نشریه تحقیقاتی فنی ـ مهندسی استقلال،دانشگاه‌صنعتی‌اصفهان شماره ۱۱ مهرماه ۷۱

یک الگوریتم جدید رمزنگار سریع داده‌ها(FDE)

محمدرضاعارف* - فرامرزهندسی** - مسعودعمومی***

چکیده :

اگر چه الگوریتم رمزنگار قالبی DES طی سالهای اخیر در زمرهٔ قویترین رمزنگارهای موجود دنیا محسوب می‌شده‌است، اما نقاط ضعف عمدهٔ آن نیز مورد توجه بوده و پیشنهاداتی برای رفع‌کردن آنها مطرح شده‌است .دو عیب مهم الگوریتم DES که روزنه‌های امیدی را برای شکستن آن گشوده‌اند ، عبارتنداز: سادگی بیش‌از اندازهٔ ساختار تولید کلیدهای فرعی که باعث سهولت و سرعت در جستجوی فضای کلید می‌شود و نیز وجود خواص نامطلوب در جعبه‌های جانشینی (S_i) که بعضاً ویژگیهای آماری خوبی را ارائه نمی‌دهند و دریچه‌هایی را برای حمله به سیستم و شکستن آن می‌گشایند.[۱]

در این مقاله با الهام از مزایای بارز الگوریتم DES،الگوریتم جدیدی ارائه می‌شود که در آن در ساختار تولید کلیدهای فرعی تجدید نظر کلّی و جدّی به عمل آمده‌است.هـمچنین در آن، امکان استفاده از کلیدهای با طول متغیّر فراهم شده‌است ، به‌طوری‌که حملهٔ جستجوی فضای کلید ناموفق می‌نماید.اشاره‌ای نیز به نحوهٔ انتخاب جعبه‌های S_i قویتر خواهیم کرد و در پایان پیشنهاداتی برای بالابردن سرعت عمل این رمزنگار مطرح خواهدشد.

۱ - الگوریتم جدید FDE[۲] و تبدیلات اساسی به کار رفته در آن

الگوریتم FDE[۱] نیزهمچون DES سعی در برآورده ساختن معیارهای شانون[۳] در مورد

---

* دانشیار دانشکده برق و کامپیوتر- دانشگاه صنعتی اصفهان

** فارغ‌التحصیل کارشناسی ارشد دانشکده برق و کامپیوتر ـ دانشگاه صنعتی‌اصفهان

*** مربی دانشکده برق و کامپیوتر- دانشگاه صنعتی‌اصفهان

۱. فرض براین است که خوانندهٔ محترم با الگوریتم DES آشنایی کامل دارد.مراجع [۲]تا[۴] بدین منظور معرفی می‌شوند.

2. Fast Data Encryption 3. Shannon

یک‌رمزنگار خوب یعنی انتشار[1] و در هم پیچیدگی[2] دارد و با به‌کارگیری متوالی تبدیلات جانشینی[3] و جایگشت[4] این مهم را انجام‌می‌دهد[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 دوزیرقالب ۳۲ بیتی به نام‌های R (زیرقالب سمت راستی یابیت‌های باوزن کمتر) و L (زیرقالب سمت چپی یا بیت‌های با وزن بیشتر) نمایش داده‌می‌شود.قالبهای X_i معرّف کلیدهای فرعی ۳۲ بیتی و قالب‌های Z_i معرّف کلیدهای فرعی ۱۶ بیتی هستند.تبدیلات اساسی در الگوریتم FDE به‌صورت زیر تعریف می‌شوند:

$$G_{X_{i+2},X_{i+1},X_i}(L,R) \triangleq (L \oplus R \oplus X_i \oplus X_{i+1}, R \oplus X_i \oplus X_{i+2}) \qquad (۱)$$

$$F_{Z_{i+1},Z_i}(L,R) \triangleq (S^{-1}_{Z_{i+1}}(P^{-1}(L)), P(S_{Z_i}(R))) \qquad (۲)$$

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

$$G'_{X_{i+2},X_{i+1},X_i}(L,R) \triangleq (L \oplus X_i \oplus X_{i+2}, R \oplus L \oplus X_i \oplus X_{i+1}) \qquad (۳)$$

$$T(L,R) \triangleq (R,L) \qquad (۴)$$

$$h_1(LR) \triangleq (L,R) \qquad (۵)$$

که بیان‌کنندهٔ تقسیم یک قالب به دو زیرقالب سمت راستی و سمت چپی است .

هریک از تبدیلات فوق معکوس پذیرند و بسادگی می‌توان تحقیق کرد که معکوس هریک از

---

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

به‌صورت زیراست :

$$G^{-1}{}_{X_{i+2},X_{i+1},X_i} = G_{X_i}, {}_{X_{i+1}}, {}_{X_{i+2}} \quad (۶)$$

$$F^{-1}{}_{Z_{i+1},Z_i}(L,R) = (P(S_{Z_{i+1}}(L)), S_{Z_i}{}^{-1}(P^{-1}(R))) \quad (۷)$$

$$G'^{-1}{}_{X_{i+2},X_{i+1},X_i} = G'{}_{X_i,X_{i+1},X_{i+2}} \quad (۸)$$

$$T^{-1}(L,R) = T(L,R) \quad (۹)$$

$$h^{-1}{}_1(L,R) = LR \quad (۱۰)$$

که بیان‌کنندهٔ کنارهم قراردادن دو زیر قالب سمت راستی و سمت چپی است .

تبدیلات معّرفی‌شدهٔ فوق دارای سه ویژگی مهم و جالب هستند که اهمیّت آنها پس از معّرفی الگوریتم FDE آشکار خواهدشد.این سه ویژگی عبارتنداز:

$$T \cdot G = G' \cdot T \quad (۱۱)$$

$$T \cdot G' = G \cdot T \quad (۱۲)$$

$$T \cdot F^{-1}{}_{Z_{i+1},Z_i} = F_{Z_i,Z_{i+1}} \cdot T \quad (۱۳)$$

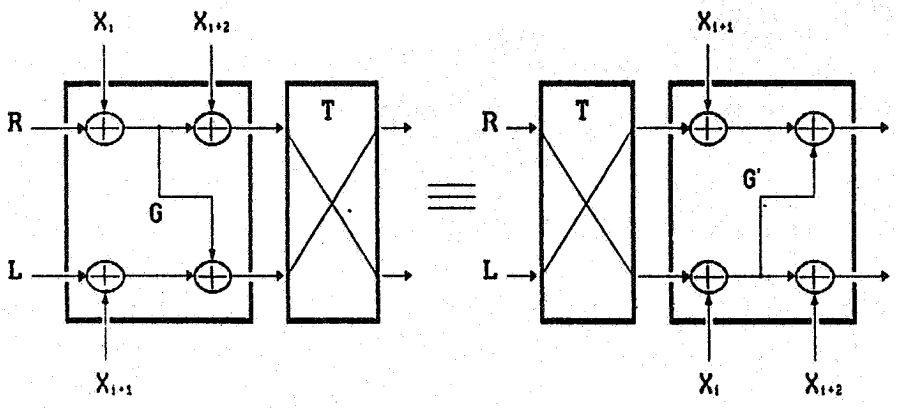
صحّت رابطهٔ (۱۱) با توجّه به شکل ۱ واضح است .

رابطهٔ (۱۲) را می‌توان از روی رابطهٔ (۱۱) و به‌صورت زیر اثبات‌کرد:

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

و از آنجاکه $T = T^{-1}$ است خواهیم‌داشت :

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



الف ب

شکل ۱ ـ نمایش صحّت رابطه ۱۱

اثبات رابطهٔ (۱۳) نیز بسادگی و با استفاده از تعاریف اخیر به‌صورت زیر میّسراست :

$$T \cdot F^{-1}_{Z_{i+1},Z_i}(L,R) = T(P(S_{Z_{i+1}}(L)) , S_{Z_i}^{-1}(P^{-1}(R)))$$

$$= (S_{Z_i}^{-1}(P^{-1}(R)) , P(S_{Z_{i+1}}(L)))$$

$$= F_{Z_i,Z_{i+1}}(R,L)$$

$$= F_{Z_i,Z_{i+1}}(T(L,R))$$

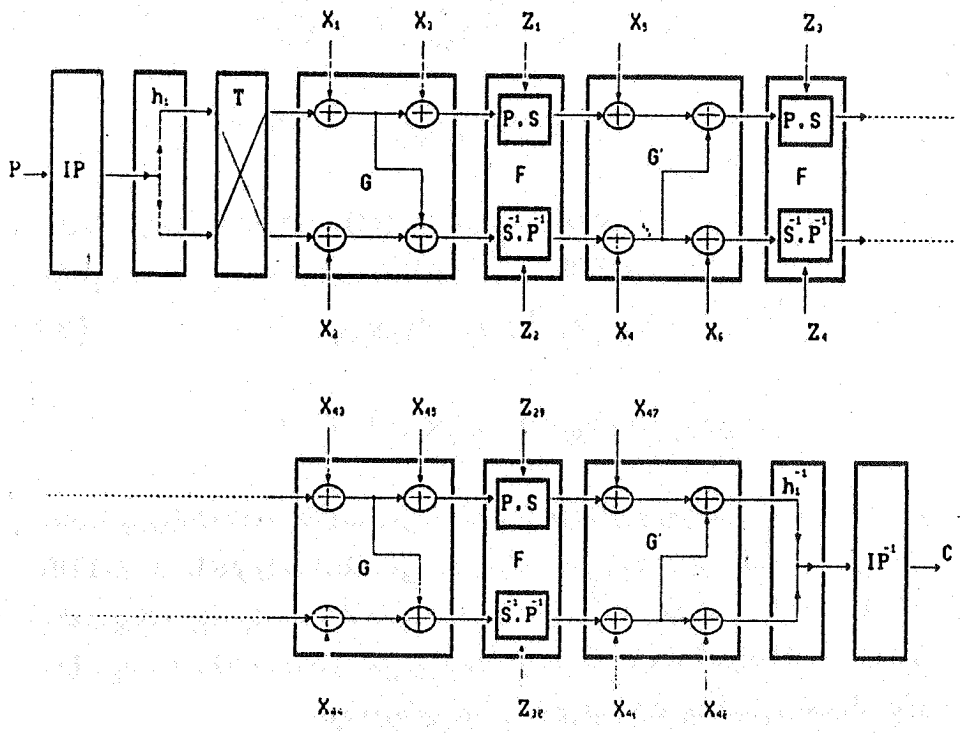
$$\Rightarrow T \cdot F^{-1}_{Z_{i+1},Z_i} = F_{Z_i,Z_{i+1}} \cdot T$$

پس از آشنائی با تبدیلات اساسی فوق و ویژگیهای آنها،تبدیل رمزگذاری FDE را به‌صورت زیر تعریف‌می‌کنیم :

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

$$G'_{X_6,X_5,X_4}.F_{Z_2,Z_1}.G_{X_3,X_2,X_1}.T.h_1.IP \qquad (۱۴)$$

(IP^{-1} , IP) به ترتیب جایگشت‌های اولیه و نهایی‌بوده و معکوس یکدیگرند.
ساختار تبدیل رمزگذاری FDE در شکل ۲ نمایش داده‌شده‌است .



شکل ۲ - ساختار رمزگذاری FDE

از ویژگیهای مهم و قابل توجه الگوریتم FDE آن است که فرآیندهای رمزگذاری و رمزگشایی هردو تحت یک ساختار واحد صورت می‌گیرند و نیازی به ساختار اضافی نیست (ایدهٔ اصلی چنین خاصیتی از الگوریتم DES گرفته‌شده‌است).
صحّت این ادعا با توجه به روابط زیر روشن می‌شود:

$$FDE^{-1} = IP^{-1} \cdot h_1^{-1} \cdot T \cdot G^{-1}_{X_3,X_2,X_1} \cdot F^{-1}_{Z_2,Z_1} \cdot G'^{-1}_{X_6,X_5,X_4} \cdots$$

$$G^{-1}_{X_{45},X_{44},X_{43}} \cdot F^{-1}_{Z_{30},Z_{29}} \cdot G'^{-1}_{X_{48},X_{47},X_{46}} \cdot h_1 \cdot IP$$

$$= IP^{-1} \cdot h_1^{-1} \cdot T \cdot G_{X_1,X_2,X_3} \cdot F^{-1}_{Z_2,Z_1} \cdot G'_{X_4,X_5,X_6} \cdots$$

$$G_{X_{43},X_{44},X_{45}} \cdot F^{-1}_{Z_{30},Z_{29}} \cdot G'_{X_{46},X_{47},X_{48}} \cdot h_1 \cdot IP$$

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

$$FDE^{-1} = IP^{-1} \cdot h_1^{-1} \cdot G'_{X_1,X_2,X_3} \cdot F_{Z_1,Z_2} \cdot G_{X_4,X_5,X_6} \cdots \qquad (۱۵)$$

$$G'_{X_{43},X_{44},X_{45}} \cdot F_{Z_{29},Z_{30}} \cdot G_{X_{46},X_{47},X_{48}} \cdot T \cdot h_1 \cdot IP$$

مقایسهٔ بین روابط (۱۴) و (۱۵) نشان‌می‌دهد که برای رمزگذاری و رمزگشایی به‌وسیلهٔ الگوریتم FDE ، ازیک ساختار واحد استفاده می‌شود و فقط کافی‌است ترتیب کلیدهای‌فرعی X_1 ، X_2،... X_{48} و Z_1 ، Z_2 ،... Z_{30} عکس شود . اگر هریک ازتبدیلات ضربی $G \cdot F$ ، $G' \cdot F$ و $IP \cdot h_1 \cdot T \cdot G$ را یک دور عمل رمزگذاری در نظر بگیریم ، رمزگذارFDE،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 مشخّصی تولید و سپس بکارگرفته می‌شوند.یکی از بخش‌های مهم و اساسی در الگوریتم FDE ، ساختار تولید کلیدهای فرعی آن است که در طرّاحی آن نقطهٔ 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.هرکلید فرعی پس از انجام چند مرحله انتخاب بیت،انتقال بیت و جایگشت ساده تولید می‌شود به‌طوری که در نهایت ۴۸ بیت هریک از کلیدهای فرعی ماهیتاً ۴۸ بیت از کلید اصلی هستند که ترتیب آنها برهم خورده‌است.بنابراین در عمل می‌توان با چند سیم‌بندی ساده ، همهٔ کلیدهای فرعی را از روی کلید اصلی و در زمان بسیار کوتاهی تولیدکرد.نقطهٔ ضعف و خطرساز DES از همین جا ناشی می‌شود،چراکه در حملهٔ 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 بلادرنگ آمادهٔ استفاده هستند و این سبب می‌شود که زمان جستجوی فضای کلید به اندازهٔ کافی و قابل اطمینان بزرگ نباشد و با پیشرفت تکنولوژی روزبه روز خطر شکسته‌شدن DES فزونی‌یابد.

این نقیصه در طراحی ساختار FDE به خوبی مورد توجّه قرارگرفته و سعی شده‌است 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 تحمّل است چراکه فقط یک بار کلیدهای فرعی را تولید و ذخیره‌کرده و تا وقتی که کلید اصلی ثابت است از آنها استفاده می‌کنند.اما بدلیل آنکه دشمن در حملهٔ نوع سوّم [۶] سعی دارد رمزکننده را از طریق جستجوی فضای کلید بشکند ، ناگزیراست که با هر بار تغییر کلید اصلی زمان زیادی را برای تولید کلیدهای فرعی صرف کند و این باعث چندین برابرشدن زمان جستجو و در نهایت عقیم‌ماندن این حمله می‌شود.پس از ذکر این مقدمهٔ لازم، به تشریح فرایند تولید کلید در ساختار FDE می‌پردازیم .

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

$$U_{2i+1} \triangleq (X_{3i+1}, X_{3i+2}) \qquad i = 0,1, \ldots ,7$$

$$U_{2i+2} \triangleq (X_{3i+3}, Z_{2i+1}, Z_{2i+2}) \qquad i = 0,1, \ldots ,6$$

$$U_{30-2i} \triangleq (X_{48-3i}, X_{47-3i}) \qquad i = 0,1, \ldots ,7 \qquad (۱۶)$$

$$U_{29-2i} \triangleq (X_{46-3i}, Z_{30-2i}, Z_{29-2i}) \qquad i = 0,1, \ldots ,6$$

$$V \triangleq (X_{24}, Z_{15}, Z_{16}, X_{25})$$

$$V' \triangleq (X_{25}, Z_{16}, Z_{15}, X_{24})$$

روشن است که U_i 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،...، U_{15} ، V ، U_{16} ، U_{17}،...، U_{30} مورد استفاده قرارمی‌گیرند و از آنجا که در حالت رمزگشایی این ترتیب معکوس می‌شود می‌توان روابط زیر را نوشت :

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

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

فرایندی که برای تولید کلیدهای فرعی در نظرگرفته‌شده ،براساس وجود حافظه برای این کلیدها می‌باشد. به‌طوری‌که در ابتدای عمل رمزگذاری یا رمزگشایی بوسیلهٔ الگوریتم FDE ، کلیدهای فرعی تولیدشده و در درون حافظه قرارمی‌گیرند.حجم حافظهٔ 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 به‌صورت زیر خواهدبود.

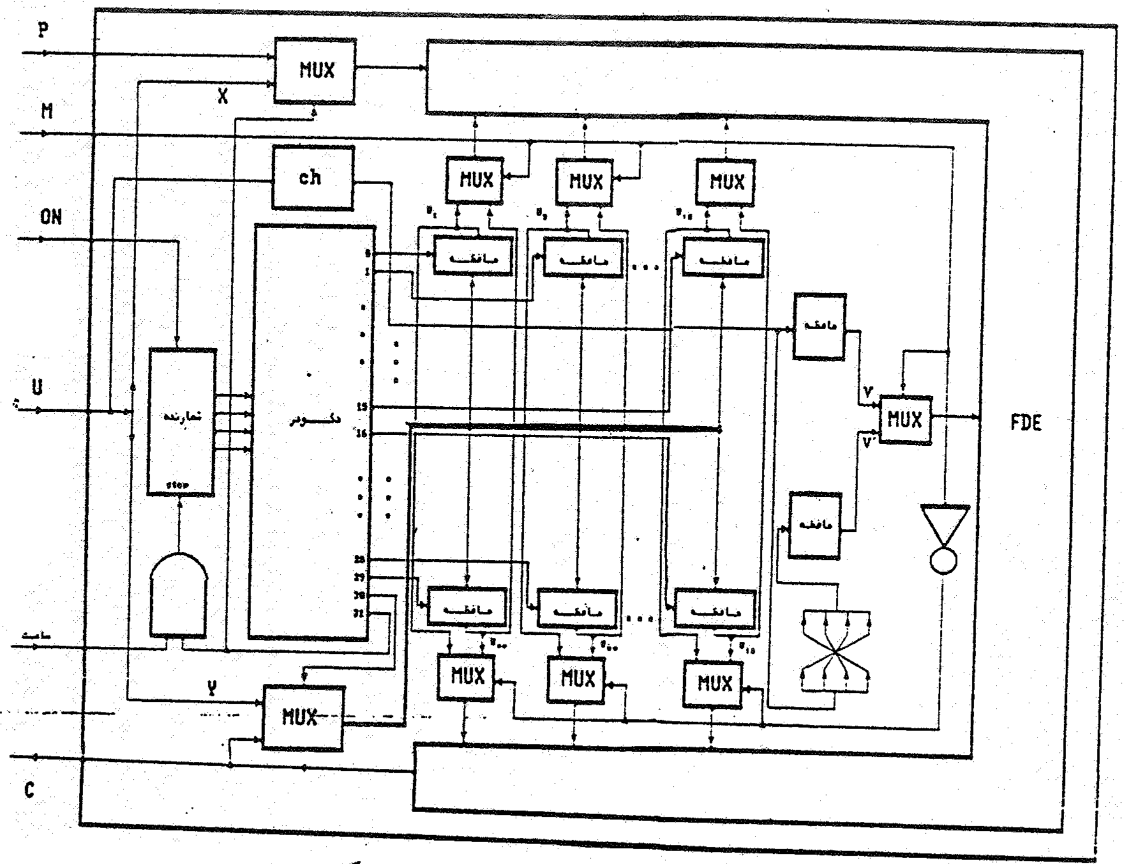
$V = Ch(U)$ (Ch یک تبدیل انتخاب ۹۶ بیت از ۱۲۸ بیت است) (۱۹)

$$U_1 = FDE_{Y,Y,...,Y,V,Y,Y,...,Y}(X)$$
$$U_2 = FDE_{U_1,Y,...,Y,V,Y,Y,...,Y}(X)$$
$$U_3 = FDE_{U_1,U_2,...,Y,V,Y,Y,...,Y}(X)$$
. (۲۰)
.
.
$$U_{30} = FDE_{U_1,U_2,...,U_{15},V,U_{16},U_{17},...,U_{29},Y}(X)$$

روابط فوق نشان می‌دهند 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 حملهٔ جستجوی فضای کلید در طرّاحی سیستم مدّ نظربوده‌است .

شکل ۳ یک ساختار عملی برای تولید کلیدهای فرعی را نمایش می‌دهد.در این شکل خروجیهای کد بردار به کنترل ورودی ثبّات‌های کلید فرعی متصل می‌باشند و دنباله‌های جدول ۱ را تولید می‌کنند.همچنین خط ضخیم بیانگر مسیر عمومی اطلاعات ۶۴بیتی است که کلیدهای فرعی را منتقل می‌کند.در این شکل هنگامی که کلید ON یک می‌گردد دنباله‌های جدول ۱ به ترتیب تولید می‌شوند و لذاکافی است زمان بین تولید دو دنباله برابر و یا بزرگتر از زمان عمل FDE باشد تا U_i ها به ترتیب تولیدشده و در محل خود قرارگیرند.در دنبالهٔ حالت سی‌ودوّم جدول ۱ بیت سی‌ویکم صفرشده و باعث قطع‌شدن ساعت شمارنده و توقف تولید دنباله‌های جدول می‌شود.علاوه‌برآن مولتی پلکس ورودی رمزنگار تغییر وضعیت داده و رمزنگار برای پذیرش متن اصلی آماده می‌گردد.در شکل ۳ بیت M تعیین‌کنندهٔ نوع عمل FDE است.اگر M=1 باشد عمل رمزگذاری و اگر M=0 باشد عمل رمزگشایی صورت می‌گیرد.

یکی دیگر از قابلیت‌های مهم الگوریتم FDE،امکان استفاده از کلیدهای با طول متغیّر است.کلیدی که از طریق کانال امن بین فرستنده و گیرنده مبادله می‌شود،می‌تواند طول متغیّری بین ۶ تا ۱۵ حرف داشته‌باشد.همچنین یک حرف برای نشان دادن طول کلید در کنار آنها قرارمی‌گیرد و لذا طول کلید دریافتی بین ۷ تا ۱۶ حرف است.پس از بررسی توازن و معلوم‌شدن



$M =$ ۱ عمل رمزگذاری
۰ عمل رمزگشایی

شکل ۳ ـ ساختار FDE همراه با ساختار تولید کلید

طول کلید،کلید اصلی ۱۲۸ بیتی U از طریق اعمال یک تبدیل جایگشت برروی کلید دریافتی به‌صورتی‌که صفرهای انتهای ثبّات محتوای کلید (درحالی که طول کلید کمتراز ۱۵ حرف است)

جدول ۱ ـ دنباله‌های خروجی کدبردار

S_{32}	S_{31}	S_{30}	---------	S_3	S_2	S_1	شماره‌بیت
0	0	0	---------	0	1	1	0
0	0	0	---------	1	0	1	1
0	0	0	---------	0	0	1	2
.	.	.	---------	.	.	.	.
.	.	.	---------	.	.	.	.
.	.	.	---------	.	.	.	.
0	0	1	---------	0	0	1	28
0	1	0	---------	0	0	1	29
1	1	1	---------	1	1	0	30
0	1	1	---------	1	1	1	31

در کنار هم قرارنگیرند،به‌دست آمده و در ثبّات محتوای U ذخیره می‌شود.در این ساختار،بیت‌های توازن و همچنین بیت‌های حرف اوّل (نشانگر طول کلید) که هیچیک از بقیهٔ بیت‌های کلید مستقل نیستند در تولید کلیدهای فرعی به کار می‌روند.انتخاب کلید با طول متغیّر برای الگوریتم FDE سبب متغیّرشدن بعد فضای کلید در یکی از ابعاد $۲^{۴۲}$ ، $۲^{۴۹}$ ، $۲^{۵۶}$،... و $۲^{۱۰۵}$می‌شود (برای هر حرف کلید غیر از بیت توازن،۷ بیت در نظرگرفته‌می‌شود).برای مقایسهٔ بعد فضای کلید و زمان جستجوی آن درالگوریتم‌های DES و FDE، ابتدا فرض‌می‌کنیم که کلیدFDE 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 $\frac{۲^{۱۰۵}}{۲^{۵۶}} \cong ۱/۶ \times ۱۰^{۱۶}$ ×۳۰ می‌شود که عدد بسیار بزرگی است.از مزایای عمدهٔ استفاده از کلید باطول متغیّر آن است که

اولاً بسته به اهمیّت کار می‌توان بعد فضای کلید را بزرگتر یا کوچکتر انتخاب نمود و ثانیاً دشمن بعد فضای کلید را نمی‌داند و انتخاب تصادفی بعدهای مختلف و جستجوی فضای کلید زمان بسیار زیادی را از او می‌طلبد و عملاً او را از شکستن سیستم مأیوس می‌سازد.

۳ ـ ایدهٔ خط لوله[1] در تراشهٔ FDE [۱]

با توجه به آنکه ساختار معرفی شده برای رمزنگار FDE سری می‌باشد،به راحتی می‌توان از ایدهٔ خط لوله در عمل رمزنگاری حداکثر استفاده را نمود.شکل ۴ تراشهٔ طراحی شده برای FDE را که براساس ایدهٔ خط لوله عمل می‌کند نشان می‌دهد.دراین شکل متن اصلی به هر دو صورت حرف و یا بیت واردمی‌گردد و متن رمزشده نیز به همان دو صورت خارج می‌شود.

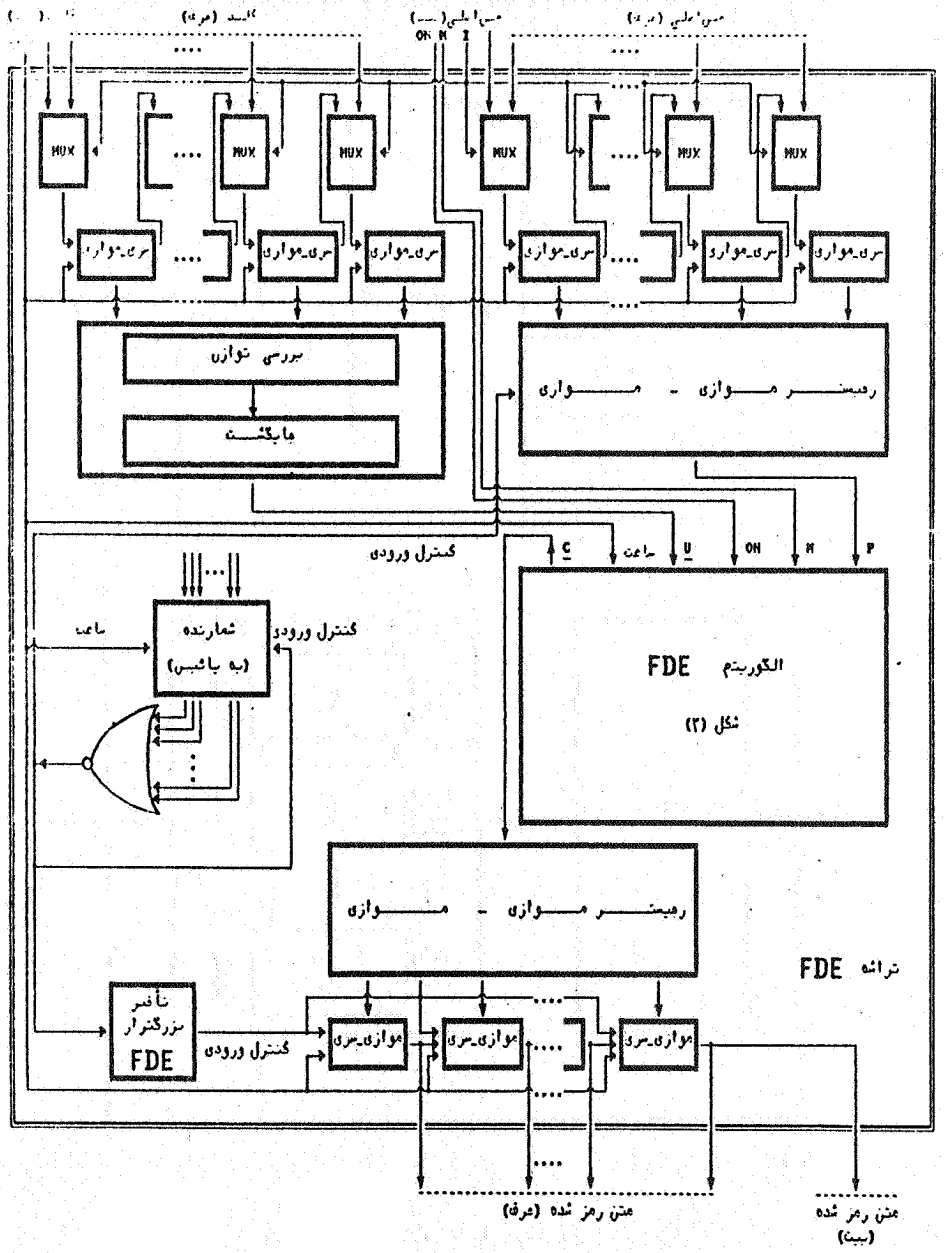
در این تراشه وقتی از حرف استفاده می‌شود بایستی شمارنده در مبنای ۸ و I=1 قرارداده شوند.در این‌صورت بعداز هشت انتقال ، یک پالس ساعت از شمارنده ارسال می‌گرددکه باعث می‌شود ثبّات موازی ـ موازی ورودی بارگردیده و همچنین ثبّات موازی ـ سری خروجی نیز بارشود.اگر انتقال داده‌ها به‌صورت بیت به بیت مورد نظر باشد بایستی مبنای شمارنده ۶۴ و I=0 قرارداده‌شود.

از آنجایی که از ایدهٔ خط لوله در ساختار فوق استفاده‌شده‌است،FDE باسرعت بسیار بالا (زمان عمل ثبّات انتقالی[2]) عمل می‌کند و از این لحاظ بسیار شبیه به رمزنگار پی‌درپی است و از مزایای‌عمدهٔ این نوع رمزنگارها نیز می‌تواند بهره‌مند باشد.به علاوه از آنجاکه FDE یک رمزنگار قالبی است ، کلیهٔ مزایای رمزنگارهای قالبی را نیز داراست.بعنوان مثال FDE نیز همانند DES می‌تواند بسته به نوع کاربرد در یکی از چهارمود عمل ECB ، CBC ، CFB و OFB [۷] به کار رود.

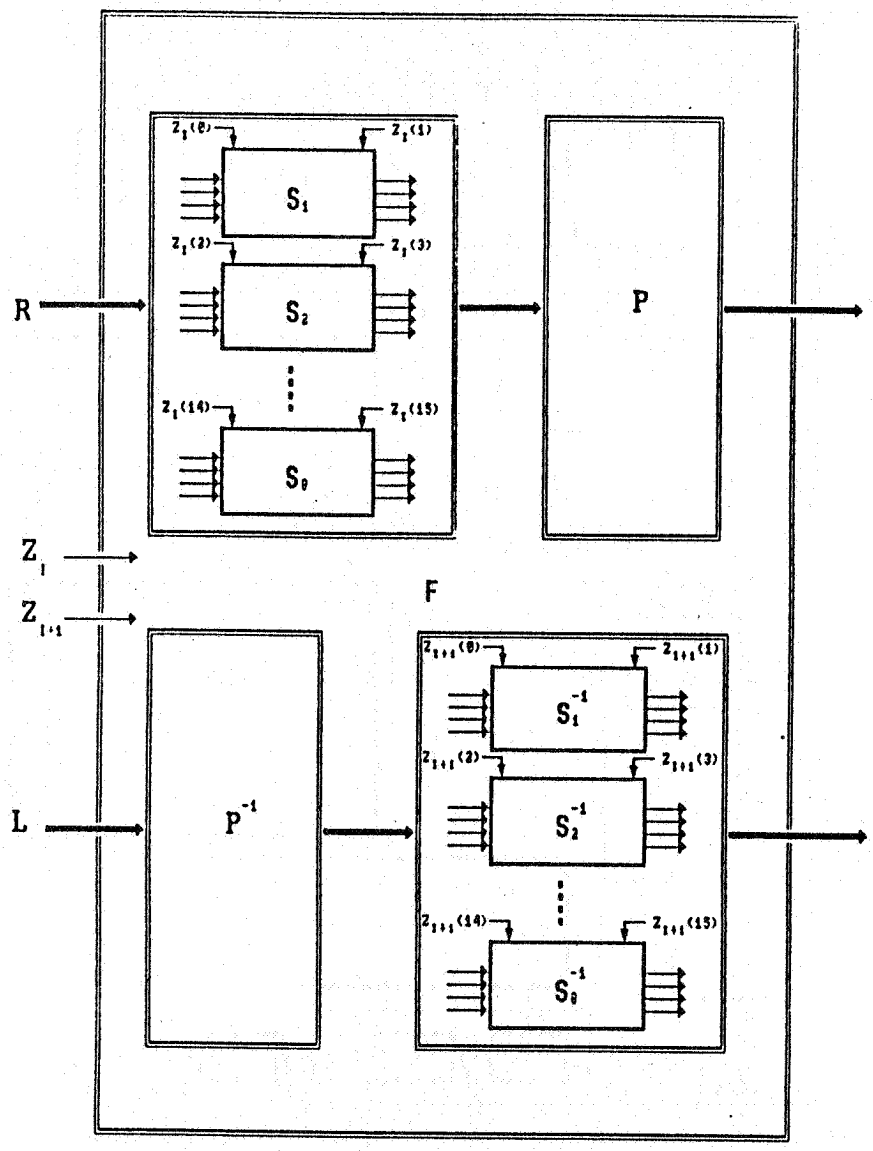
۴ ـ معیارهای انتخاب ساختار تبدیل F

دربخش ۱ تبدیل F را به اجمال معرفی‌کردیم و دیدیم که این تبدیل متشکل از دو لایهٔ ترکیبی جایگشت و جانشینی‌معکوس هم یعنی P.S و $S^{-1}.P^{-1}$ است که برروی دو زیر قالب ورودی R و L به‌طور جداگانه عمل می‌کنند.ساختارکامل تبدیل F در شکل ۵ نشان داده‌شده‌است.جایگشت‌های P و P^{-1} دو جایگشت‌اختیاری و معکوس هم هستند (به‌عنوان نمونه همان جایگشت P در الگوریتم DES) که روی یک قالب ۳۲ بیتی عمل‌می‌کنند.جعبه‌های جانشینی S_i و S_i^{-1} $(1 \leqslant i \leqslant 8)$ دارای ۴

1. Pipeline
2. Shift Register



شکل ۴ ـ تراشهٔ FDE



شکل ۵ ـ ساختار تبدیل $F_{Z_{l+1}, Z_l}(L,R)$

بیت ورودی ، ۴ بیت خروجی و ۲ بیت کلید هستند.در هر جعبه ۴ بیت ورودی شمارهٔ یک سطر و ۲بیت کلید شمارهٔ یک ستون از یک ماتریس ۴×۱۶ را مشخص می‌کنند.در هر ستون ازاین 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 جعبهٔ جانشینی عبارت‌است از یک جعبهٔ جانشینی که در هر ستون آن معکوس جایگشت واقع در همان ستون از جعبهٔ اصلی وجوددارد.این جعبه‌ها غیرخطی انتخاب می‌شوند و سبب هرچه پیچیده‌ترشدن رابطهٔ بین ورودی و خروجی تبدیل F می‌گردند.در اینجا نیز جعبه‌های S_i همانند DES از مهمترین بخشهای ساختار رمزکننده‌بوده و در انتخاب آنها معیارهای خاصی را بایستی در نظرگرفت.اولین معیار در انتخاب چنین جعبه‌هایی کامل[1] بودن آنهاست.یک جعبهٔ جانشینی راکامل گوئیم هرگاه هر بیت خروجی به همهٔ بیت‌های ورودی بستگی داشته‌باشد.بنابراین اگر پیداکردن ساده‌ترین عبارت بولی برای هر بیت از خروجی امکان پذیرباشد،در صورت کامل بودن جعبه جانشینی،هرکدام از این عبارات شامل تمام بیت‌های ورودی خواهدبود.خاصیت مهم دیگر یک رمزنگار جانشینی مناسب ،اثر بهمنی[2] است. برای آنکه یک تبدیل رمزنگاری دارای اثر بهمنی باشد باید بطور متوسط $\frac{1}{2}$ بیت‌های خروجی‌اش ،در اثر تغییر یک تک بیت ورودی تغییرنماید.هرگاه هر بیت خروجی با احتمال $\frac{1}{2}$ در اثر تغییر یک تک بیت ورودی تغییر نماید،تبدیل مؤکداً بهمنی است[۸].

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

$$V_i(X) \triangleq g(X) \oplus g(X_i) \qquad (۲۱)$$

را بردار بهمنی 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 بهمنی را یک متغیر بهمنی نامیده و به ماتریسی که از میانگین‌های آماری متغیرهای بهمنی بدست‌می‌آید،ماتریس وابستگی[3] گویند.عناصر این ماتریس را می‌توان به‌صورت زیربه‌دست‌آورد:

$$d_{ij} = \frac{1}{2^{m-1}} \sum_{\substack{\text{روی} \\ 2^{m-1} \\ \text{حالت X}}} b_i(V_j(X)) \quad , \quad 1 \le i,j \le m \qquad (۲۲)$$

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 تغییرمی‌کند و اگر $d_{ij}=0$ باشد بیت i ام خروجی مستقل از بیت j ام ورودی است.برای یک رمزنگار مؤکّداً بهمنی همهٔ عناصر ماتریس وابستگی مقدار نزدیک به ۰/۵ دارند[۸].

از دیگر ویژگیهای یک رمزنگار خوب،مستقل بودن متغیرهای بهمنی است.هرگاه یک رمزنگار جانشینی دارای این خاصیت باشد گویند رمزنگار تام[1] است [۸].

انتخاب جعبه‌های مناسب جانشینی که دارای ویژگیهای فوق باشند از مسائل قابل توجّهی است که در طراحی نهایی الگوریتم FDE بایستی بطور جدّی بدان پرداخته‌شود.تولید تصادفی تعدادی از این جعبه‌ها و بررسی معیارهای فوق برروی آنها و در نهایت انتخاب جعبه‌های مناسب ، یک روش پیشنهادی برای دست‌یابی به جعبه‌های جانشینی خوب است.

نتیجه گیری

از آنچه که در مورد الگوریتم FDE گفته‌شد ، نکات زیر حائز اهمیّت‌اند:

۱- با تجدید نظر کلی که در نحوهٔ تولید کلیدهای فرعی نسبت به الگوریتم DES به عمل آمده‌است ، ساختار تولید کلیدهای فرعی در FDE بسیار پیچیده‌ترشده به‌طوری‌که از نظر زمان جستجوی کامل فضای کلید،میزان امنیت این الگوریتم نسبت به DES (با فرض تساوی طول کلیدها) حداقل ۳۰ برابرشده‌است.

۲- از مزایای عمدهٔ 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 رمزشده به تمام بیت‌های کلید وابسته می‌شود.

۳- طول کلید در الگوریتم FDE متغیّر است .

۴- ساختار FDE برای بهره‌گیری از ایدهٔ خط لوله مناسب بوده و با توجه به سرعت عمل بالا، تراشهٔ FDE می‌تواند در سیستمهای مختلف به جای رمزنگارهای پی‌درپی قرارگیرد.

۵- تراشهٔ FDE با هر دودادهٔ 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

---

1. Perfect

اختیارشوند.

در خاتمه ضمن تأکید مجدّد بر این نکته که انتخاب و به‌کارگیری جعبه‌های جانشینی با خواص مناسب در ساختار FDE سبب می‌شود که این ساختار علاوه‌بر پیچیده‌تر نمودن حملهٔ جستجوی فضای کلید،از ویژگیهای آماری خوبی (حداقل مشابه با DES) برخوردار باشد،از خوانندگان ومحققان دعوت می‌شود تا در ارزیابی و شکستن الگوریتم رمزکنندهٔ پیشنهادی ،از نظریات کارشناسانهٔ خود ما را بهره‌مندسازند.

مراجع :

۱ . فرامرز هندسی ،نقد وبررسی رمزنگار DES،پایان نامه دوره کارشناسی ارشد مهندسی مخابرات ، دانشگاه صنعتی اصفهان ، آبان۱۳۶۸

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.محمّدرضاعارف ،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.