71 , 126, 409, 370, 196, 203, 139, 195, 194, 217, 10 , 64 , 451, 498, 92 , 137, 209, 67 , 90 , 155, 80 ,62 , 465, 371, 223, 60 , 487, 240, 384, 187, 374, 224, 53 , 401, 315, 222, 39 , 272, 326, 341, 463, 415, 324, 355, 76 , 26 , 211, 81 , 219, 24 , 172, 492, 148, 16 , 118, 464, 406, 278, 398, 460, 434, 20 , 136, 167, 392, 407, 269, 349, 390, 389, 396, 506, 21, 183, 283, 504, 106, 302, 114, 500, 78, 44, 372, 214, 110, 266, 368, 40, 281, 490, 134, 181, 265, 377, 132, 131, 138, 216, 124, 431, 241, 357, 122, 445, 112, 280, 412, 361, 23, 165, 410, 379, 150, 38, 267, 363, 5, 36, 317, 232, 457, 425, 199, 230, 475, 296, 41, 367, 33, 294, 59, 494, 162, 439, 43, 381, 160, 125, 400, 478, 279, 405, 287, 476, 289, 22, 190, 329, 305, 133, 188, 383, 178, 292, 13, 109, 259, 290, 31, 236, 420, 149, 47, 345, 418, 135, 174, 474, 307, 151, 61, 472, 332, 298, 86, 246, 328, 327, 334, 284, 497, 85, 255, 282, 483, 212, 88, 228, 493, 171, 485, 226, 511, 42, 358, 115, 495, 185, 356, 69, 108, 316, 215, 117, 473, 314, 197, 244, 382, 169, 503, 99, 380, 159, 116, 486, 235, 429, 227, 484, 221, 46, 322, 369, 205, 189, 320, 243, 375, 251, 318, 225, 502, 120, 450, 489, 143, 231, 448, 107, 309, 161, 446, 121, 436, 6, 45, 331, 291, 4, 27, 200, 239, 393, 481, 198, 253, 264, 271, 335, 263, 262, 285, 462, 388, 435, 15, 127, 386, 417, 142, 252, 311, 179, 319, 250, 293, 50, 444, 79, 55, 387, 442, 93, 182, 256, 275, 433, 29, 254, 257, 304, 96, 173, 467, 353, 94, 191, 338, 482, 207, 175, 449, 480, 261, 276, 440, 34, 303, 105, 295, 32, 229, 466, 378, 141, 245, 321, 376, 242, 364, 12, 82, 210, 74, 8, 63, 458, 416, 333, 277, 391, 414, 351, 404, 288, 469, 343, 477, 286, 455, 470, 350, 399, 471, 325, 348, 441, 84, 192, 347, 432, 248, 346, 427, 213, 103, 344, 468, 360, 97, 366, 58, 501, 113, 509, 56, 394, 488, 249, 300, 68, 83, 201, 153, 66, 65, 72, 119,

459, 443, 70, 101, 330, 312, 186, 365, 51, 423, 184, 274, 426, 206, 180, 310, 168, 385, 424, 177, 301, 123, 422, 163, 428, 220, 17, 147, 25, 218) : 492

(35, 308, 158, 111, 273, 419, 156, 89, 146, 2, 9, 73, 1, 0 , ...) : 14

پس از بررسی جامع دنباله های ایجاد شده توسط تمامی قوانین خطی و دستیابی به دنباله های کلید با دوره تکرار بالا، یکسری تست آماری نیز روی دنباله های حاصل اعمال کردیم که این تست ها را نیز به خوبی با احتمال بالای ۹۵٪ گذراندند. تستهای ارزیابی عبارتند از تست های تکرار، توالی، پوکر، ران ، پیچیدگی خطی، مشتق، و همبستگی ، که توسط نرم افزار RTest انجام شده است [۵] . برای نمونه نتیجه این بررسی ها روی دنباله فوق در پیوست آمده است .

۵- جمع بندی و نتیجه گیری

بررسی های انجام شده در اتوماتای سلولی دو بعدی نشان داد که ویژگی های مطلوب در مولد دنباله کلید با بکارگیری توپولوژی ۲ بعدی به جای خطی در اتوماتای سلولی بطور قابل توجهی افزایش می یابد. از طرفی ماهیت موازی این ساختار باعث می شود این روش نسبت به روشهای معمول تولید کلید که مبتنی بر ساختار ترتیبی Linear Feedback Shift Register می باشند دارای کارایی و سرعت بسیار بهتری بوده و ویژگی های آماری نیز به نحو مطلوبتری حاصل شود. تنها عیب استفاده از ماشین اتوماتای سلولی نیاز به سخت افزار پیچده است. برای حصول بهترین و بالاترین اتصال از توپولوژی ابر مکعب استفاده می شود که در یک ابر مکعب n بعدی (مرتبه n) هر سلول $2^n - 1$ سلول دیگر متصل است که لازمه یک سخت افزار پیچیده می باشد.با توجه به نتایج حاصله بعنوان یک حدس مطرح می نماییم که " چون با بالا بردن بعد ابرمکعب به ویژگی تمامیت نزدیک می شویم ، می توان حصول ویژگی های آماری بهتری را توقع داشته باشیم "

۶- مراجع

[1] H. Beker & F. Piper, "Cipher System ", Northwood Books , London ,1982 .

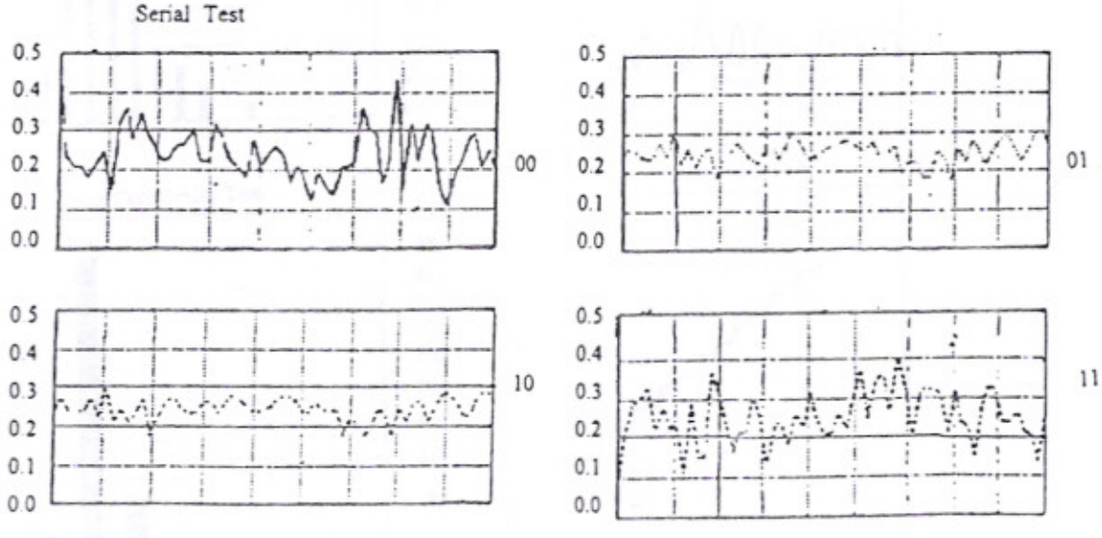
[2] J. Sebery & J.pieprzyk, "Cryptography, An Introduction to Computer Security ", Prentice Hall, Australia, 1898.

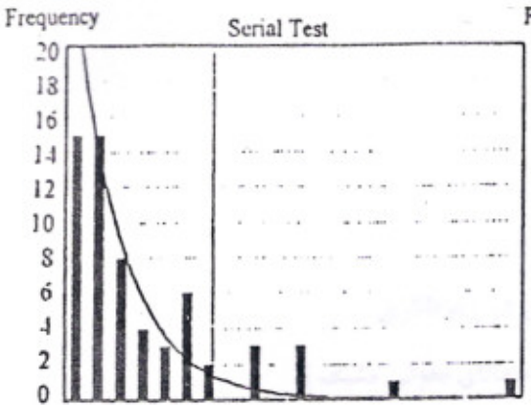
[3] S. Wolfram, "The Theory and Application of Cellular Automata", 1986.

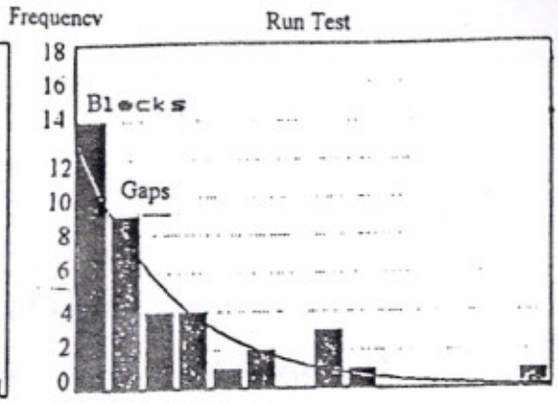
[4] Ph. Tsalides, B. Srisuchinwong, & T.A. York, "A Symmetric Cipher Using Autonomous And Non-autonomous Cellular Automata", 1995, IEEE Proceedings of Globcam, Vol.2, PP. 1172-1177.

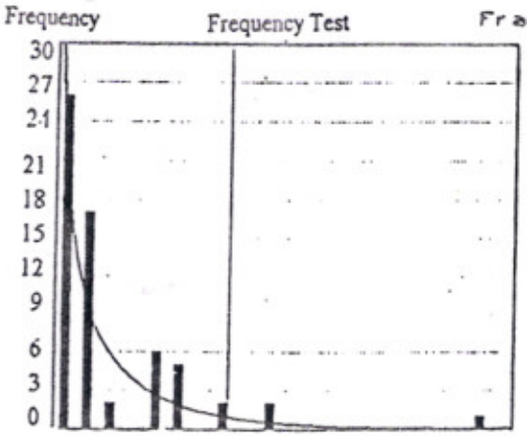
[۵] نرم افزار RTest ، " نرم افزار تحلیل و ارزیابی دنباله های دودویی تولید شده توسط سیستم های رمز " ، پژوهشکده الکترونیک دانشگاه صنعتی شریف.

