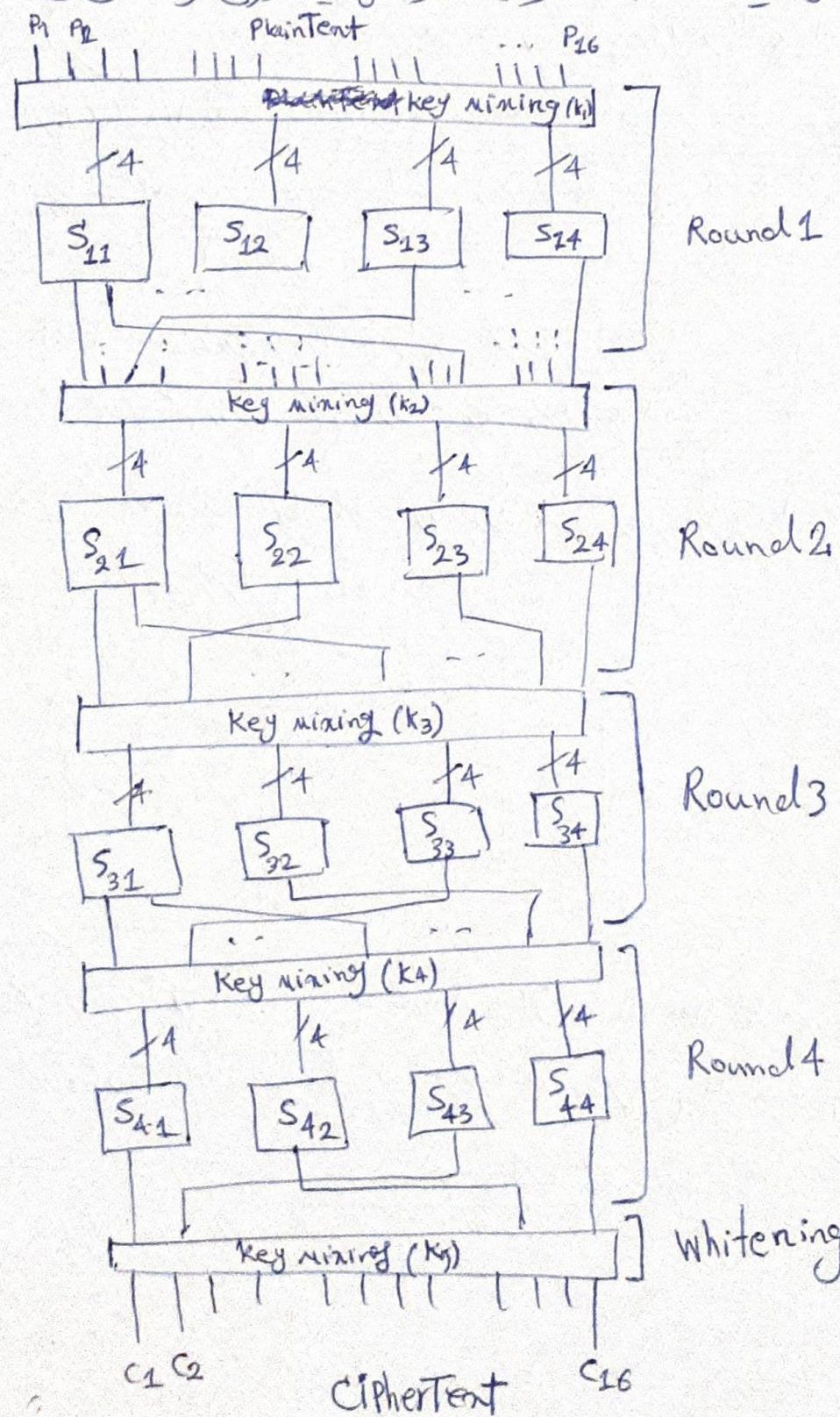


نکته: بطور معمول ساخت های ارائه داده برای بدستگیره رجایتی را بازبینی کرد
در دور آغاز همراه با زیر مدل در تظریه عمل کنید. نظریه امداداً انجام می دهد که این
عمل را استطلاع سفید ساز (Whitening) نامیده می شود. این امر صعبی سود را
جایز نمایند و چنانست دور آغاز در این ساخت ارائه شده صورت پاسخ

شکل زیر را بخوبی جایز نمایند و دری را شناسنید



برخی کات در زیر با شبکه رجیستر صیان شده است:

۱) کلید های مربوط به هر دور متفاوت بوره و از کلید اصلی (master key) رمز غالبی

(جایگشت سبد نفایخ) در هر دور مستقیم سوند

۲) هر صنعتی ترسیمه تردد شبکه SPN می باشد با این کلید (Master key) دارای خود پاسخ

۳) بیک ۵-bits برای شبکه جا نشین - جایگشت که منع بر بساخت رمز غالبی ۴۶ بتری دارد
می تواند که صادر ماترس ۱۷X۱۷ باشد که عناصر آن همگی با بایت بوره و به معوره از مکاره
آن نفسی هستند است. برای نگاشت یک بایت (۸ست) از طبق ۲۵-bits که بیک
بایت ریز میانی صورت نشاند می شود که:

۱: ۴ بایت برای میانه صادر ماترس و بیک ۲۵-bits

۲: ۴ بایت کم ارزشی بیک و میانه صادر ماترس و بیک ۲۵-bits

۳: صدراحتی عقیق را میانه صادر میانه میانه در رکام های مبکر است.

نگاشت برای

۱	۲	۱۶
a _{1,1}	a _{1,2}	a _{1,16}
۱۶	a _{16,1}	a _{16,16}

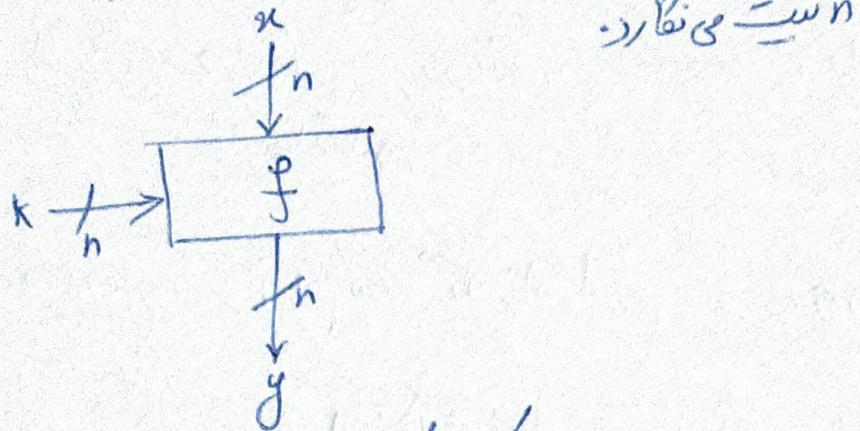
مثال: اگر فرض کنیم کات های میانه فوچ بیاندریک ۲۵-bits باشند $N = 11000000$ می عنوان

در درجه باره، آنگاه طبق ۲۵-bits فوچ باشد صدر از گلاره های لور

شبکه‌ای فاسیلیتی (Feistel Network) ۱۳

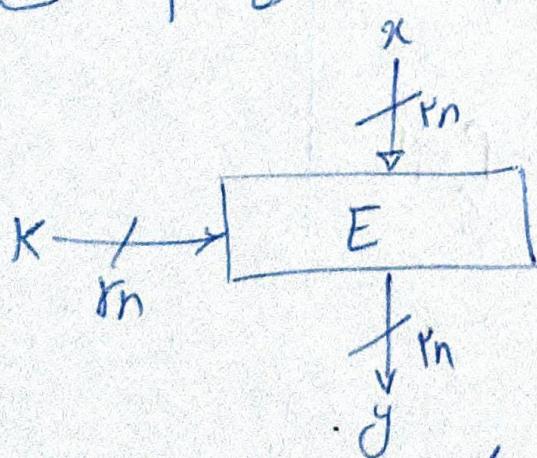
همانطور در بخش های قبلی تشریح شد، شبکه‌ای فاسیلیتی روی برآوردهای ریزهای کالبین با استفاده از ترتیب سُبْر تعدادی هستند.

فرق کنند تابع سُبْر تعدادی (f) را در اختیار داریم که نسبت را به عنوان زیر می‌نماییم:



شکل - یک تابع سُبْر تعدادی با درود و خروجی نسبت

در این بخش، در واقعی خواهیم با استفاده از شبکه‌ای فاسیلیتی، روش کالبین را طریق کنیم که آندر کل زیر، نسبت ورودی را به 2^n نسبت خروجی با استفاده از نیم کل زیر نسبت 2^n بنا آندر قدر بعنوان ابتدا در ادامه تشریح می‌کنیم) نگاهست بی‌کند.



شکل - یک روش کالبین (جا به جای سُبْر تعدادی) با درود و خروجی نسبت

شرح شبکه فاسیلیتی: یک روش کالبین با اندازه کالبین 2^n نسبت کرد برآوردهای شبکه‌های فاسیلیتی باشد از نظر ۲ دور با صاخته ریکسان (سکمیل شده است). هر دور در

این هفتار حامل دو عمل است:

عمل جانسینه: توسید تابع دور (Round Function) و این بیم است
راست اعمال سده و مها بیتا برای تفسیر نفع سست حب
صور استعاره هم رفی کند.

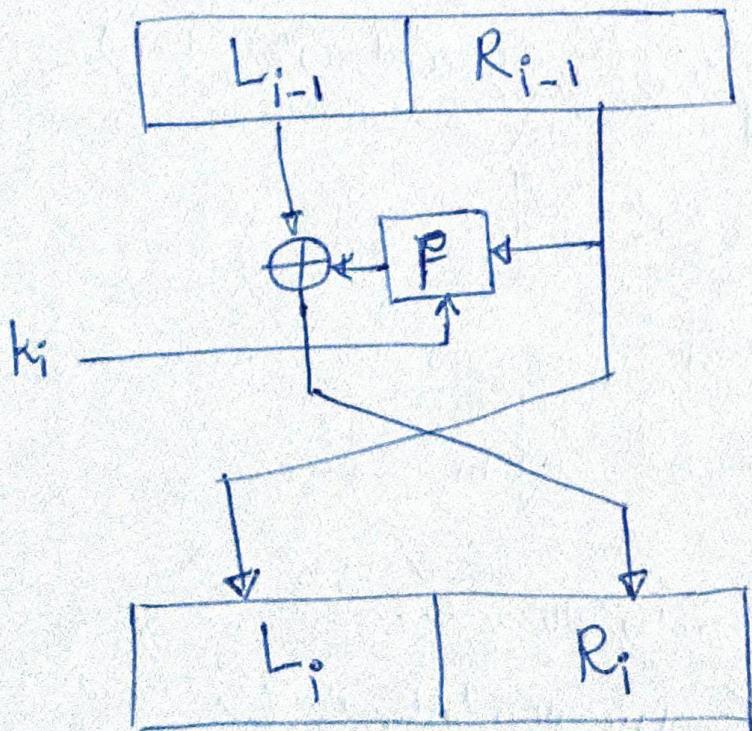
عمل جابجایی: در این قای هر دور نفع های سست حب و راست خود را
چاپجا می کند.

بنابران، بر طور دقیق تر دور آنچه ب شبکه فاسیله بر صورت زیر اجرا
می شود.

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f_{k_i}(R_{i-1})$$

کلیزیم، صورت صدور، عملیات هم دور را به تغیر کلیده است.



کلیزیم از شبکه فاسیله

نکته: لزومی تقدیر تابع دو مرکزی سیکم فاسیلیس جایگزین است با اینکه محدود نشود. نظریه جایگزین است این در واقع معمول است که سیکم فاسیلیس f_{k_i} باشد. اینکه در اینجا مذکور شده بکار رفته است روابط بازگشتی زیر قابل الجامع است:

$$R_{i-1} = L_i$$

$$L_{i-1} = R_i \oplus f_{k_i}(L_i)$$

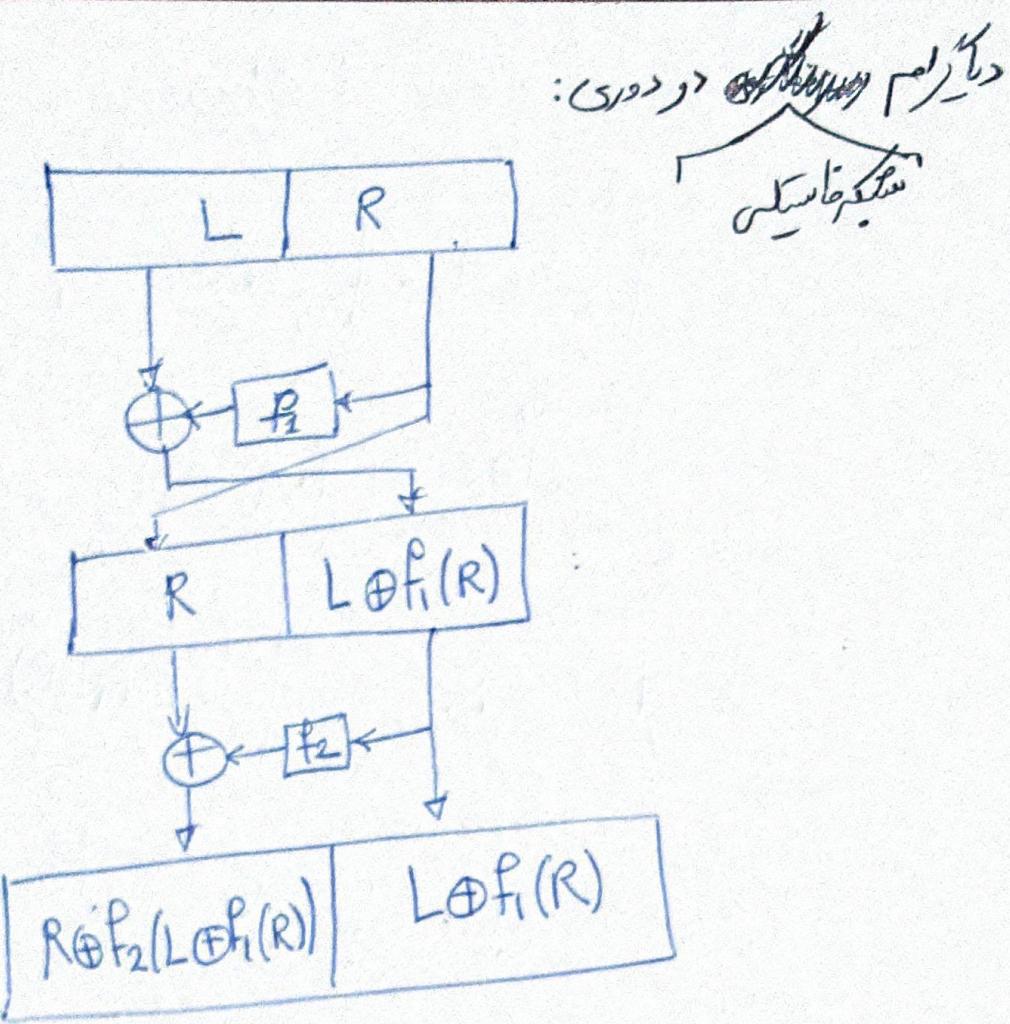
نکته: تقدیر اول جایگزین است اینکه n بیت را به n بیت نگاشت می کند برایبر (n^2) است. در حالیکه با روش بالا n بیت تقدیر دارد به 2^n کاهش می یابد. بنابراین، اگر 2^n کوچک باشد تقدیر جایگزین هارمهکن بسیار کمتر از تقدیر اول جایگزین ها خواهد بود.

نکته: در عمل، کلیدهای دور با استفاده از فرآیند توزیع کلید از کلید اصلی (Master key) استخراج می شوند و این نظریه است. از استخراج از دور به دستور $L_{i-1} = R_i \oplus f_{k_i}(L_i)$ راست است.

نکته: از آنجاییکه جایگزینی در آخر را کنند خنثی کرد و می خواهند برای نظریه استخراج از دور $L_{i-1} = R_i \oplus f_{k_i}(L_i)$ را بسیار ساده کنند. **سؤال:** تقدیر دور ما در بعد فاسیلیس i حدوداً با اینقدر باشد $\frac{1}{2^n}$ با این فرض اینکه f سیکم فاسیلیس باشد، خانواده جایگزینی که ایجاد کردند اینم، سیکم فاسیلیس باشد و

- سیکم فاسیلیس تقدیری، تنها با یک سرگشان از E از فرآیند جایگزین است که این رقابتی قابل تشخیص است.

- سیکم فاسیلیس دو تقدیری، تنها با دو سرگشان از E از فرآیند جایگزین کامل است. رقابتی متأیل سه هنف است.



$$a \parallel b - E(L_1 \parallel R_1) = R_1 \oplus f_2(L_1 \oplus f_1(R_1)) \parallel L_1 \oplus f_1(R_1) \stackrel{?}{=} C_1$$

$$c \parallel d = E(L_2 \parallel R_2) = R_2 \oplus f_2(L_2 \oplus f_1(R_2)) \parallel L_2 \oplus f_1(R_2) \stackrel{?}{=} C_2$$

Adversary's strategy = If $b \oplus d = L_1 \oplus L_2$ then
return "E is not a PRP"

else return "E is a PRP"

(15)

حقنی Luby-Rackoff : قرن لند تابع دور سکبیر فاسل، سُبْر تقادی باشد در

این صورت:

- سکبیر فاسل سه دوری با دسترسی ارالان به جایلست، قابل تمايز از یک جایلست سُبْر تقادی دست است.

- سُبْر فاسل چهار دوری، یک جایلست سُبْر تقادی قوی (strong Pseudorandom Permutation) است، بین حقنی آن و دسترسی ارالان به جایلست اضافه علاوه بر دسترسی ارالان به جایلست به داروں آن نیز دسترسی داشت باشد، جایلست ساخته دنده همچنان سُبْر تقادی است.

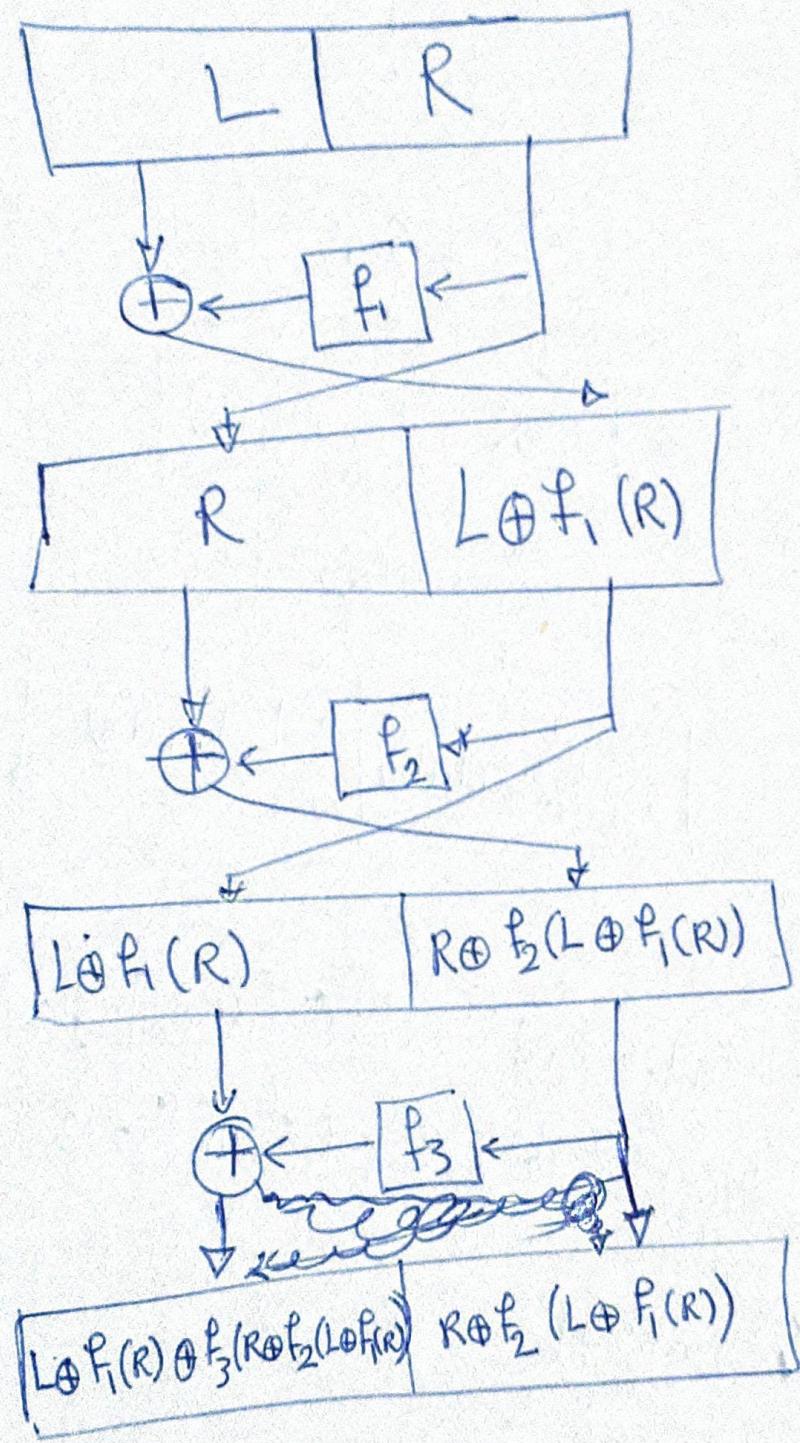
(16)

