# طراحی و ارزیابی آماری مولدهای باینری شبه‌تصادفی آشوبی[1]

محمد دخیل علیان
دانشگاه صنعتی اصفهان
دانشکده: برق و کامپیوتر
تلفن: ۸۹۱۲۲۴۵۰(۰۳۱)
Md-alian@iut.cc.ac.ir

محمدرضا عارف
دانشگاه صنعتی شریف
دانشکده: برق
تلفن: ۸۹۱۲۱۱۲(۰۲۱)
Aref@awww.dci.co.ir

بابک صادقیان
دانشگاه صنعتی امیر کبیر
دانشکده: کامپیوتر
تلفن: ۶۱۳۹۴۳۳(۰۲۱)
Basadegh@ce.aku.ac.ar

**چکیده:** در سیستمهای رمز پی‌درپی و بسیاری از سیستمها استفاده از دنباله‌های شبه‌تصادفی مناسب و گاهی ضروری است. از آنجا که سیستمهای آشوبی دارای رفتار نامنظم و تصادف‌گونه‌ای هستند می‌توانند به عنوان مولد مناسبی مطرح گردند. بدین‌جهت در این مقاله به بررسی این امر پرداخته‌ایم و سعی نموده‌ایم با تکیه بر نگاشتهای آشوبی یک بعدی، چگونگی تولید دنباله‌های باینری از روی دنباله‌های خروجی نگاشتها را ارایه کرده و متعاقب آن دنباله‌های تولید شده را مورد ارزیابی قراردهیم. نتایج نشان می‌دهد که دنباله‌های مذکور دارای خواص آماری بسیار مطلوبی هستند.

**کلمات کلیدی:** دنباله‌های شبه‌تصادفی باینری، سیستمهای رمز پی‌درپی، آشوب، نگاشتهای یک بعدی

## ۱- مقدمه

دنباله‌های آشوبی به‌واسطه دارا بودن ویژگیهای جالب توجهی از جمله حساسیت نسبت به حالت اولیه و به تعبیری غیر قابل پیشگویی بودن، می‌توانند به‌عنوان یک مولد کلید اجرایی در سیستمهای رمز پی‌درپی مورد استفاده قرار گیرند. نگاشتهای آشوبی ارگادیک در حالت ایستان دارای رفتار نامنظمی هستند که این رفتار با تابع‌چگالی پایا[2] توصیف می‌گردد و به همین منظور با در نظر گرفتن تابع چگالی پایا رفتار دنباله‌های تولید شده توسط نگاشتهای آشوبی ارگادیک مورد بررسی قرار گرفته و نشان داده شده است که رفتار دنباله‌های تولید شده توسط این نگاشتها با نمونه‌های یک متغیرتصادفی با همان تابع‌چگالی تطابق زیادی دارد[۱].

در سیستمهای رمز پی‌درپی، تاکنون مولدهای ذاتاً غیرخطی نیز پیشنهاد شده‌اند که شیفت رجیسترهای بافیدبک غیرخطی($FSR$) و شیفت رجیسترهای با فیدبک نقلی‌دار($FCSR$) نمونه‌ای از آنها می‌باشند[۲]. نگاشتهای آشوبی مشابه با این مولدها دارای سیکلهای متنوعی می‌باشند، با این تفاوت که با افزایش دقت محاسبات می‌توان دورهٔ تناوب سیکلها و طول گذرای اولیه برای رسیدن به سیکلها را بسیار بزرگ نمود[۱]. از جمله مزایای این دنباله‌ها این است که رفتار نامنظم مؤلفه‌ها در تمامی طول دنباله از تابع‌چگالی پایا پیروی می‌کند. اگر با

1- *Chaos*

2 - *Invarian density function*

روش مناسبی بتوان از ایجاد سیکلهای نهایی با دورهٔ تناوب کوچک جلوگیری نمود، می‌توان به استناد تابع‌چگالی نگاشت، دنباله‌های شبه‌تصادفی امنی را با خواص آماری بسیار مطلوب تولید نمود[۱].

در این مقاله با تکیه بر نگاشتهای آشوبی یک بعدی نظیر لجستیک، از روی دنباله‌های آشوبی تولید شده توسط این نگاشتها، دنباله‌های شبه‌تصادفی باینری مناسبی را ارائه و ارزیابی خواهیم نمود. بر همین اساس در بخش دوم روشهای تولید دنباله‌های باینری را بیان خواهیم نمود. سپس در بخش بعد به ارزیابی آماری دنباله‌های تولید شده توسط این نگاشتها خواهیم پرداخت و نشان خواهیم داد که دنباله‌های تولید شده دارای خواص آماری مطلوبی هستند. در بخش ۴ در مورد فضای کلید دنباله‌ها مطالبی را بیان خواهیم کرد و متعاقب آن به بیان غیرقابل پیشگویی بودن دنباله‌های باینری خاصی که توسط نگاشتهای آشوبی بدست می‌آیند خواهیم پرداخت. نتایج این بخش نشان می‌دهد که در حالت خاص علاوه بر خواص آماری مطلوب دنباله‌ها، با مشاهدهٔ تعداد زیادی از بیتهای دنباله نمی‌توان بیت بعدی را پیشگویی نمود.

## ۲- چگونگی تولید دنباله‌های باینری

نگاشتهای آشوبی دنباله‌های نامنظم و تصادف گونه‌ای در یک ناحیه مشخص ایجاد می‌کنند. نگاشتهای مورد نظر ما در نگاشتهایی هستند که روی یک فاصلهٔ‌پیوستهٔ $[a,b]$ دارای رفتار آشوبی می‌باشند. از آنجا که می‌خواهیم رفتار این دنباله‌ها را در حد ارقام اعشار آنها مورد بررسی قرار دهیم لذا خروجی نگاشت را با تبدیل خطی ساده‌ای به فاصلهٔ $[0,1]$ منتقل می‌نماییم. اگر $x_i$ مولفهٔ تولید شده توسط نگاشت مذکور باشد، در این صورت $y_i = \frac{x_i - a}{b-a}$ مولفه‌ای در فاصلهٔ $[0,1]$ خواهد شد. تابع‌چگالی پایا برای دنباله‌های تبدیل شده نیز دقیقا نظیر تبدیل‌خطی یک متغیرتصادفی می‌باشد. بنابراین در این بخش فرض می‌کنیم کلیهٔ دنباله‌ها یا واقعاً در فاصلهٔ $[0,1]$ هستند و یا با تبدیل‌خطی در این فاصله قرار گرفته‌اند.

برای تولید دنبالهٔ باینری فرض کنید $x_i$ مولفهٔ $i$ام تولید شده توسط نگاشت آشوبی $g(x)$ به صورت $x_i = g(g(\cdots g(x_0)))$ باشد، با تعریف $y_i^l = a^l x_i \ mod\ 1$ مؤلفه‌های دنبالهٔ باینری $S(x_0) = s_0, s_1, s_2 \cdots$ به صورت زیر قابل تعریف می‌باشند:

$$s_i = \begin{cases} 0 & if \quad 0 \le y_i^l < \frac{1}{2} \\ 1 & if \quad \frac{1}{2} \le y_i^l \le 1 \end{cases} \quad , \ i = 0,1,2,\ldots \tag{۱}$$

به منظور افزایش سرعت مولد می‌توان از هر $x_i$ بیش از یک بیت استخراج نمود. برای این کار فرض کنید بخواهیم از هر $x_i$، $L$ بیت استخراج کنیم. در این‌صورت می‌توان مؤلفه‌های $S(x_0) = s_0^1, s_0^2, \cdots, s_0^L, s_1^1, s_1^2, \cdots, s_1^L, \cdots$ را از رابطهٔ(۲) بدست آورد.

$$s_i^j = \begin{cases} 0 & if \quad 0 \le y_i^{l_j} \le \frac{1}{2} \\ 1 & if \quad \frac{1}{2} \le y_i^{l_j} \le 1 \end{cases} \quad , \ i = 0,1,2,\ldots \ , \ j = 1,2,\ldots,L \tag{۲}$$

در رابطهٔ(۲) متغیر $y_i^{l_j}$ به‌صورت زیر تعریف می گردد :

$$y_i^{l_j} = 10^{l_j} x_i \ mod\ 1 \quad , \quad i = 0,1,2,\ldots \ , \ j = 1,2,\ldots,L \tag{۳}$$

([ ] نشان دهندهٔ جزء صحیح می‌باشد)

در حالت کلی می‌توان دنبالهٔ باینری $S(x_0)$ را با استفاده از نمایش مولفهٔ $x_i$ در مبنای $a$ $(a = 2,4,6,\cdots)$ بدست آورد. از آنجا که $x_i$ عددی بین صفر و یک می‌باشد، می‌توان آن را به‌صورت (۴) نمایش داد.

$$x_i = 0.a_1^i a_2^i a_3^i \ldots \quad , \quad i = 0,1,2,\ldots \ , \ a = 2,4,6,\ldots \tag{۴}$$

بنابر این برای استخراج یک بیت از هر $x_i$ و تولید $S(x_0)$ می‌توان از رابطهٔ(۵) استفاده نمود :

$$s_i = \left[2a^{l-1} x_i\right] mod\, 2 \quad , \quad l = 1,2,\ldots \ , \ i = 0,1,2,\ldots \tag{۵}$$

اگر $l = 1$ در نظر گرفته شود دنبالهٔ $S(x_0)$ همان دنبالهٔ تولید شده توسط(۱) خواهد شد.

از آنجاکه تابع چگالی پایای نگاشتهایی نظیر لجستیک وچبی‌چف یکنواخت نیستند، بنابراین ارقام $a_1^j, a_2^j, \cdots$ لزوما دارای توزیع یکنواختی بوده وتضمینی برای یکنواختی تعداد صفرها و یکها در دنبالهٔ $S(x_0)$ وجود ندارد. البته با توجه به تابع بیان شده در[۱] انتظار این است که توزیع ارقام با وزن کمتر به سمت توزیع یکنواخت میل نماید.

اگر بخواهیم از $x_i$ (در مبنای $a$)، $L$ بیت استخراج کنیم می‌توان از رابطهٔ زیر استفاده نمود:

$$s_i^j = \left[2a^{l_{j-1}}x_i\right] mod\, 2 \quad , \quad i = 0,1,2,\dots \;,\; j = 1,2,\dots,L \qquad (۶)$$

$L$ بیت استخراج شده توسط رابطهٔ(۶) باید حتی‌المقدور از ارقام با وزن کمتر انتخاب گردد.

## ۳- ارزیابی آماری دنباله‌های باینری

ارزیابی آماری دنباله‌های کلید اجرایی اهمیت خاصی در بررسی نقاط ضعف این دنباله‌ها دارد. اگر چه ضعیف بودن خواص آماری ممکن است مستقیماً کمکی به تحلیگررمز نکند ولی ضعیف بودن خواص آماری خطر آسیب پذیری آلگوریتم را بسیار زیاد می‌کند. ارزیابی آماری اولین ارزیابی عملی است که در عین سادگی بسیار حایز اهمیت است. زیرا در سیستمهای رمز پی‌درپی آنچه مطلوب است داشتن دنباله‌های کاملاً تصادفی است و لذا هر چه دنبالهٔ کلید اجرایی از این دیدگاه نامنظم و تصادفی‌تر جلوه نماید مناسب‌تر می‌باشد.

تاکنون آزمونهای آماری متعددی برای بررسی تصادفی بودن دنباله‌ها ابداع شده است، که هر یک به نوعی دنبالهٔ کلید اجرایی را ارزیابی می‌کنند[۱]. در این بخش دنباله‌های باینری حاصل شده از دو نگاشت لجستیک و مثلثی را مورد ارزیابی قرار می‌دهیم.

**نگاشت لجستیک**: نگاشت لجستیک[1] به صورت(۶)تعریف می‌شود. رفتار این نگاشت به ازای تغییرات پارامتر $\mu$ دقیقاً مورد بررسی قرار گرفته است[۲].

$$g(x) = \mu x(1-x) \qquad x \in [0,1] \qquad (۶)$$

این بررسیها نشان می‌دهد، حوالی $\mu = 4$ رفتار نگاشت روی فاصلهٔ واحد آشوبی می‌گردد. هنگامی که $\mu$ از مقدار خاصی حوالی ۳/۸۳.. بزرگتر شود نمای لیاپانف مثبت شده و از این نقطه به بعد است که رفتار آشوبی نمایان می‌گردد. به ازای $\mu = 4$ نگاشت لجستیک دارای ویژگیهای خاص یک نگاشت آشوبی بوده و نگاشت مذکور دارای هیچ سیکل جاذبی[2] روی ناحیه واحد نخواهد بود[۳]. این نگاشت یک نگاشت ارگادیک می‌باشد که تابع چگالی پایا برای آن به صورت(۷) محاسبه شده است[۴]:

$$f(x) = \frac{1}{\pi\sqrt{x(1-x)}} \qquad x \in [0,1] \qquad (۷)$$

باتوجه به تابع چگالی پایا، نمای لیاپانف برای این نگاشت برابر $Ln2$ بدست آمده است[۴].

علاوه بر این تابع خودهمبستگی نگاشت $g(x) = 4x(1-x)$ به صورت زیر بدست می‌آید[۱]:

$$c(m) = \frac{\delta(m)}{8} \quad m = 0,1,2,\cdots \qquad (۸)$$

رابطهٔ(۸) نشان می‌دهد که نتایج حاصل شده از تکرارهای نگاشت لجستیک ناهمبسته هستند.

**نگاشت مثلثی**: نگاشت مثلثی در حالت کلی به صورت (۹) تعریف می‌شود:

$$g(x) = \begin{cases} cx & 0 < x \le 0.5 \\ c(1-x) & 0.5 < x \le 1 \end{cases} \quad 1 < c \le 2 \qquad (۹)$$

تابع چگالی پایا برای این نگاشت(به ازای $c=2$) به صورت یکنواخت می‌باشد[۵]. یعنی:

$$f(x) = 1 \qquad 0 \le x \le 1 \qquad (۱۰)$$

بر همین اساس به سادگی می‌توان دید که نمای لیاپانف این نگاشت برابر $Ln(c)$ می‌گردد.

---

1 - Logistic

2 - Attracting periodic orbit.

با توجه به یکنواخت بودن تابع‌چگالی، تابع همبستگی نگاشت مثلثی به‌صورت (۱۱) محاسبه شده است[۵] :

$$c(m) = \frac{\delta(m)}{12} \quad m = 0,1,2,\cdots \tag{۱۱}$$

رابطهٔ(۱۱) نشان می‌دهد که نتایج حاصل شده از تکرارهای نگاشت مثلثی نیز همچون نگاشت لجستیک ناهمبسته می‌باشد.

با توجه به ویژگیهای تابع چگالی پایا[1] برای این نگاشتها و بررسیهای انجام شده در [۱]، انتظار ما از دنباله‌های حاصل شده این است که از خواص آماری خوبی برخوردار باشند. علاوه بر این با توجه به ویژگی ارقام با وزن کم هر یک از مؤلفه‌های دنباله، باید دنباله‌های استخراج شده از ارقام با وزن کمتر دارای خواص آماری بهتری نسبت به ارقام با وزن بالاتر باشند.

برای تولید دنبالهٔ باینری از این نگاشتها به دو صورت بیتهای دنباله‌های باینری مورد نظر را استخراج نموده‌ایم، یکی استفاده از نمایش مؤلفه‌ها،در مبنای ده و دیگری استفاده از ارقام حاصل شده از نمایش باینری مؤلفه‌ها(رابطهٔ(۴) و (۵) به ازای $a=10$ و $a=2$)در روش اول به منظور بررسی رفتار دنباله‌های مختلف باینری هشت حالت مختلف را مورد ارزیابی قرار داده‌ایم. پنج حالت اول مربوط به اعداد باینری حاصل شده از ارقام اول، دوم، ... وپنجم می‌باشد(رابطهٔ(۱)) که به اختصار آنها را $d_5, d_4, d_3, d_2, d_1$ نامگذاری نموده‌ایم. دو حالت بعد مربوط به بیتهای استخراج شده از ارقام دهم و پانزدهم هر مؤلفه است که با $d_{15}, d_{10}$ آنها را مشخص نموده‌ایم. بالاخره آخرین حالت مربوط به استخراج ۸ بیت از ارقام متوالی پنجم تا سیزدهم می‌باشد(رابطهٔ(۲)) که با $d_{5,8}$ مشخص نموده‌ایم.

در روش دوم نیز هشت حالت مختلف را برای تولید دنباله‌های شبه‌تصادفی باینری انتخاب نموده‌ایم. پنج حالت اول مربوط به اعداد باینری حاصل شده از بیتهای اول، دوم، ... و پنجم نمایش باینری هر مؤلفه از دنبالهٔ نمونه می‌باشد(رابطهٔ(۴) به ازای $a=2$) که به اختصار آنها را $b_5, b_4, b_3, b_2, b_1$ نامگذاری نموده‌ایم. $b_{40}, b_{20}$ نیز ارقام بیستم و چهلم نمایش باینری مؤلفه‌ها بوده و $b_{40,8}$ نیز ارقام باینری چهلم تا چهل و هشتم نمایش باینری مؤلفه‌ها می‌باشد.

جداول(۱) و (۲) نتایج حاصل از آزمونهای مختلف بر روی دنباله‌های باینری تولید شده توسط نگاشت لجستیک می‌باشد. در هر آزمایش ۱۰۰۰دنباله مورد آزمون قرار گرفته است که در این جداول تعداد دنباله‌های عبور نموده از آزمونها مشخص شده است. همانطور که ملاحظه می‌شود در تمامی حالتها دنباله‌های تولید شده دارای خواص آماری فوق‌العاده خوبی بوده‌اند و حتی هنگامی که از یک مؤلفه بیش از یک بیت استخراج شود( $d_{5,8}$ و $b_{40,8}$)خواص آماری دنبالهٔ باینری حاصل شده تغییری نخواهد کرد. جداول(۳) و (۴) همین نتایج را برای نگاشت مثلثی نشان می‌دهد. همانطور که ملاحظه می‌گردد، در کلیهٔ حالتها به جز $b_{40,8}$ خواص آماری دنباله‌ها بسیار عالی می‌باشد. در مورد حالت $b_{40,8}$ خواص آماری نامطلوب به خاطر خاصیت خطی نگاشت در دو فاصلهٔ $[0,0.5],[0.5,1]$ می‌باشد. در این حالت هنگامی که مقادیر مؤلفه‌ها بسیار نزدیک به صفر یا بزرگتر از ۰/۵ ولی بسیار نزدیک به آن باشند، مشهودتر می‌گردد. در چنین حالتهایی با توجه به ضریب زاویهٔ نگاشت در این فواصل، این نگاشت روی تعداد محدودی از مؤلفه‌ها شبیه شیفت برنولی عمل کرده و باعث می‌گردد تعدادی از بیتهای استخراج شده از مؤلفه‌های مجاور هم یکسان گردند. این حالت باعث عدم یکنواختی و ایجاد وابستگی بیتها می‌گردد. این در حالی است که استفاده از رابطهٔ(۵) برای استخراج چند بیت از یک مؤلفه، چنین وضعیت نامطلوبی را ایجاد نمی‌کند، زیرا در این حالت مستقیما از نمایش باینری مؤلفه‌ها استفاده نمی‌گردد. در [۱] نگاشتهای بیکر و چیبی‌چف مورد ارزیابی قرارگرفته و نتایج مشابهی بدست آمده است، این نتایج نشان می‌دهد که دنباله‌های تولید شده توسط این مولدها از دیدگاه آماری بسیار مطلوب می‌باشند.

## ۴- فضای کلید

در مولدهای کلید اجرایی، کلید اصلی دارای اهمیت خاصی است چرا که اگر دشمن به آن دست پیدا کند، براحتی می‌تواند کلید اجرایی را مجدداً تولید نموده و توسط آن متن رمز شده را کشف نماید. حال سؤال این است که اگر بخواهیم از مولدهای آشوبی استفاده نماییم، کلید چگونه تعریف می‌گردد و فضای انتخاب کلید دارای چند عضو است. کلید می‌تواند به گونه‌های مختلف تعریف شود ولی آنچه بدیهی است این است که حالت اولیهٔ نگاشت یکی از عوامل اصلی کلید به‌شمار خواهد رفت. اگر دقت محاسبات در نمایش مبنای $a$ برابر $r$

1 - Invariant density function

رقم اعشار باشد، به تعداد $a^r$ حالت اولیه می‌توان برای نگاشت در نظر گرفت. اگر فرض کنیم الگوریتم استخراج بیتها از مؤلفه‌های دنباله مشخص باشد، فضای کلید حداکثر برابر $a^r$ خواهد شد.

اگر بطور اختیاری از هر مؤلفه $L$ بیت استخراج شود(رابطهٔ(۶)) و به صورت دلخواه ترتیب آنها جابجا گردد، به تعداد $A_r^L = \frac{r!}{(r-L)!}$ انتخاب ممکن برای این‌کار وجود خواهد داشت. از طرف دیگر چگونگی نسبت دادن یک بیت به هر مؤلفهٔ استخراج شده می‌تواند به‌صورت اختیاری باشد، مثلاً رابطهٔ(۶)را می‌توان به‌صورت زیر در نظر گرفت :

$$s_i^j = \left\{ \left[ 2a^{l_j - 1} x_i \right] mod\, 2 \right\} \oplus k_{lj} \quad , \quad i = 0,1,2,\dots \quad , \quad j = 1,2,\dots,L \qquad (۱۲)$$

در عبارت فوق $k_{l_j}$ یک بیت از کلید اصلی می‌باشد. بنابر این به تعداد $2^L$ انتخاب برای نسبت دادن یک بیت می‌توان متصور شد. پس تعداد اعضای فضای کلید برابر(۱۳)خواهد شد :

$$K = a^r\, A_r^L\, 2^L\, B \quad , \quad A_r^L = \frac{r!}{(r-L)!} \qquad (۱۳)$$

در عبارت فوق $B$ ضریبی است که وابسته به نگاشت به‌طور اختیاری تعیین می‌گردد. مثلاً اگر از نگاشت چبی‌چف استفاده نماییم، مرتبهٔ نگاشت می‌تواند به عنوان بخشی از کلید محسوب گردد. به عنوان نمونه اگر حداکثر مرتبهٔ نگاشت چبی‌چف مورد استفاده برابر $N$ باشد، مقدار $B$ برابر $N$-$1$ خواهد شد.

البته هنگام پیاده‌سازی نگاشتها هر یک از بخشهای رابطهٔ(۱۳)ممکن است به نوعی تغییر نمایند. مثلاً در نگاشتهای لجستیک، مثلثی و بکر استفاده از حالت اولیهٔ صفر نامطلوب است، چرا که منجر به تولید دنبالهٔ تماماً صفر می‌گردد یا مثلاً استفاده از ارقام با وزن بالا بواسطهٔ ایمنی و توزیع بیتها بهتر است استفاده نشود که عملاً $A_r^L$ را محدود می‌کند. علاوه بر این ممکن است استخراج یک بیت به صورتهای پیچیده‌تری انجام گردد. مثلاً فرض کنید از هر مؤلفه $L$ بیت به صورت رابطهٔ(۶)انتخاب شود و سپس با اعمال تابعی نظیر $f$ بر آنها، نهایتاً یک بیت به صورت(۱۴) از هر مؤلفه استخراج گردد.

$$s_i = f\left(s_i^1, s_i^2, \dots, s_i^L\right) \quad , \quad i = 0,1,2,\dots \qquad (۱۴)$$

در این‌صورت فضای کلید بیان شده در(۱۳)در صورتی معتبر است که ترتیب قرار گرفتن متغیرهای تابع $f$ مهم باشد. به عنوان نمونه اگر تابع $f$ به صورت زیر باشد:

$$s_i = f\left(s_i^1, s_i^2, \dots, s_i^L\right) = s_i^1 \oplus s_i^2 \oplus \dots \oplus s_i^L \qquad (۱۵)$$

(در عبارت فوق $\oplus$ علامت جمع در پیمانه ۲ می‌باشد)

در این‌صورت، تعداد اعضای فضای کلید برابر(۱۶) می‌گردد، زیرا ترتیب قرار گرفتن متغیرهای تابع $f$ حایز اهمیت نمی‌باشد.

$$K = a^r\, C_r^L\, 2^L\, B \quad , \quad C_r^L = \frac{r!}{(r-L)!\,L!} \qquad (۱۶)$$

روابط(۱۳) و (۱۶) نشان می‌دهد که می‌توان فضای کلید قابل توجه و بزرگی را بوجود آورد.

## ۵- بیانی از غیر قابل پیشگویی بودن دنباله‌های باینری

فرض کنید دنبالهٔ $x_0, x_1, x_2, \cdots, x_n$ توسط نگاشت $g(x)$ تولید شده باشد حال اگر $x_{n+1}$ در اختیار باشد، بدون اطلاع از سابقهٔ دنباله، در مورد $x_n$ چه حدسی می‌توان زد. فرض کنید $g(x)$ یک از نگاشتهای لجستیک، مثلثی، بکر و یا چبی‌جف مرتبهٔ۲ باشد، در این‌صورت دو حالت ممکن برای $x_n$ می‌توان متصور شد، یکی $x_{n,1}$ و $x_{n,2}$ مثلاً در مورد نگاشت لجستیک این دو مقدار به صورت زیر خواهد شد:

$$x_{n,1} = \tfrac{1}{2} + \frac{\sqrt{1 - x_{n+1}}}{2} \quad , \quad x_{n,2} = \tfrac{1}{2} - \frac{\sqrt{1 - x_{n+1}}}{2} \qquad (۱۷)$$

نکتهٔ جالب توجه در این است که در نگاشتهای مذکور با توجه به تقـارن تابع‌چگالی‌پایـای آنهـا، بـه شـرط داشـتن $x_n$ انتخـاب یکـی از دو جـواب(۱۷) علی‌السـویه خواهـد بـود. بـه عبـارت دیگـر ابهـام مـا در انتخـاب $x_n$ برابـر یـک بیـت بـر سـمبل خواهـد شـد.گـر دنبالـهٔ باینری $b_0, b_1, \cdots, b_n$ توسط رابطهٔ(۶-۶) از دنبالهٔ $x_0, x_1, \cdots, x_n$ بدست آمده باشد، در این‌صـورت اطلاعـات متقابل میان $b_n$ و سابقهٔ دنباله یعنی $b_0, b_1, \cdots, b_{n-1}$ چگونه خواهد بود؟ در [۱] به ازای حالات خاصی ثابت شده است که، اطلاعات متقابل بیت $n$ام دنباله وسابقهٔ دنباله برابر صفر می‌باشد.

نکتهٔحایز اهمیت این است که نمای لیاپانف نگاشتهای لجستیک، چبی‌چف مرتبهٔ۲ و مثلثی برابر $ln\,2$ می‌باشد. اگر پایهٔ لگاریتم در محاسبهٔ نمای لیاپانف برابر۲ درنظر گرفته شود، نمای لیاپانف برابر یک می‌شود. یعنی میزان گم شدن اطلاعات هر مؤلفه در یک تکرار برابـر یک بیت برسمبل خواهد بود. به عبارت دیگر باداشتن مؤلفهٔ $x_{n+1}$ از دنبالهٔ مورد نظر، برای دستیابی به $x_n$ بطور متوسط نیاز به یک بیت برسمبل اطلاعات اضافی است. حال اگر از هر مؤلفه از دنبالهٔ تولید شده توسط این نگاشت یک بیت استخراج گردد، با توجه بـه تعبیر گـم شدن اطلاعات[۴]، می‌توان استنباط نمود که اطلاعات متقابل میان بیتهای تولید شده حداقل خواهد گردید.

در مورد نگاشتهای بکر وچبی‌چف مرتبهٔ $t$ $(t=2,3,\ldots)$ نمای لیاپانف به ترتیب برابربیک و $log_2\,t$ خواهد شد بنابر این در مورد این دو نگاشت میزان گم شدن اطلاعات در هر تکرار بطور متوسط برابر یک و $log_2\,t$ می‌باشد. بنابر این برای حداقل شدن اطلاعات متقـابل میان بیتهای دنبالهٔ باینری استخراج شده از هر یک از این دو نگاشت، بـاید از هـر مؤلفـه از نگاشـت بکـر حداکثـر یـک بیـت و از نگاشـت چبی‌چف حداکثر $\lfloor log_2\,t \rfloor$ بیت استخراج کنیم($\lfloor . \rfloor$ نشان دهندهٔجزءصحیح می‌باشد).

حال اینکه در عمل این بیتها چگونه از مؤلفه‌های دنبالهٔ تولید شده توسط نگاشتها استخراج شوند، سؤالی اسـت کـه در بخـش ارزیـابی آماری دنباله‌های باینری، از دیدگاه آماری تا حدی به آن پاسخ داده‌ایم. یعنـی ارقـام بـا وزن کمتـر از ایـن جهـت کـه دارای خـواص آمـاری مطلوب‌تری هستند، برای منظور ما طبیعتاً مناسب‌ترند.

## ۶- خلاصه و نتیجه گیری

در این مقاله ابتدا چگونگی تولید دنباله‌های باینری از روی دنباله‌های تولید شده توسط نگاشتهای آشـوبی مـورد نظـر را بیـان نمودیـم. همانطور که ملاحظه گردید مؤلفه‌های این دنباله‌ها را به صورت اعدادی اعشاری در مبنای $a$ در فاصلهٔ[۰،۱] در نظر گرفتیم و روابطی کلی را برای استخراج بیتهای دنبالهٔ باینری از این مؤلفه‌ها بیان نمودیم. پس از آن به ارزیـابی دنبـاله‌های بـاینری تولیـد شـده پرداختیـم و آزمونهـای متعددی که برای ایـن منظـور مطـرح شـده‌اند را در مـورد دنبالـه‌ها بکـار بردیـم. عـلاوه بـر اینهـا آزمونهـای خودهمبسـتگی، آزمـون پلکـان پیچیدگی‌خطی که در [۱] - در فصول سوم و چهارم مطرح گردیده است- مورد استفاده قرار گرفتند. نتایج کلیهٔ آزمونها حاکی از آن است که دنباله‌های باینری تولید شده- همانطور که انتظار می‌رفت - از این دیدگاه دارای وضعیت مطلوبی بوده و خصوصاً استفاده از ارقـام بـا وزن کم مؤلفه‌ها آمارگان مطلوبی را برای دنباله‌های باینری ایجاد می‌کنند. در این میان نگاشـت مثلثی موقعـی کـه تعدادی بیـت از یـک مؤلفـه استخراج شود، رفتار آماری نامطلوبی در برخی حالات مشاهده می‌گردد.

برای استفاده از دنباله‌های باینری مورد نظر به عنوان کلید اجرایی در یک سیستم رمز پی‌درپی چگونگی تعریـف کلیـد اصـلی و فضـای مربوطه مهم می‌باشد که در بخش۳ به آن پرداختیم و نشان دادیم که می‌توان با بکارگیری حالت اولیهٔ نگاشت، چگونگـی نسـبت دادن بیتهـا، تعداد بیتهای استخراج شده از هر مؤلفه، تغییر پارامترهای نگاشت و در نظر گرفتن دقت مناسـب بـرای انجـام محاسـبات، بـه فضـای نسـبتاً بزرگی دست یافت.در بررسی از دیدگاه امنیت دنباله‌ها در حالت خاصی از نگاشتها و هنگامی که تنها یک بیت از هر مؤلفه استخراج گردد- نشان داده شده که اطلاعات متقابل میان بیت $n$ام $(b_n)$ و سابقهٔ دنبالهٔ باینری تولید شده یعنی $b_0, b_1, \cdots, b_{n-1}$ برابر صفر می‌باشد. با توجه به اینکه میزان گم شدن اطلاعات در هر تکرار از این نگاشتها حداقل یک بیت بر سمبل می‌باشد(به طور متوسط)، لذا استخراج یـک بیـت از هر مؤلفه مناسب می‌باشد. به همین علت برای حداقل شدن اطلاعات متقابل میان بیتهای دنبالهٔ بـاینری حـاصل شـده از نگاشـتها بهتر اسـت حداکثر به تعداد جزء صحیح نمای لیاپانف نگاشت مربوطه، بیت از هر مؤلفه استخراج گردد.

جدول(۶-۱) : نتایج آزمونهای مختلف بر روی نگاشت: لجستیک،طول دنباله=۱۰۰۰ بیت ، تعداد دنباله=۱۰۰۰ ، میزان اطمینان=۹۵٪ ، $\varepsilon = 10^{-14}$

پارامتر آزمون خودهمبستگی: $\tau_i = 1,2,\cdots,30$ ، پارامترهای آزمون پلکان نمودار پیچیدگی‌خطی: r=5 ، k=50 .

| آزمون | $d_1$ | $d_2$ | $d_3$ | $d_4$ | $d_5$ | $d_{10}$ | $d_{15}$ | $d_{5,8}$ |
|---|---|---|---|---|---|---|---|---|
| فرکانس | ۹۶۷ | ۹۵۷ | ۹۶۱ | ۹۵۲ | ۹۶۳ | ۹۲۹ | ۹۵۱ | ۹۷۰ |
| سریال | ۹۵۹ | ۹۵۶ | ۹۵۳ | ۹۶۰ | ۹۶۰ | ۹۲۶ | ۹۲۸ | ۹۶۵ |
| رنها | ۹۲۷ | ۹۵۵ | ۹۲۸ | ۹۵۳ | ۹۶۱ | ۹۵۱ | ۹۳۷ | ۹۲۹ |
| گپهاوبلوکها | ۹۵۶ | ۹۶۰ | ۹۶۱ | ۹۵۸ | ۹۵۹ | ۹۶۴ | ۹۴۰ | ۹۷۹ |
| پوکر | ۹۴۷ | ۹۴۷ | ۹۵۲ | ۹۲۸ | ۹۵۵ | ۹۳۷ | ۹۶۰ | ۹۷۰ |
| مشتقات باینری | ۹۵۶ | ۹۴۶ | ۹۵۰ | ۹۵۰ | ۹۵۲ | ۹۵۴ | ۹۳۸ | ۹۴۶ |
| خودهمبستگی | ۹۵۵ | ۹۶۵ | ۹۲۳ | ۹۶۰ | ۹۵۶ | ۹۵۵ | ۹۲۵ | ۹۴۶ |
| پلکان پیچیدگی خطی | ۹۳۷ | ۹۳۸ | ۹۳۸ | ۹۲۴ | ۹۲۰ | ۹۲۶ | ۹۳۳ | ۹۲۸ |

جدول (۶-۲) :

| آزمون | $b_1$ | $b_2$ | $b_3$ | $b_4$ | $b_5$ | $b_{20}$ | $b_{40}$ | $b_{40,8}$ |
|---|---|---|---|---|---|---|---|---|
| فرکانس | ۹۵۱ | ۹۴۰ | ۹۶۹ | ۹۲۹ | ۹۴۷ | ۹۲۱ | ۹۵۹ | ۹۲۲ |
| سریال | ۹۵۱ | ۹۴۷ | ۹۵۸ | ۹۵۷ | ۹۶۲ | ۹۴۷ | ۹۵۸ | ۹۱۴ |
| رنها | ۹۳۷ | ۹۵۴ | ۹۲۸ | ۹۵۸ | ۹۵۱ | ۹۵۲ | ۹۶۵ | ۹۰۲ |
| گپهاوبلوکها | ۹۶۷ | ۹۶۰ | ۹۶۷ | ۹۶۴ | ۹۷۶ | ۹۶۵ | ۹۷۱ | ۹۵۷ |
| پوکر | ۹۴۸ | ۹۵۵ | ۹۶۲ | ۹۵۴ | ۹۶۰ | ۹۴۷ | ۹۵۸ | ۹۳۱ |
| مشتقات باینری | ۹۳۵ | ۹۴۳ | ۹۵۲ | ۹۲۸ | ۹۴۲ | ۹۵۰ | ۹۵۴ | ۹۲۱ |
| خودهمبستگی | ۹۲۵ | ۹۲۵ | ۹۵۰ | ۹۵۴ | ۹۴۶ | ۹۴۷ | ۹۳۹ | ۹۰۱ |
| پلکان پیچیدگی خطی | ۹۴۴ | ۹۴۰ | ۹۵۳ | ۹۴۶ | ۹۳۸ | ۹۴۷ | ۹۲۹ | ۹۲۷ |

