رمزنگاری پیشرفته ۲۵۱۷۲۱ ۲۹ اردیبهشت ۱۴۰۲

AES، تحلیل‌رمز تفاضلی ناممکن، حملات کانال جانبی

مدرس: سیاوش احمدی دانشگاه صنعتی شریف

اهداف تمرین

هدف از این تمرین در بخش الگوریتم AES، آشنایی مقدماتی با برخی از عملیات‌های به کار رفته در الگوریتم AES، و واررسی صحت برخی از روابط به کار رفته در آن است. در این تمرین به سوالاتی مانند تغییر الگوریتم AES و بررسی نتایج حاصل، پرداخته نشد است.
در بخش حمله‌ی تفاضل ناممکن، سوالات کلی پیرامون خود این حمله، پیچیدگی‌های داده‌ی این حمله به الگوریتم AES و نمونه‌ای از اِعمال این حمله به الگوریتم HIGHT مورد سوال واقع شده است.
در بخش حملات کانال جانبی، به حمله‌ی تحلیل توانی تفاضلی به الگوریتم AES، و نقاب‌گذاری [۱] گِیت‌ها به عنوان راهی برای مقابله با حملات تحلیل توان پرداخته شده است.

برخی از سوالات مستقیما از کتاب Stallings [۱] آورده شده‌اند که به آن‌ها ارجاع داده شده است. برخی دیگر از سوالات نیز در اسلایدهای درس به عنوان تمرین مطرح شده بودند.

فهرست مطالب

۱ الگوریتم AES ۱
۲ تحلیل‌رمز تفاضلی ناممکن ۳
۳ حملات کانال جانبی ۴

۱ الگوریتم AES

سوال ۱

سوال 6.1 [۱]. در بحث پیرامون MixColumns و InvMixColumns، گفته شد که

$$b(x) = a^{-1}(x) \mod (x^4 + 1)$$

که $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$ و $b(x) = \{0\mathrm{B}\}x^3 + \{0\mathrm{D}\}x^2 + \{09\}x + \{0E\}$.
نشان دهید که این تساوی برقرار است.

[۱] masking

سوال ۲

سوال 6.3 [۱]. هشت کلمه‌ی اول گسترش کلید برای یک کلید 128 بیتی تمام یک را محاسبه کنید.

سوال ۳

سوال 6.5 [۱]. نشان دهید $x^i \mod (x^4+1) = x^{i \mod 4}$.

سوال ۴

سوال 6.6 [۱]. برای هر یک از المان‌های الگوریتم DES، تفاوت‌ها را با المان قابل مقایسه‌ی با آن در الگوریتم AES ذکر کنید.

1- اندازه‌ی کلید

2- اندازه‌ی بلوک

3- S-box

4- تابع گسترش کلید

5- جایگشت اولیه و جایگشت نهایی

سوال ۵

سوال 6.8 [۱]. در زیربخش جنبه‌های پیاده‌سازی الگوریتم AES، یک فرمول جبری منفرد توسعه داده شد که چهار مرحله‌ی یک دور نوعی الگوریتم رمزگذاری را توصیف می‌کند. فرمولی معادل برای دور دهم ارائه کنید.

سوال ۶

صحت رابطه‌ی $\mathsf{MC}\Big(\mathsf{MC}\big(\mathsf{MC}(x)\big)\Big) = \mathsf{MC}^{-1}(x)$ را بررسی کنید.
ماتریس MixColumn الگوریتم AES و واورن آن به صورت زیر است:

$$\mathsf{MC} = \begin{bmatrix} 0x02 & 0x03 & 0x01 & 0x01 \\ 0x01 & 0x02 & 0x03 & 0x01 \\ 0x01 & 0x01 & 0x02 & 0x03 \\ 0x03 & 0x01 & 0x01 & 0x02 \end{bmatrix}$$

$$\mathsf{MC}^{-1} = \begin{bmatrix} 0x0e & 0x0b & 0x0d & 0x09 \\ 0x09 & 0x0e & 0x0b & 0x0d \\ 0x0d & 0x09 & 0x0e & 0x0b \\ 0x0b & 0x0d & 0x09 & 0x0e \end{bmatrix}$$

چندجمله‌ای مولد میدان $\mathsf{GF}(2^8)$ در الگوریتم AES، $p(x) = x^8 + x^4 + x^3 + x + 1$ است.

سوال ۷

اثبات کنید به کمک الگوریتم تعمیم یافته‌ی اقلیدس می‌توان معکوس ضربی را در ضرب تعریف شده در میدان $\mathrm{GF}(2^8)$ با چندجمله‌ای ساده‌نشدنی از درجه‌ی 8 روی $\mathbb{Z}_2$ بدست آورد.
به عبارت دیگر، اگر $b(x) \neq 0$ و $\deg(b(x)) < 8$، با استفاده از الگوریتم تعمیم یافته‌ی اقلیدس داریم:

$$b(x)a(x) + m(x)c(x) = 1$$

بنابراین:

$$a(x) \cdot b(x) = 1 \mod m(x)$$

یا

$$b^{-1}(x) = a(x) \mod m(x)$$

۲ تحلیل‌رمز تفاضلی ناممکن

سوال ۸

تناقض‌های 16 دوری زیر، که در اسلایدهای درس آمده است، را چک کنید.

$$(*, 0x80, 0, 0, 0, 0, 0, 0) \overset{16r}{\nrightarrow} (0, 0x80, 0, 0, 0, 0, 0, 0)$$
$$(e_1, 0x80, 0, 0, 0, 0, 0, 0) \overset{16r}{\nrightarrow} (0, 0x80, 0, 0, 0, 0, 0, 0)$$

که به این معنی است که:

$$(A, B, 0, 0, 0, 0, 0, 0) \overset{16r}{\nrightarrow} (0, 0x80, 0, 0, 0, 0, 0, 0)$$
$$(A, B) \in \{(e_1, 0x80), (e_0, 0x80), (e_1, 0)\}$$

سوال ۹

در حمله‌ی تفاضلی ناممکن به الگوریتم HIGHT مقاله‌ی [۲] که در اسلایدهای درس بررسی شد، برای جمع‌آوری داده داشتیم:

تعداد ساختارهای انتخاب شده: $2^n = 2^{2.3}$

چگونه این مقدار محاسبه شده است؟

سوال ۱۰

به سوالات زیر در مورد حمله‌ی تفاضل ناممکن پاسخ دهید.

1- مراحل اعمال حمله‌ی تفاضلی ناممکن را نام ببرید.

2- با ذکر دلیل، در حمله‌ی تفاضل ناممکن مواردی که در ادامه آورده می‌شود را باید بیشینه کرد یا کمینه؟ تعداد دورهای مربوط به تناقض، تعداد بیت‌های کلیدی که در فاز استخراج کلید وجود ندارد، جمع بیت‌های فعال در سمت متن اصلی و متن رمز شده.

3- در فاز استخراج کلید حمله‌ی تفاضل ناممکن به یک رمز قالبی با طول کلید n و طول قالب b بیت، فرض کنید ℓ_p و ℓ_c بیت فعال به ترتیب در سمت متن اصلی و متن رمز شده وجود دارد. تعداد جفت‌های متن اصلی موجود برای اعمال حمله را محاسبه کنید.

4- مطابق شکل ۱، یک تفاضل متن اصلی و متن رمز شده برای یک سناریوی حمله‌ی تفاضلی ناممکن روی الگوریتم AES-128 داده شده است. اگر برای تولید زوج‌های این حمله بخواهیم از مجموعه‌ی ساختار استفاده کنیم، تعداد کل مجموعه های ساختار، تعداد اعضای هر مجموعه‌ی ساختار و همچنین حداقل تعداد داده‌های مورد نیاز برای داشتن 2^{40} زوج دارای تفاضل مناسب در متن اصلی و متن رمز شده را محاسبه کنید.

5- آیا می‌توان برای حمله‌ی بند 4 از 2^{104} زوج دارای تفاضل مناسب در متن اصلی و متن رمز شده استفاده کرد؟ چرا؟

شکل ۱: تفاضل متن اصلی و متن رمز شده برای یک سناریوی حمله‌ی تفاضلی ناممکن روی الگوریتم AES-128

۳ حملات کانال جانبی

سوال ۱۱

1- حمله‌ی تحلیل توانی تفاضلی به الگوریتم AES، برای استخراج یک بایت از کلید در مرحله‌ی Subbyte، را شرح دهید.

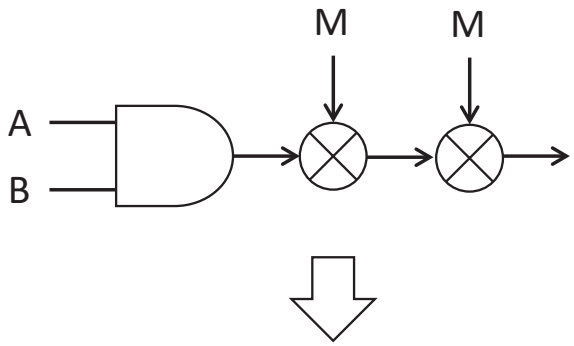
2- دلیل پایه‌ای یا الکترونیکی نشت اطلاعات از توان مصرفی چیست؟

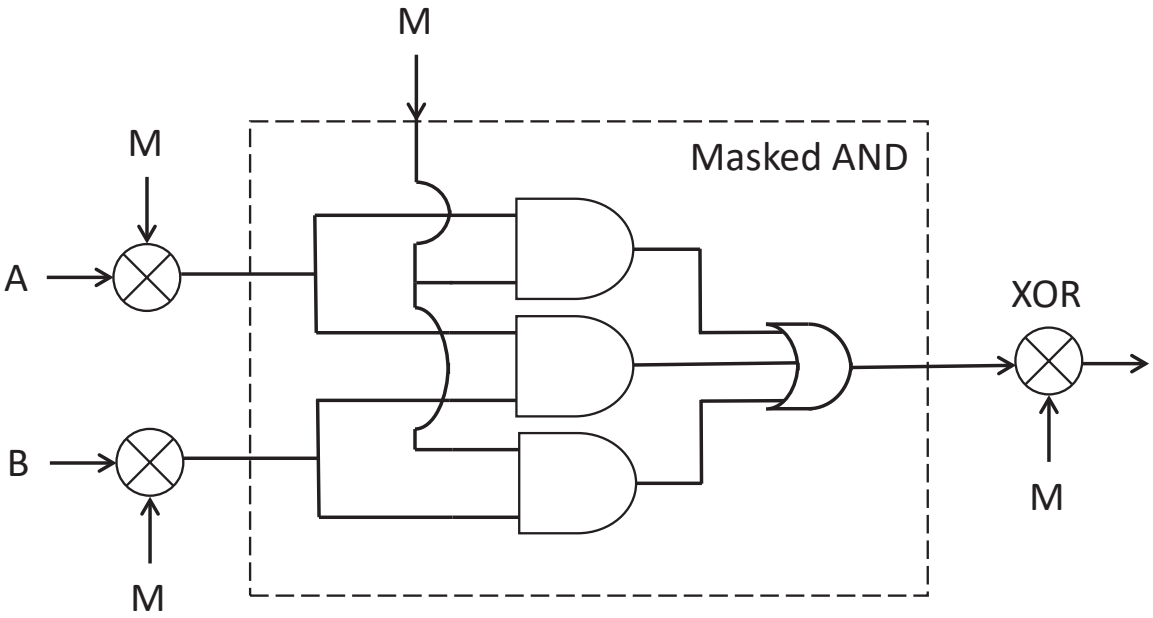
سوال ۱۲

در درس نقاب‌گذاری [۲] گیت AND ارائه شد که در شکل ۲ آمده است. با این کار، عملیات به گونه‌ای انجام می‌شود که برای تمام حالات توان یکسانی مصرف می‌کند. همان طوری که در جدول ۱، برای دو حالات $A = B = 1$ و $A = B = 0$، آمده است، اگر یک AND را با یک مقدار دوبار XOR کنیم، تغییری در مقدار خروجی گیت AND رخ نمی‌دهد. فایده‌ی این کار در این است که

[۲] Masking

محاسبه‌ی مدار نسبت به M مستقل است. $\Leftarrow$ پس می‌توان M را اعمال کرد و توان مصرفی را عوض کرد. می‌توان در جدول ۲ دید که گیت AND نقاب‌گذاری شده، همان جدول صحت گیت AND معمولی را دارد.
حال، شما یک مدار برای نقاب‌گذاری گیت OR ارائه دهید.
راهنمایی: از قانون دمورگان استفاده کنید.





شکل ۲: گیت AND نقاب‌گذاری شده

جدول ۱: دوبار XOR کردن گیت AND با یک مقدار

A	B	M	خروجی
1	1	1	1
1	1	0	1
0	0	1	0
0	0	0	0

جدول ۲: چک‌کردن عملکرد AND معمولی با AND نقاب‌گذاری شده

A	B	M	$M \oplus A$	$M \oplus B$	AND_1	AND_2	AND_3	OR	خروجی
1	1	1	0	0	0	0	0	0	1
1	1	0	1	1	0	1	0	1	1
1	0	1	0	1	0	0	1	1	0
1	0	0	1	0	0	0	0	0	0
0	1	1	1	0	1	0	0	1	0
0	1	0	0	1	0	0	0	0	0
0	0	1	1	1	1	1	1	1	0
0	0	0	0	0	0	0	0	0	0

مراجع

[1] William Stallings, ”*Cryptography and network security: principles and practice*”, 7th edition, Pearson, 2017.

[2] Seyyed Arash Azimi, Siavash Ahmadi, Zahra Ahmadian, Javad Mohajeri, Mohammad Reza Aref, ”*Improved impossible differential and biclique cryptanalysis of HIGHT*”, In WILEY, Vol. 31, No. 1, 10 January 2018. DOI:https://doi.org/10.1002/dac.3382.