عنوان مقاله:
تکمیل ساختاررمز FDE با طراحی Sbox های قوی برای آن

محل انتشار:
یازدهمین کنفرانس مهندسی برق (سال:1382)

تعداد صفحات اصل مقاله: ۱۱ صفحه

نویسندگان:
علیرضا شفیعي نژاد - کارشناس ارشد معماري کامپیوتر
فرامرز هندسي - استادیار دانشگاه صنعتي اصفهان
مرتضي اسماعیلي - استادیار دانشگاه صنعتي اصفهان

خلاصه مقاله:
امنیت بیشتر رمزنگارهای قالبی که براساس شبکه Feistel بناشدها ند بستگی به جعبه های جانشینی که درتابع دورازآنها استفاده میشود دارند FDE از جمله همین رمزنگارها می باشد که درساختار تابع دور آن از هشت Sbox با اندازه ۴×۶ استفاده شده است اگرچه جزئیات این sbox ها درساختار این رمزنگارکاملا مشخص نشده است اما معیارهایی برای طراحی آنها درنظر گرفته شده است دراین مقاله سعی شده است که الگوریتمی برای یافتن sbox هایهرچه نزدیکتر به ایده آل ارایه گردد دراین الگوریتم از روش بیت به بیت طراحی با بکارگیری توابع موکدا بهمنی با بیشترین مقدارغیرخطی استفاده شده است با اجرای این الگوریتم تعدادی sbox ایجاد و از بین آنها هشت عدد sbox مناسب انتخاب کرده و درساختار FDE قرارمیدهیم.

کلمات کلیدی:
رمزنگاری - جعبه های جانشینی - FDE - شبه DES

لینک ثابت ثبت مقاله در پایگاه سیویلیکا: