

**تکنیک کوانتومی برای کنترل دسترسی در محاسبات ابری 2 :**

**رمزگذاری و توزیع کلید**

**چکیده**

این دومین مقاله از مجموعه مقالات مربوط به کنترل دسترسی است که با مشکلات در محاسبات ابری با اتخاذ تکنیک های کوانتومی سروکار دارد. در این مقاله ما کاربرد رمزنگاری کوانتومی و توزیع کلید کوانتومی در دسترسی به مشکل کنترل را مورد مطالعه قرار می­دهیم. طرح رمزنگاری و پروتکل را برای توزیع کلید در تنظیمات مکانیک­های طبقه­بندی شده کوانتوم (CQM) تدوین و فرمولبندی می­کنیم. زبان گرافیکی CQM در این مقاله استفاده می شود. این طرح / پروتکل کوانتومی که پیشنهاد می­کنیم، دارای مزایای متعددی برای طرح­ها / پروتکل­های ارائه شده در حالت هنر برای همان هدف است. آنها از لحاظ اطلاعاتی در فن­آوری کنونی امن و قابل اجرا هستند.

**کلمات کلیدی:** رمزنگاری کوانتومی، توزیع کلید کوانتومی، طبقه­بندی مکانیک کوانتومی، کنترل دسترسی

**1. مقدمه**

این دومین مقاله از مجموعه مقالاتی است که با مسائل کنترل دسترسی در محاسبات ابری با اتخاذ تکنیک کوانتوم سروکار دارد [30]. مدلی ساده برای مسائل کنترل دسترسی در محاسبات ابری، که در شکل 1 نشان داده شده است مانند مالک داده، کاربر داده و ابر. صاحب داده، داده­های رمزگذاری شده (بیت یا کوبیت­ها) را روی ابر قرار می­دهد جائی که در آن کاربر بتواند دسترسی داشته باشد. به محض دریافت درخواست دسترسی به داده از جانب کاربر، مالک داده یک سیاست کنترل دسترسی را به منظور تصمیم­گیری به کار می­برد در مورد این موضوع که کاربر باید به دسترسی نفوذ پیدا کند. پس از آن، اگر سیاست کنترل دسترسی اظهار بر این داشته باشد که دسترسی باید به کاربر داده شود، پس مالک داده کلید مربوطه و تاییدیه را به کاربر ارسال می­کند. در نهایت، به محض تائید موفقیت­آمیز تاییدیه توسط ابر، کاربر تائیدیه را به ابر می­فرستد و داده­های رمزگشایی شده را بدست می­آورد.



شکل 1: دسترسی داده­ها در محاسبات ابری

در اولین مقاله این مجموعه [30]، استدلال ضروری کوانتومی را بعنوان یک زبان رسمی برای مشخص کردن سیاست­های کنترل دسترسی توسعه می­دهیم، که به مالک در تصمیم­گیری اینکه آیا برای دسترسی به کاربر مجوز دهد یا نه کمک می کند. اما چگونه به کاربر دسترسی مطمئن داده می­شود؟ رمزنگاری ابزار مناسبی را برای حل این مشکل ارائه می­کند. بسیاری از راه حل های رمزنگاری برای مشکل اعطای دسترسی پیشنهاد شده است [2، 6، 7، 8، 23، 24]. ایده اصلی این است: ابتدا تمام منابع را رمزگذاری کنید، سپس کلیدهایی را برای رمزگشایی به کاربرانی که اجازه دسترسی دارند اختصاص دهید. بطور دقیق­تر، فرض کنید منابع  را داریم، سپس کلیدی را به یک کاربر اختصاص می­دهیم البته اگر کاربر اجازه دسترسی به آن را داشته باشد. بنابراین، رمزگذاری و توزیع کلید نقش مهمی را در اعطای دسترسی ایفا می­کند. در این مقاله، تکنیک­های کوانتوم برای رمزنگاری و توزیع کلید را با استفاده از چارچوب ماشین­های کوانتوم دسته­بندی شده (CQM) توسعه می­دهیم.

ساختار بقیه این مقاله به شرح زیر است: در بخش 2 دانش پس­زمینه در ماشین­های کوانتوم دسته­بندی شده را ارائه می­کنیم. بنابراین رمزگذاری را با مشاهدات مکملانه در بخش 3 معرفی می­کنیم. در بخش 4 پروتکل کوانتومی خودمان را برای توزیع کلید ارائه می­کنیم. در بخش 5 آثار مرتبط را بحث میکنیم و در بخش 6 مقاله نتیجه­گیری می­شود.

**2. مکانیک کوانتومی طبقه بندی شده**

مکانیک کوانتومی طبقه بندی شده [1، 16، 17، 11، 4، 13، 14] مربوط به مطالعه محاسبات کوانتومی و پایه های کوانتومی با استفاده از نظریه طبقه بندی، همچنین به عنوان زبان گرافیکی نزدیک به موضوع نظریه طبقه بندی شده است. ترکیب بندی سیستم های کوانتومی در CQM به عنوان یک پیوند اولیه قلمداد می­شود که به راحتی با قلاب دسته بندی مونوایدال متقارن († -SMC) توصیف می شود.

**2.1 نظریه دسته ها**

**تعریف 1 (دسته).**A رده C شامل موارد زیر است:

1. مجموعه ob (C) از اشیاء،

2. برای هر جفت اجسام A، B، یک مجموعه C (A، B) از مورفیزم ها،

3. برای هر جسم A، یک مورفیسم باهویت خاص: 1A ∈ C (A، A),

4.عملیات ترکیب ترتیبی برای مورفیسم ها:

◦ : C(B,C) × C(A,B) → C(A,C),

برآورده نمودن شرایط زیر:

(1) ◦ در مورفیسم ها وابسته است: (h ◦ g) ◦ f = h ◦ (g ◦ f)

(2) ◦ در مورفیسم های متحرک است: 1B ◦ f = f = f ◦ 1A، برای همه f ∈ C (A، B).

می­توانیم به صورت گرافیکی اشیا را مانند سیم ها و مورفیسم ها ارائه دهیم وسیم ورودی و سیم خروجی مانند گره­ها به هم متصل می­شوند .این نمودارها از پایین به بالا خوانده می­شوند. در این زبان گرافیکی شرایط ترکیب ترتیبی، یکپارچگی و وابستگی بی اهمیت می­شود.



مثال 1. در FinHilb، که گروه ابعاد محدود فضاهای هیلبرت هستند، اشیاء فضاهای ابعاد محدود فضاهای هیلبرت فراتراز اعداد پیچیده هستند، مورفیسم ها نقشه های خطی هستند. هویت ها عملکرد هویت در هر فضای هیلبرت است. ترکیب ترتیبی ترکیبی از نقشه های خطی است.

تعریف 2(عملگر). فرض کنید C و D دسته بندی شده اند. یک عملگرF: C → D تعریف می­شود با

• برای هر شی A ∈ ob (C) یک شی F (A) ∈ ob (D).

• برای هر مورفیسم f ∈ C (A، B) یک مورفیسم F (f) ∈ D (F (A)، F (B)) اینگونه

F (f ◦ g) = F (f) ◦ F (g) و F (1A) = 1F (A).

تعریف 3 (ایزومورفیسم طبیعی). فرض کنید F، G: C → D عمل گرها باشد. تغییر طبیعی τ: F → G یک خانواده از مورفیسم ها در D، τA ∈ استD (F (A)، G (A))، نشان داده شده توسط اشیاء C می­باشد، به طوری که مربع زیر حرکت می کند:



برای همه مورفیسم ها f ∈ C (A، B). یک ایزومورفیسم طبیعی یک تغییر طبیعی است جایی که هر یک از τA یک ایزومورفیسم هستند. بدین معنا که یک مورفیسم وجود دارد



تعریف 4 (دسته monoidal [11]). یک رده مونوئیدی شامل داده های زیر:

• یک دسته C

• یک شیئ واحد I ∈ ob (C)،

• دوعملگرای -⊗-: C × C → C به طوری که

 1 ⊗ عملیات ترکیب موازی برای اشیاء است:

⊗ : ob(C) × ob(C) → ob(C),

 2. ⊗ عمل ترکیبی موازی برای مورفیسم ها است:

⊗ : C(A,B) × C(C,D) → C(A ⊗ C,B ⊗ D),

 3. ⊗ و ◦ قانون تبادل را برآورده می کند:

(g1 ⊗ g2) ◦ (f1 ⊗ f2) = (g1 ◦ f1) ⊗ (g2 ◦ f2).

4. 1A ⊗ 1B = 1A⊗B

• دو واحد طبیعی ایزومورفیسم



یک ایزومورفیسم وابسته طبیعی



که موضوع معادلات همبستگی مثلث و پنج ضلعی است، که می توان در Coecke و Paquette یافت [15، ص.209].

دو عملگرا ⊗ همچنین محصول تانسور نامیده می شود که به عنوان ترکیب موازی عمل می کند.به صورت گرافیکی بشکل افقی که دو مورفیسم(اشیا) باهم در آن قرار دارد ارائه می­شود. شی واحد به عنوان یک گراف خالی نمایش داده می شود. اینکه همه شرایط دسته مونوئیدی بی اهمیت است می­تواند به راحتی تأیید شود و بطور قطعی در نمایش گرافیکی می­تواند جای گیرد.



مثال 2. FinHilb یک دسته مونوئیدی است. در FinHilb، ترکیب موازی محصول تانسور فضاهای هیلبرت است. I زمینه اعداد پیچیده استC که یک فضای هیلبرت یک بعدی است. ایزومورفیسم های طبیعی چپ و راست به صورت ترتیبی هستند.



ایزومورفیسم طبیعی وابسته :



تعریف 5 (دسته مونوئیدی متقارن [20]). یک دسته مونوئیدی متقارن است اگر با ایزومورفیسم طبیعی به نام مبادله مجهز شده باشد:



تعریف شده برای تمام اجسام A، B، به شرح زیر:



مورفیسم مبادله به صورت گرافیکی به شرح زیر است:



تعریف 6 (عملگرای کاراکتر † [14، 28]). یک عملگرای + مانند برای دسته مونوئیدی متقارن یک عملیات است که به شرح زیر میباشد:

• بر روی اشیاء و مورفیسم­های هویت، تغییری نکرده است: A † = A، 1†

A = 1A،

• مورفیسم ذخیره شده: (f: A → B) †: = f †: B → A،

• غیر قابل قبول است: (f †) † = f،

• و با ساختاردسته بندی مونوئیدی متقارن مرتبط میباشد:



در زبان گرافیکی، اگر کاراکتر+ عملگرا را به یک گراف اعمال کنیم،نمودار بصورت عمودی منعکس میشود.

تعریف 7 (دسته مونوئیدی متقارن کاراکتر+ [14]).یک دسته مونوئیدی متقارن کاراکتر+ († -SMC )یک دسته مونوئیدی متقارن مجهز به کاراکتر می­باشد.

مثال 3. FinHilb یک † -SMC است. در FinHilb، مبادله برای هر فضای هیلبرتA، B یک ایزومورفیسم طبیعی است.



† اپراتور مجاور (ترانزیستور) است.

تعریف 8 (دسته بندی جمعی کاراکتر+ دوگانه) [14]). دسته بندی جمعی کاراکتر + یک † - SMC است که در آن برای هر شی A یک مورفیسم وجود دارد.





بطور گرافیکی، ساختار جمعی ηA و مجاورهای آن η†A به ترتیب بصورت نمای یک فنجان و یک کلاه نمایش می­شود:



فشرده­سازی گرافیکی به صورت زیراست:



در هر رده مونوئیدی C، یک مورفیسم s ∈ C (I، I) اسکالر نامیده می شود که بعنوان یک عدد درک می شود. به صورت گرافیکی، اسکالرها را به عنوان الماس نشان می دهیم:

 0 1

مثال 4. در FinHilb، اسکالرها ی در زمینه اعداد پیچیده C را تشکیل می دهند.

**2.2 جبر Frobenius و قابل مشاهده**

تعریف 9(جبر Frobenius [12]). فرض کنید C یک دسته مونوئیدی باشد. جبر Frobenius بر روی C جسم A با (ضرب، واحد، کپی و حذف) مورفیسم ها همراه است.



معادلات بشرح زیراست:

• وابستگی: m ◦ (m ⊗ 1A) = m ◦ (1A ⊗ m). گرافیکی، وابستگی به شرح زیر تصور می­شود:



• همبستگی: (c ⊗ 1A) ◦ c = (1A ⊗ c) ◦ c. گرافیکی



• یکپارچگی: m ◦ (u ⊗ 1A) = 1A = m ◦ (1A ⊗ u). گرافیکی



• محوریت: (d ⊗ 1A) ◦ c = 1A = (1A ⊗ d) ◦ c. گرافیکی



• شرایط Frobenius : (1A ⊗ m) ◦ (c ⊗ 1A) = c ◦ m = (m ⊗ 1A) ◦ (1A ⊗ c).گرافیکی



تعریف 10 (جبر Frobenius جایگزین [12]). جبر Frobenius وقتی معادلات زیرارائه می شوند، جایگزین می­شود:





تعریف 11 (جبر Frobenius جایگزین کاراکتر+(12)). یک کاراکتر جایگزین جبر Frobenius در یک دسته مونوئیدی متقارن کاراکتر+،جبر Frobenius ی جایگزین است که علاوه بر این معادلات را زیر را بشرح زیر ارائه می­دهد





برای توصیف جبر Frobenius جایگزین کاراکتر+،فقط نیاز به توصیف چندگانه و واحد، و تعریف کپی و حذف توسط عملگر+ داریم.

مثال 5: -SMC FinHilb را در نظر بگیرید، Cn یک شی FinHilb است. براساس وارونورال {| 0، . . ، | n-1} است. توجه داشته باشید که برای مشخص کردن یک نقشه خطی بین فضاهای هیلبرت، فقط نیاز به مشخص کردن عملکرد نقشه بر اساس وارونورال داریم. حالا فرض می­کنیم:



پس  یک جبر Frobeniusجایگزین کاراکتر+ است.

 **3 . رمزگذاری توسط تعریف مشاهدات مکمل**

 12(ساختار قابل مشاهده [11]). یک ساختار قابل مشاهده در a † -SMC یک جبر Frobenius جایگزین کاراکتر+ (A، m، u) است به طوری که m◦m † = 1A.گرافیکی



یک ساختار قابل مشاهده (A، m، u) هنگام تنظیم ηA = m † ◦u یک خود دوگانه ایجاد می کند.



مثال 6: جسم 2C را در FinHilb در نظر بگیرید، فرض کنید m †z:



پس یک ساختار قابل مشاهده است.

مثال 7. برای 2C در FinHilb، فرض کنید



پس  یک ساختار قابل مشاهده است.

مثال8: برای C2 در Fin Hilb فرض کنید





پس  یک ساختار قابل مشاهده است.

تعریف13:یک نقطه قابل کپی.فرض کنیدC یک †-SMCباشد و (A,m, u) یک جبر Frobenius بر روی C.نقطه قابل کپی از یک (A,m, u)یک نقطه p : I → A مانند c ◦ p = p ⊗ p.می­باشد.



تعریف 14 (مشتقات [11]). فرض کنید f: A → B یک مورفیسم باشد. اتصال آنf \*: A → B به صورت زیر تعریف می شود



یک مورفیسم f خودمحور است اگر f = f \*. از لحاظ گرافیکی، اتصال f یک بازتاب افقی از f است بنابراین، مورفیسم خودمحور تحت بازتاب افقی غیر قابل تغییراست.

مثال 9. تعداد / اسکالرها مورفیسم هایی از I تا I هستند. در FinHilb، یک عددمنحصر به فرد خود است اگر که یک عدد واقعی باشد

تعریف 15 (نقاط کلاسیک [11]). با توجه به ساختار قابل مشاهده (A، m، u)یک نقطه p: I → A در این ساختاراگر خودمحور، قابل کپی و u† ◦ p = 1 باشد،کلاسیک است.

مثال 10. برای ساختار قابل مشاهده Oz، | 0 و | 1 | نقاط کلاسیک هستند. برای Ox، | + و - | نقاط کلاسیک هستند. به طور کلی، هر قطر درکروک Bloch یک ساختار قابل مشاهده است و دو نقطه انتهایی قطر نقاط کلاسیک ساختارقابل مشاهده مربوطه هستند.

تعریف 16 (نقاط بی طرف [11]). با توجه به ساختار قابل مشاهده (A، m، u)یک نقطه p: I → A برای این ساختار بی طرف است اگر یک scaler وجود دارد: I → Iبه طوری که s ⊗ (m ◦ (p ⊗ p)) = p.



مثال 11. برای ساختار قابل مشاهده  نقاط بی طرف هستند. به طور کلی، هر نقطه ای بر روی استوا از حوزه Bloch برایOZیک نقطه بی طرف است.مجموعه ای از تمام نقاط بی طرف از یک ساختار قابل مشاهده یک دایره ایجاد می کند که مرکز توپ را می گیرد و بر قطر مربوط به ساختار قابل مشاهده عمود است.



**3.1 تعریف مکمل قابل مشاهده**

 17 (مکمل قابل مشاهده [11]). دو قابل مشاهده (A، M1، U1)و (A، m2، u2) در a † -SMC مکمل است اگر موارد زیر مشروح باشند

• COMP1: هر وقت k: I → A برای (m1، u1) کلاسیک است، برای آن بی طرف است m2 u2•)

• COMP2: هر زمان k: I → A برای (m2، u2) کلاسیک است، برای آن بی طرف است (m1، u1).

هرکوبیت قابل مشاهده (C2، m، u) دارای دو نقطه کلاسیک است. انها را به ترتیب با U و Uنشان می­دهیم.

مثال 12. در FinHilb، برای جسم C2، Ox،Oy و Oz به صورت جفت های مکمل هستند. به طور کلی، هر دو قطر عمود بر کرهBloch نشان دهنده دو مشاهده گر مکمل است.



**3.2 رمزگذاری توسط تغییر فاز براساس مشاهدات مکمل**

Coecke و همکاران [11] نشان دادند که یک تغییر فاز کوبیت­های قابل مشاهده (C2، m، u) برای یک ماتریس، ایزومورفیک است . از S (α) برای نشان دادن تغییر فاز استفاده می کنیم که برای ایزومورفیک است.

برای دومکمل قابل مشاهده ازکوبیت­ها (C2, m1, u1) and (C2,m2, u2),کوبیت­های قابل مشاهده منحصر به فردی وجود دارد (C2, m3, u3) که مکمل هر دو (C2, m1, u1) and (C2,m2, u2). هستند. تغییر فاز از نشان داده می­شود . نتایج کاربرد به در جدول زیر خلاصه می­شود.



جدول 1: رمزگذاری توسط تغییر فاز

یادآوری 1: تغییر فاز یک تعمیم از عملگرای در رایانش منطقی کوانتومی است. . درحقیقت ارائه ماتریس از , است که دقیقا در تغییرات فاز , OX قابل مشاهده است.

تعریف 19 (رمزگذاری توسط مکمل های قابل مشاهده). برای دو مکمل قابل مشاهده شده از کوبیت­ها (C2, m1, u1) and (C2,m2, u2),فرض میکنیم کلید= یک رمزگذاری توسط مشاهدات مکمل یک عملکرد رمزگشایی می­باشد : Key×C2 \_→ C2 که نقشه های یک کوبیت است که S ∈ Key.

همچنین از برای مشخص کردن  استفاده می­کنیم.

تعریف 20 (امنیت اطلاعاتی). یک طرح رمزگذاری اطلاعاتی ایمن است اگر برای هر کوبیت |α> باشد. اگر ما آن را با در نظر گرفتن کلید به توزیع احتمالی یکنواخت در فضای کلیدی {key1،. . . ، keyn}به آن رمزگذاری می کنیم، نتیجه یک حالت کاملا ترکیبی است.یعنی توزیع احتمالی یکپارچه یک حالت کاملا ترکیبی است.

به خوانندگان یادآوری می کنیم که حالت کاملا ترکیبی از یک کوبیت توسط ماتریس  متراکم ارائه می­شود. در توپ Bloch ، حالت کاملا ترکیبی توسط مرکز توپ نشان داده می­شود. برای دوکوبیت قابل مشاهده مکمل (C2، m1، u1) و (C2، m2، u2)، توزیع احتمالی φ بیش از مانند همیشه یک حالت کاملا ترکیبی می­باشد.

قضیه 1 رمزگذاری توسط مشاهدات مکملانه­ی کوبیت­ها از منظر اطلاعاتی امن است.

اثبات: فرض کنید  و  یک جفت اختیاری از مشاهدات مکملانه کوبیت­ها باشند. فرض کنید  فضای خالی ناشی از این جفت از مشاهدات مکملانه باشد.

برای کوبیت  پس از رمزگذاری با مشاهدات مکملانه، یک توزیع احتمالی متحد در طول را بدست می­آوریم، که در کل حالتی ترکیبی میباشد. بصورت مشابه، برای کوبیت  پس از رمزگذاری توشط مشاهدات مکملانه، یک توزیع احتمال متحد در طول  را بدست می­آوریم.

اکنون و را بعنوان اساس کوبیت­ها بگیرید. سپس هر کوبیت  برای برخی  به طوری که . اگر  را با مشاهدات مکملانه رمزگذاری کنیم یک توزیع احتمالی متحد در طول را بدست می­آوریم، که هنوز هم یک حالت کاملا ترکیبی است.

**4. توزیع کلید: پروتکل سه فازه تعمیم یافته کوانتوم**

پروتکل سه گذره در رمزنگاری [25] پروتکلی است که امکان ارسال پیام بصورت ایمن از طرف اول به ارسال پیام به طرف دوم با تبادل سه پیام رمزگذاری شده را فراهم می­کند. ایده اساسی پروتکل سه گذره این است که هر کدام از طرفها کلید های خصوصی برای رمزگذاری و رمزگشایی دارد و به طور مستقل از کلیدهای خود استفاده می کنند، ابتدا برای رمزگذاری و سپس برای رمزگشایی پیام

به صورت غیر رسمی، پروتکل سه گذر برای آلیس بصورت مخفیانه یک شی را به باب ارسال می­کند به شرح زیر:

1. آلیس شی را در یک جعبه قرار می دهد، جعبه را قفل می کند و آن را به باب می فرستد

2. باب قفل خود را به جعبه اضافه می کند و آن را به آلیس می فرستد.

3. آلیس قفل خود را برمیدارد و جعبه را به باب می فرستد.

این پروتکل می­تواند با استفاده از عملیات منحصر به فرد OR ⊕ در رمزنگاری کلاسیک اجر اشود.

1. برای یک بیت x، آلیس آن را با کلید Ka خودش رمزگذاری می کند و سپس بیت رمزگذاری شده (x ⊕ K) رابه باب ارسال میکند.

2. باب بیت رمزگشایی شده را با کلید Kb خودش رمزگذاری می کندو x⊕ka) ⊕kb را به آلیس ارسال می کند.

3. آلیس آنچه را که توسط Ka دریافت کرده است رارمزگذاری می کند ((x⊕ka) ⊕kb) ⊕ka =x ⊕ kb. سپس x ⊕ kb را به باب می فرستد.

