量子密钥分配实现挑战

Abel C. H. Chen信息与通信安全实验室，中华电信实验室台湾桃园 Email: chchen.scholar@gmail.com; ORCID: 0000-0003-3628-3033

摘 要 —近年来，量子计算技术逐渐成熟，并开始在各个领域得到实际应用。其中一个重要领域是网络通信加密，通过量子密钥分发**(Quantum Key Distribution, QKD)**协商出通信双方的共享秘密**(Shared Secret)**，再利用此共享秘密生成对称密钥，后续可用于加解密。本研究主要聚焦于在真实量子计算机环境中实现并比较两种知名的量子密钥分发协议**(**包括 **BB84**协议和 **E91** 协议**)**，并提出基于 **SX Gate** 操作生成均匀量子叠加态，利用量子叠加态、量子纠缠态等量子物理特性，使通信双方能够取得共享秘密，同时避免攻击者窃取共享秘密。本研究采用 **IBM Quantum Platform**进行实现，并在真实量子计算机上验证 **BB84** 协议和 **E91**协议的可行性，分别通过熵**(entropy)**验证、独立同分布**(Independent and Identically Distributed, IID)**验证以及错误率验证等指标进行评估。

关键字—量子密钥分发、***BB84*** 协议、***E91***协议、量子叠加态、量子纠缠态

I. 前言

随着量子计算技术的普及，许多领域开始着手把量子计算技术应用在各行各业[1],[2]，并且也开始制定相关标准[3],[4]。其中，网络通信加密也开始考虑结合量子密钥分发（量子密钥分配，QKD），来作为另一种量子安全（量子安全）的解决方案[5],[6]。因此，近几年陆续有研究开始讨论在传输层安全协议（传输层安全协议，TLS）中结合量子密钥分发[7],[8]。有鉴于此

，

未来部署量子安全网络通信时，量子密钥分发将会是重要的技术之一。

因此，本研究将聚焦于目前主流的量子密钥分配协议（包含 BB84 协议[9]和 E91 协议[10]），并分别在真实量子计算机环境中实现，验证其量子物理特性，运用量子叠加态、量子纠缠态来保护通信双方的共享秘密（Shared Secret）。其中，将深入探索在真实量子计算机环境中进行量测时产生的误差，并验证分享共享秘密的随机性，从而验证 BB84 协议和 E91 协议的可行性。本研究贡献条列如下:

- 本研究提出通过操作 SX 门产生均匀量子叠加态，为实现 BB84 协议和 E91 协议提供另一种解决方案。
- 本研究在 IBM Quantum Platform 实现 BB84 协议和 E91 协议，运用真实量子计算机实证不同量子密钥分配协议的效能，以及量子物理特性的影响。
- 本研究通过在真实量子计算机环境下实现 BB84 协议和 E91 协议，分别产生共享秘密，并且讨论随机比特熵验证和独立同分布（IID）验证结果。
- 本研究實證了 BB84 协议和 E91 协议在协商过程和测量过程中可能产生的误差，并验证了错误率，以说明量子密钥分配协议的可行性。

本文主要分为 6 个小节。其中，第 II 节介绍量子叠加态和量子纠缠态。第 III 节和第 IV 节分别介绍 BB84协议和 E91 协议的概念和测量结果。第 V 节提供真实量子电脑环境下的实测结果，并深入讨论观察到的现象。最后，第 VI 节总结本研究的发现和贡献，并讨论未来可行的研究方向。

II. 量子态

经典比特与量子比特有着显著差异；其中，经典比特只能是 0 或 1，但量子比特存在量子叠加态，在测量前有概率是 0，也有概率是 1。为了以可视化方式呈现量子叠加态，本研究采用 IBM Quantum Platform 的 Composer 功能，展示量子电路及其对应的测量结果概率。图 1 显示只有 1 个量子比特（q[0]）的情况下，并且预设值为|0，所以在不做任何操作的情况下直接测量（即 ）将得到|0的概率是 100%。本研究将于第 II.A 节介绍量子叠加态，以及第 II.B 节介绍量子纠缠态。



图 1. 默认量子态。

A. 量子叠加态

在密码学领域，为提升安全性，目标是使随机得到 0 和 1 的概率各为 50%，从而达到较高的熵值。因此，为达到此效果，主要是在量子计算机中建立均匀量子叠加态。其中，建立均匀量子叠加态的方式有很多种[11]，本研究提供采用 Hadamard 门操作（即 ）的方式来建立均匀量子叠加态，如图 2 所示。可以观察到，默认值为 100% 是|0（如图 1 所示），但在操作 Hadamard 门后，转换为 50%是|0、50%是|1。因此，在此操作后，再测量得到比特值后，可以得到真随机比特值，并且具有较高的熵值。除此之外，本研究观察到通过操作 SX 门（即 ）或反 SX 门（即 ）也可以建立均匀量子叠加态，如图 3 所示。因此，后续在 BB84 协议和 E91 协议的控制信号（或称“测量基”）中，本研究也将采用 SX 门和反 SX 门的组合来产生均匀量子叠加态。

B. 量子纠缠态

量子纠缠态的量子物理特性，使两个处于量子纠缠态的量子比特，当其中一个量子比特进行测量后，也将会

对另一个量子比特的测量结果造成影响[12]。并且在测量前，持有量子比特的双方都无法预测测量结果会是多少。本节以贝尔态(Bell state)(一种量子纠缠态)为例进行说明，案例中假设有两个量子比特，分别是 q[0] 和 q[1]。首先，对q[0]施加Hadamard 门，再对q[0]和

对 q[1] 执行 CNOT Gate（即 ）设置 q[0] 为控制比特，q[1] 为目标比特，如图 4 所示。可以观察到，默认值为 100%是|00（如图 1 所示），但在执行 Hadamard 门和 CNOT Gate 后，$|q[1]q[0]$ 转换为 50%是|00、50%是|11。因此，在此操作后进行测量，当 q[0] 测量得到 |0

，

则 q[1]也一定测量得到|0；当 q[0]测量得到|1，则 q[1] 也一定测量得到|1。

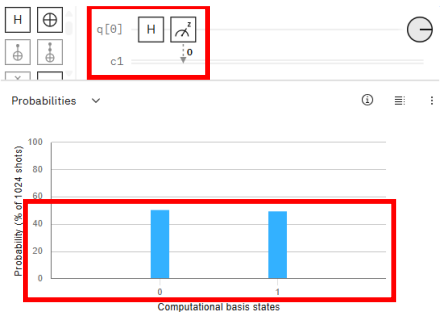

图 2. 基于 Hadamard 门的均匀量子叠加态。



图 3. 基于 SX 门的均匀量子叠加态。



图 4. 贝尔态（即量子纠缠阶段之一）。

III. BB84 协议

第 III.A 节介绍 BB84 协议的流程及步骤，第 III.B 节介绍本研究采用的控制信号（或称“测量基”）。然后，第 III.C 节和第 III.D 节分别介绍通信双方选择相同或不同控制信号的结果。最后，第 III.E 节提供案例和讨论。

A. 步 驟

本节假设 BB84 协议的传输双方分别是 Alice 和 Bob，并且由 Alice 担任发起端。首先，Alice 将随机设定每个量子比特的初始值，由于每个量子比特预设值为|0，所以 Alice 将对部分量子比特操作非门（即 ），让这些量子比特初始值为|1（如图 5 所示）。然后，Alice 随机选择她的控制信号，并且对每个量子比特进行操作，部分量子比特将会处于均匀量子叠加态（如图 5 所示）

，

之后再通过量子信道将量子比特传送给 Bob（如图 5 所示）。Bob 收到量子比特后，随机选择他的控制信号，并对每个量子比特进行操作（如图 5 所示），之后再测量每个量子比特（如图 5 所示）。最后，Bob 通过经典信道将他的控制信号序列传送给 Alice（如图 5 所示），之后 Alice 比对双方的控制信号序列，并将比对结果通过经典信道传送给 Bob（如图 5 所示）。后续双方可以取得控制信号相同的量子比特值，作为协商后的共享秘密（如图 5 所示）。详细的数学证明请参阅[13]。



图 5. BB84协议的步骤。

B. 控制信号*(*或称“测量基”*)*

本节采用两种设计方法：(1).基于 Hadamard 门和(2). 基于 SX 门（本研究提出的方法）。

1) 基于*Hadamard* 门：采用 Hadamard 门和不采用 Hadamard 门两种可选的控制信号。Alice 和 Bob 可以对每个量子比特随机选择是否采用 Hadamard 门。以图 6 为例，首先，Alice 对量子比特执行非门（即 ），使量子比特的初始值为|1，之后选择对量子比特执行 Hadamard 门（即），因此量子比特将处于均匀量子叠加态。之后，Bob 也选择对量子比特执行 Hadamard 门（即），因此量子比特还原为|1。以，之后测量时结果将 100% 为|1。再通过比对控制信号序列可知，双方对该量子比特采用了相同的控制信号，因此该量子比特的测量结果可用。



图 6. 基于 Hadamard 门的 BB84 协议。

2) 基于*SX* 门：对 Alice 有采用 SX 门和不采用 SX 门两种可选的控制信号；对 Bob 有采用 反 SX 门和不采用 反 SX 门两种可选的控制信号 。

Alice 和 Bob 可以随机选择各自的控制信号，对每个量子比特进行操作。以图 7 为例，首先，Alice 对量子比特执行非门（即 ），使量子比特的初始值为|1，之后选择对量子比特执行 SX 门操作（即 ），因此量子比特将处于均匀量子叠加态。之后，Bob 也选择对量子比特执行反 SX 门操作（即 ），因此量子比特还原为|1。所以，之后测量时结果 100% 为|1。再通过比对控制信号序列可知，双方对该量子比特采用了相同的控制信号，因此该量子比特的测量结果可用。

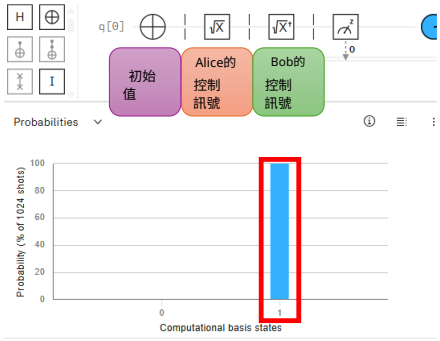

图 7. 基于 SX 门和反 SX 门的 BB84 协议。

C. 通信双方选择相同控制信号

本节介绍 Alice 和 Bob 这两位通信双方选择相同控制信号后的测量结果，如图 8 所示。其中，假设 Alice 分别对量子比特 q[0] 和 q[2] 操作非门，使量子比特|q[3]q[2]q[1]q[0]的初始值为|0101。Alice 分别选择不对量子比特 q[3] 和 q[2]采用 Hadamard 门，并分别选择对量子比特 q[1] 和 q[0]采用 Hadamard 门，然后发送量子比特|01UU，其中 U 表示均匀量子叠加态。之后，Bob 分别选择不对量子比特 q[3] 和 q[2]采用 Hadamard 门，并分别选择对量子比特 q[1] 和 q[0] 采用 Hadamard 门，因此 Bob 测量后可以得到|0101。由于 Alice 和 Bob 对每个量子比特都采用相同的控制信号，因此 Alice 和 Bob 对每个量子比特都可以得到一致的测量结果。



图 8. BB84协议中通信双方选择相同控制信号。

D. 通信双方选择不同控制信号

本节介绍 Alice 和 Bob 这两位通信双方选择不同控制信号后的测量结果，如图 9 所示。其中，假设 Alice 分别对量子比特 q[0] 和 q[2] 操作非门，使量子比特 |q[3]q[2]q[1]q[0] 的初始值为|0101。Alice 分别对量子比特 q[2] 和 q[1] 选择不采用 Hadamard 门，并分别选择对量子比特 q[3] 和 q[0] 采用 Hadamard 门，然后传送量子比特 |U10U，U 表示均匀量子叠加态。之后，Bob 分别选择对量子比特 q[3] 和 q[0] 不采用 Hadamard 门，并分别选择对量子比特 q[2] 和 q[1] 采用 Hadamard 门，因此 Bob 测量后可以得到 |UUUU。由于 Alice 和 Bob 对每个量子比特都采用不同的控制信号，因此他们无法确定每个量子比特能否得到一致的测量结果。

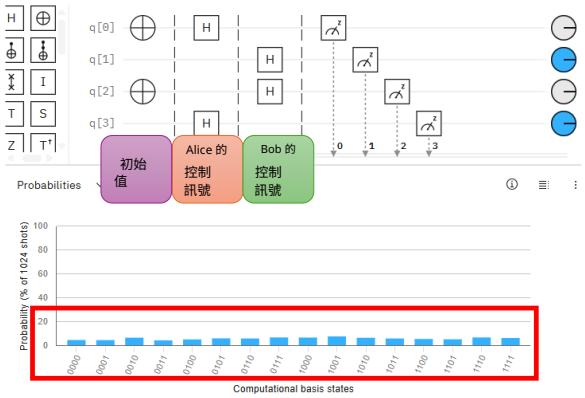

图 9. BB84协议中通信双方选择不同控制信号。

E. 案例与讨论

在实际部署 BB84 协议时，Alice 随机对平均一半的量子比特执行非门，使量子比特初始值有 50% 是|0，有 50% 是|1，让熵值（混乱度）较大。此外，就控制信号的部分而言，如果都选择执行 Hadamard 门，虽然可以让全部量子比特在传输过程中都是均匀量子叠加态，但攻击者只需对全部量子比特都执行 Hadamard 门即可还原。因此，为了提升传输安全性并增加传输值的混乱度，Alice 随机对平均一半的量子比特执行 Hadamard 门，另一半不执行 Hadamard 门；而 Bob 也是随机对平均一半的量子比特执行 Hadamard 门，另一半不执行 Hadamard 门。因此，Alice 和 Bob 平均只会有一半的量子比特采用相同的控制信号，所以只会有一半的量子比特可以作为共享秘密。以图 10 为例，假设 Alice 分别对量子比特 q[0] 和 q[2] 执行非门，使量子比特|q[3]q[2]q[1]q[0] 初始值为|0101。Alice 分别对量子比特 q[3] 和 q[2] 选择不采用 Hadamard 门，并且分别对量子比特 q[1] 和 q[0] 选择采用 Hadamard 门，然后传送量子比特|01UU，U 表示均匀量子叠加态。之后，Bob 分别对量子比特 q[3] 和 q[1] 选择不采用 Hadamard 门，并且分别对量子比特 q[2] 和 q[0] 选择采用 Hadamard 门，所以 Bob 测量后可以得到|0UU1。由于 Alice 和 Bob 在量子比特 q[3] 和 q[0] 都采用

相同的控制信号，所以 Alice 和 Bob 在量子比特 q[3]和 q[0]可以得到一致的测量结果。需要注意的是，控制信号也可以改为本研究提出的采用或不采用 SX 门和采用或不采用反 SX 门两种可选的控制信号来达到相同效果。

IV. E91 协议

第 IV.A 节介绍 E91 协议的流程及步骤，第 IV.B 节介绍本研究采用的控制信号（或称“测量基”）。然后，第 IV.C 节和第 IV.D 节分别介绍通信双方选择相同或不同控制信号的结果。最后，第 IV.E 节提供案例和讨论。

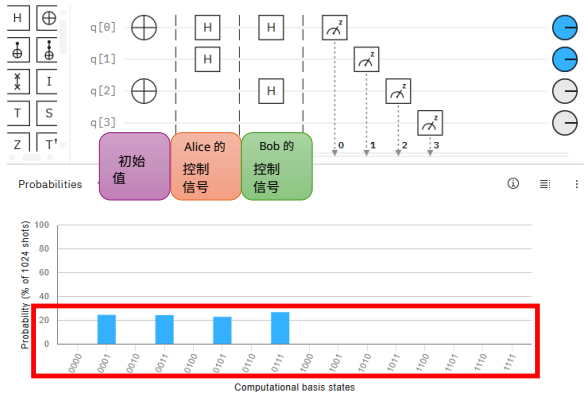

图 10. BB84协议的一个案例。

A. 步 驟

本节假设 E91 协议的传输双方分别是 Alice 和 Bob。首先，为成对的量子比特建立贝尔态（如图 11 所示），之后分别让 Alice 和 Bob 各自持有处于贝尔态的量子比特（如图 11 所示）。然后，Alice 随机选择她的控制信号，并对每个量子比特进行操作，部分处于贝尔态的量子比特将会成为均匀量子叠加态（如图 11 所示）。Bob 也随机选择他的控制信号，并对每个量子比特进行操作（如图 11 所示）。最后，Alice 和 Bob 再各自测量其持有的量子比特（如图 11 所示），以及传送和比对控制信号序列（如图 11、图 11、图 11 所示）。这样后续双方即可取得具有相同控制信号的量子比特值，作为协商后的共享秘密。详细数学证明可以参考[14]。

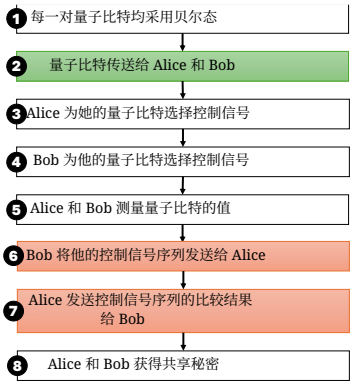

图 11. E91 协议的步骤。

B. 控制信号*(*或称“测量基”*)*

本节采用两种设计方法：(1)基于 Hadamard 门和(2)基于 SX 门（本研究提出的方法）。

1) 基于*Hadamard* 门：提供采用 Hadamard 门和不采用 Hadamard 门两种可选控制信号。Alice 和 Bob 可以随机选择是否对各自的量子比特采用 Hadamard 门。以图 12 为例，首先，为量子比特 q[1]和 q[0]建立贝尔态（也就是|00和|11的概率各为 50%），并让 Alice 持有量子比特 q[0]，而 Bob 持有量子比特 q[1]。之后，Alice 选择对量子比特采用 Hadamard 门操作（即），所以量子比特 q[1]和 q[0]将处于均匀量子叠加态，也就是|00、|01、|10、|11的概率各为 25%。之后，Bob 也选择对量子比特采用 Hadamard 门操作（即），所以量子比特还原为|00和|11的概率各为 50%。因此，之后测量时，根据量子纠缠态，可以确定 Alice 和 Bob 的测量结果会一致。由此可知，双方对该量子比特采用了相同的控制信号，因此可以使用该量子比特的测量结果。

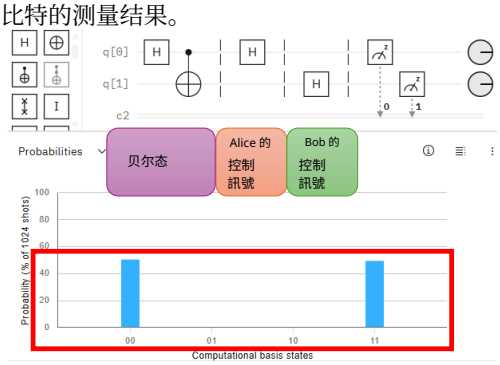

图 12. 基于 Hadamard 门的 E91 协议。

2) 基于*SX* 门：对于 Alice，有采用 SX 门和不采用 SX 门两种可选的控制信号；对于 Bob，有采用反 SX 门和不采用反 SX 门两种可选的控制信号。Alice 和 Bob 可以随机选择各自的控制信号，对各自的量子比特进行操作。以图 13 为例，首先为量子比特 q[1]和 q[0]建立贝尔态（也就是|00和|11的概率各为 50%），并且让 Alice 持有量子比特 q[0]，而 Bob 持有量子比特 q[1]。之后，Alice 选择对量子比特采用 SX 门操作（），所以量子比特 q[1]和 q[0]将会是均匀量子叠加态，也就是|00、|01、|10、|11的概率各为 25%。之后，Bob 也选择对量子比特采用反 SX 门操作（即），所以量子比特还原为|0(√X†)|11的概率各为 50%。因此，之后测量时，根据量子纠缠态可以确定 Alice 和 Bob 测量的结果会是一致的。由此可知，双方对该量子比特采用相同的控制信号，所以该量子比特的测量结果可用。



图 13. 基于 SX 门和反 SX 门的 E91 协议。

C. 通信双方选择相同控制信号

本节介绍 Alice 和 Bob 通信双方选择相同控制信号后的测量结果，如图 14 所示。首先，建立量子比特 q[0]和 q[2]的贝尔态，以及建立量子比特 q[1]和 q[3]的贝尔态。Alice 持有量子比特 q[0]和 q[1]，而 Bob 持有量子比特 q[2]和 q[3]。Alice 分别选择对量子比特 q[0]和 q[1]采用 Hadamard 门，然后量子比特将变成|UUUU，U 表示均匀量子叠加态。之后，Bob 分别选择对量子比特 q[2]和 q[3]采用 Hadamard 门，量子比特将变成|0000、|0101、|1010、|1111的概率各为 25%。可以观察到，在量子纠缠态的基础上，q[0]和 q[2]会有相同的测量结果，而且 q[1]和 q[3]會得到相同的测量结果。因此，当 Alice 和 Bob 各自对处于贝尔态的量子比特采用相同的控制信号时，Alice 和 Bob 测量各自的量子比特可以得到一致的测量结果。

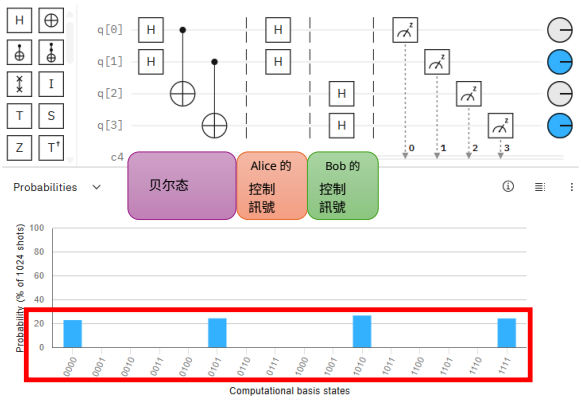

图 14. E91 协议中通信双方选择相同控制信号。

D. 通信双方选择不同控制信号

本节介绍 Alice 和 Bob 这两位通信双方选择不同控制信号后的测量结果，如图 15 所示。首先，建立量子比特 q[0]和 q[2]的贝尔态，以及量子比特 q[1]和 q[3]的贝尔态。Alice 持有量子比特 q[0]和 q[1]，Bob 则持有量子比特 q[2]和 q[3]。Alice 分别选择对量子比特 q[0]采用 Hadamard 门，对 q[1]不采用 Hadamard 门。之后，Bob 分别选择对量子比特 q[2]不采用 Hadamard 门，对 q[3]采用 Hadamard 门，量子比特将变成|UUUU。由此可知，当 Alice 和 Bob 各自对处于贝尔态的量子比特采用不同的控制信号时，Alice 和 Bob 测量各自的量子比特，无法保证得到与对方一致的测量结果。

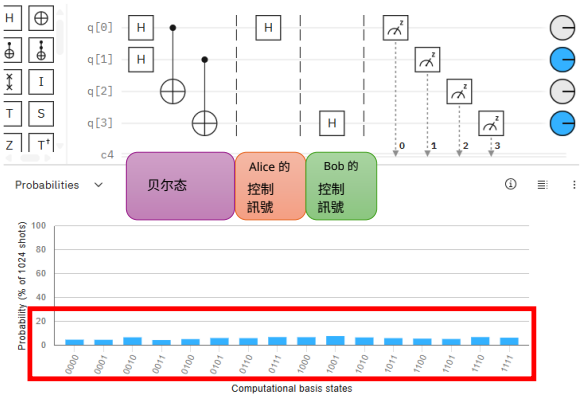

图 15. E91 协议中通信双方选择不同控制信号。

E. 案例与讨论

在实际部署 E91 协议时，若控制信号部分都选择操作 Hadamard 门，虽然可以让所有量子比特在传输过程中都处于均匀量子叠加态，但攻击者只需对所有量子比特都操作 Hadamard 门即可还原。因此，为了提升传输安全性并增加传输值的随机性，Alice 随机对其持有的平均一半量子比特操作 Hadamard 门，另一半不操作 Hadamard 门；Bob 也随机对其持有的平均一半量子比特操作 Hadamard 门，另一半不操作 Hadamard 门。因此，Alice 和 Bob 各自持有的量子比特中，平均只有一半采用相同的控制信号，所以各自持有的量子比特中只有一半可以作为共享秘密。以图 16 为例，首先，建立量子比特 q[0]和 q[2]的贝尔态，以及建立量子比特 q[1]和 q[3]的贝尔态。Alice 持有量子比特 q[0]和 q[1]，而 Bob 持有量子比特 q[2]和 q[3]。假设 Alice 分别对量子比特 q[0]和 q[1]选择采用 Hadamard 门。之后，Bob 分别对量子比特 q[2]选择采用 Hadamard 门，对 q[3]选择不采用 Hadamard 门，因此量子比特将变成 |U0U0或|U1U1，U 表示均匀量子叠加态。由于量子比特 q[0]和 q[2]处于量子纠缠态，并且 Alice 和 Bob 对该量子比特采用相同的控制信号，因此 q[0]和 q[2]将得到一致的测量结果。需要注意的是，控制信号也可以改为本研究提出的两种可选控制信号：采用或不采用 SX 门，以及采用或不采用反 SX 门，以达到相同效果。

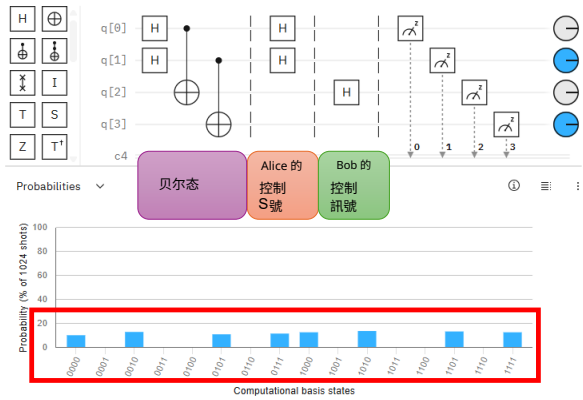

图 16. E91 协议的一个案例。

V. 实证结果与讨论

本节介绍本研究的实验环境并讨论验证结果。其中，第 V.A 节介绍实验环境，第 V.B 节~第 V.D 节分别讨论熵验证、独立同分布验证和错误率验证的结果。

A. 实验环境

为验证量子密钥分发，本研究采用 Python 3.11.14 和 IBM Qiskit 2.2.3 进行实现，并在 IBM Quantum Platform [15]上使用真实量子计算机执行和验证。其中，由于 IBM Quantum Platform 目前提供的量子处理单元的量子比特数上限分别为 133 个或 156 个（如图 17 所示），因此本研究设计的量子电路主要使用 128 个量子比特。

QPU name	Instance	Qubits ↓	Status	Pending jobs
ibm_boston		156	Online	0
ibm_kingston		156	Online	4
ibm_pittsburgh		156	Online	607
ibm_fez	open-instance	156	Online	55
ibm_marrakesh	open-instance	156	Paused - maintenance	19,992
ibm_torino	open-instance	133	Online	4

图17 2025年9月。 IBM Quantum Platform 于12月在网页上的计算资源（即 https://quantum.cloud.ibm.com/computers）。

B. 熵验证

为验证量子密钥分发协商后共享秘密的随机性，本研究采用 NIST SP 800-90B [16]的熵计算方法，并进行二项分布检验，针对多组共享秘密计算其熵值和 p值。其中，熵值和 p值越大表示效能越好，并且 NIST SP 800-90B 定义的 p值门槛为 0.000005。实验结果显示，不论是 BB84协议还是 E91 协议得到的共享秘密，其 p值皆大于 0.000005，表示测量到 0 或 1 的概率各接近 50%，可以通过熵验证，如表 I 所示。

表 I.　　熵验证

量子密钥分发协议	熵	p值
基于 Hadamard 门	0.982	0.260
BB84协议基于 SX 门（所提方法）	0.988	0.381
E91 协议基于 Hadamard 门	0.857	0.020
E91 协议基于 SX 门（所提方法）	0.989	0.597

C. 独立同分布验证

NIST SP 800-90B [16]规范的独立同分布（Independent and Identically Distributed, IID）验证包含独立性（Independent, IND）检验、拟合优度（Goodness of Fit, GOF）检验，以及最长重复子串（Longest Repeated Substring, LRS）检验，并且 p值门槛为 0.001。表 II 为独立同分布验证，实验结果显示，不论是 BB84 协议还是 E91 协议得到的共享秘密，在各项验证指标中的 p值皆大于 0.001，可以通过独立同分布验证。

表 II.　　独立同分布验证

量子密钥分发协议	IND 检验 p值	GOF 检验 p值	LRS 检验 p值
基于 Hadamard 门	0.291	0.386	0.998
基于 SX 的 BB84 协议门（所提方法）	0.333	0.002	1.000
基于 Hadamard 门	0.139	0.011	0.996
基于 SX 门（所提方法）	0.333	0.157	1.000

D. 错误率验证

為驗證在真實量子計算機環境中執行可能產生的錯誤率，本研究的實證結果如表 III 所示。其中可以觀察到，BB84協議僅使用量子疊加態，每個量子比特皆可獨立運作，因此目前的錯誤率已接近 0。然而，E91 協議需以量子糾纏態為基礎，但目前測量量子糾纏態時的誤差仍約有一成。

表 III.　　错误率验证

量子密钥分发协议	错误率
基于 Hadamard 门的 BB84 协议	0.000
基于 SX 门的 BB84 协议（所提方法）	0.000
基于 Hadamard 门的 E91 协议	0.125
基于 SX 门的 E91 协议（所提方法）	0.094

VI. 结论与未来研究

本研究在真实量子计算机上实现了 BB84 协议和 E91 协议等量子密钥分配协议，并提出了基于 SX 门的量子密钥分配协议。实证结果表明，所提方法通过了熵、独立同分布以及错误率等验证，证明了其可行性。然而，目前量子纠缠态的测量错误率仍未接近 0，未来可致力于改进量子纠缠态的测量技术。

致謝

本研究实验采用 IBM Qiskit 套件开发，并在 IBM Quantum Platform 上运行。承蒙 IBM 提供免费试用，使本研究得以顺利进行，特此致谢。本研究感谢欧洲电信标准协会（European Telecommunications Standards Institute, ETSI）量子密钥分发工作组将本文作者的相关建议纳入 ETSI GR QKD 007 V 1.4.7，感谢领域专家们的支持。

参考文獻

[1] T. Lubinski 等人，“面向应用的量子计算性能基准”，发表于*IEEE* 量子工程汇刊，第 4 卷，第 1–32 页，2023 年，文章编号 3100332，doi：10.1109/TQE.2023.3253761。[2] M. A. Shafique、A. Munir 和 I. Latif，“量子计算：电路、算法与应用”，发表于*IEEE Access*，第 12 卷，第 22296–22314 页，2024 年，doi：10.1109/ACCESS.2024.3362955。[3] “量子密钥分配（QKD）；通用准则保护概要——一对制备与测量量子密钥分配模块”，ETSI GS QKD 016 V2.1.1，第 1–93 页，2024 年 1 月，网址：https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/02.01.01_60/ gs_QKD016v020101p.pdf[4] M. Ramachandra、B. C. Ang、E. J. Rodrigues，“新兴与未来应用中的量子技术”，发表于新兴与未来应用中的量子技术，第 1–21 页，2025 年 11 月，网址：https://ieeexplore.ieee.org/document/11244610[5] Y. Fu、Y. Hong、T. Q. S. Quek、H. Wang 和 Z. Shi，“面向量子密钥分配通信网络的调度策略”，发表于*IEEE* 无线通信快报，第 9 卷，第 12 期，第 2126–2129 页，2020 年 12 月，doi：10.1109/LWC.2020.3014633。[6] E. Mikale、S. Waters、L. Swiney，“利用动态频率稳定量子比特、对后量子加密协议的影响及混合量子互联网”，发表于利用动态频率稳定量子比特、对后量子加密协议的影响及混合量子互联网，第 1–12 页，2024 年 9 月，网址：https://ieeexplore.ieee.org/document/10685053[7] C. R. Garcia、A. Cano、J. J. V. Olmos、S. Rommel 和 I. T. Monroy，“将量子密钥分配整合至 TLS 1.3：面向光网络中抗量子通信的传输层方法”，*2024* 年 *IEEE* 光纤通信会议暨展览会（*OFC*）论文集，第 1–3 页，美国加利福尼亚州圣迭戈，2024 年。[8] J. M. Sáez 等人，“量子密钥分配标准的现状、差距与未来方向：对产业的影响”，*2024* 年 *IEEE* 量子通信、网络与计算国际会议（*QCNC*）论文集，第 341–345 页，日本金泽，2024 年，doi：10.1109/QCNC62729.2024.00059。[9] C. H. Bennett 和 G. Brassard，“量子密码学：公钥分配与抛硬币”，载于*IEEE* 计算机、系统与信号处理国际会议论文集，美国纽约，1984 年，第 175 卷，第 1–8 页。[10] A. K. Ekert，“基于贝尔定理的量子密码学”，发表于*Physical Review Letters*，第 67 卷，第 6 期，第 661–663 页，1991 年，doi：10.1103/PhysRevLett.67.661。[11] A. Z. Dragicevic，“具有量子叠加与量子纠缠的交换网络”，发表于*IEEE* 计算社会系统汇刊，doi：10.1109/TCSS.2025.3601189。[12] Y. Yao 和 S. A. Jafar，“论量子纠缠在联合通信与瞬时检测中的效用”，发表于*IEEE* 通信汇刊，第 73 卷，第 11 期，第 11722–11735 页，2025 年 11 月，doi：10.1109/TCOMM.2025.3573393。[13] A. C. H. Chen，“针对量子密码学的中间人攻击”，*2025* 年 *IEEE* 智能通信网络与计算技术国际会议（*ICICNCT*）论文集，第 1–8 页，印度比达尔，2025 年，doi：10.1109/ICICNCT66124.2025.11232721。[14] A. C. H. Chen，“基于量子纠缠态的量子密钥分配安全分析”，*2025* 年 *IEEE* 北卡纳塔克分会旗舰国际会议（*NKCon*）论文集，第 1–6 页，印度巴加尔果德，2025 年。[15] S. Bravyi、A. W. Cross、J. M. Gambetta、D. Maslov、P. Rall 和 T. J. Yoder，“高阈值、低开销的容错量子存储器”，发表于*Nature*，第 627 卷，第 778–782 页，2024 年，doi：10.1038/s41586-024-07107-7。[16] M. S. Turan 等人，“随机比特生成所用熵源的建议”，发表于*NIST* 特别出版物，NIST SP 800-90B，第 1–76 页，2018 年 1 月，doi：10.6028/NIST.SP.800-90B。