arXiv:2611.32886v1 [cs.IT] 24 Nov 2026

GHZ网络上的会议密钥协商容量

Hua Sun

摘要

K 位用户共享相互独立的GHZ态，每个GHZ态由部分用户持有；他们希望通过局部操作与公开经典通信（LOCC）获得一个共同的秘密密钥。我们证明，会议密钥容量，即每份资源所能生成的最大秘密密钥比特数，等于对每个GHZ态进行测量所得到的经典源的密钥容量。因此，即使用户保留量子存储器并进行任意轮次的通信，先进行测量仍然是最优的。该容量还等于GHZ 蒸馏容量，即每份资源所能生成的由所有用户共享的最大GHZ态数量。

1 引言

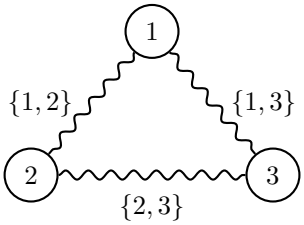
一个贝尔对可以为两位用户提供一个共同的秘密比特，而一个GHZ态可以为任意数量的用户提供一个共同的秘密比特。本文研究的问题始于这样一种情形：每个可用的GHZ态仅由部分用户持有，而所有 K 位用户都希望获得同一个密钥，即会议密钥。用户标记为1、.....、 K，资源由一个超图 $\mathcal{G} = ([K], \mathcal{E})$描述，其中包含 $\mathcal{E}$ 条边；每条边 e 都是至少包含两位用户的子集。用户为每条边各持有一个相互独立的GHZ态。边e 上的GHZ态向集合 e中的每位用户提供一个量子比特；对这些量子比特进行测量后，他们将得到相同的均匀随机比特，即 e的标签；集合 e 中的用户是该标签的持有者。用户可以执行任意局部量子操作、保留量子存储器，并通过经认证的公共信道广播经典消息，通信可进行任意轮次，每条消息都可以依赖于此前的所有消息；窃听者能够观察全部公开通信。会议密钥容量 C 是每份资源所能生成的最大共同秘密比特数，而*GHZ* 蒸馏容量 E_{D} 是每份资源所能生成的由所有 K 用户共享的最大全局GHZ态数量。量子会议密钥协商见 [1]中的综述。

最小的实例已经展现出其中的难点。在贝尔三角形（图1(a)）中，用户1、2、3在每一对用户之间各共享一个贝尔对。对每一对进行测量会得到均匀分布的比特 a、 b和 c，分别由用户对 $\{1,2\}$、$\{1,3\}$和 $\{2,3\}$知晓。在两个副本上，每个用户广播一次奇偶校验，就能让每个用户恢复全部六个比特，并留下三个秘密比特（图1(b)），速率为 $3/2$。一个割将用户划分为两个非空群组。所有用户共有的密钥尤其也是这两个群组之间的密钥，因此容量至多等于最小割上的纠缠，即最小割

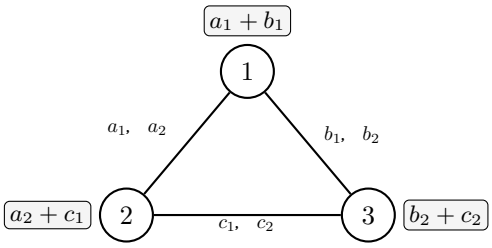
，此处为 2。Vrana 和 Christandl 证明，随机 LOCC 可以从任意贝尔对环中以速率 2 提取 GHZ 态，但成功概率可能渐消，并提出了一个问题：

Hua Sun（电子邮箱：hua.sun@unt.edu）任职于北德克萨斯大学电气工程系。

具有渐消错误的 LOCC 是否也能达到速率 2 [2]。我们所知的所有针对无限制局部操作与经典通信的反向证明，无论是基于相对熵 [3,4], 压缩纠缠 [5] 和 Partovi单调量 [6]的结果（适用于 C），还是基于多方Rains测度 [7] 的结果（适用于 E_{D}），后者通过引理 3 给出 C 的上界，都只能为这类网络给出至少等于最小割的上界，因此都无法证明三角形上的 $C < 2$ 。原因比割更根本。贝尔三角形中任意一组用户的熵，都与三个用户共同分享的两个 GHZ 态相同：每个用户的熵为 2，每一对用户的熵也为 2。两个这样的 GHZ 态每份可提供 2 个密钥比特，因此，任何仅利用用户群组熵的 C 上界（割界是其特例），在三角形上都不可能小于 2。反向证明必须利用熵以外的信息。我们证明， $3/2$ 就是容量。



（a）任何带量子存储器的局域操作与经典通信和公开通信；一个共同的秘密密钥



（b）进行测量，每人广播一个奇偶校验；密钥（a_1, a_2, b_2），速率 $3/2$

图 1：贝尔三角形。（a）资源与要求；每个割都穿过两对，因此最小割为 2。（b）测量每一对，并通过两个副本为每个用户广播一个奇偶校验，实现 $3/2$；定理 1 表明这就是容量。

1.1 主要结果

在计算基中测量每个 GHZ态，会将资源转化为独立均匀比特的经典源；每个比特对于其边的用户而言都是已知的，这就是测量源。其带公开通信的密钥容量已知为 [8, 9]:

$$C^{\mathrm{Z}}(\mathcal{G}) = \min_{\mathcal{P}:\,|\mathcal{P}|\geq 2} \frac{\sum_{e\in\mathcal{E}} \big(r_e(\mathcal{P}) - 1\big)}{|\mathcal{P}| - 1}, \tag{1}$$

其中， $\mathcal{P}$ 遍历用户的划分，而 $r_e(\mathcal{P})$ 是与 e 相交的部分数量，即将每个部分中的用户归并为一个用户后， e 的持有者数量。我们将 C^{Z} 称为测量容量。主要结果表明，先进行测量是最优的：对于每个独立 GHZ 态网络，

$$C = E_{\mathrm{D}} = C^{\mathrm{Z}},$$

在无限制局部操作与经典通信下，可以实现渐消错误（定理 1）。在有限分组长度下，容量也可作为密钥率实现，且具有零错误；对于测量源 [10], 以及作为 GHZ 率亦如此（第4节）。在渐消错误的条件下，若每个 GHZ 态按其标签的熵加权，容量结果可推广至具有非均匀标签的 GHZ 态，进而推广至每个由纯双部态构成的网络，其中每个纯双部态由两位用户共享；这是因为根据施密特分解，纯双部态就是两位用户共享的 GHZ 态（注1）。本文以两个系列作为贯穿全文的示例。在

环上的 $K \geq 3$ 贝尔对（贝尔三角形是其中的情形 $K = 3$），其容量为 $K/(K-1)$，因此 Vrana 和 Christandl 所询问的速率 2 对任何环而言都无法通过局域操作与经典通信实现。对于完全网络，若每个 J 用户子集上都有一个 J 用户 GHZ 态，则其容量为 $\binom{K}{J}\frac{J-1}{K-1}$；而对于贝尔对，$J = 2$。——

对于在任何通信前测量每个份额的方案，Neumann、Kampermann、Bruß 和 Trushechkin [4, 定理 4]证明了纯双体态网络的划分界。定理 1 结合注 1 证明了该结论适用于所有局域操作与经典通信方案；在这些方案中，用户可以保留量子存储器，并在公开通信的轮次之间对其份额执行操作。文献 [11], 声称证明了双体纯态乘积的局域操作与经典通信反向证明，但由于其中有一个尚未解决的步骤，该结果后来被撤回；据我们所知，目前尚无关于这一无限制命题的书面证明。在可达性方面，Vrana 和 Christandl [12] 以及 Salek 和 Winter [13,14]的下界给出了 $E_{\mathrm{D}} \geq C^{\mathrm{Z}}$，且错误渐消。

1.2 反向证明的思路

反向证明比较同一方案的两次运行（第 3 节）。在实际运行 中，用户将其操作应用于 GHZ网络；而在乘积运行中，这只是一次计算：将相同的局部操作应用于网络状态的边缘分布之积，在该运行中用户彼此独立。公开通信和密钥是一次测量的测量结果，该测量的效应是局部正算子的乘积。由于每个标签至少由两个用户持有，因此对每个标签应用一次柯西–施瓦茨步骤，Finner不等式 [15], 的一个特例将网络状态与任意单位积向量的重叠界定为 $1/\sqrt{2^{|\mathcal{E}|}}$ （引理1）。因此，与乘积运行相比，每个测量结果在实际运行中的概率至多为 $2^{\sum_e(|e|-1)}$倍，其中 $\sum_e(|e|-1) = \sum_k H(Y_k) - H(Y_1 \cdots Y_K)$ 是所测标签的总相关，其中 Y_k 是用户 k持有的标签元组。在实际运行下对对数取平均，得到一个熵不等式（引理2）：

$$\sum_k H(W_k \,|\, F) - H(W_1 \cdots W_K \,|\, F) \;\leq\; \sum_e (|e| - 1),$$

其中，W_k 是用户 k 的密钥，F 是公开通信：给定公开通信后，密钥的总相关不超过标签的总相关。零错误 L比特密钥的总相关为（$K-1$）L，因此 $L \leq \sum_e$（$|e|-1$）/（$K-1$），这就是测量源在量子存储器和自适应通信条件下的总相关界。将划分中每个部分的用户分组为一个用户，可得到（1）：边 e 随后有 r_e（$\mathcal{P}$）个持有者，因此其权重为 r_e（$\mathcal{P}$）-1，即其标签在各部分之间的总相关。证明仅利用了标签的持有方式：标签的数量，以及每个标签至少有两个持有者。

1.3 会议密钥与GHZ态提纯

对于每个纯源，不仅对于 GHZ 网络，会议密钥与 GHZ 蒸馏具有相同的容量（引理 3）：以量子网络编码和免费经典通信的方式相干地运行密钥方案 [16], ，每个用户都在由其密钥相干选择的基下测量其剩余寄存器，因此测量结果不会泄露任何信息，剩余寄存器也会解纠缠。特别地，每个零错误密钥方案都能以相同速率实现精确 GHZ 蒸馏，由此得到定理 1 中关于 GHZ 蒸馏的可达性部分。

2 问题陈述与主要结果

我们定义该问题并陈述主要结果。所有对数均为二进制对数。资源。对于满足 $|e| \geq 2$ 的用户子集 $e \subseteq [K]$， e 上的 GHZ 态为

$$|\mathrm{GHZ}_e\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle^{\otimes |e|} + |1\rangle^{\otimes |e|} \right),$$

每位用户在 e 中拥有一个量子比特；贝尔对是 $|e| = 2$ 的情形。共有 $K \geq 2$ 位用户，超图$\mathcal{G} = ([K], \mathcal{E})$ 描述了该资源。其边列表 $\mathcal{E}$ 可以包含任意用户子集 e，且满足 $|e| \geq 2$，因此网络可以混合贝尔对和涉及更多用户的 GHZ 态，也可以多次包含同一子集，从而在相同用户上拥有多个 GHZ 态。该资源为

$$|\Psi_{\mathcal{G}}\rangle = \bigotimes_{e \in \mathcal{E}} |\mathrm{GHZ}_e\rangle, \tag{2}$$

其中不同的边占据不同的寄存器，即使这些寄存器由同一位用户持有也是如此。这些就是 [2] 中研究的资源。用户 k 的份额 S_k 是该用户在资源中所拥有的寄存器集合。贝尔对环的边为 $\{k, k+1\}$，其索引模 K；贝尔三角形是满足 $K = 3$ 的环。完全网络 $\Psi_{K,\ J}$ 在每个 $[K]$ 的 J 元子集上各有一个 GHZ 态；当 $J = 2$ 时，它在每一对用户上各有一个贝尔对，而贝尔三角形为 $\Psi_{3,\ 2}$。

操作。一种分组长度为 N 的方案作用于 N 个纯 K 用户资源 $|\psi\rangle$ 的副本；在此处以及引理 3 中，$|\psi\rangle$ 可以是任意纯态。也就是说，该方案作用于 $|\psi\rangle^{\otimes N}$，并通过经认证的公开信道进行任意有限轮次的经典通信，且对 T 随 N 增长的方式不作限制。

- 轮次。在第 $t \in [T]$ 轮，由第 1、……、$t-1$ 轮的消息决定的一名用户，对其寄存器应用测量算子 $\{O_x\}_x$。这些测量算子具有有限个测量结果，其选择取决于这些消息；该用户随后广播测量结果 X_t。每个 O_x 都是从该用户的寄存器映射到其轮后寄存器的线性映射，这些寄存器可以包含辅助系统；而 $\sum_x O_x^\dagger O_x = I$ 是恒等算子：在量子态 $|\phi\rangle$ 上得到测量结果 x 的概率为 $\| O_x |\phi\rangle \|^2$，其中 $\| \cdot \|$ 表示向量的欧几里得范数，所得未归一化态为 $O_x |\phi\rangle$。[1]

- 密钥提取。在第 T 轮次之后，用户 k 对其最终寄存器 A_k进行测量，测量采用正算子$\{M_{k,w}\}_w$ $\sum_w M_{k,\ w} = I$，这些算子根据公开通信 $F =$（X_1、……、X_T）确定；其测量结果即为密钥 $W_k \in \{0,1\}^L$。

允许一名用户广播公共共享随机性，即可涵盖公共共享随机性的情形。给定 $F = f =$（x_1、……、x_T），每一轮次的测量由较早的消息确定；记 $O_{x_t}^{(t)}$ 为第 t 轮次中测量结果为 x_t 的算子。设用户 k 执行操作的轮次为 $t_1 < \cdots < t_{T_k}$，则用户 k在分支 f 上的算子为

$$V_{k,f} |\phi\rangle_{S_k^N} = O_{x_{t_{T_k}}}^{(t_{T_k})} \cdots O_{x_{t_2}}^{(t_2)} O_{x_{t_1}}^{(t_1)} |\phi\rangle_{S_k^N},$$

一个线性映射，将用户 k 的 N 个副本中的份额 S_k^N 的量子态 $|\phi\rangle$ 映射为其最终寄存器 A_k 上的未归一化态，并在其上测量其密钥。我们设定 $V_{k,\ f} = I$，其中 $A_k = S_k^N$，如果

[1]这是具有经典结果的一般局部操作，因为在方案中被丢弃的寄存器也可以保留而不使用。一个测量结果为 x 的量子仪器，其仪器元素具有克劳斯算子 $O_{x,\ j}$；当用户保留环境寄存器时，该仪器元素变为单个算子 $O_x = \sum_j |j\rangle_{\mathrm{env}} \otimes O_{x,\ j}$，其中 $O_x^\dagger O_x = \sum_j O_{x,\ j}^\dagger O_{x,\ j}$；丢弃环境寄存器则恢复仪器元素 $\rho \mapsto \mathrm{Tr}_{\mathrm{env}}[O_x \rho O_x^\dagger]$。

用户 k 从不行动。对于固定的公开通信 f，不同用户的算子作为作用于不同张量因子上的映射彼此对易，因此分支 f 的算子可分解为 $V_f = \bigotimes_k V_{k,\,f}$。该分支以未归一化态 $V_f\,|\psi\rangle^{\otimes N}$ 结束，并且公开通信 f 以及密钥 $\boldsymbol{w} =$（w_1，……，w_K）和 $W =$（W_1，……，W_K）以如下概率出现

$$P_F(f) = \mathrm{Tr}[V_f \psi^{\otimes N} V_f^\dagger], \qquad P_{FW}(f, \boldsymbol{w}) = \mathrm{Tr}[\Gamma_{f,\boldsymbol{w}} \psi^{\otimes N}],$$

其中 $\psi = |\psi\rangle\langle\psi|$ 为源的密度算子和局部乘积效应

$$\Gamma_{f,\boldsymbol{w}} \;=\; \bigotimes_k \Gamma_{k,f,w_k}, \qquad \Gamma_{k,f,w} \;=\; V_{k,f}^\dagger M_{k,w} V_{k,f}. \tag{3}$$

这些效应的总和为 I：$\sum_w M_{k,\;w} = I$ 将总和化简为 $\sum_f V_f^\dagger V_f$，这是通过 $\sum_x O_x^\dagger O_x = I$ I 得到的：先对最后一轮的测量结果求和，然后对倒数第二轮的测量结果求和，依此类推。反向证明仅使用效应的乘积形式（3）。除（2）之外，不存在量子通信、预共享秘密随机性或免费纠缠。窃听者观测到F，除此之外一无所知。

要求。 对于 $\varepsilon \geq 0$，密钥必须满足

$$\text{Correctness:} \qquad \Pr\{W_1 = \cdots = W_K\} \geq 1 - \varepsilon, \tag{4}$$

$$\text{Secrecy:} \qquad \tfrac{1}{2}\|P_{FW_1} - P_F \otimes U_L\|_1 \leq \varepsilon, \tag{5}$$

其中 P_{FW_1}是（F，W_1）的联合分布，是 P_{FW}的边缘分布； P_F是上述给出的在 F条件下的分布；U_L 是 $\{0,1\}^L$上的均匀分布； $\|\cdot\|_1$ 是 ℓ_1 范数，因此（5）左侧是全变差距离；对于算子，$\|\cdot\|_1$ 是迹范数，即奇异值之和；对于厄米算子，它等于特征值绝对值之和； $\frac{1}{2}\|\cdot\|_1$ 是迹距离；当 $\varepsilon = 0$时，该方案为零错误 。

定义 1. 纯 K用户态 $|\psi\rangle$ 的会议密钥容量 $C(\psi)$ 是满足以下条件的速率 R 的上确界：存在定义在 $|\psi\rangle^{\otimes N}$ 上的方案，使其满足 $L \geq RN$ 且错误为 $\varepsilon_N \to 0$。*GHZ* 蒸馏容量 $E_{\mathrm{D}}(\psi)$ 的定义方式相同，但方案中以每个用户执行的局部操作取代密钥提取；该操作根据 F选择，其联合输出σ_f在给定 $F = f$的条件下满足 $\sum_f P_F(f)\frac{1}{2}\|\sigma_f - \mathrm{GHZ}_{[K]}^{\otimes L}\|_1 \leq \varepsilon_N$，其中 $|\mathrm{GHZ}_{[K]}\rangle$是所有用户的 *GHZ*态，而 $\mathrm{GHZ}_{[K]}$是其密度算子。[2]

在计算基中测量蒸馏得到的 GHZ态会产生一个密钥比特。测量不会增加迹距离，因此，对 GHZ 蒸馏方案的输出进行测量（该方案的错误为ε），所得密钥的错误在式 (4) 和 (5) 中至多为 ε，并且 $E_{\mathrm{D}}(\psi) \leq C(\psi)$。在计算基中测量式 (2) 的每条边，得到测量源；它是一个由独立均匀比特构成的经典源，每个比特对应边的标签，并由该边的持有者知晓。其公开通信下的密钥容量即测量容量 $C^{\mathrm{Z}}(\mathcal{G})$，由式 (1) [9]给出。最细划分 是将用户划分为单个用户的划分。主要结果如下。

定理 1（GHZ网络容量）。 对于每个超图 $\mathcal{G}$,

$$C(\Psi_{\mathcal{G}}) = E_{\mathrm{D}}(\Psi_{\mathcal{G}}) = C^{\mathrm{Z}}(\mathcal{G}).$$

该容量还可在有限区块长度下以零误差实现，密钥率为 [10]，因此根据引理 3，GHZ率也为该值（第4节）。

[2]The 距离是在给定每个 f 后计算，再取平均值，因为 F 是公开的，所有用户都知道。

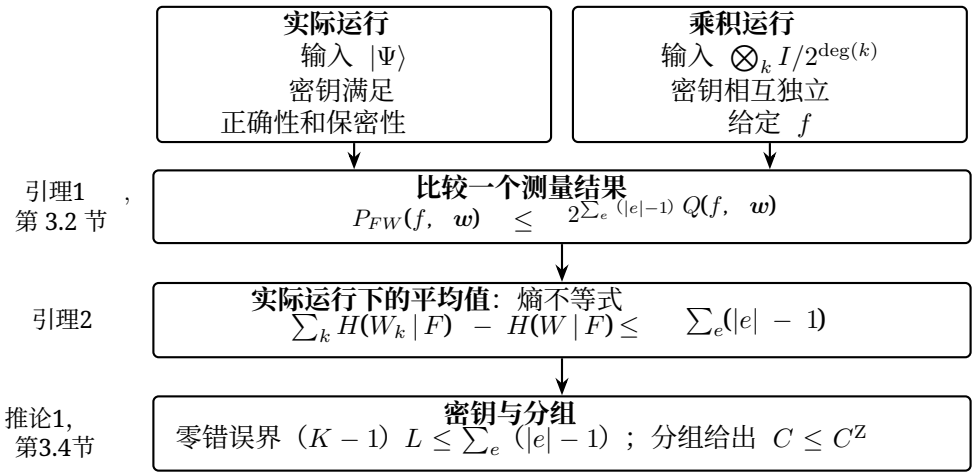


图 2：反向证明。两次运行均对具有相同边缘分布的输入应用相同的测量，并使用局部乘积效应；剩余步骤将一个测量结果的比较转化为熵不等式。

下面的示例证明了第1.1节中两个运行示例的容量，即环和完全网络的容量。

例 1 (环与完全网络**)**。 在由 $K \geq 3$ 个贝尔对构成的环中，一个划分 $\mathcal{P}$ 至少被 $|\mathcal{P}|$ 条边穿过，因此其值至少为 $|\mathcal{P}|/(|\mathcal{P}|-1) \geq K/(K-1)$，即最细划分的值；因此容量为 $K/(K-1)$，三角形上的容量为 $3/2$ 。将环的每条 K生成路径在 $K-1$ 个副本上各使用一次，每条边均被使用 $K-1$ 次；随后将每条路径融合为全局*GHZ*态，并通过广播相邻标签的奇偶校验（为进行*GHZ* 蒸馏而相干计算，见第*4*节），即可无错误地达到该速率。在完全网络中，最细划分是最优的。一条边恰好在 n 个用户的某个部分中缺失，当且仅当它连接其余 $K-n$个用户；这样的边共有 $\binom{K-n}{J}$ 条，因此具有部分大小 n_1、.....、$n_{|\mathcal{P}|}$ 的划分 $\mathcal{P}$ 的值为

$$\binom{K}{J} - \frac{1}{|\mathcal{P}|-1}\sum_i \binom{K-n_i}{J}.$$

由于 $n \mapsto \binom{K-n}{J}$ 是凸函数，对于固定的部分数，当其中一部分包含除 $|\mathcal{P}|-1$ 个用户外的所有用户时，该值最小，此时等于 $\binom{K-1}{J-1} - \binom{|\mathcal{P}|-1}{J}/\left(|\mathcal{P}|-1\right)$ 。被减去的项等于$\binom{|\mathcal{P}|-2}{J-1}/J$，它关于 $|\mathcal{P}|$单调不减，因此最小值出现在 $|\mathcal{P}| = K$，即最细划分处，并且$C\left(\Psi_{K,\ J}\right) = \binom{K}{J}\frac{J-1}{K-1}$，对应于最小割 $\binom{K-1}{J-1}$，即情形 $|\mathcal{P}| = 2$；对于贝尔对 $J = 2$，它们分别是 $K/2$ 和 $K-1$。

3 定理1的证明：反向证明

反向证明将方案在网络上的实际运行与其乘积运行进行比较；在乘积运行中，对网络状态的边缘分布之积应用相同的测量。图 2 展示了各个步骤。第 3.1 节证明了 GHZ 网络的双持有者不等式；第 3.2 节利用该不等式比较两次运行中每种测量结果的概率；第 3.3 节则将这一比较

转化为熵不等式和密钥界，并在按各个划分对网络进行分组后应用该密钥界。

在本节中，$|\Psi\rangle = |\Psi_{\mathcal{G}}\rangle$ 对于一个 GHZ网络 $\mathcal{G} = ([K],\ \mathcal{E})$，其密度算子为 Ψ。用户 k在 k 处持有每个 GHZ态的一个量子比特；其数量 deg(k) 是该用户的度，因此 $\sum_k \deg(k) = \sum_e |e|$，而其份额的密度算子 S_k（对其他用户 Ψ 进行偏迹）是最大混合态 $I/2^{\deg(k)}$，因为每个 GHZ态贡献一个均匀分布的标签，且各 GHZ态彼此独立。第3.1节至第3.3节研究单个 GHZ网络副本上的方案，$N = 1$。由于 N 个 GHZ网络副本构成一个 GHZ网络，其中每条边出现 N 次，因此这些结果同样适用于分组长度 N；第3.4节将它们应用于分组网络的 N 个副本。

3.1 双持有者不等式

以下不等式界定了 GHZ网络上所有用户的局部事件同时发生的概率；第 3.2 节用它将该网络与其边缘分布的乘积进行比较。

引理1 (每个标签对应两个持有者)。 对于正算子 Λ_k，其中 Λ_k 作用于用户 k 的份额 S_k，

$$\langle\Psi| \bigotimes_k \Lambda_k |\Psi\rangle \ \le\ \frac{1}{2^{|\mathcal{E}|}} \prod_{k=1}^{K} \operatorname{Tr} \Lambda_k. \tag{6}$$

证明。步骤 *1*：乘积向量。 设 $\boldsymbol{z} = (z_e)_e$ 为所有边的标签，$\boldsymbol{z}_{(k)} = (z_e)_{e\ni k}$ 为用户 k持有的标签，

$$|\Psi\rangle \ =\ \frac{1}{\sqrt{2^{|\mathcal{E}|}}} \sum_{\boldsymbol{z}} \bigotimes_k |\boldsymbol{z}_{(k)}\rangle_k .$$

对于 S_k中的单位向量 $|u_k\rangle$，令 $g_k(\boldsymbol{z}_{(k)}) = |\langle u_k|\boldsymbol{z}_{(k)}\rangle|$，则其 ℓ_2 范数为 $\|g_k\| = (\sum_{\boldsymbol{z}_{(k)}} g_k^2)^{1/2} = \|u_k\| = 1$，因为向量 $|\boldsymbol{z}_{(k)}\rangle$ 构成了 S_k的计算基。于是

$$\begin{aligned}\Big|\Big(\bigotimes_k \langle u_k|\Big)|\Psi\rangle\Big| \ &=\ \frac{1}{\sqrt{2^{|\mathcal{E}|}}}\Big|\sum_{\boldsymbol{z}}\prod_k \langle u_k|\boldsymbol{z}_{(k)}\rangle\Big| \ \overset{(a)}{\le}\ \frac{1}{\sqrt{2^{|\mathcal{E}|}}}\sum_{\boldsymbol{z}}\prod_k g_k(\boldsymbol{z}_{(k)}) \\ &\overset{(b)}{\le}\ \frac{1}{\sqrt{2^{|\mathcal{E}|}}}\prod_k \|g_k\| \ =\ \frac{1}{\sqrt{2^{|\mathcal{E}|}}},\end{aligned} \tag{7}$$

其中，第一个等号成立是因为两个乘积向量的内积等于其各因子内积的乘积；(a) 是对项 $c_{\boldsymbol{z}} = \prod_k \langle u_k|\boldsymbol{z}_{(k)}\rangle$应用三角不等式 $|\sum_{\boldsymbol{z}} c_{\boldsymbol{z}}| \le \sum_{\boldsymbol{z}} |c_{\boldsymbol{z}}|$，其中 $|c_{\boldsymbol{z}}| = \prod_k g_k(\boldsymbol{z}_{(k)})$；最后一个等号用到了 $\|g_k\| = 1$；(b) 则是以下不等式：对于 $\boldsymbol{z}_{(k)}$上的任意非负函数 g_k，

$$\sum_{\boldsymbol{z}}\prod_k g_k(\boldsymbol{z}_{(k)}) \ \le\ \prod_k \|g_k\|. \tag{8}$$

我们通过对边的数量进行归纳法来证明 (8)；这是 Finner不等式 [15] 的一个特例。没有边时，每个 g_k 都是常数，且 (8) 取等号。否则，选取一条边 e，其持有者为

k_1、……、k_m、 $m = |e| \geq 2$，并用 $\boldsymbol{z}'$ 表示所有其他边的标签，因此只有 g_{k_1}、……、g_{k_m} 依赖于 z_e。令

$$\hat{g}_{k_i} \;=\; \Big(\sum_{z_e} g_{k_i}^2\Big)^{1/2} \quad (i=1,\ldots,m), \qquad \hat{g}_k \;=\; g_k \quad (k \notin e),$$

用户 k 除 z_e之外的标签的函数。于是

$$\begin{aligned}\sum_{\boldsymbol{z}} \prod_k g_k \;&=\; \sum_{\boldsymbol{z}'} \prod_{k\notin e} g_k \cdot \sum_{z_e} \prod_{i=1}^{m} g_{k_i} \;\overset{(a)}{\leq}\; \sum_{\boldsymbol{z}'} \prod_{k\notin e} g_k \cdot \prod_{i=3}^{m} \hat{g}_{k_i} \cdot \sum_{z_e} g_{k_1} g_{k_2} \\ &\overset{(b)}{\leq} \sum_{\boldsymbol{z}'} \prod_{k\notin e} g_k \cdot \prod_{i=1}^{m} \hat{g}_{k_i} \;=\; \sum_{\boldsymbol{z}'} \prod_k \hat{g}_k \;\overset{(c)}{\leq}\; \prod_k \|\hat{g}_k\| \;\overset{(d)}{=}\; \prod_k \|g_k\|,\end{aligned}$$

其中，(a) 对 $i \geq 3$ 使用 $g_{k_i} \leq \hat{}g_{k_i}$，因为平方和中的任意一项都不大于总和；(b) 是柯西–施瓦茨不等式 $\sum_{z_e} g_{k_1} g_{k_2} \leq (\sum_{z_e} g_{k_1}^2)^{1/2} (\sum_{z_e} g_{k_2}^2)^{1/2} = \hat{}g_{k_1} \hat{}g_{k_2}$；(c) 是去掉 e后的网络的归纳假设；(d) 使用 $\|\hat{}g_{k_i}\| = \|g_{k_i}\|$，这是对 k_i持有的其余标签上的 $\hat{}g_{k_i}^2$ 求和得到的；并对 $k \notin e$使用 $\hat{}g_k = g_k$。

步骤 *2*：正算子。将 $\Lambda_k = \sum_i \alpha_{k,i} |u_{k,i}\rangle\langle u_{k,i}|$ 写成具有特征值 $\alpha_{k,i} \geq 0$ 和正交归一特征向量的形式。于是，根据 (7)，对任意一组选定的特征向量，

$$\begin{aligned}\langle\Psi| \bigotimes_k \Lambda_k |\Psi\rangle \;&=\; \sum_{i_1,\ldots,i_K} \prod_k \alpha_{k,i_k} \cdot \Big| \Big(\bigotimes_k \langle u_{k,i_k}| \Big) |\Psi\rangle \Big|^2 \\ &\leq\; \frac{1}{2^{|\mathcal{E}|}} \sum_{i_1,\ldots,i_K} \prod_k \alpha_{k,i_k} \;=\; \frac{1}{2^{|\mathcal{E}|}} \prod_k \operatorname{Tr} \Lambda_k. \qquad \square\end{aligned}$$

3.2 乘积运行

乘积运行将同一方案应用于 $\bigotimes_k I/2^{\deg(k)}$，即 $|\Psi\rangle$的边缘分布之积，其中各用户相互独立；这是一种计算，而非用户实际执行的操作。根据(3)，它给出(F, W)的分布

$$Q(f, \boldsymbol{w}) \;=\; \frac{\operatorname{Tr} \Gamma_{f,\boldsymbol{w}}}{2^{\sum_k \deg(k)}} \;=\; \prod_k \frac{\operatorname{Tr} \Gamma_{k,f,w_k}}{2^{\deg(k)}}. \tag{9}$$

给定 $F = f$，在 Q下各密钥相互独立：其中 $Q_F(f) = \prod_k \operatorname{Tr}[V_{k,f}^\dagger V_{k,f}]/2^{\deg(k)}$，并且对于$Q_F(f) > 0$，$Q_{W_k|F}(w|f) = \operatorname{Tr} \Gamma_{k,f,w} / \operatorname{Tr}[V_{k,f}^\dagger V_{k,f}]$，这是 w上的一个分布，因为$\sum_w \Gamma_{k,f,w} = V_{k}^\dagger{}_{,f} V_{k,f}$，

$$Q(f, \boldsymbol{w}) \;=\; Q_F(f) \prod_k Q_{W_k|F}(w_k|f).$$

比较一个测量结果。根据(3)和引理1，其中$\Lambda_k = \Gamma_{k,f,w_k}$，

$$\begin{aligned}P_{FW}(f, \boldsymbol{w}) \;&=\; \langle\Psi| \Gamma_{f,\boldsymbol{w}} |\Psi\rangle \;\overset{(6)}{\leq}\; \frac{1}{2^{|\mathcal{E}|}} \prod_k \operatorname{Tr} \Gamma_{k,f,w_k} \\ &\overset{(9)}{=}\; \frac{2^{\sum_k \deg(k)}}{2^{|\mathcal{E}|}} Q(f, \boldsymbol{w}) \;=\; 2^{\sum_e (|e|-1)} Q(f, \boldsymbol{w}),\end{aligned} \tag{10}$$

其中最后一步使用了 $\sum_k \deg(k) - |\mathcal{E}| = \sum_e |e| - |\mathcal{E}| = \sum_e (|e| - 1)$，因为每条边 e都向其 $|e|$个持有者各贡献一个量子比特。

3.3 GHZ 网络的熵不等式

比较式 (10) 给出了在公开通信条件下密钥的条件总相关 $\sum_k H(W_k \mid F) - H(W \mid F)$的界，对于零错误 L比特密钥，该值等于 $(K-1)L$ 。[3]

引理2 (熵不等式)。 对于 *GHZ*网络上的任意方案，

$$\sum_{k=1}^{K} H(W_k \mid F) - H(W \mid F) \;\le\; \sum_{e\in\mathcal{E}} (|e|-1). \tag{11}$$

证明。 根据 (10)， $P_{FW}(f,\boldsymbol{w}) > 0$ 蕴含 $Q(f,\boldsymbol{w}) > 0$，且相对熵满足

$$D(P_{FW}\|Q) \;=\; \sum_{f,\boldsymbol{w}} P_{FW}(f,\boldsymbol{w}) \log \frac{P_{FW}(f,\boldsymbol{w})}{Q(f,\boldsymbol{w})} \;\overset{(10)}{\le}\; \sum_{e} (|e|-1).$$

令 $P_{W|f}$ 和 $P_{W_k|f}$ 分别表示实际运行中给定 $F=f$ 时 W 和 W_k 的分布，并令 $Q_{W_k|f} = Q_{W_k|F}(\cdot|f)$。于是

$$\begin{aligned}
D(P_{FW}\|Q) &\overset{(a)}{=} D(P_F\|Q_F) + \sum_f P_F(f)\, D\Big(P_{W|f} \,\Big\|\, \prod_k Q_{W_k|f}\Big) \\
&\overset{(b)}{=} D(P_F\|Q_F) + \sum_f P_F(f)\Big[D\Big(P_{W|f} \,\Big\|\, \prod_k P_{W_k|f}\Big) + \sum_k D\big(P_{W_k|f} \,\big\|\, Q_{W_k|f}\big)\Big] \\
&\overset{(c)}{\ge} \sum_f P_F(f)\, D\Big(P_{W|f} \,\Big\|\, \prod_k P_{W_k|f}\Big) \;\overset{(d)}{=}\; \sum_k H(W_k \mid F) - H(W \mid F),
\end{aligned}$$

其中，(a) 是在 $Q_{W|F}(\cdot|f) = \prod_k Q_{W_k|f}$条件下相对熵的链式法则；(b) 是对 $P_{W|f}$取期望，计算 $\log \frac{P_{W|f}}{\prod_k Q_{W_k|f}} = \log \frac{P_{W|f}}{\prod_k P_{W_k|f}} + \underline{\sum_k \log \frac{P_{W_k|f}}{Q_{W_k|f}}}$ 得到的；(c) 舍去非负的相对熵；(d) 则利用 $D(P_{W|f}\|\prod_k P_{W_k|f}) = \sum_k H(W_k \mid F=f) - H(W \mid F=f)$，并对 $\overline{f}$取平均。

□

引理2对密钥长度给出如下界。

推论1 （GHZ 网络上的密钥界）。 在 *GHZ* 网络上，若某个方案生成一个 L 位的密钥 $L \ge 1$，且在（4）、（5） 中的错误为 $0 \le \varepsilon \le 1/2$ ，则满足

$$(K-1)L\big(1 - 2[\varepsilon + h_2(\varepsilon)]\big) \;\le\; \sum_{e\in\mathcal{E}} (|e|-1),$$

其中 h_2 为二元熵。特别地，对于零错误方案，（$K-1$） $L \le \sum_e$ （$|e|-1$） 。

证明。 根据链式法则，对于 $W = (W_1,\dots,W_K)$，

$$\begin{aligned}
\sum_{k=1}^{K} H(W_k \mid F) - H(W \mid F) \;&=\; \sum_{k=2}^{K} I(W_k; W_1\cdots W_{k-1} \mid F) \;\ge\; \sum_{k=2}^{K} I(W_k; W_1 \mid F) \\
&=\; \sum_{k=2}^{K} \big[H(W_1 \mid F) - H(W_1 \mid W_k, F)\big].
\end{aligned}$$

[3]如果用户先测量其标签，公开通信不会增加他们所观察到内容的总相关 [8], ; 这一单调性也是交互式安全求和通信反向证明背后的原理 [17]。引理2对保留量子存储器的用户也给出了相同的界。

由熵的连续性 [18, 定理 10.7.4]，对每个 f 应用保密性 (5)，并利用 h_2 的凹性对 f 取平均，得到 $H(W_1 \mid F) \geq (1-\varepsilon)L - h_2(\varepsilon)$；由 Fano 不等式 [19, 定理 2.10.1]，正确性 (4) 给出对每个 $k \neq 1$ 均有 $H(W_1 \mid W_k, F) \leq \varepsilon L + h_2(\varepsilon)$。因此，对每个 $k \neq 1$，有 $H(W_1 \mid F) - H(W_1 \mid W_k, F) \geq (1-2\varepsilon)L - 2h_2(\varepsilon) \geq L(1 - 2[\varepsilon + h_2(\varepsilon)])$，因为 $L \geq 1$；由 (11) 即可得到所述结论。 □

下面的例子比较了两种资源，仅根据用户群体熵的界无法区分它们。

例 2（贝尔三角形和两个 GHZ 态）。考虑 $K = 3$ 个用户的零错误密钥，其中一个共享密钥比特需要 $K - 1 = 2$ 单位的总相关。贝尔三角形是例 *1* 中取 $K = 3$的环，包含三条边 $e = \{1,2\}$、$\{1,3\}$、$\{2,3\}$，每条边都是由 $|e| = 2$ 个用户持有的贝尔对，因此每个副本的总相关为 $\sum_e (|e| - 1) = 3 \cdot 1 = 3$，而推论*1*给出 $2L \leq 3N$，即$L \leq \frac{3}{2}N$。由三个用户共享的两个 *GHZ* 态，即$\Psi_{3,\ 3}$的两个副本，具有两条平行边，均位于 $\{1,2,3\}$上，每条边由 $|e| = 3$ 个用户持有，因此 $\sum_e (|e| - 1) = 2 \cdot 2 = 4$，而推论*1*给出$2L \leq 4N$，即 $L \leq 2N$。尽管这两种资源在每个用户群体上的熵都相同，但两种速率都可以通过零错误实现。

3.4 按划分分组

定理 *1* 中逆命题的证明。由于 $E_{\mathrm{D}} \leq C$，只需给出 C 的上界。固定一个有$|\mathcal{P}| \geq 2$ 个部分的划分 $\mathcal{P}$，并将每个部分中的用户合并为一个用户，其中包含用户 1 的部分使用 W_1；这只会扩大方案集合，并保持正确性和保密性。一个部分内部的 GHZ态可以省略，因为该部分能够自行制备它；而且，在一个局部酉变换意义下，由同一部分持有的 GHZ态的量子比特等同于一个量子比特。对于一个在 N 个 $\Psi_{\mathcal{G}}$ 副本上运行、具有 L 个密钥比特且错误为 ε_N 的方案，这些 N 个副本便构成一个由 $|\mathcal{P}|$ 个用户组成的 GHZ网络，其每条剩余边 e 上有 N 个副本，此时有 r_e 个持有者（$\mathcal{P}$）；将 K 替换为 $|\mathcal{P}|$，应用推论1可得

$$(|\mathcal{P}| - 1)L\big(1 - 2[\varepsilon_N + h_2(\varepsilon_N)]\big) \;\leq\; N \sum_e \big(r_e(\mathcal{P}) - 1\big).$$

当 $\varepsilon_N \to 0$ 时，因子 $1 - 2[\varepsilon_N + h_2(\varepsilon_N)]$ 趋于 1，因此无需对 L/N 给出先验界。除以 N，令 $N \to \infty$，再对 $\mathcal{P}$ 取最小值，得到 $C(\Psi_{\mathcal{G}}) \leq C^{\mathrm{Z}}(\mathcal{G})$。对于零错误方案，该因子为 1，因此在任意分组长度 N 下都有 $L/N \leq C^{\mathrm{Z}}(\mathcal{G})$。 □

注*1*（非均匀标签）。定理 *1* 可推广至任意有限标签分布 p_e 的 *GHZ* 态$\sum_z \sqrt{p_e(z)} \bigotimes_{k \in e} |u_{e,k}(z)\rangle$，且错误渐消；对于每个持有者 k，取正交归一向量 $\{|u_{e,k}(z)\rangle\}_z$。根据施密特分解，这涵盖了所有纯双体态，其中p_e 为施密特系数平方。此时，式 *(1)* 仍成立，只需为每条边赋予权重 $H(p_e)$。在每条边的标签基上进行测量，可得到相互独立、熵为 $H(p_e)$ 的标签，因此经典划分公式 *[8, 9]* 可达到式 *(1)* 的加权值作为密钥率，而引理 *3* 则给出 *GHZ* 蒸馏的相同下界。对于反向证明，纠缠稀释 *[20,* 第 *IV.A* 节*]* 可通过局域操作与经典通信，从由相同持有者共享的标准 *GHZ* 态制备每个这样的量子态，速率为 $H(p_e)$，且错误渐消。从 *GHZ* 网络中每条边取 m_e 个副本 $m_e/N \to H(p_e)$进行稀释，再对非均匀网络应用任意 *GHZ* 蒸馏方案，即可在该 *GHZ* 网络上得到错误渐消的方案；测量其输出可获得密钥，而第*3.4*节的有限误差界中，每条边的 N 个副本替换为 m_e 个副本（其随 N 变化），再除以 N，即可得到式 *(1)* 的加权值。根据引理 *3*，会议密钥也满足相同的上界。

4 定理 1 的证明：可达性

在计算基上测量每个 GHZ 态，并对测量所得的源运行最优经典密钥协商方案，可达到 $C^{\mathrm{Z}}(\mathcal{G})$ 作为密钥率 [8, 定理 1 和命题 1], [9], ，因此 $C(\Psi_{\mathcal{G}}) \geq C^{\mathrm{Z}}(\mathcal{G})$。对于有限线性源，全知的线性通信可在有限分组长度下以零错误达到该密钥率；测量所得的源 [10] 也属于此类源。GHZ 蒸馏可由密钥协商推出，依据以下结果：该结果适用于具有 K 个用户的任意有限维纯源 $|\psi\rangle$ ，并采用第 2 节的模型。

引理 3（从密钥到 GHZ 蒸馏）。对于第 *2* 节模型中的每个有限维纯源，$E_{\mathrm{D}}(\psi) = C(\psi)$。一个零错误的 L 比特密钥协商方案可通过局域操作与经典通信扩展，从而精确生成 $|\text{GHZ态}_{[K]}\rangle^{\otimes L}$ ；而错误分别为 ε 、满足 (4) 和 (5) 的密钥协商方案可生成输出 $\sigma_{f'}$，满足 $\sum_{f'} P_{F'}(f')\frac{1}{2}\|\sigma_{f'} - \text{GHZ态}_{[K]}^{\otimes L}\|_1 \leq 2\sqrt{\varepsilon}$，其中 $\vec{F} = (X_1, \ldots, X_{T+K})$ 是密钥协商方案的公开通信 F，后接扩展过程中广播的结果 $X_{T+1}, \ldots, X_{T+K}$；当 $\varepsilon \to 0$ 时，该错误趋于 0 。

思路如下；证明见附录 A。让用户相干地运行密钥协商方案，并保留所有寄存器。给定公开通信后，零错误密钥会使量子态成为 $\frac{1}{\sqrt{2^L}} \sum_w |w\rangle^{\otimes K} |\chi_w\rangle$，其中所有其他寄存器的剩余态 $|\chi_w\rangle$ 可能彼此纠缠，也可能取决于密钥值 w。每次由一位用户测量其剩余寄存器，并根据自己的密钥寄存器相干地选择测量基：该基与其剩余态在该密钥值下的每个特征向量具有相同的重叠，这个基由特征向量经离散傅里叶变换得到。因此，对于每个密钥值，每个测量结果的概率都相同，所以广播结果不会泄露任何密钥信息，w 上的叠加态仍保持均匀分布；最后一位用户测量后，每个 w 只剩下一个已知相位，再由一位用户将其消除。

将引理 3 [10], 应用于零错误方案，可得 $E_{\mathrm{D}}(\Psi_{\mathcal{G}}) \geq C^{\mathrm{Z}}(\mathcal{G})$，在有限区块长度下同样具有零错误。结合第 3 节的反向证明，即完成了定理 1 及其后零错误陈述的证明。

对于这样一种线性方案：每位用户都能恢复所有标签，且定义密钥的线性形式构成广播形式行空间补空间的一组基，因此公开通信 f 与密钥 w 共同确定所有标签（如 [10]和例 3 所示），其扩展方式很简单。每位用户无需测量标签，只需计算将广播到辅助系统的内容，测量辅助系统，并广播测量结果。在固定 f时，每位用户的标签都是 w 的仿射函数，用户可据此恢复 w，因此，对该用户的寄存器施加一个可逆仿射映射，即可将其标签变换为（w，0）；该映射置换基态，因此是酉算子。随后，剩余寄存器为 $|0\rangle$，因此用户无需像引理 3 的证明中那样在傅里叶基下测量它们并校正相位。下面的例子展示了贝尔三角形中的这一过程。

例 *3*（贝尔三角形的两个副本）。对于带有 $K = 3$ 的例 *1* 中的环，将两个副本的标签写作 $\boldsymbol{z} = (a_1, a_2, b_1, b_2, c_1, c_2) \in \mathbb{F}_2^6$，其中 a_i、b_i、c_i 是副本 i 中 $\{1,2\}$、$\{1,3\}$、$\{2,3\}$ 上贝尔对的标签。用户 *1* 按此顺序在其寄存器中持有 (a_1, a_2, b_1, b_2)，用户 *2* 持有 (a_1, a_2, c_1, c_2)，用户 *3* 持有 (b_1, b_2, c_1, c_2)。这两个副本

$$|\Psi\rangle^{\otimes 2} = \frac{1}{\sqrt{2^6}} \sum_{\boldsymbol{z} \in \mathbb{F}_2^6} |a_1 a_2 b_1 b_2\rangle_1 |a_1 a_2 c_1 c_2\rangle_2 |b_1 b_2 c_1 c_2\rangle_3 .$$

通信。 如图*1(b)*所示，用户 k 在第 k 轮广播 x_k ，其中

$$f=(x_1,x_2,x_3)=(a_1+b_1,\ a_2+c_1,\ b_2+c_2)=\mathbf{H}\boldsymbol{z},\qquad \mathbf{H}=\begin{pmatrix}1&0&1&0&0&0\\0&1&0&0&1&0\\0&0&0&1&0&1\end{pmatrix},$$

其中$\mathbf{H}$ 的列按 $\boldsymbol{z}$中的顺序排列。

密钥。 密钥为 $w=(a_1,a_2,b_2)$。给定 f，其他标签为

$$b_1=a_1+x_1,\qquad c_1=a_2+x_2,\qquad c_2=b_2+x_3, \tag{12}$$

因此，全部六个标签由 w和 f确定。广播 x_1、 x_2、 x_3分别包含 b_1、 c_1、 c_2，而这些都不在 w中。因此， a_1、 a_2、 b_2、 x_1、 x_2、 x_3是标签的线性无关函数，(w,f)在 $\mathbb{F}_2^6$上均匀分布，且密钥均匀分布并独立于 f： $C\geq 3/2$。

恢复。 每个用户都根据(12)恢复其缺失的 w 中的条目：用户1 持有 w；用户2持有a_1、 a_2 并恢复 $b_2=c_2+x_3$；用户3 持有 b_2 并恢复 $a_1=b_1+x_1$ 和 $a_2=c_1+x_2$。

辅助系统。 量子方案在叠加态上执行相同的步骤，而不测量标签。每个用户都添加一个处于 $|0\rangle$ 的辅助量子比特，并将自己的广播加到其中；对于用户1，$|a_1a_2b_1b_2\rangle_1|0\rangle\mapsto|a_1a_2b_1b_2\rangle_1|a_1+b_1\rangle$；用户2 同理使用 a_2+c_1，用户3则使用 b_2+c_2。这可通过一个酉算子实现，即对基态进行可逆映射，将 a_1+b_1 加到辅助量子比特值上。标签保持不变，三个辅助系统在每一项中都包含$\mathbf{H}\boldsymbol{z}$ ：

$$\begin{aligned}&\frac{1}{\sqrt{2^6}}\sum_{\boldsymbol{z}\in\mathbb{F}_2^6}|a_1a_2b_1b_2\rangle_1|a_1a_2c_1c_2\rangle_2|b_1b_2c_1c_2\rangle_3|\mathbf{H}\boldsymbol{z}\rangle_{\text{anc}}\\&=\sum_{f\in\mathbb{F}_2^3}\frac{1}{\sqrt{2^6}}\sum_{\boldsymbol{z}:\,\mathbf{H}\boldsymbol{z}=f}|a_1a_2b_1b_2\rangle_1|a_1a_2c_1c_2\rangle_2|b_1b_2c_1c_2\rangle_3|f\rangle_{\text{anc}}.\end{aligned}$$

根据(12)，具有$\mathbf{H}\boldsymbol{z}=f$ 的向量由 w的 2^3 值给出。用户只测量辅助系统并广播测量结果 f，因此 f 像之前一样成为公开信息，对每个 f的概率为 $2^3/2^6=2^{-3}$。标签不进行测量：所有含有$\mathbf{H}\boldsymbol{z}=f$的项具有相同的振幅 $\frac{1}{\sqrt{2^6}}$，因此重新归一化后，它们的振幅为 $\frac{1}{\sqrt{2^3}}$；将 b_1、 c_1和c_2通过(12)写出后，量子态为

$$\frac{1}{\sqrt{2^3}}\sum_{a_1,a_2,b_2}|a_1,a_2,a_1{+}x_1,b_2\rangle_1|a_1,a_2,a_2{+}x_2,b_2{+}x_3\rangle_2|a_1{+}x_1,b_2,a_2{+}x_2,b_2{+}x_3\rangle_3.$$

提取密钥。 没有用户知道 w，但每个用户都知道 f，因此也知道在每一项中，其寄存器如何依赖于 w 。在密钥协商中，用户 k 根据其标签和 f计算出 w ；这里，它在右矢内执行相同的计算，对其寄存器的四个比特(y_1、 y_2、 y_3、 y_4)应用依赖于 f 的可逆映射，并将每一项中的寄存器变为$(w,0)$：

- 用户 1：$(y_1,y_2,y_3,y_4)\mapsto(y_1,\ y_2,\ y_4,\ y_3+y_1+x_1)$；
- 用户 2：$(y_1,y_2,y_3,y_4)\mapsto(y_1,\ y_2,\ y_4+x_3,\ y_3+y_2+x_2)$；
- 用户 3：$(y_1,y_2,y_3,y_4)\mapsto(y_1+x_1,\ y_3+x_2,\ y_2,\ y_4+y_2+x_3)$。

右矢中标签的可逆映射会置换计算基态，因此它是酉算子。将其作用于每一项后，它保持

$$\frac{1}{\sqrt{2^3}}\sum_{w\in\mathbb{F}_2^3}|w\rangle_1|w\rangle_2|w\rangle_3\otimes|0\rangle_1|0\rangle_2|0\rangle_3=|\mathrm{GHZ}_{123}\rangle^{\otimes 3}\otimes|0\rangle_1|0\rangle_2|0\rangle_3$$

for 每个 f。因此，在贝尔三角形上，使用两个副本可实现零误差$E_{\mathrm{D}}\geq 3/2$ 。

5 结论

对于每个独立 GHZ 态网络，在配备量子存储器并进行任意轮次的无限制局部操作与经典通信下，先测量每个 GHZ 态即可达到会议密钥容量，而相干实现对于 GHZ 蒸馏也能达到相同速率；该容量就是测量容量（1）。对于每个纯源，会议密钥与 GHZ 蒸馏具有相同的容量。

这些结果假设公开经典通信在通信量和轮次数方面都是免费的，GHZ态是纯态且相互独立的，窃听者只能观察公开通信，并且用户拥有无限的本地量子存储和辅助系统。

引理 3 的证明

在计算基中测量 GHZ 蒸馏方案的输出，得到的密钥错误率至多相同，因此 $E_{\mathrm{D}} \le C$，接下来只需证明 $C \le E_{\mathrm{D}}$。

相干运行。 根据第 2 节，密钥协商方案的每一轮都是先进行等距映射 $|\phi\rangle \mapsto \sum_x O_x |\phi\rangle |x\rangle$，再测量结果寄存器 $|x\rangle$；因此，给定公开通信 f，当 $P_F(f) > 0$ 时，用户的量子态是归一化的纯态 $V_f |\psi\rangle^{\otimes N}$。用户 k 不进行密钥测量 $\{M_{k,w}\}$，而是将等距映射 $|\phi\rangle_{A_k} \mapsto \sum_w M_k^{1/2}$，$_w |\phi\rangle_{A_k} |w\rangle_{W_k}$ 应用到密钥寄存器 W_k中；在计算基中测量 W_k 会得到相同的密钥，且与 F具有相同的联合分布。量子态仍保持纯态。因此，给定 f，用户 k持有其密钥寄存器 W_k和最终寄存器 A_k（即剩余寄存器），其维数为 d_k，且全局量子态是一个纯态

$$|\psi_f\rangle = \sum_{\boldsymbol{w}} \sqrt{P_{W|F}(\boldsymbol{w}|f)}\, |w_1\rangle_{W_1} \cdots |w_K\rangle_{W_K} |\chi_{\boldsymbol{w}}\rangle_{A_1 \cdots A_K}, \tag{13}$$

其中， $P_{W|F}(\cdot|f)$表示给定 f和吸收了相位的归一化态 $|\chi_{\boldsymbol{w}}\rangle$时密钥的分布。

移除剩余寄存器。对于零误差密钥，在式（13）中，只有所有用户都持有相同值 w 的密钥元组会出现，且每个元组的概率为 2^{-L}，因此

$$|\psi_f\rangle = \frac{1}{\sqrt{2^L}} \sum_w |w\rangle^{\otimes K} |\chi_w^{(1)}\rangle,$$

其中， $|\chi_w^{(1)}\rangle = |\chi_{(w,\ldots,w)}\rangle$ 是式（13）中所有用户都持有 w的密钥元组所对应的剩余态。用户按照 $k = 1$、……、 K的顺序操作。在第 k步之前，量子态为 $\frac{1}{\sqrt{2^L}} \sum_w |w\rangle^{\otimes K} |\chi_w^{(k)}\rangle$，其中 $|\chi_w^{(k)}\rangle$ 作用于$A_k \cdots A_K$。令 ρ_w表示 $|\chi_w^{(k)}\rangle$ 在 A_k上的边缘分布，其特征向量为$|v_{w,\ j}\rangle$、 $j = 0$、……、 $d_k - 1$；令G_w 表示从该本征基到计算基的傅里叶变换； ρ_w、其特征向量以及 G_w 还取决于第 k 步和目前为止广播的测量结果，本文记号中省略了这些依赖关系，

$$G_w |v_{w,j}\rangle = \frac{1}{\sqrt{d_k}} \sum_{x=0}^{d_k-1} \omega^{-jx} |x\rangle, \qquad \omega = e^{2\pi i/d_k}.$$

步骤 k 如下。

- 傅里叶变换。用户 k 由其密钥寄存器控制，对 A_k施加 G_w 酉算子$\sum_w |w\rangle\langle w|_{W_k} \otimes G_w$。

- 测量。用户 k 在计算基下测量 A_k，并将测量结果 x广播为 X_{T+k}。对于每个 w，测量结果 x 的概率均为 $\langle x| G_w \rho_w G_w^\dagger |x\rangle = 1/d_k$，因为 ρ_w 在本征基下是对角的，且$|\langle x| G_w |v_{w,j}\rangle|^2 = 1/d_k$ 对于所有 j均成立，因此该测量结果与密钥独立，量子态变为 $\frac{1}{\sqrt{2^L}} \sum_w |w\rangle^{\otimes K} |\chi_{(k+1)w}\rangle$，归一化态为 $|\chi_{(k+1)w}\rangle = \sqrt{d_k}(\langle x| G_w \otimes I)\, |\chi_{(k)w}\rangle$ 的 $A_{k+1} \cdots A_K$。

