عنوان مقاله:
انتقال امن کلید در کانال های کوانتومی با استفاده از کدهای تشخیص و تصحیح کالا

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

تعداد صفحات اصل مقاله: 8

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

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

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

خلاصه مقاله:
رشد و گسترش روز افزون شبکه های کامپیوتری خصوصا اینترنت باعث ایجاد تغییرات گسترده در نحوه زندگی و فعالیت شغلی افراد سازمان ها و موسسات شده است از این رو امنیت اطلاعات به یکی از مسائل مهم در این چرخه تبدیل شده است راه حل های مختلفی نظیر محدود کردن استفاده از اینترنت رمزنگاری داده ها و استفاده از ابزار امنیتی برای میزبان های داخلی و برقراری امنیت شبکه داخلی ارائه شده است یکی از متداول ترین روش های حفاظت اطلاعات رمزنگاری می باشد گرچه امروزه روش های متعدد مطمئنی برای رمزنگاری و جلوگیری از دسترسی نفوذگران به منابع اطلاعاتی طراحی شده ولی به خوبی روشن است که روش های معمول در رمز نگاری نمی توانند امنیت کامل اطلاعات ارسالی را تضمین و اثبات کنند در این مقاله ما با استفاده از مفاهیم اولیه مکانیک کوانتومی و رمز نگاری کوانتوم یک الگوریتم احراز هویت و توزیع کلید کوانتومی به کمک کددهای تصحیح و تشخیص خطا ارائه خواهیم کرد این الگوریتم بر خلاف پروتکل های قبلی که از کانال ارتباطی کلاسیک و کوانتومی یا دو کانال چند مرحله ای استفاده می کردند از یک کانال ارتباط کوانتومی دو مرحله به صورت متفاوت در دو طرف ارتباط که اطلاعات از طریق آن ارسال و منجر به استخراج کلید رمز اطلاعات در بین فرستنده و گیرنده می شود استفاده می شود استفاده می کند در الگوریتم ارائه شده هرچند کار شنودگر برای استراق سمع کلید و ایجاد اختلال در روند داده های ارسالی غیر ممکن نیست ولی بسیار دشوار و با هزینه ی کم قابل کشف است این الگوریتم رای انتقال تعداد کلیدهای کوتاه در کانال های کوانتومی قابلیت اطمینان بالاتری را فراهم می کند

کلمات کلیدی:
کانال های کوانتومی،کدهای تصحیح خطا،تابع درهم ساز،توزیع کلید کوانتومی

لینک ثابت مقاله در پایگاه سیویلیکا: