پرداخت کوانتومی با استفاده از امضای کور مضاعف

سیاوش خدام باشی[۱]، جلیل مظلوم[۲]

[۱]استادیار گروه کامپیوتر، واحد یادگار امام خمینی (ره) شهرری، دانشگاه آزاد اسلامی، تهران، ایران، siavashyp@yahoo.com

[۲]دانشیار دانشکده مهندسی برق، دانشگاه علوم و فنون هوایی شهید ستاری، تهران، ایران

چکیده

در این مقاله یک امضای کور مضاعف جهت پرداخت کوانتومی با الهام از ویژگی‌های مکانیک کوانتومی پیشنهاد کرده‌ایم که مشتمل بر سه فاز مقدماتی، امضاء و بررسی است. برخلاف سایر امضاءهای کور، در روش پیشنهادی علاوه بر شخص امضاء کننده، که پیغام را نمی بیند، فرستنده پیغام نیز آن را در هنگام ارسال امضاء می‌نماید. به همین ترتیب در این روش تنها به ناظر در مرحله راستی آزمایی اتکا نمی‌شود و امضای فرستنده پیغام نیز تایید کننده صحت پیغام است. امنیت امضای کور مضاعف به وسیله درهم‌تنیدگی کوانتومی تامین می‌شود. تحلیل‌های امنیتی نشان می‌دهند که پروتکل پیشنهادی توسط فرد حمله کننده و نیز هر یک از افراد اصلی، قابل جعل و انکار نخواهد بود. از امضای کور مضاعف کوانتومی که به کمک فناوری امروزی قابل پیاده سازی است، می‌توان جهت تجارت الکترونیک یا سیستم‌های پرداخت الکترونیکی بهره گرفت.

کلیدواژه

پرداخت الکترونیکی، امضای کور مضاعف، امضای کور کوانتومی، حالت های کوانتومی بل

مقدمه

قوانین فیزیک کوانتومی که حاکم بر دنیای میکروسکوپیک است، شگفتی رمزنگاری کلاسیک را برانگیخته و دریچه‌ای به سوی رمزنگاری جدید گشوده و این امکان را فراهم می‌آورد تا بتوان ارتباطی امن در حضور شنودگران ایجاد کرد [۱]. یکی از چالش‌های رمزنگاری کلاسیک چگونگی احراز هویت یک پیغام است، همچنان که یک امضای دست‌نوشته روی کاغذ می‌تواند منشأ آن را تایید کند. از امضاءهای دیجیتالی به طور گسترده به منظور احراز هویت، یکپارچگی و انکارناپذیری پیغام‌های ارسال شده استفاده می‌شود [۲]. می‌توان دریافت که همه امضاءهای رمزنگاری کلاسیک متّکی به پیچیدگی‌های محاسباتی هستند و بنابراین فقط برای کامپیوترهای کلاسیک سودمند خواهند بود، درحالی که نسبت به کامپیوترهای کوانتومی آسیب‌پذیر هستند. موازی سازی کوانتومی می‌تواند برخی مسائل پیچیده، مانند تجزیه یک عدد بزرگ به عامل‌های اول آن یا مسئله لگاریتم گسسته را بسیار سریع‌تر از کامپیوترهای کلاسیک حل نماید [۳-۴]. به همین دلیل محققین علاقه زیادی به امضاءهای کوانتومی نشان داده‌اند.

اولین امضای کوانتومی توسط ژنگ و همکارانش معرفی گردید که در آن از همبستگی حالت‌های درهم‌تنیده کوانتومی بهره گرفته شد [۵]. گاتسمن و چانگ یک تابع یک طرفه کوانتومی در [۶]ارائه کردند و با استفاده از آن یک امضای دیجیتالی کوانتومی پیشنهاد دادند. اگرچه همه امضاءهای کوانتومی که تا کنون پیشنهاد شده از امنیت مطلق و اعتبار برخوردار هستند، اما حریم خصوصی صاحب پیغام را حفظ نمی‌کنند زیرا ویژگی کور بودن امضاء را ندارند.

امضاءهای کور نوع خاصی از امضاء هستند که در آن‌ها شخص امضاء کننده بدون آنکه از محتوای پیغام مطلع گردد، می‌تواند آن را امضاء کند [۷]. بسیاری از پروتکل‌های رمزنگاری با استفاده از امضاءهای کور محقق شده‌اند. برای نمونه، در سیستم‌های پرداخت الکترونیکی یا رأی‌گیری الکترونیکی از امضاءهای کور به منظور حفظ حریم خصوصی افراد استفاده می‌گردد [۸]. به طور کلی دو نوع امضای کور وجود دارد. نوع اول امضای کور قوی است و دومی امضای کور ضعیف است [۹]. مهمترین ویژگی امضای کور ضعیف این است که از یک شخص مورد اعتماد استفاده می‌کند و بنابراین هویّت دارنده پیغام می‌تواند رهگیری شود. یک امضای کور مطمئن باید شرایط زیر را داشته باشد [۲۲]:

الف) ویژگی کور بودن: امضاء کننده نمی‌تواند از محتویات پیغام در هنگام امضاء کردن آن مطلع گردد.

تاریخ دریافت: ۱۳۹۷/۱۱/۲۷ تاریخ پذیرش: ۱۳۹۹/۰۷/۲۷

ب) غیرقابل جعل بودن: امضاء نباید قابل جعل باشد و پیغام را نمی‌توان پس از امضاء شدن تغییر داد.

ج) غیرقابل انکار بودن. شخص امضاء کننده نمی‌تواند امضای خود را انکار کند. شخص دریافت کننده پیغام علاوه بر شناسایی هویّت امضاء کننده، نمی‌تواند آن را انکار نماید.

ایده اولیه امضای کور کوانتومی توسط وِن و همکارانش در سال ۲۰۰۹ پیشنهاد شد [۹]. با این وجود طرح پیشنهادی آن‌ها نمی‌توانست ویژگی کور بودن امضاء را به خوبی حفظ نماید، زیرا هیچ امضای کور منحصر به فردی برای پیغام کور در طرح پیشنهادی آن‌ها وجود ندارد و بنابراین همچنان که توسط ناصری [۱۰]و سو [۱۱]نشان داده شده است، شخص بررسی کننده امضاء نمی‌تواند اصالت امضای کور را در ۵۰ درصد موارد تایید کند. شی و همکارانش نیز یک امضای کور کوانتومی دسته نمایندگان ارائه کرده‌اند [۱۲]. خدام‌باشی و ذاکرالحسینی نیز با استفاده از حالات درهم‌تنیده EPR توانستند یک امضای کور کوانتومی جلسه‌ای پیشنهاد دهند [۱۳]. همچنین امضاء-های کور کوانتومی متعددی با استفاده از حالت‌های چند ذرّه‌ای درهم‌تنیده تا کنون ارائه شده‌اند[۱۴-۱۵]. در [۱۶] نیز تلاش شده که با تعریف مفهوم جدید چک کوانتومی روشی برای خرید و پرداخت در آینده ارائه شود که از هر دو کانال‌های کوانتومی و کلاسیک جهت ارسال و دریافت استفاده می‌کند و برای یک سناریوی خاص پرداخت آفلاین کاربرد دارد. متاسفانه امضاءهای معرفی شده در سناریویی که در ادامه آمده است ناکارامد هستند زیرا تنها به امضاء کننده کور بسنده می‌کنند و فرستنده پیغام امضاء نمی‌کند. در این مقاله یک پروتکل همه منظوره جهت امضای کور ارائه کرده ایم که علاوه بر امضاء کننده کور، صاحب پیغام نیز پیغام را امضاء می‌نماید تا از این طریق امنیت و یکپارچگی پیغام ارسالی حفظ شود و در عین حال هویّت فرستنده پیغام نیز احراز گردد. فرض کنید باب یک فروشنده است که محصولی را می‌فروشد یا خدمتی را ارائه می-کند و قبل از خرید لازم است که ملاقاتی صورت گیرد. چارلی نیز نماینده بانک است و امضای او به عنوان پول الکترونیکی شناخته می‌شود. آلیس به عنوان خریدار در هنگام خرید، پیغامی را که توسط خویش و چارلی امضاء شده است، برای باب ارسال می‌کند. آلیس با کمک امضای خود هویّت خویش و نیز قابلیت پرداخت خود را توسط امضای چارلی نشان می‌دهد. واضح است که بانک ضمن امضای پول الکترونیکی باید حریم خصوصی مالک پول را در یک تراکنش مالی حفظ کند. به همین خاطر آلیس تمایلی به افشا شدن پیغام محرمانه خود جهت خرید از باب نداشته و چارلی پیغام را به صورت کور امضاء می‌کند. چنین سناریویی معمولاً در تجارت الکترونیکی یا سیستم‌های پرداخت الکترونیکی اتفاق می‌افتد به خصوص هنگامی که شخصی بخواهد مواد مخدر قانونی خریداری کند یا مواردی از این دست. در هر صورت انجام این گونه سناریوها به کمک امضاءهای دیجیتالی موجود به صورت کاملاً مطمئن امکان‌پذیر نیست. برای حل این مشکل در این مقاله یک امضای کور مضاعف جهت پرداخت کوانتومی پیشنهاد می‌نماییم که در آن علاوه بر شخص امضاء کننده یعنی چارلی که به صورت کور پیغام را امضاء می‌کند، فرستنده پیغام یعنی آلیس نیز آن را امضاء می‌نماید. با توجه به بکارگیری مکانیک کوانتومی در پروتکل رمزنگاری امضای کور مضاعف، این امضاء از ماهیّت کوانتومی برخوردار بوده و از ویژگی‌های آن بهره می‌بَرد. تحلیل‌های امنیتی که در این مقاله صورت می‌گیرد نشان خواهند داد که امضای پیشنهاد شده نمی‌تواند توسط یک فرد متخاصم جعل یا توسط افراد امضاء کننده انکار شود. همچنین با استفاده از فناوری‌های موجود، برخی پروتکل‌های کوانتومی مانند توزیع کلید کوانتومی و دورنوردی کوانتومی[1] در شبکه-های ارتباطی نوری به واقعیت پیوسته اند. بنابر این پیاده سازی امضای پیشنهادی این مقاله امکان پذیر خواهد بود.

بخش‌های مختلف ادامه این مقاله به ترتیب زیر آمده است: در بخش دوم، جزییات پرداخت کوانتومی از طریق امضای کور مضاعف بیان شده است. بخش سوم به تحلیل امنیت امضای پیشنهادی می‌پردازد. بخش چهارم توضیحاتی در رابطه با چگونگی پیاده‌سازی امضای پیشنهادی ارائه می‌دهد. در نهایت در بخش پنجم، یک جمع‌بندی مقاله را پایان می‌دهد.

امضای کور مضاعف کوانتومی

امضای کور مضاعف کوانتومی که در این مقاله پیشنهاد می-کنیم مزیّت‌های هر دو امضاء کور و امضاء الکترونیکی معمولی را دارد. این امضاء از سه فاز تشکیل شده است: فاز اولیه، فاز امضاء و فاز بررسی. همچنین سه نفر با نام های آلیس، به عنوان فرستنده پیغام، باب به عنوان دریافت کننده پیغام و چارلی به عنوان شخص ثالث معتمد (نماینده بانک) در فرآیند امضای پیشنهادی فعالیت می‌کنند. آلیس پیغامی را امضاء و به همراه امضای کور چارلی برای باب ارسال می‌نماید. به محض اینکه باب پیغام را دریافت کند، ابتدا امضاءهای آلیس و چارلی و سپس یکپارچگی پیغام را بررسی می‌نماید تا مطمئن شود که پیغام ارسالی دست‌نخورده است. بنابراین همه شرکت کنندگان باید مطابق آنچه که در شکل۱ نشان داده شده است مراحل امضاء را انجام دهند.