步骤 K 之后，量子态为 $\frac{1}{\sqrt{2^L}} \sum_w \gamma_w |w\rangle^{\otimes K}$，其中 $|\gamma_w| = 1$；相位 γ_w 由 w、f 和广播结果决定。用户 1 通过施加 $|w\rangle \mapsto \gamma_w^{-1} |w\rangle$来消除该相位；由于 $|\gamma_w| = 1$，这是一个对角酉算子，从而保持 $|\mathrm{GHZ}_{[K]}\rangle^{\otimes L}$不变。该方案仅使用局部操作和广播消息，并且广播消息与密钥独立。

含误差的密钥。此情形可由连续性推出。令 $p_f(w)$ 表示在给定 f 的情况下，所有用户都持有密钥值 w 的概率。将式 (13) 中的 $|\psi_f\rangle$ 与 $|\psi_f^\circ\rangle = \frac{1}{\sqrt{2^L}} \sum_w |w\rangle^{\otimes K} |\chi_w^{(1)}\rangle$ 进行比较，其中 $|\chi_w^{(1)}\rangle$ 是式 (13) 中密钥元组的剩余态，在该元组中所有用户都持有 w；当 $p_f(w) = 0$ 时，可取任意归一化态，这一选择不会影响下面的重叠。该量子态是前一步中的零错误密钥，因此，那里构造的操作会将其转化为 $|\mathrm{GHZ}_{[K]}\rangle^{\otimes L}$。只有所有用户意见一致的密钥元组会对重叠作出贡献，并且两者具有相同的剩余态，因此重叠为 $s_f = \langle\psi_f^\circ|\psi_f\rangle = \sum_w \sqrt{2^{-L} p_f(w)}$。由于 $\sqrt{ab} \geq \min\{a, b\}$ 且 $\sum_w 2^{-L} = 1$，$1 - s_f \leq \sum_w (2^{-L} - p_f(w))_+$，其中 $(a)_+ = \max\{a, 0\}$；而这至多等于在给定 f 时 W_1 的分布与均匀分布之间的全变差距离，加上在给定 f 时各密钥不一致的概率。对 f 取平均后，$\sum_f P_F(f)(1 - s_f) \leq 2\varepsilon$，由式 (4) 和 (5) 得证。

对 $|\psi_f\rangle$ $|\psi_f^\circ\rangle$ 构造的操作（包括相位校正）应用于 $|\psi_f\rangle$，并令 $q(f'|f)$ 和 $\sigma_{f'}$ 分别表示扩展方案中每种公开通信 f' 对应的概率和输出，该扩展方案将 f 扩展得到。丢弃扩展的测量结果后，这些操作构成一个量子信道 $\mathcal{N}_f$，它将 $|\psi_f^\circ\rangle$ 映射为 GHZ态$^{\otimes L}_{[K]}$，因为每种测量结果都会如此；并将 $|\psi_f\rangle$ 映射为 $\sum_{f'} q(f'|f)\sigma_{f'}$。保真度在量子信道作用下不会降低，因此

$$\sum_{f'} q(f'|f)\, \langle \mathrm{GHZ}_{[K]}|^{\otimes L} \sigma_{f'} |\mathrm{GHZ}_{[K]}\rangle^{\otimes L} \;\geq\; |\langle\psi_f^\circ|\psi_f\rangle|^2 \;=\; s_f^2.$$

由于 $\frac{1}{2}\|\sigma - \mathrm{GHZ}^{\otimes L}_{[K]}\|_1 \leq \sqrt{1 - \langle \mathrm{GHZ}_{[K]}|^{\otimes L} \sigma |\mathrm{GHZ}_{[K]}\rangle^{\otimes L}}$，且平方根函数是凹函数，给定 f 时，$\frac{1}{2}\|\sigma_{f'} - \mathrm{GHZ}^{\otimes L}_{[K]}\|_1$ 对 f' 的平均值至多为 $\sqrt{1 - s_f^2} \leq \sqrt{2(1 - s_f)}$；再对 f 求平均，也就是引理 3 中对 F' 求平均，至多为

$$\sum_f P_F(f) \sqrt{2(1 - s_f)} \;\leq\; \sqrt{2 \sum_f P_F(f)(1 - s_f)} \;\leq\; 2\sqrt{\varepsilon}.$$

对于错误为 $\varepsilon_N \to 0$ 的一系列密钥协商方案，扩展方案在相同速率下的错误至多为 $2\sqrt{\varepsilon_N} \to 0$。因此，每个密钥率都是 GHZ率，并且 $C \leq E_{\mathrm{D}}$。

参考文献

[1] G. Murta、F. Grasselli、H. Kampermann 和 D. Bruß，“量子会议密钥协商：综述”，《先进量子技术》，第 3 卷，第 11 期，第 2000025 页，2020 年。

[2] P. Vrana 和 M. Christandl，“从 Greenberger–Horne–Zeilinger 份额中进行纠缠蒸馏”，数学物理通讯，第 352 卷，第 621–627 页，2017 年。[3] S. B¨auml、M. Winczewski 和 K. Horodecki，“量子密钥分发在网络上的普适限制”，《物理评论*X*》，第 11 卷，第 041016 页，2021 年。[4] J. Neumann、H. Kampermann、D. Bruß 和 A. Trushechkin，“成对纠缠网络中的量子会议密钥协商界”，2026 年，arXiv 电子预印本：2605.18399。[5] S. B¨auml 和 K. Azuma，“量子广播网络的基本限制”，《量子科学与技术》，第 2 卷，第 024004 页，2017 年。[6] M. H. Partovi，“复合量子态的相关容量”，《物理评论快报》，第 103 卷，第 230502 页，2009 年。[7] H. S. Murray、S. Bhattacharya、M. Cerezo、L. Lyu 和 M. M. Wilde，“多方 Rains 纠缠洪流”，2026 年，arXiv 电子预印本：2608.11406。[8] I. Csisz´ar 和 P. Narayan，“多个终端的保密容量”，载于《*IEEE*信息论汇刊》，第 50 卷，第 12 期，第 3047–3061 页，2004 年。[9] C. Chan 和 L. Zheng，“秘密密钥协商的互依赖性”，载于第 *44* 届信息科学与系统会议（*CISS*）论文集，2010 年，第 1–6 页，doi:10.1109/CISS.2010.5464805。[10] C. Chan，“线性完美秘密密钥协商”，载于*IEEE*信息论研讨会（*ITW*）论文集，巴西帕拉蒂，2011 年，第 723–726 页。[11] M. Takeoka、E. Kaur、W. Roga 和 M. M. Wilde，“量子网络中的多方纠缠与秘密密钥分发”，2019 年，arXiv 电子预印本：1912.10658v1；v2 版本于 2020 年撤回，并附注：“命题11 存在一个尚未解决的问题”。[12] P. Vrana 和 M. Christandl，“通过组合方法蒸馏 Greenberger–Horne–Zeilinger 态”，《*IEEE*信息论汇刊》，第 65 卷，第 9 期，第 5945–5958 页，2019 年。[13] F. Salek 和 A. Winter，“从量子态中进行共同随机性和纠缠的多用户蒸馏”，《*IEEE*信息论汇刊》，第 68 卷，第 2 期，第 976–988 页，2022 年。[14] ——，“会议密钥和多方纠缠蒸馏的新协议”，《*IEEE*信息论汇刊》，第 71 卷，第 6 期，第 4374–4384 页，2025 年。[15] H. Finner，“H¨older 不等式及一些概率不等式的推广”，《概率年刊》，第 20 卷，第 4 期，第 1893–1901 页，1992 年。[16] H. Kobayashi、F. Le Gall、H. Nishimura 和 M.R¨otteler，“具有免费经典通信的通用量子网络编码方案”，载于《自动机、语言与程序设计国际研讨会（*ICALP*）论文集，《计算机科学讲义》系列，第 5555 卷，2009 年，第 622–633 页，doi:10.1007/978-3-642-02927-1 52。[17] H

. Sun, “Th与容量 ity of interacti安全摘要 tion,” 2026 ，电子印刷版 int arXi 2610 29954 版本：..

[18] M. M. Wilde，《量子信息理论》，第2版，剑桥大学出版社，2017年。[19] T. M. Cover 和 J. A. Thomas，《信息论基础》，第2版，Wiley，2006年。

[20] C. H. Bennett、S. Popescu、D. Rohrlich、J. A. Smolin 和 A. V. Thapliyal，《多体纯态纠缠的精确和渐近测量》，*Physical Review A*，第 63 卷，012307 页，2000 年。