عنوان مقاله:
حفاظت از اطلاعات سازمانی از طریق رمزنگاری دیتا به وسیله ی استاندارد رمزنگاری پیشرفته مبتنی بر توزیع کلید کوانتومی چندگانه

محل انتشار:
چهارمین کنفرانس بین المللی پژوهش در علوم و مهندسی (سال: 1398)

تعداد صفحات اصل مقاله: 14

نویسندگان:
حمید انیسی - *گروه مهندسی کامپیوتر، دانشکده فنی مهندسی، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران،*

سمیرا سیدصالحی - *گروه مهندسی کامپیوتر، دانشکده فنی مهندسی، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران،*

خلاصه مقاله:
امنیت رمزنگاریهای مدرن در توزیع کلید، مبتنی بر محاسبات پیچیده تولید کلید و استفاده از آن برای رمز کردن دیتا میباشد که زمان مورد نیاز برای شکستن رمز را به شکل چشمگیری افزایش میدهد. اما این سیستم توزیع کلید و کانال عمومی که انتقال دیتا و کلید در آن صورت میگیرد، در صورتی که توسط نفر سومی که از یک کامپیوتر کوانتومی با قدرت و سرعت محاسباتی بالا بهره مند است، شنود شود آسیب پذیر میباشد و امنیت لازم را نخواهد داشت و این امکان را برای شنودگر فراهم میکند تا با توان محاسباتی بالا و استفاده از کلید و دیتای رمز شده، با آنالیز داده ها در نهایت کلید تبادل شده را کشف و دیتای رمز شده را رمزگشایی کند. علاوه بر موارد بیان شده امروزه یکی از مشکلات امنیتی در سازمان ها و نهاد های مختلف سوءاستفاده از دیتا های سازمانی توسط افراد داخل سازمان میباشد. در این مقاله روشی نو به منظور کاهش ریسک شنود اطلاعات توسط افراد غیرمجاز و همچنین کاهش ریسک سوءاستفاده افراد داخل سازمان از دیتاهای سازمانی ارائه میشود.

کلمات کلیدی:
رمزنگاری کوانتومی , کانال کوانتومی , توزیع کلید کوانتومی , قطبش فوتون، استاندارد رمزنگاری پیشرفته, ناهمدوسی کوانتومی