This document is a an assignment report for the Advance Digital Communication Course, Fall 2007
Isfahan University of Technology, Isfahan, Iran - Instructor Prof. Omidi

معرفی کدی جدید و مفید برای CDMA با استفاده از

T-functions

آرش میرزائی محمدرضا عطائی نائینی

چکیده

کلمهٔ کانال[1] اصطلاحاً به راه ارتباطی گفته می‌شود که هر کاربر را به شبکه مرتبط می‌سازد و این کانال باید به گونه‌ای باشد که تداخل[2] ارتباط دیگر کاربران با شبکه در ارتباط کاربر مورد نظر با شبکه حتی‌المقدور ناچیز باشد. بنابراین کانالها باید اصطلاحاً متعامد[3] باشند. متداول‌ترین روشهای ایجاد این تعامد عبارتند از: استفاده از کانالهای فرکانسی مختلف استفاده از قاب های زمانی[4] مختلف در باند فرکانسی و استفاده از کدهای مجزا[5]. این سه روش امکان دسترسی همزمان چندین کاربر را به شبکه فراهم می نمایند که به ترتیب با نامهای دسترسی چندگانه با تقسیم فرکانس (FDMA)[6]، دسترسی چندگانه با تقسیم زمانی (TDMA)[7] و دسترسی چندگانه با تقسیم کد (CDMA)[8] شناخته می‌شوند.

در این مقاله به روش سوّم پرداخته می‌شود و سعی می گردد علاوه بر معرفی کد مبتنی بر شیفت رجیستر با فیدبک خطی[9] LFSR، یک نوع کد جدید مبتنی بر نرم‌افزار با استفاده از T-functions[10] معرفی و خواص آن بررسی گردد.

---

1 Channel
2 Interference
3 Orthogonal
4 Time Slots
5 Distinct Codes
6 Frequency Division Multiple Access
7 Time Division Multiple Access
8 Code Division Multiple Access
9 Linear Feedback Shift Register
10 Triangular Functions

1- مقدمه

کدهای مورد استفاده در CDMA باید متعامد باشند، از طرفی اعمال کامل این تعامد با استفاده از کدی همانند کد WALSH دارای محدودیت‌هایی مانند تعداد محدود کد می‌باشد[1] به طور مثال با 128 بیت تنها می‌توان 128 کد متعامد ایجاد نمود. در نتیجه تعداد کاربرانی که همزمان می‌توانند به شبکه متصل گردند به 128 محدود می‌گردد. پس در عمل از کدهای شبه تصادفی یا شبه نویز[1] استفاده می‌شود یعنی کدهایی که شبیه نویز می‌باشند و همبستگی متقابل[2] بین بیتهای آن اندک می‌باشد. همانطور که ذکر شد توسط روشهای مختلفی از جمله با استفاده از LFSR ایجاد می‌شوند که استفاده از این روش مستلزم استفاده از سخت افزار می‌باشد. در این مقاله به معرفی کدی مبتنی بر نرم‌افزار پرداخته می‌شود و بررسی می‌گردد که تا چه حد این نوع کد، خواص مورد نیاز برای یک کد شبه نویز را برآورده می‌سازد.

علاوه بر نرم‌افزاری بودن این نوع کد، فایدهٔ دیگر آن اینست که می‌توان در سیستم رمزنگاری استفاده شده در شبکه از این نوع کد بهره جست، زیرا کد جدید نسبت به کد مبتنی بر LFSR بسیار امن‌تر است و سیستم رمزنگاری مبتنی بر کد جدید می‌تواند نسبت به سیستم مبتنی بر دنبالهٔ تولید شده توسط LFSR امن‌تر باشد.

2- کاربرد LFSR در CDMA :

دسترسی چندگانه با تقسیم کد CDMAسوّمین روش دسترسی چندگانه استفاده شده در سیستم‌های مختلف بی‌سیم (از جمله سیستم‌های سلولی) می‌باشد. این روش دسترسی، بر مبنای تکنولوژی پهن باند بنا شده است و ابتدا به منظور ارتباطات نظامی ایجاد گردید.

تعامد مورد نیاز در حالت CDMA ، توسط تخصیص کدهای دیجیتالی مجزا به هر کاربر، اعمال می‌گردد. کدها به گونه‌ای انتخاب می‌شوند که با یکدیگر متعامد باشند یعنی اگر کد iام یک دنبالهٔ l بیتی باشد و با $\{x_{ik}\}$ $K=1, 2, \ldots, l$ نشان داده شود، هر x_{ik} برابر $+1$ و -1 باشد و کل این دنبالهٔ $\{x_{ik}\}$ توسط کد C_i نشان داده شود داشته باشیم:

$$C_i.C_j = \sum_k x_{ik}\, x_{jk} = 0 \qquad , \quad j \neq i \qquad (1)$$

---

[1] Pseudo Noise

[2] Cross Correlation

بنابراین چندین کاربر در صورتیکه هر یک کد مختلفی را داشته باشند می‌توانند به طور همزمان به شبکه مرتبط گردند. یک گیرنده می‌تواند با داشتن کد i به تولید مجدد سیگنال دریافتی بپردازد. تنها در صورتیکه سیگنال مورد نظر برای او ارسال شده باشد می‌تواند سیگنال را به طور مناسب دریافت نماید. زیرا با وجود تعامد، سیگنال‌های دیگر که برای او ارسال نشده‌اند و دارای کد i نیستند با ضرب در کد i حذف می‌گردند. همانطور که ذکر شد می‌توان از دنبالهٔ شبه تصادفی استفاده نمود که رابطهٔ (1) را به طور کامل برقرار نمی‌سازد ولی تضمین می‌نماید که این همبستگی متقابل در حالت i=j برابر 1 ودر غیر اینصورت عدد خیلی کوچکی می‌باشد. این دنبالهٔ شبه تصادفی را می‌توان توسط شیفت رجیستر ایجاد نمود

هر بیت از اطلاعات در دنبالهٔ شبه تصادفی ضرب می‌شود. هر بیت از دنبالهٔ شبه تصادفی یک chip نامیده می‌شود و دارای طول زمانی T_c می‌باشد که بسیار کوچکتر از طول بیت اطلاعات یعنی $\frac{1}{R}$ است پس $T_C << 1/R$. اثر ضرب بیتهای اطلاعات در دنبالهٔ شبه تصادفی تبدیل دنبالهٔ بیتهای اطلاعات به یک دنبالهٔ شبه نویز با پهنای باند سیار پهنتر می‌باشد. که این اثر باعث استفاده از نام مخابرات پهن باند برای CDMA می‌شود. پهنای باند w برای دنبالهٔحاصله از این ضرب تقریباً برابر $1/T_C$ می‌باشد. پس پهنای باند دنبالهٔ اطلاعات ابتدایی در W/R ضرب می‌گردد که این ضریب، بهرهٔ گسترش[1]نام دارد. این ضریب هر چه بزرگتر باشد عملکرد سیستم CDMA بهینه‌تر می‌شود.

در گیرنده با ضرب دنبالهٔ دریافتی در دنبالهٔ شبه تصادفی دنبالهٔ بیتهای اطلاعات بازسازی می‌گردند و سیگنالهای حاصل از کدهای دیگر بخاطر تعامد بین کدها پس از ضرب کد مربوط به کاربر مورد نظر در گیرنده حذف می‌گردند.

این دنبالهٔ شبه تصادفی، توسط شیفت رجیستر با فیدبک خطی و با طول بیشینه[2]تولید می‌گردد. رابطهٔ تولید کد برای یک شیفت رجیستر با طول nبه صورت زیر است:

$$a_m = \sum_{i=1}^{n} C_i a_{m-i} \qquad C_i = 0,1;\ C_n = 1 \qquad (2)$$

که a_m، m امین بیت تولید شده می‌باشد.

---

[1] Spreading Gain

[2] Maximal length LFSR

توجه گردد که بیتها بصورت 0و 1 می‌باشند که می‌توان صفرها را به 1- تبدیل نمود تا تبدیل به دنباله‌ای با مقادیر ± 1 گردد. البته می‌توان از 0 و 1 استفاده نمود ولی در رابطهٔ (1) ضرب‌ها به xor تبدیل می‌شوند.یک شیفت رجیستر با طول بیشینه دارای پریود $P=2^n-1$ می‌باشد.

برای آنکه بتوان یک دنباله را شبه تصادفی نامید لازم است آن دنباله سه معیاری را که در ادامه ذکر خواهد شد برآورده سازد. می توان مشاهده نمود که دنبالهٔ تولید شده توسط LFSR نیز این معیارها را برآورده می سازد ([ ] Pr به معنای احتمال [ ] می باشد).ذکر این نکته ضروری است که این معیارها،شرایط کافی برای شبه تصادفی بودن دنباله نمی باشند.

1- احتمال بیت‌های صفر و یک در یک پریود تقریباً برابر باشند. که در دنبالهٔ تولید شده توسط LFSR داریم.

$$\Pr[0]=\frac{1}{2}(1-\frac{1}{P});\ \Pr[1]=\frac{1}{2}(1+\frac{1}{P}) \qquad (3)$$

برای $n\geq 10$ چون $\frac{1}{P}\leq 10^{-3}$ داریم

$$\Pr[0]\cong\Pr[1]\cong\frac{1}{2} \qquad (4)$$

2- تعداد دنباله‌های 0 یا 1 متوالی (run) با طول l برای یک دنبالهٔ تصادفی برابر است با $\frac{1}{2^l}$ برای $l\leq n-1$ و $\frac{1}{2^{n-l}}$ برای $l=n$ برای مثال در یک دنبالهٔ تصادفی $\frac{1}{2}$ همهٔ run ها طولی برابر 1 دارند، $\frac{1}{4}$ همهٔ run ها طولی برابر 2 دارند و $\frac{1}{8}$ همهٔ runها طول 3 دارند و به همین ترتیب $\frac{1}{2^{n-l}}$ همهٔ runها طول n-1 و همچنین nدارند.دنبالهٔ تولید شده توسط شیفت رجیستر با طول بیشینه این خاصیت را دارا است.

3-در صورتیکه یک دنبالهٔ تصادفی به تعداد چند عنصر شیفت یابد دنبالهٔ جدید و دنبالهٔ اوّلیه دارای تعداد عناصر مشابه و غیر مشابه برابر می‌باشند. در شیفت رجیستر با طول بیشینه تعداد عناصر نامشابه همواره برای هر تعداد شیفت یک عدد بیشتر از تعداد عناصر مشابه می‌باشد.

مشخصهٔ اخیر، معیاری برای مشخص نمودن بهینگی ساختار کدهای متعامد در CDMA می‌باشد. برای مثال همانطور که ذکر شد در شیفت رجیستر با طول بیشینه به راحتی رابطهٔ زیر اثبات می گردد.

$$\frac{1}{P}\sum_{k=1}^{P}x_{i,k}\,x_{j,k}=\frac{1}{P}\sum_{k=1}^{P}x_{i,k}\,x_{i,k+l}=-\frac{1}{P}\ ,\ l>0;=1,\ l=0 \qquad (5)$$

که تساوی اوّل از آنجا ناشی می‌شود که دو دنبالهٔ مختلف با پریود کامل (P)در یک شیفت رجیستر با طول بیشینه شیفت یافتهٔ یکدیگر می‌باشند و تساوی دوّم از اختلاف تعداد عناصر مشابه و غیر مشابه در این دو دنباله به میزان یک واحد ناشی می‌شود. پس با توجه به رابطهٔ اخیر در دنباله‌های تولید شده توسط شیفت رجیستر با طول بیشینه، نسبت سیگنال به نویز(تداخل) SIR[1] برای هر کاربر اضافی برابر P می‌باشد. پس برای بالا بردن این نسبت می‌توان طول شیفت رجیستر (n) و در نتیجه پریود (P)را افزایش داد که هزینه‌ای که در مقابل باید صرف نمود کاهش طول T_c chip و در نتیجه افزایش پهنای باند می‌باشد.

1-3 کاربرد T-functions در CDMA

کدهای مبتنی بر LFSR به صورت سخت‌افزاری بهینه هستند و همانطور که ذکر شد مشخصات اولیه دنبالهٔ شبه تصادفی را دارا هستند. در این قسمت کدی جدید معرفی می‌گردد که همانند کدهای مبتنی بر LFSR توسط یک رابطهٔ بازگشتی تولید می‌گردد یعنی حالت فعلی دنباله توسط حالت قبلی مشخص می‌گردد ولی کد جدید توسط یک رابطهٔ بهینه برای نرم‌افزار تولید می‌شود و می‌توان توسط چند عملگر سادهٔ بولی و حسابی (دستورالعمل‌های پایهٔ ماشین) توسط میکرو پروسسورهای مدرن آنها را تولید نمود.

در تعاریفی که در ادامه ذکر خواهند شد سمبل x یک بردار nبیتی $([x]_{n-1}, [x]_{n-2}, \ldots, [x]_0)$ در B^n و به پیمانهٔ 2^n می‌باشد که خود B نیز مشخص کنندهٔ مجموعهٔ {0,1} است.

تعریف 1: در صورتیکه x و y متغیرهای n بیتی باشند. یک تابع $\phi : B^{k\times n} \longrightarrow B^n$، تابع بنیادین نامیده می‌شود اگر k=1 باشد و $\phi(x)$ یکی از عملگرهای منفی سازی $\phi(x) = -x(\mathrm{mod}\,2^n)$ و مکمل‌سازی $[\phi(x)]_i = \overline{[x]_i}$ باشد یا k=2 باشد و $\phi(x,y)$ یکی از عملگرهای جمع $\phi(x,y) = x + y(\mathrm{mod}\,2^n)$، تفریق $\phi(x,y) = x - y(\mathrm{mod}\,2^n)$، ضرب $\phi(x,y) = x.y(\mathrm{mod}\,2^n)$، xor و $[\phi(x,y)]_i = [x]_i \oplus [y]_i$ AND، $[\phi(x,y)]_i = [x]_i \wedge [y]_i$ or و $[\phi(x,y)]_i = [x]_i \vee [y]_i$ باشد.

[1] Signal to Interference Ratio

مشخص است که شیفت به چپ هم از آنجا که معادل ضرب در 2 می‌باشد تابع بنیادین است ولی شیفت‌های گردشی و شیفت به راست با آنکه جزو دستورالعمل‌های پایهٔ ماشین هستند، در تابع بنیادین تعریف نمی‌گردند.

تعریف 2: یک تابع f از $B^{m\times n}$ به $B^{l\times n}$ یک T-function نامیده می‌شود اگر k امین ستون از خروجی $[\phi(x)]_{*,k-1}$ تنها به k ستون اول ورودی وابسته باشد: $[x]_{*,0},\ldots,[x]_{*,k-1}$ که $[x]_{*,i-1}$ و $[\phi(x)]_{*,i-1}$ به ترتیب نشاندهندهٔ j امین ستون ورودی و خروجی می‌باشند.

برای مثال تابع جمع $x+y=z(\mathrm{mod}2^n)$ را در نظر بگیرید. کم ارزشترین بیت حاصل تنها به کم ارزشترین بیتهای عملوندها وابسته است $[z]_0=[x]_0\oplus[y]_0$. دومین بیت به بیتهای اول و دوم عملوندها بستگی دارد $[Z]_1=[x]_1\oplus[y]_1\oplus\alpha$ که بیت α نقلی به دومین بیت می‌باشد و توسط کم‌ارزشترین بیتهای x و y مشخص می‌شود و رابطه‌ای مشابه برای همهٔ بیتهای دیگر بین عملوندها و نتیجهٔ آنها برقرار است. پس عملگر جمع T-function می‌باشد به همین ترتیب همهٔ توابع بنیادین مذکور در تعریف (1)، T-function هستند، و به راحتی قابل اثبات است که ترکیب آنها با یکدیگر نیز T-functions می‌باشد[2]و[3]و[4].

لم 1: اگر $\circ$ یک تابع بولی و a و b کلمات n بیتی و $i>0$ باشد داریم:

$$
\begin{aligned}
&[a\circ b]_0=[a]_0\circ[b]_0\\
&[a\circ b]_i=[a]_i\circ[b]_i\\
&[a+b]_0=[a]_0\oplus[b]_0\\
&[a+b]_i=[a]_i\oplus[b]_i\oplus\alpha\\
&[a-b]_0=[a]_0\oplus[b]_0\\
&[a-b]_i=[a]_i\oplus[b]_i\oplus\alpha \qquad (6)\\
&[a.b]_0=[a]_0[b]_0\\
&[a.b]_i=[a]_i[b]_0\oplus[a]_0[b]_i\oplus\alpha\\
&[a^k]_o=[a]_0 \qquad \text{برای هر } k>0\\
&[a^k]_i=[a]_i[a]_0\oplus\alpha \qquad \text{برای هر } k \text{ فرد که } k>0\\
&[a^k]_i=\alpha \qquad \text{برای هر } K \text{ زوج که } k>0
\end{aligned}
$$

که αها پارامترهایی هستند که به بیتهای قبلی وابسته هستند در کلیه‌روابط علائم یونانی نشاندهندهٔ پارامترها می‌باشند.

اثبات: تنها ادعای آخر اثبات می‌گردد – برای دیگر حالات اثبات مشابه است. از آنجا که kزوج است. از مقدار t=k/2 استفاده می‌شود و با استفاده از رابطه برای $[ab]_i$ داریم

$$[a^k]_i = [a^t a^t]_i = [a^t]_i [a^t]_0 \oplus [a^t]_i [a^t]_0 \oplus \alpha = \alpha \qquad (7)$$

حال هدف، حصول نگاشتی است که دارای کمترین تعداد تابع بنیادین و در نتیجه ساده‌ترین و در عین حال سریعترین پیاده‌سازی نرم‌افزاری باشد. نتایج آزمایش نگاشت‌های با 1 یا 2تابع بنیادین نشان می‌دهند که تنها 8 نوع نگاشت برگشت‌پذیر با 1 یا 2 تابع بنیادین وجود دارد.

x.c'، x+c، $x \oplus c$ ، $(x + c_1) \oplus c_2$، x.c'+c، x، c'⊕c، x.c''⊕x و $(x \oplus c).c'$ که c، c_1 و c_2 ثابت‌های دلخواه، c ثابت فرد دلخواه و c' ثابت زوج دلخواه می‌باشند.متأسفانه همهٔ این نگاشت‌ها یا دارای خواص تصادفی ضعیف و یا دارای حلقه های با طول کم می‌باشند. برای مثال $x \oplus c$ تنها بین دو مقدار تغییر حالت می‌دهد پس دارای یک حلقه با طول 2می‌باشد پس نیاز به استفاده از 3 تابع بنیادین ضروری است.

یک خانوادهٔ جالب از نگاشت‌ها، نگاشت $x \to x + (x^2 \vee c)$ برای ثابت‌های مختلف c و طول کلمهٔ n می‌باشد که برای ثابت های c تئوری زیر را داریم:

تئوری 1: نگاشت $f(x) = x + (x^2 \vee c)$ روی کلمات n بیتی برگشت‌پذیر است اگر و فقط اگر کم‌ارزشترین بیت c 1 باشد. و برای $n \geq 3$ جایگشتی با تنها یک حلقه می‌باشد اگر و فقط اگر اولین و سومین بیت کم ارزش c، 1 باشند.

اثبات: تنها به اثبات برگشت‌پذیری نگاشت پرداخته می‌شود و به دلیل پیچیدگی از اثبات قسمت دوم صرف نظر می‌گردد که خواننده می‌تواند برای آشنایی با روش اثبات به مرجع [2] مراجعه نماید.

$$[f(x)]_i = [x + (x^2 \vee c)]_i = [x]_i \oplus [x^2 \vee c]_i \oplus \alpha \qquad (8)$$

$$[x]_i \oplus ([x^2]_i \vee [c]_i) \oplus \alpha = [x]_i \oplus (\beta \vee \delta) \oplus \alpha = [x]_i \oplus \gamma$$

رابطه فوق نشان می‌دهد برای i>0 با داشتن بیت‌های شماره i-1,…,1,0 از x می‌توان به γ دست یافت و توسط این پارامتر و $[f(x)]_i$ به راحتی $[x]_i$ محاسبه می‌شود. که به معنی برگشت‌پذیری رابطهٔفوق است. تنها اثبات برگشت‌پذیری بیت شماره 0 باید اثبات گردد که برای این بیت داریم:

$$[f(x)]_0 = [x + (x^2 \vee c)]_0 = [x]_0 [x^2 \vee c]_0 = [x]_0 \oplus ([x^2]_0 \vee [c]_0)) \qquad (9)$$

$$= [x]_0 \oplus ([x]_0 \vee [c]_0)$$

برای آنکه رابطهٔ اخیر برگشت پذیر باشد باید بتوان از روی $[f(x)]_0$ به $[x]_0$ دست یافت.

اگر $[c]_0$ ، 0 باشد در اینصورت داریم:

$$[f(x)]_0 = [x]_0 \oplus ([x]_0 \vee 0) = [x]_0 \oplus [x]_0 = 0 \qquad (10)$$

که به طور مشخص رابطه‌ای برگشت‌پذیر بین x و f(x) و برای بیت اوّل برقرار نمی‌سازد پس باید $[c]_0$ ، 1 باشد. در اینصورت

$$[f(x)]_0 = [x]_0 \oplus ([x]_0 \vee 1) = [x]_0 \oplus 1 \qquad (11)$$

که برگشت‌پذیری رابطهٔ فوق واضح است.

اینجا دلیل استفاده از T-function مشخص می‌گردد. مشخصه اصلی T-functionعدم وابستگی بیت i ام خروجی یا حالت بعدی به بیت‌های i+1 ام ، i + 2 ام و ... و n-1 ام ورودی یا حالت فعلی می‌باشد که این باعث سهولت اثبات برگشت‌پذیری و اثبات وجود یک حلقه برای نگاشت مذکور و نگاشتهای مشابه دیگر می‌گردد و همچنین ایجاد نگاشت‌های با مشخصات دلخواه را راحتتر می‌نماید. بطور مثال، برای محاسبهٔ نگاشت برگشت، به صورت دنباله‌ای از بیت شماره 0 شروع نموده و از $[f(x)]_0$ و رابطهٔ $[f(x)]_0 = [x]_0 \oplus 1$ یا $[x]_0 = \overline{[f(x)]_0}$ ، $[x]_0$ را می‌یابیم، سپس با $[x]_0$ یافت شده γ را محاسبه نموده و توسط γ و $[f(x)]_1$ و رابطهٔ $[f(x)]_1 = [x]_1 \oplus \gamma$ یا $[x]_1 = [f(x)]_1 \oplus \gamma$، $[x]_1$ را محاسبه نموده و توسط $[x]_0$ و $[x]_1$، γ جدید را محاسبه نموده و با رابطهٔ اخیر از $[f(x)]_2$ ، $[x]_2$ محاسبه می‌گردد و به همین ترتیب x از f(x) بدست می‌آید. در عمل، نیازی به محاسبه برگشت نگاشت نمی‌باشد. تنها در اثبات برگشت‌پذیری و اثبات وجود یک حلقه در نگاشت از روابط مذکور استفاده می گردد. پس برای تولید دنبالهٔ شبه تصادفی با پریود کامل از نگاشت $x \to x + (x^2 \vee 5) (\mathrm{mod}\, 2^n)$ استفاده می‌شود نگاشت مذکور به این دلیل معرفی می‌گردد که نتایج بررسی‌ها روی این نگاشت نشان می‌دهند که دارای خواص خوب آماری است و دنبالهٔ حاصل از آن دارای خواص یک دنبالهٔ شبه تصادفی می‌باشد. به این ترتیب از یک حالت اولیه x_0 شروع نموده x_1 را با رابطه $x_1 = x_0 + (x^2 \vee 5) \bmod 2^n$ محاسبه نموده سپس با اعمال رابطهٔ اخیر بر x_1 ، x_2 محاسبه می‌شود و به همین ترتیب 2^n پریود کامل حلقه تولید می‌گردد پس از آن دوباره دنبالهٔ 2^n بیتی حاصل تکرار می‌گردد.

دنباله مذکور مشخصاً دارای حالت تمام صفر نیز می‌باشد. به همین دلیل نسبت به دنبالهٔ حاصل از LFSR با پریود 2^n-1، یک عضو بیشتر دارد. همانطور که پیش از این ذکر شد از نگاشت فوق می‌توان در سیستم رمزنگاری بکار رفته در شبکه نیز استفاده نمود چون دنبالهٔ حاصل از این نگاشت نسبت به دنبالهٔ حاصل از LFSR امن‌تر می‌باشد.

2-3 مشخصات آماری دنبالهٔ $x_1 = x_0 + (x^2 \vee 5) \bmod 2^n$

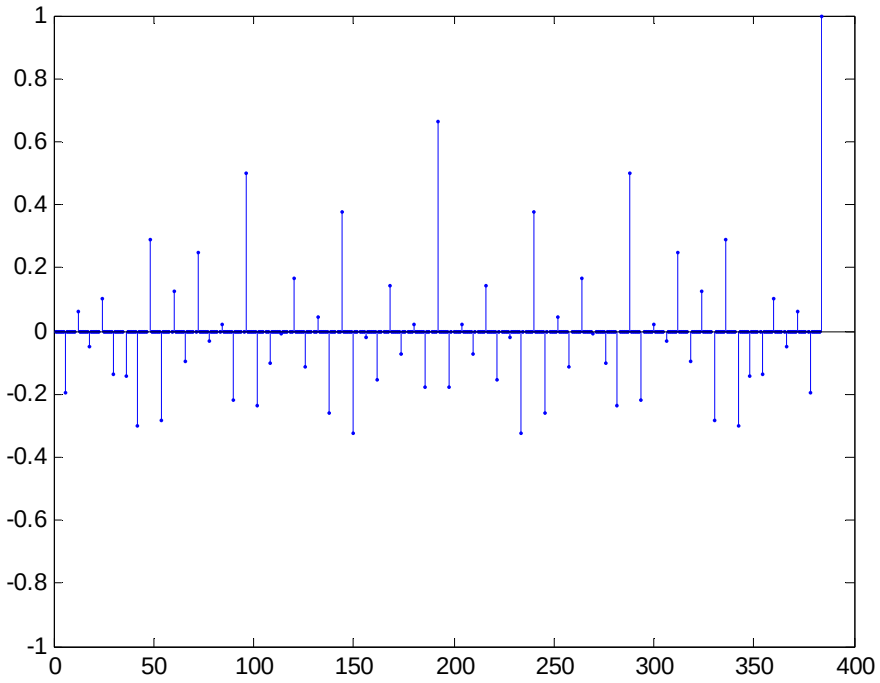
در این قسمت به بررسی خواص آماری دنبالهٔ شبه تصادفی تولید شده توسط رابطهٔ بازگشتی $x_1 = x_0 + (x^2 \vee 5) \bmod 2^n$ که تحت عنوان رابطهٔ KS از آن نام می بریم(ابتدای نام طراحان) می پردازیم.

جدول 1 دنبالهٔ اعداد تولید شده توسط این رابطه را برای n=4 و با شروع از صفر نشان می دهد.

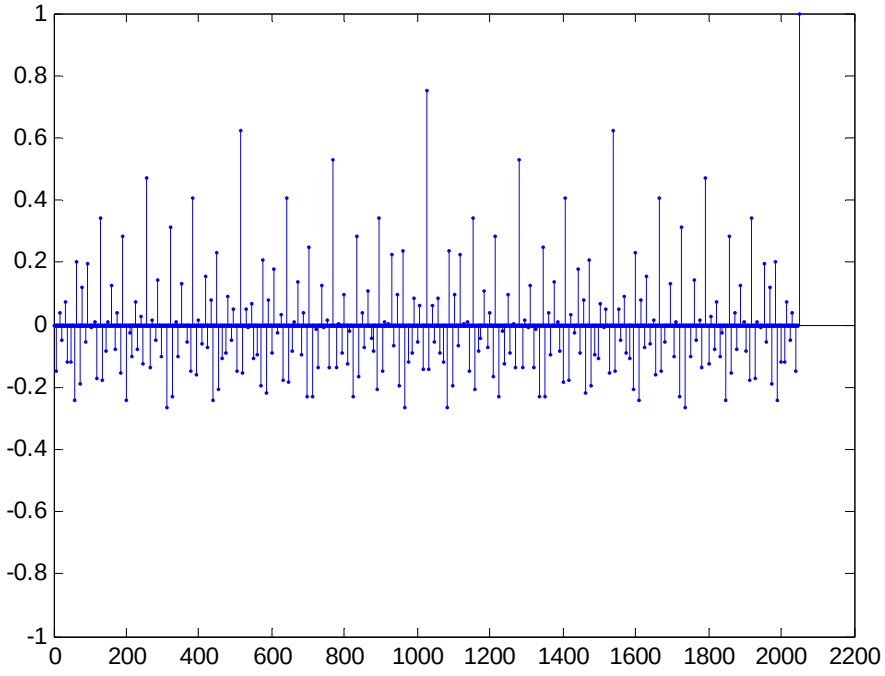
x	*f(x)*	$[f(x)]_3$	$[f(x)]_2$	$[f(x)]_1$	$[f(x)]_0$
0	5	0	1	0	1
5	2	0	0	1	0
2	7	0	1	1	1
7	12	1	1	0	0
12	1	0	0	0	1
1	6	0	1	1	0
6	11	1	0	1	1
11	8	1	0	0	0
8	13	1	0	0	1
13	10	1	1	1	0
10	15	1	0	1	1
15	4	0	0	0	0
4	9	1	1	0	1
9	14	1	0	1	0
14	3	0	1	1	1
3	0	0	1	0	0

جدول 1: مثالی از اعداد تولید شده توسط رابطهٔ KS و معادل باینری آنها

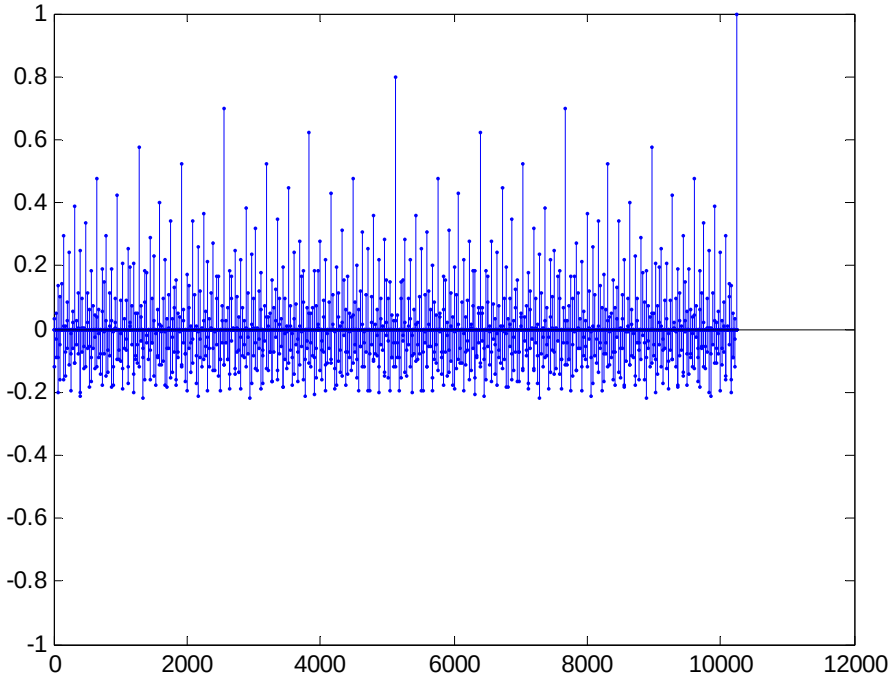
ابتدا فرض می نماییم دنبالهٔ شبه تصادفی مورد نظر با پشت سر هم نهادن معادل باینری هر عدد تولید می شود. واضح است که معیار اوّل دنباله های شبه تصادفی (تساوی تعداد 0 و 1) برای این دنباله براورده می گردد. به بررسی معیار سوَم میپردازیم. می توان مشاهده نمود که برای اعداد n بیتی هرگاه تعداد شیفت مضربی از n باشد،همبستگی دنبالهٔ اصلی و دنبالهٔ شیفت یافته عدد نسبتاً بزرگی می باشد (بوضوح کوچکتر از 1) و در غیر اینصورت این همبستگی برابر 0 می باشد.شکل های 2و3 و4 این همبستگی را بترتیب برای n=6 و n=8 و n=10 نشان می دهند.



شکل 2: $c(\tau)$ برای دنباله حاصل از پشت سر هم نهادن کلمات برای n=6



شکل3: $c(\tau)$ برای دنباله حاصل از پشت سر هم نهادن کلمات برای n=8



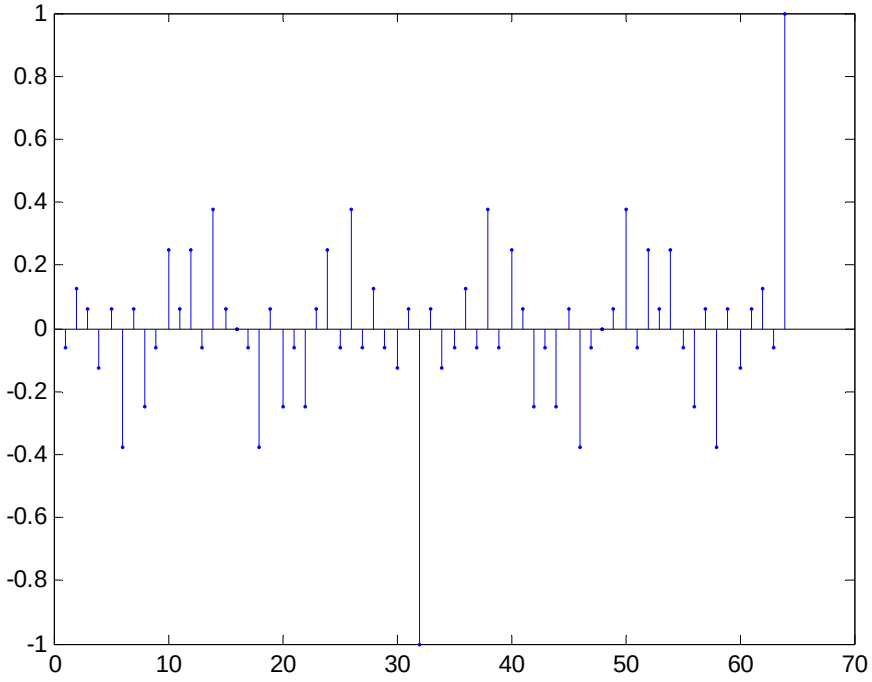
شکل4 : $c(\tau)$ برای دنباله حاصل از پشت سر هم نهادن کلمات برای n=10

مشخص است که معیار سوَم براورده نگردیده است. دلیل این مشکل نیز در جدول 1 مشخص می باشد. با نگاه مجدد به جدول 1 مشخص است که پریود کم ارزشترین بیت 2 می باشد، پریود بیت دوَم 4 می باشد،و به همین ترتیب پریود بیت iام 2^i می باشد(این مشخصه با در نظر گرفتن تعریف T-function براحتی اثبات می گردد.).پس دنبالۀ تولید شده توسط پشت سر هم نهادن معادل باینری اعداد تولید شده توسط رابطه مذکور کاملا تصادفی نیستند (به طور مثال بیت های اول هر عدد همواره معکوس می گردد) پس باید به دنبال چاره ای باشیم. یک راه حل می تواند این باشد که دنباله حاصل را از پشت سرهم نهادن بیت آخر هر عدد تولید نمود که در این صورت می توان اثبات نمود که این دنباله دارای پریود 2^n می باشد. به وضوح معیار اول دنباله های شبه تصادفی برای دنباله حاصل برآورده می گردد. جدول 2 نشان می دهد که با انتخاب $n\geq 16$, معیار دوم نیز به طور مطلوبی برآورده می شود. و اشکال 5 تا 8 نیز به ترتیب همبستگی را برای n=6 , n=8 , n=10 و n=12 نشان می دهند که مشخص است با افزایش n اعداد مربوط به هر شکل کاهش می یابد. میانگین قدرمطلق اعداد هر شکل برای اعداد n=6, n=8, n=10 و n=12 به ترتیب برابر است با 0.1719, 0.0776, 0.0409, 0.0218 و 0.0107 .

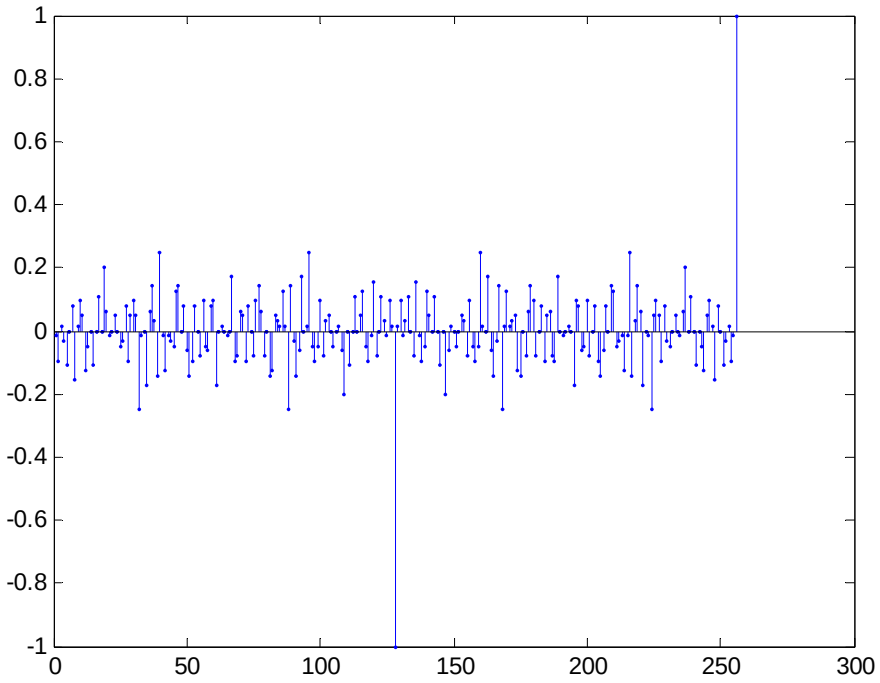
	Length →	1	2	3	4	5	6	7	8
n	Runs ↓	ratio							
8	130	0.4615	0.2615	0.1538	0.0923	0.0308	0	0	0
10	514	0.5136	0.2412	0.1284	0.0506	0.0272	0.0117	0.0156	0.0117
12	2050	0.5034	0.2400	0.1171	0.0800	0.0361	0.0107	0.0068	0.0029
14	8190	0.5004	0.2493	0.1243	0.0628	0.0291	0.0200	0.0076	0.0037
16	32770	0.5022	0.2474	0.1269	0.0592	0.0313	0.0170	0.0079	0.0040
I	∞	0.5	0.25	0.125	0.0625	0.0313	0.0156	0.0078	0.0039

	Length →	9	10	11	12	13	14	15
n	Runs ↓	ratio						
8	130	0	0	0	0	0	0	0
10	514	0	0	0	0	0	0	0
12	2050	0.0020	0.0010	0	0	0	0	0
14	8190	0.0015	0.0005	0.0005	0	0.0005	0	0
16	32770	0.0021	0.0013	0.0004	0.0001	0.0001	0	0
I	∞	0.0020	0.0010	0.0005	0.00024	0.00012	0.00006	0.00003

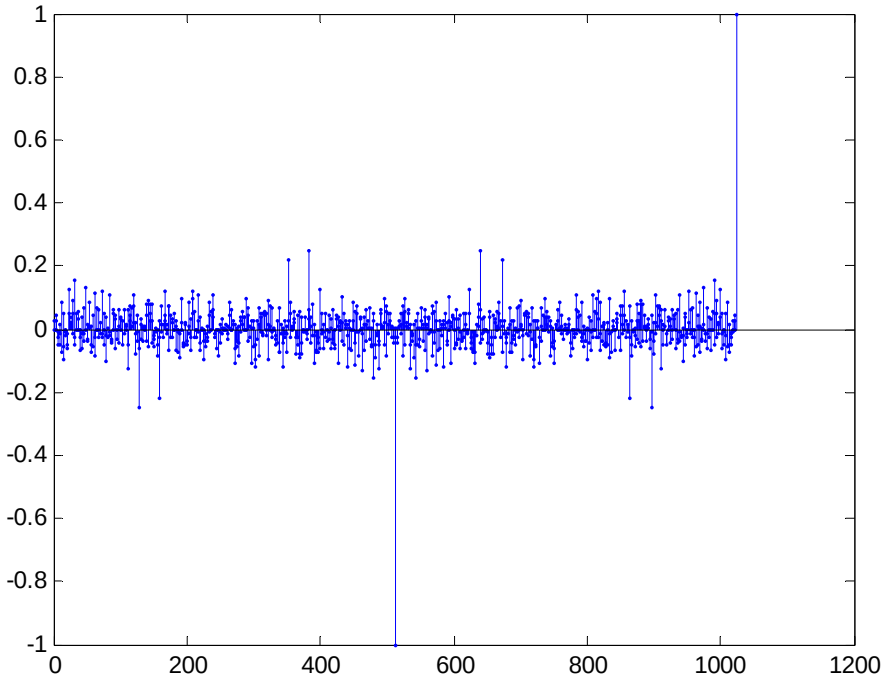
جدول2 : تعداد و نسبت runها برای دنباله حاصل از پشت سر هم نهادن بیت آخر کلمات n بیتی



