عنوان مقاله:
حمله ی بومرنگ ناممکن کلید مرتبط روی دور کاهش یافته ی رمز قالبی Simon3 / 64

محل انتشار:
فصلنامه صنایع الکترونیک, دوره 7, شماره 3 (سال: 1395)

تعداد صفحات اصل مقاله: 12

نویسندگان:
فهیمه عظیمی - *کارشناسی ارشد امنیت اطلاعات، دانشگاه صنعتی مالک اشتر تهران،*

نصور باقری - *استادیار دانشکده مهندسی برق، دانشگاه تربیت دبیر شهید رجائی،*

خلاصه مقاله:
در دهه ی گذشته حملات کلید مرتبط از جهت نظری و عملی مورد مطالعه قرار گرفته اند و آسیب ناپذیری در برابر حملات کلید مرتبط به عنوان یکی از اهداف امنیت در طراحی رمزهای قالبی درنظر گرفته شده است. ارزیابی رمزها در مقابل انواع حملات، منجر به شناسایی آسیب پذیری آن ها و بهبود طرح های رمزنگاری می شود. حمله ی بومرنگ ناممکن کلید مرتبط، از ترکیب حملات بومرنگ و تفاضلی ناممکن کلید مرتبط ساخته می شود. انعطاف پذیری در انتخاب تفاضل های کلید، امکان حمله روی تعداد دور بیشتری از رمزهای قالبی را با استفاده از این حمله فراهم می سازد. خانواده ی رمزسبک وزن Simon اخیرًا توسط NSA به صورت امن و انعطاف پذیر برای عملکرد مناسب درمحیط های محدود سخت افزاری و در ده نسخه طراحی شده است. زمانبند کلید Simon در برابر حملات کلید مرتبط، مقاوم طراحی شده است. در این مقاله برای اولین بار حمله ییومرنگ ناممکن کلید مرتبط روی 20 دور کاهش یافته رمز سبک وزن Simon32 / 64 انجام شده است.

کلمات کلیدی:
رمز قالبی، زمانبند کلید، حمله ی بومرنگ ناممکن کلید مرتبط، Simon3 / 64

لینک ثابت مقاله در پایگاه سیویلیکا: