مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال چهارم، شماره ۱، بهار ۱۳۹۵، ص ۸-۱

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

محمّد کنارکوهی[1*]، حسن توکلی[2]
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 Arikan 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 آن ها 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 Arikan، از ۸ کلید رمز استفاده می‌کنیم. سپس در ادامه این مقاله روشی ارائه می‌شود که توسط آن می‌توان تعداد کلید رمز اعمال‌شده 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

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 [۲-۱].

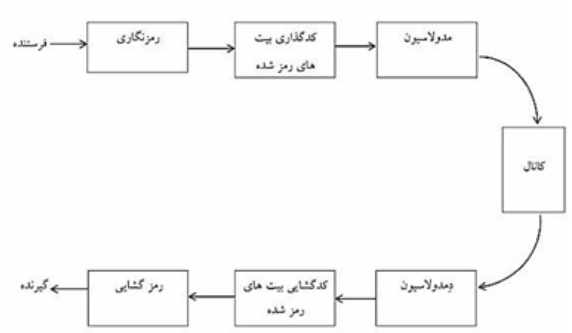
از طرف دیگر، برای داشتن ارتباطی بدون خطا یا به طور معادل انتقال و ارسال اطلاعات بدون خطا یا باکمترین خطا باید از کدهای کنترل خطا استفاده نمود. "کدگذاری کانال" در واقع استفاده از کدهای کنترل خطا می باشد. [۳]. در اصل، کدگذاری کانال با ایجاد قالب های تابعی، عمل کدگذاری کنترل خطا را انجام می‌دهد. کدکننده کانال به روش اصولی تعدادی بیت را به بیت‌های پیام ارسالی اضافه می‌کند. این بیت‌های اضافی در حالی‌که خودحامل هیچ گونه اطلاعات اضافی نیستند، کمک به 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 بیان‌شده 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 می شود [۵].

استفاده همزمان از رمزنگاری و کدگذاری کانال در شکل (۱) نمایش داده شده است. استفاده توام 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 ارایه می‌دهیم.

* رایانامه نویسنده مسئول: Mohammad_k_g@yahoo.com



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 می‌پردازیم. در بخش انتهایی، بخش هشتم، به ارائه یک فرمول برای به‌دست آوردن حداقل تعداد کلید رمز مورد نیاز پرداخته شده است. در بخش نهم به بررسی و مقایسه روش ارایه‌شده با دو روش معرفی‌شده در تحقیقات سال‌های اخیر می‌پردازیم.

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 شبکه‌های با زیرساخت سیمی و بی‌سیم با هم متفاوت است. دلیل این موضوع احتمال خطای متفاوت دو کانال سیمی و بی‌سیم است. از طرف دیگر، برای امنیت اطلاعات ارسالی نیز تفاوت محسوسی بین دو حالت سیمی و بی‌سیم وجود دارد. در شبکه‌های سیمی تنها در صورت دسترسی دشمن به محیط انتقال اطلاعات، مراکز سوییچ و سایر زیرساخت‌ها، امنیت سیستم مخدوش می‌گردد. از دیگر سو، به‌دلیل استفاده از کانال فضای آزاد، امکان شنود اطلاعات، جعل و تکرار پیام از طرف دشمن برای سیستم‌های بی‌سیم در مقایسه با سیستم‌های سیمی بیشتر است. در نتیجه در ارتباطات بی‌سیم به‌کارگیری الگوریتم‌های رمزنگار برای تأمین امنیت و اعتبار به عنوان یک نیاز پایه‌ای الزامی است [۶].

سیستم‌های موجود از بلوک‌های رمزنگاری و کدگذاری کانال به‌طور جداگانه برای برآورده ساختن خواسته‌های مذکور استفاده می‌نمایند. در بلوک کدگذاری کانال با اضافه نمودن بیت‌های افزونگی[1] به بیت‌های اصلی پیام، این امکان را فراهم می‌نماید تا در گیرنده بتوان به کمک این بیت‌ها عمل تشخیص یا تصحیح خطا را انجام داد. به این بیت‌ها، بیت‌های بررسی توازن می‌گویند. در بلوک رمزنگاری به‌دلیل این که هر بیت از متن رمزشده می‌تواند اطلاعاتی در مورد کلید به دشمن بدهد، تلاش بر این است که تا حد ممکن از انتشار اطلاعات در پیام رمزشده، جلوگیری شود [۸-۷].

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

۳- کدگذاری قطبی

یکی از انواع کدگذاری‌های قالبی، کدگذاری قطبی است. کدهای قطبی توسط Arikan و برای اولین بار معرفی شده است [۱۲] و اولین خانواده از کدهایی هستند که به ظرفیت کانال‌های بدون حافظه گسسته دودویی (B-DMC) دست پیدا می‌کنند. ایده اصلی کدگذاری قطبی، ایجاد یک سیستم کدگذاری است که در آن می‌توان به هر کانال با مختصات $W_N(i)$ به‌طور جداگانه دسترسی داشت و داده‌ها را تنها از این طریق ارسال نمود [۱۳]. نحوه طراحی کدهای قطبی بر اساس نرخ کدگذاری و دیگر مشخصه‌های آن مبتنی‌بر پارامترهای هر کانال بوده و به‌طور جداگانه طراحی می‌شوند و کد قطبی مربوط به یک کانال برای کانال دیگر قابل استفاده نمی‌باشد [۱۲].

کدهای قطبی از دسته کدهای خطی می‌باشند، بدین معنا که هر ترکیب خطی از کلمات کد، کلمات کد دیگری را تولید می‌کنند. ماتریس مولد کدهای قطبی با طول $N = 2^n$، G_2^n است که با استفاده از ماتریس پایه‌ای $G_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ و تعریف $G_2^n = \begin{pmatrix} G_2^{n-1} & 0 \\ G_2^{n-1} & G_2^{n-1} \end{pmatrix}$ به‌دست می‌آید.

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

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

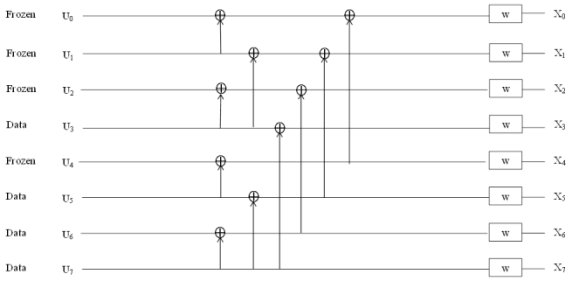
کانال و باتاچارای کانال، به ترتیب به‌صورت زیر تعریف می‌شود [۱۲]:

$$I(X;Y) \triangleq \sum_{y\in Y}\sum_{x\in X}\frac{1}{2}W(y|x)log\frac{W(y|x)}{\frac{1}{2}W(y|0)+\frac{1}{2}W(y|1)} \quad (۱)$$

$$Z(X;Y) \triangleq \sum_{y\in Y}\sqrt{W(y|0)W(y|1)} \quad (۲)$$

حال با درنظر 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 به‌دست آورد. در این صورت طبق تعریف [۱۲]، از ان جایی که باتاچارای 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 $2^nR \times 2^n$ 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.



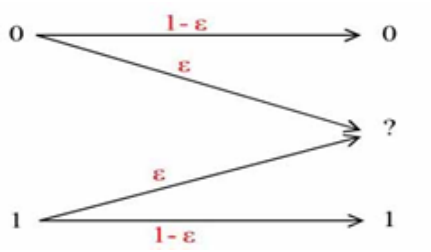
شکل (۲). ساختار ۸ بیتی کد قطبی در طرح Arikan [۱۲].

۳-۱- قطبش کانال

قضیه ۱: کانال با ورودی دودویی متقارن و گسسته W را درنظر 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 $I\left(W_N^{(i)}\right) \in (1-\delta,1)$ به $I(W)$ میل می‌کند. (کانال‌های بدون نویز) و کسری که $I\left(W_N^{(i)}\right) \in (0,\delta)$ به $1-I(W)$ میل می‌کند. (کانال‌های نویزدار). برای یک کانال BEC نوعی مانند شکل (۳)، مقدار $I\left(W_N^{(i)}\right)$ با رابطه بازگشتی زیر محاسبه می‌شود:

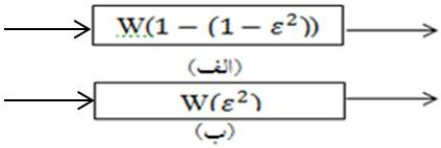
$$I\left(W_N^{(2i-1)}\right) = I\left(W_{N/2}^{(i)}\right)^2 \quad (۳)$$

$$I\left(W_N^{(2i)}\right) = 2I\left(W_{N/2}^{(i)}\right) - I\left(W_{N/2}^{(i)}\right)^2 \quad (۴)$$



شکل (۳). کانال w محک نوعی‌اثبات [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 کاهش‌یافته و کمتر می‌گردد. این عمل با افزایش تعداد مراحل، قطبی‌سازی افزایش می‌یابد. در شکل (۴) کانال بالایی با کاهش ظرفیت همراه بوده ولی کانال پایین با افزایش ظرفیت همراه است. در این حالت می‌توان با استفاده از کانال پایین اطلاعات مناسب‌تری را ارسال نمود.

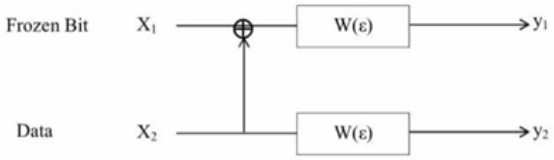


شکل (۴). کد قطبی معادل، (الف) کانال با ظرفیت کم، (ب) کانال با ظرفیت زیاد

در ساختار کدهای قطبی با مشخص بودن ظرفیت کانال‌ها، لینک‌هایی که ظرفیت زیادی دارند و حاوی اطلاعات هستند و لینک‌هایی که ظرفیت پایین 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 درنظر بگیرید.

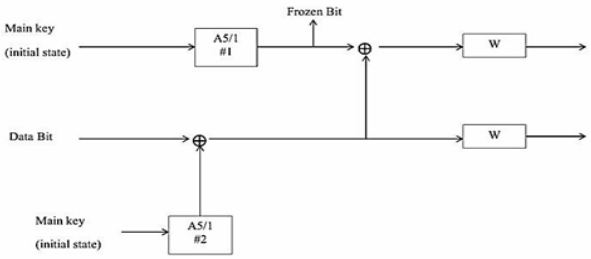


شکل (۵). کد قطبی معمولی [۱۲]

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

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 جای‌گشتی بر روی آن‌ها توسط یک جعبه جای‌گشتی 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 برروی 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 دستهٔ 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 Arikan 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 فریزشده به عنوان کلید رمز استفاده می‌شود. اضافه کردن LFSR بر روی تمام بیت‌های ثابت انجام می‌شود. همان‌طورکه گفته‌شد 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 مشخص شده است. دلیل استفاده از این *LFSR*ها این است که بیت‌های اطلاعات مستقیم و بدون تغییر بر روی کانال قرار نگیرد، چون در این‌صورت 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 بازیابی آن توسط دشمن بسیار دشوار شود. در ادامه اثبات خواهیم کرد که انجام مطالب بیان شده باعث افزایش امنیت و پیچیدگی در سیستم پیشنهادی Arikan می شود.

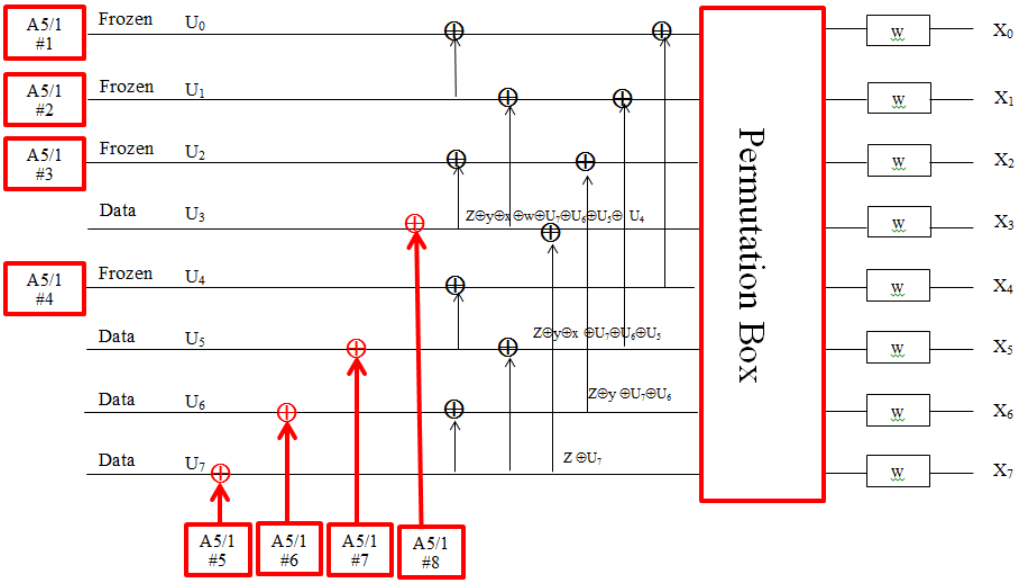
۵- طرح پیشنهادی دوم

سیستم پیشنهادی بخش ۴ را درنظر بگیرید. در این سیستم بر روی تمامی بیت‌های ثابت و اطلاعات، LFSR قرارگرفت 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 Arikan در طرح پیشنهادی اول، دارای ۸ عدد LFSR، سیستم ۱۶ بیت دارای ۱۶ عدد LFSR و به همین ترتیب به‌ازای 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:

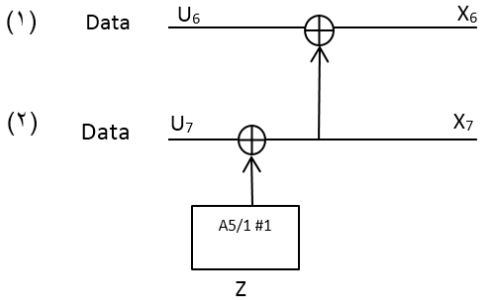
- به‌ازای n بیت، n عدد LFSR نیاز داریم که مطلوب نیست.
- استفاده از هر نوع جعبه جایگزینی برای سیستم فوق قابل قبول نیست و باید از جعبه جایگزینی استفاده شود که برای تعداد بیت‌های کم مثلا ۸ و ۱۶ بیت نیز از آن استفاده کرد(مثلا الگوریتم AES برای تعداد بیت کم قابل استفاده نیست) و جعبه جایگزینی باید حداکثر پیچیدگی 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 کارامد را ارائه می کنیم که علاوه بر کاهش تعداد کلید های رمز، میزان همبستگی اطلاعات را نیز کاهش می دهیم.



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

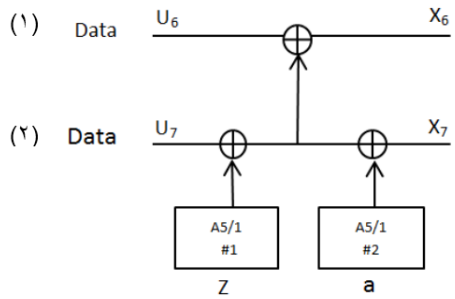
یکی از مهمترین مسایلی که برای طراحی یک سیستم رمزنگاری امن همیشه مهم است، میزان همبستگی اطلاعات زیر بخش‌هایی است که در اختیار تحلیل‌گر سیستم رمز می‌باشد. از دید یک طراح رمزنگار همواره به دنبال کاهش همبستگی اطلاعاتی که ممکن است در دسترس دشمن باشد هستیم [۱۵]. برای این منظور، در این طرح و برای کاهش میزان همبستگی ورودی اطلاعات به کانال‌ها از یک رمزدنباله‌ای 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، $U_7\oplus$ و پس از انجام XOR، در خط شماره ۱، $U_7\oplus U_6\oplus Z$ و در خط شماره ۲، $U_7\oplus Z$ خواهد بود. همان‌طور که مشاهده می‌شود درصورت استفاده از Z (تنها یک LFSR)، بین بیت‌های U_6 و U_7 همبستگی وجود وجود دارد، که دشمن به راحتی می‌تواند U_6 را از روی U_7 به‌دست آورد. (به خاطر داشته باشید که ما به دنبال کاهش تعدادی از LFSRها هستیم، پس نمی خواهیم 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 کرده یک LFSR بر روی بیت آخر هر سیستم (که با "a" نمایش داده شده است)، همبستگی بین دو بیت آخر (در این جا U6 و U7) از بین می‌رود. توجه داشته باشید که اعمال "a" بر روی کل سیستم و بیت‌ها اثر می‌گذارد.

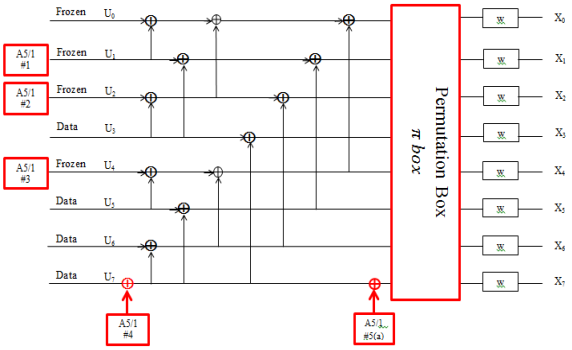
در این‌حالت و پس از انجام XORها، در خط شماره ۱، $U_6\oplus U_7\oplus Z$ و در خط شماره ۲، $U_7\oplus Z\oplus a$ خواهد بود. بدین ترتیب مشاهده می‌شود با اضافه‌کردن LFSR،"a" بر روی بیت آخر، همبستگی بین U_6 و U_7 از بین رفته و دشمن نمی‌تواند U_6 را از روی U_7 به‌دست آورد. همان‌طور که گفته شد، عملکرد و تاثیر 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 دراین روش توجه

کنیـــــــد، در ایـــــــن صـــــــورت $U_1 \oplus U_3 \oplus U_5 \oplus U_7 \oplus Z$، $U_2 \oplus U_3 \oplus U_6 \oplus U_7 \oplus Z$، $U_3 \oplus U_7 \oplus Z$، $U_4 \oplus U_5 \oplus U_6 \oplus U_7 \oplus Z$، $U_5 \oplus U_7 \oplus Z$، $U_6 \oplus U_7 \oplus Z$، $U_7 \oplus Z \oplus a$ خواهد بود.



شکل (۱۰). استفاده از کلید رمز(a) بر روی بیت آخر در سیستم ۸ بیتی Arikan

همان‌طور که مشاهده مـی‌کنیـد، هـیچ دو بیتـی بـا یکـدیگر همبستگی ندارند. در واقع دشمن با استفاده از حملـه همبسـتگی نمی‌تواند بیتی را از روی بیت دیگر به‌دست آورد. تـاثیر وعملکـرد "a" بر روی کل سیستم به خـوبی مشـاهده مـی‌شـود. اگـر کلیـد رمز"a" بر روی بیت آخر اعمال نگردد، سیسـتم در مقابـل حملـه همبستگی شکسته می‌شود و یا درصورتی‌که بخواهیم همبسـتگی بین بیت‌ها را از بین ببـریم بایـد تعـداد بیشـتری کلیـد رمـز بـر روی بیت‌ها قرار دهیم.

حـال، بـا اعمـال "a" تعـداد LFSRهـای مـورد نیـاز کـاهش میابد و LFSRهای اعمال شده بر روی بیت هـای U_0، U_3، U_5، U_6 حذف شده است. از طرفی، بیت‌های رمزشده قبل از ورود به کانال وارد سیستمی شوند تا ترتیب و چیدمان آن‌هـا تغییـر کنـد. یـک جعبه جایگزینی در سیستم قرار می‌دهیم تا عمـل جـایگزینی بـر روی بیت‌های رمزشده، قبل از ورود بـه کانـال انجـام شـود. ایـن عمل، باعث افزایش پیچیدگی سیستم می‌شود. حسن اسـتفاده از جعبه جایگزینی پیشنهادی (Π-Box) این است کـه بـرای تعـداد بیت‌های کم (مثلا ۲ بیت و ۴ بیت) نیـز قابـل اسـتفاده اسـت در حالی‌که دیگر الگوریتم‌ها (مثلا الگوریتم AES) برای تعـداد بیـت کم، قابل استفاده نیستند. طرز کار جعبـه جـایگزینی پیشـنهادی بدین صورت است که با انجام عمل جـایگزینی بـر روی بیـت‌هـا، پیچیدگی معادل $\frac{\log(n!)}{log2}$ به سیستم اضافه می‌کند. (n بیان‌کننـده تعداد کل بیت‌ها در هر سیستم است).

۶- محاسبه پیچیدگی سیستم ۸ بیتـی در طـرح پیشنهادی جدید

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

اثبات: در طرح ۸ بیتی پیشنهادی، از ۵ عدد LFSR، A5/1 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. n بیان‌کننده تعداد کل بیت‌ها است. پس پیچیدگی کل سیستم برابراست با:

$$\chi = 2^{316.6} \times 2^{15.29} = 2^{331.89}. \qquad (۱)$$

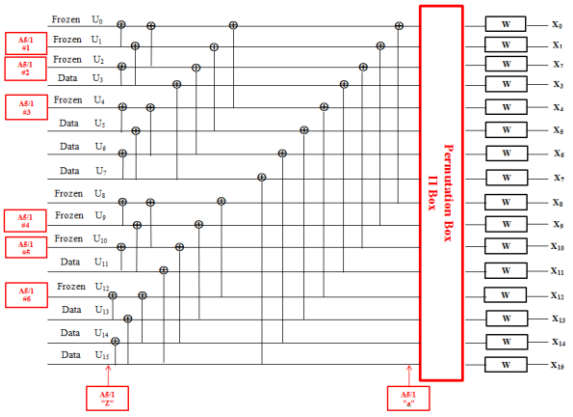
۷- سیستم ۱۶ بیتی Arikan در طـرح جدیـد و محاسبه پیچیدگی آن

در شـکل (۱۱) طـرح پیشـنهادی بـرای سیسـتم ۱۶ بیتـی 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_{14}، U_{13}، U_{11}، U_8، U_7، U_6، U_5، U_3، U_0) 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 16 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 ۸ بیتی Arikan

پیچیدگی هرA5/1 برابر $O(2^{63.32})$ می‌باشد پس پیچیدگی کل A5/1ها برابر $O(2^{506.56})$ می شود. همان‌طورکه در شکل مشاهده می‌شود سیستم دارای یک جعبه جایگزینی (Π-Box) برای انجام عمل جایگزینی است که پیچیدگی آن برای ۱۶ بیت

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

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

۸- ارائـــه فرمـــول بـــرای بـــه‌دســـت آوردن "حداقل تعداد کلید رمز" مورد نیاز

قضیه ۴: برای یک کد قطبی nتایی، تعداد بیت لازم برای رمزنگاری ایمن، ۳n-۴ می‌باشد و پیچیدگی کل سیستم، پیچیدگی فضای حداقل کلید لازم، برابر $(\chi_{A5/1})^{3n-4} \times n!$ است.

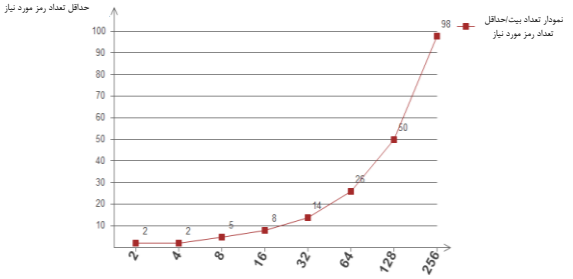
اثبات: دو بیت انتهایی به دلیل وجود بیت‌های رمزشده a و Z احتیاج به رمز ندارد. پس از n بیت تنها n-2 بیت به رمز احتیاج دارند. طبق شکل (۱۰) برای هر ۸ بیت تنها ۳ بیت $(log8 = 3)$ برای رمز احتیاج است در نتیجه برای n بیت تنها $3(n-2) = 3n-6$ لازم است و با حساب دو بیت a و Z حاصل برابر ۳n-۴ می‌شود.

طرح ۸ بیتی و ۱۶ بیتی Arikan با اعمال حداقل تعداد کلید رمز (LFSR A5/1) شرح داده شد و محاسبه پیچیدگی آن‌ها مشاهده گردید. اگر تعداد بیت‌ها افزایش یابد (مثلا ۳۲، ۶۴، ۱۲۸ بیت و ...) می‌توان حداقل تعداد کلید مورد نیاز و پیچیدی سیستم را با استفاده قضیه۳ به‌دست آورد. در جدول (۱)، تعداد بیت‌ها، حداقل کلیدهای مورد نیاز و پیچیدگی محاسبه‌شده برای هر سیستم را مشاهده می‌کنید.

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

تعداد بیت (n)	حداقل تعداد رمز مورد نیاز (۳n-۴)	پیچیدگی(Compelexity)
۲	۲	$۲^{۱۲۶.۶۴}$
۴	۲	$۲^{۱۲۸.۹۳}$
۸	۵	$۲^{۳۳۱.۸۹}$
۱۶	۸	$۲^{۵۵۰.۸۱}$
۳۲	۱۴	$۲^{۱۰۰۴.۱۴}$
۶۴	۲۶	$۲^{۱۹۴۲.۳۱}$
۱۲۸	۵۰	$۲^{۳۸۸۲.۱۴}$

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



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 ارایه‌شده این مقاله با دو روش مطرح‌شده اخیر در [۱۷-۱۶] می‌پردازیم. روش توام کدگذاری و رمزنگاری برای اولین بار توسط مک آلیس در [۱۸] ارایه شد و همه روش‌ها و مقالات ارایه‌شده در این حوزه تلاش می‌کنند تا با استفاده از تکنیک مشابه روش مک آلیس سیستم‌های توام کدینگ کانال و رمز را معرفی نمایند. در این حالت باید از مخفی نمودن ماتریس مولد کد برای رمزنگاری بهره جست.

اما روش ارایه‌شده در مقاله حاضر، به‌جای اختفای ماتریس مولد کلمه کد از ورودی‌های رمزشده و خاصیت خوب "بیت‌های ثابت‌شده" کدهای قطبی بهره می‌گیرد. در واقع روش ارایه‌شده درمقاله حاضر، تلفیق کدینگ کانال و رمزنگاری مناسبی بوده که این روش اولین تکنیک تلفیق از دسته خانواده‌های جدید تلفیق رمزنگاری و کدینگ کانال که مبتنی بر خاصیت ذاتی کدینگ قطبی می‌باشد، بوده و تاکنون چنین روشی ارایه نشده است.

برای مقایسه روش ارایه‌شده 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 می‌باشد و بر اساس ماتریس مولد کد قطبی که دارای پیچیدگی زیادی برای طراحی می‌باشد، نیست.

طبق [۱۶]، برای یک کد قطبی به طول ۱۰۲۴ با نرخ ۰,۷۵ پیچیدگی فضای کلید برابر $۲^{۲۷۱}$ می‌باشد. روش ارایه‌شده به‌جای رسیدن به این پیچیدگی در طول ۱۰۲۴، در طول ۸ و با بهره‌گیری از ۵ عدد LFSR به این پیچیدگی می‌رسد.

میزان پیچیدگی گزارش‌شده در [۱۷] نیز برابر $۲^{n(n+1)-1}$ می‌باشد. از طرفی در روش پیشنهادی با پیچیدگی $۲^{(189.96n-253.28)}$ و برابر قرار دادن توان‌های درجات پیچیدگی

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

۱۰- نتیجه‌گیری

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 جریانی مبتنی بر الگوریتم شناخته‌شده 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 می کند. 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.

[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 Shooshtari, 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 Labaratory, Pasadena, CA, pp. 114-116, 1978.

Journal Of Electronical & Cyber Defence
Vol. 4, No. 1, 2016, Serial No.13

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