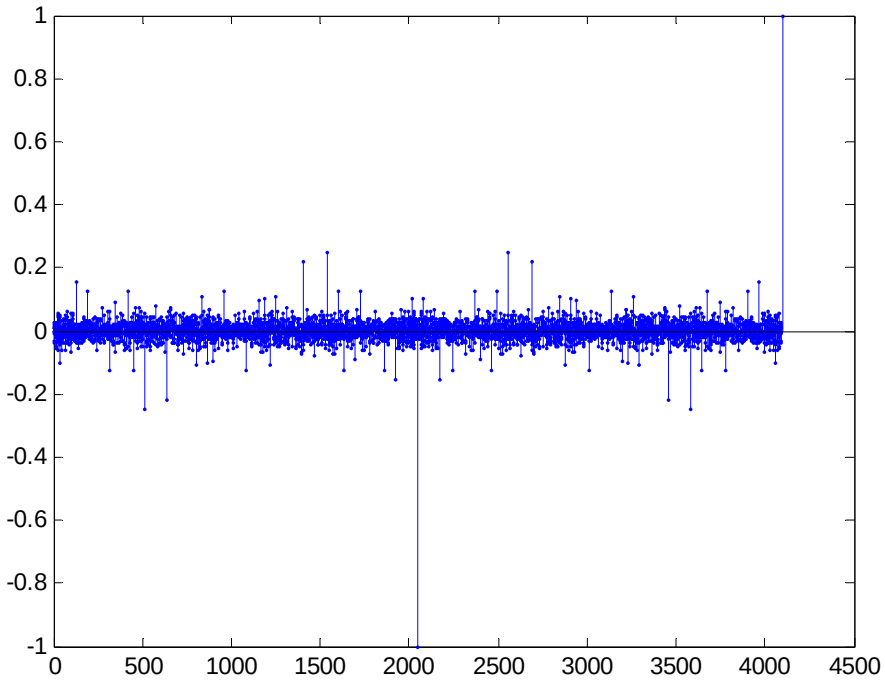
شکل5 : $c(\tau)$ برای دنباله حاصل از پشت سر هم نهادن پر ارزشترین بیت کلمات برای n=6



شکل6 : $c(\tau)$ برای دنباله حاصل از پشت سر هم نهادن پر ارزشترین بیت کلمات برای n=8

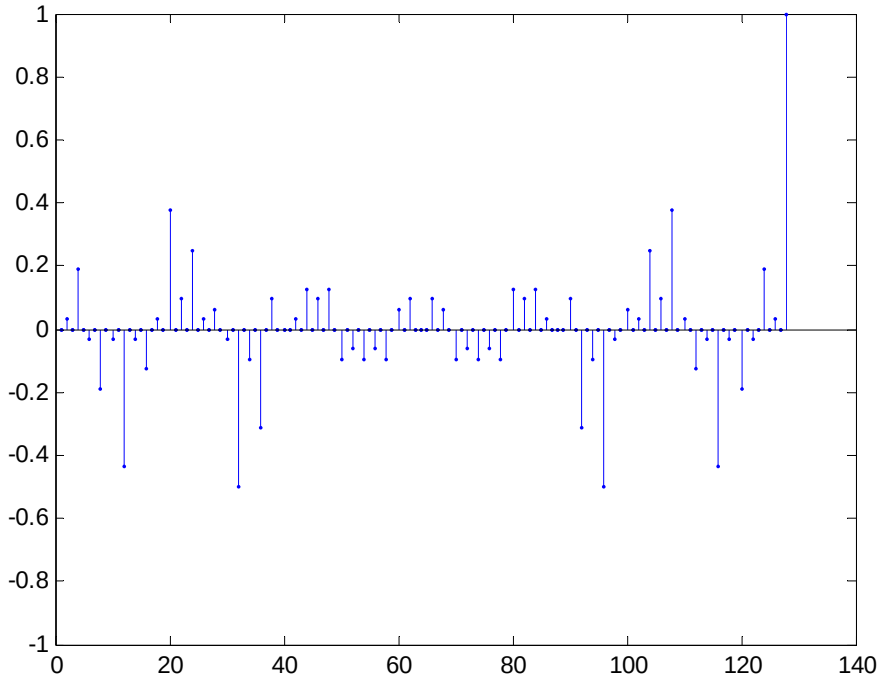


شکل7 : $c(\tau)$ برای دنباله حاصل از پشت سر هم نهادن پر ارزشترین بیت کلمات برای n=10



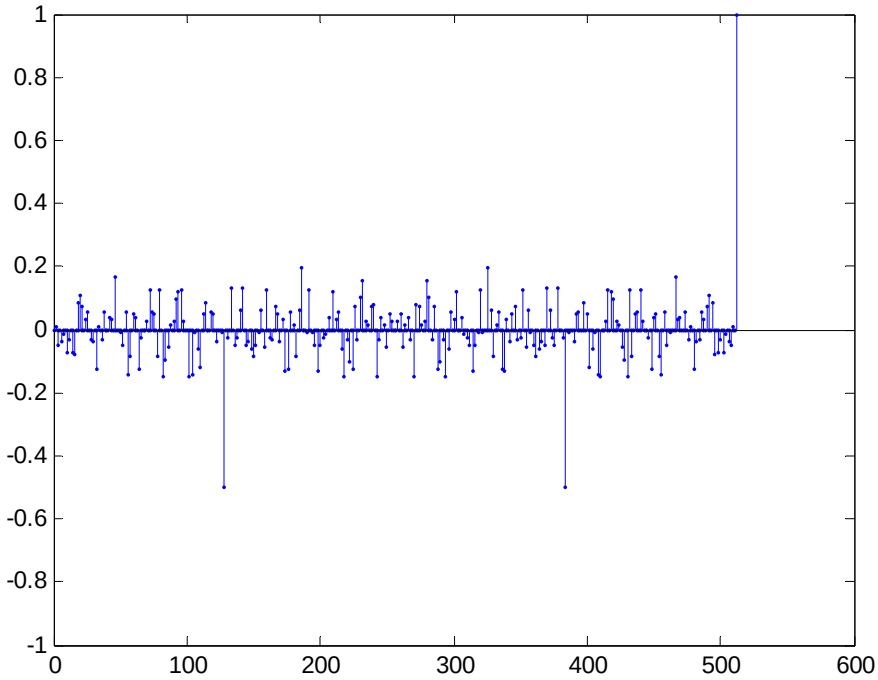
شکل 8 : $c(\tau)$ برای دنباله حاصل از پشت سر هم نهادن پر ارزشترین بیت کلمات برای n=12

دنباله اخیر نیز دارای این مشکل می باشد که نیمه دوم آن معکوس نیمه اول آن است. برای رفع این مشکل می توان دنباله را با پشت سرهم قرار دادن دو بیت پرارزش n-1 و n ام هر عدد تولید شده توسط کد مذکور ایجاد نمود, که در این صورت اشکال مربوط به همبستگی در این حالت برای اعداد n=6, n=8, n=10 و n=12 به ترتیب در اشکال 9, 10, 11 و 12 نشان داده شده اند و میانگین قدر مطلق اعداد مربوط به هر شکل به ترتیب برابر 0.0648, 0.0336, 0.0119 . 0.0093 می باشد.

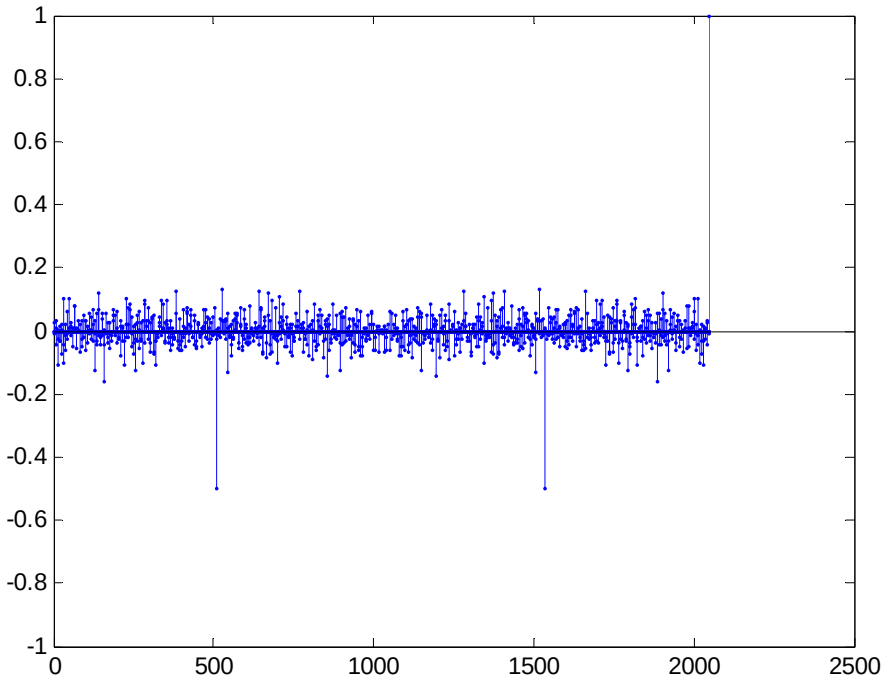


شکل 9:

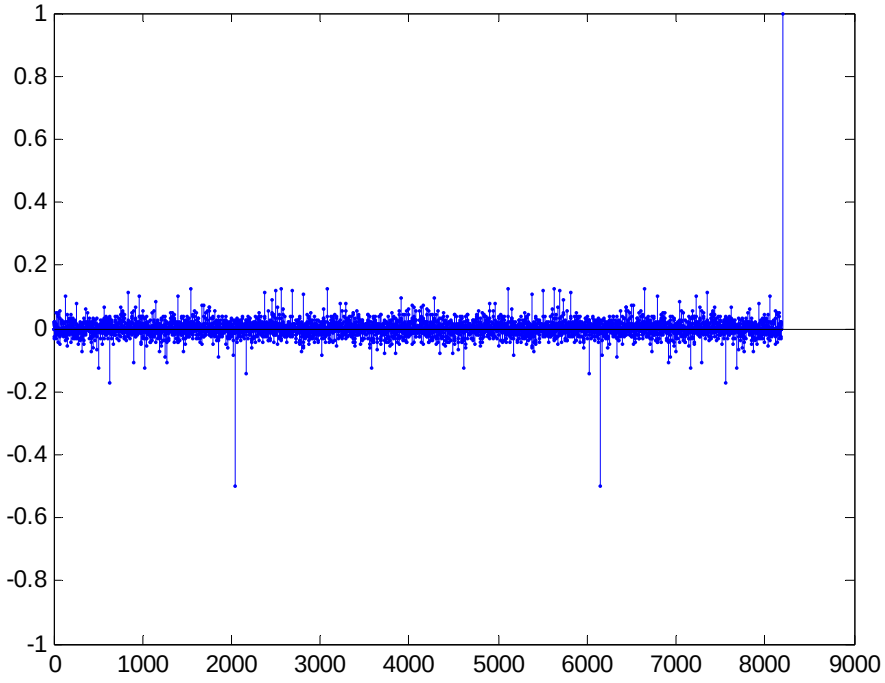
$c(\tau)$ برای دنباله حاصل از پشت سر هم نهادن 2 بیت پر ارزشتر کلمات برای n=6



شکل 10 : $c(\tau)$ برای دنباله حاصل از پشت سر هم نهادن 2 بیت پر ارزشتر کلمات برای n=8

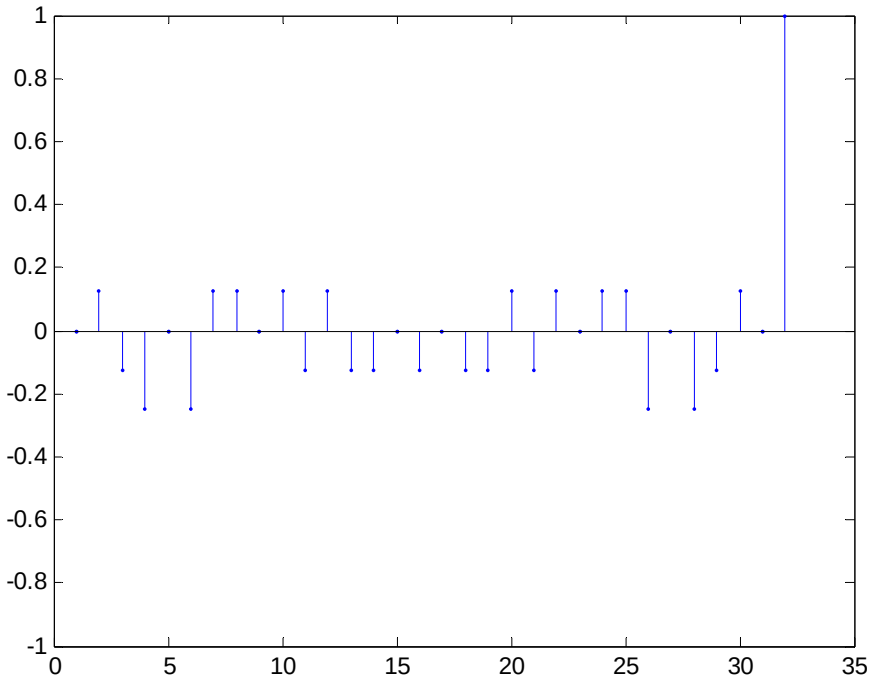


شکل 11 : $c(\tau)$ برای دنباله حاصل از پشت سر هم نهادن 2 بیت پر ارزشتر کلمات برای n=10

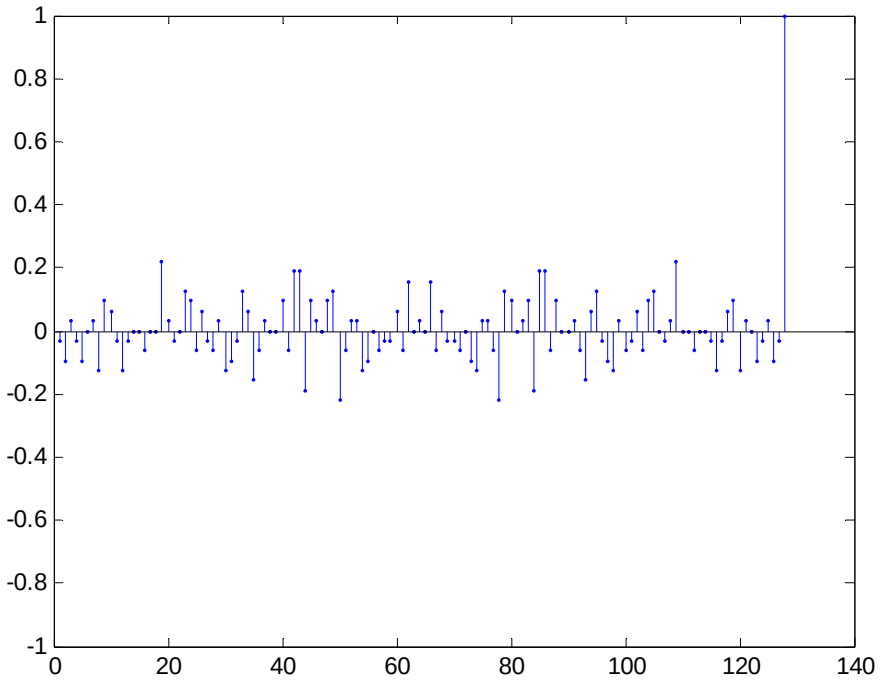


شکل 12 : $c(\tau)$ برای دنباله حاصل از پشت سر هم نهادن 2 بیت پر ارزشتر کلمات برای n=12

