دانشگاه صنعتی اصفهان
دانشکده برق و کامپیوتر

سیستم رمزنگاری مک‌آلیس با کدهای LDPC

پایان‌نامه کارشناسی ارشد مهندسی برق-مخابرات

مصطفی اسماعیلی

استاد راهنما

دکتر محمد دخیل علیان

۱۳۹۰

دانشگاه صنعتی اصفهان

دانشکده برق و کامپیوتر

پایان‌نامه کارشناسی ارشد رشته مهندسی برق-مخابرات آقای مصطفی اسماعیلی

تحت عنوان

سیستم رمزنگاری مک‌آلیس با کدهای LDPC

در تاریخ ۱۳۹۰/۱۱/۱۹ توسط کمیته تخصصی زیر مورد بررسی و تصویب نهایی قرار گرفت.

۱. استاد راهنمای پایان‌نامه	دکتر محمد دخیل‌علیان	امضا
۲. استاد مشاور پایان‌نامه	دکتر مرتضی اسماعیلی	امضا
سرپرست تحصیلات تکمیلی	دکتر امیر برجی	امضا

فهرست مطالب

عنوان	صفحه
فهرست مطالب	شش
چکیده	۱
فصل اول: مقدمه	**۲**
۱-۱ ارتباطات دیجیتال	۲
۱-۲ نگاهی اجمالی به کدگذاری کانال	۴
۱-۳ رمزنگاری	۵
۱-۳-۱ سیستم رمزنگاری کلید متقارن Hill	۷
۱-۳-۲ سیستم رمزنگاری کلید عمومی RSA	۸
۱-۴ ساختار پایان‌نامه	۹
فصل دوم: کدگذاری کانال	**۱۰**
۲-۱ کدهای قالبی خطی	۱۰
۲-۱-۱ ماتریس مولد و بررسی توازن	۱۱
۲-۱-۲ تشخیص خطا با کدهای خطی	۱۳
۲-۱-۳ کمترین فاصله همینگ یک کد خطی	۱۴
۲-۱-۴ کدگشایی کدهای خطی	۱۵
۲-۲ کدهای دوری	۱۸
۲-۳ کدهای شبه دوری	۲۰
۲-۴ کدهای LDPC	۲۱
۲-۴-۱ نمایش کدهای LDPC	۲۲
۲-۵ جابجایی پیام و قانون توربو	۲۴
۲-۶ الگوریتم کدگشایی جمع-ضرب	۲۷
۲-۶-۱ کدگشای MAP برای کد تکراری	۲۹
۲-۶-۲ کدگشای MAP برای کد معمولی	۳۰
۲-۷ شیوه ساخت کدهای QC-LDPC	۳۲
۲-۷-۱ شیوه ساخت کدهای QC-LDPC بر اساس خانواده‌های تفاضلی تعمیم یافته	۳۲
۲-۷-۲ شیوه ساخت کدهای QC-LDPC با استفاده از هندسه اقلیدسی	۳۶
۲-۸ خلاصه و جمع‌بندی	۳۷
فصل سوم: سیستم رمزنگاری مک‌آلیس	**۳۹**
۳-۱ مروری بر سیستم رمزنگاری مک‌آلیس	۴۰
۳-۲ شیوه یافتن یک کدکلمه به وزن ω	۴۲
۳-۲-۱ پیچیدگی حمله استرن	۴۷
۳-۳ خلاصه و جمع‌بندی	۴۸

فصل چهارم: سیستم‌های رمزنگاری مبتنی بر کدهای کانال ۴۹
۴-۱ سیستم رمزنگاری Rao-Nam ۴۹
۴-۱-۱ آنالیز سیستم رمزنگاری Rao-Nam ۵۱
۴-۱-۲ سیستم رمزنگاری تعمیم یافته Rao-Nam ۵۳
۴-۱-۳ نقاط ضعف سیستم رمزنگاری Rao-Nam ۵۴
۴-۱-۴ سیستم رمزنگاری تعمیم داده شده Rao-Nam بهبود یافته ۵۷
۴-۲ استفاده از کدهای QC-LDPC در سیستم رمزنگاری مک‌آلیس ۵۸
۴-۲-۱ سیستم رمزنگاری کلید عمومی با کدهای QC-LDPC ۵۹
۴-۲-۲ طراحی پارامترهای سیستم ۶۰
۴-۲-۳ سیستم رمزنگاری و کدگذاری توام کلید متقارن با کدهای QC-LDPC ۶۳
۴-۲-۴ کارآیی سیستم رمز ارتقا داده شده ۶۶
۴-۲-۵ امنیت سیستم رمزنگاری ارتقا داده شده ۶۹
۴-۳ خلاصه و جمع‌بندی ۶۹

فصل پنجم: سیستم رمزنگاری مبتنی بر حذف تصادفی برخی مولفه‌های یک کد QC-LDPC ۷۰
۵-۱ حذف کردن مولفه‌های یک کد کانال ۷۱
۵-۲ تولید تصادفی اعداد ۷۳
۵-۲-۱ تولید شبه‌تصادفی اعداد ۷۳
۵-۲-۲ تولید کاملا تصادفی اعداد ۷۶
۵-۳ سیستم رمزنگاری مبتنی بر حذف برخی مولفه‌های یک کد QC-LDPC ۷۶
۵-۳-۱ اندازه کلید ۷۸
۵-۳-۲ عملکرد کد پنچر شده ۷۹
۵-۴ بررسی امنیت سیستم رمزنگاری مبتنی بر کدهای پنچر شده ۹۴
۵-۵ جمع‌بندی و نتیجه‌گیری ۹۹

فصل ششم: نتیجه‌گیری و پیشنهادات ۱۰۱
۶-۱ نتیجه‌گیری ۱۰۱
۶-۲ پیشنهادات ۱۰۳

پیوست ۱: برنامه‌های کامپیوتری ساخت کدهای QC-LDPC بر اساس خانواده‌های تفاضلی تعمیم‌یافته ۱۰۴
واژه‌نامه ۱۱۷
مراجع ۱۲۱

چکیده

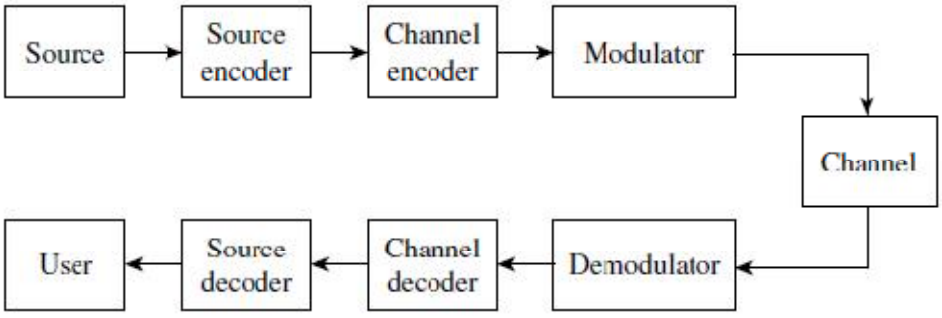
با افزایش حجم ارتباطات و دسترسی همگانی به وسایل ارتباط جمعی، انتقال مطمئن و امن اطلاعات اهمیت فراوانی یافته است. انتقال مطمئن اطلاعات از طریق کدگذاری کانال انجام می‌گیرد. طراحی کدهای کانال از سال ۱۹۴۸ با نظریه شانون شروع شد. در این نظریه، شانون ثابت کرد که کدهایی با نرخ به قدر دلخواه نزدیک به ظرفیت کانال وجود دارند که احتمال خطای کدگشایی در گیرنده به قدر دلخواه نزدیک به صفر است. در سال ۱۹۶۰ کدهای LDPC که دارای ماتریس بررسی توازن خلوت هستند معرفی شدند. ولی به دلیل نبود امکانات لازم در آن زمان، به مدت ۳۰ سال به فراموشی سپرده شدند. در اوایل دهه ۱۹۹۰، این کدها مجددا مورد توجه قرار گرفتند و تا به امروز تحقیقات زیادی روی آنها انجام گرفته است و برخی از کلاس‌های آنها مانند کدهای QC-LDPC در استانداردهای مختلف ارتباطی به کار برده شده‌اند. انتقال امن اطلاعات از طریق یک کانال ناامن بوسیله سیستم‌های رمزنگاری صورت می‌گیرد. علیرغم وجود سیستم‌های مختلف رمزنگاری که امنیت قابل قبولی دارند، سیستمی که بتواند دو عمل کدگذاری و رمزگذاری را با هم ترکیب کند در سیستم‌های مخابراتی بسیار کاربردی خواهد بود. اولین سیستمی که چنین عملی را انجام می‌داد در سال ۱۹۷۸ توسط مک‌آلیس معرفی شد که به سیستم رمزنگاری کلید عمومی مک‌آلیس معروف است. امنیت این سیستم مبتنی بر این است که بدون اطلاع از ساختار جبری یک کد کانال، کدگشایی آن یک مسئله NP خواهد بود. در این سیستم رمزنگاری مولفه‌های یک متن ساده درهم ریخته، مولفه‌های کدکلمه متناظر با یک متن ساده جایگشت و برخی از آنها به طور تصادفی تغییر داده می‌شوند. ولی این سیستم به دو دلیل هنوز کاربردی نشده است؛ (۱) اندازه کلید آن بزرگ است و (۲) نرخ ارسال اطلاعات در آن پایین می‌باشد. در طول ۳۳ سال گذشته، تغییرات زیادی روی پارامترهای این سیستم داده شد تا معایب آن برطرف شوند. برخی از این تغییرات در کد مورد استفاده، در ساختار ماتریس‌های جایگشت و درهم‌ریز و مجموعه بردارهای خطای تصادفی بوده است. ولی در هر کدام از سیستم‌های جدید یکی از دو معایب سیستم مک‌آلیس باقی مانده بود و یا از امنیت قابل قبولی برخوردار نبودند. در این پایان‌نامه یک سیستم رمزنگاری کلید متقارن جدید مبتنی بر حذف تصادفی برخی از مولفه‌های یک کد QC-LDPC ارائه شده است. در این سیستم از یک مولد شبه تصادفی اعداد برای مشخص کردن مولفه‌هایی که باید حذف گردند استفاده شده است. یکی از مزایای این سیستم نسبت به سیستم‌های مشابه پیشین آن است که با حذف ماتریس‌های جایگشت و درهم‌ریز اندازه کلید کاهش یافته و امکان استفاده از کدهایی با نرخ بالا فراهم شده است. این مزیت سبب رفع مشکل نرخ ارسال اطلاعات پایین در سیستم رمزنگاری مک‌آلیس خواهد شد. مقادیر پیشنهادی برای تعداد مولفه‌هایی که می‌توانند حذف گردند ارائه شده و نشان داده شده است که عملکرد کد با حذف این تعداد مولفه قابل قبول باقی می‌ماند. همچنین از دیگر مزایای این سیستم آن است که اگر به هر دلیلی کد مورد استفاده در سیستم رمزنگاری در اختیار فرد سوم قرار گیرد، سیستم می‌تواند امن باقی بماند. این مزیت تا به حال در هیچکدام از سیستم‌های رمزنگاری پیشین وجود نداشته است، یعنی اگر کد مورد استفاده به هر دلیلی فاش می‌شد، سیستم رمزنگاری شکسته شده محسوب می‌شد.

کلمات کلیدی: رمزنگاری، کدگذاری، کدهای LDPC، حذف مولفه، مولد شبه تصادفی اعداد.

فصل اول
مقدمه

۱-۱ ارتباطات دیجیتال

سیستم‌های ارتباط دیجیتال به‌وفور در زندگی روزمره به‌کار گرفته می‌شوند. از بدیهی‌ترین نمونه‌های آن تلفن‌های همراه، تلویزیون‌های ماهواره‌ای و اینترنت بی‌سیم می‌باشد. سیستم‌های ذخیره اطلاعات نوع خاصی از سیستم‌های ارتباطی دیجیتال می‌باشند. در سیستم‌های ذخیره اطلاعات هدف انتقال اطلاعات از یک زمان به زمان دیگر است، در حالی که در سیستم‌های ارتباطی هدف انتقال اطلاعات از یک مکان به مکان دیگر است. هر کدام از مثال‌های اخیر با وجود اینکه در شیوه عملکرد و پیاده‌سازی تفاوت‌های عمده‌ای دارند، ولی همه در چارچوبی که شانون[1] در سال ۱۹۴۸ معرفی کرد صدق می‌کنند. این چارچوب در شکل ۱-۱ نمایش داده شده است.



شکل ۱-۱: بلوک دیاگرام سیستم‌های ارتباطی (ذخیره اطلاعات) معرفی شده توسط شانون

[1] Shannon

هر قسمت از شکل ۱-۱ در ذیل توضیح داده شده است.

منبع و کاربر[1]: منبع پیام ممکن است در ابتدا آنالوگ (مانند صوت) بوده و بعد دیجیتال شود و یا ممکن است از همان اول دیجیتال باشد. منبع به عنوان تولید کننده سمبل‌هایی که از یک مدل احتمالاتی خاص پیروی می‌کند در نظر گرفته خواهد شد. کاربر نیز ممکن است یک شخص، کامپیوتر و یا یک دستگاه الکترونیکی دیگری باشد.

کدگذار و کدگشای منبع[2]: کدگذار منبع، دنباله سمبل‌های منبع پیام را به یک دنباله از بیت‌های صفر و یک تبدیل می‌کند. کدگشای منبع دقیقا عکس عمل کدگذار را انجام می‌دهد، به این معنی که دنباله سمبل‌های منبع را از روی دنباله بیت‌های خروجی کدگشای کانال استخراج می‌کند.

کدگذار و کدگشای کانال[3]: نقش کدگذار کانال محافظت از بیت‌های ارسالی در مقابل نویز، اغتشاش و اعوجاج می‌باشد. عمل محافظت با تبدیل دنباله بیت‌های ورودی به دنباله بیت‌های دیگر همراه با افزونگی انجام می‌شود. بیت-های افزونگی نقش محافظت را ایفا می‌کنند. نسبت تعداد بیت‌های ورودی به کدگذار کانال به تعداد بیت‌های خروجی را *نرخ کد*[4] گویند و با R نمایش داده می‌شود (واضح است که $0 < R < 1$). به عنوان مثال اگر یک کدکلمه ۱۰۰۰ بیتی به ۵۰۰ بیت اطلاعات در کدگذار کانال متناظر شود، $R = 0.5$ خواهد بود. در واقع ۵۰۰ بیت افزونگی در هر کدکلمه وجود دارد. وظیفه کدگشای کانال بازیابی بیت‌های اطلاعات ورودی به کدگذار کانال از دمدولاتور علیرغم وجود نویز، اعوجاج و اغتشاش در کلمه دریافتی است.

