A New Method for Blind Recognition of the Initial State of Synchronous Scramblers When Located after the Channel Encoder

S. Ghazi Maghrebi *, H. Alemi

*Dean of Islamic Azad University /Yadegar-e-Imam Khomeini (RAH) shahre Rey

(Received: 05/03/2020, Accepted: 05/08/2020)

ABSTRACT

The scrambler block is one of the most commonly used blocks in digital communication protocol design. This block is used to randomize the bit string and usually is used after the source encoder or after the channel encoder. In blind detection this block, is assumed to be located after the source encoder or after the channel encoder. LFSRs are often used to design linear scramblers. Therefore, scramblers are defined by usage of feedback polynomials and initial states. In previous works, the initial state of the scrambler after channel encoder has been identified, but under some circumstances, these algorithms cannot provide proper response. In these conditions, to identify initial state of the scrambler, a full search method may be used which takes a long time. In this paper, a new algorithm for initial state of scrambler detection, after channel encoder, is presented. The proposed algorithm is able to identify the initial state of scrambler in the cases that other algorithms cannot do anything. The new algorithm also reduces the search space and as a result, it need much less time for the identification process.

Keywords: Blind Recognition, Synchronous Scrambler, Initial State, Channel Encoder

*Corresponding Author Email: s_ghazi2002@yahoo.com

نشریه علمی "پدافند الکترونیکی و سایبری"
سال نهم، شماره ۱، بهار ۱۴۰۰، ص ۲۷-۱۹

علمی – پژوهشی

روشی جدید در شناسایی کور حالت اولیه درهم‌ساز هم‌زمان بعد از کدگذار کانال

سعید قاضی مغربی[1*]، هادی عالمی[2]

۱- دانشیار و ۲- کارشناسی ارشد، دانشگاه آزاد واحد یادگار امام خمینی (ره)، شهرری، ایران

(دریافت: ۱۳۹۸/۱۲/۱۵، پذیرش: ۱۳۹۹/۰۵/۱۵)

چکیده

بلوک درهم‌ساز یکی از پُرکاربردترین بلوک‌های مخابراتی در طراحی پروتکل‌های مخابرات دیجیتال است. این بلوک، به‌منظور تصادفی‌سازی رشته بیت‌ها مورد استفاده قرار می‌گیرد و معمولاً بعد از کدگذار منبع یا بعد از کدگذار کانال استفاده می‌شود. در شناسایی کور نیز فرض می‌کنند بلوک درهم‌ساز بعد از کدگذار منبع یا بعد از کدگذار کانال قرار گرفته باشد. غالباً در طراحی درهم‌سازهای خطی از LFSR ها استفاده می‌شود. بنابراین، درهم‌سازها را با استفاده از چندجمله‌ای بازخورد و حالت اولیه آن تعریف می‌کنند. در کارهای پیشین، به شناسایی حالت اولیه درهم‌ساز بعد از کدگذار کانال پرداخته شده است، ولیکن باید توجه داشت که در همه شرایط، الگوریتم‌های ارائه‌شده قادر به پاسخگویی نیستند. در این شرایط، ممکن است از روش جستجوی کامل جهت شناسایی حالت اولیه درهم‌ساز استفاده شود که روشی بسیار زمان‌بَر است. در این مقاله، الگوریتم جدیدی برای شناسایی حالت اولیه درهم‌ساز بعد از کدگذار کانال ارائه می‌شود، که قادر است در شرایطی که الگوریتم‌های دیگر پاسخگو نیستند، به شناسایی حالت اولیه درهم‌ساز بپردازد. در الگوریتم جدید، فضای جستجو نیز کاهش پیدا کرده و در نتیجه زمان بسیار کمتری برای شناسایی صرف می‌شود.

کلیدواژه‌ها: شناسایی کور، درهم‌ساز هم‌زمان، حالت اولیه، کدگذار کانال، شناسایی حالت اولیه

۱- مقدمه

در فناوری‌های مخابرات دیجیتال، از بلوک درهم‌ساز[1] به‌منظور درهم‌ریزی بیت‌های ارسالی استفاده می‌شود به‌نحوی که تنها، گیرنده‌ای که معکوس درهم‌ساز[2] مناسب را داشته باشد، قادر به دریافت بیت‌های ارسالی است. عملکرد درهم‌سازها بدین گونه است که با تغییر بیت‌ها، رشته بیت اصلی را به‌صورت یک دنباله تصادفی درمی‌آورند [۱].

تولید دنباله‌های کاملاً تصادفی در پیاده‌سازی فرستنده‌های مخابراتی به علت غیرقابل بازسازی بودن در گیرنده، عملاً کاربردی نیستند و در نتیجه استفاده نمی‌شوند. به همین دلیل، از دنباله‌های شبه تصادفی[3] به‌جای دنباله‌های تصادفی، برای کاربردهای مختلف از جمله در پیاده‌سازی درهم‌سازها استفاده می‌شود [۲].

یک دنباله تصادفی دودویی، دنباله‌ای از صفر و یک‌ها است که به‌طور متوسط، احتمال مشاهده صفر و یک در آن برابر باشد.

خاصیت ارسال دنباله‌های تصادفی آن است که باعث سفید شدن طیف فرکانسی می‌شود و در نتیجه مؤلفه‌های نامطلوب فرکانسی را از بین می‌برد و از طرف دیگر مشکل هم‌زمانی دمدولاسیون را برطرف می‌نماید. البته، از درهم‌سازها می‌توان به‌عنوان یک رمزکننده نیز استفاده کرد[۱].

ثبات‌های انتقالی با فیدبک خطی[4] (LFSR) یکی از بهترین ابزارها به منظور تولید دنباله‌های شبه تصادفی هستند.

ثبات انتقالی با بازخورد خطی را می‌توان به‌صورت یک مدار منطقی شامل چندین ثبات (عنصر ذخیره‌ساز)، تعدادی جمع کننده در پیمانه دو (XOR) و تعدادی ضرب کننده در پیمانه دو نشان داد. با استفاده از این مدارهای منطقی، عملیات ضرب دو چندجمله‌ای و تقسیم دو چندجمله‌ای را می‌توان پیاده‌سازی نمود [۲]. به‌عنوان مثال، در شکل (۱) مدار منطقی یک LFSR نشان داده شده است.

مقادیر ثبات‌ها و ضرایب آنها توسط عناصر میدان GF(2) یعنی 0 یا 1 انتخاب می‌شوند. ضرایب موجود در شکل (۱) که با

* رایانامه نویسنده مسئول: s_ghazi2002@yahoo.com

[1] Scrambler
[2] Descrambler
[3] Pseudo Random
[4] Linear Feedback Shift Register

ناشر: دانشگاه جامع امام حسین (ع)

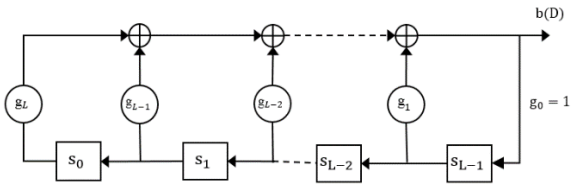
g_i نشان داده شده است، یک چندجمله‌ای به نام $\boldsymbol{g}(D)$ را تشکیل می‌دهد و به‌صورت رابطه (۱) تعریف می‌شود [۲]:

$$\boldsymbol{g}(D) = g_0 + g_1 D + g_2 D^2 + \cdots + g_L D^L \qquad (۱)$$

در این ساختار چنانچه اتصال g_i برقرار باشد، $g_i = 1$ و در غیر این صورت $g_i = 0$ است. مقادیر g_0 و g_L در این چندجمله‌ای برابر یک است.

چندجمله‌ای تعریف‌شده در رابطه (۱) را چندجمله‌ای بازخورد[1] LFSR و مقادیر اولیه موجود در ثبات‌ها را حالت اولیه[2] LFSR می‌نامند. باید توجه شود که دنباله خروجی یک LFSR، به چندجمله‌ای بازخورد و مقدار حالت اولیه آن بستگی دارد.

غالباً درهم‌سازهای خطی با استفاده از LFSR ها پیاده‌سازی می‌شوند. نحوه به‌کارگیری LFSR ها، نوع درهم‌ساز را تعیین می‌نماید [۳].

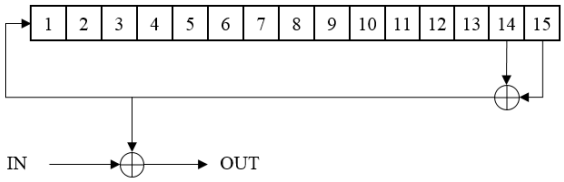


شکل (۱): مدار منطقی یک LFSR [۲]

در شکل (۲) نمونه‌ای از یک درهم‌ساز هم‌زمان[3] یا جمع شونده[4] نشان داده شده است. با توجه به این شکل، ملاحظه می‌شود که دنباله ورودی درهم‌ساز با دنباله خروجی LFSR به پیمانه دو جمع شده و سپس به خروجی می‌رود. از این‌رو، به این نوع درهم‌ساز، درهم‌ساز جمع شونده نیز می‌گویند [۳].

ازآنجاکه باید عملیات معکوس درهم‌ساز در گیرنده انجام شود، دنباله خروجی LFSR در درهم‌ساز فرستنده و عکس درهم‌ساز گیرنده باید یکسان باشد. برای این منظور، لازم است که علاوه بر چندجمله‌ای بازخورد، مقدار حالت اولیه ثبات‌ها نیز یکسان باشند. به این مقدار حالت اولیه ثبات‌ها، الگوی هم‌زمانی[5] نیز می‌گویند، زیرا باعث هم‌زمان شدن دنباله خروجی LFSR ها و در نتیجه باعث هم‌زمان‌سازی معکوس درهم‌ساز گیرنده با درهم‌ساز فرستنده می‌شود. لذا، به این نوع از درهم‌سازها، درهم‌سازهای هم‌زمان نیز می‌گویند [۳].

در بعضی از پروتکل‌ها، از قالب‌بندی[6] که برای ایجاد هم‌زمانی بکار می‌رود، استفاده نمی‌کنند و رشته بیت را به‌صورت یک دنباله پیوسته[7] ارسال می‌کنند.

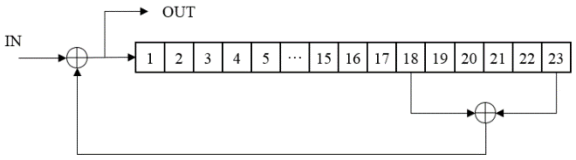


شکل (۲): ساختار درهم‌ساز هم‌زمان در پروتکل WiMAX [۴]

در این پروتکل‌ها با استفاده از درهم‌سازی بدون نیاز به اطلاعات بیرونی و فقط با استفاده از رشته بیت دریافتی، گیرنده خودش را با فرستنده هم‌زمان می‌کند.

درهم‌سازهای خودهمزمان، برعکس درهم‌سازهای هم‌زمان، به الگوی همزمان‌سازی نیاز ندارند. زیرا دنباله خروجی درهم‌سازهای خودهمزمان، علاوه بر خروجی به داخل LFSR نیز وارد می‌شوند. به همین دلیل، این درهم‌سازها را درهم‌سازهای خودهمزمان می‌نامند [۳].

در ساختار درهم‌سازهای خودهمزمان، عملیات درهم‌سازی با استفاده از تقسیم دنباله ورودی درهم‌ساز بر چندجمله‌ای بازخورد صورت می‌گیرد. عملیات عکس درهم‌سازی نیز با استفاده از ضرب دنباله ورودی در چندجمله‌ای بازخورد انجام می‌شود. لذا این نوع درهم‌سازها را درهم‌سازهای ضرب شونده نیز می‌نامند. در شکل (۳) نمونه‌ای از یک درهم‌ساز خودهمزمان نشان داده شده است [۳].



شکل (۳): ساختار درهم‌ساز خودهمزمان در پروتکل HDSL [۵]

امروزه با طیف وسیعی از سامانه‌های مخابراتی روبرو هستیم که در اطراف ما در حال ارسال و دریافت اطلاعات می‌باشند. با در نظر گرفتن مسئله امنیت لایه فیزیکی، مسائل زیادی در این حوزه دارای جذابیت می‌باشند. این مسائل عموماً می‌توانند در یک یا چند زمینه از زمینه‌های زیر خلاصه شوند: ۱- اختلال شبکه، ۲- کشف ساختار ارتباطی شبکه و شنود[8] اطلاعات ارسالی، ۳- فریب شبکه و کاربران آن، ۴- نفوذ به شبکه و جا زدن خود به‌عنوان یک کاربر مجاز و ۵- کنترل کامل یا جزئی شبکه [۶].

[1] Feedback Polynomial
[2] Initial State
[3] Synchronous Scramblers
[4] Additive
[5] Sync Pattern
[6] Framing
[7] Continuous
[8] Eavesdrop

موضوع این مقاله در زمینه دوم تعریف می‌شود که مربوط به شناسایی ساختار سامانه مخابراتی و شنود اطلاعات ارسالی آن می‌باشد. برای این منظور لازم است تا با استفاده از مهندسی معکوس[1]، سامانه مخابراتی مورد نظر شناسایی شود.

یک شنودگر[2]، هیچ اطلاعاتی از سامانه مخابراتی هدف و مدل طراحی آن را ندارد. لذا، اساساً کار شناسایی و مهندسی معکوس یک سامانه مخابراتی بسیار دشوار است. یکی از دلایل این دشواری، انتخاب‌های بسیار متنوع عناصر یک سامانه مخابراتی است. همچنین، سیگنال دریافت شده از سامانه مخابراتی هدف، لزوماً یک سیگنال سالم نیست و ممکن است که توسط عوامل مختلف، تخریب شده باشد [۷].

بنابراین، یک شنودگر باید مانند یک گیرنده برای سامانه مخابراتی عمل نماید. همان‌طور که گیرنده باید معکوس عملیات‌های طراحی‌شده در فرستنده را انجام دهد تا به اطلاعات ارسالی دست یابد، یک شنودگر نیز باید همین مراحل را به ترتیب طی نماید. برای این منظور، لازم است که ابتدا هر بلوک مخابراتی را شناسایی کرده و سپس عملیات معکوس آن را اعمال کرده تا به بلوک بعدی برسد. مجدد کار شناسایی و انجام عملیات معکوس برای بلوک بعدی تکرار می‌شود. این کار تا رسیدن به اطلاعات ارسالی ادامه می‌یابد.

برای اینکه یک شنودگر بتواند به پارامترهای یک بلوک مخابراتی دست پیدا کند، لازم است تا با استفاده از روش‌های شناسایی کور به شناسایی پارامترهای آن بلوک مخابراتی بپردازد. برای نمونه، در [۸] و [۹] روش‌هایی برای شناسایی کور کدهای چرخشی کانال و در [۱۰] و [۱۱] روش‌هایی برای شناسایی کدهای کانولوشنی کانال ارائه شده است.

در شناسایی کور بلوک مخابراتی درهم‌ساز، فرض بر این است که دنباله خروجی درهم‌ساز موجود است و با استفاده از آن باید چندجمله‌ای بازخورد درهم‌ساز شناسایی شود. البته درصورتی‌که درهم‌ساز از نوع هم‌زمان باشد، باید حالت اولیه درهم‌ساز را نیز به‌دست آورد [۷].

نکته مهمی که باید به آن توجه شود این است که در شناسایی بعضی از بلوک‌های مخابراتی که پیچیدگی بیشتری دارند، شناسایی آن بلوک، صرفاً با استفاده از دنباله خروجی صورت نمی‌گیرد. بلکه در شناسایی این بلوک‌ها، بلوک‌های قبلی اعمال‌شده بر روی رشته بیت را نیز در نظر گرفته و فرضیاتی را بر روی دنباله ورودی بلوک مورد شناسایی، لحاظ می‌کنند. برای مثال، در شناسایی پارامترهای جایگردان‌ها[3]، که در [۱۲]، [۱۳]، [۱۴] و [۱۵] به آن پرداخته شده است، فرض بر این است که بلوک جایگردان بر روی خروجی یک بلوک کدگذار کانال اعمال می‌شود. لذا، با در نظر گرفتن چنین فرضی، الگوریتم شناسایی کور طراحی شده است.

در طراحی سامانه‌های مخابرات دیجیتال، ممکن است که بلوک درهم‌ساز بعد از بلوک کدگذار منبع[4] و یا بعد از بلوک کدگذار کانال[5] استفاده شود. لذا، می‌توان در شناسایی کور این بلوک مخابراتی، در مورد دنباله ورودی آن فرضیاتی را در نظر گرفت. بنابراین، چنانچه بلوک درهم‌ساز بعد از کدگذار کانال قرار گرفته باشد، فرض شناسایی بدین‌صورت است که دنباله ورودی درهم‌ساز، خروجی کدگذار کانال است. در مواردی هم که بلوک درهم‌ساز بعد از کدگذار منبع قرار می‌گیرد، با توجه به اینکه معمولاً خروجی کدگذار منبع دارای بایاس[6] (یعنی به‌طور متوسط، احتمال مشاهده صفر با احتمال مشاهده یک در آن یکسان نیست) می‌باشد، فرض شناسایی این است که دنباله ورودی درهم‌ساز دارای بایاس باشد.

با توجه به فرضیات بالا، روش‌های ارائه‌شده در مقالات، برای شناسایی درهم‌سازهای خطی را می‌توان به دو دسته کلی زیر تقسیم نمود.

۱- شناسایی کور درهم‌سازهای خطی با ورودی دارای بایاس
۲- شناسایی کور درهم‌سازهای خطی بعد از کدگذار کانال

در مقالات [۷] ، [۱۶] ، [۱۷] ، [۱۸] و [۱۹] به شناسایی چندجمله‌ای بازخورد درهم‌سازهای خطی با ورودی دارای بایاس پرداخته شده است. در اغلب این روش‌ها از روش جستجوی کامل برای شناسایی چندجمله‌ای بازخورد درهم‌ساز استفاده می‌شود. برای توقف عملیات جستجو و اطمینان از رسیدن به پاسخ مورد نظر، یک سری محاسبات آماری بر روی دنباله دریافتی در هر بار جستجو انجام می‌شود. درصورتی‌که چندجمله‌ای مورد جستجو صحیح باشد، نتیجه محاسبات آماری، بایاس‌دار بودن ورودی را تأیید می‌کند و در غیر این صورت اعلام تصادفی بودن می‌کند.

شناسایی حالت اولیه درهم‌سازهای هم‌زمان با ورودی دارای بایاس نیز در مقالات [۷] و [۱۸] بررسی شده است. در مقاله [۷] با فرض اینکه دنباله درهم‌ساز کننده یک کلمه کد بلوکی است، با استفاده از چندجمله‌ای بازخورد درهم‌ساز به کدگشایی دنباله

[1] Reverse Engineering
[2] Eavesdropper

[3] Interleavers
[4] Source Encoder
[5] Channel Encoder
[6] Bias

درهم‌ساز شده می‌پردازد. چنانچه بایاس دنباله ورودی درهم‌ساز زیاد باشد، نویز دنباله درهم‌ساز شده کم خواهد بود و با استفاده از کدگشایی تکراری[1] قابل کدگشایی می‌باشد. پس از کدگشایی، دنباله درهم‌ساز کننده و در نتیجه مقدار حالت اولیه درهم‌ساز به‌دست می‌آید.

در مقاله [۱۸] نیز با فرض اینکه دنباله ورودی درهم‌ساز دارای بایاس زیادی است، از روش آنالیز ویژه[2] استفاده کرده و دنباله درهم‌ساز کننده را شناسایی می‌نماید. سپس، با استفاده از این دنباله، حالت اولیه درهم‌ساز را به‌دست می‌آورد.

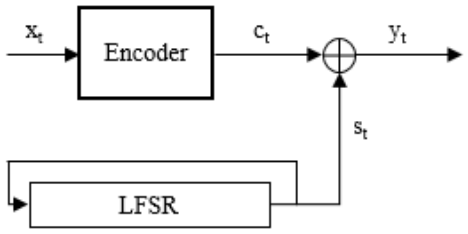
در مقالات [۲۰]، [۲۱] و [۲۲] به شناسایی چندجمله‌ای بازخورد درهم‌سازهای خطی بعد از کدگذار کانال پرداخته شده است. در این مقالات، با فرض مشخص بودن نوع و پارامترهای کد کانال قبل از درهم‌ساز و با استفاده از ماتریس بررسی توازن[3] کد، اثر کلمات کد را از بین برده و با استفاده از جستجوی کامل و محاسبات آماری به شناسایی چندجمله‌ای بازخورد درهم‌ساز می‌پردازند.

در مقالات [۲۳]، [۲۰]، [۲۱] و [۲۲] نیز به شناسایی حالت اولیه درهم‌سازهای هم‌زمان بعد از کدگذار کانال پرداخته شده است. در این مقالات، با در نظر گرفتن این نکته که کلمات کد در اکثر کدگذارهای کانال بایاس زیادی ندارند، از روش‌های قبلی برای شناسایی حالت اولیه درهم‌ساز استفاده نشده است. زیرا روش‌های مطرح‌شده در مقالات [۷] و [۱۸] بر مبنای بایاس زیاد دنباله ورودی درهم‌ساز استوار بودند و برای این شرایط کارایی مناسبی ندارند. از طرف دیگر، با فرض دانستن اطلاعات کدگذار قبل از درهم‌ساز، شرایط بهتری برای حل مسأله شناسایی به وجود می‌آید.

در این مقاله، ابتدا به معرفی روش‌های شناسایی حالت اولیه بعد از کدگذار کانال پرداخته و نقاط ضعف هر کدام بیان می‌شود. سپس، روش پیشنهادی ارائه شده و با روش‌های شناسایی موجود مقایسه می‌شود.

۲- روش‌های شناسایی حالت اولیه درهم‌ساز بعد از کدگذار کانال

در شکل (۴)، مدل کلی نحوه به‌کارگیری درهم‌سازهای هم‌زمان بعد از کدگذار کانال نشان داده شده است.



شکل (۴): مدل کلی درهم‌ساز هم‌زمان بعد از کدگذار کانال

برای شناسایی حالت اولیه درهم‌سازهای هم‌زمان بعد از کدگذار کانال، دو روش کلی بیان می‌شود. این دو روش، که هر دو در شرایط بدون نویز ارائه شده‌اند، عبارت‌اند از:

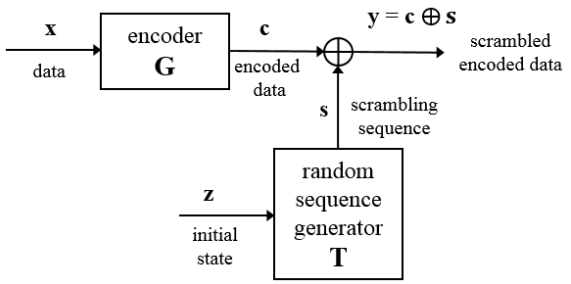
۱- روش شناسایی با استفاده از ماتریس معکوس
۲- روش شناسایی با استفاده از جستجوی کامل

در ادامه، به معرفی هر یک از این روش‌ها پرداخته و نقاط ضعف هر کدام بررسی می‌شود.

۲-۱- شناسایی با استفاده از ماتریس معکوس

در مقاله‌های [۲۳]، [۲۰] و [۲۱] به شناسایی حالت اولیه درهم‌ساز بعد از کدگذار کانال با استفاده از ماتریس معکوس پرداخته شده است. در این مراجع، با استفاده از ماتریس بررسی توازن کد کانال قبل از درهم‌ساز و نیز چندجمله‌ای بازخورد درهم‌ساز، به محاسبه حالت اولیه آن پرداخته‌اند.

در شکل (۵) ساختار درهم‌ساز بعد از کدگذار کانال ترسیم شده است. در این ساختار، رشته بیت اطلاعات (**x**) با استفاده از ماتریس مولد کد (***G***) به یک رشته کلمات کد (**c**) تبدیل می‌شود. از طرف دیگر، دنباله حالت اولیه درهم‌ساز (**z**) با استفاده از ماتریس مولد درهم‌ساز (***T***) به دنباله درهم‌ساز کننده (**s**) تبدیل می‌شود.



شکل (۵): ساختار درهم‌ساز بعد از کدگذار کانال [۲۳]

با توجه به شکل (۱)، مقدار ثبات‌های انتقالی در زمان دلخواه r را می‌توان با استفاده از رابطه زیر تعریف نمود [۲]:

[1] Iterative Decoding
[2] Eigen Analysis
[3] Parity Check Matrix

$$\boldsymbol{S}_r = \begin{bmatrix} s_{0.r} \\ s_{1.\mathrm{r}} \\ s_{2.\mathrm{r}} \\ \vdots \\ s_{L-2.r} \\ s_{\mathrm{L}-1.r} \end{bmatrix}$$

همچنین، با توجه به شکل (۱)، مقدار ثبات‌های انتقالی در زمان r+1 نیز با استفاده از روابط (۱) به‌دست می‌آید [۲]. ازآنجاکه مقدار هر ثبات در زمان $r+1$ ، شیفت یافته مقدار ثبات قبلی در زمان r می‌باشد، روابط (۱) تا قبل از آخرین ثبات برقرار است. مقدار آخرین ثبات نیز با توجه به شکل (۱) از حاصل‌ضرب همه ثبات‌های بعدی در چندجمله‌ای بازخورد به‌دست می‌آید.

$$\begin{aligned} s_{0.r+1} &= s_{1.r} \\ s_{1.r+1} &= s_{2.\mathrm{r}} \\ &\vdots \\ s_{L-2.r+1} &= s_{L-1.\mathrm{r}} \\ s_{L-1.r+1} &= g_L.s_{0.r} + g_{\mathrm{L}-1}.s_{1.r} + \cdots + g_1.s_{L-1.r} \end{aligned} \quad (۱)$$

با استفاده از روابط موجود در (۱)، رابطه (۲) به‌دست می‌آید [۲]:

$$\boldsymbol{S}_{r+1} = \begin{bmatrix} s_{0.r+1} \\ s_{1.r+1} \\ s_{2.r+1} \\ \vdots \\ s_{L-2.r+1} \\ s_{L-1.r+1} \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ g_L & g_{L-1} & g_{L-2} & g_{L-3} & \cdots & g_1 \end{bmatrix} \times \begin{bmatrix} s_{0.r} \\ s_{1.r} \\ s_{2.r} \\ \vdots \\ s_{L-2.r} \\ s_{L-1.r} \end{bmatrix} \quad (۲)$$

$$= \boldsymbol{F} \times \boldsymbol{S}_r$$

و نیز رابطه (۳) از آن نتیجه گرفته می‌شود [۲].

$$\boldsymbol{S}_r = \boldsymbol{F}^r \times \boldsymbol{S}_0 \quad (۳)$$

چنانچه چندجمله‌ای بازخورد درهم‌ساز به‌صورت چندجمله‌ای $\boldsymbol{g}(x) = 1 + g_1x + g_2x^2 + \cdots + g_Lx^L$ باشد، با استفاده از روابط (۲) و (۳) می‌توان ماتریس مولد درهم‌ساز $\boldsymbol{T}$ را به‌صورت رابطه (۴) به‌دست آورد [۲۳]. ماتریس مولد درهم‌ساز $\boldsymbol{T}$ ماتریسی است که چنانچه در مقدار حالت اولیه درهم‌ساز ضرب شود، دنباله درهم‌ساز کننده $\boldsymbol{s}$ را تولید می‌نماید. این ماتریس دارای L سطر و n ستون است. L ستون اول آن یک ماتریس واحد می‌باشد که با ضرب ماتریس $\boldsymbol{T}$ در بردار حالت اولیه، همان مقادیر حالت اولیه را در ابتدای دنباله درهم‌سازکننده $\boldsymbol{s}$ تولید می‌نماید. L ستون بعدی این ماتریس با استفاده از ماتریس $\boldsymbol{F}$ به توان L مشخص می‌شود که برای تولید L بیت دوم از دنباله درهم‌سازکننده، در نظر گرفته شده است. L بیت دوم از دنباله درهم‌سازکننده، همان مقادیر ثبات‌های انتقالی در زمان L ام هستند. بدین ترتیب L بیت‌های بعدی با استفاده از توان‌های مضارب L از ماتریس $\boldsymbol{F}$ به‌دست می‌آیند. این ماتریس مولد به اندازه‌ای که از دنباله درهم‌سازکننده نیاز باشد، می‌تواند ادامه داشته باشد. در این شرایط، n ستون ابتدایی از این ماتریس برای تولید n بیت از دنباله درهم‌سازکننده کافی است.

$$\boldsymbol{F} = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ g_L & g_{L-1} & g_{L-2} & g_{L-3} & \cdots & g_1 \end{bmatrix} \quad (۴)$$

$$\rightarrow \boldsymbol{R}_{L\times(q+1).L} = [\boldsymbol{I}_L \quad \boldsymbol{F}^L \quad \ldots \quad \boldsymbol{F}^{qL}]$$

$$\Rightarrow \boldsymbol{T} = \boldsymbol{R}(:, 1:n)$$

با xor شدن دو دنباله کلمات کد $\boldsymbol{c}$ و دنباله درهم‌ساز کننده $\boldsymbol{s}$ ، دنباله درهم‌ساز شده $\boldsymbol{y}$ تولید می‌شود که دنباله خروجی درهم‌ساز است. کلمات کد $\boldsymbol{c}$ نیز با ضرب بلوک‌های k بیتی دنباله بیت اطلاعات $\boldsymbol{x}$ در ماتریس مولد کد $\boldsymbol{G}$ به‌دست می‌آیند. روابط ریاضی نشان داده‌شده در شکل (۵) به‌صورت رابطه (۵) است [۲۳].

$$\boldsymbol{y}_{1\times n} = \boldsymbol{c}_{1\times n} \oplus \boldsymbol{s}_{1\times n} = \boldsymbol{x}_{1\times k}.\boldsymbol{G}_{k\times n} \oplus \boldsymbol{z}_{1\times L}.\boldsymbol{T}_{L\times n} \quad (۵)$$

با توجه به ساختار نشان داده‌شده، هدف محاسبه دنباله حالت اولیه درهم‌ساز ($\mathbf{z}$) است.

از طرف دیگر، مشخص است که ماتریس کلمات دوگان کد که با $\boldsymbol{H}$ نشان داده می‌شود، بر تمام کلمات کد عمود بوده و حاصل‌ضرب داخلی آن در ماتریس مولد کد برابر صفر می‌شود. لذا، رابطه زیر برقرار است:

$$\boldsymbol{G}.\boldsymbol{H}^T = \boldsymbol{0} \rightarrow \boldsymbol{c}.\boldsymbol{H}^T = \boldsymbol{0} \quad (۶)$$

اکنون، با ضرب ماتریس $\boldsymbol{H}$ در رابطه (۵) می‌توان نوشت [۲۳]:

$$\begin{aligned} &\boldsymbol{y}_{1\times n}.\boldsymbol{H}^T_{n\times(n-k)} \\ &= \boldsymbol{c}_{1\times n}.\boldsymbol{H}^T_{n\times(n-k)} \oplus \boldsymbol{s}_{1\times n}.\boldsymbol{H}^T_{n\times(n-k)} \\ &\qquad = \boldsymbol{s}_{1\times n}.\boldsymbol{H}^T_{n\times(n-k)} \\ &\qquad = \boldsymbol{z}_{1\times L}.\boldsymbol{T}_{L\times n}.\boldsymbol{H}^T_{n\times(n-k)} \end{aligned} \quad (۷)$$

با تعریف ماتریس $\boldsymbol{E}_{L\times(n-k)} = \boldsymbol{T}_{L\times n}.\boldsymbol{H}^T_{n\times(n-k)}$ ، و ضرب ماتریس $\boldsymbol{E}^T$ در طرفین رابطه (۷)، رابطه (۸) به‌دست می‌آید [۲۳].

$$\boldsymbol{y}_{1\times n}\,.\,\boldsymbol{H}^{T}_{n\times(n-k)}\,.\,\boldsymbol{E}^{T}_{(n-k)\times L} = \boldsymbol{z}_{1\times L}\,.\,\boldsymbol{E}_{L\times(n-k)}\,.\,\boldsymbol{E}^{T}_{(n-k)\times L} \quad (۸)$$

سپس، ماتریس $\boldsymbol{A}_{L\times L} = \boldsymbol{E}_{L\times(n-k)}\,.\,\boldsymbol{E}^{T}_{(n-k)\times L}$ تعریف می‌شود که یک ماتریس مربعی با ابعاد $L \times L$ است. چنانچه این ماتریس معکوس‌پذیر باشد، دارای ماتریس معکوسی به‌صورت $\boldsymbol{A}^{-1}_{L\times L}$ است و با استفاده از رابطه (۹) مقدار حالت اولیه درهم‌ساز ($\boldsymbol{z}_{1\times L}$) به‌دست می‌آید [۲۳].

$$\boldsymbol{y}_{1\times n}\,.\,\boldsymbol{H}^{T}_{n\times(n-k)}\,.\,\boldsymbol{E}^{T}_{(n-k)\times L}.\boldsymbol{A}^{-1}_{L\times L} = \boldsymbol{z}_{1\times L}\,.\,\boldsymbol{E}_{L\times(n-k)}\,.\,\boldsymbol{E}^{T}_{(n-k)\times L}.\boldsymbol{A}^{-1}_{L\times L} \quad (۹)$$

$$\boldsymbol{z}_{1\times L} = \boldsymbol{y}_{1\times n}\,.\boldsymbol{H}^{T}_{n\times(n-k)}\,.\,\boldsymbol{E}^{T}_{(n-k)\times L}.\boldsymbol{A}^{-1}_{L\times L}$$

همان‌طور که ملاحظه می‌شود، شرط معکوس‌پذیر بودن ماتریس $\boldsymbol{A}_{L\times L}$ یک شرط لازم برای رسیدن به جواب می‌باشد. درصورتی‌که این ماتریس معکوس‌پذیر نباشد، عملیات شناسایی حالت اولیه با استفاده از این روش، متوقف می‌شود. اکنون، باید بررسی کرد که تحت چه شرایطی ماتریس مورد نظر، معکوس‌پذیر نمی‌شود.

۲-۱-۱- ضعف روش شناسایی با استفاده از ماتریس معکوس

ازآنجایی‌که ماتریس $\boldsymbol{E}$ دارای ابعاد $L \times (n-k)$ است، رتبه[1] این ماتریس حداکثر برابر $\min(L\,.\,(n-k))$ است. بنابراین در حالتی که $L \le (n-k)$ باشد، $\text{rank}\,(\boldsymbol{E})$ حداکثر برابر L خواهد بود. اما اگر $L > (n-k)$ باشد، $\text{rank}\,(\boldsymbol{E})$ حداکثر برابر $(n-k)$ و کمتر از L خواهد شد [۲۴].

از طرف دیگر، معلوم است که $\text{rank}\,(\boldsymbol{E}) = \text{rank}(\boldsymbol{E}^{T})$ است. همچنین، ثابت می‌شود که رتبه حاصل‌ضرب دو ماتریس با رتبه یکسان، برابر رتبه یکی از آنها است [۲۴]. لذا، می‌توان نتیجه گرفت که $\text{rank}\,(\boldsymbol{A})$، حداکثر برابر $\min(L\,.\,(n-k))$ خواهد شد. در این صورت، چنانچه رابطه $L > (n-k)$ برقرار باشد، $\text{rank}\,(\boldsymbol{A})$ حداکثر برابر $(n-k)$ و کمتر از L خواهد شد. اما باید توجه شود که ماتریس $\boldsymbol{A}$ یک ماتریس مربعی با ابعاد $L \times L$ است، بنابراین، در این شرایط معکوس‌پذیر نخواهد بود.

این نتیجه نشان می‌دهد، در شرایطی که درجه چندجمله‌ای درهم‌ساز (L) از تعداد بیت افزونگی کلمات کد قبل از خود (n-k) بزرگ‌تر باشد، ماتریس $\boldsymbol{A}$ در رابطه (۹) معکوس‌پذیر نبوده و نمی‌توان با استفاده از این روش به شناسایی حالت اولیه درهم‌ساز پرداخت.

[1] Rank

۲-۲- شناسایی با استفاده از جستجوی کامل

در مرجع [۲۲]، برای شناسایی حالت اولیه درهم‌ساز بعد از کدگذار کانولوشنی از روش جستجوی کامل استفاده می‌شود. با توجه به اینکه مقادیر ثبات‌های درهم‌ساز توسط عناصر میدان GF(2) یعنی 0 یا 1 انتخاب می‌شوند، برای L بیت حالت اولیه درهم‌ساز 2^L حالت ممکن وجود دارد. لذا، در روش شناسایی با استفاده از جستجوی کامل، لازم است تا تمام 2^L حالت ممکن بررسی شده تا شناسایی حالت اولیه صحیح، صورت گیرد.

در روش شناسایی با استفاده از جستجوی کامل، لازم است که به ازای تمام 2^L حالت ممکن، دنباله درهم‌ساز کننده را به‌دست آورده و با استفاده از آن عملیات معکوس درهم‌سازی بر روی دنباله مورد نظر انجام شود. حالتی جواب صحیح است که دنباله معکوس درهم‌ساز شده به‌ازای آن، برابر کلمات کد مورد نظر باشد. برای بررسی این‌که دنباله معکوس درهم‌ساز شده، کلمات کد مورد نظر هست یا نه، از محاسبه رتبه ماتریس کلمات کد استفاده می‌شود. چنانچه رفتار رتبه ماتریس دنباله معکوس درهم‌ساز شده به ازای یکی از حالت‌های ممکن با سایر حالت‌ها متفاوت شود، نشان‌دهنده آن است که مقدار این حالت مشخص، مقدار حالت اولیه درهم‌ساز مورد نظر است [۲۲].

۲-۲-۱- ضعف روش شناسایی با استفاده از جستجوی کامل

با توجه به آشنایی با روش شناسایی حالت اولیه بر اساس جستجوی کامل، می‌توان دریافت که استفاده از این روش در شرایطی که درجه چندجمله‌ای درهم‌ساز (L) عدد بزرگی باشد، بسیار زمان‌بَر خواهد بود. زیرا با استفاده از این روش، فضای کامل برای جستجوی حالت اولیه درهم‌ساز، 2^L حالت است و برای درهم‌سازهای با درجه‌های بزرگ (مثل درجه ۳۲ و بزرگ‌تر از آن) فضای جستجو، فضای بسیار بزرگی خواهد شد. هر چه فضای جستجو بزرگ‌تر باشد، زمان بیشتری نیز برای جستجو و بررسی در آن فضا نیاز دارد.

۳- روش پیشنهادی برای شناسایی حالت اولیه درهم‌ساز بعد از کدگذار کانال

همان‌طور که در بخش قبل توضیح داده شد، روش شناسایی حالت اولیه با استفاده از ماتریس معکوس، در شرایطی که درجه چندجمله‌ای درهم‌ساز (L) از تعداد بیت افزونگی کلمات کد قبل از خود (n-k) بزرگ‌تر باشد، قادر به پاسخگویی نیست. همچنین، روش شناسایی حالت اولیه با استفاده از جستجوی کامل در شرایطی که درجه چندجمله‌ای درهم‌ساز (L) عدد بزرگی باشد،

به زمان بسیار زیادی برای پاسخگویی نیاز دارد. علاوه بر این باید توجه داشت که این روش فقط برای شرایطی ارائه شده است که از کدگذار کانولوشنی استفاده شده باشد.

با توجه به مواردی که ذکر شد، روش پیشنهادی برای شناسایی حالت اولیه درهم‌ساز هم‌زمان بعد از کدگذار کانال ارائه می‌شود. در روش پیشنهادی، با استفاده از ترکیب روش‌های موجود، سعی در کاهش و یا برطرف کردن ضعف‌های هر یک از این دو روش مذکور است.

یکی از ویژگی‌های روش پیشنهادی این است که در شرایطی که روش شناسایی با استفاده از ماتریس معکوس جوابگو نیست، با استفاده از روش پیشنهادی می‌توان عملیات شناسایی حالت اولیه را انجام داد. همچنین روش پیشنهادی فضای جستجوی مورد نیاز برای شناسایی را به میزان قابل توجهی کاهش می‌دهد.

در روش پیشنهادی، فرض می‌شود که سمت چپ رابطه (۸) ، یعنی $\boldsymbol{y}_{1\times n}.\boldsymbol{H}^{T}_{n\times(n-k)}\cdot\boldsymbol{E}^{T}_{(n-k)\times L}$ یک بردار سطری L بیتی معلوم است و با بردار $\boldsymbol{v}_{1\times L}$ نشان داده می‌شود. بردار L بیتی $\boldsymbol{z}_{1\times L}$ نیز در برگیرنده مجهولات مورد نظر است و ماتریس $\boldsymbol{A}_{L\times L}$ نیز ماتریس معادلات می‌باشد. در این صورت دستگاه معادلات به‌صورت زیر خواهد شد:

$$\boldsymbol{v}_{1\times L}=\boldsymbol{z}_{1\times L}.\boldsymbol{A}_{L\times L} \qquad (۱۱)$$

اکنون باید دستگاه معادلات L مجهولی موجود در رابطه (۱۱) حل شود. اما، برای این دستگاه معادلات، L معادله مستقل خطی وجود ندارد، به همین دلیل است که ماتریس $\boldsymbol{A}_{L\times L}$ معکوس‌پذیر نیست.

اکنون، فرض می‌شود که تعداد معادلات مستقل خطی در ماتریس $\boldsymbol{A}_{L\times L}$ برابر r و کمتر از L است. در این صورت، بر اساس قوانین جبر خطی، این دستگاه معادلات دارای بی‌نهایت جواب خواهد بود. ولیکن، ازآنجاکه فقط جواب‌های عضو میدان GF(2) یعنی 0 و 1 در این دستگاه معادلات مورد نظر است، می‌توان جواب‌های این دستگاه معادلات را محدود کرد.

راه‌حل پیشنهادی برای این شرایط، مقداردهی L-r مجهول از کل L مجهول موجود و محاسبه باقیمانده مجهولات با استفاده از دستگاه معادلات مورد نظر است. در این روش، ابتدا سطرها و ستون‌های مستقل خطی ماتریس $\boldsymbol{A}_{L\times L}$ را با استفاده از الگوریتم گوس-جردن[1] پیدا کرده و سپس با استفاده از این سطرها و ستون‌ها، ماتریس جدید $\boldsymbol{B}_{r\times r}$ تشکیل می‌شود. همچنین، در موقعیت‌های حذف‌شده از سطرهای ماتریس $\boldsymbol{A}_{L\times L}$ که به تعداد L-r بیت است، در بردار مجهول $\boldsymbol{z}_{1\times L}$ مقداردهی کرده و تأثیر آن مقادیر، بر روی بردار $\boldsymbol{v}_{1\times L}$ اعمال می‌شود. برای مقداردهی L-r بیت از بردار مجهول $\mathbf{z}$ باید تمام 2^{L-r} بیت ممکن از اعداد 0 و 1 را در نظر گرفت. سپس با استفاده از معکوس ماتریس جدید $\boldsymbol{B}_{r\times r}$ ، باقیمانده مجهولات موجود محاسبه می‌شود. در این صورت، 2^{L-r} جواب برای این دستگاه معادلات به‌دست می‌آید.

برای بررسی 2^{L-r} جواب ممکن، کافی است که پس از محاسبه حالت اولیه با مقداردهی مورد نظر، عملیات معکوس درهم‌ساز بر روی دنباله کلمات کد درهم‌ساز شده انجام شود. در این صورت، حالت اولیه‌ای که دنباله معکوس درهم‌ساز شده آن برابر کلمات کد مورد نظر باشد، حالت اولیه صحیح و مطلوب است. برای بررسی اینکه دنباله معکوس درهم‌ساز شده، کلمات کد مورد نظر هست یا نه، کافی است که حاصل‌ضرب آن در ماتریس کلمات کد دوگان، برابر بردار صفر شود.

۴- نتایج شبیه‌سازی

برای انجام شبیه‌سازی، از کدهای بلوکی BCH با (n,k)های مختلف و درجه‌های مختلفی از چندجمله‌ای بازخورد درهم‌ساز هم‌زمان استفاده شده است. در این بخش، مقایسه‌ای بین پاسخ‌دهی روش پیشنهادی با روش شناسایی با استفاده از ماتریس معکوس، انجام شده که نتایج آن در جدول (۱) آورده شده است. با توجه به این جدول ملاحظه می‌شود که در شرایطی که درجه چندجمله‌ای بازخورد از تعداد بیت افزونگی (n-k) کلمات کد کوچک‌تر و یا مساوی با آن باشد، روش متداول موجود و روش پیشنهادی هر دو قادر به پاسخ‌دهی می‌باشند. اما در شرایطی که درجه چندجمله‌ای بازخورد از تعداد بیت افزونگی کلمات کد بزرگ‌تر باشد، دیگر نمی‌توان از روش متداول شناسایی با استفاده از ماتریس معکوس استفاده نمود ولیکن روش پیشنهادی در این شرایط نیز قادر به پاسخ‌دهی می‌باشد.

