مجله علمی-پژوهشی «علوم و فناوری‌های پدافند غیرعامل»
سال دوم، شماره ۳، پاییز ۱۳۹۰ : ص ۱۷۷- ۱۶۹

یک الگوریتم جدید رمز قالبی برای شبکه‌های حس‌گر بی‌سیم

عبدالرسول میرقدری[۱*]، بهمن مددی گندوانی[۲] و یوسف پورابراهیم[۳]

۱- استادیار، ۲ و ۳- کارشناس ارشد، دانشکده وپژوهشکده فناوری اطلاعات و ارتباطات، دانشگاه جامع امام حسین(ع)

(دریافت: ۱۳۸۹/۰۹/۱۳، پذیرش: ۱۳۹۰/۰۷/۲۵)

چکیده

در این مقاله یک الگوریتم رمزنگاری قالبی به نام MMF2 مناسب برای کاربردهای مجتمع به همراه یک روش جدید برای بیان امنیت خطی و تفاضلی پیشنهاد می‌گردد. الگوریتم پیشنهادی دارای طول قالب ورودی ۶۴ بیت و طول کلید ۸۰ بیت شامل ۹ دور تکرار می‌باشد. ساختار کلی این الگوریتم از نوع فیستلی ساده بوده که در تابع دور آن از ساختار فیستلی تعمیم یافته نوع دوم استفاده شده است. طراحی این الگوریتم به گونه‌ای است که دارای امنیت قابل اثبات خطی و تفاضلی به‌ترتیب با مشخصه‌های $2^{-111.6}$ و $2^{-94.98}$ می‌باشد. هم‌چنین در طراحی لایه غیرخطی از روش SDS استفاده شده است که علاوه بر سادگی پیاده‌سازی، دارای امنیت قابل قبول برای ۹ دور می‌باشد. با توجه به ویژگی‌های امنیتی جعبه جانشانی با درجه جبری ۶ و درجه غیرخطی ۹۶ و سادگی پیاده‌سازی، این الگوریتم برای ماژول محرمانگی شبکه‌های حس‌گر بی‌سیم مناسب می‌باشد.

کلیدواژه‌ها: الگوریتم رمز قالبی، ساختار فیستلی، امنیت قابل اثبات.

A New Block Cipher Algorithm for Wireless Sensor Networks

A. Mirghadri[1*], B. Madadi[2], Y. Pourebrahim[3]

Faculty of Information and Communication Technology, Imam Hossein University

(Received:12/04/2010 , Accepted:10/17/2011)

Abstract

In this paper, we proposed a new block cipher algorithm called MMF2 suitable for embedded applications, employing a new linear and differential cryptanalysis method. The proposed algorithm has 64 bit block length and 80 bit key size with 9-round iteration. The main structure of this algorithm is Fiestel network that uses generalized type II Fiestel for its round function. The algorithm's design afford provable security with $2^{-111.6}$ and $2^{-94.98}$ linear and differential characteristics, respectively. We used SDS structures in designing nonlinear function of algorithm. This algorithm has a provable security and simple implementations for 9-round iteration. According to simplicity and security features of substitution box with algebraic degree of 6 and nonlinear degree of 96, this algorithm is suitable for wireless sensor networks.

Keywords: Block Cipher Algorithm, Fiestel Structure, Provable Security.

[1] Corresponding author E-mail: amrghdri@ihu.ac.ir

۱. مقدمه

شبکه‌های حس‌گر بی‌سیم نوع جدیدی از شبکه‌های راهبردی ارتباطاتی نوین هستند که دارای کاربری نظامی و استفاده موثر در مدیریت بحران می‌باشند. لذا با افزایش کاربرد این شبکه‌ها در ارتباطات نظامی و پدافند غیرعامل، امنیت این شبکه‌ها در تبادل اطلاعات از اهمیت ویژه‌ای برخوردار است. با توجه به محدودیت‌های ذاتی اجزای این شبکه‌ها، برای ایجاد محرمانگی داده بایستی از الگوریتم‌هایی استفاده نمود که با محدودیت‌های این شبکه‌ها سازگار باشند. از جمله این محدودیت‌ها می‌توان به محدودیت منابع انرژی، سطح گیت اشغالی در حالت پیاده‌سازی سخت‌افزاری، مقدار حافظه مورد نیاز در حالت پیاده‌سازی نرم‌افزاری و محدودیت‌های پردازشی اشاره نمود.

از جمله کارهای انجام شده در این زمینه می‌توان به الگوریتم هایت[1] که توسط هونگ و همکارانش درسال ۲۰۰۶ با کاربرد سخت‌افزاری طراحی شده است اشاره نمود. این الگوریتم برای استفاده شبکه‌های حس‌گر بی‌سیم مناسب می‌باشد[۱]. از جمله طرح‌های معروف دیگر می‌توان به الگوریتم پرزنت[2] ارائه شده در سال ۲۰۰۷ توسط باگدانو و همکارانش، الگوریتم پوفین[3] ارائه شده توسط چنگ و همکارانش در سال ۲۰۰۸، الگوریتم میبز[4] ارائه شده در سال ۲۰۰۹ توسط صادقیان و همکارانش، الگوریتم‌های پرینت[5] ارائه شده در سال ۲۰۱۰ توسط نادسن و همکارانش و کلین[6] توسط گونگ و همکارانش و الگوریتم البلوک[7] در سال ۲۰۱۱ ارائه شده توسط وو و ژنگ اشاره کرد. الگوریتم‌های ذکرشده در مقابل حملات بومرنگ و تفاضلی نقطه ضعف نشان داده‌اند[۷-۲].

