چهارمین کنفرانس انجمن رمز ایران
۲۴ الی ۲۶ مهر ماه ۱۳۸۶ دانشگاه علم و صنعت ایران
انجمن رمز ایران
Iranian Society of Cryptology

تحلیل تفاضلی الگوریتم رمز اَمین۱

نصور باقری
آزمایشگاه رمز و سیستمهای امن
دانشگاه علم و صنعت ایران
n_bagheri@iust.ac.ir

جواد مهاجری
پژوهشکده الکترونیک
دانشگاه صنعتی شریف
mohajer@sharif.edu

محمود سلماسی زاده
پژوهشکده الکترونیک
دانشگاه صنعتی شریف
salmasizadeh@sharif.edu

چکیده: در این مقاله الگوریتم رمز قطعه‌ای اَمین۱[1] در مقابل تحلیل تفاضل مورد بررسی قرار گرفته و بهترین مشخصهٔ قابل اعمال به یک ابر مرحله که دارای احتمالی برابر با 2^{-12} می باشد بدست می آید. برای الگوریتم اَمین۱ کاهش یافته به ٤ ابرمرحله از ۵ ابرمرحله، ۶ مشخصهٔ متفاوت با احتمال 2^{-115} معرفی می کنیم که با استفاده از 2^{117} زوج و بار محاسباتی از مرتبهٔ $O(2^{134})$، ۸۰ بیت از ۱۲۸ بیت زیر کلید دور آخر را بدست می دهد. ٤۸ بیت باقی مانده را می توان با جستجوی کامل بدست آورد. ۳ مشخصهٔ ۵ ابرمرحله ای با احتمال 2^{-193} معرفی می کنیم که برای بدست آوردن کلید دور آخر حداقل نیاز به 2^{195} زوج با تفاضل مورد نظر دارد که بسیار بیشتر از تعداد کل زوجهای ممکن با تفاضل خاص یعنی 2^{128} است. بنابراین این مشخصه ها اگر چه بهترین مشخصهٔ تفاضلی بدست آمده هستند، با این حال برای تحلیل ۵ ابر مرحله کارایی لازم را ندارد و نشان می دهد الگوریتم اَمین۱ با ۵ ابرمرحله، برای مشخصه های بدست آمده، در مقابل تحلیل تفاضلی مقاوم و این الگوریتم با ٤ ابرمرحله بسیار ضعیف است.

واژه‌های کلیدی: الگوریتم رمز امین ۱، رمز قطعه‌ای، تحلیل تفاضلی، الگوریتم کاهش یافته، مشخصه تفاضلی.

۱- مقدمه

تحلیل تفاضلی که برای اولین بار بوسیلهٔ بیهام و شامیر در [۱] معرفی شد می تواند برای تدارک یک حمله از نوع متن انتخابی بکار گرفته شود. طراحان الگوریتم اَمین ۱ اگرچه هیچ حاشیهٔ امنیتی برای پایداری این الگوریتم در مقابل این حمله ارائه نکرده اند ولی در دلایل خود برای انتخاب بخشهای مختلف این الگوریتم معیار پایداری در مقابل این حمله را به کرات تکرار کرده اند. ایدهٔ اصلی در این حمله این است که دو متن انتخابی با تفاضل $\Delta P = P_1 \oplus P_2$ می توانند متناظر با متن رمز شده C_1 و C_2 باشند، بطوریکه $\Delta C = C_1 \oplus C_2$ با یک احتمال مشخص، مقداری خاص را داشته باشد. چنین مشخصهٔ $(\Delta P, \Delta C)$ای می تواند برای بدست آوردن چندین بیت از کلید بکار گرفته شود. در تحلیل تفاضلی سعی می شود که مشخصه‌ای یافت شود که با بیشترین احتمال با یک خروجی خاص مرتبط گردد. هرچه احتمال منجر شدن یک تفاضل خاص در ورودی به یک تفاضل خاص در خروجی بیشتر باشد، می

[1] در مراجع [۳و۴] اسمی برای الگوریتم عنوان نشده بود که با نظر طراحان الگوریتم، اَمین ۱ بعنوان نام الگوریتم در نظر گرفته شد.

توان گفت امنیت الگوریتم در مقابل این حمله پایین تر است ولی برعکس این قضیه همواره صادق نیست چرا که ممکن است آن مشخصهٔ خاص که دارای بیشترین احتمال است توسط حمله کننده نادیده گرفته شده باشد. در واقع باید گفت که قلب حملهٔ تفاضلی پیدا کردن و استفاده از چنین مشخصه ای با احتمال بالا است. با توجه به اینکه اصل انتشار و فعال شدن بیشترین تعداد $Sbox$ها در این الگوریتم به خوبی لحاظ شده است، لذا باید مشخصهٔ معرفی شده به گونه ای باشد که مانع از فعال شدن $Sbox$های زیاد و در نتیجه کاهش احتمال مشخصه تفاضلی معرفی شده باشد[۱و۲].

در ادامهٔ این مقاله در بخش ۲ ساختار کلی الگوریتم رمز اَمین ۱ بصورت خلاصه معرفی می شود. در بخش ۳ به بررسی بلوکهای مختلف این الگوریتم و نتایج بدست آمده از شبیه سازی بخشهای مختلف می پردازیم. در بخش ٤ مشخصه های یک دوری که منجر به تولید یک مشخصهٔ کامل با احتمال بالا می شوند معرفی می شوند. در بخش ۵ مشخصهٔ تفاضلی الگوریتم کاهش یافته به ٤ ابرمرحله بررسی و توان حمله تجزیه و تحلیل می شود. در بخش ٦ نتیجه گیری و جمع بندی ارائه می شود.

۲- شرح کلی الگوریتم رمز اَمین ۱

۲-۱- تعاریف و علایم:

بایتها در این مقاله از سمت راست به چپ و از شمارهٔ یک نام گذاری میشوند. طبق این قرارداد $Sbox$ها را از راست به چپ و بصورت $S_1,\ldots,S_8$ نامگذاری می کنیم. ٤ بلوک P_1 استفاده شده در هر تابع F بصورت $P_{1-1},\ldots,P_{1-4}$ نامگذاری می شوند. باتوجه به اینکه در تابع F دو لایهٔ P_2 وجود دارد، بلوکهای P_2 اولین و دومین لایهٔ آنرا به ترتیب با $P_{21-1},\ldots,P_{21-4}$ و $P_{22-1},\ldots,P_{22-4}$ نامگذاری می کنیم. برای نامگذاری ورودیها و خروجیهای تفاضلی این بلوکها نیز از روشی مشابه استفاده می کنیم. بدین ترتیب برای نمایش ورودی تفاضلی به $Sbox$ شمارهٔ n از Δs_n^i و برای نمایش خروجی تفاضلی آن از ΔS_n^o استفاده می شود. بعنوان مثال پارامتر تفاضلی a مربوط به بلوک P_{22-3} با ΔP_{22-3}^a نمایش داده می شود. در کل این مقاله ⊕نمایشگر XOR، $>>>$ و $<<<$ به ترتیب نمایشگر چرخش بیتی یک بایت به تعداد مشخص، $+$و $\times$ نیز به ترتیب نمایشگر جمع و ضرب در $GF(2^8)$ هستند. برای یک تابع خاص اگر Xرا ورودی و Y را خروجی آن در نظر بگیریم، ΔX بیانگر تفاضل ورودی و ΔY بیانگر تفاضل خروجی این تابع است.

۲-۲- ساختار کلی الگوریتم رمز اَمین ۱

الگوریتم امین ۱ متشکل از ۵ ابر مرحله است. هر ابر مرحله از سه دور فایستل تشکیل شده است. دادهٔ ورودی به اولین ابر مرحله متن اصلی و داده خروجی از ابر مرحلهٔ شمارهٔ ۵ همان متن رمز شده است که باید به گیرنده ارسال شود. زیر کلیدهای استفاده شده در هر ابر مرحله با ابر مرحله های دیگر متفاوت و مختص همان ابر مرحله است. این زیر کلیدها در مرحلهٔ تولید زیر کلید تولید می شوند[۳و۴].

۲-۳- تابع F

تنها بخش غیر خطی الگوریتم امین۱ تابع F این الگوریتم است. ٦٤ بیت دادهٔ ورودی به این تابع ابتدا در قالب ۸ بایت که آنها را $b_1,\ldots,b_8$ می نامیم، قرار می گیرند. در این تابع ابتدا ۸ بایت ورودی به صورت جداگانه وارد تابعی موسوم به $Sbox$ می شوند. $Sbox$ استفاده شده در این الگوریتم، یک $Sbox$ جبری است که تحت رابطهٔ (۱) و در میدان $GF(2^8)$ عمل می کند.

$$S(x)=(x^{-1}\oplus a)^{-1} \qquad (۱)$$

۸ بایت خارج شده از ۸ $Sbox$ تحت یک عملیات خطی مشتمل بر XOR و چرخش بیتی قرار می گیرند و ۸ بایت ورودی به بخش بعدی تابع F یعنی P_1را تولید می کنند. هر بلوک P_1 دو بایت را بعنوان ورودیهای a وb می گیرد و دو بایت c و d را بعنوان خروجی تولید می کند. رابطهٔ بین ورودی و خروجی این بلوک را می توان بصورت زیر نوشت:

$$P_1(a,b)=\begin{cases} c=(2a+b)\oplus a \\ d=a+b \end{cases} \qquad (۲)$$

۸ بایت خروجی از٤ بلوک P_1 با هم ترکیب شده و ٤ بایت ورودی به لایهٔ بعدی تابع F، که ٤ بلوک P_2 هستند را تولید

می کنند. رابطهٔ بین ورودی و خروجی این تابع بصورت بیان شده در (۳) است.

$$P(a,b)=\begin{cases}c=2a+b\\ d=a+b\end{cases} \qquad (۳)$$

از ۸ بایت ورودی به بلوکهای P_2 ، ٤ بایت از ترکیب خروجی لایهٔ P_1 تولید می شود و برای ٤ بایت دیگر از زیر کلیدهای آن مرحله استفاده می شود. ۸ بایت خروجی از این لایه مجدداً با هم ترکیب می شوند و مشابه حالت قبلی وارد یک لایهٔ P_2 بعدی می شوند. ۸ بایت خروجی از این لایه وارد لایهٔ خروجی تابع F ، که عبور از $Sbox$ است، می شوند.

الگوریتم اَمین ۱ در انتهای هر ابر مرحله از یک جابجایی بایتی تحت عنوان BPP استفاده می کند. برای اطلاع بیشتر راجع به این جایگشت و بقیهٔ بخشهای الگوریتم، می توان به منابع [۳و۴] مراجعه کرد.

۳- بررسی پارامتر امنیت تفاضلی الگوریتم اَمین ۱

معمولاً برای تحلیل یک الگوریتم، هستهٔ اصلی آن بصورت دقیق مورد بررسی قرار می گیرد. به همین منظور رفتار تمام قسمتهای مختلف تابع F الگوریتم اَمین ۱ ، که تنها بخش غیر خطی آن است، بصورت جداگانه بررسی شد. در بررسی مشخصهٔ تفاضلی تابع $Sbox$ این الگوریتم نتایج درج شده در جدول ۱ بدست آمد.

جدول ۱. تعداد تفاضلها با فراوانی خاص

شاخص تفاضلی	0	2	4	6
تعداد	32893	32136	249	2

این جدول نشان می دهد که در اغلب موارد، احتمال ظهور یک مشخصهٔ خاص برای مشخصهٔ ورودی معلوم برابر است با $P=\frac{2}{256}=2^{-7}$ و این نشان می دهد که این $Sbox$ از مشخصهٔ تفاضلی نسبتاً خوبی برخوردار است.

در حملهٔ تفاضلی هرچه تعداد $Sbox$ فعال برای یک مشخصه تفاضلی بیشتر باشد تعداد بیتهای کلید که می توانند باز آوری شوند افزایش پیدا می کند در عوض احتمال مشخصهٔ تفاضلی پایین می آید و پیچیدگی حمله بالاتر می رود . بنابر این ما سعی می کنیم که در مراحل میانی کمترین تعداد $Sbox$ فعال را داشته باشیم. برای این منظور سعی می کنیم مشخصه های تفاضلی مورد نظر را بگونه ای انتخاب کنیم که تنها $Sbox$ ورودی تابع F را تحت تأثیر قرار دهند و در لایه های میانی این تابع به مشخصهٔ صفر برسیم. برای این منظور، اگر بتوانیم شرایط قید شده برای P_1 یا P_2 در (٤) را ایجاد کنیم می توانیم مطمئن باشیم که مشخصهٔ تفاضلی ورودی به لایهٔ بعدی تابع F و به تبع آن مشخصهٔ خروجی تابع با احتمال ثابت صفر می شود.

$$\begin{cases}\Delta P^{c}_{1-1}=\Delta P^{d}_{1-3}\\ \Delta P^{d}_{1-1}=\Delta P^{c}_{1-3}\end{cases} \qquad (۴-a)$$

$$\begin{cases}\Delta P^{c}_{1-2}=\Delta P^{d}_{1-4}\\ \Delta P^{d}_{1-2}=\Delta P^{c}_{1-4}\end{cases} \qquad (۴-b)$$

$$\begin{cases}\Delta P^{c}_{21-1}=\Delta P^{d}_{21-4}\\ \Delta P^{d}_{21-1}=\Delta P^{c}_{21-4}\end{cases} \qquad (۴-c)$$

$$\begin{cases}\Delta P^{c}_{21-2}=\Delta P^{d}_{21-3}\\ \Delta P^{d}_{21-2}=\Delta P^{c}_{21-3}\end{cases} \qquad (۴-d)$$

برخلاف $Sbox$ این تابع که مشخصهٔ مناسبی برای تحلیل تفاضلی ندارد، بلوکهای P_1 و P_2 بدلیل خطی بودن مشخصه ها تفاضلی با فراوانی بسیار بالایی را نتیجه می دهند. با توجه به اینکه تعداد حالتهای ممکن بسیار زیاد هستند، لذا در جداول ۲ تنها برخی از تفاضلهای ورودی و خروجی غیر صفر که در محاسبهٔ مشخصه های تفاضلی مورد نیاز کاربرد دارند آمده است.

همانگونه که در جدول ۲ مشاهده می شود، اگر چنانچه یکی از تفاضلهای ورودی ΔP_1^a یا ΔP_1^b برابر با ۱۲۸ باشد و تفاضل دیگر برابر با صفر باشد، در چنین شرایطی با احتمال $P=1$ خروجیهای ΔP_1^c و ΔP_1^d برابر با ۱۲۸ می شوند.

٤- پیدا کردن مشخصه های تفاضلی

٤-۱- مشخصهٔ تفاضلی یک دوری

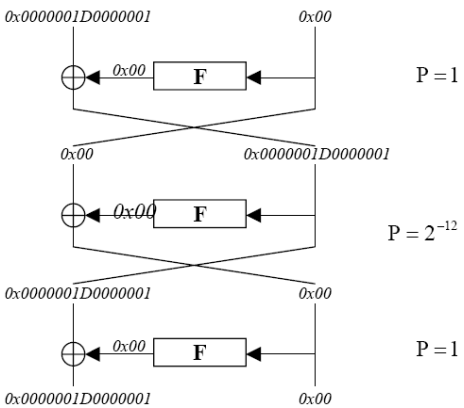
الف): در نظر بگیرید که رشتهٔ ورودی به تابع F به گونه ای انتخاب شود که $\Delta S_1^i=0x7A$ و $\Delta S_5^i=0x7A$ و بقیهٔ

ΔS^iها برابر با صفر باشند ، در این صورت ΔS_1^o و ΔS_5^o هر کدام با احتمال $P = \frac{4}{256} = 2^{-6}$ برابر با $0x80$ می شوند. این دو بایت به ترتیب بعنوان ΔP_{1-1}^b و ΔP_{1-3}^b وارد مرحلهٔ بعد می شوند. این درحالی است که بدلیل صفر بودن بقیه ΔS^iها، بقیه تفاضلهای ورودی به ΔP_1^a و ΔP_1^b برابر با صفر هستند. از طرفی با مراجعه به جدول ۲ مشاهده می کنیم که اگر $\Delta P_1^b = 0x80$ و $\Delta P_1^a = 0x00$ باشد، آنگاه $\Delta P_1^c = 0x80$ و $\Delta P_1^d = 0x80$ با احتمال $P = 1$، برابر با $0x80$ می شود. با مراجعه به معادلهٔ (٤) می بینیم در این شرایط(4-a) و(4-b) برقرار هستند و این یعنی اینکه می توانیم مطمئن باشیم که مشخصهٔ تفاضلی ورودی به لایهٔ بعدی تابع F صفر خواهد بود. بنابر این احتمال کل این مشخصه برابر است با :

$$P = (2^{-6})^2 = 2^{-12} \qquad (۵)$$

مطابق شکل ۱ و با انتخاب مشخصهٔ ورودی مناسب می توان این احتمال را برای یک ابر مرحله نیز حفظ کرد.

اگر چنانچه الگوریتم اَمین ۱ فاقد عملگر BPP بود، در این صورت می توانستیم این مشخصه تک ابر مرحله ای بدست آمده را برای تعداد ابر مرحلهٔ بیشتر نیز تکرار کنیم که نتیجتاً بعنوان مثال برای یک الگوریتم ۵ ابر مرحله ای اَمین ۱ بدون وجود BPP به مشخصه تفاضلی با احتمال $P = (2^{-12})^5 = 2^{-60}$ می رسیدیم که الگوریتم بسیار ضعیف می شد.



شکل ۱. مشخصهٔ تک ابر مرحله ای برای الگوریتم اَمین ۱

ب): در نظر بگیرید که رشتهٔ ورودی به تابع F به گونه ای انتخاب شود که $\Delta S_3^i = 0x1D$ [۲] و $\Delta S_5^i = 0x1D$ و بقیهٔ ΔS^iها برابر با صفر باشند ، در این صورت مشابه با رویهٔ قبلی، ΔS_3^o و ΔS_5^o هر کدام با احتمال $P = \frac{2}{256} = 2^{-7}$ برابر با $0x80$ می شوند که در نتیجه با توجه به شکل۲ این مشخصه با احتمال $P = 2^{-14}$ منجر به تفاضل تمام صفر در خروجی می شود.

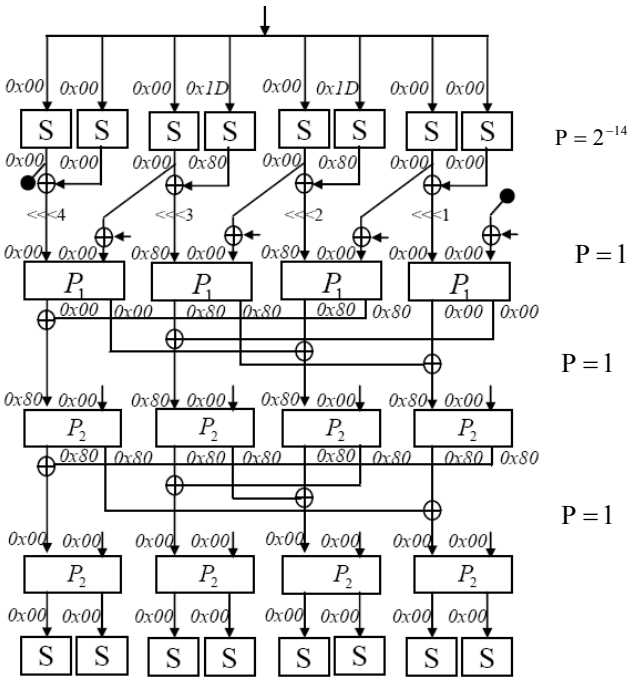
جدول ۲. بخشی از جدول توزیع تفاضلهای بلوک P_1

ΔP_1^a	ΔP_1^b	ΔP_1^c	ΔP_1^d	فراوانی	احتمال
0x0C	0x00	0xF4	0x0C	2048	$P=2^{-5}$
0x52	0x00	0xB6	0xB2	512	$P=2^{-7}$
0x80	0x00	0x80	0x80	65536	P=1
0x88	0x00	0x98	0x88	16384	$P=2^{-2}$
0x8c	0x00	0x84	0x84	8192	$P=2^{-3}$
0xF4	0x00	0x0C	0xF4	2048	$P=2^{-5}$
0x00	0x64	0x9C	0x9C	256	$P=2^{-8}$
0x00	0x80	0x80	0x80	65536	P=1
0x00	0x88	0x88	0x88	16384	$P=2^{-2}$
0x00	0x92	0xB2	0xB6	512	$P=2^{-7}$
0x00	0xA4	0xAC	0x6C	512	$P=2^{-7}$
0x00	0xA7	0xAB	0xA9	512	$P=2^{-7}$
0x00	0xE9	0xA9	0xAB	512	$P=2^{-7}$
0x00	0x01	0x01	0x01	32768	$P=2^{-1}$
0x00	0x6C	0xAC	0xAC	1024	$P=2^{-6}$
0x00	0x80	0x80	0x80	65536	P=1
0x00	0x81	0x81	0x81	32768	$P=2^{-1}$
0x00	0x84	0x84	0x84	16384	$P=2^{-2}$
0x00	0x88	0x88	0x88	16384	$P=2^{-2}$
0x00	0x98	0x88	0x88	8192	$P=2^{-3}$
0x00	0x9C	0x84	0x84	4096	$P=2^{-4}$
0x00	0xAC	0xAC	0xAC	2048	$P=2^{-5}$
0x00	0xB2	0x92	0x92	2048	$P=2^{-5}$
0x00	0xB2	0xB2	0xB2	2048	$P=2^{-5}$
0x00	0xB6	0x92	0x92	1024	$P=2^{-6}$
0x00	0xB6	0xB2	0xB2	1024	$P=2^{-6}$

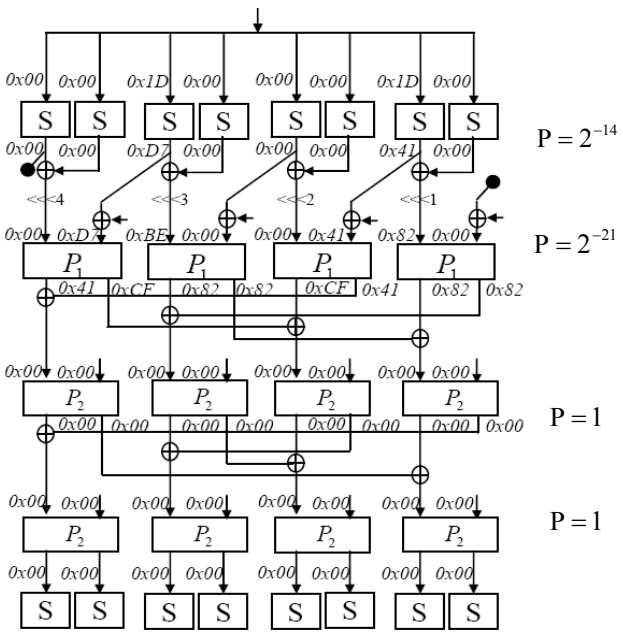
ج): در این سناریو یک حالت دیگر را در نظر میگیریم. فرض کنید رشتهٔ ورودی به تابع F به گونه ای انتخاب شود که

[۲] اگر بجای تفاضل ورودی $0x1D$ از $0x74$ یا $0x9F$ نیز استفاده کنیم. مشخصهٔ خروجی از احتمال مشابهی برخوردار خواهد بود.

$\Delta S_2^i = 0x1D$ و $\Delta S_6^i = 0x1D$ و بقیهٔ ΔS^iها برابر با صفر باشند ، در این صورت ΔS_2^o و ΔS_6^o هر کدام با احتمال $P = \frac{2}{256} = 2^{-7}$ به ترتیب برابر با $0x41$ و $0xD7$می شوند. با توجه به شکل ۳ این مشخصه با احتمال $P = 2^{-35}$ منجر به تفاضل تمام صفر در خروجی این مرحله می شود.



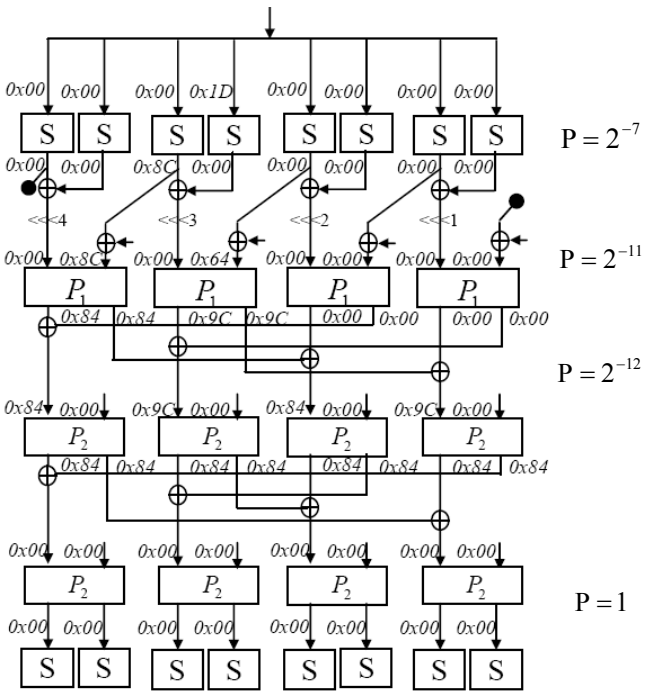
شکل ۲. رویهٔ درنظر گرفته شده در (ب)



شکل ۳. رویهٔ درنظر گرفته شده در (ج)

د): در این مرحله مشخصهٔ ورودی را طوری در نظر می گیریم که $\Delta S_3^i = 0x1D$ و $\Delta S_4^i = 0x1D$ و بقیهٔ ΔS^iها برابر با صفر باشند ، در این صورت ΔS_3^o و ΔS_4^o هر کدام با احتمال $P = \frac{2}{256} = 2^{-7}$ به ترتیب برابر با $0xA0$ و $0x80$می شوند. با روندی مشابه با شکل ۲ این مشخصه با احتمال کلی برابر با $P = (2^{-7})^2 = 2^{-14}$ منجر به تفاضل تمام صفر در خروجی می شود.

ر): مشخصهٔ ورودی را به گونه ای تغییر می دهیم که تنها یکی از حالات $\Delta S_6^i = 0x1D$ یا $\Delta S_8^i = 0x1D$ روی دهد. ابتدا حالت $\Delta S_6^i = 0x1D$ را در نظر می گیریم. این حالت تقریباً شبیه سناریو (د) است با این تفاوت که در اینجا خروجی یک $Sbox$ وارد دو بلوک P_1 می شود. در این حالت و با توجه به شکل ۴ با احتمالی برابر با $P = 2^{-30}$ مشخصهٔ خروجی تماماً صفر می شود.



شکل ۴. رویهٔ درنظر گرفته شده در (ر)

ز): در حالت بعد فرض می کنیم تنها $\Delta S_8^i = 0x1D$ باشد. در این حالت نیز می توانیم با احتمال $P = \frac{2}{256} = 2^{-7}$ انتظار $\Delta S_8^o = 0x88$ را داشته باشیم. بنابر این با توجه به شکل ۵ و با احتمالی برابر با $P = 2^{-20}$ می توانیم به مشخصهٔ خروجی تمام

صفر برسیم.

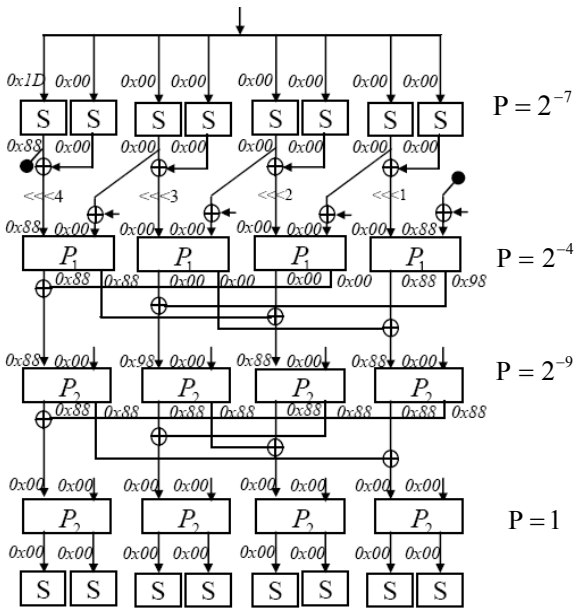
۴-۲- مشخصهٔ تفاضلی ۵ ابر مرحله ای

مشخصهٔ ورودی به تابع F را به صورت زیر در نظر می گیریم:

$$\{0x00,0x00,0x1D,0x00,0x00,0x00,0x1D,0x00;\ 0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00\} \quad (۶)$$

در این حالت می توان گفت $\Delta S_2^i = 0x1D$ و $\Delta S_6^i = 0x1D$ و بقیهٔ ΔS^iها برابر با صفر هستند. با توجه به رویهٔ (ج) می توان با احتمالی مشابه یعنی $P = 2^{-35}$ به مشخصهٔ تمام صفر در خروجی رسید. از آنجایی که مشخصهٔ غیر صفر در نیمهٔ سمت چپ قرار دارد، لذا این احتمال می تواند بعنوان مشخصه تفاضلی اولین ابر مرحله نیز لحاظ شود. در اثر عبور مشخصه از تابع BPP مشخصه تغییر کرده و به این صورت در می آید:

$$\{0x00,0x00,0x00,0x1D,0x00,0x1D,0x00,0x00;\ 0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00\} \quad (۷)$$



شکل ۵. رویهٔ درنظر گرفته شده در (ز)

در این حالت $\Delta S_3^i = 0x1D$ و $\Delta S_5^i = 0x1D$ و بقیهٔ ΔS^iها برابر با صفر هستند. با توجه به رویهٔ (ب) می توان با احتمال $P_2 = (2^{-7})^2 = 2^{-14}$ به مشخصهٔ تمام صفر در خروجی رسید. در هنگام ورود به ابر مرحلهٔ سوم، در اثر عبور مشخصه از تابع BPP مجدداً مشخصه تغییر کرده و به صورت زیر در می آید:

$$\{0x00,0x00,0x1D,0x00,0x00,0x00,0x00,0x00;\ 0x1D,0x00,0x00,0x00,0x00,0x00,0x00,0x00\} \quad (۸)$$

در این حالت از مشخصهٔ سمت راست $\Delta S_8^i = 0x1D$ و از مشخصهٔ سمت چپ $\Delta S_6^i = 0x1D$ است و بقیهٔ ΔS^iها برابر با صفر هستند. بنابراین می توان گفت برای مشخصهٔ ورودی به تابع F اولین و سومین دور فایستل این ابر مرحله $\Delta S_8^i = 0x1D$ و بقیهٔ ΔS^iها برابر با صفر است. با توجه به رویهٔ (ر) مشخصه خروجی این دورها نیز با احتمال $P = 2^{-20}$ برابر صفر می شوند.

برای مشخصهٔ تفاضلی ورودی به دومین دور فایستل این ابر مرحله $\Delta S_6^i = 0x1D$ و بقیهٔ ΔS^iها برابر با صفر است. بنابراین و با توجه به رویهٔ (ر) می توان گفت با احتمال $P = 2^{-30}$ مشخصهٔ تفاضلی خروجی این دور فایستل برابر با صفر می شود. در کل احتمال مورد انتظار برای مشخصهٔ تفاضلی در سومین ابر مرحله برابر خواهد بود با:

$$P_3 = 2^{-20} \times 2^{-30} \times 2^{-20} = 2^{-70} \quad (۹)$$

مشابه با بقیهٔ ابر مرحله ها مشخصهٔ خروجی سومین ابر مرحله نیز از تابع BPP عبور خواهد کرد و نتیجتاً مشخصهٔ تفاضلی ورودی به چهارمین ابر مرحله به این صورت است:

$$\{0x00,0x00,0x00,0x00,0x1D,0x1D,0x00,0x00;\ 0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00\} \quad (۱۰)$$

با توجه به این مشخصه متوجه می شویم که سمت چپ این مشخصه، همان مشخصهٔ مورد انتظار برای تدارک رویهٔ (د) است. بنابراین و باتوجه به صفر بودن سمت راست این مشخصه می توانیم احتمال مشخصهٔ تفاضلی این ابر مرحله را $P_4 = 2^{-14}$ در نظر بگیریم. در نهایت مشخصهٔ خروجی با عبور از تابع BPP به صورت ذکر شده در زیر در می آید و وارد آخرین ابر مرحله یعنی ابرمرحلهٔ ۵ می شود.

$$\{0x1D,0x00,0x00,0x00,0x00,0x00,0x00,0x00;\ 0x1D,0x00,0x00,0x00,0x00,0x00,0x00,0x00\} \quad (۱۱)$$

در این حالت نیز مشابه مشخصهٔ ورودی به ابر مرحلهٔ شماره ۳ هم در نیمهٔ سمت چپ و هم در نیمهٔ سمت چپ مقدار غیر صفر داریم. اما در اینجا هم برای نیمهٔ سمت راست و هم نیمهٔ سمت