[1] Quantum teleportation

فاز اولیه:

در این مرحله یک سیستم چند فوتونی درهم تنیده کوانتومی تشکیل می شود که کلیدهای مطمئن برای امضای کور مضاعف را تولید و توزیع می‌نماید.

گام۱-۱: آلیس و باب با استفاده از پروتکل‌های مرسوم توزیع کلید کوانتومی (QKD) مانند BB84 یا EPR [۱۷] یک کلید کوانتومی K_{AB} به اشتراک می‌گذارند. به روش مشابه نیز چارلی و باب هم یک کلید کوانتومی مشترک K_{CB} تولید می‌نمایند.

گام۱-۲: پس از درخواست امضای آلیس، چارلی یک رشته دودویی n بیتی به صورت تصادفی تولید می‌کند به طوری که دنباله $T=\{t_1,t_2,...,t_n\}$ که در آن $t_i\in\{0,1\}$ است، حاصل شود. چارلی مقدار T را به عنوان یک سند در پایگاه داده خود ذخیره می‌نماید.

گام۱-۳: چارلی بر اساس رشته دودویی T، یک دنباله n کیوبیتی به صورت $|R\rangle=\{|r_1\rangle,|r_2\rangle,...,|r_n\rangle\}$ مبتنی بر ویژه-حالت‌های $\{|0\rangle,|1\rangle\}$ تولید می‌کند به طوری که دنباله $|R\rangle$ نظیر کوانتومی رشته دودویی T خواهد بود .

گام۱-۴: چارلی بر اساس رشته دودویی T و رابطه (۱)، n حالت کوانتومی بل به صورت رشته $|\varphi\rangle=\{|\varphi_1\rangle,|\varphi_2\rangle,...,|\varphi_n\rangle\}$ تولید می‌کند که در آن $i\in\{1,...,n\}$ و اندیس های aو bبه ترتیب کیوبیت‌های اول و دوم حالت بل را نشان می‌دهند.

$$|\varphi_i\rangle=\begin{cases}|\varphi_i^1\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)_{ab} & ;t_i=0\\ |\varphi_i^2\rangle=\frac{1}{\sqrt{2}}\left(|01\rangle+|10\rangle\right)_{ab} & ;t_i=1\end{cases} \qquad (۱)$$

فاز امضاء:

در این مرحله چارلی برای پیغام اولیه $|P\rangle$ یک امضای کور $|S_C\rangle$ و آلیس نیز یک امضاء $|S_A\rangle$ تولید می‌نماید.

گام۲-۱: آلیس یک رشته پیغام به اندازه n کیوبیت تولید می-کند که در این مقاله آن را با $|P\rangle$نشان می‌دهیم. حداقل به دو کپی از پیغام اولیه $|P\rangle$نیاز است، یکی برای تولید پیغام محرمانه $|M\rangle$و دیگری برای ترکیب شدن با حالت‌های درهم‌تنیده بل. پیغام اولیه $|P\rangle$را می‌توان به صورت $|P\rangle=\{|p_1\rangle,|p_2\rangle,...,|p_n\rangle\}$ نشان داد که در آن به ازای $\forall i\in\{1,2,...,n\}$، هر کیوبیت $|p_i\rangle$ را می‌توان به صورت $|p_i\rangle=x_i|0\rangle+y_i|1\rangle$ نوشت به طوری که $|x_i|^2+|y_i|^2=1$ صدق کند. به منظور محافظت از محرمانگی پیغام، آلیس با استفاده از کلید K_{AB} و پروتکل کوانتومی رمزگذاری ارائه شده در [۱۸]مطابق رابطه (۲) پیغام رمز شده $|M\rangle$ را تولید می‌نماید به طوری که $|p_i\rangle$ و K^i_{AB} به ترتیب i-اُمین کیوبیت پیغام اولیه $|P\rangle$ و کلید K_{AB} را نشان می‌دهند.

$$|M\rangle=E_{K_{AB}}\left(|P\rangle\right)=\bigotimes_{i=1}^{n}\sigma_x^{K_{AB}^{2i-1}}\sigma_z^{K_{AB}^{2i}}|p_i\rangle \qquad (۲)$$

می‌توان i-اُمین کیوبیت $|M\rangle$را به صورت $|m_i\rangle=a_i|0\rangle+b_i|1\rangle$ نشان داد به طوری که رابطه $|a_i|^2+|b_i|^2=1$ برقرار است. سپس آلیس پیغام رمز شده $|M\rangle$ را به چارلی ارسال کرده و از او درخواست امضاء می‌نماید.

گام۲-۲: چارلی روی کیوبیت‌های پیغام رمز شده $|M\rangle$به عنوان هدف، یک گیت کوانتومی CNOT اعمال می‌کند به طوری که در ورودی کنترلی گیت، کیوبیت‌های $|R\rangle$را قرار می‌دهد. بر حسب وضعیت کیوبیت‌های $|R\rangle$، نتیجه به صورت یکی از حالات زیر خواهد بود:

$$|0\rangle_r\left(a_i|0\rangle+b_i|1\rangle\right)_m\rightarrow|0\rangle_r\left(a_i|0\rangle+b_i|1\rangle\right)_{m'} \qquad (۳)$$

$$|1\rangle_r\left(a_i|0\rangle+b_i|1\rangle\right)_m\rightarrow|1\rangle_r\left(a_i|1\rangle+b_i|0\rangle\right)_{m'} \qquad (۴)$$

که اندیس های r و m' به ترتیب کیوبیت‌های $|R\rangle$و $|M'\rangle$را نشان می‌دهند و $|M'\rangle$بیانگر کیوبیت خروجی گیت کوانتومی CNOT است که به صورت رشته $|M'\rangle=\{|m'_1\rangle,|m'_2\rangle,...,|m'_n\rangle\}$ به دست می‌آید.

گام۲-۳: چارلی امضای کور را از طریق رمز کردن $(|M'\rangle,T)$ توسط کلید K_{CB}به صورت رابطه (۵) تولید می‌نماید.

$$|S_C\rangle=E_{K_{CB}}\left(|M'\rangle,T\right) \qquad (۵)$$

گام۲-۴: چارلی یک کیوبیت از هرکدام از حالت‌های بل (a_i) را به آلیس و کیوبیت دیگر (b_i) را به باب ارسال می‌کند. همچنین چارلی هردو $|S_c\rangle$و $|M\rangle$را برای باب می‌فرستد.

گام۲-۵: آلیس پس از دریافت همه کیوبیت‌های a_i، هریک از آن‌ها را با $|P\rangle$متناظر ترکیب و اندازه‌گیری می‌نماید. با توجه به اینکه از ترکیب آن‌ها یک سیستم درهم‌تنیده سه کیوبیتی شامل a_iوb_iاز حالت‌های بل و کیوبیت پیغام $|p_i\rangle$به وجود می‌آید، نتیجه اندازه‌گیری به صورت رابطه‌های (۶) و (۷) خواهد بود که $\{|\psi^+\rangle,|\psi^-\rangle,|\phi^+\rangle,|\phi^-\rangle\}$چهار حالت بل را نشان می‌دهند و اندیس‌های p ، a و b کیوبیت‌های مربوطه را نشان می‌دهند. کیوبیت‌های p و a توسط آلیس و کیوبیت-های b توسط باب نگهداری می‌شوند.

گام۲-۶: آلیس روی زوج کیوبیت‌هایی که در اختیار دارد اندازه‌گیری بل انجام می‌دهد که حاصل آن به صورت $|J\rangle=\{|j_1\rangle,|j_2\rangle,...,|j_n\rangle\}$است به طوری که $|j_i\rangle\in\{|\psi^+\rangle,|\psi^-\rangle,|\phi^+\rangle,|\phi^-\rangle\}$برقرار است. سپس آلیس $|J\rangle$را با کلید K_{AB}رمز کرده و $|S_A\rangle$را به عنوان امضایش برای پیغام $|P\rangle$تولید می‌کند، یعنی $|S_A\rangle=E_{K_{AB}}(|J\rangle)$. در نهایت آلیس امضایش یعنی $|S_A\rangle$را برای باب ارسال می‌نماید.

$$\begin{aligned}\left|\phi_i^1\right\rangle &= \left|p_i\right\rangle \otimes \left|\varphi_i^1\right\rangle \\ &= \left(x_i\left|0\right\rangle + y_i\left|1\right\rangle\right)_p \otimes \tfrac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right)_{ab} \\ &= \frac{1}{2}\Big\{\left|\psi^+\right\rangle_{pa}\left(x_i\left|0\right\rangle + y_i\left|1\right\rangle\right)_b + \\ &\quad \left|\psi^-\right\rangle_{pa}\left(x_i\left|0\right\rangle - y_i\left|1\right\rangle\right)_b + \\ &\quad \left|\phi^+\right\rangle_{pa}\left(x_i\left|1\right\rangle + y_i\left|0\right\rangle\right)_b + \\ &\quad \left|\phi^-\right\rangle_{pa}\left(x_i\left|1\right\rangle - y_i\left|0\right\rangle\right)_b\Big\}\end{aligned} \quad (۶)$$

$$\begin{aligned}\left|\phi_i^2\right\rangle &= \left|p_i\right\rangle \otimes \left|\varphi_i^2\right\rangle \\ &= \left(x_i\left|0\right\rangle + y_i\left|1\right\rangle\right)_p \otimes \tfrac{1}{\sqrt{2}}\left(\left|01\right\rangle + \left|10\right\rangle\right)_{ab} \\ &= \frac{1}{2}\Big\{\left|\psi^+\right\rangle_{pa}\left(x_i\left|1\right\rangle + y_i\left|0\right\rangle\right)_b + \\ &\quad \left|\psi^-\right\rangle_{pa}\left(x_i\left|1\right\rangle - y_i\left|0\right\rangle\right)_b + \\ &\quad \left|\phi^+\right\rangle_{pa}\left(x_i\left|0\right\rangle + y_i\left|1\right\rangle\right)_b + \\ &\quad \left|\phi^-\right\rangle_{pa}\left(x_i\left|0\right\rangle - y_i\left|1\right\rangle\right)_b\Big\}\end{aligned} \quad (۷)$$

فاز ارزیابی:

باب از رویکردی برای ارزیابی امضای آلیس، یعنی $\left|S_A\right\rangle$و امضای کور چارلی، یعنی $\left|S_C\right\rangle$استفاده می‌کند. همچنین باب می‌تواند اصالت پیغام ارسال شده $\left|P\right\rangle$را اعتبار سنجی نماید.