ابتات حقنی بلا بران اسل اسوار است که تمايز بار هر کاری نیاز به پراکنده تقادم بین حقنی های صیاری (خوبی راندهای مختلف) دارد. در این راستا شان می هنگام حسین اعکان (وجود تقادم) نادر بوده و تقریباً $\frac{1}{n!}$ سرکان ارائه به جایلست بار حصول حقنی حسین هدفی نیاز است.

(17)

نکته: سکبیر فاسل سه دوری با دسترسی ارالان به جایلست و داروں آن، قابل تمايز از یک جایلست سُبْر تقادی است.

برای این شبکه ماتریس دوری برای ساخت E

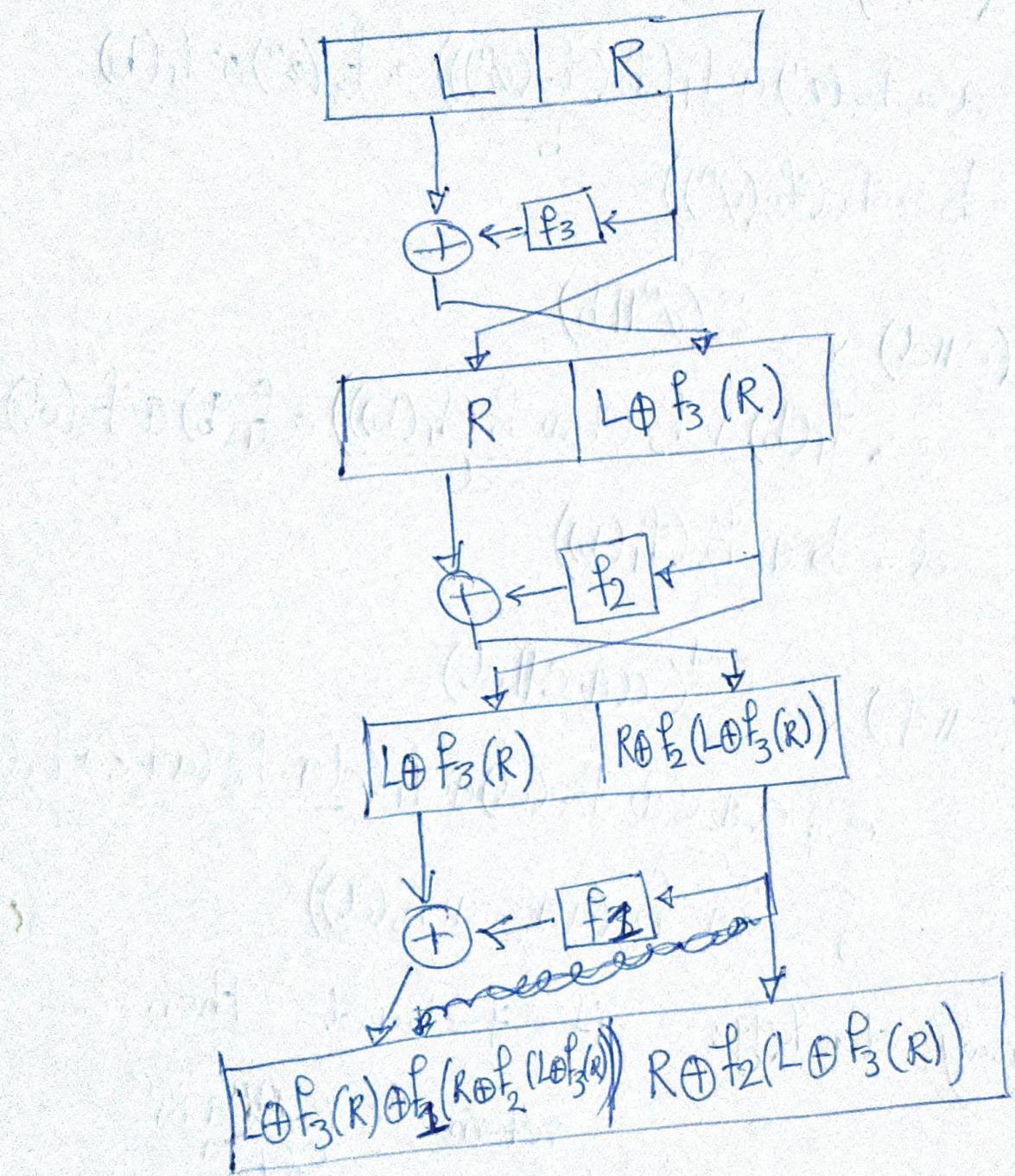


$$E(L \parallel R) = A \parallel B$$

$$A = L \oplus f_1(R) \oplus f_3(R \oplus f_2(L \oplus f_1(R)))$$

$$B = R \oplus f_2(L \oplus f_1(R))$$

دیگر ام سایر فاسیلیتی‌های دوری بطری ساخت



$$E^{-1}(L \parallel R) = A \parallel B$$

$$A = L \oplus f_3(R) \oplus f_1(R \oplus f_2(L \oplus f_3(R)))$$

$$B = R \oplus f_2(L \oplus f_3(R))$$

$$Q_1 \cdot (a || b) \leftarrow E^{-1}(\emptyset^n || \emptyset^r)$$

استجابة لـ E

$$a = f_3(\emptyset^r) \oplus f_1\left(\frac{f_2(f_3(\emptyset^r))}{b}\right) = f_3(\emptyset^r) \oplus f_1(b)$$

$$b = f_2(f_3(\emptyset^r))$$

$$Q_2 \cdot (c || d) \leftarrow E(\emptyset^n || b)$$

$$c = f_1(b) \oplus f_3\left(\frac{b \oplus f_2(f_1(b))}{d}\right) = f_1(b) \oplus f_3(d)$$

$$d = b \oplus f_2(f_1(b))$$

$$Q_3 \cdot (e || f) \leftarrow E^{-1}(a \oplus c || d)$$

$$e = a \oplus c \oplus f_3(d) \oplus f_1\left(\frac{d \oplus f_2(a \oplus c \oplus f_3(d))}{f}\right)$$

$$f = d \oplus f_2(a \oplus c \oplus f_3(d))$$

Adversary strategy: if $f = b \oplus d$ then

return " E is a PRP"

else

return " E is not a PRP"

$$a + c = f_3(\emptyset^r) \oplus f_3(d)$$

لـ E بـ b بـ d , f

$$f = d \oplus f_2(f_3(\emptyset^r) \oplus f_3(d) \oplus f_3(d)) = d \oplus f_2(f_3(\emptyset^r)) = d \oplus b$$