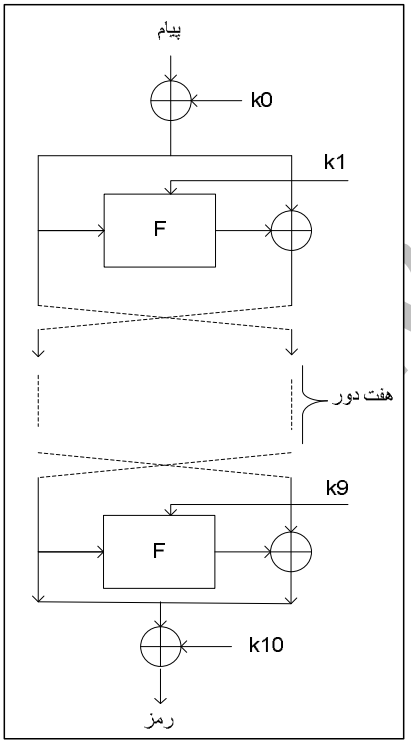
یکی از موارد اساسی که در اکثر طرح‌های رمزنگاری پیشنهادی برای شبکه‌های حس‌گر بی‌سیم در نظر گرفته می‌شود، استفاده از جعبه‌های جانشینی (S-Box)۴×۴ می‌باشد. دلیل این مساله کاهش حجم سخت‌افزار و حافظه مورد نیاز می‌باشد. با این حال انتخاب جعبه‌های جانشینی کوچک‌تر بایستی با دقت بیشتری صورت گیرد، زیرا از نظر امنیت نسبت به جعبه‌های‌جانشینی ۸×۸ ضعیف‌ترند. در این مقاله، یک الگوریتم جدید رمزنگاری از نوع قالبی با ساختار فیستلی و با جعبه جانشانی ۴×۴ ارائه می‌شود[۸].

در طراحی این الگوریتم از جعبه‌های جانشانی ۴×۴ به‌گونه‌ای استفاده شده است که ویژگی‌های امنیتی بسیار مناسب و مورد انتظار را نتیجه می‌دهد. هم‌چنین برای اطمینان از امنیت الگوریتم، ساختار پیشنهادی به‌نحوی طراحی گردیده است که امنیت قابل اثبات خطی و تفاضلی برای آن قابل ارائه باشد.

با توجه به مطالب بیان‌شده، ساختار مقاله به شرح زیر می‌باشد. در بخش دوم ساختار کلی الگوریتم پیشنهادی معرفی می‌گردد، در بخش سوم اصول طراحی قسمت‌های مختلف تشریح شده و در بخش چهارم میزان امنیت الگوریتم در مقابل برخی از حملات معروف مورد تحلیل قرار گرفته و در نهایت در بخش پنجم نتیجه‌گیری و کارهای آینده ارائه خواهد شد.

۲. ساختار کلی الگوریتم جدید

الگوریتم پیشنهادی دارای ساختار فیستلی ۹ دوری با ۶۴ بیت طول قالب ورودی مطابق شکل (۱) می‌باشد. ساختار تابع دور این الگوریتم فیستلی تعمیم یافته نوع دوم بوده که در طراحی این تابع دور از ساختار SDS[1] استفاده شده است[۹].



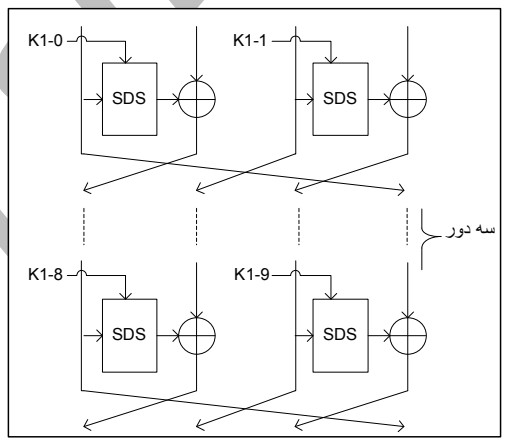
شکل۱. ساختار کلی الگوریتم جدید

[1] Hight
[2] Present
[3] Puffin
[4] MIBS
[5] Print
[6] Klein
[7] Lblock

۲-۱. ساختار تابع دور F

در شکل (۲) ساختار تابع دور F نشان داده شده که از یک ساختار فیستلی تعمیم یافته نوع دوم ۵ دوری تشکیل شده است. هدف از این طراحی، بهبود سرعت الگوریتم و کاهش حافظه مورد نیاز و از طرفی دیگر رسیدن به امنیت قابل اثبات می‌باشد.

دلیل استفاده از فسیتل نوع دوم در این طرح، عدم نیاز به جعبه‌های جانشینی بزرگ‌تر و هم‌چنین قابل بیان بودن امنیت خطی و تفاضلی اثبات‌پذیر می‌باشد و هم‌چنین در مرجع به خواص و ویژگی‌های مناسب آنها برای کاربردهای سبک وزن اشاره شده است[۱۲و۱۰]. بنابراین با این طراحی یک موازنه هوشمندانه بین حافظه مورد نیاز، سرعت اجرا، امنیت و سبک وزن بودن برقرار گردیده است.



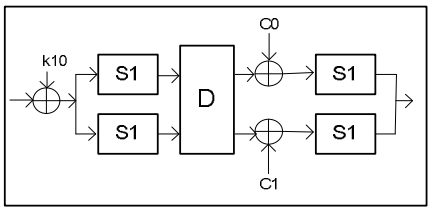
شکل۲. ساختار تابع دور F

۲-۲. ساختار تابع SDS

بلوک SDS از سه لایه متوالی غیرخطی، خطی و غیرخطی تشکیل شده است. شکل (۳)، شمای کلی این بلوک را نشان می‌دهد. قرار دادن دو لایه‌ی غیرخطی متوالی، هیچ مزیتی نسبت به یک لایه غیرخطی ندارد[۱]، اما قرار گرفتن یک لایه انتشار در بین آنها، در افزایش تعداد جعبه‌های جانشینی فعال، نقش قابل توجهی دارد و نیز امنیت خطی و تفاضلی آن قابل اثبات می‌باشد[۱۳]. هم‌چنین لازم به ذکر است چون لایه انتشار بین دو لایه غیرخطی نقش کلیدی در افزایش تعداد جعبه‌های جانشینی فعال دارد، لذا در این الگوریتم جعبه‌ها از نوع MDS[۲] انتخاب شده است.

