سیویلیکا - ناشر تخصصی مقالات کنفرانس ها و ژورنال ها
گواهی ثبت مقاله در سیویلیکا
CIVILICA.com

عنوان مقاله:
مروری بر حملات ارائه شده بر روی خانواده رمزهای قالبی SIMONوSPECK

محل انتشار:
دومین همایش ملی پژوهش های کاربردی در علوم کامپیوتر و فناوری اطلاعات (سال: 1393)

تعداد صفحات اصل مقاله: 12

نویسندگان:
احمد اسکوئیان - *دانشجوی کارشناسی ارشد دانشکده مهندسی برق و کامپیوتر،دانشگاه تربیت دبیر شهید رجایی*

نصور علیزاده - *استادیار دانشکده مهندسی برق و کامپیوتر،دانشگاه تربیت دبیر شهید رجایی*

جواد علیزاده - *مرکز تحقیقات فتح ،دانشکده و پژوهشکده مهندسی فاوا،دانشگاه جامع امام حسین (ع)*

خلاصه مقاله:
در ژوئن سال 2013 ،خانواده رمزهای قالبی SIMONو SPECK توسط بیولیو و همکارانش از آژانس امنیت ملی آمریکا معرفی شدند.این خانواده از رمزهای قالبی جزو رمزهای قالبی سیک وزن دسته بندی می شوند و می توانند طول کلید و طول قالب متفاوتی را بپذیرند.در مقایسه با بسیاری از رمزهای قالبی سبک وزن دیگر SIMONوSPECK عملکرد بهتری در سخت افزار و نرم افزار دارند. رمز قالبی SIMON برای کاربردهای سخت افزاری و رمزهای SPECK برای کاربردهای نرم افزاری طراحی شده اند.هدف اصلی از این مقاله مرور حملات مهم ارایه شده روی این دو خانواده از رمزهای قالبی است.تاکنون حمله تفاضلی ،بهترین و موفق ترین حمله ارایه شده روی رمز قالبی SIMON است.همچنین در مورد رمز قالبی SPECK حملات تفاضلی و مستطیلی نتایج بهتری در مقایسه با سایر حملات ارایه شده داشته اند.در این مقاله ،تکنیک حملات تفاضلی و مستطیلی روی رمزهای قالبی SIMON و SPECK توضیح داده شده و نتایج این حملات به صورت مختصر گزارش می شوند.

کلمات کلیدی:
رمزهای قالبی سبک وزن، تحلیل رمز،حمله تفاضلی،SPECK SIMON

لینک ثابت مقاله در پایگاه سیویلیکا:
https://civilica.com/doc/455123