ارائه یک پروتکل پرداخت الکترونیکی برون خطی مبتنی بر رمزنگاری کوآنتومی

سیاوش خدام باشی[1]، علی ذاکرالحسینی[2]

۱دانشجوی دکتری معماری کامپیوتر، دانشگاه شهیدبهشتی

۲ استادیار دانشکده مهندسی برق و کامپیوتر، دانشگاه شهیدبهشتی، a-zaker@sbu.ac.ir

تاریخ دریافت: ۹۳/۴/۶ تاریخ پذیرش: ۹۴/۶/۱۵

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. همچنین گسترش روزافزون خرید اینترنتی و بانکداری الکترونیکی نیاز به پروتکل‌ها و روش‌های امنیتی جهت تراکنش‌های مالی را ضروری ساخته است. در این مقاله یک پروتکل پرداخت الکترونیکی نوین برای تراکنش‌های برون خطی ارائه می‌دهیم که عملکردی مشابه چک‌های بانکی دارد و با تکیه بر اصول اولیه فیزیک کوآنتومی امنیت پرداخت را در کاربردهای واقعی تضمین می‌نماید. در این مقاله ما به کمک یک مثال واقعی به تشریح جزئیات پروتکل پیشنهادی می‌پردازیم و در مورد امنیت آن گفتگو می‌کنیم.

کلیدواژه

رمزنگاری کوآنتومی، پرداخت الکترونیکی، چک کوآنتومی، امضای کور.

مقدمه

تجارت الکترونیک پیشرفت‌های بسیاری را در سال‌های اخیر به خود دیده است. برای سالیان متوالی، کارت‌های اعتباری یکی از متداول‌ترین روش‌های پرداخت در تراکنش‌های تجارت الکترونیک شده‌اند. موفقیت تجارت الکترونیک در گرو فناوری‌های پرداخت کارامد است. یکی از این فناوری‌ها چک الکترونیکی می‌باشد که در حقیقت سندی الکترونیکی برای جایگزین کردن چک کاغذی در تجارت الکترونیکی است همچنان که امضاءهای دیجیتالی مبتنی بر رمزنگاری کلید عمومی جایگزین امضاءهای دست‌نویس شدند. سیستم‌های چک الکترونیکی با ویژگی اصالت پیام، تصدیق هویت و انکارناپذیری طراحی می‌شوند و به اندازه‌ای قوی هستند که می‌توانند از کلاهبرداری از بانک‌ها و مشتریانشان جلوگیری نمایند. چک الکترونیکی با تراکنش‌های تعاملی تحت وب یا ایمیل سازگار است و بنابراین به تعامل بلادرنگ یا مجوز شخص سوم متکی نیست.

پرداخت کننده‌ها و دریافت کننده‌ها می‌توانند اشخاص حقیقی، بنگاه‌ها، موسسات مالی و اعتباری یا بانک‌ها باشند. چک‌های الکترونیکی مستقیماً از پرداخت‌کننده به دریافت‌کننده ارسال می‌شود، به قسمی که زمان و هدف پرداخت برای دریافت کننده مشخص است. پرداخت کننده از طریق ایجاد یک سند الکترونیکی محتوی اطلاعات پرداخت به صدور چک الکترونیکی می‌پردازد و آن را به صورت الکترونیکی امضاء می‌نماید. پرداخت کننده چک را به بانکی می‌دهد که در آن‌جا حساب دارد تا آن را معتبر سازد. سپس دریافت کننده چک الکترونیکی را از طریق ایمیل دریافت می‌کند و تایید بانک را بررسی می‌نماید و بدین شکل عمل دادوستد کامل می‌شود.

چک‌های الکترونیکی رایج مبتنی بر پیچیدگی‌های محاسباتی هستند و امنیت آن‌ها به وسیله علم ریاضی و نیز قدرت محاسباتی محدود کامپیوترهای قدیمی تضمین می‌شود. از این رو آن‌ها تنها در مقابل پردازنده‌های قدیمی ایمن هستند [۱-۳]. متاسفانه اینگونه چک‌ها در مقابل کامپیوترهای کوآنتومی آسیب‌پذیر هستند. توازی کوآنتومی می‌تواند برخی مسائل پیچیده مانند تجزیه یک عدد به عامل‌های اول و مسائل لگاریتم گسسته را بسیار سریعتر از کامپیوترهای قدیمی حل کند [۴-۶]. بنابر این محققان علاقه زیادی به استفاده از روشهای کوآنتومی نشان داده‌اند که حتی در مقابل پردازنده‌های کوآنتومی مقاوم هستند.

امضاءهای کوآنتومی به صورت گسترده‌ای برای تضمین اصالت، دست نخوردگی و غیرقابل انکاربودن پیام‌های ارسالی در رمزنگاری کوآنتومی مورد استفاده قرار می‌گیرند و بنابراین برای پرداخت‌های الکترونیکی امروزی ضروری هستند. اولین امضای کوآنتومی را

ژنگ[1] و همکارانش در سال ۲۰۰۱ معرفی کردند [۷]. امضای کوآنتومی ژنگ از همبستگی حالت‌های درهم‌تنیده[2] کوآنتومی بهره می‌برد. در همان سال گاتسمن و چانگ یک تابع یک طرفه کوآنتومی پیشنهاد دادند و امضای دیجیتالی کوآنتومی خود را ارائه کردند [۸]. اگرچه امضای کوآنتومی آن‌ها دو شرط امنیت و اصالت پیام را شامل می‌شد اما ممکن بود به حریم خصوصی صاحب پیام آسیب وارد کند. این مشکل توسط امضاءهای کور کوآنتومی حل شد که اولین بار توسط وِن[3] در سال ۲۰۰۹ پیشنهاد شد [۹]. با این وجود امضای کوآنتومی کارامدتری توسط خدام باشی و ذاکرالحسینی در سال ۲۰۱۴ ارائه گردید [۱۰]. طرح پیشنهادی آن‌ها از قابلیت اطمینان برخوردار بوده و در برابر حملات کوآنتومی ازجمله حملات اسب تراوا و ... مطمئن است.

در سال‌های اخیر پیشرفت های زیادی در رمزنگاری کوآنتومی صورت گرفته و چندین گروه نشان داده‌اند که رمزنگاری کوآنتومی حتی بیرون آزمایشگاه نیز امکان‌پذیر است. برای مثال اخیراً یک گروه از شرکت BBN Technologies، دانشگاه بوستن و دانشگاه هاروارد یک شبکه توزیع کلید کوآنتومی[4] را به حمایت DARPA ساختند. شبکه کوآنتومی DARPA اولین شبکه رمزنگاری کوآنتومی جهان و شاید اولین سیستم توزیع کلید کوآنتومی است که بهره‌برداری مداوم را در سراسر یک کلانشهر امکانپذیر می‌سازد. بسیاری از محصولات QKD پیشتر در قالب تجاری موجود هستند از جمله ID Quantique و MagiQ [۱۱-۱۴].

در این مقاله یک پروتکل پرداخت کوآنتومی برون خطی نوین پیشنهاد می‌شود که از پروتکل‌های توزیع کلید کوآنتومی و one-time pad بهره می‌گیرد. سیستم جدید حداکثر امنیت را بدون نیاز به تعامل بلادرنگ یا مجوز شخص سوم حین فرایند پرداخت ارائه می‌کند. به علاوه در این سیستم نیازی نیست که مشتری و فروشنده قرار از پیش تعیین شده‌ای داشته باشند. با این وجود پروتکل پرداخت کوآنتومی اصالت و یکپارچگی تراکنش‌ها را ضمانت می‌کند. این امکان وجود دارد که بتوان پروتکل پیشنهادی ما را با استفاده از فناوری روز پیاده‌سازی کرده و آن را برای کاربردهای روزمره به کار بست.

ادامه مقاله به این صورت بخش بندی شده است: در بخش ۲، ویژگی‌های پروتکل پرداخت بیان شده‌اند. برخی تئوری‌های بنیادین مکانیک کوآنتومی که کیوچک[5] پیشنهادی بر پایه و اساس آن‌ها بنا شده در بخش ۳ مورد بررسی قرار می‌گیرند. بخش ۴ به معرفی جزئیات پروتکل اختصاص دارد. در بخش ۵ به تحلیل امنیت کیوچک می‌پردازیم. در پایان در بخش ۶ نتیجه گیری می نماییم.

ویژگی‌های پرداخت کوآنتومی

پرداخت الکترونیکی مزایایی نسبت به تراکنش‌های سنتی که در آن مشتری و فروشنده می‌توانستند کالا و پول را همزمان مبادله کنند، دارد که از جمله می‌توان به سهولت و سرعت تبادل اشاره کرد. در تجارت الکترونیک معمولاً دو نفر غیر قابل اعتماد هستند که اقلام خود را مبادله می‌کنند. یک طرح پرداخت منصفانه به گونه‌ای است که در آن هر دو نفر بتوانند اقلام مبادله شده خود را دریافت کنند و یا هیچ یک از آن‌ها نتواند این کار را انجام دهد.

در حقیقت چک کاغذی سندی است که سفارش پرداخت پول از یک حساب بانکی را می‌دهد. فردی که چک را می نویسد، صاحب چک، معمولا یک حساب جاری در بانک دارد و پول خود را در آن حساب از قبل سپرده گذاری کرده است. صاحب چک جزئیاتی شامل مقدار پول، تاریخ و اسم دریافت کننده را روی چک می-نویسد و بدین طریق به بانک عاملش سفارش می‌دهد که به دریافت کننده به همان اندازه پول پرداخت نماید. پرداخت کوآنتومی نیز یک راه حل مشابه برای پرداخت پول میان دو شخص به صورت برون-خط است که از قابلیت های رمزنگاری کوآنتومی برای تضمین امنیت پرداخت بهره می‌گیرد. پرداخت کوآنتومی نوعی حواله پرداخت است که امکان پرداخت بدون نیاز به حمل حجم زیادی پول را میسّر می‌سازد. پرداخت کوآنتومی به موسّسه مالی که صاحب چک در آنجا حساب دارد امر می‌کند که از حسابش به مقدار مشخصی پول پرداخت نماید. هردو صاحب چک یا دریافت کننده می‌توانند اشخاص حقیقی یا حقوقی باشند.

در پرداخت کوآنتومی از بیت‌های دودویی کلاسیک به همراه تعدادی بیت کوآنتومی(کیوبیت) استفاده شده است که توسط بانک مورد اعتماد هر دو طرف صاحب چک و فرد دریافت کننده چک تولید می‌شود و تنها برای یک بار قابل استفاده است. در حقیقت استطاعت مالی صاحب چک برای دریافت کننده آن توسط بانکی که در آنجا حساب جاری دارد با پروتکل پرداخت کوآنتومی مورد تایید قرار می‌گیرد و بانک پرداخت را در تاریخ معین شده تضمین می‌نماید. در پروتکل پرداخت کوآنتومی جزئیات متعددی در نظر گرفته می‌شود از جمله اسم صاحب چک، لیست ناخوانای اقلام خرید، مقدار پول، تاریخ و اسم دریافت کننده چک. اسم صاحب و دریافت کننده چک، رشته‌های دودویی با طول مشخص هستند. همچنین می‌توان آن‌ها را با شماره حساب هایشان جایگزین نمود. با این وجود این وظیفه بانک است که هویّت صاحب چک و دریافت کننده آن را در لحظه تراکنش شناسایی کند. وجود لیست اقلام خرید در چک کوآنتومی مزیت‌هایی را به همراه دارد به ویژه برای خاتمه دادن به اختلافات احتمالی میان صاحب چک و دریافت کننده آن ممکن است سودمند واقع شود. با

۱ Zeng
۲ Entangled
۳ Wen
۴ Quantum key distribution
۵ Qucheque

این حال بانک نباید قادر به خواندن آن باشد تا حریم خصوصی هر دو شخص حفظ شود. این مطلب که بانک نباید از اقلام خرید و فروش شده باخبر شود ضروری است زیرا در غیر این صورت می‌تواند به تجارت آن ها صدمه بزند. مقدار پول و تاریخ، هردو رشته‌های دودویی و قابل رویت توسط بانک هستند.

امنیت پرداخت کوآنتومی توسط کیوبیت، یعنی اشیاء کوآنتومی تامین می‌شود به طوری که اطلاعات کلاسیک پرداخت کوآنتومی درون کیوبیت‌های آن، که از این به بعد آن را چک کوآنتومی می‌نامیم، کدگذاری می‌شوند. ویژگی‌های امنیتی زیر برای پرداخت کوآنتومی ضروری است:

- چک کوآنتومی را نمی‌توان تکثیر نمود. تنها بانک به عنوان یک موسسه معتمد اجازه دارد یک چک کوآنتومی معتبر را پیرو درخواست صاحب چک تولید نماید.
- هیچکس قادر نیست در یک چک کوآنتومی معتبر که توسط بانک مجاز تولید شده دخل و تصرف کند. هر نوع دستکاری چک کوآنتومی را نامعتبر می‌سازد.
- لیست کالاها یا خدمات تراکنش برای بانک، یعنی صادرکننده چک کوآنتومی پوشیده است. آگاهی شخص سوم از اقلام هر تراکنش می‌تواند اطلاعات زیادی در رابطه با فرد انجام دهنده تراکنش از جمله مکان، شرکت و سبک زندگیش فاش نماید. با این حال امکان آشکار کردن لیست در هنگام بروز اختلاف وجود دارد.
- شخص دریافت کننده و بانک قادر هستند اعتبار چک کوآنتومی را بررسی کنند بدون آن که به آن آسیب برسانند. دریافت کننده چک کوآنتومی را بررسی می‌کند و درصورتی که معتبر باشد اقلام خواسته شده را برای خریدار ارسال می‌نماید. همچنین بانک چک کوآنتومی را از دریافت کننده آن تحویل می‌گیرد و درصورت اعتبار آن، مقدار پول ضمانت شده را به او می‌پردازد.
- چک کوآنتومی تنها برای یک مرتبه قابل استفاده است. به همراه آن شماره سریالی وجود دارد که پس از نقد شدن منقضی می‌شود. این شماره سریال توسط بانک صادر کننده تولید و رهگیری می‌شود و از سرقت یا پرداخت مجدد جلوگیری می‌کند.
- بانک قادر است تا تحت شرایط خاصی هویّت هر دو شخص صاحب و دریافت کننده چک کوآنتومی را شناسایی کند.

شکل ۱ نمونه‌ای از یک تراکنش انجام گرفته توسط پرداخت کوآنتومی را نشان می‌دهد. در این مثال سه شخص حضور دارند: مشتری که برای خرید کالا پول پرداخت می‌کند، فروشنده که در ازای دریافت پول کالا یا خدماتی را عرضه می‌نماید و بانک که تراکنش مالی را انجام می‌دهد. به منظور سادگی فرض می‌کنیم که هردو مشتری و فروشنده در یک بانک مشترک حساب دارند. با این حال این امکان برایشان وجود دارد تا با بانک‌های مختلفی کار کنند. مشتری لیست محصولات را برای مثال از تارنمای فروشنده دریافت می‌کند. سپس از فروشنده یک بلیت درخواست می‌کند و در وجه او یک چک دیجیتالی صادر می‌کند که شامل اطلاعات اسم دریافت کننده، لیست ناخوانای اقلام خرید، تاریخ و کل مبلغ است. پس از آن مشتری از بانک مربوطه درخواست صدور یک چک کوآنتومی می‌نماید. بانک پس از بررسی حساب مشتری و در صورت داشتن اعتبار مالی کافی، یک چک کوآنتومی برای او تولید و به او تحویل می‌دهد. در مرحله بعدی مشتری چک کوآنتومی تولید شده را به دست فروشنده می‌دهد و در صورتی که فروشنده صحت چک کوآنتومی را بررسی کرد می‌تواند اقلام خواسته شده را از او تحویل بگیرد. در نهایت فروشنده چک کوآنتومی را به بانک می‌برد و پول دریافت می‌نماید. همزمان بانک چک کوآنتومی را به منظور جلوگیری از پرداخت مجدّد باطل می‌کند.

دو روش را می‌توان برای استفاده از چک کوآنتومی تصوّر کرد. اگر فناوری‌ای وجود داشته باشد که بتوان حالت‌های کوآنتومی را روی کاغذ چاپ کرد، در این صورت این امکان وجود خواهد داشت که برای ارتقای امنیت چک‌های کاغذی در مقابل جعل از رویکرد چک کوآنتومی استفاده کرد. پیشنهاد دیگر این است که شاید مردم بتوانند تجارت خود را با استفاده از چک کوآنتومی و از طریق کامپیوتر کوآنتومی شخصی یا روی اینترنت کوآنتومی انجام دهند. این ابتکارات نیز پیش‌تر در پروتکل پول کوآنتومی در سال ۲۰۱۰ پیشنهاد شده‌اند [۱۵].

مفاهیم کوآنتومی بنیادین در پروتکل پیشنهادی

امروزه پروتکل‌های رمزنگاری جدید یا بهینه‌ای را می‌توان به کمک حالت‌های کوآنتومی برای حفاظت از اطلاعات کلاسیک به وجود آورد [۱۶]. اندازه‌گیری کوآنتومی در ریشه‌ای ترین قسمت پروتکل پیشنهادی ما جای می‌گیرد. قبل از تشریح طرح پیشنهادی لازم است در این‌جا پاره‌ای از تئوری‌های پایه‌ای اندازه‌گیری در مکانیک کوآنتومی را شرح دهیم. براساس تئوری اندازه‌گیری کوآنتومی، اندازه‌گیری با یک مشاهده پذیر A از حالت کوآنتومی Q در وضعیت $|\psi\rangle$ ویژه مقادیر a_i را با احتمال $\|P_{a_i}|\psi\rangle\|^2=\langle\psi|P_{a_i}|\psi\rangle$ تولید می‌نماید و وضعیت سیستم کوآنتومی Q را به حالت $\frac{P_{a_i}|\psi\rangle}{\sqrt{\langle\psi|P_{a_i}|\psi\rangle}}$ می‌برد که در ویژه فضای V_{a_i} قرار می‌گیرد. موضوع اندازه‌گیری کوآنتومی آن‌چنان در میان فیزیک‌دانان داغ است که دیراک بیان کرده است "یک اندازه‌گیری همواره باعث می‌شود که سیستم (مکانیک کوآنتومی) به یک ویژه حالت متغییر دینامیکی که اندازه‌گیری می‌شود جهش کند" [۱۷]. اگر Q یک سیستم کوآنتومی با حالت $|\psi\rangle=\sum_i P_{a_i}|\psi\rangle$ باشد، آنگاه اندازه‌گیری سیستم Q با مشاهده پذیر A حالت سیستم را

به $|\psi'\rangle=\frac{P_{a_j}|\psi\rangle}{\sqrt{\langle\psi|P_{a_j}|\psi\rangle}}$ تغییر خواهد داد و مقدار اندازه‌گیری شده برابر ویژه مقدار a_j با احتمال $\langle\psi|P_{a_j}|\psi\rangle$ است.

شکل ۱. فرایند پرداخت کوآنتومی

در صورتی که اندازه‌گیری بر روی سیستم Q دومرتبه تکرار شود در این صورت نتایج اندازه‌گیری مرتبه دوم دیگر احتمالاتی نخواهد بود و همان ویژه مقدار قبلی a_j را تولید خواهد کرد و سیستم Q همان حالت قبلی را حفظ می‌کند یعنی

$$|\psi'\rangle=\frac{P_{a_j|\psi\rangle}}{\sqrt{\langle\psi|P_{a_j}|\psi\rangle}}$$

یک سیستم کوآنتومی را در نظر بگیرید که حالت‌های کوآنتومی آن در فضای هیلبرت دوبعدی H هستند. در یک چنین فضایی پایه‌های متعامد بسیاری وجود دارند که ما تنها از دوتای آن‌ها به منظور پروتکل پیشنهادی خود استفاده کردیم، پایه های متعامد $\{|0\rangle,|1\rangle\}$ و پایه های قطری $|\pm\rangle$. از این رو با این پایه‌ها چهار حالت کوآنتومی $|0\rangle$، $|1\rangle$، $|+\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ و $|-\rangle=\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ می‌توانند وجود داشته باشند. پایه‌ها به صورت بیشینه مزدوج هستند به این معنی که هر زوج بردار، یکی از هر پایه، به یک اندازه همپوشانی دارد مانند $\|\langle 0|-\rangle\|^2=\frac{1}{2}$. مرسوم است که مقداردودویی '0' به حالت‌های $|0\rangle$ و $|+\rangle$ و مقدار '1' به حالت‌های $|1\rangle$ و $|-\rangle$ تخصیص داده شود و در این صورت به حالت‌ها کیوبیت اطلاق شود.

فرض کنید که سیستم در حالت $|+\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ قرار دارد و ما یک اندازه‌گیری در پایه متعامد $\{|0\rangle,|1\rangle\}$ بر روی آن انجام دهیم. در این صورت حالت اولیه سیستم از بین می‌رود و فرض کنید حاصل اندازه‌گیری $|0\rangle$ باشد. در این صورت در پایه قطری $|\pm\rangle$ حالت کوآنتومی متفاوت خواهد بود زیرا $|0\rangle=\frac{|+\rangle+|-\rangle}{\sqrt{2}}$ برقرار است و تنها ۵۰ درصد این احتمال وجود دارد که حاصل اندازه‌گیری در پایه $|\pm\rangle$ برابر $|+\rangle$ شود. بنابر این حالت به شکل برگشت ناپذیری تغییر کرده است. این مثال یک واقعیت را در فیزیک کوآنتومی نشان می‌دهد و آن این است که اندازه‌گیری در پایه‌های ناسازگار به صورت اجتناب ناپذیری سیستم را برهم می‌زند و اطلاعات ناقصی از حالت پیش از اندازه‌گیری به ما می‌دهد.

از جملات بالا می‌توان دریافت که مکانیک کوآنتومی یک سری قوانین منفی وضع می‌کند که کارهایی غیرقابل انجام را بیان می‌نماید. با این حال، پروتکل پرداخت کوآنتومی پیشنهادی ما از آنها بهره می‌جوید که در لیست زیر این قوانین آمده است:

۱- هیچکس نمی‌تواند بدون آشفته کردن یک سیستم آن را اندازه‌گیری نماید.

۲- هیچکس نمی‌تواند یک کیوبیت را همزمان در پایه‌های متعامد $\{|0\rangle,|1\rangle\}$ و قطری $|\pm\rangle$ اندازه‌گیری کند.

۳- هیچکس نمی‌تواند یک حالت کوآنتومی ناشناخته را تکثیر نماید. این قانون به اسم "تئوری منع تکثیر" [۱۸] مشهور است و بیان می‌کند که یک حالت کوآنتومی ناشناس قابل تولید مثل شدن نیست.

پروتکل پرداخت پیشنهادی

در این قسمت پروتکل پیشنهادی را با جزییات بیشتر و یک مثال کاربردی تشریح می‌کنیم. وضعیتی را تصوّر کنید که در آن سه نفر حضور دارند: مشتری به نام آلیس، فروشنده به نام باب و یک بانک. آلیس قصد دارد کالاهایی را از باب خریداری کند. اما برای او ایده‌آل خواهد بود اگر بتواند لوازم را اول تحویل بگیرد و در آینده هزینه آن را پرداخت نماید. ابتدا او لیست محصولات مورد نیازش به همراه قیمتشان را برای نمونه از طریق بازدید از تارنمای باب به‌دست می‌آورد. آلیس از باب تقاضای یک بلیت می‌کند و آن‌ها بر سر یک تاریخ پرداخت توافق می‌کنند. بلیت یک کلید سرّی مشترک میان آلیس و باب است و برای مخفی کردن لیست اقلام خرید به منظور حفظ حریم خصوصی به کار می‌رود. آلیس و باب برای به اشتراک گذاری بلیت از پروتکل QKD استفاده می‌کنند. آلیس برای اثبات اعتبار مالی خود به باب لازم است که یک چک معتبر برای او ارسال نماید. به همین ترتیب آلیس اطلاعات خرید شامل اسم باب، لیست ناخوانای اقلام خرید، مقدار پول و یک تاریخ مشخص را برای بانک ارسال می‌نماید و این عمل او مشابه نوشتن یک چک کاغذی است. در صورتی که آلیس از توانایی مالی کافی

برای پرداخت چک برخوردار باشد، بانک چک را امضاء می‌نماید و به آلیس برمی‌گرداند. این امضاء بصورت کوآنتومی و غیر قابل جعل یا تکثیر است. سپس آلیس چک امضاء شده را به باب تحویل می‌دهد و پس از آن‌که اصالت چک برای باب مشخص شد، آلیس می‌تواند خرید خود را انجام داده و لوازم مورد نیاز خود را دریافت نماید. در آخر باب می‌تواند چک را به بانک امضاء کننده آن تحویل داده و پول خود را دریافت نماید. بانک نیز چک امضاء شده را بررسی و سپس از اعتبار خارج می‌نماید تا بدین ترتیب از پرداخت مجدد آن جلوگیری شود.

این سناریو تنها یکی از کاربردهای پروتکل پیشنهادی ما را نشان می‌دهد. در ادامه کلّیه مراحل پروتکل پرداخت کوآنتومی شامل پنج گام را شرح می‌دهیم. ازنمادهای زیر برای تشریح پروتکل استفاده شده است:

گشودن حساب بانکی

گام۱-باب تقاضای گشودن یک حساب بانکی می‌کند. بانک اطلاعات شخصی باب شامل اسم کامل، شماره ملی، آدرس و ... را ثبت می‌نماید. به علاوه یک کلید رمز شخصی لازم است تا در بانک به باب تخصیص داده شود.

گام۲- باب و بانک با استفاده از پروتکل QKD بر سر یک کلید شخصی P_b توافق می‌کنند. دقت کنید که P_b یک شماره دودویی n بیتی کاملاً تصادفی است. در حقیقت بانک لیستی از کلیدهای شخصی مشتریان خود دارد و این مسئله درست مشابه ذخیره گذرواژه در بانکداری الکترونیکی است. تنها بانک و باب هستند که از این کلید P_b آگاهی دارند و بنابر این هردو برای محرمانه ماندن آن مسئول هستند.

ایجاد سفارش پرداخت بانکی

گام ۱- آلیس و باب یک کلید دودویی به نام TCK را با استفاده از پروتکل QKD به اشتراک می‌گذارند. استفاده از این کلید برای مخفی‌کردن اقلام تراکنش به منظور حفظ حریم خصوصی است. آلیس و باب تنها افرادی هستند که قادرند این لیست را مشاهده نمایند.

گام ۲- آلیس با استفاده از عملگر یای‌انحصاری لیست اقلام را به شکل کور در می‌آورد، یعنی $\{L\}_{TCK}=L\oplus TCK$. از آنجایی که TCK کاملاً تصادفی است، بازیابی لیست L بدون دانستن TCK امکان پذیر نیست.

گام ۳- آلیس با الحاق کردن اطلاعات پرداخت شامل اسم کامل باب، لیست کور اقلام خرید، مقدار پول، تاریخ پرداخت و شماره بلیت به صورت $CHK=\{N|\{L\}_{TCK}|M|D|I\}$، یک سفارش پرداخت ایجاد می‌کند. فرض بر این است که طول CHK به اندازه n بیت است.

گام ۴- آلیس و بانک بر سر کلید جلسه K_{ac} با استفاده از پروتکل QKD توافق می‌کنند. از این کلید به منظور ارتباط امن میان آن‌ها استفاده می‌شود.

گام ۵- آلیس سفارش پرداخت خود را با کلید K_{ac} و عملگر یای انحصاری به صورت $\{CHK\}_{K_{ac}}=CHK\oplus K_{ac}$ رمز می‌کند و از طریق یک کانال کلاسیک و پروتکل one-time pad برای بانک ارسال می‌کند.

امضای سفارش پرداخت بانکی

گام ۱- بانک سفارش پرداخت آلیس را با استفاده از کلید K_{ac} و عملگر یای‌انحصاری دودویی به صورت $CHK=\{CHK\}_{K_{ac}}\oplus K_{ac}$ رمزگشایی می‌کند و درصورتی که آلیس اعتبار مالی کافی داشته باشد، یک نسخه از آن را به عنوان سفارش پرداخت در پایگاه داده خود ثبت می‌کند.

گام ۲- بانک با درنظر گرفتن P_b و CHK تعداد n کیوبیت مطابق جدول ۱ به صورت $QCHK=[|\psi_1\rangle,|\psi_2\rangle,...,|\psi_i\rangle,...,|\psi_n\rangle]$ تولید می‌کند. توجه کنید که هردو P_b و CHK رشته‌های دودویی به طول n هستند.

گام ۳- بانک $QCHK$ را از طریق یک کانال کوآنتومی برای آلیس ارسال می‌کند.

انجام تراکنش

گام ۱- آلیس از طریق یک کانال کوآنتومی $QCHK$ را برای باب می‌فرستد.

گام ۲- آلیس و باب با استفاده از پروتکل QKD، کلید n بیتی جلسه ای K_{ab} را به اشتراک می‌گذارند.

گام ۳- آلیس با استفاده از K_{ab} درخواست پرداخت خود را رمز می‌کند و $\{CHK\}_{K_{ab}}=CHK\oplus K_{ab}$ را از طریق یک کانال کلاسیک برای باب ارسال می‌کند.

گام ۴- باب $\{CHK\}_{K_{ab}}$ را رمزگشایی می‌کند و $CHK=\{CHK\}_{K_{ab}}\oplus K_{ab}$ را بازیابی می‌نماید. در حقیقت CHK نقش رسید پرداخت برای باب دارد و برای بررسی $QCHK$ لازم است.

گام ۵- مطابق جدول ۲ باب پایه‌های اندازه‌گیری متناسب با بیت-های P_b و CHK را انتخاب و i-امین کیوبیت $QCHK$ را اندازه گیری می‌کند.

گام ۶- درصورتی که همه اندازه‌گیری‌ها نتایج درستی مطابق جدول ۲ داشته باشند، باب رسید پرداخت را به عنوان پول معتبر می‌شناسد در غیر این صورت تراکنش را مردود اعلام می‌نماید.

جدول۱. کدگذاری کیوبیت‌ها با توجه به داده‌های دودویی

شماره	کلید خصوصی (P_{b_i})	سفارش پرداخت (CHK_i)	حالت کیوبیت ($\|\psi_i\rangle$)
۱	0	0	$\|0\rangle$
۲	0	1	$\|+\rangle$
۳	1	0	$\|-\rangle$
۴	1	1	$\|1\rangle$

جدول۲. پایه های اندازه‌گیری و نتایج معتبر

شماره	P_{b_i}	CHK_i	پایه	حالت معتبر
۱	0	0	$\{\|0\rangle,\|1\rangle\}$	$\|0\rangle$
۲	0	1	$\|\pm\rangle$	$\|+\rangle$
۳	1	0	$\|\pm\rangle$	$\|-\rangle$
۴	1	1	$\{\|0\rangle,\|1\rangle\}$	$\|1\rangle$

گام ۷- باب با استخراج $\{L\}_{TCK}$ از CHK و رمزگشایی آن با بلیت TCK به صورت $L=\{L\}_{TCK}\oplus TCK$ لیست اقلام تراکنش را بازیابی می‌کند.

گام ۸- باب اقلام خریداری شده توسط آلیس را پس از تایید رسید پرداخت برای او می‌فرستد.

دریافت پول

گام ۱- باب و بانک به کمک پروتکل QKD یک کلید n بیتی به نام K_{bc} را به اشتراک می‌گذارند.

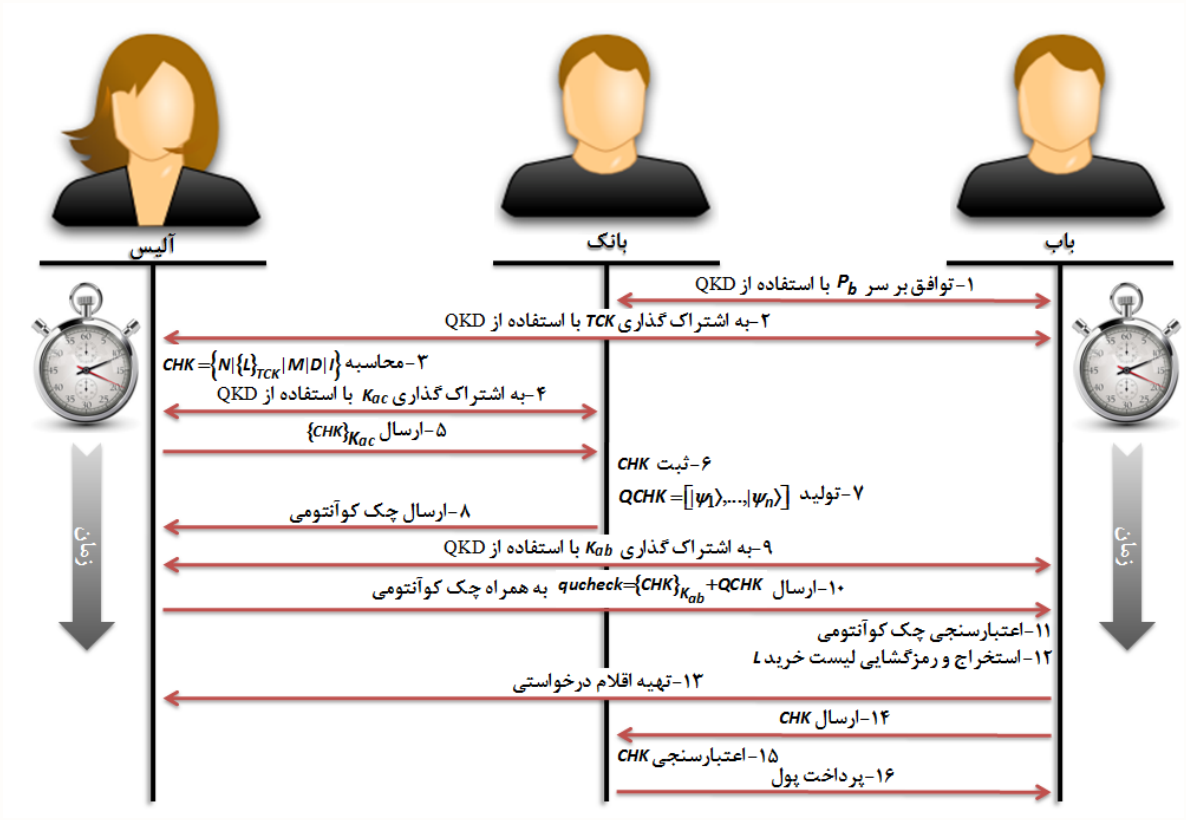
گام ۲- باب CHK را به کمک K_{bc} به صورت $\{CHK\}_{K_{bc}}=CHK\oplus K_{bc}$ رمز می‌کند و برای بانک می‌فرستد.

گام ۳- بانک CHK را به صورت $CHK=\{CHK\}_{K_{bc}}\oplus K_{bc}$ رمزگشایی می‌کند و در پایگاه داده خود به دنبال آن می‌گردد. در صورتی که یک CHK معتبر در پایگاه داده وجود داشته باشد پول مورد نظر به باب پرداخت خواهد شد. سپس به منظور جلوگیری از پرداخت مجدد، CHK ثبت شده در پایگاه داده بانک غیر فعال می‌شود.

لازم به ذکر است که آلیس، باب و بانک به عنوان شرکت کنندگان در این پروتکل هنگام اجرای QKD از پروتکل‌های احراز هویت برای شناسایی یکدیگر استفاده می‌کنند. در غیر این‌صورت هر متخاصمی می‌تواند خود را بجای آن‌ها جا بزند و از این عمل سوء استفاده کند. در حقیقت منابع نسبتاً کمی لازم است تا بتوان کانال کاملاً ناامنی را به یک کانال امن تبدیل نمود. برای نمونه آلیس و باب ممکن است یک پروتکل احراز هویّت که در [۱۹-۲۰] ارائه شده و به یک کلید اولیه کوتاه نیاز دارد مورد استفاده قرار دهند. همان‌طور که در [۲۱-۲۲] نشان داده شده در واقعیت آلیس و باب بجای کلید سرّی کوتاه تنها به اطلاعات تقریبا سرّی و همبسته ضعیف برای شروع نیاز دارند. فرآیند اجرای پروتکل پیشنهادی ما در شکل ۲ نشان داده شده است.

تحلیل امنیت پروتکل پیشنهادی

در این قسمت به بررسی امنیت پروتکل پرداخت کوآنتومی برون خطی می‌پردازیم. نشان خواهیم داد که طرح پیشنهادی ما همه شرایطی را که یک سیستم پرداخت الکترونیک ایده‌آل باید داشته باشد شامل امنیت بالا، کوری، جعل ناپذیری و انکارناپذیری را برآورده می‌نماید. امنیت پروتکل را در حضور شنودگر مجهز به فناوری کوآنتومی بررسی می‌کنیم و همچنین حالت‌هایی را درنظر می‌گیریم که یک یا چند نفر از افراد شرکت کننده رفتار خصمانه-ای از خود بروز دهند و ثابت می‌کنیم که پروتکل پیشنهادی همچنان ایمن باقی می‌ماند.



شکل۲. پروتکل پرداخت برون خطی

مقاومت در برابر حملات کوآنتومی

فرض کنید شنودگری وجود دارد که با پروتکل پیشنهادی به طور کامل آشنا است. مطابق تئوری منع تکثیر [۱۸]، این امکان وجود ندارد تا شنودگر بدون دانستن پایه‌های اولیه که یک کیوبیت در آن ایجاد شده بتواند یک کپی کامل از آن تهیه کند. در نتیجه در این پروتکل هنگامی که دو طرف در حال ارسال کیوبیت برای یکدیگر هستند عمل شنود نمی‌تواند مخفیانه انجام گیرد زیرا به سرعت آشکار خواهد شد [۱۶]. با توجه به این مطلب می‌توان دریافت که شنودگر نمی‌تواند اطلاعات درستی از کیوبیت‌های ارسالی دریافت کند و درنتیجه سفارش پرداخت یعنی CHK را که حاوی اطلاعات پرداخت است کشف نماید. همچنین به دلیل امنیت بالای پروتکل‌های QKD و one-time pad، طرح پرداخت پیشنهادی در برابر حملات intercept-resend و man-in-the-middle مقاوم است [۱۶][۲۳-۲۴]. همان‌گونه که در بخش ۳ ملاحظه شد شنودگر قادر نیست چک کوآنتومی $QCHK$ را اندازه‌گیری و CHK را بدست آورد. زیرا هرگونه اندازه‌گیری در پایه‌های اشتباه، حالت اصلی کیوبیت را برهم زده و نتایج اشتباهی به همراه دارد. با توجه به پروتکل تنها باب و بانک پایه های صحیح اندازه‌گیری را بخاطر دانستن همزمان P_b و CHK دارند.

منع گسترش

در پروتکل پرداخت کوآنتومی برون خطی از تعدادی کیوبیت به همراه یک رشته بیت دودویی به نام سفارش پرداخت تشکیل شده است به گونه‌ای که این دو به صورت متقابل به یکدیگر مربوط هستند. در حقیقت درخواست پرداخت توسط بانک مجاز درون کیوبیت‌ها با حالت‌های کوآنتومی مختلفی کدگذاری شده و بنابر این طبق تئوری منع تکثیر، نمی‌تواند توسط یک شخص غیرمجاز کپی برداری شود. تنها بانک عامل به عنوان یک نهاد مطمئن قادر به ایجاد کپی از آن است. در هر صورت بانک یک نسخه از درخواست پرداخت یعنی CHK را نزد خود ثبت می‌کند.

غیر قابل جعل بودن

حالتی را درنظر بگیرید که پرداخت‌کننده یعنی آلیس قابل اعتماد نباشد و تلاش کند از CHK به منظور جعل $QCHK$ سوء استفاده کند. از قسمت ۴ می‌توان فهمید مطابق کدگذاری جدول ۱، $QCHK$ با CHK همبسته است و بنابراین هرگونه دستکاری در

هرکدام از آن ها منجر به ابطال *QCHK* خواهد شد و در نتیجه باب پس از بررسی آن تراکنش را مردود اعلام می‌نماید. در طرح پیشنهادی همه تبادل داده از طریق QKD و one-time pad انجام می‌شود و بنابراین هیچ فردی قادر به شنود یا دستکاری داده نمی-باشد.

انکارناپذیری

بانک درخواست پرداخت یعنی *CHK* را از آلیس دریافت می‌کند که با کلید K_{ac} رمز شده است و تنها این دو نفر هستند که از این کلید آگاهی دارند. بنابر این بانک یک کپی از *CHK* را در زیرمجموعه حساب آلیس در پایگاه داده خود ثبت می‌کند و آلیس نمی‌تواند درخواست خود مبنی بر پرداخت مالی در آینده را انکار کند. به همین دلیل باب نیز نمی‌تواند دریافت *QCHK* از آلیس را منکر شود.

کوری امضاء

هنگامی که آلیس از باب تقاضای یک بلیت می‌کند، آن‌ها بر سر یک کلید سرّی *TCK* توافق می‌کنند که یک رشته دودویی کاملاً تصادفی است و هیچکس دیگری از محتوای آن اطلاعی ندارد. آلیس با استفاده از عملگر یای‌انحصاری و *TCK* لیست اقلام خریداری شده را به صورت $\{L\}_{TCK}=L\oplus TCK$ ناخوانا می‌کند. با توجه به تصادفی بودن *TCK*، شخص دیگری از جمله بانک عامل حتی با داشتن پردازنده کوآنتومی قادر نیست لیست L را بدون داشتن بلیت *TCK* کشف کند. بنابر این تنها آلیس و باب هستند که قادرند عامل ناخوانایی $\{L\}_{TCK}$ را حذف کنند.

قابلیت اطمینان

بررسی *QCHK* به دقت و کیوبیت به کیوبیت توسط باب انجام می‌شود زیرا بیت‌های دودویی *CHK* درون کیوبیت‌ها مطابق جدول ۱ کدگذاری شده‌اند که یک تناظر یک به یک میان آن‌ها برقرار است. به علاوه، یک متخاصم نمی‌تواند داده‌های کدگذاری شده را دستکاری یا از آن‌ها سوء استفاده نماید. به عبارت دیگر پروتکل پیشنهاد شده در این مقاله قابل اطمینان بوده و برای سیستم‌های پرداخت الکترونیکی مناسب است.

نتیجه‌گیری

در این مقاله یک پروتکل پرداخت الکترونیکی برون خطی جدید ارائه گردید که مبتنی بر قوانین فیزیک کوآنتومی بوده و یک تراکنش کاملاً مطمئن را در برابر کامپیوترهای کوآنتومی تضمین می‌کند. این پروتکل به یک مشتری این امکان را می‌دهد تا یک پرداخت را در آینده ترتیب داده و در عین حال به تعاملات بلادرنگ نیاز نداشته باشد، به این معنی که یک پرداخت برون خطی امکان‌پذیر است. نقطه قوت این پروتکل این است که در آن می‌توان لیست کالاهای خریداری شده را از دید شخص سوم مانند بانک عامل تراکنش مخفی نگاه داشت. با این وجود این لیست را می‌توان در هنگام وقوع یک اختلاف به سادگی فاش کرد. این مطلب در برخی کاربردها ارزشمند است به عنوان نمونه در جلوگیری از کلاه برداری یا پولشویی.

مرجع‌ها

[1]D. Chaum, “Blind signature for untraceable payments,” in: Advances in cryptology, Proc. of CRYPTO’82, Springer, pp. 199–203, 1983.

[2]M. Nikooghadam and A. Zakerolhosseini, “An effcient blind signature scheme based on the elliptic curve discrete logarithm problem,” The ISC Int’l J. of Inf. Security, vol. 1, no. 2, pp. 125–131, 2009.

[3]M. Nikooghadam, A. Zakerolhosseini and M. E. Moghaddam, “Efficient utilization of elliptic curve cryptosystem for hierarchical access control,” The J. of Systems and Software, vol. 83, pp. 1917–1929, 2010.

[4]M. Nielsen and I. Chuang, “Quantum Computation and Quantum Information,” 7th Edition, Cambridge University Press, Cambridge, 2000.

[5]C. Bennett and D. DiVincenzo, “Quantum information and computation,” Nature, vol. 404, pp. 247–255, 2000.

[6]M. Galindo and M. Delgado, “Information and computation: classical and quantum aspects,” Rev. Mod. Phys., vol. 74, pp. 347–423,2002.

[7]G. Zeng, W. Ma, X. Wang and H. Zhu, “Signature scheme based on quantum cryptography,” Acta Electron. Sinica, vol. 29, no. 8, pp. 1098–1100, 2001.

[8]D. Gottesman and I. Chuang, “Quantum digital signatures,” indexed in arXiv.org (2001). arXiv:quantph/0105032v2

[9]X. Wen, X. Niu, L. Ji and Y. Tian, “A weak blind signature scheme based on quantum cryptography,” Opt. Commun., vol. 282, pp. 666–669, 2009.

[1]S. Khodambashi, A. Zakerolhosseini, A sessional blind signature based on quantum cryptography, Quantum Information Processing, vol. 13, no. 1, pp. 121-130, 2014.

[11]www.bbn.com (Sep. 2013).

[12]www.idquantique.com (Sep. 2013).

[13]www.magiqtech.com (Sep. 2013).

[14]C. Gobby and et. al., “Quantum key distribution over 122km standard telecom fiber,” Appl. Phys. Lett., vol. 84, pp. 3762–3764, 2004.

[15]E. Farhi, D. Gosset, A. Hassidim, A. Lutomirski and P. Shor, “Quantum money from knots,” indexed in arXiv.org (2010). arXiv:quantph/1004.5127v1

[16]C. Elliott, D. Pearson and G. Troxel, “Quantum cryptography in practice,” in: SIGCOMM03: Proc. of the Conf. on Apps.,Tech., Arch., and Protocols for Comp. Commun., ACM Press, New York, pp. 227–238, 2003.

[17]P. Dirac, “The principals of quantum mechanics,” 4th Edition, Oxford university press, New York, 1858.

[18]W. Wootters and W. Zurek, “A single quantum cannot be cloned,” Nature, vol. 299, pp. 802–803, 1982.

[19]D. Stinson, “Universal hashing and authentication codes,” in: advances in Cryptology-CRYPTO’91, Vol. 576, LNCS, pp. pp. 74–85, 1991.

[20]P. Gemmell and N. Naor, “Codes for interactive authentication,” in: Advances in Cryptology-CRYPTO’93, Vol. 773, LNCS, pp. 355–367, 1993.

[21]R. Renner and S. Wolf, “Unconditional authenticity and privacy from an arbitrarily weak secret,” in: Advances in Cryptology-CRYPTO’03, Vol. 23, LNCS, pp. 78–95, 2003.
[22]R. Renner and S.Wolf, “The exact price for unconditionally secure asymmetric cryptography,” in: Advances in Cryptology-EUROCRYPT’04, Vol. 3027, LNCS, pp. 109–125, 2004.
[23]R. Renner and U. Maurer, “Security of quantum key distribution,” Ph.D. thesis, Swiss federal institute of technology, Zurich, 2005.
[24]V. Teja, P. Banerjee, N. Sharma and R. Mittal, “Quantum cryptography: state-of-art, challenges and future perspectives,” in: Int. Conf. on Nanotechnology, IEEE, pp. 1296–1301, 2007.