向量线性安全聚合中个体密钥率的容量区域

Lei Hu Sennur Ulukus 电气与计算机工程
系 马里兰大学，美国马里兰州大学公园市
20742*leihu@umd.edu* *ulukus@umd.edu*

arXiv:2601.03241v1 [cs.IT] 6 Jan 2026

摘要——我们针对 Yuan-Sun 最近在 [ISIT 2025], 提出的一个开放问题提供了新的见解，该问题涉及向量线性安全聚合问题所需的最小个体密钥率。考虑一个包含 K个用户的分布式系统，其中每个用户 $k \in [K]$ 持有一个数据流 W_k 和一个个人密钥 Z_k。服务器旨在计算线性函数 $\mathbf{F}[W_1; \ldots; W_K]$，同时不获取关于另一个线性函数 $\mathbf{G}[W_1; \ldots; W_K]$的任何信息，其中 $[W_1; \ldots; W_K]$ 表示 $W_1, \ldots, W_K$的行堆叠。这个开放问题是确定 Z_k所需的最小长度，记为 $R_k, k \in [K]$。本文刻画了速率元组 $(R_1, \ldots, R_K)$ 的一个新可达区域。该区域是多面体，其顶点由满足秩增量条件的二元速率分配 $(R_1, \ldots, R_K) = (\mathbb{1}(1 \in \mathcal{I}) \ldots, \mathbf{1}(K \in \mathcal{I}))$ 刻画：$\mathbf{rank}\left([\mathbf{F}_\mathcal{I}; \mathbf{G}_\mathcal{I}]\right) = \mathbf{rank}(\mathbf{F}_\mathcal{I}) + N$。这里，$\mathbf{F}_\mathcal{I}$ 和 $\mathbf{G}_\mathcal{I}$ 是由索引为 $\mathcal{I}$的列构成的子矩阵。我们的结果揭示了一个新颖的事实：并非每个用户都必须持有密钥，因此严格扩大了文献中已知的最佳可达区域。此外，我们还进行了逆向分析，证明在最小化持有密钥的用户数量时，该区域是最优的。

I. 引言

受联邦学习在计算机科学和工程学各领域广泛应用的推动，安全求和问题的信息论极限已得到广泛研究 [5], [6]。具体而言，考虑一个包含 K 个分布式用户的场景，其中用户 $k \in [K]$持有一个数据流 W_k 和一个密钥 Z_k。服务器旨在计算这些数据流的总和$W_1 + \ldots + W_K$，同时不获取有关消息的任何额外信息。为此，每个用户 k 向服务器发送消息X_k ，该消息是 W_k 和 Z_k的函数。文献 [6] 刻画了通信成本和密钥率的信息论极限：为计算总和的一个符号，每个用户必须传输一个符号并持有一个符号密钥，而所有密钥的总随机性（联合熵）至少应为 $K - 1$。

近期，Yuan 和 Sun [7], 研究了一种称为向量线性安全聚合的安全求和问题推广形式，其中服务器旨在获得任意线性函数$\mathbf{F}[W_1; \ldots; W_K]$，其中$\mathbf{F} \in \mathbb{F}_q^{M \times K}$具有满行秩 $\mathbf{rank(F)} = M$，且 $[W_1; \ldots; W_K]$ 表示 $W_1, \ldots, W_K$的行堆叠。同时，服务器不得获得关于另一个线性函数$\mathbf{G}$ $[W_1; \ldots; W_K]$的任何信息，其中$\mathbf{G} \in \mathbb{F}_q^{N \times K}$的秩为 $\mathbf{rank(G)} = N$。该表述将一些已有问题纳为特例，包括分布式线性变换 [8]和线性网络计算 [9]–[11]。

对于向量线性安全聚合，通信成本和密钥的最小联合熵已得到完整刻画 [7]: 对于每次聚合，每个用户至少必须发送1个符号消息，且密钥的最小联合熵为$\mathbf{rank}([\mathbf{F}; \mathbf{G}]) - \mathbf{rank(F)}$。然而，最优个体密钥率 R_k，即Z_k，$k \in [K]$的最小长度，仍然未知。由于矩阵$\mathbf{F}$ 和$\mathbf{G}$的结构复杂性，确定这些个体密钥率远比刻画随机性的总量更具挑战性。

一个关键难点在于，个体密钥之间可能存在相关性。元组$(R_1, \ldots, R_K)$构成的是一个区域，而非单一工作点。为说明这一现象，考虑 $\mathbb{F}_3$：服务器希望获得 $W_1 + W_2 + W_3$，同时不获取关于 $W_1 + W_3$的任何信息，即$\mathbf{F} = [1\ 1\ 1]$且$\mathbf{G} = [1\ 0\ 1]$。用户1或用户3的个体密钥可以为零，但二者不能同时为零。例如，如第四节的例1所示，方案 $X_1 = W_1$，$X_2 = W_2 + S$，$X_3 = W_3 - S$可实现 $R_1 = 0$ 。尽管有这些观察，元组$(R_1, \ldots, R_K)$的容量区域尚未得到明确刻画。虽然Yuan-Sun [7] 提出了一种可实现聚合方案，用于刻画密钥的最小联合熵，但其结果并未清晰揭示个体密钥率与之对应的关系，而且似乎表明，对所有$k \in [K]$ 而言，条件 $R_k \geq 1$ 都是必要的。

在这项工作中，我们证明该条件实际上并非必要：并非所有用户都必须持有个人密钥。我们刻画了一个新的可达区域，其形式为一个多面体，其顶点为 $(R_1, \ldots, R_K) = (\mathbb{1}(1 \in \mathcal{I}) \ldots, \mathbb{1}(K \in \mathcal{I}))$，其中 $\mathcal{I} \subseteq [K]$ 是任意满足秩增量条件的索引集：

$$\operatorname{rank}\left([\mathbf{F}_\mathcal{I}; \mathbf{G}_\mathcal{I}]\right) = \operatorname{rank}\left(\mathbf{F}_\mathcal{I}\right) + N, \tag{1}$$

其中 $\mathbf{F}_\mathcal{I}$ 和 $\mathbf{G}_\mathcal{I}$ 是由索引为 $\mathcal{I}$ 的列构成的矩阵。我们证明，每个这样的顶点都可通过一种线性编码方案实现，其中采用编码矩阵将源密钥映射为个人密钥。此外，我们建立了一个逆向界，证明这些顶点是容量区域的角点，因此在最小化必须存储个人密钥的用户数量方面是最优的。这一结果揭示了一种此前未曾探索的

向量线性安全聚合中用户角色的不对称性，并严格扩大了目前已知的最佳可达区域。

记号：对于正整数 M，$[M]$ 表示集合$\{1,\ldots,M\}$。对于整数 a和 b，$[a:\ b]$表示 $\{a,\ldots,b\}$。$A_{[M]}$是 $\{A_1,A_2,\ldots,A_M\}$的紧凑记法。$\mathbb{F}_q$表示阶为 q 的有限域，其中 $q=p^r$，且 p 为素数，r 为正整数。符号 $\triangleq$ 表示“定义为”。$\mathbb{F}_q^{a\times b}$是元素属于 $\mathbb{F}_q$ 的 $a\times b$ 矩阵集合。$\mathbf{I}_a$ 是一个 $a\times a$ 单位矩阵，而 $\mathbf{0}_{a\times b}$ 是 $a\times b$ 全零矩阵。$\mathbb{1}(\cdot)$ 表示指示函数。conv(·) 表示凸包。对于矩阵 $\mathbf{A}$，rowspan(**A**) 和 colspan(**A**) 分别表示由 $\mathbf{A}$ 的行和列张成的向量子空间。对于集合 $\mathcal{I}$，$|\mathcal{I}|$ 表示其基数。记号 $\mathcal{I}\backslash i$ 表示从 $\mathcal{I}$ 中移除元素i 后得到的集合，而 $\mathcal{I}\setminus\mathcal{J}$表示从 $\mathcal{I}$ 中移除集合 $\mathcal{J}$ 的所有元素后得到的集合。

II. 问题陈述

A. 系统模型

我们考虑一个由 K 个用户和一台服务器组成的分布式系统。每个用户 $k\in[K]$ 持有一个长度为 L 的数据流 $W_k\in\mathbb{F}_q^{1\times L}$，以及一个长度为 L_k 的个人密钥向量 $Z_k\in\mathbb{F}_q^{1\times L_k}$。每个数据流 W_k 在 $\mathbb{F}_q$ 上均匀分布，且数据流 $W_{[K]}$ 与密钥 $Z_{[K]}$相互独立，即

$$H(W_k)=L,\ \forall k\in[K], \tag{2}$$

$$H(W_{[K]},Z_{[K]})=\sum_{k\in[K]}H(W_k)+H(Z_{[K]}). \tag{3}$$

此外，所有个人密钥 $Z_{[K]}$ 均由一个长度为 L_Σ的公共源密钥 $Z_\Sigma\in\mathbb{F}_q^{1\times L_\Sigma}$生成，即

$$H(Z_{[K]}|Z_\Sigma)=0. \tag{4}$$

服务器的目标是计算数据流的一个线性函数 F，同时不获取关于另一个受保护线性函数 G 的任何信息。具体而言，令 $\mathbf{W}\ \triangleq[W_1;\ldots;W_K]\in\mathbb{F}_q^{K\times L}$ 为数据流的行堆叠。服务器旨在计算

$$F\triangleq\mathbf{F}\mathbf{W}\in\mathbb{F}_q^{M\times L}, \tag{5}$$

其中，rank(**F**) $=M$。与此同时，服务器不得获取关于以下内容的任何信息

$$G\triangleq\mathbf{G}\mathbf{W}\in\mathbb{F}_q^{N\times L}, \tag{6}$$

其中 rank(**G**) $=N$。不失一般性，我们作出以下假设：

1) rank($[\mathbf{F};\mathbf{G}]$) $=M+N$，确保所需计算 F 与受保护的计算 G线性无关；否则，无法完全保护 G。2) $\mathbf{F}$ 的每一列至少包含一个非零元素；如果某一列全为零，则相应的数据流未被使用，可以从模型中移除。

B. 通信过程

向量安全聚合的通信过程如下。首先，每个用户 $k\in[K]$ 向服务器发送一条长度为 L_X 的消息X_k，其中 X_k 是其本地数据流 W_k 和个人密钥 Z_k的函数，即，

$$H(X_k|W_k,Z_k)=0,\ \forall k\in[K]. \tag{7}$$

收到所有消息 $X_{[K]}$后，服务器必须能够恢复所需的计算结果，即，

$$\text{[Correctness]}\quad H(F|X_{[K]})=0, \tag{8}$$

同时，不向服务器泄露关于 G 的任何信息：

$$\text{[Security]}\quad I(G;X_{[K]}|F)=0. \tag{9}$$

C. 通信率与密钥率

现在，我们定义三个指标，用于评估该模型中的通信成本和密钥分发。

- **通信率：** 定义为每个用户每次聚合发送的符号数，

$$R_X\triangleq\frac{L_X}{L}. \tag{10}$$

- **总密钥率：** 定义为密钥的联合熵（总随机性），

$$R_{Z_\Sigma}\triangleq\frac{L_{Z_\Sigma}}{L}. \tag{11}$$

- **个体密钥率元组：** 规定每次聚合所使用的个体密钥长度，

$$(R_1,R_2,\ldots,R_K)\triangleq\left(\frac{L_1}{L},\frac{L_2}{L},\ldots,\frac{L_K}{L}\right). \tag{12}$$

如果存在一个通信方案和码块长度 L，使得使用个体密钥元组（LR_1，...，LR_K）时满足正确性和安全约束，则称个体密钥率元组（R_1，...，R_K）是可达的。此外，如果某个区域 $\mathfrak{R}_{\mathsf{achi}}$中的每个元组都是可达的，则称该区域 $\mathfrak{R}_{\mathsf{achi}}$是可达区域。最后，容量区域定义为所有可达个体密钥率元组集合的闭包。

Yuan-Sun [7] 证明了，在秩($[\mathbf{F};\ \mathbf{G}]$) $=M+N$的情况下，最优（最小）通信率 R_X^* 为 1，最优总密钥率 $R_{Z_\Sigma}^*$ 为 N。然而，他们的工作并未对个体密钥率元组的可达区域作出明确刻画。在本文中，我们引入一个新的可达区域 $\mathfrak{R}_{\mathsf{achi}}$，并证明了其在某些情况下的最优性。

III. 主要结果

定理 1. 设$\mathbf{F}\in\mathbb{F}_q^{M\times K}$和$\mathbf{G}\in\mathbb{F}_q^{N\times K}$为满足秩 $([\mathbf{F};\ \mathbf{G}])=M+N$的任意两个矩阵。以下个体密钥率区域是可实现的，

$$\mathfrak{R}_{\mathsf{achi}}=\mathsf{conv}\left(\bigcup_{\substack{\mathcal{I}\subseteq[K],\\ \mathrm{rank}([\mathbf{F}_{\mathcal{I}};\mathbf{G}_{\mathcal{I}}])=\mathrm{rank}(\mathbf{F}_{\mathcal{I}})+N}}\mathfrak{R}_{\mathcal{I}}\right), \tag{13}$$

其中

$$\mathfrak{R}_{\mathcal{I}} \triangleq \left\{(R_1,\ldots,R_K)\in\mathbb{R}_+^K \mid R_i\geq 1,\ \forall i\in\mathcal{I}\right\}. \quad (14)$$

定理 1 的证明通过第 V 节中的一般可达性方案给出。

注 1. 区域 $\mathfrak{R}_{\text{achi}}$ 是一个凸多面体，其顶点为向量 $(R_1,\ldots,R_K)=(\mathbb{1}(k\in\mathcal{I}),\ldots,\mathbb{1}(K\in\mathcal{I}))$，其中索引集 $\mathcal{I}$ 满足秩增量条件，$\text{rank}([\mathbf{F}_{\mathcal{I}};\mathbf{G}_{\mathcal{I}}])=\text{rank}(\mathbf{F}_{\mathcal{I}})+N$。通过显式构造一个实现每个此类顶点的方案，并采用时分复用，整个区域 $\mathfrak{R}_{\text{achi}}$ 均可达。

由于秩增量条件在我们的结果中起着至关重要的作用，接下来我们将进一步分析这一条件。

注 2. 满足秩增量条件的索引集族是向上封闭的：若 $\mathcal{I}$ 满足该条件且 $\mathcal{I}\subseteq\mathcal{J}$，则 $\mathcal{J}$ 也满足该条件，且 $\mathfrak{R}_{\mathcal{J}}\subseteq\mathfrak{R}_{\mathcal{I}}$。因此，按包含关系极小的索引集 $\mathcal{I}^*\subseteq[K]$ 决定了该区域的顶点。这里，“按包含关系极小”是指移除任意元素 $i\in\mathcal{I}^*$ 都会导致条件不再成立，即

$$\text{rank}([\mathbf{F}_{\mathcal{I}^*\setminus\{i\}};\mathbf{G}_{\mathcal{I}^*\setminus\{i\}}])<\text{rank}(\mathbf{F}_{\mathcal{I}^*\setminus\{i\}})+N. \quad (15)$$

注 3. 秩增量条件也可以等价地表述为

$$\text{rank}(\mathbf{G}_{\mathcal{I}})=N,\ \text{rowspan}(\mathbf{F}_{\mathcal{I}})\cap\text{rowspan}(\mathbf{G}_{\mathcal{I}})=\{0\}, \quad (16)$$

这可由以下事实推出：

$$\text{rank}([\mathbf{F}_{\mathcal{I}};\mathbf{G}_{\mathcal{I}}])\leq\text{rank}(\mathbf{F}_{\mathcal{I}})+\text{rank}(\mathbf{G}_{\mathcal{I}})\leq\text{rank}(\mathbf{F}_{\mathcal{I}})+N. \quad (17)$$

(16) 的操作性解释如下。当个体密钥被专门分配给集合 $\mathcal{I}$ 中的用户时（即只有 $\mathcal{I}$ 中的数据流受到保护），*(16)* 中的第一个条件确保受保护子空间 行空间$(\mathbf{G}_{\mathcal{I}})$张成一个 N 维子空间；第二个条件则保证行空间$(\mathbf{F}_{\mathcal{I}})$中泄露的信息与行空间$(\mathbf{G}_{\mathcal{I}})$中的受保护信息相互独立。

现在我们分析满足秩增量条件的索引集 $\mathcal{I}$ 的大小。首先，注意到

$$|\mathcal{I}|\geq\text{rank}([\mathbf{F}_{\mathcal{I}};\mathbf{G}_{\mathcal{I}}])=N+\text{rank}(\mathbf{F}_{\mathcal{I}}). \quad (18)$$

此外，一个重要的观察是，对于任意按包含关系极小的子集 $\mathcal{I}^*$，(18) 中的等式均成立；也就是说，矩阵 $[\mathbf{F}_{\mathcal{I}^*};\mathbf{G}_{\mathcal{I}^*}]$ 列满秩。这一点可形式化为以下定理。

定理 2. 任何满足秩增量条件的按包含关系极小子集 $\mathcal{I}^*$ 也满足

$$|\mathcal{I}^*|=N+\text{rank}(\mathbf{F}_{\mathcal{I}^*}). \quad (19)$$

定理 2 的证明见附录 A。

接下来，我们给出一个逆向结果，用以刻画 $\mathfrak{R}_{\text{achi}}$ 的顶点。

定理 3. 对于索引集 $\mathcal{I}\subseteq[K]$，如果仅向 $\mathcal{I}$ 中的用户分配个人密钥，那么 $\mathcal{I}$ 必须满足秩增量条件。此外，如果 $\mathcal{I}$ 也按包含关系极小，那么

$$R_i\geq 1,\quad \forall i\in\mathcal{I}. \quad (20)$$

定理 3 的证明见附录 B。

注 4。 定理 *3* 表明，秩增量条件对于持有密钥的用户集合是必要的。此外，当密钥仅分配给按包含关系极小的集合 $\mathcal{I}^*$ 中的用户时，每个此类用户必须在每次聚合中持有一个符号密钥。因此，$\mathfrak{R}_{\text{achi}}$ 的顶点，即 $(R_1、...、R_K)=(\mathbb{1}(1\in\mathcal{I}^*)...、\mathbb{1}(K\in\mathcal{I}^*))$，也是容量区域的角点。

注 5。 作为一个特殊情形，考虑 *[6]*，中研究的安全求和问题，其中 $\mathbf{F}=[1,1,\ldots,1]$ 且 $\mathbf{G}=\mathbf{I}_K$。在此设置下，$\mathbf{G}$ 的任意一行都可以删除，因为它可以表示为$\mathbf{G}$其余各行与$\mathbf{F}$各行的线性组合。根据定理 *1*，满足秩增量条件的唯一索引集是 $[K]$，从而得到可达区域

$$\mathfrak{R}_{\text{achi}}=\mathfrak{R}_{[K]}=\{(R_1,\ldots,R_K)\mid R_k\geq 1,\ \forall k\in[K]\}. \quad (21)$$

这与 *[6]* 中刻画的容量区域完全一致。因此，本文推导出的区域可简化为安全求和问题中已知的容量区域。

IV. 说明性示例

下面给出示例，以说明可达区域的描述以及相应可达方案的设计。

例1。 考虑 $K=3$ 个用户，其数据流为 W_1、W_2、$W_3\in\mathbb{F}_3$。服务器希望计算 $W_1+W_2+W_3$，同时不获知关于 W_1+W_3 的任何信息，即相应的计算矩阵为

$$\mathbf{F}=\begin{bmatrix}1 & 1 & 1\end{bmatrix},\quad \mathbf{G}=\begin{bmatrix}1 & 0 & 1\end{bmatrix}. \quad (22)$$

为应用定理 *1*，满足秩增量条件的索引集为

$$\mathcal{I}_1=\{1,2\},\quad \mathcal{I}_2=\{2,3\},\quad \mathcal{I}_3=\{1,2,3\}. \quad (23)$$

例如，我们可以验证 $\mathcal{I}_1$ 满足该条件：

$$\text{rank}(\mathbf{F}_{\{1,2\}};\mathbf{G}_{\{1,2\}})=2=\text{rank}\left(\mathbf{F}_{\{1,2\}}\right)+1. \quad (24)$$

然后，我们可以构造一个实现元组 $(R_1,R_2,R_3)=(\mathbb{1}(1\in\mathcal{I}_1),\mathbb{1}(2\in\mathcal{I}_1),\mathbb{1}(3\in\mathcal{I}_1))=(1,1,0)$ 的线性方案。设 $S\in\mathbb{F}_3$ 是一个与 $W_{[3]}$ 相互独立且均匀分布的源密钥。用户发送

$$X_1=W_1+S,\ X_2=W_2-S,\ X_3=W_3. \quad (25)$$

该方案的正确性验证如下：

$$W_1+W_2+W_3=X_1+X_2+X_3, \quad (26)$$

且安全约束由以下条件满足

$$
\begin{aligned}
&I(W_1+W_3;X_{[3]}|W_1+W_2+W_3)\\
&=H(X_{[3]},W_1+W_2+W_3)-H(W_1+W_2+W_3)\\
&\quad-H(X_{[3]}|W_1+W_2+W_3,W_1+W_3) &(27)\\
&=3-1-H(X_{[3]},X_1+X_3|W_1+W_2+W_3,W_1+W_3) &(28)\\
&=2-H(X_{[3]},S|W_1+W_2+W_3,W_1+W_3) &(29)\\
&=2-H(W_{[3]},S|W_1+W_2+W_3,W_1+W_3) &(30)\\
&=2-H(S)-H(W_{[3]}|W_1+W_2+W_3,W_1+W_3) &(31)\\
&=2-1-1=0, &(32)
\end{aligned}
$$

其中，式（*28*）是因为 $H(X_{[3]},W_1+W_2+W_3)=H(X_{[3]})+H(W_1+W_2+W_3|X_{[3]})=H(X_{[3]})=3$，而式（*31*）则是由于 S 和 $W_{[3]}$之间相互独立。

按照相同的步骤，个体密钥速率元组$(0,\ 1,\ 1)$和$(1,\ 1,\ 1)$也都是可达的。因此，以下包含更多随机性的区域也是可达的：

$$\mathfrak{R}_{\mathcal{I}_1}=\{(R_1,R_2,R_3)\in\mathbb{R}_+^3\mid R_1\geq 1,R_2\geq 1\},\tag{33}$$
$$\mathfrak{R}_{\mathcal{I}_2}=\{(R_1,R_2,R_3)\in\mathbb{R}_+^3\mid R_2\geq 1,R_3\geq 1\},\tag{34}$$
$$\mathfrak{R}_{\mathcal{I}_3}=\{(R_1,R_2,R_3)\in\mathbb{R}_+^3\mid R_1\geq 1,R_2\geq 1,R_3\geq 1\}.\tag{35}$$

由于 $\mathfrak{R}_{\mathcal{I}_3}\subseteq\mathfrak{R}_{\mathcal{I}_1}$ 和 $\mathfrak{R}_{\mathcal{I}_3}\subseteq\mathfrak{R}_{\mathcal{I}_2}$，可达区域由凸包给出

$$
\begin{aligned}
\mathfrak{R}_{\mathsf{achi}}&=\mathsf{conv}\left(\mathfrak{R}_{\mathcal{I}_1}\cup\mathfrak{R}_{\mathcal{I}_2}\right) &(36)\\
&=\left\{(R_1,R_2,R_3)\in\mathbb{R}_+^3\,\middle|\,\begin{array}{l}R_2\geq 1,\\ R_1+R_3\geq 1\end{array}\right\}. &(37)
\end{aligned}
$$

区域 $\mathfrak{R}_{\mathsf{achi}}$ 如图*1*所示。

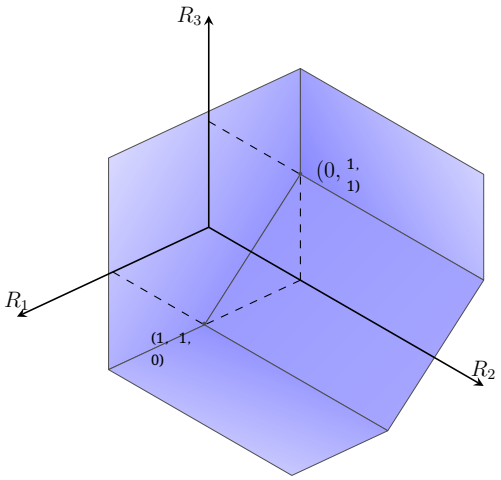

图1。例1的区域。

注6。 该区域背后的直观解释如下。为满足安全要求，W_1+W_3必须受到保护，不能泄露给服务器。同时，正确性要求允许服务器恢复 $W_1+W_2+W_3$。因此，W_2 应由用户2的个人密钥加以掩蔽，这意味着 $R_2\geq 1$。

另一方面，为了让服务器正确解码所需的和，注入 X_2 的噪声必须在服务器处抵消。这种抵消只能通过用户1 和3贡献的噪声来实现。因此，用户1 和3 提供的噪声总量必须至少为一1，由此得到约束 $R_1+R_3\geq 1$。

注7。 回顾注 *1*，$\mathfrak{R}_{\mathsf{achi}}$ 的顶点由按包含关系极小的索引集诱导。在此例中，这些集合为 $\mathcal{I}_1$ 和 $\mathcal{I}_2$。集合 $\mathcal{I}_3$ 并非按包含关系极小，因为移除元素1 或3 中的任意一个都不会违反秩增量条件。因此，分别对应于 $\mathcal{I}_1$和 $\mathcal{I}_2$的速率元组$(1,\ 1,\ 0)$和$(0,\ 1,\ 1)$构成该区域的顶点，如图*1*所示。此例说明，在刻画可达区域时，只需关注按包含关系极小的索引集，而非所有满足秩增量条件的索引集。

例2。 （*Yuan-Sun [7]*中的例*2*）在 $\mathbb{F}_7$中，令

$$\mathbf{F}=\begin{bmatrix}1&0&5&5&3&5\\0&1&5&6&0&3\end{bmatrix},\tag{38}$$

$$\mathbf{G}=\begin{bmatrix}3&0&1&4&2&4\\2&2&1&3&5&3\\1&1&3&4&3&1\end{bmatrix}.\tag{39}$$

注意，$\mathbf{G}$的最后一行是$\mathbf{F}$各行之和。因此，该行无法受到保护，可以在不失一般性的情况下将其删除。此外，通过使用$\mathbf{F}$的各行进行行变换，受保护的计算等价于

$$\mathbf{G}'=\begin{bmatrix}0&0&0&1&0&1\\0&0&1&0&3&3\end{bmatrix}.\tag{40}$$

满足秩增量条件的包含关系下极小索引集为

$$
\begin{aligned}
&\mathcal{I}_1=\{1,2,3,4\},\ \mathcal{I}_2=\{1,2,3,6\},\ \mathcal{I}_3=\{1,2,4,5\},\\
&\mathcal{I}_4=\{1,2,4,6\},\ \mathcal{I}_5=\{1,2,5,6\},\ \mathcal{I}_6=\{1,3,4,5\},\\
&\mathcal{I}_7=\{1,3,4,6\},\ \mathcal{I}_8=\{1,3,5,6\},\ \mathcal{I}_9=\{1,4,5,6\},\\
&\mathcal{I}_{10}=\{2,3,4,5\},\ \mathcal{I}_{11}=\{2,3,4,6\},\ \mathcal{I}_{12}=\{2,3,5,6\},\\
&\mathcal{I}_{13}=\{2,4,5,6\},\ \mathcal{I}_{14}=\{3,4,5,6\}. &(41)
\end{aligned}
$$

对于索引集 $\mathcal{I}_1$，我们设计如下方案。存在一个矩阵 $\mathbf{P}\in\mathbb{F}_7^{6\times 2}$，其定义为

$$\mathbf{P}=\begin{bmatrix}2&2&1&0&0&0\\2&1&0&1&0&0\end{bmatrix}^T,\tag{42}$$

使得

$$\mathbf{FP}=\mathbf{0}_{2\times 2},\quad \mathrm{rank}(\mathbf{G}'\mathbf{P})=2.\tag{43}$$

于是，线性编码方案由以下内容定义

$$\begin{bmatrix}X_1\\ \vdots\\ X_6\end{bmatrix}=\begin{bmatrix}W_1\\ \vdots\\ W_6\end{bmatrix}+\mathbf{P}\begin{bmatrix}S_1\\ S_2\end{bmatrix}=\begin{bmatrix}W_1+2S_1+2S_2\\ W_2+2S_1+S_2\\ W_3+S_1\\ W_4+S_2\\ W_5\\ W_6\end{bmatrix},\tag{44}$$

其中， S_1 和 S_2 是取值于 $\mathbb{F}_7$且服从均匀分布的独立源密钥。定义 $\mathbf{x} \triangleq [X_1; \cdots; X_6]$ 和 $\mathbf{w} \triangleq [W_1; \cdots; W_6]$。该方案的正确性可由下式验证：

$$\mathbf{Fx} = \mathbf{Fw} + \underbrace{\mathbf{FP}}_{=\mathbf{0}} \begin{bmatrix} S_1 \\ S_2 \end{bmatrix} = \mathbf{Fw}. \tag{45}$$

此外，安全约束满足

$$\begin{aligned} & I(\mathbf{Gw}; X_{[6]}|\mathbf{Fw}) = I(\mathbf{G}'\mathbf{w}; X_{[6]}|\mathbf{Fw}) && (46)\\ & = H(X_{[6]}, \mathbf{Fw}) - H(\mathbf{Fw}) - H(X_{[6]}, \mathbf{G}'\mathbf{x}|\mathbf{Fw}, \mathbf{G}'\mathbf{w}) && (47)\\ & = 6 - 2 - H(X_{[6]}, \mathbf{G}'\mathbf{P}[S_1; S_2]|\mathbf{Fw}, \mathbf{G}'\mathbf{w}) && (48)\\ & = 4 - H(W_{[6]}, S_1, S_2|\mathbf{Fw}, \mathbf{G}'\mathbf{w}) && (49)\\ & = 4 - 2 - H(W_{[6]}|\mathbf{Fw}, \mathbf{G}'\mathbf{w}) = 0, && (50) \end{aligned}$$

其中，*(49)* 是因为 秩$(\mathbf{G}'\mathbf{P}) = 2$ 在 *(43)* 中。

对于每个索引集 $\mathcal{I}_j$、 $j \in [14]$，根据 *(13)* 中的速率分配定义一个可达区域$\mathfrak{R}_{\mathcal{I}_j}$ 。通过在这些方案之间进行时分复用，可达区域由下式刻画：

$$\mathfrak{R}_{\mathsf{achi}} = \mathsf{conv}\left(\mathfrak{R}_{\mathcal{I}_1} \cup \mathfrak{R}_{\mathcal{I}_2} \cup \cdots \cup \mathfrak{R}_{\mathcal{I}_{14}}\right). \tag{51}$$

注释8。对于此示例，*Yuan-Sun* 中的方案 *[7]*要求对所有 $k \in [6]$均有 $R_k = 1$，即每个用户都持有一个密钥。相比之下，(44) 中的方案实现了 $(R_1$、...、$R_6) = (1$、1、1、1、0、$0)$，因此并非所有用户都需要持有个体密钥。因此，此处获得的可达区域 $\mathfrak{R}_{\mathsf{achi}}$ 严格更大。

V. 可达性证明

A. 向量线性安全聚合框架

我们提出了一种向量安全线性聚合的通用框架。我们的方案对每个用户只需一个符号，即数据流长度为 $L = 1$。用户发送的消息 $X_{[K]}$可重构为

$$\underbrace{\begin{bmatrix} X_1 \\ X_2 \\ \vdots \\ X_K \end{bmatrix}}_{\triangleq \mathbf{x}} = \underbrace{\begin{bmatrix} W_1 \\ W_2 \\ \vdots \\ W_K \end{bmatrix}}_{\triangleq \mathbf{w}} + \underbrace{\begin{bmatrix} Z_1 \\ Z_2 \\ \vdots \\ Z_K \end{bmatrix}}_{\triangleq \mathbf{z}} = \mathbf{w} + \mathbf{P} \underbrace{\begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ S_N \end{bmatrix}}_{\triangleq \mathbf{s}}, \tag{52}$$

其中， $Z_{[K]}$ 为个体密钥， $S_{[N]}$ 由 N个在 $\mathbb{F}_q$中相互独立且均匀分布的源密钥组成，且$\mathbf{P} \triangleq [\mathbf{p}_1^T; \ldots; \mathbf{p}_K^T] \in \mathbb{F}_q^{K \times N}$是一个编码矩阵，将源密钥 $S_{[N]}$ 映射为个体密钥 $Z_{[K]}$。用户 k 持有的个人密钥为 $Z_k = \mathbf{p}_k^T\mathbf{s}$。该方案在 [7]中实现了最优通信速率 $R_X^* = 1$和最优总密钥率 $R_{Z_\Sigma}^* = N$ 。

在此框架中，个人密钥速率分布完全由编码矩阵$\mathbf{P}$的选择决定。以下引理给出了$\mathbf{P}$ 满足正确性和安全约束的充分条件。

引理1。若编码矩阵$\mathbf{P}$满足以下条件，则式（*52*）中描述的方案满足正确性和安全约束

$$\text{Condition 1}: \mathbf{FP} = \mathbf{0}_{M \times N}, \tag{53}$$

$$\text{Condition 2}: \text{rank}(\mathbf{GP}) = N. \tag{54}$$

证明。对于正确性，服务器将消息 $\mathbf{x}$处理为$\mathbf{Fx} = \mathbf{Fw} + \mathbf{FPx} = \mathbf{Fw}$，这可由（53）中的条件 1 得出。对于安全约束，我们有

$$\begin{aligned} & I(\mathbf{Gw}; X_{[K]}|\mathbf{Fw}) \\ & = H(X_{[K]}|\mathbf{Fw}) - H(X_{[K]}|\mathbf{Fw}, \mathbf{Gw}) && (55)\\ & = H(X_{[K]}, \mathbf{Fw}) - H(\mathbf{Fw}) - H(X_{[K]}, \mathbf{Gx}|\mathbf{Fw}, \mathbf{Gw}) && (56)\\ & = K - M - H(X_{[K]}, \mathbf{Gw} + \mathbf{GPs}|\mathbf{Fw}, \mathbf{Gw}) && (57)\\ & = K - M - H(X_{[K]}, \mathbf{GPs}|\mathbf{Fw}, \mathbf{Gw}) && (58)\\ & = K - M - H(\mathbf{s}) - H(W_{[K]}|\mathbf{Fw}, \mathbf{Gw}) && (59)\\ & = K - M - N - (K - M - N) = 0, && (60) \end{aligned}$$

其中，（57）中的等式成立是因为 $H(X_{[K]}, \mathbf{Fw}) = H(X_{[K]}) + H(\mathbf{Fw}|X_{[K]}) = K$，而（59）成立是因为（54）中的条件 2。 ■

注9。回顾一下，用户 k 持有的个人密钥为 $Z_k = \mathbf{p}_k^T\mathbf{s}$，其中 $\mathbf{p}_k^T$ 是$\mathbf{P}$的第 k 行。因此，用户 k 的个体密钥率由下式确定：

$$R_k = H(Z_k)/L = \text{rank}(\mathbf{p}_k^T) = \mathbb{1}(\mathbf{p}_k \neq \mathbf{0}). \tag{61}$$

因此，$\mathbf{P}$中存在全零行会直接影响个体密钥率元组。因此，$\mathbf{P}$的设计等价于确定哪些用户持有非零个人密钥，同时满足正确性和安全条件。在下一小节中，我们将建立可行的 $\mathbf{P}$ 与前文引入的秩增量条件之间的精确联系。

B. 编码矩阵的设计

现在我们证明，对于满足秩增量条件的任意索引集 $\mathcal{I} \subseteq [K]$ ，存在一个编码矩阵$\mathbf{P}$，其索引属于 $\mathcal{I}$ 的行均为非零，而其余所有行均为零。

引理 2。对于满足$\text{rank}([\mathbf{F}_\mathcal{I}; \mathbf{G}_\mathcal{I}]) = \text{rank}(\mathbf{F}_\mathcal{I}) + N$的任意索引集 $\mathcal{I} \subseteq [K]$ ，存在一个矩阵 $\bar{\mathbf{P}} \in \mathbb{F}_q^{|\mathcal{I}| \times N}$，使得

$$\mathbf{F}_\mathcal{I}\bar{\mathbf{P}} = \mathbf{0}_{M \times N}, \quad \text{rank}(\mathbf{G}_\mathcal{I}\bar{\mathbf{P}}) = N. \tag{62}$$

引理 2 的证明见附录C。

注 10。该引理表明，只要 $\mathcal{I}$ 满足秩增量条件，就可以构造一个编码矩阵$\mathbf{P}$ ，使得由 $\mathcal{I}$ 索引的行均为非零行，而其余各行恒为零，同时仍满足正确性和安全条件。这样的$\mathbf{P}$ 对应于个体密钥率元组 $(R_1, \cdots, R_K) = (\mathbb{1}(1 \in \mathcal{I}) \cdots, \mathbb{1}(K \in \mathcal{I}))$。因此，每个这样的元组都是可实现的，由这些元组通过时分复用得到的整个多面体区域同样是可实现的。

附录

A. 定理 2 的证明

现在我们通过反证法证明（19）中的等式。假设某个按包含关系极小子集 $\mathcal{I}^*$ 满足 $\text{rank}([\mathbf{F}_{\mathcal{I}^*};\mathbf{G}_{\mathcal{I}^*}]) = N + \text{rank}(\mathbf{F}_{\mathcal{I}^*})$，但 $|\mathcal{I}^*| > N + \text{rank}(\mathbf{F}_{\mathcal{I}^*})$。于是，$[\mathbf{F}_{\mathcal{I}^*};\mathbf{G}_{\mathcal{I}^*}]$ 的列线性相关。因此，存在一个非空子集 $\mathcal{J} \subseteq \mathcal{I}^*$，使得

$$\text{rank}([\mathbf{F}_{\mathcal{I}^*\setminus\mathcal{J}};\mathbf{G}_{\mathcal{I}^*\setminus\mathcal{J}}]) = N + \text{rank}(\mathbf{F}_{\mathcal{I}^*}). \tag{63}$$

由于

$$\begin{aligned}\text{rank}([\mathbf{F}_{\mathcal{I}^*\setminus\mathcal{J}};\mathbf{G}_{\mathcal{I}^*\setminus\mathcal{J}}]) &\le N + \text{rank}(\mathbf{F}_{\mathcal{I}^*\setminus\mathcal{J}}) &(64)\\ &\le N + \text{rank}(\mathbf{F}_{\mathcal{I}^*}), &(65)\end{aligned}$$

由此可得

$$\text{rank}([\mathbf{F}_{\mathcal{I}^*\setminus\mathcal{J}};\mathbf{G}_{\mathcal{I}^*\setminus\mathcal{J}}]) = N + \text{rank}(\mathbf{F}_{\mathcal{I}^*\setminus\mathcal{J}}). \tag{66}$$

这意味着集合 $\mathcal{I}^*\setminus\mathcal{J}$ 也满足秩增量条件。这与假设 $\mathcal{I}^*$ 在包含意义下是极小的相矛盾。因此，式 (19) 中的等号必须成立。

B. 定理 3 的证明

我们首先证明该定理的第一部分。对于任意数据流长度 L，定义 $\mathbf{W} \triangleq [W_1; \cdots; W_K] \in \mathbb{F}_q^{K\times L}$。当只有索引集 $\mathcal{I}$ 中的用户持有密钥时，对于每个 $\ell \in [K]\setminus\mathcal{I}$，传输符号 X_ℓ 是 W_ℓ 的确定性函数，因此

$$H(X_\ell|W_\ell) = 0, \quad \forall \ell \in [K]\setminus\mathcal{I}. \tag{67}$$

此外，[7] 中已证明 $H(X_\ell) \ge L$。由于 $H(W_\ell) = L$，我们有

$$L \le H(X_\ell) - H(X_\ell|W_\ell) = H(W_\ell) - H(W_\ell|X_\ell) \le L, \tag{68}$$

这意味着 $H(W_\ell|X_\ell) = 0,\ \forall \ell \in [K]\setminus\mathcal{I}$。现在，根据安全约束，

$$I(\mathbf{GW}; X_{[K]}|\mathbf{FW}) = NL - H(\mathbf{GW}|X_{[K]},\mathbf{FW}) = 0. \tag{69}$$

因此，

$$\begin{aligned}NL &= H(\mathbf{GW}|X_{[K]},\mathbf{FW}) &(70)\\ &= H(\mathbf{GW}|X_{\mathcal{I}}, W_{[K]\setminus\mathcal{I}}, \mathbf{F}_{\mathcal{I}}\mathbf{W}_{\mathcal{I},:}) &(71)\\ &\le H(\mathbf{G}_{\mathcal{I}}\mathbf{W}_{\mathcal{I},:}|\mathbf{F}_{\mathcal{I}}\mathbf{W}_{\mathcal{I},:}) \le NL, &(72)\end{aligned}$$

其中 $\mathbf{W}_{\mathcal{I},:}$ 表示由索引为 $\mathcal{I}$ 的行组成的子矩阵。由此可得

$$H(\mathbf{G}_{\mathcal{I}}\mathbf{W}_{\mathcal{I},:}|\mathbf{F}_{\mathcal{I}}\mathbf{W}_{\mathcal{I},:}) = NL. \tag{73}$$

由于 $\mathbf{W}_{\mathcal{I},:}$ 在 $\mathbb{F}_q$ 上服从均匀分布，上述等式等价于

$$\text{rank}([\mathbf{F}_{\mathcal{I}};\mathbf{G}_{\mathcal{I}}]) = N + \text{rank}(\mathbf{F}_{\mathcal{I}}). \tag{74}$$

即，$\mathcal{I}$ 满足秩增量条件。

现在证明定理的第二部分。假设 $\mathcal{I}^* \subseteq [K]$ 满足秩增量条件，且按包含关系极小。对于任意 $i \in \mathcal{I}^*$，定义 $\mathcal{I}' \triangleq \mathcal{I}^*\setminus\{i\}$。由 $\mathcal{I}^*$ 的极小性可知，

$$\text{rank}([\mathbf{F}_{\mathcal{I}'};\mathbf{G}_{\mathcal{I}'}]) < \text{rank}(\mathbf{F}_{\mathcal{I}'}) + N. \tag{75}$$

回顾式（16）中秩增量条件的等价刻画，以下两种情况至少有一种成立：

- **Case 1**: $\text{rowspan}(\mathbf{F}_{\mathcal{I}'}) \cap \text{rowspan}(\mathbf{G}_{\mathcal{I}'}) \neq \{0\}$.
- **情况 2**: 秩 $\text{rk}(\mathbf{G}) \le N-1$。

接下来我们证明，在任一情况下，都有 $R_i \ge 1$。

在**情况 1**，$\mathbf{1} \in \mathbb{F}_q^{N\times 1}$ 中，存在非零向量 $\mathbf{b}$ 和 $\mathbf{c}$，使得

$$\mathbf{b}^T\mathbf{G}_{\mathcal{I}'} = \mathbf{c}^T\mathbf{F}_{\mathcal{I}'} \triangleq \mathbf{a}^T \neq \mathbf{0}, \quad \mathbf{b}^T\mathbf{G}_{\mathcal{I}^*} \neq \mathbf{c}^T\mathbf{F}_{\mathcal{I}^*}, \tag{76}$$

这也意味着

$$\mathbf{b}^T\mathbf{G}_{\{i\}} \neq \mathbf{c}^T\mathbf{F}_{\{i\}}. \tag{77}$$

于是，由式（70）–（72）可得

$$\begin{aligned}NL &= H(\mathbf{GW}|\mathbf{F}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}, X_{\mathcal{I}^*}, W_{[K]\setminus\mathcal{I}^*}) &(78)\\ &= H(\mathbf{G}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}|\mathbf{F}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}, X_{\mathcal{I}^*}, W_{[K]\setminus\mathcal{I}^*}) &(79)\\ &\le H(\mathbf{G}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}|\mathbf{F}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}, X_{\mathcal{I}^*}) \le NL, &(80)\end{aligned}$$

这意味着

$$H(\mathbf{G}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}|\mathbf{F}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}, X_{\mathcal{I}^*}) = NL. \tag{81}$$

因此，

$$\begin{aligned}&I(\mathbf{G}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}; \mathbf{F}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}, X_{\mathcal{I}^*})\\ &= H(\mathbf{G}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}) - H(\mathbf{G}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}|\mathbf{F}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}, X_{\mathcal{I}^*}) &(82)\\ &= H(\mathbf{G}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}) - NL = 0. &(83)\end{aligned}$$

由于 $i \in \mathcal{I}^*$，我们有 $I(\mathbf{G}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}; \mathbf{F}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}, X_i) = 0$，因此，

$$\begin{aligned}0 &= I(\mathbf{b}^T\mathbf{G}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}; \mathbf{c}^T\mathbf{F}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}, X_i) &(84)\\ &= I(\mathbf{a}^T\mathbf{W}_{\mathcal{I}',:} + \mathbf{b}^T\mathbf{G}_{\{i\}}W_i; \mathbf{a}^T\mathbf{W}_{\mathcal{I}',:} + \mathbf{c}^T\mathbf{F}_{\{i\}}W_i, X_i). &(85)\end{aligned}$$

因此，我们有

$$I(\mathbf{a}^T\mathbf{W}_{\mathcal{I}',:} + \mathbf{b}^T\mathbf{G}_{\{i\}}W_i; X_i|\mathbf{a}^T\mathbf{W}_{\mathcal{I}',:} + \mathbf{c}^T\mathbf{F}_{\{i\}}W_i) = 0. \tag{86}$$

由此可得

$$\begin{aligned}&H((\mathbf{b}^T\mathbf{G}_{\{i\}} - \mathbf{c}^T\mathbf{F}_{\{i\}})W_i|\mathbf{a}^T\mathbf{W}_{\mathcal{I}',:} + \mathbf{c}^T\mathbf{F}_{\{i\}}W_i)\\ &- H((\mathbf{b}^T\mathbf{G}_{\{i\}} - \mathbf{c}^T\mathbf{F}_{\{i\}})W_i|X_i, \mathbf{a}^T\mathbf{W}_{\mathcal{I}',:} + \mathbf{c}^T\mathbf{F}_{\{i\}}W_i)\\ &= L - H((\mathbf{b}^T\mathbf{G}_{\{i\}} - \mathbf{c}^T\mathbf{F}_{\{i\}})W_i|X_i, \mathbf{a}^T\mathbf{W}_{\mathcal{I}',:} + \mathbf{c}^T\mathbf{F}_{\{i\}}W_i) &(87)\\ &= 0, &(88)\end{aligned}$$

这意味着

$$\begin{aligned}L &= H((\mathbf{b}^T\mathbf{G}_{\{i\}} - \mathbf{c}^T\mathbf{F}_{\{i\}})W_i|X_i, \mathbf{a}^T\mathbf{W}_{\mathcal{I}',:} + \mathbf{c}^T\mathbf{F}_{\{i\}}W_i) &(89)\\ &\le H((\mathbf{b}^T\mathbf{G}_{\{i\}} - \mathbf{c}^T\mathbf{F}_{\{i\}})W_i|X_i) \le L. &(90)\end{aligned}$$

回顾（77）式，$\mathbf{b}^T\mathbf{G}^{\{i\}} - \mathbf{c}^T\mathbf{F}_{\{i\}} \neq 0$，进而$H(W_i|X_i) = L$。因此，

$$H(Z_i) \geq H(X_i|W_i) \tag{91}$$
$$= H(X_i) + H(W_i|X_i) - H(W_i) \tag{92}$$
$$= H(X_i) \geq L, \tag{93}$$

其中，(91) 是因为 $H(X_i|W_i, Z_i) = 0$。因此，$R_i = L_i/L \geq H(Z_i)/L \geq 1$。

在**情况 2**中，由 (73) 可得

$$NL = H(\mathbf{G}_{\mathcal{I}^*}\mathbf{W}_{\mathcal{I}^*,:}|X_{\mathcal{I}^*}) \tag{94}$$
$$\leq H(\mathbf{G}_{\mathcal{I}'}\mathbf{W}_{\mathcal{I}',:}|X_{\mathcal{I}^*}) + H(\mathbf{G}_{\{i\}}W_i|X_{\mathcal{I}^*}) \tag{95}$$
$$\leq (N-1)L + H(\mathbf{G}_{\{i\}}W_i|X_i) \tag{96}$$
$$\leq (N-1)L + H(W_i|X_i), \tag{97}$$

然后

$$R_i \geq H(W_i|X_i)/L \geq 1. \tag{98}$$

因此，两种情况均可得 $R_i \geq 1$，$\forall i \in \mathcal{I}^*$，证明完成。

C. 引理 2 的证明

设 $r \triangleq$秩$(\mathbf{F}_{\mathcal{I}})$。$\mathbf{F}_{\mathcal{I}}$ 的零空间定义为

$$\mathcal{N}(\mathbf{F}_{\mathcal{I}}) \triangleq \{\mathbf{x} \in \mathbb{F}_q^{|\mathcal{I}|} | \mathbf{F}_{\mathcal{I}}\mathbf{x} = \mathbf{0}\}. \tag{99}$$

令$\mathbf{U} \in \mathbb{F}_q^{|\mathcal{I}|\times(|\mathcal{I}|-r)}$为任意一个矩阵，其列构成 $\mathcal{N}(\mathbf{F}_{\mathcal{I}})$的一组基。这意味着$\mathbf{F}_{\mathcal{I}}\mathbf{U} = \mathbf{0}$。因此，对于任意矩阵$\bar{\mathbf{P}}$，若其各列属于 $\mathcal{N}(\mathbf{F}_{\mathcal{I}})$，则有$\mathbf{F}_{\mathcal{I}}\bar{\mathbf{P}} = \mathbf{0}$。接下来只需证明我们可以选取 N 这样的列，使得秩$(\mathbf{G}_{\mathcal{I}}\bar{\mathbf{P}}) = N$。我们先证明以下秩分解恒等式。

断言 1. 对于任意矩阵$\mathbf{A} \in \mathbb{F}_q^{a\times m}$和$\mathbf{B} \in \mathbb{F}_q^{b\times m}$，

$$\text{rank}([\mathbf{A};\mathbf{B}]) = \text{rank}(\mathbf{A}) + \dim(\mathbf{B}\mathcal{N}(\mathbf{A})), \tag{100}$$

其中$\mathbf{B}\mathcal{N}(\mathbf{A}) \triangleq \{\mathbf{B}\mathbf{x} | \mathbf{x} \in \mathcal{N}(\mathbf{A})\}$。

证明。 考虑由 $T : \mathbb{F}_q^m \to \mathbb{F}_q^{a+b}$定义的线性映射

$$T(\mathbf{x}) = [\mathbf{A};\mathbf{B}]\mathbf{x} = \begin{bmatrix}\mathbf{A}\mathbf{x}\\ \mathbf{B}\mathbf{x}\end{bmatrix}. \tag{101}$$

令 V 表示 T的像，即

$$V \triangleq \text{Im}(T) = \left\{ \begin{bmatrix}\mathbf{A}\mathbf{x}\\ \mathbf{B}\mathbf{x}\end{bmatrix} \,\middle|\, \mathbf{x} \in \mathbb{F}_q^m \right\}. \tag{102}$$

定义投影映射 $\pi : V \to$ Im$(\mathbf{A})$如下：

$$\pi\left(\begin{bmatrix}\mathbf{A}\mathbf{x}\\ \mathbf{B}\mathbf{x}\end{bmatrix}\right) = \mathbf{A}\mathbf{x}. \tag{103}$$

因此，π 是线性的且为满射，其核为

$$\ker(\pi) = \left\{ \begin{pmatrix}\mathbf{A}\mathbf{x}\\ \mathbf{B}\mathbf{x}\end{pmatrix} \in V \,\middle|\, \mathbf{A}\mathbf{x} = \mathbf{0} \right\} = \left\{ \begin{bmatrix}\mathbf{0}\\ \mathbf{B}\mathbf{x}\end{bmatrix} \,\middle|\, \mathbf{x} \in \mathcal{N}(\mathbf{A}) \right\}. \tag{104}$$

现在，定义线性映射 ϕ：$\mathbf{B}\mathcal{N}(\mathbf{A}) \to \ker(\pi)$，其定义为

$$\phi(\mathbf{B}\mathbf{x}) = \begin{bmatrix}\mathbf{0}\\ \mathbf{B}\mathbf{x}\end{bmatrix}, \quad \mathbf{x} \in \mathcal{N}(\mathbf{A}). \tag{105}$$

映射 ϕ 是良定义的、线性的、单射且满射。因此，ϕ是一个同构，并且

$$\dim(\ker(\pi)) = \dim(\mathbf{B}\mathcal{N}(\mathbf{A})). \tag{106}$$

应用秩-零化度定理 [12]，我们得到

$$\dim(V) = \dim(\text{Im}(\pi)) + \dim(\ker(\pi)) \tag{107}$$
$$= \dim(\text{Im}(\mathbf{A})) + \dim(\mathbf{B}\mathcal{N}(\mathbf{A})). \tag{108}$$

由此可得

$$\text{rank}([\mathbf{A};\mathbf{B}]) = \text{rank}(\mathbf{A}) + \dim\left(\mathbf{B}\mathcal{N}(\mathbf{A})\right), \tag{109}$$

这就证明了该断言。 ■

现在，应用断言 1，我们有

$$\text{rank}([\mathbf{F}_{\mathcal{I}};\mathbf{G}_{\mathcal{I}}]) = \text{rank}(\mathbf{F}_{\mathcal{I}}) + \dim(\mathbf{G}_{\mathcal{I}}\mathcal{N}(\mathbf{F}_{\mathcal{I}})). \tag{110}$$

根据引理 2 中的假设，可得 $\dim(\mathbf{G}_{\mathcal{I}}\mathcal{N}(\mathbf{F}_{\mathcal{I}})) = N$。由于 colspan$(\mathbf{U}) = \mathcal{N}(\mathbf{F}_{\mathcal{I}})$，因此有$\mathbf{G}_{\mathcal{I}}\mathcal{N}(\mathbf{F}_{\mathcal{I}}) =$ colspan$(\mathbf{G}_{\mathcal{I}}\mathbf{U})$，从而 rank$(\mathbf{G}_{\mathcal{I}}\mathbf{U}) = N$。因此，$\mathbf{G}_{\mathcal{I}}\mathbf{U}$ 有 N 个线性无关列，其索引为$j_1, \ldots, j_N$。我们定义

$$\bar{\mathbf{P}} \triangleq [\mathbf{U}_{:,j_1} \cdots \mathbf{U}_{:,j_N}] \in \mathbb{F}_q^{|\mathcal{I}|\times N}. \tag{111}$$

因此，rank$(\mathbf{G}_{\mathcal{I}}\bar{\mathbf{P}}) = N$ 且 $\mathbf{F}_{\mathcal{I}}\bar{\mathbf{P}} = \mathbf{0}$，因为 $\bar{\mathbf{P}}$ 由 $\mathcal{N}(\mathbf{F}_{\mathcal{I}})$ 中的列构成，这证明了引理 2。

参考文献

[1] R. Schlegel、S. Kumar、E. Rosnes 和 A. G. I. Amat。CodedPaddedFL 和 CodedSecAgg：联邦学习中的掉队者缓解与安全聚合。*IEEE*通信汇刊，71(4):2013– 2027，2023年4月。[2] J. So、C. He、C.-S. Yang、S. Li、Q. Yu、R. E. Ali、B. Guler 和 S. Avestimehr。LightSecAgg：一种用于联邦学习的轻量且多用途的安全聚合设计。机器学习与系统会议论文集，4:694–720，2022年3月。[3] J. Koneˇcn`y、H B. McMahan、F. X Yu、P. Richtárik、A. T. Suresh 和 D. Bacon。联邦学习：提升通信效率的策略。在线参见 arXiv:1610.05492。[4] S. Ulukus、S. Avestimehr、M. Gastpar、S. Jafar、R. Tandon 和 C. Tian。隐私检索、计算与学习：近期进展与未来挑战。*IEEE*通信选题领域期刊，40(3):729–748，2022年3月。[5] K. Wan、X. Yao、H. Sun、M. Ji 和 G. Caire。关于采用未编码组密钥的信息论安全聚合。*IEEE*信息论汇刊，70(9):6596–6619，2024年9月。[6] Y. Zhao 和 H. Sun。安全求和：容量区域、组密钥与可行性。*IEEE*信息论汇刊，70(2):1376–1387，2023年12月。[7] X. Yuan 和 H. Sun。向量线性安全聚合。载于*IEEE*国际信息论研讨会，2025年10月。[8] S. Dutta、V. Cadambe 和 P. Grover。Short-dot：使用编码短点积分布式计算大型线性变换。神经信息处理系统进展，29，2016年7月。[9] Y. Bai、X. Guang 和 R. W. Yeung。安全网络函数计算：函数安全。载于 *IEEE*国际信息论研讨会，2024年7月。[10] X. Guang、Y. Bai 和 R. W. Yeung。面向线性函数的安全网络函数计算——第一部分：源安全。*IEEE*信息论汇刊，70(1):676–697，2024年10月。[11] M. Xu、G. Ge 和 M. Liu。具有不同安全条件的网络函数计算。在线参见 arXiv:2206.05468。[12] G. Strang。线性代数及其应用。Academic Press，纽约，2012年。