عنوان مقاله:
تحلیل تفاضلی ناممکن الگوریتم رمز قالبی کاهشیافته Piccolo-۸۰

محل انتشار:
فصلنامه پدافند الکترونیکی و سایبری, دوره 2, شماره 1 (سال: 1393)

تعداد صفحات اصل مقاله: 11

نویسندگان:
محمدرضا دستجانی فراهانی - *اراک، کوی شهدا، بلوار شهدا،روبروی پمپ بنزین، کوچه فرهنگ ۲، پلاک ۴۸۱۶*

جواد مهاجری
علی پاینده - -

خلاصه مقاله:
حمله تفاضلی ناممکن، یکی از کارآمدترین حملات روی رمزهای قالبی به شمار میرود. ایده اصلی این حمله، جستجو برای یافتن تفاضل های با احتمال وقوع صفر برای حذف کلیدهای نادرست و دستیابی به کلید درست میباشد. الگوریتم Piccolo به دلیل برخورداری از پراکنش بسیار خوب نسبت به الگوریتم های فایستلی موجود، تاکنون در برابر حملات تفاضلی ایمن بوده است. در این مقاله با استفاده از تعدادی ضعف ساختاری موجود در این الگوریتم، یک حمله تفاضلی ناممکن روی ۹ دور آن ارائه میشود. پیچیدگی زمان، داده و حافظه برای این حمله به ترتیب ۲۸۶۶.۴ عمل رمزگذاری الگوریتم ۹ دوری، ۲۸۶۱ متن اصلی انتخابی و ۲۸۵۷ بایت حافظه برای نگهداری کلیدها و حذف کلیدهای نادرست است.

کلمات کلیدی:
رمز قالبی, تحلیل رمز, تفاضل ناممکن, حمله تفاضلی ناممکن, الگوریتم قالبی سبک Piccolo

لینک ثابت مقاله در پایگاه سیویلیکا: