مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال پنجم، شماره ۲، تابستان ۱۳۹۶، ص ۹۴-۸۹

حمله دوبخشی به الگوریتم رمز LBlock با پیچیدگی داده کم

مسعود هادیان دهکردی[1*]، رقیه تقی‌زاده[2]

۱- استاد، دانشکده ریاضی، دانشگاه علم و صنعت ایران ۲- دانشجوی دکتری رمز، دانشگاه علم و صنعت ایران

(دریافت: ۹۵/۰۴/۲۹، پذیرش: ۹۵/۱۱/۲۵)

چکیده

رمز LBlock، یک رمز سبک وزن با طول قالب ورودی ۶۴ بیت و طول کلید ۸۰ بیت است. حمله دوبخشی که به نوعی برگرفته از حمله ملاقات در میانه است، در سال‌های اخیر بیش‌تر مورد توجه تحلیل‌گران قرار گرفته است. این حمله اغلب قادر به شکستن نسخه کامل رمزهایی است که تاکنون حملات دیگر قادر به شکست آن‌ها نبوده است. در این مقاله، ابتدا به معرفی دوبخشی نامتقارن پرداخته و سپس یک حمله دوبخشی به کل الگوریتم رمز سبک وزن LBlock ارائه می‌شود. پیچیدگی محاسباتی و داده آن به‌ترتیب $2^{78/62}$ و 2^{48} می‌باشد. پیچیدگی داده این حمله به مراتب پایین‌تر از تنها حمله دوبخشی اعمال‌شده به این الگوریتم است.

واژه‌های کلیدی: رمز سبک وزن، رمز LBlock، حمله ملاقات در میانه، حمله دوبخشی.

۱- مقدمه

چندین روش مشترک برای تحلیل رمزهای قالبی و توابع چکیده‌ساز وجود دارد. به‌عنوان مثال، تحلیل تفاضلی[1] که اساساً برای تحلیل رمزهای قالبی روی کار آمده‌اند، اکنون در سطح وسیعی برای تحلیل توابع چکیده‌ساز مورد استفاده قرار می‌گیرند. به‌صورت عکس نیز دو روش از تحلیل توابع چکیده‌ساز به تحلیل رمزهای قالبی وارد شده‌اند که می‌توان به حمله ملاقات در میانه[2] و حمله دوبخشی[3] اشاره کرد. مفهوم حمله ملاقات در میانه، در سال ۱۹۹۷ در [۱] ارائه شد و پس از آن، مفهوم این حمله، در حملات پیش‌تصویر بر روی توابع چکیده‌ساز مورد استفاده قرار گرفت. ویژگی بارز این حمله، پیچیدگی داده پایین می‌باشد که یکی از ابزارهای مهم در تحلیل دوبخشی محسوب م

ی‌شود. تحلیل دوبخشی اولین بار در سال ۲۰۱۱ در [۲] برای تحلیل توابع چکیده‌ساز معرفی شد که در واقع نوعی حمله ملاقات در میانه است که با بهبود آن، به کمک دوبخشی ایجادشده در حمله پیش‌تصویر، پیچیدگی جستجوی جامع کاهش می‌یابد. بعد از معرفی حمله دوبخشی، در [۳] مفهوم حمله دوبخشی مستقل برای رمز قالبی AES به‌کار برده شد و یک دوبخشی سه دوری در الگوریتم رمز AES ایجاد شد که با ترکیب دوبخشی ایجادشده و روش حمله ملاقات در میانه، اولین حمله تک‌کلیدی بروی تمام دور AES-128 انجام شد. بعد از آن، این حمله مورد توجه اکثر تحلیل‌گران قرار گرفت و در تحلیل اکثر رمزهای قالبی از این روش استفاده کردند که نتیجه آن‌ها حمله روی کل دورهای بعضی از رمزهایی شد که تاکنون حمله مؤثری به آن‌ها وارد نشده بود.

الگوریتم رمز LBlock که اولین بار در سال ۲۰۱۱ در [۴] معرفی شد، یک رمز سبک‌وزن فیستلی[4] تعمیم یافته است که طول قالب ورودی و طول کلید آن به‌ترتیب ۶۴ و ۸۰ بیت است. به‌علت کاربرد بسیار وسیع برچسب‌های RFID و نودهای حسگر در حوزه ارتباطات و کاربردهای الکترونیکی که با محدودیت در حافظه طراحی شده‌اند، تحلیل و بررسی این الگوریتم حائز اهمیت است. امنیت الگوریتم رمز LBlock در مقالات مورد بررسی قرار گرفته است که نتایج این تحلیل‌ها در جدول (۱) خلاصه شده است.

در این مقاله به معرفی حمله دوبخشی نامتقارن می‌پردازیم و به‌کمک آن یک حمله دوبخشی به کل الگوریتم رمز LBlock ارائه می‌شود که پیچیدگی داده آن 2^{48} می‌باشد که به‌مراتب پایین‌تر از پیچیدگی داده تحلیل‌هایی است که به این الگوریتم وارد شده و

*رایانامه نویسنده مسئول: mhadian@iust.ac.ir

1- Differentials Cryptanalysis
2- Meet in the Middle Attack
3- Biclique Attack
4- Feistel

نتایج آن در جدول (۱) آمده است.

جدول (۱): خلاصه‌ای از نتایج تحلیل‌ها به الگوریتم رمز LBlock

منبع	پیچیدگی محاسباتی	پیچیدگی داده	دور	حمله
[۴]	$2^{63/7}$	$2^{63/7}$	۲۰	انتگرال[1]
[۴]	$2^{72/7}$	2^{63}	۲۰	تفاضلی ناممکن[2]
[۷]	$2^{69/5}$	2^{63}	۲۱	تفاضلی ناممکن
[۸]	$2^{71/27}$	$2^{62/1}$	۲۲	حمله صفر همبستگی[3]
[۹]	2^{76}	$2^{62/1}$	۲۳	حمله صفر همبستگی
[۶]	$2^{78/4}$	2^{52}	کل الگوریتم	حمله دوبخشی
این مقاله	$2^{78/62}$	2^{48}	کل الگوریتم	حمله دوبخشی

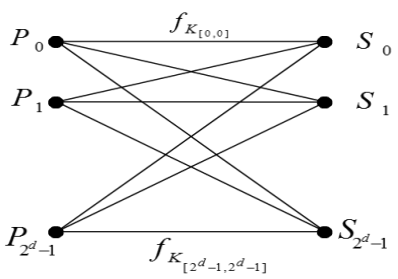
۲- حمله دوبخشی

حمله دوبخشی که اولین بار در سال ۲۰۱۱ در [۲] برای تحلیل توابع چکیده‌ساز معرفی شد، در واقع نوعی حمله ملاقات در میانه است که به کمک دوبخشی‌های ایجادشده، پیچیدگی جستجوی جامع کاهش می‌یابد. سپس به کمک روش تصادم جزئی، پیچیدگی داده را کاهش می‌دهد. روند کلی حمله دوبخشی بدین ترتیب است: در ابتدا سعی می‌شود دنباله‌ای از گراف‌های دوبخشی با بعد نسبتاً بالا به‌وسیله ابزارهایی شبیه تفاضلات کلید مرتبط ساخته می‌شود، پس از آن، با بررسی تصادم در یک متغیر درونی در دوجهت رفت و برگشت، کلیدهای نادرست حذف می‌شود. توجه داشته باشید که این دوبخشی‌ها را می‌توان در ابتدای رمز یا انتهای رمز ساخت. درصورتی‌که دوبخشی‌ها در ابتدای رمز ساخته شود حمله از نوع متن اصلی منتخب، و درصورتی‌که دوبخشی‌ها در انتهای رمز ساخته شود حمله از نوع متن رمزشده منتخب است. برای انجام حمله با فرض این‌که دوبخشی‌ها در سمت متن اصلی ساخته می‌شود مراحل زیر تعقیب می‌شود:

رمز قالبی E را به‌صورت ترکیبی از سه زیررمز، f، g و h به‌صورت $E = f \circ g \circ h$ در نظر بگیرید. فرض کنید S حالت میانی به‌دست‌آمده از اجرای f بر روی متن اصلی باشد به‌عبارتی $S = f_k(P)$. فرض کنید f به کمک 2^{2d} کلید $\{K_{[i,j]}\}$، 2^d متن اصلی $\{P_i\}$ را به 2^d حالت میانی $\{S_j\}$ بنگارد. سه‌تایی $\{\{P_i\},\{S_j\},\{K_{[i,j]}\}\}$ را یک دوبخشی متقارن از بعد d گویند هرگاه برای $0 \le i \le 2^d - 1$ و $0 \le j \le 2^d - 1$

$$S_j = f_{K_{[i,j]}}(P_i) \qquad (۱)$$

به عبارتی، همان‌گونه که در شکل (۱) نشان داده شده است، یک دوبخشی در واقع یک گراف دوبخشی با مجوعه رئوس $\{P_i\}$ و $\{S_j\}$ است که با کمک 2^{2d} یال $\{f_{K_{[i,j]}}\}$، به یکدیگر متصل شده‌اند.



شکل (۱): گراف دوبخشی

تعریف (d_1, d_2)- دوبخشی نامتقارن: فرض کنید f زیررمزی باشد که با کمک $2^{d_1} \times 2^{d_2}$ کلید $\{\{K_{[i,j]}\}\}$، 2^{d_1} متن اصلی $\{P_i\}$ را به 2^{d_2} حالت میانی $\{S_j\}$ بنگارد. سه‌تایی $\{\{P_i\},\{S_j\},\{K_{[i,j]}\}\}$ را یک دوبخشی نامتقارن از بعد (d_1, d_2) گویند هرگاه:

$$S_j = f_{K_{[i,j]}}(P_i) \quad 0 \le i \le 2^{d_1} - 1, 0 \le j \le 2^{d_2} - 1 \qquad (۲)$$

حمله دوبخشی نامتقارن از بعد (d_1, d_2) بر روی یک رمز قالبی با طول کلید n، شامل چهار گام زیر است که برای مشاهده جزئیات هر گام می‌توانید به [۳] مراجعه کنید.

گام اول) تقسیم فضای کلید: در این گام فضای کلید به گروه‌های از کلید افراز می‌شود. بدین ترتیب، کل فضای کلید که متشکل از 2^n کلید است به $2^{n-(d_1+d_2)}$ گروه کلید، که در هر گروه، $2^{d_1+d_2}$ کلید وجود دارد افراز می‌شود. در هر گروه، کلیدها به‌صورت مؤلفه‌های یک ماتریس $2^{d_1} \times 2^{d_2}$ به‌صورت $K[i,j]$ اندیس‌گذاری می‌شوند. با فرض این‌که تفاضلات ∇_i^K و Δ_j^K به‌صورت $\nabla_i^K = K[0,0] \oplus K[i,0]$ و $\Delta_j^K = K[0,0] \oplus K[0,j]$ تعریف شوند، گام‌های بعدی را ادامه می‌دهیم.

گام دوم) ساخت گراف دوبخشی: برای هر گروه کلید، یک گراف دوبخشی به‌صورت زیرساخته می‌شود.

- متن اصلی دلخواه P_0 را انتخاب کرده و مقدار میانی S_0 را به‌صورت $S_0 = f_{K[0,0]}(P_0)$ حساب کنید.
- مقادیر P_i را به‌صورت $P_i = f^{-1}{}_{K[i,0]}(S_0)$ برای $i = 1, \dots, 2^{d_1} - 1$ حساب کنید.

1- Integral
2- Impossible Differential
3- Zero Correlation

- مقادیر S_j را به‌صورت $S_j = f_{K[0,j]}(P_0)$ برای $j = 1, \dots, 2^{d_2} - 1$ حساب کنید.

درصورتی‌که دو مسیر ایجادشده در جهت رفت و برگشت مستقل باشند (هیچ جزء غیرخطی مشترک نداشته باشند) آن‌گاه سه‌تایی $\{\{P_i\}, \{S_j\}, \{K_{[i,j]}\}\}$ تشکیل یک دوبخشی نامتقارن از بعد (d_1, d_2) می‌دهد.

گام سوم) فیلتر کلیدهای نادرست: کلیدهایی که در هر گروه کلید پس از بررسی در متغیر میانی، موجب تصادم نمی‌شوند حذف می‌شوند. ترتیب کار به‌صورت زیر می‌باشد:

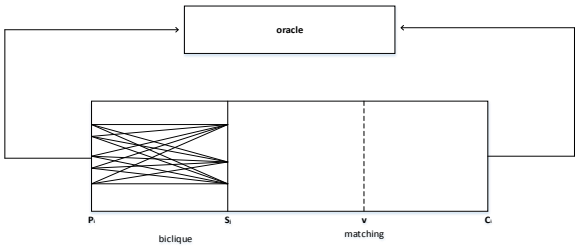
- متغیر درونی ϑ که در آن برخورد صورت می‌گیرد مشخص می‌شود.
- با رمزگذاری متن P_i تحت کلید اصلی K متن رمزشده متناظر به‌دست می‌آید: $C = E_K(P_i)\ i = 0,1, \dots, 2^{d_1}$
- فرض کنید $\vec{\vartheta} \xleftarrow{K[i,j]} C_i$ نشان‌دهنده محاسبات در جهت رفت و $S_j \xrightarrow{K[i,j]} \vec{\vartheta}$ نشان‌دهنده محاسبات در جهت برگشت باشد. برای هر $i = 0,1, \dots, 2^{d_1} - 1$ و $j = 0,1, \dots, 2^{d_2} - 1$ کلیدهایی که در شرط زیر صدق کند به‌عنوان کلید صحیح درنظر گرفته می‌شود.

$$S_j \xrightarrow{K[i,j]} \vec{\vartheta} = \vec{\vartheta} \xleftarrow{K[i,j]} C_i \qquad (۳)$$

به عبارتی، کلیدهایی که در رابطه بالا صدق نکند، به‌عنوان کلید نادرست خذف می‌شوند.

گام چهارم) جستجوی کاندیدها: در این گام کاندیدهای کلید صحیح باقی مانده تا دست‌یابی به کلید صحیح، جستجوی کامل می‌شوند.

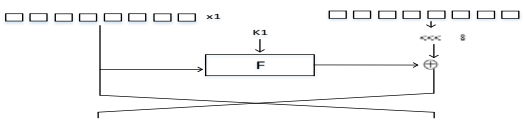
نمایی از حمله دوبخشی نامتقارن را در شکل (۲) مشاهده کنید.



شکل (۲): حمله دوبخشی نامتقارن

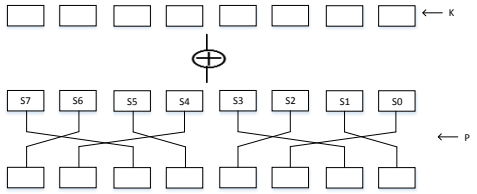
۳- توصیف رمز LBlock

LBlock یک الگوریتم رمز سبک‌وزن، با طول قالب و طول کلید به‌ترتیب ۸۰ و ۶۴ بیت است که اولین بار سال ۲۰۱۱ در [۴] معرفی شد. ساختار کلی آن یک شبکه فیستلی ۳۲ دوری تکرارشونده می‌باشد که تابع دور آن را در شکل (۳) مشاهده می‌شود.



شکل (۳): تابع دور الگوریتم رمز LBlock

تابع f از هشت جعبه جانشانی S0، S1، ...،S7 و یک لایه انتشار P که یک جای‌گشت روی کلمات ۴ بیتی است، تشکیل شده و در شکل (۴) تابع دور f نشان داده شده است.



شکل (۴): تابع دور الگوریتم رمز LBlock

الگوریتم تولید زیرکلید بدین صورت است که ۸۰ بیت کلید اصلی K در یک ثبات[1] قرار می‌گیرد $K = k_{79}k_{78} \dots k_1k_0$. در دور i، ۳۲ بیت پرارزش K، $k_{79}k_{78} \dots k_{49}k_{48}$، به‌عنوان خروجی دور i درنظر گرفته می‌شود. پس از آن رجیستر کلید به شکل زیر پر می‌شود:

$$[k_{79}k_{78} \dots k_1k_0] = [K_{50}K_{49}K_{48} \dots K_1K_0K_{79}K_{78} \dots K_{52}K_{51}]$$

$$[k_{79}k_{78}k_{77}k_{76}] = s_0[k_{79}k_{78}k_{77}k_{76}]$$

$$[k_{75}k_{74}k_{73}k_{72}] = s_1[k_{75}k_{74}k_{73}k_{72}]$$

$$[k_{50}k_{49}k_{48}k_{47}k_{46}] = [k_{50}k_{49}k_{48}k_{47}k_{46}] \oplus [i]_2$$

برای مشاهده جزئیات بیش‌تر در مورد الگوریتم رمز LBlock و الگوریتم تولید زیرکلید به [۴] مراجعه شود.

۴- بررسی حمله دوبخشی نامتقارن به الگوریتم رمز LBlock

در این بخش، برای انجام یک حمله دوبخشی نامتقارن به الگوریتم رمز Lblock، در ابتدا یک دوبخشی نامتقارن روی ۸ دور ابتدایی رمز ساخته می‌شود سپس با درنظر گرفتن یک متغیر میانی در دور ۲۰، کلیدهای نادرست حذف می‌شود که در زیر به شرح جزئیات حمله می‌پردازیم.

1- Register

۴-۱- افراز فضای کلید

فضای کلید ۸۰ بیتی الگوریتم رمز LBlock به 2^{75} گروه کلید افراز می‌شود که در هر گروه کلیدهایی وجود داردکه در آن‌ها بیت‌های $(k_0, k_1, k_3, k_4, k_5)$ تمامی مقدار ممکن را اختیار می‌کنند و بقیه بیت‌ها ثابت هستند. لذا در هر گروه 2^5 کلید وجود دارد. کلید پایه‌ای K[0,0] یک کلید۸۰ بیتی است که به جزء در ۵ بیت $(k_0, k_1, k_3, k_4, k_5)$ که مقدار ۰ دارد در بقیه بیت‌ها، تمامی حالت‌های ممکن را اختیار می‌کند. در این حمله، Δ_i^K با تغییر در بیت‌های k_3, k_4, k_5 و ∇_j^K با تغییر در بیت‌های k_0, k_1 ایجاد می‌شوند. در جداول (۲-۱) تأثیر این تغییرات در زیرکلید دورها را با رنگ خاکستری مشاهده می‌کنید.

جدول (۱): تأثیر تفاضل در بیت‌های $(k_3 k_4 k_5)$ کلید اصلی در زیرکلیدها

round	0								1								2								3								4								5								6								7							
0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48
1	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19
2	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71	70
3	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41
4	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12
5	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63
6	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34
7	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5
8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56
9	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27
10	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79	78
11	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49
12	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20
13	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71
14	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42
15	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13
16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64
17	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35
18	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6
19	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57
20	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28
21	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79
22	1	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50
23	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21
24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72
25	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43
26	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14
27	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65
28	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36
29	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7
30	9	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58
31	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29

جدول (۲): تأثیر تفاضل در بیت‌های $(k_0 k_1)$ کلید اصلی در زیرکلیدها

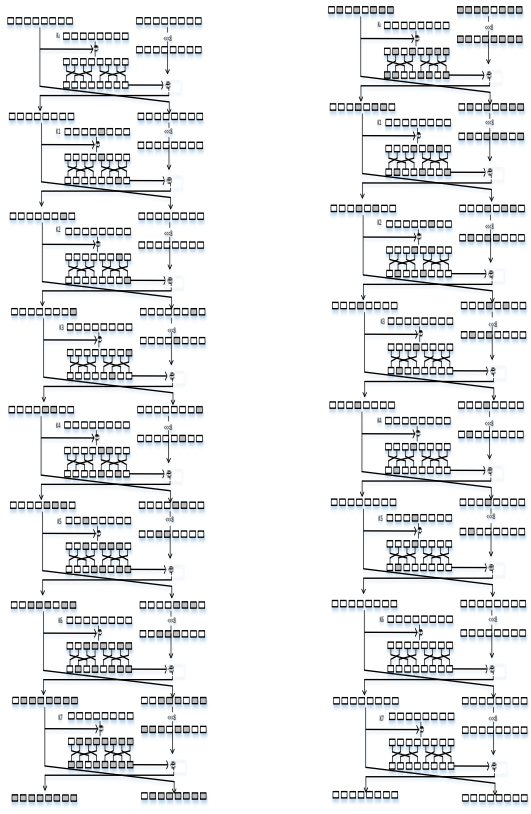
round	0								1								2								3								4								5								6								7							
0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48
1	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19
2	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71	70
3	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41
4	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12
5	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63
6	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34
7	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5
8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56
9	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27
10	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79	78
11	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49
12	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20
13	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71
14	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42
15	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13
16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64
17	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35
18	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6
19	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57
20	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28
21	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79
22	1	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50
23	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21
24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72
25	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43
26	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14
27	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65
28	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36
29	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7
30	9	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58
31	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29

۴-۲- ساخت یک دوبخشی ۸ دوری

برای هر گروه کلید، یک دوبخشی ۸ دوری نامتقارن از بعد (3,2) به‌صورت زیر ساخته می‌شود:

متن اصلی دلخواه $P_0 = 0$ را انتخاب کرده و مقدار میانی S_0، $S_0 = f_{K[0,0]}(P_0)$، را حساب کنید.

- برای $i = 1, \dots, 2^3 - 1$ ، مقدار S_0 را تحت کلیدهای $K[i, 0]$، رمزگشایی جزئی کرده و متن‌های P_i را به‌صورت $P_i = f^{-1}_{K[i,0]}(S_0)$ را حساب کنید. جعبه‌های جانشانی فعال با رنگ خاکستری در سمت چپ شکل (۵) نشان داده شده است این جعبه‌ها باید ۸ بار محاسبه شوند درحالی‌که سایر جعبه‌های جانشانی فقط یک‌بار محاسبه می‌شوند.
- برای $j = 1, \dots, 2^2 - 1$ ، مقدار P_0 را تحت کلیدهای $K[0, j]$، رمزگذاری جزئی کرده و حالت‌های میانی S_j را به‌صورت $S_j = f_{K[0,j]}(P_0)$ را حساب کنید. جعبه‌های جانشانی فعال با رنگ خاکستری در سمت راست شکل (۵) نشان داده شده است این جعبه‌ها باید ۴ بار محاسبه شوند درحالی‌که نیاز به محاسبه سایر جعبه‌های جانشانی نیست زیرا قبلاً محاسبه شده‌اند.



شکل (۵): (۳,۲)- دوبخشی ۸ دوری نامتقارن در الگوریتم رمز LBlock

همان‌گونه‌که در شکل (۵) نیز مشاهده می‌کنید مسیرهای رفت و برگشت از هم مستقل هستند. به عبارتی، هیچ جعبه جانشانی فعال مشترک ندارند، بنابراین یک (۳,۲)- دوبخشی نامتقارن را می‌توان در ۸ دور ابتدایی رمز LBlock ساخت. توجه کنید که چون در هر دوبخشی، از یک مقدار ثابت برای P_0، استفاده می‌شود لذا برای انجام این حمله حداکثر به 2^{48} متن اصلی منتخب نیاز است.

۴-۳- فیلتر کلیدهای نادرست

در این مرحله از روش تصادم جزئی، برای فیلترکردن کلیدهای نادرست استفاده می‌شود. تصادم جزئی روشی مؤثری است که در آن تمامی کلیدها در یک گروه کلید به‌صورت خاص مورد بررسی قرار می‌گیرند که نتیجه آن کاهش پیچیدگی محاسباتی جستجوی جامع است. در این حمله متغیر درونی ϑ که در آن تصادم صورت می‌گیرد، اولین کلمه از سمت راست در پایان دور ۲۰ درنظر گرفته می‌شود (در شکل (۵) این متغیر نشان داده شده است). حال با بررسی مقادیر متغیر درونی ϑ در دو جهت رفت و برگشت کلیدهای نادرست حذف می‌شوند. در هر گروه کلید، کلیدی که به ازای آن، مقدار متغیر درونی ϑ در دو جهت با هم برابر شوند به‌عنوان کاندیدی برای کلید صحیح انتخاب می‌شود.

۵- محاسبه پیچیدگی‌ها

هزینه ساخت یک دوبخشی به‌وسیله تعداد جعبه‌های جانشانی که باید محاسبه شود تعیین می‌شود. لذا تعداد جعبه‌های جانشانی که در حمله به‌کار برده می‌شود تعیین‌کننده پیچیدگی محاسباتی است. تعداد کل جعبه‌های جانشانی به‌کار رفته در الگوریتم رمز LBlock و تابع تولید زیرکلیدهای الگوریتم، برابر با $۳۱ \times ۲ + ۳۱ \times ۸ + ۳۲ = ۳۱۸$ می‌باشد.

پیچیدگی ساخت یک دوبخشی: برای ساخت یک دوبخشی، در هر کدام از 2^{75} گروه کلید، محاسبات زیر باید انجام پذیرد.

پیچیدگی ساخت دوبخشی در جهت رفت: برای ساخت یک دوبخشی در جهت رفت، ۲۱ جعبه جانشانی باید ۸ بار محاسبه شود. این جعبه‌های جانشانی با رنگ قرمز در شکل (۵) نشان داده شده است.

پیچیدگی ساخت دوبخشی در جهت برگشت: برای ساخت یک دوبخشی در جهت برگشت، ۱۳ جعبه جانشانی باید ۴ بار محاسبه شود. این جعبه‌های جانشانی با رنگ آبی در شکل (۵) نشان داده شده است. ۳۰ جعبه جانشانی باقی مانده که برای ساخت یک دوبخشی کافی مورد استفاده قرار می‌گیرد، فقط یک‌بار محاسبه شوند. بنابراین، در مجموع برای ساخت یک دوبخشی $۸ \times ۲۱ + ۴ \times ۱۳ + ۳۰ = ۲۵۰$ جعبه جانشانی باید محاسبه شود.

پیچیدگی مرحله فیلتر کلیدهای نادرست: در هر کدام از 2^{75} گروه کلید، برای حذف کلیدهای نادرست، محاسبات زیر باید انجام پذیرد.

پیچیدگی بررسی تصادم در جهت رفت: در این مرحله، ۳۴ جعبه جانشانی در الگوریتم رمز که با رنگ آبی در شکل (۵) نشان داده شده است و ۲ جعبه جانشانی در الگوریتم تولید زیرکلید، باید 2^{2} بار محاسبه شوند. ۲۷ جعبه جانشانی که با رنگ زرد نشان داده شده است فقط یک‌بار محاسبه می‌شوند. توجه داشته باشید که نیازی به محاسبه جعبه‌های جانشانی که با رنگ سفید نشان داده شده است نیست زیرا تأثیری در محاسبه مقدار متغیر درونی ϑ ندارند. عملیات فوق 2^{3} بار برای هر متن رمزشده C_i باید بازمحاسبه شود. بنابراین در مجموع در این مرحله $۸ \times (۴ \times \left(۲ + ۳۴\right) + ۲۷) = ۱۳۶۸$ جعبه جانشانی باید محاسبه شود.

پیچیدگی بررسی تصادم در جهت برگشت: در این مرحله، ۴۵ جعبه جانشانی در الگوریتم رمز که با رنگ قرمز در شکل (۵) نشان داده شده است و ۴ جعبه جانشانی در الگوریتم تولید زیرکلید، باید 2^{3} بار محاسبه شوند. ۲۳ جعبه جانشانی که با رنگ زرد نشان داده شده است فقط یک‌بار محاسبه می‌شوند. توجه داشته باشید که نیازی به محاسبه جعبه‌های جانشانی که با رنگ سفید نشان داده شده است، نیست زیرا تأثیری در محاسبه مقدار متغیر درونی ϑ ندارند. عملیات فوق 2^{2} بار برای هر متن رمزشده S_j باید بازمحاسبه شود. بنابراین در مجموع در این مرحله $۴ \times (۸ \times \left(۴۵ + ۴\right) + ۲۳) = ۱۶۶۰$ جعبه جانشانی باید محاسبه شود.

جستجوی کاندیدهای کلید صحیح: از آن‌جایی‌که در هر گروه کلید، 2^{5} کلید وجود دارد و تصادم در ۴ بیت بررسی می‌شود لذا احتمال باقی‌ماندن کلید به‌عنوان کاندیدی برای کلید صحیح 2^{-4} است بنابراین در هر گروه کلید $2^{5} \times 2^{-4} = 2$ کاندید برای کلید صحیح باقی می‌ماند.

پیچیدگی حمله دوبخشی: برای هر کدام از 2^{75} گروه کلید، عملیات بالا باید تکرار شود تا به کلید صحیح دست یابیم بنابراین در مجموع پیچیدگی محاسباتی حمله برابر است با:

$$2^{75} \times \left(\frac{250+1368+1660}{318} + 2\right) \approx 2^{78.62} \qquad (۴)$$

پیچیدگی داده: چون در هر دوبخشی، از یک مقدار ثابت برای متن اصلی دلخواه P_0، استفاده می‌شود لذا برای انجام این حمله حداکثر به 2^{48} متن اصلی منتخب نیاز است.

۶- نتایج و بحث

با توجه به این‌که حمله دوبخشی به نوعی یک حمله جستجوی جامع است لذا پیچیدگی محاسباتی این حمله به جستجوی جامع نزدیک است. بنابراین از این حمله می‌توان در حملاتی‌که در نهایت نیاز به جستجوی جامع درمیان کلیدهای کاندیدشده برای کلید صحیح است، استفاده کرد. پیشنهاد می‌شود که از ایده حمله دوبخشی در حمله‌هایی مانند حمله خطی صفر هم‌بستگی، که نیاز به جستجوی جامع در میان کلیدهای کاندیدشده برای کلید صحیح دارد، مورد استفاده قرار گیرد تا پیچیدگی محاسباتی جستجوی کلید صحیح کاهش یابد.

۷- نتیجه گیری

در این مقاله، ابتدا به معرفی دوبخشی نامتقارن پرداخته و یک دوبخشی نامتقارن روی ۸ دور ابتدایی الگوریتم رمز LBlock ساخته شد که منجر به یک حمله دوبخشی به کل الگوریتم رمز سبک‌وزن LBlock ارائه شد که پیچیدگی محاسباتی و داده آن به‌ترتیب $2^{۷۸/۶۲}$ و 2^{48} می‌باشد. پیچیدگی داده این حمله به مراتب پایین‌تر از پیچیدگی داده تمامی تحلیل‌های انجام‌شده به این الگوریتم است. با توجه به این‌که حمله، در واقع به نوعی حمله جستجوی کلی می‌باشد که از انجام محاسبات تکراری جلوگیری می‌کند، پیچیدگی محاسباتی این حمله نزدیک به جستجوی کلی می‌باشد.

۸- مراجع

[1] W. Diffie and M. E. Hellman, "Special feature exhaustive cryptanalysis of the NBS encryption standard," Computer, vol. 10, no. 6, pp. 74-84, June 1977.

[2] Y. Sasaki, "Meet-in-the-Middle preimage attacks on AES hashing modes and application to whirlpool," In Antoine Joux, editor, Fast Software Encryption, vol. 6733 of LNCS, pp. 378-396, Springer Berlin/Heidelberg, 2011.

[3] A. Bogdanov, D. Khovratovich, and C. Rechberger, "Biclique Cryptanalysis of the Full AES," ASIACRYPT 2011, LNCS, vol. 7073, pp. 344-371, Springer, Heidelberg 2011.

[4] W. Wu and L. Zang, "LBlock: A Lightweight block cipher," In Javier Lopez and Gene Tsudik, editors, Applied Cryptography and Network Security, vol. 6715 of LNCS, pp. 327-344, Springer Berlin/Heidelberg, 2011.

[5] S. Ahmadi, Z. Ahmadian, J. Mohajeri, and M. D. Aref, "Low-Data Complexity Biclique Cryptanalysis of Block Ciphers With Application to Piccolo and HIGHT," IEEE Transzctions on Information Forensics and Security," Vol. 9, no. 10, October 2014.

[6] Y. Wang, W. Wu, X. Yu, and L. Zang, "Security on LBlock against biclique cryptanalysis," in Information Security Applications, vol. 7690, Heidelberg, Germany:Springer-Verlag, pp. 1-14, 2012.

[7] F. Karakoç, H. Demirci, and A. E. Harmanci, "Impossible Differential Cryptanalysis of Reduced-Rund LBlock," In: Askoxylakis, I. G., Pöhls, H. C. ,Posegga, J. (eds.) WISTP 2012 LNCS, vol. 7322, pp. 179–188, Springer 2012.

[8] H. Soleimany and K. Nyberg, "Zero-correlation linear cryptanalysis of reduced-round LBlock Des," Codes Cryptography, vol. 73, no. 2, pp. 683–698, 2014.

[9] Y. Wang and W. Wu, "Improved multidimensional zero-correlation linear cryptanalysis and applications to LBlock and TWINE," In Information Security and Privacy - ACISP 2014, LNCS 8544, pp. 1 -16, Springer 2014.

Journal Of Electronical & Cyber Defence
Vol. 5, No. 2, 2017, Serial No. 18

Biclique Attack on Block Cipher LBlock with Low Data Complexity

M. Hadian Dehkordi*, R. Taghizadeh

*Iran University of scince and Technology

(Received: 19/07/2016, Accepted: 13/02/2017)

ABSTRACT

LBlock is a Lightweight block cipher, with a 64-bit block size and 80-bit key length. Biclique attack is a kind of MITM attack that has recently attracted lots of attention. Biclique cryptanalysis often breaks full version of the cipher on which many other existing attacks do not work. In this paper, firstly, asymmetric biclique is introduced, then by using low data complexity algorithm technique (LDC), a biclique attack on full round Lightweight block cipher LBlock is presented. The computation and data complexity of this attack are and, respectively. The data complexity is considerably less than the existing cryptanalytic result. The computational complexity remains the same as the previous ones.

Keywords: Lightweight, LBlock, Meet in the Middle Attack, Biclique Attack

* Corresponding Author Email: mhadian@iust.ac.ir