سیویلیکا - ناشر تخصصی مقالات کنفرانس ها و ژورنال ها
گواهی ثبت مقاله در سیویلیکا
CIVILICA.com

عنوان مقاله:
ارائه روشی نوین برای تلفیق کدگذاری کانال و رمزنگاری مبتنی بر کدگذاری قطبی

محل انتشار:
فصلنامه پدافند الکترونیکی و سایبری, دوره 4, شماره 1 (سال: 1395)

تعداد صفحات اصل مقاله: 9

نویسندگان:
محمد کنارکوهی - *دانشگاه گیلان-رشت*

حسن توکلی - *دانشگاه گیلان-رشت*

خلاصه مقاله:
در این مقاله، کدهای قطبی که به تازگی توسط Arikanارائه گردیده، برای تلفیق کدگذاری کانال و رمزنگاری استفاده شده است. بیت های کد قطبی به دو دسته تقسیم می شوند. دسته اول بیت هایی می باشند که به طور مجازی از کانال های با ظرفیت بالا عبور می-کنند که به اختصار بیت های با ظرفیت بالا نامیده می شوند و اطلاعات بر روی آن ها قرار می گیرد. دسته دوم بیت هایی می باشند که به-طور مجازی از کانال های با ظرفیت پایین عبور می کنند که به اختصار "بیت های ثابت" نامیده می شوند. در طرح پیشنهادی اول از بیت های ثابت به عنوان کلید رمز استفاده می کنیم، و بر روی تمامی بیت های این طرح (بیت های اطلاعات و بیت های ثابت) کلید رمز قرار می گیرد. در واقع در طرح ۸ بیتی پیشنهادی Arikan، از ۸ کلید رمز استفاده می کنیم. سپس در ادامه این مقاله روشی ارائه می-شود که توسط آن می توان تعداد کلید رمز اعمال شده بر روی بیت ها را کاهش داد. این سیستم رمزنگاری موثر و مطلوب است که در آن، علاوه بر پیچیدگی زیاد و عدم همبستگی بین بیت ها، از حداقل کلید رمز در آن استفاده شده باشد.

کلمات کلیدی:
رمزنگاری, کدگذاری کانال, تلفیق رمزنگاری و کدگذاری, کدقطبی, پیچیدگی

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/1208210