عنوان مقاله:
رمزنگاری کلیدعمومی، امضا دیجیتال، امضارمز، خم بیضوی، امنیت پیشرو MDx به کمک کدهای خطی اصلاح خطا

محل انتشار:
چهارمین کنفرانس انجمن رمز ایران (سال: 1386)

تعداد صفحات اصل مقاله: 8

نویسندگان:
نصور باقری - *آزمایشگاه رمز و سیستمهای امن، دانشگاه علم و صنعت ایران*

مجید نادری - *دانشکده مهندسی برق، دانشگاه علم و صنعت ایران*

خلاصه مقاله:
در این مقاله یک روش برای بهبود پایداری توابع درهم ساز در مقابل حملات تلاقی ارائه می شود. در اینجا روشی برای بسط پیام ارائه میشود که در صورت ب هکارگیری آن در ساختار الگوریتمهای درهم ساز گروه،MDx این الگوریتمها در مقابل حملاتی که تا به امروز برای آنها ارائه شده است با حاشیة امنیت بالایی ایمن می شوند. در این روش از یک کد انتقال خطی مناسب برای بسط پیام استفاده می شود. با توجه به اینکه اساس کار تمامی حملات معرفی شده برای توابع درهم ساز بر کنترل میزان اختلاف موجود بین دو متن مختلف که منجر به تلاقی می شوند است، نشان داده می شود که درصورت استفاده از یک بردار کد با وزن مناسب می توان این الگوریتمها را در مقابل حملات معرفی شده برای توابع فشرد هساز ایمن کرد.

کلمات کلیدی:
کدهای اصلاح خطا، بسط پیام، توابع دره مساز، تابع فشرد هساز، حمله تلاقی، خانواده،MDx

لینک ثابت مقاله در پایگاه سیویلیکا: