عنوان مقاله:
ارائه طرح عملی برای پیاده سازی جعبه های جانشینی 16 بیتی

محل انتشار:
سومین کنفرانس انجمن رمز ایران (سال: 1384)

تعداد صفحات اصل مقاله: 10

نویسندگان:
مهدی عطائی نائینی - *دانشگاه صنعتی اصفهان*

یاسر افتخاری روزبهانی - *دانشگاه صنعتی اصفهان*

حسین سعدی - *دانشگاه صنعتی اصفهان*

مهدی برنجکوب - *دانشگاه صنعتی اصفهان*

خلاصه مقاله:
هدف در این مقاله ارائه روشی قابل پیاده سازی نرم افزاری و سخت افزاری برای جعبه های جانشینی بزرگ است. برای اینمنظور از ایده جعبه های جانشینی در AES استفاده شده است. مشکلی که در این مقاله به حل آن پرداخته شده است چگونگی معکوس گیی در میدان (2 به توان 16) GF می باشد. در این راستا چگونگی تبدیل یک عنصر از میدان (2 به توان 16) GF به دو عنصر معادل در میدان (2 به توان 8) GF و عمل عکس آن تشریح گردیده است و پس از آن چگونگی انجام عمل معکوس گیری با استفاده از عناصر معادل در میدان (2 به توان 8) GF با ارائه جزئیات محاسباتی لازم آورده شده است. در نهایت، خلاصه طرح عملی برای پیاده سازی جعبه جانشینی 16 بیتی ارائه گردیده است.

کلمات کلیدی:
جعبه جانشینی ، AES ،معکوس گیری ، میدان های متناهی