

## عنوان مقاله:

طرح کارآمد از ارتباط مستقیم امن کوانتومی کنترلشده به همراه احراز هویت با هدف ارتقای قابلیت عملیاتی

## محل انتشار:

دومین کنگره بین المللی فن آوری، ارتباطات و دانش ICTCK2015 (سال: 1394)

تعداد صفحات اصل مقاله: 8

## نویسندگان:

میلاذ نانوآکناری - گروه کامپیوتر و فناوری اطلاعات دانشگاه بین المللی امام رضا (ع)

منیره هوشمند - گروه برق دانشگاه بین المللی امام رضا (ع)

امیر خادمی نجف آبادی - گروه کامپیوتر و فناوری اطلاعات دانشگاه بین المللی امام رضا (ع)

## خلاصه مقاله:

در این مقاله، طرحی کارآمد از ارتباط مستقیم امن کوانتومی کنترلشده به همراه احراز هویت با استفاده از حالت GHZ-like از طریق One time pad کوانتومی و عملیات یکانی محلی ارائه شده است. در طرح حاضر، تنها تحت مجوز کنترل کننده، فرستنده و گیرنده می توانند ارتباط مستقیم امن را با موفقیت پیاده سازی کنند و کنترل کننده نیز در هیچ شرایطی نمی تواند پیام های مخفی را به دست آورد. تشخیص استراق سمع و احراز هویت با استفاده از رشته شناسه ی قابل استفاده ی مجدد کاربران انجام می شود. این پروتکل بدون قید و شرط هم در موارد ایده آل و هم در موارد نویزدار امن است. در یک انتقال، یک کیوبیت از هر حالت به عنوان مجوز کنترل کننده استفاده می شود و یک کیوبیت برای انتقال یک بیت کلاسیک مورد استفاده قرار می گیرد. طرح پیشنهادی قابلیت پیاده سازی ساده تری در مقایسه با طرح قبلی دارد.

## کلمات کلیدی:

رمزنگاری کوانتومی، ارتباط مستقیم امن کوانتومی کنترل شده، حالت GHZ-like، احراز هویت

## لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/517609>