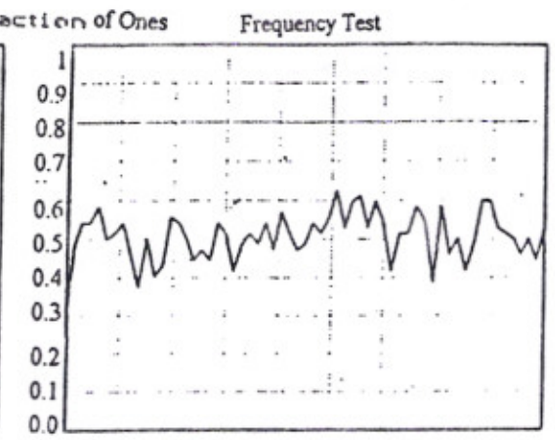
۷- پیوست

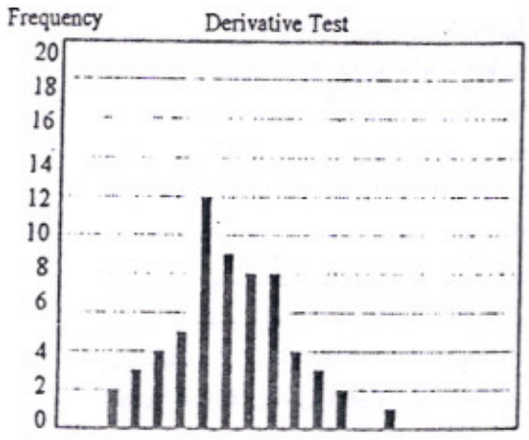


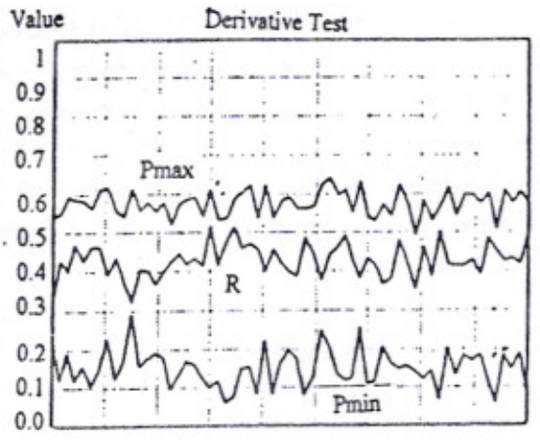

Frequency
Serial Test
20
18
16
14
12
10
8
6
4
2
0

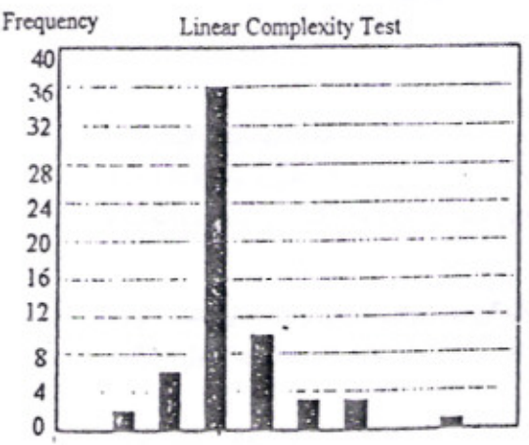

Frequency
Run Test
18
16
14
12
10
8
6
4
2
0
Blocks
Gaps

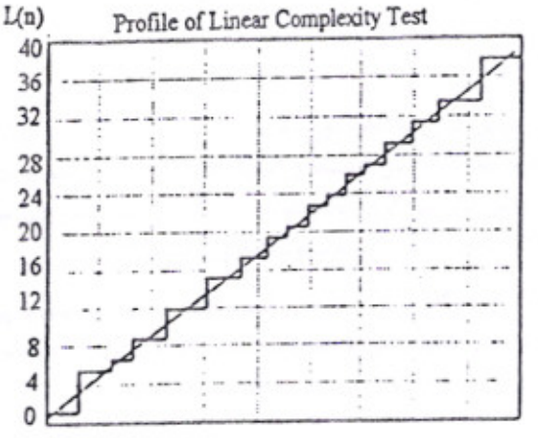

Frequency
Frequency Test
30
27
24
21
18
15
12
9
6
3
0


Fraction of Ones
Frequency Test
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0


Frequency
Derivative Test
20
18
16
14
12
10
8
6
4
2
0


Value
Derivative Test
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
Pmax
R
Pmin


Frequency
Linear Complexity Test
40
36
32
28
24
20
16
12
8
4
0


L(n)
Profile of Linear Complexity Test
40
36
32
28
24
20
16
12
8
4
0