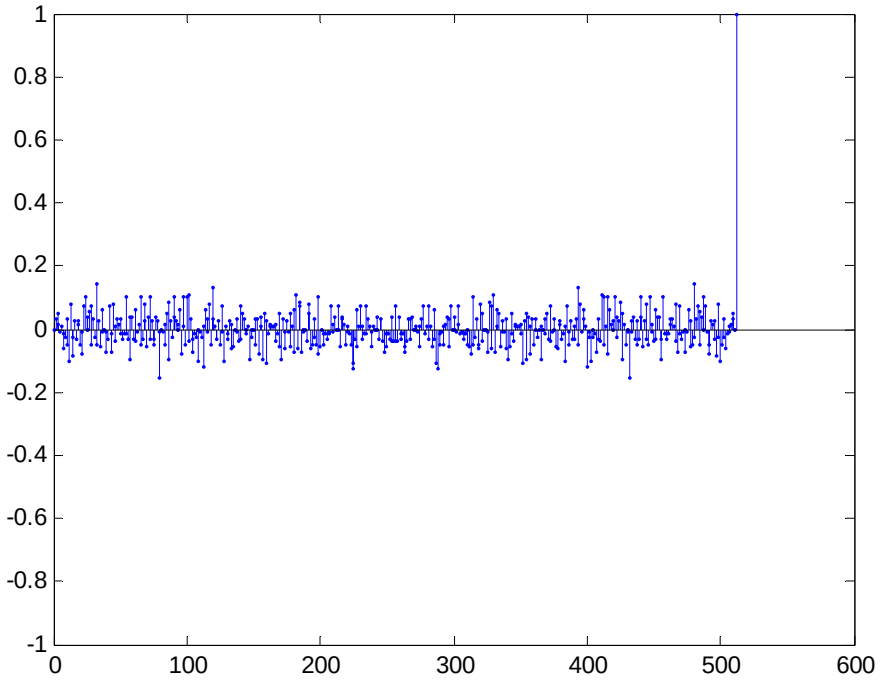
در نهایت روش نهایی که می تواند مورد استفاده قرار گیرد استفاده از تنها نیمه اول بیت های مربوط به بیت n ام اعداد تولید شده است. یعنی با بیت n ام اعداد اول تا Z^{n-1} دنباله اعداد تولید شده, دنباله شبه تصادفی پشت سرهم نهادن ایجاد می شود که به وضوح معیار اول دنباله های شبه تصادفی به طور دقیق برآورده نمی گردد ولی تغییری در معیار دوم که مثالی از آن در جدول 2 نشان داده شد ایجاد نمی گردد. اشکال مربوط به همبستگی در شکل های 13 تا 16 و برای اعداد n=6, n=8, n=10 و n=12 رسم شده اند و میانگین قدر مطلق اعداد هر شکل به ترتیب برابر با 0.1367, 0.0754, 0.0421 و 0.0200 است, که این اعداد نسبت به اعداد متناظر در شکل های 5 تا 9 به مقدار کمی کاهش نشان می دهند, و این کاهش در واریانس آنها در اشکال رسم شده نیز بوضوح آشکار می باشد.از طرف دیگر برای طول کلمات بالا (بطور مثال برای n>15)تفاوت تعداد 0و1 در نیمه اول دنباله حاصل از بیت آخر کلمات قابل صرف نظر می باشد.



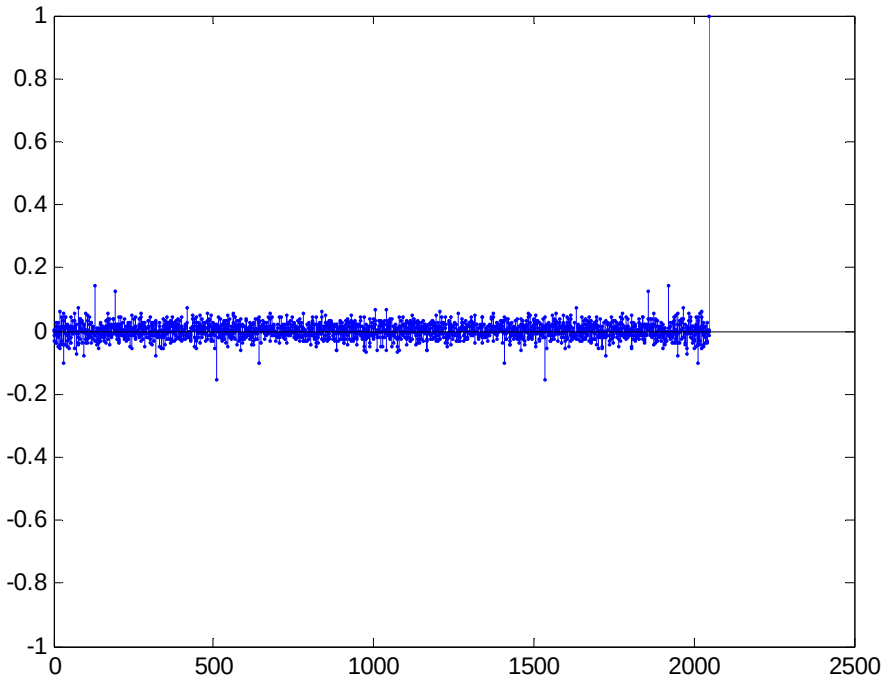
شکل 13 : $c(\tau)$ برای نیمه اول دنباله حاصل از پشت سر هم نهادن پر ارزشترین بیت کلمات برای n=6



شکل 14 : $c(\tau)$ برای نیمه اول دنباله حاصل از پشت سر هم نهادن پر ارزشترین بیت کلمات برای n=8



شکل 15 : $c(\tau)$ برای نیمه اول دنباله حاصل از پشت سر هم نهادن پر ارزشترین بیت کلمات برای n=10



شکل 16 : $c(\tau)$ برای نیمه اول دنباله حاصل از پشت سر هم نهادن پر ارزشترین بیت کلمات برای n=12

راه حل دیگری برای کاهش همبستگی بین دنباله حاصل و دنباله های شیفت یافته ترکیب دو T-function است بدین صورت که یکی دارای خاصیت T-function مذکور در این مقاله, و دیگری دقیقا دارای عکس مشخصه مذکور باشد, یعنی برای اعداد n بیتی, بیت m ام حالت بعدی یا خروجی در هر مرحله به بیت های m, m+1 و ... و n ام حالت فعلی یا ورودی بستگی داشته باشد. که این مبحث می تواند مورد مطالعه و بررسی بیشتر علاقه مندان قرار گیرد.

لازم به ذکر است که به دلیل آنکه پردازنده‌های موجود حداکثر 64 بیتی هستند کد معرفی شده در این مقاله نیز حداکثر دارای پریود 2^{64} می‌باشد بنابراین برای تولید کدی با پریود بیشتر نیاز به استفاده از T-function و اعمال آن با چند کلمه می-باشد[4]و[5]. بررسی کدهای معرفی شده در [4] و[5]نیز می‌تواند مورد بررسی بیشتر علاقمندان قرار گیرد.

نتیجه‌گیری

در این مقاله سعی شد تا دوگانی برای کدهای تولید شده توسط LFSR ارائه گردد. این کدها توسط توابعی به نام T-functions ایجاد شدند و بر خلاف LFSR بسیار بهینه برای پیاده‌سازی نرم‌افزاری می‌باشند. سپس سعی گردید تا با تغییرات

مختلف اعمال شده بر آن‌ها معیارهای اصلی و اولیهٔ دنباله‌های شبه تصادفی را برآورده سازیم و در نهایت راه حلی برای ایجاد کـد-های جدید(ترکیب دو T-function) پیشنهاد شد که یک مسئلهٔ باز می‌باشد ومی‌تواند موضوع تحقیقات بعدی قرار گیرد.

مراجع

[1] M. Schwartz 2005 " *Mobile Wireless Communication* " Cambridge University Press

[2] A. Klimov and A. Shamir, A new class of invertible mappings. *CHES 2002*, LNCS 2523, Springer-Verlag, pp.470–483, 2003.

[3] A. Klimov and A. Shamir, Cryptographic application of T-functions. *SAC 2003*, LNCS 3006, Springer-Verlag, pp.248–261, 2004.

[4] A. Klimov: Applications of T-functions in Cryptography. PhD Thesis, Weizmann Institute of Science, submitted, 2004.

[5] A. Klimov and A. Shamir, New cryptographic primitives based on multiword Tfunctions.*FSE 2004*, LNCS 3017, Springer-Verlag, pp.1–15, 2004.