دومین کنفرانس انجمن رمز ایران
دانشگاه صنعتی شریف
۳۰-۲۹ مهر ماه ۱۳۸۲

ارزیابی تحلیلی الگوریتم رمز طارق۲

قدمعلی باقری کرم
دانشجوی کارشناسی ارشد دانشگاه صنعتی اصفهان
gh_ali_bk@yahoo.com

محمد دخیل علیان
استادیار دانشگاه صنعتی اصفهان
mdalian@ec.iut.ac.ir

چکیده : در این مقاله ابتدا برخی مبانی تئوری امنیت قابل اثبات در برابر حملات تفاضلی و خطی،بررسی می‌گردد وسپس قوانین طراحی الگوریتم رمز طارق ۲ ،خصوصا مقاومت آن در برابر حملات تفاضلی و خطی مرور می گردد و ثابت می‌گردد که این الگوریتم دارای امنیت قابل اثبات در برابر مدلهای اولیه حملات تفاضلی و خطی می‌باشد.

کلمات کلیدی: طارق ۲ ، حمله تفاضلی ، حمله خطی ، امنیت قابل اثبات ، همبستگی

۱- مقدمه

پس از ابداع حملات تفاضلی و خطی،تلاشهای زیادی برای طراحی الگوریتمهای رمز قالبی مقاوم در برابر این حملات انجام شده است. یکی از این تلاشها معطوف به امنیت قابل اثبات در برابر حملات تفاضلی و خطی شده است.اولین الگوریتم رمز قالبی با امنیت قابل اثبات در برابر حملات تفاضلی و خطی تحت شرط استقلال کلیدهای دور توسط نایبرگ[1] و نادسن[2] طراحی شد[۱و۲] سپس ماتسوئی[۳] یک روش جهت طراحی الگوریتمهای رمز قالبی با امنیت قابل اثبات در برابر حملات تفاضلی و خطی مطرح کرد. این روش بر مبنای همان قوانین مطروحه توسط نایبرگ و نادسن بود اما در آن از برخی ساختارهای جدید استفاده شده بود که می تواند جهت کاهش اندازه جعبه های S-box به کار گرفته شود. این روش در طراحی برخی الگوریتمهای رمز قالبی از جمله MISTY[4] , KASUMI[5,6] و طارق ۲ استفاده شده است. در این مقاله برخی مبانی تئوری امنیت قابل اثبات در برابر حملات تفاضلی و خطی تحت شرط استقلال کلیدهای دور بررسی می گردد. در اینجا تاکید بیشتر بر روی تئوریهایی است که ارتباط بیشتری با مبنای طراحی طارق ۲ دارند . نکته قابل توجه این است که تئوریهای مطرح شده در این مقاله صرفا برای بررسی امنیت قابل اثبات در برابر حملات مرسوم تفاضلی و خطی قابل استفاده اند.

۲- تحلیلهای تفاضلی و خطی

در این قسمت یک مرور سریع بر روی حملات تفاضلی و خطی انجام می گیرد تا اینکه نمادهای به کار رفته در سایر قسمتها تعریف گردد.

1.Nyberg
2.Knudsen