چهارمین کنفرانس انجمن رمز ایران
انجمن رمز ایران
Iranian Society of Cryptology
۲۴ الی ۲۶ مهر ماه ۱۳۸۶ دانشگاه علم و صنعت ایران

رمزنگاری اطلاعات بر اساس عوامل محیطی با استفاده از اتوماتای سلولی

مجید وفایی جهان
گروه کامپیوتر، دانشکده فنی و مهندسی
دانشگاه آزاد اسلامی مشهد
vafaeiJahan@mshdiau.ac.ir

سعید ستایشی
گروه مهندسی هسته‌ای (پرتوپزشکی)، دانشکده فیزیک و علوم هسته‌ای
دانشگاه صنعتی امیرکبیر
setayesh@aut.ac.ir

محمدرضا اکبرزاده توتونچی
گروه برق، دانشکده فنی و مهندسی
دانشگاه فردوسی مشهد
akbarzadeh@ieee.org

چکیده: در این مقاله کوشش شده است روشی نوین در رمزگذاری اطلاعات با استفاده از اتوماتای سلولی ارائه شود. این روش با ترکیب قابلیت‌های ثبات‌های بازگشتی خطی (LFSR) و اتوماتای سلولی، تابعی ایمن، برای رمزگذاری بلوکی ارائه می‌دهد که علاوه بر رمزگذاری و رمزبرداری اطلاعات بصورت بلوکی، عامل‌های محیطی همچون نورآفتاب، دما، رطوبت و ... می‌توانند الگوی رمزگذاری را تغییر دهند.

مزیت روش رمزگذاری فوق نسبت به روش‌های دیگر، (۱) عدم وابستگی مولد اعداد تصادفی به هسته اولیه، (۲) ایجاد دنباله طولانی از اعداد تصادفی با آنتروپی بیشینه، (۳) قابلیت رمزگذاری بلوکی و پیاده‌سازی راحت سخت‌افزار آن، (۴) افزایش پیچیده‌گی رمزگشایی با ایجاد حساسیت به عامل محیطی همچون دما و (۵) استحکام الگوریتم در برابر تغییرات ناچیز دمای محیط(خطای حس‌گرهای حرارتی) در فرستنده و گیرنده می‌باشد.

واژه‌های کلیدی: رمزگذاری/ رمزبرداری اطلاعات، اتوماتی سلولی، LFSR، مکانیک آماری، توزیع گیبز و زنجیره‌های مارکوف

۱. مقدمه

با گسترش شبکه های کامپیوتری و نقل و انتقال اطلاعات تکنیک‌های مختلف رمزنگاری اطلاعات مورد توجه قرار گرفته‌اند. در این بین، تکنیک‌هایی که بتواند محرمانه بودن پیغام را طوری تامین کند که تهدیدکننده نتواند به اصل متن پی ببرد اهمیت پیدا می‌کنند.

در این مقاله، روشی پیشنهاد شده است که علاوه بر رمزگذاری اطلاعات، به‌واسطه توانایی در تولید اعداد تصادفی، حساس به عوامل محیط اطراف مثلا دما، نورآفتاب و ... نیز می‌باشد. بطوری‌که تهدیدکننده علاوه بر داشتن دانش تولید عدد تصادفی و کلید، بایستی رمزبرداری را در محیطی انجام دهد که مشابه محیط رمزگذاری باشد و این امر باعث پیچیده‌گی در رمزبرداری پیغام‌های دریافتی توسط تهدیدکننده می‌گردد. برای این منظور در بخش ۲، مفاهیم مرتبط و مورد استفاده در مقاله تعریف شده‌اند. در بخش ۳، فعالیت‌های نزدیک، در زمینه رمزگذاری و رمزبرداری اطلاعات مرور شده‌اند. در بخش ۴، روش تولید اعداد تصادفی پیشنهادی به همراه سخت‌افزار آن معرفی و ارزیابی شده است. در بخش ۵ و ۶، روش رمزگذاری و رمزبرداری پیشنهادی بررسی و ارزیابی شده است. در بخش ۷ و ۸، حساسیت رمزگذاری به محیط ارسال و دریافت پیغام بررسی شده که در این مقاله دما بعنوان عامل محیطی مورد آزمایش می‌باشد و الگوریتمی در خصوص رمزگذاری و رمزبرداری پیغام که حساس به دمای محیط می‌باشد ارائه شده است در بخش ۹، تاثیر دمای محیط بر سیستم رمزنگاری بحث شده است. در بخش ۱۰، تاثیر اختلاف دما در فرستنده و گیرنده بررسی شده است و دست‌آخر نتیجه‌گیری مقاله ذکر شده است.

۲. مفاهیم

بطور کلی هر عملی که امنیت اطلاعات را به مخاطره اندازد تهدید ایمنی اطلاعات نامیده می‌شود. یکی از روشهای تامین ایمنی اطلاعات، رمزنگاری است. با رمزنگاری محرمانه ماندن و اعتبار پیغام حفظ می‌گردد. مشکل اصلی در رمزنگاری، ارائه روشی است که تهدیدکننده نتواند از متن رمز شده متن اصلی را بدست آورد حتی نتواند با داشتن متن اصلی مبدل رمزگشایی را پیدا کند. در این خصوص مقدار اطلاعات بدست آمده از متن رمز شده (آنتروپی) و روش رمزگذاری دارای اهمیت می‌باشند[12].

آنتروپی[1]، متوسط اطلاعات موجود در هر پیغام را گویند. اگر منبعی بتواند n پیغام مختلف تولید کند آنگاه پیغام iام دارای مقدار اطلاعات

[1] Entropy

اطلاعات $-n.p_i.\log(p_i)$ خواهد بود. که p_i احتمال رخداد پیغام i در رشته ارسالی پیغام‌هاست. بنابراین آنتروپی منبع برابر است با $H=-\sum_{i=1}^{n} p_i.\log_2(p_i)$. به‌عبارت دیگر، اگر احتمال رخداد پیغام‌ها متفاوت باشد باید پیغام‌های مهم‌تر با بیت کمتر و پیغام‌های کم ارزش‌تر با بیت بیشتر ارسال شوند بطوری‌که متوسط آنها ثابت H باشد. مقدار آنتروپی منبع وقتی حداکثر است که $p_i=\frac{1}{n}$ یا همه پیغامها احتمال یکسان داشته باشند. که در این حالت آنتروپی منبع مساوی $H=\log_2 n$ خواهد بود[17, 18].

روشهای مختلفی در رمزگذاری اطلاعات مطرح است که بطور کلی به دو دسته رمزگذاری جویباری[1] و بلوکی[2] تقسیم می‌شوند[12, 18]. که در نوع اول، در هر لحظه، رمزگذاری بیت به بیت یا کاراکتر به کاراکتر انجام می‌گیرد ولی در نوع دوم تمام رشته پیغام به یکباره رمز شده و ارسال می‌گردد. بطورکلی برای هر دو روش رمزگذاری از کلیدهایی استفاده می‌گردد که از اعداد شبه‌تصادفی[3] ایجاد شده‌اند. برای تولید اعداد تصادفی روشهای مختلفی وجود دارد که از آن‌جمله می‌توان به مولدهای همنهشتی خطی[4] و غیر خطی، ثباتهای بازگشتی خطی[5] (LFSR) و غیرخطی و اتوماتای سلولی[6] (CA) و ... اشاره کرد. LFSRها به‌دلیل سادگی سخت افزار و قابلیت ایجاد دنباله طولانی از اعداد تصادفی بسیار مورد استفاده قرار می‌گیرند اما در این‌گونه روش‌ها، رمزگذاری بصورت جویباری انجام می‌گیرد و برای رمز کردن n بیت اطلاعات نیاز به n کلاک می‌باشد. همچنین مجموعه مقادیر تولید شده توسط این روش مرتبا طبق یک الگوی مشخص تکرار می‌شوند[15].

اتوماتای سلولی بدلیل داشتن الگوریتم و پیاده‌سازی ساده سخت‌افزاری از اهمیت خاصی در تولید اعداد شبه‌تصادفی برخوردار است. در این روش مجموعه‌ای سلول تشکیل یک اتوماتای سلولی را می‌دهند هر سلول به‌همراه سلولهای همسایه، بر اساس قانون تعریف شده‌ای مقدار خود را بروز می‌کند[19]. از آنجا که به راحتی نمی‌توان عملکرد اتوماتا سلولی را در مرحله بعد حدس زد از آن برای تولید اعداد شبه‌تصادفی استفاده می‌گردد. مشکل این روش، تولید دنباله کوتاهی از اعداد است بطوری‌که مجموعه‌ای از اعداد تولید شده مرتبا تکرار می‌گردد. برای رفع این مشکل قانون‌های ترکیبی یا اتوماتی ترکیبی ارائه شده‌است که تا حد قابل توجه‌ای وضعیت تولید اعداد تصادفی را بهبود می‌بخشد ولی مشکل آن استفاده از چندین قانون و در نتیجه سخت‌افزار پیچیده‌تر است. همچنین به‌دلیل سادگی عملکرد اتوماتا، رمزگشایی اطلاعات آسان است.

۳. فعالیت‌های مرتبط

فعالیتهای مختلفی در زمینه تولید اعداد تصادفی و رمزنگاری اطلاعات صورت گرفته است. برخی از فعالیت‌ها، کاربرد اتوماتای سلولی را در رمزگذاری بررسی کرده‌اند. در [1,2] استفاده از اتوماتای سلولی در رمزگذاری جویباری و بلوکی بررسی شده است که با استفاده از اتوماتای سلولی ترکیبی توانسته است اعداد تصادفی با دنباله طولانی قابل قبولی تولید کند و روشی برای رمزنگاری بلوکی با ارائه سخت‌افزار قابل برنامه‌ریزی ارائه دهد.

برخی از فعالیت‌ها، قابلیت‌های قوانین اتوماتای سلولی در رمزنگاری را بررسی کرده‌اند. در [3] روش بهینه‌سازی برای تولید قانونی ترکیبی در اتوماتای سلولی ارائه شده است که دنباله طولانی از اعداد تصادفی می‌تواند تولید کند. در [4, 5] با استفاده از الگوریتم ژنتیک روشی برای پیدا کردن قانون ترکیبی با آنتروپی حداکثر ارائه داده است که در نهایت توانسته است ترکیب مناسبی از قوانین اتوماتا برای تولید اعداد تصادفی و در نهایت رمزنگاری ارائه دهد. همچنین در [6] نیز تولید قوانین ترکیبی اتوماتای سلولی برای رمزنگاری مورد تاکید قرار گرفته است.

در [7, 8, 9] سخت افزار اتوماتای سلولی برای تولید اعداد تصادفی مورد بررسی قرار گرفته است سخت‌افزارهای ارائه شده اکثرا قابل برنامه‌ریزی بوده و می‌توانند قوانین ترکیبی مختلفی را برای رمزنگاری اطلاعات استفاده کنند.

در برخی دیگر از فعالیت‌ها نیز صرفا نحوه رمزگشایی اطلاعات توسط اتوماتای سلولی بررسی شده است که روش‌های مختلفی از جمله ایجاد محیط متقارن فرستنده پیغام یا استفاده از روشهای بهینه‌سازی پیمایش و حدس پیغام‌های رمز شده مورد توجه می‌باشند. در [10] با استفاده از روش بهینه‌سازی شبیه‌سازی گداختگی[7]، روشی ارائه شده است که بتواند متن رمز شده را رمزگشایی کند که البته دقت روش به طول پیغام وابسته می‌باشد. در این روش اختلاف بین متن رمز شده و اصلی بعنوان تابع هزینه در نظر گرفته شده است که با استفاده از روش شبیه‌سازی گداختگی سعی در کاهش این تفاوت دارد. در [11] ضعفهای اتوماتای سلولی در مقابل حمله‌های رمزگشایی بررسی و روشی ساده جهت رمزگشایی برخی از قوانین اتوماتای سلولی برشمرده شده است.

[1] Stream Ciphering
[2] Block Ciphering
[3] Pseudorandom number
[4] Liner Congruentional generators
[5] Linear Feedback Registers
[6] Cellular Automata
[7] Simulated Annealing -

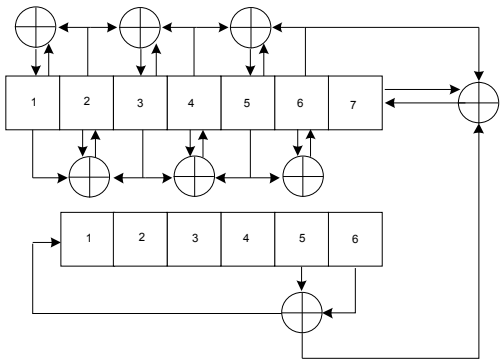
در برخی از فعالیت‌ها، عملکرد LFSRها بررسی و توسعه داده شده‌اند. در [12] ثباتهای بازگشتی خطی تعریف شده و عملکرد آنها برای تولید اعداد تصادفی با دنباله طولانی بررسی شده است. در [13, 14] راههای توسعه LFSRها و ایجاد LFSRهای ترکیبی بررسی شده و راهکارهایی برای تولید اعداد تصادفی با دنباله بیشتر ارائه شده است.

۴. روش پیشنهادی تولید اعداد تصادفی

قسمت بالای شکل (۱) عملکرد یک اتوماتای سلولی ۷ بیتی را نشان می‌دهد. این اتوماتا طبق قانون ۱۵۰ کار می‌کند[16, 19] طبق این قانون در هر مرحله مقدار هر سلول برابر است با جمع در مبنای ۲، مقدار قبلی سلول بعلاوه مقدار ۲ سلول مجاور آن. به‌عبارت دیگر مقدار هر سلول از فرمول (۱) محاسبه می شود.

$$s_i(t+1) = (s_{i-1}(t) + s_i(t) + s_{i+1}(t)) \bmod 2 \qquad (۱)$$

اتوماتای سلولی فوق، توانایی ایجاد اعداد تصادفی با دنباله محدودی را دارد که در نمودار شکل (۲)، آنتروپی آن برای اجرای ۲۵۰۰ عدد تصادفی در رنج ۰ تا ۱۲۷ نمایش داده شده است.

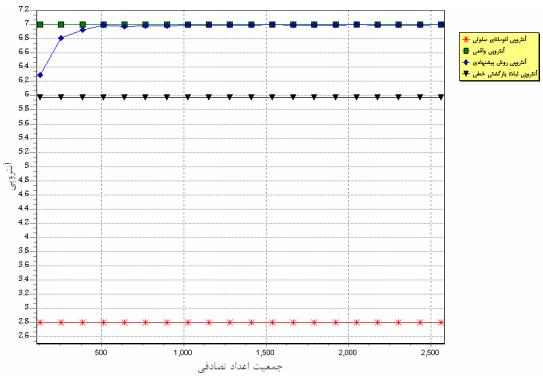


شکل ۱: سخت افزار رمزگذاری، ترکیب اتوماتای سلولی ۷ بیتی با قانون ۱۵۰ و LFSR ۶ بیتی

همان‌طور که مشاهده می‌گردد دنباله تولید شده کوتاه بوده و برخی از اعداد این بازه مرتبا تکرار می‌گردند. بنابراین آنتروپی با افزایش تولید اعداد تصادفی به نقطه ثابت ۲،۸۰ همگرا می‌شود که این نقطه از آنتروپی حداکثر ۷، بسیار فاصله دارد و نشان می‌دهد اعداد توسط مولد تصادفی مناسبی تولید نشده‌اند.

ثباتهای بازگشتی خطی برای تولید اعداد تصادفی توانایی بیشتری دارند یک ثبات بازگشتی خطی ۶ بیتی در قسمت پائین شکل (۱) نمایش داده شده است. همان‌طور که مشاهده می‌گردد بیت ۵ و۶ بایکدیگر جمع مبنای ۲ شده سپس بیت‌های ثبات یکی به راست شیفت می‌یابد و مقدار حاصل جمع در بیت آخر قرار می‌گیرد. در شکل (۲)، توانایی تولید LFSR ۶ بیتی نشان داده شده است. بطوری‌که برای ۲۵۰۰ عدد تولید شده اعداد تصادفی به این روش در بازه ۰ تا 63 مقدار آنتروپی ۵،۹۷۷ است که نزدیک به مقدار ماکزیمم ۶ می‌باشد.

البته LFSR نمی تواند عدد صفر را تولید کند بنابراین در بهترین حالت با هسته اولیه مناسب، LFSR شکل (۱) مقدار حداکثر یا ۶ را نخواهد داشت.



شکل ۲: تغییرات آنتروپی اتوماتای سلولی با قانون ۱۵۰، LFSR و روش پیشنهادی

روش پیشنهاد شده در این مقاله ترکیب اتوماتای سلولی با قانون ۱۵۰ و LFSR مانند شکل (۱) می‌باشد. قانون ۱۵۰ با کمی تغییر استفاده شده است. سلول شماره (۱) (سمت چپ‌ترین) از جمع دو سلول اول و برای سلول شماره n (سمت راست‌ترین) از جمع دو سلول سمت راست و خروجی LFSR محاسبه می‌گردد.

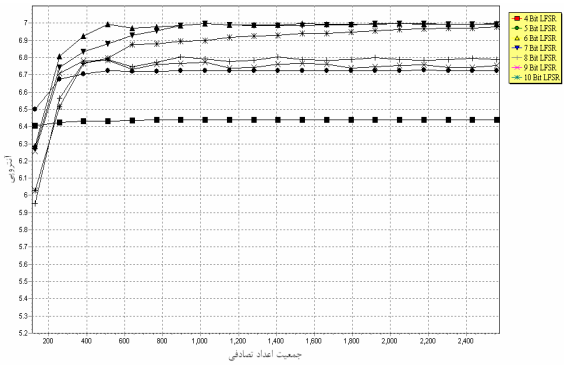
دنباله اعداد تصادفی تولید شده توسط اتوماتای سلولی روش پیشنهادی، خیلی سریع به سمت آنتروپی حداکثر همگرا می‌شود و این نشان می‌دهد که تمام اعداد تصادفی در این رنج تولید شده و دارای توزیع یکنواخت می‌باشند. توانایی روش ارائه شده در نمودار شکل (۲) نمایش داده شده است. در این نمودار ۲۵۰۰ عدد تصادفی با هسته اولیه دلخواه با آنتروپی ۶،۹۹۶ تولید شده است که به آنتروپی حداکثر بسیار نزدیک می‌باشد.

در آزمایشهایی که انجام شده است روش پیشنهادی خواص زیرا نشان داده است:

۱- دنباله اعداد تصادفی تولید شده مستقل از هسته اولیه اتوماتای سلولی می‌باشد و متناسب با طول LFSR است. نمودار شکل (۳) مقدار آنتروپی اعداد تصادفی تولید شده بواسطه LFSRهای با طول متفاوت را نشان می‌دهد.

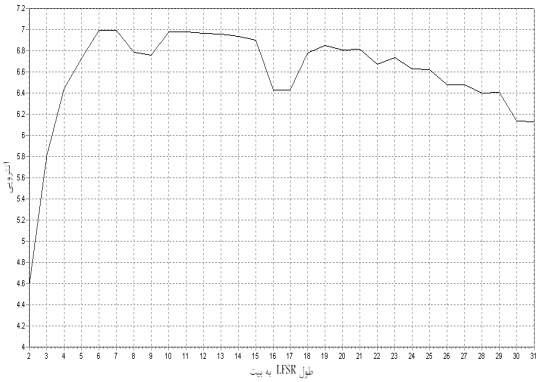
همان‌طور که مشاهده می‌گردد ۲۵۰۰ عدد تصادفی با اتوماتای سلولی ۷ بیتی و LFSRهای ۴ تا ۱۰ بیتی تولید شده است. در این میان LFSR ۵ بیتی دارای آنتروپی ۶،۱۰ و LFSR ۹ بیتی دارای آنتروپی ۵،۵۳ می‌باشد. حداکثر آنتروپی با LFSR ۶ بیتی تولید شده است که ۶،۹۹۶ است.

