عنوان مقاله:
ارائه یک طرح شناسایی امن و کارآ مبتنی بر کدهای قطبی

محل انتشار:
هفدهمین کنفرانس بین المللی انجمن رمز ایران (سال: 1399)

تعداد صفحات اصل مقاله: 8

نویسندگان:
علیرضا جعفری - *دانشگاه هوایی شهید ستاری، مرکز تحصیلات تکمیلی*

رضا هوشمند - *دانشگاه هوایی شهید ستاری، دانشکده مهندسی برق*

معصومه کوچک شوشتری - *دانشگاه صنعتی شریف، دانشکده مهندسی برق*

غلامرضا کرمعلی - *دانشگاه هوایی شهید ستاری، دانشکده علوم پایه*

خلاصه مقاله:
رمزنگاری کدمبنا یکی از نامزدهای رمزنگاری پساکوانتوم است که در سال های اخیر تحقیقات فراوانی در این حوزه انجام شده است.یکی از شاخه های رمزنگاری کدمبنا، طرح های شناسایی کدمبنا هستند که می توان از آنها جهت احراز هویت بین طرفین استفاده نمود در این مقاله، با استفاده از طرح شناسایی Stern، یک طرح شناسایی کدمبنا ارائه می کنیم. کیه در آن به جای استفاده از کدهای تصادفی از کدهای قطبی استفاده شده است. یکی از خواص کدهای قطبی این است که میتوان ماتریس مولد و ماتریس توازن آزما آنها را با توجه به خصوصیات کانال از روی ماتریس آشکار بدست آورد. این خاصیت به ما کمک می کند که در طرح شناسایی کدمبنا پیشنهادی مجبور نباشی کل ماتریس مولد یا توازن آزما را به عنوان داده عمومی ذخیره نماییم. این راهکار به طور قابل ملاحظه ای باعث کاهش حافظه مورد نیاز جهت ذخیره داده عمومی می شود. همچنین در طرح شناسایی پیشنهادی با استفاده از راهکارهایی هزینه ارتباطات نیز نسبت به طرح شناسایی Stern کاهش می یابد. سطح امنیت طرح شناسایی پیشنهادی نیز از دو دیدگاه احتمال تقلب و اثبات هیچ ادمی مورد بررسی قرار گرفته است. علاوه بر آن، نشان می دهیم که طرح شناسایی پیشنهادی در برابر حملهکدبرداری مجموعه اطلاعات مقاوم است.

کلمات کلیدی:
رمزنگاری پساکوانتوم، طرح شناسایی Stern، کدهای قطبی

لینک ثابت مقاله در پایگاه سیویلیکا: