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/

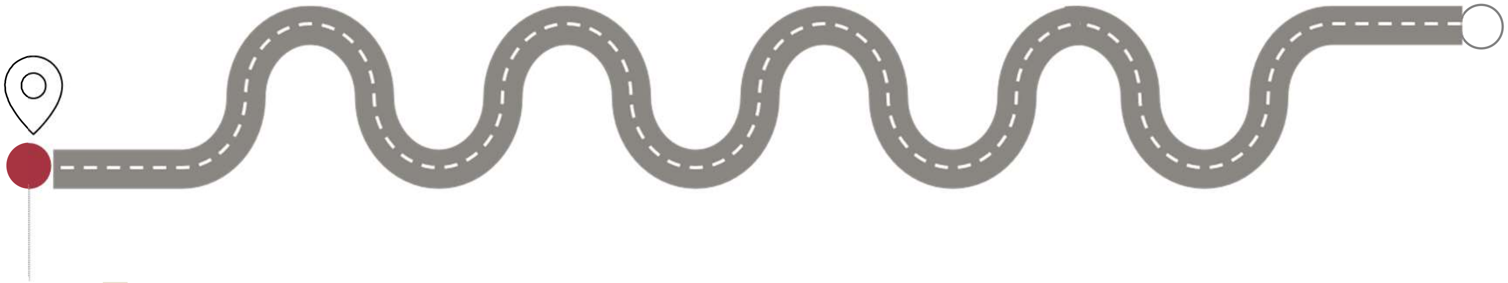
درس اول

تحلیل تفاضلی

فهرست عناوین درس

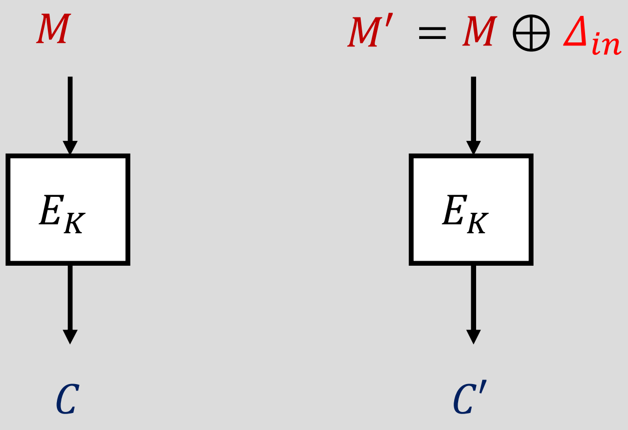
تحلیل تفاضلی

- مقدمه (مفهوم تفاضل و تحلیل تفاضلی)
- سرنوشت تفاضل در عبور از تابع دور
- مشخصه‌ی تفاضلی و احتمال آن
- استفاده از مشخصه‌ی تفاضلی به عنوان تمایزگر
- استفاده از مشخصه‌ی تفاضلی برای بازیابی کلید
- روش فیلتر کردن برای بهبود حمله‌ی تفاضلی
- امنیت DES در مقابل تحلیل تفاضلی
- امنیت AES در مقابل تحلیل تفاضلی
- مروری بر برخی از حملات خانواده‌ی تحلیل تفاضلی
- جمع‌بندی



مقدمه

نمای کلی از تحلیل تفاضلی و تعاریف اولیه



$$\Pr(C \oplus C' = \Delta_{out} | M \oplus M' = \Delta_{in}) = ?$$

- برای یک جایگشت ایده‌آل، انتظار داریم که بین متن‌های رمزشده و متن‌های اصلی هیچ رابطه‌ی آماری‌ای وجود نداشته باشد. بنابراین:

$$\Pr(C \oplus C' = \Delta_{out} | M \oplus M' = \Delta_{in}) \\ = \Pr(C \oplus C' = \Delta_{out}) = 2^{-b}$$

✓ یادآوری: احتمال آن‌که یک مقدار b بیتی تصادفی دقیقا برابر با یک مقدار مشخص مثل Δ_{out} شود، تقریبا برابر است با 2^{-b}.

نمای کلی از تحلیل تفاضلی و تعاریف اولیه

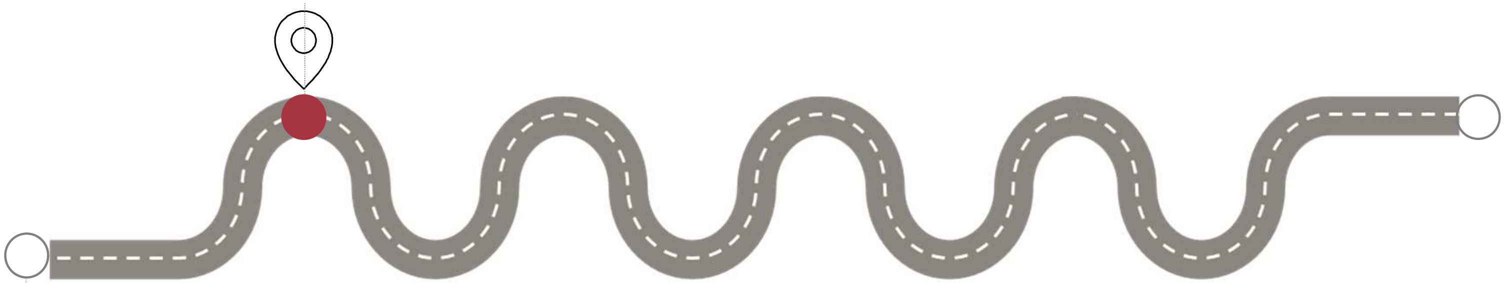
ادامه ...

- **تکنیک به کار رفته در تحلیل تفاضلی:**

پیدا کردن زوج تفاضل $(\Delta_{in},\Delta_{out})$ برای یک الگوریتم رمز قالبی به طول b، به‌نحوی که احتمال انتقال تفاضل ورودی Δ_{in} به تفاضل خروجی Δ_{out} به صورت قابل توجهی بیشتر از حالت تصادفی شود.

$$\Pr(C \oplus C' = \Delta_{out} | M \oplus M' = \Delta_{in}) > 2^{-b}$$

- سناریوی به کار رفته در تحلیل تفاضلی سناریوی "متن اصلی منتخب" است، چون برای اجرای آن به متون خاصی نیاز داریم.
- سال ۱۹۹۰ توسط Biham و Shamir به منظور تحلیل DES ارائه شد.
- به دورهای کاهش‌یافته‌ی اکثر رمزهای قالبی قابل اعمال است.
- انواع پیشرفته‌تر این تحلیل معرفی و به رمزهای متنوعی اعمال شده‌اند.
  - تفاضل مرتبه‌ی بالا، تفاضل ناممکن، تفاضل منقطع، انتگرالی، ...



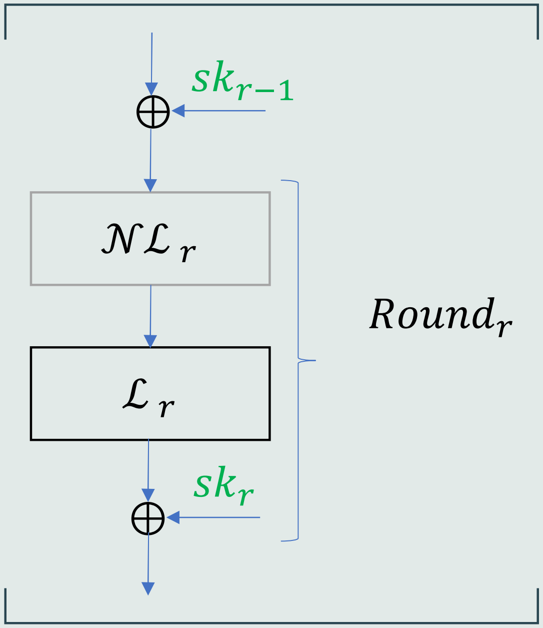
سرنوشت
تفاضل در عبور
از تابع دور

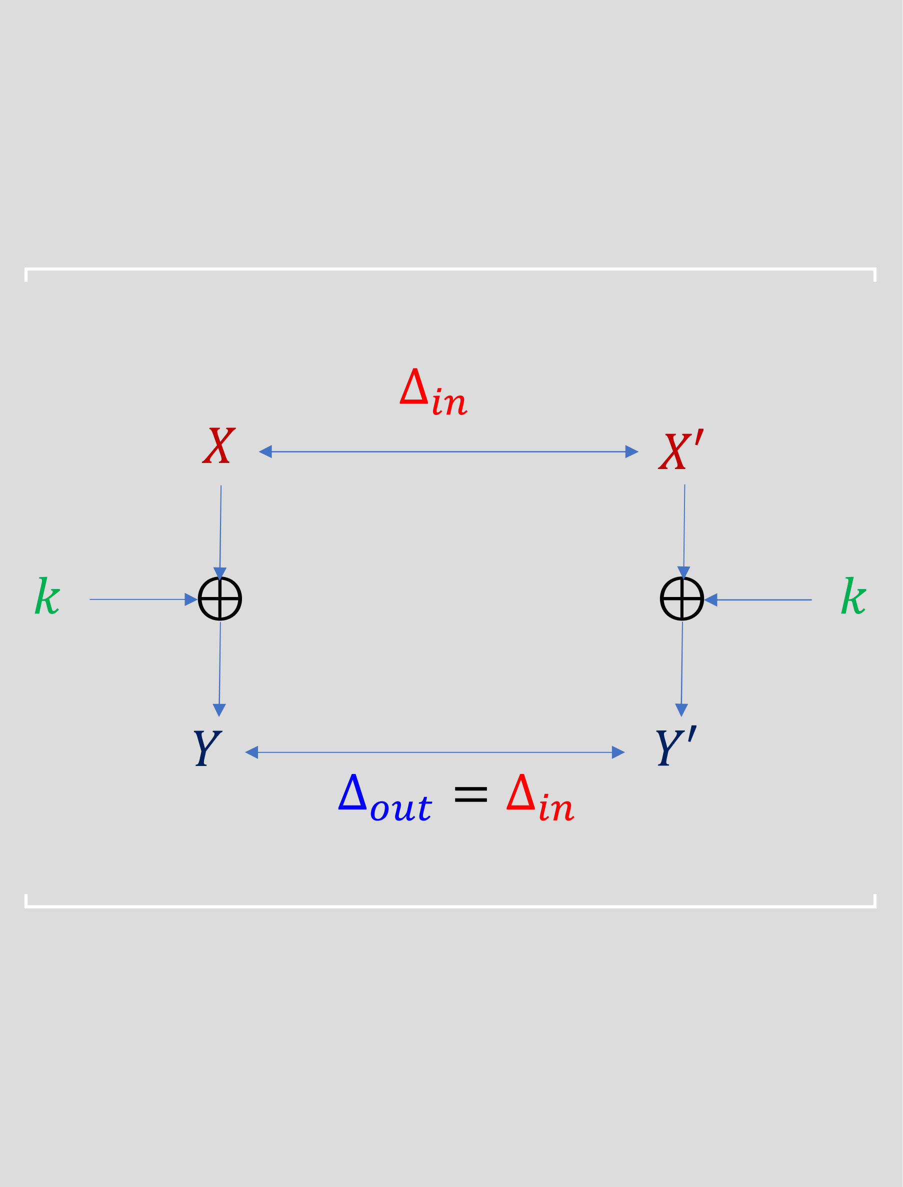
مقدمه

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 (k_0) نیز جمع می‌شود.
- تاثیر اجزای مختلف این ساختار بر مقدار تفاضل؟





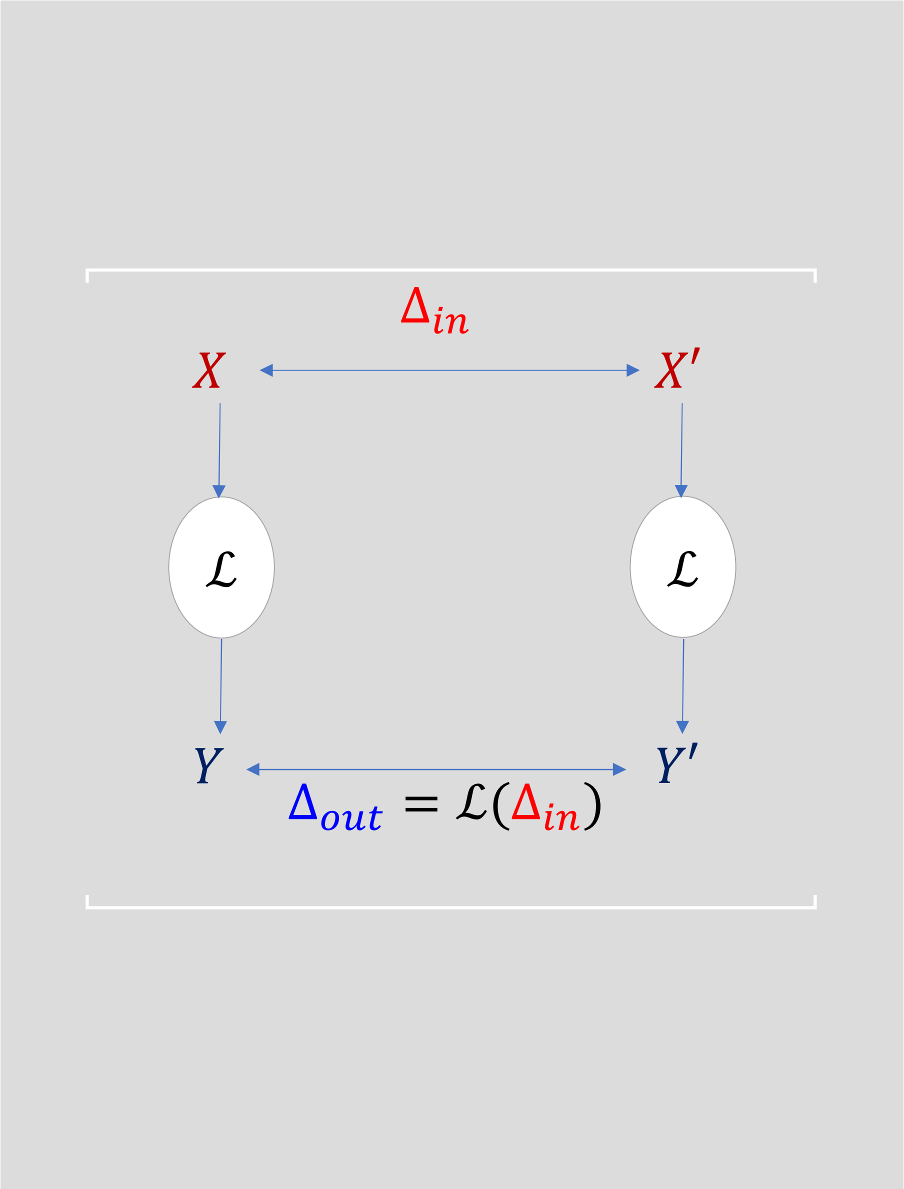
تاثیر اجزای مختلف الگوریتم بر مقدار تفاضل

اثر اضافه شدن کلید

- با فرض اضافه شدن کلید به صورت XOR، برای تفاضل خروجی داریم:

$$\begin{aligned} \Delta_{out} &= Y \oplus Y' \\ &= (X \oplus k) \oplus (X' \oplus k) \\ &= X \oplus X' \\ &= \Delta_{\mathrm{in}} \end{aligned}$$

- بنابراین تفاضل خروجی و تفاضل ورودی به صورت قطعی $(\Pr = 1)$ با هم برابر هستند.



تاثیر اجزای مختلف الگوریتم بر مقدار تفاضل

اثر لایه‌ی خطی

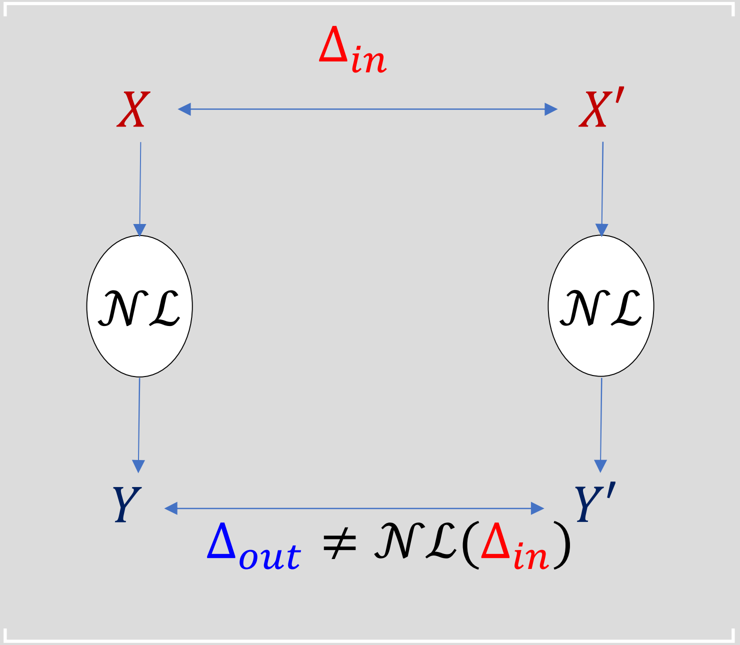
- تفاضل خروجی به صورت زیر قابل محاسبه است:

$$\begin{aligned}\Delta_{out} &= Y \oplus Y' = \mathcal{L}(X) \oplus \mathcal{L}(X')\\ &= \mathcal{L}(X \oplus X')\\ &= \mathcal{L}(\Delta_{in})\end{aligned}$$

- تفاضل خروجی تغییر می‌کند اما به صورت قطعی قابل محاسبه است.

تاثیر اجزای مختلف الگوریتم بر مقدار تفاضل

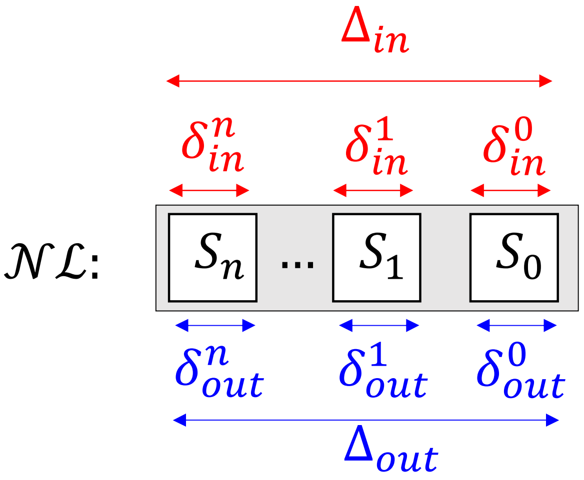
اثر لایه‌ی غیرخطی



- نمی‌توان تفاضل خروجی لایه غیرخطی را براساس تفاضل ورودی به صورت قطعی پیش‌بینی کرد (برخلاف لایه‌ی خطی).
- راه‌کار جایگزین: محاسبه‌ی تفاضل خروجی به صورت احتمالاتی (غیرقطعی).
- چالش: محاسبه‌ی احتمال انتقال یک تفاضل به تفاضل دیگر، برای تابعی با طول قالب بزرگ ممکن است در عمل کار چندان ساده‌ای نباشد (براساس مشخصات الگوریتم)!

محاسبه‌ی احتمال انتقال تفاضل در لایه‌ی غیرخطی

- در رمزهای قالبی لایه غیرخطی ($\mathcal{NL}$) عموما از عناصر کوچک‌تر موسوم به جعبه‌های جانشانی تشکیل می‌شود.
- احتمال انتقال یک تفاضل ورودی Δ_{in} به یک تفاضل خروجی Δ_{out} در لایه‌ی غیرخطی را می‌توان براساس (ضرب) احتمال‌های انتقال تفاضل در جعبه‌های جانشانی محاسبه کرد.



$$\Pr\left[\delta_{in}^0 \xrightarrow{S_0} \delta_{out}^0\right] \times \Pr\left[\delta_{in}^1 \xrightarrow{S_1} \delta_{out}^1\right] \cdots \times \Pr\left[\delta_{in}^n \xrightarrow{S_n} \delta_{out}^n\right] = \Pr\left[\Delta_{in} \xrightarrow{\mathcal{NL}} \Delta_{out}\right]$$

مثالی از محاسبه‌ی احتمال انتقال تفاضل در جعبه‌ی جانشانی

- جعبه‌ی جانشانی ۴ بیت به ۴ بیت S را با توصیف زیر در نظر بگیرید.
- می‌خواهیم $\Pr[\delta_{in} = F_x \xrightarrow{S} \delta_{out}]$ را برای تمامی مقادیر ممکن δ_{out} محاسبه کنیم.
- راه‌کار؟
- برای تمامی مقادیر $0 \leq x \leq 15$، مقدار $\delta_{out} = S(x) \oplus S(x \oplus F_x)$ را محاسبه کنیم.

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

مثال

ادامه ...

احتمال	تعداد دفعات	$\delta_{out} \mid \delta_{in} = F_x$
$2/16$	2	4_x
$2/16$	2	6_x
$10/16$	10	D_x
$2/16$	2	F_x
0	0	سایر مقادیر

α	$\alpha' = \alpha \oplus 1111$	$S(\alpha)$	$S(\alpha')$	$\delta_{out} = S(\alpha) \oplus S(\alpha')$
0_x	F_x	6_x	B_x	D_x
1_x	E_x	4_x	9_x	D_x
2_x	D_x	C_x	A_x	6_x
3_x	C_x	5_x	8_x	D_x
4_x	B_x	0_x	D_x	D_x
5_x	A_x	7_x	3_x	4_x
6_x	9_x	2_x	F_x	D_x
7_x	8_x	E_x	1_x	F_x
8_x	7_x	1_x	E_x	F_x
9_x	6_x	F_x	2_x	D_x
A_x	5_x	3_x	7_x	4_x
B_x	4_x	D_x	0_x	D_x
C_x	3_x	8_x	5_x	D_x
D_x	2_x	A_x	C_x	6_x
E_x	1_x	9_x	4_x	D_x
F_x	0_x	B_x	6_x	D_x

جدول تفاضلی جعبه‌ی جانشانی

- می‌توان تمام تفاضل‌های خروجی ممکن را به‌ازای هر تفاضل ورودی محاسبه کرد (با روش مثال قبل).
- تعداد دفعاتی که یک تفاضل مانند δ_{in}، می‌تواند به تفاضل δ_{out} منجر شود را در سطر δ_{in} و ستون δ_{out} یک جدول ذخیره می‌کنیم.
- به عنوان نمونه، جدول زیر برای جعبه‌ی جانشانی مثال قبلی به‌دست آمده است.

δ_{out}

		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	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1_x	0	0	6	0	0	0	0	2	0	2	0	0	2	0	4	0
	2_x	0	6	6	0	0	0	0	0	0	2	2	0	0	0	0	0
δ_{in}	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
	D_x	0	0	0	0	0	0	2	2	0	0	0	0	6	2	0	4
	E_x	0	2	0	4	2	0	0	0	0	0	2	0	0	0	0	6
	F_x	0	0	0	0	2	0	2	0	0	0	0	0	0	10	0	2

مشاهده‌ی ۱ در رابطه با جدول تفاضلی Sbox

- قطعی بودن انتقال تفاضل صفر به تفاضل صفر در هر جعبه‌ی جانشانی.

$S(x) \oplus S(x') = 0$ if $x = x'$

- **تعریف جعبه‌ی جانشانی غیرفعال:** جعبه‌ی جانشانی‌ای که تفاضل ورودی آن صفر باشد.
- **تعریف جعبه جانشانی فعال:** جعبه‌ی جانشانی‌ای که تفاضل ورودی آن صفر نباشد و در نتیجه تفاضل خروجی آن به صورت احتمالاتی قابل مشخص شدن باشد.

									δ_{out}								
		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	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1_x	0	0	6	0	0	0	0	2	0	2	0	0	2	0	4	0
	2_x	0	6	6	0	0	0	0	0	0	2	2	0	0	0	0	0
δ_{in}	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
	D_x	0	0	0	0	0	0	2	2	0	0	0	0	6	2	0	4
	E_x	0	2	0	4	2	0	0	0	0	0	2	0	0	0	0	6
	F_x	0	0	0	0	2	0	2	0	0	0	0	0	0	10	0	2

مشاهده‌ی ۲ در رابطه با جدول تفاضلی Sbox

- زوج بودن تمام مقادیر جدول تفاضلیِ هر جعبه‌ی جانشانی به علت تقارن:

$$\delta_{out} = S(x) \oplus S(x \oplus \delta_{in})$$
$$\delta_{out} = S(x \oplus \delta_{in}) \oplus S(x)$$

								δ_{out}									
		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	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1_x	0	0	6	0	0	0	0	2	0	2	0	0	2	0	4	0
	2_x	0	6	6	0	0	0	0	0	0	2	2	0	0	0	0	0
δ_{in}	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
	D_x	0	0	0	0	0	0	2	2	0	0	0	0	6	2	0	4
	E_x	0	2	0	4	2	0	0	0	0	0	2	0	0	0	0	6
	F_x	0	0	0	0	2	0	2	0	0	0	0	0	0	10	0	2

مثالی دیگر برای جدول تفاضلی

جدول تفاضلی جعبه‌ی جانشانی رمز استاندارد PRESENT

	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	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	4	0	0	0	4	0	4	0	0	0	4	0	0
2_x	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
3_x	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
4_x	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
5_x	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
6_x	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
D_x	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
E_x	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
F_x	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

ویژگی‌ها:

- حداکثر مقداری که در جدول تفاضلی PRESENT وجود دارد، 4 است (رفتار نزدیک به تصادفی).
- نشان‌دهنده‌ی انتخاب آگاهانه‌ی طراحان این جعبه‌ی جانشانی!

جمع‌بندی و مرور

تاثیر اجزای مختلف ساختار بر تفاضل

اضافه شدن کلید:

- عدم تغییر مقدار تفاضل.

لایه‌ی خطی:

- تغییر مقدار تفاضل.
- مقدار جدید قابل محاسبه‌ی قطعی.

لایه‌ی غیرخطی:

- تغییر مقدار تفاضل.
- محاسبه‌ی مقدار جدید به صورت احتمالاتی.

در مجموع؟

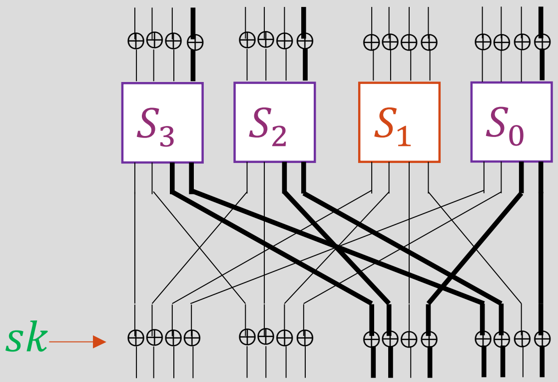
❖ محاسبه‌ی مقدار جدید به صورت احتمالاتی!

احتمال انتقال تفاضل

محاسبه‌ی احتمال انتقال تفاضل برای تابع دور

- تفاضل ورودی جعبه‌ی جانشانی S_1 صفر است (غیرفعال است)، پس با احتمال قطعی می‌توان گفت که تفاضل خروجی نیز صفر است.
- براساس جدول تفاضلی جعبه‌ی جانشانی PRESENT، تفاضل **0001** با احتمال $\frac{4}{16} = 2^{-2}$ به تفاضل **0011** تبدیل می‌شود.
- پس از لایه‌ی خطی مقدار تفاضل تغییر پیدا می‌کند اما قابل محاسبه است.
- اضافه شدن زیرکلید تاثیری در تفاضل ندارد.

$\Delta_{in} = \mathbf{0001\ 0001\ 0000\ 0001}$



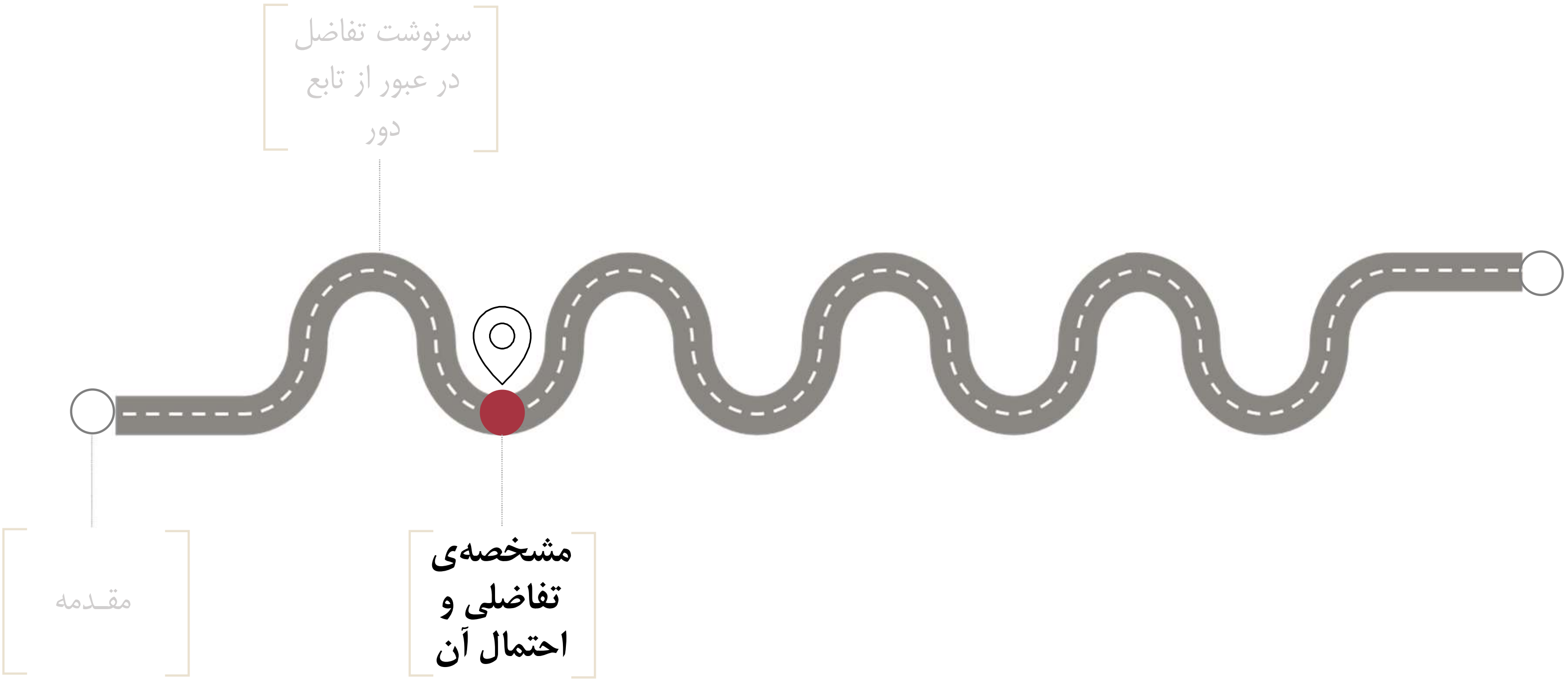
Sboxهای غیرفعال: $\Pr\left[0000 \xrightarrow{S} 0000\right] = 1$

Sboxهای فعال: $\Pr\left[\mathbf{0001} \xrightarrow{S} \mathbf{0011}\right]^3 = (2^{-2})^3 = 2^{-6}$

تفاضل پس از لایه‌ی غیرخطی: $\mathbf{0011\ 0011}\ 0000\ \mathbf{0011}$

تفاضل پس از لایه‌ی خطی: $\Delta_1 = 0000\ 0000\ \mathbf{1101\ 1101}$

احتمال کل: $\Pr\left[\Delta_{in} \xrightarrow{round} \Delta_1\right] = 2^{-6}$



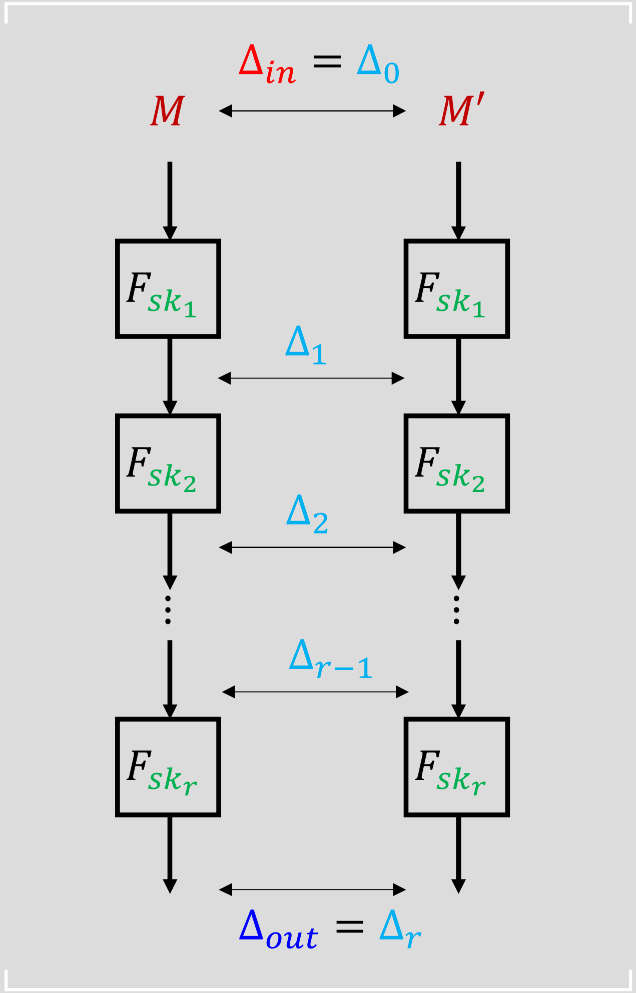
مقدمه

سرنوشت تفاضل
در عبور از تابع
دور

**مشخصه‌ی
تفاضلی و
احتمال آن**

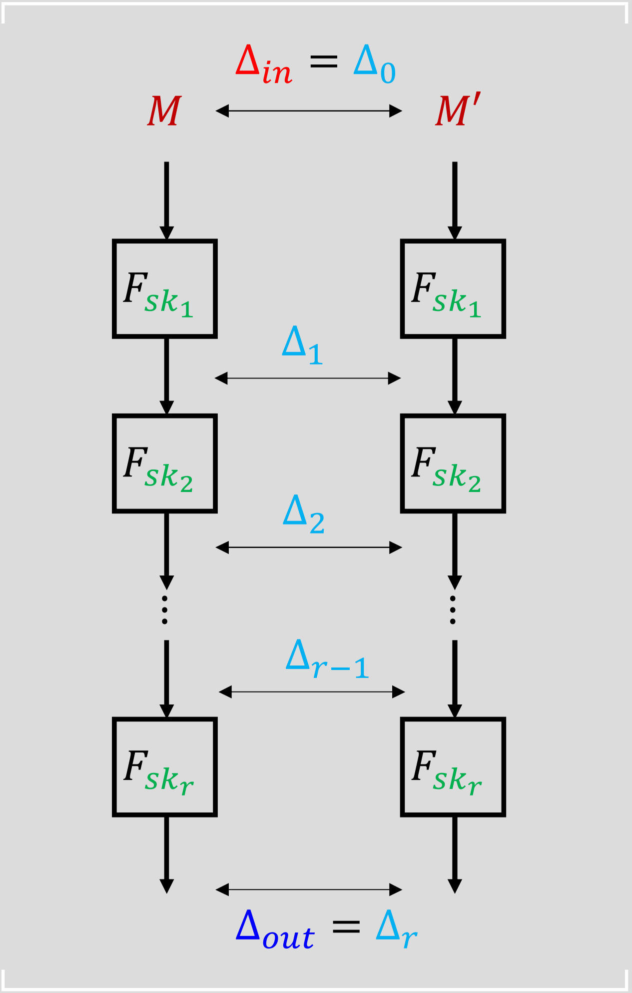
مثالی دیگر برای جدول تفاضلی

(Differential Characteristic)



- با در نظر گرفتن تمام دورهای یک الگوریتم (و نه فقط یک دور)، به جای احتمال انتقال تفاضل از مفهوم کلی‌تر مشخصه‌ی تفاضلی استفاده می‌کنیم.
- مشخصه‌ی تفاضلی r دوری: $r + 1$ مقدار تفاضل Δ_i برای $0 \leq i \leq r$ که مسیر تفاضلی را مشخص می‌کنند.
- مقدار Δ_0 نمایش دهنده تفاضل ورودی Δ_{in}، و مقدار Δ_r نمایش دهنده تفاضل خروجی دور rام است.
- مقدار تفاضل Δ_i برای $1 \leq i \leq r - 1$ نشان دهنده تفاضل خروجی دور iام است که برابر تفاضل ورودی دور $(i + 1)$ام است.

محاسبه‌ی احتمال مشخصه‌ی تفاضلی



$$\Pr[\Delta_0 \to \Delta_1] \times \Pr[\Delta_1 \to \Delta_2] \times \cdots \times \Pr[\Delta_{r-1} \to \Delta_r]$$

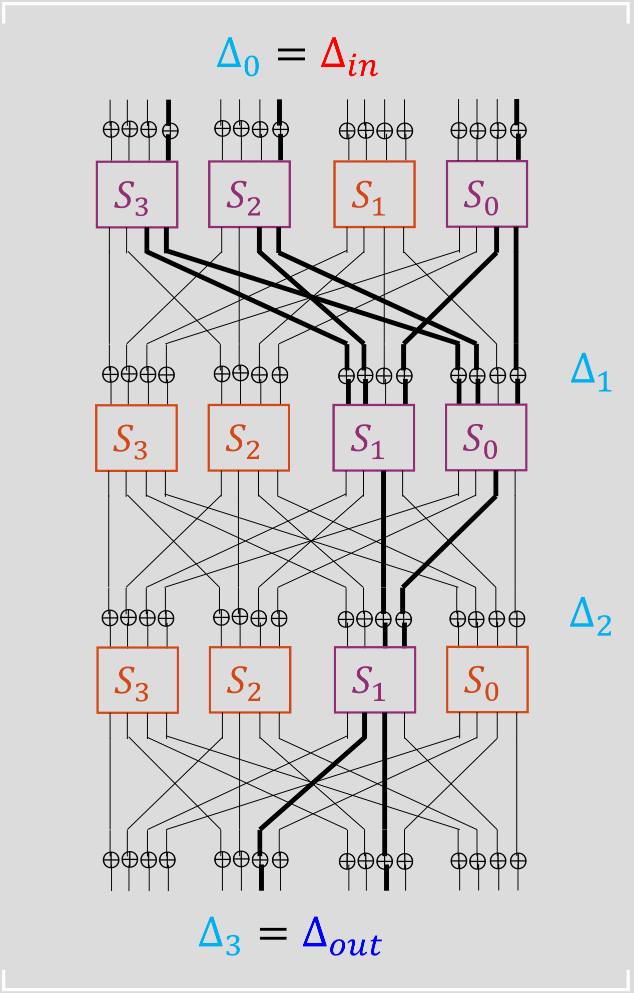
$$= \Pr[\Delta_0 \to \Delta_1 \to \cdots \to \Delta_r]$$

با فرض استقلال احتمالات

با فرض استقلال زیرکلیدها

- بنابراین، احتمال مشخصه‌ی تفاضلی از حاصل‌ضرب احتمال انتقال تفاضلِ تک تک دورها محاسبه می‌شود.

مثال: مشخصه‌ی سه دوری SMALL-PRESENT-16



Example's source: Céline Blondeau

$$p_1 = \Pr[\Delta_0 \to \Delta_1] = \Pr\left[0001 \xrightarrow{S} 0011\right]^3 = (2^{-2})^3$$

$$p_2 = \Pr[\Delta_1 \to \Delta_2] = \Pr\left[1101 \xrightarrow{S} 0010\right]^2 = (2^{-2})^2$$

$$p_3 = \Pr[\Delta_2 \to \Delta_3] = \Pr\left[0011 \xrightarrow{S} 0110\right] = 2^{-2}$$

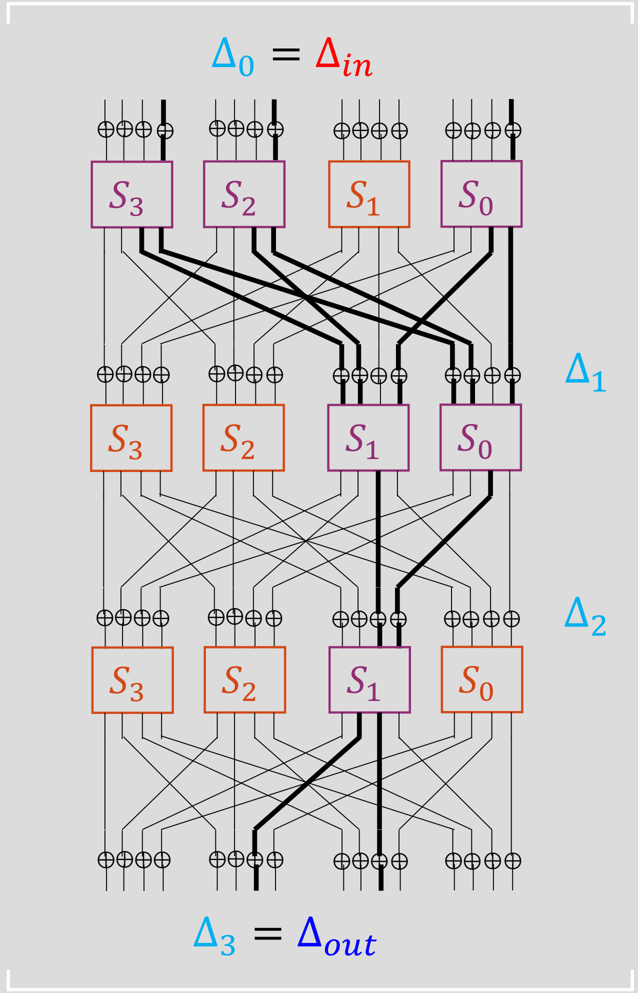
$$\Pr[\Delta_0 \to \Delta_1 \to \Delta_2 \to \Delta_3] = 2^{-12} \gg 2^{-16}$$

مشاهداتی در خصوص احتمال مشخصه‌ی تفاضلی

- اگر حداکثر مقداری که در جدول تفاضلی یک جعبه‌ی جانشانی موجود است، δ باشد، در این صورت آن جعبه‌ی جانشانی را δ-یکنواخت تفاضلی گوییم.

$$|\{x: \delta_{out} = S(x) \oplus S(x \oplus \delta_{in})\}| \leq \delta$$

  - مثال: جعبه‌ی جانشانی PRESENT، 4-یکنواخت تفاضلی است.
- به عبارت دیگر، حداکثر احتمال انتقال یک تفاضل ورودی (δ_{in}) به یک تفاضل خروجی (δ_{out}) در جعبه‌ی جانشانی با ورودی m بیت، برابر ${}^{\delta}/_{2m}$ است.
- هر چقدر مقدار δ کمتر باشد، حداکثر احتمال انتقال ممکن کمتر است.
- کمترین مقدار غیرصفر ممکن برای δ برابر با ۲ است (به علت تقارن).
- **مشاهده‌ی ۱:** (حداکثر) احتمال انتقالِ جعبه(های) جانشانی به‌کار گرفته‌شده در الگوریتم، بر (بیش‌ترین) احتمال مشخصه نیز تاثیر مستقیم دارد.



مشاهداتی در خصوص احتمال مشخصه‌ی تفاضلی

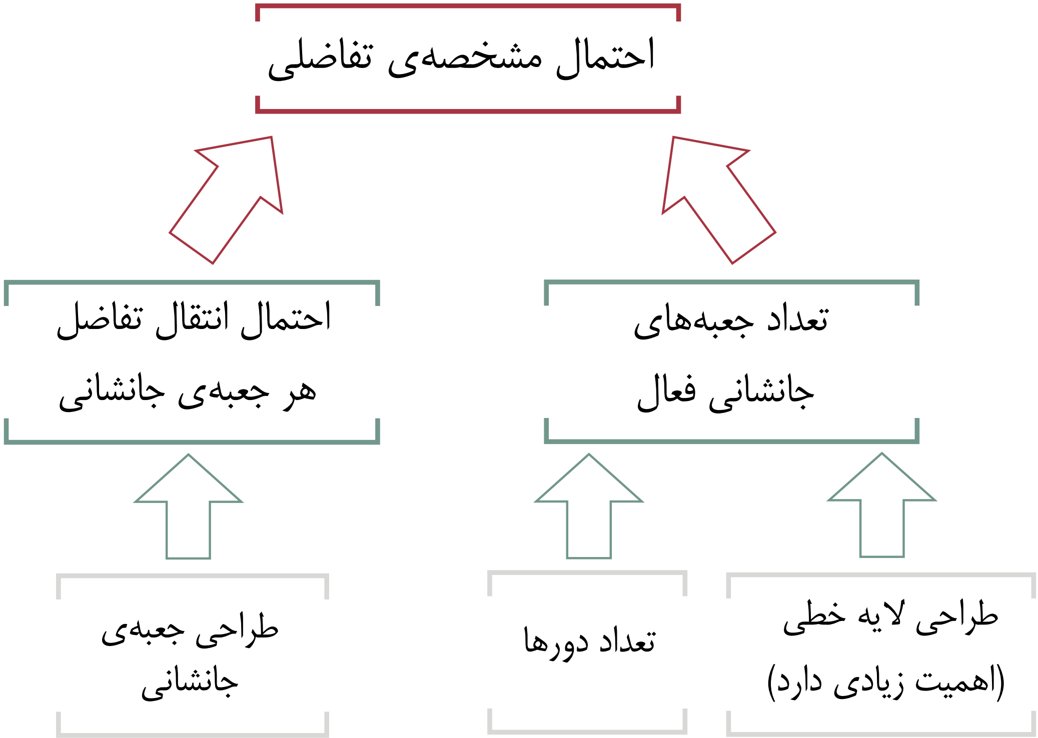
ادامه ...

- **مشاهده‌ی ۲:** تعداد جعبه‌های جانشانی فعال نیز بر احتمال مشخصه تاثیر مستقیم دارد.
  - تعداد آن‌ها (به خصوص) به نوع طراحی لایه خطی بستگی دارد.
- **مشاهده‌ی ۳:** افزایش تعداد دورها می‌تواند بر افزایش تعداد جعبه‌های جانشانی فعال، و در نتیجه بر کاهش بیش‌ترین مقدار ممکن برای احتمال مشخصه تاثیر داشته باشد.

❖ نکته: یافتن مشخصه‌ی تفاضلی‌ای که بیشترین احتمال را دارد کار سختی است، چرا که تعداد حالات ممکن بسیار زیاد است.

جمع‌بندی بخش

(از منظر عوامل موثر بر احتمال مشخصه‌ی تفاضلی)



احتمال مشخصه‌ی تفاضلی

احتمال انتقال تفاضل هر جعبه‌ی جانشانی

تعداد جعبه‌های جانشانی فعال

طراحی جعبه‌ی جانشانی

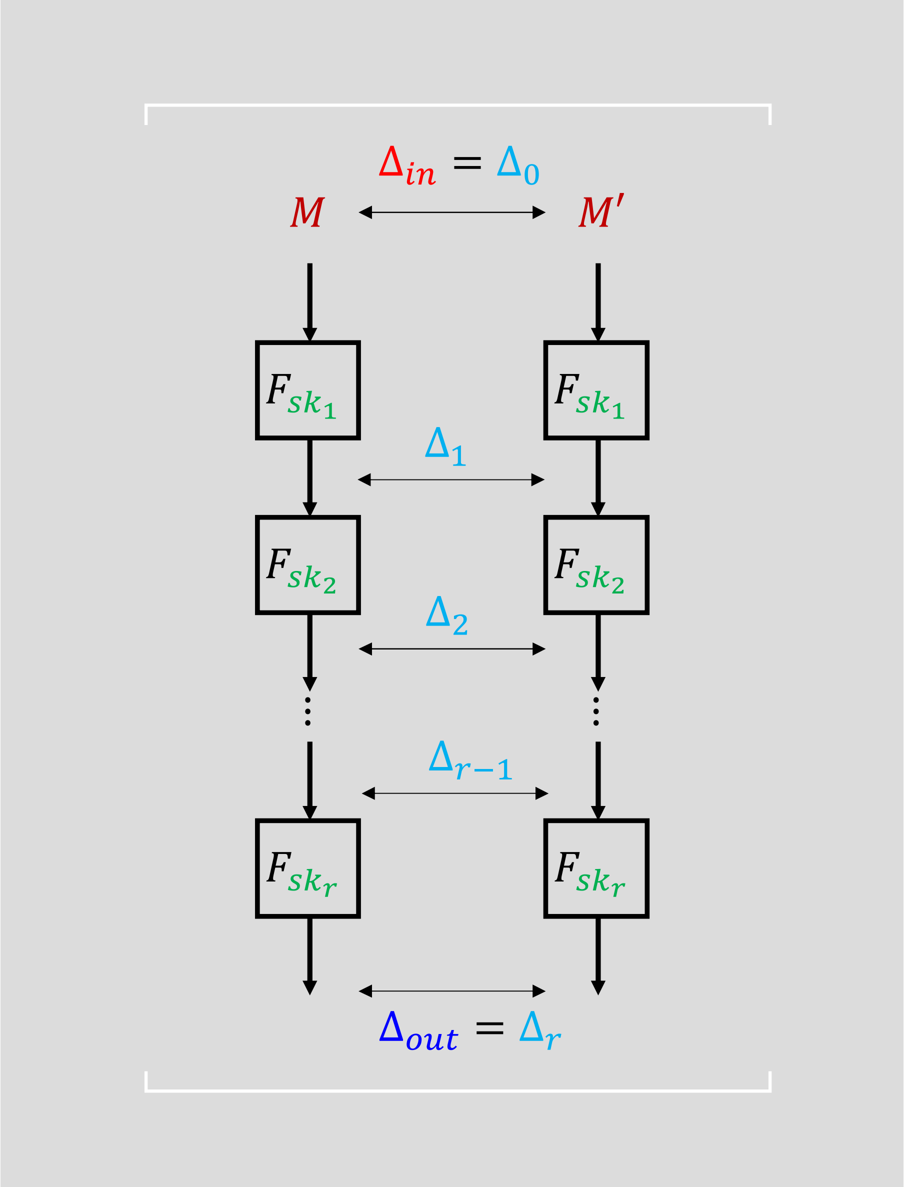
تعداد دورها

طراحی لایه خطی (اهمیت زیادی دارد)

جمع‌بندی بخش

(از منظر چگونگی تاثیر اجزای مختلف الگوریتم بر احتمال مشخصه)

نحوه‌ی تاثیر کلید	• عدم تاثیر در صورتی که به صورت XOR اضافه شود.
نحوه‌ی تاثیر لایه‌ی خطی	• عدم تاثیر در احتمال یک دور • تاثیرگذار در فعال‌سازی تعداد جعبه‌های فعال دورهای بعد
نحوه‌ی تاثیر لایه‌ی غیرخطی	• مشخصه‌ی تفاضلی عناصر به کار رفته در لایه‌ی غیرخطی • به طور خاص: حداکثر مقدار جدول تفاضلی
تعداد دور بیشتر	• در صورت فعال شدن جعبه‌های جانشانی بیشتر، مقدار احتمال بهترین مشخصه‌ی تفاضلی (با بیشترین احتمال) کمتر می‌شود.



مفهوم تفاضل

(Differential)

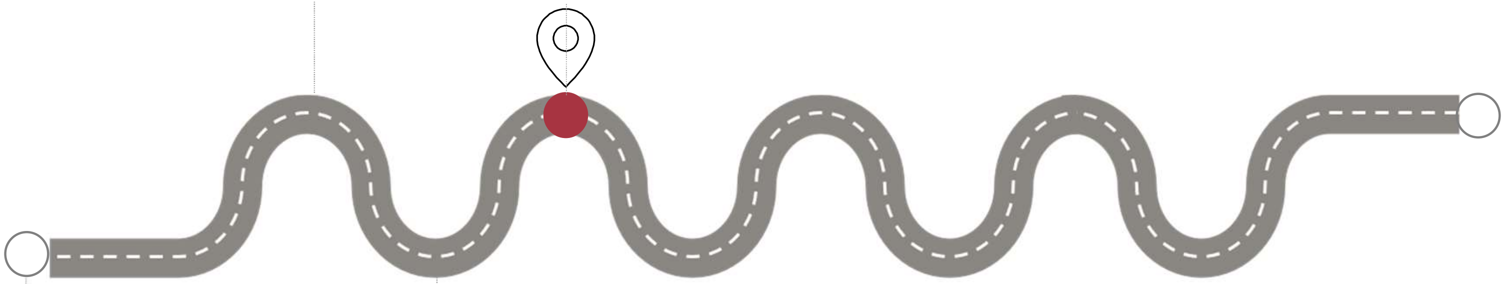
- آنچه در تحلیل تفاضلی اهمیت دارد، احتمال انتقال تفاضل ورودی (Δ_{in}) به تفاضل خروجی (Δ_{out}) است و نه احتمال مشخصه‌ی تفاضلی!
- احتمال تفاضل ($\Delta_{in} \longrightarrow \Delta_{out}$) برابر است با مجموع احتمال تمامی مشخصات تفاضلی با مقدار تفاضل ورودی $\Delta_{in} = \Delta_0$ و تفاضل خروجی $\Delta_{out} = \Delta_r$.

$$\Pr[\Delta_{in} \to \Delta_{out}]$$

$$= \sum_{\{\Delta_0=\Delta_{in},\Delta_1,\ldots,\Delta_{r-1},\Delta_r=\Delta_{out}\}} \prod_{0<i<r} \Pr[\Delta_i \to \Delta_{i+1}]$$

ارتباط بین تفاضل و مشخصه‌ی تفاضلی

- وجود تعداد زیادی مشخصه‌ی تفاضلی با احتمال نزدیک به حالت تصادفی می‌تواند منجر به ضعف در مقابل حمله‌ی تفاضلی شود.
  - شاید مشخصه‌ی تفاضلی با احتمال بالا وجود نداشته باشد، اما الگوریتم کماکان در مقابل تحلیل تفاضلی ضعیف باشد.
- محاسبه‌ی دقیق تفاضل در عمل امکان‌پذیر نیست.
  - چراکه تعداد حالات ممکن (مسیرهای مختلف برای رسیدن از تفاضل ورودی به تفاضل خروجی) بسیار زیاد است.
- به همین دلیل، معمولا تنها احتمال مشخصه‌ی تفاضلی توسط طراحان بررسی می شود و با در نظر گرفتن یک حاشیه‌ی امن (Security Margin) نظیر افزایش تعداد دورها، ادعا می‌شود که طرح امن است.



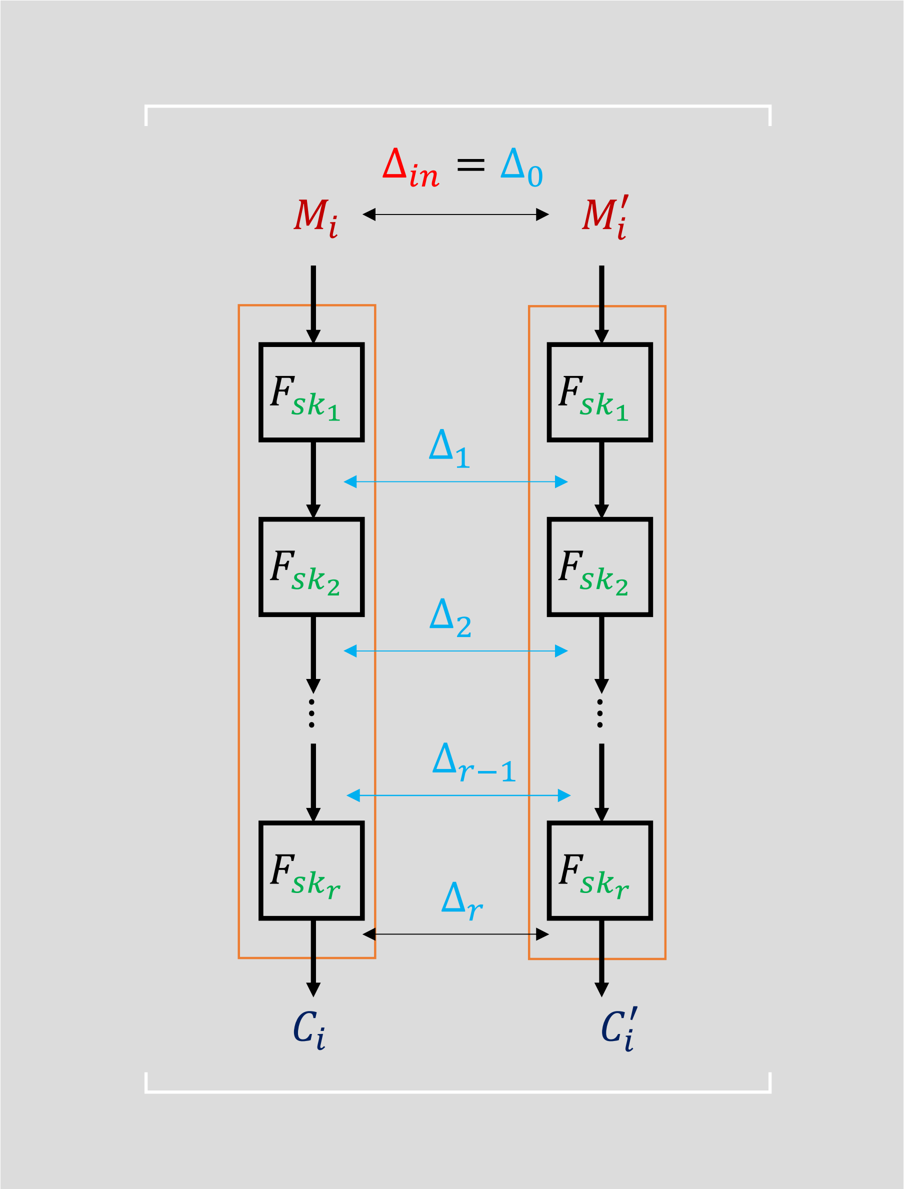
مقـدمه

سرنوشت تفاضل در عبور از تابع دور

مشخصه‌ی تفاضلی و احتمال آن

استفاده از مشخصه‌ی تفاضلی به عنوان تمایزگر

هدف از تمایزگر تفاضلی



- فرض کنید که احتمال یک مشخصه‌ی تفاضلی $(\Delta_0, \ldots, \Delta_r)$ برای یک الگوریتم رمزنگاری قالبی r دوری با طول قالب b بیت، $p > 2^{-b}$ باشد.
- فرض کنید N مقدار (M_i, M'_i, C_i, C'_i) داده شده است، به‌گونه‌ای که $M_i \oplus M'_i = \Delta_0$ باشد $(1 \leq i \leq N)$.
- آیا راه‌کاری وجود دارد که بتوان با استفاده از آن قضاوت کرد که متون رمزشده‌ی موجود،

  توسط این الگوریتم رمزنگاری تولید شده‌اند؟

  یا

  کاملا تصادفی هستند؟

نحوه‌ی تمایز دادن الگوریتم از جایگشت ایده‌آل

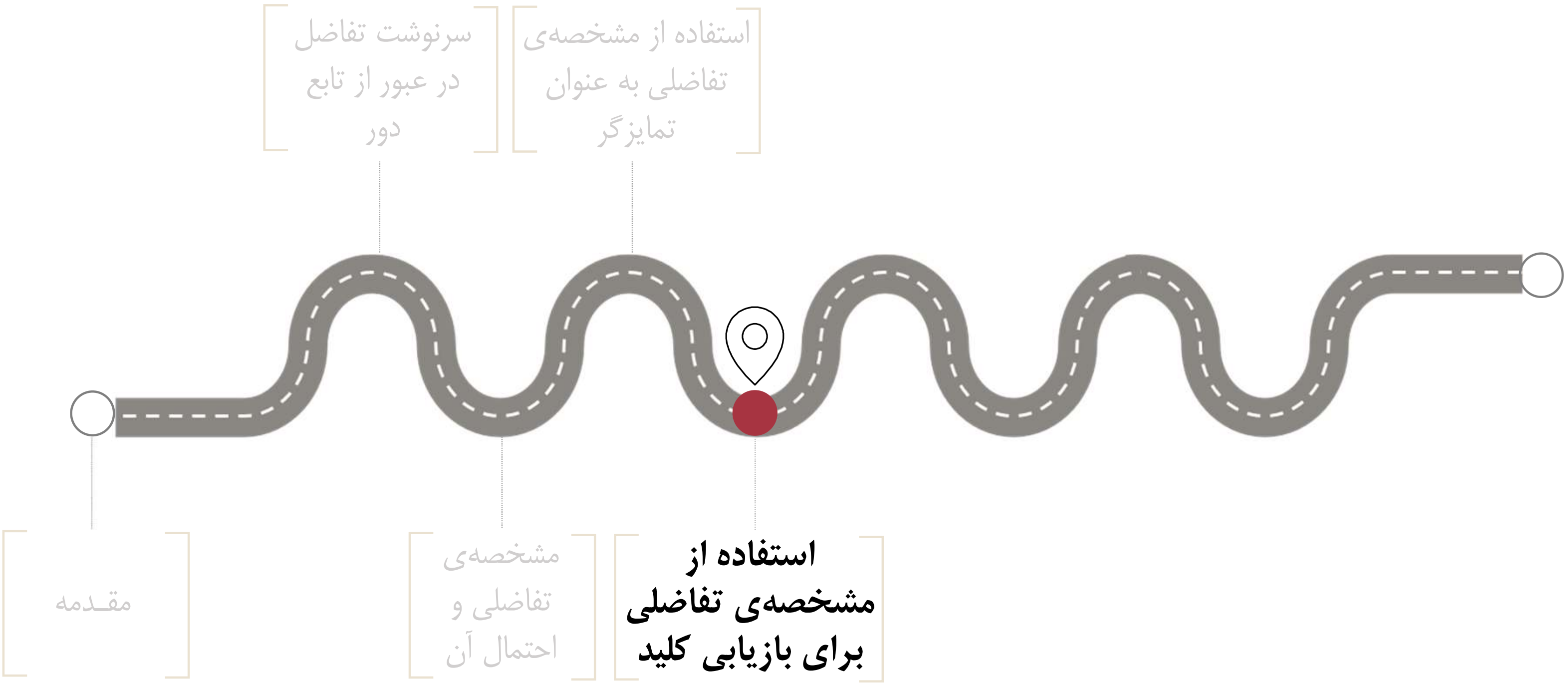
- اگر زوج‌های (C_i,C_i') معادل رمزشده‌ی زوج متن‌های اصلی (M_i,M_i') توسط الگوریتم باشند، انتظار داریم حدود $N.p$ بار در رابطه‌ی $C_i \oplus C_i' = \Delta_r$ صدق کنند.
- در غیر این صورت انتظار داریم حدود $N.2^{-b}$ بار در رابطه صدق کنند.
  - ✓ یادآوری: 2^{-b} احتمال حدودی برای رویداد تصادفی است.

پیچیدگی زمانی حمله

- با فرض بزرگ بودن احتمال p، اگر N به اندازه کافی بزرگ باشد، می‌توان الگوریتم رمزنگاری را از یک جایگشت ایده آل تمایز داد.
- اگر برای تولید این متن‌ها از الگوریتم مورد هدف استفاده شده باشد، باید حداقل یک زوج صحیح وجود داشته باشد:

$$N \times p > 1 \ \Rightarrow N > 1/p$$

- $O(1/p)$ زوج متن منتخب لازم است.



مقـدمه

سرنوشت تفاضل در عبور از تابع دور

مشخصه‌ی تفاضلی و احتمال آن

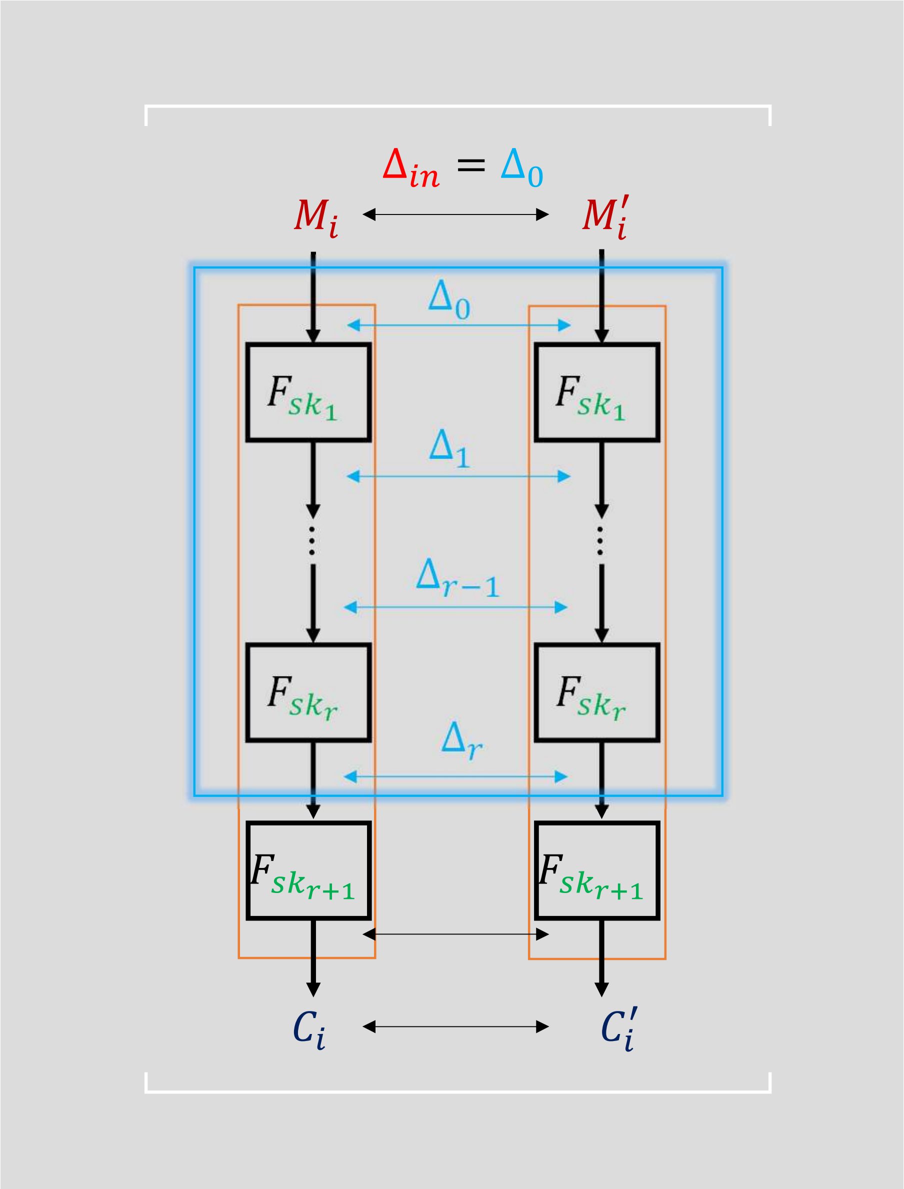
استفاده از مشخصه‌ی تفاضلی به عنوان تمایزگر

