تحلیل همبستگی دنباله خروجی مولدهای پرشی در رمزهای جریانی

حامد مؤمنی[۱]، کارشناس ارشد؛ محمدعلی طاهری[۲]، کارشناس ارشد؛ عبدالرسول میر قدری[۳]، دانشیار

۱- مرکز تحقیقات صدر - تهران - ایران - h.momeni87@gmail.com
۲- مرکز تحقیقات صدر - تهران - ایران taheri.nodh@gmail.com
۳- دانشکده فناوری اطلاعات و ارتباطات – دانشگاه جامع امام حسین (ع) - تهران - ایران – amrghdri@ihu.ac.ir

چکیده: یکی از روش‌های طراحی رمزهای جریانی مبتنی بر LFSR ها، استفاده از روش کلاک نامنظم است کـه از معـروف‌تـرین سـاختارهای آن، ساختار انقباضی است. در سال‌های اخیر روشی به نام کنترل کلاک پرشی مطرح شد که باعث بهبود کارایی در مقایسه با مولدهای انقباضی گشـته است. در این روش به‌جای اینکه چندین کلاک زده شده و مقادیر تغییر یابند، درواقع از روی حالت‌های میانی عبور می‌شود. به‌ازای هر چندجمله‌ای اولیه، یک‌میزان پرش ثابت وجود دارد که شاخص پرش نام دارد. بدیهی است که به‌ازای طول هر LFSR، چندجمله‌ای‌های اولیه متعددی وجود دارد که دوره تناوب یکسان دارند، اما اندازه شاخص پرش آن‌ها متفاوت است. در این مقاله با تحلیل حمله همبستگی روی مولدهای پرشی، ایـن نتیجـه حاصل شد که انتخاب چندجمله‌ای با حداکثر شاخص پرش، موجب حداقل همبستگی بین دنباله خروجی و ورودی مولد می‌گردد. لـذا در طراحـی رمزهای جریانی با ساختار مولدهای پرشی، از دیدگاه حملات همبستگی، اولویت با انتخاب چندجمله‌ای‌هایی با حداکثر میزان شاخص پرش است.

واژه‌های کلیدی: مولدهای پرشی، شاخص پرش، حمله همبستگی، مولدهای انقباضی، رمز جریانی.

Correlation Analysis of Output Streams Jump Generators in Stream Ciphers

H. Momeni, MSc[1]; M.A. Taheri, MSc[2]; A.R. Mirghadri, Associate Professor[3]

1- Sadr Researcher Center, Tehran, Iran, Email: h.momeni87@gmail.com
2- Sadr Researcher Center, Tehran, Iran, Email: taheri.nodh@gmail.com
3- Faculty of Information and Communication Technology, Imam Hussein University, Tehran, Iran, amrghdri@ihu.ac.ir

Abstract: One method of design the LFSR-based stream ciphers is using irregular clock that it is most famous structures. In recent years became a springboard technique called clock control that improves efficiency compared to generators has become tighter. In this way, instead of several clock has been changed and values, in the state through the middle. Per basic polynomials, a jump in the index jump is still there. It is clear that for the length of each LFSR, there are several initial polynomials that same period, but the size of the jump index is different. In this paper, by analyzing the correlation attack on generators springboard, it was concluded that the selection of index jump polynomials with maximum results in minimum correlation between output and input sequence is productive. So in the design of stream ciphers with a springboard generation structure, in terms of correlation attacks, the polynomial with most rate of jump up the index is priority.

Keywords: Jump Generator, Jump Index, Correlation Attack, Stream Cipher, Shrink Generator.

تاریخ ارسال مقاله: ۱۳۹۶/۰۴/۰۳
تاریخ اصلاح مقاله: ۱۳۹۶/۰۶/۲۶ و ۱۳۹۶/۰۷/۲۳
تاریخ پذیرش مقاله: ۱۳۹۶/۰۸/۱۸
نام نویسنده مسئول: عبدالرسول میر قدری
نشانی نویسنده مسئول: ایران – تهران – بزرگراه شهید بابایی – دانشگاه جامع امام حسین (ع).

۱ -مقدمه

یکی از عناصر سازنده رمزهای جریانی، ثبات‌های انتقال با پس‌خورد خطی[۱] هستند که کاربرد وسیعی در مولدهای اعداد تصادفی دارند. دنباله‌های تولیدشده توسط LFSR ها دارای دوره تناوب بزرگ و ویژگی‌های آماری مطلوبی هستند؛ اما ازلحاظ ذاتی خطی هستند که این ضعف، موجب آسیب‌پذیری آن‌ها در مقابل حملاتی نظیر حمله همبستگی[۲] و جبری[۳] می‌گردد. به همین دلیل LFSR ها را به‌تنهایی در مولدهای رشته‌کلید به کار نمی‌برند [۱].

به‌طورمعمول رمزهای جریانی مبتنی بر LFSR به سه دسته مولدهای ترکیبی غیرخطی[۴]، مولدهای فیلتر غیرخطی[۵] و مولدهای کلاک کنترل‌شده[۶] تقسیم می‌شوند. هرکدام از این سه دسته، دارای مزایا و معایبی هستند که در این مقاله تمرکز بر روی دسته سوم یا روش کنترل کلاک قرار می‌گیرد. رمزهای کلاک کنترل‌شده که به آن‌ها کلاک نامنظم نیز گفته می‌شود، خود انواع گوناگونی دارند که از آن‌ها می‌توان مولدهای افت‌وخیز[۷] [۲]، مولدهای گام متغیر[۸] [۳] و مولدهای انقباضی[۹] [۴] را نام برد. مهم‌ترین مزیت مولدهای انقباضی نسبت به دو مولد دیگر، سخت‌تر بودن اعمال حمله همبستگی است.

با توجه به ساختار مولدهای انقباضی، نرخ تولید رشته‌کلید متغیر بوده که در مقابل حملات کانال جانبی[۱۰]، آسیب‌پذیر خواهند بود [۵]. جهت رفع برخی از مشکلات مولدهای انقباضی نظیر کارایی پایین و آسیب‌پذیری در مقابل حملات کانال جانبی، روش پرشی در طراحی رمزهای جریانی مطرح شد[۶]. این روش نیز به دنبال برهم زدن کلاک‌های خروجی مولد بوده، ولی کارایی و نسبت تولید رشته‌کلید خروجی آن در مقایسه با مولدهای انقباضی بسیار مطلوب‌تر است. برای مثال الگوریتم‌های رمز جریانی نظیر Pomaranch [۷] و Mickey [۸] با استفاده از مولدهای پرشی طراحی شده‌اند.

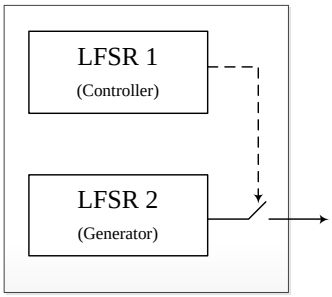
در این مقاله، وضعیت همبستگی دنباله خروجی برای مولدهای پرشی بررسی می‌گردد. همچنین، تأثیر اندازه شاخص پرش[۱۱] بر روی همبستگی و اریبی خروجی متناظر نیز مورد ارزیابی قرار می‌گیرد.

با توجه به مطالب بیان‌شده، ساختار بقیه مقاله به شرح زیر است. در بخش دوم مولدهای انقباضی معرفی می‌گردد. همچنین در بخش سوم مولدهای پرشی بیان می‌شود. بخش چهارم به بررسی همبستگی دنباله خروجی در مولدهای پرشی و نقش شاخص پرش، اختصاص دارد. بخش پایانی نیز نتیجه‌گیری را در بر می‌گیرد.

۲ -مولدهای انقباضی

LFSR ها در کنار ویژگی‌های مطلوب رمزنگاری خود، یک ضعف بسیار مهم دارند و آن اینکه کاملاً خطی هستند. به خاطر این ویژگی ذاتی، در مقابل حملات همبستگی و جبری ضعیف می‌باشند [۹]. از طرفی این ضعف موجب می‌شود تا با در اختیار داشتن بیت‌های دنباله خروجی به‌اندازه تنها ۲ برابر طول LFSR، به‌راحتی و با استفاده از الگوریتم برکلمب- مسی[۱۲] [۱۰]، ساختار تابع بازخورد آن‌ها استخراج شود. به همین دلیل معمولاً LFSR ها را به‌طور مستقیم در مولدهای رشته‌کلید به کار نمی‌برند؛ لذا یکی از روش‌های بهبود ویژگی غیرخطی[۱۳] دنباله خروجی الگوریتم رمز جریانی، استفاده از روش کنترل کلاک است.

همان‌طور که بیان شد مولدهای انقباضی گونه‌ای از رمزهای کلاک کنترل‌شده هستند. در این روش مطابق شکل (۱) از دو LFSR استفاده می‌شود. LFSR1 وظیفه کنترل دنباله خروجی LFSR2 را بر عهده دارد. به این صورت که هرگاه بیت iام دنباله خروجی LFSR1 برابر یک باشد، بیت iام دنباله خروجی LFSR2 به‌عنوان بخشی از خروجی مولد انقباضی ثبت می‌گردد. درصورتی‌که بیت iام دنباله خروجی LFSR1 برابر صفر باشد، آنگاه بیت خروجی متناظر LFSR2 (فارغ از صفر یا یک بودن) حذف می‌گردد. درواقع ساختار انقباضی تنها به‌ازای کلاک‌هایی که بیت خروجی LFSR1 برابر یک باشد، خروجی خواهد داشت [۱۱].



شکل ۱: ساختار کلی مولدهای انقباضی

دنباله خروجی چنین ساختاری علاوه بر دوره تناوب بزرگ و ویژگی‌های آماری مطلوب، پیچیدگی خطی بالایی را نیز تأمین خواهد کرد [۱۲].

۳ -مولدهای پرشی

یکی از ضعف‌های مولد انقباضی نرخ تولید پایین رشته‌کلید است؛ یعنی به‌ازای هر n کلاک، m دنباله خروجی تولید می‌شود که $m \leq n$. در حقیقت وزن همینگ[۱۴] دنباله خروجی LFSR کنترلی برابر تعداد دنباله خروجی کل ساختار انقباضی خواهد بود. این ضعف موجب کاهش کارایی می‌گردد.

در رمزشکنی نظری تنها الگوریتم رمز مورد تجزیه و تحلیل قرار می‌گیرد که تحلیل‌های خطی و تفاضلی ازجمله معروف‌ترین مثال‌های آن هستند [۱۳]. نوع دیگری از حملات به‌گونه‌ای کاملاً متفاوت از دسته اول، سیستم رمز را موردتهاجم قرار می‌دهند. هنگامی‌که سخت‌افزار در حال پردازش و رمزکردن اطلاعات است، می‌توان با استفاده از اطلاعاتی نظیر توان مصرفی سخت‌افزار، تشعشات الکترومغناطیس و یا زمان اجرای الگوریتم و با کمک تحلیل‌های آماری و سایر فن‌های رمزشکنی، کلید رمزنگاری را به‌دست آورد. به این دسته

از حملات که از اطلاعات جانبی برای حمله بهره می‌برند، حملات کانال جانبی اطلاق می‌گردد [۱۵-۱۴].

با توجه به اینکه تعداد کلاک‌ها ارتباط مستقیمی با توان مصرفی پردازنده الگوریتم رمز دارند؛ لذا به‌راحتی می‌توان از روی رفتار نمونه‌های توان به اطلاعات پردازشی مولدهای انقباضی دست‌یافت. همچنین زمان مصرفی برای تولید یک بیت در خروجی نیز بسیار حائز اهمیت است؛ چراکه زمان موردنیاز برای تولید یک بیت با تعداد صفرهای متوالی در دنباله کنترلی متناسب است؛ بنابراین ضعف بسیار مهم دیگر مولدهای کلاک نامنظم، آسیب‌پذیری بسیار زیاد آن‌ها در مقابل حملات تحلیل توان[۱۵] و تحلیل زمان[۱۶] است که از مهم‌ترین حملات کانال جانبی محسوب می‌شوند [۱۱].

همان‌طور که گفته شد در مرجع [۶]، یک روش کارآمد و مؤثر برای برداشتن چندین گام (معادل چند کلاک LFSR) معرفی شد. در این روش با استفاده از فن پرش درواقع از روی حالت‌های میانی عبور می‌شود. با بهره‌گیری از LFSR های پرشی به‌جای LFSR های سنتی، علاوه بر مقابله با حملات کانال جانبی، می‌توان تمام مزایای حالت کلاک نامنظم را حفظ کرد؛ چراکه به‌ازای هر کلاک، خروجی داشته و از روی توان یا زمان مصرفی نمی‌توان به اطلاعات مفیدی دست یافت. در ضمن مشکل نرخ پایین تولید رشته‌کلید نیز با این فن مرتفع می‌گردد [۷].

اگر A به‌عنوان ماتریس انتقال و $f(x)$ به‌عنوان چندجمله‌ای مشخصه یک LFSM [۱۷] در نظر گرفته شود که مطابق رابطه (۱)، لزوماً یک ثبات انتقال نیست.

$$f \qquad (۱)$$

آنگاه تغییر ماتریس انتقال یک LFSR از A به $A+I$ با پریدن به J گام بعدی بردار حالت اصلی، معادل است که صرف‌نظر از مقدار اولیه انجام می‌شود. به J شاخص پرش گفته می‌شود.

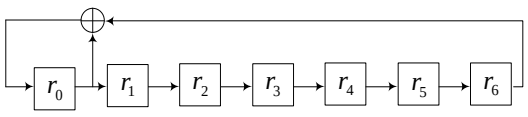
بنابراین دو فرآیند زیر معادل یکدیگر خواهند بود:

- گام برداشتن (کلاک) LFSR برای J مرتبه
- گام برداشتن LFSR برای یک مرتبه و سپس xor شدن با حالت اصلی (حالت قبل کلاک)[۱۶].

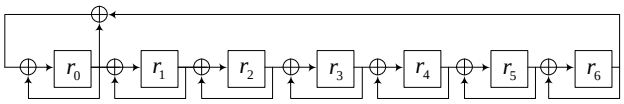
برای مثال در شکل (۲) یک LFSR با چندجمله‌ای بازخورد اولیه رابطه (۲) وجود دارد که به‌صورت عادی کلاک می‌خورد.

$$f \qquad (۲)$$

در شکل (۳) همان LFSR وجود دارد که کلاک آن به‌صورت پرشی است و پیاده‌سازی آن معادل یک کلاک عادی و xor تمام مقادیر با حالت اصلی است.



شکل ۲: یک LFSR با کلاک عادی [۱۶]



شکل ۳: یک LFSR با کلاک پرشی [۱۶]

شاخص پرش برای چندجمله‌ای بازخورد مذکور برابر ۱۲۱ است و بنابراین در شکل (۳) در هر کلاک بدون محاسبه مقادیر میانی، پرشی به طول ۱۲۱ واحد صورت می‌گیرد.

به همین دلیل علاوه بر دوره تناوب، شاخص پرش نیز یک پارامتر مهم برای چندجمله‌ای‌های تحویل‌ناپذیر محسوب می‌گردد. شاخص پرش برای چندجمله‌ای اولیه $f(x)$ از درجه n، همیشه وجود دارد و اندازه بیشینه و کمینه آن نیز دارای رابطه (۳) است.

$$deg\ \mathrm{f(x)} \ \le\ \mathrm{J} \ \le\ 1 + per\ \mathrm{f(x)} - deg\ \mathrm{f(x)} \qquad (۳)$$

$per\ \mathbf{f(x)}$: دوره تناوب LFSR متناظر

$deg\ \mathbf{f(x)}$: درجه چندجمله‌ای

در مورد پیاده‌سازی روش پرشی نیز باید گفت، با جمع‌کردن عدد یک به ورودی قطر اصلی ماتریس انتقال، یک تعداد از انتقال‌های چندتایی به‌دست می‌آید که معادل شاخص پرش چندجمله‌ای مشخصه است.

اصلاح ماتریس انتقال، پیچیدگی بسیار پایینی دارد، بدین‌صورت که برای همه سلول‌های LFSR تنها با یک xor جمع می‌شوند [۱۷]. البته لازم به ذکر است محاسبه شاخص پرش به‌سختی حل مسئله لگاریتم گسسته ارتباط دارد و در عمل این کمیت برای چندجمله‌ای‌ها تا درجه محدودی، قابل‌محاسبه است [۱۸].

۴ -بررسی همبستگی مولدهای پرشی

حمله همبستگی یکی از مهم‌ترین حملات علیه رمزهای متقارن بوده که بر روی رمزهای جریانی توسط سیگنتالر[۱۸] در سال ۱۹۸۵ ارائه شده است [۱۹]. هدف حمله همبستگی، بازیابی حالت های اولیه LFSR است. بیان می‌شود دو دنباله z و a همبستگی دارند، هرگاه رابطه (۴) برقرار باشد.

$$\Pr(z_i = a_i) \neq 0.5 \qquad (۴)$$

اگر چنین همبستگی‌ای وجود داشته باشد، بازیابی حالت‌های داخلی سامانه امکان‌پذیر خواهد بود.

ازآنجایی‌که مولدهای پرشی ازلحاظ ساختاری شباهت زیادی با مولدهای انقباضی دارند، لذا تحلیل همبستگی مولدهای پرشی نیز مطابق تحلیل همبستگی صورت‌گرفته بر روی مولدهای انقباضی است [۱۱]. همانند ساختار مولدهای انقباضی در مولدهای پرشی نیز یک LFSR با چندجمله‌ای اولیه وجود دارد که یک بیت آن نقش دنباله کنترلی یا رابطه (۵) را بازی می‌کند.

$$C = (c_i)_{i\in \mathrm{N}} \quad (۵)$$

جهت تحلیل همبستگی برای هر یک از بخش‌های مولدهای انقباضی، نمادگذاری زیر در نظر گرفته شده است:

- $C = (c_i)_{i\in \mathrm{N}}$: دنباله کنترلی ($\mathrm{LFSR}_1$)
- $X = (x_i)_{i\in \mathrm{N}}$: دنباله مولد ($\mathrm{LFSR}_2$)
- $Y = (y_i)_{i\in \mathrm{N}}$: دنباله خروجی ساختار کلی (مولد انقباضی)
- X^n: زیر دنباله n بیتی ابتدایی
- x_m^n: زیر دنباله $n-m+1$ بیتی برای $x_m,\cdots,x_n$
- $w(\mathrm{C}^i)$: وزن همینگ i بیت ابتدائی دنباله کنترلی

تعریف: دنباله $x_1,\cdots,x_n$ را متغیرهای تصادفی مستقل با توزیع یکنواخت روی $\mathrm{F_q}$ در نظر گرفته و آن را به‌اختصار با iid[۱۹] نشان می‌دهند.

برای اعمال یک حمله همبستگی در مقابل دنباله مولد، مهاجم باید احتمال رابطه (۶) را حساب کند.

$$\hat{p}_i = \Pr(x_i = 1 | Y^n) \quad (۶)$$

در این مدل، دنباله مولد و دنباله کنترلی با iid جایگزین می‌شوند. احتمال رخداد متغیرهای تصادفی با رابطه (۷) بیان می‌گردد و همچنین دنباله خروجی نیز یک دنباله iid است.

$$\Pr(x_i = 1) = \Pr(c_i = 1) = \frac{1}{2} \quad (۷)$$

همان‌طور که بیان شد مهم‌ترین تفاوت بین مولدهای پرشی و انقباضی استفاده از فن پرشی در نامنظم سازی کلاک است؛ بنابراین به‌جای اینکه برای $c_i = 1$ خروجی i ام دنباله مولد (LFSR2) حذف شود، به‌اندازه jump-1 خروجی از مولد LFSR2 حذف شده و دنباله بعدی ثبت می‌گردد. پس می‌توان روابط (۸) را نوشت.

$$\begin{aligned} &c_i = 0 \quad \Rightarrow \quad clock = Jump \quad \Rightarrow \\ &\quad \begin{cases} x_i,\cdots,x_{i+jump-1} : delete, \\ x_{i+jump} : save \end{cases} \\ &c_i = 1 \quad \Rightarrow \quad clock = Normal \quad \Rightarrow \quad x_i : save \end{aligned} \quad (۸)$$

درنتیجه در محاسبه احتمالات مربوط به همبستگی، می‌توان به‌جای $c_i = 0$ عبارت $0,\cdots,0,1$ ($jump-1$) را جایگزین کرد. در واقع این حالت معادل مولد ساختار انقباضی است که به‌جای حذف یک بیت در شرایط $c_i = 0$، به تعداد jump مرتبه کلاک خورده و فقط خروجی کلاک آخر مولد (LFSR2) ثبت شده و مابقی خروجی‌ها دور ریخته شده‌اند. پس می‌توان دنباله کنترلی پرشی را به‌صورت معادل برای مولد انقباضی به شیوه دیگری نوشت.

حال جهت تحلیل مولد پرشی در دنباله C، به‌جای $c_i = 0$ عبارت $0,\cdots,0,1$ ($jump-1$) جایگزین می‌گردد. آنگاه دنباله C جدید به‌عنوان دنباله کنترلی ساختار مولد انقباضی در نظر گرفته شده و نتایج آن به مولد پرشی تعمیم داده می‌شود.

در ساختار مولدهای انقباضی، i بیت ابتدائی دنباله خروجی مولد حداکثر می‌تواند بر روی i بیت ابتدائی خروجی مولد انقباضی تأثیر بگذارد. درنتیجه می‌توان به رابطه (۹) رسید.

$$\hat{p}_i = \Pr(x_i = 1 | Y^n) = \Pr(x_i = 1 | Y^i) \quad (۹)$$

از طرفی، با استفاده از قضیه بیز[۲۰] رابطه (۱۰) به‌دست می‌آید.

$$\hat{p}_i = \frac{\Pr(x_i = 1)\ \Pr(Y^i | x_i = 1)}{\Pr(Y^i)} = 2^{i-1} \Pr(Y^i | x_i = 1) \quad (۱۰)$$

هدف محاسبه احتمال $\Pr(Y^i | x_i = 1)$ در رابطه (۱۰) است. در صورت تمایز قائل‌شدن بین حالت‌های $w(\mathrm{C}^i) = k$ برای $k = 0,\cdots,i$، رابطه (۱۱) به‌دست می‌آید.

$$\begin{aligned} &\Pr(Y^i | x_i = 1) = \\ &\sum_{k=0}^{i} \Pr(Y^i, w(C^i) = k | x_i = 1) = \\ &\sum_{k=0}^{i} \Pr(Y_{k+1}^i | Y^k, w(C^n) = k, x_i = 1) \\ &\Pr(Y^k, w(C^n) = k | x_i = 1) \end{aligned} \quad (۱۱)$$

اگر وزن C^i برابر k باشد، خروجی Y_{k+1}^i از دنباله‌های روابط (۱۲) و (۱۳) به‌دست می‌آید.

$$C_{i+1} = (C_L)_{L\geq i+1} \quad (۱۲)$$

$$Y_{i+1} = (y_L)_{L\geq i+1} \quad (۱۳)$$

بنابراین می‌توان شرط احتمال ابتدایی را نادیده گرفت و رابطه (۱۴) را نوشت.

$$\begin{aligned} \Pr(Y^i | x_i = 1) &= \sum_{k=0}^{n} \Pr(Y_{k+1}^i) \Pr(Y^k, w(C^n) = k | x_i = 1) \\ &= \sum_{k=0}^{i} 2^{k-i} \Pr(Y^k, w(C^n) = k | x_i = 1) \end{aligned} \quad (۱۴)$$

با توجه به اینکه احتمال وقوع ۰ یا ۱ در دنباله کنترلی یکسان لحاظ می‌شود، پس می‌توان طول دنباله C را برابر ۲m در نظر گرفت که بیانگر m تا صفر و m تا یک در دنباله C است. حال اگر به‌ازای $\mathrm{Ci} = 0$ حالت پرشی و همچنین برای $\mathrm{Ci} = 1$ حالت نرمال در نظر گرفته شود، رابطه (۱۵) به‌دست می‌آید. (j بیانگر اندازه شاخص پرش است).

$$c_i = 0 \rightarrow jump \Rightarrow Number\ of\ 0 = (j-1)\times m$$
$$c_i = 1 \rightarrow normal \Rightarrow Number\ of\ 1 = 2m$$
$$\Pr_0(c_i = 0) = \frac{(j-1)m}{2m + jm - m} = \frac{(j-1)m}{(j+1)m} = \frac{j-1}{j+1} \qquad (۱۵)$$
$$\Pr_1(c_i = 1) = \frac{2m}{2m + jm - m} = \frac{2m}{(j+1)m} = \frac{2}{j+1}$$

از طرفی احتمال اینکه وزن همینگ دنباله کنترلی برابر k باشد از رابطه (۱۶) به‌دست می‌آید.

$$\Pr(w(c^{i-1}) = k) = \binom{n}{k} \Pr_1^{\,k}\ \Pr_0^{\,n-k} \qquad (۱۶)$$

برای محاسبه احتمال رابطه (۱۷) باید بین دو حالت تمایز قائل شد.

$$P(Y^k, w(C^i) = k \mid x_i = 1) \qquad (۱۷)$$

حالت اول، $c_i = 0$. در این حالت خروجی i ام مولد حذف شده و رابطه (۱۸) به‌دست می‌آید.

$$\begin{aligned}
&\Pr(Y^k, w(C^i) = k, c_i = 0 \mid x_i = 1)\\
&= \Pr_0 \Pr(Y^k) \Pr(w(C^{i-1}) = k)\\
&= \frac{j-1}{j+1} \cdot \frac{1}{2^k} \cdot \binom{i-1}{k} \Pr_1^{\,k}\ \Pr_0^{\,i-1-k}\\
&= \frac{j-1}{2^k (j+1)} \cdot \binom{i-1}{k} \left(\frac{2}{j+1}\right)^k \left(\frac{j-1}{j+1}\right)^{i-1-k}\\
&= \frac{j-1}{j+1} \cdot \binom{i-1}{k} (j+1)^{-k} \left(\frac{j-1}{j+1}\right)^{i-1-k}\\
&= \frac{j-1}{j+1} \cdot \binom{i-1}{k} (j+1)^{1-i}\ (j-1)^{i-1-k}\\
&= \frac{(j-1)^{i-k}}{(j+1)^i} \cdot \binom{i-1}{k}
\end{aligned} \qquad (۱۸)$$

حالت دوم، $c_i = 1$. بیت i ام دنباله مولد (xi)، در خروجی ثبت می‌گردد. به دلیل اینکه $w(C^i) = k$ آنگاه $y_k = x_i = 1$. درنتیجه رابطه (۱۹) به‌دست می‌آید.

$$\begin{aligned}
&\Pr(Y^k, w(C^i) = k, c_i = 1 \mid x_i = 1)\\
&= \Pr_1 \Pr(Y^k, y_k = 1) \Pr(w(C^{i-1}) = k-1)\\
&= \frac{2}{j+1} \cdot \frac{y_k}{2^k} \cdot \binom{i-1}{k-1} \Pr_1^{\,k-1}\ \Pr_0^{\,i-k}\\
&= \frac{2y_k}{2^k (j+1)} \cdot \binom{i-1}{k-1} \left(\frac{2}{j+1}\right)^{k-1} \left(\frac{j-1}{j+1}\right)^{i-k}\\
&= \frac{2y_k \times 2^{k-1} \times (j-1)^{i-k}}{2^k (j+1)^i} \cdot \binom{i-1}{k-1}\\
&= \frac{y_k \times (j-1)^{i-k}}{(j+1)^i} \cdot \binom{i-1}{k-1}
\end{aligned} \qquad (۱۹)$$

حال با لحاظ‌کردن روابط (۱۸) و (۱۹) در رابطه (۱۰)، رابطه (۲۰) به‌دست می‌آید.

$$\begin{aligned}
\hat{p}_i &= 2^{i-1} \sum_{k=0}^{i} 2^{k-i} \left(\frac{(j-1)^{i-k}}{(j+1)^i} \cdot \binom{i-1}{k} + \frac{y_k \times (j-1)^{i-k}}{(j+1)^i} \cdot \binom{i-1}{k-1} \right)\\
&= \frac{1}{2} \left(\frac{j-1}{j+1} \right)^i \left(\sum_{k=0}^{i-1} \left(\frac{2}{j-1} \right)^k \binom{i-1}{k} + \sum_{k=1}^{i} \left(\frac{2}{j-1} \right)^k \binom{i-1}{k-1} y_k \right)
\end{aligned} \qquad (۲۰)$$

با توجه به رابطه (۲۱)، اگر شاخص پرش به‌سمت بی‌نهایت میل کند، آنگاه $\hat{p}_i = \frac{1}{2}$ خواهد شد، درنتیجه اریبی به سمت صفر میل می‌کند.

$$Limit_{j \to \infty} \left(\frac{1}{2} \left(\frac{j-1}{j+1} \right)^i \left(\sum_{k=0}^{i-1} \left(\frac{2}{j-1} \right)^k \binom{i-1}{k} + \sum_{k=1}^{i} \left(\frac{2}{j-1} \right)^k \binom{i-1}{k-1} y_k \right) \right) = \frac{1}{2} \qquad (۲۱)$$

بنابراین می‌توان گفت هر چه اندازه شاخص پرش در مولدهای پرشی بزرگ‌تر باشد، وابستگی دنباله‌های خروجی مولد به دنباله‌های ورودی آن کمتر می‌شود.

به‌منظور درک بهتر تأثیر اندازه شاخص پرش بر روی همبستگی دنباله، تمام چندجمله‌ای‌های اولیه درجه ۶ به‌همراه اندازه شاخص پرش آن‌ها مطابق جدول (۱) در نظر گرفته شده است.

