عنوان مقاله:
بهبود حمله تمایز خطی برروی الگوریتم رمز جریانی SOBER-128

محل انتشار:
سومین کنفرانس مهندسی برق و الکترونیک ایران (سال: 1390)

تعداد صفحات اصل مقاله: 7

نویسندگان:
عبدالرسول میرقدری - *تهران دانشگاه جامع امام حسین (ع) دانشکده و پژوهشکده فناوری اطلاعات و ا*

سعید شاهچراغی
علیرضا جلفایی

خلاصه مقاله:
دراین مقاله با معرفی مختصر الگوریتم رمزنگاری SOBER-128 به بررسی و تحلیل این الگوریتم توسط حمله تمایز با پوشانه خطی می پردازیم دراین تحلیل یک تقریب خطی برای فیلتر غیرخطی به کاررفته دراین الگوریم به دست می آوریم و نشان میدهیم که اریب تمایز دهنده می تواند با در نظر گرفتن جمله های درجه دوم از تقریب بهبود یابد اریب احتمالی تقریب درجه دوم به کاررفته در تمایز دهنده تقریبا برابر با O(2 -51.8) می باشد که درصورتی که ادعا داریم SOBER-128 با مشاهده O(2 103.6) کلمه از دنباله کلید از یک دنباله رمز تصادفی واقعی قابل تمایز است نشان میدهیم که اریبی تقریب خطی برابر مقدار 2 -8.8 می باشد همچنین نتیجه گیری خواهیم نمود که با استفاده ا زجمله های درجه دوم در رمز SOBER-128 می توان اریبی به دست امده را بهبود بخشید.

کلمات کلیدی:
رمز جریانی، الگوریتم SOBER-128 ، حمله تمایز، پوشانه خطی، تقریب خطی، فیلتر غیرخطی، اریبی

لینک ثابت مقاله در پایگاه سیویلیکا: