



رمزنگاری اطلاعات بر اساس عوامل محیطی با استفاده از اتوماتای سلولی

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

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

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

چکیده: در این مقاله کوشش شده است روشی نوین در رمزگذاری اطلاعات با استفاده از اتوماتای سلولی ارائه شود. این روش با ترکیب قابلیت‌های ثابت‌های 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، اتوماتای سلولی، LFSR، مکانیک آماری، توزیع گیبز و زنجیره‌های مارکوف

۱. مقدمه

با گسترش شبکه‌های 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 برد 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 مثلاً 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^۱، متوسط اطلاعات موجود در هر پیغام را گویند. اگر منبعی بتواند n پیغام مختلف تولید کند آنگاه پیغام n م دارای مقدار اطلاعات

¹ Entropy

ترکیبی ارائه شده است که تا حد قابل توجهی وضعیت تولید اعداد تصادفی را بهبود می بخشد ولی مشکل آن استفاده از چندین قانون و در نتیجه سخت افزار پیچیده تر است. همچنین به دلیل سادگی عملکرد اتوماتا، رمزگشایی اطلاعات آسان است.

۳. فعالیت های مرتبط

فعالتهای مختلفی در زمینه تولید اعداد تصادفی و رمزنگاری اطلاعات صورت گرفته است. برخی از فعالیت ها، کاربرد اتوماتای سلولی را در رمزگذاری بررسی کرده اند. 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 سخت افزار قابل برنامه ریزی ارائه دهد.

برخی از فعالیت ها، قابلیت های قوانین اتوماتای سلولی در رمزنگاری را بررسی کرده اند. در [3] روش بهینه سازی برای تولید قانونی ترکیبی در اتوماتای سلولی ارائه شده است که دنباله طولانی از اعداد تصادفی می تواند 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 سخت افزارهای ارائه شده اکثرا قابل برنامه ریزی بوده و می توانند قوانین ترکیبی مختلفی را برای رمزنگاری اطلاعات استفاده کنند.

در برخی دیگر از فعالیت ها نیز صرفا نحوه رمزگشایی اطلاعات توسط اتوماتای سلولی بررسی شده است که روش های مختلفی از جمله ایجاد محیط متقارن فرستنده پیغام یا استفاده از روش های بهینه سازی پیمایش و حدس پیغام های رمز شده مورد توجه می باشند. در [10] با استفاده از روش بهینه سازی شبیه سازی گداختگی^۷، روشی ارائه شده است که بتواند متن رمز شده را رمزگشایی کند که البته دقت روش به طول پیغام وابسته می باشد. در این روش اختلاف بین متن رمز شده و اصلی بعنوان تابع هزینه در نظر گرفته شده است که با استفاده از روش شبیه سازی گداختگی سعی در کاهش این تفاوت دارد. در [11] ضعف های اتوماتای سلولی در مقابل حمله های رمزگشایی بررسی و روشی ساده جهت رمزگشایی برخی از قوانین اتوماتای سلولی برشمرده شده است.

اطلاعات $-n \cdot p_i \cdot \log(p_i)$ خواهد بود. که p_i احتمال رخداد پیغام i در رشته ارسالی پیغام هاست. بنابراین آنتروپی منبع برابر است با $H = -\sum_{i=1}^n p_i \cdot \log_2(p_i)$. به عبارت دیگر، اگر احتمال رخداد پیغامها متفاوت باشد باید پیغام های مهم تر با بیت کمتر و پیغام های کم ارزش تر با بیت بیشتر ارسال شوند بطوری که 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].

روش های مختلفی در رمزگذاری اطلاعات مطرح است که بطور کلی به دو دسته رمزگذاری جویباری^۱ و بلوکی^۲ تقسیم می شوند [12, 18]. که در نوع اول، در هر لحظه، رمزگذاری بیت به بیت یا کاراکتر به کاراکتر انجام می گیرد ولی در نوع دوم تمام رشته پیغام به یکباره رمز شده و ارسال می گردد. بطور کلی برای هر دو روش رمزگذاری از کلیدهایی استفاده می گردد که از اعداد شبه تصادفی^۳ ایجاد شده اند. برای تولید اعداد تصادفی روش های مختلفی وجود دارد که از آن جمله می توان به مولدهای همبستگی خطی^۴ و غیر خطی، ثباتهای بازگشتی خطی^۵ (LFSR) و غیر خطی و اتوماتای سلولی^۶ (CA) و ... اشاره کرد. LFSRها به دلیل سادگی سخت افزار و قابلیت ایجاد دنباله طولانی از اعداد تصادفی بسیار مورد استفاده قرار می گیرند اما در این گونه روش ها، رمزگذاری بصورت جویباری انجام می گیرد و برای رمز کردن n بیت اطلاعات نیاز به n کلک می باشد. همچنین مجموعه مقادیر تولید شده توسط این روش مرتباً طبق یک الگوی مشخص تکرار می شوند [15].

اتوماتای سلولی بدلیل داشتن الگوریتم و پیاده سازی ساده سخت افزاری از اهمیت خاصی در تولید اعداد شبه تصادفی برخوردار است. در این روش مجموعه ای سلول تشکیل یک اتوماتای سلولی را می دهند هر سلول به همراه سلولهای همسایه، بر اساس قانون تعریف شده ای مقدار خود را بروز می کند [19]. از آنجا که به راحتی نمی توان عملکرد اتوماتا سلولی را در مرحله بعد حدس زد از آن برای تولید اعداد شبه تصادفی استفاده می گردد. مشکل این روش، تولید دنباله کوتاهی از اعداد است بطوری که مجموعه ای از اعداد تولید شده مرتباً تکرار می گردد. برای رفع این مشکل قانون های ترکیبی یا اتوماتای

¹ Stream Ciphering

² Block Ciphering

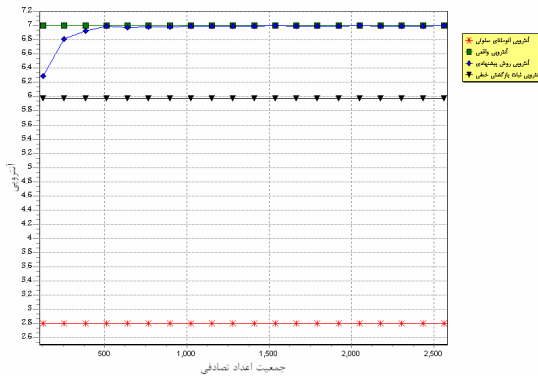
³ Pseudorandom number

⁴ Liner Congruential generators

⁵ Linear Feedback Registers

⁶ Cellular Automata

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

دنباله اعداد تصادفی تولید شده توسط اتوماتای سلولی روش پیشنهادی، خیلی سریع به سمت آنتروپی حداکثر همگرا می شود و این نشان می دهد که تمام اعداد تصادفی در این رنج تولید شده و دارای توزیع یکنواخت می باشند. 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 می باشد.

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

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

همان طور که مشاهده می گردد 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 می باشد. حداکثر آنتروپی با LFSR ۶ بیتی تولید شده است که ۶،۹۹۶ است.

به نظر می رسد بر اساس نتیجه ای 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.

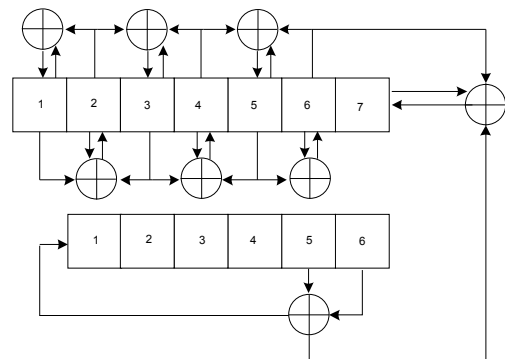
در برخی از فعالیتها، عملکرد LFSRها بررسی و توسعه داده شده اند. در [12] ثباتهای بازگشتی خطی تعریف شده و عملکرد آنها برای تولید اعداد تصادفی با دنباله طولانی بررسی شده است. در [13] و [14] راههای توسعه LFSRها و ایجاد LFSRهای ترکیبی بررسی شده و راهکارهایی برای تولید اعداد تصادفی با دنباله بیشتر ارائه شده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

۴. روش پیشنهادی تولید اعداد تصادفی

قسمت بالای شکل (۱) عملکرد یک اتوماتای سلولی ۷ بیتی را نشان می دهد. این اتوماتا طبق قانون ۱۵۰ کار می کند [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. به عبارت دیگر مقدار هر سلول از فرمول (۱) محاسبه می شود.

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

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

همان طور که مشاهده می گردد دنباله تولید شده کوتاه بوده و برخی از اعداد این بازه مرتباً تکرار می گردند. بنابراین آنتروپی با افزایش تولید اعداد تصادفی به نقطه ثابت ۲،۸۰ همگرا می شود که این نقطه از آنتروپی حداکثر ۷، بسیار فاصله دارد و نشان می دهد اعداد توسط مولد تصادفی مناسبی تولید نشده اند.

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. همان طور که مشاهده می گردد بیت ۵ و ۶ بایکدیگر جمع مبنای ۲ شده سپس بیت های ثبات یکی به راست شیفت می یابد و مقدار حاصل جمع در بیت آخر قرار می گیرد. در شکل (۲)، توانایی تولید LFSR ۶ بیتی نشان داده شده است. بطوری که 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 می باشد.

بطور کلی مکانیک آماری^۱ بیان می‌کند که یک سیستم با محیط اطرافش در تعادل دمایی^۲ است اگر حالت T ام سیستم با احتمال زیر اتفاق بیفتد.

$$P(s_i) = \frac{e^{-\frac{E(s_i)}{kT}}}{Z} \quad Z = \sum_{i=1}^n e^{-\frac{E(s_i)}{kT}} \quad (8)$$

که s_i حالت سیستم از میان n حالت منتهای است. $P(s_i)$ احتمال اینکه سیستم در حالت s_i باشد و $\sum_i P(s_i) \cdot E(s_i) = 1$ انرژی سیستم در حالت s_i است، T دمای تعادل بر اساس مقیاس کلین و k ثابت بولتزمن^۳ می‌باشد. هنگامی که T مقیاسی ندارد نیازی به مقدار k نیست بنابراین توزیع احتمال (۸) که به توزیع گیبز^۴ معروف است به فرم زیر بیان می‌شود.

$$P(s_i) = \frac{e^{-\frac{E(s_i)}{T}}}{Z} \quad Z = \sum_{i=1}^n e^{-\frac{E(s_i)}{T}} \quad (9)$$

بدلیل اینکه مولد اعداد تصادفی پیشنهادی می‌تواند دنباله طولانی از اعداد تصادفی با آنتروپی بیشینه و حدود $H = \log_2 n$ تولید کند تمام n مقدار ممکن ظاهر خواهند شد. به عبارتی تمام حالات سیستم (اعداد ممکن) از یکدیگر قابل حصول هستند بنابراین بر طبق قانون تعادل در زنجیره‌های مارکوف^۵ [20] داریم:

$$P(s_i) \cdot P(s_i \rightarrow s_j) = P(s_j) \cdot P(s_j \rightarrow s_i) \quad (10)$$

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

$$\frac{P(s_j)}{P(s_i)} = \frac{P(s_i \rightarrow s_j)}{P(s_j \rightarrow s_i)} = e^{-\frac{\Delta E}{T}} \quad (11)$$

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

یعنی اگر احتمال $P(s_j \rightarrow s_i) = 1$ بگیریم آنگاه

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

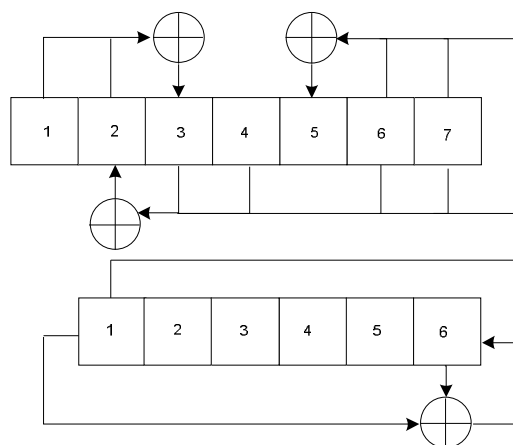
حالت را $P(s_i \rightarrow s_j) = \min[1, e^{-\frac{\Delta E}{T}}]$ در نظر بگیریم آنگاه سیستم در حالت تعادل ترمودینامیکی خواهد بود و احتمال رخداد هر وضعیت از توزیع گیبز تبعیت می‌کند. با توجه به دستاورد بالا اگر انرژی هر حالت سیستم عددی باشد که LFSR نشان می‌دهد همچنین $n = 2^m - 1$ (برابر تعداد بیت‌های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

$$0 = (s_{i+1}(t+1) + s_{i+2}(t+1) + s_{i+4}(t+1) + \quad (7)$$

$$s_{i+5}(t+1) + \dots + s_{i+N-2}(t+1) + s_{i+N-1}(t+1))$$

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

با توجه به قضیه ۱ می‌توان الگوریتم رمزبرداری را به صورت زیر بیان کرد. رشته رمز شده وارد ساختار بیتی شکل (۵) شده (به دلیل فشردگی، مدار سخت‌افزار آن برای بیت ۲، ۳ و ۵ کامل کشیده شده است)، مقدار اولیه LFSR نیز برابر عددی قرار می‌گیرد که از k امین کلاک حالت تمام ۱ (فرض مقدار اولیه) بدست می‌آید. در این صورت سیستم شروع به کار کرده و زمانی که 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 n ها 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)

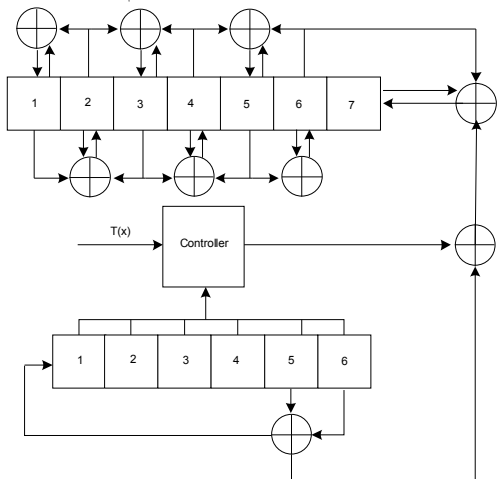
۷. رمزگذاری اطلاعات بر اساس دمای محیط

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 تقریباً 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].

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

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 کنترل‌کننده صفر) و گرنه خروجی اعمال نمی‌شود (خروجی کنترل‌کننده برابر $(LFSR_1(t+1))$). این موضوع چه در فرستنده و چه در گیرنده 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 سؤال مطرح است که نقش دما در عملکرد سیستم رمزگذاری چیست؟ در پاسخ به این سؤال 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

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

$ThermalCiphering(PlainText, Key, Temperature): CipherText$

Begin

$CipherText := PlainText;$

$T := Temperature;$

For $i := 1$ to Key do

begin

$CipherText := CA(CipherText);$

$current_LFSR := LFSR();$

$E(s_i) = last_LFSR;$

$E(s_j) = current_LFSR;$

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

if $\Delta E < 0$ then

$CipherText := CipherText \text{ Xor } current_LFSR[1];$

Else

begin

$rn := create_random_number; //with known generator in [0,1]$

$\frac{-\Delta E}{T}$

if $rn \leq e^{-\frac{\Delta E}{T}}$ then

$CipherText := CipherText \text{ Xor } current_LFSR[1];$

end;

$last_LFSR := current_LFSR;$

end;

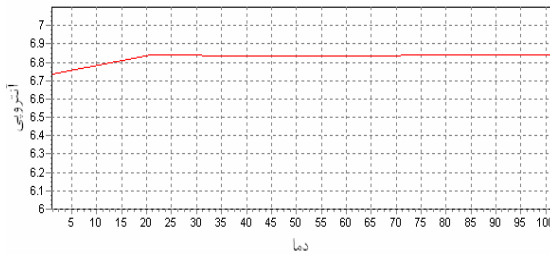
End;

به عبارت 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 کنترل‌کننده مساوی مقدار صفر شده تا $LFSR_1(t+1)$ اعمال گردد. در غیر این صورت یک عدد تصادفی با توزیع یکنواخت با مولد شناخته شده (مولدی که در فرستنده و گیرنده به یک شکل عمل کنند) تولید می‌شود اگر عدد تصادفی تولید شده از $e^{-\frac{\Delta E}{T}}$ کوچکتر باشد خروجی کنترل‌کننده صفر شده که باعث می‌شود $LFSR_1(t+1)$ بر اتوماتا تاثیر بگذارد. در غیر این صورت خروجی کنترل‌کننده مساوی $LFSR_1(t+1)$ خواهد بود که باعث عدم تاثیر LFSR بر اتوماتا می‌گردد.