مدولاتور و دمدولاتور[5]: مدولاتور وظیفه تبدیل دنباله بیت‌های صفر و یک به شکل سازگار با کانال برای ارسال را دارد. به عنوان مثال برای ارتباطات بی‌سیم، دنباله بیت‌ها باید به یک سیگنال با فرکانس بالا تبدیل شود تا از یک آنتن با اندازه قابل قبول ارسال شود. دمدولاتور وظیفه بازیابی دنباله ورودی به مدولاتور از روی خروجی کانال را دارد.

کانال[6]: یک کانال محیط فیزیکی است که خروجی مدولاتور از آن عبور می‌کند (یا در آن ذخیره می‌شود). تجربه نشان می‌دهد که در حین ارسال، نویز و سیگنالهای ناخواسته دیگر با سیگنال مورد نظر جمع می‌شود. بیشتر اوقات یک مدل احتمالاتی به کانال نسبت داده و از آن در محاسبات استفاده می‌شود. از نظر فیزیکی، کانال می‌تواند شامل آنتن، تقویت کننده‌ها و فیلترها باشد. برای یک هارد دیسک کانال شامل سر نویسنده[7]، محیط مغناطیسی[8] و سر خواننده[9] است.

---

[1] Source and user
[2] Source encoder and decoder
[3] Channel encoder and decoder
[4] Code rate
[5] Modulator and Demodulator
[6] Channel
[7] Write head
[8] Magnetic medium
[9] Read head

۱-۲ نگاهی اجمالی به کدگذاری کانال

تا به امروز روشهای متعددی برای کدگذاری کانال ارائه شده است. همه این روشها را می‌توان به دو دسته کلی تقسیم کرد. اول الگوی *تقاضای اتوماتیک تکرار*[1] *(ARQ)* و دوم الگوی *تصحیح خطا*[2] *(FEC)* می‌باشد. در الگوهای ARQ کد فقط قابلیت تشخیص خطا را دارد. اگر در کلمه دریافتی خطایی وجود داشته باشد (یعنی کلمه دریافتی یک کدکلمه نباشد)، تقاضای ارسال مجدد آن کدکلمه از طرف گیرنده به فرستنده ارسال می‌شود. این کدها را *کدهای تشخیص خطا*[3] می‌نامند. ولی در الگوی FEC، علاوه بر قابلیت تشخیص خطا، قابلیت تصحیح آن از طریق یک الگوریتم نیز وجود دارد. این قابلیت به دلیل وجود شاخصه‌هایی در شیوه ساخت آن کد است. این کدها را *کدهای تصحیح خطا*[4] *(یا کنترل کننده خطا*[5]*)* می‌نامند. البته کدهایی هم هستند که ترکیبی از ARQ و FEC را به‌کار می‌گیرند. در این نوع کدها تقاضای ارسال مجدد در صورتی به فرستنده ارسال می‌شود که گیرنده نتواند خطای ایجاد شده در کدکلمه، در اثر عبور از کانال، را درست تصحیح نماید. این کدها در سیستم‌های ذخیره اطلاعات بسیار مفید هستند، زیرا اگر کدگشا نتواند اطلاعات را درست کدگشایی نماید، دوباره اطلاعات خوانده می‌شود. این کدها را *کدهای تشخیص و تصحیح خطا*[6] می‌نامند.

از جمله کانال‌های متداول در مدل‌سازی سیستم‌های مخابراتی می‌توان به کانال متقارن دودویی[7] (BSC)، کانال جمعی گوسی سفید[8] (AWGN) و کانال پاک‌کننده دودویی[9] (BEC) اشاره کرد. در اینجا به صورت مختصر به معرفی این سه کانال می‌پردازیم.

کانال متقارن دودویی: این کانال با ورودی $x_i \in \{0,1\}$، خروجی $y_i \in \{0,1\}$ ، احتمالات گذار $P(y_i|x_i)$ معرفی می‌شود که در آن ε *احتمال خطای کانال*[10] نامیده می‌شود.

$$P(y_i = 1|x_i = 0) = P(y_i = 0|x_i = 1) = \varepsilon,$$
$$P(y_i = 1|x_i = 1) = P(y_i = 0|x_i = 0) = 1 - \varepsilon.$$

کانال جمعی گوسی سفید: فرض کنید $v_i \in \{0,1\}$ و $x_i = (-1)^{v_i}$. خروجی این کانال به واسطه نویزی که دارای توزیع نرمال با میانگین صفر و واریانس σ^2 می‌باشد توسط تابع احتمال زیر توصیف می‌شود.

$$p(y_i|x_i) = \frac{1}{\sqrt{2\pi}\sigma}\exp(-(y_i - x_i)^2/(2\sigma^2)).$$

کانال پاک‌کننده دودویی: در این کانال سمبل‌های ورودی به‌صورت $x_i \in \{0,1\}$ و سمبل‌های خروجی به صورت $y_i \in \{0,1,\varepsilon\}$ است ،که ε به این معنا است که بیت ورودی کاملا پاک شده است. این کانال با احتمالات گذار زیر مشخص می‌شود که p احتمال پاک‌شدگی[11] نامیده می‌شود.

---

[1] Automatic Request for Repeat
[2] Forward error correcting
[3] Error detection codes
[4] Error correcting codes
[5] Error control codes
[6] Error detection and correction codes
[7] Binary symmetric channel
[8] Additive white Gaussian noise channel
[9] Binary erasure channel
[10] Crossover probability
[11] Erasure probability

$$P(y_i = 1|x_i = 1) = P(y_i = 0|x_i = 0) = 1 - p,$$
$$P(y_i = 1|x_i = 0) = P(y_i = 0|x_i = 1) = 0,$$
$$P(y_i = \varepsilon|x_i = 0) = P(y_i = \varepsilon|x_i = 1) = p.$$

در شکل ۱-۱ اثری از بلوک‌های رمزگذاری و رمزگشایی دیده نمی‌شود. دلیل آن این است که وجود آنها در حالت کلی ضروری نیست، یعنی می‌توانند در یک سیستم باشند و در سیستم دیگری نباشند. بر اساس چنین مدلی شانون نشان داد کانال می‌تواند توسط یک پارامتر C، به نام *ظرفیت کانال* مشخص شود. این پارامتر بیان کننده میزان اطلاعاتی است که کانال می‌تواند انتقال دهد. با توجه به تعریف نرخ کد، شانون ثابت کرد که کدهایی وجود دارند که احتمال خطا در کدگشایی آنها با رعایت شرط $R < C$، به قدر دلخواه کوچک است. ولی ایشان کدی با چنین ویژگی را معرفی نکرد.

از اینجا بود که تلاشها برای یافتن کدهایی با نرخ نزدیک به ظرفیت کانال (برای کمینه بودن هزینه ارسال) و احتمال خطای کدگشایی به‌قدر دلخواه کوچک شروع شد. در سال ۱۹۶۱ *کدهای*[1] $LDPC$ [۱] معرفی شدند که احتمال خطای کدگشایی آنها بسیار کم بود، ولی به دلیل امکانات محدود آن زمان پژوهش قابل توجهی بر روی آنها صورت نگرفت. البته یک استثنا کار تنر[2] است که در سال ۱۹۸۱، کدهای LDPC را تعمیم داده و یک نمایش گرافی برای آنها معرفی کرد و اکنون به گراف تنر معروف است[۲]. در سال ۱۹۹۳ بود که *توربو کدها*[3][۳] معرفی شدند و نرخ نزدیک به ظرفیت کانال داشتند. در سال ۱۹۹۶ کدهای LDPC [۴-۷] مجددا مورد توجه قرار گرفتند. در فصل ۲ به تفصیل در مورد این کدها بحث خواهد شد.

۱-۳ رمزنگاری

با توجه به آنچه که گفته شد، روش‌های مختلف کدگذاری کانال امکان ارسال پیام از طریق کانال در حضور نویز را ممکن می‌سازند. ولی رمزنگاری امکان محرمانه ماندن پیام برای همه غیر از گیرنده مورد نظر را فراهم می‌آورد. سابقه رمزنگاری به ۴۰۰۰ سال قبل، در زمان مصریان، بر می‌گردد. تا همین چند دهه گذشته انجام کارهای رمزنگاری مختص نهادهای نظامی و دولتی بود. در آن زمان جرم خروج الگوریتم‌های رمزنگاری از کشورها معادل جرم قاچاق سلاح‌های اتمی بود، زیرا رمزنگاری نوعی ابزار جنگ به حساب می‌آمد. ولی تحولی که در صنایع الکترونیک و کامپیوتر بوجود آمد و فراگیر شدن آن، انحصار علم رمزنگاری را از بین برد. امروزه رمزنگاری به‌قدری در زندگی روزمره مورد استفاده قرار می‌گیرد که عدم وجود آن تقریبا محال به نظر می‌رسد. از ابتدائی‌ترین کارها مثل کنترل حساب بانکی تا پیچیده‌ترین آنها مانند رأی گیری اینترنتی، علم رمزنگاری حضور دارد.

رمزنگاری شیوه‌های مختلف محرمانه نمودن و مبادله امن اطلاعات می‌باشد. چند اصطلاح مرتبط با رمزنگاری در اینجا تعریف می‌شود که در ادامه بحث مورد نیاز هستند.

- *متن اصلی*[4]: متن یا پیامی که قرار است رمز شود را متن اصلی نامند.

---

[1] Low Density Parity-check Codes
[2] Tanner
[3] Turbo codes
[4] Plain-text

- *رمزگذاری*[1]: فرآیند تبدیل متن اصلی به متن رمز شده را رمزگذاری نامند. متنی که بعد از این فرآیند حاصل می‌شود متن رمز شده[2] نامیده می‌شود.
- *الگوریتم*: روشی که برای امنیت بخشی به داده ها استفاده می‌شود را الگوریتم می‌نامند.
- *رمزگشایی*[3]: استخراج متن اصلی از متن رمز شده را رمزگشایی می‌نامند.
- *کلید*: الگوریتم رمز با تکیه بر یک کلید، متن اصلی را به متن رمز شده (و متن رمز شده را به متن اصلی) طی فرآیند رمزگذاری (رمزگشایی) تبدیل می کند.
- *تحلیلگر رمز*[4]: شخصی که در جستجوی متن اصلی یا کلید رمزنگاری است. تحلیلگر می‌تواند خودی یا غیر خودی (دشمن) باشد. در صورت خودی بودن تحلیلگر، هدف از تحلیل، ارزیابی الگوریتم و ارتقای آن می‌باشد و در صورت غیر خودی بودن تحلیلگر، هدف اخلال در مبادله امن اطلاعات است.
- *تحلیل رمز*[5]: دانش و مطالعه روش‌های مختلف به دست آوردن کلید از روی متن رمز شده.

تعریف ۱-۱ : یک سیستم رمزنگاری، یک پنج تائی $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ می‌باشد که

- $\mathcal{P}$ مجموعه متن های اصلی است؛
- $\mathcal{C}$ مجموعه متن های رمز شده است؛
- $\mathcal{K}$ ، فضای کلید، مجموعه کلیدهای لازم برای رمزگذاری متن اصلی می‌باشد؛
- برای هر $K \in \mathcal{K}$، یک الگوریتم رمزگذاری $e_K \in \mathcal{E}$ ، از $\mathcal{P}$ به $\mathcal{C}$ و متناظر با آن یک الگوریتم رمزگشایی $d_{\mathrm{K}} \in \mathcal{D}$ از $\mathcal{C}$ به $\mathcal{P}$ وجود دارد به قسمی که برای هر $x \in \mathcal{P}$ داریم

$$d_{\mathrm{K}}\big(e_{\mathrm{K}}(x)\big) = x.$$

برای اینکه یک سیستم رمزنگاری کاربردی باشد، باید دو شرط را برآورده کند. نخستین شرط آن است که هر تابع رمزگذاری e_{K} و رمزگشایی d_{K} باید در زمان های معقول قابل محاسبه باشند. دوم آنکه هر شخصی، غیر از گیرنده مورد نظر، نباید با دیدن متن رمز شده بتواند به کلید K پی ببرد. در واقع شرط دوم ایده *امنیت*[6] را تعریف می-کند. تحلیل هایی‌که دشمن (فرد سوم) برای پی بردن به کلید رمزگذاری انجام می‌دهد، *حمله*[7] نامیده می‌شود. حمله صور مختلفی دارد که در اینجا اشاره‌ای به برخی از مهمترین آنها می‌شود.

[1] Encryption
[2] Cipher-text
[3] Decryption
[4] Cryptanalyst
[5] Cryptanalysis
[6] Security
[7] Attack

- حمله *بر اساس متن رمز شده*[1]: در این حمله فرض بر این است که دشمن تنها یک سری متن رمز شده در اختیار دارد.
- حمله *بر اساس متن اصلی-رمز شده*[2]:حمله دشمن بر پایه تعدادی متن اصلی و رمز شده آنها صورت می‌گیرد.
- حمله *بر اساس متن اصلی انتخابی*[3]: در این حمله فرض بر این است که دشمن دسترسی موقت به الگوریتم رمزگذاری دارد. او می‌تواند یک متن اصلی را انتخاب و متن رمز شده نظیر آنرا بسازد.
- حمله *بر اساس متن رمز شده انتخابی*[4]: در این حمله فرض بر این است که دشمن دسترسی موقت به الگوریتم رمزگشایی دارد. او این توانایی را دارد که یک متن رمز شده را انتخاب و متن اصلی نظیر آنرا بسازد.

در هر یک از موارد بالا هدف دشمن یافتن کلیدی است که برای رمزگذاری استفاده شده است. پس از یافتن کلید این امکان برای دشمن میسر است که هر متن رمز شده با این کلید را رمزگشایی کند.

سیستم های رمزنگاری به دو دسته، کلید متقارن و کلید عمومی تقسیم می‌شوند. در سیستم رمزنگاری کلید متقارن فرستنده و گیرنده روی یک کلید توافق کرده و با استفاده از آن اطلاعات را به‌صورت امن بین یکدیگر مبادله می کنند. چنانچه این کلید به هر وسیله‌ای آشکار شود تبادل اطلاعات بین فرستنده و گیرنده دیگر امن نخواهد بود. البته موضوع تبادل کلید بین فرستنده و گیرنده برای مبادله امن اطلاعات یا به طور کلی مدیریت کلید خود مبحث مفصلی است. در سیستم‌های رمزنگاری کلید عمومی، هر شخص یک کلید عمومی و یک کلید خصوصی دارد. کلید عمومی به همه اعلام می‌شود، ولی کلید خصوصی نزد خود شخص مخفی نگه‌داشته می‌شود. برای مبادله امن اطلاعات در این سیستم، پیام با کلید عمومی گیرنده رمزگذاری می‌شود و شخص گیرنده با دریافت متن رمز شده با کلید خصوصی خود اقدام به رمزگشایی آن می‌کند. برای مشاهده بهتر تفاوت و شیوه عملکرد سیستم‌های رمزنگاری کلید متقارن و کلید عمومی، دو سیستم رمزنگاری Hill و RSA در ادامه آورده شده‌اند.

۱-۳-۱ سیستم رمزنگاری کلید متقارن Hill

فرض کنید m یک عدد صحیح مثبت باشد. در این سیستم رمزنگاری $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$ و مجموعه $\mathcal{K}$ کلیه ماتریس‌های معکوس‌پذیر در $\mathbb{Z}_{26}$، از مرتبه m، با اعداد صحیح به عنوان عناصر آنها است. برای کلید

$$K = \begin{pmatrix} k_{1,1} & k_{1,2} & \cdots & k_{1,m} \\ k_{2,1} & k_{2,2} & \cdots & k_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ k_{m,1} & k_{m,2} & \cdots & k_{m,m} \end{pmatrix},$$

[1] Cipher-text attack
[2] Plain-cipher text attack
[3] Chosen plain-text attack
[4] Chosen cipher-text attack

متن رمز شده $\mathbf{y} = (y_1, \cdots, y_m)$، متناظر با متن اصلی $\mathbf{x} = (x_1, \cdots, x_m)$ از رابطه $\mathbf{y} = \mathbf{x}K$ به دست می‌آید که کلیه عملیات در $\mathbb{Z}_{26}$ انجام می‌شود. برای رمزگشایی متن رمز شده $\mathbf{y} = (y_1, \cdots, y_m)$، باید معکوس ماتریس K، K^{-1}، محاسبه شود. با استفاده از آن، متن اصلی $\mathbf{x} = (x_1, \cdots, x_m)$ از رابطه $\mathbf{x} = \mathbf{y}K^{-1}$ به دست می‌آید.

مثال ۱-۱: فرض کنید $m = 2$ و $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$ باشد. در این صورت

$$y_1 = (11x_1 + 3x_2)\ mod\ 26,$$
$$y_2 = (8x_1 + 7x_2)\ mod\ 26.$$

معکوس ماتریس K در $\mathbb{Z}_{26}$ برابر با $K^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$ است. بنابراین

$$x_1 = (7y_1 + 23y_2)\ mod\ 26,$$
$$x_2 = (18y_1 + 11y_2)\ mod\ 26.$$

۱-۳-۲ سیستم رمزنگاری کلید عمومی RSA

فرض کنید $n = pq$ باشد،که p و q دو عدد اول متمایز هستند. در سیستم رمزنگاری RSA، $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$ و $\mathcal{K} = \{(n, p, q, a, b) | ab = 1\ mod\ \varphi(n)\}$ است که $\varphi(n)$ برابر با تعداد اعداد صحیح مثبت کوچکتر از n که نسبت به آن اول هستند، می‌باشد. مقادیر n و b کلید عمومی و مقادیر p، q و a کلید خصوصی را تشکیل می‌دهند. متن رمز شده متناظر با متن اصلی $x \in \mathcal{P}$ از رابطه $y = x^b\ mod\ n$ و متن اصلی متناظر با متن رمز شده $y \in \mathcal{C}$ از رابطه $x = y^a\ mod\ n$ به دست می‌آیند. با استفاده از تئوری اعداد به‌راحتی قابل اثبات است که دو عمل رمزگذاری و رمزگشایی عکس یکدیگرند. فرض کنید $x \in \mathbb{Z}_n^*$ است، که $\mathbb{Z}_n^*$ مجموعه اعداد صحیح مثبت کوچکتر از n که نسبت به آن اول هستند، می‌باشد. از آنجا که $ab = 1\ mod\ \varphi(n)$، برای یک $t \geq 1$،

$$ab = t\varphi(n) + 1,$$

است. بنابراین

$$(x^b)^a mod\ n = x^{t\varphi(n)+1}\ mod\ n = (x^{\varphi(n)})^t x\ mod\ n = 1^t . x\ mod\ n = x.$$

به روش کاملا مشابه قابل اثبات است که اگر $x \notin \mathbb{Z}_n^*$، عمل رمزگشایی و رمزگذاری عکس یکدیگرند.

مثال ۱-۲: فرض کنید $p = 101$ و $q = 113$ باشد. بنابراین $n = pq = 11413$ و

$$\varphi(n) = 100 \times 112 = 11200,$$

است. اگر $b = 3533$ انتخاب شود آنگاه

$$a = b^{-1}\ mod\ 11200 = 6597.$$

بنابراین کلید عمومی برابر با $(n, b) = (11413,3533)$ و کلید خصوصی برابر با $(p, q, a) = (101,113,6597)$ است. فرض کنید بخواهیم متن اصلی $x = 9726$ را رمز کنیم. با توجه به الگوریتم رمزگذاری، متن رمز شده متناظر با آن برابر است با

$$y = 9726^{3533}\ mod\ 11413 = 5761.$$

چنانچه این متن رمز شده در گیرنده دریافت شود، با توجه به کلید خصوصی و الگوریتم رمزگشایی، متن اصلی متناظر با متن رمز شده $y = 5761$ برابر است با

$$x = 5761^{6597}\ mod\ 11413 = 9726.$$

۱-۴ ساختار پایان‌نامه

در فصل دوم نظریه کدگذاری کانال به طور اجمالی معرفی خواهد شد. در این فصل ویژگی‌های یک کد کانال همراه با مثال‌های متنوع ارائه خواهد شد. در این فصل نوع خاصی از کدهای کانال که به کدهای LDPC معروف هستند معرفی خواهند شد. در فصل سوم اولین سیستم رمزنگاری که امنیت آن بر پایه کدگشایی کدهای کانال است به همراه حملات مطرح شده برای آن معرفی می‌گردد و نشان داده می‌شود که این سیستم که تاکنون غیر قابل شکست باقی مانده است دو مشکل عمده بزرگی اندازه کلید و نرخ پایین ارسال اطلاعات وجود دارد که مانع از کاربردی شدن آن گشته است. در فصل چهارم انواع سیستم‌های رمزنگاری که مبتنی بر کدهای کانال هستند به همراه نقاط ضعف و قدرت آنها ارائه می‌شود. در انتهای فصل چهارم یک سیستم کدگذاری/ رمزگذاری (کدگشایی/ رمزگشایی) توام ارائه خواهد شد. در فصل پنجم یک الگوریتم جدید کدگذاری/رمزگذاری(کدگشایی/رمزگشایی) توام جدید مبتنی بر حذف تصادفی برخی مولفه‌های یک کد ارائه شده و این الگوریتم با الگوریتم‌های مشابه مقایسه خواهد شد. همچنین به دلیل عدم استفاده از ماتریس‌های جایگشت و درهم‌ریز امکان استفاده از کدهای با نرخ بالاتر فراهم شده است که سبب رفع مشکل نرخ ارسال اطلاعات پایین شده است. یک ویژگی که در الگوریتم‌های پیشین وجود نداشته ولی در این روش وجود دارد آن است که حتی اگر کد مورد استفاده در این سیستم افشا شود سیستم هنوز می‌تواند امن باقی بماند.

فصل دوم
کدگذاری کانال

کدگذاری یکی از روشهای موثر برای کنترل خطا در سیستم‌های مخابراتی است. از آنجا که موضوع پایان‌نامه در راستای ترکیب رمزنگاری و کدگذاری کانال می‌باشد، در این فصل سعی شده است به اجمال مباحث مورد استفاده در موضوع کدگذاری کانال بیان گردد. کلیه تعاریف و روابط این فصل از [۸] آورده شده است.

۲-۱ کدهای قالبی خطی

تعریف ۲-۱ : فرض کنید $A = \{a_1, a_2, \cdots, a_q\}$ مجموعه‌ای از q سمبل باشد. هر زیرمجموعه $C \subseteq A^n$ یک کد q- آرایه‌ای به طول n روی A نامیده می‌شود. مجموعه A الفبای کد و هر یک از اعضای C، یک کدکلمه نامیده می‌شوند.

فرض کنید خروجی یک منبع دنباله‌ای از سمبل‌های $\{a_1, a_2, \cdots, a_q\}$ باشد. در کدگذاری قالبی، برای یک k صحیح که $0 < k \leq \log_q M$، (M برابر با تعداد کدکلمات C است)، خروجی منبع به دنباله‌هایی به طول k سمبل، که پیام نام دارد، تقسیم شده و به هر پیام یک و فقط یک کدکلمه از C نسبت داده می‌شود.

تعریف ۲-۲: فرض کنید F_q یک میدان q عضوی باشد. F_q^n یک فضای برداری n بعدی روی F_q است. هر زیر فضای k بعدی C از F_q^n یک کد خطی q-تایی با بعد k روی F_q نامیده می‌شود. واضح است که تعداد اعضای C برابر با q^k است. دقت کنید که q توانی از یک عدد اول است.

در این پایان‌نامه فقط کدهای خطی روی میدان F_2 مورد استفاده قرار می‌گیرند. در ادامه یک کد قالبی خطی به طول n و بعد k با $C(n,k)$ و یا به اختصار با C نشان داده می‌شود.

۲-۱-۱ ماتریس‌های مولد و بررسی توازن

از آنجا که یک $C(n,k)$، یک زیرفضای k بعدی از فضای برداری F_2^n می‌باشد، k کدکلمه مستقل خطی $\mathbf{g}_0$، $\mathbf{g}_1$،⋯،$\mathbf{g}_{k-1}$ وجود دارند، به‌طوری که هر کدکلمه $\mathbf{v} \in C$ یک ترکیب خطی از آنها است. این k کدکلمه یک پایه برای C تشکیل می دهند. فرض کنید $\mathbf{u} = (u_0, u_1, \cdots, u_{k-1})$ یک پیام باشد. کدکلمه متناظر آن از رابطه زیر به‌دست می‌آید.

$$\mathbf{v} = u_0\mathbf{g}_0 + u_1\mathbf{g}_1 + \cdots + u_{k-1}\mathbf{g}_{k-1}.$$

اگر k کد کلمه مستقل خطی $\mathbf{g}_0$، $\mathbf{g}_1$،⋯،$\mathbf{g}_{k-1}$ در سطرهای یک ماتریس قرار داده شوند، یک ماتریس $k \times n$ به شکل زیر به‌دست می‌آید.

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix} = \begin{bmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{bmatrix}.$$

در این صورت کدکلمه $\mathbf{v}$ متناظر با پیام $\mathbf{u}$ از رابطه $\mathbf{v} = \mathbf{uG}$ به‌دست می‌آید. در این حالت واضح است که کدکلمه $\mathbf{v}$ برای پیام $\mathbf{u}$ ترکیبی خطی از سطرهای $\mathbf{G}$ است که بیت‌های $\mathbf{u}$ نقش ضرایب را ایفا می‌کنند. ماتریس $\mathbf{G}$ را *ماتریس مولد*[1] کد C می‌نامند.

از آنجا که یک کد C زیر فضایی k بعدی از فضای برداری F_2^n می باشد، *فضای تهی*[2] (یا دوگان) C ، نمایش داده شده با $C^{\perp}$، یک زیرفضای $(n-k)$ بعدی از F_2^n است که با مجموعه بردارهای n-تایی زیر مشخص می‌شود:

$$C^{\perp} = \{\mathbf{w} \in F_2^n \ : < \mathbf{w}, \mathbf{v} >= 0, \ for\ all\ \ \mathbf{v} \in C\ \},$$

که $< \mathbf{w}, \mathbf{v} >$ بیانگر ضرب داخلی دو بردار $\mathbf{v}$ و $\mathbf{w}$ است. $C^{\perp}$ را می توان یک کد خطی $(n, n-k)$ در نظر گرفت که کد دوگان C نامیده می‌شود. مشابه بحثی که برای کد C مطرح شد، فضای دوگان C از $(n-k)$ پایه مستقل خطی چون $\mathbf{h}_0$، $\mathbf{h}_1$،⋯،$\mathbf{h}_{n-k-1}$ دارد که هر کدکلمه در آن ترکیبی خطی از اعضای این پایه است. مشابه ماتریس مولد برای کد C، می‌توان ماتریس مولد $(n-k) \times n$ زیر را برای $C^{\perp}$ تشکیل داد،

$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_{n-k-1} \end{bmatrix} = \begin{bmatrix} h_{0,0} & h_{0,1} & \cdots & h_{0,n-1} \\ h_{1,0} & h_{1,1} & \cdots & h_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n-k-1,0} & h_{n-k-1,1} & \cdots & h_{n-k-1,n-1} \end{bmatrix}.$$

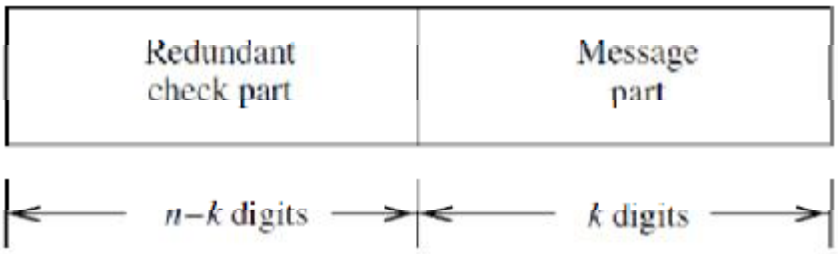
[1] Generator matrix
[2] Null space

به‌راحتی قابل اثبات است که $\mathbf{GH^T} = \mathbf{0}$ است، که $\mathbf{0}$ ماتریس $k \times (n-k)$ تمام صفر می‌باشد. کد C را می‌توان با ماتریس $\mathbf{H}$ معرفی کرد:

$$C = \{\mathbf{v} \in F_2^n : \mathbf{vH^T} = \mathbf{0}\}.$$

ماتریس $\mathbf{H}$ را *ماتریس بررسی توازن*[1] کد C می‌نامند. بنابراین یک کد خطی به‌طور منحصر به‌فرد با ماتریس مولد یا ماتریس بررسی توازن خود معرفی می‌شود. عمل کدگذاری در یک کد خطی با ماتریس مولد و عمل کدگشایی با ماتریس بررسی توازن آن صورت می‌گیرد.

اگر هر کدکلمه در یک کد خطی ساختاری قاعده‌مند نظیر شکل ۲-۱ داشته باشد، کد را کد *خطی قاعده‌مند*[2] نامند.



شکل ۲-۱: ساختار یک کدکلمه قاعده‌مند.

در این ساختار یک کدکلمه به دو بخش پیام و افزونگی تقسیم شده است. قسمت پیام متشکل از k بیت پیام و قسمت افزونگی متشکل از $n-k$ بیت بررسی توازن است. ماتریس مولد یک کد خطی قاعده‌مند با کدکلمه‌هایی مشابه شکل ۲-۱ به صورت زیر است.

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix} = \Big[\underbrace{\begin{matrix} p_{0,0} & p_{0,1} & \cdots & p_{0,n-k-1} \\ p_{1,0} & p_{1,1} & \cdots & p_{1,n-k-1} \\ \vdots & \vdots & \ddots & \vdots \\ p_{k-1,0} & p_{k-1,1} & \cdots & p_{k-1,n-k-1} \end{matrix}}_{P\ matrix} \quad \underbrace{\begin{matrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{matrix}}_{k \times k\ identity\ matrix\ I_k} \Big].$$

این ماتریس از دو زیرماتریس تشکیل شده است، یک زیرماتریس $\mathbf{P}$ به ابعاد $k \times (n-k)$، در سمت چپ و ماتریس واحد از مرتبه k در سمت راست. برای سادگی این ماتریس را به‌صورت $\mathbf{G} = [\mathbf{P} \quad \mathbf{I}_k]$ نمایش می‌دهیم. با ساختار ارائه شده برای $\mathbf{G}$ مشخص است که هر پیام که در آن ضرب شود، k بیت سمت راست کدکلمه حاصل همان k بیت پیام (بدون هیچگونه جابه‌جایی) است. ماتریس مولدی با چنین ساختار را یک *ماتریس مولد قاعده‌مند*[3] می‌نامند.

[1] Parity-check matrix
[2] Systematic linear code
[3] Systematic generator matrix

اگر ماتریس مولد یک کد خطی C'، یعنی $\mathbf{G}'$، قاعده‌مند نباشد، با عملیات سطری مقدماتی (و احتمالا جایگشت ستون‌ها) می‌توان آن را به حالت قاعده‌مند تبدیل کرد. ماتریس حاصل را *ماتریس معادل ترکیبیاتی*[1] $\mathbf{G}'$ می‌نامند و کد حاصل از این ماتریس را کد *معادل ترکیبیاتی*[2] C' گویند. C' و C احتمالا در چیدمان (یا ترتیب) بیت-هایشان با هم تفاوت دارند، به این معنی که کدکلمات C توسط یک جایگشت در بیت‌های کدکلمات C' حاصل می‌شوند.

اگر ماتریس مولد یک کد خطی قاعده‌مند باشد، ماتریس بررسی توازن آن نیز به شکل زیر است.

$$\mathbf{H} = [\mathbf{I}_{n-k} \quad \mathbf{P}^{\mathbf{T}}] = \begin{bmatrix} 1 & 0 & \cdots & 0 & p_{0,0} & p_{1,0} & \cdots & p_{k-1,0} \\ 0 & 1 & \cdots & 0 & p_{0,1} & p_{1,1} & \cdots & p_{k-1,1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & p_{0,n-k-1} & p_{1,n-k-1} & \cdots & p_{k-1,n-k-1} \end{bmatrix}.$$

به‌راحتی قابل اثبات است که $\mathbf{GH^T} = \mathbf{0}$ که $\mathbf{0}$ ماتریس تمام صفر به ابعاد $k \times (n-k)$ است.

۲-۱-۲ تشخیص خطا با کدهای خطی

فرض کنید یک کدکلمه $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ در یک کد خطی C ارسال شده و $\mathbf{r} = (r_0, r_1, \cdots, r_{n-1})$ کلمه دریافتی باشد. به‌دلیل وجود نویز، برخی از مولفه‌های متناظر $\mathbf{v}$ و $\mathbf{r}$ با هم متفاوت خواهند بود. بردار حاصل جمع $\mathbf{r}$ و $\mathbf{v}$ را به‌صورت زیر در نظر بگیرید،

$$\mathbf{e} = \mathbf{r} + \mathbf{v} = (e_0, e_1, \cdots, e_{n-1}) = (r_0 + v_0, r_1 + v_1, \cdots, r_{n-1} + v_{n-1}), \qquad (۱-۲)$$

که عمل $+$، جمع در پیمانه ۲ است. در این صورت اگر $r_j \neq v_j$، $e_j = 1$ و اگر $r_j = v_j$، $e_j = 0$ خواهد بود. بنابراین مولفه‌هایی از بردار $\mathbf{e}$ برابر با ۱ هستند که خطا در اثر عبور از کانال رخ داده است. از این رو بردار $\mathbf{e}$ را *الگوی خطا*[3] می‌نامند. واضح است که $2^n - 1$ الگوی خطای متمایز وجود دارد. با استفاده از معادله (۲-۱) می‌توان کلمه دریافتی $\mathbf{r}$ را به‌صورت زیر نوشت،

$$\mathbf{r} = \mathbf{v} + \mathbf{e}.$$

در گیرنده کدکلمه ارسالی و الگوی خطای ناشی از نویز کانال مشخص نیست. در مرحله اول گیرنده باید تشخیص دهد که آیا خطایی در کلمه دریافتی $\mathbf{r}$ وجود دارد یا خیر. اگر وجود خطا تشخیص داده شد، کدگشا باید یک برآوردی از بردار خطای $\mathbf{e}$ بر مبنای ساختار کد C و اطلاعاتی که از کانال در اختیار دارد، بکند. برای اینکه گیرنده تشخیص دهد خطایی در کلمه دریافتی وجود دارد، بردار $\mathbf{s}$ از معادله زیر را محاسبه می‌کند،

$$\mathbf{s} = (s_0, s_1, \cdots, s_{n-k-1}) = \mathbf{rH^T}.$$

اگر $\mathbf{s=0}$ ، آنگاه $\mathbf{r}$ یک کدکلمه است و گیرنده خطایی در آن مشاهده نمی‌کند (از بخش قبل می‌دانیم که اگر $\mathbf{v}$ یک کدکلمه در C باشد، $\mathbf{vH^T} = \mathbf{0}$). البته اگر $\mathbf{r}$ کدکلمه‌ای در C باشد که با آنچه ارسال شده متفاوت باشد، گیرنده دچار خطای کدگشایی می‌شود. این اتفاق زمانی رخ می‌دهد که نویز کانال بتواند کدکلمه ارسالی $\mathbf{v}$ را به

[1] Combinatorially equivalent matrix
[2] Combinatorially equivalent code
[3] Error pattern

کدکلمه دیگری در C تبدیل کند. الگوی خطایی که چنین خطایی را ایجاد می‌کند، *الگوی خطای نامحسوس*[1] نامیده می‌شود و تعداد آنها برابر با $2^k - 1$ می‌باشد. از آنجا که بردار $\mathbf{s}$ برای تشخیص وجود خطا در $\mathbf{r}$ استفاده می‌شود، آن را مشخصه[2] $\boldsymbol{r}$ می‌نامند.

