عنوان مقاله:
حمله تحلیل زمان روی یک الگوریتم رمز جریانی

محل انتشار:
فصلنامه پدافند الکترونیکی و سایبری, دوره 4, شماره 1 (سال: 1395)

تعداد صفحات اصل مقاله: 9

نویسندگان:
حامد مومنی - *مرکز تحقیقات صدر*

محمد علی طاهری - *مرکز تحقیقات صدر*

خلاصه مقاله:
زمان اجرای یک الگوریتم رمزنگاری می تواند یک کانال اطلاعاتی مفید برای مهاجم باشد و اطلاعات فوق العاده ارزشمندی را در اختیار وی قرار دهد. در حمله تحلیل زمان که از حملات کانال جانبی محسوب می گردد، اندازه گیری زمان های اجرای الگوریتم به ازای ورودی های مختلف به یک مدل آماری داده می شود که می تواند با محاسبه همبستگی بین اندازه گیری های زمانی مختلف و تحلیل آن ها برخی از بیت های کلید یا مقادیر حالت را با درصدی عدم قطعیت به دست آورد. در این مقاله آسیب پذیری یک الگوریتم رمز جریانی مبتنی بر کلمه از دید حمله تحلیل زمان، بررسی می گردد. استفاده از تابعی در کنترل کلاک LFSR های الگوریتم، حمله مذکور را امکان پذیر ساخته و باعث فاش شدن چندین بیت از LFSR ها در هر کلاک می گردد. همچنین تعداد کلاک های LFSR ها را نیز قابل پیش بینی خواهد ساخت. در ادامه، با تغییر آن تابع، الگوریتم در مقابل حمله تحلیل زمان مقاوم شد. در ضمن با استفاده از تابع جدید کنترل کلاک، علاوه بر مقاوم سازی، بیش از ۲۶ درصد نیز سرعت تولید کلید الگوریتم افزایش یافت.

کلمات کلیدی:
الگوریتم رمز جریانی, حمله ی تحلیل زمان, تابع کنترل کلاک, مقاوم سازی