رمزنگاری پیشرفته

هادی سلیمانی

پژوهشکده فضای مجازی دانشگاه شهید بهشتی

پاییز سال ۱۴۰۰

مجوز استفاده و نشر

- اجازه‌ی ایجاد نسخه‌های دیجیتالی جدید براساس بخشی یا تمام مطالب این اسلاید بدون پرداخت هزینه اعطا می‌شود، مشروط بر این‌که:
  - فقط به‌منظور و در راستای استفاده‌ی آموزشی (شخصی و یا کلاسی) ساخته شده باشند و برای کسب هرگونه سود و یا مزیت تجاری استفاده نشوند.
  - نسخه‌های جدید حاوی ارجاع مستقیم به نام تهیه‌کننده اسلاید (هادی سلیمانی) و محل کار وی (پژوهشکده فضای مجازی دانشگاه شهید بهشتی) باشند.
- مجموعه‌ی حاضر براساس نظرات ارزشمند دانشجویان (سابق) دانشگاه شهید بهشتی و همکاران محترم تهیه شده است که از تمام آن‌ها قدردانی می‌شود؛

(به‌خصوص خانم‌ها **سارا زارعی و فاطمه عزیزی** نقش مهمی را در تهیه نسخه‌ی نهایی بر عهده داشته‌اند. خانم مهندس زارعی علاوه بر کمک در آماده‌سازی نسخه‌ی فعلی اسلایدها، در تصحیح اشتباهات نسخه‌ی قبلی و همچنین تکمیل و بازتعریف محتوای درس‌ها بسیار تاثیرگذار بوده‌اند).

- برای مشاهده‌ی اسلایدها و ویدئوهای تدریس این درس به آدرس زیر مراجعه فرمایید:

http://facultymembers.sbu.ac.ir/h_soleimany/advanced-cryptography-course/

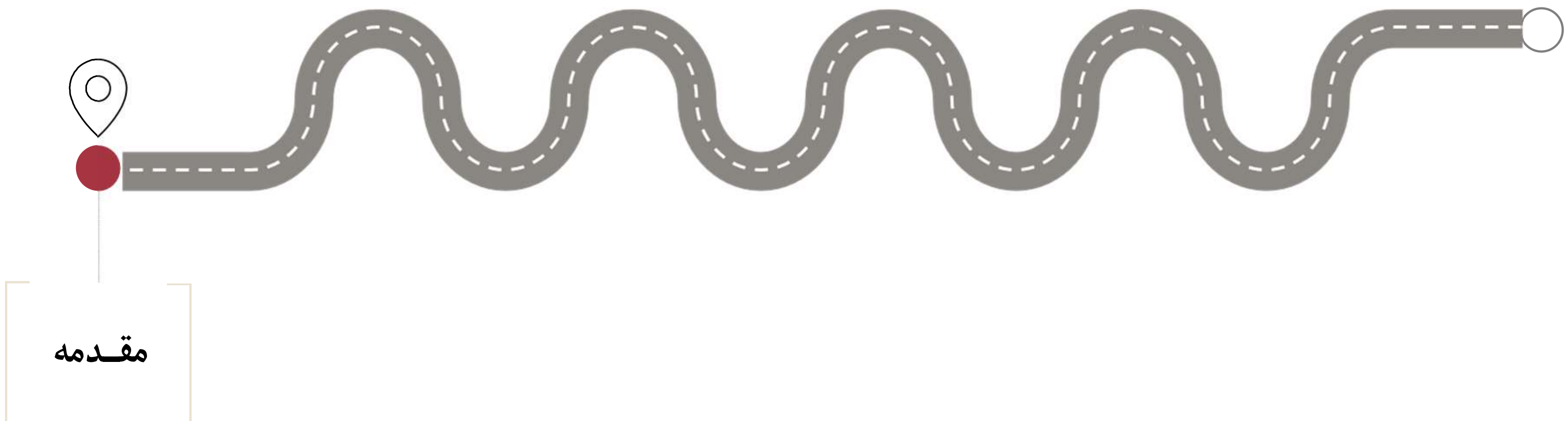
درس دوم

تحلیل خطی

فهرست عناوین درس

تحلیل خطی

- مقدمه
- تقریب خطی عملگرهای مختلف تابع دور
- محاسبه‌ی اریبی تقریب خطی برای یک دور
- مسیرخطی
- استفاده از تقریب خطی به عنوان تمایزگر
- استفاده از تقریب خطی برای بازیابی کلید
- پیچیدگی داده در تحلیل خطی
- امنیت DES و AES در مقابل تحلیل خطی
- برخی مباحث تکمیلی
- جمع‌بندی


مقدمه

تعاریف اولیه: ضرب داخلی

(Inner Product)

- برای بردارهای $\boldsymbol{a} = (a_1, \dots, a_n)$ و $\boldsymbol{b} = (b_1, \dots, b_n)$ که a_iها و b_iها در آن‌ها مقادیری باینری هستند، ضرب داخلی به صورت زیر تعریف می‌شود:

$$\boldsymbol{a}.\boldsymbol{b} = \sum_{i=1}^{n} a_i b_i$$

به تعبیر دیگر، $\boldsymbol{a}$ ماسک یا نقاب خطی (Linear Mask) بردار $\boldsymbol{b}$ خوانده می‌شود.

- مثال (محاسبات در $GF(2)$):

$$(1,1,0,0,1).(0,1,1,1,1) = 0 + 1 + 0 + 0 + 1 = 0$$

تعاریف اولیه: تابع بولی

(Boolean Function)

- هر تابعی را که m متغیر باینری ورودی $(\{0,1\}^m)$ را به یک متغیر باینری خروجی $(\{0,1\})$ نگاشت کند، تابع بولی گویند:

$$f: \mathbb{F}_2^m \to \mathbb{F}_2$$

- تابع بولی خطی را می‌توان به شکل $x \mapsto a.x$ توصیف کرد.
- تابع بولی می‌تواند به صورت برداری (Vectorial Boolean Function) نیز باشد که به صورت زیر تعریف می‌شود:

$$f = \mathbb{F}_2^m \to \mathbb{F}_2^n \text{ where } f = (f_1, \dots, f_n)$$

- ضریب فوریه‌ی تابع بولی برداری $f = \mathbb{F}_2^m \to \mathbb{F}_2^n$ در نقطه‌ی $(u,v) \in \mathbb{F}_2^m \times \mathbb{F}_2^n$ به شکل زیر تعریف می‌شود:

$$\hat{F}(u,v) = \sum_x (-1)^{u.x \oplus v.f(x)}$$

مفهوم تقریب خطی

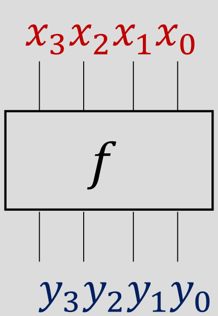
(Linear Approximation)

- برای تابع بولی برداری $f:\mathbb{F}_2^n \to \mathbb{F}_2^m$ با ورودی $x \in \mathbb{F}_2^n$ یک تقریب خطی با نقاب ورودی $u \in \mathbb{F}_2^n$ و نقاب خروجی $v \in \mathbb{F}_2^m$ به شکل زیر تعریف می‌شود:

$$x \mapsto u.x \oplus v.f(x)$$

- مفهوم ساده: xor تعدادی از بیت های ورودی و خروجی.
- مثال: تقریب خطی تابع $f:\mathbb{F}_2^4 \to \mathbb{F}_2^4$ با نقاب ورودی $u = 0x6$ و نقاب خروجی $v = 0x\mathrm{b}$ به صورت زیر محاسبه می‌شود:

$u = 0\,\mathbf{1}\,\mathbf{1}\,0$



$v = \mathbf{1}\,0\,\mathbf{1}\,\mathbf{1}$

$$u.x = x_2 \oplus x_1$$

$$v.f(x) = y_3 \oplus y_1 \oplus y_0$$

$$x \mapsto x_2 \oplus x_1 \oplus y_3 \oplus y_1 \oplus y_0$$

مفهوم احتمال تقریب خطی

- احتمال یک تقریب خطی به صورت زیر تعریف می‌شود:

$$p_f(u,v) = \Pr[u.x \oplus v.f(x) = 0] = \Pr[u.x = v.f(x)]$$

- این احتمال برای یک جایگشت ایده‌آل چقدر است؟
- اگر بین خروجی الگوریتم و ورودی الگوریتم هیچ رابطه‌ی آماری‌ای وجود نداشته باشد، آن‌گاه داریم:

$$p_f(u,v) = \Pr[u.x = v.f(x)] = \Pr[u.x = 0] = 1/2$$

- بنابراین هرچه احتمال تقریب خطی یک تابع از مقدار ½ فاصله داشته باشد، مشخصات آماری تابع از حالت تصادفی فاصله‌ی بیشتری دارد.

مفهوم اریبی و همبستگی

(Correlation) & (Bias)

- اریبی به‌صورت فاصله‌ی احتمال تقریب خطی از 1/2 تعریف می‌شود:

$\epsilon_f(u,v) = p_f(u,v) - 1\backslash 2 \, , -1\backslash 2 \leq \epsilon_f \leq 1/2$

- هرچه قدر مطلق اریبی بیشتر باشد، به‌معنای فاصله‌ی بیشتر از رفتار تصادفی است.
- در تحلیل خطی چون به دنبال ویژگی غیرتصادفی هستیم، عموما از اریبی تقریب خطی (به جای احتمال آن) استفاده می‌شود.
- در مقالات و مباحث پیشرفته‌تر، به جای اریبی از همبستگی تقریب خطی استفاده می‌شود (علت: نرمال‌سازی).
  - تعریف همبستگی به این صورت است:

$c_f(u,v) = 2\epsilon_f(u,v)$

- در این درس ما به منظور سادگی، تحلیل خطی را با استفاده از اریبی معرفی خواهیم کرد.

نمای کلی از تحلیل خطی و هدف آن

- الگوریتم رمزنگاری قالبی، یک تابع بولی برداری است:

$C = E_K(M) = f(M, K) \qquad , \qquad f: \mathbb{F}_2^b \times \mathbb{F}_2^k \to \mathbb{F}_2^b$

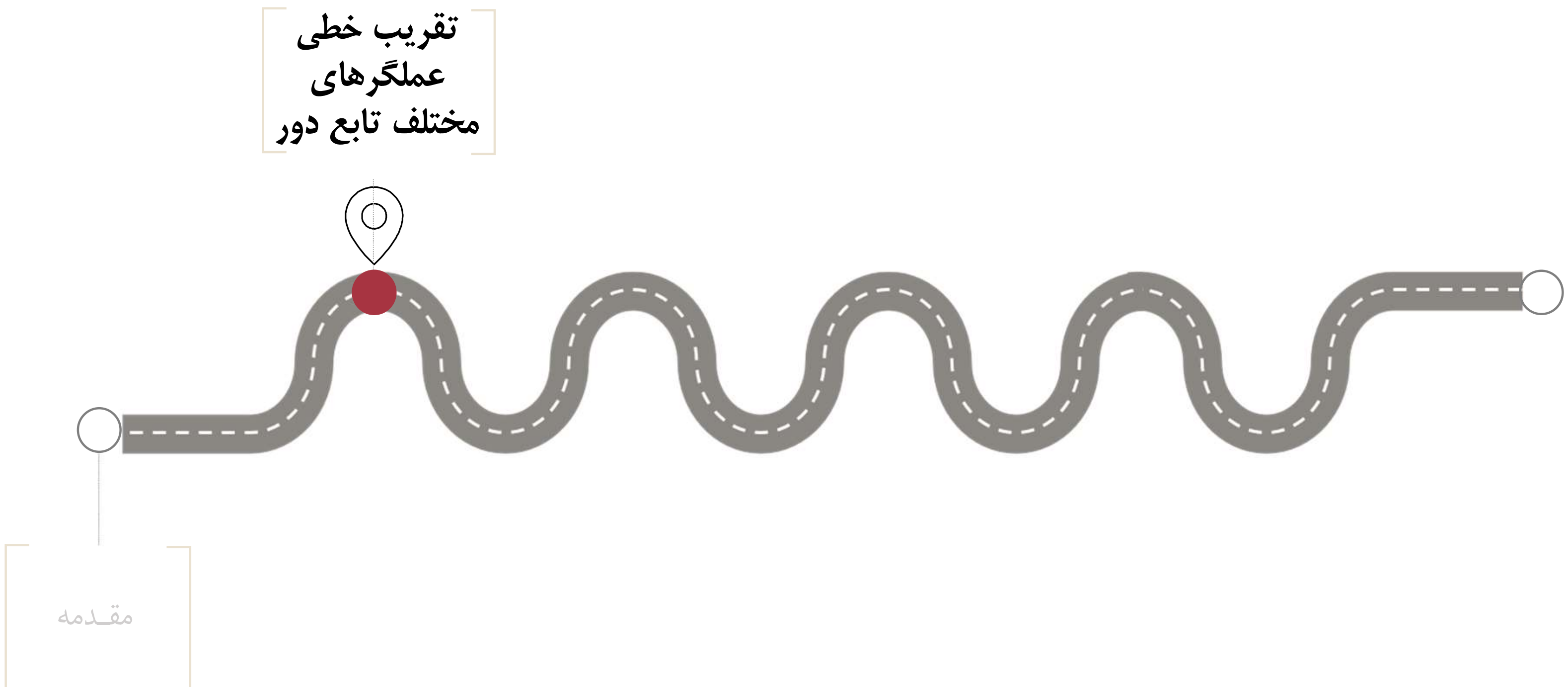
- تقریب خطی رمز قالبی b بیتی تحت کلید نامعلوم K را به شکل زیر تعریف می‌کنیم:

$u.M \oplus v.C \oplus \omega.K \quad ; \quad u, v \in \mathbb{F}_2^b, \omega \in \mathbb{F}_2^k$

- **تکنیک به کار رفته توسط ماتسوئی (Eurocryp1993):** پیدا کردن نقاب‌های ورودی و خروجی (u,v) برای یک الگوریتم رمزنگاری قالبی $C = E_K(M)$ به نحوی که قدر مطلق اریبی زیاد باشد (از صفر فاصله داشته باشد).

$$|\epsilon_E(u, v)| = |\Pr[u.M = v.C] - 1/2| > 0$$

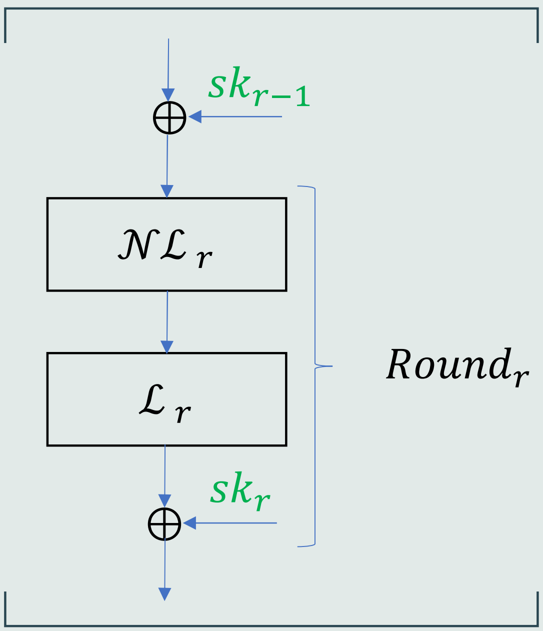
- سناریوی به کار رفته در تحلیل خطی سناریوی "متن اصلی معلوم" است، چون برای اجرای آن به متون خاصی نیاز نداریم.
- به دورهای کاهش‌یافته‌ی اکثر رمزهای قالبی قابل اعمال است.


تقریب خطی
عملگرهای
مختلف تابع دور
مقـدمه

ساختار (معمول) تابع دور

یادآوری

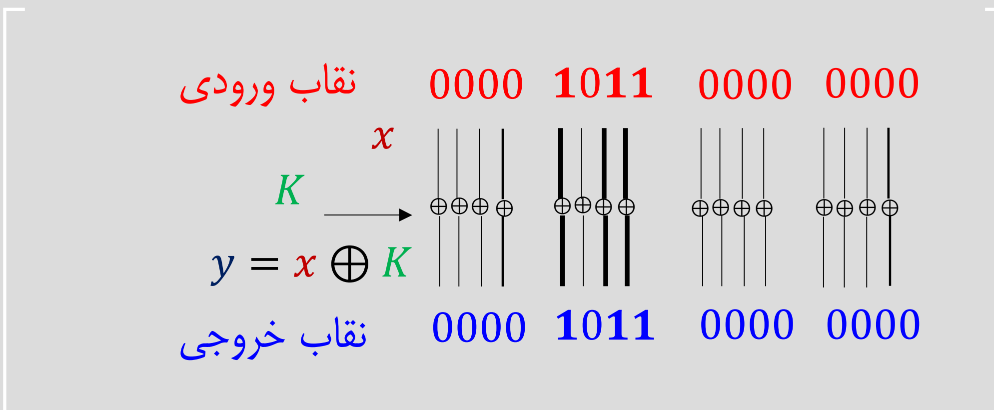
- ساختار دور در رمزهای قالبی به طور معمول شامل سه لایه‌ی غیرخطی ($\mathcal{NL}_r$)، خطی ($\mathcal{L}_r$) و اضافه شدن کلید دور(sk_r) است.
- در دور اول ($r = 1$)، متن اصلی پیش از ورود به ساختار دور با کلید سفیدسازی (sk_0) نیز جمع می‌شود.
- تقریب خطی هر کدام از اجزای مختلف این ساختار؟



تقریب خطی اضافه شدن کلید

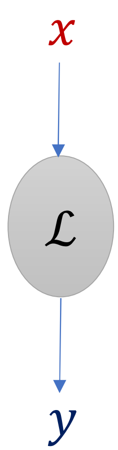
- اگر کلید به صورت xor اضافه شود، تقریب‌های خطی متعددی با احتمال 1 و اریبی 1/2 (حداکثر اریبی ممکن) بین ورودی، کلید و خروجی وجود دارد.
- چگونه؟
- کافی است که نقاب ورودی، نقاب کلید و نقاب خروجی با هم برابر باشند:

$$x = y \oplus K \qquad \Rightarrow \alpha . x = \alpha . y \oplus \alpha . K$$



تقریب خطی لایه‌ی خطی

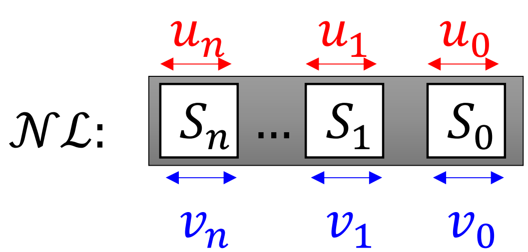
- تقریب خطی با نقاب ورودی u و نقاب خروجی v برای نگاشت خطی $\mathcal{L}(x) = \boldsymbol{M}x$ دارای اریبی 1/2 (حداکثر) است، اگر و فقط اگر: $u = \boldsymbol{M}v$.



$$y = \boldsymbol{M}x \;\Rightarrow v.y = v.(\boldsymbol{M}x) \;= \boldsymbol{M}(v.x) \;= \underbrace{(\boldsymbol{M}v)}_{u}.x$$

تقریب خطی لایه‌ی غیرخطی

- چالش: تقریب خطی لایه‌ی غیرخطی و محاسبه‌ی اریبی آن به خصوص برای تابعی با طول قالب بزرگ، ممکن است که در عمل کار چندان ساده‌ای نباشد (براساس مشخصات تابع).
- راه‌کار: شکستن مسئله به مسئله‌های کوچک‌تر و حل آن‌ها!
  - یادآوری: لایه‌ی غیرخطی رمزهای قالبی به طور معمول از عناصر کوچکتری موسوم به جعبه‌های جانشانی تشکیل شده است.
- ابتدا اریبی تقریب خطی (u_i, v_i) را برای یک جعبه‌ی جانشانی محاسبه کرده، و سپس بررسی می‌کنیم که چگونه می‌توان بر اساس اریبی جعبه‌های جانشانی، اریبی کل تابع غیرخطی را تخمین زد.



تقریب خطی لایه‌ی غیرخطی

محاسبه‌ی اریبی جعبه‌ی جانشانی

- می‌خواهیم اریبی تقریب خطی با نقاب‌های ورودی و خروجی (u,v) را برای جعبه‌ی جانشانی $S: \mathbb{F}_2^m \to \mathbb{F}_2^n$ محاسبه کنیم.
- راه‌کار؟

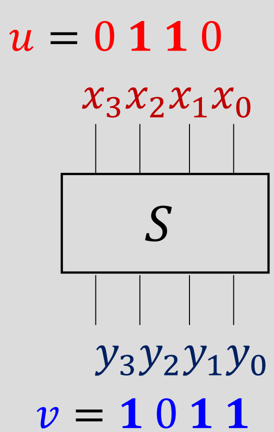
1. ابتدا باید به‌ازای تمام مقادیر ورودی $x \in \mathbb{F}_2^m$، بررسی کنیم که رابطه‌ی $u.x \oplus v.S(x) = 0$ چند بار برقرار است.
2. سپس باید فاصله‌ی عدد به‌دست آمده را از 2^{m-1} (نصف کل حالات ممکن) محاسبه کنیم.
3. فاصله‌ی محاسبه شده در مرحله‌ی قبل را بر 2^m (کل حالات ممکن) تقسیم می‌کنیم.

مثالی از محاسبه‌ی اریبی جعبه‌ی جانشانی

- جعبه‌ی جانشانی ۴ بیت به ۴ بیت S با توصیف زیر را در نظر بگیرید:

x	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
$S(x)$	E_x	4_x	D_x	1_x	2_x	F_x	B_x	8_x	3_x	A_x	6_x	C_x	5_x	9_x	0_x	7_x

- می‌خواهیم اریبی این جعبه‌ی جانشانی را برای تقریب خطی با نقاب ورودی $u = 0x6 = 0110$ و نقاب خروجی $v = 0xb = 1011$ محاسبه کنیم.



$$u.x = x_2 \oplus x_1$$

$$v.S(x) = y_3 \oplus y_1 \oplus y_0$$

$$x \mapsto x_2 \oplus x_1 \oplus y_3 \oplus y_1 \oplus y_0$$

Example's source: A Tutorial on Linear and Differential Cryptanalysis by Howard M. Heys

مثالی از محاسبه‌ی اریبی جعبه‌ی جانشانی

ادامه ...

$x_3x_2x_1x_0$	$y_3y_2y_1y_0$	$u.x = x_2 \oplus x_1$	$v.S(x) = y_3 \oplus y_1 \oplus y_0$
0000	1110	0	0
0001	0100	0	0
0010	1101	1	0
0011	0001	1	1
0100	0010	1	1
0101	1111	1	1
0110	1011	0	1
0111	1000	0	1
1000	0011	0	0
1001	1010	0	0
1010	0110	1	1
1011	1100	1	1
1100	0101	1	1
1101	1001	1	0
1110	0000	0	0
1111	0111	0	0

مرحله‌ی ۱

مرحله‌ی ۲

نصف حالات ممکن
$(m = 4)$

$$12 - 8 = 4$$

فاصله از حالت تصادفی (با اریبی رابطه‌ی مستقیم دارد)

مرحله‌ی ۳

$$\epsilon = \frac{4}{2^4} = 0.25$$

جدول تقریب خطی جعبه‌ی جانشانی

- می‌توان فاصله (عدد به‌دست آمده در مرحله‌ی ۲) را به‌ازای تمام نقاب‌های ورودی و نقاب‌های خروجی ممکن محاسبه کرد (با روش مثال قبل).
- اگر هر عدد را در سطر u و ستون v جدولی ذخیره کنیم، جدول به‌دست آمده جدول تقریب خطی آن جعبه‌ی جانشانی نام دارد.
- به عنوان نمونه تقریب خطی با نقاب‌های ورودی $u = 0x6$ و خروجی $v = 0xb$، برای جعبه‌ی جانشانی مثال قبلی دارای عدد فاصله‌ی 4 بود که آن را در سطر و ستون مربوط به خود قرار می‌دهیم.

نقاب خروجی (v)

نقاب ورودی (u)

	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x																
1_x																
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$
6_x												4				
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
F_x																

جدول تقریب خطی جعبه‌ی جانشانی

ادامه ...

- تکمیل جدول تقریب خطی برای جعبه‌ی جانشانی مثال قبل.

نقاب خروجی (v)

نقاب ورودی (u)

	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	-2	-2	0	0	-2	6	2	2	0	0	2	2	0	0
2_x	0	0	-2	-2	0	0	-2	-2	0	0	2	2	0	0	-6	2
3_x	0	0	0	0	0	0	0	0	2	-6	-2	-2	2	2	-2	-2
4_x	0	2	0	-2	-2	-4	-2	0	0	-2	0	2	2	-4	2	0
5_x	0	-2	-2	0	-2	0	4	2	-2	0	-4	2	0	-2	-2	0
6_x	0	2	-2	4	2	0	0	2	0	-2	2	4	-2	0	0	-2
7_x	0	-2	0	2	2	-4	2	0	-2	0	2	0	4	2	0	2
8_x	0	0	0	0	0	0	0	0	-2	2	2	-2	2	-2	-2	-6
9_x	0	0	-2	-2	0	0	-2	-2	-4	0	-2	2	0	4	2	-2
A_x	0	4	-2	2	-4	0	2	-2	2	2	0	0	2	2	0	0
B_x	0	4	0	-4	4	0	4	0	0	0	0	0	0	0	0	0
C_x	0	-2	4	-2	-2	0	2	0	2	0	2	4	0	2	0	-2
D_x	0	2	2	0	-2	4	0	2	-4	-2	2	0	2	0	0	2
E_x	0	2	2	0	-2	-4	0	2	-2	0	0	-2	-4	2	-2	0
F_x	0	-2	-4	-2	-2	0	2	0	0	-2	4	-2	-2	0	2	0

مشاهده‌ی ۱ در مورد جدول تقریب خطی

- مقادیر جدول می‌توانند مثبت یا منفی باشند.
- تقریب‌های خطی‌ای که دارای قدرمطلق فاصله (که با اریبی متناسب است) بیش‌تری هستند، می‌توانند موردتوجه مهاجم قرار گیرند.

نقاب خروجی (v)

نقاب ورودی (u)

	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	-2	-2	0	0	-2	6	2	2	0	0	2	2	0	0
2_x	0	0	-2	-2	0	0	-2	-2	0	0	2	2	0	0	-6	2
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
E_x	0	2	2	0	-2	-4	0	2	-2	0	0	-2	-4	2	-2	0
F_x	0	-2	-4	-2	-2	0	2	0	0	-2	4	-2	-2	0	2	0

مشاهده‌ی ۲ در مورد جدول تقریب خطی

- اگر تعداد دفعاتی که $u.x \oplus v.S(x)$ برابر 0 می‌شود با تعداد دفعاتی که برابر 1 می‌شود، برابر باشند، رفتار آماری جعبه‌ی جانشانی برای آن تقریب خطی شبیه حالت ایده‌آل است.
- بنابراین، تقریب‌های خطی با اریبی 0 نمی‌توانند موردتوجه مهاجم قرار گیرند.

نقاب خروجی (v)

نقاب ورودی (u)

	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	-2	-2	0	0	-2	6	2	2	0	0	2	2	0	0
2_x	0	0	-2	-2	0	0	-2	-2	0	0	2	2	0	0	-6	2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
E_x	0	2	2	0	-2	-4	0	2	-2	0	0	-2	-4	2	-2	0
F_x	0	-2	-4	-2	-2	0	2	0	0	-2	4	-2	-2	0	2	0

مشاهده‌ی ۳ در مورد جدول تقریب خطی

- برای نقاب ورودی و نقاب خروجی صفر داریم: $u.x = 0.x = 0, v.S(x) = 0.S(x) = 0$
- بنابراین به‌ازای تمامی مقادیر ممکن برای ورودی x، رابطه‌ی $u.x \oplus v.S(x) = 0$ همیشه برقرار است (مستقل از ویژگی‌های جعبه‌ی جانشانی).
- این حالت برای مهاجم ایده‌آل است، چرا که اریبی دارای حداکثر مقدار ممکن است.
  - در ادامه‌ی درس خواهیم دید که اگر کل لایه‌ی غیرخطی (شامل چند جعبه‌ی جانشانی) را در نظر بگیریم، این حالت می‌تواند مفید باشد.

نقاب خروجی (v)

نقاب ورودی (u)

	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	-2	-2	0	0	-2	6	2	2	0	0	2	2	0	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
F_x	0	-2	-4	-2	-2	0	2	0	0	-2	4	-2	-2	0	2	0

مشاهده‌ی ٤ در مورد جدول تقریب خطی

- برای $u = 1$ و $v = 0$ تقریب خطی به این صورت است: $u.x \oplus v.S(x) = 1.x_1 \oplus 0.S(x) = x_1$
- چون دقیقا به‌ازای نصف مقادیر ورودی $x_1 = 1$ و به‌ازای نصف دیگر آن‌ها $x_1 = 0$ است، اریبی این تقریب خطی 0 است.
- اگر نقاب ورودی غیر صفر و نقاب خروجی 0 باشد، اریبی تقریب خطی (مستقل از ویژگی‌های جعبه‌ی جانشانی) 0 است.
- اگر نقاب خروجی غیر صفر و نقاب ورودی 0 باشد، اریبی تقریب خطی (در صورت پوشا بودن جعبه‌ی جانشانی) 0 است.

نقاب خروجی (v)

نقاب ورودی (u)

	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	-2	-2	0	0	-2	6	2	2	0	0	2	2	0	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
F_x	0	-2	-4	-2	-2	0	2	0	0	-2	4	-2	-2	0	2	0

تقریب خطی لایه‌ی غیرخطی

ادامه ...

- جمع‌بندی و مرور محاسبه‌ی اریبی لایه‌ی غیرخطی تا این لحظه:

- قدم اول: محاسبه‌ی اریبی تقریب‌های خطی جعبه‌های جانشانی به عنوان اجزاء تشکیل‌دهنده‌ی لایه‌ی غیرخطی. ✓

- قدم دوم: محاسبه‌ی اریبی تقریب خطی کل تابع غیرخطی بر اساس اریبی جعبه‌های جانشانی.

چگونه؟

لم Piling Up

- اگر متغیرهای تصادفی باینری Y_1 و Y_2 مستقل باشند و اریبی آنها به ترتیب برابر با ϵ_1 و ϵ_2 باشد، اریبی $Y_1 \oplus Y_2$ برابر $2\epsilon_1\epsilon_2$ است.

اثبات:

$$\Pr[Y_1 = 0] = p_1 = 1\backslash 2 + \epsilon_1$$
$$\Pr[Y_2 = 0] = p_2 = 1\backslash 2 + \epsilon_2$$
$$\begin{aligned}
\Pr[Y_1 \oplus Y_2 = 0] &= \Pr[Y_1 = Y_2] \\
&= \Pr[Y_1 = Y_2 = 0] + \Pr[Y_1 = Y_2 = 1] \\
&= p_1p_2 + (1 - p_1)(1 - p_2) \\
&= 2p_1p_2 + 1 - p_1 - p_2 \\
&= 2(1\backslash 4 + 1\backslash 2\epsilon_1 + 1\backslash 2\epsilon_2 + \epsilon_1\epsilon_2) + 1 - 1\backslash 2 - \epsilon_1 - 1\backslash 2 - \epsilon_2 \\
&= 1\backslash 2 + \epsilon_1 + \epsilon_2 + 2\epsilon_1\epsilon_2 - \epsilon_1 - \epsilon_2 \\
&= 1\backslash 2 + 2\epsilon_1\epsilon_2 \Rightarrow \epsilon = 2\epsilon_1\epsilon_2
\end{aligned}$$

تعمیم یافته‌ی لم Piling Up

- اگر متغیرهای تصادفی باینری Y_1 و Y_2 و … و Y_n مستقل باشند و اریبی متغیر تصادفی Y_i را با ϵ_i نمایش دهیم، اریبی $Y_1 \oplus Y_2 \oplus \cdots \oplus Y_n$ برابر است با:

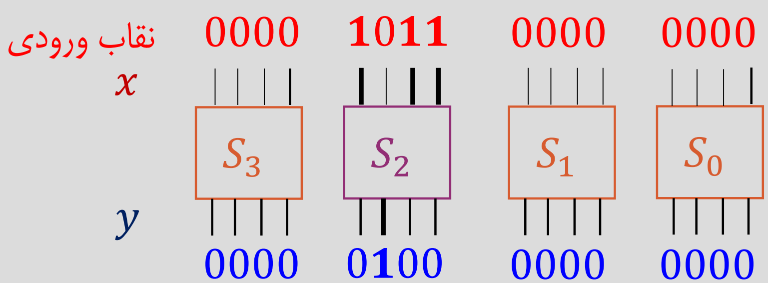
$$\epsilon = 2^{n-1} \prod_{i=1}^{n} \epsilon_i$$

- با در نظر گرفتن تعریف همبستگی، می‌توان معادل رابطه‌ی فوق را برای همبستگی نیز به صورت زیر به‌دست آورد:

$$c = \prod_{i=1}^{n} c_i$$

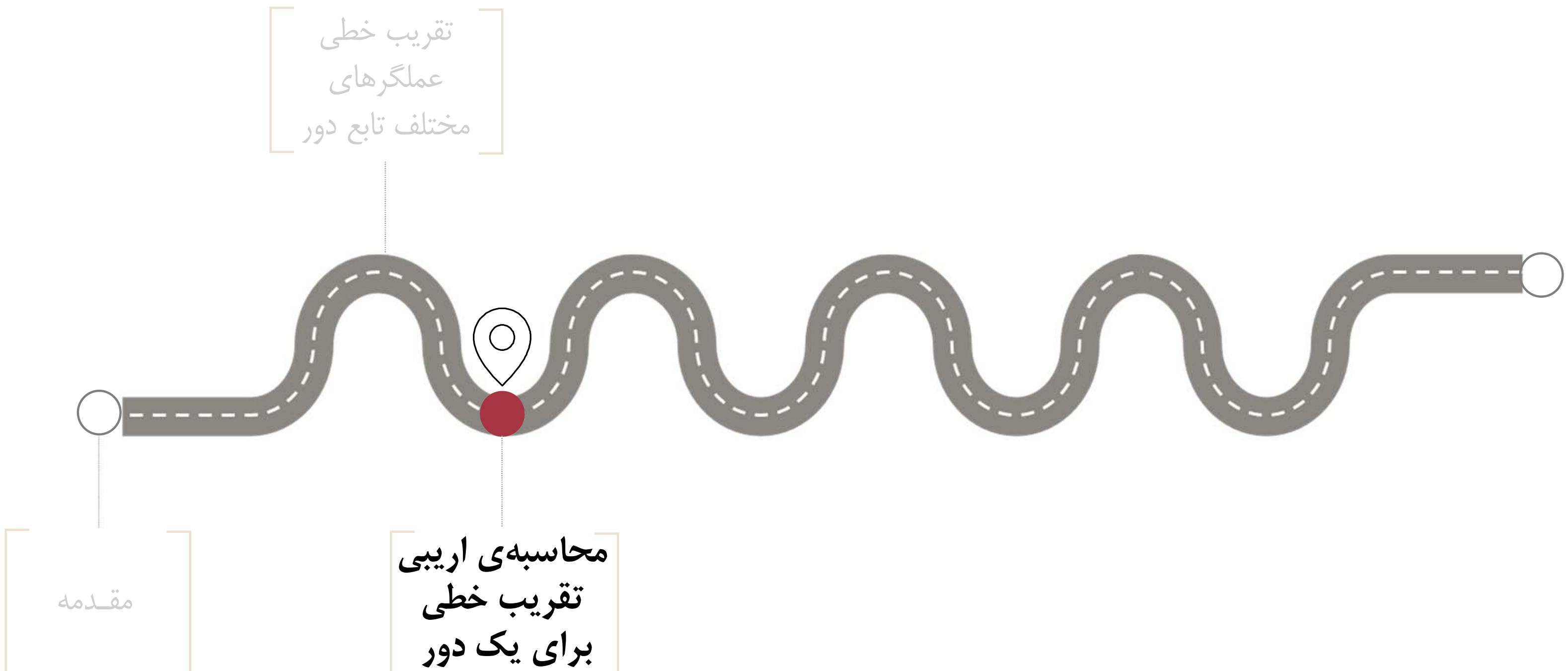
محاسبه‌ی اریبی تابع غیرخطی

- اریبی تقریب خطی ($u = b$ و $v = 4$) جعبه‌ی جانشانی دوم را می‌توان با مراجعه به جدول خطی جعبه‌ی جانشانی (و تقسیم مقدار بر 16) محاسبه کرد.
  - در این مثال اریبی برابر $\frac{1}{4} = \frac{4}{16}$ است.
- اریبی سایر جعبه‌های جانشانی برابر ½ است.
- براساس لم Piling Up، اریبی کل تقریب خطی برای لایه‌ی غیرخطی برابر است با $\frac{1}{4} = \frac{1}{4} \times \left(\frac{1}{2}\right)^3 \times 2^{4-1} = \epsilon$.
- همان‌طور که مشاهده می‌شود (و قابل پیش‌بینی نیز بود)، جعبه‌های جانشانی با نقاب ورودی و خروجی 0 تاثیری در اریبی ندارند.



$$x_8 \oplus x_9 \oplus x_{11} = y_{10}$$

شماره‌گذاری بیت‌ها از سمت راست به چپ (شروع از 0) است.


تقریب خطی
عملگرهای
مختلف تابع دور
مقدمه
محاسبه‌ی اریبی
تقریب خطی
برای یک دور

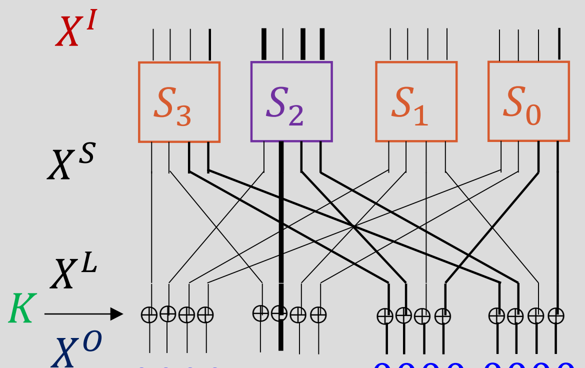
■ تقریب خطی برای یک دور

- مفهوم: Xor مجموعه‌ای از بیت‌های خروجی دور را با Xor مجموعه‌ای از بیت‌های ورودی دور و مجموعه‌ای از بیت‌های زیرکلید، تقریب زدیم.
- همان‌طور که انتظار داشتیم، اضافه شدن کلید تاثیری در مقدار اریبی ندارد.
- لایه‌ی خطی، تاثیری در اریبی ندارد اما مقدار نقاب خروجی براساس آن تعیین می‌شود.

$$\boxed{\epsilon = 1/4}$$

$$\Rightarrow X^I[8] \oplus X^I[9] \oplus X^I[11] \oplus K[10] = X^O[10]$$

نقاب ورودی 0000 **1011** 0000 0000



نقاب خروجی 0000 0100 0000 0000

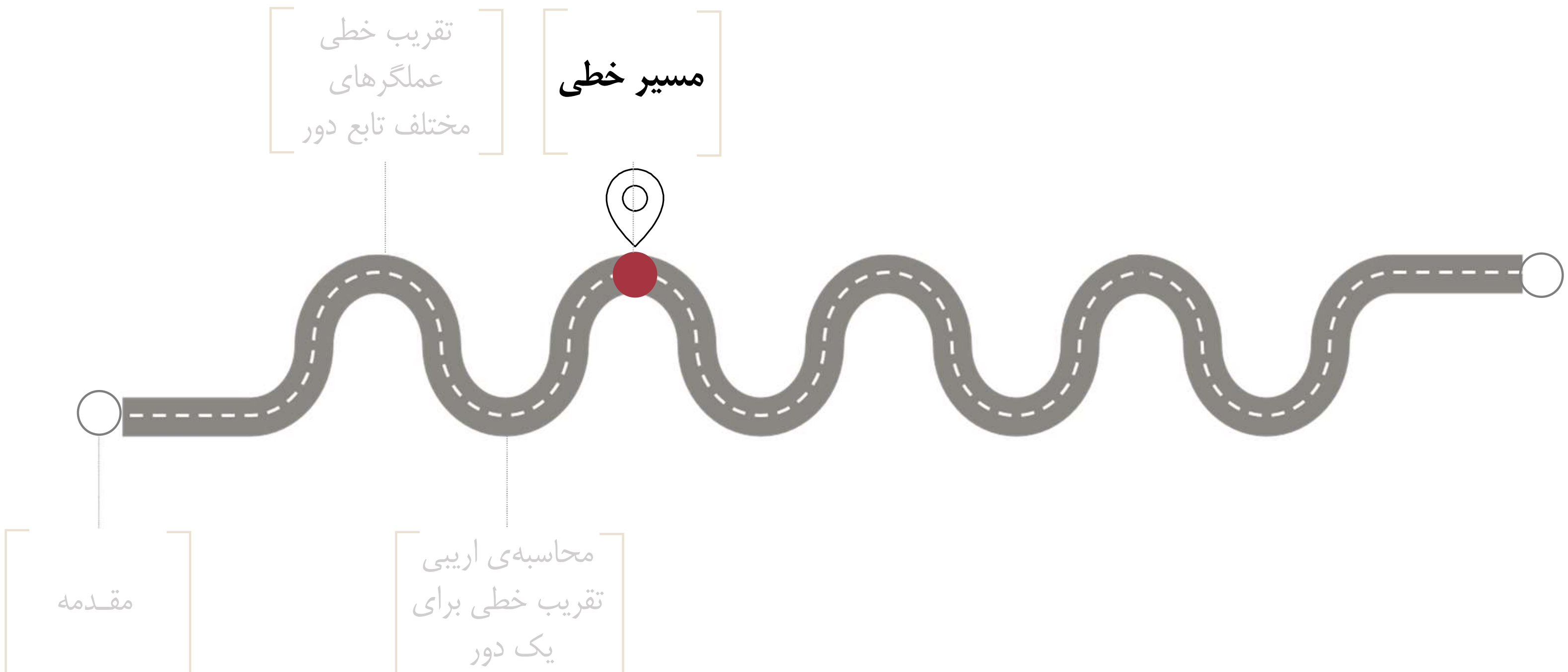
$$\boxed{\epsilon = 1/4}$$

$$X^I[8] \oplus X^I[9] \oplus X^I[11] = X^S[10]$$

$$X^S[10] = X^L[10]$$

$$X^L[10] = K[10] \oplus X^O[10]$$

توجه: شماره‌گذاری بیت‌ها از سمت راست به چپ (شروع از 0) است.


تقریب خطی عملگرهای مختلف تابع دور
مسیر خطی
مقـدمه
محاسبه‌ی اریبی تقریب خطی برای یک دور

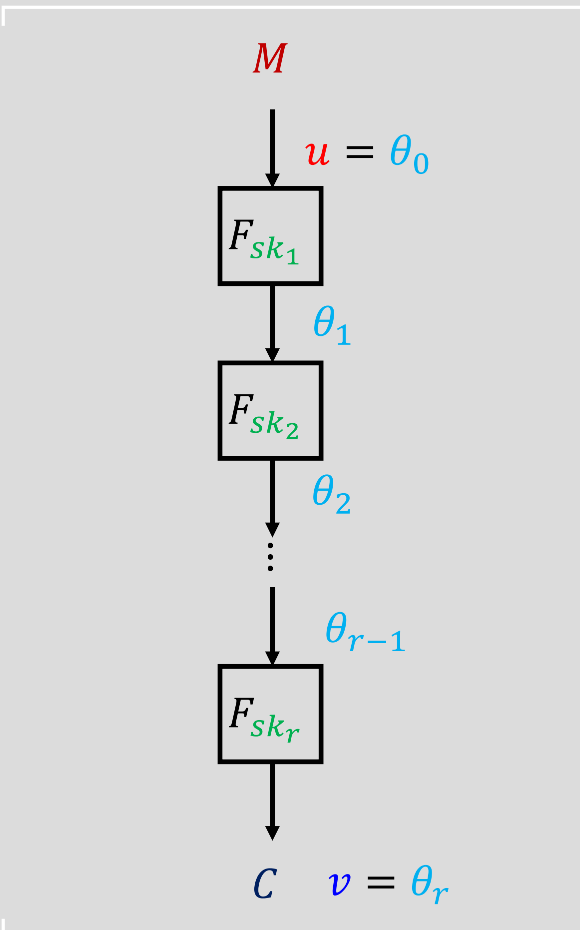
مسیر خطی

(Linear Trail)

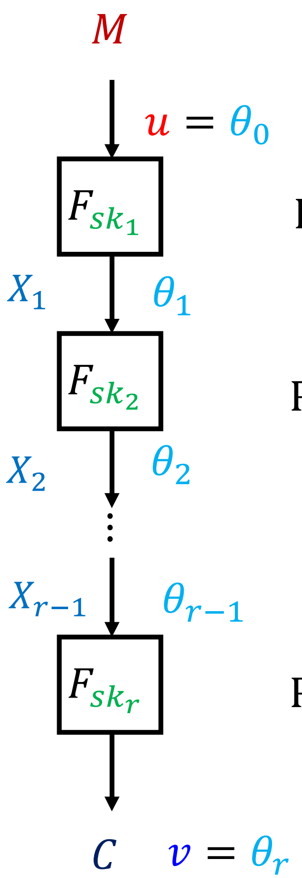
- مسیر خطی r دوری: مجموعه‌ای از $r+1$ مقدار میانی که نقاب‌های ورودی و خروجی دورها را مشخص می‌کنند.
$\boldsymbol{\theta} = (\theta_0 = u, \theta_1, \ldots, \theta_{r-1}, \theta_r = v)$
- به عبارت دقیق‌تر، تقریب خطی دور iاُم با نقاب ورودی θ_{i-1} و نقاب خروجی θ_i تعریف می‌شود.
- با در نظر گرفتن تقریب‌های خطی دورهای متوالی، می‌توان یک تقریب خطی برای کل الگوریتم به شکل کلی زیر به دست آورد:

$$v.C = u.M \oplus \omega.K$$

که u نقاب متن اصلی، v نقاب متن رمزشده و ω نقاب کلید (زیرکلیدها) هستند.



■ محاسبه‌ی اریبی مسیر خطی



$$\Pr[u.M \oplus \omega_1.sk_1 \oplus \theta_1.X_1 = 0] = \frac{1}{2} + \epsilon_1$$

$$\Pr[\theta_1.X_1 \oplus \omega_2.sk_2 \oplus \theta_2.X_2 = 0] = \frac{1}{2} + \epsilon_2$$

$$\vdots$$

$$\Pr[\theta_{r-1}.X_{r-1} \oplus \omega_r.sk_r \oplus v.C = 0] = \frac{1}{2} + \epsilon_r$$

Xor مجموعه‌ای از بیت‌های

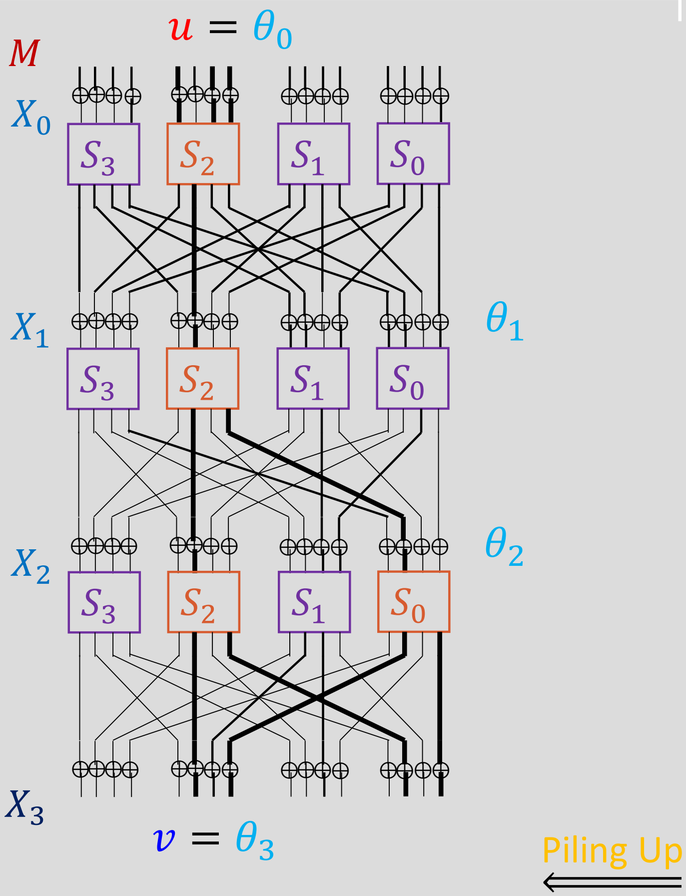
زیرکلیدها

$$\xRightarrow{\text{Piling Up}} \Pr[u.M \oplus \overbrace{\omega.K} \oplus v.C = 0] = \frac{1}{2} + \underbrace{2^{r-1}\prod_{i=1}^{r}\epsilon_i}$$

با فرض استقلال (زیرکلیدها)

اریبی مسیر خطی (با افزایش دورها کاهش می‌یابد)

مثال از محاسبه‌ی اریبی مسیر خطی



$$\Pr[\omega.K \oplus M[8,9,11] \oplus X_3[0,2,8,10]\,] = 0]$$
$$= \frac{1}{2} + 2^{3-1}\prod_{i=1}^{3}\epsilon_i = \frac{1}{2} - \frac{1}{32}$$

$$u.M \oplus u.sk_0 \oplus u.X_0 = 0$$
$$M[8,9,11] \oplus sk_0[8,9,11] \oplus X_0[8,9,11] = 0$$

$$\Pr[u.X_0 \oplus \omega_1.sk_1 \oplus \theta_1.X_1 = 0]$$
$$= \Pr[X_0[8,9,11] \oplus sk_1[10] \oplus X_1[10]\,] = 0$$
$$= \frac{1}{2} + \frac{1}{4}$$

$$\Pr[\theta_1.X_1 \oplus \omega_2.sk_2 \oplus \theta_2.X_2 = 0]$$
$$= \Pr[X_1[10] \oplus sk_2[2,10] \oplus X_2[2,10] = 0]$$
$$= \frac{1}{2} - \frac{1}{4}$$

$$\Pr[\theta_2.X_2 \oplus \omega_3.sk_3 \oplus v.C = 0]$$
$$= \Pr[X_2[2,10] \oplus sk_3[0,2,8,10] \oplus X_3[0,2,8,10] = 0]$$
$$= \frac{1}{2} + 2\left(\frac{1}{4}\right)^2 = \frac{1}{2} + \frac{1}{8}$$

مسیر خطی مناسب از دید مهاجم

- اصطلاحا به جعبه‌های جانشانی با نقاب ورودی و نقاب خروجی 0، جعبه‌های جانشانی غیرفعال می‌گوییم.
- به طور مشابه به جعبه‌های جانشانی با نقاب ورودی و نقاب خروجی غیرصفر، جعبه‌های جانشانی فعال می‌گوییم.
- مهاجم به دنبال مسیرهای خطی‌ای است که جعبه‌های جانشانی غیرفعال (فعال) بیشتری (کمتری) داشته باشند.
- در خصوص جعبه‌های جانشانی فعال، مهاجم به دنبال تقریب‌های خطی‌ای است که در آن‌ها، قدر مطلق اریبی مقدار بیشتری باشد.
- اگر تقریب خطی برای یک جعبه‌ی جانشانی دارای اریبی 0 باشد، اریبی کل تقریب خطی آن دور 0 می‌شود.
  - بنابراین باید از چنین تقریب‌هایی پرهیز کرد.

تاثیر اجزای مختلف بر اریبی مسیر خطی (جمع‌بندی)

نحوه‌ی تاثیر کلید

- عدم تاثیر کلید بر مقدار اریبی.
- تاثیر کلید بر علامت اریبی (در بخش بعدی به آن می‌پردازیم).

نحوه‌ی تاثیر لایه‌ی خطی

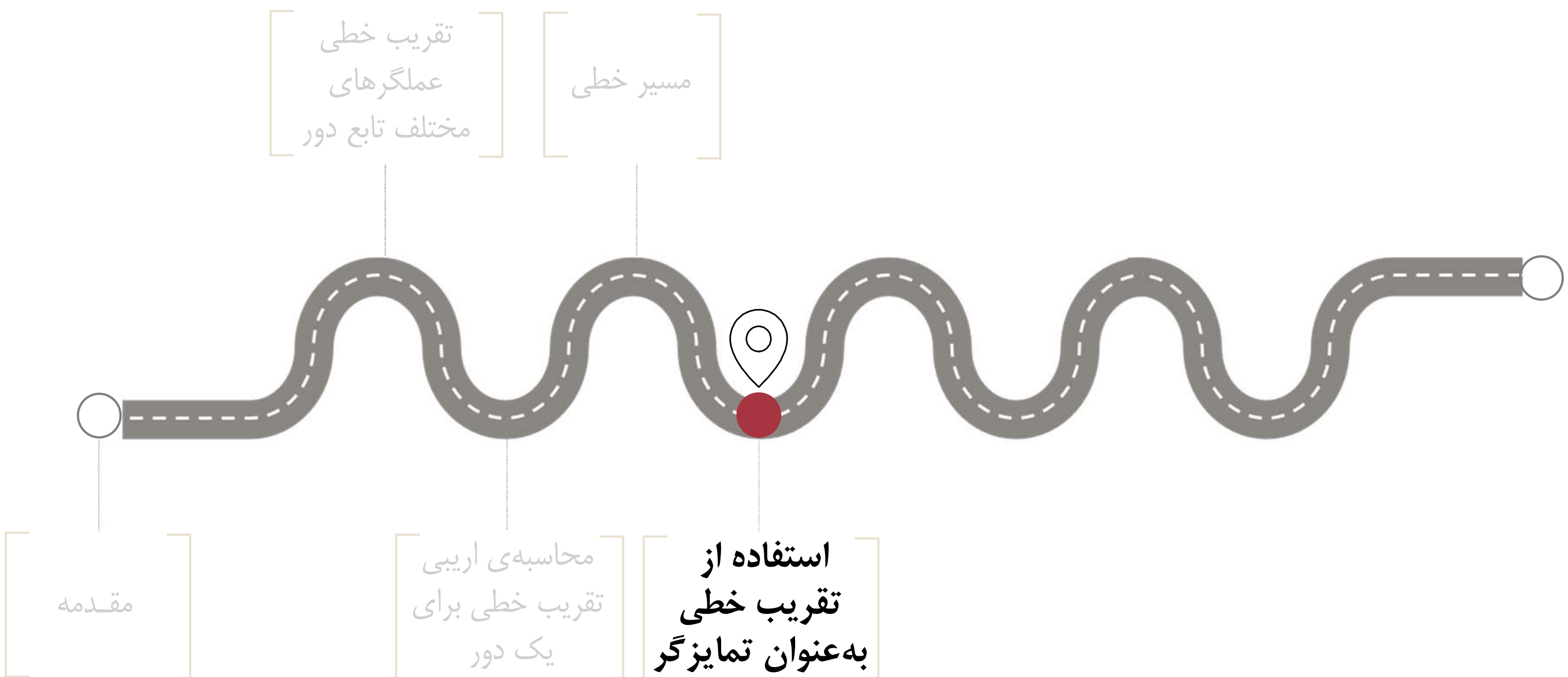
- عدم تاثیر در مقدار اریبی یک دور.
- تاثیرگذار در فعال‌سازی تعداد جعبه‌های فعال دورهای بعد.

نحوه‌ی تاثیر لایه‌ی غیرخطی

- تاثیر مسیر خطی عناصر به کار رفته در لایه غیرخطی.
- به طور خاص: حداکثر مقدار جدول تقریب خطی

تاثیر تعداد دورها

- اریبی بهترین مسیر خطی با افزایش تعداد دورها کاهش پیدا می‌کند.


مقدمه
محاسبه‌ی اریبی تقریب خطی برای یک دور
تقریب خطی عملگرهای مختلف تابع دور
مسیر خطی
استفاده از تقریب خطی به‌عنوان تمایزگر

چالش مخفی بودن کلید در تقریب خطی

- تقریب خطی حاصل از یک مسیر خطی ($\omega.K \oplus v.C \oplus u.M$) که قدرمطلق اریبی آن به اندازه کافی بزرگ است، یک ویژگی غیرتصادفی برای الگوریتم محسوب می‌شود.
- در سناریوی متن معلوم، می‌توان فرض کرد که مهاجم به متن اصلی M و همچنین متن رمزشده C معادل آن دسترسی دارد.
- اما مهاجم به مقدار کلید مخفی K دسترسی ندارد و این در حالی است که تقریب حاصل از مسیر خطی شامل بیت‌هایی از کلید نیز می‌شود.
- چگونه می‌توان بدون دانستن کلید مخفی، از تقریب حاصل از مسیر خطی برای تمایز دادن الگوریتم رمزنگاری از یک جایگشت تصادفی ایده‌آل استفاده کرد؟

تاثیر مخفی بودن کلید

- برای کلید ثابت و مخفی K مقدار $\omega.K$ ناشناخته است اما مهاجم می‌داند که این مقدار ثابت است (یا 0 یا 1 است).
- اگر $\omega.K = 0$، در این صورت داریم:

$$\Pr[u.M \oplus v.C = 0] = \frac{1}{2} + \epsilon$$

- اگر $\omega.K = 1$، در این صورت داریم:

$$\Pr[u.M \oplus v.C \oplus 1 = 0] = \frac{1}{2} + \epsilon$$

$$\Rightarrow \Pr[u.M \oplus v.C = 0] = 1 - \Pr[u.M \oplus v.C = 1] = \frac{1}{2} - \epsilon$$

- بنابر این، مقدار کلید K صرفا می‌تواند بر علامت اریبی یک تقریب خطی به شکل $u.M \oplus v.C = 0$ تاثیر بگذارد، نه بر مقدار آن.

تمایزگر خطی

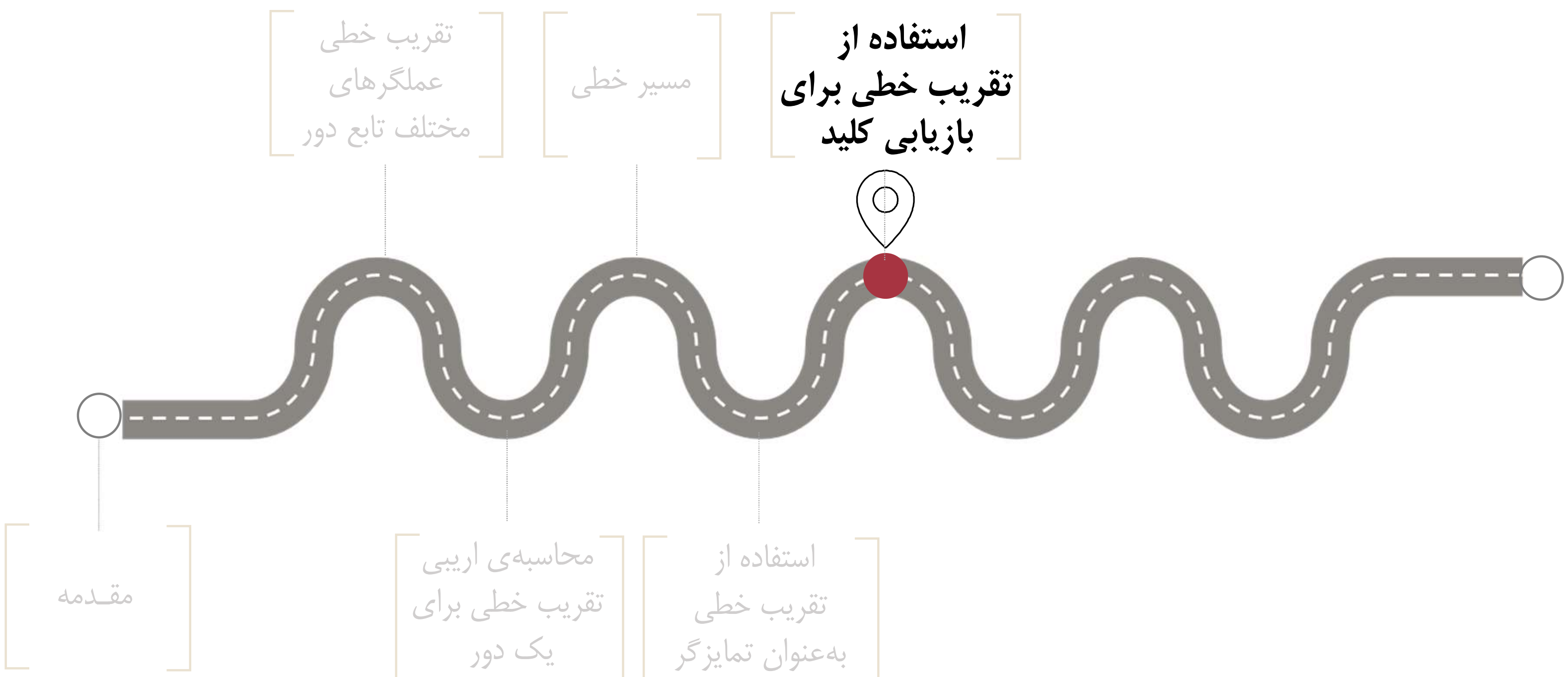
- فرض کنید که برای الگوریتم رمزنگاری، تقریب خطی زیر صادق باشد:
$|\epsilon| = |\Pr[u.M \oplus v.C = 0] - 1/2| > 0$
- فرض کنید N مقدار (M_i,C_i) داده شده است.
- می‌خواهیم قضاوت کنیم که آیا متون رمزشده‌ی داده شده توسط الگوریتم رمزنگاری مورد هدف تولید شده‌اند یا خیر؟

حمله‌ی تمایز:

- برای N مقدار (M_i,C_i) داده شده، تعداد دفعاتی که $u.M_i \oplus v.C_i = 0$ است را شمارش می‌کنیم.

$$T = \#\{i: u.M_i \oplus v.C_i = 0\}$$

- اگر T به صورت قابل توجهی بزرگ‌تر (یا کوچک‌تر) از $N/2$ بود، متون رمزشده‌ی داده شده (C_iها) توسط الگوریتم رمزنگاری مورد هدف تولید شده‌اند و اگر T تقریبا برابر با $N/2$ بود، متون موجود حاصل یک جایگشت تصادفی است.


مقـدمه
تقریب خطی
عملگرهای
مختلف تابع دور
محاسبه‌ی اریبی
تقریب خطی برای
یک دور
مسیر خطی
استفاده از
تقریب خطی
به‌عنوان تمایزگر
استفاده از
تقریب خطی برای
بازیابی کلید

بهدست‌آوردن کلید براساس تقریب خطی

- فرض کنیم که یک تقریب خطی r دوری $(u.M \oplus v.C \oplus \omega.K)$ برای الگوریتم رمزنگاری با اریبی ϵ وجود دارد.
- همچنین فرض کنیم N زوج (M_i, C_i) داده شده است که C_iها معادل رمزشده‌ی M_iها توسط الگوریتم هستند.
- ماتسوئی دو الگوریتم را برای به دست آوردن (اطلاعاتی درباره) کلید پیشنهاد کرد که به الگوریتم‌های ماتسوئی ۱ و ماتسوئی ۲ معروف هستند.
- **الگوریتم ماتسوئی ۱:**
  - از یک تقریب خطی r دوری برای حمله به r دور استفاده می‌کند.
- **الگوریتم ماتسوئی ۲:**
  - مشابه روش به دست آوردن کلید در تحلیل تفاضلی (که توسط بیهام و شمیر ارائه شده بود) است.
  - (در حالت ساده) از یک تمایزگر r دوری برای حمله به $r+1$ دور استفاده می‌کند.

نمای کلی از الگوریتم ماتسوئی ۱

- فرض کنید که اریبی یک مسیر خطی الگوریتم برای ما مشخص است:

$$\Pr[u.M \oplus v.C \oplus \omega.K = 0] = p = \frac{1}{2} + \epsilon$$

- براساس آنکه مقدار $\omega.K$ برابر با 0 باشد یا 1، دو حالت امکان‌پذیر است:

$$\Pr[u.M \oplus v.C = 0] = \begin{cases} p & \text{if } \omega.K = 0 \\ 1-p & \text{if } \omega.K = 1 \end{cases}$$

- برای N زوج (M_i,C_i) داده شده، تعداد دفعاتی که $u.M_i \oplus v.C_i$ برابر 0 است را شمارش می‌کنیم: $T = \#\{i: u.M_i \oplus v.C_i = 0\}$
- در حالتی که اریبی تقریب خطی مثبت است ($\epsilon > 0$):
  - اگر $T > N/2$ شد، $\omega.K = 0$ است. در غیر این صورت $\omega.K = 1$ است.
- در حالتی که اریبی تقریب خطی منفی است ($\epsilon < 0$):
  - اگر $T < N/2$ شد، $\omega.K = 0$ است. در غیر این صورت $\omega.K = 1$ است.

■ الگوریتم ماتسوئی ۱

For all known plaintexts (M_i, C_i) **do**

If $u.M_i \oplus v.C_i = 0$ **then**

$T = T + 1$

End if

End for

If $T > N/2$ **then**

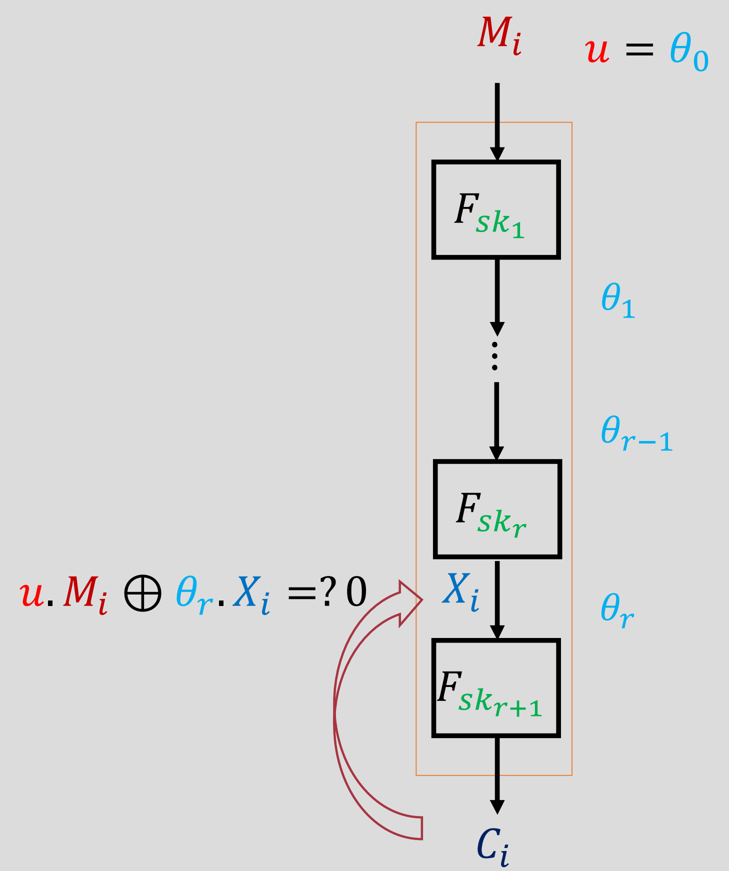
Guess $\omega.K = 0$ (when $\epsilon > 0$) or $\omega.K = 1$ (when $\epsilon < 0$)

Else

Guess $\omega.K = 1$ (when $\epsilon > 0$) or $\omega.K = 0$ (when $\epsilon < 0$)

End if

نمای کلی از الگوریتم ماتسوئی ۲



- زیر کلید دور آخر (sk_{r+1}) را حدس می‌زنیم، و تمامی متن‌های رمزشده‌ی C_i را یک دور رمزگشایی می‌کنیم تا به مقدار میانی در انتهای دور rام (X_i) برسیم.
- تعداد دفعاتی که $u.M_i \oplus \theta_r.X_i$ برابر با 0 و یا 1 می‌شود را شمارش می‌کنیم.

$$T = \#\{i: u.M_i \oplus \theta_r.X_i = 0\}$$

- کاندید صحیح برای sk_{r+1}، کلیدی است که به ازای آن $|T - N/2|$ حداکثر شود (حدود $|\epsilon| \times N$).

الگوریتم ماتسوئی ۲

For all candidates $k_g = 0$ to $2^t - 1$ do

For all known plaintexts (M_i, C_i) do

Decrypt C_i over the last round under k_g and compute the binary $b = u.M_i \oplus v.R^{-1}(C_i, k_g)$

If $b = 0$ **then**

$T_j = T_j + 1$

End if

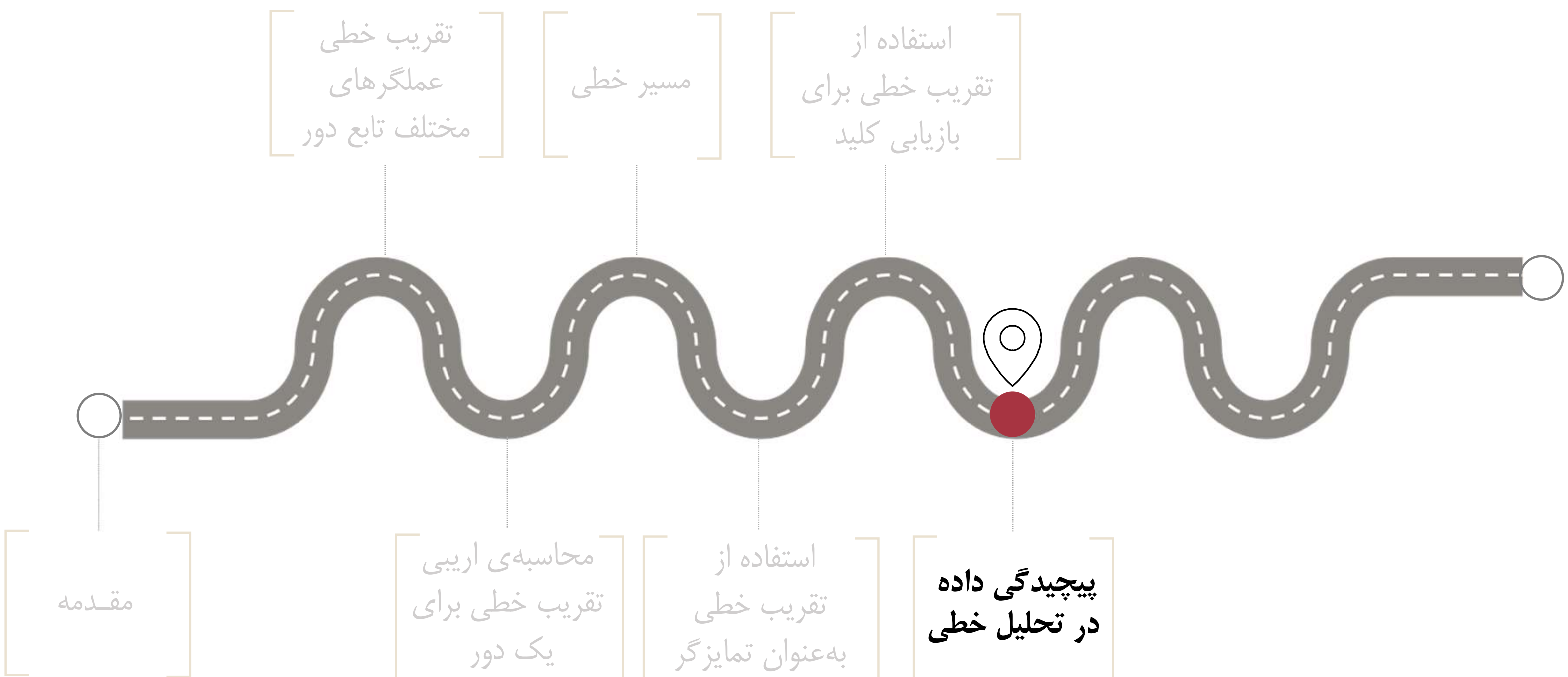
End for

End for

Find the maximum value of $|T_j - \frac{N}{2}|$ and guess the last round key (sk_{r+1}) as the corresponding key candidate

اثر کلید غلط در فرآیند بازیابی کلید

- می‌توان فرض کرد که مشخصه‌ی آماری برای کلید غلط به حالت تصادفی نزدیک‌تر است (یعنی مقدار $|T - N/2|$ برای کلید غلط، کمتر از مقداری است که برای حالت کلید صحیح رخ می‌دهد).
- همانند بازیابی کلید در تحلیل تفاضلی، در اینجا نیز می‌توان صحت الگوریتم ماتسوئی ۲ را توجیه کرد.
- اگر بیشینه شدن $|T - N/2|$ را به عنوان یک مشخصه در نظر بگیریم، باید برای کاندید صحیح اتفاق بیافتد، چرا که استفاده از زیرکلید غلط به معنای رفتن به دور بعدی است و با اضافه شدن یک دور انتظار داریم که احتمال یک مشخصه‌ی آماری کمتر شود.
- مشابه مباحثی که در بخش تحلیل تفاضلی داشتیم، این توجیه صرفا یک شهود مناسب برای ما ایجاد می‌کند و به لحاظ نظری خیلی دقیق نیست.



مقـدمه
تقریب خطی عملگرهای مختلف تابع دور
محاسبه‌ی اریبی تقریب خطی برای یک دور
مسیر خطی
استفاده از تقریب خطی به‌عنوان تمایزگر
استفاده از تقریب خطی برای بازیابی کلید
پیچیدگی داده در تحلیل خطی

پیچیدگی داده

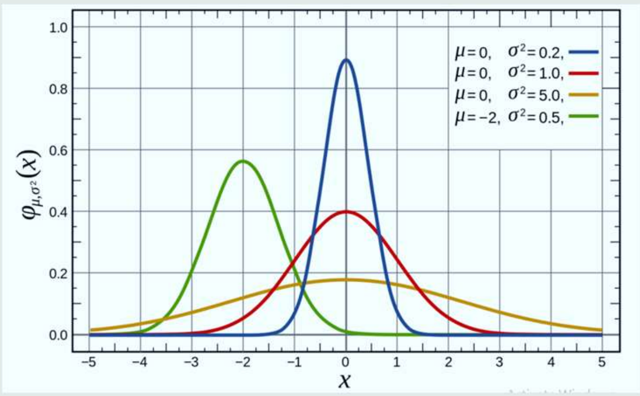
- برای تحلیل خطی به حدود $N = \text{const}\left|p - \frac{1}{2}\right|^{-2} = \text{const}.\epsilon^{-2}$ داده نیاز است.
- مقدار const یک عدد ثابت و کوچک است که به الگوریتم بستگی دارد.
- با اضافه شدن تعداد کلیدهای حدس زده شده، میزان داده‌ی مورد نیاز افزایش پیدا می‌کند.
  - علت: احتمال آن‌که برخی از کلیدهای غلط به طور اتفاقی رفتاری مشابه کلید صحیح داشته باشند بیشتر می‌شود.

یادآوری: برخی تعاریف احتمالات

- تابع چگالی احتمال (Probability Density Function): تابعی که انتگرال آن در هر بازه‌ی معین، برابر با احتمال قرار داشتن متغیر تصادفی در آن بازه است.
  - برای توزیع نرمال (واریانس σ^2 و میانگین μ):

$$\phi(x;\mu,\sigma) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

- تابع توزیع تجمعی (Cumulative Distribution Function): این تابع احتمال آن‌که متغیر تصادفی X دارای مقداری کوچک‌تر از x باشد را نشان می‌دهد. تابعی است غیرصفر و صعودی، و برد آن در بازه‌ی [0,1] است.



$$\Phi(x) = \Pr(X \le x) = \int_{-\infty}^{x} \phi(t)dt$$

$$\Phi(-x) = 1 - \Phi(x)$$

Figure’s source: Wikipedia

پیچیدگی داده

ادامه ...

- $T = \sum_{i=1}^{N} X_i$ یک توزیع دو جمله‌ای است (Binomial Distribution):

$$\Pr[T > N/2] = 1 - \Pr[T < N/2]$$

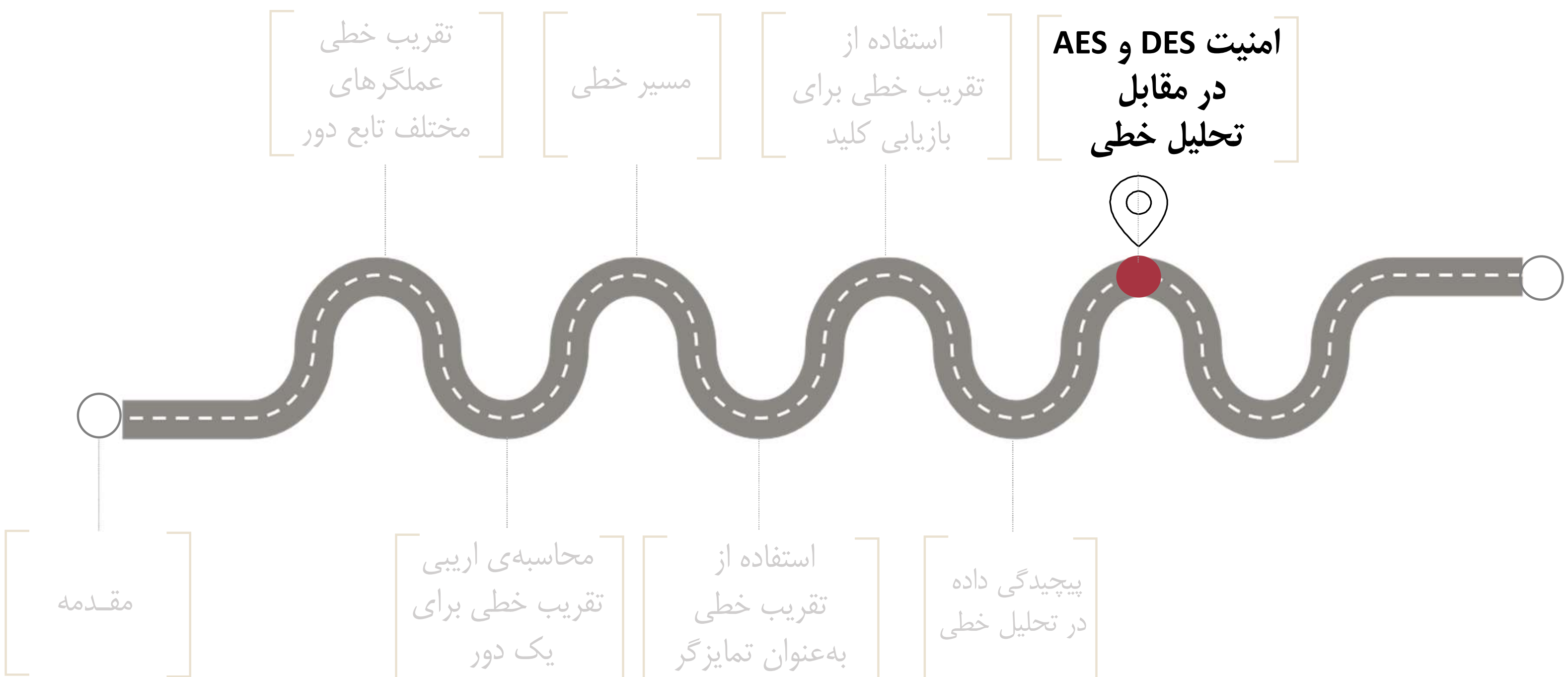
- با فرض $p > 1/2$ برای مقادیر بسیار بزرگ N داریم:

$$\approx 1 - \Phi\left(\frac{N/2 - Np}{\sqrt{Np(1-p)}}\right)$$

$$\approx 1 - \Phi\left(-2\sqrt{N} \times (p - \frac{1}{2})\right)$$

$$= \Phi\left(2\sqrt{N} \times (p - \frac{1}{2})\right) = \Phi(2\sqrt{N}|\epsilon|)$$

- یعنی برای $N = c\epsilon^{-2}$ احتمال موفقیت 97% است (محاسبه از طریق مراجعه به جدول‌های مربوط به توزیع نرمال).


مقـدمه
تقریب خطی عملگرهای مختلف تابع دور
محاسبه‌ی اریبی تقریب خطی برای یک دور
مسیر خطی
استفاده از تقریب خطی به‌عنوان تمایزگر
استفاده از تقریب خطی برای بازیابی کلید
پیچیدگی داده در تحلیل خطی
امنیت DES و AES در مقابل تحلیل خطی

جدول تقریب خطی جعبه‌ی جانشانی S5 در DES

- در جدول تقریب خطی جعبه‌های جانشانی DES، **مقادیری** مشاهده می‌شوند که دارای **فاصله‌ی زیاد از 0** هستند.
- بزرگترین **مقدار 20-** است که برای تقریب خطی $(10_x, F_x)$ است.
  - جالب است که این خاصیت از قبل توسط Shamir در CRYPTO’85 ارائه شده بود (مقاله با عنوان ”On the Security of DES“).

نقاب خروجی (v)

نقاب ورودی (u)

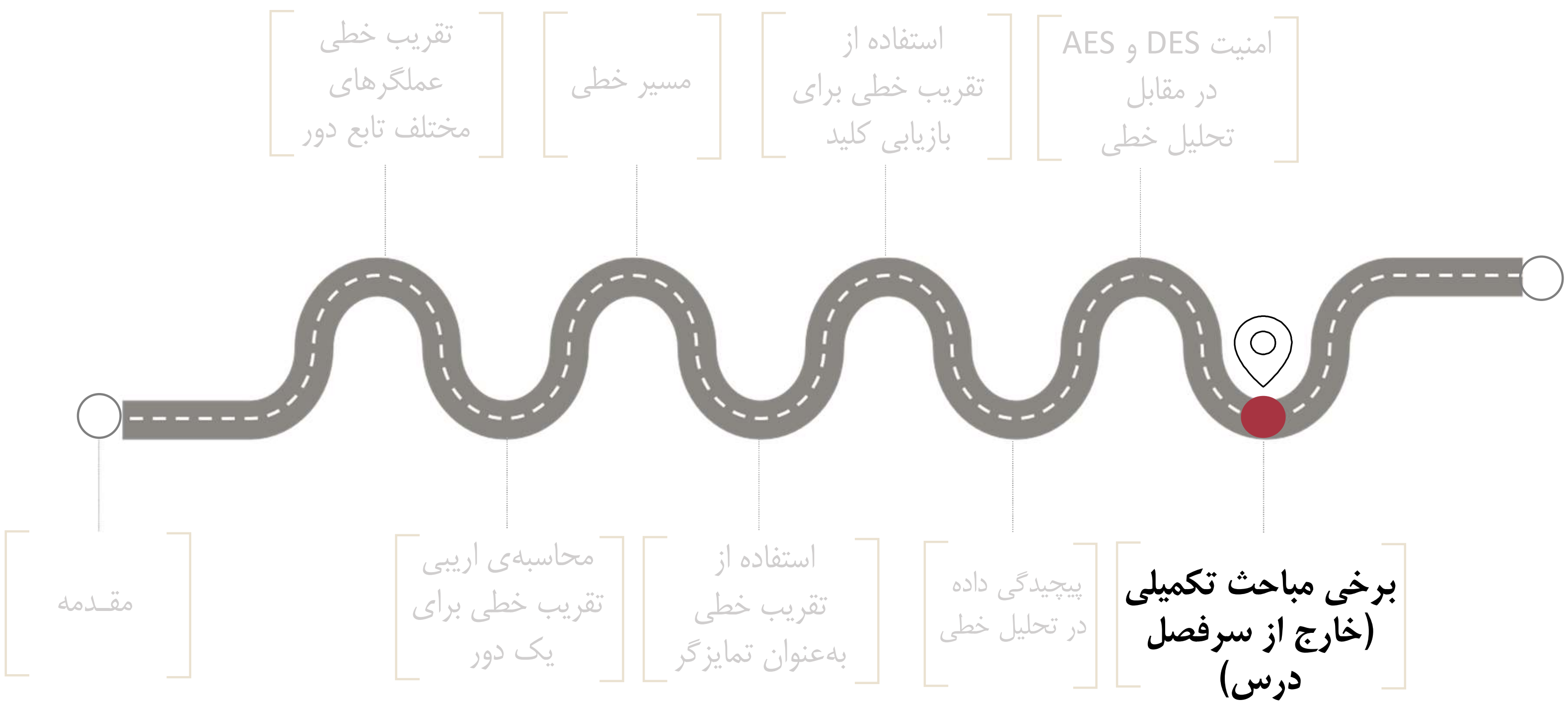
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
5_x	0	2	2	-4	0	**10**	-6	-4	0	2	**-10**	0	4	-2	2	4
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
8_x	0	0	2	6	0	0	-2	-6	-2	2	4	**-12**	2	6	-4	4
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
10_x	0	2	-2	0	0	-2	-6	-8	0	-2	-2	-4	0	2	10	**-20**
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

امنیت DES در مقابل تحلیل خطی

- نتایج تحلیل خطی نشان‌دهنده‌ی ضعف (نسبی) DES نسبت به تحلیل خطی است.
  - لااقل می‌توان چنین گفت که نتایج آن نسبت به تحلیل تفاضلی بهتر است.
- ماتسوئی یک مسیر خطی چهار دوری تکرارپذیر با اریبی بالا را به دست آورد و از آن برای ساخت یک مسیر خطی ۱۴ دوری با اریبی 1.2×2^{-21} استفاده کرد.
- در حمله به DES براساس این مسیر خطی ۱۴ دوری، مجموعا ۲۴ بیت از کلید به دست می‌آید.
- ۳۲ بیت باقیمانده‌ی کلید را می‌توان با جست و جوی کامل به دست آورد.
- داده مورد نیاز برای این حمله 2^{45} متن معلوم است.
- در ژانویه ۱۹۹۴، ماتسوئی نشان داد که می‌توان کلید DES را با استفاده از سناریوی متن معلوم، در ۵۰ روز (با استفاده از فن‌آوری وقت) به دست آورد.

امنیت AES در مقابل تحلیل خطی

- مشابه بحثی که در خصوص امنیت AES در مقابل تحلیل تفاضلی داشتیم، می‌توان امنیت آن را با در نظر گرفتن یک مسیر خطی در مقابل تحلیل خطی نیز بررسی کرد.
- می‌توان ثابت کرد که هر مسیر خطی برای چهار دور AES حداقل ۲۵ جعبه‌ی جانشانی فعال دارد.
- بهترین اریبی در جعبه‌ی جانشانی AES برابر 2^{-6} است.
- بنابراین اریبی هر مسیر خطی چهار دوری AES حداکثر برابر است با:
$2^{24}(2^{-6})^{25} = 2^{-126}$
- تولید تعداد متن‌های لازم برای تمایز دادن چهار دور AES ($(2^{126})^2$) امکان ندارد.


مقـدمه
تقریب خطی عملگرهای مختلف تابع دور
محاسبه‌ی اریبی تقریب خطی برای یک دور
مسیر خطی
استفاده از تقریب خطی به‌عنوان تمایزگر
استفاده از تقریب خطی برای بازیابی کلید
پیچیدگی داده در تحلیل خطی
امنیت DES و AES در مقابل تحلیل خطی
برخی مباحث تکمیلی (خارج از سرفصل درس)

پوسته‌ی خطی

(Linear Hull)

- آنچه در تحلیل خطی اهمیت دارد، اریبی تقریب خطی الگوریتم است (یعنی مقدار اریبی $u.M \oplus v.C$) و نه اریبی مسیر خطی!
- این مسئله مشابه مسئله‌ی وجود تفاوت بین احتمال تفاضل و احتمال مشخصه‌ی تفاضلی است که در درس مربوط به تحلیل تفاضلی (درس اول) به آن پرداختیم.
- اما محاسبه‌ی دقیق اریبی یک تقریب خطی با در نظر گرفتن تمامی مسیرهای خطی چالش برانگیز است.
- اریبی مسیرهای خطی مختلف با نقاب ورودی و خروجی یکسان (u,v)، مختلف هستند (برخی مثبت و برخی منفی) و ممکن است که باعث کم شدن مقدار نهایی اریبی یک تقریب خطی شود.

پوسته‌ی خطی

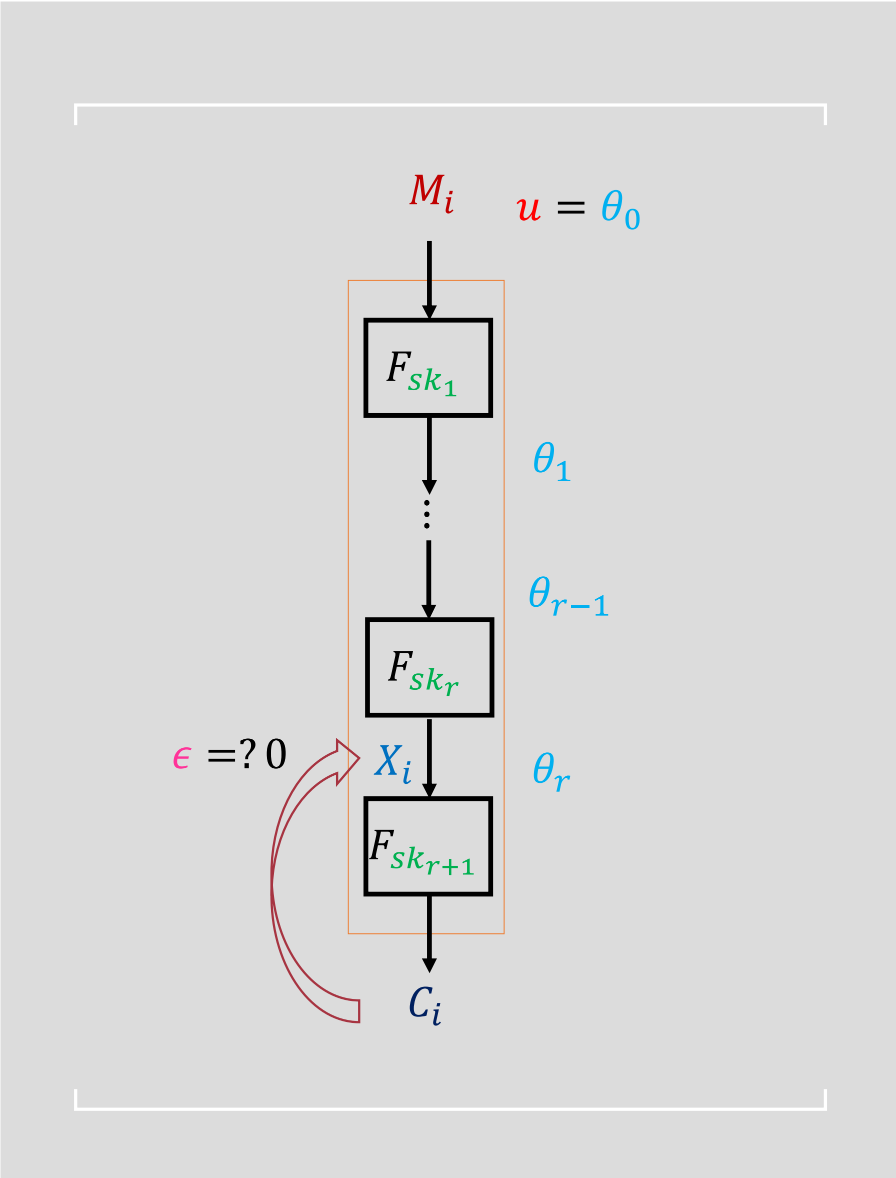
ادامه ...

- **قضیه:** برای رمز قالبی R دوری $\mathcal{E}_K$ که تابع دور آن به شکل $F(x \oplus sk_r)$ هست، داریم:

$$E_K\left[c\left(u\,.\,M \oplus \omega.K \oplus v.\mathcal{E}_K(M)\right)^2\right]$$
$$= E_K\left[c\left(u.M \oplus v.\mathcal{E}_K(M)\right)^2\right]$$
$$= \sum_{\theta|\theta_0=u,\theta_R=v} \prod_{r=0}^{R-1} c\left(\theta_i.X_i \oplus \theta_{i+1}.F(X_i)\right)^2$$

- **مفهوم:** میانگین همبستگی یک تقریب خطی بر روی فضای کلید با جمع همبستگی‌های تمام مسیرهای خطی برابر است.

تحلیل خطی با همبستگی صفر



- اگر یک تقریب خطی با نقاب‌های ورودی و خروجی (u,v) برای یک الگوریتم رمزنگاری $C = E_K(M)$ وجود داشته باشد، به‌نحوی که اریبی دقیقا برابر با 0 باشد، این ویژگی خود یک ویژگی غیرتصادفی برای الگوریتم محسوب می‌شود.
- رخ دادن اریبی دقیقا 0 برای کلید حدس زده شده به معنی غلط بودن کلید حدس زده شده است.
- با حذف کاندیدهای غلط، می‌توان کلید صحیح را پیدا کرد.
- **چالش**: برای تشخیص اریبی دقیقا 0، در ساده‌ترین راهکار به تمام متن‌های ممکن (2^b) نیاز خواهیم داشت.
- روش‌های برای حل این مشکل ارائه شده است (استفاده از تحلیل خطی چندبعدی با اریبی 0).

ارتباط بین تحلیل خطی و تحلیل تفاضلی

- طی سالیان اخیر در باب بررسی روابط بین خانواده‌ی تحلیل‌های خطی و خانواده‌ی تحلیل‌های تفاضلی مطالعات زیاد صورت گرفته است.
- برخلاف آن‌چه که ممکن است در ظاهر به نظر برسد، این دو تحلیل ارتباطات معنی‌داری با یکدیگر دارند!
  - رابطه‌ی بین تحلیل خطی با تحلیل تفاضلی
  - رابطه‌ی بین تحلیل خطی چندبعدی با تحلیل تفاضلی منقطع
  - رابطه‌ی بین تحلیل خطی با همبستگی صفر و تفاضل ناممکن
  - ...
- چند مورد از مهم‌ترین مراجع در این زمینه:

- Céline Blondeau, Kaisa Nyberg: Links between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities. **EUROCRYPT 2014**
- Céline Blondeau, Andrey Bogdanov, Meiqin Wang: On the (In)Equivalence of Impossible Differential and Zero-Correlation Distinguishers for Feistel- and Skipjack-Type Ciphers. **ACNS 2014**
- Céline Blondeau, Kaisa Nyberg: New Links between Differential and Linear Cryptanalysis. **EUROCRYPT 2013**

ترکیب تحلیل‌های خطی و تفاضلی

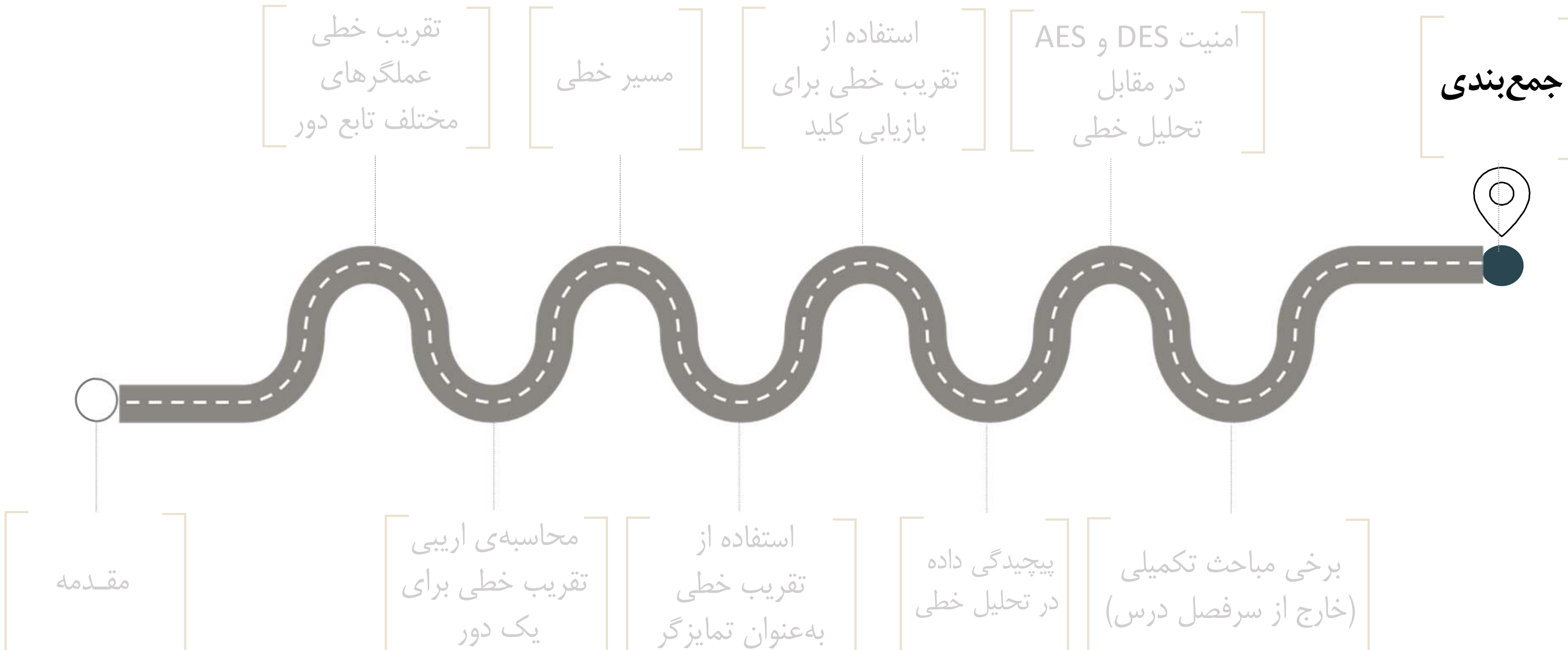
- ترکیب‌های مختلف تحلیل‌ها و استفاده از آن‌ها نیز، یکی دیگر از جهت‌گیری‌های مهم این حوزه بوده است:
  - ترکیب تحلیل‌های ریاضی متفاوت با یک‌دیگر
    - اولین بار: تحلیل تفاضلی ـ خطی بر روی DES
  - ترکیب تحلیل‌های ریاضی مشابه (مانند بومرنگ)
- از مراجع مرتبط برای تحلیل تفاضلی ـ خطی:

- Eli Biham, Orr Dunkelman, and Nathan Keller. Di erential-Linear Cryptanalysis of Serpent. **FSE 2003**
- Zhiqiang Liu, Dawu Gu, Jing Zhang, and Wei Li. Differential-Multiple Linear Cryptanalysis. Inscrypt 2009.
- Jiqiang Lu. A Methodology for Di erential-Linear Cryptanalysis and Its Applications, **FSE 2012**
- Céline Blondeau, Gregor Leander, Kaisa Nyberg: Differential-Linear Cryptanalysis Revisited. **FSE 2014**

ابزار خودکار

- پیدا کردن بهترین مشخصه‌ی تفاضلی، تقریب خطی، مشخصه‌ی تفاضل ناممکن، و ... در عمل کار دشواری است، چرا که فضای حالت‌های ممکن بسیار بزرگ است.
- برای اولین بار Mouha و همکارانش استفاده از روش MILP را برای یافتن مشخصه‌های آماری بهینه در الگوریتم‌های رمزنگاری پیشنهاد کردند.
- این روش و روش‌های دیگر (نظیر SAT Solver) طی سالیان اخیر به طور گسترده‌ای مورد توجه محققین قرار گرفته اند.

📖 Nicky Mouha, Qingju Wang, Dawu Gu, Bart Preneel: Differential and Linear Cryptanalysis Using Mixed-Integer Linear Programming. Inscrypt 2011

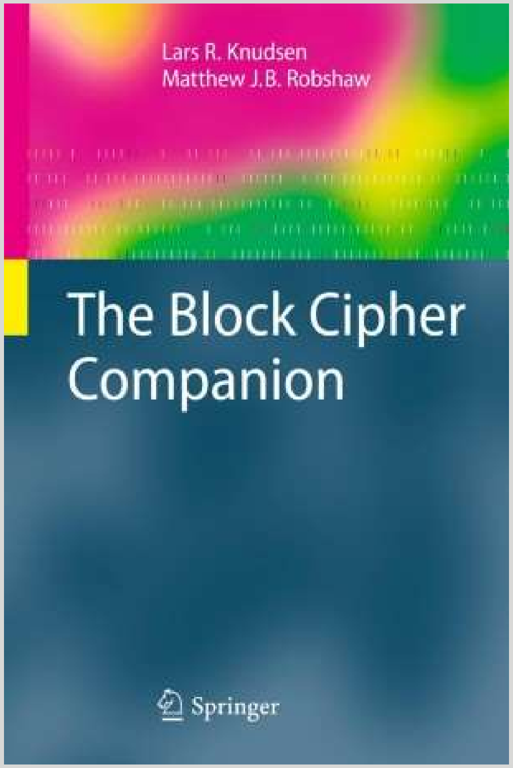

مقدمه
تقریب خطی عملگرهای مختلف تابع دور
محاسبه‌ی اریبی تقریب خطی برای یک دور
مسیر خطی
استفاده از تقریب خطی به‌عنوان تمایزگر
استفاده از تقریب خطی برای بازیابی کلید
پیچیدگی داده در تحلیل خطی
امنیت DES و AES در مقابل تحلیل خطی
برخی مباحث تکمیلی (خارج از سرفصل درس)
جمع‌بندی

جمع‌بندی

- در این بخش از درس با مفاهیم پایه‌ی تحلیل خطی آشنا شدیم.
- تحلیل خطی در کنار تحلیل تفاضلی از مهم‌ترین تحلیل‌های قابل اعمال به رمزهای قالبی است.

معرفی مـــراجع تکمیلی جهت مطالعه‌ی بیشتر

تحلیل خطی



1. Knudsen, L. R., & Robshaw, M. (2011). The block cipher companion. Springer Science & Business Media.
2. Heys, H. M. (2002). A tutorial on linear and differential cryptanalysis. Cryptologia, 26(3), 189-221.