جدول ۱: چندجمله‌ای‌های اولیه درجه ۶ و شاخص پرش آن‌ها

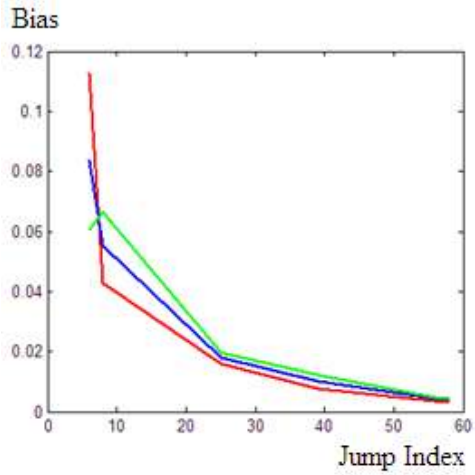
شاخص پرش متناظر	چندجمله‌ای اولیه درجه ۶
۶	$x^6 + x + 1$
۸	$x^6 + x^5 + x^3 + x^2 + 1$
۲۵	$x^6 + x^5 + x^2 + x + 1$
۳۹	$x^6 + x^5 + x^4 + x + 1$
۵۶	$x^6 + x^4 + x^3 + x + 1$
۵۸	$x^6 + x^5 + 1$

جدول (۲) اریبی شاخص پرش را با استفاده از رابطه (۱۱)، برای چندجمله‌ای‌های جدول (۱) و به‌ازای سه کلاک ۵۰، ۴۰، ۳۰ = i، نشان می‌دهد.

جدول ۲: اریبی شاخص پرش برای چندجمله‌ای‌های اولیه درجه ۶ به‌ازای کلاک‌های مختلف

jump	clock = ۳۰	clock = ۴۰	clock = ۵۰
۶	۰/۱۱۲۵۸۱۴	۰/۰۸۳۹۹۴۵	۰/۰۶۰۴۲۹۰
۸	۰/۰۴۲۸۱۵۶	۰/۰۵۵۱۹۳۴	۰/۰۶۶۴۶۸۷
۲۵	۰/۰۱۵۷۳۳۸	۰/۰۱۸۰۴۹۰	۰/۰۱۹۵۰۳۴
۳۹	۰/۰۰۷۷۱۱۲	۰/۰۱۰۱۰۹۸	۰/۰۱۲۱۰۶۵
۵۶	۰/۰۰۳۳۵۰۶	۰/۰۰۴۳۰۷۳	۰/۰۰۴۸۶۱۱
۵۸	۰/۰۰۳۱۱۶۳	۰/۰۰۴۰۲۸۷	۰/۰۰۴۵۲۸۸

همچنین نمودار شکل (۴) نتایج جدول (۲) را به تصویر می‌کشد.



شکل ۴. نمودار اریبی شاخص پرش برای چندجمله‌ای‌های اولیه درجه ۶ به‌ازای کلاک‌های مختلف.
نمودار قرمز؛ ۳۰ کلاک، نمودار آبی؛ ۴۰ کلاک، نمودار سبز؛ ۵۰ کلاک.

همان‌طور که در شکل (۴) مشاهده می‌شود، نتایج به‌دست‌آمده در تأثیر اندازه شاخص پرش تأیید می‌گردد؛ ازاین‌رو انتخاب چندجمله‌ای با حداکثر اندازه شاخص پرش بر روی کاهش میزان همبستگی دنباله خروجی و همچنین اریبی متناظر تأثیرگذار است.

به‌بیان‌دیگر، شکل (۴) نشان می‌دهد که از دیدگاه حملات همبستگی در طراحی مولدهای پرشی، اولویت با انتخاب چندجمله‌ای‌هایی با حداکثر اندازه شاخص پرش است؛ چراکه میزان همبستگی دنباله خروجی از این مولدها را به سمت ۰/۵ خواهد برد و بنابراین اریبی به صفر نزدیک می‌گردد.

۵ -نتیجه‌گیری

مولدهای پرشی به‌عنوان یکی از ساختارهای رمز جریانی مبتنی بر LFSR، علاوه بر بهبود کارایی نسبت به ساختارهای انقباضی، مقاومت در برابر حملات کانال جانبی را نیز فراهم می‌کنند. در این مقاله به بررسی وضعیت همبستگی دنباله خروجی این مولدها پرداخته شده است.

با تحلیل‌های صورت‌گرفته بر روی ساختار پرشی، رابطه محاسبه همبستگی دنباله خروجی مولد نسبت به دنباله ورودی آن به‌دست آمد. این رابطه نشان می‌دهد که در مقایسه با ساختارهای انقباضی، استفاده از روش پرشی باعث کاهش همبستگی می‌گردد.

در گام دیگر مقاله، در خصوص تأثیر شاخص پرش بر روی همبستگی دنباله خروجی مولدهای پرشی تمرکز شد. نتیجه بررسی‌ها نشان داد که هرچه اندازه شاخص پرش بزرگ‌تر باشد، همبستگی دنباله خروجی کوچک‌تر و درنتیجه به ۰/۵ نزدیک‌تر می‌گردد. ازاین‌رو در طراحی رمزهای جریانی با ساختار مولدهای پرشی، از دیدگاه حملات همبستگی، اولویت با انتخاب چندجمله‌ای‌هایی با حداکثر میزان شاخص پرش است.

