عنوان مقاله:
بررسی حمله کانال جانبی cache attack بر روی الگوریتم AES

محل انتشار:
کنفرانس ملی تحقیقات نوین در مهندسی برق،کامپیوتر و فناوری اطلاعات (سال: 1397)

تعداد صفحات اصل مقاله: 5

نویسندگان:
سجاد صابری - *دانشجوی کارشناسی مهندسی فناوری اطلاعات دانشگاه خیام*

سعید ناصری - *دانشجوی کارشناسی مهندسی کامپیوتر – نرم افزار دانشگاه خیام*

محمدرضا جعفری - *عضو هیات علمی گروه مهندسی کامپیوتر دانشگاه خیام*

خلاصه مقاله:
امروزه اهمیت رمزنگاری در حفظ برقراری امنیت روز به روز در حال توسعه و گسترش می باشد و همگان در این زمینه را بر آن داشته تا به دنبال روش ها وشیوه های جدید باشند تا از نفوذ بد اندیشان و مجرمین اینترنتی به اطلاعات دیگران و سو استفاده از این اطلاعات را جلوگیری کنند. الگوریتم های زیادی نیز در زمینه ی رمزنگاری کشف شده است. الگوریتم های رمزنگاری به دو گروه عمده تقسیم می گردند این دو گروه عبارت هستند از الگوریتم های رمزنگاری متقارن و نا متقارن. از گروه الگوریتم های رمزنگاری متقارن، الگوریتم های رمزنگاری AES دارای سرعت بالا و قابلیت اجرا در سخت افزار و نرم افزار می باشند. به دلیل اهمیت الگوریتم های رمزنگاری AES حملاتی بر روی آن انجام می شود که یکی از این حملات، حملات کانال جانبی می باشد. در این مقاله به بررسی الگوریتم AES و تاثیر حمله cache attack که از انواع حملات کانال جانبی هستند، پرداخته می شود.

کلمات کلیدی:
الگوریتم ای یی اس، حمله کانال جانبی، کش اتک، رمزنگاری