网络中的多重密钥广播

Michael Langberg Michelle Effros

arXiv:2302.03524v1 [cs.IT] 7 Feb 2023

摘要——**Langberg 和 Effros [ITW 2022],提出的无噪声网络组播密钥分发问题（此处称为密钥广播问题），描述了通过给定网络向一组终端分发共享秘密随机密钥的任务。与传统通信不同，传统通信要求消息从源节点原封不动地传送到目的地，而密钥广播更加灵活，因为它不一定要求目的节点进行源重构。例如，分布式密钥可以是源节点的混合，而这些源节点本身可能无法恢复。**

本文研究单源、多组播网络编码设置下的密钥分发问题，即多重密钥广播问题。不同的密钥需同时从单个源节点传送到多个终端集合，每个组播集合对应一个共享随机密钥。相关场景包括安全设置，即只有源节点和预期目的地能够获取给定密钥的信息；以及非安全设置，在这种设置下，唯一要求是一个密钥的知识不会泄露另一个密钥的信息。在这两种设置下，我们都提出了密钥分发的组合条件，并设计了相应的多重密钥广播方案。此外，我们比较了有无源重构限制时的多重密钥广播速率；前者对应传统通信形式。放宽源重构要求时，密钥广播可实现严格更高的速率。

I. 引言

共享随机性这一资源在网络通信系统的理论与实践中发挥着基础性作用。在一些网络用户之间共享、且有时对其他用户保密的均匀分布密钥，是多种通信任务中的核心资源；例如，它可用于信息的安全传输、不确定噪声模型下的随机编码技术，也可用于分布式计算、统计推断和分布式学习（借助公共随机币）；此外，还可通过共享采样和哈希等方式，用于分布式认证、识别和局部差分隐私，例如 [1]–[6]。

密钥分发通信协议是指这样一种协议：多个用户共享一个密钥 K 或一组密钥 $\mathcal{K} = \{K_1, \ldots, K_\ell\}$，这些密钥可能需要保密，以此为未来需要共享随机性的通信任务做准备。密钥分发（也称为秘密密钥协商）这一任务在过去几十年中，尤其是在孤立网络结构的背景下，受到了广泛研究，例如 [2], [3], [7]–[34] ，其中多个用户希望通过易受窃听的有噪网络结构共享一个共同的密钥。

网络编码（即无噪声网络）背景下的密钥分发问题最近在[35]中被提出。具体而言， [35] 研究了多源单组播设置，本文称之为密钥广播 设置。在该设置中，目标是向一组终端节点组播速率为 R 的均匀密钥 K 。源节点可以使用相互独立的随机性；由于网络无噪声，生成的密钥 K 是源节点信息的函数。在这种背景下，密钥分发与安全组播网络编码的任务类似，例如 [36]–[42], , 因为终端之间最终共享的信息不会泄露给网络窃听者。然而，这两项任务有所不同，前者更加灵活。具体而言，在后者中，源节点持有必须由终端节点重构的消息信息；而在前者中，不要求进行源重构，因为密钥可以是源节点信息的组合，而源节点自身的信息未必能够被恢复。这种密钥分发上的灵活性，使得密钥速率 R 有可能超过通过要求源重构的安全组播所能达到的速率。事实上，对于密钥广播设置， [35] 展示了在要求和不要求源重构的情况下可实现的密钥速率之间存在显著差距。

本研究延续了这一研究方向，探讨单源多播组网络编码设置下的密钥分发问题：其中存在多个终端集合，每个集合都需要一个不同的密钥。我们将这一问题称为（单源）多重密钥广播问题。在网络中同时向不同终端集合分发不同密钥，可作为各终端集合未来通信任务的前奏，也适用于需要通过密钥分发实现唯一标识、身份验证和私密通信的多方应用，例如 [43]–[49]。我们研究安全和非安全设置下的多重密钥广播。

在安全设置下，我们旨在向不同终端集合分发不同密钥，并要求除源节点 s 和每个预定终端节点之外，任何网络节点都无法获知有关任何密钥的信息。所有概念均在第二节中详细介绍。借鉴秘密共享范式（例如 [50]–[52],），并受到单源网络编码背景下分布式秘密共享研究 [53], [54],的启发，我们提出了安全多重密钥广播的一个紧确充分组合条件（及其对应的通信方案）。

在非安全情形下，我们要求每个终端集合都能解码出一个不同的密钥，并且获知一个密钥不会泄露通过网络传播的任何其他密钥的信息。受以下研究的分析启发，

M. Langberg 任职于纽约州立大学布法罗大学电气工程系。电子邮箱：mikel@buffalo.edu。M. Effros 任职于加州理工学院电气工程系。电子邮箱：effros@caltech.edu。本研究部分由美国国家科学基金会资助，项目编号为 CCF-1817241 和 CCF- 1909451。

[55]–[57],该研究讨论了 2-单播网络编码的编码方案和上界，我们给出了多重密钥广播的紧确必要且充分的组合条件（以及相应的通信方案）。

最后，为了更好地理解源重构在密钥分发协议中的作用，我们将密钥分发与一种更传统的通信形式进行比较：在这种形式中，源信息首先在终端处重构，然后才（或许）经过后处理以导出共享密钥。我们分别针对安全情形和非安全情形表明，在要求进行源重构与不要求进行源重构时可获得的密钥率之间存在显著差距。

本文其余部分的结构如下。第二节给出详细模型。第三节首先介绍非安全情形、再介绍安全情形下的主要结果。第五节针对第三节的分析，给出安全和非安全实例；在这些实例中，要求进行源重构与不要求进行源重构时可获得的密钥率存在显著差异。若干技术性证明放在附录中。

II. 模型

我们采用 [35]，中给出的模型和定义，并稍作修改以适用于本文研究的问题。以下记号有助于理解后续定义。对于任意整数 ℓ，令 $[\ell]=\{1,2,\dots,\ell\}$。

- **有向无环多重密钥广播实例：** 多重密钥广播问题的一个实例 $\mathcal{I}=(G,\ s,\ \{D_i\}_{i=1}^{\ell},\ \{\mathcal{B}_i\}_{i=1}^{\ell})$ 包括一个有向无环网络 $G=(V,\ E)$，其中每条边 $e\in E$ 的容量均为单位容量（我们允许使用多条平行边来表示更高的整数容量连通性），一个源节点 $s\in V$，一组互不相交的终端集合 $D_i\subseteq V$（对应 $i\in[\ell]$），每个终端集合都由若干终端节点组成；对于 $i\in[\ell]$，还有一个由边的子集构成的集合 $\mathcal{B}_i=\{\beta_{i,1},\dots,\beta_{i,|\mathcal{B}_i|}\}$，用于指定保密要求。源节点$s$ 持有无限多个相互线性无关且均匀分布的比特 $M=\{b_i\}_{i}$。按照有向无环网络编码研究中常见的约定，我们假设 s 没有入边，且终端 $d\in\cup_{i\in[\ell]}D_i$没有出边。

- 密钥码：对于块长 n，网络码 $(\mathcal{F},\mathcal{G})=(\{f_e\},\{g_{i,j}\})$ 是为每条边 $e\in E$ 指定一个（局部）编码函数f_e，并为每个终端 $d_{i,j}\in D_i$指定一个译码函数 $g_{i,j}$，其中 $i\in[\ell]$。对于每条边 $e=(u,v)$，从 u 到 v 的边消息 $X_e^n\in\mathcal{X}_e^n=[2^n]$ 等于编码函数 f_e在输入 $X^n\mathrm{In}(u)$ 上的取值；对于一般节点 u_0 X^n $_{u_0}$ $X_{e'}^n$ $e'=v\ u_0\ \in$，E M $\mathrm{In}(\cdot)$ 等于 $((:(,)),(:\ u_0=s))$，涵盖了节点u_0 在通信过程中可获得的全部信息。为确保节点 u 在编码之前能够获得$X^n\mathrm{In}(u)$，通信按照网络E上预先确定的拓扑序进行。若目标速率为 R，则当对于每个 $i\in[\ell]$ 和每个终端 $d_{i,j}\in D_i$，译码函数 $g_{i,j}$ 在随机变量向量$X^n\mathrm{In}(d_{i,j})$ 上的取值等于一个均匀随机变量的再现时，该密钥码即为成功的

K_i 取值于字母表 $[2^{Rn}]$，并满足以下条件。首先，密钥 K_i 满足保密约束 $\mathcal{B}_i$，即对于每个 $\beta\in\mathcal{B}_i$, $I(K_i;(X_e^n:\ e\in\beta))=0$。其次，每个终端集 D_i 都需要一个不同的密钥 K_i，使得对于 $i\neq i'$，密钥 K_i 与密钥 $K_{i'}$线性无关；也就是说，随机变量 $\{K_i\}_{i=1}^{\ell}$ 两两独立（PWI），因此对所有 $i\neq i'$都有$I(K_i;K_{i'})=0$。

定义 *2.1*（多重密钥广播可行性）：若存在一个分组长度为 n 的密钥码（$\mathcal{F}$，$\mathcal{G}$），使得对于实例 $\mathcal{I}$，则称该实例是（R，n）-可行的

- **解码：** 对于所有 $i\in[\ell]$ 以及所有 $d_{i,j}\in D_i$、$H(K_i|X^n{}_{\text{输入 }(d_{i,j})})=0$。
- **两两独立密钥速率：** 对于所有 $i\in[\ell]$、K_i 是一个均匀随机变量，且 $H(K_i)=Rn$。对于 $i\neq i'\in\{1,\dots,\ell\}$，$I(K_i;\ K_{i'})=0$。
- **保密性：** 对于所有 $i\in[\ell]$、$I(K_i;\ (X_e^n:\ e\in\beta))=0$，对于任意子集 $\beta\in\mathcal{B}_i$。

在本研究中，我们还将密钥分发与更传统的通信形式进行了比较。在这些通信形式中，源信息首先在终端处进行源重构，然后才（可能）经过后处理以导出共享密钥 K_i；我们将这种方法称为源重构（SR）密钥分发。

定义 *2.2*（源重构多重密钥广播可行性）：若存在一个分组长度为 n 的密钥码 $(\mathcal{F},\mathcal{G})$，使得实例 $\mathcal{I}$ 满足以下条件，则称其为 $(R,n)_{\mathrm{SR}}$-可行：

- **源重构：** 对于所有 $i\in[\ell]$ 以及所有 $d_{i,j}\in D_i$，存在一组源信息位$M_{i,j}\subseteq M$，使得 $H(M_{i,j}|X^n{}_{\mathrm{In}(d_{i,j})})=0$，即，消息比特 $M_{i,j}$ 在终端 $d_{i,j}$ 处被解码。
- **两两独立密钥构造与速率（后处理）：** 对于所有 $i\in[\ell]$，存在一个均匀随机变量 K_i，满足 $H(K_i)=Rn$，使得对于所有 $d_{i,j}\in D_i$，$H(K_i|M_{i,j})=0$。对于 $i\neq i'\in\{1,\dots,\ell\}$，$I(K_i;\ K_{i'})=0$。
- **保密性：** 对于所有 $i\in[\ell]$，$I(K_i;(X_e^n:\ e\in\beta))=0$，对任意子集 $\beta\in\mathcal{B}_i$均成立。

定义 *2.3*（多重密钥广播容量）：$\mathcal{I}$ 的（对称）多重密钥广播容量记为 $\mathbf{R}(\mathcal{I})$，它是满足以下条件的最大 R：对于所有 $\Delta>0$，存在无穷多个分组长度 n，使得 $\mathcal{I}$ 是 $(R-\Delta,n)$- 可行的。先重构源信息，再对共享密钥进行后处理所能达到的容量记为 $\mathbf{R}_{\mathrm{SR}}(\mathcal{I})$，其定义与此类似。

III. 结果

A. 非安全情形

本节介绍一种在非安全设置下进行多重密钥广播的协议，并将可实现的密钥率与重构源信息的传统协议进行比较。我们研究的问题是：向给定终端集合中的所有成员分发密钥，同时向不同的终端集合分别分发不同的密钥。分布式密钥应满足以下性质：任意终端节点持有的密钥都不会泄露关于由另一个终端集中的终端共享的任何密钥的信息。也就是说，我们要求这些密钥两两独立。

我们的协议和分析受到 [55]–[57], 中分析的启发，该分析研究了编码解以及

具有整数边容量的 2-单播网络编码的上界。粗略地说，我们在此证明，对于具有多个终端集合的单源实例，当且仅当对于终端集合 D_i 中的每个终端 d_i 以及每个 $j \neq i$，都存在一条从源节点 s 到 d_i 的单位容量路径，且该路径不经过与终端 $d_j \in D_j$对应的某些割集 C_j 时，才能实现单位速率的多重密钥广播。必要性可由标准的割集论证得出，而可达性论证则结合了一个两阶段过程：首先修改初始的 2-组播线性网络码，以确保对于每个 j， D_j 中的所有终端都能解码出相同的密钥 K_j，并且对于 $i \neq j$，该密钥与任何其他终端集合 D_i 中终端解码出的密钥线性无关 K_j。

为指定与终端$d_j \in D_j$ 对应的割集 C_j，我们采用 [55]–[57]中的以下定义。全文中，我们假设在 G的边上预先给定一个拓扑序。

定义 *3.1*（割集 C_j）：对于每个 $j \in [\ell]$ 和$d \in D_j$，若存在一条或多条边，移除这些边后会将 d 与源节点 s分隔开，则令 e_d 为 G中拓扑序最靠前的分隔边；否则，令 $e_d = \phi$。对于每个 $j \in [\ell]$，令 $C_j = \{e_d | d \in D_j,\ e_d \neq \phi\}$。

本节的主要定理给出了单位速率下密钥分发的组合刻画。证明见附录 A。下面简要概述可达性方案的证明思路。

定理 *3.1*（多重密钥广播）：考虑多重密钥广播问题的一个实例 $\mathcal{I} = (G,\ s,\ \{D_i\}_{i=1}^{\ell},\ \{\mathcal{B}_i\}_{i=1}^{\ell})$，其中 $\mathcal{B}_i = \phi$ 对 $i \in [\ell]$ 成立（即没有安全约束）。那么$\mathbf{R}(\mathcal{I}) \geq 1$，当且仅当对于每个 $i,\ j \in [\ell]$，使得$j \neq i$，并且对于每个终端 $d \in D_i$，都存在一条单位容量路径连接 s 和 d，且该路径不经过 C_j中的边。

在第五节中，我们将本方案的可达密钥率$\mathbf{R}(\mathcal{I})$与通过源重构可获得的最大密钥率$\mathbf{R}_{\text{SR}}(\mathcal{I})$进行比较，并展示两者之间存在显著差距。具体而言，我们证明以下定理。

定理 *3.2*（通过源重构实现多重密钥广播）：设 $\epsilon > 0$。存在非安全多重密钥广播问题的实例 $\mathcal{I}$，满足定理 3.1 的充分条件，且$\mathbf{R}_{\text{SR}}(\mathcal{I}) \leq 3/4 + \epsilon$。

B. 定理 *3.1* 的证明：可达性的粗略概述

为证明可达性，我们设计了一种两阶段编码方案；两个阶段都是确定性的。首先，我们使用 G 的一种特定边着色，设计一个 2-多播编码方案。然后，修改该着色和编码方案，使之满足我们的密钥分发要求。通过边着色来描述 2-多播的方法，例如见 [58]。

设源节点 s持有 2 条消息 a 和 b。在我们的边着色中，着色为颜色 α 的边 e 表示在 e上传输线性组合 $a + \alpha b$，其中 a、b和 α 都是足够大的域 $F = [2^n]$中的元素，分组长度为 n，且所有运算都在 F上进行。我们的着色遵循 G中预先确定的边拓扑序。不失一般性，我们假设 G 中的每个节点都与 s连通。否则，可以从 G 中移除这些节点，而不会影响通信协议。

• **第一着色阶段：**考虑拓扑序最靠前的边 e。令 T_e 为移除 e 后与 s 断开的边集（我们称这些边为 e-紧边）。我们将 e 以及每条 $e' \in T_e$ 着色为颜色 $\alpha = 1$，对应消息 $a + \alpha b = a + b$。请注意，在 e 上为 $\alpha = 1$ 传输 $a + \alpha b$，并在 T_e 中所有从 e 出发的边上传输该消息的编码方案，是一种有效的密钥码，因为任何边的输入信息都足以计算其出边信息。接下来，我们按照 G中边 e 的拓扑序，通过归纳法继续着色：每一步都按拓扑序考虑下一条尚未着色的边 e，并将 e 以及相应的边集 T_e（移除 e后与 s 断开的边）着色为一个新颜色 α；该颜色比之前分配的所有颜色都大 1，对应于要在 e上传输的消息 $a + \alpha b$。在附录 A 中，我们证明，在归纳法的任何中间阶段，任何已分配颜色的边都足以根据其输入信息计算其出边信息。我们的第一着色阶段如图 2(a) 所示。

• **第二着色阶段：**为了开始第二个着色/编码阶段，我们现在聚焦于先前定义的割集 C_j，以及在移除 C_j 后与 s 断开的边集 e'。我们将后一边集记为 T_j，并称其中的边为 j-紧的。在附录 A 中，我们证明任意一条边至多对一个 $j \in [\ell]$ 值是 j-紧的。根据边 $e \in C_j$ 定义（定义 3.1）中的拓扑极小性条件，e 要么与 s 2-边连通，要么是 s 的一条出边。这意味着，对于任意 j 和 j'（j 可以等于 j'），不同的边 $e \in C_j$ 和 $e' \in C_{j'}$ 将具有不同的颜色。在第二个着色阶段，我们为所有 $j \in [\ell]$，给 C_j 中的所有边 e 以及所有 j- 紧边 $e' \in T_j$ 指定一种新颜色 α_j。与之前一样，用 α_j 为一条边着色，对应于在该边上传输 $a + \alpha_j b$。在附录 A 中，我们证明这种修改后的着色不会影响网络编码可行性。也就是说，任意边 e 都能根据其输入信息计算出边信息。

• **对 $K_j = a + \alpha_j b$ 在终端 $d \in D_j$的解码：**为了完成证明，我们需要证明，对于任意 $j \in [\ell]$，任意终端 $d \in D_j$ 都能够解码 $K_j = a + \alpha_j b$（速率为 1）。注意，这组密钥是两两独立的。不失一般性，我们假设所有终端节点 d 在 G 中都只有一条入边。否则，对于任意终端 $d \in D_j$，可以通过向 G 添加一个新节点 d'、添加一条新边（$d,\ d'$），并通过移除 d、添加 d' 来修改D_j，从而构造一个新实例。新实例可达速率 1，当且仅当原实例可达速率 1。在此假设下，进入 $d \in D_j$ 的唯一边 e 要么属于 C_j，要么属于 T_j。这是因为，移除其唯一入边后，d与 s 被分隔开，因此存在一条拓扑序最小的边 $e_d \in C_j$，将 d与 s 断开。由于 C_j 和 T_j 中的边都被 α_j着色，终端 $d \in D_j$ 可以解码 $K_j = a + \alpha_j b$。这就完成了可达性证明的概要。完整细节见附录 A。

IV. 安全情形

本节研究（单源）多密钥广播问题，其中将一组密钥 $\mathcal{K} = \{K_1, \ldots, K_\ell\}$ 分发给属于不相交终端集合 $\{D_1, \ldots, D_\ell\}$ 的终端，并要求对于每个 $j \in [\ell]$，唯一单独持有关于密钥 K_j 的任何信息的网络节点 $v \in V \setminus \{s\}$ 是节点 $v \in D_j$。我们通过秘密共享的视角研究此设置下的密钥容量。

在秘密共享范式中（例如，[50]–[52]），持有均匀分布的秘密消息的分发者需要将份额分发给一组用户，并为每位用户分配一个份额。每个份额都是由分发者使用秘密消息和额外随机性计算得到的随机变量。访问结构 $(\mathcal{A}_{\text{access}}, \mathcal{A}_{\text{no-access}})$ 是预先确定的一组用户子集，其中 $\mathcal{A}_{\text{access}}$ 中的每个用户子集都可以联合解码秘密，而 $\mathcal{A}_{\text{no-access}}$ 中的每个用户子集即使尝试联合解码，也无法获知任何关于秘密的信息。例如，阈值访问结构[50], [59] 要求任何 k 用户子集都无法获知关于秘密消息的任何信息，而 $k+1$ 用户组成的任何集合都可以联合恢复秘密。

受 [53], [54], 启发（其研究在网络结构上设计秘密共享协议），我们提出了满足上述安全要求的单源多重密钥广播的组合条件。

定理 *4.1*（安全的多重密钥广播）：考虑多重密钥广播问题的一个实例 $\mathcal{I} = (G, s, \{D_i\}_{i=1}^{\ell}, \{\mathcal{B}_i\}_{i=1}^{\ell})$，其中对于 $i \in [k]$，$\mathcal{B}_i = \{\text{In}(v) \mid v \in V \setminus (D_i \cup \{s\})\}$。那么，若对每个终端 $d \in \cup_i D_i$，都存在两条从 s 到 d 的顶点不相交路径，并且对每个非终端节点 v，都存在两条从 s 到 v 的边不相交路径，则 $\mathbf{R}(\mathcal{I}) \geq 1$。此外，这些组合条件是紧的，即存在满足这些条件的实例 $\mathcal{I} = (G, s, \{D_i\}_{i=1}^{\ell}, \{\mathcal{B}_i\}_{i=1}^{\ell})$，使得 $\mathbf{R}(\mathcal{I}) = 1$。

下面给出定理 4.1 的证明。在第五节中，我们将本方案的可达密钥率与通过源重构可获得的最大密钥率进行比较，并展示二者之间存在显著差距。具体而言，我们证明以下定理。

定理 *4.2*（通过源重构实现安全的多重密钥广播）：令 $\epsilon > 0$。存在一个实例 $\mathcal{I}$，它属于安全多重密钥广播问题，满足定理 4.1 的组合条件，且 $\mathbf{R}_{\text{SR}}(\mathcal{I}) \leq 3/4 + \epsilon$。

A. 定理 *4.1* 的证明

该证明受到 [53], [54] 中针对阈值 $k = 1$ 所提出的分布式秘密共享方案的启发，并与之密切相关。所提出的传播方案使用有向无环图 G 中顶点的一种特殊图着色。

我们首先定义图着色，它为每个顶点 $v \in V$ 指定一个整数颜色 c_v。我们的着色旨在确保：两个顶点 u 和 v 颜色不同（$c_u \neq c_v$），当且仅当存在从 s 到 u 的有向路径 P（s, u）以及从 s 到 v 的有向路径 P（s, v），且这两条路径顶点不相交。这里，若路径 P（s, u）和 P（s, v）中共同出现的唯一顶点是源节点 s，则称它们顶点不相交。

我们的着色按照预先定义的拓扑序进行。这里及下文中，我们假设颜色按递增的线性顺序分配，即每次分配一个不同的颜色时，其值都比先前分配的颜色大一。源节点 s 的颜色为 $c_s = 1$。对于每个仅从 s 接收入边的 s 的邻居节点 u，均分配一个独特的颜色。对于之后的每个顶点 u，根据归纳法，假设拓扑序中排在 u 之前的所有顶点 v 都已着色。若 u 有两条入边（v, u）和（v', u），满足 $c_v \neq c_{v'}$，则为 u 分配一个与此前分配的所有颜色都不同的颜色。这样的顶点称为新着色的顶点。否则，c_u 取其入边邻居节点的颜色，即对于任意入边（v, u），$c_u = c_v$。这样的顶点称为颜色保持顶点。对于 s 的每个仅从 s 接收入边的邻居节点 u，称其为颜色保持顶点（尽管在过程开始时为其分配了一个不同的颜色）。在附录 B 的命题 A.1 中，我们证明：G 中的顶点 u 与 s 二顶点连通（即在 G 中存在两条顶点不相交路径 P_1（s, u）和 P_2（s, u））当且仅当它是新着色的。

命题 A.1 表明，每个终端节点都会被重新着色。如下所示，每个终端的颜色决定其密钥，不同颜色对应的密钥两两独立。为使同一终端集合中的终端能够解码出相同的密钥，我们对着色方案稍作修改。具体而言，对于每个终端集合 D_i，我们选取一个代表终端 $d_i \in D_i$，并将 D_i 中的所有终端都赋予颜色 c_{d_i}。因此，代表终端集合 D_i 的颜色为 c_{d_i}。由于本文假设终端节点没有任何出边，所提出的修改后着色不会改变任何网络节点 u 的入邻节点的颜色。

现在介绍分组长度为 n 的密钥分发方案。假设图 G 由颜色 $\{1, 2, 3, \ldots, c\}$（的一个子集）着色。我们取足够大的 n，使得 $2^n > c$。考虑有限域 $F = [2^n]$。源节点 s 从 F 中均匀随机地选取三个线性无关的值 s、a、b。对于 s 的每个邻居节点 v，若其入边仅来自 s，则源节点向 v 传输 $s + c_v a$ 和 $a + c_v b$（所有运算均在 F 上进行）。这是可行的，因为 G 中的任意节点与源节点之间都是 2-边连通的（也就是说，在此情形下，有两条边连接 s 和 v）。我们按拓扑序进行，并通过归纳法证明每个顶点 u 都能收到计算 $s + c_u a$ 和 $a + c_u b$ 所需的信息。考虑一个网络节点 u（它也可能是终端节点）。如果 u 是新着色的，那么它至少有两条入边（v, u）和（v', u），且 $c_v \neq c_{v'}$。在这种情况下，v 在（v, u）上传输（$s + c_v a$）$+ c_u$（$a + c_v b$），而 v' 在（v', u）上传输（$s + c_{v'} a$）$+ c_u$（$a + c_{v'} b$）。整理上述线性方程中的各项后，我们得出 u 收到（$s + c_u a$）$+ c_v$（$a + c_u b$）和（$s + c_u a$）$+ c_{v'}$（$a + c_u b$），这使它能够解码 $s + c_u a$ 和 $a + c_u b$（因为 $c_v \neq c_{v'}$）。如果 u 不是新着色的，那么 u 就是颜色保持节点。请注意，任何节点（包括节点 u）都必须至少有两条入边（否则它与 s 之间就不是双边连通或双点连通）。设（v, u）和（v', u）是 u 的两条入边。这里 v 可能等于 v'，并且由于 u 是颜色保持节点，$c_u = c_v = c_{v'}$。因此，v 可以在（v, u）上转发 $s + c_u a$，而 v' 可以在（v', u）上转发 $a + c_u b$。

在此过程结束时，图 G 中的每个顶点 u 都已

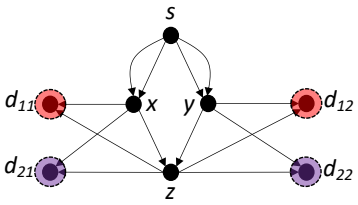

图1：定理 4.1 的一个紧致示例。

恰好收到两条不同的消息， $s+c_u a$ 和 $a+c_u b$ （或它们的两个线性无关线性组合）。对于每个 $i \in [\ell]$，将终端集合 D_i 的密钥定义为 $K_i = s + c_{d_i} a$。由此可知，协议完成后， D_i 中的每个终端 d 都能恢复 K_i。

为了证明保密性，我们现在利用这样一个事实：每个终端节点都被赋予了一个新颜色；也就是说，对于 $d \in D_i$，对于任意顶点 $v \notin D_i$，颜色 c_{d_i} 都不同于 c_v。由于任何这样的 v 在协议执行期间只会接收 $(s+c_v a)$ 和 $(a+c_v b)$（或它们的线性组合），因此 v 的消息与 K_i 之间的互信息为零。形式化地，对于任意 $i \in [\ell]$，如果 $v \notin D_i \cup \{s\}$，那么 $c_{d_i} \neq c_v$，因此

$$I(X_{\mathrm{In}(v)}; K_i) = I((s + c_v a), (a + c_v b); s + c_{d_i} a) = 0.$$

为了说明在定理 4.1 所假设的组合条件下，界 $\mathbf{R}(\mathcal{I}) \geq 1$ 是紧的，我们现在给出一个满足这些条件的示例实例 $\mathcal{I}$（如图 1 所示），其中 $\mathbf{R}(\mathcal{I}) = 1$。在我们的示例中，单个源节点 s 必须将两个密钥 K_1 和 K_2 分别分发给终端集合 $D_1 = \{d_{11}, d_{12}\}$（红色）和 $D_2 = \{d_{21}, d_{22}\}$（紫色），并满足：(i) 对于每个节点 $v \in \{x, y, z\}$ 和任意 $i \in \{1, 2\}$，$I(K_i; X_{\mathrm{In}(v)}) = 0$；(ii) 对于每个 $i,\ j \in \{1, 2\}$、$i \neq j$ 以及任意终端节点 $d \in D_j$，$I(K_i; X_{\mathrm{In}(d)}) = 0$。图 1 中所有边的容量均为 1。注意，每个终端都与 s 之间有两条顶点不相交路径，并且所有节点都与 s 边连通两次。我们证明，此情况下的最大可达密钥率为 1。

考虑任意一个秘密传播协议。对于任意顶点v，令 $X_{\mathrm{In}(v)}$ 表示协议期间输入到 v 的信息；对于任意边（u, v），令 X_{uv} 表示在（u, v）上传输的信息。由于网络无环，我们按照 G上的拓扑序进行通信。接下来，我们给出若干信息不等式，用以证明我们的断言。

首先考虑边（x, z）和（y, z），并注意到$H(X_{\mathrm{In}(z)}) \leq H(X_{xz}) + H(X_{yz})$。不失一般性，设 $H(X_{xz}) \geq H(X_{yz})$。于是 $H(X_{xz}) \geq 0.5H(X_{\mathrm{In}(z)})$，且$H(X_{yz}|X_{xz}) \leq 0.5H(X_{\mathrm{In}(z)})$。

此外，现在我们有

$$\begin{aligned} H(X_{\mathrm{In}(x)}, X_{\mathrm{In}(z)}) &= H(X_{\mathrm{In}(x)}) + H(X_{\mathrm{In}(z)}|X_{\mathrm{In}(x)}) \\ &\leq 2 + H(X_{xz}, X_{yz}|X_{\mathrm{In}(x)}) \\ &\leq 2 + H(X_{xz}, X_{yz}|X_{xz}) \\ &= 2 + H(X_{yz}|X_{xz}) \\ &\leq 2 + 0.5H(X_{\mathrm{In}(z)}). \end{aligned}$$

根据我们的安全要求和图拓扑，我们知道 $X_{x,\ d_{11}}$ 与 K_1线性无关，并且 $X_{z,\ d_{11}}$ 线性无关于 K_1，并且 K_1 是$X_{x,\ d_{11}}$ 和 $X_{z,\ d_{11}}$的函数。这些观察结果表明

$$\begin{aligned} H(K_1) &= H(K_1|X_{z,d_{11}}) \leq H(K_1, X_{x,d_{11}}|X_{z,d_{11}}) \\ &= H(X_{x,d_{11}}|X_{z,d_{11}}) + H(K_1|X_{x,d_{11}}X_{z,d_{11}}) \\ &= H(X_{x,d_{11}}|X_{z,d_{11}}). \end{aligned}$$

类似地， $H(K_1) \leq H(X_{z,\ d_{11}}|X_{x,\ d_{11}})$，因此

$$\begin{aligned} H(X_{z,d_{11}}, X_{x,d_{11}}) \geq \\ H(X_{x,d_{11}}|X_{z,d_{11}}) + H(X_{z,d_{11}}|X_{x,d_{11}}) \geq 2H(K_1). \end{aligned}$$

结合我们的安全性假设——输入到 d_{11} 的信息与 K_2线性无关——现在可得

$$\begin{aligned} H(X_{\mathrm{In}(x)}, X_{\mathrm{In}(z)}) &\geq H(X_{x,d_{11}}, X_{z,d_{11}}, K_2) \\ &= H(X_{x,d_{11}}, X_{z,d_{11}}) + H(K_2) \\ &\geq 2H(K_1) + H(K_2). \end{aligned}$$

将密钥速率 $H(K_1) = H(K_2)$ 记为 R。最后，利用 $X_{\mathrm{In}(z)}$ 与 K_1 线性无关这一事实，我们得到

$$\begin{aligned} H(X_{\mathrm{In}(x)}, X_{\mathrm{In}(z)}) &= H(X_{\mathrm{In}(x)}, X_{\mathrm{In}(z)}, K_1) \geq H(X_{\mathrm{In}(z)}, K_1) \\ &= H(X_{\mathrm{In}(z)}) + H(K_1) = H(X_{\mathrm{In}(z)}) + R. \end{aligned}$$

现在我们得到以下不等式

- $H(X_{\mathrm{In}(x)}\ X_{\mathrm{In}(z)}) \geq 3R$
- $H(X_{\mathrm{In}(x)}\ X_{\mathrm{In}(z)}) \leq 2 + 0.5H(X_{\mathrm{In}(z)})$
- $H(X_{\mathrm{In}(x)}\ X_{\mathrm{In}(z)}) \geq R + H(X_{\mathrm{In}(z)})$

上述第二个和第三个不等式共同推出 $2H(X_{\mathrm{In}(x)}, X_{\mathrm{In}(z)}) \leq 4 + H(X_{\mathrm{In}(z)}) \leq 4 + H(X_{\mathrm{In}(x)}, X_{\mathrm{In}(z)}) - R$，进而推出 $H(X_{\mathrm{In}(x)}, X_{\mathrm{In}(z)}) \leq 4 - R$。将其与第一个不等式结合，得到 $3R \leq H(X_{\mathrm{In}(x)}, X_{\mathrm{In}(z)}) \leq 4 - R$，从而证明了我们的断言$R \leq 1$。

V. 要求源重构的局限性

本节将说明，在非安全和安全设置中，与不要求源重构时所能达到的密钥率相比，要求进行源重构都会显著降低可实现的密钥率。我们首先给出一个与 Plotkin 界性质相似的技术引理 [60], ，该引理指出，较大的二元码中必然存在一对总支撑集较小的码字。该引理的证明见附录 C。

引理 *5.1*：任何大小为-M、分组长度为-n 的二元码，若其中码字的汉明重量不超过 wn，则必定包含一对码字 $x = (x_1, \ldots, x_n)$ 和 $x' = (x'_1, \ldots, x'_n)$，使得它们支撑集的并集（即集合 $\{i \in [n] \mid x_i = 1\} \cup \{i \in [n] \mid x'_i = 1\}$）大小至多为 $nw(2 - w) \cdot \left(1 + \frac{1}{M-1}\right)$。

在附录C中，我们证明定理3.2和4.2，并使用引理 5 1 $M-1 =$ 的以下推论，该推论通过设定 $\frac{1}{\epsilon} \geq \frac{w\ 2-w}{\epsilon}$ 得到。

推论 *5.1*：设 $\epsilon > 0$。任意分组长度为 n、大小为 $M = 1 + \frac{1}{\epsilon}$ 的二元码，若其码字的汉明重量不超过 wn，则其中存在一对码字 $x = (x_1, \ldots, x_n)$ 和 $x' = (x'_1, \ldots, x'_n)$，使得它们的支撑集并集（即集合 $\{i \in [n] \mid x_i = 1\} \cup \{i \in [n] \mid x'_i = 1\}$）的大小至多为 $n(2w - w^2) + \epsilon n$。

VI. 结束语

本文研究安全和非安全设置下的多重密钥广播问题。针对这两种设置，我们给出了允许以单位速率进行多重密钥广播的组合条件。在非安全设置下，我们的条件是紧的，并刻画了密钥率。在安全情形下，我们证明了该分析是紧的，即存在满足这些组合条件的实例，使得单位密钥率是最优的。我们的模型假设图为有向无环图，且边容量是所研究的（单位）密钥率的整数倍；这两个假设均用于组合着色方案及其分析。正在尝试将该分析扩展到有向循环图，例如利用 [53]–[56], 中的思想，或推广到一般边容量。我们的模型假设密钥服从两两独立密钥集合的分布，并且在安全设置下考虑由单个网络节点控制的有限窃听者。对于更强的窃听模型，研究两两独立之外的其他独立形式（例如 k 重独立）也是正在进行的研究课题。

附录

A. 定理 3.1 的证明

该证明受到 [55]–[57], 的启发，这些文献研究了具有整数边容量的 2-单播网络编码的编码方案与逆定理。我们先给出逆定理。考虑任意速率为 $R \geq 1$ 的密钥分发协议。对于任意顶点v，令 $X_{\mathrm{In(v)}}$ 表示协议期间传入 v 的信息。对于任意边 e，令 X_e 表示在 e上传输的信息。对于任意边集 A，令 $X_A = (X_e : e \in A)$表示在边 $e \in A$上传输的信息。首先注意，对于 C_j 中的任意边e，必有 $H(K_j|X_e) = H(X_e|K_j) = 0$; 这是因为 $e = e_d$，对于某个需要速率为 $R \geq 1$ 的密钥 K_j 的终端 $d \in D_j$，且 e 的容量为单位容量。因此可得 $H(K_j|X_{C_j}) = H(X_{C_j}|K_j) = 0$。现在反设存在 i、 $j \in [\ell]$、$j \neq i$以及一个终端$d \in D_i$，使得 C_j 将 s 与 d分隔开。根据我们的译码要求，这意味着 $H(K_i|X_{C_j}) = 0$。然而，由于 $H(X_{C_j}|K_j) = 0$，我们得出 $H(K_i|K_j) = 0$。因此，根据两两独立性要求， $R = H(K_i) = H(K_i|K_j) = 0$，这与我们的假设 $R \geq 1$矛盾。

为证明可达性，我们设计一种两阶段编码方案；两个阶段都是确定性的。为完整起见，以下部分内容重复了第三节中的内容。首先，我们使用 G的某种边着色设计一种2-多播编码方案。然后，修改着色和编码方案，使其符合我们的密钥分发要求。

设源节点 s 持有两条消息， a 和 b。在我们的边着色中，着色为颜色 α 的边 e 表示在 e上传输线性组合 $a + \alpha b$，其中 a、b和 α 都是分组长度为 n时足够大的域 $F = [2^n]$中的元素，且所有运算均在 F上进行。我们的着色遵循边在 G中的预定拓扑序。我们不失一般性地假设， G 中的每个节点都与 s连通。否则，可以从 G 中移除这些节点，而不影响通信协议。

- **第一着色阶段：** 考虑拓扑序最靠前的边 e。令 T_e 为移除 e后与 s 断开的边集；我们称这类边为 e-紧边。我们用对应于消息 $a+\alpha b = a+b$的颜色 $\alpha = 1$ 为 e 以及每条 $e' \in T_e$ 着色。请注意，在 T_e 中，针对 e 上的 $\alpha = 1$ 以及所有从 e 延伸出的边传输 $a + \alpha b$ 的编码方案，是有效的密钥码，因为任意边的输入信息都足以计算其出边信息。接下来，我们按边 e 在 G中的拓扑序，通过归纳法继续着色。每一步中，我们考虑拓扑序中下一条尚未着色的边 e。我们用一个新颜色 α为 e 以及相应的集合 T_e （即移除 e后与 s 断开的边集）着色，该颜色比此前分配的所有颜色都大 1；颜色 α 对应于要在 e 上传输的消息 $a + \alpha b$。下面我们证明，在归纳法的任意中间阶段，任何已着色的边都足以根据其输入信息计算其出边信息。我们的第一着色阶段如图 2(a)所示。

- **与第一着色阶段相对应的编码的有效性：** 假设G的边已进行部分着色，并令 e 为拓扑序最小的未着色边。令 α 为我们现在赋予 e和 T_e中 e-紧边的不同颜色。我们首先证明T_e 中的所有边此前都未着色。反设存在一条已着色的边 $e' \in T_e$。这意味着 e' 的拓扑序大于 e的拓扑序。进而，这意味着对于一条此前已着色的边 e^*， $e' \in T_{e^*}$ 成立；换言之，移除 e^*后， e' 与 s 不连通。因此，从 s 到 e' 的每条路径都必须先经过 e^*，然后经过 e。然而，由于 $e \notin T_{e^*}$，存在一条连接 s 和 e 且不经过 e^*的路径。这意味着存在一条从 s 到 e' 且不经过 e^*的路径，这与 $e' \in T_{e^*}$矛盾。

现在我们证明， e 能够根据其输入信息计算出其输出消息。如果 e 是 s的一条出边，那么 e 上的出边信息可由s 计算得出，因为 s 同时满足 a 和 b。否则，注意到 e 的所有入边都已被赋予颜色。e 不可能有一条颜色为 $\alpha' < \alpha$ 的入边 e'，否则移除 e' 就会使 e 与 s 断开连接，因此e 早已在归纳过程的前一阶段着色。 e 也不可能有多条入边，且 e 的所有入边 e' 颜色都相同。在这种情况下，所有指向 e 的入边e' 都属于集合 T_{e^*}，其中边 e^* 已在归纳过程中着色；这意味着移除 e^*后，所有这类 e' 都与 s 断开连接，因此 e 本身属于 T_{e^*}。如果 e 属于 T_{e^*}，那么 e 早已在归纳过程的前一阶段着色。剩下的情况是，e 有两条颜色不同的入边。在这种情况下，由于这两条边上的信息线性无关， e的尾顶点能够计算出输出消息 $a+\alpha b$。

这就完成了我们着色/编码过程的第一阶段。经过这次着色，任何与 s 2-边连通的边 $e = (u, v)$（即存在至少两条边不相交的路径连接 s 和 u）都不能属于任何其他边 e^* 的集合 T_{e^*}；否则，根据我们的定义，边 e 会

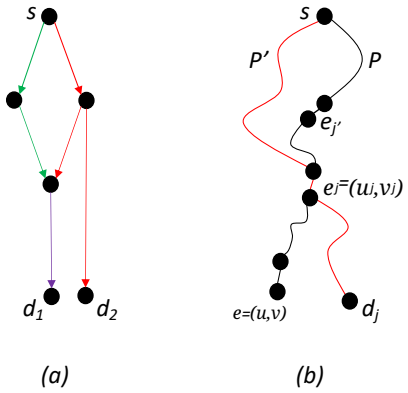

图 2：(a) 定理 3.1 证明中第一着色阶段的示意图。(b) 示意图表明，任意一条边对于至多一个 $j \in [\ell]$ 值可以是 j-紧的（摘自定理 3.1 的证明）。红色路径连接 s 和 e，且不与 $C_{j'}$ 相交。

通过移除边 e^* 而与 s 不连通，并且边 e 与 s 不满足 2-边连通。 s 的出边也同样如此。因此， s 的出边和与 s 2-边连通的边 e 必须具有不同的颜色。

- **第二着色阶段：** 现在开始第二个着色/编码阶段，我们将重点关注先前定义的割集 C_j，以及在移除 C_j 后与 s 断开的边集 e'。我们将后一边集记为 T_j，并称其中的边为 j-紧的。我们稍后将证明，任意一条边对于至多一个 $j \in [\ell]$ 值可以是 j-紧的。根据边 $e \in C_j$ 定义（定义 3.1）中的拓扑极小性条件， e 要么与 s 2-边连通，要么是 s 的出边。由上述讨论可知，对于任意 j 和 j'（j 可以等于 j'），不同的边 $e \in C_j$ 和 $e' \in C_{j'}$ 必须具有不同的颜色。在第二着色阶段，对于每个 $j \in [\ell]$，我们给 C_j 中的所有边 e 以及所有 j-紧的边 $e' \in T_j$ 赋予一种新的颜色 α_j。

- 集合 T_j 和 $T_{j'}$ 对于 $j \neq j'$ 是互不相交的：在讨论与第二阶段修改后的着色相对应的编码方案是否有效之前，我们先证明，任意一条边至多对一个 $j \in [\ell]$ 值是 j-紧的。证明如图 2(b) 所示。反设结论不成立，设 $e = (u, v)$ 是一条同时为 j 和 j' 紧的边。考虑任意一条从 s 到 e 的路径 P。该路径必定同时与 C_j 和 $C_{j'}$ 相交。不失一般性地假设， P 中距离 s 最远（即拓扑序最大的）且与 $C_j \cup C_{j'}$ 相交的边来自 C_j，并将这条边记为 $e_j = (u_j, v_j)$。将 $P \cap C_{j'}$ 中的一条边记为 $e_{j'}$。由于 $e_j \in C_j$，必定存在一个终端 $d_j \in D_j$，在移除 e_j 后与 s 断开。根据我们对 G 的假设，存在一条路径 P'，连接 d_j 和 s，且不与 $C_{j'}$ 相交。由于 P' 必须经过 e_j，从 s 到 e 的路径先沿用连接 s 和 e_j 的 P' 部分，再沿用从 e_j 到 e 的 P 部分；该路径连接 s 和 e，且不包含来自 $C_{j'}$ 的任何边。这样的路径存在，与 e 是 j'-紧的假设矛盾。

- **与第二着色阶段对应的编码的有效性：** 接下来我们证明，我们修改后的赋值在第二着色阶段对颜色的分配不会影响网络编码可行性；也就是说，我们证明任意边 e 都能根据其输入信息计算出其出边信息。我们按照第一着色阶段所使用的归纳顺序进行证明。对于拓扑序最小的边 e， e 是 s 的一条出边；因此，无论 e 的颜色在第二着色阶段是否发生改变，e 以及 T_e 中的所有 e' 都能根据其输入信息计算出其出边信息。下面，我们证明在归纳的任意中间阶段，任何此前能够根据其输入信息计算出其出边信息的边，在第二着色阶段采用修改后的着色方案后仍然可以做到这一点。

考虑在第一着色阶段的某个中间步骤中被赋予新颜色的一条边 e 和集合 T_e。我们考虑几种情况。

– e 的颜色在不同阶段之间发生了变化：如果 e 的颜色发生了变化，那么要么 $e \in C_j$，要么 $e \in T_j$。如果 $e \in T_j$，那么移除 C_j 后，它与 s 不连通，因此所有入边 e' 也必须属于 T_j 或 C_j。这意味着 e 的输入信息等于其出边信息。如果 $e \in C_j$，那么它要么是 s 的一条出边，此时它可以根据 s 的消息计算出边信息；要么它与源节点 s 之间是 2-边连通的，此时它至少有 2 条入边。考虑指向 e 的入边。其中一些边在第二着色阶段可能改变了颜色，而另一些则可能保留了原始颜色。不可能所有指向 e 的入边都为 $j' \neq j$ 变成了 $\alpha_{j'}$，否则移除 $C_{j'}$ 后， e 就会与 s 不连通，进而（根据 C_j 的定义）会存在一个终端 $d_j \in D_j$，移除 $C_{j'}$ 后它与 s 不连通。这与我们对 G 的假设矛盾。指向 e 的所有入边也不可能具有相同的颜色 α，且该颜色与前一着色阶段相比没有变化。这可由第一着色阶段的归纳分析得出。具体来说，在这种情况下，移除颜色为 α 的边后，边 e 会不连通，因此它本应属于某条边 e^* 对应的 T_{e^*}；这意味着 e 在第一着色阶段不会获得新颜色（这与我们对 e 的假设矛盾）。因此， e 必须有 2 条颜色不同的入边（可能是两种都未改变的颜色、一种未改变的颜色和一种改变了的颜色，或者两种在第二阶段改变了的颜色）。这意味着有两条线性无关的入向消息发给 e，从而使 e 的尾顶点能够计算 e 上的出边信息。

– **颜色 e 在各阶段之间没有变化：** 最后，我们考虑一条在第一阶段和第二阶段之间颜色没有变化的边 e。这种情况与上述分析类似。如果 e 是 s 的出边，那么它可以根据 s 的消息计算出边信息。否则，根据对第一着色阶段的分析， e 不可能只有一条入边 e'。考虑指向 e 的入边。其中一些边在第二着色阶段可能改变了颜色，而另一些边可能保留了原始颜色。指向 e 的所有入边不可能都变成 α_j，否则，移除 C_j 后， e 将与 s 断开连接，这意味着 $e \in T_j$；由此得到一个

矛盾，因为如果 $e \in T_j$，那么 e 在着色阶段之间就会改变颜色。指向 e 的所有入边也不可能都具有相同的颜色 α，且该颜色未在第二着色阶段发生变化。这可由对第一着色阶段的归纳分析得出。因此，同样地， e 必须有两条颜色不同的入边（两条颜色均未改变、一条未改变而另一条改变，或两条颜色都在第二阶段发生了变化）。这意味着 e 收到两条线性无关的入向消息，使得 e 的尾顶点能够计算 e 上的出边信息。至此，我们完成了对着色/编码过程第二阶段的分析。

• **终端处的解码 $K_j = a + \alpha_j b$ 在终端 $d \in D_j$：** 为了完成证明，我们需要证明，对于任意 $j \in [\ell]$，任意终端 $d \in D_j$ 都能够解码 $K_j = a + \alpha_j b$（速率为 1）。注意，这组密钥是两两独立的。正如本文正文所述，我们在此不失一般性地假设， G 中的所有终端节点 d 都只有一条入边。在这一假设下，指向 $d \in D_j$ 的唯一入边 e 要么属于 C_j，要么属于 T_j。这是因为根据观察，移除其唯一入边后， d 与 s 分离，因此存在一条拓扑序最小的边 $e_d \in C_j$，使得 d 与 s断开。由于 C_j 和 T_j 中的边均由 α_j 着色，终端 $d \in D_j$ 可以解码 $K_j = a + \alpha_j b$。至此，可达性证明完成。

B. 定理 *4.1* 证明中使用的命题 *A.1*

命题 *A.1*：图 G 中的顶点 u 从 s 点双连通，当且仅当它被新着色。

证明：对于正向，反设存在一个点双连通的顶点 u，使得所有入边（v、u）都已针对给定的颜色 c_0 具有 $c_v = c_0$。令 v^* 为 G 中拓扑序最小且满足 $c_{v^*} = c_0$ 的顶点。注意，根据我们的着色过程，对于图 G 中的每个顶点 $v' \neq v^*$，如果 $c_{v'} = c_{v^*} = c_0$，那么必然所有指向 v' 的入边（w、v'）都满足 $c_w = c_0$。现在我们声称，移除 c_{v^*} 会使 u 与 s 断开，这与我们关于 u 从 s 点双连通的假设相矛盾。反设存在一条从 s 到 u 的路径 P，且不经过 v^*。令 v' 为 P 上满足 $c_{v'} = c_0$ 且拓扑序最小的顶点。由于所有指向 u 的入边（v、u）都满足 $c_v = c_0$，顶点 v' 的定义是良好的。根据我们的假设，即 P 不经过 v^*，顶点 v' 不可能是 v^*。由于除了 s 之外没有其他顶点具有颜色 1。因此，沿路径 P 指向 v' 的入边 (w, v') 满足 $c_w = c_0$；这与关于 v' 拓扑序的最小性假设矛盾。

反向地，假设 u 不是 2-顶点-连通的。这意味着存在一个单独的顶点 v 位于 G中，移除该顶点后会使 s 与 u断开。考虑由移除 v 所隐含的 V 的割划分（V_s, V_u），其中 $s \in V_s$ 和 $u \in V_u$。现在，根据 G 的拓扑序进行归纳可知，V_u 中的所有顶点（包括 u）都以颜色 c_v保持颜色不变。 ■

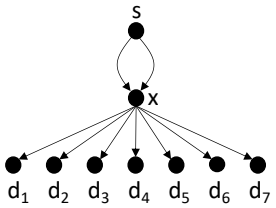

图 3：定理 3.2 的一个实例。

C. 引理 *5.1* 和定理*3.2*和*4.2*的证明

1) 引理 *5.1* 的证明：对于任意两个码字 x 和 x'，令 $\ell_{x,x'} = |\{i \in [n] \mid x_i = 1\} \cup \{i \in [n] \mid x'_i = 1\}|$。令 $\ell = \min_{x,x'} \ell_{x,x'}$。我们希望证明，对于大小为 M的码，有 ℓ 至多为 $n(2w - w^2) + \frac{nw}{(1-w)M-1}$。令 $\ell^c_{x,x'} = n - \ell_{x,x'}$，$\ell^c_{x,x'} = |\{i \in [n] \mid x_i = 0\} \cap \{i \in [n] \mid x'_i = 0\}|$ 表示条目 i 的数量，其中 x_i 和 x'_i 均等于 0；并令 $\ell^c = n - \ell$。一方面，

$$\sum_{x \neq x'} \ell^c_{x,x'} \leq \binom{M}{2} \ell^c$$

另一方面，若 M_i 是满足 $x_i = 0$ 的码字 x 的数量，则

$$\sum_{x \neq x'} \ell^c_{x,x'} = \sum_{i=1}^{n} \binom{M_i}{2}$$

鉴于码字的重量限制，注意到$\sum_i M_i \geq M(1-w)n$。此外，在此约束下，当对每个 i， $M_i = M(1-w)$ 时，表达式 $\sum_i \binom{M_i}{2}$ 取得最小值。因此我们得出结论：

$$\binom{M}{2} \ell^c \geq \sum_{x \neq x'} \ell^c_{x,x'} = \sum_i \binom{M_i}{2} \geq n \binom{M(1-w)}{2}$$

因此， $\ell^c \geq n(1-w)^2 - \frac{nw}{(1-w)M-1}$，或者等价地，

$$\ell \leq n - n(1-w)^2 + \frac{nw(1-w)}{M-1} \leq nw(2-w) \cdot \left(1 + \frac{1}{M-1}\right).$$

2) 非安全情形：定理 *3.2* 的证明：现在，我们使用图 3 所示的实例来证明定理 3.2。

证明：（定理 3.2 的证明）考虑图 3 所示的三层实例。该网络包含一个源节点s ，它通过 2 条单位容量边连接到一个中间节点 x。源节点 s 和节点 x 代表网络的前两层。第三层由终端节点 d_1、…、d_ℓ 组成，对于 $\ell = 1 + 1/\epsilon$，每个节点都通过一条单位容量边与 x相连，且分别属于不同的终端集合 $D_i = \{d_i\}$。注意，该实例满足定理 3.1 的条件。每个终端都会对源信息位 $M = \{b_1, b_2, \ldots\}$的一个子集进行解码；子集M_i 在终端 d_i 处解码，对于 $i \in [\ell]$。考虑网络上的任意分组长度为n 的码。令 M_x 为可在节点 x处解码的源信息位子集。首先注意到$|M_x| \leq 2n$，因此不失一般性，我们假设 $M_x \subseteq \{b_1, \ldots, b_{2n}\}$。根据图拓扑，我们还

观察到，对于每个 $i \in [\ell]$， M_i 都是 M_x 的子集，且 $|M_i| \le n$。将M_i的特征二进制向量 c_i 视为 M_x的子集，可得到一个码本 c_1、...、c_ℓ，其中每个码字的分组长度至多为 $2n$，重量至多为 n。必要时在码字后补零，可得到一个码本 c_1、...、c_ℓ，其分组长度为 $2n$，重量至多为n。应用推论 5.1，其中 $w = 1/2$ 且分组长度为 $2n$，我们得出存在指标 $i \neq j$，使得 c_i 与 c_j的总支撑集，以及 M_i 与 M_j的总支撑集，相应地至多为 $(2w - w^2 + \epsilon)2n = (3 + 4\epsilon)n/2$。由于 K_i 是 M_i的函数， K_j 是 M_j的函数，且 K_i 与 K_j线性无关，我们得出 $H(K_i) + H(K_j) \le (3 + 4\epsilon)n/2$，进而推出 $\mathbf{R}_{\mathtt{SR}}(\mathcal{I}) \le (3 + 4\epsilon)/4 = 3/4 + \epsilon$。 ■

备注 *A.1*： 根据定理 3.1 的连通性条件，可以通过分组长度为 n的随机线性网络编码证明，每个终端节点都能解码两条消息（均匀分布），每条消息的熵为 $n/2$。因此，每个终端都可以利用解码所得消息的线性组合（各终端使用的组合可能不同），获得速率为 $1/2$ 的密钥，并且该密钥与不同解码集合中的终端所解码的任何密钥均线性无关。这个简单方案表明 $\mathbf{R}_{\mathtt{SR}}(\mathcal{I}) \ge 1/2$。因此，定理 3.2 中有源重构与无源重构的密钥分发方案之间的差距虽不一定是最优的，但其数量级是正确的。

D. 安全情形：定理 *4.2* 的证明

现在我们证明，可以对图 1 所示的实例（该图展示了定理 4.1 的一个紧确例子）稍作修改，以证明定理 4.2。

证明： （定理 4.2）我们先定义实例$\mathcal{I}$，它是图 1 所示实例的一个修改版本。令终端集合的数量 D_i 为 $\ell = \frac{9}{\epsilon}\left(1 + \frac{9}{\epsilon}\right)$，而非 $\ell = 2$。在 $\mathcal{I}$中，对于 $i \in [\ell]$，单个源节点 s 必须向终端集合 $D_i = \{d_{i1}, d_{i2}\}$ 分发密钥 K_i，使得 (i) 对每个节点$v \in \{x, y, z\}$及任意 $i \in [\ell]$， $I(K_i;\ X_{\mathtt{In}(v)}) = 0$；并且 (ii) 对任意终端节点 d，$\mathtt{In}(d)$ 不会泄露任何有关在 d处并不需要的密钥的信息。连接 s 和 x 的边有两条，连接 s 和 y的边也有两条。图 1 中的所有边容量均为单位容量。注意，每个终端都有两条来自 s的顶点不相交路径，并且所有节点都与 s双边连通。下文将证明 $\mathbf{R}_{\mathtt{SR}}(\mathcal{I}) \le 3/4 + \epsilon$。

对于每个 $i \in [\ell]$，令 M_i 为终端节点 d_{i1} 重构的源消息比特。令 $B = \cup_i M_i$。对于每个M_i，我们有 $H(M_i|X_{\mathtt{In}(x)}X_{\mathtt{In}(z)}) = 0$。因此，也有 $H(B|X_{\mathtt{In}(x)}X_{\mathtt{In}(z)}) = 0$。我们得出， $H(B) \le H(X_{\mathtt{In}(x)}X_{\mathtt{In}(z)}) \le H(X_{\mathtt{In}(x)}) + H(X_{\mathtt{In}(z)}|X_{\mathtt{In}(x)}) \le 3$。

将 c_i 的特征二进制向量视为 M_i 的子集 B，我们得到一个码本 $c_1, \ldots, c_\ell$，其中码字的分组长度均为 $|B| \le 3n$，重量至多为 $2n$。必要时在码字后补零，我们得到一个分组长度为 $3n$、重量至多为 $2n$ 的码本 $c_1, \ldots, c_\ell$。根据鸽巢原理，存在某个重量 w，使得至少有 $1 + \frac{9}{\epsilon}$ 个终端 $\{d_{i1}\}_i$ 解码得到 M_i，其大小范围为 $[3wn, 3(w + \epsilon/9)n]$。将推论 5.1 应用于这样的 w 和分组长度 $3n$，我们得出存在指标 $i \neq i'$，使得 c_i 与 $c_{i'}$的总支撑集，以及 M_i 与 $M_{i'}$的总支撑集，均至多为 $(2w - w^2)3n + \epsilon n$。由于 K_i 是 M_i 的函数， $K_{i'}$ 是 $M_{i'}$的函数，并且 K_i 与 $M_{i'}$线性无关，我们得出

$$\begin{aligned} H(K_i) &\le |M_i \setminus M_{i'}| = |M_i \cup M_{i'}| - |M_{i'}| \\ &\le (2w - w^2 - w)3n + \epsilon n \\ &= (w - w^2)3n + \epsilon n \le \frac{3n}{4} + \epsilon n. \end{aligned}$$

这意味着 $\mathbf{R}_{\mathtt{SR}}(\mathcal{I}) \le 3/4 + \epsilon$。 ■

备注 *A.2*： 在定理 4.1 的连通性条件下，可以证明，结合额外思路使用随机线性网络编码可得 $\mathbf{R}_{\mathtt{SR}}(\mathcal{I}) \ge 1/2$。因此，与备注 A.1 一样，定理 4.2 中无论是否进行源重构的密钥分发方案之间的差距虽然不一定是最优的，但其量级是正确的。

参考文献

[1] Claude E. Shannon。《保密系统的通信理论》。《贝尔系统技术期刊》，28(4)：656–715，1949年。[2] Ueli M. Maurer。通过公开讨论利用共同信息进行密钥协商。《IEEE 信息论汇刊》，39(3)：733–742，1993年。[3] Rudolf Ahlswede 和 Imre Csisz´ar。信息论与密码学中的共享随机性。I. 秘密共享。《IEEE 信息论汇刊》，39(4)：1121–1132，1993年。[4] Amos Lapidoth 和 Prakash Narayan。不确定信道下的可靠通信。《IEEE 信息论汇刊》，44(6)：2148–2177，1998年。[5] Wei-Ning Chen 、 Peter Kairouz 和 Ayfer Ozgur。在通信约束下的稀疏分布估计中打破维度依赖。在《学习理论会议》，第1028–1059页。PMLR，2021年。[6] Jayadev Acharya 和 Ziteng Sun。局部隐私分布估计与重频项中的通信复杂度。在《国际机器学习会议》，第51–60页。PMLR，2019年。[7] Peter G´acs 和 J´anos K¨orner。共同信息远少于互信息。《控制与信息论问题》，2(2)：149–162，1973年。[8] Aaron D. Wyner。两个相关随机变量的共同信息。《IEEE 信息论汇刊》，21 179，1975 2 163( )：–。[9] Aaron D. Wyner。窃听信道。《贝尔系统技术期刊》，54(8)：1355–1387，1975年。[10] Hans S. Witsenhausen。关于相关随机变量对的序列。《SIAM应用数学杂志》，28(1)：100–113，1975年。[11] Imre Csisz´ar 和 Janos Korner。带机密消息的广播信道。《IEEE 信息论汇刊》，24 348，1978 3 339( )：–。[12] Charles H. Bennett、Gilles Brassard 和 Jean-Marc Robert。通过公开讨论进行隐私放大。《SIAM计算杂志》，17(2)：210–229，1988年。[13] Charles H. Bennett、Gilles Brassard、Claude Cr´epeau 和 Ueli M. Maurer。广义隐私放大。《IEEE 信息论汇刊》，41(6)：1915–1923，1995年。[14] Ueli Maurer 和 Stefan Wolf。抵抗主动对手的隐私放大。在《国际密码学年会》，第307–321页。施普林格，1997年。[15] Rudolf Ahlswede 和 Imre Csisz´ar。信息论与密码学中的共享随机性。II. 共同随机性容量。《IEEE 信息论汇刊》，44(1)：225–240，1998年。[16] Imre Csisz´ar 和 Prakash Narayan。辅助者参与下的共享随机性与密钥生成。《IEEE 信息论汇刊》，46(2)：344–366，2000年。[17] Imre Csisz´ar 和 Prakash Narayan。多终端的保密容量。《IEEE 信息论汇刊》，50(12)：3047–3061，2004年。[18] Elchanan Mossel、Ryan O’Donnell、Oded Regev、Jeffrey E. Steif 和 Benny Sudakov。非交互相关性提取、非齐次马尔可夫链与反向 Bonami-Beckner不等式。《以色列数学杂志》，154(1)：299–336，2006年。[19] Chung Chan 和 Lizhong Zheng。多终端密钥协商。《IEEE 信息论汇刊》，60(6)：3379–3412，2014年。[20] Imre Csisz´ar 和 Prakash Narayan。多终端信道模型的保密容量。《IEEE 信息论汇刊》，54(6)：2437–2452，2008年。[21] Amin Aminzadeh Gohari 和 Venkat Anantharam。多终端的信息论密钥协商——第一部分。《IEEE 信息论汇刊》，56(8)：3973–3996，2010年。[22] Amin Aminzadeh Gohari 和 Venkat Anantharam。多终端的信息论密钥协商——第二部分：信道模型。《IEEE 信息论汇刊》，56(8)：3997–4010，2010年。[23] Mahdi Jafari Siavoshani、Christina Fragouli、Suhas Diggavi、Uday Pul- leti 和 Katerina Argyraki。广播擦除信道上的群组密钥生成。在第四十四届 IEEE 阿西洛马会议：信号、系统与计算，第719–723页，2010年。[24] Andrej Bogdanov 和 Elchanan Mossel。关于从相关源中提取共同随机比特。《IEEE 信息论汇刊》，57(10)：6351–6355，2011年。[25] Himanshu Tyagi。共同信息与密钥容量。《IEEE 信息论汇刊》，59(9)：5627–5640，2013年。[26] Siu On Chan、Elchanan Mossel 和 Joe Neeman。如何从大字母表上的相关源中提取共同随机比特。IEEE 信息论汇刊，60(3):1630–1637，2014年。[27] Jingbo Liu、Paul Cuff 和 Sergio Verd´u。通过超收缩性实现单个通信者的密钥生成及其单次反定理。载于2015年IEEE国际信息论研讨会（ISIT），第710–714页，2015年。[28] Venkatesan Guruswami 和 Jaikumar Radhakrishnan。通信辅助一致性提取的紧界。载于第31届计算复杂性会议（CCC），2016年。[29] Peng Xu、Zhiguo Ding、Xuchu Dai 和 George K. Karagiannidis。关于 m中继两两独立网络的私钥容量。IEEE 信息论汇刊，62(7):3831–3843，2016年。[30] Masahito Hayashi、Himanshu Tyagi 和 Shun Watanabe。密钥协商：一般容量与二阶渐近。IEEE 信息论汇刊，62(7):3796–3810，2016年。[31] Prakash Narayan 和 Himanshu Tyagi。通过公开讨论实现多终端保密。Now出版社，汉诺威，马萨诸塞州，美国，2016年。[32] Badih Ghazi 和 T. S. Jayram。资源高效的共享随机性与密钥方案。载于第二十九届ACM-SIAM离散算法年会论文集，第1834–1853页，2018年。[33] Jingbo Liu、Paul Cuff 和 Sergio Verd´u。有限交互下的共享随机性与密钥生成。arXiv预印本 arXiv:1601 00899，2016年。.[34] Cl´ement L. Canonne、Venkatesan Guruswami、Raghu Meka 和 Madhu Sudan。使用不完美共享随机性的通信。IEEE 信息论汇刊，63(10):6799–6818，2017年。[35] Michael Langberg 和 Michelle Effros。网络编码多播密钥容量。载于IEEE信息论研讨会（ITW），第422 427页，2022年 –。[36] Ning Cai 和 Raymond W. Yeung。安全网络编码。载于IEEE 信息论国际研讨会，第323页，2002年。[37] Jon Feldman、Tal Malkin、C. Stein 和 Rocco A. Servedio。关于安全网络编码容量。载于第 42 届 Allerton 通信、控制与计算年会，第63–68页，2004年。[38] Ning Cai 和 Raymond W. Yeung。多源线性网络编码的安全条件。IEEE 信息论国际研讨会，第561–565页，2007年。[39] Ning Cai 和 Raymond W. Yeung。关于安全网络码构造的最优性。IEEE 信息论国际研讨会，第166–170页，2008年。[40] Salim El Rouayheb、Emina Soljanin 和 Alex Sprintson。II型窃听网络的安全网络编码。IEEE 信息论汇刊，58(3):1361–1371，2012年。[41] Danilo Silva 和 Frank R. Kschischang。通过秩度量码实现通用安全网络编码。IEEE 信息论汇刊，57(2):1124–1135，2011年。[42] Sidharth Jaggi 和 Michael Langberg。安全网络编码：保密可靠通信的界与算法。载于《网络编码：基础与应用》第7章（Muriel M´edard 和 Alex Sprintson 编），第183–215页。学术出版社，2012年。[43] Daihyun Lim、Jae W. Lee、Blaise Gassend、Edward G. Suh、Marten Van Dijk 和 Srinivas Devadas。从集成电路中提取密钥。IEEE超大规模集成（VLSI）系统汇刊，13(10):1200–1205，2005年。[44] Ying Su、Jeremy Holleman 和 Brian P. Otis。利用工艺变化实现的数字1.6 pj/bit芯片识别电路。I EEE 信号处理精选主题期刊，43(1):69–77，2008年。[45] G. Edward Suh 和 Srinivas Devadas。用于设备认证和密钥生成的物理不可克隆函数。载于2007年第44届ACM/IEEE设计自动化会议，第9–14页，2007年。[46] Haile Yu、Philip Heng Wai Leong、Heiko Hinkelmann、Leandro Moller、Manfred Glesner 和 Peter Zipf。迈向一种利用工艺变化的独特FPGA识别电路。载于国际现场可编程逻辑与应用会议，第397–402页，2009年。[47] Wei-Ning Chen、Peter Kairouz 和 Ayfer Ozgur。打破通信-隐私-准确性三难困境。《神经信息处理系统进展》，33:3312–3324，2020年。[48] David Byrd 和 Antigoni Polychroniadou。用于金融应用中联邦学习的差分隐私安全多方计算。载于首届ACM金融人工智能国际会议，第1 9页，2020年 –。[49] Rudolf Ahlswede、Alexander Ahlswede、Ingo Alth¨ofer、Christian Deppe 和 Ulrich Tamm。《识别与其他概率模型》。施普林格，2021年。[50] Adi Shamir。如何共享秘密。ACM通讯，22(11):612–613，1979年。

[51] Mitsuru Ito、Akira Saito 和 Takao Nishizeki。实现一般访问结构的秘密共享方案。日本电子与通信（第三部分：基础电子科学），72(9):56–64，1989年。[52] Amos Beimel。秘密共享方案：综述。载于国际编码与密码学会议，第11–46页。施普林格，2011年。[53] Nihar B. Shah、K. V. Rashmi 和 Kannan Ramchandran。用于低通信成本分布式秘密共享的安全网络编码。载于*IEEE* 信息论国际研讨会，第2404–2408页，2013年。[54] Nihar B. Shah、K. V. Rashmi 和 Kannan Ramchandran。通过网络分布式秘密分发。*IEEE* 信号处理精选主题期刊，9(7):1206–1216，2015年。[55] Chih-Chun Wang 和 Ness B. Shroff。针对两个简单多播会话的会话间网络编码。载于第*45*届 *Allerton* 通信、控制与计算年会（*Allerton*），第 682 689 页，2007 年 –。[56] Chih-Chun Wang 和 Ness B. Shroff。有向网络上的成对会话间网络编码。*IEEE* 信息论汇刊，56(8):3879–3900，2010年。[57] Sagar Shenvi 和 Bikash Kumar Dey。双单播问题的一个简单充要条件。载于*IEEE* 国际通信会议，第1–5页，2010年。[58] Christina Fragouli 和 Emina Soljanin。网络编码基础。*Foundations and Trends® in Networking*，2(1):1–133，2007年。[59] George Robert Blakley。保护密码密钥。载于*IEEE* 需求知识管理国际研讨会，第313页，1979年。[60] Morris Plotkin。具有指定最小距离的二元码。*IRE* 信息论汇刊，6(4):445–450，1960年。