پروتکل سه گذره کوانتومی برای شنیدن مقاومت میکند . یکی از ضررهای پروتکل سه گذره کوانتومی کاناموری و یو این است که فضای کلیدی رمزگذاری آنها یک مجموعه بی نهایت است. اخیرا، Qiu و همکاران [27] پروتکل های سه فازه کوانتومی دیگر در چارچوب CQM را توسعه می­دهند به طوری که اندازه فضای کلیدی به طور قابل توجهی کوچکتر میشود. در این مقاله، پروتکل پیشنهاد شده در27 را تعمیم می­دهیم.

با توجه به دو مشاهدات تکمیلی داده شده از کوبیدها (C2، m1، u1) و (C2، m2، u2)از جفت نقاط کلاسیک از یک ساختار قابل مشاهده استفاده می کنیم، می گویند u1 و u1،برای کد کردن 0 و 1 به ترتیب. فضای کلیدی ما برای رمزگذاری و رمزگشایی کلید = {S3 (0)، S3 (π است2)، S3 (π)، S3 (3π2)}است. فرض می­کنیم (k، k †) یک جفت کلید رمزگذاری /رمزگشایی است ، که در آن k † = S3 (2π - iπ2) برای k = S3 (iπ2).

پروتکل سه­فازه کوانتوم خودمان برای آلیس به منظور ارسال یک کوبیت  برای باب متشکل از مراحل زیر است:

1. آلیس بصورت تصادف کلید خصوصی خودش  را تولید می­کند. باب بصورت تصادفی کلید خصوصی خودش  را ارائه میکند.

2. آلیس  را توسط  رمزگذاری می­کند و  را به باب ارسال می­کند.

3. باب متن رمز دریافتی  را توسط  رمزگذاری می­کند و  را به آلیس ارسال می­کند.

4. آلیس  را توسط  رمزگشایی میکند و  را به باب می­فرستد.

5. باب  را توسط  رمزگشایی می­کند و  را بدست می­آورد.

این پروتکل را می­توان توسط مالک داده­ها به منظور ارسال کلید وی و گواهی برای کاربر استفاده کرد، همانطور که توسط مرحله 4 در شکل 1 نشان داده شده است. صحت پروتکل خودمان با جابجایی تغییر فاز در طول مشاهدات مکملانه تضمین می­شود.

قضیه 2. پروتکل کوانتوم سه گذری صحیح است.

اثبات: فرض کنید آلیس u را بعنوان کلید خودش و باب v را بعنوان کلید خودش انتخاب می­کند، پس مشتقات گرافیکی زیر را داریم:

که بدان معناست که ترکیب ترتیبی عملیات 2 نهاد به کاررفته در پروتکل معادل با اپراتور هویت است. بنابراین، کوبیت بصورتی صحیح انتقال می­یابد.

امنیت بیشتر پروتکل­های موجود از توزیع کلید برای کنترل دسترسی در محیط­های ابری متکی بر پیچیدگی محاسباتی مسائلی همچون فاکتورازیسیون اصلی است. بنابراین زمانی که یک کامپیوتر کوانتوم ساخته می­شود، پروتکل آنها ممکن است در زمان چند جمله­ای به خطر بیافتد [29]. در نتیجه، پروتکل خودمان با توجه به کامپیوترهای کوانتوم امن است، از آنجا که این امنیت اطلاعاتی را با توجه به متمم مشاهدات ارائه می­کند. در اینجا یک پروتکل توزیع کلید از نقطه نظر اطلاعاتی امن است اگر که داده­ها باشند.

**قضیه 3.** پروتکل سه گذری کوانتوم از منظر اطلاعاتی امن است بدین معنا که کوبیتی که در هر مرحله از پروتکل منتقل می­شود که در کل حالتی ترکیبی می­باشد.

اثبات: این یک نتیجه ساده از قضایای 1 و 2 است.

**5. اثر مرتبط**

طرح رمزگذاری پد بموقع کوانتوم [5] احتمالا مهمترین رمز شناخته شده در رمزنگاری کوانتوم است. فضای کلید برای پد بموقع کوانتوم  است. در حالی که این فضای کلید بسیار شبیه به نتیجه خطا و آزمون است، طرح رمزنگاری ما بسیار نظاممند است و دارای یک پس­زمینه تئوریکی بسیار عمیق است، و در عین حال همان امنیت را بعنوان یک پد بموقع کوانتوم تضمین می­کند.

اولین و مهمترین پروتکل برای توزیع کلیدی کوانتوم توسط بنهت و براسارد [3] توسعه یافت، که بعنوان پروتکل BB84 شناخته می­شود. در پروتکل BB84، بیش از نیمی از کوبیت­های منتقل شده باید حذف شود. پروتکل سه گذره کوانتوم بسیار کارآمد است بدان معنا که هیچ کوبیت انتقالی نباید حذف شود. علاوه بر این، پروتکل کوانتوم سه گذره را می­توان استفاده کرد تا بصورتی مخفیانه داده­های کوانتوم ارسال شود، در حالی که BB84 نمی­تواند انجام دهد. پروتکل سه گذره کوانتوم کعرفی شده در [27] موجب استفاده از تغییر فاز در طول دو مشاهده مکملانه یعنی  و  می­شود. پروتکل سه گذره معرفی شده در این مقاله بسیار کلی است، بدین معنا که دو مشاهده مکملانه نمی­توانند  و  باشند.

