

## ارائه روشی نوین برای تلفیق کدگذاری کانال و رمزنگاری مبتنی بر کدگذاری قطبی

محمد کنارکوهی<sup>۱\*</sup>، حسن توکلی<sup>۲</sup>

۱- دانشجوی کارشناسی ارشد، دانشگاه گیلان، رشت

۲- استادیار گروه برق، دانشکده فنی و مهندسی، دانشگاه گیلان، رشت

(دریافت: ۹۳/۱۰/۰۹، پذیرش: ۹۵/۰۲/۱۴)

## چکیده

در این مقاله، کدهای قطبی که به تازگی توسط Arikian ارائه گردیده، برای تلفیق کدگذاری کانال و رمزنگاری استفاده شده است. بیت‌های کد قطبی به دو دسته تقسیم می‌شوند. دسته اول بیت‌هایی می‌باشند که به‌طور مجازی از کانال‌های با ظرفیت بالا عبور می‌کنند که به اختصار بیت‌های با ظرفیت بالا نامیده می‌شوند و اطلاعات بر روی آن‌ها قرار می‌گیرد. دسته دوم بیت‌هایی می‌باشند که به‌طور مجازی از کانال‌های با ظرفیت پایین عبور می‌کنند که به اختصار "بیت‌های ثابت" نامیده می‌شوند. در طرح پیشنهادی اول از بیت‌های ثابت به عنوان کلید رمز استفاده می‌کنیم، و بر روی تمامی بیت‌های این طرح (بیت‌های اطلاعات و بیت‌های ثابت) کلید رمز قرار می‌گیرد. در واقع در طرح ۸ بیتی پیشنهادی Arikian، از ۸ کلید رمز استفاده می‌کنیم. سپس در ادامه این مقاله روشی ارائه می‌شود که توسط آن می‌توان تعداد کلید رمز اعمال شده بر روی بیت‌ها را کاهش داد. این سیستم رمزنگاری موثر و مطلوب است که در آن، علاوه بر پیچیدگی زیاد و عدم همبستگی بین بیت‌ها، از حداقل کلید رمز در آن استفاده شده باشد.

واژه‌های کلیدی: رمزنگاری، کدگذاری کانال، تلفیق رمزنگاری و کدگذاری، کدقطبی، پیچیدگی

## ۱- مقدمه

عمل تشخیص و تصحیح خطا در داده‌های ارسالی می‌کنند که این امر باعث کاهش خطای کل سیستم می‌شود [۴].

یکی دیگر از دلایل کدگذاری کانال مقابله با عوامل مخربی مانند نویز بر روی پیام ارسالی است. کدگذاری کانال برای غلبه بر این مشکلات ایجاد شده است. با توجه به مطالب بیان شده و برای مقابله با حملات دشمن و همچنین برای کاهش اثرات نویز بر روی پیام، تلفیق رمزنگاری و کدگذاری کانال مورد بررسی قرار می‌گیرد که این امر باعث کاهش خطا و همچنین حفظ ساختار اصلی پیام می‌شود [۵].

استفاده همزمان از رمزنگاری و کدگذاری کانال در شکل (۱) نمایش داده شده است. استفاده توأم و ترکیبی هر دو بلوک رمزنگاری و کدگذاری کانال، برای پیام‌های ارسالی در طرف فرستنده، و رمزگشایی آن در طرف گیرنده، امری است که باعث بهبود امنیت و حفظ ساختار پیام می‌شود.

در ادامه مقاله به بررسی تلفیق کدگذاری و کدینگ می‌پردازیم و با بررسی کدهای قطبی در بخش سوم، دو طرح پیشنهادی خود را در بخش‌های چهارم و پنجم ارائه می‌دهیم.

رمزنگاری علم و روشی برای بررسی اصول و روش‌های ارسال و ذخیره‌سازی اطلاعات به صورت امن می‌باشد. در واقع، رمزنگاری دانش استفاده از روش‌های ریاضی برای برقراری و ایجاد امنیت برای اطلاعات است. در اصل، رمزنگاری دانش تغییردادن متن اصلی پیام یا اطلاعات اصلی به کمک کلید رمز با استفاده از یک الگوریتم رمزنگاری است. بر طبق اصل دوم کرکهف، امنیت یک سیستم رمزنگاری تنها مبتنی بر کلید رمزنگاری، نه سیستم رمزنگاری، می‌باشد [۱-۲].

از طرف دیگر، برای داشتن ارتباطی بدون خطا یا به طور معادل انتقال و ارسال اطلاعات بدون خطا یا با کمترین خطا باید از کدهای کنترل خطا استفاده نمود. "کدگذاری کانال" در واقع استفاده از کدهای کنترل خطا می‌باشد [۳]. در اصل، کدگذاری کانال با ایجاد قالب‌های تابعی، عمل کدگذاری کنترل خطا را انجام می‌دهد. کدکننده کانال به روش اصولی تعدادی بیت را به بیت‌های پیام ارسالی اضافه می‌کند. این بیت‌های اضافی در حالی که خودحامل هیچ گونه اطلاعات اضافی نیستند، کمک به

جلوگیری شود [۷-۸].

از دیگر سو، در ارسال یک پیام ممکن است اطلاعات ارسالی که در فرستنده رمز و کد شده اند در عبور از بخش های مختلف با کدهای تصحیح خطای متفاوت، بر حسب پروتکل مورد استفاده بین بخش های متفاوت، مواجه شود ولی تنها در مقصد نهایی است که رمزگشایی می گردد. با توجه به بار محاسباتی و زمان مورد نیاز در هر بار اجرای عملیات رمزنگاری و رمزگشایی در الگوریتم های رمزنگاری، بحث تأمین امنیت اعتبار یک چالش جدی به نظر می رسد. سیستم های رمزنگاری مبتنی بر تئوری کدگذاری از این لحاظ نسبت به دیگر سیستم های رمزنگاری برتری دارند [۹-۱۲].

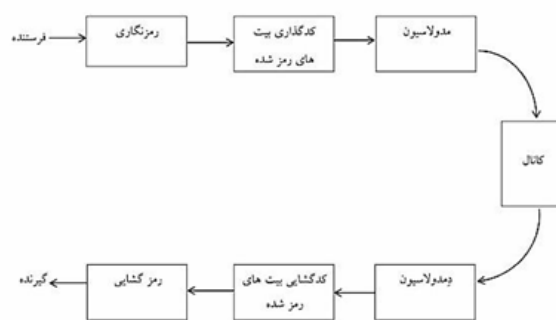
### ۳- کدگذاری قطبی

یکی از انواع کدگذاری های قالبی، کدگذاری قطبی است. کدهای قطبی توسط Arkan و برای اولین بار معرفی شده است [۱۲] و اولین خانواده از کدهایی هستند که به ظرفیت کانال های بدون حافظه گسسته دودویی (B-DMC) دست پیدا می کنند. ایده اصلی کدگذاری قطبی، ایجاد یک سیستم کدگذاری است که در آن می توان به هر کانال با مختصات  $W_N(i)$  به طور جداگانه دسترسی داشت و داده ها را تنها از این طریق ارسال نمود [۱۳]. نحوه طراحی کدهای قطبی بر اساس نرخ کدگذاری و دیگر مشخصه های آن مبتنی بر پارامترهای هر کانال بوده و به طور جداگانه طراحی می شوند و کد قطبی مربوط به یک کانال برای کانال دیگر قابل استفاده نمی باشد [۱۲].

کدهای قطبی از دسته کدهای خطی می باشند، بدین معنا که هر ترکیب خطی از کلمات کد، کلمات کد دیگری را تولید می کنند. ماتریس مولد کدهای قطبی با طول  $N = 2^n$ ،  $G_2^n$  است که با استفاده از ماتریس پایه ای  $G_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$  و تعریف  $G_2^n = \begin{pmatrix} G_2^{n-1} & 0 \\ G_2^{n-1} & G_2^{n-1} \end{pmatrix}$  به دست می آید.

کدهای قطبی از  $N$  کانال موازی برای ارسال اطلاعات استفاده می کند. در این صورت، کانال ها به دو دسته خوب و بد تقسیم می شوند. کانال های با ظرفیت کم، کانال های بد، و دسته دیگری از کانال ها با ظرفیت زیاد، کانال های خوب، تقسیم می شوند. کدینگ قطبی در واقع ارسال اطلاعات روی کانال های با ظرفیت بالا و ارسال ترکیب خطی از اطلاعات روی کانال های با ظرفیت پایین است. برای تعیین دقیق کانال های خوب و بد باید دو پارامتر مهم زیر را تعریف نمود.

تعریف: برای یک کانال نقطه به نقطه دو پارامتر، ظرفیت



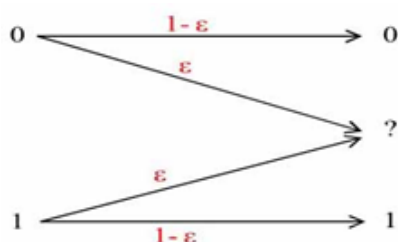
شکل (۱). ساختار یک فرستنده و گیرنده مخابراتی نوعی

در بخش ششم و هفتم، با محاسبه پیچیدگی سیستم ۸ بیتی و ۱۶ بیتی در طرح پیشنهادی می پردازیم. در بخش انتهایی، بخش هشتم، به ارائه یک فرمول برای به دست آوردن حداقل تعداد کلید رمز مورد نیاز پرداخته شده است. در بخش نهم به بررسی و مقایسه روش ارائه شده با دو روش معرفی شده در تحقیقات سال های اخیر می پردازیم.

### ۲- تلفیق رمزنگاری و کدگذاری

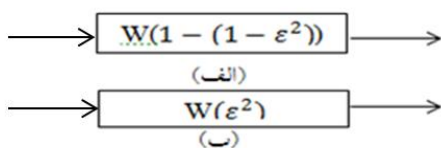
در هر ارتباط مخابراتی، با توجه به عبور اطلاعات از یک کانال با نویز، نیاز به انجام عملیات تشخیص و تصحیح خطا داریم. این نیاز در شبکه های با زیرساخت سیمی و بی سیم با هم متفاوت است. دلیل این موضوع احتمال خطای متفاوت دو کانال سیمی و بی سیم است. از طرف دیگر، برای امنیت اطلاعات ارسالی نیز تفاوت محسوسی بین دو حالت سیمی و بی سیم وجود دارد. در شبکه های سیمی تنها در صورت دسترسی دشمن به محیط انتقال اطلاعات، مراکز سویچ و سایر زیرساخت ها، امنیت سیستم مخدوش می گردد. از دیگر سو، به دلیل استفاده از کانال فضای آزاد، امکان شنود اطلاعات، جعل و تکرار پیام از طرف دشمن برای سیستم های بی سیم در مقایسه با سیستم های سیمی بیشتر است. در نتیجه در ارتباطات بی سیم به کارگیری الگوریتم های رمزنگار برای تأمین امنیت و اعتبار به عنوان یک نیاز پایه ای الزامی است [۶].

سیستم های موجود از بلوک های رمزنگاری و کدگذاری کانال به طور جداگانه برای برآورده ساختن خواسته های مذکور استفاده می نمایند. در بلوک کدگذاری کانال با اضافه نمودن بیت های افزونگی<sup>۱</sup> به بیت های اصلی پیام، این امکان را فراهم می نماید تا در گیرنده بتوان به کمک این بیت ها عمل تشخیص یا تصحیح خطا را انجام داد. به این بیت ها، بیت های بررسی توازن می گویند. در بلوک رمزنگاری به دلیل این که هر بیت از متن رمز شده می تواند اطلاعاتی در مورد کلید به دشمن بدهد، تلاش بر این است که تا حد ممکن از انتشار اطلاعات در پیام رمز شده،



شکل (۳). کانال w محک نوعی اثبات [۱۲]

در کدینگ قطبی، یکی از کانال‌ها دارای ظرفیت بیشتر و یکی از کانال‌ها دارای ظرفیت کم می‌باشد. بعد از دو مرحله قطبی کردن، یکی از کانال‌ها ظرفیتش افزایش یافته و بیش از قبل می‌گردد و ظرفیت دیگری کاهش یافته و کمتر می‌گردد. این عمل با افزایش تعداد مراحل، قطبی‌سازی افزایش می‌یابد. در شکل (۴) کانال بالایی با کاهش ظرفیت همراه بوده ولی کانال پایینی با افزایش ظرفیت همراه است. در این حالت می‌توان با استفاده از کانال پایینی اطلاعات مناسب‌تری را ارسال نمود.

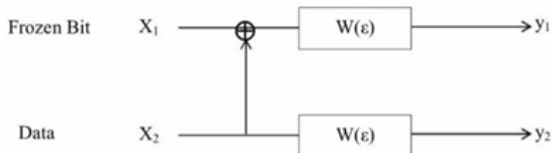


شکل (۴). کد قطبی معادل، (الف) کانال با ظرفیت کم، (ب) کانال با ظرفیت زیاد

در ساختار کدهای قطبی با مشخص بودن ظرفیت کانال‌ها، لینک‌هایی که ظرفیت زیادی دارند و حاوی اطلاعات هستند و لینک‌هایی که ظرفیت پایینی و نزدیک به صفر دارند مانند شکل (۴)، حاوی بیت‌های ثابت هستند [۱۲].

### ۴- طرح پیشنهادی اول

در این طرح، بیت‌های ثابت فرض شده در طرح Arikan را به عنوان کلید در نظر می‌گیریم. در ابتدا ساختار قطبی‌سازی دوکاناله شکل (۵) را در نظر بگیرید.



شکل (۵). کد قطبی معمولی [۱۲]

استفاده از شکل (۵) برای رمزنگاری در یک سیستم مخابراتی به دلیل وجود ضعف امنیتی مناسب نمی‌باشد. به دلیل این که بیت اطلاعات بدون هیچ کلید رمزی بر روی کانال قرار می‌گیرد و در واقع هیچ رمزنگاری بر روی آن انجام نمی‌شود. بدون انجام

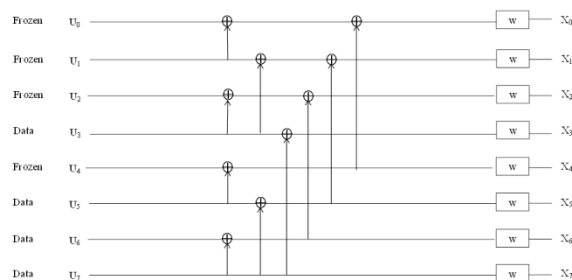
کانال و باتاچاری کانال، به ترتیب به صورت زیر تعریف می‌شود: [۱۲]

$$I(X; Y) \triangleq \sum_{y \in Y} \sum_{x \in X} \frac{1}{2} W(y|x) \log \frac{W(y|x)}{\frac{1}{2}W(y|0) + \frac{1}{2}W(y|1)} \quad (1)$$

$$Z(X; Y) \triangleq \sum_{y \in Y} \sqrt{W(y|0)W(y|1)} \quad (2)$$

حال با در نظر گرفتن ورودی‌های معلوم درگیرنده برای کانال‌های بد،  $U_1, U_2, \dots, U_{i-1} \triangleq U^{i-1}$  می‌توان تقریب مناسبی برای  $U_i$  به دست آورد. در این صورت طبق تعریف [۱۲]، از آن جایی که باتاچاری یک کانال معیاری از خطای آن کانال است، کانالی که دارای  $Z(U_i; U^{i-1}Y) < \delta$  کانال خوب بوده و کانالی که دارای  $Z(U_i; U^{i-1}Y) \geq \delta$  کانال بد است.

با در نظر گرفتن  $R \leq I(X; Y)$  نرخ ارسال اطلاعات همواره کمتر از ظرفیت ارسال است، در واقع کدگذاری قطبی براساس مجموعه‌ای از ماتریس  $G_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^n$  است تا یک ماتریس  $2^n R \times 2^n$  را تشکیل دهد که به عنوان ماتریس مولد کد، در فرآیند رمزگذاری کانال استفاده می‌شود،  $R$  نرخ کد قطبی است. در شکل (۲)، یک ساختار ۸ بیتی کد قطبی را نشان می‌دهد.



شکل (۲). ساختار ۸ بیتی کد قطبی در طرح Arikan [۱۲].

### ۳-۱- قطبش کانال

**قضیه ۱:** کانال با ورودی دودویی متقارن و گسسته  $W$  را در نظر بگیرید، کانال  $\{W_N^{(i)}\}$  قطبیده نامیده می‌شود. هرگاه برای هر  $\delta \in (0, 1)$  و با افزایش  $N$  و میل به سمت بی‌نهایت، کسری از کانال‌ها که اندیس‌ها  $i \in \{1, \dots, N\}$  که  $I(W_N^{(i)}) \in (1 - \delta, 1)$  به  $I(W)$  میل می‌کند. (کانال‌های بدون نویز) و کسری که  $I(W_N^{(i)}) \in (0, \delta)$  به  $1 - I(W)$  میل می‌کند. (کانال‌های نویزدار). برای یک کانال BEC نوعی مانند شکل (۳)، مقدار  $I(W_N^{(i)})$  با رابطه بازگشتی زیر محاسبه می‌شود:

$$I(W_N^{(2i-1)}) = I(W_{N/2}^{(i)})^2 \quad (3)$$

$$I(W_N^{(2i)}) = 2I(W_{N/2}^{(i)}) - I(W_{N/2}^{(i)})^2 \quad (4)$$

مشخص شده است. دلیل استفاده از این LFSRها این است که بیت‌های اطلاعات مستقیم و بدون تغییر بر روی کانال قرار نگیرد، چون در این صورت دسترسی و بازخوانی آن توسط دشمن ساده خواهد بود. همان‌طور که در شکل نمایش داده شده بیت‌های خروجی قبل از ورود به کانال، وارد یک جعبه جایگزینی می‌شود. جعبه جایگزینی، ترکیب و ترتیب خروجی‌های LFSRها را قبل از ورود به کانال تغییر دهد تا بازبایی آن توسط دشمن بسیار دشوار شود. در ادامه اثبات خواهیم کرد که انجام مطالب بیان شده باعث افزایش امنیت و پیچیدگی در سیستم پیشنهادی Arikani می‌شود.

### ۵- طرح پیشنهادی دوم

سیستم پیشنهادی بخش ۴ را در نظر بگیرید. در این سیستم بر روی تمامی بیت‌های ثابت و اطلاعات، LFSR قرار گرفت و پس از آن بیت‌های رمز شده وارد یک جعبه جایگزینی گردید تا عمل جایگزینی بر روی بیت‌ها انجام شود. در حقیقت سیستم ۸ بیت Arikani در طرح پیشنهادی اول، دارای ۸ عدد LFSR، سیستم ۱۶ بیت دارای ۱۶ عدد LFSR و به همین ترتیب به ازای  $n$  بیت در سیستم (ثابت و اطلاعات)  $n$  عدد LFSR به سیستم اعمال نموده و پس از اضافه کردن کلید رمز بر روی تمامی بیت‌ها، جایگزینی را قبل از ورود به کانال بر روی آن‌ها انجام دادیم.

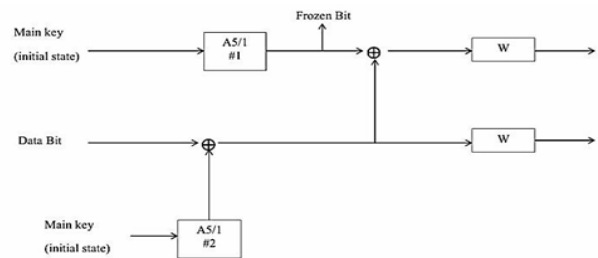
طرح فوق دارای دو ایراد اساسی است:

- به ازای  $n$  بیت،  $n$  عدد LFSR نیاز داریم که مطلوب نیست.
- استفاده از هر نوع جعبه جایگزینی برای سیستم فوق قابل قبول نیست و باید از جعبه جایگزینی استفاده شود که برای تعداد بیت‌های کم مثلاً ۸ و ۱۶ بیت نیز از آن استفاده کرد (مثلاً الگوریتم AES برای تعداد بیت کم قابل استفاده نیست) و جعبه جایگزینی باید حداکثر پیچیدگی را بر روی بیت‌ها قبل از ورود به کانال اضافه کند.

از طرفی، یک سیستم رمزنگاری مطلوب، سیستمی است که دارای پیچیدگی زیاد و سادگی در پیاده سازی، می‌توان در اینجا سادگی در پیاده سازی را متناسب با کاهش تعداد کلید مورد لزوم دانست، باشد که با استفاده از حداقل تعداد کلید رمز، حداکثر پیچیدگی و امنیت را در سیستم ایجاد کند [۱]. در طرح پیشنهادی قبلی به ازای هر بیت، یک کلید رمز (LFSR) اعمال شد. حال روشی کارآمد را ارائه می‌کنیم که علاوه بر کاهش تعداد کلید های رمز، میزان همبستگی اطلاعات را نیز کاهش می‌دهیم.

عمل جایگزینی بر روی بیت اطلاعات و بیت ثابت، تشخیص این بیت‌ها از یکدیگر برای دشمن امری ساده خواهد بود، پس نیاز به بیت کلید برای رمز نمودن بیت‌ها و انجام عمل جایگزینی بر روی آن‌ها توسط یک جعبه جایگزینی قبل از ورود به کانال ضروری است. لذا، نیاز به انجام تغییراتی برای افزایش امنیت در این سیستم وجود دارد. در سیستم و طرح پیشنهادی اول ۳ عمل، مطابق شکل (۶) به صورت زیر بر روی بیت‌ها انجام می‌گیرد:

۱. اضافه کردن یک بیت کلید به بیت اطلاعات
۲. بیت ثابت را به عنوان کلید رمز در نظر بگیریم. (اضافه کردن یک بیت کلید به بیت ثابت)
۳. انجام عمل جایگزینی بر روی بیت‌های خروجی قبل از ورود به کانال.

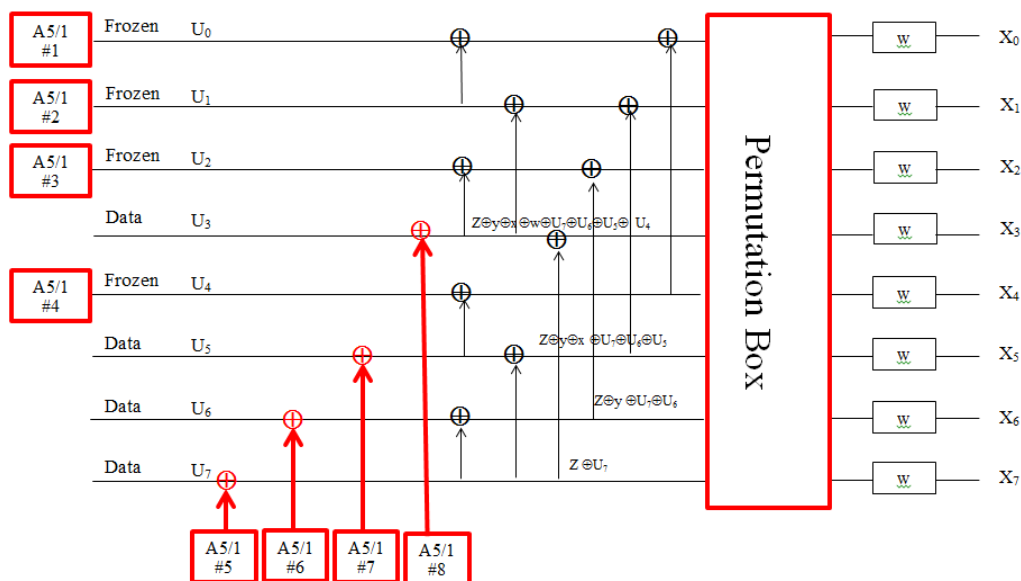


شکل (۶). اضافه کردن کلید رمز بر روی بیت‌ها

در حالت کلی، سیستم‌های رمز دنباله‌ای هنگامی که سرعت ارسال اطلاعات زیاد باشد، به‌طور مطلوبی مورد استفاده قرار می‌گیرد. سیستم‌های رمز دنباله‌ای معمولاً دارای سخت‌افزاری ساده و در مواقعی که احتمال خطای انتقال زیاد باشد، عملکرد مناسبی دارند. این رمزها را می‌توان به دو دسته همزمان و غیرهمزمان تقسیم نمود. یکی از رمزهای دنباله‌ای غیرهمزمان مناسب برای سیستم مخابراتی سیستم رمز دنباله‌ای A5/1 است. مولد رمز دنباله‌ای A5/1 برای رمز ارتباطات در استاندارد نسل دوم و سوم ارتباطات بی‌سیم به‌طور موثری مورد استفاده قرار می‌گیرد [۱۴]. در این مقاله از مولد رمز دنباله‌ای A5/1 نوعی استفاده شده است.

حال ساختار ۸ بیتی Arikani را در نظر بگیرید، همان‌طور در شکل نمایش داده شده، یک LFSR، A5/1 بر روی هر کدام از بیت‌های ثابت قرار گرفته است. در حقیقت از بیت فریز شده به عنوان کلید رمز استفاده می‌شود. اضافه کردن LFSR بر روی تمام بیت‌های ثابت انجام می‌شود. همان‌طور که گفته شد در طرح پیشنهادی از الگوریتم A5/1 استفاده می‌شود.

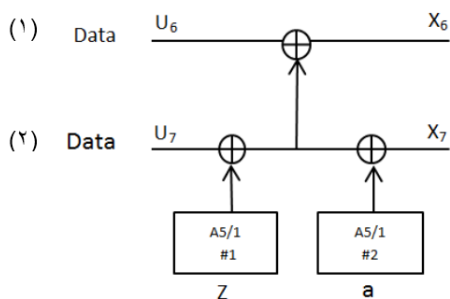
بر روی تمامی بیت‌های اطلاعات نیز از رمز دنباله‌ای A5/1 بهره گرفته شده است، که در شکل با عنوان #5, #6, #7, #8



شکل (۷). اضافه کردن LFSR ها و نمایش طرح پیشنهادی اول

سیستم (که با "a" نمایش داده شده است)، همبستگی بین دو بیت آخر (در این جا  $U_6$  و  $U_7$ ) از بین می‌رود. توجه داشته باشید که اعمال "a" بر روی کل سیستم و بیت‌ها اثر می‌گذارد.

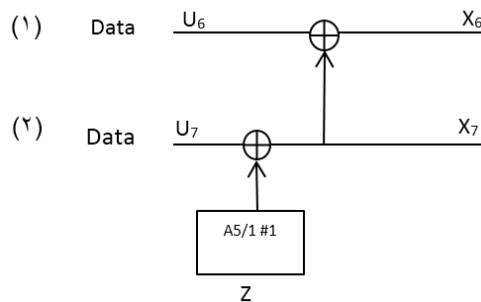
در این حالت و پس از انجام XORها، در خط شماره ۱،  $U_6 \oplus U_7 \oplus Z$  و در خط شماره ۲،  $U_7 \oplus Z \oplus a$  خواهد بود. بدین ترتیب مشاهده می‌شود با اضافه کردن LFSR، "a" بر روی بیت آخر، همبستگی بین  $U_6$  و  $U_7$  از بین رفته و دشمن نمی‌تواند  $U_6$  را از روی  $U_7$  به دست آورد. همان‌طور که گفته شد، عملکرد و تاثیر a به همین جا ختم نمی‌شود. حال سیستم کامل ۸ بیتی Arikan با اعمال "a" بر روی بیت آخر در نظر بگیرید:



شکل (۹). اعمال دو کلید رمز بر روی بیت آخر

مشاهده می‌شود که با اعمال "a" بر روی بیت آخر علاوه بر حذف LFSR،  $U_6$  می‌توان LFSRهای  $U_5$ ،  $U_3$ ،  $U_0$  را نیز حذف نمود بدون این که همبستگی بین بیت‌ها به وجود آید. تاثیر "a" بر روی کل سیستم می‌باشد. یعنی علاوه بر این که باعث از بین رفتن همبستگی  $U_6$  و  $U_7$  می‌شود، همبستگی بین سایر بیت‌ها تا  $U_0$  را هم از بین می‌برد. به XOR بیت‌ها در این روش توجه

یکی از مهمترین مسایلی که برای طراحی یک سیستم رمزنگاری امن همیشه مهم است، میزان همبستگی اطلاعات زیر بخش‌هایی است که در اختیار تحلیل‌گر سیستم رمز می‌باشد. از دید یک طراح رمزنگار همواره به دنبال کاهش همبستگی اطلاعاتی که ممکن است در دسترس دشمن باشد هستیم [۱۵]. برای این منظور، در این طرح و برای کاهش میزان همبستگی ورودی اطلاعات به کانال‌ها از یک رمز دنباله‌ای دیگری تحت عنوان "a" بهره می‌گیریم. دو بیت آخر، سیستم ۸ بیتی را در نظر بگیرید. اگر فقط از یک LFSR برای رمز کردن هر دو بیت استفاده کنیم (شکل (۸))، در این حالت قبل از انجام XOR، در خط شماره ۱،  $U_7 \oplus a$  و پس از انجام XOR، در خط شماره ۱،  $U_6 \oplus U_7 \oplus Z$  و در خط شماره ۲،  $U_7 \oplus Z$  خواهد بود. همان‌طور که مشاهده می‌شود در صورت استفاده از Z (تنها یک LFSR)، بین بیت‌های  $U_6$  و  $U_7$  همبستگی وجود دارد، که دشمن به راحتی می‌تواند  $U_6$  را از روی  $U_7$  به دست آورد. (به خاطر داشته باشید که ما به دنبال کاهش تعدادی از LFSRها هستیم، پس نمی‌خواهیم بر روی بیت  $U_6$  LFSR اعمال کنیم.)



شکل (۸). اعمال یک کلید رمز بر روی دو بیت آخر سیستم ۸ بیتی حال عملکرد زیر را در نظر بگیرید. در این طرح پیشنهادی بسیار جالب با اضافه کردن یک LFSR بر روی بیت آخر هر

اثبات: در طرح ۸ بیتی پیشنهادی، از ۵ عدد A5/1، LFSR استفاده می‌شود. هر A5/1 برابر  $O(2^{63.32})$  می‌باشد، پس پیچیدگی کل A5/1 ها برابر  $O(2^{316.6})$  می‌شود. همان‌طور که بیان شد از یک جعبه جایگزینی برای انجام عمل جایگزینی بیت-های خروجی در سیستم استفاده می‌شود که پیچیدگی آن برابر  $n!$  می‌باشد. بیان‌کننده تعداد کل بیت‌ها است. پس پیچیدگی کل سیستم برابر است با:

$$\chi = 2^{316.6} \times 2^{15.29} = 2^{331.89} \quad (1)$$

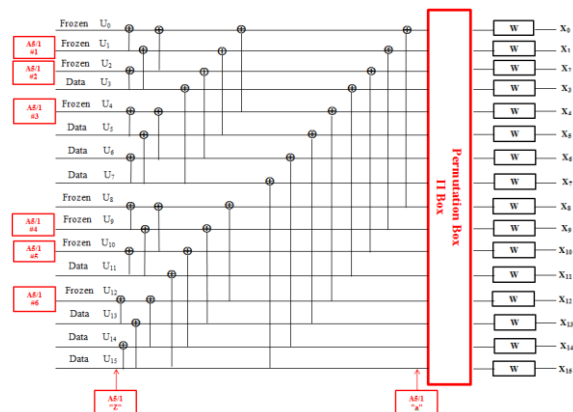
### ۷- سیستم ۱۶ بیتی Arikan در طرح جدید و محاسبه پیچیدگی آن

در شکل (۱۱) طرح پیشنهادی برای سیستم ۱۶ بیتی Arikan نمایش داده شده است:

همان‌طور که مشاهده می‌کنید با اضافه کردن "a" بر روی بیت آخر  $(U_{15})$  تاثیر آن بر روی کل سیستم اعمال می‌شود و باعث حذف کلید لازم برای LFSR های  $(U_0, U_3, U_5, U_6, U_7, U_8, U_{11}, U_{13}, U_{14})$  می‌شود. چون "a" با اثر گذاشتن بر روی بیت آخر باعث تاثیر بر کل بیت‌ها می‌شود و همبستگی بین تمامی بیت‌ها را از بین می‌برد.

قضیه ۳: پیچیدگی کل سیستم، پیچیدگی فضای حداقل کلید لازم، در طرح ۱۶ بیتی برابر  $O(2^{550.81})$  می‌باشد.

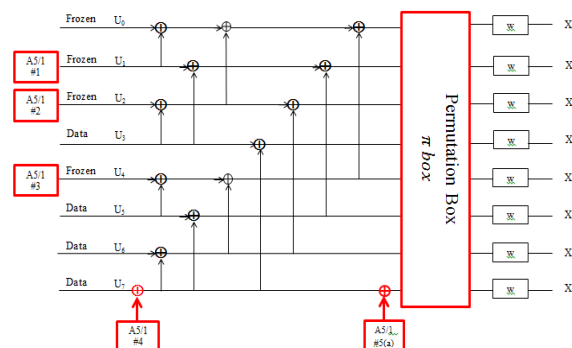
اثبات: در طرح ۱۶ بیتی از ۸ عدد A5/1 استفاده می‌شود.



شکل (۱۱). استفاده از کلید رمز (a) بر روی بیت آخر در سیستم ۱۶ بیتی Arikan

پیچیدگی هر A5/1 برابر  $O(2^{63.32})$  می‌باشد پس پیچیدگی کل A5/1 ها برابر  $O(2^{506.56})$  می‌شود. همان‌طور که در شکل مشاهده می‌شود سیستم دارای یک جعبه جایگزینی (II-Box) برای انجام عمل جایگزینی است که پیچیدگی آن برای ۱۶ بیت

کنیسه، در این صورت  $U_1 \oplus U_3 \oplus U_5 \oplus U_7 \oplus Z$ ،  $U_2 \oplus U_3 \oplus U_6 \oplus U_7 \oplus Z$ ،  $U_3 \oplus U_7 \oplus Z$ ،  $U_4 \oplus U_5 \oplus U_6 \oplus U_7 \oplus Z$ ،  $U_5 \oplus U_7 \oplus Z$ ،  $U_6 \oplus U_7 \oplus Z$ ،  $U_7 \oplus Z \oplus a$  خواهد بود.



شکل (۱۰). استفاده از کلید رمز (a) بر روی بیت آخر در سیستم ۱۶ بیتی Arikan

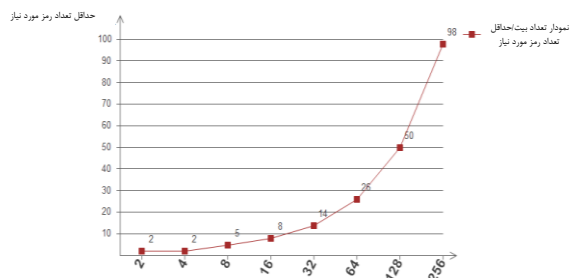
همان‌طور که مشاهده می‌کنید، هیچ دو بیتی با یکدیگر همبستگی ندارند. در واقع دشمن با استفاده از حمله همبستگی نمی‌تواند بیتی را از روی بیت دیگر به دست آورد. تاثیر و عملکرد "a" بر روی کل سیستم به خوبی مشاهده می‌شود. اگر کلید رمز "a" بر روی بیت آخر اعمال نگردد، سیستم در مقابل حمله همبستگی شکسته می‌شود و یا در صورتی که بخواهیم همبستگی بین بیت‌ها را از بین ببریم باید تعداد بیشتری کلید رمز بر روی بیت‌ها قرار دهیم.

حال، با اعمال "a" تعداد LFSR های مورد نیاز کاهش می‌یابد و LFSR های اعمال شده بر روی بیت های  $U_0, U_3, U_5, U_6$  حذف شده است. از طرفی، بیت‌های رمز شده قبل از ورود به کانال وارد سیستمی شوند تا ترتیب و چیدمان آن‌ها تغییر کند. یک جعبه جایگزینی در سیستم قرار می‌دهیم تا عمل جایگزینی بر روی بیت‌های رمز شده، قبل از ورود به کانال انجام شود. این عمل، باعث افزایش پیچیدگی سیستم می‌شود. حسن استفاده از جعبه جایگزینی پیشنهادی (II-Box) این است که برای تعداد بیت‌های کم (مثلاً ۲ بیت و ۴ بیت) نیز قابل استفاده است در حالی که دیگر الگوریتم‌ها (مثلاً الگوریتم AES) برای تعداد بیت کم، قابل استفاده نیستند. طرز کار جعبه جایگزینی پیشنهادی بدین صورت است که با انجام عمل جایگزینی بر روی بیت‌ها، پیچیدگی معادل  $\frac{\log(n!)}{\log 2}$  به سیستم اضافه می‌کند.  $n$  بیان‌کننده تعداد کل بیت‌ها در هر سیستم است.

### ۶- محاسبه پیچیدگی سیستم ۸ بیتی در طرح پیشنهادی جدید

قضیه ۲: پیچیدگی کل سیستم در طرح ۸ بیتی برابر  $O(2^{331.89})$  می‌باشد.





نمودار (۱). افزایش حداقل تعداد رمز مورد نیاز با افزایش تعداد بیت

### ۹- مقایسه روش ارایه شده با روش های موجود

در این بخش به بررسی و مقایسه روش ارایه شده این مقاله با دو روش مطرح شده اخیر در [۱۶-۱۷] می پردازیم. روش توام کدگذاری و رمزنگاری برای اولین بار توسط مک آلیس در [۱۸] ارایه شد و همه روش ها و مقالات ارایه شده در این حوزه تلاش می کنند تا با استفاده از تکنیک مشابه روش مک آلیس سیستم های توام کدینگ کانال و رمز را معرفی نمایند. در این حالت باید از مخفی نمودن ماتریس مولد کد برای رمزنگاری بهره جست.

اما روش ارایه شده در مقاله حاضر، به جای اختفای ماتریس مولد کلمه کد از ورودی های رمز شده و خاصیت خوب "بیت های ثابت شده" کدهای قطبی بهره می گیرد. در واقع روش ارایه شده در مقاله حاضر، تلفیق کدینگ کانال و رمزنگاری مناسبی بوده که این روش اولین تکنیک تلفیق از دسته خانواده های جدید تلفیق رمزنگاری و کدینگ کانال که مبتنی بر خاصیت ذاتی کدینگ قطبی می باشد، بوده و تاکنون چنین روشی ارایه نشده است.

برای مقایسه روش ارایه شده با مراجع مذکور باید دقت نمود که روش ارایه شده برای هر تعداد کانال و حتی کد قطبی نامتقارن قابل بهره گیری است. دلیل این امر آن است که این روش تنها متکی به یافتن کانال های خوب و بد می باشد و بر اساس ماتریس مولد کد قطبی که دارای پیچیدگی زیادی برای طراحی می باشد، نیست.

طبق [۱۶]، برای یک کد قطبی به طول ۱۰۲۴ با نرخ ۰.۷۵، پیچیدگی فضای کلید برابر  $2^{271}$  می باشد. روش ارایه شده به جای رسیدن به این پیچیدگی در طول ۱۰۲۴، در طول ۸ و با بهره گیری از ۵ عدد LFSR به این پیچیدگی می رسد.

میزان پیچیدگی گزارش شده در [۱۷] نیز برابر  $2^{n(n+1)-1}$  می باشد. از طرفی در روش پیشنهادی با پیچیدگی (189.96n-253.28) ۲ و برابر قرار دادن توان های درجات پیچیدگی

برابر  $O(2^{44.25})$  می باشد، پس پیچیدگی کل سیستم ۱۶ بیتی با استفاده از طرح پیشنهادی برابر است با:

$$\chi = 2^{506.56} \times 2^{44.25} = 2^{550.81} \quad (۶)$$

### ۸- ارائه فرمول برای به دست آوردن "حداقل تعداد کلید رمز" مورد نیاز

قضیه ۴: برای یک کد قطبی n تایی، تعداد بیت لازم برای رمزنگاری ایمن،  $3n-4$  می باشد و پیچیدگی کل سیستم، پیچیدگی فضای حداقل کلید لازم، برابر  $(\chi_{A5/1})^{3n-4} \times n!$  است.

اثبات: دو بیت انتهایی به دلیل وجود بیت های رمز شده a و Z احتیاج به رمز ندارد. پس از n بیت تنها n-2 بیت به رمز احتیاج دارند. طبق شکل (۱۰) برای هر ۸ بیت تنها ۳ بیت ( $\log 8 = 3$ ) برای رمز احتیاج است در نتیجه برای n بیت تنها  $3(n-2) = 3n-6$  لازم است و با حساب دو بیت a و Z برابر  $3n-4$  می شود.

طرح ۸ بیتی و ۱۶ بیتی Arikan با اعمال حداقل تعداد کلید رمز (LFSR A5/1) شرح داده شد و محاسبه پیچیدگی آن ها مشاهده گردید. اگر تعداد بیت ها افزایش یابد (مثلا ۳۲، ۶۴، ۱۲۸ بیت و ...) می توان حداقل تعداد کلید مورد نیاز و پیچیدگی سیستم را با استفاده قضیه ۳ به دست آورد. در جدول (۱)، تعداد بیت ها، حداقل کلید های مورد نیاز و پیچیدگی محاسبه شده برای هر سیستم را مشاهده می کنید.

جدول (۱). نمایش تعداد بیت، حداقل کلید رمز مورد نیاز و

پیچیدگی هر سیستم

تعداد بیت (n)	حداقل تعداد رمز مورد نیاز ( $3n-4$ )	پیچیدگی (Complexity)
۲	۲	$2^{126.64}$
۴	۲	$2^{128.93}$
۸	۵	$2^{331.89}$
۱۶	۸	$2^{550.81}$
۳۲	۱۴	$2^{1004.14}$
۶۴	۲۶	$2^{1942.31}$
۱۲۸	۵۰	$2^{3882.14}$

در نمودار زیر روند افزایشی حداقل تعداد کلید رمز مورد نیاز با افزایش تعداد بیت ها نمایش داده شده است:

- [8] L. Guardia and G. Giuliano, "Nonbinary convolutional codes derived from group character codes," *Discrete Mathematics* 313, no. 23, pp. 2730-2736, 2013.
- [9] M. Kenarkouhi and H. Tavakoli, "New method for combining the channel coding with polar coding-based encryption," *Journal of Advanced Computer Science & Technology* 4, no. 1, pp. 90-94, 2015.
- [10] A. Canteaut and S. Nicolas, "Cryptanalysis of the original McEliece cryptosystem," In *Advances in Cryptology-ASIACRYPT'98*, Springer Berlin Heidelberg, pp. 187-199, 1998.
- [11] J.-C. Faugere, G.-U. Valérie, O. Ayoub, P. Ludovic, and J.-P. Tillich, "A distinguisher for high-rate McEliece cryptosystems," *Information Theory, IEEE Transactions on* 59, no. 10, pp. 6830-6844, 2013.
- [12] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *Information Theory, IEEE Transactions on* 55, no. 7, pp. 3051-3073, 2009.
- [13] N. Hussami, B. K. Satish, and U. Rüdiger, "Performance of polar codes for channel and source coding," In *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, pp. 1488-1492, 2009.
- [14] A. Biryukov, S. Adi, and W. David, "Real Time Cryptanalysis of A5/1 on a PC," In *Fast Software Encryption*, Springer Berlin Heidelberg, pp. 1-18, 2000.
- [15] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications (Corresp.)," *Information Theory, IEEE Transactions on* 30, no. 5, pp. 776-780, 1984.
- [16] R. Hooshmand, M. Koochak Shoostari, and M. R. Aref, "Secret key cryptosystem based on polar codes over binary erasure channel," In *Information Security and Cryptology (ISCISC), 2013 10th International ISC Conference on*, IEEE, pp. 1-6, 2013.
- [17] S. R. Shrestha and K. Young-Sik, "New McEliece cryptosystem based on polar codes as a candidate for post-quantum cryptography," In *Communications and Information Technologies (ISCIT), 2014 14th International Symposium on*, IEEE, pp. 368-372, 2014.
- [18] R. McEliece, "A public-key cryptosystem based on algebraic codes," *DNS Progress Reports, NASA Jet Propulsion Laboratory, Pasadena, CA*, pp. 114-116, 1978.

می‌توان به این نتیجه رسید که روش ارائه شده برای  $n < 187$  از [۱۷]، بهتر می‌باشد و برای مقادیر بیشتر  $n$  برای داشتن پیچیدگی بیشتر از روش [۱۷]، بهره گرفت.

#### ۱۰- نتیجه گیری

در این مقاله پس از بررسی کدگذاری قطبی که توسط Arikan ارائه شده، یک روش تلفیقی در کدینگ کانال و سیستم رمز قالبی مبتنی بر جعبه جایگزینی و سیستم رمز جریان مبتنی بر الگوریتم شناخته شده A5/1 ارائه شده است. از آن جایی که کارایی این روش در ساختار کدینگ کانال معنی دارد، لذا، کارایی این روش با افزایش پیچیدگی کاهش پیدا نمی‌کند. نتایج این الگوریتم نشان دهنده آن است که در سیستم تلفیقی علاوه بر عدم دانایی دشمن از کلیدهای الگوریتم های رمز جریانی A5/1، خرابی کانال و قطبی شدگی کانال به کمک رمزگذار آمده و حداکثر میزان ابهام و گیجی مورد نظر شانون را برای دشمن فراهم می‌کند. دلیل این امر آن است که، دشمن نه تنها با نداشتن کلید بیت ثابت روبروست، بلکه در مورد انتخاب کانال درست که اطلاعات بر روی آن است، با ابهام روبرو است. نتایج بررسی حاصل از پیچیدگی، بیانگر توانایی این الگوریتم است.

#### ۱۱- مراجع

- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal* 28, no. 4, pp. 656-715, 1949.
- [2] W. Stallings, "Cryptography and Network Security," 4/E Pearson Education India, 2006.
- [3] T. M. Cover and A. T. Joy, "Elements of information theory," John Wiley & Sons, 2012.
- [4] S. Lin and J. C. Daniel, "Error control coding," Pearson Education India, 2004.
- [5] R. J. McEliece, "A public-key cryptosystem based on algebraic," *Coding Thv4244*, pp. 114-116, 1978.
- [6] E. R. Berlekamp, R. J. McEliece, and H. C. Van Tilborg, "On the inherent intractability of certain coding problems," *IEEE Transactions on Information Theory* 24, no. 3, pp. 384-386, 1978.
- [7] R. McEliece, "The theory of information and coding," Cambridge University Press, 2002.



---

## A New Method for Combining the Channel Coding with Polar Coding-Based Encryption

M. Kenarkouhi\*, H. Tavakoli

\*University of Guilan

(Received: 30/12/2014, Accepted: 03/05/2016)

### ABSTRACT

*In this article, polar codes that have recently been presented by Arikan, to integrate channel coding and encryption is used. Polar coded bits are divided into two categories. The first batch are the bits that virtual high-capacity channels of the passage that briefly bits of high-capacity are called and the information on it. The second group are bits that are virtual channels with capacity for short passes that "constant bits" are called. In the first proposal of fixed bits as we use encryption key, and on all bits of the plan (data bits and fixed bits) are key. In fact, the plan proposed 8-bit Arikan, we use the 8 key. Then, the proposed method is that it can be applied to the number of key bits can be reduced. The encryption system is effective and desirable that, in addition to the high complexity and lack of correlation between bits, the least it used to be key.*

**Keywords:** Encryption, Channel Coding, The Combination of Encryption and Coding, Polar Code, Complexity.

---

\* Corresponding Author Email: Mohammad\_k\_g@yahoo.com