مقادیر عددی جعبه جانشینی S1 و جعبه جانشینی SDS معادل در جداول پیوست آمده است.

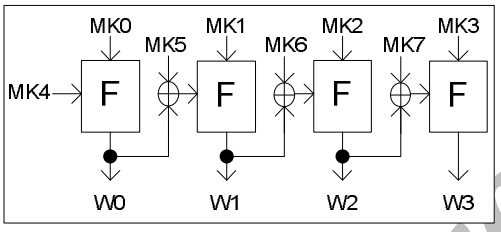
[۱] در صورتی که هر لایه، یک به یک باشد و طراحی آنها مناسب باشد.
[2] Maximum Distance Separable Codes



شکل۳. ساختار تابع SDS

۳. فرآیند تولید کلید

این الگوریتم دارای کلیدی به‌طول ۸۰ بیت می‌باشد و برای استخراج و توسعه زیرکلیدها، از توابع F و ثابت MK استفاده شده که شمای کلی آن در شکل (۴) نشان داده شده است. از مقادیر Wiهای ۳۲ بیتی برای استخراج کلیدهای دور به‌صورت زیر استفاده می‌گردد که در آن KEY کلید اصلی می‌باشد و مقدار ثابت CK از مراجع انتخاب شده است[۱۴].



شکل۴. شماتیک توسعه کلید

$$MK = KEY \,\|\, \mathrm{CK}$$
$$\mathrm{CK} = 0x6db14acc9e21c820ff28b1d5ef5de2b0$$

$$
\begin{aligned}
&M0=W0\|W1,\ M1=W1\|W2,\ M2=W2\|W3,\ M3=W3\|W0\\
&k0=(M0\lll 3)\oplus M1\\
&k1=(M1\lll 3)\oplus M2\|MK0L\\
&k2=(M2\lll 3)\oplus M3\|MK0R\\
&k3=(M0\lll 19)\oplus(M3\ggg 3)\|MK1L\\
&k4=(M0\lll 7)\oplus(M2\ggg 3)\|MK1R\\
&k5=(M1\lll 23)\oplus(M3\ggg 11)\|MK2L\\
&k6=(M1\lll 13)\oplus(M2\ggg 7)\|MK2R\\
&k7=(M0\lll 33)\oplus(M3\ggg 17)\|MK3L\\
&k8=(M0\lll 3)\oplus(M1\ggg 19)\oplus MKL\|MK3R\\
&k9=(M1\lll 11)\oplus(M2\ggg 17)\oplus(M3\ggg 23)\|\sim MK3L\\
&k10=(M2\lll 31)\oplus(M3\ggg 37)\oplus MKR
\end{aligned}
\qquad (۱)
$$

۴. اصول طراحی الگوریتم

به دلیل محدودیت‌های پیاده‌سازی سخت‌افزاری و محدودیت‌های حافظه مورد نیاز در اجزای شبکه‌های حس‌گر بی‌سیم، استفاده از ساختارهای خودبازگشتی بسیار مناسب می‌باشد. به همین دلیل، در طراحی الگوریتم از ساختارهای فیستلی استفاده شده است. هم‌چنین در طراحی تابع F بایستی به مسئله پیاده‌سازی و امنیت توجه شود. در این مورد نیز ساختارهای فیستلی می‌توانند گزینه مناسبی باشند. از بین سه نوع ساختار فیستلی تعمیم‌یافته نوع اول، دوم و سوم، به دلیل داشتن پیچیدگی کم و برآورد تمامیت در حداقل تعداد دور و هم‌چنین داشتن امنیت قابل اثبات، نوع دوم انتخاب گردید[۱۴].

در طراحی تابع دور تابع F از ساختار SDS استفاده شده است. جعبه جانشانی به‌کار برده شده در تابع SDS از اندازه ۴×۴ بوده و دارای ماکزیمم احتمال خطی و تفاضلی 2^{-2} می‌باشد. هم‌چنین کل تابع SDS را می‌توان به‌صورت یک جعبه جانشانی با اندازه ۸×۸ فرض کرد که در ضمیمه آورده شده است. ویژگی‌های امنیتی این جعبه جانشانی معادل در جدول (۱) آورده شده است. با این شیوه طراحی هم مسئله پیاده‌سازی و هم مسئله امنیت به‌خوبی برآورده می‌شود.

لایه انتشار در ساختار SDS به فرم MDS است. بعد از لایه انتشار مقادیر ثابت $C1 = 14$ و $C0 = 10$ به فرم نشان داده شده در شکل (۳) به خروجی SD اضافه می‌گردد. هدف از این نوع طراحی کاهش پیچیدگی پیاده‌سازی با در نظر گرفتن سطح امنیتی مناسب می‌باشد. برای طراحی شماتیک توسعه کلید، معیارهای زیر در نظر گرفته شده‌اند:

۱- قابلیت استفاده از کلیدهای ۱۲۸ و ۱۹۲ و ۲۵۶ بیتی
۲- استفاده از عملگرهای منطقی از قبیل & و | ...
۳- عدم استفاده از زیرکلیدها در استخراج کلید اصلی
۴- حداقل کردن تاخیر ناشی از توسعه کلید رمزنگاری و رمزگشایی

مشخصات کلی این الگوریتم، که به اختصار با نماد MMF2 نشان داده می‌شود، در جدول (۲) با برخی الگوریتم‌های سبک وزن قالبی مقایسه شده است. با توجه به جدول (۲)، مشاهده می‌شود که الگوریتم MMF2 پیشنهادی، نسبت به سایر الگوریتم‌های مطرح شده اندازه‌های مشخصه کمتری دارد و هم‌چنین تعداد دور لازم این الگوریتم از سایر الگوریتم‌ها خیلی کمتر است لذا سرعت انتشار آن از بقیه سریع‌تر بوده و در اجرا کارآمدتر می باشد[۱۱].

جدول۱. ویژگی‌های امنیتی Sbox معادل SDS به‌کار برده شده در الگوریتم

غیرخطی بودن	درجه جبری	نقطه ثابت	ماکزیمم احتمال خطی	ماکزیمم احتمال تفاضلی	نقطه ثابت معکوس	N.Bi-affine Equations	N.Quadratic Equations
۹۶	۶	ندارد	2^{-4}	$2^{-5}+2^{-7}$	ندارد	۰	۰

جدول۲. اندازه‌های مشخصه چند الگوریتم رمز قالبی

الگوریتم رمز	AES	KLEIN	HIGHT	PUFFIN	MIBS	PRINT	PRESENT	LBlock	MMF2
اندازه قالب	۱۲۸	۶۴	۶۴	۶۴	۶۴	۴۸	۶۴	۶۴	۶۴
طول کلید	۱۲۸	۶۴	۱۲۸	۸۰	۶۴	۸۰	۸۰	۸۰	۸۰
تعداد دور	۱۰	۱۲	۳۲	۳۴	۳۲	۴۸	۳۱	۳۲	۹

۵. اصول پیاده‌سازی

این الگوریتم به‌گونه‌ای طراحی شده است که از لحاظ پیاده‌سازی سخت‌افزاری و نرم‌افزاری به‌ویژه برای پردازنده‌های ۸ بیتی بسیار کارآمد بوده و در نتیجه برای استفاده در شبکه‌های حس‌گر بی‌سیم مناسب می‌باشد.

برای پیاده‌سازی ۸ بیتی در پردازنده‌ای ۸ بیتی ساختار SDS به راحتی به‌صورت یک جدول انتخاب با ۲۵۶ بایت حافظه قابل جایگزینی است. در صورتی که از لحاظ حافظه محدودیت وجود داشته باشد، برای پیاده‌سازی آن تنها ۱۶ بایت جدول انتخاب لازم خواهد بود. برای پیاده‌سازی لایه انتشار MDS در صورت عدم به کار گیری جعبه جانشانی معادل SDS از رابطه (۲) استفاده می‌شود.

$$\begin{bmatrix} b2 \\ b1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a2 \\ a1 \end{bmatrix} \Rightarrow \begin{cases} b2 = (a2 <<<1) \oplus ((a2 >> 3) << 1) \oplus a1 \\ b1 = a1 \oplus a2 \end{cases} \quad (۲)$$

قابل ذکر است که میدان گالوای به‌کار برده شده دارای مشخصه x^4+x+1 است که برابر ۱۹ دسیمال می‌باشد. a_i, b_i هر کدام ۴ بیتی می‌باشند. اگر دو خروجی ۴ بیتی به‌صورت $b_1 \| b_2$ به هم‌دیگر الحاق شود، یک ۸ بیتی خواهد بود که در آن ۴ بیت با اندیس بزرگتر همان ۴ بیت با ارزش خواهد بود.

۶. تحلیل الگوریتم

حملات خطی و تفاضلی و بومرنگ از مهمترین حملات معروف علیه رمزکننده‌های قالبی می‌باشند[۹ و۸]. لذا برای نشان دادن امنیت الگوریتم در برابر این حملات با بیان یک‌سری قضایا، هر دو امنیت اثبات‌پذیر و امنیت عملی ارائه می‌شود. همچنین یک روش جدید با ترکیب امنیت اثبات‌پذیر و امنیت کاربردی برای بیان امنیت خطی و تفاضلی ارائه می‌گردد که از این طریق می‌توان امنیت بسیاری از الگوریتم‌های قالبی را ارزیابی نمود. در نهایت تحلیل انتگرالی (مربعی) که یک تحلیل کارساز و پراستفاده علیه الگوریتم‌های قالبی می‌باشد را برای الگوریتم پیشنهادی ارائه می‌شود.

۶-۱. تحلیل خطی و تفاضلی

برای روشن شدن امنیت در مقابل حملات خطی و تفاضلی اثبات‌پذیر قضایای زیر بیان می‌شوند:

قضیه۱: برای هر ساختار فیستلی ساده با تابع دور دوسوئی F احتمال خطی (LP[1]) و تفاضلی (DP[2]) بزرگتر مساوی سه دور به صورت زیر می‌باشد که در آن p و q به ترتیب احتمال تفاضلی و خطی تابع دور F می‌باشند [۱۶].

$$DP_{max} \le p_F^2 \qquad LP_{max} \le q_F^2 \qquad (۳)$$

قضیه ۲: برای هر ساختار فیستلی نوع دوم تعمیم یافته با تابع دور یک به یک و پوشای F احتمال خطی (LP) و تفاضلی (DP) بزرگتر مساوی پنج دور به صورت زیر می‌باشد که در آن p و q به ترتیب احتمال تفاضلی و خطی تابع دور F می‌باشد [۱۷]:

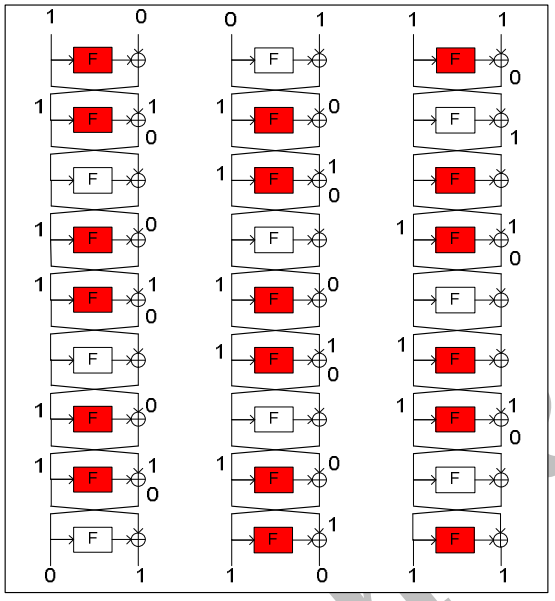
$$DP_{max} \le p_F^4 + 2p_F^5 \qquad LP_{max} \le q_F^4 + 2p_F^5 \qquad (۴)$$

از آنجا که ساختار کلی این الگوریتم تابع فیستلی ساده با تابع دور فیستلی نوع دو تعمیم یافته شامل تابع دور SDS می‌باشد لذا سه دور آن دارای احتمال تفاضلی قابل اثبات $((p_{SDS})^4+2(p_{SDS})^5)^2$ و احتمال خطی قابل اثبات برابر $((q_{SDS})^4+(q_{SDS})^5)^2$ می‌باشد. طبق جدول (۱)، $p_{SDS}=2^{-5}+2^{-7}$ و $q_{SDS}=2^{-4}$ می باشد لذا با صرف نظر از جمله دوم، رابطه (۵) به صورت زیر به‌دست می‌آید:

$$DP \le ((2^{-5}+2^{-7})^4+2(2^{-5}+2^{-7})^5)^2 \approx 2^{-37.207}$$
$$LP \le (2^{-16}+2\times 2^{-20})^2 \approx 2^{-31.66} \qquad (۵)$$

۶-۱-۱. روش جدید تحلیل امنیت خطی و تفاضلی

از آنجا که بیان امنیت قابل اثبات خطی و تفاضلی در الگوریتم‌های قالبی با افزایش تعداد دور بسیار مشکل می‌باشد و از طرفی صرف تکیه بر امنیت کاربردی بر مبنای تعداد جعبه‌های جانشینی فعال اعتبار بالایی ندارد، لذا روشی پیشنهاد می‌گردد که ترکیبی از دو روش قبلی بوده و قابلیت اطمینان بیشتری نسبت به امنیت کاربردی دارد.

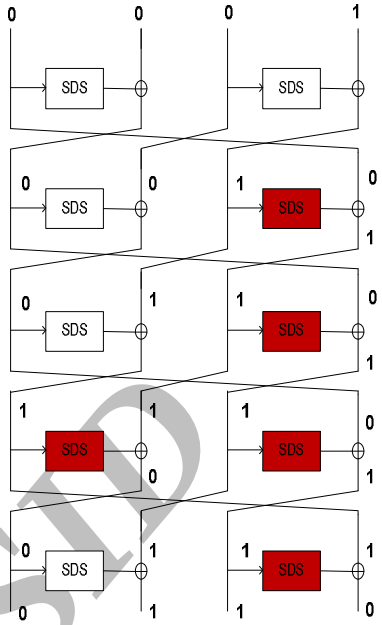


شکل۵. تعداد توابع دور فعال در بدترین شرایط

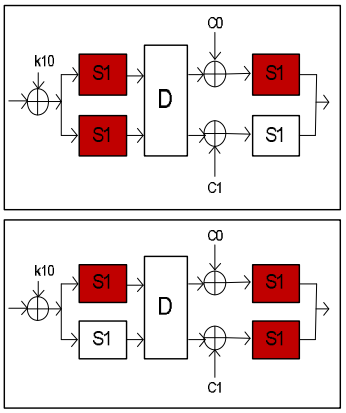
شکل(۵) تعداد توابع F فعال در بدترین شرایط را نشان می‌دهد (بدترین حالات از طریق جستجوی رایانه‌ای به‌دست آمده است)، همان‌طور که مشخص است، در بدترین شرایط حداقل ۶ مورد از Fها فعال شده‌اند، برای این که بهتر مشخص شود بایستی برای خود تابع F هم بدترین حالت به دست آورده شود.

در شکل(۶) این حالت نشان داده که به ازای بدترین حالت ۵ مورد از توابع SDS فعال شده‌اند و با توجه به شکل(۷) تابع SDS دو حالت بیشتر ندارد که در هر دو حالت ۳ مورد از S-B0xها فعال شده‌اند، لذا برای اینکه در تحلیل عملی خطی و تفاضلی و روش جدید بتوانیم دقیق صحبت کنیم تعداد S-Boxهای فعال برای تعداد دورهای مختلف الگوریتم در جدول(۲) آورده شده است، لازم به ذکر است که در تنظیم جدول از شکل (۵) حالت وسطی مد نظر بوده است.

[1] Linear Probability
[2] Differential Probability



شکل۶. تعداد توابع دور فعال در بدترین شرایط



شکل۷. تعداد توابع دور فعال در بدترین شرایط

جدول۳. تعداد Sbox های فعال برای تعداد دورهای مختلف

تعداد دور	تعداد S-Boxهای فعال
1	0
2	15
3	30
4	30
5	45
6	60
7	60
8	75
9	90

در تحلیل خطی عملی با توجه به این که $DL^{s}_{max} = 2^{-2}$، لذا با توجه به جدول (۳) برای ۹ دور، تعداد ۹۰ مورد S-box فعال شده است، لذا:

$$DL^{9-round}_{max} \le 2^{-2\times 90} = 2^{-180} \qquad (۶)$$

که نشان می‌دهد با توجه به طول قالب الگوریتم، تحلیل خطی عملی بر روی این الگوریتم موثر نخواهد بود. هم‌چنین با توجه به اینکه $DP^{s}_{max} = 2^{-2}$ و با توجه به جدول (۳) برای ۹ دور تعداد ۹۰ S-Box فعال شده است، لذا:

$$DP^{9-round}_{max} \le 2^{-2\times 90} = 2^{-180} \qquad (۷)$$

یعنی الگوریتم در مقابل تحلیل تفاضلی عملی نیز مقاوم است.

روش جدید ترکیبی به این صورت پیشنهاد می‌شود که در الگوریتم‌های قالبی به جای شمارش حداقل تعداد جعبه‌های جانشینی فعال، حداقل تعداد توابع دور فعال شمارش گردد. هم‌چنین به دلیل سادگی توابع دور، امنیت قابل اثبات این توابع به‌راحتی قابل محاسبه خواهد بود. به این ترتیب امنیتی سخت‌گیرانه‌تر از امنیت کاربردی و نزدیک به امنیت قابل اثبات به‌دست می‌آید که قابل اعتمادتر می‌باشد. با توجه به شکل (۵) در بدترین شرایط تعداد توابع F فعال در ۹ دور الگوریتم ۶ مورد می‌باشد. هر تابع F خود امنیت خطی و تفاضلی قابل اثبات به صورت زیر دارد:

$$DP_F \le ((2^{-5}+2^{-7})^4 + 2(2^{-5}+2^{-7})^5) \approx 2^{-18.60}$$
$$LP_F \le (2^{-16} + 2\times 2^{-20}) \approx 2^{-15.83} \qquad (۸)$$

لذا با توجه به تعداد توابع F فعال امنیت خطی و تفاضلی الگوریتم از طریق روش ترکیبی به صورت ذیل می باشد:

$$DP \le (DP_F)^6 \approx 2^{-111.6}$$
$$LP \le (LP_F)^6 \approx 2^{-94.98} \qquad (۹)$$

لازم به ذکر است که در شکل (۵) ورودی تفاضلی غیرصفر با مقدار ۱ نشان داده شده است. هم‌چنین به دلیل یک به یک بودن به جای ماسک خروجی غیرصفر از ماسک ورودی غیرصفر استفاده شده است.

۶-۲. تحلیل بومرنگ

در حمله بومرنگ الگوریتم به دو قسمت دلخواه تقسیم و هر قسمت با حمله تفاضلی تحلیل می‌شود که لازم نیست دو قسمت دارای تعداد دور مساوی باشند[۱۸]. اگر قسمت اول دارای احتمال تفاضلی برابر p و قسمت دوم دارای احتمال تفاضلی q باشند، آنگاه (با توجه به طول قالب) در صورتی که $p^2q^2 \le 2^{-64}$ باشد، الگوریتم در برابر این حمله امنیت قابل قبول دارد. جدول (۴) مشخصه تفاضلی را برای حمله بومرنگ در سه حالت مختلف نشان می‌دهد، با توجه به اطلاعات جدول (۳)، نتایج تحلیل الگوریتم با ۹ دور در ۳ حالت دلخواه در جدول (۴) نشان داده شده است.

جدول۴. نتایج تحلیل بومرنگ

case	E_0E_1		E
I	(E_0, E_1) P,Q	۷ و۲ دور $\leq 2^{-2\times15}, 2^{-2\times75} \geq$	۹دور $P^2Q^2 \leq 2^{-2\times30} \times 2^{-2\times150} = 2^{-360}$
II	P,Q	۶ و۳ دور $\leq 2^{-2\times30}, 2^{-2\times60} \geq$	۹ دور $P^2Q^2 \leq 2^{-2\times60} \times 2^{-2\times120} = 2^{-360}$
III	P,Q	۴.۵ و ۴.۵ دور $\leq 2^{-2\times45}, 2^{-2\times45} \geq$	۹ دور $P^2Q^2 \leq 2^{-2\times90} \times 2^{-2\times90} = 2^{-360}$

با توجه به مشخصه‌های تفاضلی به‌دست آمده برای هر سه حالت در جدول فوق، مشخص است که حمله بومرنگ برای ۹ دور الگوریتم طراحی شده کارساز نخواهد بود.

۶-۳. حمله مربعی (انتگرالی)

از آنجایی که الگوریتم ارائه شده از توابعی با ورودی‌های ۴ بیتی استفاده می‌کند، می‌بایست میزان مقاومت الگوریتم در برابر حمله مربعی (انتگرالی)[1] بررسی شود[۱۹]. در حمله مربعی مجموعه‌های چندگانه[2] با حالت‌های زیر تعریف می‌شوند:

۱- حالت ثابت (C): در این مجموعه چندگانه همه عناصر مقدار یکسانی دارند.

۲- حالت کامل (A): در این مجموعه چندگانه همه عناصر با هم متفاوت هستند و تمامی فضای متناظر را می‌پوشانند.

۳- حالت جمعی (S): در این مجموعه‌های چندگانه حاصل جمع همه عناصر برابر صفر است.

۴- حالت نامشخص (؟): در این مجموعه چندگانه هیچ‌یک از ویژگی‌های ۱ تا ۳ برقرار نیست.

حمله تا جایی ادامه پیدا می‌کند که یک پورت با یکی از ویژگی‌های ۱ تا ۳ داشته باشیم.

جدول (۵) نحوه تغییر حالت‌ها را در عبور از لایه‌های خطی و غیرخطی نشان می‌دهد. برای بررسی مقاومت الگوریتم در برابر حمله مربعی، ابتدا عملکرد تابع دور بررسی می‌شود. با توجه بررسی‌های انجام شده، بدترین مجموعه چندگانه ورودی برای تابع دور به صورت شکل (۸) است که هر ستون، ورودی یک پورت است؛ یعنی باید یکی از ورودی‌های پورت دوم فعال شود.

C	A	C	C		
C	C	C	C		

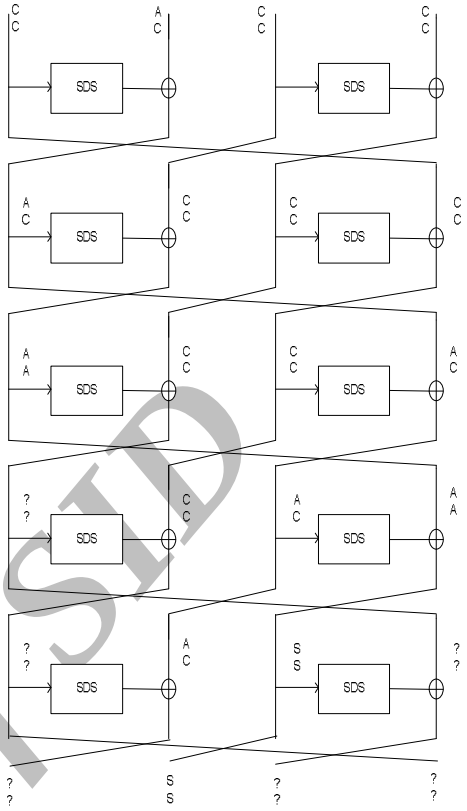
شکل۸. بدترین مجموعه چندگانه ورودی برای تابع دور

جدول۵. نحوه تغییر حالت‌ها در عبور از لایه‌های خطی و غیرخطی

	C C	A C	A A	S S	? ?
لایه‌ی خطی	C C	A A	S S	? ?	? ?
لایه‌ی غیرخطی	C C	C C	C C	? ?	? ?

شکل (۹) نحوه تغییرات این مجموعه چندگانه را نشان می‌دهد. پس از ۵ دور، خروجی به صورت شکل(۱۰) است. اکنون دوباره بدترین مجموعه چندگانه ورودی برای کل الگوریتم در نظر گرفته می‌شود. این مجموعه چندگانه به‌صورت شکل (۱۱) است.

[1] Square (Integral) Attack
[2] Multi Set



شکل۹. نحوه تغییرات مجموعه چندگانه برای تابع دور

?	S	?	?
?	S	?	?

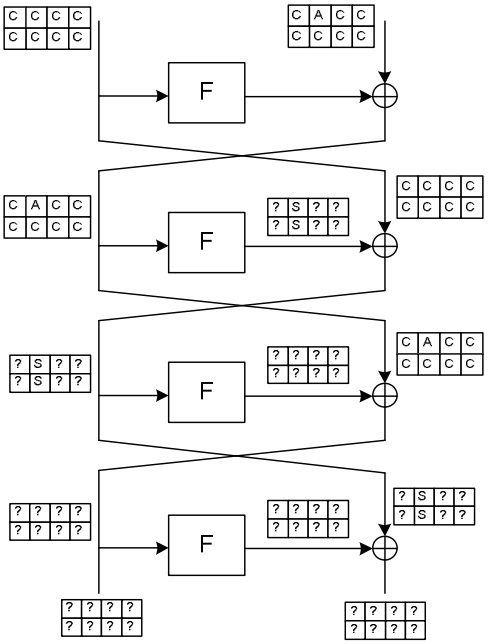
شکل۱۰. تغییرات مجموعه چندگانه بعد از تابع دور

C	C	C	C
C	C	C	C

C	A	C	C
C	C	C	C

شکل۱۱. بدترین مجموعه چندگانه ورودی برای کل الگوریتم

همان‌طور که در شکل (۱۲) دیده می‌شود، پس از ۴ دور به مجموعه چندگانه‌ای با حالت کاملا نامشخص می‌رسد؛ بنابراین برای بیشتر از ۴ دور هیچ مشخصه مناسبی برای الگوریتم وجود ندارد و الگوریتم معرفی شده در برابر حمله انتگرالی امن است.



شکل۱۲. نحوه تغییرات مجموعه چندگانه برای ۴ دور الگوریتم کلی

۷. نتیجه‌گیری

در این مقاله یک الگوریتم جدید رمز قالبی با ویژگی امنیت قابل اثبات ارائه گردید. در طراحی الگوریتم از لحاظ پیاده‌سازی و حافظه مورد نیاز یک مصالحه صورت گرفته است که باعث مناسب شدن آن برای کاربردهای شبکه‌های حس‌گر بی‌سیم گردیده است. به منظور رسیدن به مصالحه اشاره شده، از جعبه‌های جانشینی ۴×۴ در ساختار SDS استفاده شده است که در پیاده‌سازی بر مبنای نرم‌افزار به‌صورت یک S-box به اندازه ۸×۸ خواهد بود. هم‌چنین الگوریتم با روش جدید ترکیبی از نقطه نظر امنیت خطی و تفاضلی تحلیل گردید که احتمال خطی و تفاضلی آن به ترتیب برابر $2^{-111.6}$ و $2^{-94.98}$ تعیین شد و لذا امنیت به‌دست آمده با این روش دارای قابلیت اطمینان بیشتری نسبت به امنیت کاربردی می‌باشد، الگوریتم طراحی شده در مقابل حمله انتگرالی نیز دارای امنیت می‌باشد. از نقطه نظر امنیتی این الگوریتم از سایر الگوریتم‌های ذکرشده در مقدمه بهتر می‌باشد. به عنوان کار آتی می‌توان این الگوریتم را در محیط‌های مختلف سخت‌افزاری و نرم‌افزاری پیاده‌سازی نمود و نتایج اجرا با سایر الگوریتم‌های مطرح مقایسه و تحلیل شود، هم‌چنین رویکرد طراحان الگوریتم از سال ۲۰۱۰ به بعد بیشتر بر روی ساختارهای فیستلی تعمیم یافته و خواص ویژه آنها می‌باشد، لذا مطالعه ساختارهای فیستل تعمیم‌یافته حوزه تحقیقاتی آینده الگوریتم‌های قالبی می‌باشد.

۸. مراجع

[1]. Hong, D.; Sung, J.; Hong, S.; Lim, J.; Lee, S.; Lee, C. "HIGHT: A New Block Cipher Suitable for Low-Resource Device."; Goubin, L. and Matsui, M. Editors, Proceeding of CHES 2006, LNCS, 4249, 46-59.

[2]. Bondanov, A. "PRESENT: An Ultra-Lightweight Block Cipher Attack."; Cryptographic Hardware and Embedded Systems (CHES2007), Springer-Verlag 2007, LNCS, 4727, 450-466.

[3]. Cheng, H.; Heys, H. M.; Wang, C. "PUFFIN: A New Compact Block Cipher Targeted to Embedded Digital Systems."; 11th Euromicro Conference on Digital System Design Architectures, Methods and Tools (DSD 2008), 2008, 383-390.

[4]. Izadi, M. I.; Sadeghian, B.; Sadeghian, S. S.; Hanooki, H. A. "MIBS: A New Lightweight Block Cipher."; In: Garay, J. A., Miyaji, A., Otsuka, A. Editors, CANS'09, Springer-Vellag 2009, LNCS, 5888, 334-348.

[5]. Knudsen, L.; Leander, G.; Poschmann, A.; Robshaw, M. J. B. "PRINT Cipher: A Block Cipher for IC-Printing, Cryptographic Hardware and Embedded Systems."; CHES 2010, LNCS, 6225, 16-32.

[6]. Gong, Z.; Nikova, S.; Law, Y. W. "KLEIN: A New Family of Lightweight Block Ciphers."; FSE 2011, LNCS, 7055, 32-47.

[7]. Wu, W.; Zhang, L. "Lblock: A Lightweight Block Cipher."; ACNS 2011, LNCS, 6715, 327-344.

[8]. Feistel, H. "Cryptography and Computer Privacy."; Scientific American 1973, 228(5), 15-23.

[9]. Sung Kang, J. "Practical and Provable Security against Differential and Linear Cryptanalysis for Substitution-Permutation Networks."; ETRI Journal 2001, 23(4), 158-167.

[10]. Suzaki, T.; Minematsu, K. "Improving the Generalized Feistel."; In: Hong, S., Iwata, T. editors, FSE 2010, LNCS, 6147, 19–39.

[11]. Shibutani, K. "On the Diffusion of Generalized Feistel Structures Regarding Differential and Linear Cryptanalysis."; In: Biryukov, A.; Gong, G.; Stinson, D. R. Editors, SAC 2010 Springer, Heidelberg 2011, LNCS, 6544, 211–228.

[12]. Bogdanov, A. "On the Differential and Linear Efficiency of Balanced Feistel Networks."; Inf. Process. Lett. 2010, 110 (20), 861–866.

[13]. Bogdanov, A.; Shibutani, K. "Double SP-Functions: Enhanced Generalized Feistel Networks Extended Abstract."; ACISP 2011, LNCS, 6812, 106–119.

[14]. Kwon, D.; Kim, J.; Park, S.; Sung, S.; Sohn, H. Y.; Song, J.; Yeom, H. Y.; Yoon, E. J.; Lee, S.; Chee, D.; Han, D.; Hong, J. "New Block Cipher: ARIA."; In Jong L., Dong H. L., editors, ICISC 2003, LNCS, 2971, 432-445.

[15]. Ibrahim, S.; AziainiMarof, M. "Diffusion Analysis of a Scalable Feistel Network."; Proceeding in 3rd World nformatica Conference, Istanbul, Turkey, 2005, 5, 98-101.

[16]. Biham, E.; Shamir, A. "Differential Cryptanalysis of DES-Like Cryptosystems."; Advances in Cryptology, CRYPTO'90, Springer-Verlag, 1991, LNCS, 537, 2–21.

[17]. KIM, J.; Lee, C.; Sung, J.; Hong, S.; Lee, S.; Lim, J. "Seven New Block Cipher Structures with Provable Security against Differential Cryptanalysis."; IEICE Trans. Fundamentals 2008, E91-A(10), 3047-3058.

[18]. Wagner, D. "The Boomerang Attack."; 6th International Workshop on Fast Software Encryption (FSE'99), Springer-Verlag, 1999, 156-170.

[19]. Knudsen, L. R.; Wagner, D. "Integral Cryptanalysis."; 9th International Workshop on Fast Software Encryption, FSE 2002, Springer-Verlag 2002, LNCS, 2365, 9, 112-127.

پیوست

جدول‌های مربوط به جدول جانشینی ۴×۴ و جانشینی معادل SDS

جدول جانشینی معادل SDS

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	60	2	97	117	175	195	137	250	228	22	152	87	32	78	189	219
1	226	124	251	4	24	64	218	105	53	173	191	46	83	199	150	129
2	113	235	140	57	190	86	101	212	10	147	23	200	77	47	160	242
3	165	148	73	188	61	247	33	203	18	232	6	211	142	96	127	90
4	207	40	30	93	252	58	144	163	70	100	130	123	9	225	213	183
5	131	240	118	103	42	156	56	15	222	81	201	21	162	180	75	237
6	185	26	37	161	112	216	76	82	155	7	227	246	111	141	62	196
7	154	169	84	27	3	143	194	44	177	126	48	109	248	214	231	69
8	20	181	202	146	230	110	91	65	172	63	125	128	215	243	8	41
9	102	221	51	136	68	17	119	238	255	204	85	153	187	170	34	0
A	72	95	167	38	98	233	179	16	205	245	220	1	122	59	132	158
B	39	206	184	67	139	5	166	157	80	217	241	236	52	114	106	31
C	208	99	13	254	89	178	239	120	135	43	74	164	28	149	193	54
D	94	71	159	192	209	116	29	182	35	138	107	50	229	12	249	168
E	253	134	224	223	197	171	14	15	104	66	36	186	145	25	92	115
F	11	49	210	234	151	45	244	133	121	176	174	79	198	88	19	108

جدول جانشینی S1

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S1(x)	0	14	9	1	2	4	8	6	15	13	12	5	10	11	3	7