
بسم الله الرحمن الرحيم

بررسی و تحلیل محاسبات کوانتومی خصوصی (محاسبات کوانتومی کور)

- درس: الکترونیک کوانتومی
- استاد: دکتر شهرام محمد نژاد

فهرست مطالب


مقدمه
معرفی محاسبات کوانتومی کور
مدلسازی امنیت
پروتکل MBQC
جمع بندی

مقدمه

- انجام بهتر وظایف محاسباتی خاص با کامپیوترهای کوانتومی نسبت به کامپیوترهای کلاسیک
- تلاش های اخیر صورت گرفته برای دسترسی به پردازنده های کوانتومی از طریق اینترنت و اعطای محاسبات به سیستم های راه دور

- نگرانی های امنیتی؛ اگر محاسبات بر روی سخت افزار غیرقابل اعتماد صورت پذیرد، این احتمال وجود دارد که حریم خصوصی و یا درستی محاسبات به خطر بیفتد
- برای غلبه بر این نگرانی ها، خواستار راهی برای انتقال وظایف به سرور دور با اطمینان از حفظ حریم خصوصی و اطمینان از صحت نتیجه هستیم، حتی از سرورهایی که خودشان اجرا کننده هستند.

معرفی محاسبات کوانتومی کور

- ✓ استفاده از کامپیوترهای کوانتومی برای انجام محاسبات کوانتومی نیازمند سخت افزار گران قیمت و پیچیده است.

غیرقابل دسترس
برای اکثر کاربران

- ❑ دسترسی از راه دور به کامپیوترهای کوانتومی از طریق کامپیوترهای متعارف
- ❑ وجود شبکه های ارتباط جهانی با سرعت بالا و پردازشگرهای کلاسیک موجود

نگرانی های امنیتی

معرفی محاسبات کوانتومی کور

- رمزگذاری یک راه مخفی کردن ارتباط بین سرویس گیرنده و سرور
- کدهای احراز هویت برای شناسایی هر گونه تلاش برای تغییر و اصلاح این پیام ها

محاسبات کوانتومی کور (BQC)

مطرح شدن تعدادی از پروتکل ها با هدف حل مسائل مربوط به حریم خصوصی برای محول کردن محاسبات کوانتومی

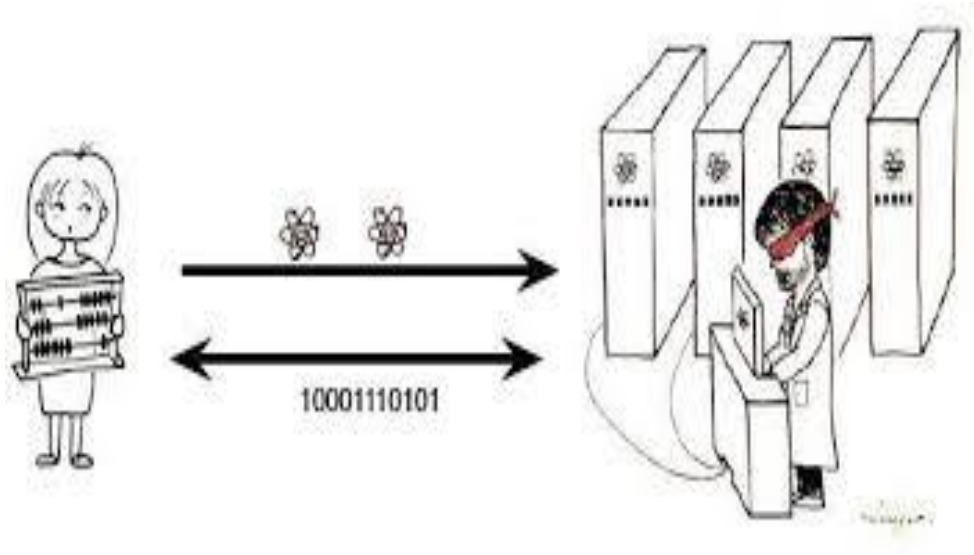
اجرای محاسبات کوانتومی با استفاده از یک یا چند سرور کوانتومی دور برای سرویس گیرنده فراهم می کند، در حالی که ساختار محاسبات را پنهان نگه می دارند.

معرفی محاسبات کوانتومی کور

محاسبات کوانتومی کور به کاربران اجازه می‌دهد تا بدون داشتن یک کامپیوتر کوانتومی شخصی، کارهای محاسباتی خود را به سرورهای کوانتومی بسپارند.

محاسبات کوانتومی کور

✓ آماده سازی یا اندازه گیری حالت های کیوبیت



معرفی محاسبات کوانتومی کور

اجرای محاسبات کوانتومی برای سرویس گیرنده ی کاملا کلاسیکی و سرور کوانتومی

- آماده سازی یا اندازه گیری حالت های تک کیوبیتی
- داشتن پردازنده کوانتومی کوچک

تنظیماتی که نیازهای یک سرویس گیرنده کلاسیکی را تامین کند

- برقراری ارتباط سرویس گیرنده با چندین سرور

تنظیماتی که برای چندین سرور کوانتومی غیرمرتبط مجاز شمرده شود

امنیت

تعریف امنیت:

- ✓ سرور یا سرورهای مخرب، بر اساس اطلاعاتی که در طول پروتکل دریافت می کنند در تمایز بین محاسبات احتمالی که توسط سرویس گیرنده انتخاب می شود باید ناتوان باشند.
- ✓سرورها همیشه باید منابعی که به آن ها متعهد هستند برای محاسبات را بدانند. بنابراین ابعاد مدار اطلاعات کمی را در ارتباط با محاسبات پنهان شده فاش می کنند.
- ✓ در تعریف امنیت برای محاسبات کور، مهم است که این نشت اطلاعات را به حساب آوریم.

ویژگی نامطلوب

- به طور کامل مشخص نمی کند که چگونه یک پروتکل به عنوان بخشی از یک سیستم بزرگتر رفتار خواهد کرد

x → توصیف محاسبات سرویس گیرنده

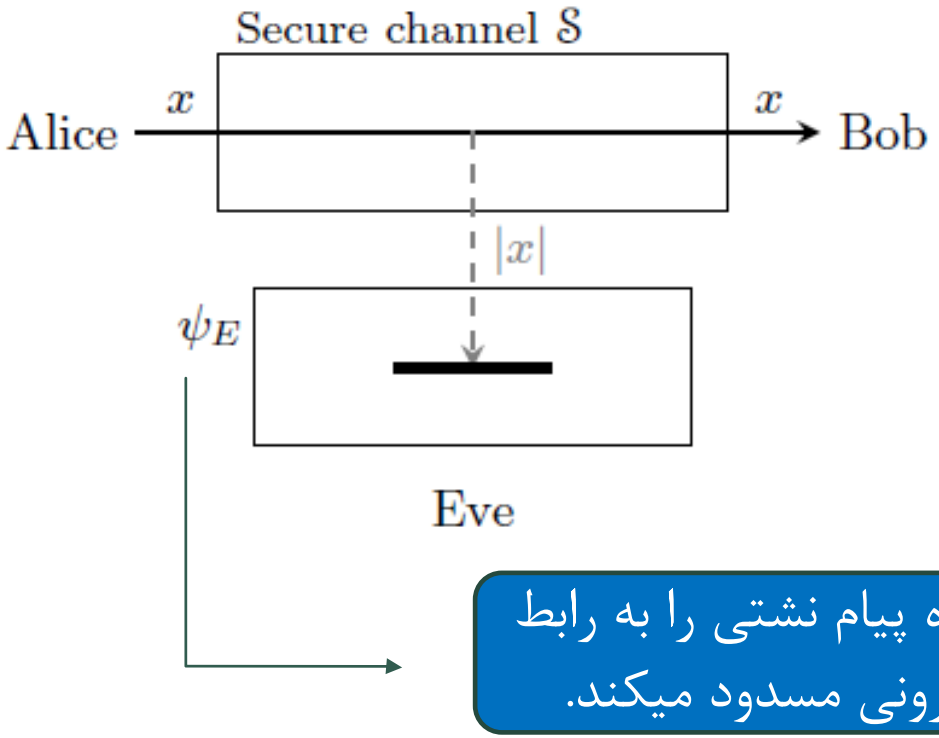
L(x) → توزیع اطلاعات کوانتومی و کلاسیکی دریافت شده توسط سرور

پروتکل در بیشترین مقدار L(x) ⟵ "کوری همزمان با نشت"

اطلاعاتی است که به طور اجتناب ناپذیر نشت کرده

امنیت

- ✓ پیام x از رابط A دریافت می شود
- ✓ طول پیام در رابط E نشت داده می شود
- ✓ خروجی x به رابط B می رود



اندازه پیام نشتی را به رابط درونی مسدود میکند.

تعریف کامل تر از رفتار پروتکل های BQC

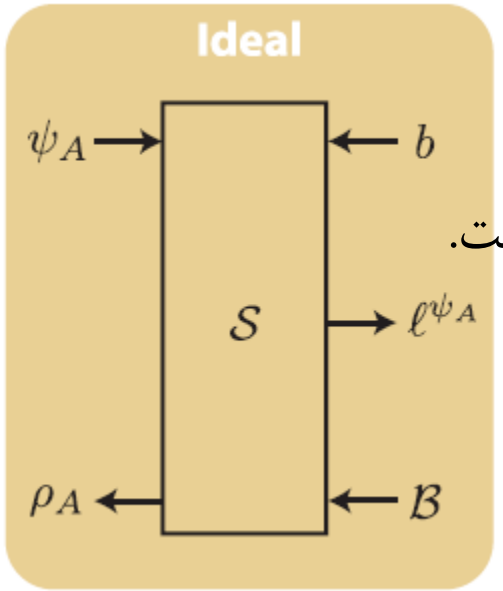
مفهوم منبع ایده آل

سیستم ψA: توصیف محاسبات سرویس گیرنده همراه با هر ورودی کوانتومی

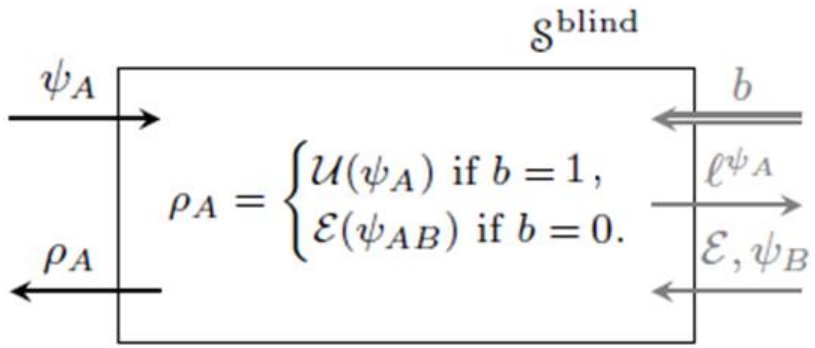
سیستم ρA: نشان دهنده خروجی حاصل توسط سرویس گیرنده

$l^{\psi A}$: نشان دهنده اطلاعات نشت شده بر اساس محاسبات سرویس گیرنده برای سرور

تک بیت b: به صورت پیش فرض صفر است که نشان دهنده ی غیرفعال بودن B (رابط تقلب) است.



مدلسازی امنیت



فعال بودن رابط B

$\rho A = U(\psi A)$

سرور قابلیت مداخله در خروجی نهایی را نیز دارد.

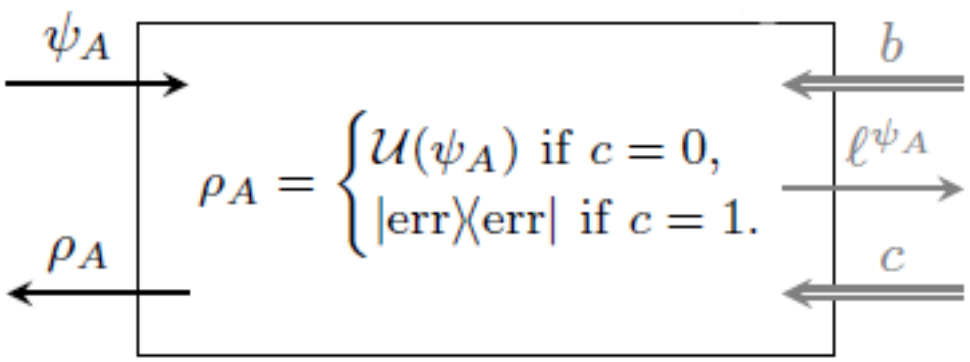
به منبع ایده آل حالت کوانتومی ψB می دهد به همراه نگاشت ε که می تواند با ورودی ψA درهم آمیخته شود.

$\rho A = \varepsilon(\psi AB)$

در این حالت تنها کوری به حساب آورده شده و چیزی درباره توانایی سرور برای دست کاری خروجی نهایی نمی گوید.

مدلسازی امنیت

در مواردی که در آن قابلیت تایید وجود دارد، منبع ایده آل S با انتخاب B به عنوان تک بیت c تکمیل می شود.