به‌نظر می رسد بر اساس نتیجه‌ای که در بیش از چندین آزمایش مختلف نیز تکرار شده است طول LFSR بایستی نزدیک به طول اتوماتای سلولی باشد تا بهترین پاسخ نتیجه شود.



شکل ۳: آنتروپی اعداد تولید شده توسط اتوماتای سلولی و انواع LFSR مختلف

نمودار شکل (۴)، تغییرات آنتروپی برای اتوماتای سلولی ۷ بیتی با LFSRهای با طول متفاوت از ۲ بیتی تا ۳۱ بیتی را نشان می‌دهد.



شکل ۴: تغییرات آنتروپی روش پیشنهادی با تغییر طول LFSR برای اتوماتای سلولی 7 بیتی

۲- این روش از حیث سخت افزاری به راحتی قابل تولید است. بطوری‌که برای تولید آن محدودیت خاصی از حیث پیچیدگی سخت‌افزار وجود ندارد.

۳- این روش می‌تواند دنباله طولانی‌تری از اعداد تصادفی نسبت به اتوماتای سلولی و LFSR تولید کند. زیرا همان‌طور که آزمایش نشان داد، اتوماتای سلولی توانایی خود را با تاثیر از LFSR افزایش می‌دهد و این افزایش باعث تولید دنباله طولانی‌تری از اعداد تصادفی می‌گردد بطوری‌که آنتروپی اطلاعات تولید شده به مقدار بیشینه بسیار نزدیک می‌گردد و این موضوع برای اتوماتاهای با طول متفاوت بررسی و صحت آن آزمایش شده است.

۴- از آنجا که محدودیتی برای اتوماتای سلولی از حیث طول وجود ندارد بنابراین این روش می‌تواند برای رمزنگاری بلوکی مناسب باشد و نسبت به رمزگذاری جویباری دارای سرعت رمزگذاری بیشتری باشد.

۵. رمزگذاری اطلاعات

بر اساس روش پیشنهاد شده اطلاعاتی که قرار است رمز شود در اتوماتای سلولی قرار می گیرد. LFSR نیز با هسته اولیه دلخواه شروع به کار می‌کند (در این نوشته مقدار اولیه تمام رجیسترها ۱ می‌باشد) با هر کلاک ساعت یک مقدار جدید در اتوماتا تولید می‌گردد بنابراین می‌توان با یک مجموعه کلاک $c \geq 1$، اطلاعات را رمز و آماده ارسال به گیرنده کرد.

اگر مقدار c=k باشد آنگاه k می تواند بعنوان کلید برای رمزگذاری و رمزبرداری اطلاعات محسوب شود. به این ترتیب که بعد از ورود پیغام به اتوماتای سلولی، بعد از k کلاک، رشته رمز شده آماده ارسال می‌گردد. با ارسال رشته رمز شده به هدف در صورت دسترسی تهدیدکننده به اطلاعات، تهدیدکننده بایستی هم کلید k و هم مقدار اولیه LFSR را داشته باشد تا بتواند اطلاعات را رمزگشایی کند.

۶. رمزبرداری اطلاعات

برای رمزبرداری اطلاعات از آنجا که این الگوریتم برای اتوماتای سلولی با طول خاصی دارای جواب است. عملکرد عکس آن دیگر اتوماتای سلولی نیست بنابراین برای رمزبرداری اطلاعات بایستی بتوان عکس عمل فوق را محاسبه و سخت‌افزار مناسبی طراحی کرد. برای اینکه مکانیزم رمزبرداری بررسی شود بایستی ثابت شود که اتوماتای سلولی ارائه شده برای چه مقادیری از n (طول اتوماتای سلولی به بیت) برگشت‌پذیر است.

قضیه ۱: اتوماتای سلولی روش پیشنهادی برای n=3k و n=3k+1 برگشت‌پذیر است و برای n=3k+2 برگشت‌پذیر نیست(k یک عدد صحیح مثبت است).

اثبات: با توجه به قانون اعمال شده در اتوماتای سلولی می‌توان فرمولهای (۲) تا (۴) را با درنظر گرفتن شرایط مرزی و زمان t بصورت زیر نوشت:

$$s_i(t+1) = (s_{i-1}(t) + s_i(t) + s_{i+1}(t)) \bmod 2 \quad (۲)$$

$$s_1(t+1) = (s_1(t) + s_2(t)) \bmod 2 \quad (۳)$$

$$s_n(t+1) = (s_{n-1}(t) + s_n(t) + LFSR_1(t+1)) \bmod 2 \quad (۴)$$

از آنجا که جمع، در مبنای ۲ می باشد با ساده‌سازی فرمول (۲) فرمول (۵) حاصل می‌گردد.

$$s_i(t) = (s_{i+1}(t+1) + s_{i+2}(t+1) + s_{i+3}(t)) \bmod 2 \quad (۵)$$

برای محاسبه فرمولهای معکوس، از فرمولهای (۲) تا (۴) استفاده شده که برای n=3k و n=3k+1 پاسخ داریم ولی برای n=3k+2 بعد از ساده سازی داریم:

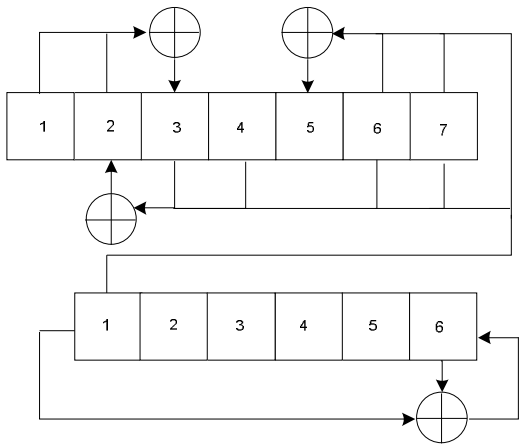
$$s_i(t) = (s_{i+1}(t+1) + s_{i+2}(t+1) + \quad (۶)$$
$$s_{i+4}(t+1) + s_{i+5}(t+1) + \ldots +$$
$$s_{i+N-2}(t+1) + s_{i+N-1}(t+1) + s_i(t)$$

که در اینصورت اگر $s_i(t)$ را از دو طرف حذف کنیم بایستی برای مابقی عبارت همیشه برقرار باشد که غیرممکن است.

$$0 = (s_{i+1}(t+1) + s_{i+2}(t+1) + s_{i+4}(t+1) + s_{i+5}(t+1) + ... + s_{i+N-2}(t+1) + s_{i+N-1}(t+1)) \quad (۷)$$

بنابراین اگر اتوماتای سلولی دارای طول n باشد بایستی مقدار آن 3k یا 3k+1 باشد.♣

با توجه به قضیه ۱ می‌توان الگوریتم رمزبرداری را به‌صورت زیر بیان کرد. رشته رمز شده وارد ساختار بیتی شکل (۵) شده (به‌دلیل فشردگی، مدار سخت‌افزار آن برای بیت ۲، ۳ و ۵ کامل کشیده شده است)، مقدار اولیه LFSR نیز برابر عددی قرار می‌گیرد که از kامین کلاک حالت تمام ۱ (فرض مقدار اولیه) بدست می‌آید. در این صورت سیستم شروع به‌کار کرده و زمانی‌که مقدار LFSR به حالت تمام ۱ رسید یا k کلاک سپری شد مقدار ساختار بیتی برابر رشته اصلی می‌گردد. فرمول‌های رمزبرداری اتوماتای سلولی شکل (۵) در پیوست (۱) لیست شده است و برای تکمیل آن می‌تواند مورد استفاده قرار گیرد. همان‌طور که مشاهده می‌گردد، LFSR برگشت‌پذیر است ولی اتوماتای سلولی طبق قضیه ۱ برای تمام nها برگشت‌پذیر نیست. پس برای استفاده از این روش بایستی طول n را مناسب انتخاب کرد.



شکل ۵: سخت افزار رمزبرداری، طبق پیوست ۱(برای بیت ۲، ۳ و ۵ کامل است)

۷. رمزگذاری اطلاعات بر اساس دمای محیط

برای ایجاد حساسیت سیستم رمزنگاری، عوامل محیطی متفاوتی را می‌توان در نظر گرفت که در این مقاله دما بعنوان عامل محیطی مدنظر قرار گرفته است. با توجه به اینکه مولد اعداد تصادفی روش ارائه شده توانایی تولید دنباله طولانی از اعداد تصادفی با آنتروپی بیشینه را دارد بنابراین اعدادی که تولید می‌کند دارای توزیع تقریبا یکنواخت می‌باشد. برای ایجاد حساسیت نسبت به دمای محیط، نوع توزیع اعداد تولید شده به شکلی تغییر داده شده است که از قوانین ترمودینامیک تبعیت کند. برای نیل به این هدف از مکانیک آماری کمک گرفته شده است[15, 16].

بطور کلی مکانیک آماری[1] بیان می‌کند که یک سیستم با محیط اطرافش در تعادل دمایی[2] است اگر حالت iام سیستم با احتمال زیر اتفاق بیفتد.

$$P(s_i) = \frac{e^{-\frac{E(s_i)}{k.T}}}{Z} \qquad Z = \sum_{i=1}^{n} e^{-\frac{E(s_i)}{k.T}} \quad (۸)$$

که s_i حالت سیستم از میان n حالت متناهی است. $P(s_i)$ احتمال اینکه سیستم در حالت s_i باشد و $\sum_i P(s_i) = 1$. $E(s_i)$ انرژی سیستم درحالت s_i است، T دمای تعادل بر اساس مقیاس کلوین و k ثابت بولتزمن[3] می‌باشد. هنگامی‌که T مقیاسی ندارد نیازی به مقدار k نیست بنابراین توزیع احتمال (۸) که به توزیع گیبز[4] معروف است به فرم زیر بیان می‌شود.

$$P(s_i) = \frac{e^{-\frac{E(s_i)}{T}}}{Z} \qquad Z = \sum_{i=1}^{n} e^{-\frac{E(s_i)}{T}} \quad (۹)$$

بدلیل اینکه مولد اعداد تصادفی پیشنهادی می تواند دنباله طولانی از اعداد تصادفی با آنتروپی بیشینه و حدود $H = \log_2 n$ تولید کند تمام n مقدار ممکن ظاهر خواهند شد. به‌عبارتی تمام حالات سیستم (اعداد ممکن) از یکدیگر قابل حصول هستند بنابراین بر طبق قانون تعادل در زنجیره‌های مارکوف[5] [20] داریم:

$$P(s_i).P(s_i \to s_j) = P(s_j).P(s_j \to s_i) \quad (۱۰)$$

یعنی احتمال تغییر حالت از s_i به s_j با احتمال حضور سیستم در حالت‌های ذکرشده متناسب است. بنابراین با توجه به فرمول (۹)، تغییر حالت از یک وضعیت به وضعیت دیگر برابر است با:

$$\frac{P(s_j)}{P(s_i)} = \frac{P(s_i \to s_j)}{P(s_j \to s_i)} = e^{-\frac{\Delta E}{T}} \quad (۱۱)$$

$$\Delta E = E(s_j) - E(s_i)$$

یعنی اگر احتمال $P(s_j \to s_i) = 1$ بگیریم آنگاه $P(s_i \to s_j) = e^{-\frac{\Delta E}{T}}$ خواهد بود. به‌عبارت دیگر اگر احتمال تغییر حالت را $P(s_i \to s_j) = \min[1, e^{-\frac{\Delta E}{T}}]$ در نظر بگیریم آنگاه سیستم در حالت تعادل ترمودینامیکی خواهد بود و احتمال رخداد هر وضعیت از توزیع گیبز تبعیت می‌کند. با توجه به دستاورد بالا اگر انرژی هر حالت سیستم عددی باشد که LFSR نشان می‌دهد همچنین $n = 2^m - 1$ (m برابر تعداد بیتهای LFSR) باشد، آنگاه الگوریتم

[1] Statistical mechanics
[2] equilibrium
[3] Boltzmann's constant
[4] Gibbs Distribution
[5] Markov chains

رمزگذاری(۱) منطبق بر قانون ترمودینامیک، حالات مختلف سیستم را با احتمال‌های متفاوت و بر اساس تابع توزیع گیبز تولید می‌کند.

الگوریتم (۱): الگوریتم رمزگذاری اطلاعات حساس به دمای محیط

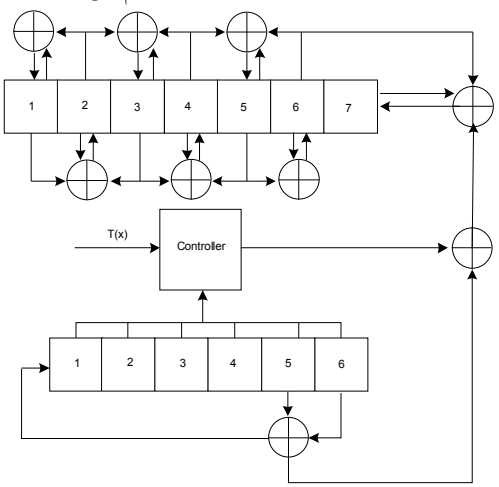
```
TermalCiphering(PlainText, Key, Temperature):CipherText
Begin
  CipherText := PlainText;
  T:= Temperture;
  For i:= 1 to Key do
  begin
     CipherText := CA(CipherText);
     current_LFSR := LFSR();
     E(s_i) = last_LFSR;
     E(s_j)=current_LFSR;
     ΔE = E(s_j) − E(s_i);
     if ΔE < 0 then
       CipherText := CipherText Xor current_LFSR[1];
     Else
     begin
      rn := create_random_number; //with known generator in [0,1]
                  −ΔE/T
      if rn <= e        then
        CipherText := CipherText Xor current_LFSR[1];
     end;
     last_LFSR := current_LFSR;
  end;
End;
```

به‌عبارت دیگر، هرچه اعداد (مقدار LFSR) بزرگتر شوند احتمال رخداد آنها کمتر می‌گردد. یعنی اعداد کوچکتر یا اعداد بزرگتری که در دمای بیشتری تولید شده‌اند با احتمال بیشتری رخ خواهند داد و هنگامی که در دمای بیشتر است اعداد بزرگتری را می‌تواند تولید کند. از این خاصیت استفاده کرده و سیستم رمزگذاری حساس به دما مطابق شکل (۶) با عملکرد الگوریتم (۱) پیشنهاد شده است.

در شکل (۶)، کنترل‌کننده، مقدار تولید شده LFSR و دمای محیط را اخذ می‌کند سپس با توجه به الگوریتم (۱) اگر مقدار فعلی LFSR از مقدار قبلی آن کوچکتر باشد آنگاه خروجی کنترل کننده مساوی مقدار صفر شده تا $LFSR_1(t+1)$ اعمال گردد. در غیراین‌صورت یک عدد تصادفی با توزیع یکنواخت با مولد شناخته شده (مولدی که در فرستنده و گیرنده به یک شکل عمل کند) تولید می‌شود اگر عدد تصادفی تولید شده از $e^{-\frac{\Delta E}{T}}$ کوچکتر باشد خروجی کنترل کننده صفر شده که باعث می‌شود $LFSR_1(t+1)$ بر اتوماتا تاثیر بگذارد. در غیر این‌صورت خروجی کنترل کننده مساوی $LFSR_1(t+1)$ خواهد بود که باعث عدم تاثیر LFSR بر اتوماتا می‌گردد.

با توجه به عملکرد کنترل کننده شکل (۶)، می‌توان روش رمزگذاری بخش ۴ را به‌صورت زیر توسعه داد:

اطلاعات وارد اتوماتای سلولی شده و یک مقدار اولیه ثابت در LFSR قرار می‌گیرد با توجه به کلید k و دمای محیط، LFSR شروع به کار می‌کند. در هر مرحله، عدد تولید شده LFSR توسط کنترل‌کننده بررسی می‌شود اگر از عملکرد کنترل‌کننده تبعیت کند آنگاه خروجی LFSR بر اتوماتای سلولی اعمال می‌گردد (خروجی کنترل کننده صفر) وگرنه خروجی اعمال نمی‌شود (خروجی کنترل کننده برابر $LFSR_1(t+1)$). این موضوع چه درفرستنده و چه درگیرنده یکسان و برای یک رشته اطلاعات، k مرتبه انجام می‌گیرد.



شکل ۶: سخت افزار رمزگذاری حساس به دمای محیط

۸. رمزبرداری اطلاعات بر اساس دمای محیط

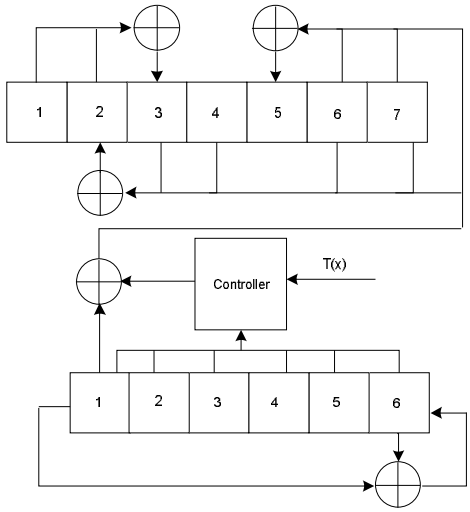
برای رمزبرداری اطلاعات سخت افزار شکل (۷) پیشنهاد شده است. در سخت افزار شکل (۷)، کنترل‌کننده ورودی LFSR و دمای محیط را دریافت کرده و تصمیم می‌گیرد که آیا بیت اول LFSR بر اتوماتا اعمال شود یا خیر. از آنجا که دریافت‌کننده و ارسال‌کننده از کنترل‌کننده و تابع T(x) مشابه استفاده می‌کنند تهدید کننده بایستی هم کلید و تابع دمای محیط را داشته باشد و این موضوع پیچیدگی الگوریتم رمزگذاری را بیشتر می‌کند.

۹. بررسی تاثیر دمای محیط بر سیستم رمزنگاری

برای اینکه سیستم رمزنگاری از تغییرات دمای محیط مصون نگه داشته شود عملکرد سیستم رمزنگاری بر پایه حالات LFSR گزارده شده است. این امر باعث شده است که تغییرات دما تاثیر چندانی بر آنتروپی اتوماتا (سیستم) نداشته باشد. در نمودار شکل (۸) تغییرات دما بر آنتروپی سیستم رمزنگاری تاثیر بسیار ناچیز دارد. این موضوع نشان می‌دهد که دماهای مختلف تاثیر زیادی بر عملکرد سیستم ندارد. شکل (۹) تغییرات آنتروپی را نسبت به تغییرات دما نشان می‌دهد.

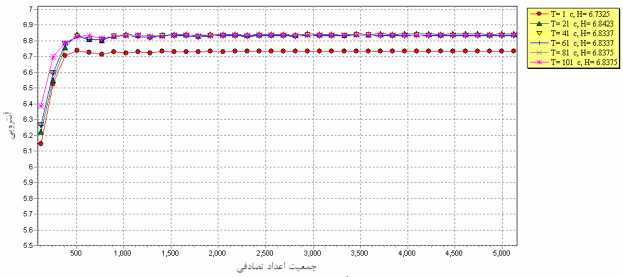
اما این سئوال مطرح است که نقش دما در عملکرد سیستم رمزگذاری چیست؟ در پاسخ به این سئوال بایستی متذکر شد که وجود دما باعث پیچیده شدن فرایند رمزگشایی توسط تهدیدکننده می‌گردد. برای بررسی تاثیر دمای محیط بر پیچیدگی سیستم، ابتدا دمای محیط ثابت T در نظر گرفته شده است فرستنده و گیرنده پیغام نیز در دمای T

توافق دارند. در این حالت، عملکرد اتوماتا و آنتروپی آن برای دماهای مختلف بررسی شده است.



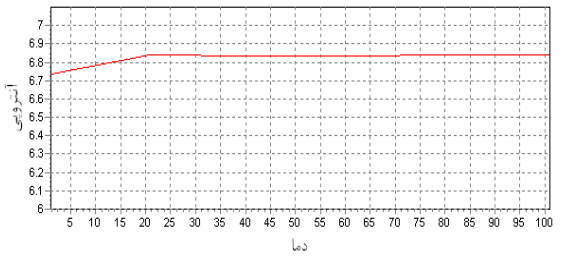
شکل ۷: سخت افزار رمزبرداری حساس به دمای محیط (اتوماتا برای بیت ۲، ۳ و ۵)

شکل (۸) نشان می‌دهد که آنتروپی اتوماتا با تغییر دمای محیط تغییر نمی‌کند. با فرض اینکه تهدید کننده روش رمزنگاری و کلید را بداند اگر دمای محیط را نداشته باشد نمی‌تواند اطلاعات را رمزگشایی کند زیرا دمای T در نقش کنترل‌کننده‌ای است که تاثیر خروجی LFSR بر اتوماتا را کنترل می‌کند و چون تهدید کننده این الگو را نمی‌داند به سادگی نمی‌تواند اطلاعات را رمزگشایی کند. این موضوع به خاصیت انتشار خطا در اتوماتاهای سلولی نیز مربوط است که در صورت وجود خطا در اطلاعات، عملکرد بیشتر اتوماتا، خطا را در سیستم پخش می‌کند.



شکل ۸: تغییرات آنتروپی اتوماتا با افزایش دما

اگر دمای محیط متغیر T(x) و تابعی متغیر از شرایط محیطی سیستم باشد رمزگشایی پیچیده‌تر می‌گردد. در این‌صورت فرستنده و گیرنده باید تابع T(x) را داشته باشند تا بتوانند اطلاعات را رمزگذاری و رمزبرداری کنند. در این حالت اگر پیغام‌ها در دماهای متفاوت رمز شوند آنگاه رمزگذاری سیستم به مراتب پیچیده‌تر می‌گردد. با توجه به دستاوردهای ذکر شده کلید k بایستی مقدار مناسبی انتخاب شود که تاثیر دما بر رمزنگاری اطلاعات ملحوظ شود یعنی هر چه k بیشتر باشد احتمال تاثیر LFSR بر اتوماتا بیشتر بوده و تهدید کننده در صورت تلاش برای رمزگشایی، باید زحمت بیشتری را برای تعیین الگوی تکراری متحمل شود.

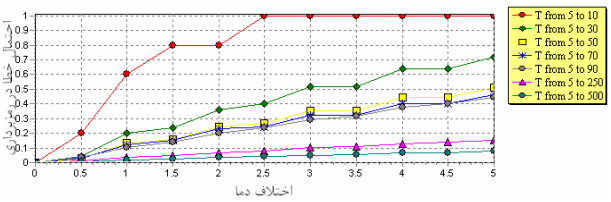


شکل ۹: تغییرات آنتروپی اتوماتا بر اساس تغییر دما

۱۰. بررسی تاثیر اختلاف دما در فرستنده و گیرنده

از آنجا که فرستنده و گیرنده در دمای یکسانی باید عمل رمزگذاری و رمزبرداری را انجام دهند تا امکان رمزگذاری و رمزبرداری باشد این عمل بدلیل خطا در برداشت اطلاعات محیطی با مشکلاتی مواجه است. در این قسمت استحکام الگوریتم در مقابل خطای حس‌گرها بررسی شده است. با توجه به خطایی که حس‌گرها دارند فرض شده است فرستنده، اطلاعات را در دمای T ارسال کند درحالی‌که گیرنده در دمای $T\pm\Delta\tau$ اطلاعات را رمزبرداری کند.

الگوریتم فوق برای ۱۰۰۰نمونه عدد در بازه دمایی مختلف مجددا بررسی شده است. بدین ترتیب که در دمای T رمزگذاری و در دمای $T-\Delta\tau$ رمزبرداری شده است نمودارهای شکل (۱۰) احتمال مشاهده خطا در رمزبرداری اطلاعات در دماهای مختلف و کلید مساوی ۵۰ نمایش داده شده است در دمای ۱۰، احتمال خطا در رمزبرداری با اختلاف دمایی ۵، یک است. اما در دمای ۵۰۰ احتمال خطا در رمزبرداری به کمتر از ۰،۱ کاهش می‌یابد. آزمایش‌ها نشان می‌دهد هرچه k بزرگتر باشد پیچیدگی سیستم بیشتر می‌شود همچنین سیستم به دماهای پائین‌تر حساس‌تر است. بدین معنی که هرچه دما بالاتر باشد احتمال اعمال خروجی بر اتوماتا بیشتر شده و تغییرات دمایی کمتر بر خروجی تاثیر دارد. بنابراین در این مسئله اگر k مقداری کوچک باشد (حدود ۲۰)، و دما بالا باشد (حدود ۴۵)، اختلاف دمایی بین فرستنده و گیرنده می تواند تا ۱ درجه باشد. مثلا اگر اطلاعات در دمای ۴۵ رمز شود، گیرنده می‌تواند اطلاعات را در دمای بین ۴۴ تا ۴۶ رمزگشایی کند.



شکل ۱۰-۱: احتمال خطا در رمزبرداری با K=50

۱۱. نتیجه‌گیری

در این نوشته سعی شد روش نوینی در تولید اعداد تصادفی با استفاده از اتوماتای سلولی و LFSRها ارائه گردد که علاوه بر داشتن آنتروپی بالا و قابلیت تولید دنباله طولانی اعداد تصادفی، توانایی

رمزگذاری و رمزبرداری اطلاعات را نیز دارد. همچنین روش پیشنهادی بر خلاف اکثر روش‌های تولید اعداد تصادفی همچون همنهشتی خطی، اتوماتای سلولی، LFSR به هسته اولیه وابسته نیست و بر اساس آزمایشهای مختلف طول دنباله اعداد تصادفی تولید شده تمام محدوده ممکن را در بر می‌گیرد و آنتروپی حداکثر را تولید می‌کند.

همچنین با توسعه روش ارائه شده و ایجاد حساسیت به عوامل محیطی همچون دمای محیط ارسال، عملیات رمزگذاری طبق الگوی دمایی محیط انجام می‌گیرد و رمزگشایی پیغام را برای تهدیدکننده در صورتی که الگوی دمایی محیط را نداشته باشد بسیار مشکل می‌کند. با آزمایش‌های به‌عمل آمده مشخص شد آنتروپی کل سیستم متاثر از دمای محیط نیست بنابراین صحت عملکرد سیستم رمزنگاری با تغییر دما تغییر نمی‌کند. همچنین مشخص شد که دما باعث حساسیت سیستم به خطا می‌گردد یعنی هرچه دما پائین‌تر باشد ساختار سیستم احتمالی‌تر می‌شود به‌عبارتی تاثیر LFSR بر اتوماتا با احتمال کمتری مواجه است در صورتی‌که هرچه دما بالاتر رود ساختار سیستم ثابت‌تر است یعنی همیشه LFSR بر اتوماتا تاثیر می‌گذارد.

مراجع

[1] S. Nandi, B. Kar, and P. Chaudhuri, "*Theory and Applications of Cellular Automata in Cryptography*," IEEE Transaction Computers, vol. 43, no. 12, pp. 1346-1357, Dec. 1994.

[2] S. Blackburn, S. Merphy, and K. Paterson, "Comments on *'Theory and Applications of Cellular Automata in Cryptography'*," IEEE Transaction Computers, vol. 46, no. 5, pp. 637-638, May 1997.

[3] M. Tomassini, M. Perrenoud, "*Cryptography with cellular automata*", Applied Soft Computing no.1, pp 151-160, 2001.

[4] M. Szaban, F. Seredynski, P. Bouvry, "*Collective Behavior of Rules for Cellular Automata-based Stream Ciphers*", IEEE Proceeding of Evolutionary Computation, Sheraton Vancouver, July 2006.

[5] M. Szaban, F. Seredynski, P. Bouvry, "*Evolving Collective Behavior of Cellular Automata for Cryptography*", IEEE Proceeding of Melecon, Malaga, Spain, May 2006,

[6] F. Seredynski, P. Bouvry, A. Zomzyz, "*Cellular Automata computations and secret key cryptography*", Parallel Computing, no. 30, pp. 753-766, 2004.

[7] H. Li, C.N. Zhang, "*A Cellular Automata Based Reconfigurable Architecture for Hybrid Cryptosystems*", The Computer Journal, vol 47, no.3, 2004.

[8] S.U. Guen, S. Zhang, "*Pseudorandom number generation based on controllable cellular automata*", Future generation computer systems, no. 20, pp. 627-641, 2004.

[9] S.U. Guan, S.K. Tan, "*Pseudorandom Number Generation With Self-Programmable Cellular Automata*", IEEE Transactions on computer-aided design of integrated circuits and systems, vol.23, no.7, July 2004.

[10] J.P. Giddy, R.Safavi Naini, "*Automated Cryptanalysis of Transposition Ciphers*", The Computer Journal, vol.37, no. 5, 1994.

[11] F. Bao, "*Cryptanalysis of a Partially Known Cellular Automata Cryptosystem*", IEEE Transactions on Computers, vol. 53, no. 11, November 2004.

[12] A. Menezes, P.van Oorschot and S. Vanstone, "*Handbook of Applied Cryptography*", CRC Press, 1996.

[13] B. Tsaban, U. Vishne, "*Efficient Linear Feedback Shift Registers with Maximal Period*", Finite Fields and Their Applications, no 8, pp.256–267, 2002.

[14] Z. Jiang, Y. Zhan, D. Chen, Y. Wang, "*Two methods of directly constructing probabilistic public-key encryption primitives based on third-order LFSR sequences*", Applied Mathematics and Computation, no 171, pp. 900–911, 2005

[۱۵] S. Haykin, "*Neural Networks – A Comprehensive Fundation*", 2th Edition, Prentice Hall, ©1999.

[16] Bar-Yam, Yaneer, "*Dynamics of Complex Systems*", Copyright © 1997, , Addison Wesley Longman, Inc.

[17] T.M. Cover, J.A. Thomas, "*Elements of Information Theory*", Copyright @ 1991 John Wiley & Sons, Inc.

[18] D.J.C. MacKay, "*Information Theory, Inference, and Learning Algorithms*", June 26, 2003, Cambridge university Press.

[19] S. Wolfram, "*Cryptography with Cellular Automata*" Proceeding of Advances in Cryptology, pp. 429-432, 1986.

[20] G. Bolch, Stefan Greiner, H. de Meer, K. S. Trivedi, "*Queueing Networks and Markov Chains Modeling and Performance Evaluation with Computer Science Applications*", Copyright © 2006,John Wiley & Sons, Inc.

پیوست ۱:

فرمول‌های رمزبرداری برای اتوماتای سلولی ۷ بیتی که از قضیه ۱ تبعیت می‌کند به شرح زیر است:

$$s_1(t) = (s_1(t+1) + s_3(t+1) + s_4(t+1) + s_6(t+1) + s_7(t+1) + LFSR_1(t+1)) \bmod 2$$

$$s_2(t) = (s_3(t+1) + s_4(t+1) + s_6(t+1) + s_7(t+1) + LFSR_1(t+1)) \bmod 2$$

$$s_3(t) = (s_1(t+1) + s_2(t+1)) \bmod 2$$

$$s_4(t) = (s_1(t+1) + s_2(t+1) + s_4(t+1) + s_6(t+1) + s_7(t+1) + LFSR_1(t+1)) \bmod 2$$

$$s_5(t) = (s_6(t+1) + s_7(t+1) + LFSR_1(t+1)) \bmod 2$$

$$s_6(t) = (s_1(t+1) + s_2(t+1) + s_4(t+1) + s_5(t+1)) \bmod 2$$

$$s_7(t) = (s_1(t+1) + s_2(t+1) + s_4(t+1) + s_5(t+1) + s_7(t+1) + LFSR_1(t+1)) \bmod 2$$

♣ در جدول بالا $LFSR_1(t+1)$ مقدار سمت چپ‌ترین بیت $LFSR$ در زمان $t+1$ می‌باشد.