

یک الگوریتم جدید رمزنگار سریع داده‌ها (FDE)

محمد رضا عارف* - فرامرز هندسی** - مسعود عمومی***

چکیده:

اگر چه الگوریتم رمزنگار قالبی DES طی سالهای اخیر در زمره قویترین رمزنگارهای موجود دنیا محسوب می شده است، اما نقاط ضعف عمده آن نیز مورد توجه بوده و پیشنهاداتی برای رفع کردن آنها مطرح شده است. دو عیب مهم الگوریتم DES که روزه‌های امیدی را برای شکستن آن گشوده اند، عبارتند از: سادگی بیش از اندازه ساختار تولید کلیدهای فرعی که باعث سهولت و سرعت در جستجوی فضای کلید می شود و نیز وجود خواص نامطلوب در جعبه‌های جانشینی (S_i) که بعضاً ویژگیهای آماری خوبی را ارائه نمی دهند و در بجه‌هایی را برای حمله به سیستم و شکستن آن می گشایند.^۱

در این مقاله با الهام از مزایای بارز الگوریتم DES، الگوریتم جدیدی ارائه می شود که در آن در ساختار تولید کلیدهای فرعی تجدید نظر کلی و جدی به عمل آمده است. همچنین در آن، امکان استفاده از کلیدهای با طول متغیر فراهم شده است، به طوری که حمله جستجوی فضای کلید ناموفق می نماید. اشاره‌ای نیز به نحوه انتخاب جعبه‌های S_i قویتر خواهیم کرد و در پایان پیشنهاداتی برای بالا بردن سرعت عمل این رمزنگار مطرح خواهد شد.

۱- الگوریتم جدید FDE و تبدیلات اساسی به کار رفته در آن
الگوریتم FDE [۱] نیز همچون DES سعی در برآورده ساختن معیارهای شانون^۲ در مورد

* دانشیار دانشکده برق و کامپیوتر- دانشگاه صنعتی اصفهان

** فارغ التحصیل کارشناسی ارشد دانشکده برق و کامپیوتر- دانشگاه صنعتی اصفهان

*** مربی دانشکده برق و کامپیوتر- دانشگاه صنعتی اصفهان

۱. فرض بر این است که خواننده محترم با الگوریتم DES آشنایی کامل دارد. مراجع [۲] تا [۴] بدین منظور معرفی می شوند.

یک رمزنگار خوب یعنی انتشار^۱ و در هم پیچیدگی^۲ دارد و با به کارگیری متوالی تبدیلات جانشینی^۳ و جایگشت^۴ این مهم را انجام می دهد [۵]. قبل از معرفی تبدیلات اساسی مورد استفاده در الگوریتم FDE لازم است اندازه و ماهیت هریک از متغیرها مشخص شود. یک قالب ۶۴ بیتی متن اصلی یا متن رمز شده توسط دوزیر قالب ۳۲ بیتی به نام های R (زیر قالب سمت راستی یا بیت های با وزن کمتر) و L (زیر قالب سمت چپی یا بیت های با وزن بیشتر) نمایش داده می شود. قالب های X_i معرّف کلید های فرعی ۳۲ بیتی و قالب های Z_i معرّف کلید های فرعی ۱۶ بیتی هستند. تبدیلات اساسی در الگوریتم FDE به صورت زیر تعریف می شوند:

$$G_{X_{i+2}, X_{i+1}, X_i}(L, R) \triangleq (L \oplus R \oplus X_i \oplus X_{i+1}, R \oplus X_i \oplus X_{i+2}) \quad (1)$$

$$F_{Z_{i+1}, Z_i}(L, R) \triangleq (S_{Z_{i+1}}^{-1}(P^{-1}(L)), P(S_{Z_i}(R))) \quad (2)$$

که در آن P^{-1}, P تبدیلات جایگشت معکوس هم و S, S^{-1} تبدیلات جانشینی معکوس هم، تحت کنترل کلید های فرعی Z_{i+1}, Z_i هستند. ساختار دقیق این تبدیلات در بخش (۴) معرفی خواهد شد.

$$G'_{X_{i+2}, X_{i+1}, X_i}(L, R) \triangleq (L \oplus X_i \oplus X_{i+2}, R \oplus L \oplus X_i \oplus X_{i+1}) \quad (3)$$

$$T(L, R) \triangleq (R, L) \quad (4)$$

$$h_1(LR) \triangleq (L, R) \quad (5)$$

که بیان کننده تقسیم یک قالب به دو زیر قالب سمت راستی و سمت چپی است. هریک از تبدیلات فوق معکوس پذیرند و بسادگی می توان تحقیق کرد که معکوس هریک از

-
- | | |
|-----------------|----------------|
| 1. Diffusion | 2. Confusion |
| 3. Substitution | 4. Permutation |

به صورت زیر است:

$$G^{-1}_{x_{i+2}, x_{i+1}, x_i} = G_{x_i, x_{i+1}, x_{i+2}} \quad (6)$$

$$F^{-1}_{z_{i+1}, z_i}(L, R) = (P(S_{z_{i+1}}(L)), S_{z_i}^{-1}(P^{-1}(R))) \quad (7)$$

$$G'^{-1}_{x_{i+2}, x_{i+1}, x_i} = G'_{x_i, x_{i+1}, x_{i+2}} \quad (8)$$

$$T^{-1}(L, R) = T(L, R) \quad (9)$$

$$h^{-1}_1(L, R) = LR \quad (10)$$

که بیان‌کننده کنارهم قراردادن دو زیر قالب سمت راستی و سمت چپی است. تبدیلات معرفی شده فوق دارای سه ویژگی مهم و جالب هستند که اهمیت آنها پس از معرفی الگوریتم FDE آشکار خواهد شد. این سه ویژگی عبارتند از:

$$T \cdot G = G' \cdot T \quad (11)$$

$$T \cdot G' = G \cdot T \quad (12)$$

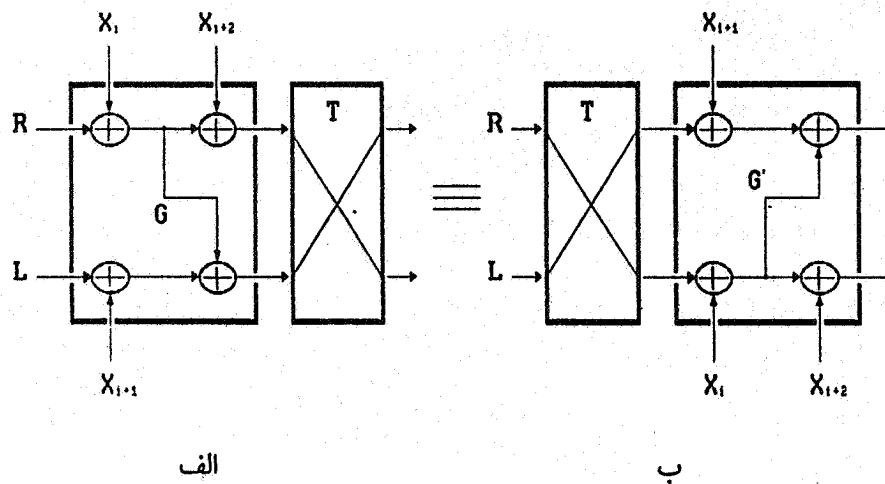
$$T \cdot F^{-1}_{z_{i+1}, z_i} = F_{z_i, z_{i+1}} \cdot T \quad (13)$$

صحت رابطه (۱۱) با توجه به شکل ۱ واضح است. رابطه (۱۲) را می‌توان از روی رابطه (۱۱) و به صورت زیر اثبات کرد:

$$T \cdot G = G' \cdot T \Rightarrow T \cdot T \cdot G \cdot T = T \cdot G' \cdot T \cdot T$$

و از آنجا که $T^{-1} = T$ است خواهیم داشت:

$$G \cdot T = T \cdot G'$$



شکل ۱- نمایش صحت رابطه ۱۱

اثبات رابطه (۱۳) نیز بسادگی و با استفاده از تعاریف اخیر به صورت زیر میسر است:

$$\begin{aligned} T \cdot F_{Z_{i+1}, Z_i}^{-1}(L, R) &= T(P(S_{Z_{i+1}}(L)), S_{Z_i}^{-1}(P^{-1}(R))) \\ &= (S_{Z_i}^{-1}(P^{-1}(R)), P(S_{Z_{i+1}}(L))) \\ &= F_{Z_i, Z_{i+1}}(R, L) \\ &= F_{Z_i, Z_{i+1}}(T(L, R)) \end{aligned}$$

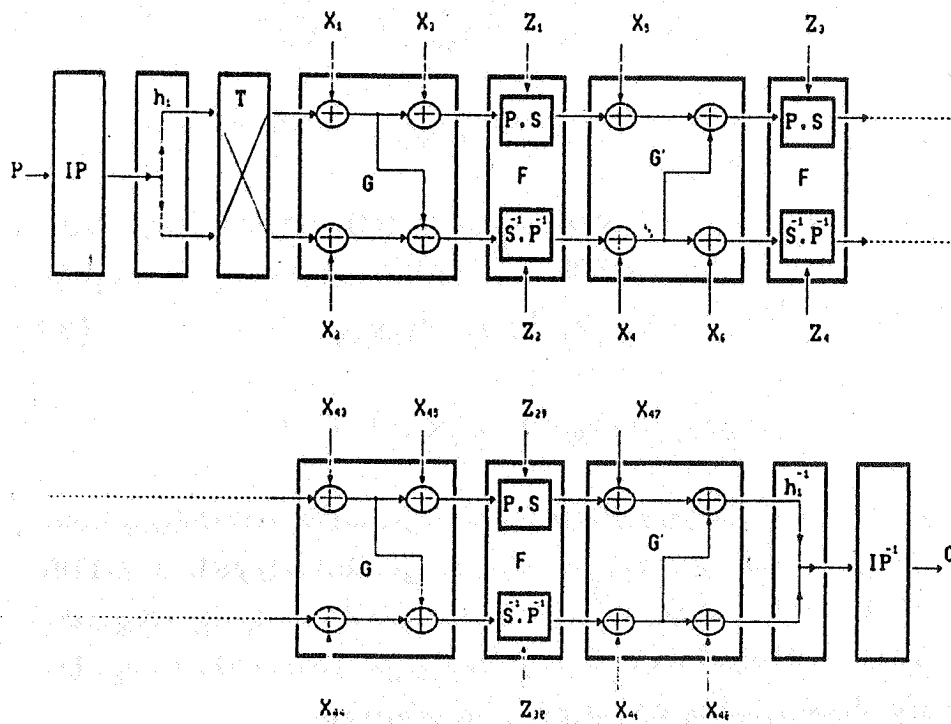
$$\Rightarrow T \cdot F_{Z_{i+1}, Z_i}^{-1} = F_{Z_i, Z_{i+1}} \cdot T$$

پس از آشنائی با تبدیلات اساسی فوق و ویژگیهای آنها، تبدیل رمزگذاری FDE را به صورت زیر تعریف می‌کنیم:

$$FDE \triangleq IP^{-1} \cdot h_1^{-1} \cdot G'_{X_{48}, X_{47}, X_{40}} \cdot F_{Z_{30}, Z_{29}} \cdot G_{X_{45}, X_{44}, X_{43}} \dots$$

$$G'_{X_6, X_5, X_4} \cdot F_{Z_2, Z_1} \cdot G_{X_3, X_2, X_1} \cdot T \cdot h_1 \cdot IP \quad (14)$$

به ترتیب جایگشت‌های اولیه و نهایی بوده و معکوس یکدیگرند. ساختار تبدیل رمزگذاری FDE در شکل ۲ نمایش داده شده است.



شکل ۲ - ساختار رمزگذاری FDE

از ویژگیهای مهم و قابل توجه الگوریتم FDE آن است که فرآیندهای رمزگذاری و رمزگشایی هر دو تحت یک ساختار واحد صورت می‌گیرند و نیازی به ساختار اضافی نیست (ایده اصلی چنین خاصیتی از الگوریتم DES گرفته شده است). صحت این ادعا با توجه به روابط زیر روشن می‌شود:

$$\begin{aligned} FDE^{-1} &= IP^{-1} \cdot h_1^{-1} \cdot T \cdot G_{X_3, X_2, X_1}^{-1} \cdot F_{Z_2, Z_1}^{-1} \cdot G_{X_6, X_5, X_4}^{-1} \\ &\quad G_{X_{45}, X_{44}, X_{43}}^{-1} \cdot F_{Z_{30}, Z_{29}}^{-1} \cdot G_{X_{48}, X_{47}, X_{46}}^{-1} \cdot h_1 \cdot IP \\ &= IP^{-1} \cdot h_1^{-1} \cdot T \cdot G_{X_1, X_2, X_3} \cdot F_{Z_2, Z_1}^{-1} \cdot G_{X_4, X_5, X_6} \\ &\quad G_{X_{43}, X_{44}, X_{45}} \cdot F_{Z_{30}, Z_{29}} \cdot G_{X_{46}, X_{47}, X_{48}} \cdot h_1 \cdot IP \end{aligned}$$

با اعمال روابط (۱۱) و (۱۲) و (۱۳) به ترتیب و به دفعات مکرر می‌توان اثر تبدیل T را به مراحل بعدی منتقل کرد و در نتیجه رابطه نهایی برای FDE^{-1} به صورت زیر به دست می‌آید:

$$FDE^{-1} = IP^{-1} \cdot h_1^{-1} \cdot G_{X_1, X_2, X_3} \cdot F_{Z_1, Z_2} \cdot G_{X_4, X_5, X_6} \quad (15)$$

$$G_{X_{43}, X_{44}, X_{45}} \cdot F_{Z_{29}, Z_{30}} \cdot G_{X_{46}, X_{47}, X_{48}} \cdot T \cdot h_1 \cdot IP$$

مقایسه بین روابط (۱۴) و (۱۵) نشان می‌دهد که برای رمزگذاری و رمزگشایی به وسیله الگوریتم FDE، از یک ساختار واحد استفاده می‌شود و فقط کافی است ترتیب کلیدهای فرعی X_1 ، X_2 ، X_3 ، X_4 ، X_5 ، X_6 ، Z_1 ، Z_2 ، Z_3 ، Z_4 ، Z_5 ، Z_6 ، Z_7 ، Z_8 ، Z_9 ، Z_{10} ، Z_{11} ، Z_{12} ، Z_{13} ، Z_{14} ، Z_{15} ، Z_{16} ، Z_{17} ، Z_{18} ، Z_{19} ، Z_{20} ، Z_{21} ، Z_{22} ، Z_{23} ، Z_{24} ، Z_{25} ، Z_{26} ، Z_{27} ، Z_{28} ، Z_{29} ، Z_{30} عکس شود. اگر هر یک از تبدیلات ضربی $G \cdot F$ ، $G' \cdot F$ و $IP \cdot T \cdot h_1$ را یک دور عمل رمزگذاری در نظر بگیریم، رمزگذار FDE، ۱۶ دور عمل رمزگذاری را در بر می‌گیرد. وجود دورهای متوالی حاوی تبدیلات جانشینی و جایگشت در الگوریتم FDE امکان برآورده ساختن معیارهای شانون یعنی انتشار و درهم پیچیدگی را فراهم می‌کند.

۲- فرایند تولید کلیدهای فرعی

در دورهای متوالی الگوریتم FDE، مجموعاً ۷۸ کلید فرعی بکارگرفته می‌شوند که شامل ۴۸ کلید ۳۲ بیتی یعنی X_i ها و ۳۰ کلید ۱۶ بیتی یعنی Z_i ها می‌شود. این کلیدها از روی یک کلید اصلی و با روند مشخصی تولید و سپس بکارگرفته می‌شوند. یکی از بخش‌های مهم و اساسی در الگوریتم FDE، ساختار تولید کلیدهای فرعی آن است که در طراحی آن نقطه ضعف بارز الگوریتم DES، یعنی سهولت و سادگی فرایند تولید کلیدهای فرعی مورد نظر بوده و سعی شده است که این اشکال مهم برطرف گردد. همان‌گونه که می‌دانیم در رمزگذار DES، ۱۶ کلید فرعی ۴۸ بیتی از روی یک کلید اصلی ۶۴ بیتی (شامل ۸ بیت توازن) تولید می‌شوند. هر کلید فرعی پس از انجام چند مرحله انتخاب بیت، انتقال بیت و جایگشت ساده تولید می‌شود به طوری که در نهایت ۴۸ بیت هر یک از کلیدهای فرعی ماهیتاً ۴۸ بیت از کلید اصلی هستند که ترتیب آنها برهم خورده است. بنابراین در عمل می‌توان با چند سیم‌بندی ساده، همه کلیدهای فرعی را از روی کلید اصلی و در زمان بسیار کوتاهی تولید کرد. نقطه ضعف و خطر ساز DES از همین جا ناشی می‌شود، چراکه در حمله جستجوی فضای کلید، دشمن از نظر زمانی هیچ مشکلی برای تولید کلیدهای فرعی ندارد و در حقیقت با انتخاب یک کلید اصلی تصادفی، کلیدهای فرعی مربوط به کلید آماده استفاده هستند و این سبب می‌شود که زمان جستجوی فضای کلید به اندازه کافی و قابل اطمینان بزرگ نباشد و با پیشرفت تکنولوژی روزبه روز خطر شکسته شدن DES فزونی یابد.

این نقیصه در طراحی ساختار FDE به خوبی مورد توجه قرار گرفته و سعی شده است که فرایند تولید کلیدهای فرعی بسیار پیچیده‌تر و زمان تولید آنها بسیار بیشتر از DES باشد. این پیچیدگی و زمان بیشتر برای فرستنده‌ها و گیرنده‌های مجاز قابل تحمل است چراکه فقط یک بار کلیدهای فرعی را تولید و ذخیره کرده و تا وقتی که کلید اصلی ثابت است از آنها استفاده می‌کنند. اما بدلیل آنکه دشمن در حمله نوع سوم [۶] سعی دارد رمزکننده را از طریق جستجوی فضای کلید بشکند، ناگزیر است که با هر بار تغییر کلید اصلی زمان زیادی را برای تولید کلیدهای فرعی صرف کند و این باعث چندین برابر شدن زمان جستجو و در نهایت عقیم ماندن این حمله می‌شود. پس از ذکر این مقدمه لازم، به تشریح فرایند تولید کلید در ساختار FDE می‌پردازیم.

X_i ها و Z_i ها را در بردارهایی که به صورت زیر تعریف می‌شوند، دسته‌بندی می‌کنیم:

$$\begin{aligned}
 U_{2i+1} &\triangleq (X_{3i+1}, X_{3i+2}) & i = 0, 1, \dots, 7 \\
 U_{2i+2} &\triangleq (X_{3i+3}, Z_{2i+1}, Z_{2i+2}) & i = 0, 1, \dots, 6 \\
 U_{30-2i} &\triangleq (X_{48-3i}, X_{47-3i}) & i = 0, 1, \dots, 7 \\
 U_{29-2i} &\triangleq (X_{46-3i}, Z_{30-2i}, Z_{29-2i}) & i = 0, 1, \dots, 6 \\
 V &\triangleq (X_{24}, Z_{15}, Z_{16}, X_{25}) \\
 V' &\triangleq (X_{25}, Z_{16}, Z_{15}, X_{24})
 \end{aligned} \tag{۱۶}$$

روشن است که U_1 ها قالبهای ۶۴ بیتی و V و V' قالبهای ۹۶ بیتی هستند. اگر به ترتیب استفاده از کلیدهای فرعی در شکل ۲ دقت شود مشاهده می‌گردد که در حالت رمزگذاری به ترتیب از دور اول تا دور آخر بردارهای $U_1, U_2, \dots, U_{15}, V, U_{16}, U_{17}, \dots, U_{30}$ مورد استفاده قرار می‌گیرند و از آنجا که در حالت رمزگشایی این ترتیب معکوس می‌شود می‌توان روابط زیر را نوشت:

$$C = FDE_{U_1, \dots, U_{15}, V, U_{16}, \dots, U_{30}}(P) \tag{۱۷}$$

$$P = FDE_{U_{30}, \dots, U_{16}, V', U_{15}, \dots, U_1}(C) \tag{۱۸}$$

فرایندی که برای تولید کلیدهای فرعی در نظر گرفته شده، براساس وجود حافظه برای این کلیدها می‌باشد. به طوری که در ابتدای عمل رمزگذاری یا رمزگشایی بوسیله الگوریتم FDE، کلیدهای فرعی تولید شده و در درون حافظه قرار می‌گیرند. حجم حافظه مورد نیاز برای ذخیره‌سازی کلیدهای فرعی مجموعاً ۲۶۴ بایت است. به منظور خودداری از بکارگیری مدارات اضافی برای تولید کلیدهای فرعی از خود ساختار FDE برای تولید آنها استفاده می‌شود. اگر قالب ۱۲۸ بیتی U را به عنوان کلید اصلی و زیر قالبهای ۶۴ بیتی سمت راستی و سمت چپی آن را به ترتیب X و Y در نظر بگیریم، روند تولید کلیدهای فرعی به صورت زیر خواهد بود.

$$V = Ch(U) \quad (19) \quad (Ch \text{ یک تبدیل انتخاب } 96 \text{ بیت از } 128 \text{ بیت است})$$

$$U_1 = FDE_{Y,Y,\dots,Y,V,Y,Y,\dots,Y}(X)$$

$$U_2 = FDE_{U_1,Y,\dots,Y,V,Y,Y,\dots,Y}(X)$$

$$U_3 = FDE_{U_1,U_2,\dots,Y,V,Y,Y,\dots,Y}(X)$$

(۲۰)

$$U_{30} = FDE_{U_1,U_2,\dots,U_{15},V,U_{16},U_{17},\dots,U_{29},Y}(X)$$

روابط فوق نشان می دهند که برای تولید کلیدهای فرعی نیاز به ۳۰ بار عمل رمزنگاری توسط FDE است و این همان نکته‌ای است که برای ناکام گذاشتن دشمن در حمله جستجوی فضای کلید در طراح سیستم مد نظر بوده است.

شکل ۳ یک ساختار عملی برای تولید کلیدهای فرعی را نمایش می دهد. در این شکل خروجیهای کد بردار به کنترل ورودی ثبات‌های کلید فرعی متصل می باشند و دنباله‌های جدول ۱ را تولید می کنند. همچنین خط ضخیم بیانگر مسیر عمومی اطلاعات ۴۶ بیتی است که کلیدهای فرعی را منتقل می کند. در این شکل هنگامی که کلید ON یک می گردد دنباله‌های جدول ۱ به ترتیب تولید می شوند و لذا کافی است زمان بین تولید دو دنباله برابر و یا بزرگتر از زمان عمل FDE باشد تا U_i ها به ترتیب تولید شده و در محل خود قرار گیرند. در دنباله حالت سی و دوم جدول ۱ بیت سی و یکم صفر شده و باعث قطع شدن ساعت شمارنده و توقف تولید دنباله‌های جدول می شود. علاوه بر آن مولتی پلکس ورودی رمزنگار تغییر وضعیت داده و رمزنگار برای پذیرش متن اصلی آماده می گردد. در شکل ۳ بیت M تعیین کننده نوع عمل FDE است. اگر $M=1$ باشد عمل رمزگذاری و اگر $M=0$ باشد عمل رمزگشایی صورت می گیرد.

یکی دیگر از قابلیت‌های مهم الگوریتم FDE، امکان استفاده از کلیدهای با طول متغیر است. کلیدی که از طریق کانال امن بین فرستنده و گیرنده مبادله می شود، می تواند طول متغیری بین ۶ تا ۱۵ حرف داشته باشد. همچنین یک حرف برای نشان دادن طول کلید در کنار آنها قرار می گیرد و لذا طول کلید دریافتی بین ۷ تا ۱۶ حرف است. پس از بررسی توازن و معلوم شدن

طول کلید، کلید اصلی ۱۲۸ بیتی U از طریق اعمال یک تبدیل جایگشت بر روی کلید دریافتی به صورتی که صفرهای انتهای ثبات محتوای کلید (درحالی که طول کلید کمتر از ۱۵ حرف است)

جدول ۱ - دنباله‌های خروجی کد بردار

شماره بیت	S ₁	S ₂	S ₃	-----	S ₃₀	S ₃₁	S ₃₂
0	1	1	0	-----	0	0	0
1	1	0	1	-----	0	0	0
2	1	0	0	-----	0	0	0
.	.	.	.	-----	.	.	.
.	.	.	.	-----	.	.	.
.	.	.	.	-----	.	.	.
28	1	0	0	-----	1	0	0
29	1	0	0	-----	0	1	0
30	0	1	1	-----	1	1	1
31	1	1	1	-----	1	1	0

در کنار هم قرار نگیرند، به دست آمده و در ثبات محتوای U ذخیره می‌شود. در این ساختار، بیت‌های توازن و همچنین بیت‌های حرف اول (نشانگر طول کلید) که هیچیک از بقیه بیت‌های کلید مستقل نیستند در تولید کلیدهای فرعی به کار می‌روند. انتخاب کلید با طول متغیر برای الگوریتم FDE سبب متغیر شدن بعد فضای کلید در یکی از ابعاد 2^{22} ، 2^{29} ، 2^{56} ، ... و 2^{105} می‌شود (برای هر حرف کلید غیر از بیت توازن، ۷ بیت در نظر گرفته می‌شود). برای مقایسه بعد فضای کلید و زمان جستجوی آن در الگوریتم‌های DES و FDE، ابتدا فرض می‌کنیم که کلید FDE نیز ۸ حرفی یعنی برابر با طول کلید DES انتخاب شود. اگر زمان عمل هر دو الگوریتم را نیز یکسان فرض کنیم، از آنجایی که ساختار تولید کلیدهای فرعی در FDE نیازمند ۳۰ بار عمل رمزنگاری توسط آن است، زمان جستجوی فضای کلید FDE حداقل ۳۰ برابر این زمان در DES می‌شود. اگر از حداکثر بعد فضای کلید در FDE استفاده شود، نسبت زمان جستجو در FDE به زمان جستجو در DES تقریباً $10^{16} \times 1/6 \approx \frac{2^{105}}{51}$ می‌شود که عدد بسیار بزرگی است. از مزایای عمده استفاده از کلید با طول متغیر آن است که

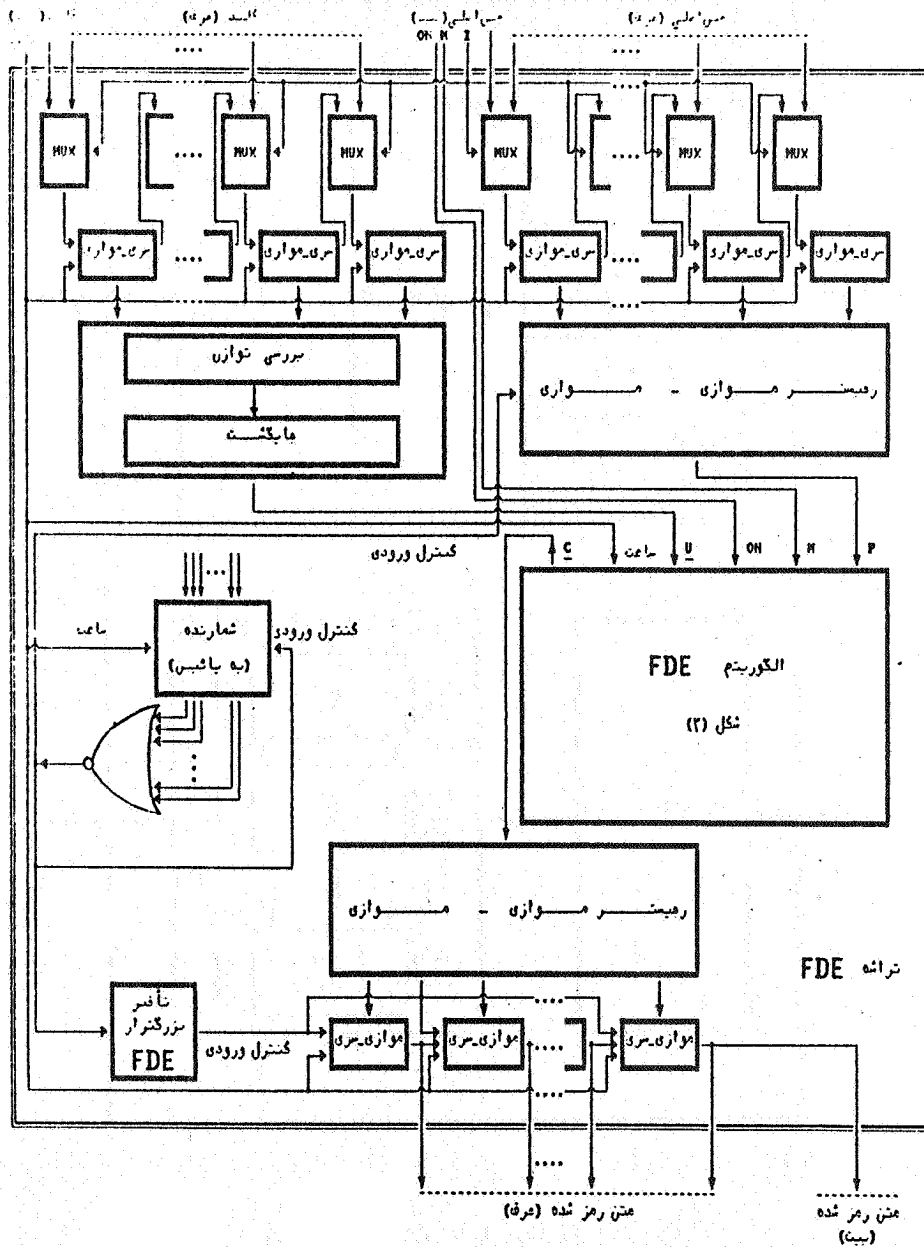
اولاً بسته به اهمیت کار می توان بعد فضای کلید را بزرگتر یا کوچکتر انتخاب نمود و ثانیاً دشمن بعد فضای کلید را نمی داند و انتخاب تصادفی بعدها می مختلف و جستجوی فضای کلید زمان بسیار زیادی را از او می طلبد و عملاً او را از شکستن سیستم مأیوس می سازد.

۳- ایده خط لوله^۱ در تراشه FDE [۱]

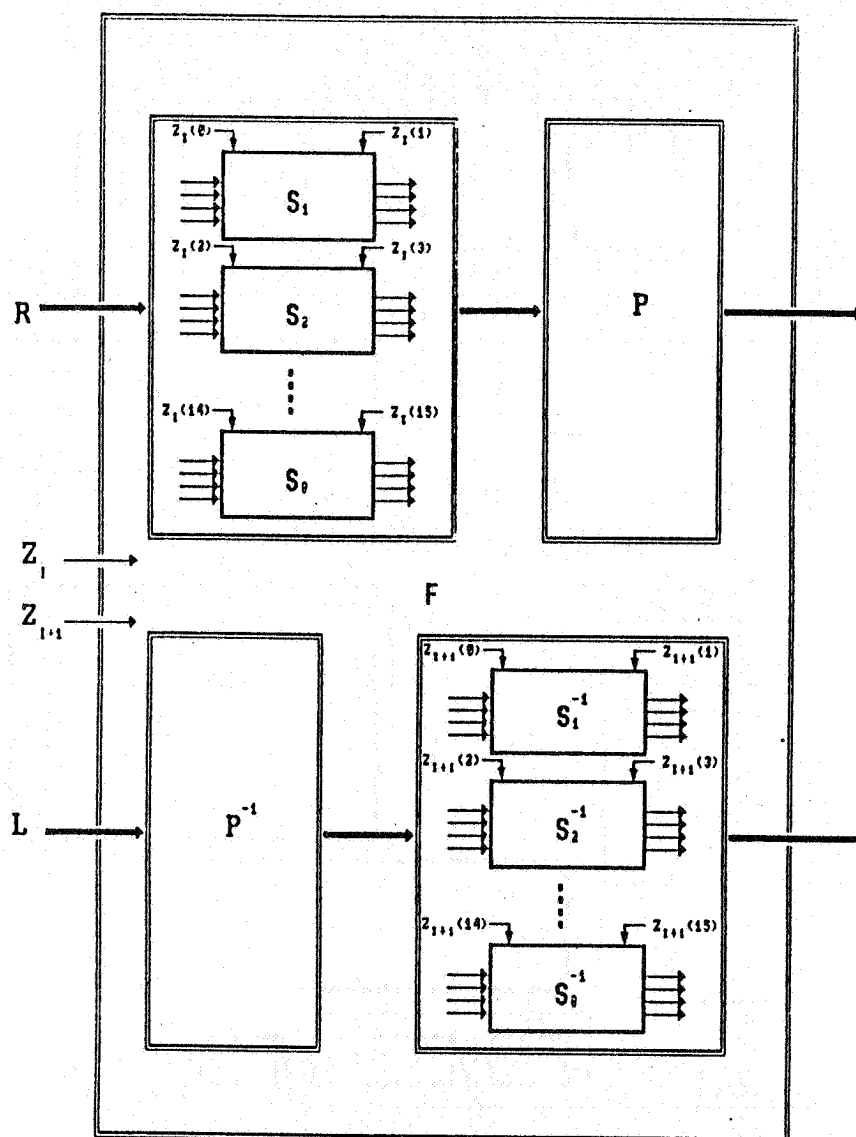
با توجه به آنکه ساختار معرفی شده برای رمزنگار FDE سری می باشد، به راحتی می توان از ایده خط لوله در عمل رمزنگاری حداکثر استفاده را نمود. شکل ۴ تراشه طراحی شده برای FDE را که براساس ایده خط لوله عمل می کند نشان می دهد. در این شکل متن اصلی به هر دو صورت حرف و یا بیت وارد می گردد و متن رمز شده نیز به همان دو صورت خارج می شود. در این تراشه وقتی از حرف استفاده می شود بایستی شمارنده در مبنای ۸ و $I=1$ قرار داده شوند. در این صورت بعد از هشت انتقال، یک پالس ساعت از شمارنده ارسال می گردد که باعث می شود ثبات موازی - موازی ورودی بارگردیده و همچنین ثبات موازی - سری خروجی نیز بارشود. اگر انتقال داده ها به صورت بیت به بیت مورد نظر باشد بایستی مبنای شمارنده ۶۴ و $I=0$ قرار داده شود. از آنجایی که از ایده خط لوله در ساختار فوق استفاده شده است، FDE با سرعت بسیار بالا (زمان عمل ثبات انتقالی^۱) عمل می کند و از این لحاظ بسیار شبیه به رمزنگار پی در پی است و از مزایای عمده این نوع رمزنگارها نیز می تواند بهره مند باشد. به علاوه از آنجا که FDE یک رمزنگار قالبی است، کلیه مزایای رمزنگارهای قالبی را نیز داراست. بعنوان مثال FDE نیز همانند DES می تواند بسته به نوع کاربرد در یکی از چهارمود عمل ECB، CBC، CFB و OFB [۷] به کار رود.

۴- معیارهای انتخاب ساختار تبدیل F

در بخش ۱ تبدیل F را به اجمال معرفی کردیم و دیدیم که این تبدیل متشکل از دو لایه ترکیبی جایگشت و جانشینی معکوس هم یعنی P.S و $S^{-1}.P^{-1}$ است که بر روی دو زیر قالب ورودی R و L به طور جداگانه عمل می کنند. ساختار کامل تبدیل F در شکل ۵ نشان داده شده است. جایگشت های P و P^{-1} دو جایگشت اختیاری و معکوس هم هستند (به عنوان نمونه همان جایگشت P در الگوریتم DES) که روی یک قالب ۳۲ بیتی عمل می کنند. جعبه های جانشینی S_i و S_i^{-1} ($1 \leq i \leq 8$) دارای ۴



شکل ۴ - تراشه FDE



شکل ۵ - ساختار تبدیل $F_{Z_{t+1}, z_t}(L, R)$

بیت ورودی، ۴ بیت خروجی و ۲ بیت کلید هستند. در هر جعبه ۴ بیت ورودی شماره یک سطر و ۲ بیت کلید شماره یک ستون از یک ماتریس 16×4 را مشخص می‌کنند. در هر ستون از این ماتریس یک جایگشت به ظاهر تصادفی از اعداد ۰ تا ۱۵ وجود دارد و ۴ بیت خروجی جعبه نمایش باینری عددی است که محل آن توسط بیت‌های ورودی و کلید تعیین می‌شود. معکوس هر جعبه جانشینی عبارت است از یک جعبه جانشینی که در هر ستون آن معکوس جایگشت واقع در همان ستون از جعبه اصلی وجود دارد. این جعبه‌ها غیرخطی انتخاب می‌شوند و سبب هرچه پیچیده‌تر شدن رابطه بین ورودی و خروجی تبدیل F می‌گردند. در اینجا نیز جعبه‌های S_i همانند DES از مهمترین بخشهای ساختار رمزکننده بوده و در انتخاب آنها معیارهای خاصی را بایستی در نظر گرفت. اولین معیار در انتخاب چنین جعبه‌هایی کامل^۱ بودن آنهاست. یک جعبه جانشینی را کامل گوئیم هرگاه هر بیت خروجی به همه بیت‌های ورودی بستگی داشته باشد. بنابراین اگر پیدا کردن ساده‌ترین عبارت بولی برای هر بیت از خروجی امکان پذیر باشد، در صورت کامل بودن جعبه جانشینی، هر کدام از این عبارات شامل تمام بیت‌های ورودی خواهد بود. خاصیت مهم دیگر یک رمزنگار جانشینی مناسب، اثر بهمینی^۲ است. برای آنکه یک تبدیل رمزنگاری دارای اثر بهمینی باشد بطور متوسط $\frac{1}{4}$ بیت‌های خروجی اش، در اثر تغییر یک تک بیت ورودی تغییر نماید. هرگاه هر بیت خروجی با احتمال $\frac{1}{4}$ در اثر تغییر یک تک بیت ورودی تغییر نماید، تبدیل مؤکداً بهمینی است [۸].

اگر تبدیل رمزنگاری را با g نمایش دهیم، طبق تعریف:

$$V_i(X) \triangleq g(X) \oplus g(X_i) \quad (21)$$

را بردار بهمینی گوئیم که در آن X و X_i دو بردار ورودی هستند که فقط در بیت i ام با یکدیگر متفاوتند. هر یک از مؤلفه‌های بردار بهمینی را یک متغیر بهمینی نامیده و به ماتریسی که از میانگین‌های آماری متغیرهای بهمینی بدست می‌آید، ماتریس وابستگی^۳ گویند. عناصر این ماتریس را می‌توان به صورت زیر به دست آورد:

$$d_{ij} = \frac{1}{2^{m-1}} \sum_{\substack{\text{روی} \\ 2^{m-1}}} b_i(V_j(X)) \quad , \quad 1 \leq i, j \leq m \quad (22)$$

حالت X

1. Complete

2. Avalanche Effect

3. Dependence Matrix

که در آن b_i نشانگر بیت i ام و m تعداد بیت‌های بردار ورودی است. اگر $d_{ij} = 1$ باشد، بیت i ام خروجی همواره در اثر تغییر بیت j ام ورودی تغییر می‌کند و اگر $d_{ij} = 0$ باشد بیت i ام خروجی مستقل از بیت j ام ورودی است. برای یک رمزنگار مؤکداً بهمنی همه عناصر ماتریس وابستگی مقدار نزدیک به $0/5$ دارند [۸].

از دیگر ویژگی‌های یک رمزنگار خوب، مستقل بودن متغیرهای بهمنی است. هرگاه یک رمزنگار جانشینی دارای این خاصیت باشد گویند رمزنگار تام^۱ است [۸].
انتخاب جعبه‌های مناسب جانشینی که دارای ویژگی‌های فوق باشند از مسائل قابل توجهی است که در طراحی نهایی الگوریتم FDE بایستی بطور جدی بدان پرداخته شود. تولید تصادفی تعدادی از این جعبه‌ها و بررسی معیارهای فوق بر روی آنها و در نهایت انتخاب جعبه‌های مناسب، یک روش پیشنهادی برای دست‌یابی به جعبه‌های جانشینی خوب است.

نتیجه‌گیری

از آنچه که در مورد الگوریتم FDE گفته شد، نکات زیر حائز اهمیت‌اند:

- ۱- با تجدید نظر کلی که در نحوه تولید کلیدهای فرعی نسبت به الگوریتم DES به عمل آمده است، ساختار تولید کلیدهای فرعی در FDE بسیار پیچیده‌تر شده به طوری که از نظر زمان جستجوی کامل فضای کلید، میزان امنیت این الگوریتم نسبت به DES (با فرض تساوی طول کلیدها) حداقل ۳۰ برابر شده است.
- ۲- از مزایای عمده FDE آن است که هر بیت از کلیدهای فرعی به تمام بیت‌های کلید اصلی بستگی دارد و بنابراین با یک دور عمل رمزنگاری، هر بیت متن رمز شده به تمام بیت‌های کلید وابسته می‌شود.
- ۳- طول کلید در الگوریتم FDE متغیر است.
- ۴- ساختار FDE برای بهره‌گیری از ایده خط لوله مناسب بوده و با توجه به سرعت عمل بالا، تراشه FDE می‌تواند در سیستم‌های مختلف به جای رمزنگارهای پی‌درپی قرارگیرد.
- ۵- تراشه FDE با هر دوداده حرف و یا بیت عمل می‌کند.
- ۶- جعبه‌های S_i و S_i^{-1} به کاررفته در این الگوریتم می‌توانند تام و با ماتریس وابستگی مناسب

اختیار شوند.

در خاتمه ضمن تأکید مجدد بر این نکته که انتخاب و به کارگیری جعبه‌های جانشینی با خواص مناسب در ساختار FDE سبب می‌شود که این ساختار علاوه بر پیچیده‌تر نمودن حمله جستجوی فضای کلید، از ویژگیهای آماری خوبی (حداقل مشابه با DES) برخوردار باشد، از خوانندگان و محققان دعوت می‌شود تا در ارزیابی و شکستن الگوریتم رمزکننده پیشنهادی، از نظریات کارشناسانه خود ما را بهره‌مند سازند.

مراجع:

۱. فرامرز هندسی، نقد و بررسی رمزنگار DES، پایان نامه دوره کارشناسی ارشد مهندسی مخابرات، دانشگاه صنعتی اصفهان، آبان ۱۳۶۸
2. National Bureau of Standard, "Announcing the Data Encryption Standard", *Federal Register*, Vol.46, 15 Jan., 1977.
3. Denning, D.E., *Cryptography and Data Security*, Addison - Wesley, 1983.
4. Konheim, A. G., *Cryptography: A Primer*, Wiley - Interscience, 1981.
5. Shannon, C. E., "Communication Theory of Secrecy Systems", *Bell Syst. Tech. J.*, Vol.28, PP.656-715, Oct 1949.
۶. محمدرضا عارف، اصول رمزنگاری، قسمت اول، دانشکده برق دانشگاه صنعتی اصفهان، ۱۳۶۷.
7. National Bureau of Standard, "DES Modes of Operation", FIPS Pub. 81, Washington.DC, 2 Dec., 1980.
8. Webster, A. F., Tavers, S. E., "On the Design of S-Boxes", *Advances in Cryptology, Proc. of Crypto, 85*, LNCS, Vol.218, PP.523-534, Springer-Verlag, 1986.