عنوان مقاله:
تحلیل خطی الگوریتم رمز معماگر۵ مرحله ای

محل انتشار:
نهمین کنفرانس سالانه انجمن کامپیوتر ایران (سال: 1382)

تعداد صفحات اصل مقاله: 12

نویسندگان:
رضا سپهی - *دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی امیرکبیر*

محمود سلماسی زاده - *پژوهشکده الکترونیک دانشگاه صنعتی شریف*

بابک صادقیان - *دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی امیرکبیر*

خلاصه مقاله:
معماگر یک الگوریتم رمز بلوکی 610بیتی است که شامل ۷ مرحلهٔ جانشینی می باشد . در این مقاله امنیت ۵ مرحلهٔ جانشینی از الگوریتم رمز معماگر با استفاده از روش تحلیل خطی مورد بررسی و تحلیل قرار گرفته است . بدین منظور، یک تقریب خطی برای ۴ مرحلهٔ جانشینی از معماگر با احتمال منفی 22 به توان 10 ضربدر 2/146473- 0/5 ارائه کرده ایم؛ با بکارگیری این تقریب، 25 بیت از کلید 160 بیتی یک سیستم رمز معماگر ۵ مرحله ای را با پیچیدگی محاسباتی 10 به توان 46 ضربدر 2/146473 - 0/5(عمل رمز) و پیچیدگی داده ای 10 به توان 15 ضربدر 1/125899(تعداد شمارنده) تخمین زده و امنیت آن را به مخاطره می اندازیم .

کلمات کلیدی:
تحلیل خطی، تحلیل رمز، الگوریتم رمز معماگر، رمز بلوکی

لینک ثابت مقاله در پایگاه سیویلیکا: