عنوان مقاله:
حمله تفاضلی با دور کاهش یافته بر روی رمزهای قالبی SIMON۳۲و SIMON۴۸ و SIMON۶۴

محل انتشار:
فصلنامه پدافند الکترونیکی و سایبری, دوره 5, شماره 1 (سال: 1396)

تعداد صفحات اصل مقاله: 8

نویسندگان:
احمد اسکوئیان - *دانشگاه تربیت دبیر شهید رجایی*

نصور باقری - *دانشگاه تربیت دبیر شهید رجایی*

خلاصه مقاله:
در ژوئن سال ۲۰۱۳ خانواده ای از رمزهای قالبی با نام SIMON توسط بیولیو و همکارانش از آژانس امنیت ملی آمریکا معرفی شد. این خانواده از رمزهای قالبی جزء رمزهای قالبی سبک وزن دسته بندی می شود و می تواند طول کلید و طول قالب متفاوتی را بپذیرد. SIMON در مقایسه با بسیاری از رمزهای قالبی سبک وزن دیگر، عملکرد بهتری در سخت افزار و نرم افزار دارد این برتری در زمینه سخت افزاری محسوس تر است. هدف اصلی این مقاله، بهبود حملات تفاضلی ارائه شده بر روی این خانواده از رمزهای قالبی است. با کمک گرفتن از ایده ها و دیدگاههای جدید مطرح شده در مورد روش ها و سیاستهای حدس کلید، توانستیم حمله تفاضلی بهبودیافته ای را بر روی ۲۲ دور ۲۳ ،SIMON۳۲/۶۴دور۹۶ /۴۸ SIMON و ۲۹ دور SIMON۶۴/۱۲۸ به انجام برسانیم.

کلمات کلیدی:
SIMON, حمله تفاضلی, رمزهای قالبی سبک وزن

لینک ثابت مقاله در پایگاه سیویلیکا: