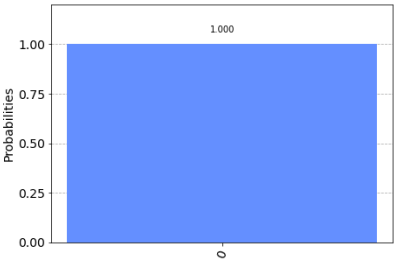
۱ توزیع کلید کوانتومی

اگر آلیس و باب بخواهند اطلاعات حساسی را از طریق یک شبکه غیرامن تبادیل کنند باید از روش‌های «رمزنگاری» استفاده کنند. رمزنگاری حوزه وسیعی است که هدف ما در این درس پرداختن به آن نیست. برای ادامه این ارائه کافی است که بدانید داشتن یک «کلید مخفی» که شخص دیگری به جز آلیس و باب از آن اطلاع ندارد برای تبادل اطلاعات کاربردی خواهد بود. اصطلاحاً آلیس و باب می‌توانند از طریق آن «رمزنگاری متقارن» انجام دهند. در ادامه فرض می‌کنیم که آلیس و باب از طریق یک لینک کوانتومی می‌توانند با یکدیگر تبادل اطلاعات داشته باشند و حوا سعی می‌کند که از طریق شنود لینک اطلاعات حساس آنها را استخراج کند. یکی از روش‌های پیاده‌سازی لینک‌های کوانتومی استفاده از «فیبر نوری» است که از طریق آن می‌توان ذرات نور (فوتون) را جابه‌جا کرد. هر فتون دارای یک ویژگی به نام «قطبیت» است که دو حالت ممکن دارد (معادل $|0\rangle$ و $|1\rangle$). به این ترتیب می‌توان از طریق آن کیوبیت جابه‌جا کرد.

در ادامه با یک پروتکل برای به اشتراک‌گذاری یک کلید مخفی بین آلیس و باب می‌پردازیم. این پروتکل بر این واقعیت استوار است که «اندازه‌گیری» یک کیوبیت حالت آن را تغییر می‌دهد. به این ترتیب، اگر حوا کیوبیتی که آلیس برای باب فرستاده است را اندازه‌گیری کند، ممکن است حالت کیوبیت را تغییر دهد و حالت کیوبیتی که باب دریافت می‌کند با حالت ارسالی آلیس متفاوت باشد. برای مشاهده این پدیده، می‌توانیم از یک شبیه‌سازی ساده کمک بگیریم. به این منظور دو سناریوی مختلف بدون حضور حوا و با حضور او را شبیه‌سازی می‌کنیم. در سناریوی اول، آلیس صفر در پایه هادامارد را برای باب ارسال می‌کند ($|+\rangle$) و باب نیز پس از تبدیل کیوبیت دریافتی آن را اندازه‌گیری می‌کند. در این شرایط، بدون مزاحمت حوا، باب همیشه صفر را به عنوان حاصل اندازه‌گیری بدست می‌آورد. به قطعه کد زیر و مدار معادل آن در شکل ۱ نگاه کنید:

```
from qiskit import QuantumCircuit, execute, Aer
from qiskit.visualization import plot_histogram, plot_bloch_multivector
from numpy.random import randint
import numpy as np

qc = QuantumCircuit(1,1)
qc.h(0)
```



(ب) حاصل اندازه‌گیری باب

(آ) مدار تبادل داده

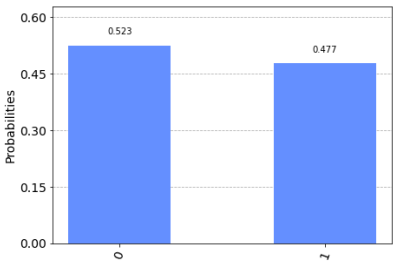
شکل ۱: تبادل داده بدون دخالت حوا

```
qc.barrier()
qc.h(0)
qc.measure(0,0)

display(qc.draw("mpl"))
svs = Aer.get_backend('qasm_simulator')
job = execute(qc, svs)
plot_histogram(job.result().get_counts())
```

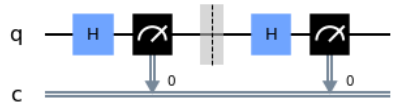
در سناریوی دوم، حوا در میانه راه کیوبیت ارسالی آلیس را اندازه‌گیری می‌کند. در نتیجه این دخالت حوا باعث می‌شود که حالت کیوبیت ارسالی آلیس به یکی از حالت‌های $|0\rangle$ یا $|1\rangle$ تبدیل شود. در این شرایط باب در نیمی از اوقات مقدار متفاوتی از مقدار ارسالی آلیس را مشاهده می‌کند. قطعه کد زیر و مدار معادل آن در شکل ۲ را ببینید. در شکل ملاحظه می‌کنید که در ۵۰ درصد مواقع باب مقدار اشتباهی را ملاحظه می‌کند و به این ترتیب او و آلیس می‌توانند تشخیص دهند که دخالتی رخ داده است. با تکرار این فرایند (استفاده از کیوبیت‌های بیشتر) می‌توان کاری که دخالت هر عنصر شنودکننده‌ای با احتمال بالا تشخیص داده شود.

```
qc = QuantumCircuit(1,1)
qc.h(0)
qc.measure(0, 0)
qc.barrier()
qc.h(0)
qc.measure(0,0)

display(qc.draw())
svs = Aer.get_backend('qasm_simulator')
job = execute(qc, svs)
plot_histogram(job.result().get_counts())
```

پروتکل به اشتراک‌گذاری امن کلید مخفی به صورت کلی به شکل زیر کار می‌کند:



(ب) حاصل اندازه‌گیری باب



(آ) مدار تبادل داده

شکل ۲: تبادل داده با دخالت حوا

۱. آلیس یک رشته بیت تصادفی را تولید می‌کند و برای هر بیت به صورت تصادفی یکی از پایه‌های محاسباتی و یا هادامارد را انتخاب می‌کند.

۲. آلیس هر بیت را به پایه‌ای که انتخاب کرده است منتقل می‌کند و حاصل را از طریق لینک کوانتومی برای باب ارسال می‌کند.

۳. باب برای هر کیوبیت به صورت تصادفی یکی از پایه‌های محاسباتی و یا هادامارد را انتخاب می‌کند و کیوبیت‌ها را در پایه‌های انتخاب‌شده اندازه می‌گیرد.

۴. آلیس و باب پایه‌های انتخابی برای هر کیوبیت را به صورت عمومی با یکدیگر به اشتراک می‌گذارند. کیوبیت‌هایی که در پایه‌های یکسان تولید و اندازه‌گیری شده‌اند ذخیره می‌شوند و سایر کیوبیت‌ها دور ریخته می‌شوند.

۵. آلیس و باب بخشی از بیت‌های متناظر کیوبیت‌های حفظ‌شده را با هم به اشتراک می‌گذارند. اگر این بیت‌ها یکسان باشند آن‌ها می‌توانند تا حد زیادی مطمئین باشند که کلیدشان شنود نشده است و می‌توانند از آن استفاده کنند. بیت‌هایی که برای مقایسه به صورت عمومی منتشر شده‌اند از کلید نهایی حذف می‌شوند، چرا که دیگر مخفی نیستند و قدرت رمزنگاری را کاهش می‌دهند.

در عمل ممکن است بیت‌های بیشتری جهت مقابله با خطای کانال و تصحیح پیام نیز لحاظ شود که در اینجا به آنها پرداخته نشده است. همچنین، ممکن است به جهت افزایش مقاومت در برابر شنود تعداد بیت‌ها افزایش یابد.