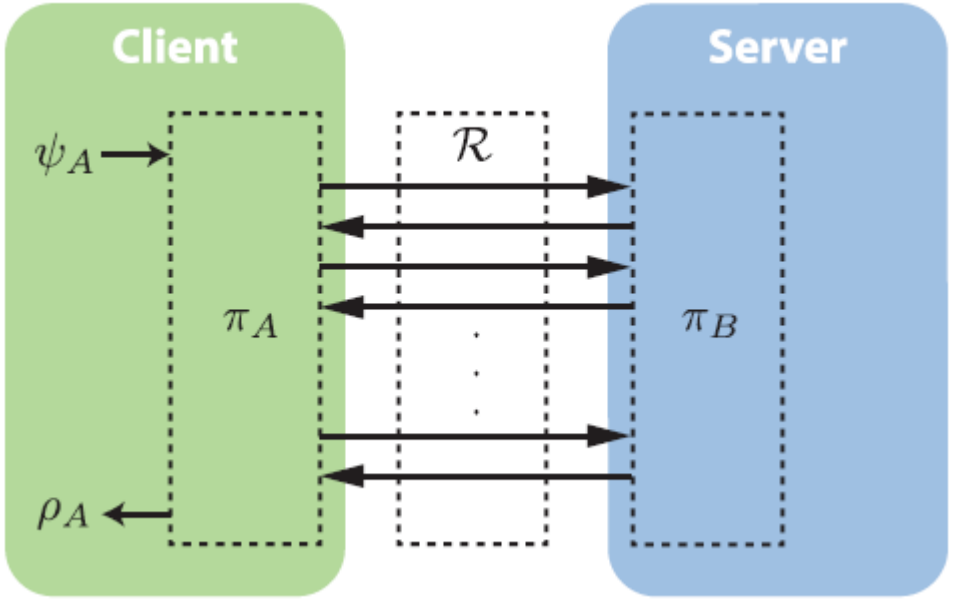


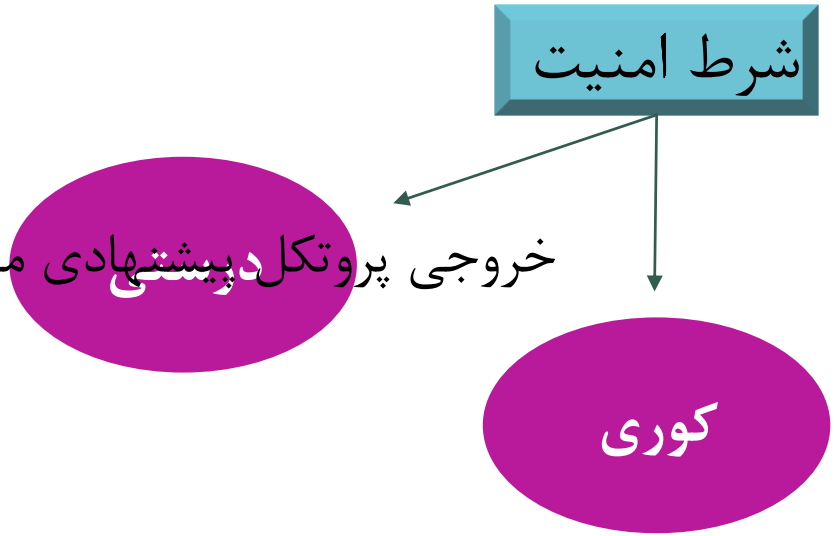
سرور متقلب تشخیص داده می شود و پرچم خطا به جای محاسبات اشتباه خارج می شود.

- ✓ C احتمال این که سرور موجب خطا در محاسبات شود را ذخیره می کند

رفتار پروتکل BQC

- یک پروتکل BQC واقعی از یک جفت پروتکل، π_A برای سرویس گیرنده و π_Bبرای سرور تشکیل شده است که از طریق کانال ارتباطی نشان داده شده توسط Rبرهمکنش می کنند.



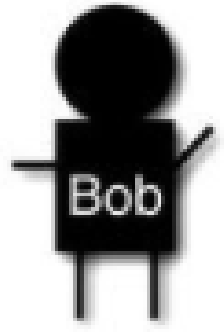


خروجی پروتکل منطبق با رفتار منبع ایده آل

سرور تنها قادر به دانستن برهمکنش با عملکرد ایده آل باشد.

پروتکل MBQC

محاسبات کوانتومی کور مبتنی بر اندازه گیری (MBQC)