استفاده از مشخصه‌ی تفاضلی برای بازیابی کلید

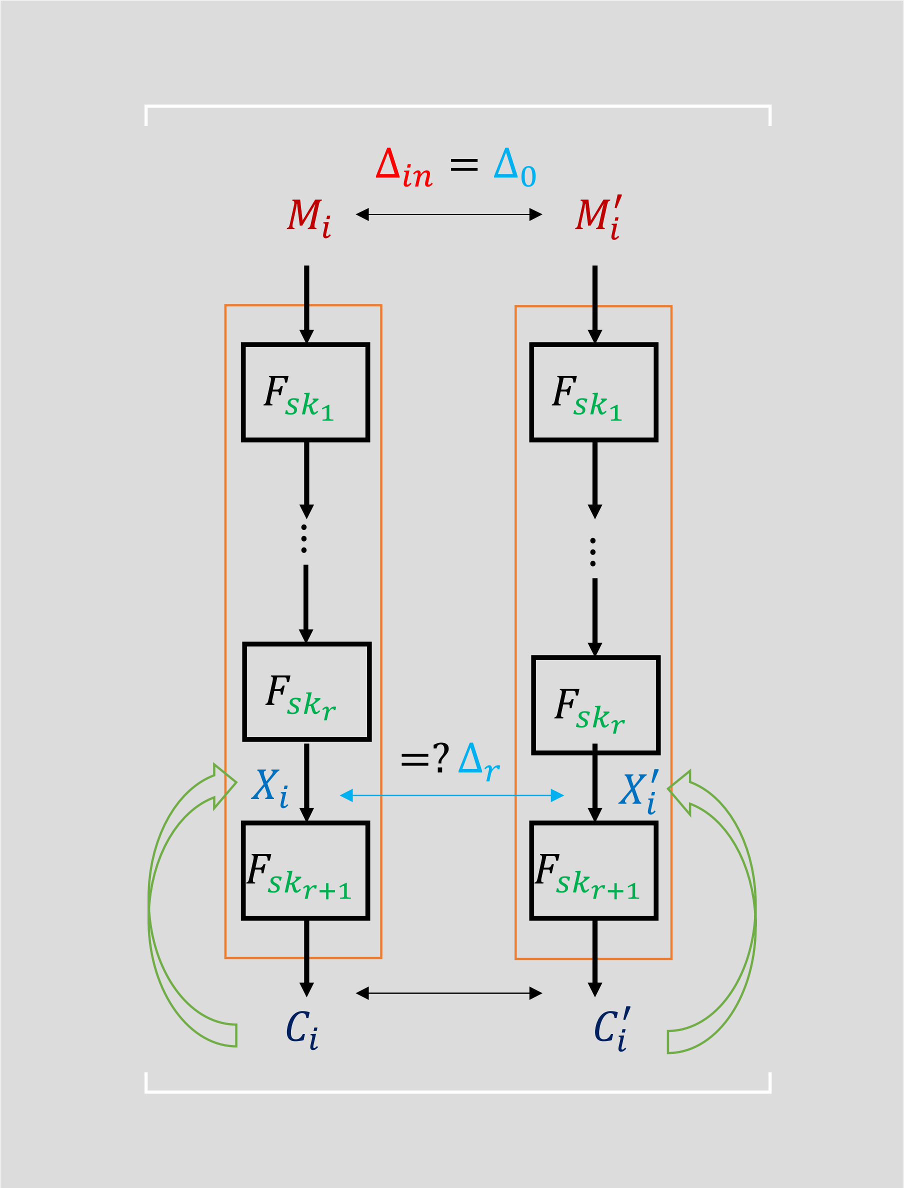
هدف در بازیابی کلید

(Key Recovery)

- فرض کنید که احتمال یک مشخصه‌ی تفاضلی $(\Delta_0, \dots, \Delta_r)$ برای یک الگوریتم رمزنگاری قالبیِ $r + 1$ دوری با طول قالب b بیت، برابر $p > 2^{-b}$ باشد.
- فرض کنید N مقدار (M_i, M_i', C_i, C_i') داده شده است، به‌گونه‌ای که $M_i \oplus M_i' = \Delta_0$ باشد $(1 \le i \le N)$ و زوج‌های (C_i, C_i') معادل رمزشده‌ی زوج متن‌های اصلی (M_i, M_i') توسط الگوریتم باشند.
- آیا راه‌کاری وجود دارد که بتوان با استفاده از آن اطلاعاتی درباره کلید الگوریتم پیدا کرد؟

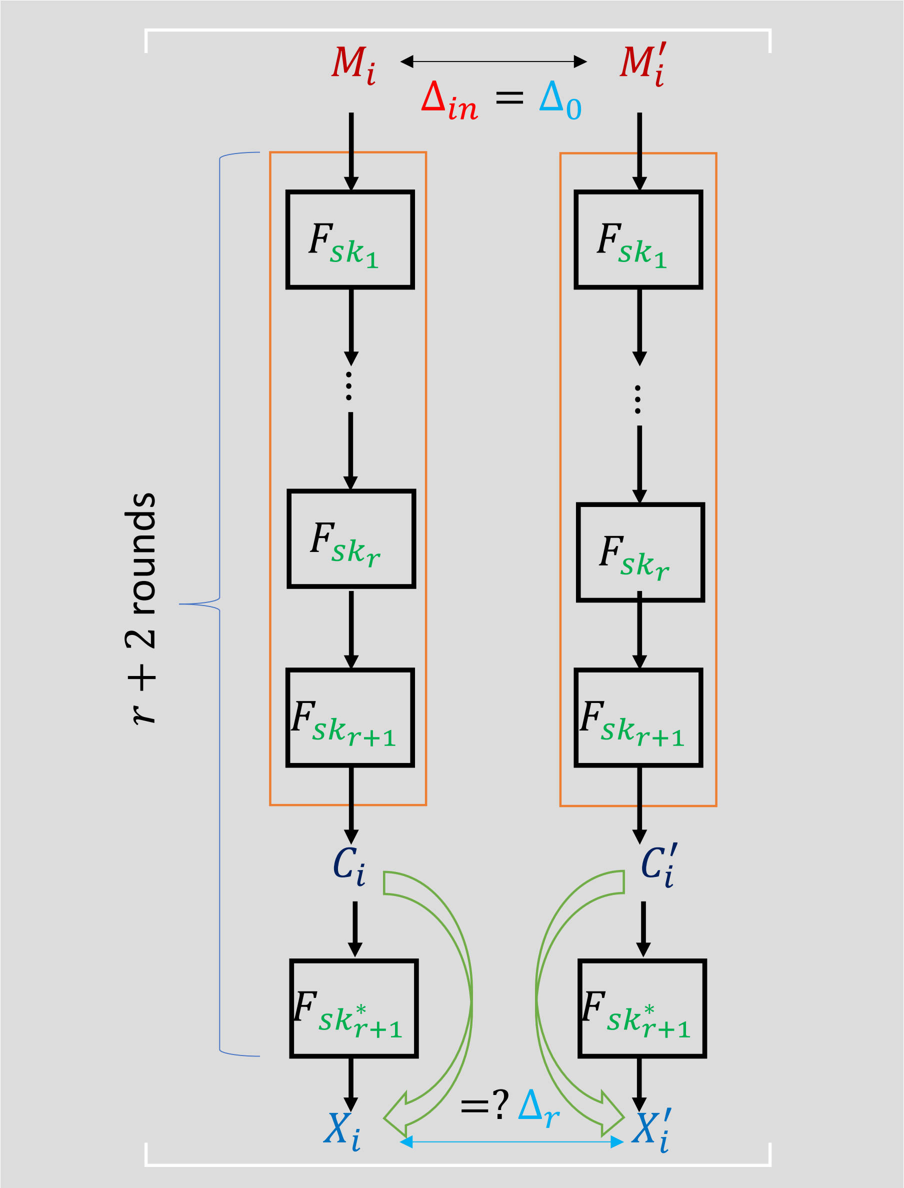


نمایی کلی از حمله‌ی بازیابی کلید



- زیر کلید دور آخر را حدس می‌زنیم، و تمامی زوج متن‌های رمزشده (C_i,C_i') را یک دور رمزگشایی می‌کنیم تا به مقادیر میانی در انتهای دور rام (X_i,X_i') برسیم.
- تعداد دفعاتی که رابطه‌ی $X_i \oplus X_i' = \Delta_r$ برقرار است را می‌شماریم.
- کاندید صحیح برای sk_{r+1}، کلیدی است که رابطه‌ی تفاضلی به دفعات بیشتری برای آن صادق باشد (حدود $N \times p$ بار).
- چرا انتظار داریم که به ازای کلید غلط، به صورت معمول تعداد دفعات کمتری رابطه‌ی تفاضلی در انتهای دور rام صادق باشد؟

اثر کلید غلط در فرآیند حمله



- به عنوان یک شهود ساده، می‌توان به این نکته اشاره کرد که رمزگشایی تحت کلید غلط sk^*_{r+1} در حقیقت منجر به رمزگشایی نمی‌شود.
- (به صورت فرضی) می‌توان آن را معادل رمزکردن یک دوری متون رمزشده تحت کلید غلط sk^*_{r+1} در نظر گرفت.
- انتظار داریم که یک مشخصه‌ی تفاضلی برای $r + 2$ دور با احتمال کمتری صادق باشد (نسبت به یک مشخصه‌ی تفاضلی r دوری).

اثر کلید غلط در فرآیند حمله

ادامه ...

- فرض کنید حداکثر احتمال یک مشخصه‌ی تفاضلی برای r دور از یک الگوریتم رمزنگاری قالبی برابر p باشد.
- در فرآیند حمله به $r+1$ دور الگوریتم، اگر کلید دور آخر را غلط حدس بزنیم، احتمال رخ دادن مشخصه‌ی مذکور کم‌تر از p خواهد بود (Wrong-Key-Randomization Hypothesis).
- معمولا فرض صحیحی است و شواهد عملی متعددی برای آن ارائه شده است.
- پژوهش‌های نظری فراوانی در این خصوص ارائه شده‌اند که می‌توان با استفاده از آن‌ها، به صورت دقیق‌تری مدل کرد که در صورت زدن غلط حدس کلید غلط چه اتفاقاتی رخ می‌دهد.
- مرجع پیشنهادی برای علاقه‌مندان:

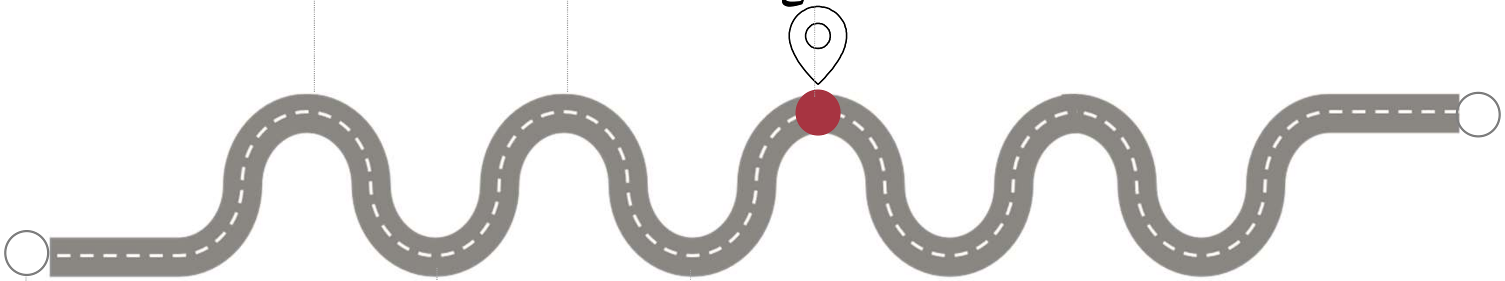
📖 Accurate estimates of the data complexity and success probability for various cryptanalyses Céline Blondeau, Benoît Gérard & Jean-Pierre Tillich Designs, Codes and Cryptography volume 59, pages3–34(2011)

تعداد متون مورد نیاز برای بازیابی کلید

- به‌ازای کلید صحیح، باید تمایزگری قابل مشاهده داشته باشیم ($N.p$ باید از 1 بزرگتر باشد).
- حداقل p^{-1} زوج لازم است.
- در عمل $c.p^{-1}$ زوج لازم است که مقدار c معمولا کوچک است.
- مقدار دقیق داده‌ی مورد نیاز به تعداد کاندیدهای کلید وابسته است.

پیچیدگی زمانی بازیابی کلید

- به ازای هر مقدار ممکن برای زیرکلید دور آخر، باید N زوج متن (پیچیدگی داده) را یک دور رمزگشایی کنیم.
  - بنابراین به ازای هر فرض زیرکلید، $2 \times N$ عملیات رمزگشایی یک دوری نیاز است.
- اگر اندازه‌ی زیرکلید آخر را $|k|$ بیت در نظر بگیریم، $2^{|k|}$ کاندید برای زیرکلید دور آخر خواهیم داشت.
- بنابراین در مجموع باید $N \times 2 \times 2^{|k|}$ عملیات رمزگشایی یک دوری انجام دهیم.
- این پیچیدگی زمانی در عمل می تواند بسیار زیاد باشد (در مواردی حتی بیشتر از جست‌وجوی کامل!).
- لزوم به‌کارگیری راه‌کارهایی به منظور بهینه سازی این چارچوب.



مقدمه

سرنوشت تفاضل
در عبور از تابع
دور

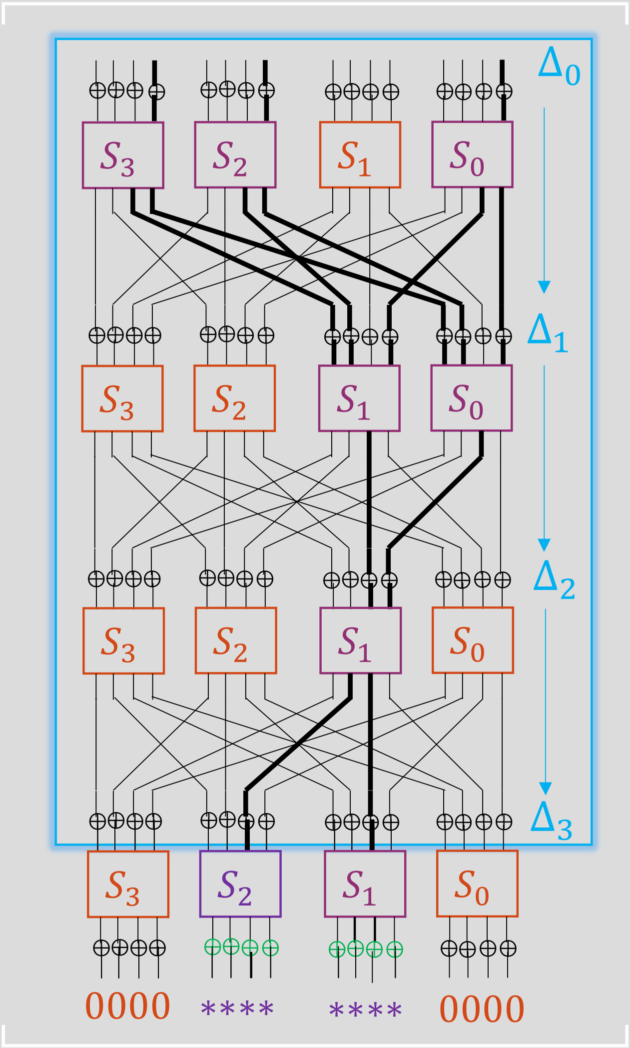
مشخصه‌ی
تفاضلی و
احتمال آن

استفاده از مشخصه‌ی
تفاضلی به عنوان
تمایزگر

استفاده از
مشخصه‌ی تفاضلی
برای بازیابی کلید

**روش فیلتر کردن
برای بهبود حمله‌ی
تفاضلی**

فیلتر کردن زوج متن‌ها



- فرض کنید براساس مشخصه‌ی تفاضلی سه دوری برای SMALL-PRESENT-16 که در شکل نمایش داده شده است، می‌خواهیم به چهار دور الگوریتم حمله کنیم.
- زوج متن‌های صحیح حتما در رابطه‌ی زیر صدق می‌کنند:

$$C_i \oplus C_i' = 0000\ \ \text{****}\ \text{****}\ 0000$$

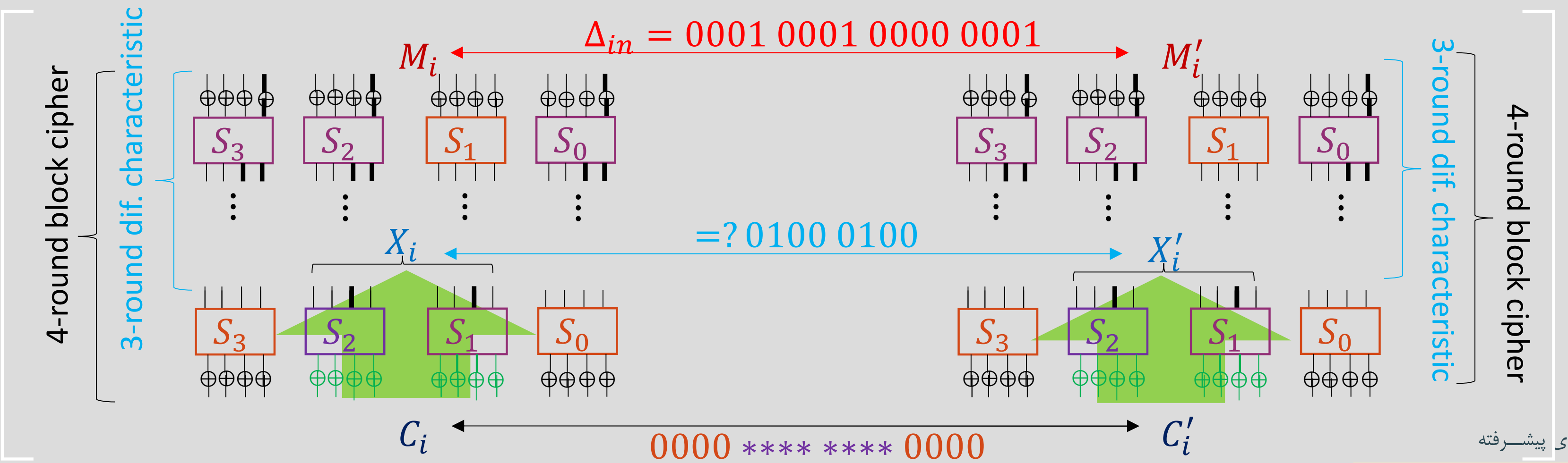
- دلیل: اگر تفاضل ورودی جعبه‌ی جانشانی 0 باشد، تفاضل خروجی هم حتما 0 است.

1. لزومی ندارد حمله را برای همه‌ی متون اجرا کنیم (Filtering).
2. لزومی ندارد تمام بیت‌های زیرکلید را حدس بزنیم (کافی است بیت‌های زیرکلیدی که بر جعبه‌های جانشانی فعال منطبق هستند حدس زده شوند).

فیلتر کردن زوج متن‌ها

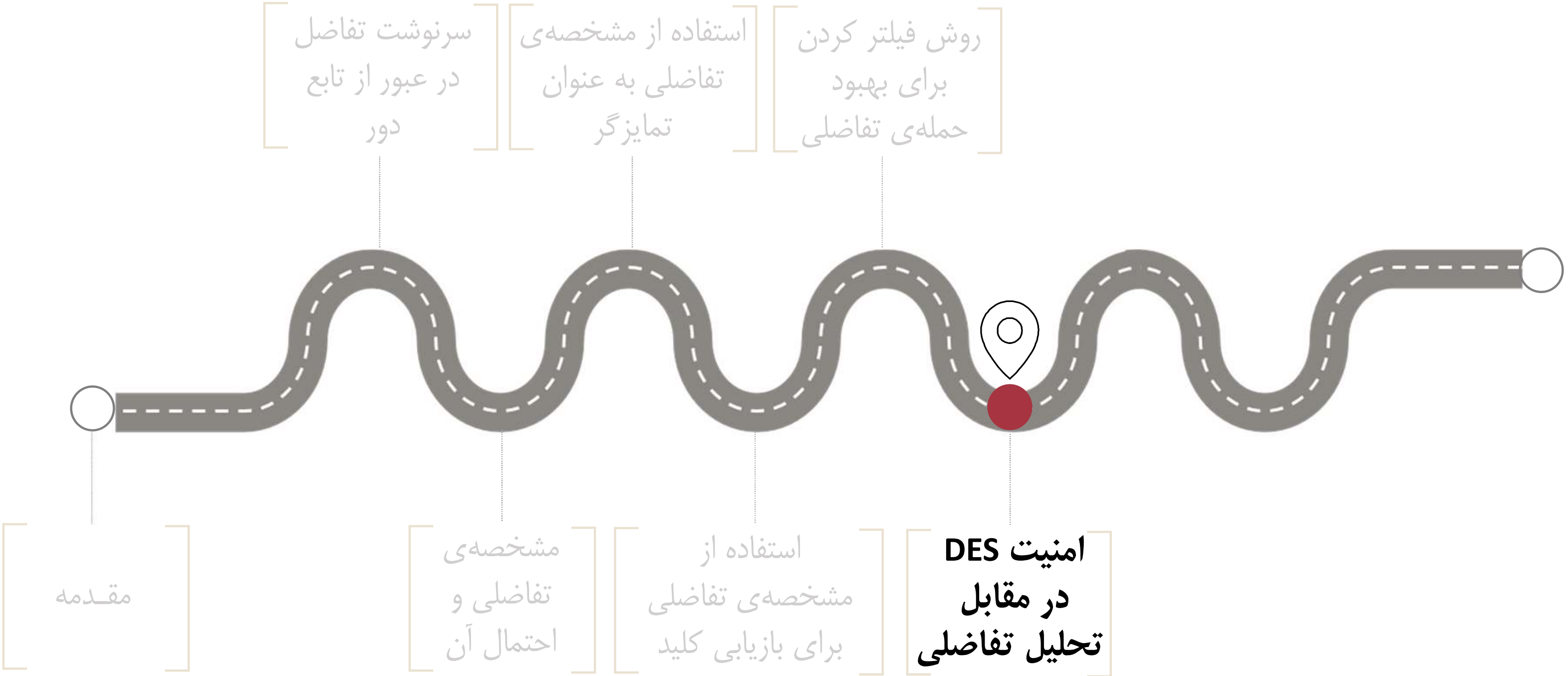
ادامه ...

- زوج‌های به شکل $C_i \oplus C_i' = 0000\ {*}{*}{*}{*}\ {*}{*}{*}{*}\ 0000$ را در نظر می‌گیریم.
- به‌ازای تمام کاندیدهای ممکن برای هشت بیت زیرکلید دور آخر، هشت بیت منطبق بر جعبه‌های جانشانی فعال را یک دور رمزگشایی می‌کنیم.
- تعداد دفعاتی که رابطه‌ی تفاضلی در دور یکی مانده به آخر صدق می‌کند را می‌شماریم؛ یعنی تعداد دفعاتی که $X_i \oplus X_i' = \Delta_3$ می‌شود.
- کلید صحیح، کلیدی است که رابطه‌ی تفاضلی را به دفعات بیشتری برقرار کند.



پیچیدگی زمانی بازیابی کلید به روش بهینه‌سازی شده

- تعداد زوج متون رمزشده (C_i,C_i') که در رابطه‌ی
$$C_i \oplus C_i' = 0000\ \ {*}{*}{*}{*}\ {*}{*}{*}{*}\ 0000$$
صدق می‌کنند، تقریبا برابر $N \times 2^{-8}$ است.
- تعداد کاندیدها برای ۸ بیت زیرکلید دور آخر (منطبق بر جعبه‌های جانشانی شماره‌ی ۱ و ۲) برابر با 2^8 است.
- تمامی زوج متن‌های به شکل فوق را یک دور تحت تمام کاندیدهای ۸ بیت زیرکلید دور آخر رمزگشائی می‌کنیم. پس پیچیدگی زمانی تقریبا برابر است با $2^8 \times (2 \times N \times 2^{-8}) = 2 \times N$ عمل رمزگشایی یک دوری.
- اگر روش فیلتر کردن را اعمال نمی‌کردیم، باید تمام ۱۶ بیت زیرکلید دور آخر را حدس زده و به‌ازای تمام متون رمزگشایی می‌کردیم که پیچیدگی برابر $2^{16} \times 2 \times N$ می‌شد.
  - توجه: مرتبه‌ی تعداد متون مورد نیاز تغییر نمی‌کند.



مقـدمه

سرنوشت تفاضل در عبور از تابع دور

مشخصه‌ی تفاضلی و احتمال آن

استفاده از مشخصه‌ی تفاضلی به عنوان تمایزگر

استفاده از مشخصه‌ی تفاضلی برای بازیابی کلید

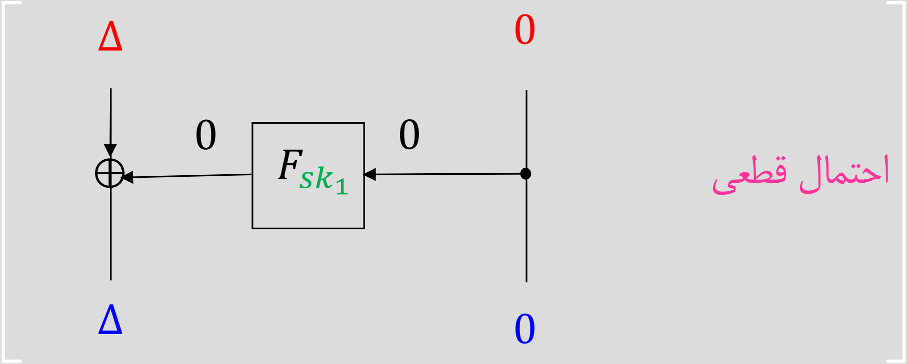
روش فیلتر کردن برای بهبود حمله‌ی تفاضلی

امنیت DES در مقابل تحلیل تفاضلی

مشخصه‌ی تفاضلی یک دوری در DES

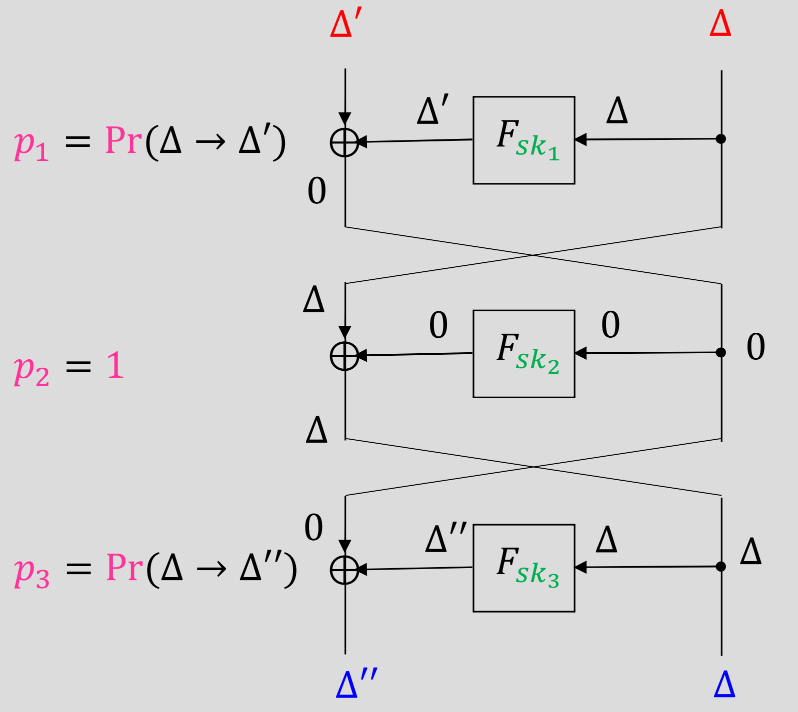
(یا هر ساختار فیستلی دیگر)

- تفاضل $(\Delta,0)$ به تفاضل $(\Delta,0)$ منجر می‌شود که $\Delta \in \mathbb{F}_2^{b/2}$ یک مقدار دلخواه است.
- بنابراین با توجه به اینکه تنها نیمی از حالت (State) وارد تابع دور می‌شود، می‌توان بسیار ساده نتیجه‌گیری کرد که برای یک الگوریتم فیستلی یک دوری، مشخصه‌های تفاضلی متعددی با احتمال قطعی $(\Pr = 1)$ وجود دارند.



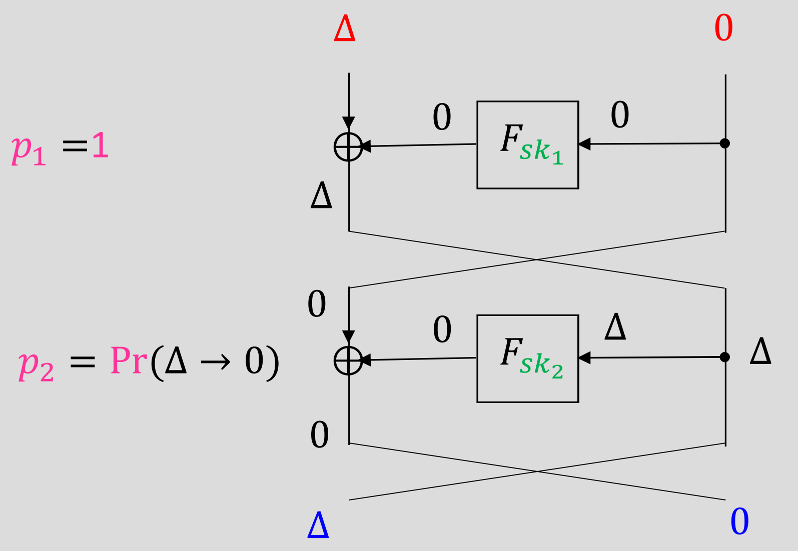
مشخصه‌ی تفاضلی سه دوری در DES

- مشخصه‌ی تفاضلی سه دوریِ پیشنهاد شده توسط بیهام و شمیر برای DES: تولید تفاضل 0 در قسمتی از ورودی دور دوم که وارد تابع دور می‌شود (نیمه‌ی سمت راست).
- وجود تعداد کمتری تابع فعال (و یا جعبه‌های جانشانی) سبب افزایش احتمال مشخصه‌ی تفاضلی می‌شود.



$$\Pr\big((\Delta',\Delta) \to (\Delta,0) \to (\Delta'',\Delta)\big)$$
$$= p_1 \times p_2 \times p_3 = p_1 \times p_3$$

مشخصه‌ی تفاضلی تکرارپذیر



$$\Pr\big((\Delta, 0) \rightarrow (\Delta, 0)\big) = p_1 \times p_2 = \Pr(\Delta \rightarrow 0)$$

- اگر تفاضل خروجی یک مشخصه‌ی تفاضلی rدوری (با احتساب عمل جابه‌جایی دور آخر) با تفاضل ورودی برابر باشد، آن را مشخصه‌ی تفاضلی تکرارپذیر (iterative) می‌نامیم.
- بیهام و شمیر: بهترین مشخصه‌ی تفاضلی تکرارپذیر DES، ساده‌ترین مشخصه‌ی دو دوری است.
- دقت شود که چون تابع دور DES یک‌به‌یک نیست، تفاضل غیرصفر در ورودی تابع دور می‌تواند منجر به تفاضل صفر شود.

نتایج تحلیل تفاضلی DES

تعداد دورها	پیچیدگی
4	2^{4}
8	2^{16}
13	2^{44}
14	2^{51}
15	2^{52}
16	2^{58}

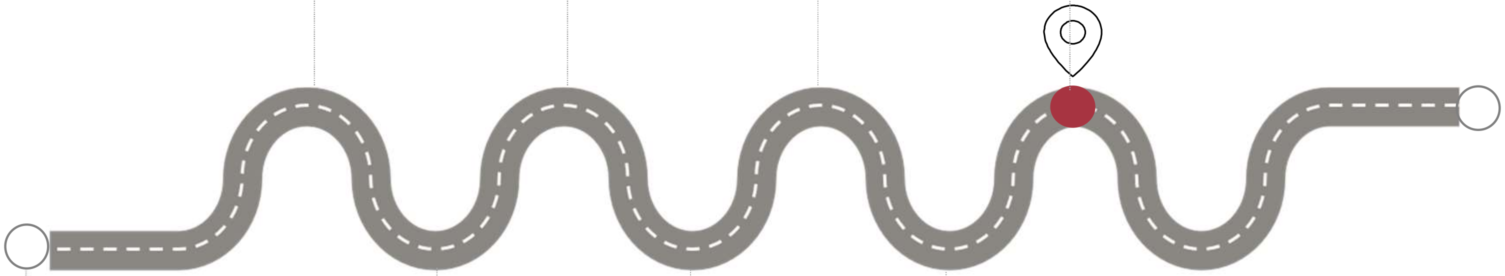
- نتایج منتشر شده نشان می‌دهند که تعداد دورهای انتخابی DES (نسبتا) مناسب انتخاب شده‌اند.

امنیت DES در مقابل تحلیل تفاضلی

- یکی از اعضای برجسته تیم طراحی DES در IBM با انتشار مقاله‌ای ادعا کرد که در زمان طراحی از تحلیل تفاضلی اطلاع داشته و آن را مدنظر قرار داده بودند!
- با توجه به نتایج جدول صفحه‌ی قبل، این ادعا به نظر صحیح می‌آید.

Source: Coppersmith, Don (May 1994). "The Data Encryption Standard (DES) and its strength against attacks" (PDF). IBM Journal of Research and Development. 38 (3): 243

> “The design took advantage of certain cryptanalytic techniques, most prominently the technique of “differential cryptanalysis”. After discussions with NSA, it was decided that disclosure of the design considerations would reveal the technique of differential cryptanalysis, a powerful technique that could be used against many ciphers. This in turn would weaken the competitive advantage the United States enjoyed over other countries in the field of cryptography."



مقـدمه

سرنوشت تفاضل
در عبور از تابع
دور

مشخصه‌ی
تفاضلی و
احتمال آن

استفاده از مشخصه‌ی
تفاضلی به عنوان
تمایزگر

استفاده از
مشخصه‌ی تفاضلی
برای بازیابی کلید

روش فیلتر کردن
برای بهبود
حمله‌ی تفاضلی

امنیت DES
در مقابل
تحلیل تفاضلی

امنیت AES
در مقابل
تحلیل تفاضلی

مشخصات تفاضلی جعبه‌ی جانشانی AES

- جعبه‌ی جانشانی AES به نحوی طراحی شده است که ۴-یکنواخت تفاضلی است.
  - بهترین جعبه‌ی جانشانی شناخته‌شده‌ی ۸ بیتی به لحاظ مشخصات آماری!
- به عبارت دیگر حداکثر احتمال انتقال یک تفاضل ورودی به یک تفاضل خروجی در جعبه جانشانی AES، برابر $2^{-6} = \frac{4}{2^8}$ است.

مفهوم عدد انشعاب

(Branch Number)

- فرض کنید تبدیل خطی $\mathcal{L}$، n کلمه‌ی m بیتی (مثلا هشت بیتی) را به n کلمه‌ی m بیتی دیگر تبدیل می‌کند.

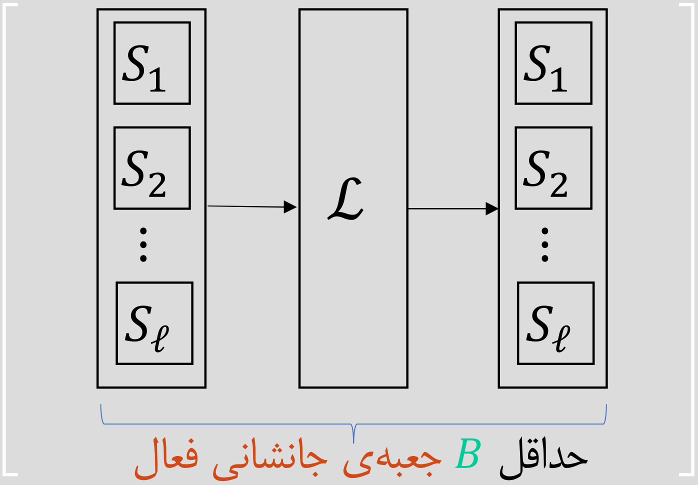
$$\begin{bmatrix}x_1\\x_2\\\vdots\\x_n\end{bmatrix} \longrightarrow \boxed{\mathcal{L}} \longrightarrow \begin{bmatrix}y_1\\y_2\\\vdots\\y_n\end{bmatrix}$$

- فرض کنید این تبدیل دارای یک ویژگی باشد: اگر کلمات ورودی همزمان صفر نباشند، حداقل تعداد کلمات غیرصفر ورودی و خروجی برابر B است.
- در این صورت B را عدد انشعاب تبدیل خطی $\mathcal{L}$ گویند.
- تعریف دقیق ریاضی:

$$B(L) = \min_{a\neq 0}(wt(x) + wt(L(x)))$$

تاثیر عدد انشعاب بر تعداد جعبه‌های جانشانی فعال

- تبدیل‌های خطی با عدد انشعاب بالا، در صورت استفاده‌ی هوشمندانه می‌توانند تاثیر مناسبی در افزایش تعداد جعبه‌های جانشانی فعال (غیرصفر) داشته باشند.
- البته نمی‌توان گفت که لایه‌ی غیرخطی تاثیری در تعداد جعبه‌های جانشانی ندارد.
  - مثال مناسب برای علاقه‌مندان: الگوریتم رمزنگاری استاندارد PRESENT.

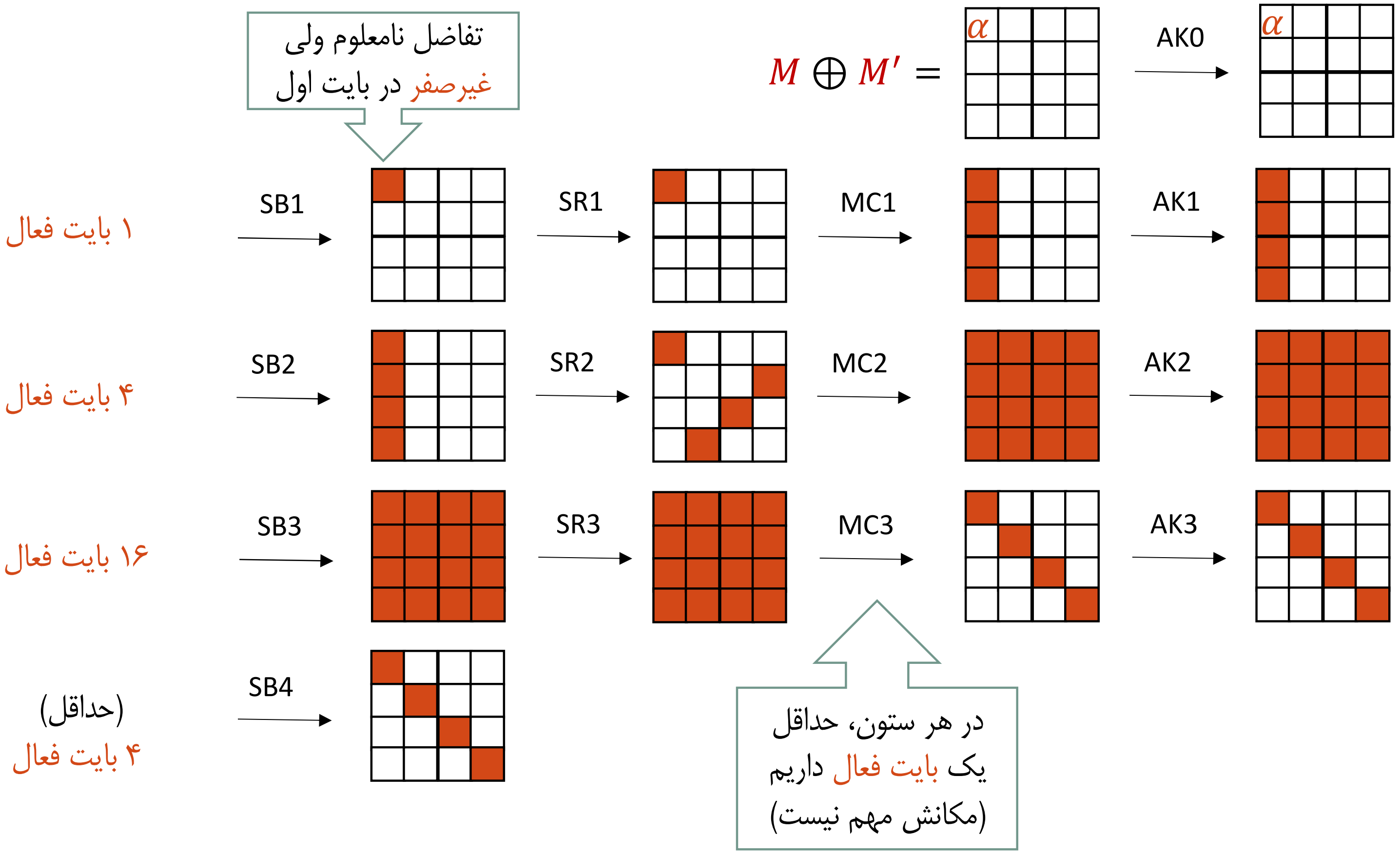


مثال: عدد انشعاب مخلوطساز ستونی AES

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$$

- عدد انشعاب مخلوطساز ستونی AES، ۵ است.
- اگر تفاضل ورودی فقط ۱ بایت فعال داشته باشد، آنگاه تفاضل خروجی دارای ۴ بایت فعال خواهد بود.
- اگر تفاضل ورودی فقط ۲ بایت فعال داشته باشد، آنگاه تفاضل خروجی حداقل ۳ بایت فعال خواهد داشت.
- اگر تفاضل ورودی فقط ۳ بایت فعال داشته باشد، آنگاه تفاضل خروجی حداقل ۲ بایت فعال خواهد داشت.

تاثیر لایه‌ی خطی AES بر تعداد جعبه‌های جانشانی فعال



تفاضل نامعلوم ولی
غیرصفر در بایت اول

۱ بایت فعال

۴ بایت فعال

۱۶ بایت فعال

(حداقل)
۴ بایت فعال

در هر ستون، حداقل
یک بایت فعال داریم
(مکانش مهم نیست)

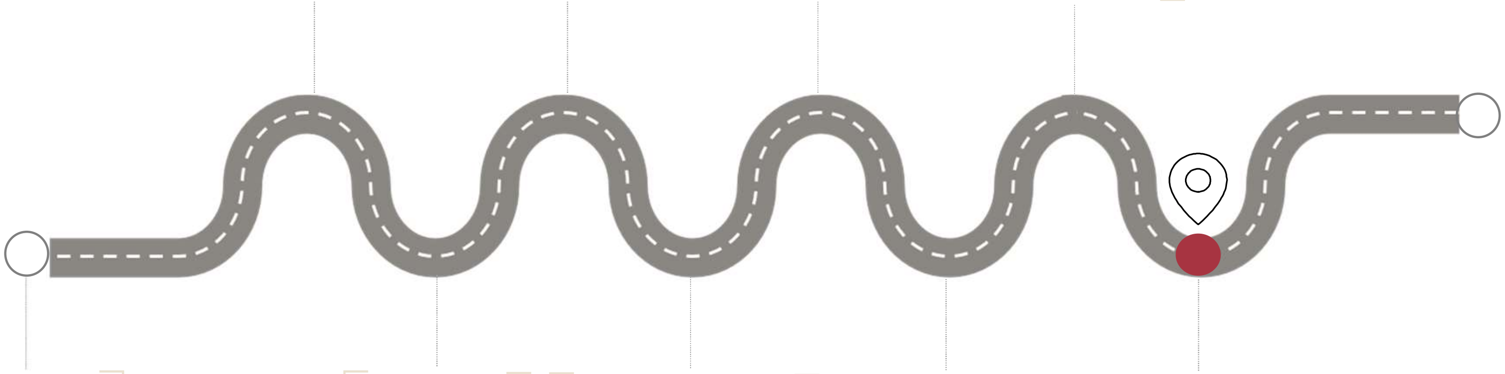
امنیت AES در مقابل تحلیل تفاضلی

1. می توان ثابت کرد که هر مشخصه‌ی تفاضلی چهار دوری AES حداقل ۲۵ جعبه‌ی جانشانی فعال دارد.
2. حداکثر احتمال انتقال در جعبه‌ی جانشانی AES برابر $2^{-6} = \frac{4}{256}$ است.

- بنابراین احتمال هر مشخصه‌ی تفاضلی چهار دوری AES حداکثر برابر است با: $(2^{-6})^{25} = 2^{-150}$
- به عبارت دیگر هیچ مشخصه‌ی تفاضلی چهار دوری برای AES با احتمال بیش‌تر از 2^{-128} وجود ندارد.

راه‌کار امنیتی AES در مقابل تحلیل تفاضلی

- راه‌کاری که توسط طراحان AES به کار گرفته شده است، به عنوان Wide Trail Design Strategy شناخته می‌شود.
- این راه‌کار به صورت گسترده در طراحی رمزهای قالبی بعدی (و بعضا توابع درهم‌ساز) مورد استفاده قرار گرفته و در حالت کلی بدین صورت است:
- اثبات می‌کنیم که برای r دور از الگوریتم، حداقل n جعبه‌ی جانشانی فعال وجود دارد.
- اگر بهترین احتمال انتقال تفاضل در جعبه‌ی جانشانی آن الگوریتم $2^{-\alpha}$ بود، کران بالای احتمال مشخصه‌ی تفاضلی r دوری دلخواه آن برابر $2^{-\alpha.n}$ می‌شود.



مقـدمه

سرنوشت تفاضل در عبور از تابع دور

مشخصه‌ی تفاضلی و احتمال آن

استفاده از مشخصه‌ی تفاضلی به عنوان تمایزگر

استفاده از مشخصه‌ی تفاضلی برای بازیابی کلید

روش فیلتر کردن برای بهبود حمله‌ی تفاضلی

امنیت DES در مقابل تحلیل تفاضلی

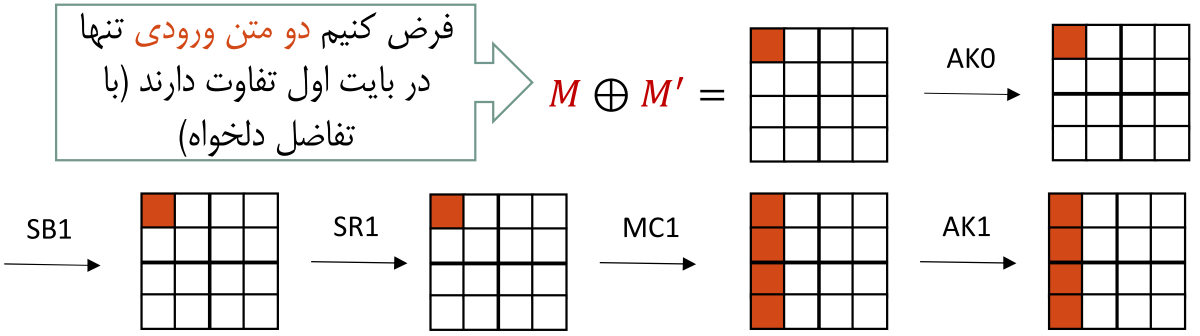
امنیت AES در مقابل تحلیل تفاضلی

مروری بر برخی از حملات خانواده‌ی تحلیل تفاضلی

تفاضل منقطع

(Truncated Differential)

- **توصیف ساده شده:** به جای یک مقدار خاص برای تفاضل خروجی، مجموعه‌ای از تفاضل‌های خروجی $\{\Delta_{out}^1, \ldots, \Delta_{out}^n\}$ را در نظر می‌گیریم.
- احتمال رخ دادن یکی از تفاضل‌های مورد نظر برای یک جایگشت ایده‌آل به طول b برابر $\frac{n}{2^b}$ است.
- اگر احتمال مشخصه‌ی تفاضلی منقطع برای الگوریتم هدف بیشتر از $\frac{n}{2^b}$ شد، یک رفتار غیرتصادفی (تمایزگر) محسوب می‌شود.



فرض کنیم دو متن ورودی تنها در بایت اول تفاوت دارند (با تفاضل دلخواه)

$M \oplus M' =$

۴ بایت تفاضل خروجی فعال و کل حالات ممکن تقریبا $(2^8)^4$ است.

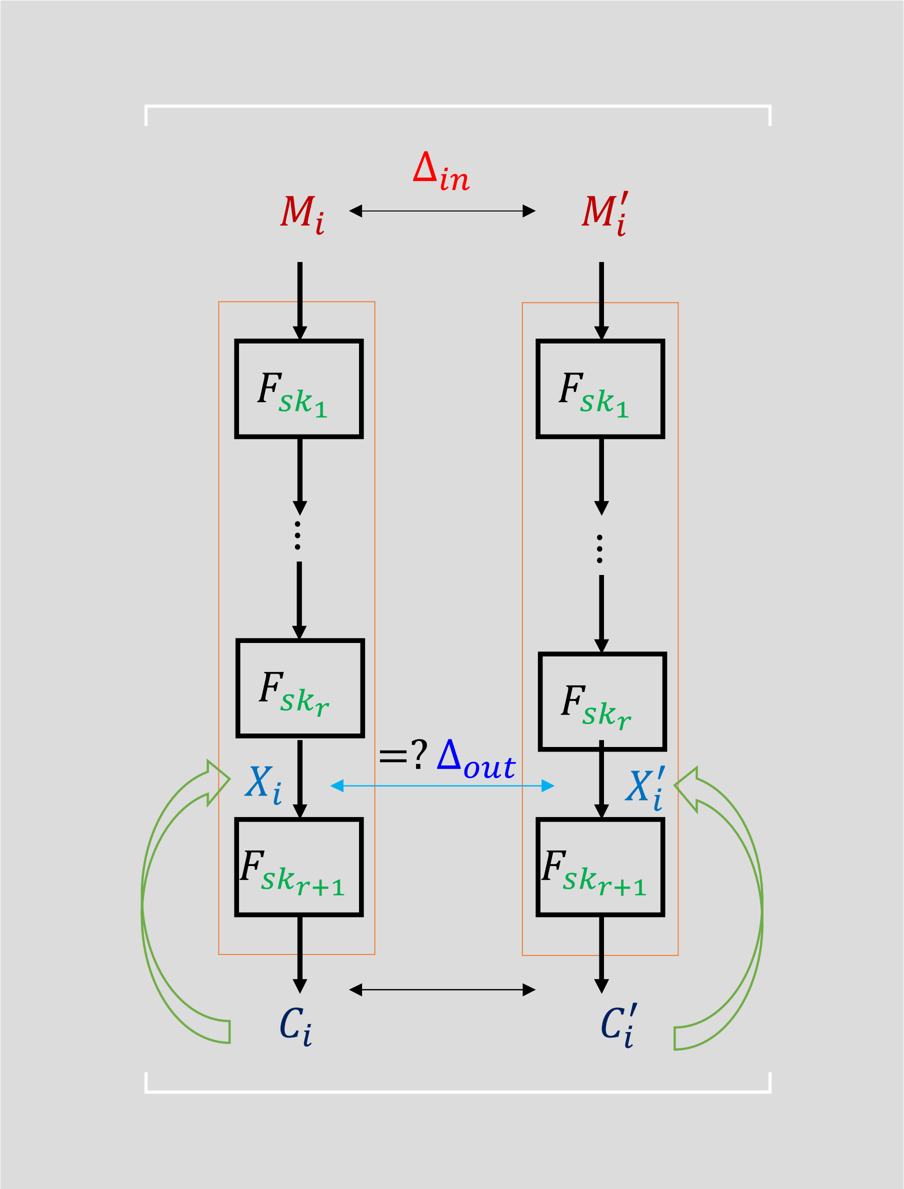
احتمال تفاضل منقطع برای یک دور از AES

$$1 > \frac{2^{32}}{2^{128}} = 2^{-9}$$

احتمال تفاضل منقطع برای جایگشت ایده‌آل

تفاضل ناممکن

(Impossible Differential)

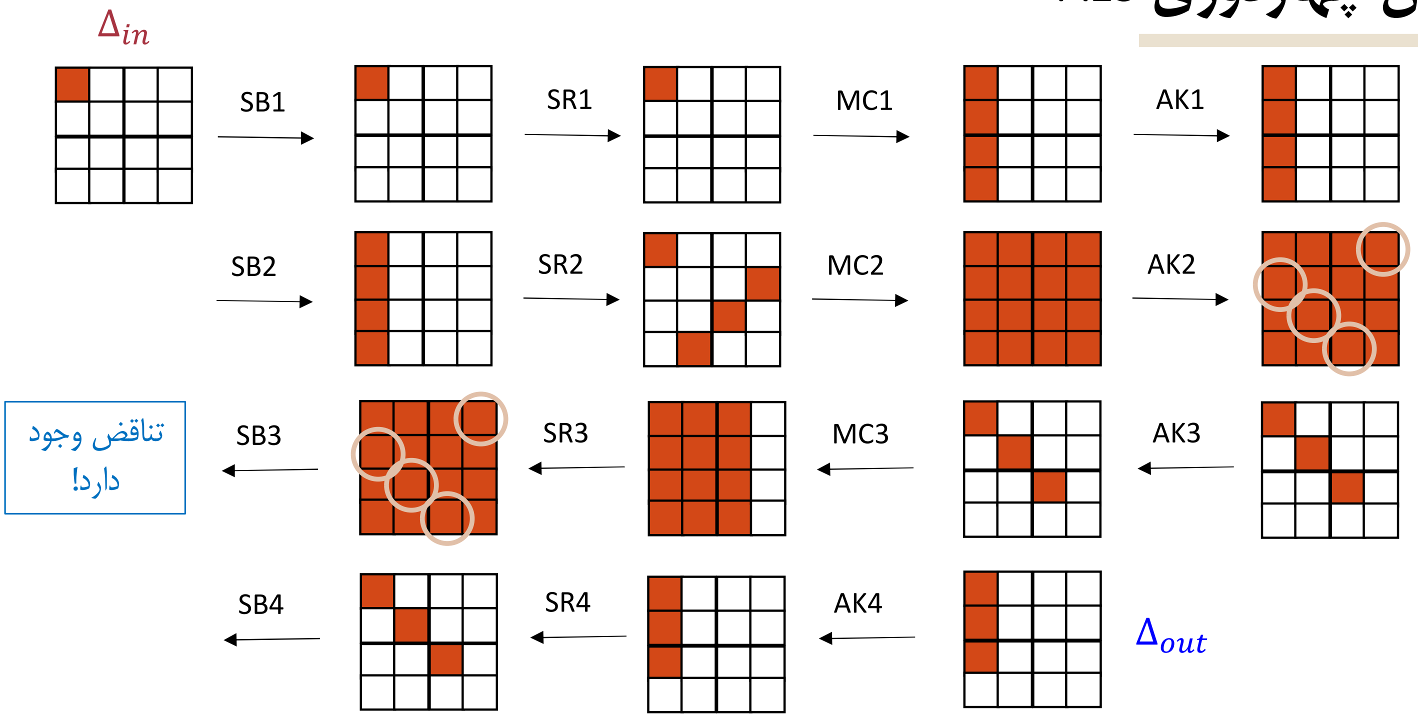


- اگر احتمال انتقال تفاضل ورودی Δ_{in} به تفاضل خروجی Δ_{out} برابر 0 شود، این رفتار تصادفی نیست!

$$\Pr[C \oplus C' = \Delta_{out} | M \oplus M' = \Delta_{in}] = 0 \neq 2^{-b}$$

- رخ دادن تفاضل ناممکن برای کلید حدس زده شده بدین معنی است که کلید حدس زده شده، غلط است.
- با حذف کاندیدهای غلط، می‌توان کلید صحیح را پیدا کرد.

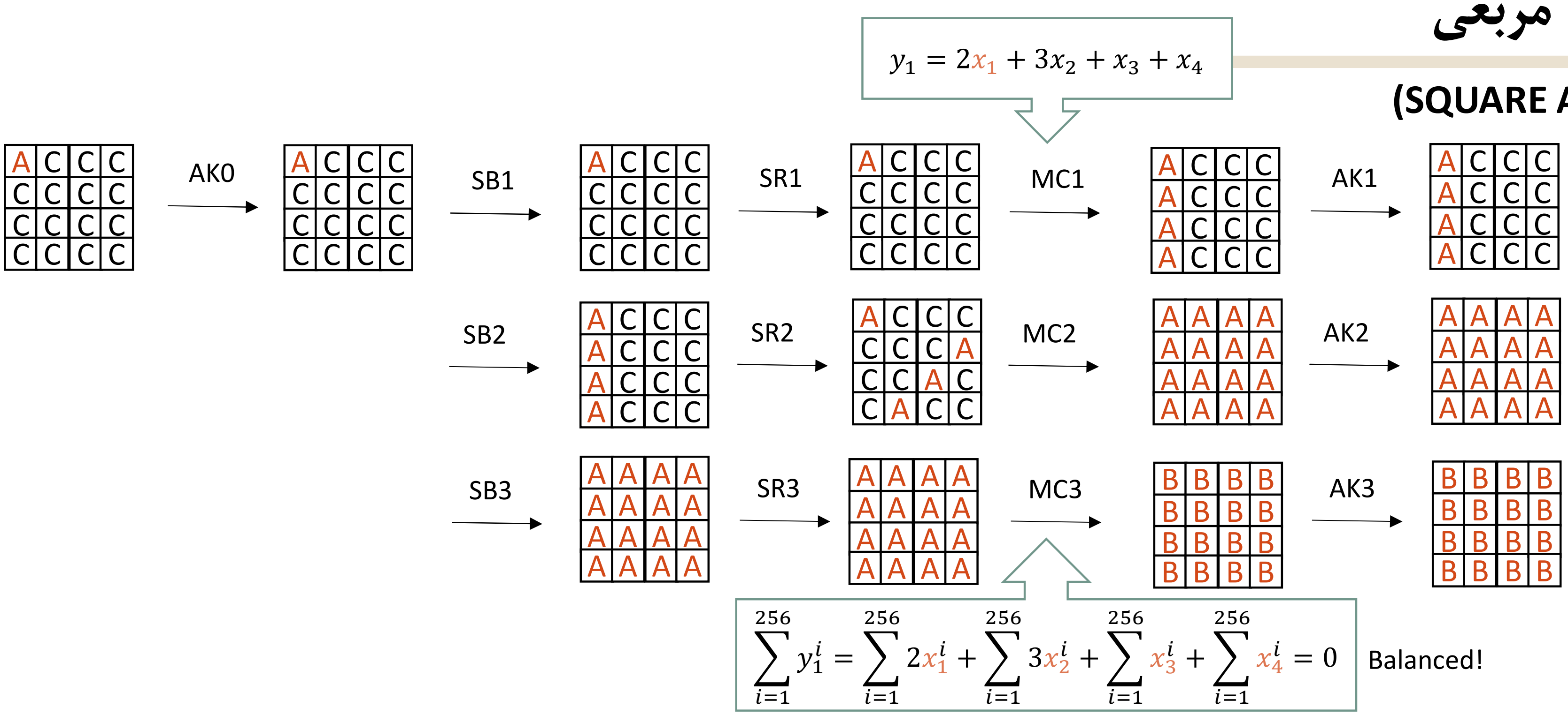
تفاضل ناممکن چهاردوری AES



- اگر تفاضل ورودی جعبه‌ی جانشانی غیرصفر باشد، تفاضل خروجی نمی‌تواند 0 شود.
- پس می‌توان نتیجه گرفت که: تفاضل ورودی به شکل نمایش داده شده‌ی Δ_{in}، هیچ‌گاه نمی‌تواند منجر به تفاضل خروجی نمایش داده شده به شکل Δ_{out} در دور چهارم (بدون احتساب مخلوط‌ساز ستونی) شود.

حمله‌ی مربعی

(SQUARE Attack)

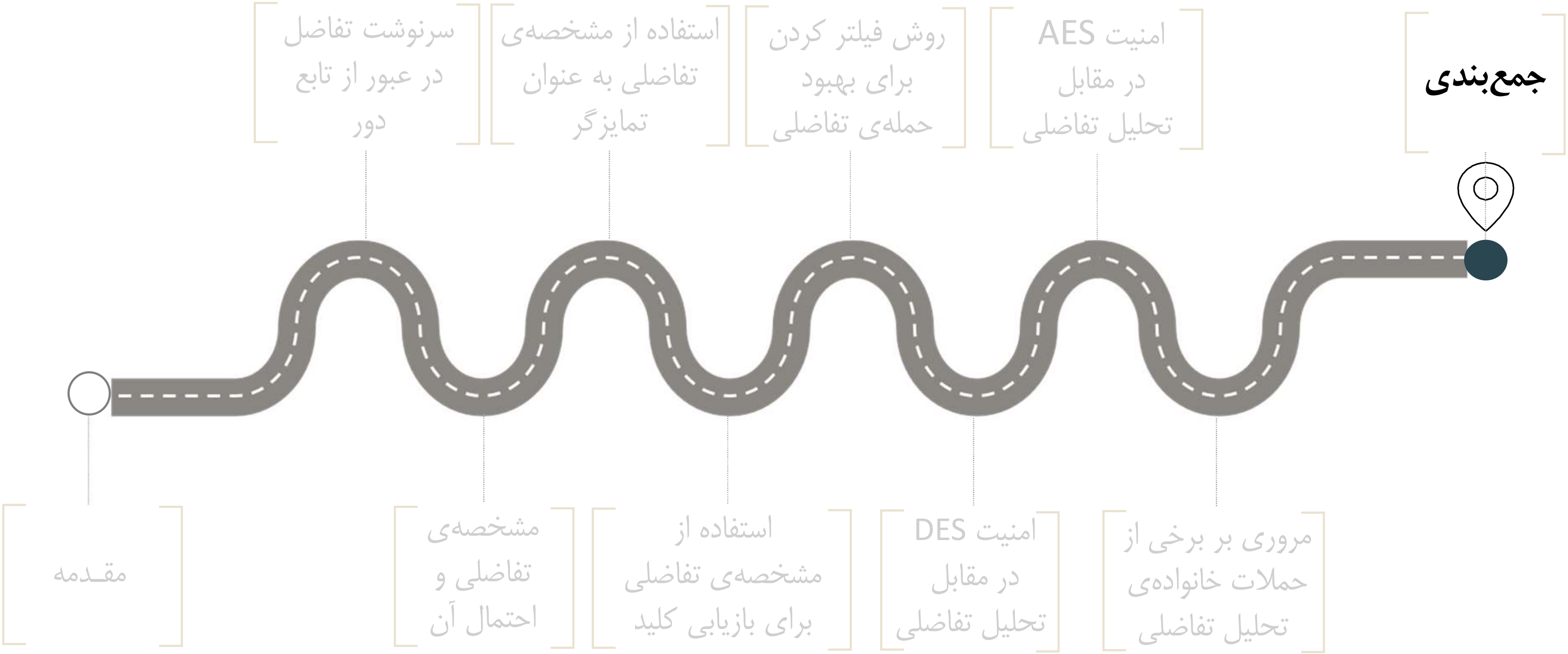


$$y_1 = 2x_1 + 3x_2 + x_3 + x_4$$

$$\sum_{i=1}^{256} y_1^i = \sum_{i=1}^{256} 2x_1^i + \sum_{i=1}^{256} 3x_2^i + \sum_{i=1}^{256} x_3^i + \sum_{i=1}^{256} x_4^i = 0$$

Balanced!

- ۲۵۶ متن در نظر می‌گیریم که در بایت اول تمام مقادیر ممکن را داشته باشند و در سایر بایت‌ها با هم برابر باشند.
- با احتمال ۱ جمع تمامی خروجی‌ها در یک بایت خاص در انتهای دور سوم برابر 0 خواهد بود، در صورتی‌که برای یک جایگشت تصادفی این احتمال 2^{-8} است.



مقـدمه

سرنوشت تفاضل در عبور از تابع دور

مشخصه‌ی تفاضلی و احتمال آن

استفاده از مشخصه‌ی تفاضلی به عنوان تمایزگر

استفاده از مشخصه‌ی تفاضلی برای بازیابی کلید

روش فیلتر کردن برای بهبود حمله‌ی تفاضلی

امنیت DES در مقابل تحلیل تفاضلی

امنیت AES در مقابل تحلیل تفاضلی

مروری بر برخی از حملات خانواده‌ی تحلیل تفاضلی

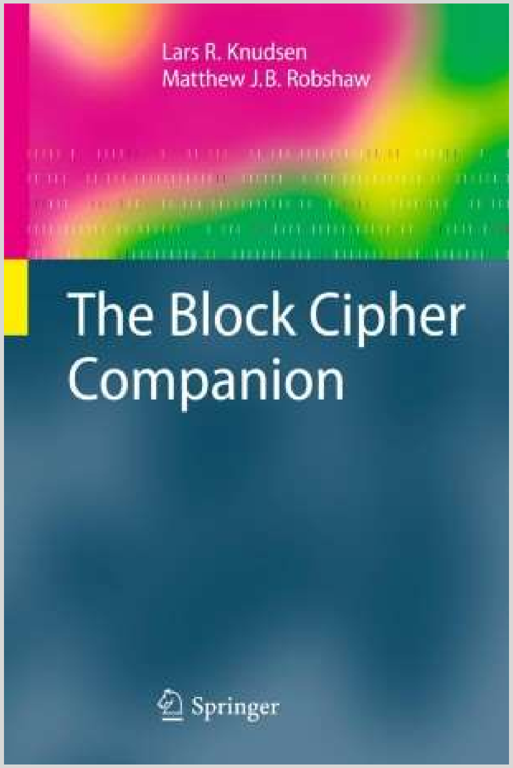
جمع‌بندی

جمع‌بندی

- در این درس با مفاهیم پایه تحلیل تفاضلی آشنا شدیم.
- تحلیل تفاضلی به (دورهای کاهش یافته‌ی) اکثر رمزهای قالبی قابل اعمال است.
- برای مقابله با این دسته از حملات، باید ساختار الگوریتم، اجزای الگوریتم و تعداد دورها به دقت طراحی شوند.

معرفی مـــراجع تکمیلی جهت مطالعه‌ی بیشتر

تحلیل تفاضلی



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.