با توجه به عملکرد کنترل‌کننده شکل (۶)، می‌توان روش رمزگذاری بخش ۴ را به صورت 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

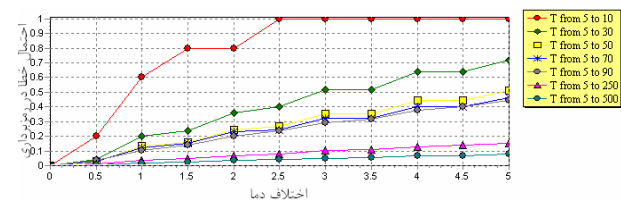


شکل ۹: تغییرات آنتروپی اتوماتا بر اساس تغییر دما

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 درحالی که گیرنده در دمای $T \pm \Delta T$ اطلاعات را رمزبرداری کند.

الگوریتم فوق برای ۱۰۰۰ نمونه عدد در بازه دمایی مختلف مجدداً بررسی شده است. بدین ترتیب که در دمای T رمزگذاری و در دمای $T - \Delta T$ 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 می‌باشد. 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 می‌تواند تا ۱ درجه باشد. مثلاً اگر اطلاعات در دمای ۴۵ رمز شود، گیرنده می‌تواند اطلاعات را در دمای بین ۴۴ تا ۴۶ رمزگشایی کند.

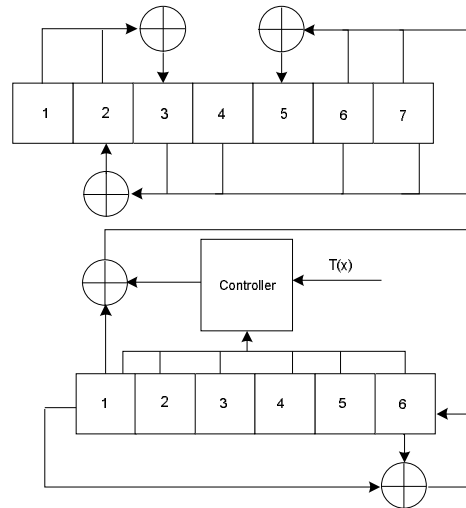


شکل ۱۰-۱: احتمال خطا در رمزبرداری با $K=50$

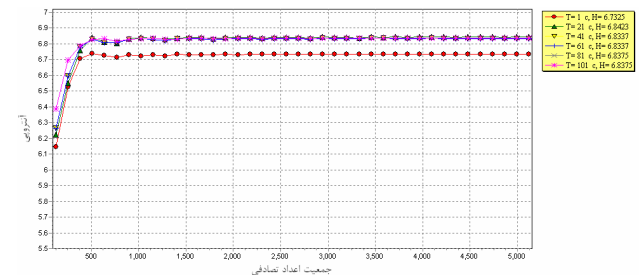
۱۱. نتیجه‌گیری

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

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 کنترل کننده‌ای 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 این صورت 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.

[6] F. Serebinski, P. Bouvry, A. Zomzoy, "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

[15] S. Haykin, "Neural Networks – A Comprehensive Foundation", 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.

رمزگذاری و رمزبرداری اطلاعات را نیز دارد. همچنین روش پیشنهادی بر خلاف اکثر روش‌های تولید اعداد تصادفی همچون همبستگی 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 به عمل آمده مشخص شد آنتروپی کل سیستم متأثر 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 به عبارتی تأثیر LFSR بر اتوماتا با احتمال کمتری مواجه است در صورتی که هرچه دما بالاتر رود ساختار سیستم ثابت‌تر است یعنی همیشه LFSR بر اتوماتا تأثیر 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. Serebinski, 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. Serebinski, P. Bouvry, "Evolving Collective Behavior of Cellular Automata for Cryptography", IEEE Proceeding of Melecon, Malaga, Spain, May 2006,

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.