تاریخ دریافت: ۱۴۰۳/۰۱/۲۳ پژوهشنامه علوم دفاعی، شماره ۱۷، بهار ۱۴۰۴

تاریخ پذیرش: ۱۴۰۴/۰۳/۲۳ ص ص ۴۱ تا ۵۲

ساخت کدهای مدارجدید در سیستم های مخابراتی بر پایه حاصل‌ضرب های حلقوی غیر اولیه و حاصل ضرب‌های تانسوری حلقوی

سلیمان عسکری[۱]

چکیده

هدف اصلی این مقاله استفاده از حاصل‌ضرب های حلقوی غیر اولیه و حاصل ضرب‌های تانسوری حلقوی و روابط بین آنها در فرایند کدگذاری شبکه به جهت مقابله با حملات تخریبی و آلودگی دشمن به شبکه انتقال اطلاعات می‌باشد. برای این منظور با استفاده از حاصل‌ضرب های حلقوی گروه‌ها و مفاهیم عمل غیر اولیه گروه‌های جایگشتی، زیر فضاهای خاصی از گراسمانیان را در نظر گرفته و به ارائه روشی نظام‌مند جهت ساخت کدهای مدار غیر جابجایی روی این فضاها خواهیم پرداخت. در این پژوهش جهت افزایش توان عملیاتی شبکه انتقال اطلاعات و نیز به منظور مقابله با تهدیدات شنود، تخریب و آلودگی شبکه، به ارائه روش هایی برای ساخت رده‌های جدیدی از کدهای مدار از اندازه بزرگ و دارای بیشینه حداقل فاصله کد کلمات می‌پردازیم.

در این راستا و در جهت مقابله با حملات آلودگی شبکه، رده جدیدی از کدهای مدارجدید بر پایه حاصل‌ضرب های حلقوی غیر اولیه و حاصل ضرب‌های تانسوری حلقوی را مورد بررسی قرار داده و با استفاده ازحاصل ضرب تانسوری حلقوی دو زیرفضا، چند روش ساخت کدهای جدید را بیان می‌کنیم.

واژه‌های کلیدی : کدهای مدار ، حاصل ضرب حلقوی، حاصل‌ضرب تانسوری حلقوی، حملات آلودگی، امنیت تبادل اطلاعات.

---

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

مقدمه و بیان مسئله

می‌دانیم که دامنه جنگ ها در سال‌های اخیر به جنگ‌های سایبری و جنگ‌های اطلاعاتی به طور گسترده‌ای افزایش یافته است و حملات سایبری و آلودگی های شبکه یکی از حملات مخرب به کشورها به حساب می‌آید. جنگ اطلاعاتی، دیگر ماجراجویی ساده در عرصه سرقت‌های کامپیوتری محسوب نمی‌شود، بلکه یکی از اصلی‌ترین فعالیت‌های نظامی ارتش‌های جهان است که در کنار پهپادها، موشک ها، 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 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. 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.

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

فناوری‌های پیچیده دوران مدرن که تمامی حوزه‌های حیات انسانی را درنوردیده، به حوزه جنگ و منازعات نیز رسوخ کرده و بر پویش امنیتی جوامع تاثیر نهاده است. همچنین، تحولات نوظهور از قبیل پایان جنگ سرد، ظهور تروریسم فراملی، و جهانی شدن در دو دهه اخیر ماهیت منازعات و امنیت را دگرگون ساخته است. به گونه‌ای که شیوه نقش‌آفرینی فناوری در حوزه جنگ و منازعات بیشتر به حوزه‌های پدافند غیرعامل معطوف شده است . پیرو این دگرگونی، مفاهیمی نظیر جنگ اطلاعات و جنگ سایبر مطرح گردیده‌اند. اکنون با قاطعیت می‌توان گفت ماشین به عنوان زیربنای تولید تسلیحات برای تامین امنیت، جای خود را به فناوری‌های اطلاعات و ارتباطات داده است. در نتیجه، این فناوری‌ها در محور استراتژی‌پردازی‌های نظامی قرار گرفته‌اند. این وضعیت، آسیب‌پذیری جوامع را به شدت افزایش داده و تهدیدهای امنیتی را بیش از پیش پیچیده‌تر ساخته است. در واقع، 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 کشور از اهمیتی غیرقابل انکار برخوردار است و استفاده از روش‌های کدگذاری پیام‌ها و اطلاعات یکی از راه‌های موثر و کارا در این راستا می‌باشد. برای حل این مشکل یک مدل ریاضی از کدگذاری تصادفی شبکه بنام کدهای مدار جدید بر پایه حاصل ضرب‌های حلقوی غیر اولیه و حاصل‌ضرب‌های تانسوری حلقوی 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. هدف اصلی ما در این تحقیق بررسی این مسئله و ارائه ساختارهای جدیدی از کدهای مدار جدید بر پایه حاصل ضرب‌های حلقوی غیر اولیه و حاصل‌ضرب‌های تانسوری حلقوی می‌باشد که دارای بیشینه حداقل فاصله کدکلمات هستند. برای این منظور از حاصل‌ضرب تانسوری حلقوی درخصوص رده‌بندی زیرگروه‌های ماکسیمال گروه خطی عام یعنی $GL(n,q)$ برای انتخاب فرم زیرگروه تولیدکننده مدار استفاده می نمائیم که ساختار کدهای ارائه‌شده در این تحقیق و پارامترهای کدهای ساخته‌شده در (چن [۱]، ۲۰۲۰، ۳) و (کلیمنت[۲] ، ۲۰۱۹، ۴) را بطور محسوسی بهبود می‌بخشیم.

روش‌شناسی پژوهش

استفاده از کدهای مدار جدید بر پایه حاصل ضرب‌های حلقوی غیر اولیه و حاصل‌ضرب‌های تانسوری حلقوی جهت ساخت کدهای مدار یکی از پژوهش‌های نوین در بحث کدگذاری شبکه به منظور

---

۱ Chen

۲ Climent

جلوگیری از حملات آلودگی و تخریب می‌باشد. در واقع استفاده از حاصل‌ضرب تانسوری حلقوی 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 G یک گروه باشد و X یک مجموعه غیر تهی باشد. آنگاه عمل چپ گروه G بر مجموعه X تابعی به شکل

$$*: G \times X \rightarrow X$$

است که در شرایط زیر صدق می‌کند:

الف) $e * x = x = x * e$

ب) $g * (h * x) = (gh) * x$

و در آن داریم $g, h \in G$ و $x \in X$. لازم به ذکر است که اگر گروه G بر مجموعه X عمل کند، آنگاه گروه G به طور طبیعی در گروه متقارن S_X می نشیند.

تعریف ۲. فرض کنید گروه G بر مجموعه X عمل کند. در این صورت گوییم عمل گروه G بر مجموعه X متعدی است، هر گاه به ازای هر $x, y \in G$ عنصر $g \in G$ موجود باشد که $g * x = y$. در غیر این صورت عمل را غیر متعدی گویند. یک سیستم بلوکی برای زیر گروه G از S_X در واقع یک افراز از X است که توسط عمل G پایا نگه داشته می‌شود. این افراز در واقع گردایه‌ای از زیر مجموعه‌های دو به دو مجزا از X است که اجتماع آن ها برابر با کل X بوده و تحت عمل G پایا می‌مانند. هر گروه جایگشتی دارای دو سیستم بلوکی پیش فرض می‌باشد. یکی سیستمی که در آن بلوک‌ها در واقع نقاط متمایز مجموعه X می‌باشند و دیگری سیستم بلوکی تک عضوی که در آن تنها بلوک کل مجموعه X است. این سیستم‌های بلوکی را سیستم‌های بلوکی بدیهی می‌نامند. یک سیستم بلوکی غیر بدیهی برای یک گروه متناهی G را معمولا یک سیستم غیر اولیه برای گروه G

می‌نامند و گروهی که دارای چنین سیستم بلوکی نابدیهی باشد را نیز غیر اولیه گویند. به طور طبیعی اگر گروهی تنها و تنها دارای سیستم‌های بلوکی بدیهی باشد، آن گروه را اولیه گویند.

ساختارهای حاصل‌ضرب حلقوی

مفهوم حاصل‌ضرب حلقوی دو گروه بر پایه مفهوم عمل‌های غیر اولیه گروه‌های جایگشتی بنا می گردد. یادآوری می‌گردد که برای دو گروه متناهی G و H حاصل‌ضرب مستقیم G و H که با نماد $G \times H$نمایش می‌دهیم، به صورت

$$G \times H = \{(g,h) | g \in G, h \in H\}$$

$$(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1h_2)$$

تعریف می‌شود که در آن عنصر همانی $1_{G\times H} = (1_G, 1_H)$ می‌باشد.

تعریف ۳. فرض کنید G و H دو گروه متناهی و $\varphi : H \to Aut(G)$ یک همریختی گروهی باشد. در این صورت حاصل‌ضرب نیم مستقیم G با H به صورت

$$G \propto_{\varphi} H = \{(g,h) | g \in G, h \in H\}$$

$$(g_1,h_1)(g_2,h_2) = (g_1(\varphi(h_1^{-1}).g_2, h_1h_2)$$

تعریف میشود که در آن عنصر همانی $1_{G \rtimes_{\varphi} H} = (1_G, 1_H)$ می‌باشد.

فرض کنید H یک گروه جایگشتی باشد که روی مجموعه $X = \{1, \dots, n\}$ عمل می‌کند. در این صورت تعریف می‌کنیم

$$G^n = G \times \cdots \times G = \{(g_1, \cdots, g_n) \, | g_i \in G\}$$

در این صورت H با جایگشت دادن n مولفه روی G^n عمل می‌کند. در واقع داریم

$$\varphi : H \to Aut(G)$$

که در آن

$$\varphi(\sigma^{-1}) : (g_1, \cdots, g_n) \to \left(g_{\sigma(1)}, \cdots, g_{\sigma(n)}\right)$$

در این صورت حاصل‌ضرب حلقوی که با نماد $G \wr H$ نشان داده می‌شود به صورت

$$G \wr H := G^m \rtimes_\varphi H$$

تعریف می‌گردد. به سادگی دیده می‌شود که هر حاصل‌ضرب مستقیم دو گروه متناهی در واقع یک حاصل‌ضرب نیم‌مستقیم آن دو گروه نیز می‌باشد که در آن نگاشت عمل، بدیهی در نظر گرفته شده است. در لم زیر تمام حالات ممکن که یک ضرب نیم‌مستقیم تبدیل به ضرب مستقیم دو گروه می‌شود را رده‌بندی می‌نماییم.

تعریف ۴: یک ضرب نیم مستقیم $G \rtimes_\varphi H$ از دو گروه متناهی G و H یک ضرب مستقیم است اگر و فقط اگر نگاشت بدیهی باشد.

برهان . فرض کنید

$$(g_1, h_1), (g_2, h_2) \in G \rtimes_\varphi H$$

در این صورت خواهیم داشت

$$(g_1, h_1)(g_2, h_2) = (g_1(\varphi(h_1^{-1}).g_2, h_1h_2) = (g_1g_2, h_1h_2)$$

اگر و تنها اگر برای هر $g_2 \in G$ و $h_2 \in H$ داشته باشیم $\varphi(h_1^{-1})(g_2) = g_2$.

ضرب تانسوری ماتریس‌ها و فضای برداری

در ابتدا به تشریح مفهوم ضرب تانسوری برای فضاهای برداری خواهیم پرداخت. اگر U یک فضای برداری با پایه $\{u_1, \cdots, u_k\}$ و W یک فضای برداری با پایه $\{w_1, \cdots, w_m\}$ 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 $\{v_1, \cdots, u_{km}\}$ 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 یا حاصل‌ضرب کرونکر دو ماتریس A و B می‌نامند.

لم زیر ساختار دقیق حاصل‌ضرب کرونکر دو گروه ماتریس را مشخص می‌کند.

لم ۵ : 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.

قضیه ۶ (قضیه اشباخر) : هر زیر گروه GL(n,q) که شامل SL(n,q) نمی‌باشد، پایدار ساز یکی از زیرفضاهای به فرم زیر می‌باشد :

- زیرفضاهای کاملا منفرد یا نامنفرد از بعد k .
- جمع مستقیم m زیرفضای از بعد k ، که در آن n=mk.
- حاصل ضرب تانسوری $F_q^k \otimes F_q^m$ که در آن n=mk.
- حاصل ضرب تانسوری m نسخه از F_q^k که در آن $n = k^m$.
- یک گروه فراخاص از مرتبه r^{1+2k} که در آن $n = r^k$.

یک گروه تقریبا ساده که به صورت تحویل‌ناپذیر روی فضای برداری متناظر عمل می‌کند.

کدهای مدار بر پایه حاصل‌ضرب حلقوی غیرمتعدی

در این بخش با استفاده عمل حاصل‌ضرب‌های حلقوی غیر متعدی جهت ساخت کدهای مدار غیر جابجایی استفاده می‌کنیم. این نتیجه، روشی نظام‌مند جهت ساخت کدهای مدار از اندازه بزرگتر از روی کدهای مدار کوچکتر به دست می‌دهد. در واقع اگر C یک کد مدار با پارامترهای $[k, r, d; k_1]$ باشد، آنگاه قضیه زیر منجر به ساخت یک کد مدار از اندازه mr می‌شود که دارای بعد و کمترین فاصله یکسان با کد C می‌باشد. در قضیه زیر با استفاده از تجزیه جمع مستقیم، ما ساختار کد مداری را ارائه می‌دهیم که حداقل فاصله کدکلمات را حفظ می‌کند. بنابر قضیه اشباخر، این تجزیه به حاصل جمع‌های مستقیم به‌طور طبیعی و در عمل‌های غیرمتعدی گروه GL(n,q) بر زیرفضاهای متناظر آن رخ می‌دهند.

قضیه ۷ : فرض کنید n=mk و $V = V_1 \oplus ... \oplus V_m$ تجزیه‌ای از V به m زیرفضای k بعدی V_i باشد. همچنین فرض کنید $W_1 \leq V_1$ از بعد $k_1 \leq k$ باشد، به‌طوری‌که برای $G \leq GL_k(q)$ کد مدار C=G.

W_1 یک کد با پارامترهای $[k,r,d;2k_1]$ باشد. در این صورت عمل حاصل‌ضرب حلقوی $G\wr S_m$ بر زیرفضای تانسوری

$$(W_1,0,\cdots,0)=\{(w_1,0,\cdots,0):w\in W_1\to(V_1\oplus\ldots\oplus V_m)\}$$

یک کد مدار غیر جابجایی با پارامترهای $[n,mr,d;k_1]$ تشکیل می‌دهد.

برهان. فرض کنید D کد مدار حاصل از عمل $G\wr S_m$ بر $(W_1,0,\cdots,0)$ باشد. توجه داریم که

$$G\wr S_m\leq GL_k(q)\wr S_m$$

و

$$GL_k(q)\wr S_m$$

بر $V_1\oplus\cdots\oplus V_m$ به صورت گروه تبدیلات خطی عمل می‌کند. شایان ذکر است که گروه متقارن S_m بر V به صورت جایگشت m عامل V_i عمل می‌کند.

در ابتدا پایدارساز $(W_1,\cdots,0)$ تحت عمل $G\wr S_m$ را بدست می‌آوریم. برای این منظور فرض کنید

$$(g_1,\cdots,g_m,\sigma)\in(G\times\cdots\times G)\rtimes S_m=G\wr S_m$$

در این صورت عمل $(g_1,\cdots,g_m,\sigma)$ بر یک بردار دلخواه به صورت

$$(g_1,\cdots,g_m,\sigma).(v_1,\cdots,v_m)=\sigma((g_1.v_1,\cdots,g_m.v_m))$$

است که در آن $(v_1,\cdots,v_m)\in V_1\oplus\cdots\oplus V_m$.

در این صورت

$$(g_1,\cdots,g_m,\sigma).(W_1,0,\cdots,0)=\sigma((g_1.W_1,0,\cdots,0))$$

که نتیجه می‌دهد

$$(g_1,\cdots,g_m,\sigma).(W_1,0,\cdots,0)\subseteq(W_1,0,\cdots,0)$$

اگر و فقط اگر

$$g_1.W_1\subseteq W_1,\sigma(V_1)=V_1,\sigma\in S_{m-1}$$

بنابراین خواهیم داشت

$$Stab_{(G\wr S_m)}\big((W_1,0,\cdots,0)\big)=Stab_G(W_1)\times G\times\cdots\times G)\rtimes\ S_{m-1}$$

حال با استفاده از رابطه مدارساز- پایدارساز خواهیم داشت

$$|Orb_{(G\wr S_m)}\big((W_1,0,\cdots,0)\big)|=m|Orb_G(W_1)|=mr$$

حال فرض کنید برای یک $j\neq 1$ داریم

$$\sigma\big((V_1\ ,V_2,\cdots\ ,V_m)\big)=\big(V_j\ ,V_{\sigma(2)},\cdots\ ,V_{\sigma(m)}\big)$$

در این صورت

$$\sigma((W_1,0,\cdots,0))=(0,\cdots,W_1,\cdots\ ,0)$$

و در نتیجه

$$(W_1,0,\cdots,0)\cap\sigma\big((W_1,0,\cdots,0)\big)=(0,\cdots,0)$$

بنابراین برای هر

$$(g_1,\cdots,g_m)\in(G\times\cdots\times G)$$

داریم

$$\mathrm{d}((W_1,0,\cdots,0)\ ,(g_1,\cdots,g_m,\sigma).(W_1,0,\cdots,0)\subseteq(W_1,0,\cdots,0))$$

$$=\dim\big((W_1,0,\cdots,0)\big)+\dim\ (\sigma(g_1.W_1,0,\cdots,0))$$

$$-2\dim\big((W_1,0,\cdots,0)\big)\ \cap\ \sigma((g_1.W_1,0,\cdots,0)))=2k_1$$

که این در واقع بیشترین فاصله ممکن دو کد کلمه است. بنابراین این استدلال ایجاب می‌کند که

$$\mathrm{d(D)}=\min\{\mathrm{d}((W_1,0,\cdots,0)\ ,(g_1,\cdots,g_m,\sigma).(W_1,0,\cdots,0)\subseteq (W_1,0,\cdots,0))\}$$

$$=\min\{\mathrm{d}\big((W_1,0,\cdots,0)\big),\big(\sigma(g_1.W_1,0,\cdots,0)\big):\ g_1\in G,\sigma\in S_m\}$$

$$g_1\in G,\sigma(V_1)=V_1\}\min\{\mathrm{d}\big((W_1,0,\cdots,0)\big)\ ,\sigma\big((g_1.W_1,0,\cdots,0)\big):$$

$$g_1\in G\}\min\{\mathrm{d}\big((W_1,0,\cdots,0)\big)\ .\ \big((g_1.W_1,0,\cdots,0)\big):$$

$$\}=\mathrm{d(C)}\min\{\mathrm{d}(W_1, g_1.W_1): g_1 \in G$$

بنابراین ثابت کردیم که D یک کد مدار با پارامترهای $[n, mr, d: k_1]$ می‌باشد.

مثال : فرض کنید $C_1 \subseteq F_q^{n_1}$ با طول n_1 ، بعد k_1 و فاصله مینیمم d_1 و $C_1 \subseteq F_q^{n_2}$ با طول n_2 ، بعد k_2 و فاصله مینیمم d_2 دو کد خطی باشند. اگر ضرب تانسوری این دو فضا را به صورت

$$C = C_1 \otimes C_2$$

با طول $n = n_1 n_2$ ، بعد $k = k_1 k_2$ و فاصله مینیمم $d = d_1 d_2$ در نظر بگیریم، آنگاه واضح است که ضرب تانسوری مثل یک روش ترکیب کدها عمل می‌کند و می‌تواند کد قویتری بسازد.

مثال عددی : فرض کنید $C_1 \subseteq F_2^3$ باشد. هر بیت به شکل (b,b,b) کد می‌شود. پس

$$n_1 = 3, k_1 = 1, d_1 = 3$$

همپنین فرض کنید $C_2 \subseteq F_2^2$. پس

$$n_2 = 2, k_2 = 1, d_2 = 2$$

حال هر بیت اطلاعات در ضرب تانسوری $C = C_1 \otimes C_2$ به شکل یک بلوک ۶- تایی با فاصله مینیمم ۶ کد می‌شود که در برابر خطا بسیار مقاوم است.

نتیجه گیری

همان‌طور که اشاره شد؛ یکی از تهدیدات مهم شبکه‌های کدگذاری شده، حمله سایبری و مخرب می‌باشد که با ورود بسته‌های نرم‌افزاری غیر مجاز به جریان اطلاعاتی در گردش شبکه، سعی در 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، ضمن معرفی کدهای مدار غیر جابجایی، به ارائه روش هایی برای ساخت رده‌های جدیدی از کدهای مدار از اندازه بزرگ و دارای بیشینه حداقل فاصله کد کلمات می‌پردازیم. در این راستا و در جهت مقابله با حملات آلودگی شبکه، رده جدیدی از کدهای مدارجدید بر پایه حاصل‌ضرب های حلقوی غیر اولیه و حاصل ضرب‌های تانسوری حلقوی را مورد بررسی قرار داده و با استفاده ازحاصل ضرب تانسوری حلقوی دو زیرفضا، یک روش ساخت کدهای جدید را بیان نمودیم. همچنبن این روش علاوه بر بهبود نتایج پیشین، 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 Liang, J. (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 circuit codes in telecommunication systems based on non-prime cyclic products and cyclic tensor products

Soleman Askari

Assistant Professor of Mathematics, Department of Mathematics, Faculty of Basic Sciences, Imam Ali Military University, Tehran, Iran

Abstract

The main goal of this paper is to use non-prime cyclic products and cyclic tensor products and the relationships between them in the network coding process to counter destructive attacks and enemy contamination of the information transmission network. For this purpose, using cyclic products of groups and the concepts of non-prime action of permutation groups, we will consider certain subspaces of Grassmannian and present a systematic method for constructing non-commutative circuit codes on these spaces. In this research, to increase the operational capacity of the information transmission network and also to counter the threats of eavesdropping, destruction and network contamination, we present methods for constructing new classes of circuit codes of large size and with maximum and minimum codeword distances. In this regard, and to combat network contamination attacks, we investigate a new class of new circuit codes based on non-prime cyclic products and cyclic tensor products, and using the cyclic tensor product of two subspaces, we present several methods for constructing new codes.

Keywords: Circuit codes, cyclic product, cyclic tensor product, contamination attacks, information exchange security.