چپ $\Delta S_8^i = 0x1D$ و بقیهٔ ΔS^iها برابر با صفر هستند. بنابراین می توان گفت برای مشخصهٔ ورودی به تابع F اولین و دومین و سومین دور فایستل این ابر مرحله $\Delta S_8^i = 0x1D$ و بقیهٔ ΔS^iها برابر با صفر است. این همان مشخصه های مورد انتظار در رویهٔ (ر) است که با احتمال $P = 2^{-20}$ منجر به مشخصهٔ صفر در خروجی تابع F می شود. بنابراین انتظار داریم که در نهایت احتمال مشخصهٔ بیان شده در این ابر مرحله به این صورت باشد:

$$P = 2^{-20} \times 2^{-20} \times 2^{-20} = 2^{-60} \qquad (۱۲)$$

نتیجتاً با توجه به مطالب بالا می توان گفت احتمال بدست آمده برای این مشخصهٔ تفاضلی ۵ ابرمرحله ای به این صورت است:

$$P_t = \prod_{i=1}^{5} P_i = 2^{-35} \times 2^{-14} \times 2^{-70} \times 2^{-14} \times 2^{-60} = 2^{-193} \qquad (۱۳)$$

و مشخصهٔ نهایی پس از عبور از تابع BPP پنجمین ابر مرحله، که همان مشخصهٔ خرجی است، به این صورت در می آید:

$$\{0x00,0x00,0x00,0x00,0x1D,0x00,0x00,0x00; \\ 0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x1D\} \qquad (۱۴)$$

۵- تحلیل تفاضلی الگوریتم اَمین ۱ کاهش یافته

در قسمت قبل یک مشخصهٔ تفاضلی ۵ ابر مرحله ای با احتمال $P_t = 2^{-193}$ بدست آمد. بنابراین برای بدست آوردن زیر کلید دور آخر، حداقل نیاز به 2^{195} زوج با تفاضل مشخص داریم که بسیار بیشتر از کل زوجهای ممکن با تفاضل خاص یعنی 2^{128} است. بنابر این بصورت کلی می توان گفت برای بهترین مشخصهٔ تفاضلی بدست آمده الگوریتم اَمین۱ در مقابل تحلیل تفاضلی پایدار است. در این بخش یک مشخص تفاضلی برای تحلیل الگوریتم اَمین۱ کاهش یافته به ٤ ابر مرحله معرفی می کنیم. اگر چنانچه مشخصهٔ ورودی به اولین ابرمرحله را بصورت زیر درنظر بگیریم:

$$\{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00; \\ 0x2D,0x2D,0x00,0x00,0x00,0x00,0x00,0x00\} \qquad (۱۵)$$

در اینصورت اگر روندی مشابه با رویهٔ انجام شده در بخش قبل را طی کنیم،مطابق با جدول ۳ با احتمالی برابر با 2^{-115} برای این مشخصه می رسیم. اگر تفاضل دور آخر را با تفاضلهای ممکن حاصل از تفاضل مورد انتظار در ورودی توابع $Sbox$ مقایسه کنیم، می توانیم زوج های نامناسب یا غلط را کنار گذاشته و برای تحلیل بکار نگیریم . از میان زوجهای موجود زوجهایی که تفاضل آنها برابر با تفاضل مورد انتظار در دور آخر یعنی[۳]:

$$\{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00; \\ 0x00,0x00,0x00,0x00,0x00,0x2D,0x00,0x2D\} \qquad (۱۶)$$

نباشد، به عنوان زوج نامناسب تشخیص داده می شوند. اگر چنانچه احتمال رخداد تمامی 2^{64} خروجی ممکن را یکسان در نظر بگیریم، در این صورت با احتمال 2^{-64} تفاضل خروجی یک تفاضل درست تشخیص داده می شود. اگر احتمال رخداد هر یک از 2^8 مقدار ممکن در خروجی $Sbox$ ها را یکسان فرض کنیم در این صورت با توجه به اینکه ورودی ٦ عدد $Sbox$ برابر با صفر است، پس زوج بدست آمده در این مرحله با احتمال $\left(2^{-8}\right)^6$ دور ریخته نمی شود. پس از مقایسهٔ تفاضلهای بدست آمده برای هر زوج مورد بررسی با تفاضل مورد انتظار در خروجی و فرض توزیع یکنواخت تفاضلهای خروجی احتمال اینکه زوج بدست آمده بعنوان زوج غلط شناسایی نشود برابر است با:

$$\beta = \left(2^{-8}\right)^6 \times 2^{-64} = 2^{-112} \qquad (۱۷)$$

از طرفی با توجه به تفاضل ورودی دور آخر، تنها تفاضل ورودی به $Sbox$های ششم و هشتم مخالف صفر است، بنابراین تنها زیر کلیدهای متناظر با آن یعنی ١٦ بیت شمارش می شوند پس $\alpha \le 2^{16}$. از طرفی با توجه به تعریف تابع F، برای این مشخصه، مجموعاً ٧٢ بیت کلید قابل بازیابی خواهد بود که ١٦ بیت با ورودی $Sbox$های ششم و هشتم XOR شده اند و ٥٦ بیت آن در تعریف توابع P_1 و P_2 بکار می روند. نتیجتاً معیار سیگنال به نویز برای این حمله، با توجه به تعریف ارائه شده در [۱،۲،۵و٦]، بصورت زیر خواهد بود:

[۳] اگر در مشخصهٔ ورودی مقدار2D را با یکی از مقادیر{0x3C,0x60,0x6C,0Xd9,0xE8} را جایگزین کنیم نیز با روندی مشابه به مشخصه ای با احتمال یکسان می رسیم.

$$S/N = \mathrm{P}.2^{K}/\alpha.\beta \geq \frac{2^{-115}\times 2^{80}}{2^{-112}\times 2^{16}} = 2^{61} \qquad (۱۸)$$

برای چنین سیگنال به نویز بالایی تنها نیاز به ۳ الی ٤ متن صحیح داریم[۱،۲،۵و٦]. در نتیجه لازم است $2^{115}\times 2^{2} = 2^{117}$زوج متن واضح با تفاضل مورد نظر بررسی شوند. در نتیجه باید متناظر با هر مقدار زیر کلید $2^{117}\times 2 = 2^{118}$ عملیات وارون انجام شود. بنابراین پیچیدگی محاسباتی برای پیدا کردن ۸۰ بیت از کلید متناظر با دو دور آخر ابر مرحلهٔ چهارم از مرتبهٔ $O(2^{118+16})$ است که نسبت به فضای جستجوی کامل یعنی 2^{256} کاهش بسیار زیادی را نشان می دهد. جدول ۳ خلاصهٔ تحلیل انجام شده برای الگوریتم کاهش یافته را نمایش می دهد. که در این حالت مشخصهٔ خروجی با احتمالی برابر با $۲^{-۱۱۵}$ بصورت زیر خواهد بود:

$$\{L=0x000000000000002D;\ R=0x00000000002D0000\} \qquad (۱۹)$$

جدول ۳. مقدار احتمال مربوط به هر ابرمرحله در تحلیل الگوریتم کاهش یافته به ۴ ابر مرحله

ابرمرحله	مشخصهٔ ورودی به ابر مرحله	احتمال
۱	$\{L=0x2D2D000000000000;\ R=0x0000000000000000\}$	$\mathrm{P}=2^{-28}$
۲	$\{L=0x000000002D\ 002D\ 00;\ R=0x0000000000000000\}$	$\mathrm{P}=2^{-38}$
۳	$\{L=0x002D\ 002D\ 00000000;\ R=0x0000000000000000\}$	$\mathrm{P}=2^{-14}$
٤	$\{L=0x2D\ 002D\ 0000000000;\ R=0x0000000000000000\}$	$\mathrm{P}=2^{-35}$

۶- نتیجه گیری

در این مقاله امنیت الگوریتم اَمین ۱ در مقابل تحلیل تفاضلی مورد ارزیابی قرار گرفت. نشان داده شد بهترین مشخصهٔ یک ابرمرحله ای ممکن برای یک ابر مرحله از این الگوریتم دارای احتمالی برابر با $۱۲^{-۱۲}$ است. بدلیل وجود تابع BPP در ساختار این الگوریتم امکان تعمیم این مشخصه به تعداد ابرمرحلهٔ بیشتر با احتمال مناسب وجود ندارد. با توجه به ساختار الگوریتم بنظر می رسد معرفی یک مشخصهٔ تفاضلی تکرار پذیر با احتمال مناسب وجود نداشته باشد. در این مقاله با توجه به ساختار الگوریتم سعی شد یک مشخصهٔ ۵ ابر مرحله ای که از بیشترین احتمال ممکن برخوردار باشد، ارائه گردد. ۳ مشخصهٔ ۵ ابرمرحله ای با احتمال مشابه $۲^{-۱۹۳}$ برای الگوریتم بدست آمد، که کارایی لازم برای تحلیل الگوریتم کامل را نداشت.

در ادامه یک مشخص تفاضلی برای تحلیل الگوریتم اَمین۱ کاهش یافته به ۴ ابر مرحله معرفی شد که با استفاده از $۲^{۱۱۷}$ زوج متن با تفاضل مورد نظر و بار محاسباتی از مرتبهٔ $O(۲^{۱۳۴})$ ، ۸۰ بیت زیر کلید دور آخر را بازیابی می کند که ۴۸ بیت باقی مانده را می توان با جستجوی کامل بدست آورد. بررسی این الگوریتم نشان می دهد که تابع BPP و جایگشتهای بیتی استفاده شده برای نامتوازن کردن، علی رقم ساده بودن تأثیر بسیار بالایی در افزایش امنیت این الگوریتم در مقابل حملهٔ تفاضلی داشته اند.

۷- مراجع

[1] E.Biham, A.Shamir "Differential Cryptanalysis of DES-like Cryptosystems", Crypto1990, Lecture Notes in Computer Science 537, Springer, pp. 2-21, 1991.

[2] B.V.Rompay, L.R.Knudsen, V.Rijmen" Differential Cryptanalysis of the ICE Encryption Algorithm", FSE 1998, Lecture Notes in Computer Science 1372, Springer, pp.270-283,1998.

[۳] اَ.عبدلی ، م.نادری ،"ارائهٔ یک الگوریتم رمز قطعه ای مقاوم در مقابل تحلیل های تفاضلی و خطی"، سومین کنفرانس انجمن رمز ایران، ص. ۳۳-۴۴، اصفهان، دی ۱۳۸۲.

[٤] اَ.عبدلی ،"طراحی و پیاده سازی یک الگوریتم رمز قطعه ای"، پایان نامهٔ کارشناسی ارشد، دانشگاه علم و صنعت ایران شهریور ۱۳۸٤.

[۵] م.ر. یارندی ،ع.میرقدری، ج.مهاجری ،"حملهٔ تفاضلی کارآمد به الگوریتم رمز قطعه ای فجر۱ "، سومین کنفرانس انجمن رمز ایران، ص. ۴۵-۵۴، اصفهان، شهریور ۱۳۸٤.

[٦] ع.قائمی بافقی، ب. صادقیان ،"تحلیل تفاضلی الگوریتم رمز قطعه ای آی ای اس ۸۰"، دهمین کنفرانس سالانهٔ انجمن کامپیوتر ایران، تهران، بهمن ۱۳۸۳.