۲-۱-۳ کمترین فاصله همینگ یک کد خطی

فرض کنید $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ یک بردار n-مولفه ای روی F_2 باشد. *وزن همینگ*[3] (یا به‌طور ساده وزن) بردار $\mathbf{v}$ برابر با تعداد مولفه‌های ناصفر $\mathbf{v}$ می‌باشد و با $w(\mathbf{v})$ نمایش داده می‌شود. کمترین وزن بین وزن کدکلمه‌های ناصفر یک کد C ، *کمترین وزن*[4] C نامیده می‌شود، که با $w_{min}(C)$ نمایش داده می‌شود. بنابراین

$$w_{\min}(C) = \min\{\mathrm{w}(\mathbf{v}): \mathbf{v} \in C, \mathbf{v} \neq \mathbf{0}\}.$$

فرض کنید $\mathbf{v}$ و $\mathbf{w}$ دو کدکلمه در یک کد خطی C باشند. تعداد مکان‌هایی (بیت‌هایی) که این دو کدکلمه با هم متفاوتند را *فاصله همینگ*[5] (یا به‌طور ساده فاصله) آنها گویند و با $d(\mathbf{v},\mathbf{w})$ نمایش می‌دهند. فاصله همینگ یک تابع متری است، به این معنی که در نامساوی مثلث صدق می‌کند. اگر $\mathbf{v}$، $\mathbf{w}$ و $\mathbf{x}$ سه کدکلمه در یک کد خطی باشند، آنگاه

$$d(\mathbf{v}, \mathbf{w}) + d(\mathbf{w}, \mathbf{x}) \geq d(\mathbf{v}, \mathbf{x}).$$

از تعریف فاصله همینگ بین دو کدکلمه و وزن همینگ یک کدکلمه نتیجه می شود که فاصله همینگ بین $\mathbf{v}$ و $\mathbf{w}$ برابر با وزن همینگ $\mathbf{w} + \mathbf{v}$ است. طبق تعریف کمترین فاصله یک کد C ، که با $d_{min}(C)$ نمایش داده می‌شود، برابر با کوچکترین فاصله بین کدکلمه‌های C است. به عبارت دیگر

$$d_{min}(C) = \min\ \{d(\mathbf{v}, \mathbf{w}): \mathbf{v}, \mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\}.$$

قابلیت تشخیص و تصحیح خطای یک کد C زمانی که از کانال BSC استفاده می‌شود، توسط کمترین فاصله آن تعیین می‌شود. برای یک $C(n,k)$ با کمترین فاصله $d_{min}(C)$، جمع هیچ بردار خطایی با حداکثر وزن $d_{min}(C) - 1$ با یک کدکلمه منجر به کدکلمه دیگری نخواهد شد. بنابراین همه خطاهای با حداکثر وزن $d_{min}(C) - 1$ توسط کدگشا قابل تشخیص هستند. البته اگر $\mathbf{v}$ یک کدکلمه در C باشد و بردار خطایی با وزن $d_{min}(C)$ با $\mathbf{v}$ جمع شود که اتفاقا بردار حاصل نیز یک کدکلمه باشد، مشخصه آن برابر صفر است و در نتیجه خطا قابل تشخیص نخواهد بود. بنابراین به‌طور کلی، تمام بردارهای خطا با حداکثر وزنی برابر با $d_{min}(C) - 1$ حتما تشخیص داده می‌شوند، ولی بردار خطاهایی با وزنی حداقل برابر با $d_{min}(C)$ الزاما قابل تشخیص نیستند. به همین علت مقدار $d_{min}(C) - 1$، *توانایی تشخیص خطای کد*[6] C نامیده می‌شود.

---

[1] Undetectable error pattern
[2] Syndrome
[3] Hamming weight
[4] Minimum weight
[5] Hamming distance
[6] Error detecting capability

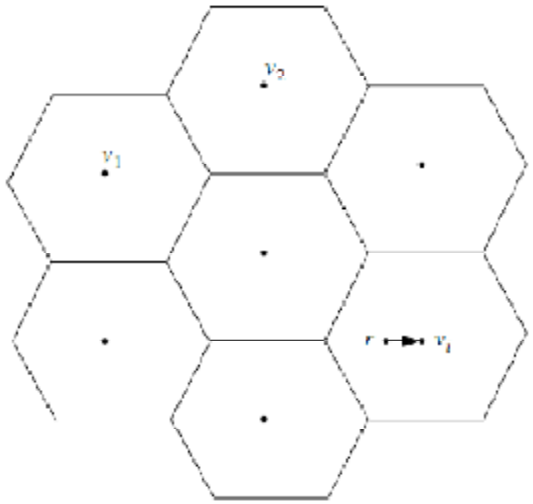
۲-۱-۴ کدگشایی کدهای خطی

فرض کنید C کدی با ماتریس بررسی توازن $\mathbf{H}$، کمترین فاصله $d_{min}(\mathrm{C})$ و مجموعه کدکلمات $\{\mathbf{v}_i | 1 \le i \le 2^k\}$ باشد. اگر کدکلمه‌ای ارسال وکلمه $\mathbf{r}$ دریافت شود، در کدگشایی MLD[1]، کلمه $\mathbf{r}$ به کدکلمه $\mathbf{v}_j$ کدگشایی می‌شود اگر و فقط اگر

$$P(\mathbf{r}|\mathbf{v}_j) > P(\mathbf{r}|\mathbf{v}_i),\ \ 1 \le i \le 2^k,\ \ i \ne j.$$

در یک کانال BSC رابطه بالا معادل یافتن نزدیکترین کدکلمه به $\mathbf{r}$ است (کدکلمه‌ای که فاصله آن با $\mathbf{r}$ کمترین مقدار باشد). این نوع کدگشایی، *کدگشایی کمترین فاصله*[2] (MDD) نامیده می‌شود. پس در MDD، کدگشا باید فاصله بین کلمه دریافتی و همه کدکلمات را محاسبه و کدکلمه‌ای که کمترین فاصله با کلمه دریافتی دارد (که الزاما منحصر بفرد نیست) را به عنوان کدکلمه ارسالی معرفی کند. این کدگشا، *کدگشا و تصحیح خطای کامل*[3] نامیده می‌شود و نیاز به 2^k محاسبه دارد. اگر در یک کد C تعداد کدکلمات زیاد باشد (k مقدار بزرگی باشد)، این روش کدگشایی زمان زیادی احتیاج خواهد داشت و عملا به دست آوردن کدکلمه مورد نظر غیر ممکن است. ولی برای بسیاری از کدهای خطی، الگوریتم‌های بهینه کدگشایی و تصحیح خطای غیر کامل ارائه شده‌اند که احتمال خطای کدگشایی مقدار کوچکی دارد و پیچیدگی محاسباتی کمتری دارند.

در هر الگوریتم کدگشایی هدف افراز فضای F_2^n به 2^k ناحیه است به‌طوری که هر ناحیه شامل یک و فقط یک کدکلمه باشد. با مشخص شدن ناحیه‌ای که کلمه دریافتی در آن قرار دارد، کدکلمه درون آن ناحیه به عنوان کدکلمه ارسال شده معرفی می‌شود. این نواحی، *نواحی کدگشایی*[4] نامیده می‌شوند. شکل ۲-۲ یک نمایش هندسی از این نواحی را ارائه می‌دهد.



شکل ۲-۲: یک نمایش هندسی از نواحی کدگشایی.

[1] Maximum likelihood decoding
[2] Minimum distance decoding
[3] Complete error correction decoding
[4] Decoding regions