کانال کوانتومی و کانال کلاسیک

کامپیوتر کلاسیک

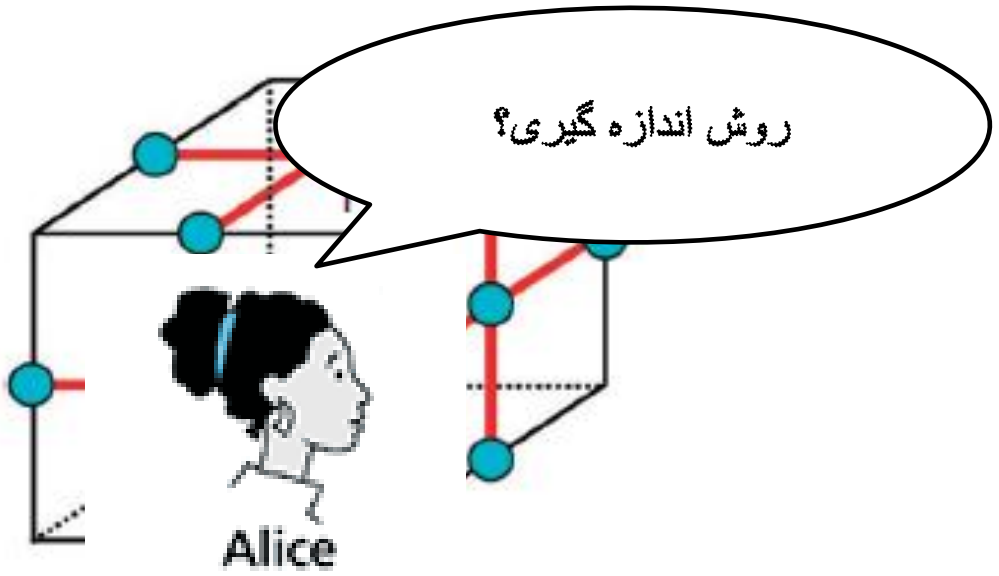
دستگاه کوانتومی

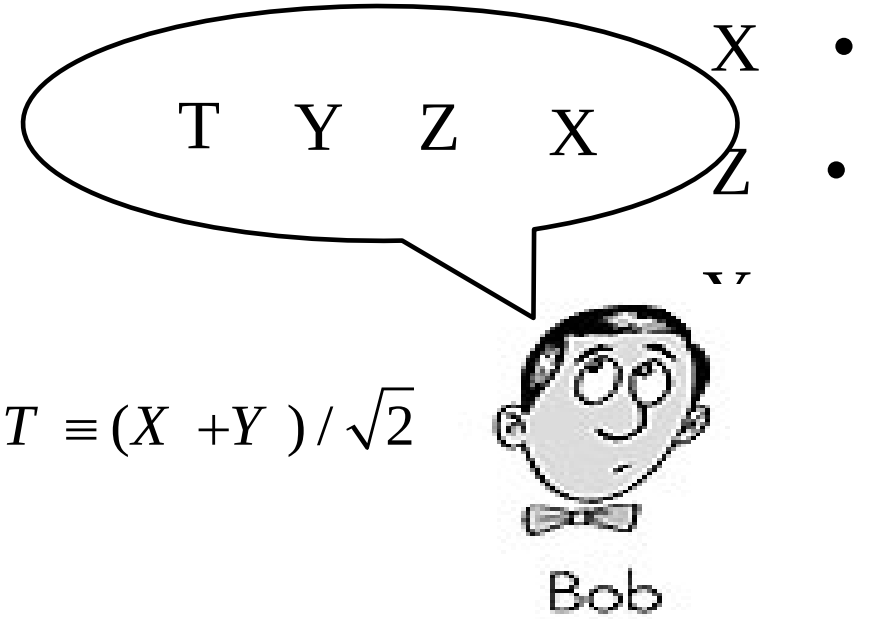
فاقد حافظه کوانتومی

تکنولوژی کاملا کوانتومی

پروتکل MBQC

حالت گراف در شبکه مکعبی سه بعدی L





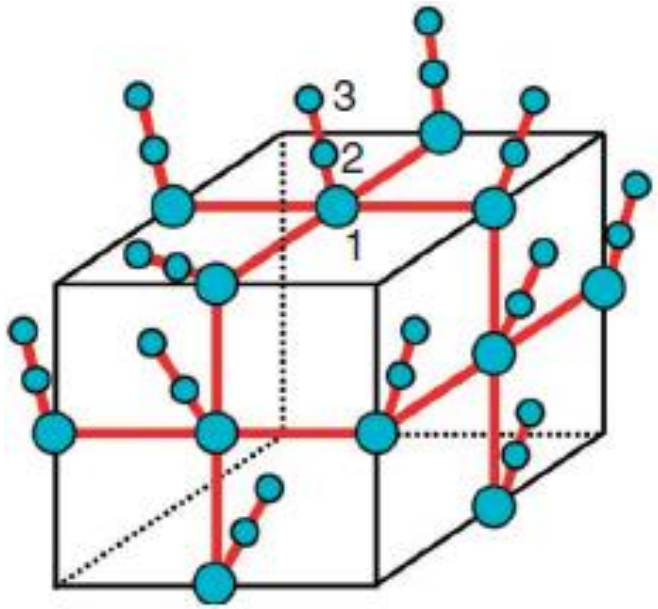
اندازه گیری را در هر کیوبیت انجام می دهد و می تواند الگوریتم آلیس را بفهمد

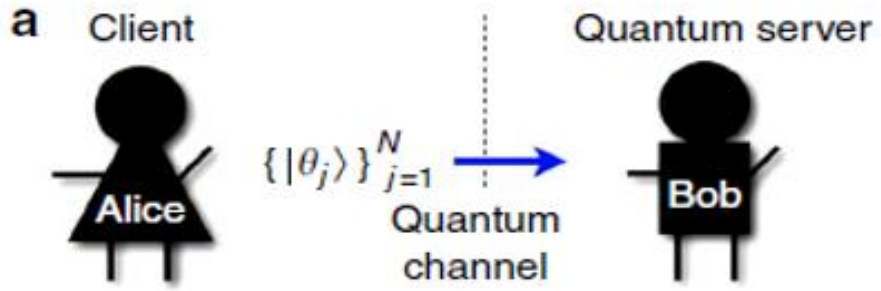
پروتکل MBQC

۱. آلیس می تواند اجازه دهد باب اندازه گیری را بر اساس $\{|0\rangle \pm e^{i\phi}|1\rangle\}$ برای هر کیوبیت از حالت گراف انجام دهد که باب در حالتی است که نمی تواند چیزی راجع به Φ بفهمد.

$$\phi \in \{(k\pi/4)|k = 0,1,..,7\}$$

۲. اندازه گیری تک کیوبیت بر اساس X، Y، T یا Z می تواند روی حالت خوشه ای سه کیوبیت خطی تنها بر مبنای اندازه گیری $\{|0\rangle \pm e^{i\phi}|1\rangle\}$ شبیه سازی می شود.

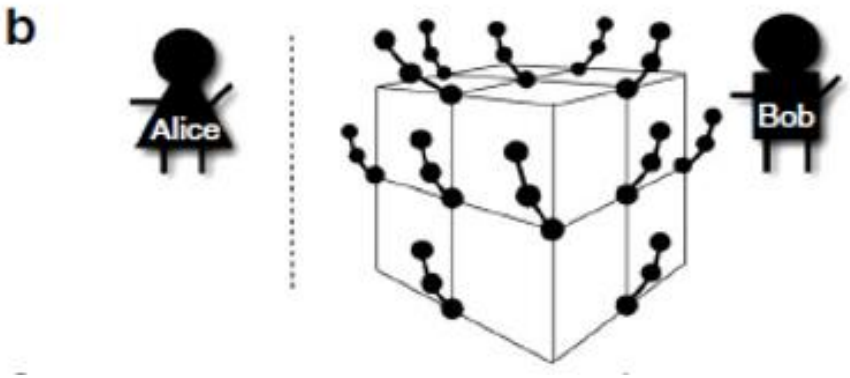




$$\left|\theta_j\right\rangle \equiv \left|0\right\rangle + e^{i\theta j}\left|1\right\rangle$$

$$\theta_j \in \{(k\pi/4)\big|k = 0,1,...,7\}(j = 1,2,...,N)$$

$$\Theta \equiv \{\theta_j\}_{j=1}^{N}$$

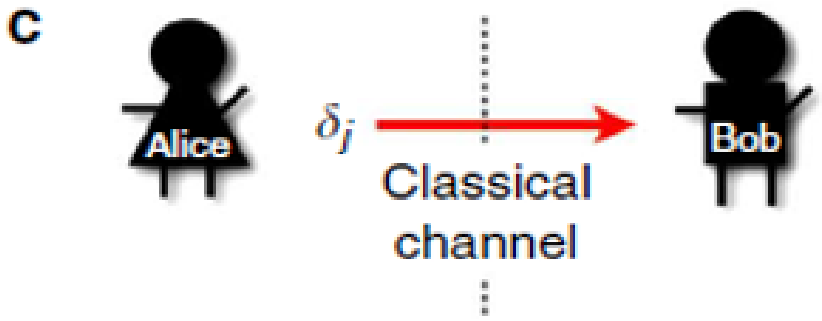


حالت N کیوبیت توسط $\left|C_\Theta\right\rangle$ ایجاد می شود

$$|C_\Theta\rangle = \left(\bigotimes_{k,l} CZ_{k,l}\right)\left(\bigotimes_{j=1}^{N} e^{-iZ\theta_j/2}\right)|+\rangle^{\otimes N}$$

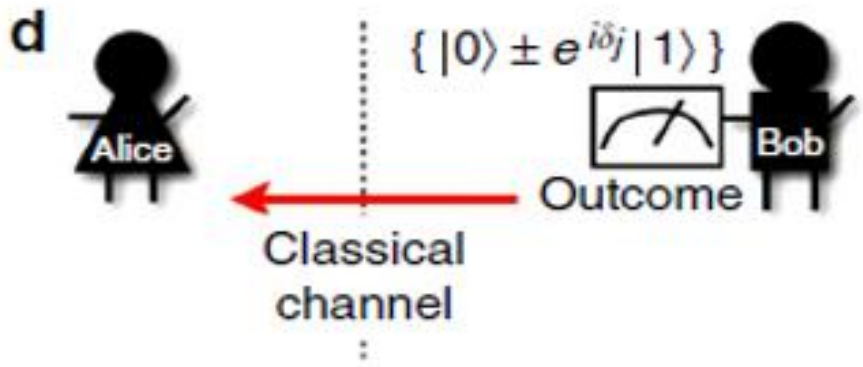
$$= \left(\bigotimes_{j=1}^{N} e^{-iZ\theta_j/2}\right)\left(\bigotimes_{k,l} CZ_{k,l}\right)|+\rangle^{\otimes N}$$

آلیس از باب می خواهد تا jامین کیوبیت از $|C_\Theta\rangle$ اندازه گیری کند.

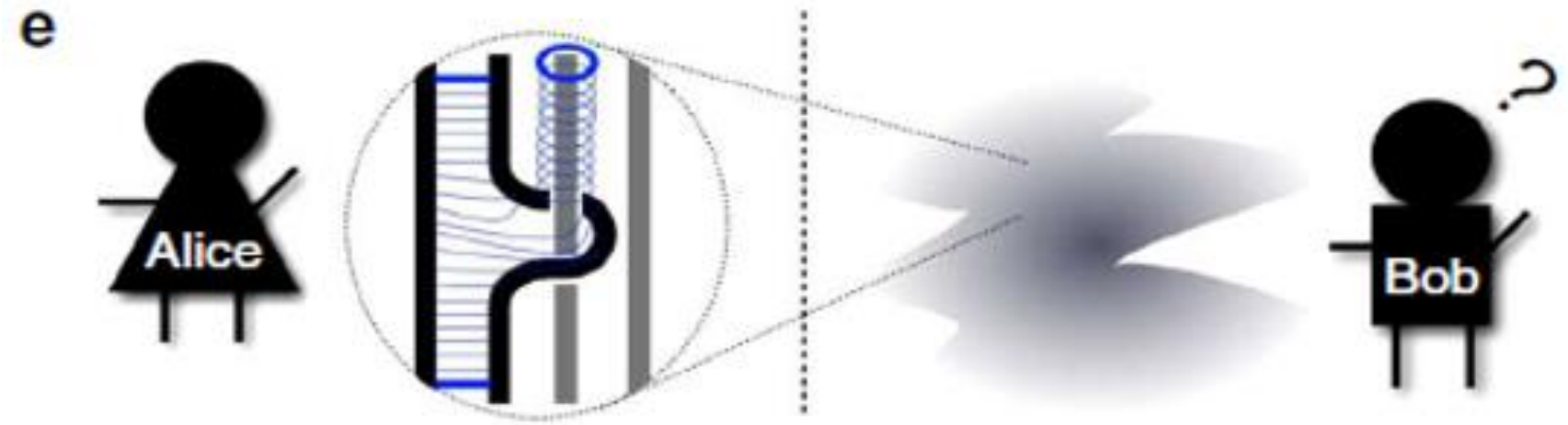


$$\delta_j \equiv \phi'_j + \theta_j + r_j\pi \pmod{2\pi}$$

یک عدد تصادفی
$r_j \in \{0,1\}$

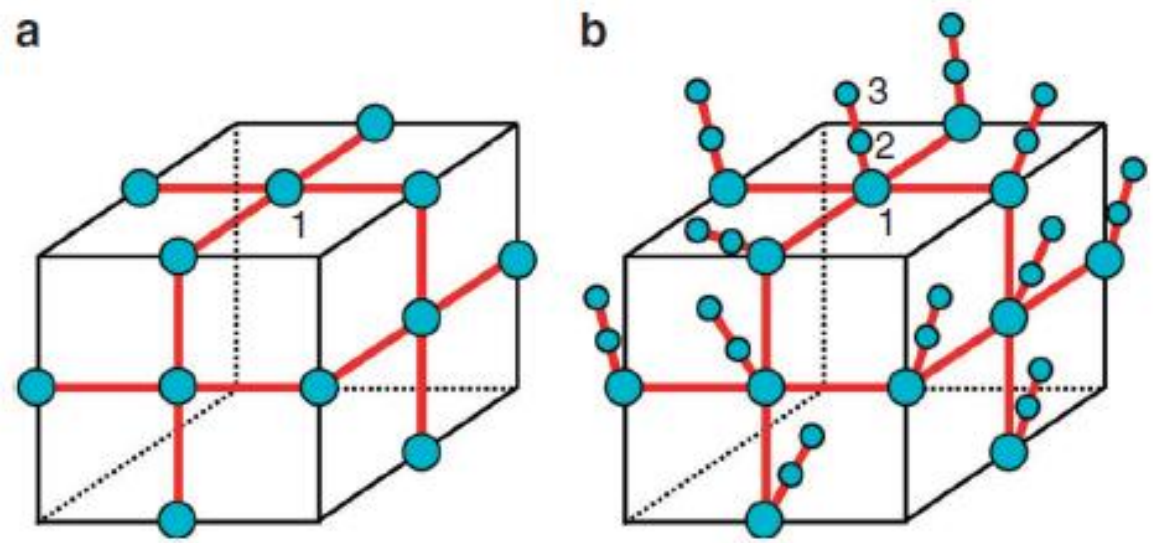


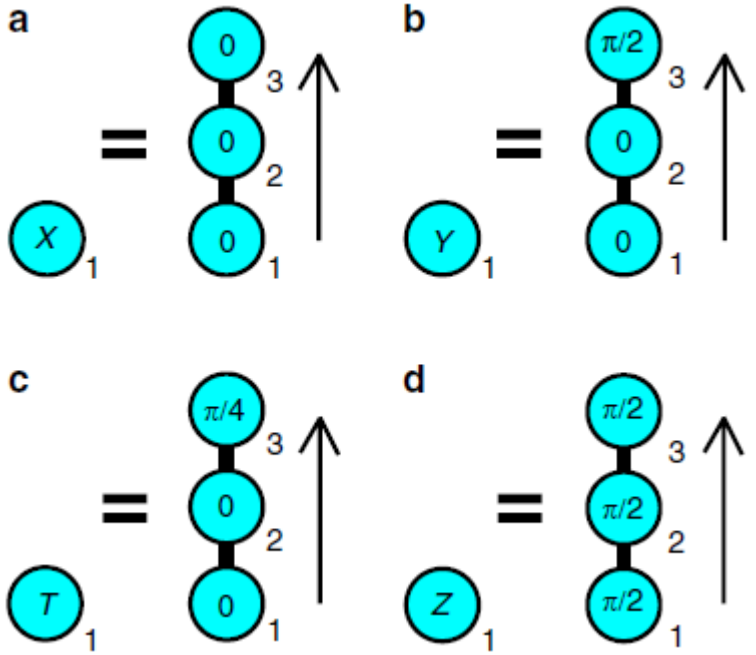
باب jامین کیوبیت را اندازه گیری می کند و نتایج اندازه گیری را به آلیس از طریق کانال کلاسیکی باز می گرداند.



آلیس ساختار محاسبات کوانتومی خود را از باب مخفی نگه می دارد و پردازش کلاسیکی برای تصحیح خطا با استفاده از نتایج اندازه گیری باب انجام می دهد.

پروتکل MBQC





$|C_\Theta\rangle$ بر شبکه ' L می تواند MBQC را روی شبکه L، به تنهایی و بر مبنای اندازه گیری $\{|0\rangle \pm e^{i\phi}|1\rangle\}$ شبیه سازی کند.

پروتکل MBQC

درستی

آلیس جواب صحیح از محاسبات کوانتومی مورد نظر خود به دست می آورد.

کوری

باب نمی تواند چیزی درباره ورودی، خروجی و الگوریتم آلیس پی ببرد.

جمع بندی

- در سال های اخیر، تعدادی از پروتکل ها با هدف حل مسائل مربوط به حریم خصوصی برای محول کردن محاسبات کوانتومی مطرح شده اند

- وجود پروتکل های کور به اندازه کافی امن، برای یک سرویس گیرنده کلاسیکی و سرور کوانتومی اجرای محاسبات کوانتومی را امکان پذیر کرده است.

- با تقویت یک سرویس گیرنده کلاسیکی به قابلیت های کوانتومی مانند اندازه گیری و آماده سازی حالت های تک کیوبیتی می توان به محاسبات کوانتومی دست یافت.


با تشکر از توجه شما