جدول(۶-۳) : نتایج آزمونهای مختلف بر روی نگاشت: مثلثی ، طول دنباله=۱۰۰۰ بیت ، تعداد دنباله=۱۰۰۰ ، میزان اطمینان=۹۵٪ ، $\varepsilon = 10^{-14}$

پارامتر آزمون خودهمبستگی: $\tau_i = 1,2,\cdots,30$ ، پارامترهای آزمون پلکان نمودار پیچیدگی‌خطی: r=5 ، k=50 .

| آزمون | $d_1$ | $d_2$ | $d_3$ | $d_4$ | $d_5$ | $d_{10}$ | $d_{15}$ | $d_{5,8}$ |
|---|---|---|---|---|---|---|---|---|
| فرکانس | ۹۳۸ | ۹۳۳ | ۹۵۲ | ۹۴۰ | ۹۵۲ | ۹۵۹ | ۹۵۰ | ۹۴۷ |
| سریال | ۹۴۵ | ۹۴۶ | ۹۶۲ | ۹۵۸ | ۹۴۶ | ۹۵۶ | ۹۵۵ | ۹۲۳ |
| رنها | ۹۳۶ | ۹۴۳ | ۹۶۱ | ۹۶۲ | ۹۴۳ | ۹۲۲ | ۹۵۵ | ۹۳۳ |
| گپهاوبلوکها | ۹۷۵ | ۹۵۸ | ۹۶۶ | ۹۷۳ | ۹۶۳ | ۹۵۲ | ۹۷۱ | ۹۴۶ |
| پوکر | ۹۴۶ | ۹۲۱ | ۹۵۵ | ۹۶۰ | ۹۵۵ | ۹۵۹ | ۹۳۶ | ۹۴۷ |
| مشتقات باینری | ۹۲۶ | ۹۴۷ | ۹۲۹ | ۹۵۳ | ۹۲۵ | ۹۵۰ | ۹۴۰ | ۹۳۹ |
| خودهمبستگی | ۹۵۸ | ۹۶۲ | ۹۳۸ | ۹۲۹ | ۹۳۳ | ۹۳۳ | ۹۶۰ | ۹۲۸ |
| پلکان پیچیدگی خطی | ۹۴۰ | ۹۲۹ | ۹۳۸ | ۹۲۲ | ۹۴۵ | ۹۶۷ | ۹۴۸ | ۹۵۴ |

جدول (۶-۴) :

| آزمون | $b_1$ | $b_2$ | $b_3$ | $b_4$ | $b_5$ | $b_{20}$ | $b_{40}$ | $b_{40,8}$ |
|---|---|---|---|---|---|---|---|---|
| فرکانس | ۹۴۰ | ۹۴۴ | ۹۵۱ | ۹۲۸ | ۹۲۱ | ۹۲۱ | ۹۶۹ | ۹۳۹ |
| سریال | ۹۴۱ | ۹۵۱ | ۹۶۶ | ۹۲۳ | ۹۲۹ | ۹۳۷ | ۹۵۷ | ۵۹۴ |
| رنها | ۹۲۹ | ۹۴۲ | ۹۶۱ | ۹۲۸ | ۹۴۴ | ۹۲۸ | ۹۴۷ | ۵۲۸ |
| گپهاوبلوکها | ۹۶۷ | ۹۷۰ | ۹۷۰ | ۹۶۹ | ۹۶۳ | ۹۷۱ | ۹۷۳ | ۲۸۷ |
| پوکر | ۹۵۵ | ۹۵۱ | ۹۲۹ | ۹۴۴ | ۹۶۲ | ۹۹۵ | ۹۷۰ | ۴۰۷ |
| مشتقات باینری | ۹۴۶ | ۹۵۲ | ۹۴۲ | ۹۵۵ | ۹۵۲ | ۹۴۴ | ۹۴۶ | ۲۲۷ |
| خودهمبستگی | ۹۶۳ | ۹۴۱ | ۹۲۹ | ۹۴۶ | ۹۵۳ | ۹۴۴ | ۹۳۳ | ۲۲۵ |
| پلکان پیچیدگی خطی | ۹۵۲ | ۹۳۳ | ۹۲۵ | ۹۳۳ | ۹۲۵ | ۹۲۵ | ۹۲۵ | ۹۳۴ |

## ۷- مراجع

[۱] محمد دخیل‌علیان "*ارزیابی دنباله‌های شبه تصادفی و طراحی مولدهای آشوبی*" ، دانشگاه صنعتی اصفهان، دانشکدهٔ برق و کامپیوتر، رسالهٔ دکرا ، آبان ۱۳۷۷.

*[2] Schineir B.*, Applied Cryptography, *John Wiley & Son Inc. New York, 1996.*

*[3] Devaney R.L.*, An Introduction to Chaotic Dynamically Systems, *Second Edition,Addison Wesley, 1989.*

*[4] Schuster H.G.*, Deterministic Chaos, *Third augmented edition, Weiheim, New York, VCH, 1995.*

*[5] Walker W.T.*, Chaotic Pseudo-Random Sequences and Radar, *Ph.D. Thesis University of Arizona, 1993.*