طّراحی و ارزیابی رمزکننده‌های پی‌درپی و معرفی یک ساختار جدید[1]

دکتر محمدرضا عارف

دانشکده برق و کامپیوتر ـ دانشگاه صنعتی اصفهان

مهندس سید محمود مدرس هاشمی

دانشکده برق و کامپیوتر ـ دانشگاه صنعتی اصفهان

چکیده

رمزکننده‌های پی در پی رمزکننده‌هایی هستند که در آنها برای تولید یک متن رمزشده، یک دنبالهٔ دودویی به نام کلید اجرائی با دنبالهٔ دودویی متن اصلی به هنگ دو جمع می‌شود. جهت مصون ماندن رمزکننده از حملات رمزنگاری، کلید اجرائی و مولّد آن باید خواص ویژه‌یی را دارا باشند. در این مقاله مهمترین این ویژگیها مانند دورهٔ تناوب، پیچیدگی خطی، خواص آماری، مصونیت از همبستگی و معیار بهمنی مورد بحث قرار می‌گیرند. سپس با مروری به برخی از ساختارهای مولّد کلید اجرائی حافظه‌دار، سیستمهای مبتنی بر تسهیم‌کننده مورد توجه قرار گرفته و برای دستیابی به یک ساختار بسیار قوی، اصلاحی اساسی بر روی ساختار منطقی جامع صورت می‌گیرد. برخی از ویژگیهای این ساختار جدید به اثبات می‌رسد و با استفاده از شبیه‌سازی، نتایج تجربی در مورد سایر خصوصیّات ارائه می‌گردد.

۱ـ مقدمه

دسته‌ای از مهمترین و کاربردی‌ترین رمزکننده‌های امروزه را رمزکننده‌های "پی در پی"[2] تشکیل می‌دهند. در این رمزکننده‌ها یک دنبالهٔ شبه تصادفی توسط ساختاری موسوم به "مولّد کلید اجرایی"[3] تولیدشده و با دنبالهٔ دودویی متن اصلی XOR می‌شود که متن رمزشده را به وجود می‌آورد. این دنبالهٔ شبه تصادفی که دنبالهٔ کلید اجرایی نامیده می‌شود، با استفاده از الگوریتمی خاص که بر روی کلید اصلی سیستم (پارامتر سری تطابقی بین فرستنده و گیرنده) عمل می‌کند، تولید می‌گردد. هستهٔ اصلی یک رمزکنندهٔ پی در پی همین مولد کلید اجرایی است و هدف نهایی این مقاله نیز معرفی برخی از مولّدهای این کلید اجرایی و مقایسهٔ آنها با یکدیگر و معرفی یک مولد کلید اجرایی جدید است.

به طور کلّی تاکنون چهار روش برای طّراحی یک مولّد کلید اجرایی پیشنهاد شده است که عبارتند از: روش نظری اطلاعاتی، روش نظری پیچیدگی، روش نظری سیستمی و روش جستجو جهت رمزهای با ایمنی قابل اثبات [۱]. گذشته از مزایا و معایبی که هر یک از روشهای فوق دارند، تاکنون هیچ یک از این روشها به جز روش نظری سیستمی منجر به

۱ـ انجام پژوهشهای این مقاله با حمایت جهاددانشگاهی دانشگاه صنعتی اصفهان همراه بوده است که بدین وسیله از این نهاد تشکر می‌شود.

2- Stream Cipher Systems

3- Running Key Generator

رمزکننده‌های با ایمنی بالا و عملی نشده است. به همین دلیل روش نظری سیستمی به عنوان رایج‌ترین روش طراحی سیستمهای رمزکنندهٔ پی‌درپی مطرح است. از دیدگاه این روش، یک رمزکنندهٔ پی‌درپی "امن عملی" نامیده می‌شود. هرگاه، توسط هیچ یک از حملات شناخته‌شدهٔ رایج، در زمان معقول شکسته نشود. در این مقاله نیز همین روش را انتخاب نموده و بر اساس آن، معیارهایی که در ارتباط با حملات رایج علیه این سیستمها هستند را مورد بررسی قرار می‌دهیم. در انتها نیز برخی از مهمترین سیستمهای ارائه‌شده به عنوان مولّد کلید اجرایی را از دیدگاه این معیارها بررسی نموده و قویترین آنها را معرفی خواهیم نمود.

۲ـ معیارهای طراحی و ارزیابی:

چنانکه گفتیم در طراحی سیستمی رمزکننده‌های پی‌درپی، سؤال اساسی آن است که جهت دستیابی به ایمنی لازم، چه معیارهایی را باید در نظر گرفت و برای تحقّق این معیارها چگونه باید کلید اجرایی مورد نیاز را تولید نمود.

از نقطه نظر ایمنی، حالت ایده‌آل آن است که دنبالهٔ رمزشد ، یک دنبالهٔ کاملاً مستقل بوده و احتمال صفر و یک بودن هـ ـهٔ بیت‌ها نیز یکسان باشد (یعنی دنباله i.i.d باشد). به راحتی می‌توان ثابت نمود که برای دستیابی به این منظور کافی است کلید اجرائی $\bar{z}$ دنباله‌ای i.i.d باشد. بنابراین هدف اساسی طراحی رمزکننده‌های پی در پی ، طراحی مولد کلید اجرایی است به گونه‌ای که دنبالهٔ خروجی آن یک دنبالهٔ i.i.d باشد.

واضح است که استفاده از کلید اصلی جهت تولید کلید اجرایی همواره منجر به یک دنبالهٔ متناوب می‌شود. بنابراین دنبالهٔ کلید اجرایی مسلّماً یک دنبالهٔ واقعاً تصادفی نخواهد بود. امّا اگر دورهٔ تناوب دنباله بسیار زیاد باشد، و خواص دیگر تصادفی بودن دنباله‌ها نیز برقرار باشد آن را دنبالهٔ "شبه تصادفی" نامیده و می‌توان از آن به عنوان کلید اجرایی استفاده نمود. در این بخش به توضیح این ویژگیهای لازم می‌پردازیم.

الف ـ خواص آماری:

در سال ۱۹۶۷ "گالوب"[1] [10] سه معیار: تساوی صفر و یکها در یک دورهٔ تناوب، توزیع مناسب "رنها"[2] (زیردنباله‌های تمام صفر یا تمام یک) و کوچک بودن تابع خود همبستگی دنباله را به عنوان معیارهای اساسی شبه‌تصادفی بودن دنباله‌ها مطرح نمود. وی همچنین "ثبّاتهای تغییر مکان بازخوردی خطی"[3] را به عنوان ابزار تولید این دنباله‌ها پیشنهاد کرد. امّا به دلیل خطی بودن ثباتهای بازخوردی، به راحتی این ساختارها شکسته شده و با داشتن ۲n بیت متوالی از خروجی ثبّاتهای بازخوردی به طول n می‌توان چندجمله‌یی فیدبک و حالت اولیهٔ ثبّاتهای بازخوردی را با انجام عملیاتی از مرتبهٔ n^3 به دست آورد [۲]. بنابراین به نظر می‌رسد که علیرغم لزوم وجود معیارهای گالوب در دنباله‌های کلید اجرایی، این معیارها به هیچ وجه شرایط کافی جهت شبه‌تصادفی بودن دنباله‌ها نبوده و بایستی معیارهای دیگری را نیز به آنها افزود.

قبل از بیان معیارهای دیگر، مناسب است نحوهٔ ارزیابی یک دنباله و یا یک ساختار را از دیدگاه خواص آماری شرح دهیم: در ابتدا با استفاده از روابط آزمون χ^2 (مربع خی) و شرایط مورد نظر هر آزمون، رابطهٔ χ^2 را برای آن آزمون به دست می‌آوریم. سپس جهت ارزیابی یک دنباله مقدار χ^2 را از روی این رابطه محاسبه نموده و آن را با مقدار موجود در

1 - Golomb 2- Runs 3- Linear Feedback Shift Register

جدول χ^2 مقایسه می‌کنیم. عموماً میزان ۹۵٪ به عنوان معیار انتخاب می‌گردد. جهت ارزیابی یک ساختار تعداد زیادی از دنباله‌های تولید شده توسط ساختار را می‌آزمائیم و درصد دنباله‌های عبور کرده از آزمون را تعیین می‌نمائیم. میزان نزدیکی این مقدار به ۹۵٪ قوت ساختار را از دیدگاه آن آزمون نشان می‌دهد. البته واضح است که انجام آزمونها روی دنباله‌هایی به طول دورهٔ تناوب ساختار امکان‌پذیر نیست. به همین علّت آزمونها عموماً بر روی دنباله‌هایی کوچکتر اعمال شده و جهت اطمینان، از آزمونهای آماری متفاوتی استفاده می‌شود.

جهت انجام بررسیهای مربوط به ساختارها، شش آزمون آماری فراوانی، سریال، خودهمبستگی، پوکر، مشتقات دودویی و رنها را به کار می‌بریم.

ب - پیچیدگی خطی[1]

مهمترین معیاری که پس از میعارهای گالوب سطرح گردید، معیار پیچیدگی خطی است. طول طبقات کوچکترین ثبّاتهای تغییر مکان بازخوردی خطی که قادر به تولید یک دنباله باشد را پیچیدگی خطی یا معادل خطی آن دنباله می‌نامند. معیار پیچیدگی خطی، بزرگ بودن پیچیدگی خطی دنباله‌ها را شرطی لازم و اساسی برای شبه‌تصادفی بودن آنها می‌داند (مقیاس بزرگ بودن پیچیدگی خطی یک دنباله «L» آن است که دشمن نتواند به ۲L بیت از دنباله دسترسی پیدا کند و یا حتی در صورت دسترسی به آن انجام عملیاتی از مرتبهٔ L^3 برای او غیرعملی باشد). مقادیر نمونهٔ پیچیدگی خطی مناسب برای دنباله‌ها در عمل $10^{30}, 10^{40}, 10^{50}$ و مقادیری نظیر آنهاست.

اگر چه توسط "الگوریتم B-M"[2] می‌توان پیچیدگی خطی هر دنباله را به دست آورد، امّا اوّلاً به علّت فوق‌العاده بزرگ بودن دورهٔ تناوب دنباله‌های کلید اجرایی، به دست آوردن پیچیدگی خطی آنها غیر عملی است، ثانیاً به علّت نوسان پیچیدگی خطی خروجی یک ساختار به ازای حالات اولیهٔ مختلف، مشخص نمودن یک عدد ثابت به عنوان پیچیدگی خطی یک ساختار غالباً امکان‌پذیر نیست. لذا جهت ارزیابی یک مولد کلید اجرایی از دیدگاه پیچیدگی خطی، بایستی به صورت نظری مقدار پیچیدگی خطی یا حدود بالایی و پائینی آن را به دست آورد.

در اغلب موارد از خود ثباتهای تغییرمکان برای تولید دنباله‌های کلید اجرایی استفاده می‌شود و برای از بین بردن نقص ثبّاتهای تغییر مکان بازخوردی خطی و دستیابی به پیچیدگی خطی بسیار بالا، توابع غیرخطی را بر روی ثباتهای تغییرمکان اعمال می‌نماید. بطّور کلی این ساختارها را می‌توان در یکی از سه دستهٔ زیر جای داد [۳]:

۱ـ ثبّاتهای تغییرمکان که تابع بازخوردی آنها غیر خطی است.

۲ـ ساختارهائی که از ترکیب خروجیهای چند ثبّات تغییر مکان بازخوردی خطی توسط یک تابع غیرخطی تشکیل شده‌اند (فیدفوروارد ترکیب‌کنندهٔ حالت).

۳ـ ساختارهائی که از اعمال یک تابع غیرخطی به طبقات مختلف یک ثبّات تغییر مکان بازخوردی خطی تشکیل شده‌اند (فیدفوروارد‌فیلتر حالت).

به دلیل ساده‌تر بودن تحلیل ساختارهای فیدفوروارد نسبت به ساختارهای نوع بازخوردی و امکان دستیابی به خواص مطلوب ساختارهای با بازخوردی غیرخطی توسط ساختارهای فیدفوروارد، بررسی خود را بر روی ساختارهای فیدفوروارد متمرکز می‌کنیم.

1- Linear Complexity

2- Berlekamp - Massey

چنانکه گفتیم هدف عمده در اینجا، یافتن پیچیدگی خطی ساختارهای مختلف است. چندین روش برای تحلیل ساختارها از این دیدگاه مطرح شده است که از مهمترین آنها روش ماتریسی و روش جبری است [۳]. روش ماتریسی در حالتی که طول ثبّاتهای تغییر مکان بازخوردی خطی بزرگ باشد کارآیی ندارد، زیرا ابعاد ماتریسها بسیار بزرگ خواهند شد. امّا روش جبری در همهٔ حالات روشی کارآمد و مناسب است که ذیلاً به توضیح آن می‌پردازیم:

هرگاه دنبالهٔ... $\bar{a} = a_0 a_1 ... a_n$ توسط یک ثبّات تغییر مکان بازخوردی خطی به طول L تولید شده باشد، بطور کامل توسط حالت اولیه‌اش یعنی $(a_0, a_1, ..., a_{L-1})$ و رابطهٔ برگشتی زیر که مبیّن ثبّات تغییر مکان بازخوردی خطی است مشخص می‌شود:

$$a_k + \sum_{i=1}^{L} C_{L-i}\, a_{k-i} = 0 \qquad k \geq L \qquad (۱)$$

با استفاده از عملگر شیفت رابطهٔ فوق را می‌توان به صورت زیر نوشت:

$$(T^L + \sum_{i=1}^{L} C_{L-i}\, T^{L-i})\, a_n = 0 \qquad (۲)$$

$$n \geq 0 \quad , \quad T(a_n) = a_{n+1}$$

که این رابطه معادلهٔ مشخصهٔ زیر را نتیجه می‌دهد:

$$x^L + \sum_{i=1}^{L} C_{L-i}\, x^{L-i} = 0 \qquad (۳)$$

معادلهٔ فوق در حالت کلی ریشه‌هایی در $GF(2^m)$ دارد که m کوچکترین مضرب مشترک درجات عوامل ساده‌نشدنی چندجمله‌یی فوق است. اگر α چنین ریشه‌یی باشد، $A\alpha^n$ جوابی برای معادلهٔ برگشتی است (A ثابتی است در $GF(2^m)$) و واضح است که ترکیب خطی این جوابها، جواب عمومی معادله را تشکیل می‌دهد.

ثابت می‌شود که هرگاه P(x) یک چندجمله‌یی ساده‌نشدنی درجهٔ L روی GF(2) باشد، در این صورت این چند جمله‌یی دارای L ریشهٔ متمایز می‌باشد و اگر α یکی از این ریشه‌ها باشد، بقیه ریشه‌ها به صورت α^{2^k} $(k = 1,...,L-1)$ خواهند بود. بنابراین در این حالت داریم:

$$a_n = \sum_{i=0}^{L-1} A_i (\alpha^{2^i})^n \qquad (۴)$$

این رابطه مبنای روش جبری تحلیل پیچیدگی خطی را تشکیل می‌دهد.

به عنوان مثال فرض کنید که در ساده‌ترین حالت، خروجی دو طبقهٔ از یک ثبّات تغییر مکان بازخوردی خطی (a^*_n, a_n) را در یکدیگر ضرب نموده و یک فیلتر حالت ساده طراحی نموده‌ایم. در این حالت داریم:

$$\text{خروجی نهائی} = a_n a^*_n = \sum_{i=0}^{L-1} \sum_{j=0}^{L-1} A_i A^*_j \left(\alpha^{2^i + 2^j}\right)^n \qquad (۵)$$

نمای α در رابطهٔ اخیر $(2^i + 2^j)$ می‌تواند به عنوان نمایش باینری L رقمی یک عدد صحیح m در نظر گرفته شود. چون $\alpha^{2^L - 1} = ۱$ است بنابراین تمام μهایی که در هنگ $2^L - 1$ مساویند یک عنصر را نتیجه می‌دهند (α^μ برای آنها برابر است). اگر i=j باشد، μ تنها یک بیت غیر صفر دارد و تعداد چنین μهائی L است. اگر $i \neq j$ باشد عدد صحیح μ دارای دو بیت غیرصفر است که $\binom{L}{2} = \frac{L}{2}(L-1)$ تا از چنین μهائی وجود دارد. بنابراین کلاً $\frac{L}{2}(L+1) + L = \frac{L}{2}$ نمای متمایز برای α وجود دارد و چون در این حالت می‌توان ثابت نمود که هیچ یک از ضرائب $A_i A^*_j$ صفر نیستند [۳]، بنابراین پیچیدگی خطی دنبالهٔ مذکور همان $\binom{L}{2} + L$ خواهد بود.

با استفاده از این روش، نتایجی در مورد پیچیدگی خطی فیلترهای حالت و ترکیب‌کننده‌های حالت به دست می‌آید که به برخی از آنها اشاره می‌کنیم. امّا قبل از بیان این نتایج، مرتبهٔ غیرخطی یک تابع را تعریف می‌نمائیم. هر تابع f که روی N متغیّر $x_1, ..., x_N$ عمل می‌کند را می‌توان به صورت زیر که آن را

فرم معمولی "جبری"[1] (ANF) تابع می‌نامند نوشت:

$$f(x_1,\dots,x_N) = a_0 + \sum_{i=1}^{N} a_i x_i + \sum_{i=1}^{N}\sum_{i=1}^{N} a_{ij}\, x_i x_j + \dots + a_{12..N}\, x_1 \dots x_N \qquad (۶)$$

هر جمله که حاصلضرب n متغیّر x_i باشد دارای مرتبهٔ ضربی n است و مرتبهٔ غیرخطی تابع f عبارتست از حداکثر مرتبهٔ ضربی موجود در نمایش آن تابع.

حال به ذکر برخی از قواعد مهمّ مربوط به تعیین پیچیدگی خطی می‌پردازیم:

۱ـ فیلتر حالت [۳]: اگر تابع f با مرتبهٔ غیرخطی k به طبقات مختلف ثبّاتهای تغییر مکان بازخوردی خطی به طول L اعمال شود اولاً:

$$L(\tilde{z}) \le \sum_{i=1}^{k} \binom{L}{i} \qquad (۷)$$

و ثانیاً احتمال فاصله گرفتن پیچیدگی خطی از باند بالایی فوق کمتر از $1\text{-}e^{-1/L}$ بوده که با افزایش L کاهش می‌یابد.

۲ـ ترکیب‌کنندهٔ حالت [۳]: فرض کنید تابع f به دنباله‌های ورودی $\tilde{a}_1,\dots,\tilde{a}_N$ اعمال گردد که این دنباله‌ها خروجیهای مولدهایی با فیلتر حالت باشند. اگر چند جمله‌ییهای بازخوردی به کار رفته در ثبّاتهای تغییر مکان بازخوردی خطی راه‌انداز این دنباله‌ها، ساده‌نشدنی بوده و درجهٔ آنها نیز دو به دو نسبت به هم اوّل باشند آنگاه پیچیدگی خطی خروجی تابع f عبارآزمون از:

$$L(\tilde{z}) = f(L(\tilde{a}_1),\dots,L(\tilde{a}_N)) \qquad (۸)$$

امّا در صورتی که دنباله‌های $\tilde{a}_i$ خروجی ثبّاتهای تغییر مکان بازخوردی خطی باشند، برای برقراری رابطهٔ فوق کافیست که طول ثبّاتهای تغییر مکان بازخوردی خطی از یکدیگر متمایز باشد.

۳ـ ترکیب‌کنندهٔ حالت [۴]: هرگاه تنها اطّلاع ما از دنباله‌های ورودی تابع f یعنی $\tilde{a}_i$ها، اوّل بودن دورهٔ تناوب آنها نسبت به یکدیگر باشد می‌توان نوشت:

$$L(\tilde{z}) \ge \hat{f}\,(L(\tilde{a}_1)-1,\dots,L(\tilde{a}_N)-1) \qquad (۹)$$

که در آن $\hat{f}$ تنها شامل جملات با بزرگترین مرتبهٔ ضربی در تابع f است.

از روابط فوق به ویژه نتیجهٔ (۱) در تحلیل ساختارهائی که در ادامه خواهد آمد یاری خواهیم جست.

ج ـ پلّه‌ای بودن پیچیدگی خطی:

به راحتی می‌توان مشاهده نمود که تنها بالا بودن پیچیدگی خطی یک دنباله جهت تصادفی بودن آن کافی نیست. به عنوان مثال فرض کنید دنباله‌یی را در نظر بگیریم که در یک دورهٔ تناوب، تمام بیتهای آن صفر و تنها بیت آخر آن 1 باشد، یعنی:

$$\tilde{Z}^{T} = 00.....001 \qquad (۱۰)$$

که در آن، T معرّف دورهٔ تناوب دنباله است. پیچیدگی خطی چنین دنباله‌ای برابر با دورهٔ تناوب آن یعنی T (بیشترین مقدار ممکن) است امّا واضح است که این دنباله به هیچ وجه شرایط یک دنبالهٔ شبه‌تصادفی را ندارد.

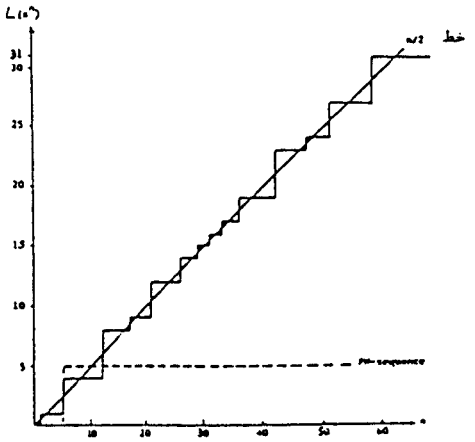
شرط دیگری که جهت حذف چنین دنباله‌هایی از دنباله‌های با پیچیدگی خطی بالا پیشنهاد شده است پلّه‌یی بودن نمودار پیچیدگی خطی است. "نمودار پیچیدگی خطی"[2] یک دنباله به این صورت به دست می‌آید که از ابتدای دنباله شروع کرده و پیچیدگی خطی مربوط به اولین بیت، دو بیت اول، سه بیت اول و ... را می‌یابیم تا به پیچیدگی خطی نهائی برسیم و آنگاه این مقادیر را در مقابل تعداد بیتهای متناظرشان رسم می‌کنیم.

شرط فوق بیان می‌دارد که این نمودار باید به صورت پلّه‌یی افزایش یابد و ضعف دنباله‌هائی نظیر دنبالهٔ (۱۰) در

1 - Algebric Normal Form (ANF)

2 - Linear Complexity Profile (LCP)

جهشی بودن LCP آن است. شکل (۱) نمونه‌یی از یک دنباله با دورهٔ تناوب T= ۳۱، پیچیدگی خطی L=۳۱ و دارای پیچیدگی خطی پلّه‌یی را نشان می‌دهد.



شکل ۱ـ LCP یک دنبالهٔ متناوب شبه‌تصادفی

ثابت می‌شود [۳] که نمودار پیچیدگی خطی دنباله‌های تصادفی خط $\frac{n}{2}$ را دنبال می‌کند و میانگین افزایش بیتها برای رسیدن مجدّد به مقدار $\frac{n}{2}$ برابر چهار و میانگین جهش پیچیدگی خطی برابر دو می‌باشد.

براساس شبیه‌سازیهای انجام شده [۱۱]، به نظر می‌رسد که برای دنباله‌هایی که پیچیدگی خطی آنها نزدیک به دورهٔ تناوب است شرط خواص آماری مطلوب نسبت به پلّه‌یی بودن LCP شرط قویتری است.

لازم به ذکر است که جهت بررسی وجود این شرط در دنباله‌های واقعی، به علّت بزرگی دورهٔ تناوب بایستی از آزمونهای آماری استفاده نمود. به عبارت دیگر بایستی پلّه‌یی بودن پیچیدگی خطی قطعات کوچک دنباله‌ها را بررسی نموده و درصد دنباله‌های موّفق را به عنوان معیار وجود یا عدم وجود شرط پلّه‌یی بودن LCP مورد توجه قرار داد.

د ـ مصونیت از همبستگی:

معیارهایی که تاکنون بیان نمودیم شرایط لازمی را برای دنباله‌های کلید اجرایی مطرح می‌کردند. از این پی به بررسی معیارهایی خواهیم پرداخت که شرایط و ویژگیهای خاصی را برای ساختارهای مولّد کلید اجرایی مطرح می‌نمایند.

یک ساختار ترکیب‌کنندهٔ حالت را در نظر بگیرید که در آن از S عدد LFSR به عنوان ورودی تابع f استفاده شده و خروجی تابع f به عنوان کلید اجرایی با متن اصلی XOR می‌شود. می‌دانیم که در یک حملهٔ جستجوی کامل برای یافتن همهٔ چند جمله‌یهای فیدبک و حالات اولیه، نیاز به $K \triangleq \prod_{i=1}^{s} R_i(2^{r_i}-1)$ جستجوی مختلف داریم که در آن r_i طول LFSR شمارهٔ i و R_i تعداد چند جمله‌یهای اولّیهٔ مربوط به آن است.

در سال ۱۹۸۳ "سیژن تالر"[1] با استفاده از $\frac{1}{2}$ نبودن احتمال تطابق خروجی تابع f با خروجی ثبّاتهای تغییرمکان بازخوردی خطی در برخی از ساختارها و نیز غیریکنواخت بودن توزیع متن اصلی، اقدام به حمله‌یی علیه این سیستمها نمود که حاصل آن کاهش عملیات مورد نیاز جهت شکستن سیستم از مقدار K به مقدار $\sum_{i=1}^{s} R_i(2^{r_i}-1)$ بود و این موفقیّت بزرگی در حمله به این سیستمهاست [۵]. این حمله به صورت دیگری نیز علیه ساختارهای فیلتر حالت عملی گردید [۶]. به همین دلیل مصونیّت ساختارها در قبال حملهٔ همبستگی به عنوان یکی از معیارهای امنیت ساختارها مطرح شده و جهت ارزیابی کمّی ساختارها از این دیدگاه تعریف زیر جهت مصونیت از همبستگی پیشنهاد می‌گردد. تابع بدون حافظهٔ f با ورودیهای $x_1,...,x_N$ و خروجی Z را دارای مصونیت از همبستگی مرتبهٔ m نامند هرگاه:

$$I(Z;x_{i_1},...,x_{i_m}) = 0$$

$$1 \le i_1 < i_2 < ... < i_m \le N \qquad (11)$$

1 - T.Siegenthaler

به راحتی می‌توان ثابت نمود که مرتبهٔ غیرخطی یک تابع با مرتبهٔ مصونیت از همبستگی آن "معاوضه"[1] داشته و افزایش یکی منجر به کاهش دیگری می‌گردد [۳]. در نتیجه، تحقّق همزمان مصونیت از همبستگی و پیچیدگی خطی مطلوب امکان‌پذیر نیست. جهت حل این مشکل می‌توان از ساختارهای حافظه‌دار استفاده نمود. زیرا که در اینگونه ساختارها، می‌توان وظیفهٔ تأمین پیچیدگی خطی و مصونیت از همبستگی را از یکدیگر جدا ساخت. به عنوان نمونه، می‌توان با در نظر گرفتن M بیت حافظه برای سیستم، خروجی و حالت بعدی را به صورت زیر تولید نمود:

$$\begin{cases} Z_j = \sum_{i=1}^{N} x_{ij} + \sum_{i=1}^{M} S_{ij} & \text{(۱۲ ـ الف)} \\ S_j = f_s(x_{1j}, \dots, x_{Nj}, S_{j-1}) & \text{(۱۲ ـ ب)} \end{cases}$$

در چنین ساختاری مرتبهٔ مصونیت از همبستگی برابر با مقدار ماکزیمم خود (N) بوده و با انتخاب f_s می‌توان پیچیدگی خطی بالایی را به دست آورد.

لازم به ذکر است که استفاده از حافظه جهت رفع مشکل مذکور نه شرطی لازم و نه کافی است، امّا یکی از روشهای مفید و کارآمدی است که در صورت استفادهٔ صحیح از آن، می‌توان به طور همزمان به مصونیت از همبستگی و پیچیدگی خطی مطلوبی دست یافت.

هـ ـ معیار بهمنی:[2]

خاصیت بهمنی توابع، یکی از ویژگیهای مهمّی است که هنگام استفاده از این توابع در طراحی سیستمهای رمز بایستی مورد توجه قرار گیرد. تابع $f(x_1,\dots,x_N)$ را دارای خاصیت بهمنی مطلق نامند هر گاه در صورت مکمل شدن هر یک از بیتهای ورودیش (در حالیکه بقیهٔ بیتها ثابت است)، هر یک از بیتهای خروجی آن با احتمال $\frac{1}{2}$ تغییر کند.

اگر چه مباحث فراوانی در رابطه با خواص و نحوهٔ انتخاب توابعی که دارای خاصیت بهمنی مطلق هستند مطرح شده است، امّا به این دلیل که غالباً از توابع غیرخطی بدون حافظه با تعداد ورودیهای اندک در مولّدهای کلید اجرایی استفاده نمی‌شود از ذکر آنها خودداری می‌کنیم.

کاربرد دیگری که از مفهوم معیار بهمنی حاصل می‌شود آن است که مولّد کلید اجرایی را کلاً یک تابع غیرخطی عمل کننده بر روی کلید اصلی تلقّی نموده و معیار بهمنی را در این مورد به کارگیریم. از این دیدگاه بایستی به ازای مکمّل نمودن هر بیت کلید اصلی (در حالیکه بقیه بیتها ثابت است)، بیتهای کلید اجرایی با احتمال $\frac{1}{2}$ تغییر کنند. برای ارزیابی یک ساختار از نظر معیار بهمنی، ابتدا کلید خاصی برای مولّد در نظر گرفته و بیت jام کلید اجرایی را به دست می‌آوریم. سپس فقط بیت i ام کلید اصلی را تغییر داده، به ازای کلید جدید مجدّداً بیت j ام کلید اجرایی را به دست می‌آوریم. تفاوت این بیت با بیت j ام قبلی را با اضافه نمودن یک شمارنده (مثل m) نشان داده، این کار را به ازای کلیدهای اصلی فراوانی (مثلاً n بار) تکرار می‌کنیم. واضح است که احتمال تغییر بیت jام کلید اجرایی به ازای تغییر بیت iام کلید اصلی تقریباً برابر با $\frac{m}{n}$ است که هر چه این مقدار به $\frac{1}{2}$ نزدیک‌تر باشد مطلوبتر است. این روند بایستی به ازای i های مختلف و j های زیادی تکرار شده و از مجموع این نتایج، معیار بهمنی ساختار ارزیابی می‌گردد. در انتهای این بخش یادآور می‌شویم که معیارهای دیگری نیز جهت طراحی و ارزیابی مولّدهای کلید اجرایی مطرح شده‌اند [۱۱]، که از آن جمله، می‌توان پیچیدگی مرتبهٔ دو، پیچیدگی مرتبهٔ

1 - Trade Off

2- Avalanche Criterion

ماکزیمم، مصونیت در قبال "حملهٔ سیندروم خطی"[1]، مصونیت در قبال "حملهٔ سازگاری خطی"[2] و معیار غیرخطی کامل را نام برد. امّا به دلیل اهمیّت کم این معیارها از توضیح آنها صرف نظر نموده و جهت مقایسهٔ ساختارها از همان پنج معیار استفاده خواهیم نمود. البتّه چون مولّدهای واقعی عموماً ترکیبی از مولّدهای جزء و کوچک مورد بحث ما هستند و معیار بهمنی در ارتباط با کل ساختار مولّد به عنوان یک تابع عمل‌کننده بر روی کلید اصلی است، لذا معیار بهمنی را نیز ما در مقایسهٔ ساختارها به کار نگرفته‌ایم. امّا واضح است که جهت استفاده از هر مولّدی، پی بردن به این خاصیت مولّد نیز مهم و ضروری است.

۳- ارزیابی ساختارها و معرفی ساختاری بهینه:

چنانکه گفتیم همهٔ ساختارهای بدون حافظه در مقابل حملهٔ همبستگی ضعیف و قابل شکست می‌باشند. علاوه بر آن با پیاده‌سازی برخی از ساختارها مانند ضرب کننده، "سیستم جف"[3]، مالتی پلکسر و "ساختار مبتنی بر کوله‌پشتی"[4] مشاهده گردید [۱۱]، که غالب این ساختارها از نظر خواص آماری وضعیت مطلوبی نداشته و حتی دورهٔ تناوب و پیچیدگی خطی دنباله‌های خروجی آنها نیز ایده‌آل نیستند. بنابراین ساختارهای سادهٔ بودن حافظه جهت استفاده به عنوان مولّد کلید اجرایی مناسب نیستند.

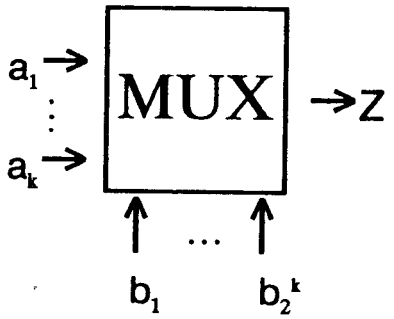
در میان ساختارهای حافظه‌دار پیشنهاد شده‌ای که مورد بررسی قرار گرفتند [۱۱] سه دستهٔ مهم و قابل توجه وجود دارند که عبارتند از: ساختارهای مبتنی بر JK-FF، ساختارهای مبتنی بر جمع‌کنندهٔ نقلی‌دار و ساختارهای مبتنی بر مالتی پلکسر. غالب ساختارهای JK-FF علیرغم داشتن دورهٔ تناوب، پیچیدگی خطی و خواص آماری نسبتاً مطلوب، در مقابل حملهٔ همبستگی بسیار ضعیف می‌باشند. با توجّه به حافظه‌دار بودن JK-FF، عدم کفایت شرط حافظه‌دار بودن را برای مصونیت در قبال حملهٔ همبستگی روشن می‌سازد.

ساختارهای مبتنی بر جمع‌کننده نقلی‌دار همهٔ معیارهای مذکور را به صورت مطلوبی برآورده می‌سازند. امّا مهمترین ضعف این ساختارها آن است که جهت دستیابی به دورهٔ تناوب و پیچیدگی خطی بالا در این سیستمها باید از سری کردن ساختار سادهٔ جمع‌کنندهٔ سه بیتی استفاده کرد. امّا به دلیل شرکت بیت نقلی هر جمع در جمع بعدی، تأخیر زمانی سیستم بسیار بوده و در نتیجه سرعت تولید بیت‌ها در این ساختار بسیار کم است به گونه‌ای که عملاً استفاده از آن با مشکلات فراوانی توأم است [۱۱].

بر خلاف دو نوع ساختار فوق، مالتی پلکسر یک مدار ترکیبی بدون حافظه است که ویژگیهای چندان مطلوبی را نیز از خود نشان نمی‌دهد. امّا چنانکه خواهیم دید با استفاده از شیوه‌یی مناسب می‌توان ضعفهای آن را برطرف نموده و به یک ساختار مطلوب دست یافت. لذا جهت نیل به یک ساختار بهینه، سیستمهای مبتنی بر مالتی پلکسر را بطور نسبتاً مشروح بررسی خواهیم نمود.

شکل (۲) فرم‌کلی یک ساختار بدون حافظهٔ مبتنی بر مالتی پلکسر را نشان می‌دهد در این ساختار می‌توان دنباله‌های a_i و b_i را توسط ثبّاتهای تغییر مکان بازخوردی خطی تولید

1 - Linear Syndrome Attack
2- Attack Based On Linear Consistency Test (LCT)
3- Geffe
Knapsack



شکل (۲): فرم کلی ساختار مالتی پلکسر

نمود. به عنوان مثال هر گاه همهٔ a_iها از طبقات مختلف ثبّاتهای تغییر مکان بازخوردی خطی به طول L_1و همهٔ b_j ها توسط ثبّاتهای تغییر مکان بازخوردی خطی به طول L_2 تأمین گردد، به شرط برقراری رابطهٔ $\gcd(L_1, L_2)$ ، داریم [۲]:

$$\begin{cases} T = (2^{L_1}-1)(2^{L_2}-1) \\ L(\tilde{Z}) \le L_2 \left[1 + \sum_{i=1}^{K} \binom{L_1}{i} \right] \end{cases} \qquad (۱۳)$$

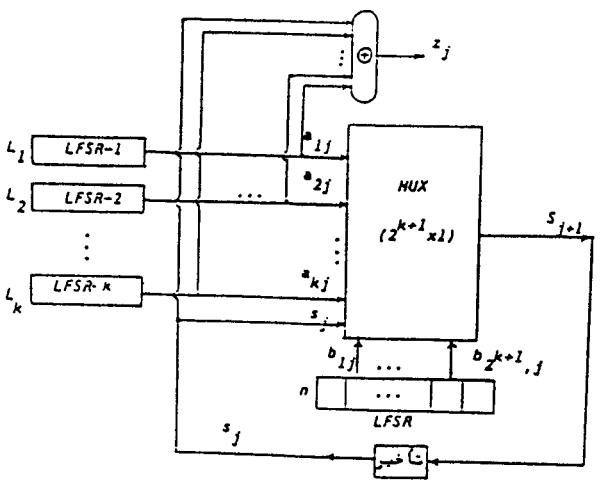
همچنین اگر a_iها توسط ثبّاتهای تغییر مکان بازخوردی خطی مختلفی با طولهای $L_1,...,L_k$ تولید شوند در حالیکه b_iها همچنان از یک ثبّاتهای تغییر مکان بازخوردی خطی به طول n گرفته شوند داریم [۷]:

$$\begin{cases} T = (2^n-1)\prod_{i=1}^{K}(2^{L_i}-1) \\ L(\tilde{Z}) = n\prod_{i=1}^{K}(L_i+1) \end{cases} \qquad (۱۴)$$

چنانکه مشاهده می‌شود پیچیدگی خطی ساختار با دورهٔ تناوب آن فاصلهٔ زیادی دارد. علاوه بر آن به علت تطابق خروجی مالتی پلکسر با ورودیهای b_i با احتمال بیشتر از $\frac{1}{2}$، حمله همبستگی به ساختار به ویژه جهت دستیابی به حالت اولیه و چند جمله‌یی ثبّاتهای تغییر مکان بازخوردی خطی مربوط به b_iها امکانپذیر است [۸]. شبیه‌سازی ساختارهای مذکور نیز نشان می‌دهد که هیچیک، از خواص آماری مطلوبی برخوردار نیستند[۱۱].

اخیراً جهت رفع ضعف ساختار در زمینه مصونیت از همبستگی، پیشنهاد شده است که خروجی مالتی پلکسر با تأخیر به عنوان یکی از ورودیهای آدرس‌دهندهٔ آن قرار گرفته و خروجی نهائی با XOR این ورودیها تولید گردد [۹]. شکل (۳) این ساختار راکه موسوم به "ساختار منطقی جامع"[1] است نشان می‌دهد. در حقیقت طراحان این ساختار بر آن بوده‌اند که جهت قوّت بخشیدن ساختار در قبال حملهٔ همبستگی از روابط (۱۲ـالف) و (۱۲ـب) استفاده نمایند.

ثابت شده است [۹]که دورهٔ تناوب این ساختار به شرط



شکل (۳): ساختار منطقی جامع

اول بودن طول ثبّاتهای تغییر مکان بازخوردی خطی نسبت به یکدیگر، برابر است با:

$$T = (2^n-1)\prod_{i=1}^{K}(2^{L_i}-1) \qquad (۱۵)$$

1 - Universal Logic

همچنین می‌توان ثابت نمود [۱۱] که پیچیدگی خطی ساختار بسیار نزدیک به دورهٔ تناوب آن است. به دلیل اهمیّت این ساختار و استفاده از آن در ارائه ساختار بهینه، اثبات مذکور را که مبتنی بر روش جبری است بطور مختصر بیان می‌کنیم [۹].

فرض کنید در شکل (۳) K=۱ باشد. در این صورت تنها دو ثبات تغییر مکان بازخوردی خطی در سیستم وجود دارد که یکی از آنها در قسمت اطلاعات و دیگری در قسمت آدرس دهندهٔ مالتی پلکسر است. واضح است که در این حالت مالتی پلکسر به کار رفته ۱×۴ خواهد بود. حال اگر طول ثباتهای تغییر مکان بازخوردی خطی به کار رفته برابر با n و L_1 بوده و نسبت به هم اول باشند داریم:

$$\begin{cases} Z_j = a_j + S_j \\ S_j = b_j(a_j+1)(S_{j-1}+1) + b_{j-1}(a_j+1)S_{j-1} + \\ b_{j-2}a_j(S_{j-1}+1) + b_{j-3}a_jS_{j-1} \end{cases} \quad (۱۶)$$

حال فرض کنید حافظهٔ محدود ساختار (m) صفر باشد که در اینصورت خروجی یا حالت جدید تنها به خروجی یا حالت همان لحظه وابسته خواهد بود. در نتیجه داریم:

$$Z_j = a_j + b_j + a_jb_j \Rightarrow L^{(0)}(\tilde{Z}) = L_1n + L_1 + n \quad (۱۷)$$

که در آن منظور از $L^{(0)}(\tilde{Z})$ پیچیدگی خطی ساختار به ازاء حافظهٔ محدود صفر است. اما اگر m=۱ باشد داریم:

$$\begin{aligned} Z_j = {} & a_j + a_jb_j(a_{j-1}b_{j-1} + b_{j-1}) + a_jb_j + \\ & b_j(a_{j-1}b_{j-1} + b_{j-1}) + a_jb_{j-1}(a_{j-1}b_{j-1} + b_{j-1}) + \\ & b_{j-1}(a_{j-1}b_{j-1} + b_{j-1}) \end{aligned} \quad (۱۸)$$

حال به عنوان نمونه جملهٔ $a_jb_ja_{j-1}b_{j-1}$ را در نظر بگیرید. با توجه به مباحث بخش (۲ـب)، اگر β و α به ترتیب ریشه‌های چندجمله‌ییهای مربوط به ثباتهای تغییر مکان بازخوردی خطی بطول L_1 و n باشند $\alpha^{e_1}\beta^{e_2}$ ریشهٔ چندجمله‌یی مولّد دنبالهٔ $a_jb_ja_{j-1}b_{j-1}$ خواهد بود به شرط آنکه e_2 و e_1 هر یک حداکثر دارای دو بیت یک در نمایش باینری خود باشند (یعنی وزن هامینگ آنها $W(e_1)$ و $W(e_2)$ حداکثر دو باشد). حال با در نظر گرفتن همهٔ جملات رابطهٔ (۱۸) و حذف شرطهای مشترک روی e_2 و e_1 تنها سه شرط مجزای زیر باقی خواهند ماند که با توجه به قاعدهٔ (۱) مذکور در بخش (۲) داریم:

$$\begin{cases} W(e_1)=1 & \Rightarrow \quad L_1 \\ W(e_1)\le 2\ ,\ W(e_2)\le 2 & \Rightarrow \quad \left[L_1+\binom{L_1}{2}\right]\left[n+\binom{n}{2}\right] \\ W(e_2)=2 & \Rightarrow \quad n+\binom{n}{2} \end{cases} \quad (۱۹)$$

در نتیجه با جمع مقادیر اخیر و صرف نظر از مقدار L_1 داریم:

$$L^{(1)}(\tilde{Z}) \le \left[1+L_1+\binom{L_1}{2}\right]\left[n+\binom{n}{2}\right] \quad (۲۰)$$

به همین ترتیب با افزایش m می‌توان رابطهٔ کلی زیر را به دست آورد:

$$L^{(m)}(\tilde{Z}) \le \left[\sum_{i=0}^{m+1}\binom{L_1}{i}\right]\left[\sum_{j=1}^{m+1}\binom{n}{j}\right] \quad (۲۱)$$

اما اصولاً ساختارهای حافظه‌دار دارای حافظهٔ محدود ثابت و کوچکی نیستند و لذا می‌توان فرض نمود که مقدار m از L_1 و n بیشتر است. با این فرض داریم:

$$L(\tilde{Z}) \le 2^{L_1}(2^n-1) \quad ,$$
$$m \ge \max\{L_1, n\} \quad (۲۲)$$

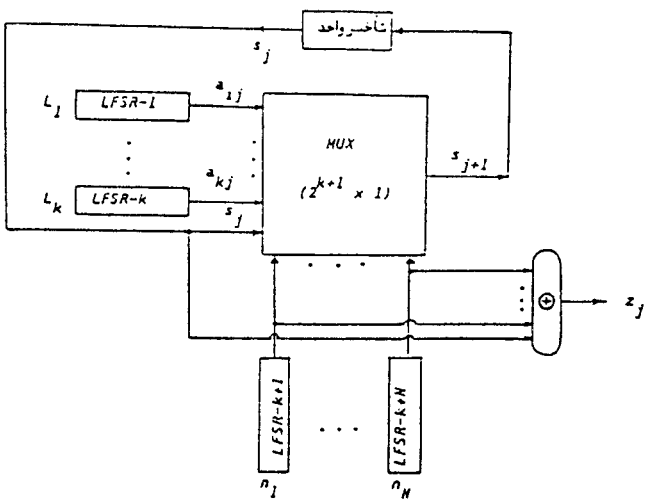
به دلیل استفاده از رابطهٔ (۷) در اثبات این نامساوی و به دلیل احتمال بسیار زیاد برقراری تساوی در آن رابطه، در نامساوی فوق $L(\tilde{Z})$ به باند بالائی خود بسیار نزدیک خواهد بود. البته به دلیل بزرگتر بودن این باند بالائی از دورهٔ تناوب،

مسلماً $L(\tilde{Z})$ به دورهٔ تناوب ساختار محدود شده و رابطهٔ (۲۲) نتیجهٔ جدیدی را از نظر باند بالائی پیچیدگی خطی در بر نخواهد داشت. امّا مهمترین نتیجهٔ بحث فوق همان اثبات نزدیکی بسیار زیاد $L(\tilde{Z})$ به این باند بالائی است که توسط شبیه‌سازی نیز این مطلب تأئید شده است [۱] و در جدول (۱) نمونه‌ای از آن دیده می‌شود (در این آزمایش $T=(2^{3}-1)(2^{4}-1)=105$ بوده است).

علیرغم دورهٔ تناوب، پیچیدگی خطی و خوّاص آماری مطلوب ساختار منطقی جامع [۱۱] به نظر می‌رسد عامل مهمی که انگیزهٔ طراحان این ساختار بوده است به صورت مطلوب بر آورده نشده است زیرا چنانکه قبلاً اشاره شد حملهٔ همبستگی به ساختار مالتی پلکسر از روزنهٔ ثبّاتهای تغییر مکان بازخوردی خطی مربوط به خطوط اطلاعاتی مالتی پلکسر امکانپذیر است و ساختار مذکور هیچگونه مصونیتی در قبال این حمله ایجاد نکرده است.

جهت رفع این عیب، راه حلی که به نظر می‌رسد استفاده از چند ثبّاتهای تغییر مکان بازخوردی خطی برای تأمین خطوط اطلاعاتی مالتی‌پلکسر، وارد کردن خط تأخیر یافته به عنوان یکی از خطوط اطلاعاتی (به جای استفاده به عنوان یک خط آدرس) و تولید خروجی نهائی توسط XOR نمودن این ورودیهای اطلاعاتی است. اما علیرغم بهبود مصونیت از همبستگی ساختار در این حالت می‌توان نشان داد که پیچیدگی خطی ساختار به شدّت کاهش می‌یابد [۱۱]. راه حل دیگری که مناسب به نظر می‌رسد آن است که مانند ساختار منطقی جامع، خط تأخیر یافته به قسمت آدرس‌دهنده وارد شود اما جهت تأمین خطوط اطلاعاتی از چند ثبّاتهای تغییر مکان بازخوردی خطی استفاده شده و خروجی نهائی از XOR نمودن این خطوط همراه با خط تأخیر یافته تأمین شود.

شکل (۴) این ساختار اصلاح شده را نشان می‌دهد. بطور مشابه با استدلال مربوط به ساختار منطقی جامع می‌توان نشان داد که دورهٔ تناوب ساختار به شرط تباین طول ثبّاتهای تغییر مکان بازخوردی خطی نسبت به یکدیگر، برابر با حاصلضرب دورهٔ تناوبهای همهٔ ثبّاتهای تغییر مکان بازخوردی خطی بوده و پیچیدگی خطی ساختار بسیار نزدیک به آن است [۱۱]. جدول (۱) نتایج شبیه‌سازی این ساختار را در کنار ساختار منطقی جامع نشان می‌دهد.



شکل (۴) ساختار اصلاح‌شده منطقی جامع

ساختار اصلاح شده منطقی جامع	ساختار منطقی جامع
$K=1,n_1=3,n_2=4$	$K=1,L_1=3,n_1=4$
۱۰۵	۱۰۳
۱۰۵	۱۰۵
۱۰۵	۱۰۳
۱۰۲	۹۷

خواص آماری ساختار اخیر نیز چنانکه در جدول (۲) دیده می‌شود بسیار مطلوب و مناسب است. در نتیجه می‌توان این ساختار را یک ساختار بسیار قوی جهت تولید کلید

اجرائی قلمداد نمود که علاوه بر دارا بودن ویژگیهای مطلوب مربوط به امنیت، نقطهٔ قوّت آن در مقایسه با ساختارهای مطلوب دیگری مانند سیستمهای مبتنی بر جمع‌کننده، سرعت بسیار زیاد آن است.

جدول (۲): خواص آماری ساختار اصلاح‌شده منطقی جامع

۹۴/۰۰: آزمون فرکانس

۸۴/۰۰: آزمون رنها

۹۴/۶۶: آزمون سریال

۱۰۰/۰۰: آزمون خودهمبستگی

۸۸/۰۰: آزمون پوکر

۸۹/۶۶: آزمون مشتقات باینری

۹۳/۳۳: آزمون LCP

۴ـ نتیجه:

جهت طراحی و ارزیابی رمزکننده‌های پی در پی با استفاده از روش تئوری سیستمی، مشخص نمودن معیارهای مقایسهٔ سیستمها از اهمیت خاصی برخوردار است. در این نوشتار پنج معیار دورهٔ تناوب، پیچیدگی خطی، مصونیت از همبستگی، خواص آماری و معیار بهمنی به عنوان مهمترین معیارها مورد بحث قرار گرفته و روش بررسی این معیارها در یک ساختار معین نیز مورد توجه قرار گرفت.

پس از آن با معرفی چند نوع مختلف از ساختارهای مولّد کلید اجرائی حافظه‌دار، معیارهای مذکور (به جز معیار بهمنی) را در مورد ساختارهای مبتنی بر مالتی‌پلکسر به کار گرفته و بویژه با اثبات پیچیدگی خطی مربوط به ساختار منطقی جامع نشان دادیم که این ساختار از ویژگیهای مطلوبی برخوردار است، اما برای قوّت بخشیدن به این ساختار در قبال حملهٔ همبستگی ساختاری پیشنهاد نمودیم که همهٔ ویژگیهای مورد نظر را داراست و بنابراین می‌توان آن را به عنوان یک مولد کلید اجرائی خوب و یا جزئی از یک ساختار پیچیده‌تر مورد استفاده قرار داد.

لازم به ذکر است که جهت طراحی یک رمزکنندهٔ قوی و قابل استفاده، بایستی مسائل جنبی دیگری مانند مدیریت کلید، سرعت سیستم و کدینگ منبع را نیز مورد توجه قرار داد که پرداختن به آنها از حوصلهٔ این نوشتار خارج است.

فهرست منابع

1- Rueppel. R. A; "Good Stream Ciphers are Hard to Design", ICCST, Zurich, Switzerland, 163-174, 1989.

2- Beker. H, Piper, F; Cipher systems: the protection of Communication ; Northwood Books, London, 1982.

3-Rueppel. R.A; Analysis and Design of Stream Ciphers; Springer - Verlag, 1986.

4- Golic, "On the Linear Complexity of Functions of Periodic GF(q) Sequence", IEEE Trans. Information Theory, Vol. 35, No.1, 69 - 75, Jan. 1989.

5- Siegnthaler. T, "Decrypting a Class of Stream Ciphers Using Ciphertext Only Attack", IEEE Trans. Computers, Vol. 34,No.1,81-85, Jan. 1985.

6- Siegenthaler. T,"Cryptanalysis Representation of Nonlinearly Filtered ML-Sequences", Springer - Verlag, Advances in Cryptology, Eurocrypt' 85,103-110, 1985.

7- Mu-Lan Liu, Zhe-Xian Wan, "Generalized Multiplexed Sequences", Springer-Verlag, Advances in Cryptology, Eurocrypt' 85, 135-141, 1985.

8- Mund.S, Gollman. D,Beth. T, "Some Remarks On the Cross - Correlation Analysis of Pseudo Random Generators", Springer - Verlag, Advances in Cryptology, Eurocrypt' 87,25-36, 1987.

9- Ed Dawson, Goldburg. B,"Universal Logic Sequences", Springer - Verlag, Advances in Cryptology, Auscrypt' 90, 426-632, 1990.

10- Golomb,S.; Shift Register Sequences; Holden - Day, 1967.

۱۱ـ مدّرس هاشمی، محمود، "طراحی رمزکننده‌های پی‌درپی"، پایان نامهٔ کارشناسی ارشد، دانشگاه صنعتی اصفهان، ۱۳۷۰