۱.۱ مثال ۱: بدون دخالت حوا

فرض کنید که آلیس رشته شش بیتی زیر را به صورت تصادفی تولید می‌کند:

$$0, 0, 1, 0, 1, 0.$$

سپس آلیس برای هر بیت یک پایه انتخاب می‌کند. فرض کنید به صورت تصادفی سه پایه اول محاسباتی و سه پایه دوم هادامارد انتخاب شده باشند. به این ترتیب آلیس به کیوبیت‌های زیر می‌رسد:

$$|0\rangle, |0\rangle, |1\rangle, |+\rangle, |-\rangle, |+\rangle.$$

حال آلیس این رشته کیوبیتی را برای باب ارسال می‌کند. باب برای هر کیوبیت یک پایه اندازه‌گیری به تصادف انتخاب می‌کند. فرض کنید حاصل به این ترتیب است که اولی در پایه محاسباتی، دومی هادامارد و همین طور یکی در میان تا آخر باشد. در نتیجه، باب بیت‌های زیر را اندازه‌گیری می‌کند:

$$0, 1, 1, 0, 0, 0.$$

فرض می‌کنیم که بیت‌های دوم و پنجم به دلیل مغایرت پایه‌های کدگذاری و اندازه‌گیری در سمت آلیس و باب متفاوت شده‌اند. حال آلیس و باب پایه‌ها را با هم به اشتراک می‌گذارند و متوجه می‌شوند که برای کیوبیت‌های غیر از دوم و پنجم از پایه‌های یکسان استفاده کرده‌اند. در نهایت، فرض کنید که باب بیت‌های اول و آخر را برای آلیس ارسال می‌کند. آلیس متوجه می‌شود که این بیت‌ها با بیت‌های تولیدی خودش یکسان هستند. در نتیجه آلیس و باب به توافق می‌رسند که رمز آنها شنود نشده است. به این ترتیب آلیس و باب بیت‌های سوم و چهارم را که به صورت عمومی اعلان نشده‌اند به عنوان کلید مخفی خود انتخاب می‌کنند.

۲.۱ مثال ۲: با دخالت حوا

فرض کنید که سناریوی بالا تکرار شود. اما در حین ارسال کیوبیت‌ها از سمت آلیس به باب، حوا در حال شنود کانال بوده است. حوا تمام کیوبیت‌ها را شنود و در پایه‌های محاسباتی اندازه‌گیری می‌کند. در نتیجه او رشته بیت را بدست می‌آورد:

$$0, 0, 1, 0, 1, 1.$$

در این شرایط حوا بیت آخر را اشتباه متوجه شده است. او سپس این بیت‌ها را برای باب ارسال می‌کند. باب، مشابه سناریوی قبلی آنها را یکی در میان در پایه‌های محاسباتی و هادامارد اندازه می‌گیرد. در نتیجه او به رشته زیر دست پیدا می‌کند:

$$0, 1, 1, 1, 1, 0.$$

باب به دلیل استفاده از پایه هادامارد بیت‌های زوج ارسالی از سمت حوا را برعکس می‌کند (هر نتیجه تصادفی دیگر نیز قابل تصور است). حال آلیس و باب پایه‌های انتخابی خودشان را مقایسه می‌کنند و مشابه سناریوی قبل بیت‌های

دوم و پنجم را دور می‌اندازند. سپس بیت‌های اول و آخر را مقایسه می‌کنند. چون یکسان است آلیس و باب به این نتیجه می‌رسند که شنودی اتفاق نیفتاده است. در حالی که اگر بیت‌های سوم و چهارم را مقایسه می‌کردند متوجه شنود می‌شدند. این مثال نشان می‌دهد که شش بیت برای حصول احتمال بالای موفقیت کافی نیست و امکان اشتباه زیاد است.

۳.۱ اسلایدها

اسلایدهای شماره ۱۰ تا ۱۷ ارائه شماره ۶ تکمیلی را مطالعه کنید. مثال‌های اسلایدهای ۱۴ و ۱۶ را به دقت بررسی کنید و مطمئن شوید که دلیل هر بخش را به خوبی متوجه شده‌اید. در پایان، به نکته اسلاید شماره ۱۷ توجه کنید. طبق اصل عدم امکان کپی، حوا نمی‌تواند از کیوبیت‌ها کپی تهیه کند و آنها را بدون تغییر برای باب ارسال کند و به این ترتیب با پرهیز از اندازه‌گیری از ایجاد تغییر در حالت کیوبیت‌ها دوری کند.