مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال هفتم، شماره ۳، پاییز ۱۳۹۵؛ ص ۲۵۹-۲۵۱

دو روش جدید برای طراحی رمزهای قالبی ۱۹۲ بیتی بر اساس ساختار سوئیچینگ و لایه‌های انتشار بازگشتی

عبدالرسول میرقدری[۱*]، محمود یوسفی‌پور[۲]، بهروز خادم[۳]، سید مهدی سجادیه[۴]

۱- دانشیار، ۲- دانشجوی دکتری، ۳- استادیار، دانشگاه امام حسین (ع)، ۴- استادیار، دانشگاه آزاد اسلامی اصفهان (واحد خوراسگان)

(دریافت: ۹۵/۰۱/۳۰، پذیرش: ۹۵/۰۶/۲۲)

چکیده

در سال‌های اخیر به رمزهای قالبی در مقایسه با رمزهای دنباله‌ای به‌دلیل وجود اثبات امنیتی و دامنه کاربرد گسترده بیشتر توجه شده است. طراحی اغلب رمزهای قالبی بر اساس ساختار جانشانی- جایگشتی(SPN) یا فیستلی است. گرچه ساختارهای فیستلی در مقایسه با ساختار SPN مزایای بیشتری دارند اما به دلیل داشتن تعداد جعبه‌های جانشانی فعال کمتر، لذا دارای ضعف امنیتی هستند. در این مقاله دو روش جدید برای طراحی الگوریتم‌های رمز قالبی ۱۹۲ بیتی ارائه می‌شود که در آن‌ها از ساختار سوئیچینگ و لایه‌های انتشار بازگشتی به‌منظور افزایش تعداد جعبه‌های جانشانی فعال و کارایی بیشتر استفاده شده است. روش اول مبتنی بر ساختار سوئیچینگ و لایه‌های انتشار بازگشتی چندگانه ۳×۳ و روش دوم مبتنی بر ساختار سوئیچینگ و لایه‌های انتشار بازگشتی چندگانه ۲×۲ است. امنیت ساختارهای ارائه‌شده با استفاده از روش برنامه‌ریزی خطی مورد تحلیل و ارزیابی قرار گرفته است که نتایج حاصل نشان از مقاومت آن‌ها در برابر تحلیل‌های خطی و تفاضلی دارد. همچنین، با توجه به این که لایه‌های انتشار بازگشتی در مقایسه با ماتریس‌های MDS از سرعت و کارایی مناسبی در نرم‌افزار و سخت‌افزار برخوردارند لذا می‌توان گفت که الگوریتم‌های طراحی‌شده با استفاده از این روش‌ها کارایی بیشتری دارند.

کلید واژه‌ها: ساختار سوئیچینگ، لایه‌های انتشار بازگشتی، برنامه‌ریزی خطی، تحلیل تفاضلی، تحلیل خطی

Two New Methods for Designing 192-bit Block Ciphers Based on Switching Structure and Recursive Diffusion Layers

A. Mirghadri[*], M. Yosefipour, B. Khadem, M. Sajadieh

Imam Hossein University

(Received: 18/04/2016; Accepted: 12/09/2016)

Abstract

In recent years, compared with stream ciphers more attention has been to block ciphers because of their proved security and wide application. Design of most block ciphers are based on substitution-permutation network (SPN) or Fiestel structure. Although Fiestel structures compared with SPN has many benefits, but since they have less active S-boxes in round function, it has a security weakness. In this paper, we introduce two new methods for designing 192-bit block cipher algorithms that use Switching Structure and Recursive Diffusion Layers to increase active S-boxes. The first method is based on switching structure and 3×3 multiple Recursive Diffusion Layers and the second method used switching structure and 2×2 multiple Recursive Diffusion Layers. Security of tow structures using linear programming offered analysed with linear programming and evaluated the results show of resistance to linear and differential cryptoanalysis. Also, since the Recursive Diffusion Layers are more efficient than MDS matrices in software and hardware, thus designed algorithms with these methods have high performance in various platforms.

Keywords: Switching Structure, Recursive Diffusion Layers, Linear Programming, Differential Cryptoanalysis, Linear Cryptoanalysis.

[*]Corresponding Author E-mail: amrghdri@ihu.ac.ir

۱. مقدمه

در عصر حاضر که به عصر اطلاعات مشهور است، امنیت اطلاعات و ارتباطات مقوله‌ی راهبردی پدافند نوین برای مقابله با نفوذ و دسترسی بیگانگان به حریم خصوصی و اطلاعات محرمانه افراد و سازمان‌ها است. یک ویژگی مهم در رابطه با امنیت اطلاعات و ارتباطات، محرمانگی اطلاعات است که می‌بایست به روشی مطمئن و موثر برآورده شود. موثرترین روش حفظ محرمانگی اطلاعات و حریم خصوصی، استفاده از الگوریتم‌های رمزنگاری است. این الگوریتم‌ها با عاملی به نام کلید، اطلاعات آشکار را به اطلاعات رمزی تبدیل می‌کنند. الگوریتم‌های رمز بسته به این‌که کلید بین فرستنده و گیرنده یکسان بوده یا اینکه کلید رمزگشایی به راحتی از کلید رمزگذاری به دست آمدنی است و یا برعکس (یعنی کلیدها یکسان نبوده یا این که کلید رمزگشایی را نتوان از کلید رمزگذاری به دست آورد)، را به ترتیب به دو دسته الگوریتم‌های متقارن و الگوریتم‌های نامتقارن تقسیم‌بندی می‌کنند. الگوریتم‌های متقارن به دلیل سرعت و کارایی بالای خود در مقایسه با الگوریتم‌های نامتقارن از اهمیت خاصی برخوردار هستند و در اکثر ارتباطات برای تأمین محرمانگی اطلاعات از این الگوریتم‌ها استفاده می‌کنند.

الگوریتم‌های رمز متقارن را می‌توان در دو دسته الگوریتم‌های رمز قالبی و الگوریتم‌های رمز دنباله‌ای در نظر گرفت. در سال‌های اخیر جامعه رمزنگاری، در مقایسه با رمزهای دنباله‌ای، توجه خاصی را به رمزهای قالبی معطوف داشته است. یکی از دلایل این امر روش‌های اثبات امنیتی برای رمزهای قالبی است که در مقایسه با رمزهای دنباله‌ای روش راحت‌تری است. علاوه بر این گستردگی دامنه کاربرد رمزهای قالبی است. به طوری که با داشتن یک الگوریتم رمز قالبی، می‌توان یک الگوریتم رمز دنباله‌ای، یک تابع چکیده‌ساز، یک کد احراز اصالت پیام و یک مولد شبه تصادفی به دست آورد. این توجه باعث شده است تا در بسیاری از کاربردها، رمزهای دنباله‌ای جای خود را به رمزهای قالبی دهند. به عنوان یک مثال در این مورد می‌توان به جایگزینی رمزهای دنباله‌ای A5/1 [۱] و A5/2 [۲] با الگوریتم رمز قالبی Kasumi [۳] در نسل جدید تلفن همراه اشاره کرد.

یک الگوریتم رمز قالبی، یک جایگشت مبتنی بر کلید است که متن آشکار را با استفاده از یک کلید محرمانه به متن رمزی تبدیل می‌کند. متن رمزی نیز با استفاده از همان کلید (یا کلیدی که به راحتی از کلید رمزگذاری محاسبه می‌شود) و الگوریتم رمزگشایی، کشف شده و متن آشکار به دست می‌آید [۴]. رمزهای قالبی دو خانواده اصلی دارند که عبارتند از ساختارهای SPN[1] و فایستل[2]. از نمونه‌های استانداردشده الگوریتم رمز قالبی می‌توان به ساختار فیستلی الگوریتم DES و به ساختار SPN الگوریتم رمز AES اشاره کرد. همچنین می‌توان به رمزهای قالبی LBlock [۵]، PRINCE [۶]، PRIDE [۷]، MIDORI [۸] و LS-Design [۹] اشاره کرد که در چند سال اخیر ارائه شده‌اند. برای طراحی یک رمز قالبی، ابتدا یک تابع، به نام تابع دور طراحی شده و سپس این تابع دور به صورت تکراری روی یک متن آشکار اعمال می‌شود. تابع دور رمز قالبی باید طوری طراحی شود که بتواند آشفته‌سازی[3] تولید کرده و آن را پراکنش[4] دهد. این مفاهیم برای اولین بار توسط شانون [۱۰] ارائه شد. بر همین اساس در طراحی رمزهای قالبی دو عنصر تبدیل غیرخطی (که عموماً از جعبه‌های جانشانی تشکیل شده است) و لایه خطی (مانند ماتریس‌های MDS[5]) به کار می‌روند. دو مسئله مهم که در رابطه با هر الگوریتم رمزنگاری، از جمله الگوریتم‌های رمز قالبی می‌بایست مورد مطالعه و بررسی قرار گیرند، امنیت و کارایی این الگوریتم‌ها است. در تعریف کارایی الگوریتم‌های رمز قالبی می‌توان سرعت محاسباتی و الزامات منابع و حافظه برای پیاده‌سازی این الگوریتم‌ها را در نظر گرفت. امنیت این رمزها نیز به صورت مقاومت آن‌ها در برابر حملات شناخته‌شده تعریف می‌شود.

تحلیل تفاضلی [۱۱] و تحلیل خطی [۱۲] دو روش حمله مهم روی رمزهای قالبی است که بعد از گذشت ده‌ها سال از معرفی آن‌ها هنوز هم مطالعه و بررسی می‌شوند، به طوری که اکثر روش‌های تحلیل روی رمزهای قالبی که در چند سال اخیر معرفی شده‌اند، بهبودی از این روش‌ها بوده یا اینکه در بخشی از فرآیند خود، یکی از این روش‌ها را استفاده می‌کنند. هر طراح رمز قالبی در وهله اول تلاش می‌کند تا رمز جدید خود را در برابر این دو تحلیل مهم مقاوم کند. برای مقاومت یک الگوریتم رمز در برابر این تحلیل‌ها، مؤلفه‌های غیرخطی به‌کاررفته در الگوریتم رمز نقش مهمی دارند. در اکثر رمزهای قالبی از جعبه‌های جانشانی به عنوان مؤلفه‌های غیرخطی استفاده می‌شود. اگر یک رمز قالبی از یک جعبه جانشانی با ویژگی‌های تفاضلی و خطی خوب استفاده کرده و لایه انتشار آن باعث افزایش تعداد جعبه‌های جانشانی فعال در دورهای متوالی گردد، می‌توان از امنیت آن در برابر تحلیل‌های تفاضلی و خطی مطمئن بود. با توجه به این امر اهمیت لایه‌های انتشار خوب و نیز ساختارهای طراحی رمزهای قالبی که باعث افزایش تعداد حداقل جعبه‌های جانشانی فعال می‌شوند بیشتر از قبل آشکار می‌شود [۱۳].

[1] Substitution and Permutation Networks (SPN)
[2] Fiestel Ciphers
[3] Confusion
[4] Diffusion
[5] Maximum Distance Spreadable

اگرچه ساختارهای فایستل در مقایسه با ساختارهای SPN مزیت‌هایی دارند که از آن‌ها می‌توان به سرعت بالای آن‌ها و عدم نیاز به معکوس تابع دور در فرآیند رمزگشایی استفاده کرد، ولی این ساختارها تعداد جعبه‌های جانشانی فعال کمتری دارند. علت این امر به خاطر عمل حذف تفاضلات است که در طول xor شدن نیمه راست و چپ حالت در ساختارهای فیستلی رخ می‌دهد [۱۳]. برای افزایش تعداد جعبه‌های جانشانی فعال در ساختارهای فایستل، کارهایی صورت گرفته است که از مهم‌ترین آن‌ها می‌توان به ساختار سوئیچینگ اشاره کرد که توسط شیرایی و شیبوتانی ارائه شد [۱۴].

در این مقاله از ساختار سوئیچینگ استفاده شده و دو ساختار جدید برای طراحی الگوریتم‌های رمز قالبی ۱۹۲ بیتی معرفی می‌شود. برای افزایش کارایی این ساختارها و نیز به دست آوردن لایه‌های انتشار چندگانه مناسب ساختار سوئیچینگ، به جای ماتریس‌های MDS چندگانه از لایه‌های انتشار بازگشتی چندگانه استفاده می‌شود. این لایه‌های انتشار را با استفاده از الگوریتم جستجوی ارائه‌شده در این مقاله می‌توان به دست آورد.

۲. لایه‌های انتشار بازگشتی

یک معیار مهم در طراحی لایه انتشار رمزهای قالبی این است که لایه انتشار طوری باشد که بتواند تغییرات ایجادشده در یک دور را در دورهای بعدی به تغییرات بیشتری منتشر نماید. به عبارت دیگر باعث درگیر شدن جعبه‌های جانشانی بیشتری شود.

ماتریس MDS: ماتریسMDS ، ماتریسی مربعی است که درتمینان تمام زیر ماتریس‌های آن مخالف صفر است. ماتریس‌های MDS به عنوان لایه انتشار یک رمز قالبی، یک وجود حداکثری از جعبه‌های جانشانی فعال را ضمانت می‌کنند. به عبارت دیگر، ماتریس‌های MDS، انتشار کامل ایجاد می‌کنند. بنابراین لایه انتشاری مطلوب است که تا حد امکان منجر به جعبه‌های جانشانی فعال بیشتری شود. یک معیار مهم برای ارزیابی یک لایه انتشار، مفهومی تحت عنوان عدد انشعاب برای این لایه انتشار است که در ادامه تعریف می‌شود. برای این منظور لازم است تا ابتدا مفهوم وزن همینگ تعریف شود.

وزن همینگ: برای یک بردار w به طول n با درایه‌های صحیح، $Hm(w)$ وزن همینگ آن تعریف می‌شود که برابر است با تعداد درایه‌های غیرصفر بردار w. برای دو بردار u و w، فاصلهٔ همینگ برابر با وزن همینگ تفاضل xor آن دو بردار تعریف می‌شود، یعنی $d_H(u,w) = Hm(u \oplus w)$.

عدد انشعاب: لایهٔ انتشار D در یک سیستم رمز را در نظر بگیرید که s کلمه $w = (w_1, w_2, \dots, w_s)$ را به عنوان ورودی گرفته و بردار $D(w)$ شامل s کلمه را به عنوان خروجی تولید می‌کند. در این صورت عدد انشعاب لایهٔ D برابر با حداقل مقدار برای مجموع وزن همینگ بردارهای ورودی و خروجی تعریف می‌شود:

$$B_D = \min_{w \neq 0} \{Hm(w) + Hm(D(w))\}.$$

به‌طوری که این حداقل مقدار، روی مجموعهٔ تمام مقادیر غیرصفر ورودی محاسبه شده است.

عدد انشعاب یک تبدیل خطی، معیاری برای سنجش قدرت انتشار آن است. برای یک لایه انتشار با ورودی و خروجی $\boldsymbol{s}$ کلمه، حداکثر عدد انشعاب برابر $\boldsymbol{s}+1$ است.

لایه انتشار کامل (ماتریس MDS): لایه انتشار $\boldsymbol{s} \times \boldsymbol{s}$ که عدد انشعاب آن، حداکثر مقدار ممکن برابر $\boldsymbol{s}+1$ باشد، لایه انتشار کامل نامیده می‌شود و لایه انتشار با عدد انشعاب $\boldsymbol{s}$ لایه انتشار تقریباً کامل نامیده می‌شود. یک نوع از لایه‌های انتشار که اخیراً مورد توجه قرار گرفته و دارای ویژگی‌های مناسبی جهت پیاده-سازی هستند، لایه‌های انتشار بازگشتی هستند که در ادامه معرفی می‌شوند.

لایه انتشار بازگشتی: یک لایه انتشار مانند D با s کلمه x_i به عنوان ورودی و s کلمه y_i به عنوان خروجی، یک لایه انتشار بازگشتی نامیده می‌شود، اگر نمایش آن به صورت زیر باشد:

$$D: \begin{cases} y_0 = x_0 \oplus F_0(x_1, x_2, \dots, x_{s-1}) \\ y_1 = x_1 \oplus F_1(x_2, x_3, \dots, x_{s-1}, y_0) \\ \vdots \\ y_{s-1} = x_{s-1} \oplus F_{s-1}(y_0, y_1, \dots, y_{s-2}) \end{cases}$$

$$D^{-1}: \begin{cases} x_{s-1} = y_{s-1} \oplus F_{s-1}(y_0, y_1, \dots, y_{s-2}) \\ x_{s-2} = y_{s-2} \oplus F_{s-2}(x_{s-1}, y_0, \dots, y_{s-3}) \\ \vdots \\ x_0 = y_0 \oplus F_0(x_1, x_2, \dots, x_{s-1}) \end{cases}$$

که در آن F_iها توابع خطی دلخواه هستند. همان طور که مشاهده می‌شود برای محاسبه معکوس لایه انتشار D یعنی D^{-1} نیازی به معکوس توابع F_iها نیست [۱۷].

توجه شود که توابع F_i به‌کاررفته در لایه انتشار می‌توانند ساختاری ساده و سبک داشته باشند. این امر منجر به حاصل شدن لایه‌های انتشار ساده و سبک خواهد شد که از آن نیز می‌توان برای طراحی رمزهای قالبی سبک‌وزن استفاده کرد.

به عنوان یک مثال از این لایه‌های انتشار، می‌توان یکی از لایه‌های انتشار بازگشتی با چهار ورودی و چهار خروجی را به صورت زیر در نظر گرفت [۱۷]:

$$D:\begin{cases} y_0 = x_0 \oplus x_2 \oplus x_3 \oplus L(x_1 \oplus x_3) \\ y_1 = x_1 \oplus x_3 \oplus y_0 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus y_0 \oplus y_1 \oplus L(x_3 \oplus y_1) \\ y_3 = x_3 \oplus y_1 \oplus y_2 \oplus L(y_0 \oplus y_2) \end{cases}$$

که در آن منظور از L ، یک تابع خطی است. ثابت شده است که شرط کافی برای اینکه لایه انتشار بالا کامل بوده و حداکثر عدد انشعاب یعنی برابر ۵ را داشته باشد، لازم است تا توابع $L(x), x \oplus L(x), x \oplus L^3(x), x \oplus L^7(x)$ معکوس‌پذیر باشند [۱۸]. منظور از $L^3(x)$ و $L^7(x)$، به ترتیب توان‌های سوم و هفتم تابع L است.

به عنوان مثال دوم از این لایه‌های انتشار، می‌توان یکی از لایه‌های انتشار بازگشتی معرفی‌شده در [۱۷] با دو ورودی و دو خروجی را به شکل کلی زیر در نظر گرفت:

$$D:\begin{cases} y_0 = x_0 \oplus L(x_1) \\ y_1 = x_1 \oplus L(y_0) \end{cases}$$

برای آشنایی بیشتر با این نوع لایه‌های انتشار می‌توان به [۱۷-۱۸] مراجعه کرد.

۳. ساختار سوئیچینگ

ایده جلوگیری از حذف تفاضلات در ساختار فایستل برای بار اول توسط شیرایی و شیبوتانی [۱۴] ارائه شد. آن‌ها روش استفاده از ماتریس‌های MDS چندگانه را در یک ساختار مبتنی بر جابه‌جایی این ماتریس‌ها پیشنهاد دادند. با این کار جلوگیری از حذف تفاضلات در ساختار فایستل و افزایش تعداد جعبه‌های جانشانی اتفاق می‌افتد . لازم به ذکر است که مؤلفان در این مقاله تنها روی مقاومت در برابر تحلیل تفاضلی تمرکز داشتند و مقاومت در برابر تحلیل خطی را بررسی نکردند و به طور تجربی بیان کردند که اگر در یک ساختار فایستل از سه ماتریس MDS متفاوت استفاده شود، مقاومت بهتری در برابر تحلیل تفاضلی خواهد داشت ولی اثبات نظری برای آن ارائه ندادند. کار شیرایی و شیبوتانی توسط شیرایی و پرینل [۱۵] مورد بررسی بیشتر قرار گرفت. در این مقاله، ابتدا دلیل استفاده از سه MDS متفاوت که می‌تواند باعث بهبود ساختار فایستل در برابر تحلیل تفاضلی شود [۱۴]، به صورت نظری اثبات شد. علاوه بر این شرایطی تعیین شد که با تأمین این شرایط می‌توان مقاومت ساختار رمز را هم در برابر تحلیل تفاضلی و هم تحلیل خطی بهبود داد.

مهم‌ترین خروجی تحقیقات شیرایی و پرینل [۱۵]، اثبات این قضیه است که ساختار پیشنهادی در 3r دور می‌تواند r(m+1) تعداد جعبه جانشانی فعال را ضمانت کند که در آن m عدد شاخه لایه انتشار است و r بزرگ‌تر مساوی ۲ است. مهم‌ترین مسئله در این تحقیق،]یافتن شرایط لازم برای ماتریس‌های MDS که با تأمین آن شرایط نتیجه قضیه اثبات‌شده برقرار شود. شیرایی و شیبوتانی[۱۶] کار شیرایی و پرنیل را مورد مطالعه و بررسی بیشتر قرار دارند و توانستند کران دقیق برای تعداد حداقل جعبه‌های جانشانی فعال در ساختارهای فایستل به دست آورند. علاوه بر این آن‌ها کار شیرایی و پرنیل را وقتی‌که شرایط گفته‌شده روی لایه‌های انتشار تسهیل شده یا حذف‌شده باشند [۱۵]، مورد مطالعه و بررسی قرار دارند و تعداد جعبه‌های جانشانی فعال در این حالت را حساب کردند.

اگر در روش ارائه‌شده در گزارش شیرایی و شیبوتانی [۱۶] به جای یک ماتریس MDS در تابع دور از دو ماتریس MDS با ابعاد m×m مانند D_1 و D_2 استفاده شود، به طوری که هم عدد انشعاب هر یک از این ماتریس‌ها برابر β=m+1 و هم عدد انشعاب الحاق شده دو ماتریس D_1 و D_2 یعنی،

$[\ D_2\ D_1\ ]$ برابر m+1 باشد، تعداد جعبه‌های جانشانی فعال تفاضلی در ۶ دور برابر 2(m+1) خواهد بود. اگر عدد انشعاب الحاق دو ماتریس $(D_1^{\ T})^{-1}$ و $(D_2^{\ T})^{-1}$ یعنی $[\ (D_1^{\ T})^{-1}\ (D_2^{\ T})^{-1}\ ]$ نیز برابر m+1 باشد، همین مباحث برای تعداد جعبه‌های جانشانی فعال خطی نیز برقرار است.

مهم‌ترین کار برای استفاده از ساختار سوئیچینگ، پیدا کردن ماتریس‌های MDS چندگانه است. در این حالت اگر m و طول قالب کوچک باشد، می‌توان ماتریس‌های MDS را به طور تصادفی تولید کرده و بررسی کرد که بردارهای ستونی حاصل از الحاق آن‌ها شرایط MDS بودن را دارند یا نه. اما گر m و طول قالب، بزرگ باشند، جستجوی چنین مجموعه‌ای از ماتریس‌ها سخت خواهد بود. به عبارت دیگر برای طراحی رمزهای قالبی ۶۴ بیتی و ۱۲۸ بیتی می‌توان از ساختار پیشنهادی قبلاً گزارش‌شده [۱۴] استفاده کرد ولی برای طراحی رمزهای قالبی با طول قالب بزرگ‌تر، برای مثال ۱۹۲ بیت، نمی‌توان به راحتی از ساختار ذکرشده استفاده کرد. در ادامه این مقاله روشی پیشنهاد می‌شود که با استفاده از آن می‌توان ساختار مبتنی بر سوئیچینگ لایه‌های انتشار را برای طراحی رمزهای قالبی با طول قالب بزرگ‌تر نیز استفاده کرد. ایده اصلی این است که به جای جستجوی ماتریس‌های MDS چندگانه با شرایط لازم، لایه‌های انتشار بازگشتی چندگانه جستجو می‌شود و این لایه‌های انتشار در ساختارهای فایستل معمولی یا سه‌شاخه استفاده می‌شود.

۴. توصیف ساختارهای پیشنهادی برای طراحی رمزهای قالبی ۱۹۲ بیتی

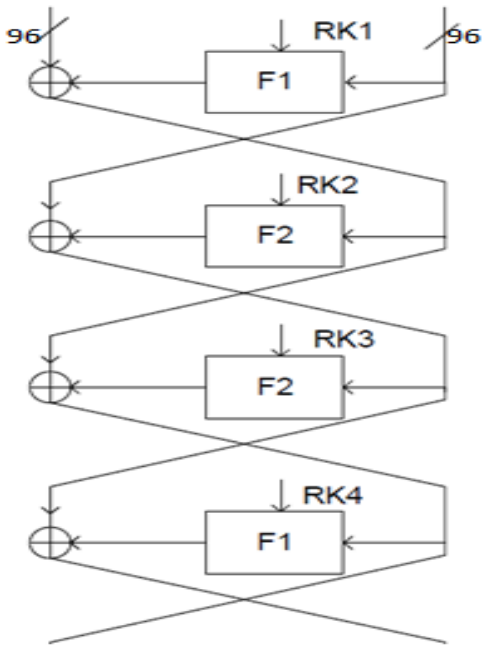
در این بخش توضیح داده می‌شود که چگونه می‌توان برای طراحی رمزهای قالبی ۱۹۲ بیتی، از ساختار سوئیچینگ استفاده

کرد. همان طور که در بخش‌های قبل این مقاله ذکر شد، کار مهم برای استفاده از ساختار سوئیچینگ، به دست آوردن ماتریس‌های MDS و یا لایه‌های انتشار چندگانه است. در این مقاله برای طراحی رمزهای قالبی ۱۹۲ بیتی مبتنی بر ساختار سوئیچینگ، دو روش پیشنهاد می‌شود که در ادامه ابتدا روش پیشنهادی ۱ و سپس روش پیشنهادی ۲ توصیف می‌شود.

۴-۱. توصیف ساختار پیشنهادی ۱

ساختار پیشنهادی اول، یک ساختار سوئیچینگ متداول همراه با لایه‌های انتشار بازگشتی است که کلیات آن در شکل (۱) آورده شده است. این ساختار به طور مختصر به صورت زیر قابل توصیف است:

- در ساختار ۱ از دو تابع F_1 و F_2 با ورودی ۹۶ بیتی و به صورت دو بار تکرار استفاده شده است.
- تابع F_1 با استفاده از ۳ جعبه جانشانی ۳۲ بیتی S_1 و تبدیل انتشار ۳ورودی/ خروجی D_1 طراحی می‌شود.
- تابع F_2 با استفاده از ۳ جعبه جانشانی ۳۲ بیتی S_2 و تبدیل انتشار ۳ورودی/ خروجی D_2 طراحی می‌شود.
- D_1 و D_2 طوری طراحی شده‌اند که علاوه بر این‌که عدد انشعاب D_1 و D_2 برابر ۴ است، این دو لایه انتشار، شرایط لازم برای استفاده در ساختار سوئیچینگ را دارند. یعنی عدد انشعاب $[D_1\ D_2]_{3*6}$ و همچنین $[(D_1{}^t)^{-1}(D_2{}^t)^{-1}]_{3*6}$ نیز برابر ۴ است.



شکل ۱. ساختار۱ برای طراحی رمز قالبی ۱۹۲ بیتی

D_1 و D_2 دو لایه انتشار بازگشتی هستند. برای به دست آوردن این لایه‌های انتشار ساختار یک در ابتدا جستجویی برای تبدیل‌های انتشار منظم تنها با یک تابع و حداقل تعداد دور به شکل کلی زیر انجام می‌شود:

$$D:\begin{cases} Y_0 = x_0 \oplus \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus L(\beta_1 x_1 \oplus \beta_2 x_2) \\ Y_1 = x_1 \oplus \alpha_1 x_2 \oplus \alpha_2 y_0 \oplus L(\beta_1 x_2 \oplus \beta_2 y_0) \\ Y_2 = x_2 \oplus \alpha_1 y_0 \oplus \alpha_2 y_1 \oplus L(\beta_1 x_2 \oplus \beta_2 y_1) \end{cases} \quad (۳)$$

برای جستجوی گسترده‌تر مکان عناصر به‌روز شده تغییر داده شدند. به این معنا که در D ابتدا Y_0 به‌روز می‌شود سپس Y_1 و بعد Y_2. ولی در روش فعلی ترتیب به صورت تصادفی است. با این روش دو ساختار کلی برای لایه‌های انتشار D_1 و D_2 که شرایط لازم ساختار سوئیچینگ را داشته باشند به صورت زیر به دست آمد:

$$D1:\begin{cases} Y_{0(32)} = X_{0(32)} \oplus X_{1(32)} \oplus X_{2(32)} \\ Y_{1(32)} = X_{1(32)} \oplus X_{2(32)} \oplus L(X_{2(32)} \oplus X_{0(32)}) \\ Y_{2(32)} = X_{0(32)} \oplus X_{1(32)} \oplus X_{2(32)} \end{cases} \quad (۴)$$

$$D_2:\begin{cases} Y_{0(32)} = X_{0(32)} \oplus X_{1(32)} \oplus X_{2(32)} \oplus L(X_{1(32)} \oplus X_{2(32)}) \\ Y_{1(32)} = X_{1(32)} \oplus X_{2(32)} \oplus X_{0(32)} \oplus L(X_{2(32)} \oplus X_{0(32)}) \\ Y_{2(32)} = X_{2(32)} \oplus X_{1(32)} \oplus X_{0(32)} \oplus L(X_{1(32)} \oplus X_{0(32)}) \end{cases}$$

قضیه ۱: برای آنکه D_1 و D_2 دارای خاصیت سوییچینگ تفاضلی باشند باید چهار تابع خطی L، $I \oplus L$، $I \oplus L^3$ و $I \oplus L^7$ معکوس پذیر باشند.

اثبات: برای بررسی باید تمام زیر ماتریس‌های زیر مورد بررسی قرار گیرد:

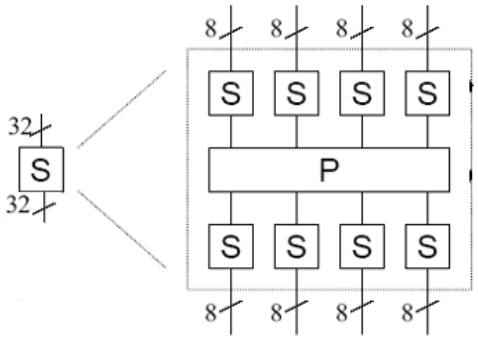
$$\begin{pmatrix} 1 & 1 & 1 & 1 & L\oplus 1 & L\oplus 1 \\ L^{-1} & L^{-1}\oplus 1 & 1 & L\oplus 1 & L^2 & L^2\oplus L \\ L^{-1}\oplus 1 & L^{-1} & 1 & L^2\oplus L & L^3\oplus 1 & L^3\oplus L^2\oplus L \end{pmatrix}$$

با محاسبه دترمینان همه ماتریس‌ها از جمله زیرماتریس‌های ۲×۲ و ۳×۳ چهار ویژگی فوق برای ساختار فوق به دست می‌آید. برای استفاده از این ساختارها لازم است تا تابع L با شرایط لازم ذکرشده در قضیه ۱ به دست آورده شود. یک نمونه از توابع L که شرایط ذکرشده را دارد و برای ورودی‌های ۸ بیتی نیز مناسب است عبارت است از:

$$L(X_{(32)}) = (X_{(32)}) \ggg 15) \oplus x\&0xFF \quad (۵)$$

- جعبه‌های جانشانی ۳۲ بیتی S_1 و S_2 نیز مطابق شکل (۲) و با استفاده از ساختار SPS[1] و جعبه‌های جانشانی هشت بیتی و لایه انتشار P با عدد انشعاب بیشینه ۵ تولید می‌شوند [۱۹].

[1] Substitution Permutation Substitution (SPS)

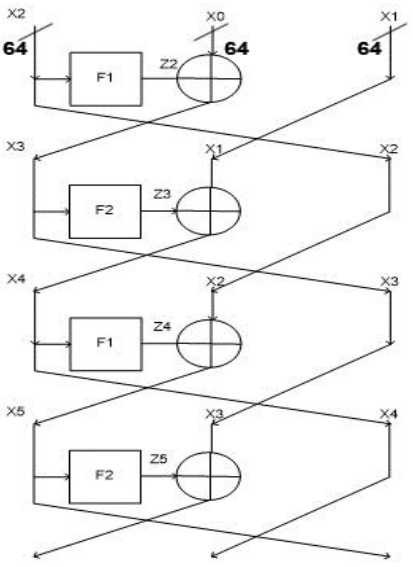


شکل ۲. ساختار SPS برای طراحی جعبه جانشانی ۳۲ بیتی با استفاده از جعبه‌های جانشانی ۸ بیتی[۱۹].

۴-۲. توصیف ساختار پیشنهادی ۲

ساختار پیشنهادی دوم، یک ساختار ۳ شاخه‌ای جدید با ویژگی‌های بهتر از ساختار سوئیچینگ متداول (ساختارهای ۲ شاخه‌ای) است. این ساختار از نوع سوئیچینگ فایستل نوع اول همراه با لایه‌های انتشار بازگشتی است که در شکل (۳) نشان داده‌شده است. از ویژگی‌های مهم این ساختار می‌توان به موارد زیر اشاره کرد:

- پیاده‌سازی آن ساده است چون لایه انتشار آن ۲×۲ و از نوع بازگشتی، با تابع خطی و معکوس‌پذیر سبک مطابق رابطه (۹) است.
- توابع F_1 و F_2 به صورت یک دور در میان به‌کارگیری شده‌اند که این امر برای پیاده‌سازی سخت‌افزاری مناسب است.
- همان طور که در جدول (۱) نشان داده شده است از لحاظ تحلیل خطی و تفاضلی دارای ویژگی‌های بهتری نسبت به ساختار پیشنهادی ۱ است.



شکل۳. ساختار۲ رمز ۱۹۲ بیتی

برای توصیف دقیق این ساختار ابتدا مباحث مربوط به سوئیچینگ را در نظر بگیرید که بر اساس آن و با توجه به شکل (۳) داریم:

$$X_{i-3} \oplus Z_{i-1} = X_i \Rightarrow X_{i-6} \oplus Z_{i-4} \oplus Z_{i-1} = X_i \qquad (۶)$$

در ساختار سوئیچینگ، اگر لایه‌های انتشار چندگانه یک‌درمیان استفاده شوند، رابطه زیر را خواهیم داشت:

$$[D_1\ D_2]\begin{bmatrix} X_{i-4} \\ X_{i-1} \end{bmatrix} = X_{i-6} \oplus X_i \qquad (۷)$$

با بررسی صورت گرفته، مشخص گردید درصورتی‌که از یک تابع F در ساختار ۲ (ساختار فایستل نوع ۱) استفاده شود، پس از ۴ دور حذف تفاضلات رخ می‌دهد. بنابراین هرچند ساختار سوئیچینگ برای ساختارهای دوشاخه‌ای بیان‌شده است ولی برای ساختارهای فایستل نوع یک مانند شکل ۳ نیز قابل تعمیم است. ساختار شکل ۳، یک ساختار جدید است. اگر عدد انشعاب D_1 و D_2 برابر m+1 باشد، تنها شرط اضافه در این حالت، به صورت رابطه ۸ است (فرض کنید تعداد ورودی‌های غیر صفر هر جعبه جانشانی ۳۲ بیتی در تابع F دور iام با $|X_i|$ نمایش داده شود):

$$|X_{i-6}| + |X_{i-4}| + |X_{i-1}| + |X_i| \geq m+1 \qquad (۸)$$

در ساختار پیشنهادی ۲، جعبه‌های جانشانی همانند جعبه‌های جانشانی ساختار ۱ به دست آورده می‌شوند و لایه‌های انتشار D_1 و D_2 که با جستجوی منظم به دست آمده‌اند به شکل زیر می‌باشند:

$$D2: \begin{cases} Y_{0(32)} = X_{0(32)} \oplus L(X_{1(32)}) \\ Y_{1(32)} = X_{1(32)} \oplus L(X_{0(32)}) \end{cases} \qquad (۹)$$

$$D1: \begin{cases} Y_{0(32)} = X_{0(32)} \oplus X_{1(32)} \\ Y_{1(32)} = X_{1(32)} \oplus L(X_{0(32)}) \end{cases}$$

۵. بررسی امنیت و کارایی دو ساختار پیشنهادی

۵-۱. امنیت

برای بررسی امنیت ساختارهای پیشنهادی، حداقل تعداد جعبه‌های جانشانی فعال برای یک تعداد دور مشخص از این الگوریتم‌ها شمارش می‌شود. برای این منظور از روش برنامه‌ریزی خطی [۲۰] که یک ابزار قوی برای شمارش حداقل تعداد جعبه‌های جانشانی فعال است، استفاده می‌شود.

یک مسئله برنامه‌ریزی خطی صحیح (MIP[1]) به شکل کلی زیر است :

$$\min_x \{c^T x \mid Ax \leq b, x \in \mathcal{Z}^k \times \mathcal{R}^l\} \qquad (۱۰)$$

[1] Mixed-Integer Programming

که در آن c یک بردار n بیتی است، A یک ماتریس $m \times n$ ، $n = k + l$ و b یک بردار m بیتی است. رابطه (۱۰) به این معنی است که می‌خواهیم یک تابع خطی را کمینه کنیم که در معرض قیدهای تساوی و نامساوی خطی است. علاوه بر آن برخی از متغیرها نیز محدود به مقادیر صحیح هستند، درحالی‌که برخی متغیرهای دیگر می‌توانند مقادیر حقیقی به خود بگیرند. بعد از شمارش حداقل جعبه‌های جانشینی فعال توسط روش فوق برای دو ساختار پیشنهادی فوق، جدول زیر به دست می‌آید. همان طور که در جدول (۱) مشاهده می‌شود، ساختار دوم تعداد جعبه-های جانشانی فعال بیشتری نسبت به ساختار اول دارد، به عبارت دیگر ساختار ۲ از امنیت بالاتری نسبت به ساختار ۱ برخوردار است.

جدول۱. تعداد جعبه‌های جانشانی فعال در دو ساختار یشنهادی

ساختار دوم			ساختار اول		
تعداد جعبه‌های جانشانی فعال ۸ بیتی	تعداد جعبه‌های جانشانی فعال ۳۲ بیتی	تعداد دور	تعداد جعبه‌های جانشانی فعال ۸ بیتی	تعداد جعبه‌های جانشانی فعال ۳۲ بیتی	تعداد دور
۵	۱	۳	۵	۱	۲
۴۰	۸	۶	۴۰	۸	۶
۸۵	۱۷	۹	۸۰	۱۶	۱۲
۱۳۰	۲۶	۱۵	۱۲۰	۲۴	۱۸
۱۷۵	۳۵	۲۴	۱۶۰	۳۲	۲۴
۲۱۵	۴۳	۳۰	۲۰۰	۴۰	۳۰

مقاومت در برابر حمله‌های تفاضلی و خطی: در حال حاضر جعبه-های جانشانی هشت بیتی (به طور مثال جعبه جانشانی استفاده شده در AES) می‌توانند مشخصه‌های تفاضلی و خطی برابر 2^{-6} داشته باشند. بنابراین با استفاده از این نوع جعبه‌های جانشانی در ساختار پیشنهادی، بهترین مشخصه تفاضلی و خطی برای شش دور ساختار ۱ و ساختار ۲، حداکثر احتمال برابر با $(2^{-6})^{40} = 2^{-240}$ خواهد داشت. ازآنجاکه طول قالب الگوریتم برابر ۱۹۲ بیت است، بنابراین می‌توان نتیجه گرفت که ساختارهای پیشنهادی در برابر روش حمله تفاضلی و حمله خطی مقاوم است. اگر بخواهیم ساختارهای مورد نظر را با رمز Rijndael-192 مقایسه کنیم مشاهده می‌شود که ساختار پیشنهادی اول بعد از ۱۲ دور دارای ۸۰ جعبه جانشانی فعال است و ساختار پیشنهادی دوم بعد از ۱۲ دور دارای ۸۵ جعبه جانشانی فعال است درحالی‌که این مقدار برای Rijndael-192 برابر ۸۷ است که تفاوت چندانی ندارد. بقیه ویژگی‌های امنیتی ساختار پیشنهادی از جمله مقاومت در مقابل سایر حملات، مانند ساختارهای فیستل است که در این بخش دیگر به آن نمی‌پردازیم.

۵-۲. کارایی

ساختارهای پیشنهادی ۱ و ۲ از نوع ساختارهای فیستلی هستند که در مقایسه با ساختارهای SPN از کارایی بالایی برخوردار هستند. . البته لازم به ذکر است که مقایسه وقتی انجام می‌شود که هر دو رمز فیستلی و SPN مورد نظر دارای طول قالب و طول کلید یکسانی بوده و در تابع دور خود از معماری یکسانی مانند SP یا SPS استفاده کنند.

علت کارآیی فیستلی‌ها در مقایسه با SPNها به این دلیل است که چون در ساختارهای فیستلی محاسبات روی نصف حالت انجام می‌شود. یعنی در هر دور نصف طول قالب از تابع F عبور می‌کند بنابراین دارای سرعت بیشتری نسبت به ساختارهای SPN هستند. به عبارت دیگر اگر ما یک رمز ۱۹۲ بیتی SPNای داشته باشیم برای رمز کردن آن لازم است تا تمام محاسبات روی کل این ۱۹۲ بیت انجام شود. درحالی‌که اگر یک رمز فیستلی ۱۹۲ بیتی داشته باشیم در هر دور تنها لازم است تا محاسبات روی ۹۶ بیت انجام شود. روشن است که محاسبات روی ۹۶ بیت می‌تواند سریع‌تر از محاسبات روی ۱۹۲ بیت انجام شود. اگر چه تابع دور یک رمز SPN در مقایسه با تابع دور یک رمز فیستل قوی‌تر است، به این علت که نصف حالت در تابع دور فیستل دست‌نخورده جا به جا می‌شود، ولی باور عمومی بر این است که می‌توان یک و نیم دور فیستل را معادل با یک دور SPN در نظر گرفت و این هم به این معنی است که در شرایط امنیتی یکسان یک رمز فیستلی در مقایسه با یک رمز SPN کاراتر خواهد بود.

علاوه بر توضیحات فوق، به این خاطر که طراحی و پیاده‌سازی تابع‌های با ورودی و خروجی با اندازه کوچک نیاز به منابع و محاسبات کمتری در مقایسه با طراحی و پیاده‌سازی تابع‌های با ورودی و خروجی با اندازه بزرگ دارد، بنابراین رمزهای فیستلی برای محیط‌های سخت‌افزاری و محیط‌های با محدودیت حافظه از اهمیت خاصی برخوردار هستند. برای نشان دادن صحت این گفته می‌توان به رمزهای قالبی سبک‌وزن مانند SIMON و KASUMI اشاره کرد که ساختار فیستلی دارند.

توجه شود که در ساختارهای فیستلی تعمیم یافته که بیش از دو شاخه دارند، طول ورودی و خروجی تابع مورد استفاده کاهش داده می‌شود و طبق توضیحات قبلی این توابع می‌توانند برای محیط‌های ذکرشده مناسب باشند. برای مثال در این مقاله ساختار فیستلی سه شاخه‌ای ارائه شده است که هر شاخه ۶۴ بیت ورودی و خروجی دارد درحالی‌که در فیستلی معمولی

ارائه‌شده در این مقاله هر شاخه ۹۶ بیت ورودی و خروجی دارد. به عبارت دیگر هر مقدار که تعداد شاخه‌ها بیشتر باشند می‌توان از توابع با اندازه‌های ورودی و خروجی کوچک‌تر استفاده کرد. برای مثال در این مورد می‌توان به CLEFIA اشاره کرد که دارای چهار شاخه است.

در یک بخش دیگر مقاله روی بهبود ساختارهای فیستلی یا فیستلی تعمیم یافته با استفاده از مکانیزم سویچینگ کار شده است که این کار تأثیری روی کارآیی ساختارهای فیستلی در مقایسه با ساختارهای SPNای ندارد. حتی روش استفاده شده در این مقاله باعث افزایش کارایی مکانیزم سویچینگ برای طراحی رمزهای قالبی فیستلی می‌شود. برای توضیح این برتری، لازم است توجه شود که در ساختارهای سویچینگ از ماتریس‌های MDS چندگانه استفاده می‌شود که به دست آوردن این ماتریس‌ها برای طول‌های حالت بزرگ‌تر از ۱۲۸ بیت سخت است ولی در این مقاله همان طور که توضیح داده شده است اگر از لایه‌های انتشار بازگشتی چندگانه به جای ماتریس‌های MDS چندگانه استفاده شود با توجه به ساختار لایه‌های انتشار بازگشتی، روشن است که این ساختارها نیازی به ضرب در میدان را ندارند چون از توابع سبک‌وزن در طراحی ماتریس‌های بازگشتی استفاده می‌شود. همچنین در تابع دور این ساختارها از یک جعبه جانشانی ۳۲ بیتی استفاده شده است که می‌توان آن را با استفاده از جدول‌های جستجو پیاده‌سازی کرد. لایه انتشار این تابع‌ها نیز از نوع بازگشتی هستند که در مقایسه با ماتریس‌های MDS قابلیت پیاده‌سازی مناسبی دارند. با توجه به این توضیحات می‌توان گفت که کارایی ساختارهای پیشنهادی از لحاظ سرعت و پیاده‌سازی مناسب است. در ادامه کارایی این دو ساختار با یکدیگر مقایسه می‌شود.

با توجه به اینکه تابع F در ساختار اول در هر دور از ۳ جعبه جانشانی ۳۲ بیتی S و تبدیل انتشار ۳ورودی/ خروجی و در ساختار دوم در هر دور از ۲ جعبه جانشانی ۳۲ بیتی S و تبدیل انتشار ۲ورودی/ خروجی تشکیل شده است در نتیجه تعداد عملیات در هر دو دور از ساختار ۱ (فایستل دوشاخه‌ای) بیشتر از سه دور از ساختار ۲ است. بنابراین در طرح اول در ۲ دور و در طرح دوم در ۳ دور ۶ تابع S به کار می‌رود و این یعنی سرعت طرح ۲ بیشتر است. علاوه بر این ساختار ۲ که در آن از لایه‌های انتشار بازگشتی ۲ در ۲ استفاده شده است، در مقایسه با ساختار ۱ که در آن از لایه‌های انتشار بازگشتی ۳ در ۳ استفاده شده است، پیاده‌سازی راحت‌تری دارد. ساختار ۲ برخلاف روش متعارف ساختارهای سوئیچینگ که تاکنون معرفی‌شده‌اند (ساختار۱) که در آن‌ها توابع F_1 و F_2 دو بار پشت سر هم استفاده شده‌اند این ویژگی را دارد که در آن توابع F_1 و F_2 (شکل ۲) یک‌درمیان به‌کاررفته‌اند. این ویژگی برای پیاده‌سازی سخت‌افزاری مناسب است.

۶. نتیجه‌گیری

در این مقاله، دو ساختار فیستلی مبتنی بر سوئیچینگ، برای طراحی رمزهای قالبی ۱۹۲ بیتی ارائه شد. در ساختار اول از لایه‌های انتشار ۳×۳ و جعبه‌های جانشانی ۳۲ بیتی استفاده و در ساختار دوم که یک ساختار ۳ شاخه‌ای است، از لایه‌های انتشار ۲×۲ و جعبه‌های جانشانی ۳۲ بیتی استفاده می‌شود. برای یافتن لایه‌های انتشار بازگشتی چندگانه مناسب از یک روش جستجوی جدید استفاده شد. در نهایت امنیت ساختارهای پیشنهادی در برابر حملات متداولی مانند حمله خطی و تفاضلی با شمردن حداقل تعداد جعبه‌های جانشانی، با استفاده از روش برنامه‌ریزی خطی مورد بررسی قرار گرفت که نتایج نشان از مقاومت این ساختارها در برابر حملات ذکرشده دارد. همچنین با توجه به به‌کارگیری توابع سبک‌وزن در طراحی ماتریس‌های بازگشتی سرعت این ساختار قابل مقایسه با خانواده رمز قالبی AES است.

۷. مراجع

[1] Briceno, M.; Goldberg, I.; Wagner, D. "A Pedagogical Implementation of the GSM A5/1 "Voice Privacy" Encryption Algorithms"; http://cryptome.org/gsm-a512, 1999.

[2] Briceno, M.; Goldberg, I.; Wagner, D. "A Pedagogical Implementation of the GSM A5/2 "Voice Privacy" Encryption Algorithms"; http://cryptome.org/gsm-a512, 1999.

[3] Kunz, O. "3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Specification of the 3GPP Confidentiality and Integrity Algorithms"; Document2: KASUMI Specification, V3.1.1; http://www.3gpp.org, 2001.

[4] Biham, E.; Dunkelman, O.; Keller, N. "Differential-Linear Cryptanalysis of Serpent"; Fast Software Encryption, FSE2003 2003, 2887, 9–21.

[5] Wu, W.; Zhang, L. "LBlock: A Lightweight Block Cipher"; Applied Cryptography and Network Security, ACNS2011 2011, 6715, 327–344.

[6] Borghoff, J.; Canteaut, A.; Güneysu, T.; Kavun, E. B.; Knezevic, M.; Knudsen, L. R.; Leander, G.; Nikov, V.; Paar, C.; Rechberger, C.; Rombouts, P.; Thomsen, S. S.; Yalçın, T. "PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications"; Advances in Cryptology, Asiacrypt2012, 2012, 7658, 208–225.

[7] Albrecht, M. R.; Driessen, B.; Kavun, E. B.; Leander, G.; Paar, C.; Yalçın, T. "Block Ciphers – Focus on the Linear Layer (Feat. PRIDE)"; Advances in Cryptology, Crypto2014 2014, 8616, 57–76.

[8] Banik, S.; Bogdanov, A.; Isobe, T.; Shibutani, K.; Hiwatari, H.; Akishita, T.; Regazzoni, F. "Midori: A Block Cipher for Low Energy"; Advances in Cryptology, Asiacrypt2015 2015, 9453, 411–436.

[9] Grosso, V.; Leurent, G.; Standaert, F. X.; Varıcı, K. "LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations"; Fast Software Encryption, FSE2014 2015, 8540, 18–37.

[10] Shannon, C. E. “Communication Theory of Secrecy Systems”; Bell System Technical Journal 1949, 28-4, 656–715.

[11] Biham, E.; Shamir, A. “Differential Cryptanalysis of DES-like Cryptosystems”; J. Cryptology 1991, 4, 3–72.

[12] Matsui, M. “Linear Cryptanalysis Method for DES Cipher”; Advances in Cryptology, Eurocrypt’93 1994, 386–397.

[13] Mouha, N. "Differential and Linear Cryptanalysis using Mixed-Integer Linear Programming"; Information Security and Cryptology 2011, 7537, 57-76.

[14] Shirai T.; Shibutani, K. “Improving Immunity of Feistel Ciphers Against Differential Cryptanalysis by using Multiple MDS Matrices”; Proceedings of Fast Software Encryption, FSE’04 2004, 260-278.

[15] Shirai, T.; Preneel, B. “On Feistel Ciphers using Optimal Diffusion Mappings Across Multiple Rounds”; Advances in Cryptology, Asiacrypt'04 2004, 1-15.

[16] Shirai, T.; Shibutani, K. “On Feistel Structures using a Diffusion Switching Mechanism”; Fast Software Encryption 2006, 4047, 41-56.

[17] Sajadieh, M.; Dakhilalian, M.; Mala, H.; Sepehrdad, P. “Recursive Diffusion Layers for Block Ciphers and Hash Functions”; Fast Software Encryption 2012, 7549, 385-401.

[18] Sajadieh M.; Dakhilalian, M.; Mala, H.; Sepehrdad, P. “Efficient Recursive Diffusion Layers for Block Ciphers and Hash Functions”; J. Cryptology 2015, 28, 240-256.

[19] Ohkuma, K.; Muratani, H.; Sano, F.; Kawamura, S. “The Block Cipher Hierocrypt”; Selected Areas in Cryptography 2012, 72-88.

[20] Mouha, N.; Wang, Q.; Gu, D.; Preneel, B. “Differential and Linear Cryptanalysis Using Mixed-Integer Linear Programming”; Information Security and Cryptology, Inscrypt2011 2012, 7537, 57–76.