ارائه یک روش امضای کور کوانتومی بر اساس فوتون های قطبیده شده

آزاده مرادی[۱]، مصیب ناصری[۲]

[۱]دانشگاه آزاد اسلامی واحد کرمانشاه / azadehmoradi88@yahoo.com
[۲]دانشگاه آزاد اسلامی واحد کرمانشاه / m.naseri@iauksh.ac.ir

چکیده

اخیرا، پروتکل های امضای کور کوانتومی متفاوتی ارائه شده اند. امضای کور نوعی از امضا است که محتوای پیام را برای حفاظت از حریم خصوصی صاحب پیام، از امضا کننده مخفی می کند. چندی پیش یک نوع امضای کور کوانتومی مبتنی بر رمزنگاری کوانتومی و زوج های در هم تنیده ارائه شد.مدتی بعد ادعا شد که روش ذکر شده دارای نشت اطلاعات کلید می باشد و امنیت بی قید و شرط را تضمین نمیکند. در این مقاله یک پروتکل امضای کور بر اساس قوانین فیزیک کوانتوم را ارائه می کنیم که در این روش صاحب پیام می تواند پیام خودش را با گرفتن یک امضای کور از امضا کننده قابل اعتماد معتبر سازد. بررسی اعتبار پیام به عهده گیرنده می باشد.درضمن شخص امضا کننده هیچ اطلاعی از محتویات پیام ندارد. با توجه به حضور پررنگ اینترنت و نیاز به امنیت اینترنتی بیشتر در زندگی روزمره، این نوع امضای کور کوانتومی برای استفاده در خرید ها و پرداخت های الکترونیکی بسیار مفید است.

واژه های کلیدی

امضای کور کوانتومی؛ رمزنگاری کوانتومی؛ امنیت؛ زوج هـای در هـم تنیده

۱- مقدمه

از آن جا که امضاهای دیجیتال استاندارد نمی توانند از گم نامی صاحب پیام حفاظت کنند، پس نمی توانند ویژگی حفاظت از حریم خصوصی صاحب پیام را برآورده سازند. در نتیجه برای استفاده در سیستم های پرداخت الکترونیک یا رای گیری الکترونیک مناسب نیستند. دیفی وهلمن[1] و مرکل[2] یک امضای دیجیتالی برای معرفی روشی جهت الحاق ماهیت یک شخص به قطعه ای از اطلاعات معرفی کردند. در سال۱۹۸۳، اولین پروتکل امضای کور کوانتومی ارائه شد[3] و ایده کامپیوتر های کوانتومی پدیدار شد. بنابراین اولین امضای کوانتومی با استفاده از تاثیرات کوانتوم و امضاهای کلاسیک برای دستیابی به امنیت بی قید و شرط پیشنهاد شد.

زنگ و همکارانش [4] اولین امضای کوانتومی بر اساس حالت های در هم تنیده سه ذره ای و رمزنگاری متقارن را ارائه دادند. گاتسمن و همکارانش [5] امضای کوانتومی با استفاده از توابع یک طرفه کوانتومی ارائه دادند. در سال ۲۰۰۲، زنگ و همکارانش [6] روش دیگری با حضور یک داور پیشنهاد کردند. بعدها گاوو و همکارانش [7] و چوی و همکارانش [8] مشکلات امنیتی در امضای کوانتومی با حضور داور پیدا کردند.

ون و همکارانش [9]، ابتدا یک امضای کور ضعیف ارائه دادند اما طبق بررسی های ناصری [10] و سو [11] روش آن ها درست عمل نمی کرد زیرا بیش از یک امضا کور برای یک پیام کور وجود داشت. در امضای کور ون، بررسی کننده قادر به شناسایی امضا کور در نیمی از موارد نبود. واژه ضعیف به این معناست که اگر اختلاف یا مغایرتی پیش آمد، ردیابی افراد شرکت کننده در امضا مانند صاحب پیام مقدور است. از طرف دیگر در یک امضای کور قوی، ردیابی افراد شرکت کننده در فرآیند امضا در زمان اختلافات غیر ممکن است. این نوع از امضا برای استفاده در رای گیری های الکترونیک مناسب می باشد.

قبل از توضیح پروتکل امضای کور کوانتومی پیشنهادی، بعضی از تئوری های پایه درباره مکانیک کوانتوم ارائه می شود.

یک بیت کوچکترین واحد اطلاعات در ارتباطات دیجیتال و محاسبات می باشد که دو مقدار ۰ و ۱ دارد. اما یک کیوبیت واحد اطلاعات کوانتومی است و مقدار آن $|0>$ و $|1>$ می باشد.کیوبیت ها متفاوت از بیت ها می باشند در نتیجه نمی توان از آن ها به جای یکدیگر استفاده کرد. بر خلاف بیت ها، کیوبیت ها قابلیت کپی شدن یا خراب شدن ندارند.

امروزه با حضور کامپیوتر های کوانتومی، مجبور به استفاده از اطلاعات و مفاهیم فیزیک کوانتوم هستیم زیرا دارای یک سری ویژگی های متمایز از فیزیک کلاسیک هستند.در روش پیشنهادی ما از خاصیت در هم تنیدگی استفاده می شود. در هم تنیدگی پدیده ای در فیزیک کوانتوم می باشد و وقتی اتفاق می افتد که دو یا گروهی از ذرات به هم وابسته هستند. به این معنی که حالت کوانتومی ذرات به طور وابسته تعریف می شود.

ذرات در هم تنیده دوتایی سه ویژگی مهم دارند:

- هرگونه تغییر یا دستکاری روی ذره اول، ذره دوم را هم تحت تاثیر قرار می دهد.
- تغییرات ذرات مرتبط به فاصله بستگی ندارد.