گام۳-۱: باب $\left|S_C\right\rangle$ را با استفاده از کلید K_{CB} رمزگشایی کرده و $\left|M'\right\rangle$ و T را بازیابی می‌نماید. سپس باب مطابق عملیاتی که در اینجا ذکر شده است، اصالت $\left|S_C\right\rangle$ را بررسی می‌کند. اگر $t_i = 1$ باشد، باب عملگر یکتایی σ_x را روی i-اُمین کیوبیت $\left|M'\right\rangle$اعمال می‌کند و بدین گونه $\left|M''\right\rangle$را به دست می‌آورد. در شرایطی که $\left|M''\right\rangle = \left|M\right\rangle$ باشد امضای چارلی برای پیغام، معتبر خواهد بود. در این حالت باب می‌تواند به ادامه بررسی امضای آلیس بپردازد.

گام۳-۲: باب $\left|S_A\right\rangle$و $\left|M\right\rangle$را با استفاده از کلید K_{AB} رمزگشایی کرده و $\left|J\right\rangle$و $\left|P\right\rangle$را ذخیره‌سازی می‌نماید. باب سپس مطابق مقادیر t_iو $\left|j_i\right\rangle$، یک تبدیل Uروی کیوبیت b_iکه از چارلی دریافت می‌نماید اعمال می‌کند. جدول۱ چگونگی عملگر Uرا توضیح می‌دهد که در آن نمادهای I، σ_x و σ_z نشانگر ماتریس‌های پائولی هستند. به عنوان نمونه اگر $t_i = 0$ و $\left|j_i\right\rangle = \left|\psi^+\right\rangle$ باشد، باب عملگر I را روی کیوبیت b_i اجرا می‌نماید.

گام۳-۳: پس از به کار گیری عملگر U، باب $\left|P'\right\rangle = \{\left|p_1'\right\rangle, \left|p_2'\right\rangle, ..., \left|p_n'\right\rangle\}$ را به دست می‌آورد که در آن $\left|p_i'\right\rangle = x_i'\left|0\right\rangle + y_i'\left|1\right\rangle$ و $\left|x_i'\right|^2 + \left|y_i'\right|^2 = 1$ برقرار است.

گام۳-۴: باب یکپارچگی پیغام $\left|P\right\rangle$را از طریق مقایسه $\left|P'\right\rangle$و $\left|P\right\rangle$بررسی می‌کند. در صورتی که $\left|P\right\rangle = \left|P'\right\rangle$برقرار باشد، باب $\left|S_A\right\rangle$را به عنوان امضای معتبر برای پیغام می‌پذیرد، در غیر این صورت آن را فاقد اعتبار می‌داند.

تحلیل امنیت

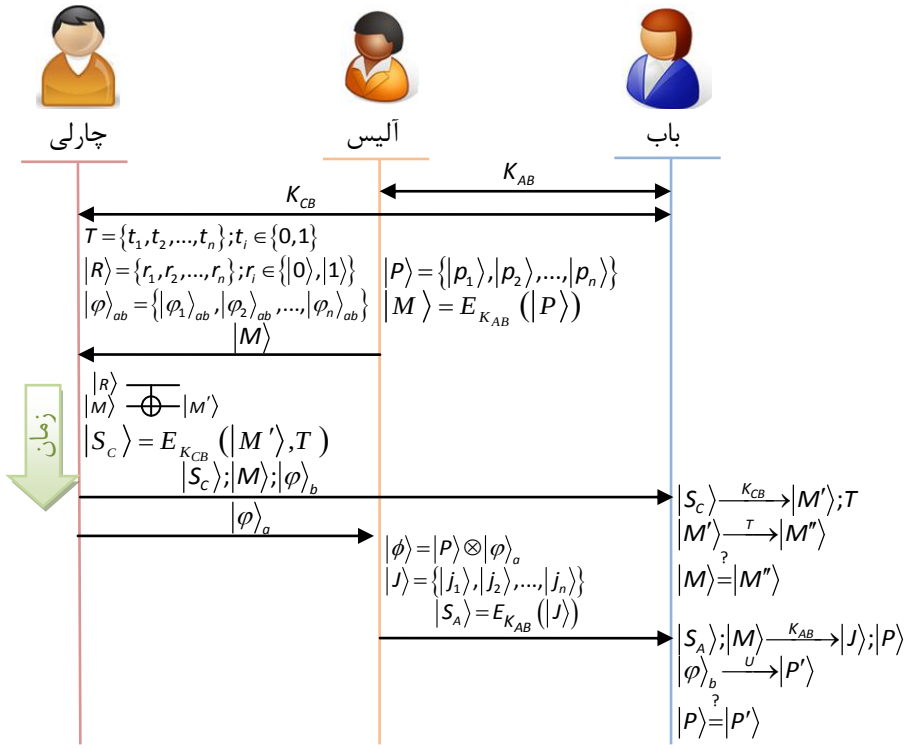
در این قسمت از مقاله به ارزیابی امنیت امضای کور پیشنهادی بر اساس آنچه در قسمت مقدمه ذکر شد می‌پردازیم. با توجه به کور بودن امضاء و اینکه فرد امضاء کننده نباید از محتوای پیغام آگاه شود بنابر این فرستنده پیغام، یعنی آلیس پیغام رمز شده $\left|M\right\rangle$را بجای $\left|P\right\rangle$برای چارلی ارسال می‌کند. از آنجایی که کلید K_{AB} تنها توسط آلیس و باب با کمک الگوریتم QKD به اشتراک گذاشته شده، چارلی نمی‌تواند کلید K_{AB}را به دست آورده و پیغام $\left|M\right\rangle$را رمزگشایی نماید. بنابر این چارلی به هنگام امضاء از محتوای پیغام $\left|P\right\rangle$اطلاعی ندارد. در ادامه به بررسی تحلیل امنیت امضای کور پیشنهادی در برابر جعل، انکار و شنود در کانال‌های کوانتومی غیر ایده آل می‌پردازیم.

غیر قابل جعل بودن امضاء

بیایید فرض کنیم که آلیس، باب یا هر شخص دیگری مثل شنودگر بخواهد تلاش کند تا امضای کور چارلی $\left|S_C\right\rangle$را جعل نماید. نظر به اینکه کلید K_{CB}با استفاده از پروتکل QKD توزیع شده است، لذا بجز دو فرد قانونی باب و چارلی، هیچ شخص دیگری نمی‌تواند آن را به دست آورد. پس آلیس و شنودگر نمی‌توانند K_{CB}را داشته باشند.

جدول۱. انتخاب عملگر یکتایی باب (U)

رشته دودویی چارلی T	نتیجه اندازه گیری آلیس $\left\|J\right\rangle$	عملگر باب U
$t_i = 0$	$\left\|\psi^+\right\rangle$	I
	$\left\|\psi^-\right\rangle$	σ_z
	$\left\|\phi^+\right\rangle$	σ_x
	$\left\|\phi^-\right\rangle$	$\sigma_z\sigma_x$
$t_i = 1$	$\left\|\psi^+\right\rangle$	σ_x
	$\left\|\psi^-\right\rangle$	$\sigma_z\sigma_x$
	$\left\|\phi^+\right\rangle$	I
	$\left\|\phi^-\right\rangle$	σ_z



شکل۱. مراحل امضای کور مضاعف جهت پرداخت کوانتومی

توجه کنید که امضای کور $|S_C\rangle$ شامل رشته دودویی T نیز هست که توسط چارلی تولید و در پایگاه داده او ذخیره شده است. حتی اگر باب کلید K_{CB} را بداند نمی‌تواند امضای $|S_C\rangle$ را جعل کند زیرا او نمی‌تواند یک T معتبر تولید کند. به همین دلیل جعل امضای کور $|S_C\rangle$ توسط شنودگر، آلیس و باب امکان پذیر نخواهد بود.

در سناریو ای دیگر فرض کنیم که شنودگر تلاش می‌کند تا امضای آلیس $|S_A\rangle$ را جعل نماید. مشابه تحلیل قبلی شنودگر نمی‌تواند کلید K_{AB} را سرقت کند. درضمن شنودگر نمی‌تواند کیوبیت‌های a_i را به دست آورد زیرا حالت‌های بل توسط چارلی تولید و توزیع شده اند و شنودگر از نتایج اندازه‌گیری بل $|J\rangle$ که در امضای $|S_A\rangle$ وجود دارد بی‌اطلاع است. در بدترین حالت حتی اگر شنودگر کلید K_{AB} را به دست آورد، جعل امضای آلیس به راحتی در فاز ارزیابی آشکار خواهد شد. فرض کنیم شنودگر با انتخاب حالت‌های بل $\{|\psi^+\rangle,|\psi^-\rangle,|\phi^+\rangle,|\phi^-\rangle\}$ به طور تصادفی $|J'\rangle$ را تولید کرده و مشابه آلیس فرایند امضاء را انجام دهد. تا اینجا او توانسته اندازه‌گیری آلیس را مطابق جدول۱ انجام دهد. اما در نهایت به جعل امضای چارلی موفق نخواهد شد زیرا امکان جعل رشته دودویی T که در $|S_C\rangle$ موجود است را ندارد. در حقیقت هرگونه جعل توسط شنودگر نمی‌تواند همبستگی نتایج اندازه-گیری را برقرار کند و احتمال کشف حمله شنودگر در پروتکل پیشنهادی از مقدار $\gamma=1-\left(\frac{1}{4}\right)^{\||J\rangle\|}$ بیشتر است که در این رابطه $\||J\rangle\|$ طول $|J\rangle$ را نشان می‌دهد که برابر طول پیغام $|P\rangle$ است. اگر $\||J\rangle\|$ به اندازه کافی بزرگ باشد، احتمال آشکار سازی به ۱.۰ میل می‌نماید در نتیجه جعل امضای آلیس برای شنودگر بسیار سخت خواهد بود.

آلیس نمی‌تواند پیغام خود را پس از آنکه توسط چارلی امضاء شد، تغییر دهد. زیرا آلیس در ابتدای پروتکل، پیغام رمز شده $|M\rangle$ را برای چارلی ارسال می‌کند و در نهایت امضای چارلی با پیغام رمزشده همبسته است. چنانچه آلیس پیغام خود را در گام۲-۵ تغییر دهد، به هنگام فاز ارزیابی در گام۳-۴ $|P\rangle\neq|P'\rangle$ خواهد شد و بنابراین به عنوان پیغام و امضای معتبر تشخیص داده نمی‌شوند.

غیرقابل انکار بودن امضاء

در فاز امضاء، آلیس و چارلی همزمان پیغام را امضاء می‌نمایند. از آنجایی که پروتکل پیشنهادی مبتنی بر QKD و وابسته به رمزنگاری کوانتومی بوده و امنیت مطلق را برای کلیدهای توزیع شده به همراه می‌آورد، چارلی به عنوان یک فرد مورد اعتماد نمی‌تواند امضای خویش را انکار کند زیرا $|S_C\rangle$ شامل کلیدهای K_{CB}، T و $|M'\rangle$ است. به روش مشابه، امضای $|S_A\rangle$ شامل کلید K_{AB} و نتایج اندازه‌گیری کیوبیت‌های a_i که همگی متعلق به آلیس هستند و بنابراین آلیس نمی‌تواند منکر امضای خود شود. به همین ترتیب باب نیز نمی‌تواند امضایی را که دریافت می‌کند تکذیب نماید زیرا در فاز ارزیابی به کیوبیت‌های b_i از طرف چارلی احتیاج دارد که منشاء این کیوبیت‌ها از حالت‌های درهم‌تنیده بِل هستند. با توجه به آنچه بیان گردید، هیچ کدام از آلیس و چارلی نمی‌توانند امضاءهایشان را انکار کنند و باب نیز نمی‌تواند امضایی را که دریافت کرده تکذیب نماید.

مقاوم در برابر حملات شنودگر

در کانال‌های کوانتومی غیر ایده آل، یک شنودگر ممکن است با استفاده از درهم‌تنیده کردن یک کیوبیت فرعی با فوتون‌های ارسالی بخواهد حمله ارسال-دریافت[۲] را اجرا کند. به منظور پیشگیری از این نوع حمله و ارتقای امنیت امضای کور مضاعف پیشنهادی لازم است که فاز بررسی شنود نیز به فرآیند پروتکل اضافه گردد. برای روشن شدن مطلب کیوبیت‌های b_i که از چارلی به باب ارسال می‌گردد را در نظر بگیرید. قبل از ارسال b_i به باب، چارلی باید کیوبیت‌های طعمه را که هریک در یکی از حالت‌های $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ است، آماده کند به طوری که رابطه $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ برقرار است. چارلی سپس کیوبیت‌های طعمه را به طور تصادفی انتخاب و در لابلای دنباله کیوبیت‌های b_i قرار داده و محل و حالت آن‌ها را ثبت می‌نماید. پس از دریافت کیوبیت‌های b_i چارلی محل و حالت کیوبیت‌های طعمه را اعلام می‌نماید تا باب بتواند با پایه صحیح آن‌ها را اندازه‌گیری و نتیجه را با حالت اولیه چارلی مقایسه کند. در صورتی که نرخ خطا از مقدار آستانه‌ای بیشتر شود چارلی و باب این ارتباط را قطع کرده و ارسال کیوبیت‌های b_i را مجدداً از سر می‌گیرند تا به نرخ خطای قابل قبول برسند. به محض تکمیل ارسال، چارلی و باب به مرحله بعدی فرایند امضاء اقدام می‌نمایند.

[2] Intercept-resend

در این قسمت چگونگی آشکار شدن حمله شنودگر را در فاز بررسی شنود نشان می‌دهیم. تصور کنید شنودگر دنباله e_i از کیوبیت‌های $|0\rangle$ را ایجاد کرده و از ارسال کیوبیت‌های چارلی به باب یعنی b_i جلوگیری کند. جهت خواندن b_iها شنودگر از یک عملگر CNOT استفاده می‌نماید به طوری که b_i را به عنوان کیوبیت کنترلی و $|0\rangle$ را به عنوان کیوبیت هدف قرار می‌دهد. از آنجایی که شنودگر محل و حالت اولیه کیوبیت‌های طعمه را نمی‌داند بنابر این کیوبیت‌های $|0\rangle$ که توسط شنودگر مهیّا می‌شوند با کیوبیت‌های طعمه و b_i همبستگی پیدا خواهند کرد. پس از این حمله شنودگر b_iها را برای باب ارسال می‌کند. نتیجه عملگر CNOT مطابق روابط (۹-۱۱) چهار حالت خواهد بود که اندیس های d و e به ترتیب کیوبیت‌های طعمه و کیوبیت‌های تولید شده توسط شنودگر یعنی e_i را نشان می‌دهند:

$$|0\rangle_d|0\rangle_e \rightarrow |0\rangle_d|0\rangle_e \qquad (۹)$$
$$|1\rangle_d|0\rangle_e \rightarrow |1\rangle_d|1\rangle_e$$

$$|+\rangle_d|0\rangle_e \rightarrow \tfrac{1}{\sqrt{2}}(|0\rangle|0\rangle+|1\rangle|1\rangle)_{de} = \tfrac{1}{\sqrt{2}}(|+\rangle|+\rangle+|-\rangle|-\rangle)_{de} \qquad (۱۰)$$

$$|-\rangle_d|0\rangle_e \rightarrow \tfrac{1}{\sqrt{2}}(|0\rangle|0\rangle-|1\rangle|1\rangle)_{de} = \tfrac{1}{\sqrt{2}}(|+\rangle|-\rangle+|-\rangle|+\rangle)_{de} \qquad (۱۱)$$

واضح است که اگر کیوبیت‌های طعمه در حالت $\{|0\rangle,|1\rangle\}$ باشند تغییر نخواهند کرد ولی اگر حالت $\{|+\rangle,|-\rangle\}$ باشند باب با احتمال ۰.۵ نتیجه عکس دریافت خواهد کرد. بنابراین حمله شنودگر یقیناً در فاز بررسی شنود آشکار خواهد شد.

پیاده سازی پروتکل پیشنهادی

نظر به اینکه در پروتکل پیشنهادی تنها از پروتکل‌های توزیع کلید کوانتومی QKD و دورجابجایی کوانتومی استفاده شده است و با توجه به عملیاتی شدن هر دو پروتکل کوانتومی، به راحتی می‌توان امضای کور مضاعف را که در این مقاله به منظور پرداخت کوانتومی پیشنهاد شده، پیاده‌سازی کرد. پروتکل QKD این امکان را فراهم می‌آورد که دو نفر یک کلید محرمانه تولید شده به صورت تصادفی را میان خودشان به اشتراک بگذارند به طوری که هیچ فرد سومی از آن مطلع نباشد. از این کلید مشترک در فازهای امضاء و ارزیابی پروتکل پیشنهاد شده در این مقاله استفاده شده است. تا کنون پروتکل‌های QKD متعددی چه به صورت تئوری و چه پیاده سازی شده توسط محققین پیشنهاد گردیده است. برای نمونه در [۱۹] چگونگی

پیاده سازی پروتکل توزیع کلید کوانتومی BB84 روی سیستم ارتباطی نوری توضیح داده شده است. به علاوه یک شبکه ارتباطی امن مبتنی بر توزیع کلید کوانتومی پیاده سازی شده در سطح یک کلان شهر در [۲۰]گزارش شده است. همچنین پیاده‌سازی دور جابجایی کوانتومی نیز در عمل به واقعیت پیوسته است که این امکان را فراهم می‌سازد تا بتوان یک کیوبیت را از مکانی به مکان دیگری بدون جابجایی فیزیکی ذره انتقال داد. ارسال پیغام‌ها به کمک روش دورجابجایی که در بسیاری از پروتکل‌های ارتباطی کوانتومی به شکل‌های گوناگون پیاده سازی شده است، می‌تواند فرآیند فاز ارزیابی در پروتکل پیشنهاد شده در این مقاله را تکمیل نماید. برای مثال در [۲۱]نشان داده شده که استفاده از دورجابجایی کوانتومی در شبکه‌های ارتباطی نوری عملاً امکان‌پذیر است. بر اساس تحلیل‌هایی که در این بخش صورت گرفت و با توجه به اینکه امضای کور مضاعف کوانتومی که در این مقاله پیشنهاد کردیم تنها از پروتکل‌های توزیع کلید کوانتومی QKD و دورجابجایی کوانتومی سود می‌برد، بنابر این پیاده سازی پروتکل پیشنهادی با استفاده از فناوری موجود به صورت بهینه کاملاً امکان پذیر است.

نتیجه گیری

در این مقاله یک روش پرداخت کوانتومی را که از امضای کور مضاعف بهره می‌برد معرفی کردیم که در شبکه‌های ارتباطی کوانتومی قابل استفاده است. برخلاف امضاءهای کور پیشین، ویژگی روش پیشنهاد شده در این مقاله آن است که پیغام نه فقط توسط امضاء کننده کور، بلکه توسط خود صاحب پیغام نیز امضاء می‌گردد تا اصالت پیغام نیز به طور همزمان بررسی شود. امنیت این امضاء به وسیله ذرات کوانتومی درهم‌تنیده بل که میان اعضای اصلی توزیع شده‌اند تأمین می‌گردد. ثابت کردیم که امضای کور کوانتومی پیشنهادی مطمئن بوده و برای سیستم‌های حساس تجارت الکترونیکی و پرداخت الکترونیکی قابل استفاده است.

مراجع

[1] M. Nielsen and I. Chuang, “Quantum computation and quantum information,” Cambridge university press, Cambridge, 2000.

[2] S. Khodambashi and A. Zakerolhosseini, “A quantum blind signature scheme for electronic payments,” The IEEE 22nd Iranian Conference on Electrical Engineering (ICEE2014), pp. 879-884, 2014.

[3] C.H. Bennett, D.P. DiVincenzo, “Quantum information and computation,” Nature vol. 404, pp. 247–55, 2000.

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

[5] 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.

[6] D. Gottesman and I.L. Chuang, “Quantum digital signatures,” URL: http://arxiv.org/abs/quant-ph/0105032v2, 2001.

[7] D. Chaum, “Blind signature for untraceable payments,” Advances in cryptology, proceeding of CRYPTO’82, Springer, New York, pp. 199–203, 1983.

[8] S. Khodambashi and A. Zakerolhosseini, “A weak blind signature based on quantum key distribution,” Journal of computing and security, vol. 1, no. 3, pp. 179-186, 2014.

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

[10] M. Naseri, “Comment on a weak blind signature based on quantum cryptography,” Int. J. Phys. Sci., vol. 6, no. 21, pp. 5051–5053, 2011.

[11] Q. Su, Z. Huang, Q. Wen and W. Li, “Quantum blind signature based on two-state vector formalism,” Opt. Commun., vol. 283, pp. 4408–4410, 2010.

[12] J.J. Shi, R.H. Shi, Y. Guo and et al., “Batch proxy quantum blind signature scheme,” Sci China Inf Sci, vol. 56, 052115(9), 2013.

[13] S. Khodambashi and A. Zakerolhosseini, “A sessional blind signature based on quantum cryptography,” Quant. Inf. Process., vol. 13, pp. 121–130, 2014.

[14] X.F. Zou and D.W. Qiu, “Attack and improvements of fair quantum blind signature schemes,” Quant. Inf. Process., vol. 12, no. 6, pp. 2071-2085, 2013.

[15] S. Khodambashi and A. Zakerolhosseini, “An Electronic Payment Protocol Based on Quantum Key Distribution,” Quantum Matter, vol. 4, no. 6, pp. 1-5, 2015.

[16] S. Khodambashi and A. Zakerolhosseini, “A quantum blind signature scheme for electronic payments,” IEEE 22nd Iranian Conference on Electrical Engineering (ICEE 2014), pp. 879-884, 2014.

[17] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys., vol. 74, pp. 145–195, 2002.

[18] P.O. Boykin and V. Roychowdhury, “Optimal encryption of quantum bits,” Phys. Rev. A, vol. 67, no. 4, pp. 042317, 2003.

[19] Y.S. Kim, Y.C. Jeong and Y.H. Kim, “Implementation of polarization-coded free-space BB84 quantum key distribution,” Laser Physics, vol. 18, no. 6, pp. 810-814, 2008.

[20] D. Stucki, N. Walenta, F. Vannel and et al., “High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres,” New Journal of Physics, vol. 11, no. 7, pp. 075003, 2009.

[21] S. Olmschenk, D.N. Matsukevich, P. Maunz, D. Hayes, L.M. Duan and C. Monroe, “Quantum teleportation between distant matter qubits,” science, vol. 23, pp. 486-489, 2009.

[۲۲] ناصر محمدزاده، رمزنگاری کوانتومی، نشر دانشگاه شاهد، ۱۳۹۴، دانشگاه شاهد تهران.