面向目标数据量的安全去中心化柔性索引编码

Anjali Padmanabhan[1]，Danya Arun Bindhu[1],Nujoom Sageer Karat[1],和 Shanuja Sasi[2]1印度卡利卡特国家理工学院电子与通信工程系2印度坎普尔印度理工学院电气工程系 电子邮箱：{anjali_b220700ec、danya_b220817ec、nujoom}@nitc.ac.in、shaunjas@iitk.ac.in

arXiv:2602.03579v1 [cs.IT] 3 Feb 2026

摘要——**去中心化柔性索引编码（DPIC）问题研究的是分布式系统中的高效信息交换，其中客户端彼此通信，无需中央服务器。DPIC 中一个重要的考量因素是侧信息和需求规模的异质性。尽管许多先前研究假设系统处于同质设置，即侧信息基数相同且每个客户端仅有单条消息需求，但这些假设限制了其在现实场景中的适用性，因为客户端通常拥有数量不等的先验信息。本文研究侧信息基数异质情况下的 DPIC 问题。我们提出一种传输方案，通过协调客户端广播来提高编码效率，同时确保每个客户端达到共同的目标层级 T。此外，我们施加严格的安全约束，确保没有客户端获得超过目标数量 T 的消息，从而保证每个客户端最终恰好获得 T 条消息。我们分析了所提方案在该安全约束下产生的通信成本。**

一、引言

索引编码（*IC*） [1] 问题研究高效的广播通信：单个服务器通过无噪声信道向多个接收方传输编码消息，每个接收方拥有部分消息作为侧信息，并请求一条未知消息。通过利用这些侧信息，目标是最小化广播传输的总数量 [2]。传统的 IC 问题假设每个接收方请求一条预先确定的消息，而许多实际系统则允许更大的灵活性。柔性索引编码（*PIC*） [3]问题对这一框架进行了推广，允许每个接收方解码其尚未拥有的任意消息，而不是预先确定的消息。现有大多数 IC 和 PIC 研究还假设由一个拥有所有消息和侧信息全局知识的集中式发送端进行传输；然而，在现代分布式系统中，这种假设往往并不现实[4]。这促使了对去中心化可延展索引编码（*DPIC*） [5]问题的研究：客户端仅基于本地可用的侧信息自行生成并广播编码传输。由于缺乏全局协调，这通常会导致传输数量增加。DPIC 问题可应用于点对点网络、边缘缓存和分布式内容共享平台，这些场景中不存在中心发送端。另一个关键方面是侧信息的基数和需求大小。许多现有 DPIC 研究假设同质设置，即所有客户端拥有相同数量的侧信息，并且恰好需要一条新消息。虽然这简化了编码设计，但它限制了其在现实异构场景中的适用性。在[6],DPIC中，研究了客户端持有不同侧信息基数的情况，并提出了一种最优传输方案，使所有客户端都能达到共同的目标知识水平。

除效率外，隐私和安全性也是索引编码系统中的关键问题。以往研究探讨了在存在或不存在侧信息的情况下如何防范外部窃听者，并提出了弱安全性、块安全性和强安全性等概念，还刻画了线性索引码能够防止非预期消息泄露的条件[7]–[9]。另一类研究则关注接收方之间的隐私，要求每个用户除自身的侧信息和目标消息外，不得获知其他信息；这通常通过服务器与部分用户之间共享密钥来实现 [10]。研究人员也在 PIC 问题中探讨了安全性问题，通过施加限制，确保每个客户端只解码一个新的消息，从而在解码层面有效实现个体安全性[11]。在去中心化场景中，安全问题更为突出，因为传输由用户自身发起，而非由中央服务器发起。近期有关安全 DPIC 的研究施加了个体安全约束，确保每个用户只解码一个新的消息 [12]。研究表明，与集中式场景相比，在安全约束下实现去中心化可能会显著增加传输开销。尽管取得了这些进展，现有的大多数安全 DPIC 研究都假设侧信息规模均匀，且每个用户只有单消息需求。这些假设简化了分析，但限制了相关方法在现实异构网络中的适用性。

A. 我们的贡献

本文针对客户端侧信息大小不均的场景，将安全性纳入 DPIC。我们采用 [6],提出的固定重叠线性递增集合（*LPS-FO*）模型，该模型反映了去中心化网络中的实际异质性：客户端持有的侧信息量各不相同，这种情况在智能交通系统中十分常见。在此类系统中，车辆或路侧单元会交换交通相关信息，并且通常具有可塑性，即只要收到任何新的、有用的消息便会感到满意。由于感知

能力和路线覆盖范围各不相同，不同车辆自然会积累数量不等但彼此重叠的信息集合，这些集合可用于系统地设计高效的去中心化传输策略。在该模型下，我们设计了一种传输算法，通过安排客户端广播，在确保所有客户端达到共同目标知识水平的同时，使每次传输的编码增益最大化，并满足安全约束。安全要求规定，任何客户端获取的消息数量都不得超过预先指定的目标数量T；也就是说，在传输阶段结束时，每个客户端必须恰好拥有 T 条消息。我们还证明，当客户端数量为 3 或 4 时，所提出的方案是最优的。

符号说明：$[a,b]$ 表示集合 $\{a,a+1,a+2,\ldots,b\}$。按位异或（XOR）运算记为 $\oplus$。对于任意集合 A，集合中元素的数量（集合的基数）记为 $|A|$。对于同一集合，其中的第 i 个元素表示为 $A[i]$。

II. 系统模型

我们考虑一个包含 M 条消息的 DPIC 问题，这些消息记为 $\mathcal{X}=\{x_1,x_2,\ldots,x_M\}$，以及包含 C 个客户端的系统，这些客户端记为$\{\mathcal{C}_1,\mathcal{C}_2,\ldots,\mathcal{C}_C\}$。每个客户端 $\mathcal{C}_i$ 都拥有一个消息子集，称为侧信息集 $\mathcal{I}_i\subseteq\mathcal{X}$。在本文中，我们考虑一类特定的异构侧信息结构，并将其称为固定重叠线性递增集合（*LPS-FO*）。

定义1. 固定重叠线性递增集合（LPS-FO） *[6]*：如果客户端的侧信息集满足以下两个性质，则称其为 *LPS-FO*：

- 线性递增：客户端的侧信息集满足这样的条件：每个客户端恰好比前一个客户端多一条消息，且侧信息集中的消息连续。
  - 第一个客户端，$\mathcal{C}_1$，拥有 K 条消息：$\mathcal{I}_1=\{x_1,x_2,\ldots,x_K\}$。– 侧信息集的大小呈线性增长：$|\mathcal{I}_i|=K+(i-1)$，对任意 $i\in[1,C]$ 均成立。– 因此，最后一个客户端 $\mathcal{C}_C$ 拥有最大的集合：$|\mathcal{I}_C|=K+(C-1)$。
- 固定连续重叠：任意两个连续客户端恰好共享 P 条消息，对任意 $P\le K$ 均成立。具体而言，客户端 $\mathcal{C}_i$ 的最后 P 条消息是客户端 $\mathcal{C}_{i+1}$ 的前 P 条消息，其中 $i\in[1,C-1]$。□

本文中，我们假设旁信息集均为 LPS-FO。客户端按顺序编号，直至客户端 $\mathcal{C}_C$，其旁信息集的大小最大。我们的目标是在满足安全约束的条件下，使所有客户端达到共同的知识层级，这在定义2中作了正式定义。该目标定义为比当前知识最丰富的客户端（$\mathcal{C}_C$）所持有的信息多一条消息：$T=|\mathcal{I}_C|+1=K+C$. 在满足安全约束的情况下，传递过程结束后，每个客户端必须恰好拥有 T 条不同的消息。初始

表I 例1和例2中的客户端及侧信息集

客户端	侧信息
$\mathcal{C}_1$	$x_1,x_2,x_3,x_4,x_5,x_6,x_7$
$\mathcal{C}_2$	$x_5,x_6,x_7,x_8,x_9,x_{10},x_{11},x_{12}$
$\mathcal{C}_3$	$x_{10},x_{11},x_{12},x_{13},x_{14},x_{15},x_{16},x_{17},\ x_{18}$
$\mathcal{C}_4$	$x_{16},x_{17},x_{18},x_{19},x_{20},x_{21},x_{22},x_{23},x_{24},x_{25}$
$\mathcal{C}_5$	$x_{23},x_{24},x_{25},x_{26},x_{27},x_{28},x_{29},x_{30},x_{31},x_{32},x_{33}$
$\mathcal{C}_6$	$x_{31},x_{32},x_{33},x_{34},x_{35},x_{36},x_{37},x_{38},x_{39},x_{40},x_{41},x_{42}$
$\mathcal{C}_7$	$x_{40},x_{41},x_{42},x_{43},x_{44},x_{45},x_{46},x_{47},x_{48},x_{49},x_{50},x_{51},x_{52}$
$\mathcal{C}_8$	$x_{50},x_{51},x_{52},x_{53},x_{54},x_{55},x_{56},x_{57},x_{58},x_{59},x_{60},x_{61},x_{62},x_{63}$
$\mathcal{C}_9$	$x_{61},x_{62},x_{63},x_{64},x_{65},x_{66},x_{67},x_{68},x_{69},x_{70},x_{71},x_{72},x_{73},x_{74},x_{75}$

知识库最小的客户端 $\mathcal{C}_1$起初只有 K 条消息。为了达到T，该客户端因此必须恰好接收 C 条新消息，因为 $T-K=(K+C)-K=C$.

定义2. 具有 LPS-FO 的安全 DPIC：对于具有 *LPS-FO* 侧信息集的 *DPIC* 问题，若某一传输方案使所有客户端均提升至同一目标知识水平 $T=|\mathcal{I}_C|+1=K+C$，且满足以下条件，则称该传输方案是安全的。

- 传递过程结束后，每个客户端必须恰好拥有 T 条不同的消息。没有客户端获得超过目标知识水平 T 的知识。

□

定理1 (下界 [6])。对于具有 *LPS-FO* 侧信息集的 *DPIC* 问题，若 $C\ge3$，则所有客户端达到目标知识水平 $T=K+C$ 所需的最优传输次数为 $S_{opt}=C$；若$C=2$，则为 $S_{opt}=3$。

在 [6], 中，针对 $K\ge2P$ 的情形提出了一种最优传输方案，该方案使每个客户端都能达到目标层级，且不受安全约束。本文研究具有 LPS-FO 的安全 DPIC，并提供了一种专门设计的传输方案，以满足该模型中的安全约束。

例1。表 *I* 展示了一个具有 *LPS-FO* 侧信息结构的 *DPIC* 示例，其初始侧信息集大小为$K=7$，固定重叠为 $P=3$。在此示例中，$M=75$，客户端数量为 $C=9$，客户端集合为 $\{\mathcal{C}_i:\ i\in[9]\}$。此配置是有效的 *LPS-FO*，因为它满足两个定义属性。

线性递增：侧信息集的大小会随着后续每个客户端增加 *1*，遵循 $|\mathcal{I}_i|=K+(i-1)$。我们有 $|\mathcal{I}_1|=7$、$|\mathcal{I}_2|=8$、$|\mathcal{I}_3|=9$、.....、$|\mathcal{I}_9|=15$。每个集合中的消息也都是连续的。

固定连续重叠：任意两个连续客户端恰好共享 $P=3$ 条消息。具体而言，$\mathcal{I}_1\cap\mathcal{I}_2=\{x_5,x_6,x_7\}$、$\mathcal{I}_2\cap\mathcal{I}_3=\{x_{10},x_{11},x_{12}\}$、.....、$\mathcal{I}_8\cap\mathcal{I}_9=\{x_{61},x_{62},x_{63}\}$。

在此示例中，目标设为 $T=|\mathcal{I}_C|+1=16$。传递阶段结束时，每个客户端必须恰好拥有 *16* 条不同的消息。

III. 采用 LPS-FO 侧信息集的安全 DPIC 传输方案

本节将介绍一种传输方案，用于一类具有 LPS-FO 侧信息集的安全 DPIC,

符号	描述
C	原始问题中的客户端总数
C^l	递归层级 l 的**算法1**中的客户端数量
$\mathcal{C}_i^l$	递归层级 l中的第 i个客户端
$r_{\max}^l$	在层级 l由 C^l 确定的参数
$\mathcal{I}_{F_j}^{l,i}$	j 条初始重叠段中 客户端 $\mathcal{C}^l_i$的旁信息集
$\mathcal{I}_{L_j}^{l,i}$	j 条末端重叠段中 客户端 $\mathcal{C}^l_i$的旁信息集
$\mathcal{I}_{U_j}^{l,i}$	j 条唯一的（非重叠）消息，位于 客户端 $\mathcal{C}^l_i$的旁信息集
$\mathcal{I}_{U_L}^{l,i}$	最后一条唯一（不重叠）消息 客户端 $\mathcal{C}_i^l$ 的侧信息集
$W_j^{l,i}$	客户端 $\mathcal{C}_i^l$ 在递归层级 l完成的第 j次传输
$\mathcal{W}^l$	层 l的传输集合

表 II 算法1-3中使用的数学符号汇总。

如定理2所述。该方案的可达性通过一种递归算法得到证明，该算法生成所需数量的传输。此过程在算法1中作了形式化说明。

定理2. 考虑一个具有 *LPS-FO* 侧信息集的安全*DPIC*问题，其中 $K \geq 2P$、 $P \geq r_{\max} - 2$ 和 $C \geq 3$，且 $r_{\max}$ 是满足以下条件的正整数

$$\frac{(r_{\max}-2)(r_{\max}-1)}{2} < C \leq \frac{r_{\max}(r_{\max}-1)}{2}. \quad (1)$$

对于此类实例，算法*1*中描述的递归传输方案可使每个客户端达到精确的目标知识水平 $T = K + C$ 。 C 个客户端所需的传输总数为 $N(C)$，其中

$$N(C) = C + N(C - r_{\max}), \quad (2)$$

with $N(0) = 0$, $N(1) = 1$, *and* $N(2) = 3$. □

证明. 我们通过构造一个显式传输方案并证明它能以 $N(C)$ 次传输满足所有客户端的需求，来证明其可达性，从而确保在这一过程结束时，每个客户端恰好持有 T 条消息。算法1针对 LPS-FO 侧信息集设置求解安全 DICP，通过递归方法系统地将原始问题分解为更小的子问题，确保每个客户端恰好获得 $T = K + C$ 条消息。所有必要的符号均见表 II。算法首先初始化递归层级 $l = 1$，并设置 $C^1 = C$（即客户端总数），同时在每一层适当地重新命名客户端以保持一致。在每个递归层级 l，算法确定一个关键参数 $r_{\max}^l$，该参数是基于当前客户端数 C^l、满足组合不等式 (3) 的正整数。此参数决定该层传输的结构。(3) 中的三角数条件确保将 C^l 个客户端划分为一个大小为 $r_{\max}^l$ 的传输组和一个大小为 $C^l - r_{\max}^l$ 的剩余组，后者转至第 $l+1$ 层。

Algorithm 1 Main Recursive Algorithm related to Theorem 2

Require: Number of clients C, client set $\mathcal{C} = \{\mathcal{C}_i, i \in [C]\}$ and their side-information sets with LPS-FO structure.
Ensure: Complete transmission scheme $\mathcal{W}$

Initialize: $l = 1$, $C^1 = C, K^1 = K, \mathcal{W} = \emptyset$
Initial set of clients: $\mathcal{C}^1 = \{\mathcal{C}_i^1 : \mathcal{C}_i^1 = \mathcal{C}_i, i \in [C]\}$
while $C^l > 2$ **do**
  Step 1: Find the positive integer $r_{\max}^l$ satisfying

$$\frac{(r_{\max}^l-2)(r_{\max}^l-1)}{2} < C^l \leq \frac{r_{\max}^l(r_{\max}^l-1)}{2} \quad (3)$$

  if $C^l \neq \frac{(r_{\max}^l-2)(r_{\max}^l-1)}{2} + 1$ **then**
    $\mathcal{W}^l \leftarrow$ Execute **Algorithm 2**$(C^l, K^l, r_{\max}^l, \mathcal{C}^l)$
  else
    $\mathcal{W}^l \leftarrow$ Execute **Algorithm 3**$(C^l, K^l, r_{\max}^l, \mathcal{C}^l)$
  end if
  Add all transmissions from $\mathcal{W}^l$ to $\mathcal{W}$
  Step 2: Prepare clients for next recursive level
  $C^{l+1} = C^l - r_{\max}^l$
  $K^{l+1} = K^l + r_{\max}^l$
  if $C^{l+1} > 0$ **then**
    for $i = 1$ **to** C^{l+1} **do**
      $\mathcal{C}_i^{l+1} \leftarrow \mathcal{C}^l_{r_{\max}^l+i}$
    end for
  end if
  $l \leftarrow l + 1$ {Move to next recursive level}
end while
Base Cases:
if $C^l = 2$ **then**
  $\mathcal{C}_2^l$ transmits $W_1^{l,2} = \mathcal{I}_{F_1}^{l,2} \oplus \mathcal{I}_{U_1}^{l,2}$
  $\mathcal{C}_2^l$ transmits $W_2^{l,2} = \mathcal{I}_{F_1}^{l,2} \oplus \mathcal{I}_{U_2}^{l,2}$
  $\mathcal{C}_1^l$ transmits $W_1^{l,1} = \mathcal{I}_{L_1}^{l,1} \oplus \mathcal{I}_{U_1}^{l,1}$
  $\mathcal{W}^l = \{W_1^{l,2}, W_2^{l,2}, W_1^{l,1}\}$
  Add $\mathcal{W}^l$ to $\mathcal{W}$
else if $C^l = 1$ **then**
  $\mathcal{C}_{C-1}^1$ transmits $W_1^{l,C-1} = \mathcal{I}_{F_1}^{1,C-1} \oplus \mathcal{I}_{U_L}^{1,C-1}$
  $\mathcal{W}^l = \{W_1^{l,C-1}\}$
  Add $\mathcal{W}^l$ to $\mathcal{W}$
end if
return $\mathcal{W}$

根据 C^l 是否属于特殊情况，算法1会分支进入两个传输子程序之一：一般情况（算法 2）或特殊情况（算法 3）。这两个子程序都会从 $\mathcal{C}^l$ 该层的一部分客户端中生成一组 C^l 编码传输 $\mathcal{W}^l$。这些传输经过精心设计，是由客户端旁信息集中的消息构成的异或组合，并利用初始重叠段、末端重叠段和独有非重叠消息。生成层 l 的传输并将其添加到整体方案 $\mathcal{W}$后，算法便为下一递归层级做准备。需要注意的是，在每个递归层级开始时，对于该层所考虑的客户端，其旁

算法 2一般情形传输方案

要求： C^l 个客户端，$\mathcal{C}^l = \{\mathcal{C}_i^l, i \in [C^l]\}$，第一个客户端侧信息集合的基数为 在 $\mathcal{C}^l$ as K^l中，参数 $r_{\max}^l$ 使得 $C^l \neq \frac{(r^l\text{最大值}-2)(r^l\text{最大值}-1)}{2}+1$

确保： 层 l的传输方案 $\mathcal{W}^l$

$\mathcal{W}^l = \emptyset$

第1阶段：中间客户端 ($\mathcal{C}_2^l$ **至** $\mathcal{C}_{r^l_{\max}-2}^l$)

对于 $i = 1$ **至** $r^l_{\max} - 3$ **执行**

$\mathcal{C}_{i+1}^l$ 发送 $W^l_{1,\,j+1} = \mathcal{I}^l_{F_1} \oplus \mathcal{I}^l_{L_1}$

对于 $j = 1$ **至** $i-1$ **执行**

$\mathcal{C}_{i+1}^l$ 发送 $W^l_{j+1,\,j+1} = \mathcal{I}^l_{F_1} \oplus \mathcal{I}^l_{U_j}$

结束循环

结束循环

令 $T^l = \frac{(r^l_{\max}-2)(r^l_{\max}-3)}{2}$

阶段 2：客户端 $\mathcal{C}^l_{r^l_{\max}-1}$

传输 $W^l_{1,\,r^l\text{最大值}-1} = \mathcal{I}^l_{F_1} \oplus \mathcal{I}^l_{L_1}$

对于 $j = 1$ **到** $(C^l - r^l_{\max} - T^l)$ **执行**

$\mathcal{C}^l_{r^l_{\max}-1}$ 传输 $W^l_{j+1,\,r^l\text{最大值}-1} = \mathcal{I}^l_{F_1} \oplus \mathcal{I}^l_{U_j}$

结束 for

对于 $j = (C^l - r^l_{\max} - T^l + 1)$ **到** $r^l_{\max} - 3$ **执行**

$q = j - (C^l - r^l_{\max} - T^l)$

$\mathcal{C}^l_{r^l_{\max}-1}$ 传输 $W^l_{j+1,\,r^l\text{最大}} = \mathcal{I}^l_{L_1} \oplus \mathcal{I}^l_{L_{q+1}}$

结束 for

第3阶段：客户端 $\mathcal{C}^l_{r^l_{\max}}$

对于 $j = 1$ **到** $(C^l - r^l_{\max} - T^l + 2)$ **执行**

$\mathcal{C}^l_{r^l_{\max}}$ 传输 $W^l_{j,\,r^l\text{最大值}} = \mathcal{I}^l_{F_1} \oplus \mathcal{I}^l_{U_j}$

结束循环

$\mathcal{W}^l \leftarrow$此层的所有传输均已完成 l

返回 $\mathcal{W}^l$

算法 3 特殊情况传输方案

要求： C^l 个客户端，$\mathcal{C}^l = \{\mathcal{C}_i^l, i \in [C^l]\}$，边信息集合基数，其中第一个客户端在 $\mathcal{C}^l$ 中的边信息集合为 K^l，参数 $r_{\max}^l$ 使得 $C^l = \frac{(r^l\text{最大值}-2)(r^l\text{最大值}-1)}{2}+1$

确保： 层 l 的传输方案 $\mathcal{W}^l$

初始化：$\mathcal{W}^l = \emptyset$

第1阶段：中间客户端 ($\mathcal{C}_2^l$ **至** $\mathcal{C}_{r^l_{\max}-2}^l$)

$\mathcal{C}_2^l$ 传输 $W^l_{1,\,2} = \mathcal{I}^l_{F_1} \oplus \mathcal{I}^l_{F_2} \oplus \mathcal{I}^l_{L_1}$

对于 $i = 1$ **至** $r^l_{\max} - 4$，**执行**

$\mathcal{C}^l_{i+2}$ 传输 $W^l_{1,i+2} = \mathcal{I}^l_{F_1} \oplus \mathcal{I}^l_{L_1}$

对于 $j = 1$ **到** $i-1$，**执行**

$\mathcal{C}^l_{i+2}$ 发送 $W^l_{j+1,\,i+2} = \mathcal{I}^l_{F_1} \oplus \mathcal{I}^l_{U_j}$

结束循环

结束循环

$T^l = \frac{(r^l\text{最大值}-3)(r^l\text{最大值}-4)}{2}+1$

阶段 2：客户端 $\mathcal{C}^l_{r^l_{\max}-1}$

传输 $W^l_{1,\,r^l_{\max}-1} = \mathcal{I}^l_{F_1} \oplus \mathcal{I}^l_{L_1}$

$\mathcal{C}^l_{r^l_{\max}-1}$

对于 $j = 1$ **到** $r^l_{\max} - 4$ **执行**

传输 $W^l_{j+1,\,r^l\text{最大}-1} = \mathcal{I}^l_{L_1} \oplus \mathcal{I}^l_{U_j}$

结束循环

第3阶段：客户端 $\mathcal{C}^l_{r^l_{\max}}$

对于 $j = 1$ **到** $(C^l - r^l_{\max} - T^l + 3)$ **执行** $\mathcal{C}^l$

传输 $W^l_{j,\,r^l\text{最大}} = \mathcal{I}^l_{F_1} \oplus \mathcal{I}^l_{U_j}$

结束循环

$\mathcal{W}^l \leftarrow$此层的所有传输均已完成 l

返回 $\mathcal{W}^l$

□

信息集中的 LPS-FO 结构会得到保留，从而确保递归分解的一致性。

完成第 l层后，客户端$\mathcal{C}_1^l$ 至 $\mathcal{C}_{r^l_{\max}}^l$ 已达到目标知识水平 T，而其余客户端 $\mathcal{C}_{r^l_{\max}+1}^l$ 至 $\mathcal{C}_{C^l}^l$ 仍保持原有知识水平，未从该层的传输中解码出任何消息。这些剩余客户端会重新编入索引，形成 $\mathcal{C}^{l+1} = \{\mathcal{C}_i^{l+1} = \mathcal{C}^l_{r^l_{\max}+i} \mid i \in [1, C^l - r^l_{\max}]\}$，以供下一递归层级 $l+1$使用。实质上，在每一层 l，只有前 $r^l_{\max}$ 个客户端参与解码；传输仅为满足这些客户端的需求而设计，并会在算法继续执行前完全满足其需求。该过程递归重复，直至剩余客户端数量为 $C^l \leq 2$，此时应用基例传输方案。对于两个客户端，三次特定的异或传输可确保双方都能解码所需的剩余消息数量；对于单个客户端，则只需由指定的原始客户端进行一次传输即可。最后，算法返回从所有递归层级累积得到的完整集合 $\mathcal{W}$，确保所有客户端都能利用其侧信息和接收到的编码分组，解码出所需数量的消息。

备注1。 在没有安全约束的情况下，传输次数的下界由客户端数量 C 给出，如定理*1*所示。在安全约束下，我们在定理*2*中提出的方案所需的传输次数比下界多 $N(C - r_{\max})$。这一差距体现了实施安全性所需的代价。

备注2。 从算法*1*可以看出，如果 $C \in \{3, 4\}$，那么 $r_{\max} = C$。因此，递归在单层后终止，所需的传输总次数为 C，这与定理*1*中的下界相符。因此，对于这些情况，所提出的方案是最优的。

现在，我们通过一个例子来说明定理2。

例2。 本例中，我们说明一种传输方案，其中 $M = 75$、$K = 7$ 和 $P = 3$ （这在例*1*中已有讨论）。这里，客户端数量为$C = 9$，$\mathcal{C} = \{\mathcal{C}_i : \ i \in [9]\}$ 是现有客户端的集合。目标是在传输结束时，每个客户端恰好拥有 $T = K + C = 16$ 条消息。客户端的侧信息集见表*I*，每次传输后各客户端解码的消息见表*III*。传输方案如下。

首先计算 $r^l_{\max}$ 层 $l = 1$ 。这里，$l = 1, C^1 =$

表III 例1的解码过程

客户端	$x_5 \oplus x_{10}$	$x_{10} \oplus x_{16}$	$x_{10} \oplus x_{13}$	$x_{16} \oplus x_{23}$	$x_{16} \oplus x_{19}$	$x_{23} \oplus x_{24}$	$x_{23} \oplus x_{26}$	$x_{23} \oplus x_{27}$	$x_{23} \oplus x_{28}$	$x_{40} \oplus x_{41} \oplus x_{50}$	$x_{50} \oplus x_{61}$	$x_{61} \oplus x_{64}$	$x_{61} \oplus x_{65}$
$\mathcal{C}_1$	x_{10}	x_{16}	x_{13}	x_{23}	x_{19}	x_{24}	x_{26}	x_{27}	x_{28}	-	-	-	-
$\mathcal{C}_2$	–	x_{16}	x_{13}	x_{23}	x_{19}	x_{24}	x_{26}	x_{27}	x_{28}	-	-	-	-
$\mathcal{C}_3$	x_5	–	–	x_{23}	x_{19}	x_{24}	x_{26}	x_{27}	x_{28}	-	-	-	-
$\mathcal{C}_4$	x_5	x_{10}	x_{13}	–	–	–	x_{26}	x_{27}	x_{28}	-	-	-	-
$\mathcal{C}_5$	x_5	x_{10}	x_{13}	x_{16}	x_{19}	–	–	–	–	–	-	-	-
$\mathcal{C}_6$	–	–	–	–	–	–	–	–	–	x_{50}	x_{61}	x_{64}	x_{65}
$\mathcal{C}_7$	–	–	–	–	–	–	–	–	–	–	x_{61}	x_{64}	x_{65}
$\mathcal{C}_8$	–	–	–	–	–	–	–	–	–	–	–	x_{64}	x_{65}
$\mathcal{C}_9$	–	–	–	–	–	–	–	–	–	–	x_{50}	–	–

$9, K^1 = 7$和 $P = 3$。我们设定 $\mathcal{C}^1 = \{\mathcal{C}_i, i \in [9]\}$。根据**算法1**的**步骤 1**，$r^1_{\max} = 5$。因此，将在此层考虑前五个客户端。这里 C^1 $_2$ $= 9$ 和 $(r^1$ 最大值$-2)$ $(r^1$ 最大值$-1)$ $1 = 7$ $C^1 \neq$ r^1 -2 r^1 -1 $+1$ 5，所以 (最大值)(最大值) 。因此，~~按照~~**算法1**~~的~~相应行，执行**算法 2**。

第*1*阶段：在此阶段，客户端 $\mathcal{C}_2$ 和 $\mathcal{C}_3$ 进行传输。首先，$\mathcal{C}_2$ 发送编码消息 W^1,$_1$ $^2 = x_5 \oplus x_{10}$，其中包含其与 $\mathcal{C}_1$ 重叠部分中的第一条消息，以及其与 $\mathcal{C}_3$重叠部分中的第一条消息。这使得 $\mathcal{C}_1$ 能够解码 x_{10}（因为 $\mathcal{C}_1$ 已经解码了 x_{10}），并使 $\mathcal{C}_3$ 能够解码 x_5。接着，$\mathcal{C}_3$ 传输 W^1,$_1$ $^3 = x_{10} \oplus x_{16}$，将其与 $\mathcal{C}_2$ 重叠部分中的第一条消息和与 $\mathcal{C}_4$重叠部分中的第一条消息组合起来。由此，$\mathcal{C}_1$和 $\mathcal{C}_2$解码 x_{16}，而 $\mathcal{C}_4$解码 x_{10}；获得 x_{10}后，$\mathcal{C}_4$现在也可以从 W^1解码 x_5，*2 1*。最后，$\mathcal{C}_3$发送 W^1,$_2$ $^3 = x_{10} \oplus x_{13}$，该消息由其与 $\mathcal{C}_2$ 重叠部分中的第一条消息和其第一条独有消息构成，使得 $\mathcal{C}_1$、 $\mathcal{C}_2$和 $\mathcal{C}_4$ 各自都能解码 x_{13}。根据算法 *2*第*9*行，此阶段的传输总数为 $T^1 = 3$。

阶段 *2*：此处，客户端 $\mathcal{C}_4$ 进行传输。它首先发送 W^1,$_1$ $^4 = x_{16} \oplus x_{23}$，其中编码了它与 $\mathcal{C}_3$ 重叠部分中的第一条消息，以及它与 $\mathcal{C}_5$重叠部分中的第一条消息。这使$\mathcal{C}_1$、 $\mathcal{C}_2$和 $\mathcal{C}_3$ 能够解码 x_{23}，而 $\mathcal{C}_5$ 则解码 x_{16}。现在已知x_{16} ， $\mathcal{C}_5$ 便可从先前的传输 W^1,*3 1* 、 W^1,*2 1* 和 W^1,*3 2* 中依次解码 x_{10}、 x_5和 x_{13}。接下来，$\mathcal{C}_4$发送 W^1,$_2$ $^4 = x_{16} \oplus x_{19}$，将其重叠消息与 $\mathcal{C}_3$ 以及其第一条独有消息组合起来，使得 $\mathcal{C}_1$、 $\mathcal{C}_2$、 $\mathcal{C}_3$和 $\mathcal{C}_5$都能解码 x_{19}。此时，客户端 $\mathcal{C}_5$ 已达到其目标层级，因为 $\mathcal{C}_5$的旁信息集已包含 *11* 条消息，而它只需再获得 *5* 条即可达到目标，因此不应再接收更多消息。因此， $\mathcal{C}_4$ 传输 W^1,$_3$ $^4 = x_{23} \oplus x_{24}$，由其与 $\mathcal{C}_5$重叠部分中的第一条和第二条消息构成。这次传输没有为 $\mathcal{C}_5$提供任何新消息，但使 $\mathcal{C}_1$、 $\mathcal{C}_2$和 $\mathcal{C}_3$ 能够解码 x_{24}。经过此阶段后，前四个客户端各自还恰好需要三条新消息才能达到其目标层级。

第*3*阶段： 在最后一个阶段，客户端 $\mathcal{C}_5$ 进行传输。它发送 $W^{1,}{}_1$ $^5 = x_{23} \oplus x_{26}$，对其与 $\mathcal{C}_4$ 重叠部分中的第一条消息和第一条独有消息进行编码； $\mathcal{C}_1$、 $\mathcal{C}_2$、 $\mathcal{C}_3$和 $\mathcal{C}_4$ 均可从中解码出 x_{26}。接下来， $\mathcal{C}_5$ 传输 $W^{1,}{}_2$ $^5 = x_{23} \oplus x_{27}$，其构成方式相同，由同一条重叠消息和第二条独有消息组成，使相同的四个客户端能够解码出 x_{27}。最后， $\mathcal{C}_5$ 发送 $W^{1,}{}_3$ $^5 = x_{23} \oplus x_{28}$，将重叠消息与第三条独有消息结合，从而向$\mathcal{C}_1$、 $\mathcal{C}_2$、 $\mathcal{C}_3$和 $\mathcal{C}_4$提供 x_{28} 。

通过这些传输，前五个客户端都已达到其目标消息数量。接下来，我们进入下一个递归层级。在此， $l = 2$, $C^2 = 4, K^2 = 12$和 $\mathcal{C}^2 = \{\mathcal{C}_i, i \in [6, 9]\}$。根据**算法1的步骤 1**，**算法1**，$r^2_{\max} = 4$。因此，本层将考虑最后四个客户端。这里 $C^2 = 4$ 和$(r^2$ max$-2)(r^2$ max$-1)$ $_2$ $+ 1 = 4$，所以 $C^2 = \overline{(r^1 \text{ max}-2)(r^1 \text{ max}-1)}$ $_2$ $+ 1$。因此，将执行**算法 3** 。

第*1*阶段： 在此阶段，客户端 $\mathcal{C}_7$ 传输一条编码消息，该消息由其与$\mathcal{C}_6$ 重叠部分中的第一条和第二条消息，以及其与 $\mathcal{C}_8$重叠部分中的第一条消息组成，具体为$W^{2,}{}_1$ $^2 = x_{40} \oplus x_{41} \oplus x_{50}$。这种构造确保只有$\mathcal{C}_6$ 能够从此次传输中解码出一条新消息（x_{50}）。

阶段 *2*：在此，客户端 $\mathcal{C}_8$ 传输编码消息$W^{2,}$ $_1$ $^3 = x_{50} \oplus x_{61}$，该消息由其与 $\mathcal{C}_7$ 重叠中的第一条消息及其与 $\mathcal{C}_9$重叠中的第一条消息构成。这使得$\mathcal{C}_6$ 和 $\mathcal{C}_7$ 能够解码 x_{61}，而 $\mathcal{C}_9$ 解码 x_{50}。此次传输之后，客户端 $\mathcal{C}_9$ 已达到其目标，其余客户端$\mathcal{C}_6$、 $\mathcal{C}_7$和 $\mathcal{C}_8$ 各自仍需两条新消息。

第*3*阶段：在最后阶段，客户端 $\mathcal{C}_9$进行两次传输。首先，它传输 $W^{2,}{}_1$ $^4 = x_{61} \oplus x_{64}$，将其与 $\mathcal{C}_8$ 重叠中的第一条消息与其第一条独有消息相结合，使 $\mathcal{C}_6$、 $\mathcal{C}_7$和 $\mathcal{C}_8$ 能够解码 x_{64}。其次，它传输$W^{2,}{}_2$ $^4 = x_{61} \oplus x_{65}$，同样由同一重叠消息及其第二条独有消息构成，从而向同样的三个客户端提供 x_{65} 。

通过这些传输，所有客户端的消息数量均已达到各自的目标数量。

IV. 算法1的正确性证明

本节证明算法1这一主要递归算法的正确性。该算法在多个迭代层级上运行。在每一层 l，算法都会考虑一个大小为 C^l 的客户端集合 $\mathcal{C}^l$ ，其中第一个客户端 $\mathcal{C}^l_1$ 的旁信息集基数为 K^l。在每一层，算法都会利用不等式 (3) 确定参数 $r^l_{\max}$ 。此参数指定当前集合中有多少客户端可以在该层得到完全服务。

根据当前客户端数量 C^l，算法 1 会选择适当的传输方案：一般情况下使用算法 2，满足特定等式条件时使用算法 3。这些方案经过设计，使得层 l 处的传输仅满足 $\mathcal{C}^l$ 中前 $r^l_{\max}$ 个客户端的需求，而使 $\mathcal{C}^l$ 中其余客户端完全不受影响。引理1和引理2分别在第五节和第六节中得到证明，从而对这一性质提供了形式化保证。

此外，引理 3 确保当前递归集合 $\mathcal{C}^l$ 之外的客户端无法解码在层 l 传输的任何消息。这种包含关系对于递归结构至关重要。

引理 1。 在每个 l层，如果 $C^l \neq (r^l \text{ 最大值}-2)(r^l \text{ 最大值}-1)$ $+1$，则算法 *2* 提供 C^l 次传输，使 $\mathcal{C}^l$ 中的前 $r^l_{\max}$ 个客户端（每个客户端 $\mathcal{C}^l_i$ 具有 $i \le r^l_{\max}$）达到目标大小 $T = K + C$。除了这前 $r^l_{\max}$ 个客户端之外， $\mathcal{C}^l$ 中的其他客户端均无法解码在 l层期间传输的任何消息。

引理 2。 在每个 l层，如果 $C^l = (r^l \text{ 最大值}-2)(r^l \text{ 最大值}-1)$ $+1$，则算法 *3* 提供 C^l 次传输，使 $\mathcal{C}^l$ 中的前 $r^l_{\max}$ 个客户端（每个客户端 $\mathcal{C}^l_i$ 具有 $i \le r^l_{\max}$）达到目标大小 $T = K + C$。除了这前 $r^l_{\max}$ 个客户端之外， $\mathcal{C}^l$ 中的其他客户端均无法解码在 l层期间传输的任何消息。

引理 3。 在每个 l层， $\mathcal{C}\backslash\mathcal{C}^l$ 中的任何客户端都无法解码在该层期间传输的任何消息。

在任意递归层级 l，计算 $r^l_{\max}$ 并执行选定的传输方案（算法 2 或 3）后，前$r^l_{\max}$ 个客户端达到目标知识水平 $T = K + C$。根据上述引理， $\mathcal{C}^l$ 中的其他客户端不会从这些传输中获得任何信息。因此，这些已满足的客户端将从后续步骤中移除。剩余的 $C^l - r^l_{\max}$ 个客户端保留其原始侧信息集，并重新编号以形成下一层的客户端集合：

$$\mathcal{C}^{l+1} = \{\mathcal{C}^{l+1}_i = \mathcal{C}^l_{r^l_{\max}+i} : i \in [1, C^l - r^l_{\max}]\}.$$

参数更新为 $C^{l+1} = C^l - r^l_{\max}$和 $K^{l+1} = K^l + r^l_{\max}$。

在任意层 l，传输的构造方式使得，对于 C_l之外的任意客户端，两个消息中没有任何一个传输可用作其侧信息。因此，这些客户端都无法解码任何传输。

引理 4. 在每个递归层级 l 开始时，旁信息集对于 $\mathcal{C}^l = \{\mathcal{C}^l_1, \mathcal{C}^l_2, \ldots, \mathcal{C}^l_{C^l}\}$ 中的 C^l 个客户端保持 *LPS-FO* 结构，其中第一个客户端 $\mathcal{C}^l_1$ 的旁信息集基数为 K^l。

引理 4 的证明见第七节。此递归过程持续进行，直到剩余客户端数量减少至基本情形 $C^l = 2$ 或 $C^l = 1$，这些情形在算法1中进行了明确处理。

引理 5. 对于算法*1*中的基本情形， $N(2) = 3$（剩余两个客户端时需要三次传输），而 $N(1) = 1$ （剩余一个客户端时需要一次传输）。

引理 5 的证明见第八节。因此，算法1生成一个完整传输方案 $\mathcal{W}$，使系统中的每个客户端都达到目标知识水平 $T = K + C$。

为计算传输总数 $N(C)$，注意在第 1 层有 C 次传输，满足前 $r_{\max}$ 个客户端的需求，其中 $r_{\max}$ 根据算法1由式 (1) 确定（这等价于式 (3)）。其余 $C - r_{\max}$ 个客户端进入第 2 层，此时对包含 $C - r_{\max}$ 个客户端的问题重新处理。由此得到递推关系：

$$N(C) = C + N(C - r_{\max}).$$

递归持续进行，直到 $C^l \le 2$，其中基本情况要求 $N(2) = 3$、 $N(1) = 1$以及 $N(0) = 0$ 次传输。由于对所有 $C^l > 2$， $r^l_{\max} \ge 2$ ，序列 $C^{l+1} = C^l - r^l_{\max}$ 严格递减，因此可保证算法在有限步内终止。终止后，每个客户端恰好拥有 T 条消息，且没有客户端超过这一目标，从而满足 LPS-FO 模型下 DPIC 问题的完整性和安全要求。

至此，算法1的正确性证明完毕。

V. 算法 2 的正确性证明

本节将全面证明算法 2 的正确性，该算法处理我们递归传输方案中的一般情况。证明按照算法的三个阶段展开，说明所有阶段完成后，每个具有 $i \le r^l_{\max}$ 的客户端 $\mathcal{C}^l_i \in \mathcal{C}^l$ 都恰好获得 $T = K + C$ 条消息，而具有 $i > r^l_{\max}$ 的客户端不受影响，从而保留递归结构。

A. 第1阶段：中间客户端传输结构

对于每个中间客户端 $\mathcal{C}^l_i$，其中 $i \in [2, r^l_{\max} - 2]$，其传输模式恰好由 $i-1$ 条编码消息组成。首次传输形式为 $W^{l,}_{1, F_1^{i+1}} = \mathcal{I}^{l,}_{F_1^{i+1}} \oplus \mathcal{I}^{l,}_{L_1^{i+1}}$，它将一条来自客户端旁信息集的初始重叠段（前 P 条消息）的消息，与一条来自末端重叠段（最后 P 条消息）的消息组合起来。其余 $i-2$次传输构造为 $W^{l,}_{j+1, U_j^{i+1}} = \mathcal{I}^{l,}_{F_1^{i+1}} \oplus \mathcal{I}^{l,}_{U_j^{i+1}}$，$j \in [1, i-2]$，其中每个异或都涉及同一条初始重叠消息 $\mathcal{I}^{l,}_{F_1^{i+1}}$ 以及客户端旁信息集中的一条不同的独有（非重叠）消息 $\mathcal{I}^{l,}_{U_j^{i+1}}$。这些传输的有效性基于假设 $K \ge 2P$，该假设保证每个客户端 $\mathcal{C}^l_i$ 至少拥有 $i-1$ 条独有消息。该条件可由 LPS-FO 结构推出。因此，所有必需的异或组合都有明确的定义，且可由发送客户端生成。

该传输模式支持一种双重解码机制：每个客户端都能从后续客户端的每次传输以及先前客户端的每次传输中，恰好解码出一条新消息。

考虑客户端 $\mathcal{C}^l_i$ 拥有 $1 \le i \le r^l_{\max} - 3$的情况。要从后续客户端解码时，流程从客户端 $\mathcal{C}^l_{i+1}$开始，客户端 $\mathcal{C}^l_i$可以根据其传输解码消息。由于客户端 $\mathcal{C}^l_i$通过与 $\mathcal{C}^l_{i+1}$重叠（$\mathcal{I}^{l,}_{F_1^{i+1}} = \mathcal{I}^{l,}_{i}$，根据定义1）得知 $\mathcal{I}^{l,}_{F_1^{i+1}}$，因此可以从传输 $W^{l,}_{1, F_1^{i+1}} = \mathcal{I}^{l,}_{L_1^{i+1}} \oplus \mathcal{I}^{l,}_{L_1^{i+1}}$中解码出 $\mathcal{I}^{l,}_{L_1^{i+1}}$。此外，根据形式为 $W^{l,}_{j+1, U_j^{i+1}} = \mathcal{I}^{l,}_{F_1^{i+1}} \oplus \mathcal{I}^{l,}_{U_j^{i+1}}$的传输，它可以解码每个 $\mathcal{I}^{l,}_{U_j^{i+1}}$

对于 $j \in [1, i-2]$。此时会形成一条前向解码链：根据 LPS-FO 结构，$\mathcal{I}^{l,\,i+2}_{F_1} = \mathcal{I}^{l,\,i+1}_{L_1}$，而客户端 $\mathcal{C}^l_i$ 现在已拥有这些内容。这使客户端 $\mathcal{C}^l_i$ 能够根据客户端 $\mathcal{C}^l_{i+2}$ 的传输进行解码，获得 $\mathcal{I}^{l,\,i+2}_{L_1}$ 和 $\mathcal{I}^{l,\,i+2}_{U_j}$。这一过程会递归地对所有满足 $i < k \le r^l_{\max} - 2$ 的客户端 k 继续进行，使客户端 $\mathcal{C}^l_i$ 能够从后续客户端累积集合 $\{\mathcal{I}^{l,k}_{L_1} \mid k \in [i+2, r^l_{\max}-2]\} \cup \{\mathcal{I}^{l,k}_{U_j} \mid k \in [i+1, r^l_{\max}-2], j \in [1, k-2]\}$。

与此同时，对于 $i \in [3, r_{\max}-1]$，$\mathcal{C}^l_i$ 从前序客户端进行反向解码。客户端 $\mathcal{C}^l_i$ 知道 $\mathcal{I}^{l,\,i-1}_{L_1}$（它与自身的旁信息集重叠，即 $\mathcal{I}^{l,\,i-1}_{F_1} = \mathcal{I}^{l,\,i-1}_{L_1}$）。通过客户端 $\mathcal{C}^l_{i-1}$ 的传输 $W^{l,\,i-1} = \mathcal{I}^{l,\,i-1}_{F_1} \oplus \mathcal{I}^{l,\,i-1}_{L_1}$，它接收到 $\mathcal{I}^{l,\,i-1}_{F_1}$，从而能够进一步从针对 $j \in [i-3]$ 的传输 $W^{l,\,i-1}_{j+1} = \mathcal{I}^{l,\,i-1}_{F_1} \oplus \mathcal{I}^{l,\,i-1}_{U_j}$ 中解码出 $\mathcal{I}^{l,\,i-1}_{U_j}$。后向解码链继续进行，因为 $\mathcal{I}^{l,\,i-1}_{L_1} = \mathcal{I}^{l,\,i-2}_{L_1}$，使得 $\mathcal{C}^l_i$ 能够从 $\mathcal{C}^l_{i-2}$ 解码，获得 $\mathcal{I}^{l,\,i-2}_{F_1}$，随后获得 $\mathcal{I}^{l,\,i-2}_{U_j}$。这种迭代式反向解码扩展至所有满足 $2 \le k < i$ 的客户端 k，为 $\mathcal{C}^l_i$ 提供集合 $\{\mathcal{I}^{l,k}_{F_1} \mid k \in [2, i-1]\} \cup \{\mathcal{I}^{l,k}_{U_j} \mid k \in [2, i-1], j \in [1, k-2]\}$。

每个中间客户端 $\mathcal{C}^l_i$（对于 $i \in [2, r^l_{\max}-2]$）在第1阶段恰好传输 $i-1$ 条消息，因此该阶段的传输总数为 $T^l = \sum_{i=2}^{r^l_{\max}-2}(i-1) = \frac{(r^l_{\max}-2)(r^l_{\max}-3)}{2}$ 条。令 T^l_i 表示客户端 $\mathcal{C}^l_i$（其中 $i \in [1, r^l_{\max}-1]$）从第1阶段传输中解码出的新消息数量。由于每次传输恰好包含一条相应客户端可以恢复的未知消息，因此，每个客户端都能从其能够解码的每次传输中获得一条新消息。对于具有 $i \in [2, r^l_{\max}-2]$ 的传输客户端 $\mathcal{C}^l_i$ 而言，其进行的 $i-1$ 次传输无法由自身解码；因此，它可以从剩余的 $T^l - (i-1)$ 次传输中解码。因此，对于 $i \in [2, r^l_{\max}-2]$，$T^l_i = T^l - (i-1)$。该阶段中未进行传输的两个客户端 $\mathcal{C}^l_1$ 和 $\mathcal{C}^l_{r^l_{\max}-1}$ 分别完整参与正向解码链和后向解码链，因此，每个客户端都能从每次第1阶段传输中恰好解码出一条新消息。于是，$T^l_1 = T^l_{r^l_{\max}-1} = T^l$。第1阶段结束后，每个具有 $i \in [1, r^l_{\max}-1]$ 的客户端 $\mathcal{C}^l_i$ 在其初始旁信息集之外又获得了 T^l_i 条额外消息。

B. 阶段 2：客户端 $\mathcal{C}^l_{r^l_{\max}-1}$ 传输策略

阶段 2 仅包含来自客户端 $\mathcal{C}^l_{r^l_{\max}-1}$ 的传输，该客户端恰好传输 $r^l_{\max}-2$ 条编码消息。这些传输分为两类互补类别，分别服务于不同的客户端组。

第一类包含 $C^l - r^l_{\max} - T^l + 1$ 传输，包括 $W^{l,r^l\max}_1 = \mathcal{I}^{l,r^l\max}_{F_1} \oplus \mathcal{I}^{l,r^l\max}_{L_1}$ 和 $W^{l,r^l\max}_{j+1} = \mathcal{I}^{l,r^l\max}_{F_1} \oplus \mathcal{I}^{l,r^l\max}_{U_j}$，其中 $j \in [1, C^l - r^l_{\max} - T^l]$。我们首先验证这些传输的有效性。由于根据不等式 (3)，有 $C^l > \frac{(r^l\max-2)(r^l\max-1)}{2}$，而 $T^l = \frac{(r^l\max-2)(r^l\max-3)}{2}$，因此量 $C^l - r^l_{\max} - T^l$ 非负。直接比较可得 $C^l - T^l > r^l_{\max} - 2$，这意味着 $C^l - r^l_{\max} - T^l > 0$。根据不等式 (3)，有 $C^l \le \frac{(r^l\max-1)r^l\max}{2}$。将其与 $T^l = \frac{(r^l\max-3)(r^l\max-2)}{2}$ 结合可得

$$\begin{aligned} C^l - T^l &\le \frac{(r^l_{\max}-1)r^l_{\max}}{2} - \frac{(r^l_{\max}-2)(r^l_{\max}-3)}{2} \\ &\le 2r^l_{\max} - 3. \end{aligned} \tag{4}$$

因此，

$$C^l - r^l_{\max} - T^l \le (2r^l_{\max}-3) - r^l_{\max} = r^l_{\max} - 3. \tag{5}$$

因此，所需的独有消息数量 $C^l - r^l_{\max} - T^l$ 至多为 $r^l_{\max}-3$，严格小于 $r^l_{\max}-2$。

在假设 $K \ge 2P$ 下，可以保证每个客户端 $\mathcal{C}^l_i$ 的旁信息集中至少有 $i-1$ 条独有（不重叠）消息。因此，客户端 $\mathcal{C}^l_{r^l_{\max}-1}$ 至少拥有 $r^l_{\max}-2$ 条独有消息。传输 $W^{l,\,r^l\text{最大}-1}_{j+1}$ 恰好需要 $C^l - r^l_{\max} - T^l$ 条不同的独有消息。由于 $C^l - r^l_{\max} - T^l < r^l_{\max} - 2$ 成立（由式（5）可知），所需的独有消息数量不超过可用数量。因此，本阶段规定的所有异或组合均定义良好，且可由发送客户端生成。

这些传输有助于继续集合 $\{\mathcal{C}^l_i, i \in [r^l_{\max}-2]\}$ 中客户端的前向解码链，并为客户端 $\mathcal{C}^l_{r^l_{\max}}$ 引入后向解码链。对于任何满足 $i < r^l_{\max}-1$ 的客户端 $\mathcal{C}^l_i$，已知 $\mathcal{I}^{l,r^l\max-1}_{F_1}$（因 $\mathcal{I}^{l,r^l\max-1}_{F_1} = \mathcal{I}^{l,r^l\max-2}_{L_1}$，可从第1阶段获得）即可从 $W^{l,r^l\max-1}_1$ 解码出 $\mathcal{I}^{l,r^l\max-1}_{L_1}$，并从 $W^{l,r^l\max-1}_{j+1}$ 解码出 $\mathcal{I}^{l,r^l\max-1}_{U_j}$，适用于 $j \in [1, C^l - r^l_{\max} - T^l]$。客户端 $\mathcal{C}^l_{r^l_{\max}}$ 可以从 $W^{l,r^l\max-1}_1$ 解码出 $\mathcal{I}^{l,r^l\max-1}_{F_1}$，因为它已获得 $\mathcal{I}^{l,r^l\max-1}_{L_1} = \mathcal{I}^{l,r^l\max}_{F_1}$。因此，对于 $j \in [1, C^l - r^l_{\max} - T^l]$，它还可以从 $W^{l,r^l\max-1}_{j+1}$ 解码出 $\mathcal{I}^{l,r^l\max-1}_{U_j}$，因为它知道 $\mathcal{I}^{l,r^l\max-1}_{F_1}$。

第二类由 $r^l_{\max}-3-(C^l-r^l_{\max}-T^l)$ 传输构成，针对形式为 $W^{l,\,r^l\max-1}_{j+1} = \mathcal{I}^{l,\,r^l\max-1}_{L_1} \oplus \mathcal{I}^{l,\,r^l\max-1}_{L_{q+1}}$，$q = j - (C^l - r^l_{\max} - T^l)$，$P \ge r_{\max}-2$ 的情况，其中 $(\cdot)$。根据假设，我们有 $r^l_{\max} \le r_{\max}$，其中 q 定义为满足以下条件的整数

$$\frac{(r_{\max}-2)(r_{\max}-1)}{2} < C \le \frac{r_{\max}(r_{\max}-1)}{2}.$$

由于 $C^l < C$，因此 $r^l_{\max} \le r_{\max}$。因此，$P \ge r^l_{\max}-2$ 保证每个客户端的末端重叠段至少包含 $r^l_{\max}-2$ 条消息。这确保形式为 $\mathcal{I}^{l,\,r^l\max-1}_{L_j}$（对于 $j \le r^l_{\max}-2$）的所有所需消息都存在于重叠区域内，从而验证了传输方案中相应异或组合的可行性。

这些传输仅扩展客户端 $i < r^l_{\max}-1$ 的前向解码链。解码 $\mathcal{I}^{l,\,r^l\max-1}_{L_1}$（来自 $W^{l,\,r^l\max-1}_1$）后，这些客户端还可以进一步解码 $\mathcal{I}^{l,\,r^l\max-1}_{L_{q+1}}$。对于客户端 $\mathcal{C}^l_{r^l_{\max}}$，$\mathcal{I}^{l,\,r^l\max-1}_{L_1}$ 和 $\mathcal{I}^{l,\,r^l\max-1}_{L_{q+1}}$ 都已存在于其旁信息集内（因为根据 $\mathcal{I}^{l,\,r^l\max-1}_{F_j} = \mathcal{I}^{l,\,r^l\max-1}_{L_j}$

LPS-FO 结构），因此这些传输不会为其带来新的消息。

令 $T^{l,2}_{i}$ 表示客户端$\mathcal{C}^l_i$ 完成本层**阶段 2** 后为 $i \in [1, r_{\max}]$ 解码的消息数。**阶段 2**结束后，满足 $i < r^l_{\max} - 1$的中间客户端 $\mathcal{C}^l_i$ 额外解码了 $r^l_{\max} - 3$ 条消息，使其解码消息总数达到 $T^{l,2}_{i} = T^{l,1}_{i} + (r^l_{\max} - 3)$。客户端$\mathcal{C}^l_{r^l_{\max}-1}$作为发送端，不会通过自身的传输获得新消息，因此解码消息总数仍为 $T^{l,2}_{r^l_{\max}-1} = T^{l,1}_{r^l_{\max}-1}$。

客户端 $\mathcal{C}^l_{r^l_{\max}}$ 从**阶段 2** （具体而言，来自类别1）解码了 $C^l - r^l_{\max} - T^l + 1$条新消息。现在，由于它已解码消息 $\mathcal{I}^{l,r^l\max}_{F_1}$，结合 $\mathcal{I}^{l,r^l\max}_{F_1} = \mathcal{I}^{l,r^l\max}_{L_1}$ 它进入反向链并解码集合 $2]\} \cup \{\mathcal{I}^{l,k}_{U_j} \mid k \in [2, r^l_{\max} - 2], j \in [1, k-2]\}$

中的所有消息。因此，累计解码消息总数为 $T^{l,2}_{r^l_{\max}} = T^l + (C^l - r^l_{\max} - T^l + 1) = C^l - r^l_{\max} + 1$。这使 $\mathcal{C}^l_{r^l_{\max}}$ 达到其目标消息数量，后文将对此进行验证（本节稍后证明）。

C. 第3阶段：客户端 $\mathcal{C}^l_{r^l_{\max}}$ 传输策略

第3阶段仅通过客户端 $\mathcal{C}^l_{r^l_{\max}}$ 的传输完成传递过程，该客户端恰好发送 $C^l - r^l_{\max} - T^l + 2$ 条消息，每条消息的形式为 $\underline{W}^{l,r^l\max}_{j} \mathcal{I}^{l,r^l\max}_{F_1} \oplus \mathcal{I}^{l,\max U_j}$，其中 $j \in [1, C^l - r^l_{\max} - T^l + 2]$。这些传输的可解码性取决于接收客户端对 $\mathcal{I}^{l,r^l\max F_1}$ 的了解。正如前文所述，$C^l - T^l > r^l_{\max} - 2$，这保证了 $C^l - r^l_{\max} - T^l + 2$ 为正。

在假设 $K \geq 2P$下，每个客户端 $\mathcal{C}^l_i$ 至少拥有 $i-1$ 条独有消息。对于 $i = r^l_{\max}$，这意味着至少有 $r^l_{\max} - 1$ 条独有消息可用。不等式$C^l - r^l_{\max} - T^l + 2 \leq r^l_{\max} - 1$ 由式 (5) 得出（因为$C^l - r^l_{\max} - T^l \leq r^l_{\max} - 3$意味着 $C^l - r^l_{\max} - T^l + 2 \leq r^l_{\max} - 1$）。因此，传输所需的独有消息数量不会超过 $\mathcal{C}^l_{r^l_{\max}}$处可用的数量，从而确保所有异或组合都有定义且有效。

设完成该层 l的第3阶段后，客户端$\mathcal{C}^l_i$ 为 $i \in [1, r^l_{\max}]$ 解码的消息数量为 $T^{l,3}_{i}$。对于具有 $i \in [2, r^l_{\max} - 2]$ 的中间客户端 $\mathcal{C}^l_i$，根据阶段 2 的内容，它已解码 $\mathcal{I}^{l,r^l\max}_{F_1}$，因为 $\mathcal{I}^{l,r^l\max}_{F_1} = \mathcal{I}^{l,r^l\max}_{L_1}$。这些客户端在阶段 2 中获得了 $\mathcal{I}^{l,r^l\max}_{L_1}$（具体来说，是来自类别1的 $W^l_{r^l\max}$），因此拥有 $\mathcal{I}^{l,r^l\max}_{F_1}$。因此，对于每次传输 $W^{l,r^l\max}_{j} = \mathcal{I}^{l,r^l\max}_{F_1} \oplus \mathcal{I}^{l,r^l\max U_j}$，它们都会解码 $\mathcal{I}^{l,r^l\max U_j}$，从而获得 $C^l - r^l_{\max} - T^l + 2$ 条新消息。因此，截至目前在该层 l中获得的消息总数为

$$T^{l,3}_{i} = T^{l,2}_{i} + C^l - r^l_{\max} - T^l + 2 = C^l - (i-1).$$

客户端 $\mathcal{C}^l_{r^l_{\max}-1}$ 自然知道 $\mathcal{I}^{l,r^l\max F_1}$，因为它等于 $\mathcal{I}^{l,r^l\max}_{L_1}$，后者属于其自身的旁信息集。因此，它可以直接从每个 $W^{l,r^l\max}_{j}$ 中解码 $\mathcal{I}^{l,r^l\max U_j}$，同时获得 $C^l - r^l_{\max} - T^l + 2$ 新消息。因此，截至目前在这一层获得的消息总数为 l

$$T^{l,3}_{r^l_{\max}-1} = T^{l,2}_{r^l_{\max}-1} + C^l - r^l_{\max} - T^l + 2 = C^l - (r^l_{\max} - 2).$$

客户端 $\mathcal{C}^l_{r^l_{\max}}$ 作为发送端，无法从**第3阶段** 传输中获得额外消息。因此，截至目前在该层 l 中获得的消息总数为

$$T^{l,3}_{r^l_{\max}} = T^{l,2}_{r^l_{\max}} = C^l - (r^l_{\max} - 1).$$

简而言之，到第3阶段结束时，每个客户端 $\mathcal{C}^l_i \in \mathcal{C}^l$ 已从本层进行的传输中解码了 $T^{l,3}_{i} = C^l - (i-1)$条消息。

由于 $T = K + C$ 根据定义，并且我们有 $K^l = K^{l-1} + r^{l-1}_{\max}$ 和 $C^l = C^{l-1} - r^{l-1}_{\max}$，因此可得 $K^l + C^l = K^{l-1} + C^{l-1}$。根据归纳法，$K^l + C^l = K + C = T$，从而确立 $T = K^l + C^l$。这证实了集合 $\mathcal{C}^l$ 中的第一个客户端为达到目标所需的额外消息数量仍然恰好为 C^l。因此，对于任意客户端 $\mathcal{C}^l_i \in \mathcal{C}^l$，在 $i \in [C^l]$的情况下，为达到目标所需的额外消息数量恰好为 $C^l - (i-1)$。我们已经证明，每个客户端 $\mathcal{C}^l_i \in \mathcal{C}^l$，对于 $i \leq r^l_{\max}$，已从本层进行的传输中解码了 $T^{l,3}_{i} = C^l - (i-1)$条消息。因此，这些客户端均通过本层进行的传输而得到满足。

客户端 $\mathcal{C}^l_i \in \mathcal{C}^l$ 和 $i > r^l_{\max}$ 在当前递归层级中没有收到任何消息。对于索引为 $i > r^l_{\max}$的客户端，出现了一项关键性质：这些客户端无法从第1阶段的传输中解码任何消息。本层级中的所有传输 W都属于以下类型：$W = \mathcal{I}^{l,k}_{F_1} \oplus \mathcal{I}^{l,k}_{L_1}$，或 $W = \mathcal{I}^{l,k}_{L_1} \oplus \mathcal{I}^{l,k}_{L_j}$（其中 $k \leq r^l_{\max} - 1$），或 $W = \mathcal{I}^{l,k}_{F_1} \oplus \mathcal{I}^{l,k}_{U_j}$，其中 $k \leq r^l_{\max}$，且 j为某个整数。客户端 $\mathcal{C}^l_i$（其中 $i > r^l_{\max}$）对这些类型的传输中的两个异或项都缺乏认知，因为它们与异或中的任何消息都没有重叠。由于各阶段的传输结构意味着任意两次传输最多只有一条共同消息，因此，接收到的传输的任何线性组合都无法将未知项的数量减少到一项。因此，客户端 $\mathcal{C}^l_i$（其中 $i > r^l_{\max}$）不受本层级传输的影响，保留其原有的消息集合，从而能够进行递归分解。

VI. 算法 3 的正确性证明

本节将全面证明算法 3 的正确性。该算法处理递归传输方案中的特殊情况。证明按照算法的三个阶段展开，说明所有阶段完成后，每个拥有 $i \leq r^l_{\max}$ 的客户端 $\mathcal{C}^l_i \in \mathcal{C}^l$ 都恰好获得 $T = K + C$ 条消息，而拥有 $i > r^l_{\max}$ 的客户端不受影响，从而保持递归结构。

A. 第1阶段：中间客户端传输结构

客户端 $\mathcal{C}^l_2$进行一次形式为$W^{l,2}_{1} = \mathcal{I}^{l,2}_{F_1} \oplus \mathcal{I}^{l,2}_{L_1} \oplus \mathcal{I}^{l,2}_{F_2}$的单次传输，该传输将初始重叠段中的前两条消息（前 P条消息）与来自末端重叠的一条消息相结合

段（客户端旁信息集中的最后 P 条消息）。进行此传输是为了确保只有第一个客户端接收到一条新消息。对于每个中间客户端 $\mathcal{C}_i^l$，其中$i \in [3, r_{\max}^l - 2]$，传输模式恰好由$i-2$ 条编码消息组成。第一次传输的形式为$W_1^{l,\,i} = \mathcal{I}_{F_1}^{l,\,i} \oplus \mathcal{I}_{L_1}^{l,\,i}$，它将来自初始重叠段的一条消息（前 P 条消息）与来自客户端旁信息集末端重叠段的一条消息（最后 P条消息）相结合。其余

$$W_{j+1}^{l\,i} = \mathcal{I}_{F_1}^{l\,i} \oplus \mathcal{I}_{U_j}^{l\,i} \quad j \in \text{次} \; i-3 \; [1, i-3]$$

传输构造为,,,,,，其中每个异或都涉及同一条初始重叠消息 $\mathcal{I}^{l,}_{F_1}{}^{i}$，并与来自客户端旁信息集的一条不同的唯一（非重叠）消息 $\mathcal{I}^{l,}_{U_j}{}^{i}$配对。这些传输的有效性基于假设 $K \geq 2P$，该假设保证每个客户端 $\mathcal{C}_i^l$ 至少拥有 $i-1$ 条唯一消息。该条件源自 LPS-FO 结构。因此，所有所需的异或组合都是良定义的，并且可以由进行传输的客户端生成。

考虑具有 $1 \leq i \leq r_{\max}^l - 3$ 的客户端 $\mathcal{C}_i^l$。对于从后续客户端进行的解码，该过程从客户端 $\mathcal{C}_{i+1}^l$开始；根据其传输，$\mathcal{C}_i^l$ 可以解码消息。考虑客户端 $\mathcal{C}_1^l$（$i=1$）。由于 $\mathcal{C}_1^l$ 通过与 $\mathcal{C}_2^l$（$\mathcal{I}^{l}_{F_1}{}^{2} = \mathcal{I}^{l}_{L_1}{}^{1}$ 和，以及根据定义1的 $\mathcal{I}^{l}_{F_2}{}^{2} = \mathcal{I}^{l}_{L_2}{}^{1}$）重叠而知道 $\mathcal{I}^{l}_{F_1}{}^{2}$、$\mathcal{I}^{l}_{F_2}{}^{2}$ 和 $\mathcal{I}^{l}_{F_1}{}^{2}$、$\mathcal{I}^{l}_{F_2}{}^{2}$、$\mathcal{I}^{l}_{L_1}{}^{2}$ 中解码出 $\mathcal{I}^{l}_{L_1}{}^{2}$。对于 $i>1$，由于 $\mathcal{C}_i^l$ 通过与 $\mathcal{C}_{i+1}^l$（根据定义1的 $\mathcal{I}^{l}_{F_1}{}^{i+1} = \mathcal{I}^{l}_{L_1}{}^{i}$）重叠而知道 $\mathcal{I}^{l}_{F_1}{}^{i+1}$，因此它可以从传输 $W^{l}_{j+1} = \mathcal{I}^{l}_{F_1}{}^{i+1} \oplus \mathcal{I}^{l}_{L_1}{}^{i+1}$ 中解码出 $\mathcal{I}^{l}_{L_1}{}^{i+1}$。此外，对于 $i>2$，对于形式为 $W^{l}_{j+1} = \mathcal{I}^{l}_{F_1}{}^{i+1} \oplus \mathcal{I}^{l}_{U_j}{}^{i+1}$ 的传输，每个具有 $3 \leq i \leq r_{\max}^l - 3$的客户端 $\mathcal{C}_i^l$，都会为 $j \in [1, i-3]$ 解码每个 $\mathcal{I}^{l}_{U_j}{}^{i+1}$。随后形成一条前向解码链：根据 LPS-FO 结构，$\mathcal{I}^{l}_{F_1}{}^{i+2} = \mathcal{I}^{l}_{L_1}{}^{i+1}$，而这些内容现由 $\mathcal{C}_i^l$ 持有。这使得 $\mathcal{C}_i^l$ 能够根据 $\mathcal{C}_{i+2}^l$的传输进行解码，从而获得 $\mathcal{I}^{l}_{L_1}{}^{i+2}$ 和 $\mathcal{I}^{l}_{U_j}{}^{i+2}$。这一过程对所有具有 $i < k \leq r_{\max}^l - 2$ 的客户端 k 递归进行，使 $\mathcal{C}_i^l$ 能够从后续客户端累积集合 $\{\mathcal{I}_{L_1}^{l,k} \mid k \in [i+1, r_{\max}^l - 2]\} \cup \{\mathcal{I}_{U_j}^{l,k} \mid k \in [i+1, r_{\max}^l - 2], j \in [1, k-3]\}$。

与此同时，$\mathcal{C}_i^l$对于 $i \in [4, r_{\max}-1]$ 从前面的客户端开始进行反向解码。客户端 $\mathcal{C}_i^l$已知 $\mathcal{I}^{l,}_{L_1}{}^{i-1}$（它与自身的旁信息集重叠，即 $\mathcal{I}^{l,}_{F_1}{}^{i} = \mathcal{I}^{l,}_{L_1}{}^{i-1}$）。通过客户端 $\mathcal{C}_{i-1}^l$的传输 $W^{l,}_{1}{}^{i-1} = \mathcal{I}^{l,}_{F_1}{}^{i-1} \oplus \mathcal{I}^{l,}_{L_1}{}^{i-1}$，它接收到 $\mathcal{I}^{l,}_{F_1}{}^{i-1}$，从而能够进一步从传输 $W^{l,}_{j+1}{}^{i-1} = \mathcal{I}^{l,}_{F_1}{}^{i-1} \oplus \mathcal{I}^{l,}_{U_j}{}^{i-1}$中解码出 $\mathcal{I}^{l,}_{U_j}{}^{i-1}$，以用于 $j \in [i-4]$。后向解码链继续进行，因为 $\mathcal{I}^{l,}_{F_1}{}^{i-1} = \mathcal{I}^{l,}_{L_1}{}^{i-2}$，这使得 $\mathcal{C}_i^l$能够从 $\mathcal{C}_{i-2}^l$中解码，获得 $\mathcal{I}^{l,}_{F_1}{}^{i-2}$，随后获得 $\mathcal{I}^{l,}_{U_j}{}^{i-2}$。这一迭代式反向解码扩展至所有满足 $3 \leq k < i$的客户端 k，为 $\mathcal{C}_i^l$提供集合 $\{\mathcal{I}_{F_1}^{l,k} \mid k \in [2, i-1]\} \cup \{\mathcal{I}_{U_j}^{l,k} \mid k \in [2, i-1], j \in [1, k-2]\}$。除了客户端 $\mathcal{C}_1^l$之外，没有人会从客户端 $\mathcal{C}_2^l$发送的传输中解码出任何内容

客户端 $\mathcal{C}_2^l$ 进行一次传输。每个中间客户端 $\mathcal{C}_i^l$（$i \in [3, r_{\max}^l - 2]$）在**第1阶段**恰好传输 $i-2$ 条编码消息，因此总计为 $T^l = 1 + \sum_{i=3}^{r^l\max_{-2}} (i-2) = 1 + (r^l\max_{-3})(r^l\max_{-4})$ 次传输用于此阶段。令 $T^{l,}_{i}{}^{1}$ 表示客户端 $\mathcal{C}_i^l$（其中 $i \in [1, r_{\max}^l - 1]$）从第1阶段的传输中解码出的新消息数量。由于每次传输都恰好包含一条相应客户端能够恢复的未知消息，因此每个客户端都能从其可以解码的每次传输中获得一条新消息。对于满足 $i \in [3, r_{\max}^l - 2]$的发送客户端 $\mathcal{C}_i^l$，它进行的 $i-2$次传输无法由自身解码，而且它也无法从客户端 $\mathcal{C}_2^l$传输的编码消息中解码，因此，它可以从其余的 $T^l - (i-2) - 1$ 次传输中解码。于是，对于 $i \in [3, r_{\max}^l - 2]$，有 $T^{l,}_{i}{}^{1} = T^l - (i-1)$。客户端 $\mathcal{C}_2^l$无法从自己的传输中解码，而该传输是一条编码消息。因此，$T^{l,}_{2}{}^{1} = T^l - 1$。在此阶段不进行传输的客户端 $\mathcal{C}_1^l$ 分别完整参与正向和后向解码链，因此，它从第1阶段的每次传输中恰好解码出一条新消息。因此，$T^{l,}_{1}{}^{1} = T^l$。不进行传输的客户端$\mathcal{C}^l_{r^l_{\max}-1}$也完整参与正向和后向解码链，但不包括客户端 $\mathcal{C}_2^l$进行的传输，因此它恰好解码出 $T^{l,}_{r^l_{\max}-1}{}^{1} = T^l - 1$ 条消息。第1阶段结束后，每个满足 $i \in [1, r_{\max}^l - 1]$ 的客户端 $\mathcal{C}_i^l$ 都在其初始旁信息集之外额外获得了 $T^{l,}_{i}{}^{1}$ 条消息。

B. 阶段 2：客户端 $\mathcal{C}^l_{r^l_{\max}-1}$ 传输策略

阶段 2仅包含来自客户端$\mathcal{C}^l_{r^l_{\max}-1}$的传输，该客户端恰好传输 $r_{\max}^l - 3$条消息。第一条传输构造为 $W_1^{l\quad -1} = \mathcal{I}_{F_1}^{l\quad -1} \oplus \mathcal{I}^{l\,r^l}_{\max,\;\max\quad L_1}{}^{-1}$。其余 $r_{\max}^l - 4$条传输构造为 $W^{l,}_{j+1}{}^{r^l\max\quad -1} = \mathcal{I}^{l,}_{F_1}{}^{r^l\max\quad -1} \oplus \mathcal{I}^{l,}_{U_j}{}^{r^l\max\quad -1}$，其中 $j \in [1, r_{\max}^l - 4]$。

这些传输有助于继续推进集合 $\{\mathcal{C}_i^l, i \in [r_{\max}^l - 2]\}$ 中客户端的前向解码链，并为客户端 $\mathcal{C}^l_{r^l_{\max}}$ 引入后向解码链。对于任意满足 $i < r_{\max}^l - 1$ 的客户端$\mathcal{C}_i^l$，已知 $\mathcal{I}^{l,}_{F_1}{}^{r^l\max\quad -1}$（由 **第1阶段** 获得）即可从 $W^{l,}_{1}{}^{r^l\max\quad -1}$ 解码出 $\mathcal{I}^{l,}_{L_1}{}^{r^l\max\quad -1}$，并从 $W^{l,}_{j+1}{}^{r^l\max\quad -1}$ 解码出 $\mathcal{I}^{l,}_{U_j}{}^{r^l\max\quad -1}$，对于 $j \in [1, r_{\max}^l - 4]$。

客户端 $\mathcal{C}^l_{r^l_{\max}}$ 可以从 $W^{l,}_{1}{}^{r^l\max\quad -1}$解码 $\mathcal{I}^{l,}_{F_1}{}^{r^l\max\quad -1}$，因为它可以使用 $\mathcal{I}^{l,}_{F_1}{}^{r^l\max\quad -1} = \mathcal{I}^{l,}_{L_1}{}^{r^l\max\quad -1}$。因此，对于 $j \in [1, r_{\max}^l - 4]$，它还可以从 $W^{l,}_{j+1}{}^{r^l\max\quad -1}$解码 $\mathcal{I}^{l,}_{U_j}{}^{r^l\max\quad -1}$，因为它知道 $\mathcal{I}^{l,}_{F_1}{}^{r^l\max\quad -1}$。

令 $T^{l,}_{i}{}^{2}$ 表示客户端$\mathcal{C}_i^l$ 在完成本层的**阶段 2** 后，为 $i \in [1, r_{\max}]$ 解码的消息数l。**阶段 2**结束后，具有 $i < r_{\max}^l - 1$的中间客户端 $\mathcal{C}_i^l$ 额外解码了 $r_{\max}^l - 3$条消息，使其已解码消息总数达到 $T^{l,}_{i}{}^{2} = T^{l,}_{i}{}^{1} + (r_{\max}^l - 3)$。客户端$\mathcal{C}^l_{r^l_{\max}-1}$作为发送端，无法从自身的传输中获得新消息，因此解码消息总数仍为 $T^{l,}_{r^l_{\max}-1}{}^{2} = T^{l,}_{r^l_{\max}-1}{}^{1}$。

客户端 $\mathcal{C}^l_{r^l_{\max}}$ 从**阶段 2**解码出 $r_{\max}^l - 3$ 条新消息。现在，由于它已解码消息 $\mathcal{I}^{l,}_{F_1}{}^{r^l\max\quad -1}$ 组合

结合 $\mathcal{I}^{l,\,r^l\max}_{F_1}{}^{-1} = \mathcal{I}^{l,\,r^l\max}_{L_1}{}^{-2}$ 这一事实，它进入反向链，并解码集合 $\{\mathcal{I}^{l,k}_{F_1} \mid k \in [3, r^l_{\max}-2]\} \cup \{\mathcal{I}^{l,k}_{U_j} \mid k \in [3, r^l_{\max}-2], j \in [1, k-3]\}$ 中的所有消息。它无法解码客户端 $\mathcal{C}^l_2$所进行传输中的任何内容。上述集合中的元素数量等于**第1阶段**传输总数减一。因此，累计解码消息数为 $T^{l,\,2}_{r^l_{\max}} = T^l + r^l_{\max} - 4$。

我们知道，$T^l = \frac{(r^l\text{最大值}-3)(r^l\text{最大值}-4)}{2} + 1$，并且 $\mathcal{C}^l_{r^l_{\max}}$ 所需的新消息总数为 $C^l - r^l_{\max} + 1$。现在，

$$T^{l,2}_{r^l_{\max}} = \frac{(r^l_{\max}-3)(r^l_{\max}-4)}{2} + r^l_{\max} - 3 = \frac{(r^l_{\max})^2 - 5r^l_{\max} + 6}{2}. \tag{6}$$

算法 3 的条件是 $C^l = \frac{(r^l\text{最大值}-2)(r^l\text{最大值}-1)}{2} + 1$。计算 $C^l - r^l_{\max} + 1$ 后，得到：

$$C^l - r^l_{\max} + 1 = \frac{(r^l_{\max}-2)(r^l_{\max}-1)}{2} - r^l_{\max} + 2 = \frac{(r^l_{\max})^2 - 5r^l_{\max} + 6}{2}. \tag{7}$$

因此，根据（ 6 7 $T^{l\,2}_{r^l_{\max}} = C^l -$ ）$r^l_{\max}+1$ 和（ ）可以证明 . 。这样，$\mathcal{C}^l_{r^l_{\max}}$ 便达到了目标消息数量。

C. 第3阶段：客户端 $\mathcal{C}^l_{r^l_{\max}}$ 传输策略

第3阶段 仅通过客户端 $\mathcal{C}^l_{r^l_{\max}}$ 的传输来完成传递过程，该客户端恰好发送 $C^l - r^l_{\max} - T^l + 3$ 条消息，每条消息的形式为 $W^{l,}_{j}{}_{r^l\text{最大值}}\mathcal{I}^{l\,r^l}{}_{\text{最大值}F_1} \oplus \mathcal{I}^{l,\,r^l\text{最大值}U_j}$，其中 $j \in [1, C^l - r^l_{\max} - T^l + 3]$。这些传输能否解码取决于接收客户端是否知晓 $\mathcal{I}^{l,\,r^l\text{最大值}F_1}$。本阶段执行的传输总数可计算如下：

$$\begin{aligned} C^l - r^l_{\max} - T^l + 3 &= \left(\frac{(r^l_{\max}-2)(r^l_{\max}-1)}{2} + 1\right) - r^l_{\max} \\ &\quad - \left(\frac{(r^l_{\max}-3)(r^l_{\max}-4)}{2} + 1\right) + 3 \\ &= \frac{{r^l_{\max}}^2 - 3r^l_{\max} + 2}{2} - r^l_{\max} \\ &\quad - \frac{{r^l_{\max}}^2 - 7r^l_{\max} + 12}{2} + 3 \\ &= \frac{4r^l_{\max} - 10}{2} - r^l_{\max} + 3 \\ &= 2r^l_{\max} - 5 - r^l_{\max} + 3 \\ &= r^l_{\max} - 2. \end{aligned} \tag{8}$$

在假设 $K \geq 2P$ 下，每个客户端 $\mathcal{C}^l_i$ 至少拥有 $i-1$ 条独有消息。对于 $i = r^l_{\max}$，这意味着至少有 $r^l_{\max} - 1$ 条独有消息可供 $\mathcal{C}^l_{r_{\max}}$ 使用。由于此阶段传输所需的独有消息数量为 $r^l_{\max} - 2$，显然少于 $\mathcal{C}^l_{r_{\max}}$ 可用的独有消息数量，因此所有异或组合都有明确的定义且有效。

令 $T^{l,}_{,i}{}^{3}$ 表示客户端 $\mathcal{C}^l_i$ 在完成该层的第3阶段后解码的消息数量 $i \in [1, r^l_{\max}]$ l。对于满足 $i \in [1, r^l_{\max} - 2]$ 的中间客户端 $\mathcal{C}^l_i$，根据阶段 2，它已经解码了 $\mathcal{I}^{l,r^l\max}_{L_1}{}^{-1}{}^{r^l}{}^{\max}_{F_1} = \mathcal{I}^{l,r^l\max}_{L_1}{}^{-1}$ **2**，，因为 $\mathcal{I}^{l,}_{r^l\max}$，$\max$。这些客户端从阶段获得了 $\max$，因此它们拥有 $\mathcal{I}^{l,}_{r^l\max F_1}$。因此，对于每次传输 $W^{l,r^l\max}_{j} = \mathcal{I}^{l,r^l\max}_{F_1} \oplus \mathcal{I}^{l,r^l\max U_j}$，它们解码出 $\mathcal{I}^{l,r^l\max U_j}$，从而获得 $C^l - r^l_{\max} - T^l + 3$ 条新消息。因此，到目前为止在该层 l 获得的消息总数为

$$T^{l,3}_i = T^{l,2}_i + C^l - r^l_{\max} - T^l + 3 = C^l - (i-1).$$

客户端 $\mathcal{C}^l_{r^l_{\max}-1}$ 自然知道 $\mathcal{I}^{l,r^l\max F_1}$，因为它等于 $\mathcal{I}^{l,}_{r^l\max}{}^{-1}$，而这属于它自己的旁信息集。因此，它可以直接从每个 $W^{l,r^l\max j}$ 中解码出 $\mathcal{I}^{l,r^l\max U_j}$，也获得 $C^l - r^l_{\max} - T^l + 3$ 条新消息。因此，到目前为止在该层 l 获得的消息总数为

$$T^{l,3}_{r^l_{\max}-1} = T^{l,2}_{r^l_{\max}-1} + C^l - r^l_{\max} - T^l + 3 = C^l - (r^l_{\max} - 2).$$

客户端 $\mathcal{C}^l_{r^l_{\max}}$ 作为发送端，无法从**第3阶段**的传输中获得额外消息。因此，到目前为止在这一层 l 获得的消息总数为

$$T^{l,3}_{r^l_{\max}} = T^{l,2}_{r^l_{\max}} = C^l - (r^l_{\max} - 1).$$

简而言之，到第3阶段结束时，每个客户端 $\mathcal{C}^l_i \in \mathcal{C}^l$ 都已从在这一层进行的传输中解码出 $T^{l,}_{,i}{}^{3} = C^l - (i-1)$ 条消息。

由于根据定义有 $T = K + C$，且我们有 $K^l = K^{l-1} + r^{l-1}_{\max}$ 和 $C^l = C^{l-1} - r^{l-1}_{\max}$，因此可得 $K^l + C^l = K^{l-1} + C^{l-1}$。根据归纳法，$K^l + C^l = K + C = T$，从而证明了 $T = K^l + C^l$。这证实了集合 $\mathcal{C}^l$ 中的第一个客户端达到目标所需的额外消息数恰好为 C^l。因此，任意客户端 $\mathcal{C}^l_i \in \mathcal{C}^l$（对于 $i \in [C^l]$）达到目标所需的额外消息数恰好为 $C^l - (i-1)$。我们已证明，每个客户端 $\mathcal{C}^l_i \in \mathcal{C}^l$（对于 $i \leq r^l_{\max}$）都已从在这一层进行的传输中解码出 $T^{l,}_{,i}{}^{3} = C^l - (i-1)$ 条消息。因此，这些客户端均已通过在这一层进行的传输满足要求。

客户端 $\mathcal{C}^l_i \in \mathcal{C}^l$（拥有 $i > r^l_{\max}$）在当前递归层级中没有收到任何消息。对于索引为 $i > r^l_{\max}$ 的客户端，一个关键性质显现出来。这些客户端无法解码第1阶段传输中的任何消息。此层中的所有传输 W $W =$ 均属于以 $\mathcal{I}^l$ $W_i = \mathcal{I}^{l,}_{,}{}^{k}$ 下类型：$W = \mathcal{I}^{l,}_{,}{}^{k}_{F_1} \oplus \mathcal{I}^{l,}_{,}{}^{k}_{F_2} \oplus \mathcal{I}^{l,}_{,}{}^{k}_{L_1}$，，$\mathcal{I}^{l,}_{,}{}^{k}_{F_1} \oplus \mathcal{I}^{l,}_{,}{}^{k}_{L_1}$，或 $\mathcal{I}^{l,}_{,}{}^{k}_{F_1} \oplus \mathcal{I}^{l,}_{,}{}^{k}_{U_j}$，其中 $k \leq r^l_{\max}$，且 j 为某个整数。客户端 $\mathcal{C}^l_i$（其中 $i > r^l_{\max}$）对所有这类传输中的两个异或项都一无所知，因为这些项与

异或中的任何消息都没有重叠。由于各阶段的传输结构保证任意两条传输至多共有一条消息，因此，对收到的传输进行任何线性组合，都无法将未知项的数量减少到一个。因此，对于 $i > r^l_{\max}$，客户端 $\mathcal{C}^l_i$ 不受此层传输的影响，从而保留其原有的消息集合，并使递归分解成为可能。

VII. 递归结构保持

递归算法在每一层都保持 LPS-FO 结构，从而能够在整个分解过程中一致地应用算法2和算法3。本节将证明 LPS-FO性质的归纳保持，并验证确保各递归层级上算法正确性的参数关系。递归过程将原始客户端集合系统地划分为连续层。在每一层 l，算法仅关注当前集合 $\mathcal{C}^l$ 中的前 $r^l_{\max}$ 个客户端，并使用算法2或算法3将其提升至目标知识水平 T。在这一层中，其余客户端会被有意隔离，不接收任何消息，以确保其知识状态保持不变（依据第五节和第六节中的证明）。处理完这些$r^l_{\max}$ 个客户端后，会将其移出处理范围，而接下来的$r^{l+1}_{\max}$ 个客户端将在第 $l+1$ 层成为处理对象。这种顺序处理方式保证在任意给定层中，只有当前正在处理的客户端会受到影响，其他客户端均保留其原有的侧信息。

这种分解策略天然保留了 LPS-FO 结构，因为每个子集 $\mathcal{C}^l$ 都构成原始客户端序列中的一个连续片段。线性递增和固定重叠性质是局部特征，在任何连续子序列中均保持成立。因此，该算法可以递归应用而无需修改，在每一层都只依赖相同的传输方案（算法2和算法3）。

A. 初始层（$l = 1$）

在初始递归层级 $l = 1$，根据问题定义，原始客户端集合 $\mathcal{C}^1 = \{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_C\}$ 具有 LPS-FO 结构。旁信息集满足$|\mathcal{I}_i| = K + (i-1)$，其中 $i \in [1, C]$，且连续客户端恰好共享 P 个重叠消息。在第 1 层执行算法 2 或算法 3 后，$\mathcal{C}^1$ 中前 $r^1_{\max}$ 个客户端恰好获得 $T = K + C$ 条消息（证明见第 V 节和第 VI 节），并停止传输。至关重要的是，如第 V 节和第 VI 节所证明的，在这一层中没有其他客户端收到任何新消息。其余客户端 $\{\mathcal{C}_i \mid i \in [r^1_{\max} + 1, C]\}$ 保持原有旁信息集不变。

B. 归纳步骤：从第 l 层到第 $l+1$ 层

假设在递归层级 l，有一组客户端 $\mathcal{C}^l = \{\mathcal{C}^l_1, \mathcal{C}^l_2, \ldots, \mathcal{C}^l_{C^l}\}$ 维护着 LPS-FO 结构，其参数为 K^l 和 P，其中 K^l 表示第一个客户端 $\mathcal{C}^l_1$的旁信息集中的消息数量。客户端 $\mathcal{C}^l_i$ 的旁信息集的基数为 $K^l + (i-1)$.

1) 对于 $i \in [1, C^l]$，连续客户端恰好共享 P条重叠消息。

在第 l 层应用算法 2 或 3 后，$\mathcal{C}^l$ 中前 $r^l_{\max}$ 个客户端恰好获得 $T = K + C$ 条消息，并停止传输。其余 $C^l - r^l_{\max}$ 个客户端在这一层没有收到新消息，因此保留了原有的知识状态。接着，我们将第 $l+1$ 层的客户端集合构造为 $\mathcal{C}^{l+1} = \{\mathcal{C}^{l+1}_1, \mathcal{C}^{l+1}_2, \ldots, \mathcal{C}^{l+1}_{C^{l+1}}\}$，其中 $\mathcal{C}^{l+1}_i = \mathcal{C}^l_{r^l_{\max}+i}$ 对于 $i \in [1, C^{l+1}]$ 和 $C^{l+1} = C^l - r^l_{\max}$。

现在验证 $\mathcal{C}^{l+1}$ 继承了 LPS-FO 结构。第一个客户端 $\mathcal{C}^{l+1}_1 = \mathcal{C}^l_{r^l_{\max}+1}$ 最初拥有 $K^l + r^l_{\max}$ 条消息。记 $K^{l+1} = K^l + r^l_{\max}$，我们观察到，对于任意客户端 $\mathcal{C}^{l+1}_i = \mathcal{C}^l_{r^l_{\max}+i}$，旁信息集的基数为 $K^l + (r^l_{\max} + i - 1) = (K^l + r^l_{\max}) + (i-1) = K^{l+1} + (i-1)$。因此，线性递增性质成立。此外，连续客户端之间 P 条消息的固定重叠得以保留，因为客户端的相对顺序和重叠结构保持不变。因此，$\mathcal{C}^{l+1}$ 满足 LPS-FO 条件，其参数为 K^{l+1}（$\mathcal{C}^{l+1}$ 中第一个客户端的旁信息集的基数）和 P（重叠参数）。

VIII. 基本情形验证

当层 l 上剩余客户端的数量（记为 C^l）减少至 2 或 1 时，递归算法终止。这些基本情形通过明确的传输方案处理，确保最终客户端达到目标知识水平$T = K + C$。关键在于，这些传输经过专门设计，使系统中的其他客户端无法解码出额外消息，从而维持安全约束，确保每个客户端恰好获得 T 条消息。

A. 双客户端基本情形 ($C^l = 2$)

当递归层级 l 上仅剩两个客户端时，它们对应于原始顺序中的最后两个客户端，即 $\mathcal{C}^l_1 = \mathcal{C}_{C-1}$ 和 $\mathcal{C}^l_2 = \mathcal{C}_C$。传输方案由三次编码广播组成。首先，客户端 $\mathcal{C}^l_2$传输 $W^l_1 = \mathcal{I}^{l,\ 2}_{F_1} \oplus \mathcal{I}^{l,\ 2}_{U_1}$和 $W^l_2 = \mathcal{I}^{l,\ 2}_{F_2} \oplus \mathcal{I}^{l,\ 2}_{U_2}$。客户端 $\mathcal{C}^l_1$拥有 $\mathcal{I}^{l,\ 2}_{F_1}$，通过与 $\mathcal{C}^l_2$的固定重叠，解码出 $\mathcal{I}^{l,\ 2}_{F_1}$和 $\mathcal{I}^{l,\ 2}_{U_2}$，获得两条新消息。随后，客户端 $\mathcal{C}^l_1$传输 $W^l_3 = \mathcal{I}^{l,\ 1}_{L_1} \oplus \mathcal{I}^{l,\ 1}_{U_1}$。客户端 $\mathcal{C}^l_2$已知 $\mathcal{I}^{l,\ 1}_{L_1}$，通过与 $\mathcal{C}^l_1$的重叠，解码出 $\mathcal{I}^{l,\ 1}_{U_1}$，获得一条新消息。完成这些交换后，两个客户端都恰好获得了达到总计 $T = K + C$条消息所需的额外消息数量（这一点将在第 节中证明）。

对于系统中的所有其他客户端（索引为$i < C - 1$的客户端），这些传输不会带来任何新消息。考虑任意一个满足 $i < C - 1$的客户端 $\mathcal{C}_i$。传输W^l_1和 W^l_2都涉及 $\mathcal{I}^{l,\ 2}_{F_1}, \mathcal{I}^{l,\ 2}_{U_j}$（对于 $j \in \{1, 2\}$），这些对 $\mathcal{C}_i$而言都是未知项，因为 $\mathcal{I}^{l,\ 2}_{F_1}$仅属于 $\mathcal{C}_{C-1}$与 $\mathcal{C}_C$之间的重叠区域，而 $\mathcal{I}^{l,\ 2}_{U_j}$仅属于$\mathcal{C}_C$。同样，$W^l_3$涉及 $\mathcal{I}^{l,\ 1}_{L_1}, \mathcal{I}^{l,\ 1}_{U_1}$，这些对$\mathcal{C}_i$而言都是未知项，因为 $\mathcal{I}^{l,\ 1}_{F_1}$仅属于 $\mathcal{C}_{C-1}$与 $\mathcal{C}_C$之间的重叠区域，而 $\mathcal{I}^{l,\ 1}_{U_1}$仅属于 $\mathcal{C}_{C-1}$。

这对 $\mathcal{C}_i$ 而言也同样是未知项，因为它位于$\mathcal{C}_{C-1}$ 和 $\mathcal{C}_C$之间的重叠区域中。此外，这些消息均未参与此前任何递归层级中的传输。由于每次传输都是两个未知消息的异或，除预期接收方外，没有其他客户端能够解码出任何新信息。此外，接收到的传输的任何线性组合都无法将未知项的数量减少到一个，因为共有3次传输，且每次传输的异或和中都包含1条新消息。这满足了安全条件，可防止非预期的知识获取。

B. 单客户端基本情形（$C^l = 1$）

当递归层级 l仅剩一个客户端时，该客户端对应于原始顺序中的最后一个客户端 $\mathcal{C}_C$ 。在这种情况下，客户端 $\mathcal{C}_{C-1}^1$（按原始索引）传输一条编码消息 $W_1^l = \mathcal{I}^{1,}_{L_1}{}^{C-1} \oplus \mathcal{I}^{1,}_{U_L}{}^{C-1}$。客户端 $\mathcal{C}_1^l$（按原始索引为 $\mathcal{C}_C$）通过与 $\mathcal{C}_{C-1}$的固定重叠，已知 $\mathcal{I}^{1,}_{L_1}{}^{C-1}$，因此能够解码 $\mathcal{I}^{1,}_{U_L}{}^{C-1}$，从而获得达到 $T = K + C$条消息所需的最后一条消息（这一点已在第五节和第六节中证明）。

对于所有其他满足 $i < C - 1$的客户端 $\mathcal{C}_i$，这次传输不包含任何可解码的信息。特别是，这些客户端不知道消息 $\mathcal{I}^{1,}_{L_1}{}^{C-1}$，因为它位于 $\mathcal{C}_{C-2}$ 和 $\mathcal{C}_{C-1}$的交集中，而 $\mathcal{I}^{1,}_{U_L}{}^{C-1}$ 则是$\mathcal{C}_{C-1}$独有的。

现在我们证明，$\mathcal{I}^{1,}_{U_L}{}^{C-1}$ 不会出现在客户端 $\mathcal{C}_{C-1}$ 在前一层 $l-1$进行的任何传输中。在第 $l-1$层，客户端 $\mathcal{C}_{C-1}$ 对应于 $\mathcal{C}^{l-1}_{r^{l-1}_{\max}}$。因此，只需检查第 $l-1$层第3阶段的传输。

如果在第 $l-1$层执行**算法 3**，则第3阶段需要 $r^{l-1}_{\max} - 2$ 条唯一消息。客户端 $\mathcal{C}^{l-1}_{r^{l-1}_{\max}}$ 至少有 $r^{l-1}_{\max} - 1$ 条消息，因此最后一条唯一消息不会用于第3阶段，并且 $\mathcal{I}^{1,}_{U_L}{}^{C-1}$ 不会参与其中。

如果在第 $l-1$层执行**算法 2**，则第3阶段需要$r^{l-1}_{\max} - 1$条唯一消息。根据 LPS-FO 侧信息结构，当 $l > 3$时，客户端 $\mathcal{C}^{l-1}_{C^1}$ 至少有 $r^{l-1}_{\max} - 1$ 条消息。由于 $r^{l-1}_{\max} \le r^{l-2}_{\max}$ 且 $r^1_{\max} > 2$，第 $l-1$层第一个客户端的侧信息大小，即 $\mathcal{C}^{l-1}_1$，超过了 K。因此，$K^{l-1} > K$，这意味着客户端 $\mathcal{C}^{l-1}_{C^{l-1}}$至少有 $r^{l-1}_{\max}$ 条消息，其中只有 $r^{l-1}_{\max} - 1$ 条消息用于该层 $l-1$。因此，最后一条唯一消息不会用于第3阶段，并且 $\mathcal{I}^{1,}_{U_L}{}^{C-1}$ 不会参与其中。因此，唯一需要考虑的剩余情况是 $l = 2$。通过穷举检查，基例传播到第 2 层的唯一配置出现在 $C = 5$时。在这种情况下，客户端 $\mathcal{C}_{C-2}$（倒数第二个客户端）在第 1 层的**算法 2** 第3阶段仅使用两条消息，至少留下一条未使用的唯一消息。因此，即使在这种情况下，最后一条唯一消息也不会出现在任何先前的传输中。

由于两个异或后的分量对非预期客户端都是未知的，任何客户端都无法从该传输中提取任何新消息。因此，安全约束仍然得到满足。

基本情形由此完成了递归算法，确保当过程终止时，每个客户端恰好拥有 $T = K + C$ 条互不相同的消息，且没有任何客户端超出该目标。针对 $C^l = 2$和 $C^l = 1$的显式传输方案，结合其固有的安全性，为算法1中实现的递归分解提供了必要的终止条件。

IX. 讨论

在这项工作中，我们采用 LPS-FO 模型研究了异构侧信息条件下的安全 DPIC，该模型刻画了客户端知识的不均匀性这一实际情况。我们提出了一种传输调度算法，可高效协调客户端广播，在确保所有客户端达到共同目标知识水平的同时，最大限度地提高每次传输的编码增益。重要的是，该设计实施了严格的安全约束，确保任何客户端获取的消息数都不超过规定的目标数量。仅当 $C = 3$ or 4 时，我们提出的方案才是最优的。下一步，我们计划进一步缩小可实现传输次数与相应下界之间的差距；目前该差距为 $N(C - r_{\max})$，并朝着传输次数最优的安全去中心化方案迈进。

参考文献

[1] Z. Bar-Yossef、Y. Birk、T. S. Jayram 和 T. Kol，“带边信息的索引编码”，*IEEE*信息论汇刊，第 57 卷，第 3 期，第 1479–1494 页，2011 年。[2] Y. Birk 和 T. Kol，“广播信道上的知情源按需编码（iscod）”，载于论文集。*IEEE INFOCOM '98*，计算机通信会议。*IEEE*计算机与通信学会第十七届年度联合会议。通往 *21* 世纪的门户（第 *98* 号目录），第 3 卷，美国加利福尼亚州旧金山，1998 年，第 1257–1264 页，第 3 卷。[3] S. Brahma 和 C. Fragouli，“柔性索引编码”，*IEEE*信息论汇刊，第 61 卷，第 11 期，第 6192–6203 页，2015 年。[4] S. El Rouayheb、A. Sprintson 和 P. Sadeghi，“关于协作数据交换的编码”，载于*IEEE*信息论研讨会，埃及开罗，2010 年，第 1–5 页。[5] T. Liu 和 D. Tuninetti，“去中心化可延展索引编码”，载于*IEEE*国际信息论研讨会（*ISIT*），法国巴黎，2019 年，第 532–536 页。[6] D. A. Bindhu、A. Pad manabhan、K. Rajesh、E. M. Baby、N. S. Karat 和 S. Sasi，“面向目标数据规模的去中心化可延展索引编码”，载于全国通信会议（*NCC*），2026 年。[7] S. H. Dau、V. Skachek 和 Y. M. Chee，“带边信息索引编码的安全性”，*IEEE*信息论汇刊，第 58 卷，第 6 期，第 3975–3988 页，2012 年。[8] M. M. Mojahedian、M. R. Aref 和 A. Gohari，“完全安全索引编码”，*IEEE*信息论汇刊，第 63 卷，第 11 期，第 7382–7395 页，2017 年。[9] L. Ong、B. N. Vellambi、P. L. Yeoh、J. Kliewer 和 J. Yuan，“安全索引编码：存在性与构造”，载于*IEEE*国际信息论研讨会（*ISIT*），西班牙巴塞罗那，2016 年，第 2834–2838 页。[10] V. Narayanan、J. Ravi、V. K. Mishra、B. K. Dey、N. Karamchandani 和 V. M. Prabhakaran，“私有索引编码”，*IEEE*信息论汇刊，第 68 卷，第 3 期，第 2020–2049 页，2022 年。[11] S. Sasi 和 B. S. Rajan，“柔性索引编码的码构造”，载于*IEEE*国际信息论研讨会（*ISIT*），法国巴黎，2019 年，第 527–531 页。[12] T. Liu 和 D. Tuninetti，“安全去中心化可延展索引编码”，载于*IEEE*国际信息论研讨会（*ISIT*），美国加利福尼亚州洛杉矶，2020 年，第 1729–1734 页。