جدول (۱): مقایسه پاسخ‌دهی روش پیشنهادی با روش شناسایی با استفاده از ماتریس معکوس

BCH (n,k)	چندجمله‌ای فیدبک / حالت اولیه	پاسخ‌دهی روش ماتریس معکوس	پاسخ‌دهی روش پیشنهادی
BCH (31,21)	$x^9+x^6+x^4+x^3+1$ / [1 0 0 0 1 0 1 0 1]	✓	✓
BCH (31,26)	$x^{10}+x^6+x^5+x^3+x^2+x+1$ / [0 1 1 0 1 1 1 0 1 0]	×	✓
BCH (63,57)	$x^{11}+x^9+x^6+x^3+1$ / [0 0 1 0 1 0 1 0 1 1 1]	×	✓
BCH (31,21)	$x^{12}+x^{11}+x^{10}+x^8+x^7+x^2+1$ / [1 1 0 0 0 1 0 0 1 0 0 1]	×	✓
BCH (63,51)	$x^{15}+x^5+x^4+x^2+1$ / [1 1 1 1 0 0 1 0 0 0 1 0 0 1 0]	×	✓

[1] Gauss Jordan

در جدول (۲) نیز مقایسه‌ای بین بزرگی فضای جستجو در روش پیشنهادی با روش متداول شناسایی با استفاده از جستجوی کامل صورت گرفته است. همان‌طور که می‌دانیم، رابطه مستقیمی بین بزرگی فضای جستجو و زمان جستجو وجود دارد. لذا هر چه فضای جستجو بزرگ‌تر باشد، زمان مورد نیاز برای جستجو کردن در آن فضا نیز بیشتر خواهد شد.

با توجه به این جدول ملاحظه می‌شود که فضای جستجو در روش جستجوی کامل 2^L حالت است، در حالی که در روش پیشنهادی $2^{L-(n-k)}$ حالت می‌باشد.

جدول (۲): مقایسه فضای جستجو در روش پیشنهادی با روش شناسایی با استفاده از جستجوی کامل

BCH (n , k)	چندجمله‌ای فیدبک حالت اولیه	فضای جستجو در جستجوی کامل	فضای جستجو در روش پیشنهادی
BCH (63,45)	$x^{20}+x^{19}+x^4+x^3+1$ [0 1 1 0 1 0 0 0 1 0 0 1 0 0 0 1 0 1 0 1]	2^{20}	2^2
BCH (31,21)	$x^{18}+x^9+x^7+x^6+x^5+x^4+1$ [0 1 1 0 1 1 1 0 1 0 0 0 0 0 0 1 0 1 1]	2^{18}	2^8
BCH (63,51)	$x^{21}+x^{14}+x^7+x^2+1$ [1 0 0 0 1 1 0 1 1 1 1 0 0 1 0 1 0 1 0 1 0 1 1 1]	2^{21}	2^9
BCH (127,99)	$x^{31}+x^{16}+x^8+x^4+x^3+x^2+1$ [1 1 0 0 0 1 0 0 1 1 1 0 1 0 1 1 1 1 1 0 0 1 1 0 1 1 0 1 0 1 0 1 0 0 0 1]	2^{31}	2^3
BCH (127,106)	$x^{32}+x^{22}+x^2+x+1$ [1 1 1 1 0 1 0 0 0 1 0 0 1 1 1 0 1 0 1 0 1 1 1 0 0 1 0 0 0 1 0 0 1 0]	2^{32}	2^{11}

نکته دیگری که در روش‌های شناسایی اهمیت دارد موضوع پیچیدگی محاسباتی است. در روش جستجوی کامل، برای بررسی صحیح بودن حالت اولیه مورد جستجو، رتبه دنباله معکوس درهم‌ساز شده را در هر بار جستجو محاسبه می‌نماید. در حالی که در روش پیشنهادی، حداکثر به میزان L بار عملیات گوس-جردن بر روی ماتریس $\boldsymbol{A}$ انجام می‌شود و 2^{L-r} بار عملیات ضرب ماتریسی صورت می‌گیرد. ازآنجایی‌که محاسبه رتبه یک ماتریس با استفاده از عملیات گوس-جردن انجام می‌شود، ملاحظه می‌شود که تعداد عملیات گوس-جردن در روش پیشنهادی چقدر کمتر از روش جستجوی کامل است. بر این اساس، پیچیدگی محاسباتی این دو روش به‌صورت جدول (۳) خواهد بود.

جدول (۳): مقایسه پیچیدگی محاسباتی در روش پیشنهادی با روش شناسایی با استفاده از جستجوی کامل

BCH (n , k)	چندجمله‌ای فیدبک حالت اولیه	تعداد عملیات در جستجوی کامل	تعداد عملیات در روش پیشنهادی
BCH (63,45)	$x^{20}+x^{19}+x^4+x^3+1$ [0 1 1 0 1 0 0 0 1 0 0 1 0 0 0 1 0 1 0 1]	2^{20}	2^2+20
BCH (31,21)	$x^{18}+x^9+x^7+x^6+x^5+x^4+1$ [0 1 1 0 1 1 1 0 1 0 0 0 0 0 0 1 0 1 1]	2^{18}	2^8+18
BCH (63,51)	$x^{21}+x^{14}+x^7+x^2+1$ [1 0 0 0 1 1 0 1 1 1 1 0 0 1 0 1 0 1 0 1 0 1 1 1]	2^{21}	2^9+21
BCH (127,99)	$x^{31}+x^{16}+x^8+x^4+x^3+x^2+1$ [1 1 0 0 0 1 0 0 1 1 1 0 1 0 1 1 1 1 1 0 0 1 1 0 1 1 0 1 0 1 0 1 0 0 0 1]	2^{31}	2^3+31
BCH (127,106)	$x^{32}+x^{22}+x^2+x+1$ [1 1 1 1 0 1 0 0 0 1 0 0 1 1 1 0 1 0 1 0 1 1 1 0 0 1 0 0 0 1 0 0 1 0]	2^{32}	$2^{11}+32$

۵- نتیجه‌گیری

در این مقاله، به شناسایی حالت اولیه درهم‌ساز بعد از کدگذار کانال با در اختیار داشتن دنباله خروجی درهم‌ساز پرداخته شده است. با بررسی‌ها و شبیه‌سازی‌های صورت گرفته ثابت شد که روش شناسایی با استفاده از ماتریس معکوس در شرایطی که درجه چندجمله‌ای بازخورد درهم‌ساز از تعداد بیت افزونگی کلمات کد بکار رفته بزرگ‌تر باشد، قادر به شناسایی حالت اولیه درهم‌ساز نیست. درصورتی‌که کد کانال قبل از درهم‌ساز یک کد بلوکی باشد، از این روش استفاده می‌شود. حال، در صورت برقراری شرایط مذکور، عملیات شناسایی ناموفق خواهد شد. در این شرایط می‌توان از روش جستجوی کامل استفاده نمود، هر چند که این روش فقط برای زمانی ارائه شده است که کدگذار قبل از درهم‌ساز از نوع کانولوشنی باشد.

