عنوان مقاله:
تحلیل تفاضلی الگوریتم رمزقطعه ای معماگر

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

تعداد صفحات اصل مقاله: 8

نویسندگان:
عباس قائمی بافقی - *دانشگاه صنعتی امیرکبیر دانشکده مهندسی کامپیوتر آزمایشگاه امنیت داد*

بابک صادقیان

خلاصه مقاله:
دراین مقاله میزان مقاومت الگوریتم رمزمعماگر که یک الگوریتم رمزقطعه ای 160بیتی می باشد درمقابل تحلیل تفاضلی مورد بررسی قرارگرفته است بهترین مشخصه تفاضلی بدست آمده دراین مقاله دارای احتمال 149- 2 می باشد و براساس آن حمله ای با پیچیدگی 152 2 ارایه شده است که کمتر از بررسی کل فضای کلیدمی باشد و به لحاظ تئوری نشان دهنده قابل شکست بودن این الگوریتم رمز درمقابل تحلیل تفاضلی است.

کلمات کلیدی:
الگوریتم رمز قطعه ای - الگوریتم رمز معماگر - تحلیل تفاضلی

لینک ثابت مقاله در پایگاه سیویلیکا: