نوزدهمین کنفرانس ملی سالانه انجمن کامپیوتر ایران
دانشکده مهندسی کامپیوتر، دانشگاه شهید بهشتی، تهران، ۱۵-۱۳ اسفندماه ۱۳۹۲

امضای کور مبتنی بر رمزنگاری کوآنتومی

سیاوش خدام باشی[۱]، علی ذاکرالحسینی[۲]

[۱] دانشکده مهندسی برق و کامپیوتر، دانشگاه شهیدبهشتی، تهران،
siavashyp@yahoo.com

[۲] استادیار گروه کامپیوتر، دانشکده مهندسی برق و کامپیوتر، دانشگاه شهیدبهشتی، تهران،
a-zaker@sbu.ac.ir
شماره پرداخت: ۵۱۵۱۴

چکیده

این روزها مکانیک کوآنتومی شگفتی رمزنگاری سنتی را برانگیخته و این امکان را برای محققین فراهم آورده تا بتوانند ارتباطات امنی در حضور شنودگر برقرار نمایند. در این مقاله یک طرح امضای کور نوین پیشنهاد می‌کنیم که امنیت آن به کمک اصول بنیادین فیزیک کوآنتومی تضمین می‌شود. برخلاف امضاءهای کور پیشین، امضای کور پیشنهادی تنها بر الگوریتم توزیع کلید کوآنتومی QKD تکیه می‌کند و از درهم تنیدگی کوآنتومی مستقل است. در ادامه این مقاله نشان می‌دهیم که امضای کور پیشنهادی در قابلیت اطمینان و امنیت نسبت به سایر امضاءهای کور پیشین برتری دارد. به علاوه نظر به اینکه این امضاء به وسیله فناوری نوین قابل پیاده سازی می‌باشد می‌توان در کاربردهایی نظیر پرداخت الکترونیکی، دولت الکترونیکی و ... از آن بهره برد.

کلمات کلیدی

امضای کور کوآنتومی، توزیع کلید کوآنتومی، رمزنگاری کوآنتومی، پرداخت کوآنتومی.

۱- مقدمه

اعتبارسنجی یک پیام مسئله مهمی در رمزنگاری است، همچنان که یک امضای دست نوشته روی کاغذ اصالت آن پیام را تایید می کند. از امضاءهای دیجیتالی به شکلی گسترده برای اعتبار بخشیدن و حفظ اصالت پیام به صورت انکار ناپذیر استفاده می‌شود. با این وجود امضاء-های دیجیتالی سنتی ممکن است به حریم خصوصی مالک پیام آسیب برساند زیرا آن‌ها دارای ساز و کاری برای ناشناس ماندن صاحب پیام ندارند.

نوع جدیدی از امضاء توسط چام در سال ۱۹۸۳ معرفی گردید که به یک سیستم پرداخت الکترونیکی خودکار امکاناتی می‌داد که تا قبل از آن برای امضاءهای پیش از خود میسّر نبود. از جمله عدم توانایی شخص ثالث در شناختن پرداخت کننده، توانایی هر فرد در اثبات پرداخت خود و امکان جلوگیری از پرداخت‌های به سرقت رفته [۱]. امضای کور شکل دیگری از امضای دیجیتالی است که در آن محتوی پیام پیش از آن که امضا شود پنهان می‌شود. بنابر این شخص امضاء کننده از آنچه که امضاء می‌کند چیزی نمی‌داند و در عین حال کاربر نمی‌تواند بدون کمک امضاء کننده، امضای دیگری را تولید نماید. با این وجود امضای کور تولید شده را می توان به شکل عمومی و با توجه به اصل پیام همانند یک امضای معمولی راستی آزمایی نمود. به طور کلی امضاءهای کور را در پروتکل‌هایی می‌توان به کار بست که امضاء کننده و دارنده پیام دو شخص مجزّا بوده و ناشناخته ماندن دارنده پیام اهمیت داشته باشد. مانند سیستم های رأی گیری الکترونیکی و پول الکترونیکی و ... .

برای مقایسه، تصور کنید که آلیس دارنده نامه ای است که باید توسط رئیس خود یعنی باب امضاء شود. به منظور حفظ حریم خصوصیِ آلیس، باب نباید چیزی از محتویات نامه بداند. بنابر این آلیس نامه را در یک پاکت مخصوصی با آستر کاربن قرار می‌دهد و آن را مهر و موم می‌کند و به دست باب می‌رساند. سپس باب بدون اینکه پاکت کاربنی را باز کند بیرون آن را امضاء زده و دومرتبه به آلیس برمی‌گرداند. به خاطر وجود کاربن درون پاکت، اثر امضای باب روی نامه آلیس افتاده است و بنابراین آلیس می‌تواند پاکت را باز کرده و نامه امضاء شده خود را بردارد درحالیکه باب از محتویات داخل آن اطلاعی ندارد.

امضای کور پیشنهادی چام مبتنی بر پیچیدگی تجزیه اعداد صحیح بزرگ به عامل های اول بود. برخی امضاءهای کور مبتنی بر منحنی های بیضوی نیز در [۲] و [۳] ارائه شده اند. در حقیقت تمامی