**6. نتیجه­گیری**

در این مقاله کاربرد رمزگذاری کوانتوم و توزیع کلیدی کوانتوم در مسئله کنترل دسترسی را مطالعه می­کنیم. پروتکل/ طرح کنترل که در این مقاله ارائه می­کنیم دارای مزایای مختلفی در طول پروتکل­ها/ طرح­های موجود ارائه شده برای همان طرح است. آنها از نقطه نظر عملیاتی تمن و توسط فنآوری کنونی قابل اجرا است. خاطر نشان می­سازیم که پیاده­سازی پروتکل­های ناهننگاری کوانتوم بسیار آسانتر از ایجاد کامپیوترهای کوانتوم است. بسیاری از پروتکل­های نهان­نگاری کوانتوم در لابراتوارها در دهه­ها سال پیش تحقق یافت. علاوه بر این، امروزه شرکتهای تجاری وجود دارد که در حال فروش دستگاه­ها برای توزیع کلید کوانتوم و فن­آوری­های مورد نیاز برای اجرای پروتکل­ها در مقاله است که در عین حال همین فن­آوری­ها برای توزیع کلید کوانتوم مورد نیاز است که توسط شرکت­های تجاری تحقق می­یابد.

**Reference**

 [1] Abramsky S, Coecke B. A categorical semantics of quantum protocols. In: 19th IEEE Symposium on Logic in Computer Science (LICS 2004), 14-17 July 2004, Turku, Finland, Proceedings. IEEE Computer Society; 2004. p. 415–25. URL: https://doi.org/10.1109/LICS.2004.1319636. doi:10.1109/LICS.2004.1319636.

[2] Akl SG, Taylor PD. Cryptographic solution to a problem of access control in a hierarchy. ACM Trans Comput Syst 1983;1(3):239–48. URL: http: //doi.acm.org/10.1145/357369.357372. doi:10.1145/357369.357372.

 [3] Bennetta C, GillesBrassard . Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. 1984. p. 175–9.

[4] Bian X, Wang Q. Graphical calculus for qutrit systems. IEICE Transactions 2015;98-A(1):391–9. URL: http://search.ieice.org/bin/ summary.php?id=e98-a\_1\_391.

[5] Boykin PO, Roychowdhury V. Optimal encryption of quantum bits. Physical Review A 2003;67:645–8.

[6] Castiglione A, Santis AD, Masucci B, Palmieri F, Castiglione A, Huang X. Cryptographic hierarchical access control for dynamic structures. IEEE Trans Information Forensics and Security 2016;11(10):2349–64. URL: http://dx.doi.org/10.1109/TIFS.2016.2581147. doi:10.1109/ TIFS.2016.2581147.

[7] Castiglione A, Santis AD, Masucci B, Palmieri F, Castiglione A, Li J, Huang X. Hierarchical and shared access control. IEEE Trans Information Forensics and Security 2016;11(4):850–65. URL: http://dx.doi.org/10. 1109/TIFS.2015.2512533. doi:10.1109/TIFS.2015.2512533.

 [8] Castiglione A, Santis AD, Masucci B, Palmieri F, Huang X, Castiglione A. Supporting dynamic updates in storage clouds with the akl-taylor scheme. Inf Sci 2017;387:56–74. URL: http://dx.doi.org/10.1016/j.ins.2016. 08.093. doi:10.1016/j.ins.2016.08.093.

 [9] Cattaneo G, Chiara MLD, Giuntini R, Leporini R. An unsharp logic from quantum computation. International Journal of Theoretical Physics 2004;43(7):1803–17. URL: https://doi.org/10.1023/B:IJTP. 0000048821.56239.cb. doi:10.1023/B:IJTP.0000048821.56239.cb.

[10] Chiara MD, Giuntini R, Sergioli G, Leporini R. A many-valued approach to quantum computational logics. Fuzzy Sets and Systems 2016;URL: http: //www.sciencedirect.com/science/article/pii/S0165011416304560. doi:https://doi.org/10.1016/j.fss.2016.12.015.

[11] Coecke B, Duncan R. Interacting quantum observables: categorical algebra and diagrammatics. New Journal of Physics 2011;13(043016):1–85.

 [12] Coecke B, Heunen C, Kissinger A. Compositional quantum logic. In: Coecke B, Ong L, Panangaden P, editors. Computation, Logic, Games, and Quantum Foundations. The Many Facets of Samson Abramsky - Essays Dedicated to Samson Abramsky on the Occasion of His 60th Birthday. Springer; volume 7860 of Lecture Notes in Computer Science; 2013. p. 21–36. URL: https://doi.org/10.1007/978-3-642-38164-5\_3. doi:10. 1007/978-3-642-38164-5\_3.

[13] Coecke B, Heunen C, Kissinger A. Categories of quantum and classical channels. Quantum Information Processing 2016;15(12):5179– 209. URL: https://doi.org/10.1007/s11128-014-0837-4. doi:10. 1007/s11128-014-0837-4.

[14] Coecke B, Kissinger A. Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning. Cambridge University Press, 2017.

 [15] Coecke B, Paquette E. Categories for the Practising Physicist; Berlin, ´ Heidelberg: Springer Berlin Heidelberg. p. 173–286. URL: https://doi. org/10.1007/978-3-642-12821-9\_3. doi:10.1007/978-3-642-12821-9\_ 3.

[16] Coecke B, Perdrix S. Environment and classical channels in categorical quantum mechanics. Logical Methods in Computer Science 2010;8(4). URL: https://doi.org/10.2168/LMCS-8(4:14)2012. doi:10. 2168/LMCS-8(4:14)2012.

[17] Coecke B, Wang Q, Wang B, Wang Y, Zhang Q. Graphical calculus for quantum key distribution (extended abstract). Electr Notes Theor Comput Sci 2011;270(2):231–49. URL: https://doi.org/10.1016/j.entcs.2011. 01.034. doi:10.1016/j.entcs.2011.01.034.

 [18] Giuntini R, Ledda A, Paoli F. Expanding quasi-mv algebras by a quantum operator. Studia Logica 2007;87(1):99–128. URL: https://doi.org/10. 1007/s11225-007-9079-0. doi:10.1007/s11225-007-9079-0.

[19] Kanamori Y, Yoo S. Quantum three-pass protocol: Key distribution using quantum superposition states. International Journal of Network Security and Its Applications 2009;1(2):64–70.

[20] Lane SM. Categories for the Working Mathematician. Springer-Verlag, 1998.

 [21] Ledda A, Konig M, Paoli F, Giuntini R. Mv-algebras and quantum computation. Studia Logica 2006;82(2):245–70. URL: https://doi.org/10. 1007/s11225-006-7202-2. doi:10.1007/s11225-006-7202-2.

[22] Ledda A, Sergioli G. Towards quantum computational logics. International Journal of Theoretical Physics 2010;49(12):3158–65. URL: https://doi. org/10.1007/s10773-010-0368-4. doi:10.1007/s10773-010-0368-4.

[23] Liu Z, Huang X, Hu Z, Khan MK, Seo H, Zhou L. On emerging family of elliptic curves to secure internet of things: ECC comes of age. IEEE Trans Dependable Sec Comput 2017;14(3):237–48. URL: https://doi.org/10. 1109/TDSC.2016.2577022. doi:10.1109/TDSC.2016.2577022.

[24] Liu Z, Weng J, Hu Z, Seo H. Efficient elliptic curve cryptography for embedded devices. ACM Trans Embedded Comput Syst 2017;16(2):53:1–53:18. URL: http://doi.acm.org/10.1145/2967103. doi:10.1145/2967103.

[25] Massey J. An introduction to contemporary cryptology. Proceedings of the IEEE 1988;76:533–49.

 [26] Nielsen M, Chuang I. Quantum Computation and Quantum Information. Cambridge University Press, 2011.

[27] Qiu L, Sun X, Xu J. Categorical quantum cryptography for access control in cloud computing. Soft Computing 2017;URL: https://doi.org/10. 1007/s00500-017-2688-2. doi:10.1007/s00500-017-2688-2.

[28] Selinger P. Dagger compact closed categories and completely positive maps: (extended abstract). Electr Notes Theor Comput Sci 2007;170:139– 63. URL: https://doi.org/10.1016/j.entcs.2006.12.018. doi:10. 1016/j.entcs.2006.12.018.

 [29] Shor PW. Polynominal time algorithms for discrete logarithms and factoring on a quantum computer. In: Adleman LM, Huang MA, editors. Algorithmic Number Theory, First International Symposium, ANTS-I, Ithaca, NY, USA, May 6-9, 1994, Proceedings. Springer; volume 877 of Lecture Notes in Computer Science; 1994. p. 289. URL: http://dx.doi.org/10. 1007/3-540-58691-1\_68. doi:10.1007/3-540-58691-1\_68.

 [30] Sun X, Wang Q, Kulicki P, Zhao X. Quantum technique for access control in cloud computing I: Quantum imperative logic. Studia Logica 2017;:– Submitted.

[31] Yanofsky N, Mannucci M. Quantum Computing for Computer Scientists. Cambridge University Press, 2008.