عنوان مقاله:
مقدمه ای بر مقاوم سازی الگوریتم های رمزنگاری در برابر حملات کانال جانبی با استفاده از روش پیاده سازی آستانه ای

محل انتشار:
مجله پدافند غیر عامل, دوره 12, شماره 2 (سال: 1400)

تعداد صفحات اصل مقاله: 13

نویسندگان:
جواد علیزاده - *دانشکده فناوری اطلاعات و ارتباطات، مرکز علم و فناوری فتح*

حمید قنبری - *دانشگاه جامع امام حسین ع - دانشکده فناوری اطلاعات و ارتباطات - مرکز علم و فناوری فتح*

خلاصه مقاله:
برای تامین امنیت اطلاعات و ارتباطات لازم است تا یک الگوریتم رمزنگاری به صورت نرم افزاری یا سخت افزاری پیاده سازی و به کار گرفته شود. در سال ۱۹۹۶ کوچر، حملاتی روی سامانه های رمزنگاری مطرح کرد که در آن ها از نشت اطلاعات مربوط به پیاده سازی الگوریتم‌های رمز استفاده می‌شد. از این نوع حملات که با نام حملات کانال جانبی شناخته شده‌اند، می‌توان به حمله تحلیل توان اشاره کرد. برای مقابله با حملات کانال جانبی، روش‌های مقاوم‌سازی مانند نقاب گذاری یا نهان کردن ارائه شد ولی بعدها نشان داده شد که این نوع روش‌ها در حضور گلیچ اثربخشی لازم را ندارند. جهت برطرف کردن این مشکل و مقاوم سازی سامانه های رمزنگاری در برابر حملات کانال جانبی، حتی در حضور گلیچ، روش پیاده سازی آستانه‌ای در سال ۲۰۰۶ توسط نیکووا و همکاران ارائه شد. این روش کاربردی از سه مبحث رمزنگاری آستانه ای، سهم نهان و محاسبه چندجانبه تشکیل شده است. در واقع خود این روش هم نوعی مقاوم سازی به روش نقاب گذاری است که شرط هایی اضافه برای تامین امنیت در حضور گلیچ دارد. در سال‌های اخیر موسسه استانداردسازی NIST فعالیت‌هایی در حوزه پیاده سازی آستانه‌ای شروع کرده است که یکی از اهداف آن ها، تدوین یک استاندارد در این زمینه است. این موضوع باعث شده است تا در حال حاضر رمزنگاران موضوع پیاده سازی آستانه‌ای را به عنوان یک موضوع مهم در نظر بگیرند. در این مقاله روش رمزنگاری آستانه‌ای به عنوان یک روش جهت مقاوم‌سازی سامانه های رمزنگاری در برابر حملات کانال جانبی توصیف و به نکات برتری و چالش‌های آن در مقایسه با روش‌های مقاوم‌سازی قبلی مانند نقاب‌گذاری اشاره می‌شود.

کلمات کلیدی:
حمله کانال جانبی, حمله تحلیل توان, پیاده سازی آستانه ای