عنوان مقاله:
حمله خطای چند مرحله ای به PRINCE

محل انتشار:
چهارمین کنفرانس ملی و دومین کنفرانس بین المللی پژوهش های کاربردی در مهندسی برق، مکانیک و مکاترونیک (سال: 1395)

تعداد صفحات اصل مقاله: 13

نویسندگان:
فاطمه ولادتی - *دانشجوی کارشناسی ارشد علوم کامپیوتر، دانشگاه دامغان*

مصطفی زارع خورمیزی - *استادیار دانشکده ریاضی و علوم کامپیوتر، دانشگاه دامغان*

سیدهاشم طبسی - *استادیار دانشکده ریاضی و علوم کامپیوتر، دانشگاه دامغان*

خلاصه مقاله:
وابستگی های بین دورهای مختلف الگوریتم های رمز که توسط طرح کلید ایجاد می شوند، حمله های مختلفی را امکان پذیر می سازد. به همین دلیل، جدیدترین رمزها مانند PRINCE هیچ طرح کلیدی ندارند. در این مقاله یک روش تحلیل خطای تفاضلی که ترکیب حمله های خطا و تحلیل رمز تفاضلی است، برای رمزهای بلوکی که زیرکلیدهای مستقل داشته باشند، معرفی می شود. همچنین یک الگوریتم که این تکنیک را پیاده سازی می کند، توصیف می شود. علاوه بر این، نشان داده می شود که با کاربرد الگوریتم فوق روی رمز بلوکی سبک وزن PRINCE، تقریبا 4 تزریق خطا کافی است تا کلید 128 بیتی کامل بازسازی شود.

کلمات کلیدی:
تحلیل رمز، تحلیل خطای تفاضلی، PRINCE، رمز بلوکی سبک وزن، حمله ی خطای چند مرحله ای

لینک ثابت مقاله در پایگاه سیویلیکا: