باسمه تعالی

گزارش پروژه دوم درس معماشناسی کاربردی

موضوع سمینار:

تحلیل تفاضلی و خطی بر روی دو دور از سیستم رمز متقارن قطعه‌ای Twofish

نگارندگان:

سید محمد مهدی احمدپناه ۹۴۱۳۱۰۸۶

سید امیر حسین ناصرالدینی ۹۴۱۳۱۰۱۹

استاد:

دکتر بابک صادقیان

پاییز ۱۳۹۴

فهرست مطالب

معرفی و کلیات

تحلیل‌های تفاضلی و خطی، دو حمله بسیار پرکاربرد بر روی سیستم‌های رمز قطعه‌ای کلید متقارن هستند. تحلیل خطی توسط ماتسویی در سال ۱۹۹۳به عنوان یک حمله تئوری معرفی شد که بعدها به صورت عملی نیز مورد استفاده قرار گرفت. تحلیل تفاضلی اولین بار توسط بیهام و شامیر در سال ۱۹۹۰ ارائه شد.

تحلیل خطی سعی دارد تا از احتمال بالای وقوع عبارات خطی شامل بیت‌های متن واضح، بیت‌های متن رمزشده و بیت‌های زیرکلید بهره ببرد. یک حمله متن واضح معلوم است، که در آن مهاجم مجموعه‌ای از متن‌های واضح و متن‌های رمزشده متناظر آن‌ها را داراست. گرچه مهاجم هیچ راهی ندارد تا بداند کدام متن واضح و متن رمزشده متناظر آن در دسترس است. در بسیاری از کاربردها و سناریوها، می‌توان چنین فرض کرد که مهاجم مجموعه‌ای از متن‌های واضح دلخواه و متن‌های رمزشده متناظر آن‌ها را در نظر می‌گیرد. در حالی که تحلیل تفاضلی سعی دارد از تفاضل میان بیت‌های ورودی و تفاضل بیت‌های متن‌های رمز شده حاصل از آنها اطلاعاتی را استنتاج کند و از این اطلاعات برای به دست آوردن بخشی از بیت‌های کلید سیستم رمز استفاده کند. در ادامه بررسی‌ها و تحلیل‌های انجام شده بر روی سیستم رمز متقارن قطعه‌ای Twofish ذکر شده است.

فصل اول: سیستم رمزنگاری متقارن قطعه‌ای Twofish

معرفی کلی سیستم

سیستم رمز متقارن Twofish یک سیستم رمز قطعه‌ای است که در طراحی آن از ساختار فایستل بهره-گیری شده است. این سیستم رمز ۱۶ دور است. تابع F در این سیستم رمز یک تابع پوشاست. قطعه‌های ورودی ۱۲۸بیت و خروجی نیز یک قطعه‌ی ۱۲۸بیتی است. در نسخه اولیه این سیستم رمز کلید ۱۲۸بیتی است، اما امکان استفاده از کلید های با طول بیشتر تا ۲۵۶ بیت نیز وجود دارد. [1]

معرفی S-box

یک S-box یک جابجایی غیرخطی است که غالبا به صورت یک جدول نمایش داده می‌شود. استفاده از S-box ها در سیستم‌های رمز قطعه‌ای امری شایع است. S-box ها در تعداد بیت‌های ورودی و خروجی، تنوع زیادی دارند. و شیوه ساخت آنها می‌تواند به صورت بی‌قاعده[۱] و یا بر اساس الگوریتم خاصی باشد. S-box اولین بار در سیستم رمز Lucifer مورد استفاده قرار گرفت و سپس در سیستم رمز DES و پس از آن در غالب سیستم‌های رمز نگاری مورد استفاده قرار گرفته است. سیستم رمز Twofish از چهار S-box متفاوت که دارای ویژگی‌های زیر هستند بهره می‌برد:

- ۸-بیت ورودی
- ۸-بیت خروجی
- وابسته به کلید
- پوشا[۲] (احتمال تبدیل ورودی به هر کدام از مقادیر فضای برد[۳] وجود دارد)

ساختار سیستم

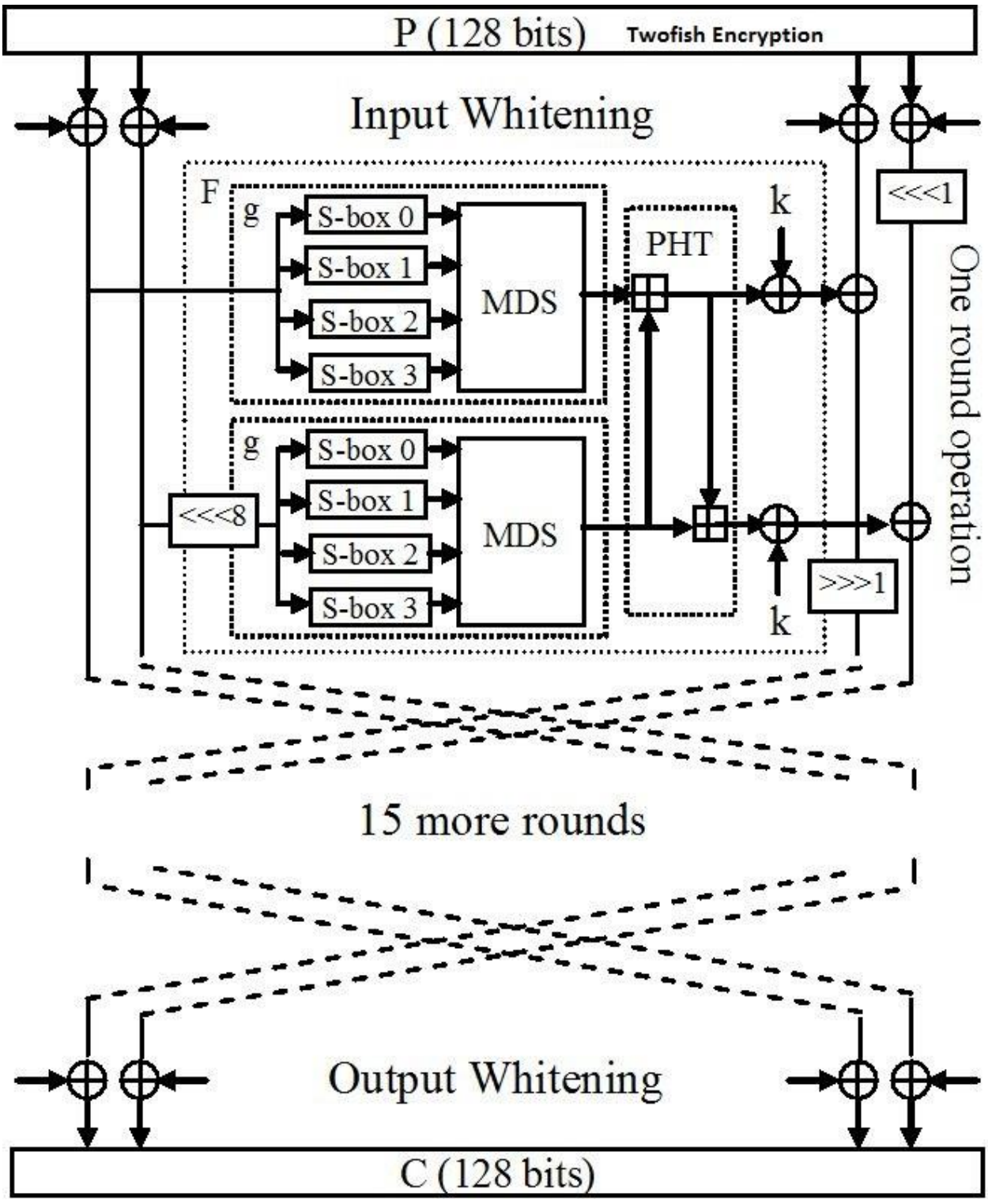
ساختار به صورت فایستل به همانند شکل زیر است:

---

۱ Randomly

۲ Bijective

۳ Range


P (128 bits)
Twofish Encryption
Input Whitening
F
g
S-box 0
S-box 1
S-box 2
S-box 3
MDS
PHT
k
<<<1
One round operation
g
S-box 0
S-box 1
S-box 2
S-box 3
MDS
<<<8
>>>1
k
15 more rounds
Output Whitening
C (128 bits)

فصل دوم: تحلیل بر روی سیستم رمزنگاری قطعه‌ای Twofish

تحلیل تفاضلی

اولین روش موثر تحلیل سیستم‌های رمز قطعه‌ای در اواخر دهه ۱۹۸۰ میلادی توسط آقایان بیهام[۴] و شامیر[۵] مطرح شد، که بر روی الگوریتم رمز FEAL برای به دست آوردن نقاط ضعف این الگوریتم پیاده سازی شده بود. این روش که تحلیل تفاضلی[۶] نام داشت در سال ۱۹۹۰ به صورت کلی مطرح شد و در همان سال بر روی نسخه کاهش یافته DES ارائه شد. در سال ۱۹۹۱ سرانجام این تحلیل بر روی نسخه کامل ۱۶دور DES اعمال شد و نتایج آن برای شکستن سیستم رمز، بسیار سریع تر از جستجوی جامع[۷] بود. ایده کلی در این نوع تحلیل استفاده از تفاوت‌های میان ورودی‌ها و نتایج حاصله از این تفاوت‌ها در خروجی است. بدین وسیله تحلیل‌گر در صدد استنباط اطلاعات از این تفاوت‌های موجود و نتایج به دست آمده است.

این تحلیل بر اساس تفاوت‌های موجود در قطعه‌های ورودی و بررسی نتایج به دست آمده در خروجی شکل می‌گیرد. در تحلیل انجام شده ابتدا با توجه به کلید داده شده (کلید: 0123456789ABCDEFFEDCBA9876543210) XOR Profile مورد نیاز برای تحلیل به دست می‌آید. XOR Profile برای ۴ S-Box سیستم رمز با توجه به کلید، تولید شده و در پیوست به صورت کامل بیان شده اند. پس از تولید XOR Profile مشخصه‌های تفاضلی برای ادامه تحلیل استخراج شده؛ همچنین یک مشخصه تفاضلی نیز از مقاله[2] استخراج شد. پس از استخراج برای تحلیل دو دور از سیستم رمز، متن رمز شده تا پایان دور اول(U) را به دست می‌آوریم، همچنین متن رمز شده تا پایان دور دوم(C) نیز به دست آورده شد. حال با تست $۲^{۱۶}$ جفت تلاش برای به دست آوردن تعدادی از بیت‌های کلید اینگونه صورت گرفت که، تمام حالات مختلف بیت‌های متناظر بیت‌های فعال Uرا در کلید امتحان کردن و XOR C می‌کنیم، و مراحل سیستم رمز در دور دوم را به صورت معکوس انجام داده احتمال درستی کلیدهای مختلف را بررسی می‌کنیم. حال کلیدی که بیشترین احتمال را داشته باشد کلید را به عنوان کلید در نظر می‌گیریم و سعی می‌کنیم با جستجوی جامع سایر بیت‌های کلید را به دست آوریم. تمام نتایج به دست آمده و همچنین برنامه های نوشته شده در پیوست ذکر شده اند.

در زیری بخشی از XOR پروفایل به دست آمده برای چهارمین S-box سیستم رمز ذکر شده است.

---

[۴] Biham

[۵] Shamir

[۶] Differential Cryptanalysis

[۷] Exhaustive Search

[256, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0]

[0, 4, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 0, 4, 0, 0, 0, 0, 6, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 2, 0, 0, 0, 0, 2, 0, 0, 2, 2,
2, 0, 0, 0, 0, 0, 2, 0, 0, 2, 0, 2, 0, 0, 2, 2, 0, 4, 2, 0, 4, 0, 0, 0, 2, 0, 2, 0, 2, 2, 0, 4, 0, 0, 0, 0, 0, 2, 0, 2, 4, 0, 0, 0, 2, 2, 0, 2, 0, 0,
0, 0, 2, 0, 0, 0, 2, 4, 2, 6, 0, 0, 0, 0, 0, 2, 0, 2, 0, 2, 4, 4, 0, 0, 2, 2, 0, 0, 2, 0, 2, 0, 0, 0, 0, 0, 0, 0, 4, 4, 0, 0, 0, 2, 0, 0, 0, 0, 0, 6,
2, 0, 2, 2, 0, 4, 0, 2, 0, 0, 2, 2, 0, 2, 2, 2, 0, 0, 0, 2, 0, 0, 2, 0, 2, 2, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 2, 4, 0, 2, 0, 2, 0, 4, 2, 0,
4, 6, 0, 0, 0, 2, 2, 2, 0, 2, 2, 0, 2, 2, 2, 0, 0, 2, 0, 2, 2, 0, 2, 2, 2, 0, 0, 2, 2, 0, 2, 0, 2, 0, 0, 2, 2, 0, 0, 0, 2, 0, 2, 0, 0, 2, 0, 0, 0, 4,
2, 2, 0, 0, 2, 2]

[0, 0, 0, 6, 0, 2, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 6, 2, 0, 0, 0, 0, 0, 0, 0, 2, 4, 0, 4, 4, 0, 0, 0, 0,
0, 0, 6, 2, 2, 4, 0, 0, 2, 4, 2, 2, 0, 0, 0, 0, 2, 2, 2, 2, 0, 0, 0, 0, 0, 0, 0, 0, 6, 0, 2, 0, 4, 0, 2, 4, 4, 2, 0, 0, 2, 2, 2, 0, 2, 2, 0, 0, 0, 0,
0, 0, 0, 0, 2, 2, 4, 0, 0, 0, 2, 2, 4, 2, 0, 0, 0, 0, 0, 2, 2, 0, 0, 2, 2, 0, 0, 0, 8, 0, 0, 2, 2, 2, 2, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 2, 2, 2, 0,
0, 0, 0, 0, 0, 0, 4, 2, 4, 2, 0, 2, 0, 2, 0, 2, 0, 0, 0, 2, 0, 0, 0, 2, 0, 0, 0, 0, 0, 2, 2, 4, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6, 0, 0, 2, 4, 0, 2, 0,
2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 0, 0, 4, 0, 0, 0, 0, 2, 4, 4, 2, 0, 4, 2, 0, 0, 2, 2, 0, 4, 2, 4, 0, 2, 2, 0, 2, 0, 0, 2, 0, 0, 2, 0, 0, 0, 2, 2, 0,
0, 0, 0, 2, 0, 0]

[0, 2, 0, 0, 0, 4, 2, 0, 0, 0, 0, 0, 2, 0, 2, 2, 2, 0, 0, 6, 0, 0, 0, 0, 0, 0, 0, 4, 0, 2, 2, 0, 0, 0, 0, 2, 2, 0, 6, 0, 0, 4, 0, 0, 0, 2, 0, 2, 2, 0,
2, 0, 0, 2, 4, 4, 2, 0, 0, 0, 0, 2, 0, 0, 2, 0, 0, 0, 0, 2, 0, 0, 0, 0, 2, 0, 0, 0, 0, 2, 0, 0, 2, 2, 2, 0, 0, 0, 0, 4, 0, 0, 0, 2, 2, 0, 2, 2, 0, 0,
2, 0, 2, 0, 10, 0, 0, 2, 0, 0, 0, 2, 0, 0, 2, 2, 0, 2, 0, 0, 2, 0, 0, 0, 0, 2, 2, 2, 0, 0, 2, 2, 2, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 0, 0, 0, 0,
0, 4, 2, 0, 4, 2, 2, 2, 0, 2, 0, 0, 4, 2, 0, 0, 0, 0, 0, 2, 0, 0, 2, 0, 2, 2, 0, 2, 0, 0, 0, 0, 0, 2, 2, 0, 0, 0, 6, 0, 0, 2, 0, 0, 6, 2, 2, 0, 0, 0,
0, 0, 4, 0, 0, 0, 2, 4, 2, 0, 0, 0, 0, 2, 4, 2, 2, 0, 0, 0, 0, 4, 2, 4, 0, 0, 2, 0, 2, 0, 2, 2, 0, 0, 2, 4, 0, 0, 0, 2, 0, 0, 2, 0, 0, 0, 0, 0, 2, 0,
0, 2, 4, 0, 2, 2, 2]

تحلیل خطی

دومین تحلیل موثر مطرح شده را می‌توان تحلیل خطی[8] در نظر گرفت. این تحلیل برای اولین بار توسط آقایان ماتسویی[9] و یاماگیشی[10] در سال ۱۹۹۲ بر روی سیستم رمز FEAL اعمال شد. بلافاصله پس از آن آقای ماتسویی تحلیل را بر روی سیستم رمز DES اعمال کرد. در نهایت در سال ۱۹۹۳ آقای ماتسویی این تحلیل را تحت عنوان تحلیل خطی در قالب یک مقاله مطرح کرد. در حالی که تمرکز تحلیل تفاضلی بر روی تفاوت میان قطعه‌های داده است، در تحلیل خطی روابط و همبستگی میان بیت‌های متن واضح و متن رمز شده در نظر گرفته می‌شود. تحلیل بر پایه یافتن یک تقریب خطی مناسب برای روابط ذکر شده انجام می‌شود. یکی از مزیت‌های این نوع تحلیل نسبت به تحلیل تفاضلی این است که این تحلیل از نوع تحلیل متن واضح است در حالی که تحلیل تفاضلی از نوع متن واضح انتخابی است.

[8] Linear Cryptanalysis

[9] Matsui

[10] Yamagishi

ایده اولیه، تقریب‌زدن بخشی از متن رمزشده با یک عبارت خطی است که خطی‌بودن به معنای عملیات بیتی در مبنای دو، همان XOR، است.

$$X_{i_1} \oplus X_{i_2} \oplus \ldots \oplus X_{i_u} \oplus Y_{j_1} \oplus Y_{j_2} \oplus \ldots \oplus Y_{j_v} = 0$$

رویکرد در تحلیل خطی این‌گونه است که عباراتی به شکل بالا با یک احتمال وقوع بالا یا پایین تعیین شود. در صورتی‌که سیستم رمزی تمایل به داشتن احتمال وقوع بالا یا پایینی برای عبارت فوق داشته باشد، بیان‌گر ضعیف‌بودن توانایی تصادفی‌سازی آن سیستم رمز است. هرچه احتمال برقراری یک عبارت خطی دورتر از ½ باشد، تحلیل‌گر می‌تواند تحلیل خطی را بهتر انجام دهد. اگر این احتمال برابر یک باشد، به این معناست که یک تعبیر خطی مناسب برای سیستم رمز پیدا شده است و سیستم رمز از این منظر ضعیف است. اگر این احتمال برابر صفر باشد، یک رابطه affine با سیستم رمز دارد، که این نیز بیانگر ضعف سیستم رمز است. زیر در سیستم بر مبنای دو، یک تابع affine مکمل یک تابع خطی است. پس تقریب‌های خطی یا affine در این حمله کاربرد خواهند داشت.

تنها قسمت سیستم‌های رمز که غیرخطی هستند، s-boxها می‌باشند. پس در صورتی که بتوان خاصیت غیرخطی‌بودن این ساختارها را با عبارات خطی تقریب زد، پس می‌توان با در کنار هم گذاشتن این عبارت‌ها، کل سیستم رمز را تحلیل کرد.

برای این کار، باید همه حالت‌های ورودی و همه حالت‌های خروجی را در نظر گرفت. از طرفی تمامی توابع خطی از بیت‌های ورودی و تمامی توابع خطی از بیت‌های خروجی را با یکدیگر مقایسه کرد. به این ترتیب، به عنوان مثال، برای یک s-box با ۴بیت ورودی و ۴بیت خروجی جدولی به شکل زیر خواهیم داشت:

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4	$X_2 \oplus X_3$	$Y_1 \oplus Y_3 \oplus Y_4$	$X_1 \oplus X_4$	Y_2	$X_3 \oplus X_4$	$Y_1 \oplus Y_4$
0	0	0	0	1	1	1	0	0	0	0	1	0	1
0	0	0	1	0	1	0	0	0	0	1	1	1	0
0	0	1	0	1	1	0	1	1	0	0	1	1	0
0	0	1	1	0	0	0	1	1	1	1	0	0	1
0	1	0	0	0	0	1	0	1	1	0	0	0	0
0	1	0	1	1	1	1	1	1	1	1	1	1	0
0	1	1	0	1	0	1	1	0	1	0	0	1	0
0	1	1	1	1	0	0	0	0	1	1	0	0	1
1	0	0	0	0	0	1	1	0	0	1	0	0	1
1	0	0	1	1	0	1	0	0	0	0	0	1	1
1	0	1	0	0	1	1	0	1	1	1	1	1	0
1	0	1	1	1	1	0	0	1	1	0	1	0	1
1	1	0	0	0	1	0	1	1	1	1	1	0	1
1	1	0	1	1	0	0	1	1	0	0	0	1	0
1	1	1	0	0	0	0	0	0	0	1	0	1	0
1	1	1	1	0	1	1	1	0	0	0	1	0	1

حال با در نظر گرفتن تمامی این حالات، می‌توان جدول تقریب خطی مربوط به s-box را ، که جدولی مشابه با جدول زیر خواهد بود، قابل حصول است.

		Output Sum															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Input Sum	0	+8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	–2	–2	0	0	–2	+6	+2	+2	0	0	+2	+2	0	0
	2	0	0	–2	–2	0	0	–2	–2	0	0	+2	+2	0	0	–6	+2
	3	0	0	0	0	0	0	0	0	+2	–6	–2	–2	+2	+2	–2	–2
	4	0	+2	0	–2	–2	–4	–2	0	0	–2	0	+2	+2	–4	+2	0
	5	0	–2	–2	0	–2	0	+4	+2	–2	0	–4	+2	0	–2	–2	0
	6	0	+2	–2	+4	+2	0	0	+2	0	–2	+2	+4	–2	0	0	–2
	7	0	–2	0	+2	+2	–4	+2	0	–2	0	+2	0	+4	+2	0	+2
	8	0	0	0	0	0	0	0	0	–2	+2	+2	–2	+2	–2	–2	–6
	9	0	0	–2	–2	0	0	–2	–2	–4	0	–2	+2	0	+4	+2	–2
	A	0	+4	–2	+2	–4	0	+2	–2	+2	+2	0	0	+2	+2	0	0
	B	0	+4	0	–4	+4	0	+4	0	0	0	0	0	0	0	0	0
	C	0	–2	+4	–2	–2	0	+2	0	+2	0	+2	+4	0	+2	0	–2
	D	0	+2	+2	0	–2	+4	0	+2	–4	–2	+2	0	+2	0	0	+2
	E	0	+2	+2	0	–2	–4	0	+2	–2	0	0	–2	–4	+2	–2	0
	F	0	–2	–4	–2	–2	0	+2	0	0	–2	+4	–2	–2	0	+2	0

که به عنوان مثال، بخشی از ابتدای جدول تقریب خطی برای s-box شماره دو در سیستم رمز TwoFish به شکل زیر است. (جدول کامل به پیوست آمده است.)

[128, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0]

[0, -2, 14, 12, 0, -6, 6, -8, 0, -14, -18, 8, 12, -14, -6, 0, 4, -10, 2, -20, 0, 6, -2, -12, 4, 2, -6, -8, 4, -2, 2, -12, -10, 0, 12, -10, -6, -8, 0, -10, 2, -8, 0, -2, -14, 4, 8, -6, 2, -8, 0, -2, 2, -12, 8, -6, -10, 16, 4, -18, -6, 8, -8, 14, -10, -8, -4, 14, -2, -4, -4, 2, 2, 8, 0, 14, 6, 0, 4, -2, 10, -8, 8, -2, -10, -8, 4, 6, -2, 8, 12, 22, -2, 4, 4, 2, 4, -14, -6, -8, -8, -6, -2, 8, 4, -2, 10, 12, 4, -6, 2, -8, 8, 10, -2, -8, 0, -2, -18, -4, -8, -2, 6, -4, -12, -18, 2, 4, 10, 8, -8, -18, -2, 8, 4, 14, -2, -8, -4, -10, -10, 4, -12, 10, 6, 0, 4, -2, -10, 4, 4, -6, 2, 0, 8, 14, -2, 8, -4, -10, -8, -6, -2, 8, 0, 6, 6, -4, 16, -10, 14, 4, -4, -2, 2, -4, 4, -6, 2, -8, -8, 10, -2, -8, -4, -2, -6, 4, -4, 2, 10, 0, -12, -10, -14, -4, 16, 14, 6, -12, -12, 2, -6, 8, -12, 6, -6, -12, 0, 6, 6, -4, 0, 10, 6, 8, 0, -6, 6, 8, 12, 2, -6, 0, -6, 0, 8, 6, -14, 12, 0, -6, -10, 0, 4, -2, 2, -8, -8, 6, 14, 0, -4, -2, -6, -8, 0, -10, 2, 0, 24, -2, 10, -4, 0, 2]

[0, 2, 8, -10, -6, 12, -6, -8, 10, 4, -10, 4, 0, 2, -4, 2, 16, 6, 4, 6, -6, 0, 6, 8, -10, -4, -10, 0, 4, 2, 4, 6, -12, -2, 8, -2, -6, 4, 6, -4, -6, 4, 10, -8, -12, 6, 4, 10, 0, -10, -8, -6, -10, -4, -10, -8, 10, 8, -10, 8, -4, 2, 8, 2, -2, 4, -14, 4, -4, 10, -8, 2, 4, 2, 12, -18, 6, -12, 14, 0, 14, -8, 6, 12, 4, 6, 4, 2, 0, -6, 4, 2, 2, 12, -10, -12, 2, 0, -6, 4, 4, -6, 4, -10, -12, -14, 8, -6, 2, 16, 6, 8, -2, -8, 2, -8, -8, 10, 20, 2, -12, -10, -4, -14, 2, 4, -6, 0, -6, -8, 6, -8, 0, -10, -12, -2, -12, -14, -12, -2, -2, -4, -2, -8, -6, 12, 2, -8, 8, 2, 8, -10, 0, -6, 4, 10, 10, 4, -18, -12, 2, -8, -6, 4, -20, 10, 12, -2, -16, -2, -12, -2, -10, 4, 10, 4, 22, -8, 18, -8, -8, 2, -4, -6, 8, -6, 8, -10, -2, 0, -2, -4, 0, 10, 8, -10, 10, -12, 10, 8, -2, -8, 10, 16, 4, -10, 0, -2, 8, -10, 4, -10, 2, 16, 6, -8, -14, -8, 10, 12, 0, -18, 8, 2, 0, 2, -4, 2, 6, -8, -6, 0, -14, -4, -6, 0, -4, -2, 4, 2, -4, -6, 4, 6, 2, 0, 2, 4, 2, 0, -2, 8, 4, -6, -16, 2]

[0, -4, -6, 2, 2, -6, 4, 16, -6, 2, 0, 4, -4, 16, -6, 2, 16, 4, -18, 6, -2, 6, -4, 0, -10, -10, 0, 4, 4, 8, 14, -2, -2, -2, -4, -8, 8, -4, 6, -2, 0, 12, 10, -14, -14, 2, -4, 0, 2, -6, -12, -16, -8, -4, 2, 2, 0, -12, -2, 6, -2, 14, 4, 16, 8, 4, -2, -10, -2, -2, 12, 0, 2, 10, 12, 0, 16, -4, 2, 2, 8, 4, 2, 2, -6, 2, -12, 8, -10, -2, -12, 0, 0, -12, -2, 14, 6, 6, 16, -4, 4, 0, -2, -2, 0, -4, -2, 6, -2, -10, 12, -8, -14, 2, -16, 4, 12, 0, 2, 2, 0, -4, 2, -14, -6, -6, 4, -16, 8, 0, -10, -6, 2, 14, -8, 8, 14, 2, -8, -8, 24, 16, -6, 6, 24, 0, -6, 6, 6, -6, 8, 8, 2, 6, 0, -8, 0, 0, -2, 10, 18, -10, 4, -12, -4, 12, -2, -14, 0, 0, 14, 10, 2, -2, 0, 0, 6, -6, -4, 4, 4, -4, 2, -10, 8, 8, -6, 14, -2, -14, 8, 8, 12, -4, -2, -6, -6, 6, 4, 4, 10, 6, 0, 8, 0, -8, -2, -6, -12, -20, 10, -10, 6, 2, -4, 4, -2, 2, 8, -16, -8, 0, 2, -10, -2, -22, 4, -4, -4, -4, 2, -10, -4, 4, 6, 10, 10, 6, -12, 4, 2, 6, -4, 4, 4, 4, 6, 2, 12, -4, -6, 14, -2, 10, 4, -4]

[0, 8, 0, 4, -8, 12, 0, 8, 6, 2, 2, -6, 6, -10, -6, 14, 8, 0, 4, -8, -8, -4, -4, -12, -18, 2, -2, -2, -10, -2, -2, -6, 6, 2, -2, -10, -2, -10, -10, 2, -20, 4, -16, 4, -4, -8, 0, 0, -2, -6, 10, 2, -2, -10, -6, 6, 4, 4, -12, 0, -4, 0, -4, -12, 6, 22, 2, -10, 6, -6, 10, -6, -20, 8, -4, 12, -4, 4, 20, -8, 10, 2, -6, 6, -6, 6, 2, -6, -8, 4, 4, 4, -8, 0, -4, 0, 0, 20, 4, -4, -8, -16, -4, -16, -10, -2, 14, 10, 14, 2, -10, 6, -12, 0, -12, -12, -4, -4, -4, 8, 2, 10, -2, -6, -6, -2, 6, 6, -10, -2, 2, 6, -2, 2, 2, -6, 12, 0, 4, 20, -4, -12, 12, 8, -2, 14, -2, 10, -10, 2, -18, 14, 4, 8, -8, 8, -12, -4, 0, -4, -4, -8, 0, -8, -12, -4, 8, 4, -6, -6, 10, 6, -6, 14, 10, 2, -4, 0, -4, -4, 4, -12, 4, 8, 10, -6, -2, -6, -6, -2, -2, -10, -4, -12, 4, 0, -4, -8, -4, -12, -14, -2, -2, -2, 18, 10, 6, -6, 0, 8, 4, 0, 8, 4, -12, -4, -2, 2, -2, -10, 6, 6, -2, -6, 6, -14, 6, -10, 14, -2, -2, 10, -12, 12, 8, -12, -4, 0, 0, 0, 2, -2, -10, 6, 2, -14, 6, 2, 8, -8, 8, 12, -8, 4, 8, 16]

[0, 6, -2, 0, 4, 10, 10, 12, 14, 12, 8, 10, -10, 4, 0, 2, 8, 2, 2, 0, 0, 2, 10, -16, 6, 8, -4, -6, -6, 4, 8, -2, 4, 10, 10, -4, -4, -6, -6, 4, -10, 4, 0, 2, 2, 8, -4, 6, 12, 14, -2, 4, -8, 10, 10, 0, -10, -16, -4, 18, -2, -8, -4, 2, -12, -2, 14, -4, -8, -6, -6, 0, 6, 0, -4, 2, 6, 8, -4, -6, 0, -2, 6, 0, 8, 22, -2, 8, 2, 0, -12, 6, 14, -4, 8, -6, 4, -2, -2, 12, -4, -10, -18, -4, 2, 12, 0, 6, -10, 0, -12, 10, -8, -2, 14, -16, 4, -14, -6, 4, -2, 4, -8, 18, -2, -4, 0, 2, 0, -10, -14, -4, 0, 6, -22, 20, 2, 0, 0, -6, -18, -4, -4, 6, 8, 2, -2, 4, 4, 6, 10, 8, -14, -12, 4, 10, 2, -4, -4, -6, -4, 10, -10, -8, 16, 6, 2, -4, 2, 8, 0, 2, 2, 0, 0, -6, -12, -2, 2, 8, 4, -2, 2, 8, -6, -4, 12, 2, 14, 0, -8, -2, 0, 18, 6, -12, 0, -6, -2, 4, 6, 8, -8, -2, 10, -12, -4, -22, 12, 2, 6, 0, 24, -2, 2, -4, -6, 0, 0, 2, 2, 8, 0, 2, -8, 2, -2, 4, 12, 6, 10, -16, -6, -12, 4, 2, 2, -4, -4, -6, 12, 2, -10, 0, -4, -6, -10, -8, -2, 4, -4, 14, 10, -8, -16, 10]

در ابتدا برای S-box های سیستم رمز Linear Profile را به صورت مجزا به آوردیم. سپس با توجه به Linear Profile ها یک مشخصه خوب برای تحلیل خطی سیستم استخراج می‌کنیم. پس از استخراج مشخصه، حال، خروجی دور اول سیستم رمز (U) را به دست می‌آوریم و سپس خروجی دور دوم (C) را نیز محاسبه خواهیم کرد. سپس بیت‌های فعال U را در نظر می‌گیریم و به ازای تمام حالا همان بیت‌ها در کلید، آن کلیدها را با XOR C کرده‌ایم. و سپس عکس عملیات مرحله دوم را بر روی آن انجام می‌دهیم. حال احتمال هر کدام را محاسبه کرده و بررسی می‌کنیم که احتمال کدام کلید بالاتر است و آن را انتخاب می‌کنیم و سپس برای دیگر بیت‌های کلید جستجوی جامع را اعمال می‌کنیم. تمام فعالیت‌های ذکر شده و نتایج به همراه برنامه های استفاده شده در پیوست ذکر شده اند.

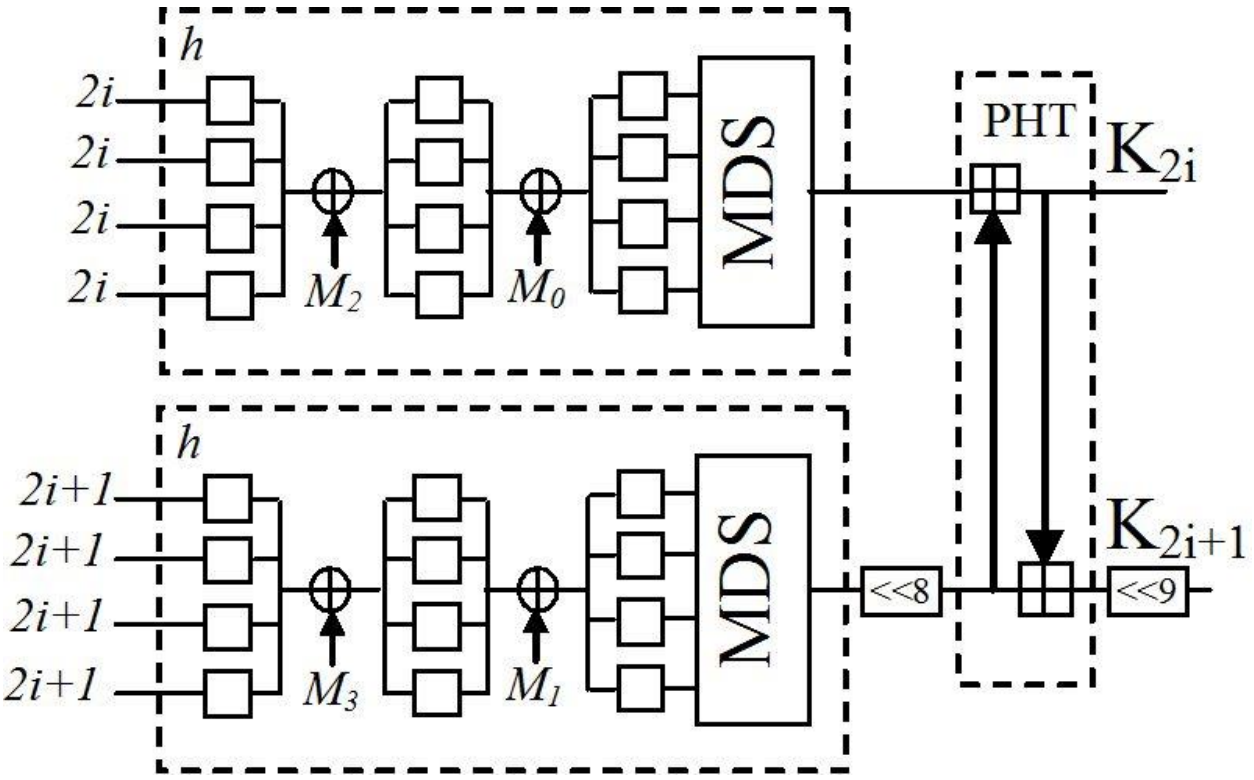
نتایج به دست آمده

در تحلیل تفاضلی با 2^{16} جفت تولید شده هیچکدام از بیت های کلید به دست نیامده و تعداد عملیات بیشتری می‌بایست انجام می‌شد. عملیات تخمین زده شده حدود 2^{40} بود که به دلیل محدودیت محاسباتی انجام نشد. هر چند که XOR Profile برای تمامی S-Box ها با توجه به کلید مورد نظر تولید شده و در پیوست به صورت کامل ذکر شده اند.

همچنین در تحلیل خطی با 2^{24} عملیات انجام شده هیچکدام از بیت‌های کلید استخراج نشدند. تخمین انجام شده برای به دست آمدن تعدادی از بیت‌های کلید عملیاتی با پیچیدگی 2^{39} بود که به دلیل پیچیدگی محاسباتی بالا انجام نشد. هر چند که Linear Profile برای تمامی S-Box ها با توجه به کلید مورد نظر تولید شده و در پیوست به صورت کامل ذکر شده اند.

فصل سوم: نتیجه گیری و جمع بندی

با توجه به موارد ذکر شده و همچنین با توجه به طراحی انجام شده برای Key Schedule این سیستم رمز، با به دست آوردن کلید دور می‌توان کلید سیستم رمز را به دست آورد. Key Schedule سیستم رمز به طرح زیر است:



در نتیجه با توجه به موارد ذکر شده در تحلیل و همچنین Key Schedule طراحی شده سیستم رمز، می‌توان گفت که به دست آوردن کلید دور به نظر امری مشکل است.

فهرست منابع

[۱] B. Schneier, "Twofish: A 128-Bit Block Cipher," [Online]. Available: https://www.schneier.com/cryptography/paperfiles/paper-twofish-paper.pdf.

[۲] S. Murphy and M. J. Robshaw, "Differential Cryptanalysis, Key-Dependent S-boxes, and Twofish".

پیوست

کد برنامه‌های نوشته شده برای انجام کار به زبان Java به عنوان پیوست به پروژه ضمیمه شده است. لازم به ذکر است که تمام کدهای پیوست شده (حتی کد اصلی الگوریتم رمز) توسط نگارندگان پروژه پیاده سازی شده است.