تاریخ دریافت: ۱۴۰۲/۱۰/۲۵ پژوهشنامه علوم دفاعی، بهار ۱۴۰۳
تاریخ پذیرش: ۱۴۰۳/۰۳/۲۳ ص ص ۲۹ تا ۴۳

ساخت کدهای جدید بر پایه ساختارهای ضرب تانسوری

سلیمان عسکری[۱]

چکیده

هدف اصلی این مقاله استفاده از ضرب‌های تانسوری و روابط بین آنها در فرایند کدگذاری شبکه به جهت مقابله با حملات تخریبی و آلودگی دشمن به شبکه انتقال اطلاعات می‌باشد. همان‌طور که می‌دانیم یکی از پیچیده‌ترین و در عین حال جدیدترین تهدیدات مهم شبکه‌های کدگذاری شده، حمله آلودگی و مخرب می‌باشد که با ورود، هدایت و نفوذ بسته‌های اطلاعاتی غیر مجاز به جریان اطلاعاتی در گردش شبکه، سعی و تلاش در انحراف و تخریب گردش اطلاعات می‌نماید. در این پژوهش جهت افزایش توان عملیاتی شبکه انتقال اطلاعات و نیز به منظور مقابله با تهدیدات شنود، تخریب و آلودگی شبکه، یک مدل ریاضی از کدگذاری تصادفی شبکه بنام کدهای ساخته شده با استفاده حاصل‌ضرب تانسوری ساده دو زیرفضا را مورد مطالعه قرار داده و ساختارهای جدیدی از کدها با پارامترهای بهینه شده را به دست آوردیم که علاوه بر بهبود نتایج پیشین، موجب افزایش توان عملیاتی شبکه، کاهش زمان انتقال اطلاعات، افزایش ضریب ایمنی شبکه و کاهش انرژی و هزینه‌های پهنای باند مصرفی شبکه می‌شوند.
در این راستا و در جهت مقابله با حملات آلودگی شبکه، رده جدیدی از کدهای مدار آبلی را مورد بررسی قرار داده و با استفاده ازحاصل ضرب تانسوری ساده دو زیرفضا، چند روش ساخت کدهای جدید را بیان می‌کنیم.

واژه‌های کلیدی : کدهای مدار آبلی، حاصل‌ضرب تانسوری ساده، حملات آلودگی، امنیت تبادل اطلاعات.

[۱] استادیار ریاضی، گروه ریاضی دانشکده علوم پایه، دانشگاه امام علی (ع)، تهران، ایران

مقدمه و بیان مسئله

همان‌طور که می‌دانیم دامنه جنگ‌های اطلاعاتی به طور گسترده‌ای افزایش یافته است و حوزه‌های مختلفی را در بر گرفته است. جنگ اطلاعاتی، دیگر ماجراجویی ساده در عرصه سرقت‌های کامپیوتری محسوب نمی‌شود، بلکه یکی از اصلی‌ترین فعالیت‌های نظامی ارتش‌های جهان است که در کنار تجهیزات لجستیکی و تسلیحات هدایت‌شونده جدید به کار می‌آید. در واقع، جنگ اطلاعاتی، آن دسته از فعالیت‌هایی است که با هدف ایجاد اختلال، تخریب، و جلوگیری از دستیابی دشمن به اطلاعات در عملیات‌های پدافندی و آفندی انجام می‌گیرد.
با توجه به پیشرفت فناوری اطلاعات در کشورهای مختلف به ویژه کشور ایران که در این حوزه نیز پیشگام بوده و بودجه‌های قابل توجهی را نیز به این مهم اختصاص داده است، ضرورت استفاده از فناوری اطلاعات در همه سازمان‌های تابعه کشور امری غیر قابل انکار است. ارتش جمهوری اسلامی ایران نیز همانند سایر ارگان‌ها بسیاری از خدمات خود را از طریق فناوری اطلاعات انجام می‌دهد که از این جنبه، ضرورت تبادل داده‌ها در یک بستر امن امری انکارناپذیر است. از مهمترین رویکردهای جلوگیری از دستیابی دشمن به اطلاعات در عملیات‌های پدافندی و آفندی، استفاده از کدگذاری می‌باشد. اگرچه برخی سیستم‌های کدگذاری با استفاده از روش‌های ریاضی به صورت از پیش تعریف شده موجودند، اما با توجه به ماهیت سازمانی ارتش لزوما قابل استفاده برای ارتش جمهوری اسلامی ایران نمی‌باشند. لذا نیاز است تا برخی از این سیستم‌های کدگذاری بهینه‌سازی و بومی‌سازی گردند که این امر از اهداف اصلی این پژوهش می‌باشد. در یک شبکه اطلاعات، شبکه نسبت به انتشار خطا بسیار حساس خواهد بود. در واقع ورود حتی یک بسته‌ی خراب می‌تواند منجر به خراب شدن همه‌ی اطلاعات شود. این نکته خود گویای اهمیت و ضرورت استفاده از سیستم‌های کدگذاری شبکه می‌باشد. این وضعیت، با توجه به موقعیت ویژه ایرانِ مستقل در جهان دو قطبی امروز و نیز جنگ نرم همه جانبه‌ای که از سوی قدرت‌های بزرگ علیه سازمان‌های علمی و نظامی کشورمان در جریان است، ضرورت و اهمیت استفاده از سیستم‌های کدگذاری را برای ارتش جمهوری اسلامی ایران دوچندان می‌کند. همچنین، از دیدگاه نظامی و امنیتی، عدم بکارگیری سیستم‌های کدگذاری علاوه بر اینکه موجب دریافت اطلاعات با اختلال بسیار بالا در مقصد خواهد شد، بلکه ضریب امنیت اطلاعات را نیز بسیار کاهش داده و خطر مسدودسازی یا ایجاد اختلال در آن اطلاعات توسط دشمن را نیز افزایش می‌دهد. در این پروژه روش‌های موثر جبری در ایجاد سیستم‌های کدگذاری اطلاعات را مورد مطالعه قرار داده و از طریق بهبود بخشیدن به برخی ساختارهای بکاررفته در این فرآیند، امکان ایجاد سیستم‌های جدید کدگذاری اطلاعات را فراهم می‌نمائیم. همچنین فرض بر این است که خواننده با تعاریف و اصطلاحات مقدماتی جبر آشنایی دارد.

پیشینه تحقیق و مبانی نظری

به دنبال ارتقای جایگاه و اهمیت سیستم‌های اطلاعاتی و شبکه‌های مخابراتی در سیاست‌های دفاعی بسیاری از کشورها، موضوع وابستگی به فناوری ارتباطات و اطلاعات بیش از پیش مورد توجه قرار گرفته است. در چنین شرایطی، حفظ امنیت پیام‌ها و اطلاعات نظامی ارتش جمهوری اسلامی ایران از اهمیتی غیرقابل انکار برخوردار است و استفاده از روش‌های کدگذاری پیام‌ها و اطلاعات یکی از راه‌های موثر و کارا در این راستا

می‌باشد. افزایش توان عملیاتی یکی از چالش‌های مهم تحقیقاتی در سیستم‌های ارتباطی بی‌سیم است. پیش‌بینی می‌شود که نیازهای توان عملیاتی شبکه برای شبکه‌های بی‌سیم در آینده بسیار بیشتر از امروز باشد. باند فرکانس یک منبع محدود است، بنابراین راه‌حل‌های جدیدتر و پیچیده‌تری برای به حداکثر رساندن داده‌های تحویل‌شده در این طیف محدود مورد نیاز است. کدگذاری شبکه خطی تصادفی برای افزایش توان عملیاتی اطلاعات با اجازه دادن به ترکیب خطی تصادفی بسته‌ها در یک شبکه استفاده می‌شود. یعنی هر گره داخلی شبکه ترکیبات خطی تصادفی بسته‌های دریافتی را به گره‌های مجاور منتقل می‌کند. با توجه به روش کدگشایی، گیرنده‌ها قادر به بازسازی بسته‌های اصلی هستند که در منابع آن به شبکه تزریق شده است. اگرچه این روش بسیار موثر است، اما نسبت به انتشار خطا بسیار حساس است. برای حل این مشکل یک مدل ریاضی از کدگذاری تصادفی شبکه بنام کدهای مدار آبلی ساخته شده با استفاده از حاصل‌ضرب تانسوری ارائه می‌شود؛ که در آن پیام‌ها به صورت زیرفضاهایی از یک فضای برداری ثابت روی یک میدان متناهی در نظر گرفته می‌شوند. کدهای زیرفضای اخیر مورد توجه تحقیقات بسیاری قرار گرفته‌اند. یک رده مهم از کدهای زیرفضا، کدهای موسوم به کدهای مدار می‌باشند. کدهای مدار معمولا بوسیله گروهی که مدار را تولید می‌نماید شناسایی و دسته‌بندی می‌شوند. به عنوان مثال اگر گروه مولد مدار گروهی دوری باشد، کد مدار حاصل را دوری می‌نامند. هدف اصلی ما در این تحقیق بررسی این مسئله و ارائه ساختارهای جدیدی از کدهای مدار آبلی می‌باشد که دارای دارای بیشترین فاصله کمینه کدکلمات هستند.برای این منظور از صورت حاصل‌ضرب تانسوری قضیه مشهور اشباخر- دنکین[۱] درخصوص رده‌بندی زیرگروه‌های ماکسیمال گروه خطی عام یعنی $\mathrm{GL}(n,q)$ برای انتخاب فرم زیرگروه تولیدکننده مدار استفاده می نمائیم که ضمن پاسخ‌گویی به مسئله ارائه‌شده فوق، ساختار کدهای ارائه‌شده در این تحقیق و پارامترهای کدهای ساخته‌شده در (چن[۲]، ۲۰۲۰، ۳) و (کلیمنت[۳]، ۲۰۱۹، ۴) را بطور محسوسی بهبود می‌بخشیم.

روش‌شناسی پژوهش

استفاده از حاصل‌ضرب تانسوری ساده جهت ساخت کدهای مدار آبلی و غیر آبلی یکی از پژوهش‌های نوین در بحث کدگذاری شبکه به منظور جلوگیری از حملات آلودگی و تخریب می‌باشد. در واقع استفاده از حاصل‌ضرب تانسوری ساده روشی نظام‌مند جهت ساخت کدهای مدار از اندازه بزرگتر و با پارامترهای بهینه از روی کدهای مدار کوچکتر به دست می‌دهد. با استفاده از روش‌های محاسباتی در نظریه گروه‌ها، به تازگی زیرگروه‌های ماکسیمال گروه‌های کلاسیک از بعد حداکثر ۱۲ به طور دقیق رده‌بندی و مشخص گردیدند. بنابراین این رده از زیرگروه‌ها انتخاب مناسبی برای ساخت کدهای مدار می‌باشند.

یافته‌ها

تعریف ۱. فرض کنید q توانی از عدد اول p باشد. میدان متناهی با q عضو را با F_q نشان می‌دهیم. در این صورت p مشخصه میدان است و

$$F^{*}_{q} = F_q - \{0\}$$

گروه ضربی میدان است که شامل تمام عناصر وارون‌پذیر میدان می‌باشد.

تعریف ۲. فضای برداری F_q^n را در نظر بگیرید. یک هندسه تصویری از F_q^n مجموعه همه زیرفضاهای فضای برداری F_q^n است که با $PG(n-1,q)$ نشان داده می‌شود. مجموعه همه زیرفضاهای با بعد k از F_q^n را گراسمانیان می‌گوییم و با نماد $\varsigma_q(k,n)$ نشان می‌دهیم. همچنین تعداد اعضای یک گراسمانیان از رابطه

$$|\varsigma_q(k,n)| = \frac{\prod_{i=n-k+1}^{i=n}(q^i-1)}{\prod_{i=1}^{i=k}(q^i-1)}$$

محاسبه می‌گردد.

تعریف ۳. یک کد زیرفضایی C زیر مجموعه‌ای از $PG(n-1,q)$ است. اگر همه کد کلمات C دارای بعد یکسان k باشند، آنگاه C را یک کد با بعد ثابت می‌نامیم و داریم $C \subseteq \varsigma_q(k,n)$

عملگر ضرب تانسوری برای کدهای زیرفضایی

در این بخش مفهوم عملگر ضرب تانسوری را برای کدهای زیرفضایی معرفی می‌کنیم. استفاده از این مفهوم روشی را جهت ساخت کدهای زیرفضایی جدید از اندازه بزرگتر از روی کدهای زیرفضایی کوچکتر ارائه می‌دهد که بسیاری از ویژگی‌های کد اصلی اولیه، از جمله بعد و کمترین فاصله کد کلمات را نیز حفظ می‌کنند. به طور خاص با استفاده از عملگر ضرب تانسوری کدهای مدار جدیدی از اندازه‌های بزرگ می‌سازیم. در ابتدا مفهوم ضرب تانسوری را مرور می‌نماییم.

ساختار جبری ضرب تانسوری

ابتدا به تعریف مفهوم R - مدول می‌پردازیم. مدول‌ها در واقع تعمیم طبیعی فضاهای برداری می‌باشند. اگر در تعریف F- فضای برداری، به جای میدان F ، حلقه R را قرار دهیم، ساختار مدولی به دست می‌آید.

تعریف ۴. فرض کنید R یک حلقه یکدار و M مجموعه‌ای ناتهی باشد. M را همراه عمل جمع

$$+ : M \times M \to M$$

و عمل ضرب

$$. : R \times M \to M$$

یک R - مدول چپ می‌نامند، هرگاه

الف) $(M, +)$ یک گروه آبلی باشد؛

ب) به ازای هر $x,y \in M$ و $r \in R$ داشته باشیم

$$r(x+y) = rx + ry$$

ج) به ازای هر $x \in M$ و $r,s \in R$ داشته باشیم

$$(r+s)x = rx + sx$$

و

$$(rs)x = r(sx)$$

د) به ازای هر $x \in M$ داشته باشیم $1x = x$.

فرض کنید M و N دو مجموعه ناتهی باشند. $\mathbf{Z}^{(M\times N)}$ را مجموعه تمام حاصل جمع‌های صوری مثل

$$\sum_{i=1}^{t} n_i(x_i y_i)$$

در نظر می‌گیریم. یعنی

$$\mathbf{Z}^{(M\times N)} = \{\sum_{i=1}^{t} n_i(x_i y_i), n_i \in \mathbf{Z}, (x_i, y_i) \in M \times N\}$$

تساوی دو عضو از $\mathbf{Z}^{(M\times N)}$ را به طور طبیعی، تساوی ضرایب متناظر آنها تعریف می‌کنیم. یعنی دو عضو دلخواه از $\mathbf{Z}^{(M\times N)}$ مثل $\sum_{i=1}^{t} n_i(x_i y_i)$ و $\sum_{i=1}^{t} n_i'(x_i y_i)$ را مساوی می‌نامیم و می‌نویسیم $\sum_{i=1}^{t} n_i(x_i y_i) = \sum_{i=1}^{t} n_i'(x_i y_i)$ اگر و فقط اگر برای هر $1 \le i \le t$ داشته باشیم $n_i = n_i'$.

حال می‌خواهیم یک عمل جمع روی $\mathbf{Z}^{(M\times N)}$ تعریف کنیم که آن را به گروهی آبلی تبدیل کند. این کار نیز به صورت طبیعی انجام می‌شود. کافی است عمل

$$+ : \mathbf{Z}^{(M\times N)} \times \mathbf{Z}^{(M\times N)} \to \mathbf{Z}^{(M\times N)}$$

را به صورت

$$\sum_{i=1}^{t} n_i'(x_i y_i) + \sum_{i=1}^{t} n_i(x_i y_i) = \sum_{i=1}^{t} (n_i + n_i')(x_i y_i)$$

تعریف کنیم. به راحتی دیده می‌شود که $\mathbf{Z}^{(M\times N)}$ با این عمل جمع به گروهی آبلی تبدیل می‌شود. حاصل‌ضرب تانسوری دو مدول که در زیر آورده شده است؛ به کمک این گروه آبلی تعریف می‌شود.

تعریف ۵. فرض کنید M یک R- مدول راست، N یک R - مدول چپ و F را گروه آبلی $\mathbf{Z}^{(M\times N)}$ در نظر بگیرید. گیریم K زیرگروهی از F باشد که توسط اعضای

$$(x+x',y)-(x,y)-(x',y)$$

و

$$(x,y+y')-(x,y)-(x,y')$$

و

$$(xr,y)-(x,ry)$$

تولید شده که در آن $x,x'\in M$ ، $y,y'\in N$ و $r\in R$ است. در این صورت گروه آبلی F/K را حاصل ضرب تانسوری M و N می‌نامیم و آن را با $M\otimes_R N$ نشان می‌دهیم. اگر M یک R- مدول راست و N یک R- مدول چپ باشد، عضو $(x,y)+K$ از گروه آبلی $M\otimes_R N=F/K$ را با $x\otimes y$ نشان می‌دهیم.

در ادامه برخی از خواص مهم حاصل ضرب تانسوری مدول‌ها که مورد استفاده قرار خواهد گرفت را مرور می‌نماییم.

ملاحظه ۱. با استفاده از تساوی‌های

$$(x+x')\otimes y=(x\otimes y)+(x'\otimes y)$$

و

$$x\otimes(y+y')=(x\otimes y)+(x\otimes y')$$

به راحتی نتیجه می‌شود که

$$0\otimes y=x\otimes 0=0$$

که چنین خاصیتی در ضرب و جمع مستقیم دو مدول یا فضای برداری وجود ندارد.

ضرب تانسوری ماتریس‌ها و فضای برداری

در این قسمت به تشریح مفهوم ضرب تانسوری برای فضاهای برداری خواهیم پرداخت.

اگر U یک فضای برداری با پایه $\{u_1,...,u_k\}$ و W یک فضای برداری با پایه $\{w_1,...,w_k\}$ باشد، آنگاه حاصل‌ضرب تانسوری U و W که آن را با نماد $V=U\otimes W$ نمایش می‌دهیم یک فضای برداری با بعد $n=km$ و پایه $\{v_1,...,v_{km}\}$ است که در آن $v_{i+k(j-1)}=u_i\otimes w_j$. اگر $A=(a_{ij})$ یک ماتریس $k\times k$ باشد که روی U عمل می‌کند و $B=(b_{ij})$ یک ماتریس $m\times m$ باشد که روی W عمل می‌کند، آنگاه عمل

$A\otimes B$ را روی $U\otimes W$ خواهیم داشت که هر عنصر $u_i\otimes w_j$ را به عنصر $Au_i\otimes Bw_j$ نگاشت می‌کند که در آن

$$Au_i\otimes Bw_j=\sum_{r=1}^{k}\sum_{s=1}^{m}a_{ir}b_{js}(u_r\otimes w_s).$$

ماتریس $n\times n$ متناظر که آن را با نماد $A\circ B$ نمایش می‌دهیم را حاصل‌ضرب تانسوری دو ماتریس A و B می‌نامند.

لم ۱: فرض کنید $G_1\in GL_{n1}(q)$ و $G_2\in GL_{n2}(q)$ دو زیرگروه ماتریسی باشند.در این صورت

$$G_1\circ G_2=\frac{G_1\times G_2}{\{(\lambda I_{n1},\lambda^{-1}I_{n2}):\lambda I_{n1}\in G_1,\lambda^{-1}I_{n2}\in G_2\}}.$$

برهان : به مرجع [3] مراجعه شود.

حاصل‌ضرب تانسوری کدهای زیرفضایی

در این بخش مفهوم ضرب تانسوری کدهای زیرفضایی را معرفی نموده و پارامترهای اساسی چنین کدهایی را به طور دقیق مشخص می‌نماییم. سپس با استفاده از این مفهوم روش ساخت کدهای مدار جدید از اندازه‌های بزرگ را ارائه می‌نماییم.

تعریف ۶ : فرض کنید $C_1\subseteq\varsigma_q(k_1,n_1)$ و $C_2\subseteq\varsigma_q(k_2,n_2)$ دو کد زیرفضایی باشند. در این صورت حاصل‌ضرب تانسوری C_1 و C_2 که آن را با نماد $C_1\otimes C_2$ نشان می‌دهیم به صورت

$$C_1\otimes C_2=\{(U\otimes W):U\in C_1,W\in C_2\}$$

تعریف می‌شود.

قضیه۱ : فرض کنید $C_i\subseteq\varsigma_q(k_i,n_i)$ برای $i=1,2$ یک کد زیرفضایی با پارامترهای $[n_i,M_i,d_i;k_i]$ باشد. در این صورت $C_1\otimes C_2$ نیز یک کد زیرفضایی با پارامترهای $[n_1n_2,M_1M_2,d;k_1k_2]$ است که در آن

$$d=2(k_1k_2-d_1^{\max}d_2^{\max})$$

و

$$d_i^{\max}=\max\{\dim(U\bigcap W):U,W\in C_i\}$$

برهان : فرض کنید $U_i \in C_i$. از تعریف حاصل‌ضرب تانسوری نتیجه می‌شود

$$\dim(U_1 \otimes U_2) = \dim(U_1)\dim(U_2) = k_1 k_2$$

و $U_1 \otimes U_2 \in \varsigma(k_1 k_2, n_1 n_2)$. بعلاوه با توجه به تعریف ۶ نتیجه می‌شود

$$|C| = |C_1| \times |C_2| = M_1 M_2$$

حال به تعیین مینیمم فاصله کد حاصل‌ضرب می‌پردازیم. با توجه به تعریف داریم

$$d(C) = \min\{\mathrm{d}((U_1 \otimes U_2),(W_1 \otimes W_2)) := U_i \in C_i, W_i \in C_i\}$$

$$= \min\{\dim(U_1 \otimes U_2) + \dim(W_1 \otimes W_2)$$

$$-2\dim((U_1 \otimes U_2) \bigcap (W_1 \otimes W_2)) : U_i \in C_i, W_i \in C_i\}$$

$$= \min\{2k_1 k_2 - 2\dim((U_1 \bigcap W_1) \otimes (U_2 \bigcap W_2)) : U_i \in C_i, W_i \in C_i\}$$

$$= \min\{2k_1 k_2 - 2\dim((U_1 \bigcap W_1)\dim(U_2 \bigcap W_2)) : U_i \in C_i, W_i \in C_i\}$$

$$= 2k_1 k_2 - 2{d_1}^{\max}{d_2}^{\max}$$

□

حال مفهوم عملگر جمع را برای کدهای زیرفضایی به صورت

$$C_1 + C_2 := \{U + W : U \in C_1, W \in C_2\}$$

تعریف می‌کنیم. لازم به ذکر است که به ندرت پیش می‌آید که حاصل جمع دوکد زیرقضایی که هر دو اسپرید جزئی هستند نیز خود یک اسپرید جزئی باشد. مثال زیر این حقیقت را روشن می‌کند.

مثال ۱: فرض کنید C_1 و C_2 دو کد زیرفضایی باشند که اسپرید جزئی هستند. بعلاوه فرض کنید $U_1 \in C_1$ و $W_1, W_2 \in C_2$. در این صورت داریم

$$U_1 + W_1 \in C_1 + C_2$$

و

$$U_1 + W_2 \in C_1 + C_2$$

که از آن نتیجه می‌شود

$$U_1 \subseteq (U_1 + W_1) \bigcap (U_1 + W_2)$$

بنابراین دو کد کلمه فوق دارای اشتراک نابدیهی بوده و بنابراین $C_1 + C_2$ اسپرید جزئی نیست.

بر خلاف عملگر جمع که در بالا تعریف شد، نشان می‌دهیم که عملگر ضرب تانسوری خاصیت اسپرید جزئی بودن را حفظ می‌کند. در واقع نشان می‌دهیم که حاصل‌ضرب تانسوری دو کد زیرفضا که لااقل یکی از آنها اسپرید جزئی باشد، خود یک کد زیرفضایی اسپرید جزئی می‌باشد.

قضیه ۲: فرض کنید $C_i \subseteq \varsigma_q(k_i, n_i)$ برای $i = 1, 2$ دو کد زیرفضایی باشند که لااقل یکی از آنها اسپرید جزئی می‌باشد. در این صورت $C_1 \otimes C_2$ نیز یک اسپرید جزئی از اندازه $|C_1| \times |C_2|$ است.

برهان : با توجه به اینکه یکی از دو کد زیرفضایی اسپرید جزئی می‌باشند، خواهیم داشت $d_1^{\max} = 0$ یا $d_2^{\max} = 0$. در نتیجه از قضیه ۱ حکم نتیجه خواهد شد.

ملاحظه زیر توضیح می‌دهد چگونه بسیاری از کدهای مدار اسپرید جزئی به طور طبیعی به عنوان توسیعی از یک کد مدار از طول کوچکتر رخ می‌دهند.

ملاحظه ۲: فرض کنید گروه $G \le GL_n(q)$ روی فضای برداری n بعدی V به صورت غیر اولیه عمل کند. بنابراین تجزیه $V = V_1 \oplus V_2 \oplus ... \oplus V_m$ به جمع مستقیم $m > 1$ زیر فضای k بعدی V_i را خواهیم داشت که در آن G به صورت متعدی بلوک‌های V_i را جابجا می‌کند. بنابراین کد مدار $C = G.V_1$ یک اسپرید جزئی با پارامترهای $[n, M, 2k; k]$ است. حال با فرض اینکه عمل گروه $H = Stab_G(V_1)$ روی V_1 نیز یک عمل غیر اولیه است، مشابه قبل خواهیم داشت $V_1 = W_1 \oplus ... \oplus W_s$ که در آن گروه H زیرفضاهای t بعدی W_i را به صورت متعدی جابجا می‌کند. در این حالت کد مدار C توسیعی از کد مدار $C_1 = H.V_1$ خواهد بود که دارای پارامترهای $[k, s, 2t; t]$ می‌باشد. بنابراین نشان دادیم که یک کد مدار با پارامترهای $[n, M, 2k; k]$ به طور طبیعی به عنوان توسیعی از کد مدار با پارامترهای $[k, s, 2t; t]$ رخ می‌دهد که در آن $n > k$. شایان ذکر است که چنین شرایطی برای اکثر کدهای مدار اسپرید جزئی رخ می‌دهد. زیرا بنا بر داده‌های محاسباتی، تعداد گروه‌های جایگشتی غیر اولیه از یک درجه ثابت بسیار بیشتر از تعداد گروه‌های اولیه است.

در ادامه نتایج به دست آمده در بالا را برای کدهای مدار بررسی و بیان می‌کنیم.

تعریف ۷. فرض کنید U_i که $i \in \{1, 2\}$ زیرفضایی از $\mathrm{F}_q^{n_i}$ و $G_i \le GL_{n_i}(q)$ گروه‌هایی باشند به طوری که $C_i = G_i U_i$ یک کد مدار است. در این صورت ضرب تانسوری این دو کد مدار که با نماد $C_1 \otimes C_2$ نمایش داده می‌شود به صورت

$$C_1 \otimes C_2 = \{(A.U \otimes B.W) : A \in G_1, B \in G_2\}$$

تعریف می‌شود.

قضیه ۳. فرض کنید U_i که $i \in \{1,2\}$ زیرفضایی از $\mathrm{F}_q^{n_i}$ و $G_i \le GL_{n_i}(q)$ گروه‌هایی باشند به طوری که $C_i = G_i U_i$ یک کد مدار با پارامترهای $[n_i, M_i, d_i; k_i]$ است. در این صورت $C_1 \otimes C_2$ نیز یک کد مدار با پارامترهای $[n_1 n_2, M_1 M_2, d; k_1 k_2]$ بوده و داریم $C = (G_1 \circ G_2).(U_1 \otimes U_2)$ که در آن $d = 2(k_1 k_2 - d_1^{\max} d_2^{\max})$.

برهان. مشابه اثبات قضیه ۲ است.

نتیجه ۱. فرض کنید U_i که $i \in \{1,2\}$ زیرفضایی از $\mathrm{F}_q^{n_i}$ و $G_i \le GL_{n_i}(q)$ گروه‌هایی باشند به طوری که $C_i = G_i U_i$ کدهای مدار باشند که حداقل یکی از آنها اسپرید جزئی باشد. در این صورت $C_1 \otimes C_2$ نیز یک کد مدار اسپرید جزئی از اندازه $|C_1| \times |C_2|$ است.

برهان. ابتدا توجه داریم که $C_1 \otimes C_2$ یک کد مدار است. برای اثبات اینکه این کد مدار یک اسپرید جزئی است، کافی است نشان دهیم که اشتراک هر دو عضو متمایز از کد مدار برابر صفر است. برای این منظور فرض کنید $g_1 \in G_1$ و $g_2 \in G_2$ به طوری که

$$(g_1, g_2) \notin Stab_{G_1}(U_1) \times Stab_{G_2}(U_2).$$

با فرض خلف گیریم

$$(U_1 \otimes U_2) \bigcap (g_1.U_1 \otimes g_2.U_2) \neq 0$$

در این صورت، با استفاده از [۵ صفحه ۳۵۸۳] خواهیم داشت

$$(U_1 \otimes U_2) \bigcap (g_1.U_1 \otimes g_2.U_2) = (U_1 \bigcap g_1.U_1) \otimes (U_2 \bigcap g_2.U_2) \neq 0$$

از اینجا نتیجه می‌شود

$$U_1 \bigcap g_1.U_1 \neq 0$$

و

$$U_2 \bigcap g_2.U_2 \neq 0$$

که با فرض قضیه متناقض است. بنابراین فرض خلف باطل و حکم ثابت می‌شود.

ساختارهای تانسوری و کدهای مدار آبلی غیر دوری

در این بخش با استفاده از نتیجه ۱ روش ساخت رده‌های جدیدی از کدهای مدار آبلی غیردوری از اندازه بزرگ را ارائه نموده و در ضمن نشان می‌دهیم که این کدها اسپرید جزئی نیز می‌باشند.

گروه مولد کد

فرض کنید $V = U \otimes W$ یک تجزیه از فضای برداری mk بعدی به دو زیرفضای k بعدی U و m بعدی W روی میدان متناهی F_q باشد. همچنین فرض کنید $U_1 \leq U$ یک زیرفضای k_1 بعدی و $W_1 \leq W$ یک زیرفضای m_1 بعدی باشند به طوری که $k_1 \leq k/2$ و $m_1 \leq m/2$. بعلاوه فرض کنید $p(x) \in \mathrm{F}_q(x)$ و $q(x) \in \mathrm{F}_q(x)$ دو چندجمله‌ای اولیه از درجات به ترتیب k_1 و m_1 باشند.

با استفاده از ماتریس‌های همراه $p(x)$ و $q(x)$ گروه‌های $G_1 \leq GL_k(q)$ و $G_2 \leq GL_m(q)$ متناظر با چندجمله‌ای‌های $p(x)$ و $q(x)$ را در نظر می‌گیریم. حال حاصل‌ضرب

$$G = G_1 \circ G_2$$

را به عنوان گروه مولد کد در نظر می‌گیریم. به وضوح

$$G \leq GL_k(q) \circ GL_m(q).$$

لم ۲. با مفروضات فوق گروه $G = G_1 \circ G_2$ آبلی است.

برهان . ابتدا توجه داریم که گروه‌های G_1 و G_2 آبلی هستند. بنابراین به راحتی می‌توان دید که $G = G_1 \circ G_2$ نیز آبلی است.

تشریح ساختار کد

فرض کنید $\beta_1 = \{e_1, ..., e_k\}$ و $\beta_2 = \{f_1, ..., f_m\}$ دو پایه ستونی برای زیرفضاهای U و W باشند. قرار می‌دهیم

$$U_1 = < e_{k-k_1+1}, ..., e_k >$$

و

$$W_1 = < f_{m-m_1+1}, ..., f_m >.$$

در این صورت داریم $\dim(U_1) = k_1$ و $\dim(W_1) = m_1$.

قضیه ۴. با مفروضات فوق کد $C = C_1 \otimes C_2$ که در آن $C_1 := G_1.U_1$ و $C_2 := G_2.W_1$ می‌باشند یک کد مدار اسپرید جزئی با پارامترهای

$$\left[n, q^{k_1+m_1}, 2k_1m_1; k_1m_1 \right]$$

است.

برهان. ابتدا توجه داریم که کدهای مدار آبلی C_1 و C_2 به ترتیب کدهایی با پارامترهای $\left[n, q^{k_1}, 2k_1; k_1 \right]$ و $\left[n, q^{m_1}, 2m_1; m_1 \right]$ می‌باشند. به طور خاص این دو کد هر دو اسپرید جزئی هستند. بنابراین از نتیجه ۱ می‌توان دید که کد مدار $C_1 \otimes C_2$ یک کد اسپرید جزئی با پارامترهای

$$\left[mk, q^{k_1+m_1}, 2k_1m_1; k_1m_1 \right]$$

است.

نتیجه گیری

همان‌طور که می‌دانیم یکی از به روزترین تهدیدات مهم شبکه‌های کدگذاری شده، حمله آلودگی و مخرب می‌باشد که با ورود بسته‌های اطلاعاتی غیر مجاز به جریان اطلاعاتی در گردش شبکه، سعی و تلاش در انحراف و تخریب گردش اطلاعات می‌نماید. در این پژوهش جهت افزایش توان عملیاتی شبکه انتقال اطلاعات و نیز به منظور مقابله با تهدیدات شنود، تخریب و آلودگی شبکه، یک مدل ریاضی از کدگذاری تصادفی شبکه بنام کدهای ساخته شده با استفاده حاصل‌ضرب تانسوری ساده دو زیرفضا را مورد مطالعه قرار داده و ساختارهای جدیدی از کدها با پارامترهای بهینه شده را به دست آوردیم که در این صورت تاثیر خطا و انحراف حاصل شده از ورود یک بسته مخرب در شبکه تا حدی قابل مدیریت خواهد بود. همچنین این روش علاوه بر بهبود نتایج پیشین، موجب افزایش توان عملیاتی شبکه، کاهش زمان انتقال اطلاعات، افزایش ضریب ایمنی شبکه و کاهش انرژی و هزینه‌های پهنای باند مصرفی شبکه می‌شوند.

مراجع

[1] Askary, S. Biranvand, N. and Shirjian, F. (2023). "New constructions of orbit codes based on imprimitive wreath products and wreathed tensor products", The Rendiconti del Circolo Matematico di Palermo 2, Vol. 72, No. 4, PP. 1-14.

[2] Bardestani, F. and Iranmanesh. (2015). "Cyclic orbit codes with the nor-malizer of a Singer subgroup" J. Sci. Islamic Republic Iran. Vol. 26, No.1, PP. 49–55.

[3] Chen, S. and LiangJ. (2020). "New Constructions of Orbit Codes Based on the Operations of Orbit Codes". Acta Math. Appl. Sin. Engl. Ser. Vol. 36, PP. 803–815.

[4] Climent, J. Requena, V. and Soler X. (2019)." A construction of Abelian non-cyclic orbit codes" Cryptogr. Commun. Vol. 11, PP. 839–852.

[5] Kotter, R. and Kschischang, F. (2008). "Coding for errors and erasures in random network coding". IEEE Trans. Inf. Theory, Vol. 54, No.8, PP. 3579–3591.

[6] Trautmann, A Manganiello, F. and Rosenthal. (2010)." Orbit codes a new concept in the area of network coding" In: Proceedings of the 2010 IEEE information theory workshop (ITW 2010), Dublin, Ireland. IEEE.

Construction of new codes based on tensor multiplication structures

Soleyman Askary

Abstract:

The main purpose of this article is to use tensor multiplications and the relationships between them in the network coding process to deal with destructive attacks and enemy contamination to the information transmission network. As we know, one of the most complex and at the same time the most important threats of coded networks are the contamination and malicious attack that attempts to divert and destroy the information flow by entering, directing and penetrating unauthorized information packets into the information flow in the network.

In this research, in order to increase the operational capacity of the information transmission network and also in order to deal with the threats of eavesdropping, destruction and pollution of the network, a mathematical model of random coding of the network called codes made using the simple tensor product of two subspaces has been studied and We obtained new structures of codes with optimized parameters that, in addition to improving the previous results, increase network throughput, reduce information transfer time, increase network safety factor, and reduce energy and bandwidth costs of network consumption.

In this direction and in order to deal with network pollution attacks, we have investigated a new class of Abelian circuit codes and using the simple tensor product of two subspaces, we have expressed some methods of constructing new codes.

Key Words: Abelian circuit codes, simple tensor product, contamination attacks, information exchange security.