

عنوان مقاله:

سامانه توام رمزنگاری کلیدمتقارن - کدگذاری کانال مبتنی بر کدهای بررسی توازن کم چگال منظم

محل انتشار:

هشتمین کنفرانس انجمن رمز ایران (سال: 1390)

تعداد صفحات اصل مقاله: 6

نویسندگان:

رضا هوشمند - دانشگاه هوایی شهید ستاری مرکز تحصیلات تکمیلی

ترانه اقلیدس - دانشگاه صنعتی شریف پژوهشکده الکترونیک

محمدرضا عارف - دانشگاه صنعتی شریف دانشکده مهندسی برق

خلاصه مقاله:

در این مقاله یک سامانه توام رمزنگاری کلید متقارن - کد گذاری کانال با استفاده از کدهای بررسی توازن کم چگال شبه دوری منظم مبتنی بر خانواده های تفاضلی گسترش یافته (EDF-QC-LDPC) ارائه می شود با استفاده از ویژگی قالبی دوری ماتریس های به کار رفته در کلید مخفی سامانه پیشنهادی و استفاده از یک روش جدید فشرده سازی طول کلید از $24/4$ کیلوبیت به $3/55$ کیلوبیت کاهش یافته است همچنین سامانه توام کلید متقارن پیشنهادی برخلاف سامانه توام کلید متقارن رانو - نام، به دلیل دارا بودن تعداد زیادی از بردارهای خطای عمدی در برابر حمله متن اصلی منتخب دارای مقاومتی با پیچیدگی از مرتبه 2^{253} است. در سامانه پیشنهادی با بهره گیری از ویژگیهای مطلوب کدهای (EDF-QC-LDPC) به نرخ کد $0/9$ و بیشترین محدوده برای فاصله همینگ کمینه در میان کدهای شبه دوری مبتنی بر خانواده های تفاضلی گسترش یافته دست یافته ایم

کلمات کلیدی:

سامانه رمزنگاری کلید متقارن، کدهای بررسی توازن کم چگال، خانواده های تفاضلی

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/125093>

