مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال چهارم، شماره ۳، پاییز ۱۳۹۵، ص ۹۲-۸۳

تسهیم راز نیمه کوانتومی با استفاده از سه ذره غیردرهم تنیده

زهرا کریمی‌فرد[۱]، سمانه مشهدی[۲]، داود ابراهیمی بقا[۳*]

۱- دانشجوی دکتری، گروه ریاضی و آمار، دانشکده علوم پایه، دانشگاه آزاد اسلامی، واحد تهران مرکزی

۲- استادیار، گروه ریاضی محض، دانشکده ریاضی، دانشگاه علم و صنعت ایران

۳- استادیار، گروه ریاضی و آمار، دانشکده علوم پایه، دانشگاه آزاد اسلامی، واحد تهران مرکزی

(دریافت: ۹۵/۰۳/۰۳، پذیرش: ۹۵/۰۵/۱۱)

چکیده

در این مقاله، یک پروتکل تسهیم راز (۳،۳)، آستانه‌ای نیمه‌کوانتومی با بهره‌گیری از حالات غیردرهم‌تنیده پیشنهاد می‌شود که در آن آلیس، به عنوان واسطه کوانتومی، یک کلید راز را بین سه شرکت‌کننده کلاسیک به اشتراک می‌گذارد. شرکت‌کنندگان کلاسیک تنها قادر به اندازه‌گیری ذرات در پایه محاسباتی $\{|0\rangle,|1\rangle\}$ و یا بازتاب ذرات بدون ایجاد اختلال هستند. در این پروتکل تسهیم راز نیمه‌کوانتومی و خصوصا زمانی که تعداد شرکت کنندگان تسهیم راز زیاد باشد به خاصیت درهم‌تنیدگی نیازی نیست. همچنین نشان می‌دهیم که پروتکل پیشنهادی در برابر استراق سمع ایمن است.

واژه‌های کلیدی: تسهیم راز کوانتومی، تسهیم راز نیمه‌کوانتومی، کوانتوم بدون درهم‌تنیدگی، فوتون منفرد، توزیع کلید کوانتومی

۱- مقدمه

فرض کنیم آلیس به‌عنوان واسطه قصد دارد اطلاعات محرمانه‌ای را بین سه سهام‌دار یعنی باب، چارلی و دیوید توزیع کند. این سه نفر لزوما افراد مورد اعتماد نیستند. از آن‌جایی‌که آلیس نمی‌داند کدام‌یک از این سه نفر قابل اعتماد هستند، تصمیم می‌گیرد این اطلاعات محرمانه را به‌گونه‌ای توزیع نماید که افراد، تنها با همکاری یکدیگر بتوانند به اطلاعات دست پیدا کنند و هیچ‌کدام از اعضا به تنهایی قادر به دست‌یابی به اطلاعات نباشند. بنابراین باب، چارلی و دیوید با همکاری یکدیگر می‌توانند به اطلاعات محرمانه دسترسی پیدا کنند ولی به تنهایی قادر به انجام آن نخواهند بود. رمزنگاری کلاسیک راه‌حلی برای این مسئله فراهم کرده است که از آن به نام تسهیم راز یاد می‌شود [۲-۱]. آلیس می‌خواهد پیام محرمانه (S_A) را به باب، چارلی و دیوید بفرستد. آلیس به منظور حفظ امنیت پیام، آن‌را به سه پیام رمزی (S_B)، (S_C) و (S_D) تقسیم می‌کند. سپس پیام (S_B) را به باب، (S_C) را به چارلی و (S_D) را به دیوید ارسال می‌نماید. هریک از پیام‌ها به تنهایی شامل اطلاعات پیام اولیه نمی‌باشند اما باهم حاوی پیام کامل هستند. چنانچه تسهیم راز کلاسیک با سایر تکنیک‌ها مانند رمزنگاری ترکیب نشود، قادر به حل مسئله‌ی استراق‌سمع نخواهد بود. همچنین در حالت تسهیم راز کلاسیک اگر شنودگری مانند ایو و یا یکی از سه نفر باب، چارلی و دیوید، کانال ارتباطی را کنترل نمایند و به اطلاعات ارسالی توسط آلیس دست پیدا کنند، می‌توانند به محتوای پیام او پی‌ببرند. خوشبختانه پروتکل تسهیم راز کوانتومی، ما را قادر ساخته است که به توزیع پیام با امنیت بالا و تشخیص استراق‌سمع بپردازیم [۵-۳].

۱-۱- کارهای مرتبط

اولین پروتکل تسهیم راز کوانتومی (QSS)[1] توسط مارک و همکاران، مبتنی بر حالت سه‌تایی GHZ[2] معرفی شد. در سال‌های اخیر پروتکل‌های تسهیم راز کوانتومی بسیاری مبتنی‌بر حالات درهم‌تنیده ارائه شده است [۹-۶]. در تمامی پروتکل‌های تسهیم راز کوانتومی، تمام شرکت‌کنندگان می‌بایست دارای قابلیت‌های کوانتومی باشند. اما معمولا منابع و عملیات کوانتومی بسیار گران هستند. بنابراین، در شرایط واقعی شرکت‌کنندگان استطاعت فراهم کردن سیستم‌های کوانتومی را ندارند. به‌منظور جلوگیری از چنین مشکلی، لی و همکاران [۱۰]، دو پروتکل

1- Quantum Secret Sharing
2- Greenberger-Horne-Zeilinger

* رایانامه نویسنده مسئول: D-ebrahimibagha-math@iauctb.ac.ir

تسهیم راز نیمه‌کوانتومی (SQSS)[1] مبتنی‌بر حالت سه‌تایی GHZ ارائه کردند وانگ و همکاران [۱۱]، نیز پروتکل تسهیم راز نیمه‌کوانتومی مبتنی‌بر حالت دوتایی درهم‌تنیده‌ای ارائه نمودند که در آن آلیس به‌عنوان واسطه، مجهز به سیستم‌های کوانتومی است اما سهام‌داران فقط توانایی‌های کلاسیک دارند [۱۲]. بنابراین، به دلیل کارایی بیشتر، ترجیح بر استفاده از تسهیم راز نیمه‌کوانتومی می‌باشد.

۱-۲- پیش زمینه

آلیس را کوانتومی، می‌نامیم هرگاه او مجاز به تولید حالات کوانتومی دلخواه و انجام هر عملیات کوانتومی باشد [۱۰]. به طور دقیق‌تر واسطه، قادر به انجام عملیات زیر می‌باشد:

۱. تولید و آماده‌سازی حالت مبتنی‌بر حالت سه‌تایی GHZ
۲. اندازه‌گیری در پایه محاسباتی
۳. ذخیره فوتون‌ها در یک حافظه کوانتومی کوتاه مدت

تعاریف مربوط به کلاسیک را آن‌گونه که در مقاله [۱۲]، آمده است دنبال می‌کنیم. سهام‌دارانی را مانند باب، چارلی و دیوید، کلاسیک گوییم هرگاه آنان محدود به انجام عملیات زیر روی کانال کوانتومی باشند:

۱. آماده‌سازی کیوبیت‌های جدید در مبنای کلاسیک {0,1}
۲. اندازه‌گیری کیوبیت‌ها در مبنای کلاسیک {0,1}
۳. مرتب‌سازی کیوبیت‌ها
۴. ارسال یا بازتاب کیوبیت‌ها بدون ایجاد اختلال در آن‌ها

پروتکلی که تمامی شرایط فوق را داشته باشد تسهیم راز نیمه‌کوانتومی نامیده می‌شود. در تسهیم راز نیمه‌کوانتومی، نماد کلاسیک {0, 1} جایگزین پایه محاسباتی {$|0>, |1>$} می‌گردد.

۱-۳- انگیزه و مشارکت

بازده پروتکل‌های تسهیم راز کوانتومی مبتنی بر حالات درهم‌تنیده به سبب ویژگی‌های ذاتی درهم تنیدگی، حداکثر ۵۰٪ می‌باشد. گوا و همکاران [۱۳]، یک طرح تسهیم راز ارائه کردند که به جای حالات درهم‌تنیده از حالات حاصل‌ضربی استفاده می‌کرد. بنابراین بازده تا حدود ۱۰۰٪ افزایش یافت. به بیان دیگر، پروتکل‌های تسهیم راز کوانتومی مبتنی بر حالت درهم‌تنیدگی، دست نیافتنی می‌باشند. همچنین بازده فراهم‌سازی حالات درهم‌تنیده برای سه یا چهار شرکت کننده بسیار پایین است [۳ و ۱۴و ۱۵]، بنابراین نه‌تنها درهم‌تنیدگی دراین پروتکل تسهیم راز نیمه‌کوانتومی ضروری نمی‌باشد بلکه عدم استفاده از این حالت با توجه به تعداد شرکت‌کنندگان، موجب بالا رفتن کارایی طرح نیز می‌گردد. به‌علاوه بازده پروتکل تسهیم راز بدون درهم‌تنیدگی تقریبا ۱۰۰٪ است زیرا کلیدها می‌توانند در حالت ایده‌آل بدون استراق‌سمع استفاده شوند.

در این مقاله ما به بررسی پروتکل تسهیم راز نیمه‌کوانتومی می‌پردازیم که در آن آلیس کوانتومی قصد به‌اشتراک گذاشتن یک راز را با باب کلاسیک، چارلی کلاسیک و دیوید کلاسیک دارد درحالی‌که برای بازسازی پیام رمز باید هرسه سهام‌دار با یکدیگر همکاری نمایند و هیچ کدام به‌تنهایی قادر به دست‌یابی اطلاعات نیستند.

۱-۴- ساختاربندی

شمای کلی این مقاله به این‌صورت است که بخش ۲، شامل تعاریف اولیه می‌باشد. در بخش ۳، به معرفی طرح تسهیم راز نیمه‌کوانتومی پرداخته می‌شود. تعاریف و بررسی پروتکل پیشنهادی در بخش ۴، ارائه می‌گردد. امنیت پروتکل معرفی شده در فصل ۵، بررسی می‌شود. نتایج مقایسه پروتکل پیشنهادی با دو پروتکل مشابه دیگر در بخش ۶، ارائه شده است و در نهایت در فصل ۷، با نتیجه‌گیری، مقاله پایان می‌پذیرد.

۲- تعاریف اولیه

بیت کوانتومی یا کیوبیت یک واحد اطلاعات کوانتومی است. رمزنگاری کوانتومی یا توزیع کوانتومی کلید (QKD)[2] که اولین بار توسط بنت و براسارد [۱۶] به طور جداگانه‌ای معرفی شد، از قوانین اساسی فیزیک کوانتوم برای ضمانت یک ارتباط امن استفاده می‌کند. BB84 طرحی برگرفته از طرح QKD است که در آن آلیس، هر کیوبیت را به یکی از چهار حالت ممکن در دو پایه محاسباتی و هادامارد ارسال می‌کند.

دو حالت ممکن برای کیوبیت‌ها $|0>$ و $|1>$ است که می‌توانند به‌صورت $|\psi>=\alpha|0>+\beta|1>$ باشد که در آن $|0>$ نماد استاندارد دیراک برای حالات کوانتومی است و $\alpha,\beta\in\mathbb{C}$ به طوری‌که $|\alpha|^2+|\beta|^2=1$. α^2 بیانگر احتمال اندازی‌گیری ۰ و β^2 بیانگر احتمال اندازه‌گیری ۱ است. کیوبیت‌ها در دو پایه تولید و اندازه‌گیری می‌شوند. یکی پایه محاسباتی (پایه Z) است که به‌صورت $Z=\{|0>,|1>\}$ نشان داده می‌شود و دیگری پایه هادامارد[3] می‌باشد که به‌صورت $|+>=\frac{1}{\sqrt{2}}(|0>+|1>)$ و $|->=\frac{1}{\sqrt{2}}(|0>-|1>)$ نمایش داده می‌شود. برای سیستم‌های سه کیوبیتی، 2^3 حالت در هر پایه وجود دارد یعنی ۸ پایه محاسباتی و ۸ پایه هادامارد که به ترتیب $|001>, |010>, |100>, |000>, |110>, |101>, |011>, |+++>, |++->, |+-+>, |+-->, |-++>, |-+->, |--+>, |--->$ می‌باشند که به‌صورت $|\psi>=\sum_{i=0}^{2^n-1}\alpha_i|i\rangle$ نشان داده می‌شود که در آن $\alpha\in\mathbb{C}$ و

1- Semi-Quantum Secret Sharing

2- Quantum Key Distribution

3- Hadamard

همچنین i به‌صورت نمایش دودویی نوشته می‌شود و $\sum_i|\alpha_i|^2 = 1$. حال اگر داشته باشیم $|\psi_1> = \alpha_1|0> + \beta_1|1>$، $|\psi_2> = \alpha_2|0> + \beta_2|1>$ و $|\psi_3> = \alpha_3|0> + \beta_3|1>$ آن‌گاه حالت یک سیستم سه کیوبیتی متشکل از ψ_1، ψ_2 و ψ_3 توسط حاصل‌ضرب تانسوری آن‌ها می‌باشد که به‌صورت زیر نمایش داده می‌شود.

$$\begin{aligned}|\psi_1\rangle\otimes|\psi_2\rangle\otimes|\psi_3\rangle = {} & \alpha_1\alpha_2\alpha_3|000\rangle \\ & + \alpha_1\alpha_2\beta_3|001\rangle \\ & + \alpha_1\beta_2\alpha_3|010\rangle \\ & + \alpha_1\beta_2\beta_3|011\rangle \\ & + \beta_1\alpha_2\alpha_3|100\rangle \\ & + \beta_1\alpha_2\beta_3|101\rangle \\ & + \beta_1\beta_2\alpha_3|110\rangle + \beta_1\beta_2\beta_3|111\rangle.\end{aligned}$$

حالات چندکیوبیتی، جدایی‌پذیر یا حالات حاصل‌ضربی نامیده می‌شوند هرگاه بتوان آن‌ها را به‌صورت حاصل‌ضرب تانسوری از کیوبیت‌های منفرد نشان داد. درغیراین‌صورت درهم‌تنیده نامیده می‌شوند.

۳- پروتکل پیشنهادی

حال به ارائه پروتکل تسهیم راز نیمه‌کوانتومی بدون به‌کارگیری خاصیت درهم‌تنیدگی می‌پردازیم. فرایند خاص این تسهیم راز نیمه‌کوانتومی به شرح زیر می‌باشد.

• آلیس به طور تصادفی دو رشته n بیتی $\gamma = (\gamma_1, \gamma_2, \dots, \gamma_i, \dots, \gamma_n)$ و $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_i, \dots, \lambda_n)$ را تولید می‌کند که در آن γ_i و λ_i نشان‌دهنده بیت متناظر رشته‌های γ و λ هستند.

برای هر بیت γ و λ آلیس حالت حاصل‌ضربی سه کیوبیتی $|bcd\rangle$ را به گونه‌ای تولید می‌کند که اگر $\gamma = 0$ آن‌گاه $|bcd\rangle$ در پایه محاسباتی $Z = \{|0>, |1>\}$ و اگر $\gamma = 1$ آن‌گاه $|bcd\rangle$ در پایه هادامارد $X = \{|+>, |->\}$ تولید شود. نتیجه $\overline{XOR}$ سه کیوبیت b، c و d برابر مقدار متناظر رشته λ است. یعنی

$$\overline{b \oplus c \oplus d} = \begin{cases} 0 & if\ \lambda_i = 0 \\ 1 & if\ \lambda_i = 1 \end{cases}$$

بردارهای سه کیوبیتی پایه‌های محاسباتی و هادامارد به ترتیب به صورت:

$$T_1 = \{|000>, |011>, |101>, |110>, |100>, |010>, |001>, |111>\}$$

$$T_2 = \{|+++>, |++->, |+-+>, |+-->, |-++>, |-+->, |--+>, |--->\}$$

هستند که در آن، $|+> = \frac{1}{\sqrt{2}}(|0> + |1>)$ و می‌باشد.

جدول (۱) کدگذاری حالات سه کیوبیتی در محورهای متناظر را نشان می‌دهد. به عنوان مثال اگر بیت‌های متناظر γ و λ به ترتیب ۱ و ۰ باشند، آن‌گاه حالت سه کیوبیتی که توسط آلیس تولید می‌شود می‌تواند یکی از حالات $|+++>$، $|++->$، $|+-+>$، $|+-->$، $|-++>$، $|-+->$، $|--+>$ یا $|--->$ باشد که احتمال تولید هریک ۲۵٪ است.

جدول (۱). کدگذاری حالات سه کیوبیتی بر اساس رشته‌های γ و λ

1		*0*		γ
1	0	1	0	λ
$\|--+>$	$\|++->$	$\|111>$	$\|110>$	$\|bcd>$
$\|-+->$	$\|+-+>$	$\|001>$	$\|101>$	
$\|+-->$	$\|-++>$	$\|010>$	$\|011>$	
$\|+++>$	$\|---\>$	$\|100>$	$\|000>$	

• پس از آن که آلیس حالت حاصل‌ضربی N کیوبیتی $|\psi> = \prod_{i=1}^{n} \overline{|bcd>}_i$ را آماده کرد، سه رشته به‌دست آمده B، C و D را براساس $|bcd\rangle$ به طور جداگانه و به ترتیب برای باب، چارلی و دیوید می‌فرستد. در حقیقت هر بیت از سه رشته B، C و D به یکدیگر مرتبط هستند و نتیجه $\overline{XOR}$ آن سه برابر بیت متناظر از رشته λ است.

• سپس باب، چارلی و دیوید هر کیوبیت دریافتی را به طور تصادفی در پایه‌ی محاسباتی اندازی‌گیری و آن‌را مجددا به آلیس ارسال می‌کنند (از این عمل به عنوان اندازه‌گیری یاد می‌شود) و یا کیوبیت‌های دریافتی را پس از مرتب سازی به سمت آلیس بازتاب می‌نمایند (از این عمل به عنوان بازتاب یاد می‌شود).

• آلیس کیوبیت‌های ارسالی توسط باب، چارلی و دیوید را در یک حافظه کوانتومی ذخیره می‌کند و به آنها اطلاع می‌دهد که رشته‌های B، C و D را دریافت کرده‌است.

• پس از آنکه آلیس از رسیدن کیوبیت‌ها اطمینان حاصل کرد، باب، چارلی و دیوید اعلام می‌کنند که کدام کیوبیت‌ها را اندازه‌گیری و کدام کیوبیت‌ها را بازتاب کرده‌اند.

• در مرحله‌ی بررسی، با مقایسه کیوبیت‌های بازتابی با حالت اولیه این کیوبیت‌ها، آلیس می‌تواند وجود استراق‌سمع کننده را تشخیص دهد. اگر نرخ خطا بیش از یک حد آستانه‌ای باشد، با صرف نظر از نتایج به‌دست‌آمده، فرایند فوق از مرحله اول از سر گرفته می‌شود.

• بقیه بیت‌های چک نشده رشته‌های A، B و C می‌توانند به عنوان کلید در تسهیم راز مورد استفاده قرار گیرند. آلیس پیام رمز را با کلید مخفی به اشتراک گذاشته شده توسط طرح تسهیم راز، رمزگذاری می‌کند. سپس باب، چارلی و دیوید با همکاری یکدیگر در مرحله بازسازی، کلید تسهیم راز را به‌دست آورده و متن را رمزگشایی می‌کنند.

۴- تحلیل و توصیف پروتکل پیشنهادی

بدیهی است در این طرح تسهیم راز نیمه‌کوانتومی، ضرورتی برای آلیس در ارسال هم‌زمان کیوبیت‌های b، c و d نیست. او می‌تواند کیوبیت‌ها را به طور مجزا برای باب، چارلی و دیوید بفرستد. آن سه نفر می‌توانند رشته‌های خود را تا زمانی که آلیس از آنها بخواهد اطلاعات ارسالی او را استخراج کنند، پیش خود نگه دارند. درحقیقت این طرح، ترکیبی از سه پروتکل بهبودیافته توزیع نیمه‌کوانتومی کلید BB84 است؛ آلیس به باب، آلیس به چارلی و آلیس به دیوید که در آن، حالت آلیس به طور کلاسیک رمزی شده‌است و هیچ‌یک از باب، چارلی و دیوید بدون همکاری یکدیگر قادر به یافتن هیچ‌گونه اطلاعات نیستند.

براساس محور ارسالی توسط آلیس و عملیاتی که باب، چارلی و دیوید انجام می‌دهند، یکی از ۱۶ حالت جدول (۲) اتفاق می‌افتد.

جدول (۲). عملیات باب، چارلی و دیوید روی کیوبیت‌های ارسالی آلیس

نمونه	پایه انتخابی آلیس	باب	چارلی	دیوید
1	Z	اندازه‌گیری	اندازه‌گیری	*اندازه‌گیری*
2	Z	اندازه‌گیری	اندازه‌گیری	*بازتاب*
3	Z	اندازه‌گیری	بازتاب	*اندازه‌گیری*
4	Z	بازتاب	اندازه‌گیری	*اندازه‌گیری*
5	Z	اندازه‌گیری	بازتاب	*بازتاب*
6	Z	بازتاب	اندازه‌گیری	*بازتاب*
7	Z	بازتاب	بازتاب	*اندازه‌گیری*
8	Z	بازتاب	بازتاب	*بازتاب*
9	X	اندازه‌گیری	اندازه‌گیری	*اندازه‌گیری*
10	X	اندازه‌گیری	اندازه‌گیری	*بازتاب*
11	X	اندازه‌گیری	بازتاب	*اندازه‌گیری*
12	X	بازتاب	اندازه‌گیری	*اندازه‌گیری*
13	X	اندازه‌گیری	بازتاب	*بازتاب*
14	X	بازتاب	اندازه‌گیری	*بازتاب*
15	X	بازتاب	بازتاب	*اندازه‌گیری*
16	X	بازتاب	بازتاب	*بازتاب*

با توجه به جدول (۲)، در نمونه اول رشته‌های B، C و D در پایه محاسباتی توسط آلیس ارسال می‌شوند و از آن‌جایی که باب، چارلی و دیوید کیوبیت‌های دریافتی رشته‌های خود را در همان پایه محاسباتی اندازه‌گیری کرده‌اند، نتایج اندازه‌گیری قطعی بوده و برای کلید استفاده می‌شوند و $A = \overline{b \oplus c \oplus d}$ در نمونه‌های دوم تا هفتم، رشته‌های B، C و D در پایه محاسباتی توسط آلیس ارسال می‌شوند و باب، چارلی و دیوید این کیوبیت‌ها را اندازه‌گیری و یا بازتاب می‌کنند.

در نمونه هشتم، هرسه نفر کیوبیت‌های دریافتی را بدون هیچ‌گونه تغییر بازتاب می‌کنند. در نمونه‌های نهم تا پانزدهم، از آن‌جایی که کیوبیت‌های تولید شده در پایه هادامارد، به‌طور تصادفی در پایه استاندارد اندازه‌گیری و یا بازتاب می‌شوند، نمی‌توان از آن به‌عنوان کلید استفاده کرد و تنها به‌منظور کنترل استراق‌سمع از آن‌ها استفاده می‌شود. آلیس با بررسی کیوبیت‌های بازتابی با حالت کیوبیت‌های اولیه خود قادر به تشخیص استراق‌سمع می‌باشد. اگر خطا از یک حد آستانه‌ای بیشتر باشد آن‌گاه پروتکل از ابتدا دوباره راه‌اندازی می‌گردد.

به این ترتیب، آلیس پیام خود را براساس کلید به‌اشتراک گذاشته شده در نمونه اول رمزی می‌کند. بنابراین باب، چارلی و دیوید تنها با همکاری یکدیگر می‌توانند این متن رمزی را رمزگشایی کنند.

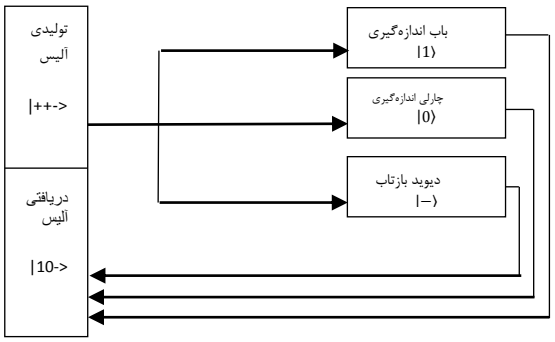
۴-۱- مثال‌ها

در ادامه به ارائه دو مثال می‌پردازیم.

مثال ۴-۱-۱: فرض کنیم $K = k_1 k_2 \dots k_n$ یک کلید n بیتی مرتب است که در آن $k_i \in \{0,1\}$. آلیس قصد دارد K را با باب، چارلی و دیوید به اشتراک بگذارد. بدین منظور دو رشته ۸۰ بیتی $\lambda = 011 \dots 0$ و $\gamma = 101 \dots 0$ را به طور تصادفی انتخاب می‌کند. سپس برای هر بیت از λ و γ حالت حاصل‌ضربی ۳ کیوبیتی $|\psi>= \prod_{i=1}^{n} |\overline{bcd}>_i$ را آماده می‌کند. از آنجایی‌که $\gamma_1 = 0$ ، آلیس پایه هادامارد {Z={|+>,|−>} را انتخاب می‌کند و چون $\lambda = 0$ بنابراین $\overline{b \oplus c \oplus d} = 0$ و این به معنای آن است که $|bcd\rangle_1 \in \{|++->, |+-+>, |-++>, |---+>\}$ و $\overline{|bcd\rangle}_1 \in \{|+++>, |+--->, |--+->, |-+-+>\}$. بنابراین، آلیس حالت‌های ۳-کیوبیتی $|+--+>_1 \; |001>_{80} \dots |+--+>_3 \; |101>_2$ را آماده می‌کند. سپس فوتون‌های اول، دوم و سوم از هر ۸۰ کیوبیت را به ترتیب برای باب، چارلی و دیوید می‌فرستد. فرض کنیم آلیس $|101>_2$ را آماده کرده و |1> را برای باب، |0> را برای چارلی و |1> را برای دیوید می‌فرستد. آن‌ها ذرات دریافتی از سوی آلیس را اندازه‌گیری‌کرده و ذرات حاصل |1>، |0> و |1> را دوباره برای آلیس می‌فرستند. از آن‌جایی‌که نتایج قطعی‌اند، به عنوان بیت کلید مورد استفاده قرار می‌گیرند. بنابراین بیت اول کلید برابر است با $k_1 = \overline{1 \oplus 0 \oplus 1} = 1$.

مثال ۴-۱-۲: شکل (۱) نشان می‌دهد که آلیس ذرات |+>، |+< و |−> را به‌ترتیب برای باب، چارلی و دیوید

می‌فرستد. پس از دریافت کیوبیت‌های ارسالی، باب و چارلی تصمیم به اندازه‌گیری و دیوید تصمیم به بازتاب ذره دریافتی خود می‌کنند. سپس ذرات $|1> <$، $|0> <$ و $|-> <$ را دوباره برای آلیس ارسال می‌کنند.



شکل (۱). فرآیند اجرای پروتکل

۵- بررسی امنیت پروتکل پیشنهادی

تاکنون به ارائه پروتکل تسهیم راز نیمه‌کوانتومی خود پرداختیم. اکنون به بحث پیرامون امنیت این پروتکل پیشنهادی می‌پردازیم. بررسی امنیت، مهم‌ترین بخش پروتکل تسهیم راز نیمه‌کوانتومی است که در واقعیت کار دشواری است. در سال‌های اخیر ثابت شده‌است که برخی از پروتکل‌های تسهیم راز کوانتومی دارای امنیت نیستند [۱۸-۱۷]. اساس امنیت این پروتکل در محرمانه نگه داشتن این حقیقت است که کدام کیوبیت‌ها اندازه‌گیری و کدام‌یک بازتاب شده‌اند. حفظ محرمانگی شماره‌ی ذرات اندازه‌گیری شده یا بازتابی قبل از مرحله‌ی آشکارسازی، می‌تواند امنیت پروتکل را تضمین کند. در این بخش نشان داده می‌شود که ایو یا یک شخص غیرقابل اعتماد بتواند به اطلاعات کلید دست‌یابد، آلیس می‌تواند حضور استراق‌سمع کننده را تشخیص دهد.

فرض کنیم باب یک شخص غیرقابل اعتماد است و می‌تواند به ذرات ارسالی برای چارلی و دیوید همانند ذرات خودش دسترسی داشته باشد. باب غیرقابل اعتماد را باب* می‌نامیم. باب* می‌تواند ذرات رشته‌های C و D را قطع کرده و آنها را اندازه‌گیری کند و دوباره به سمت چارلی و دیوید بفرستد. همچنین درصورت نیاز، چارلی غیرقابل اعتماد را چارلی* و دیوید غیرقابل اعتماد دیوید* می‌نامیم. در ادامه به بحث پیرامون امنیت پروتکل دربرابر حملات متفاوت باب* و یا هر سهام‌دار غیرقابل اعتماد دیگر می‌پردازیم.

۵-۱- اندازه‌گیری رشته‌ها در پایه‌ی محاسباتی توسط باب*

هنگامی‌که باب* رشته‌های C یا D را در پایه‌ی محاسباتی اندازه‌گیری می‌کند، حالت پس از اندازه‌گیری باب* یکی از حالات $|0>$ یا $|1>$ هریک با احتمال $\frac{1}{2}$ خواهد بود. ابتدا فرض کنیم باب* فقط روی رشته‌ی C یعنی ذرات ارسالی برای چارلی شنود کند. بدون درنظر گرفتن عملیات دیوید، به بررسی نرخ خطای تولید شده توسط باب* در تمام شانزده نمونه‌ی معرفی شده می‌پردازیم.

در نمونه‌های اول و دوم که باب و چارلی هر دو در پایه محاسباتی اندازه‌گیری می‌کنند، باب می‌تواند نتایج آلیس را به‌دست آورد درحالی‌که حضورش در فاز کنترل استراق‌سمع تشخیص داده نمی‌شود. در نمونه‌های سوم تا هشتم که ذرات در پایه محاسباتی تولید شده‌اند، اندازه‌گیری ذرات هیچ‌گونه تغییری در آن‌ها ایجاد نمی‌کند و حضور استراق‌سمع کننده توسط آلیس تشخیص داده نمی‌شود. در نمونه‌های نهم تا شانزدهم، از آن‌جایی که ذرات در پایه هادامارد تولید شده‌اند، اندازه‌گیری ذرات باعث ایجاد تغییر در آن‌ها می‌گردد اما بازتاب ذرات در نمونه‌های یازدهم، سیزدهم، چهاردهم و شانزدهم حضور استراق‌سمع کننده را با نرخ خطای ۱۰۰٪ آشکار می‌کند. با توجه به توضیحات فوق در شانزده نمونه معرفی شده، میانگین نرخ خطای تولید شده توسط باب* برابر است با

$$\frac{1}{16}\times(0+0+0+0+0+0+0+0+0+0+0+1+0+1+0+1+1)=25\%.$$

به‌طور مشابه از آن‌جایی که سیستم متقارن است، اگر باب* روی رشته‌ی D یعنی دیوید شنود کند، بدون توجه به عملیات چارلی، استراق‌سمع باب* زمانی که دیوید ذرات تولید شده در پایه هادامارد را به سمت آلیس بازتاب می‌کند، قابل تشخیص است و میانگین نرخ خطای تولید شده توسط باب* برابر است با ۲۵٪. به‌علاوه اگر باب* هر دو رشته C و D را در پایه محاسباتی اندازه‌گیری کند، میانگین نرخ خطای تولید شده توسط باب* برابر است با ۳۷/۷٪. همچنین اگر به‌جای باب* عمل شنود توسط یکی دیگر از سهام‌داران مانند چارلی* و یا دیوید* روی رشته‌ها انجام گیرد، میانگین نرخ خطای تولید شده توسط آنها برابر با نرخ خطای باب* است زیرا سیستم متقارن است.

۵-۲- بازتاب و اندازه‌گیری تصادفی رشته‌ها توسط باب*

در این حالت باب* به‌طور تصادفی ذرات متعلق به رشته‌های دیگر را اندازه‌گیری یا بازتاب می‌کند. احتمال هر عمل توسط او برابر $\frac{1}{2}$ است. ابتدا فرض کنیم باب* روی رشته C شنود کند. در

نمونه‌های اول و دوم اگر باب* ذرات مربوطه را بازتاب کند درحالی‌که باب و چارلی هردو روی آن ذره اندازه‌گیری کرده‌اند، باب* با انجام عمل تصادفی، نیمی از اطلاعات کلید را از دست می‌دهد. در نمونه‌های دوم تا هشتم، اندازه‌گیری یا بازتاب، حالت ذرات را تغییر نمی‌دهد و نمی‌توان از آن‌ها برای تشخیص وجود استراق‌سمع استفاده کرد. در نمونه‌های نهم، دهم، دوازدهم و چهاردهم، وجود استراق‌سمع کننده توسط آلیس قابل تشخیص نیست اما نمونه‌های یازدهم، سیزدهم، پانزدهم و شانزدهم هریک به احتمال ۵۰ ٪ استراق‌سمع را آشکار می‌کنند. به این ترتیب در شانزده نمونه معرفی شده، میانگین نرخ خطای تولید شده توسط باب* برابر است با

$$\frac{1}{16}\times\left(0+0+0+0+0+0+0+0+0+0+0+\frac{1}{2}+0+\frac{1}{2}+0+\frac{1}{2}+\frac{1}{2}\right)=12/5\%.$$

به‌طور مشابه اگر باب* فقط روی رشته D شنود کند، بدون توجه به عملیات چارلی، شنود او تنها زمانی مشخص می‌شود که دیوید ذرات را در پایه هادامارد به سوی آلیس بازتاب کند. بنابراین میانگین نرخ خطای تولید شده توسط باب* برابر است با ۱۲/۵٪. علاوه بر این اگر باب* روی رشته‌های C و D به طور تصادفی اندازه‌گیری یا بازتاب کند و سپس آن ذرات را به سایر سهام‌داران بفرستد، شنود او نرخ خطای ۱۸/۷۵٪ را تولید می‌کند. به طور مشابه اگر به‌جای باب* یکی از چارلی* یا دیوید* روی رشته‌ها شنود کنند، نرخ خطای تولید شده توسط آن‌ها همانند نرخ خطای تولید شده توسط باب است زیرا سیستم متقارن می‌باشد.

بنابراین، با انجام تصادفی اندازه‌گیری یا بازتاب، علاوه بر این‌که حضور استراق‌سمع کننده تشخیص داده می‌شود، نیمی از اطلاعات کلید نیز نابود می‌گردد و قابل دست‌یابی نیست.

۵-۳- عملیات مشابه باب روی رشته‌ها توسط باب*

بهترین کاری که باب می‌تواند روی رشته C انجام دهد این است که همان عملیاتی را که خودش بر روی کیوبیت‌های رشته B انجام می‌دهد، روی رشته C نیز اعمال کند. به عبارتی اگر باب* روی ذره رشته B اندازه‌گیری انجام می‌دهد، آن‌گاه کیوبیت متناظر در رشته C را اندازه‌گیری کند و اگر کیوبیت رشته B را بازتاب می‌کند، کیوبیت متناظر در رشته C را نیز بازتاب کند.

در نمونه اول باب* روی رشته C اندازه‌گیری انجام می‌دهد و می‌تواند بدون تولید خطا به اطلاعات کلید دسترسی پیدا کند. در نمونه‌های دوم تا هشتم، از آن جایی‌که ذرات در پایه محاسباتی تولید شده‌اند، هیچ تفاوتی بین بازتاب یا اندازه‌گیری نمی‌باشد و تغییری درحالت ذرات ایجاد نمی‌کند. در نمونه‌های نهم، دهم، پانزدهم و شانزدهم از آن‌جایی که چارلی و باب، هر دو یا ذره را بازتاب یا اندازه‌گیری می‌کنند، وجود استراق‌سمع کننده قابل تشخیص نیست. در نمونه‌های یازدهم و سیزدهم، ذرات توسط آلیس در پایه هادامارد تولید شده‌اند و چارلی آن ذرات را برای آلیس بازتاب می‌کند. بنابراین زمانی‌که باب* آن ذرات را اندازه‌گیری کند، استراق‌سمع با احتمال ۱۰۰٪ تشخیص داده می‌شود. بنابر موارد ذکر شده فوق، میانگین نرخ خطای تولید شده توسط باب* برابر است با:

$$\frac{1}{16}\times(0+0+0+0+0+0+0+0+0+0+0+1+0+1+0+0+0)=12/5\%.$$

به‌طور مشابه اگر باب* فقط روی رشته D شنود کند، بدون در نظر گرفتن عملیات چارلی، در شانزده نمونه معرفی شده، میانگین نرخ خطای تولید شده توسط باب* همان ۱۲/۵٪ است. به‌علاوه اگر باب* عملیات مشابه خود را بر روی هر دو رشته C و D اعمال کند، نرخ خطای تولید شده توسط او ۱۸/۷۵٪ است. به همین ترتیب اگر به‌جای باب*، یکی از چارلی* یا دیوید* روی رشته‌ها عملیات مشابه خود را انجام دهند، نرخ خطای تولید شده توسط آن‌ها به اندازه نرخ خطای تولید شده توسط باب* خواهد بود زیرا سیستم متقارن است.

۵-۴- عملیات متفاوت روی دو رشته

فرض کنیم باب* روی هر دو رشته C و D شنود کند اما در این قسمت روش‌های شنود روی هر رشته لزوما مشابه نیست. به بیان دیگر زمانی‌که باب* روشی را برای استراق‌سمع روی یک ذره برمی‌گزیند، لزوما همان روش را روی ذره دیگر اعمال نمی‌کند. در ادامه حالاتی را که ممکن است اتفاق بیفتد بررسی می‌کنیم.

فرض کنیم باب* یک ذره را اندازه‌گیری و ذره دیگر را به‌طور تصادفی بازتاب یا اندازه‌گیری نماید. میانگین نرخ خطای تولید شده توسط او برابر ۳۱/۲۵٪ است. اگر باب* یک ذره را اندازه‌گیری و عملیات مشابه خود را روی ذره دیگر انجام دهد، میانگین نرخ خطای تولید شده همان ۳۱/۲۵٪ خواهد بود. چنانچه باب* یک ذره را به‌طور تصادفی اندازه‌گیری یا بازتاب کند و روی ذره دیگر عملیات مشابه خود را اعمال کند، میانگین نرخ خطای تولید شده‌ی او برابر ۱۸/۷۵٪ است.

به وضوح اگربه‌جای باب* یکی دیگر مثلا چارلی* یا دیوید* روی دو رشته دیگر با این روش شنود کنند، میانگین نرخ خطای تولید شده توسط هریک از آن‌ها همانند باب* خواهد بود زیرا هیچ‌یک نسبت به دیگری برتری ندارند.

۵-۵- تبانی دو سهام‌دار غیرقابل اعتماد

تاکنون به بررسی شگردهای متفاوت استراق‌سمع توسط یک سهام‌دار غیرقابل اعتماد روی یک یا دو رشته دیگر بحث کردیم و میانگین خطای تولید شده توسط آن شخص را در شانزده حالت

بررسی کردیم. حال فرض کنیم دو سهام‌دار غیرقابل اعتماد به منظور دست‌یابی به اطلاعات کلید با یکدیگر علیه نفر سوم تبانی کنند. فرض کنیم باب* و چارلی* دو سهام‌دار غیرقابل اعتماد باشند که با یکدیگر روی رشته D تبانی کنند و سعی بر به‌دست آوردن اطلاعات دیوید داشته باشند. در این شرایط آن‌ها می‌توانند هریک از شگردهای ذکر شده در قسمت‌های قبل را برگزینند اما از آن‌جایی که این دو برای به‌دست آوردن اطلاعات کلید با یکدیگر تبانی کردند، پس باید روش استراق‌سمع را عاقلانه انتخاب کنند.

بهترین روش برای رسیدن به هدف، انتخاب روش مشابه خود می‌باشد. بنابراین باب* و چارلی* فقط زمانی باید ذرات رشته D را اندازه‌گیری کنند که هر دو نفرشان، ذراتشان را اندازه‌گیری کرده‌اند. در نمونه‌های اول و دوم چون ذرات توسط آلیس در پایه محاسباتی تولید شده‌اند، استراق‌سمع آن دو آشکار نمی‌شود. در نمونه نهم چون دیوید ذره خود را اندازه‌گیری کرده‌است، باز هم استراق‌سمع آن دو آشکار نمی‌شود. در نمونه دهم که دیوید ذره را بازتاب کرده چون باب* و چارلی* اندازه‌گیری می‌کنند، استراق‌سمع آن‌ها توسط آلیس با احتمال ۱۰۰٪ تشخیص داده می‌شود. بنابراین میانگین خطای تولید شده توسط باب* و چارلی* در این روش برابر ۶/۲۵٪ است.

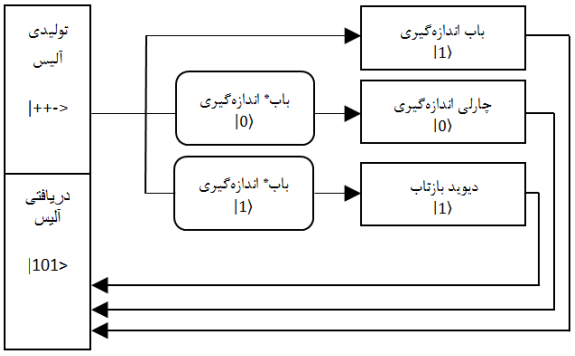
همان‌طور که بررسی شد هیچ راهی برای دست‌یابی به اطلاعات کلید، بدون تولید خطا وجود ندارد و در شرایط استراق‌سمع و به‌دست آوردن اطلاعات کلید، این مسئله حتما در فاز کنترل استراق‌سمع تشخیص داده شده و کلید تولید شده نادیده گرفته می‌شود و پروتکل دوباره از مرحله نخست اجرا می‌شود.

۵-۶- مثال‌ها

در ادامه به‌منظور روشن شدن بیشتر پروتکل پیشنهادی و چگونگی تشخیص وجود استراق سمع به ارائه دو مثال می‌پردازیم.

مثال ۵-۶-۱: فرض کنیم $\varphi = |++-->_i$، i-امین فوتون آلیس باشد. او ذرات $<+|$، $<-|$ و $<+|$ را به ترتیب برای باب، چارلی و دیوید ارسال می‌کند اما باب* به کیوبیت چارلی دست پیدا می‌کند. فرض کنیم باب* هر دو کیوبیت را اندازه‌گیری کند و حاصل با احتمال ۵۰٪ به‌ترتیب برابر $<1|$ و $<0|$ است. سپس کیوبیت خود را برای آلیس و کیوبیت دیوید را برایش ارسال می‌کند. حال اگر دیوید کیوبیت دریافتی را بازتاب نماید، آلیس کیوبیت $<0|$ را دریافت می‌کند که با کیوبیت ارسالی اولیه متفاوت است. بدین ترتیب آلیس به وجود استراق‌سمع کننده پی می‌برد. در روش‌های دیگر نیز آلیس به همین ترتیب استراق‌سمع را تشخیص می‌دهد.

مثال ۵-۶-۲: در شکل (۱) نشان داده شد که آلیس ذرات $<+|$، $<+|$ و $<-|$ را به ترتیب برای باب، چارلی و دیوید ارسال می‌کند و ذرات $<1|$، $<0|$ و $<1|$ را دریافت می‌کند. در شکل (۲) نشان داده می‌شود که باب* به ذرات چارلی و دیوید روی کانال کوانتومی دسترسی پیدا می‌کند. بنابراین کیوبیت دریافتی از دیوید متفاوت از آن چیزی است که آلیس انتظار دارد. در این شرایط آلیس وجود استراق سمع کننده را تشخیص داده و فرایند فوق از مرحله اول از سر گرفته می‌شود.



شکل (۲): فرآیند انجام پروتکل درصورت وجود استراق سمع کننده

۶- مقایسه

در این بخش به مقایسه پروتکل پیشنهادی خود با پروتکل گوا [۱۳]، پروتکل وانگ [۱۱] و پروتکل زی [۱۷] می‌پردازیم.

۱- گوا یک طرح تسهیم راز کوانتومی ارائه کرد که در آن به علاوه بر آلیس، تمام سهام‌داران باید دارای تجهیزات کوانتومی باشند. از طرفی تجهیزات کوانتومی بسیار گران هستند و از طرف دیگر به سهام‌داران قدرت تقلب و استراق‌سمع می‌دهد اما در این پروتکل پیشنهادی، سهام‌داران محدود به انجام عملیات کلاسیکی ذکر شده روی ذرات هستند که هزینه بسیار کمتری دارد.

۲- پروتکل وانگ و پروتکل زی مبتنی بر حالات درهم‌تنیده هستند که درصورت بالا بودن تعداد شرکت‌کنندگان تسهیم راز، قابلیت اجرا شدن ندارند. در این پروتکل تسهیم راز نیمه‌کوانتومی، خاصیت درهم‌تنیدگی ضروری نیست. این پروتکل برای سه سهام‌دار طراحی شده‌است که نه‌تنها از لحاظ تئوری بلکه در عمل نیز امکان‌پذیر است.

۳- بازده آن دسته از پروتکل‌های تسهیم راز نیمه‌کوانتومی که مبتنی‌بر حالات درهم‌تنیده هستند در اصل

می‌تواند به ٪۵۰ برسد. حال آن‌که پروتکل پیشنهاد شده بدون درهم‌تنیدگی است و بنابراین دارای بازده ٪۱۰۰ است.

جدول (۳) به طور خلاصه مقایسه‌ای بین طرح‌های مذکور با طرح پیشنهادی را نشان می‌دهد.

جدول (۳). مقایسه پروتکل پیشنهادی با پروتکل‌های وانگ، گوا و زی

	پروتکل وانگ	پروتکل گوا	پروتکل زی	پروتکل پیشنهادی
حالت کوانتومی	GHZ	فوتون منفرد	GHZ	فوتون منفرد
نیمه‌کوانتومی	بله	خیر	بله	بله
هزینه‌بر	بله	خیر	بله	خیر
درهم‌تنیده	بله	خیر	بله	خیر
تعداد سهام-داران	۲	۲	۲	۳
بازده	٪۵۰	٪۱۰۰	٪۵۰	٪۱۰۰
امن در برابر استراق‌سمع	بله	بله	بله	بله

۷- نتیجه‌گیری

در این مقاله یک پروتکل تسهیم راز نیمه‌کوانتومی بدون حالت درهم‌تنیدگی ارائه گردید و امنیت آن مورد بررسی قرار گرفت. از مزایای سیستم‌های نیمه‌کوانتومی غیر در هم‌تنیده در جهت کاهش هزینه‌ها بهره بردیم. زیرا تمام شرکت‌کنندگان استطاعت تهیه‌ی تجهیزات گران کوانتومی را ندارند. در این پروتکل، آلیس کوانتومی قصد دارد کلید مخفی خود را با باب، چارلی و دیوید کلاسیک به اشتراک بگذارد. باب، چارلی و دیوید کلاسیک محدود به انجام عملیات کلاسیک هستند مانند اندازه‌گیری ذرات در پایه‌ی محاسباتی و ارسال آن‌ها به آلیس و بازتاب ذرات بدون ایجاد اختلال در آن‌ها. باب، چارلی و دیوید نمی‌توانند به اطلاعات محرمانه‌ی آلیس دست پیدا کنند مگر آن‌که بایکدیگر همکاری کنند. سپس نشان دادیم که این پروتکل در برابر استراق‌سمع ایمن است. حتی اگر یکی از باب، چارلی و یا دیوید، غیرقابل اعتماد باشند، با تولید خطا در فاز تشخیص استراق‌سمع توسط آلیس شناسایی می‌شوند. همچنین در این پروتکل تسهیم راز نیمه‌کوانتومی به حالت درهم‌تنیدگی نیازی نیست که موجب افزایش کارایی این طرح می‌گردد خصوصا زمانی‌که تعداد شرکت‌کنندگان تسهیم راز زیاد باشد. بنابراین طرح پیشنهادی، یک پروتکل امن با هزینه‌ی پایین و قابل اجرا می‌باشد.

۸- مراجع

[1] B. Schneier, "Applied Cryptography," Second Edition, John Wiley & Sons, ISBN 0-471-11709-9, 1996.

[2] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613, Nov. 1979.

[3] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," Physical Review A, vol. 59, no. 3, pp. 1829-1834, March 1999.

[4] W. Tittel, H. Zbinden, and N. Gisin, "Experimental demonstration of quantum secret sharing," Physical Review A, vol. 63, no. 4, p. 042301, Mar. 2001.

[5] D. Gottesman, "Theory of quantum secret sharing," Physical Review A, vol. 61, no. 4, p. 042311, Mar. 2000.

[6] A. Karlsson, N. Koashi, and N. Imoto, "Quantum entanglement for secret sharing and secret splitting," Physical Review A, vol. 59, no. 1, p. 162, Jan. 1999.

[7] R. Cleve, D. Gottesman, and H. Klo, "How to share a quantum secret," Physical Review Letters, vol. 83, no. 3, p. 648, 1999.

[8] V. Karimipour, A. Bahraminasab, and S. Bagherinezhad. "Entanglement swapping of generalized cat states and secret sharing," Physical Review A, vol. 65, no. 4, p. 042320, 2002.

[9] S. Bagherinezhad, and V. Karimipour, "Quantum secret sharing based on reusable Greenberger-Horne-Zeilinger states as secure carriers," Physical Review A, vol. 67, no. 4, p. 044302, 2003.

[10] Q. Li, WH. Chan, and DY. Long, "Semiquantum secret sharing using entangled states," Physical Review A, vol. 82, no. 2, p. 022303, 2010.

[11] J. Wang, et al., "Semiquantum secret sharing using two-particle entangled state," Int. J. Quantum Inf, vol. 10, no. 5, p. 1250050, 2012.

[12] M. Boyer, D. Kenigsberg, and T. Mor, "Quantum key distribution with classical Bob," Quantum, Nano, and Micro Technologies, 2007, ICQNM'07, First International Conference on IEEE, p. 10, Jan. 2007.

[13] GP. Guo, and GC. Guo, "Quantum secret sharing without entanglement," Physics Letters A, vol. 310, no. 4, pp. 247-251, 2003.

[14] D. Bouwmeester, et al., "Observation of three-photon Greenberger-Horne-Zeilinger entanglement," Physical Review Letters, vol. 82, no. 7, p. 1345, 1999.

[15] JW. Pan, et al., "Experimental demonstration of four-photon entanglement and high-fidelity teleportation," Physical Review Letters, vol. 86, no. 20, p. 4435, 2001.

[16] CH. Bennett, and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theoretical computer science, vol. 560, pp. 7-11, 2014.

[17] C. Xie, L. Li, and D. Qiu, "A novel semi-quantum secret sharing scheme of specific bits," International Journal of Theoretical Physics, vol. 54, no. 10, pp. 3819-3824, 2015.

[18] A. Yin and F. Fu, "Eavesdropping on Semi-Quantum Secret Sharing Scheme of Specific Bits," International Journal of Theoretical Physics, pp. 1-9, 2016.

Journal Of Electronical & Cyber Defence
Vol. 4, No. 3, 2016, Serial No.15

Semiquantum Secret Sharing Using Three Particles Without Entanglement

Z. Karimifard, S. Mashhadi, D. Ebrahimi Bagha*

*Islamic Azad University, Central Tehran Branch, Tehran, Iran

(Received: 23/05/2016, Accepted: 01/08/2016)

ABSTRACT

In this paper we propose a (3,3)*-threshold semiquantum secret sharing protocol without entanglement in which the quantum service provider shares a secret key with three classical parties who are restricted to measuring the qubits in the classical basis* {0, 1} *and sending or reflecting the qubits without disturbance. Also entanglement is not necessary in this semiquantum secret sharing protocol especially when the number of the parties of secret sharing is large. The presented protocols are also showed to be secure against eavesdropping.*

Keywords: Quantum Secret Sharing, Semiquantum Secret Sharing, Quantum Without Entanglement, Quantum Information, Quantum Communication, Quantum Key Distribution

* Corresponding Author Email: D-ebrahimibagha-math@iauctb.ac.ir