مراجع

[1] A. A. Alhamdan, Secure Stream Cipher Initialization Processes, Ph.D. Thesis, University of Queensland, 2014.

[2] T. Beth and F. Piper, “The stop-and-go generator,” Advances in Cryptology, Eurocrypt, vol. 84, pp. 88–92, 1985.

[3] C.G. Günther, “Alternating step generators controlled by De Bruijn sequences,” Advances in Cryptography, Eurocrypt ’87, vol. 304, pp. 5–14, 1988.

[4] D. Coppersmith, H. Krawczyk and Y. Mansour, “The shrinking generator,” Advances in Cryptology, CRYPTO ’93, Santa Barbara, vol. 773, pp. 22–39, 1994.

[۵] حامد مؤمنی و محمدعلی طاهری، «حمله تحلیل زمان روی یک الگوریتم رمز جریانی»، مجله علمی-پژوهشی پدافند الکترونیکی و سایبری، سال چهارم، شماره ۱، صفحات ۵۷-۵۱، ۱۳۹۵.

[6] C. J. Jansen, “Modern stream cipher design: A new view on multiple clocking and irreducible polynomials,” Acts de la VII Reunion Espanola sobre Criptologia y Seguridad de la Information, vol. 1, pp.11-29, 2002.

[7] C. J. A. Jansen, T. Helleseth and A. Kholosha, “Cascade jump controlled sequence generator and Pomaranch stream cipher,” Lecture Notes in Computer Science 4986, pp. 224-243, 2008.

[8] S. H. Babbage and M.W. Dodd, “The stream cipher MICKEY 2.0,” ECRYPT stream cipher project, 2006. http://www.ecrypt.eu.org/stream/.

[9] F. Masoodi, S. Alam and M. U. Bokhari, “An analysis of linear feedback shift register in stream ciphers,” International journal of Computer Applications, Vol. 46, No. 17, pp.46-49, 2012.

[10] A. C. Lechtaler, M. Cipriano, E. Garcia, J. Liporace. A. Maoirano and E. Malvacio, “Model design for a reduced variant of a Trivium type stream cipher,” JCS&T. Vol. 14, No. 1, 2014

[11] A. Klein, *Stream Cipher*. Dept. of Pure Mathem. & Computer Algebra, State University of Ghent, Belgium. London Heidelberg New York Dordrecht. Springer 2013

[12] J. D. Golic, “Correlation analysis of the shrinking generator,” CRYPTO 2001, vol. 2139, pp. 440-457, 2001.

[۱۳] محمدعلی طاهری و حامد مؤمنی، «ارائه روش طراحی رمزهای قالبی مبتنی بر کلید وابسته به داده برای مقاومت در برابر حملات خطی و تفاضلی»، مجله علمی-پژوهشی پدافند الکترونیکی و سایبری، سال پنجم، شماره ۱، صفحات ۴۵-۳۷، ۱۳۹۶.

[14] H. Momeni, M. Masoumi, and A. Dehghan, “A practical fault induction attack against an FPGA implementation of AES cryptosystem,” World Congress on Internet Security (World CIS2013), pp. 134-138, 2013.

[۱۵] شهرام جمالی و عرفان آقایی کیاسری، «بهبود حمله مکعبی کانال جانبی بر روی الگوریتم‌های بلوکی»، مجله مهندسی برق دانشگاه تبریز، جلد ۴۵، شماره ۴، زمستان ۱۳۹۴.

[16] S. Babbage and M. Dodd, “Finding characteristic polynomials with jump indices,” IACR Cryptology ePrint Archive, p. 10, 2006.

[17] C. J. A. Jansen, “Stream cipher design based on jumping finite state machines,” IACR Cryptology ePrint Archive, p. 267, 2005.

[18] G. Zeng, Y. Yang, W. Han and S. Fan, “Word oriented cascade jump σ−LFSR,” M. Bras Amor´os and T. Høholdt (Eds.), AAECC vol. 9, pp. 127–136, 2009.

[19] T. Siegenthaler, “Decrypting a class of stream ciphers using cipher text only”. IEEE Trans. Computers, no. 34(1), pp.81–85, 1985.

زیرنویس‌ها

[1] Linear Feedback Shift Register (LFSR)
[2] Correlation Attack
[3] Algebraic Attack
[4] Non Linear Combination Generators
[5] Non Linear Filter Generator
[6] Clock Controlled Generator
[7] Stop and Go Generator
[8] Alternating Step Generator
[9] Shrink Generator
[10] Side Channel Attack
[11] Jump Index
[12] Bereklamb Messy
[13] Nonlinearity
[14] Hamming Weight
[15] Power Analysis Attack
[16] Time Analysis Attack
[17] Linear Feedback State Machine
[18] Siegenthaler
[19] Independent Identically Distribution
[20] Bayes