از طرف دیگر، روش شناسایی با استفاده از جستجوی کامل در شرایطی که درجه چندجمله‌ای بازخورد درهم‌ساز عدد بزرگی باشد، نیاز به فضای جستجوی بسیار بزرگی دارد و در نتیجه زمان زیادی برای شناسایی با این روش صرف می‌شود.

اما با استفاده از روش پیشنهادی ارائه‌شده در این مقاله، هم می‌توان در شرایطی که درجه چندجمله‌ای درهم‌ساز از تعداد بیت افزونگی کلمات کد بکار رفته بزرگ‌تر است، شناسایی را انجام داد و هم اینکه فضای جستجوی مورد نیاز برای شناسایی حالت اولیه درهم‌ساز به مراتب کمتر و در نتیجه زمان مورد نیاز برای شناسایی به مراتب کمتر از روش شناسایی با استفاده از جستجوی کامل خواهد بود.

در واقع نوآوری این مقاله عبارت است از شناسایی حالت اولیه درهم‌سازهای بعد از کدگذار بلوکی در شرایطی که درجه چندجمله‌ای بازخورد درهم‌ساز از تعداد بیت افزونگی کلمات کد قبل از آن بزرگ‌تر باشد. این روش پیشنهادی در مقایسه با روش‌های جستجوی کامل از نظر زمان و پیچیدگی محاسباتی نیز بهتر عمل می‌نماید.

در پایان لازم به ذکر است که هم در روش پیشنهادی و هم در روش‌های شناسایی با استفاده از ماتریس معکوس و روش شناسایی با جستجوی کامل، فرض بر این است که دنباله مورد استفاده کاملاً سالم است. لذا، برای کارهای آتی پیشنهاد می‌شود که موضوع حضور نویز در شرایط نویزی هم مد نظر قرار گیرد.

۶- مراجع

[1] P. B. Crilly, "Communication systems: An introduction to signals and noise in electrical communication," McGraw-Hill, 2010.

[2] R. L. Peterson, R. E. Ziemer, and D. E. Borth, "Introduction to spread-spectrum communications," Prentice hall New Jersey, vol. 995, 1995.

[3] K. A. S. Immink, "Codes for mass data storage systems: Shannon Foundation Publisher," 2004.

[4] I. W. Group, "IEEE standard for local and metropolitan area networks-Part 16: Air interface for fixed broad-band wireless access systems," In IEEE Std. 802.16-2004, ed, 2004.

[5] T. ETSI, "Transmission and Multiplexing (TM)," 101 135 (V1. 5.3), In High bit-rate Digital Subscriber Line (HDSL) transmission systems on metallic local lines, ed.

[6] M. Teimouri and S. M. Ahmadiyan, "Blind Estimation of the Number of User in TDMA Networks Using the Redundancy of Adaptive Channel Coding (in Persian)," Journal of Electronical & Cyber Defence, vol. 6, pp. 11-20, 2018.

[7] M. Cluzeau, "Reconstruction of a linear scrambler," IEEE Transactions on Computers, vol. 56, 2007.

[8] A. D. Yardi, "Blind Reconstruction of Binary Cyclic Codes over Binary Erasure Channel," 2019.

[9] P. Liu, Z. Pan, and J. Lei, "Parameter Identification of Reed-Solomon Codes Based on Probability Statistics and Galois Field Fourier Transform," IEEE Access, 2019.

[10] H. Yan, Y. Huang, B. Li, and J. Lei, "Research on Block-Based Blind Identification of High-rate Punctured Convolutional Codes," In MATEC Web of Conferences, p. 01037, 2018.

[11] J. B. Tamakuwala, "Blind Identification of Block Interleaved Convolution Code Parameters," Defence Science Journal, vol. 69, pp. 274-279, 2019.

[12] R. Swaminathan, A. Madhukumar, G. Wang, and T. S. Kee, "Blind Reconstruction of Reed-Solomon Encoder and Interleavers Over Noisy Environment," IEEE Transactions on Broadcasting, 2018.

[13] C. Choi and D. Yoon, "Novel Blind Interleaver Parameter Estimation in a Non-Cooperative Context," IEEE Transactions on Aerospace and Electronic Systems, 2018.

[14] G. Kim, M. Jang, and D. Yoon, "Improved Method for Interleaving Parameter Estimation in a Non-Cooperative Context," IEEE Access, vol. 7, pp. 92171-92175, 2019.

[15] Y. Xu, Y. Zhong, and Z. Huang, "An improved blind recognition method of the convolutional interleaver parameters in a noisy channel," IEEE Access, 2019.

[16] X.-B. Liu, S. N. Koh, X.-W. Wu, and C.-C. Chui, "Investigation on scrambler reconstruction with minimum a priori knowledge," In Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE, pp. 1-5, 2011.

[17] X.-B. Liu, S. N. Koh, X.-W. Wu, and C.-C. Chui, "Reconstructing a linear scrambler with improved detection capability and in the presence of noise," IEEE Transactions on information forensics and security, vol. 7, pp. 208-218, 2012.

[18] H. Xie, F. Wang, and Z. Huang, "Blind reconstruction of linear scrambler," Journal of Systems Engineering and Electronics, vol. 25, pp. 560-565, 2014.

[19] H. Wenjia, "Reconstructing the feedback polynomial of a linear scrambler with the method of hypothesis testing," IET Communications, vol. 9, pp. 1044-1047, 2015.

[20] X.-B. Liu, S. N. Koh, C.-C. Chui, and X.-W. Wu, "A study on reconstruction of linear scrambler using dual words of channel encoder," IEEE Transactions on information forensics and security, vol. 8, pp. 542-552, 2013.

[21] Y. Ma, L.-M .Zhang, and H.-T. Wang, "Reconstructing synchronous scrambler with robust detection capability in the presence of noise," IEEE Transactions on Information Forensics and Security, vol. 10, pp. 397-408, 2015.

[22] S. Han and M. Zhang, "A Method for Blind Identification of a Scrambler Based on Matrix Analysis," IEEE Communications Letters, 2018.

[23] R. Gautier, G. Burel, J. Letessier, and O. Berder, "Blind estimation of scrambler offset using encoder redundancy," In Signals, Systems and Computers, 2002. Conference Record of the Thirty-Sixth Asilomar Conference on, pp. 626-630, 2002.

[24] J. B. Carrell, "Fundamentals of linear algebra," Springer, 2005.

A New Method for Blind Recognition of the Initial State of Synchronous Scramblers When Located after the Channel Encoder

S. Ghazi Maghrebi *, H. Alemi

*Dean of Islamic Azad University /Yadegar-e-Imam Khomeini (RAH) shahre Rey

(Received: 05/03/2020, Accepted: 05/08/2020)

ABSTRACT

The scrambler block is one of the most commonly used blocks in digital communication protocol design. This block is used to randomize the bit string and usually is used after the source encoder or after the channel encoder. In blind detection this block, is assumed to be located after the source encoder or after the channel encoder. LFSRs are often used to design linear scramblers. Therefore, scramblers are defined by usage of feedback polynomials and initial states. In previous works, the initial state of the scrambler after channel encoder has been identified, but under some circumstances, these algorithms cannot provide proper response. In these conditions, to identify initial state of the scrambler, a full search method may be used which takes a long time. In this paper, a new algorithm for initial state of scrambler detection, after channel encoder, is presented. The proposed algorithm is able to identify the initial state of scrambler in the cases that other algorithms cannot do anything. The new algorithm also reduces the search space and as a result, it need much less time for the identification process.

Keywords: Blind Recognition, Synchronous Scrambler, Initial State, Channel Encoder

*Corresponding Author Email: s_ghazi2002@yahoo.com