عنوان مقاله:
الگوریتم احراز هویت و توزیع کلید در رمزنگاری کوانتومی با استفاده از تابع درهمساز

محل انتشار:
اولین کنفرانس بین المللی چشم انداز های نو در مهندسی برق و کامپیوتر (سال: 1395)

تعداد صفحات اصل مقاله: 10

نویسندگان:
حمید شبابی - *فارغ التحصیل کارشناسی ارشد مهندسی کامپیوتر و فناوری اطلاعات دانشگاه آزاد اسلامی واحد گرمسار*

مجید شبابی - *مدرس مهندسی کامپیوتر و فناوری اطلاعات دانشگاه علمی کاربردی واحد جهاد دانشگاهی ایلام*

کوروش منوچهری - *هیات علمی دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه آزاد اسلامی واحد پرند*

خلاصه مقاله:
رمز نگاری یک روش قدیمی برای مبادله اطلاعات حساس بین دو طرف ارتباط می باشد برای بهره برداری از رمز نگاری در دستگاه های مختلف به منظور بهبود عملکرد و قابلیت اطمینان از این فناوری تلاش های زیادی انجام گرفته است رمز نگاری مبتنی بر رمز نگاری کوانتومی بسیار امیدوار کننده است و همچنین بهبود این فناوری بیشتر و بیشتر در تطابق با الزامات می باشد بهترین و بیشترین کاربرد استفاده از اطلاعات کوانتومی تا به امروز توزیع کلید کوانتومی بوده است توزیع کلید کوانتومی روشی برای تبادل کلید مخفی بین احزایی است که نیاز به برقراری ارتباط محرمانه و مخفی دارند امنیت پروتکل کوانتومی در وجود یک تابع کوانتوم به وسیله اصل اساسی کوانتوم نهفته می باشد که عدم احراز هویت در پروتکل های کوانتومی آن را در مقابل هکرها آسیب پذیر کرده است ما با استفاده از مفاهیم اولیه مکانیک کوانتومی و روش های موجود به توزیع کلید کوانتومی سیستم کاربردی با استفاده از توابع در هم ساز در رمز نگاری کوانتوم برای ارتباطات تمرکز و حالتی از هنر رمزنگاری کوانتومی بیان خواهیم کرد در این طرح با اجرای سه مرحله به صورت متفاوت در دو طرف ارتباط به احراز هویت و توزیع کلید از طریق کانال کوانتومی خواهیم پرداخت که یکی از متنوع ترین برنامه های رمز نگاری خواهد بود با توجه به اینکه خانواده تابع در هم ساز امنیت قوی را تضمین می کنند ما از کلاس توابع در هم ساز به منظور فرایند توزیع کلید برای امنیت بیشتر و شناسایی شنودگر با احتمال بالا استفاده خواهیم کرد

کلمات کلیدی:
رمز نگاری،رمزنگاری کوانتومی،تابع درهم ساز،توزیع کلید کوانتومی،احراز هویت،ارتباط کوانتومی