عنوان مقاله:
مقاوم سازی Midori۶۴ در مقابل حمله تحلیل توان همبستگی

محل انتشار:
هجدهمین کنفرانس بین المللی انجمن رمز ایران (سال: 1400)

تعداد صفحات اصل مقاله: 9

نویسندگان:
حمید قنبری - *دانشکده و پژوهشکده برق، مخابرات و جنگال، دانشگاه جامع امام حسین (ع)*

بهروز خادم - *استادیار، دانشکده و پژوهشکده کامپیوتر و قدرت سایبری، دانشگاه جامع امام حسین (ع)*

محمد جدیدی - *دانشکده و پژوهشکده کامپیوتر و قدرت سایبری، دانشگاه جامع امام حسین (ع)*

خلاصه مقاله:
کاربرد رمزهای سبک وزن و کم مصرف در اینترنت اشیا اجتناب ناپذیر شده است. اخیرا Midori۶۴ به دلیل مصرف توان بسیار کم در بین سایر رمزهای سبک وزن مورد توجه زیادی قرار گرفته است. امنیت Midori۶۴ از طرف حملات مختلفی از جمله حملات کانال جانبی مورد تهدید قرار گرفته است. یکی از انواع حملات کانال جانبی حمله تحلیل توان همبستگی است که در آن مهاجم با استفاده از نشت توان تراشه رمزنگاری و در حین اجرای الگوریتم، داده ی درحال پردازش و عملیات در حین اجرا می تواند کلید رمزنگاری را کشف کند. نقاب گذاری در برابر حملات تحلیل توان به عنوان یکی از موثرترین روش های مقاوم سازی الگوریتم های رمزنگاری شناخته شده است. هدف از نقاب گذاری برهم زدن رابطه بین توان مصرفی و عملیات درحال انجام است. در این مقاله یک نسخه پیاده سازی شده رمز Midori۶۴ روی میکروکنترلر AVR مدل Atmega۳۲ مورد حمله تحلیل توان همبستگی قرار گرفته و کلید رمزنگاری با ۳۰۰ بلوک متن اصلی کشف شده است. پس از مقاوم سازی Midori۶۴ با روش نقاب گذاری بولی، مجددا این حمله انجام شده و نتایج به دست آمده از آزمایشات نشان داده که روش نقاب گذاری بولی می تواند مانع کشف کلید شود.

کلمات کلیدی:
امنیت اینترنت اشیا، رمز سبک وزن، Midori۶۴، حمله تحلیل توان همبستگی، نقاب گذاری

لینک ثابت مقاله در پایگاه سیویلیکا: