私密求和计算：通信、随机性与隐私之间的权衡

R´emi A. Chou，J¨org Kliewer，Aylin Yener

arXiv:2602.06238v1 [cs.IT] 5 Feb 2026

摘要——**考虑多个用户和一个融合中心。每个用户持有一个比特序列，并可通过单向公共信道与融合中心通信。融合中心的任务是在满足隐私要求的前提下计算所有序列的和：一组合谋用户与融合中心联合起来，无法通过互信息获知其他用户序列中超过预定数量 δ 的信息。我们的第一项贡献是刻画用户与融合中心之间必要通信量的下限，以及用户所需随机性的下限。我们的第二项贡献是通过证明私密求和计算所需的局部随机性必须借助秘密共享来生成，建立私密求和计算与秘密共享之间的联系，并证明这一结论对任意 $\delta \geqslant 0$ 均成立。**

I. 引言

在安全约束下对分布式求和的研究，与安全聚合问题密切相关，已有包括 [2]–[11]在内的研究对此进行了证明。该研究领域在分布式计算中有着广泛应用。值得注意的是，零信息泄漏的安全求和已得到广泛研究，并在 [6], [12]–[15]中分析了最优的通信和随机性速率。

本文将安全求和计算的范围扩展到允许可控程度的信息泄漏，并建立信息泄漏、通信速率和所需随机性之间的权衡关系。具体而言，我们旨在量化在付出可控隐私泄露代价的情况下可实现的通信和随机性收益；这对于通信带宽有限或随机性生成这一资源实现成本高昂的场景尤其重要。更具体地说，我们考虑这样一种情形：有 $L \geqslant 2$ 个用户，每个用户都拥有一个私有序列，融合中心则负责根据每个用户发送的、由其序列编码得到的版本，计算这些序列之和。为此，用户利用共享随机性，本文将其称为全局随机性，但其速率必须最小化。随后，从全局随机性中提取局部随机性，每个用户利用该局部随机性对自己的序列进行编码，然后将其发送给融合中心。隐私要求其目标是确保任意一组规模为 T 的合谋用户（其中 $T \leqslant L-2$ 固定）与融合中心共同参与时，都不能获知关于其他用户序列的超过预定量 δ 的信息。信息泄漏通过条件互信息来衡量，即在给定合谋用户和融合中心掌握的全部信息后，所有编码序列与所有未编码序列之间的条件互信息。此外，受渐进式秘密共享的启发，例如 [16], [17], ，我们引入一种隐私求和设定，其中受控的信息泄漏量对所有用户一视同仁，确保没有用户能够优先访问其他用户的私有数据，并使隐私保证在所有用户和合谋场景下保持一致。

我们的第一项贡献是推导通信量和随机性需求的容量结果。具体而言，我们证明了用户向融合中心进行通信所需的个体速率，以及用户之间所需共享随机性的速率的逆定理结果。这些结果主要通过组合论证得出。当信息泄漏满足对称性假设时，我们还推导了每个用户所需局部随机性个体速率的逆定理结果。此外，我们提出了一种可达方案，可同时达到上述所有逆定理界，从而确立一个容量结果。我们的第二项贡献是揭示秘密共享与隐私求和之间的基本联系。具体而言，我们证明，要实现最优的通信速率和随机性速率，每个用户的局部随机性必须对应于渐进式秘密共享方案中的份额。我们证明，这一条件对于实现最优性既是必要的，也是充分的。

相关工作：与本文最接近的相关工作是 [18],，该文研究了我们设定中的一个特殊情况，其中 (i) 不允许信息泄漏，即 $\delta = 0$；(ii) 所有用户的个体通信速率均相等；(iii) 所有用户的个体局部随机性速率均相等。该特殊情况下的容量区域已在 [18, 定理 1]中确立。当 $\delta = 0$，即不允许信息泄漏时，我们的结果通过在不假设 (ii) 和 (iii) 成立的情况下，为个体用户的通信速率、个体用户的局部随机性速率以及所有用户的本地随机性总速率给出容量结果，从而拓展了 [18,定理 1] 。此外，我们的结果将[18, 定理 1] 拓展到 $\delta > 0$ 的情形，并在不假设 (ii) 和 (iii) 成立的情况下，为个体用户的通信速率、所有用户的本地随机性总速率以及全局随机性速率确立了容量结果。我们的结果还为个体用户的局部随机性确立了容量结果

R´emi A. Chou 任职于德克萨斯大学阿灵顿分校计算机科学与工程系，地址为美国德克萨斯州阿灵顿市 76019。J. Kliewer 任职于新泽西理工学院电气与计算机工程系，地址为美国新泽西州纽瓦克市。Aylin Yener 任职于俄亥俄州立大学电气与计算机工程系，地址为美国俄亥俄州哥伦布市 43210。电子邮箱：remi.chou@uta.edu、jkliewer@njit.edu、yener@ece.osu.edu。本研究的初步版本曾发表于 [1] 举行的 2024 年 IEEE 国际信息论研讨会（ISIT）。本研究部分由美国国家科学基金会（NSF）资助（项目编号 CCF-2201824 和 CCF-2425371），另有部分经费来自 Chope讲席基金。

速率 $\delta > 0$ 在某种信息泄漏对称条件下。定理 1] 的可达性部分还表明，当 $\delta = 0$时，可以采用秘密共享为安全求和生成用户所需的局部随机性。在本研究中，我们通过证明秘密共享不仅足以生成隐私求和达到最优性所需的局部随机性，而且也是必要的，从而确立了安全求和与秘密共享之间更强的联系。此外，除 的情形外，我们还证明，对于任意 $\delta \neq 0$，该结论都成立。

我们注意到，其他研究已在各种设定下探讨了基于任意相关随机性、借助交互式通信进行的安全计算，例如 [19]–[22]。此外，允许信息泄漏的相关随机性计算也在 [23], [24]中得到研究。上述研究与本文的主要区别在于：在我们的设定中，用户可用的共享随机性的结构是编码方案设计的一部分，类似于 [18],；而在 [19]–[24]中，用户可用的共享随机性的统计特性是预先确定的，不属于设计范畴。

本文其余部分组织如下。问题陈述在第II节给出。我们的主要结果总结于第III节。我们的逆定理结果的证明在第IV 节和第V节给出。为生成局部随机性而进行秘密共享的必要性在第VII节给出。最后，结束语在第VIII节给出。

II. 问题陈述

记号：设 $\mathbb{N}$、 $\mathbb{R}$和 $\mathbb{Q}$ 分别为自然数、实数和有理数的集合。对于 a， $b \in \mathbb{R}$，定义$[\![a,\ b]\!] \triangleq [\lfloor a \rfloor, \lceil b \rceil] \cap \mathbb{N}$ 以及 $[a] \triangleq [\![1,\ a]\!]$。指示函数记为 $\mathbb{1}\{\omega\}$，当谓词 ω 为真时其值为1，否则为0。

考虑一个融合中心和 L 个用户，每个用户都拥有各自的私有序列。用户通过单向、公开且无噪声信道与融合中心通信，目的是让融合中心按下文所述计算这些序列的和。

定义 1. 一个$(L, n, (R_l^{(X)})_{l\in[L]}, R^{(U)}, (R_l^{(K)})_{l\in[L]})$私有求和计算协议由以下部分组成：

- L 个用户，索引集合为 $[L]$;
- L 个$(S_l)_{l\in[L]}$独立序列，其中序列 S_l 由用户 $l \in [L]$ 持有，并在有限域 $\mathbb{F}_2^n$ 上均匀分布；
- 一个全局随机性的来源，与序列 $(S_l)_{l\in[L]}$ 相互独立，由 U 描述，并在 $\mathbb{F}^{nR_{(U)}}$ 上均匀分布；
- L 编码函数 e_l：$\mathbb{F}^{nR_{(U)}} \times \mathbb{F}_2^n \to \mathbb{F}_2^{nR_l}$；
- 一个解码函数 d：$\bigtimes_{l\in[L]} \mathbb{F}^{nR_l} \to \mathbb{F}_2^n$；

其运作方式如下：

1) 用户 $l \in [L]$ 接收局部随机性 $K_l \triangleq e_l(U)$；*2)* 用户 $l \in [L]$ 将序列编码为 S_l 并通过公共信道发送 $X_l \triangleq e_l^{(X)}(S_l, K_l)$；

3) The fusion center computes $\hat{\Sigma}_{[L]} \triangleq d(X_{[L]})$ *an estimate of* $\Sigma_{[L]} \triangleq \sum_{l\in[L]} S_l$, *where* $X_{[L]} \triangleq (X_l)_{l\in[L]}$.

接下来，我们定义如下的 $(L, n, (R_l^{(X)})_{l\in[L]}, R^{(U)}, (R_l^{(K)})_{l\in[L]})$ 私有求和计算协议，如定义1所示。

定义 2。 令 $\delta \geqslant 0$和 $T \in [\![0, L-2]\!]$。一个$(L, n, (R_l^{(X)})_{l\in[L]}, R^{(U)}, (R_l^{(K)})_{l\in[L]})$ 私有求和计算协议称为(δ, T)-私有的，当且仅当

$$\hat{\Sigma}_{[L]} = \Sigma_{[L]}, \tag{1}$$

$$\max_{\substack{\mathcal{T}\subset[L]\\ :|\mathcal{T}|\leqslant T}} \frac{I(S_{[L]}; X_{[L]}|\Sigma_{[L]}, S_{\mathcal{T}}, K_{\mathcal{T}})}{n} \leqslant \delta, \tag{2}$$

where for any $\mathcal{T} \subset [L]$, $S_{\mathcal{T}} \triangleq (S_l)_{l\in\mathcal{T}}$ *and* $K_{\mathcal{T}} \triangleq (K_l)_{l\in\mathcal{T}}$.

公式（1）表示融合中心无误差地计算总和 $\Sigma_{[L]}$ 。如果融合中心与一组 $\mathcal{T}$个 T 用户串通，那么公式（2）量化了在已知 $(\Sigma_{[L]}, S_{\mathcal{T}}, K_{\mathcal{T}})$ 的条件下， $X_{\mathcal{T}^c}$泄露的关于 $S_{\mathcal{T}^c}$ 的归一化信息量；事实上，注意到根据定义 1，$I(S_{[L]}; X_{[L]}|\Sigma_{[L]}, S_{\mathcal{T}}, K_{\mathcal{T}}) = I(S_{\mathcal{T}^c}; X_{\mathcal{T}^c}|\Sigma_{[L]}, S_{\mathcal{T}}, K_{\mathcal{T}})$。该设置如图 1 所示。

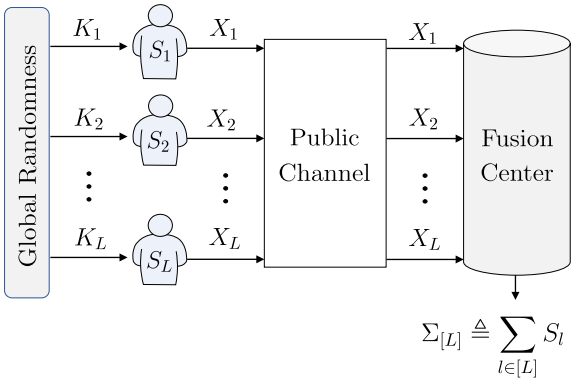


图 1：求和计算设置：$(S_i)_{i\in[L]}$ 和 $(X_i)_{i\in[L]}$ 分别表示用户的私有序列及其编码版本。$(K_i)_{i\in[L]}$ 表示局部随机性。

在本研究中，对于满足定义2要求的协议，我们希望刻画(i)最小全局随机性 U 所需的量，(ii)每个用户所需的最小公共通信量，(iii)用户所需的最小局部随机性量。为此，我们引入以下量。

定义 3. 令 $\delta \geqslant 0$ 和 $T \in [\![0, K-2]\!]$。令 $\mathcal{C}$ 为由满足以下条件的元组构成的集合：存在$(L, n, (R_l^{(X)})_{l\in[L]}, R^{(U)}, (R_l^{(K)})_{l\in[L]})$ 私有求和计算协议，且这些协议是(δ, T)私有的： $\Lambda \triangleq (R_l^{(X)})_{l\in[L]}, R^{(U)}, (R_l^{(K)})_{l\in[L]})$ 。然后，定义

$$R_{l,\star}^{(X)} \triangleq \inf_{\Lambda\in\mathcal{C}} R_l^{(X)}, \forall l \in [L],$$

$$R_{l,\star}^{(K)} \triangleq \inf_{\Lambda\in\mathcal{C}} R_l^{(K)}, \forall l \in [L],$$

$$R_{\Sigma,\star}^{(K)} \triangleq \inf_{\Lambda\in\mathcal{C}} \sum_{l\in[L]} R_l^{(K)},$$

$$R_\star^{(U)} \triangleq \inf_{\Lambda\in\mathcal{C}} R^{(U)}.$$

示例 1 (设置见 [18])。 考虑特殊情形 $\delta = 0$。在该设定中，*[18]*描述了以下可达方案。全局随机性为 $U \triangleq (N_l)^{l\in[L-1]}$，其中 N_l各自独立且服从$\mathbb{F}_2^n$上的均匀分布。 U 随后编码为

$$K_l = e_l(U) \triangleq N_l,\ \textit{for}\ l \in [L-1],$$
$$K_L = e_L(U) \triangleq -\sum_{l\in[L-1]} N_l.$$

收到 X_l、 $l \in [L]$ 后，用户 l 将序列 S_l 编码为

$$X_l = e_l^{(X)}(K_l, S_l) \triangleq K_l + S_l,\ \textit{for}\ l \in [L].$$

最后，融合中心将 $\Sigma_{[L]}$ 恢复为

$$d(X_{[L]}) \triangleq \sum_{l\in[L]} X_l = \sum_{l\in[L]} S_l = \Sigma_{[L]},$$

并且隐私约束 (2) 由一次一密引理保证满足，例如，*[25, 2 4]* $l \in [L]$ $R_l^{(X)}$ = 定理.....因此，对于，1 $R^{(U)} = L-1$ 速率， $R_l^{(K)} = 1$，以及 均可实现。

此外， *[18]* 证明，在以下假设下，该可达方案是最优的：*(i)* 所有用户的本地随机性速率相同（即 $\exists C_1 \in \mathbb{R}$、$R_l^{(K)} = C_1$、$\forall l \in [L]$）；*(ii)* 所有用户的通信速率相同（即 $\exists C_2 \in \mathbb{R}$、$R_l^{(X)} = C_2$、$\forall l \in [L]$）。

注 1。在示例 *1*中，利用全局随机性生成局部随机性对应于一种秘密共享方案，详见第 *III-D* 节。因此，示例 *1*表明，秘密共享足以利用全局随机性生成局部随机性。此外，在第 *III-D* 节中，我们将证明，秘密共享对于此目的不仅是充分的，也是必要的。

备注 2。当 $\delta = 0$时，我们的模型恢复了 *[18]*, 示例 *1*中所述的设定。不过，与*[18]*, 针对 $\delta = 0$的情形不同，我们的设定无需依赖示例*1*中所述的假设 *(i)* 和 *(ii)* 来建立逆定理结果。

备注 3。在定义*2*中，只需考虑 $T \in [\![0,\ L-2]\!]$。若 $T = L$, 则(2) 始终成立，因为左边等于零。若 $T = L-1$，这同样成立，因为$S_{[L]}$ 可以根据$(\Sigma_{[L]},\ S_{\mathcal{T}})$ 对于任意满足 $\mathcal{T} \subset [L]$的 $|\mathcal{T}| = L-1$重构得到。

III. 主要结果

我们首先在第 III-A 节证明，定义 2在不失一般性的前提下可以简化。随后，我们分别在第 III-B 节和第 III-C节给出逆定理和容量结果。最后，我们在第 III-D节阐明秘密共享与隐私求和中所需随机性之间的联系。

A. 预备知识

正如附录 A所证明的，在定义 2的隐私约束（2）中，只需考虑 δ 具有以下形式 $\delta = \alpha(L-1)$，其中 $\alpha \in [0,1]$，也就是说，（2）可以替换为

$$\max_{\substack{\mathcal{T}\subset[L]\\ :|\mathcal{T}|\leqslant T}} I(S_{[L]}; X_{[L]}|\Sigma_{[L]}, S_{\mathcal{T}}, K_{\mathcal{T}}) \leqslant n\alpha(L-1). \tag{3}$$

B. 逆定理结果

我们首先推导关于个体通信速率、局部随机性和速率以及全局随机速率的一个逆定理。

定理 1 (逆定理)。 考虑任意一个$(L, n, (R_l^{(X)})^{l\in[L]},$ $R^{(U)}$ $,(R_l^{(K)})^{l\in[L])}$ 私有求和计算协议，该协议满足$(\delta = \alpha(L-1)\ T)$-隐私，其中 $\alpha \in [0,1]$。于是，我们有

$$R_l^{(X)} \geqslant 1, \forall l \in [L], \tag{4}$$
$$\textstyle\sum_{l\in[L]} R_l^{(K)} \geqslant (1-\alpha)L, \tag{5}$$
$$R^{(U)} \geqslant (1-\alpha)(L-1). \tag{6}$$

证明。 参见第 IV节。 ∎

接下来，在以下泄漏对称性假设下，我们推导局部随机性的个体速率的一个逆定理：

(*) 对于任意一组合谋用户 $\mathcal{T} \subseteq [L-2]$，向 $\mathcal{T}$ 中添加一个用户，会使关于其余用户输入的泄漏改变一个固定量，该量与 $\mathcal{T}$ 的选择或所添加用户的身份无关。

这一假设反映了一种将所有用户对称对待的模型，确保没有用户能够特权访问其他用户的私有数据，并且所有用户及各种合谋场景下的隐私保证保持一致。泄漏的固定变化意味着，无论新增用户加入哪个子集，也无论其身份如何，每增加一个用户都会带来相同程度的泄漏。对于 $\mathcal{T} \subseteq [L]$，定义泄漏

$$\mathbb{L}(\mathcal{T}) \triangleq I(S_{[L]}; X_{[L]}|\Sigma_{[L]} S_{\mathcal{T}} K_{\mathcal{T}}),$$

那么，泄漏对称性公理 **(*)** 在数学上可表述如下：

$$\exists \Delta \in \mathbb{R}, \forall \mathcal{T} \subseteq [L-2], \forall j \in \mathcal{T}^c, \mathbb{L}(\mathcal{T}) - \mathbb{L}(\mathcal{T}\cup\{j\}) = \Delta. \tag{7}$$

由（7），我们可以推出以下性质，其证明见附录 B。

性质 1。我们有

$$\forall l \in [\![0, L]\!], \exists C_l \in \mathbb{R}_+, \forall \mathcal{T} \subseteq [L], |\mathcal{T}| = l \implies \mathbb{L}(\mathcal{T}) = C_l.$$

性质 2。考虑 $(C_l)^{l\in[\![0,\ L]\!]}$ 如性质*1*所示。那么，我们有

$$\forall l \in [\![0, L-1]\!], C_l \geqslant C_{l+1}.$$

性质 3。 考虑$(C_l)^{l\in[\![0,\ L]\!]}$ 如性质 *1*所述。则有

$$\Delta \leqslant n\alpha,$$
$$C_0 \leqslant n\alpha(L-1).$$

定理 2（逆定理）。假设要求满足泄漏对称性，即 (7)。那么，对于任意 $(L,\ n,\ (R_l^{(X)})_{l\in[L]},\ R^{(U)},\ (R_l^{(K)})_{l\in[L]})$ 私有求和计算协议，且该协议是 $(\delta=\alpha(L-1)\ T)$-私有的，其中 $\alpha\in[0,1]$，有

$$R_l^{(X)} \geqslant 1, \forall l\in[L], \tag{8}$$
$$R_l^{(K)} \geqslant 1-\alpha, \forall l\in[L], \tag{9}$$
$$R^{(U)} \geqslant (1-\alpha)(L-1). \tag{10}$$

证明。 参见第 V节。 ∎

注 4。 设 $\alpha=0$。由于 (7) 在 α =0时始终成立，定理 *2* 推广了 *[18]*，中的逆定理，因为在推导我们的逆定理时，并未假设局部随机性速率和通信速率必然全部相等。

C. 容量结果

下述定理表明，定理 1和2的逆定理界可以同时达到。

定理 3。 对于任意 $\alpha\in[0,1]\cap\mathbb{Q}$，我们有

$$R_{l,\star}^{(K)} = 1-\alpha, \forall l\in[L],\ \textit{when (7) holds},$$
$$R_{\Sigma,\star}^{(K)} = (1-\alpha)L,$$
$$R_{l,\star}^{(X)} = 1, \forall l\in[L],$$
$$R_{\star}^{(U)} = (1-\alpha)(L-1).$$

此外，存在一个私有求和计算协议，该协议是 $(\delta=\alpha(L-1)\ T)$-私有的，并且同时达到 $(R_{l\ \star}^{(X)},)_{l\in[L]}$, $R_{\star}^{(U)}$、$(R_{l\ \star}^{(K)},)_{l\in[L]}$ 和 $R_{\Sigma\ \star}^{(K)}$。

证明。 参见第VI节。 ∎

在定理3中， α 是一个有理数。然而，注意到由于 $\mathbb{Q}$ 在 $\mathbb{R}$ 中稠密，对于任意 $\alpha'\in\mathbb{R}_+$，对于任意 $\epsilon>0$，都存在 $\alpha\in\mathbb{Q}_+$ 使得 $|\alpha-\alpha'|\leqslant\epsilon$。

注 5。 泄漏对称性假设仅用于证明定理*3*中局部随机性个体速率的最优性。因此，在不存在泄漏对称性的情况下，定理*3* 中得到的以下刻画仍然成立：

(i) 局部随机性的最优总速率，*(ii)* 通信的最优个体速率，*(iii)* 全局随机性的最优速率。

这三个结果对任意 $\alpha>0$ 均成立，因此涵盖了此前针对 $\alpha=0$ 推导出的结果，例如 *[18]*。

D. 秘密共享与隐私求和之间的联系

在第III-D2节建立局部随机性结构与秘密共享之间的联系之前，我们先在第III-D1节回顾秘密共享的概念。

1）预备知识：带泄漏的均匀秘密共享，例如 [26]–[29], ，定义如下。

定义 4（带泄漏的均匀秘密共享）。设 $\alpha\in[0,1]$、 $t\in[L]$ 和 $z\in[t-1]$。一个(α,t,z)-秘密共享方案由以下部分组成

- 秘密 S 在 $\{0,1\}^{n_s}$ 上均匀分布；
- 随机编码器 $e:\{0,1\}^{n_s}\times\{0,1\}^{n_r}\to\{0,1\}^{n_{sh}}$，$(S,R)\mapsto(H_l)_{l\in[L]}$，以秘密 S 和在 $\{0,1\}^{n_r}$ 上均匀分布且独立于 S 的随机化序列 R 为输入，并输出 L 条序列$(H_l)_{l\in[L]}$，其长度之和为 n_{sh}，这些序列的长度不必相同。$(H_l)_{l\in[L]}$ 被称为该秘密共享的份额。对于任意 $\mathcal{S}\subseteq[L]$，我们定义 $H_{\mathcal{S}}=(H_l)_{l\in\mathcal{S}}$;

并满足以下两个条件

$$\max_{\mathcal{T}\subseteq[L]:|\mathcal{T}|=t} H(S|H_{\mathcal{T}})=0, \quad \textit{(Recoverability)} \tag{11}$$
$$\max_{\mathcal{U}\subseteq[L]:|\mathcal{U}|\leqslant z} I(S;H_{\mathcal{U}})\leqslant\alpha H(S), \quad \textit{(Privacy leakage)} \tag{12}$$

以及泄漏对称条件

$$\forall l\in[L], \exists C_l\in\mathbb{R}^+, \forall\mathcal{T}\in[L], |\mathcal{T}|=l \implies \frac{I(S;H_{\mathcal{T}})}{H(S)}=C_l. \tag{13}$$

定义 5。一个(t,Δ,L) 渐进式秘密共享方案，例如 *[16], [17],* , 是一个(α,t,z)-秘密共享方案，具有 $\alpha=0$、$z=t-\Delta$，且份额大小最优。

注意，根据 [29], 对于一个（t， Δ， L）渐进式秘密共享方案，我们有

$$C_l \triangleq \begin{cases} 0 & \text{if } l\in[\![0,t-\Delta]\!] \\ \frac{l-t+\Delta}{\Delta} & \text{if } l\in[\![t-\Delta+1,t]\!] \\ 1 & \text{if } l\in[\![t+1,L]\!] \end{cases}, \tag{14}$$

这意味着任意 t 份额都可以重构 S，任意份额数小于或等于 $t-\Delta$的集合都不会泄漏关于S的任何信息，而对于基数属于 $[\![t-\Delta+1,\ t]\!]$的份额集合，泄漏会随集合基数线性增加。

2）隐私求和与秘密共享：虽然已知，当 $\alpha=0$ 在我们的设定中，例如，[18,定理 1], 定理4 通过表明秘密共享是生成隐私求和所需局部随机性的必要条件，确立了隐私求和与秘密共享之间更强的联系。此前已知，在用户端生成局部随机性时可以采用秘密共享。

定理 4（必要条件）。假设要求泄漏对称性，即 （7），并考虑一个最优隐私求和计算协议，即

$$R_l^{(K)} = R_{l,\star}^{(K)}, \forall l\in[L],$$
$$\textstyle\sum_{l\in[L]} R_l^{(K)} = R_{\Sigma,\star}^{(K)},$$
$$R_l^{(X)} = R_{l,\star}^{(X)}, \forall l\in[L],$$
$$R^{(U)} = R_{\star}^{(U)}.$$

那么，$(K_l)_{l\in[L]}$ 必定是一个$(L-1,L-1,L)$ 渐进式秘密共享方案的份额，其中 U 是秘密。

证明。 参见第 VII节。 ∎

注释 6。 当 $\alpha=0$， （7） 始终成立时，因此定理*4* 证明了，生成安全求和所需的局部随机性始终需要秘密共享。

对于 $\alpha > 0$，只有在泄漏对称性假设 （7）下才能证明相同的结果。

IV. Proof of Theorem 1

A. Communication rate converse: Proof of (4)

For any $l \in [L]$, we have

$$
\begin{aligned}
& nR_l^{(X)} \\
& \overset{(a)}{\geqslant} H(X_l) \\
& \overset{(b)}{\geqslant} H(X_l|S_{[L]\setminus\{l\}}, K_{[L]\setminus\{l\}}) \\
& \geqslant I(X_l; \Sigma_{[L]}|S_{[L]\setminus\{l\}}, K_{[L]\setminus\{l\}}) \\
& = H(\Sigma_{[L]}|S_{[L]\setminus\{l\}}, K_{[L]\setminus\{l\}}) \\
& \quad - H(\Sigma_{[L]}|X_l, S_{[L]\setminus\{l\}}, K_{[L]\setminus\{l\}}) \\
& \overset{(c)}{=} H(\Sigma_{[L]}, S_{[L]\setminus\{l\}}|S_{[L]\setminus\{l\}}, K_{[L]\setminus\{l\}}) \\
& \quad - H(\Sigma_{[L]}|X_l, S_{[L]\setminus\{l\}}, K_{[L]\setminus\{l\}}) \\
& \overset{(d)}{=} H(\Sigma_{[L]}, S_l, S_{[L]\setminus\{l\}}|S_{[L]\setminus\{l\}}, K_{[L]\setminus\{l\}}) \\
& \quad - H(\Sigma_{[L]}|X_l, S_{[L]\setminus\{l\}}, K_{[L]\setminus\{l\}}) \\
& \overset{(e)}{\geqslant} H(S_l|S_{[L]\setminus\{l\}}, K_{[L]\setminus\{l\}}) - H(\Sigma_{[L]}|X_l, S_{[L]\setminus\{l\}}, K_{[L]\setminus\{l\}}) \\
& \overset{(f)}{=} H(S_l|S_{[L]\setminus\{l\}}, K_{[L]\setminus\{l\}}) \\
& \quad - H(\Sigma_{[L]}|X_{[L]}, S_{[L]\setminus\{l\}}, K_{[L]\setminus\{l\}}) \\
& \overset{(g)}{=} H(S_l|S_{[L]\setminus\{l\}}, K_{[L]\setminus\{l\}}) \\
& \overset{(h)}{=} H(S_l) \\
& \overset{(i)}{=} n,
\end{aligned}
$$

其中
(a) 根据定义1成立；(b) 成立是因为条件化降低熵；(c) 根据链式法则成立；(d) 成立是因为可以从S_l 重构出$(\Sigma_{[L]}, S_{[L]\setminus\{l\}})$；(e) 根据链式法则成立；(f) 成立是因为 $X_{[L]\setminus\{l\}}$ 是一个函数$(S_{[L]\setminus\{l\}}, K_{[L]\setminus\{l\}})$；(g) 成立是因为

of

$$H(\Sigma_{[L]}|X_{[L]}, S_{[L]\setminus\{l\}}, K_{[L]\setminus\{l\}}) \leqslant H(\Sigma_{[L]}|X_{[L]}) = 0,$$

其中等式根据（1）成立；
（h）根据 S_l 与（$S_{[L]\setminus\{l\}}$, $K_{[L]\setminus\{l\}}$）之间的独立性成立；（i）根据 S_l的均匀性成立。

B. 局部随机性和速率逆定理：式（5）的证明

我们首先证明以下引理，该引理给出了各用户编码器输出所泄露的关于其个体序列的信息总和的上界。

引理 1. 我们有

$$\sum_{l\in[L]} I(S_l; X_l) \leqslant \alpha n L. \tag{15}$$

证明。对于任意 $i \in [L]$，我们有

$$
\begin{aligned}
& \alpha n(L-1) \\
& \overset{(a)}{\geqslant} I(S_{[L]}; X_{[L]}|\Sigma_{[L]}) \\
& \overset{(b)}{=} \sum_{l\in[L]\setminus\{i\}} I(S_l; X_{[L]}|S_{[l-1]\setminus\{i\}}, \Sigma_{[L]}) \\
& \quad + I(S_i; X_{[L]}|S_{[L]\setminus\{i\}}, \Sigma_{[L]}) \\
& \overset{(c)}{=} \sum_{l\in[L]\setminus\{i\}} I(S_l; X_{[L]}|S_{[l-1]\setminus\{i\}}, \Sigma_{[L]}) \\
& \overset{(d)}{\geqslant} \sum_{l\in[L]\setminus\{i\}} I(S_l; X_l|S_{[l-1]\setminus\{i\}}, \Sigma_{[L]}) \\
& \overset{(e)}{=} \sum_{l\in[L]\setminus\{i\}} I(S_l; X_l|S_{[l-1]\setminus\{i\}}, \Sigma_{[l:L]\cup\{i\}}) \\
& \overset{(f)}{=} \sum_{l\in[L]\setminus\{i\}} [I(S_l; X_l, S_{[l-1]\setminus\{i\}}|\Sigma_{[l:L]\cup\{i\}}) \\
& \quad - I(S_l; S_{[l-1]\setminus\{i\}}|\Sigma_{[l:L]\cup\{i\}})] \\
& \overset{(g)}{=} \sum_{l\in[L]\setminus\{i\}} I(S_l; X_l, S_{[l-1]\setminus\{i\}}|\Sigma_{[l:L]\cup\{i\}}) \\
& \overset{(h)}{=} \sum_{l\in[L]\setminus\{i\}} [I(S_l; X_l|\Sigma_{[l:L]\cup\{i\}}) \\
& \quad + I(S_l; S_{[l-1]\setminus\{i\}}|X_l, \Sigma_{[l:L]\cup\{i\}})] \\
& \overset{(i)}{=} \sum_{l\in[L]\setminus\{i\}} I(S_l; X_l|\Sigma_{[l:L]\cup\{i\}}) \\
& = \sum_{l\in[L]\setminus\{i\}} [I(S_l; X_l, \Sigma_{[l:L]\cup\{i\}}) - I(S_l; \Sigma_{[l:L]\cup\{i\}})] \\
& \overset{(j)}{=} \sum_{l\in[L]\setminus\{i\}} I(S_l; X_l, \Sigma_{[l:L]\cup\{i\}}) \\
& \geqslant \sum_{l\in[L]\setminus\{i\}} I(S_l; X_l),
\end{aligned} \tag{16}
$$

其中
(a) 根据（3）成立，其中 $\mathcal{T} = 0$;
(b) 根据链式法则成立；
(c) 成立，因为可以从 $(S_{[L]\setminus\{i\}}, \Sigma_{[L]})$ 中恢复 S_i ；
(d) 根据链式法则成立；
(e) 采用以下记号成立

$$\Sigma_{[l:L]\cup\{i\}} \triangleq \sum_{j\in\{l,l+1,\ldots,L\}\cup\{i\}} S_j;$$

(f) 根据链式法则成立；
(g) 成立是因为

$$
\begin{aligned}
& I(S_l; S_{[l-1]\setminus\{i\}}|\Sigma_{[l:L]\cup\{i\}}) \\
& \leqslant I(S_l, \Sigma_{[l:L]\cup\{i\}}; S_{[l-1]\setminus\{i\}}) \\
& = 0
\end{aligned}
$$

其中，不等式由链式法则和互信息的非负性成立；等式成立是因为（S_l, $\Sigma_{[l:L]\cup\{i\}}$）是$S_{[\![l,\ L]\!]\cup\{i\}}$的确定性函数，而后者根据用户序列的独立性，与 $S_{[l-1]\setminus\{i\}}$ 相互独立——

性，因为 $(\llbracket l,\ L\rrbracket \cup \{i\}) \cap ([l-1]\backslash\{i\}) = \emptyset$;

(h) 根据链式法则成立;
(i) 成立，因为

$$\begin{aligned}
&I(S_l; S_{[l-1]\backslash\{i\}} | X_l, \Sigma_{[l:L]\cup\{i\}}) \\
&\leqslant I(S_l, \Sigma_{[l:L]\cup\{i\}}, X_l; S_{[l-1]\backslash\{i\}}) \\
&\leqslant I(S_l, \Sigma_{[l:L]\cup\{i\}}, K_l; S_{[l-1]\backslash\{i\}}) \\
&\leqslant I(S_l, \Sigma_{[l:L]\cup\{i\}}, U; S_{[l-1]\backslash\{i\}}) \\
&= I(S_l, \Sigma_{[l:L]\cup\{i\}}; S_{[l-1]\backslash\{i\}}) \\
&= 0,
\end{aligned}$$

其中，第一个不等式根据链式法则以及互信息的非负性成立；第二个不等式成立，因为 X_l 是 (S_l, K_l) 的函数；第三个不等式成立，因为 K_l 是 U 的函数；第一个等式根据用户序列与全局随机性的独立性成立；最后一个等式与 (g) 中相同;

(j) 根据一次一密引理成立，例如 [25, 定理 2。4], 利用用户序列的均匀性以及 $l \neq i$。

因此，注意到

$$\sum_{i\in[L]} \sum_{l\in[L]\backslash\{i\}} I(S_l; X_l) = (L-1) \sum_{l\in[L]} I(S_l; X_l), \tag{17}$$

由 (16) 和 (17)，可得 (15)。

■

因此，我们有

$$\begin{aligned}
\sum_{l\in[L]} nR_l^{(K)} &\overset{(a)}{\geqslant} \sum_{l\in[L]} H(K_l) \\
&\overset{(b)}{=} \sum_{l\in[L]} H(K_l|S_l) \\
&\geqslant \sum_{l\in[L]} I(K_l; X_l|S_l) \\
&= \sum_{l\in[L]} [H(X_l|S_l) - H(X_l|K_l, S_l)] \\
&\overset{(c)}{=} \sum_{l\in[L]} H(X_l|S_l) \\
&= \sum_{l\in[L]} [H(X_l) - I(X_l; S_l)] \\
&\overset{(d)}{\geqslant} nL - \sum_{l\in[L]} I(X_l; S_l) \\
&\overset{(e)}{\geqslant} nL - \alpha nL \\
&= nL(1-\alpha),
\end{aligned}$$

其中
（a）根据定义成立1；（b）根据 U 与 $S_{[L]}$ 之间的独立性成立1；（d）由（4）成立；（e）由（15）成立。

C. Global randomness rate converse: Proof of (6)

We have

$$\begin{aligned}
&nR^{(U)} \\
&\overset{(a)}{\geqslant} H(U) \\
&\overset{(b)}{\geqslant} H(K_{[L]}) \\
&\overset{(c)}{\geqslant} H(K_{[L]}|S_{[L]}) \\
&\geqslant I(K_{[L]}; X_{[L]}|S_{[L]}) \\
&\overset{(d)}{=} H(X_{[L]}|S_{[L]}) \\
&= H(X_{[L]}) - I(X_{[L]}; S_{[L]}) \\
&\overset{(e)}{=} H(X_{[L]}) - I(X_{[L]}; \Sigma_{[L]}, S_{[L]}) \\
&= H(X_{[L]}) - I(X_{[L]}; \Sigma_{[L]}) - I(X_{[L]}; S_{[L]}|\Sigma_{[L]}) \\
&\overset{(f)}{\geqslant} H(X_{[L]}) - I(X_{[L]}; \Sigma_{[L]}) - \alpha n(L-1) \\
&= H(X_{[L]}) - H(\Sigma_{[L]}) + H(\Sigma_{[L]}|X_{[L]}) - \alpha n(L-1) \\
&\overset{(g)}{=} H(X_{[L]}) - H(\Sigma_{[L]}) - \alpha n(L-1) \\
&\overset{(h)}{=} H(X_{[L]}) - n - \alpha n(L-1) \\
&= \sum_{l\in[L]} H(X_l|X_{[l-1]}) - n - \alpha n(L-1) \\
&\overset{(i)}{\geqslant} \sum_{l\in[L]} H(X_l|S_{[L]\backslash\{l\}}, K_{[L]\backslash\{l\}}, X_{[l-1]}) - n - \alpha n(L-1) \\
&\overset{(j)}{=} \sum_{l\in[L]} H(X_l|S_{[L]\backslash\{l\}}, K_{[L]\backslash\{l\}}) - n - \alpha n(L-1) \\
&\geqslant \sum_{l\in[L]} I(X_l; \Sigma_{[L]}|S_{[L]\backslash\{l\}}, K_{[L]\backslash\{l\}}) - n - \alpha n(L-1) \\
&= \sum_{l\in[L]} [H(\Sigma_{[L]}|S_{[L]\backslash\{l\}}, K_{[L]\backslash\{l\}}) \\
&\quad - H(\Sigma_{[L]}|X_l, S_{[L]\backslash\{l\}}, K_{[L]\backslash\{l\}})] - n - \alpha n(L-1) \\
&\overset{(k)}{=} \sum_{l\in[L]} H(\Sigma_{[L]}|S_{[L]\backslash\{l\}}, K_{[L]\backslash\{l\}}) - n - \alpha n(L-1) \\
&\overset{(l)}{=} \sum_{l\in[L]} H(\Sigma_{[L]}, S_l|S_{[L]\backslash\{l\}}, K_{[L]\backslash\{l\}}) - n - \alpha n(L-1) \\
&\geqslant \sum_{l\in[L]} H(S_l|S_{[L]\backslash\{l\}}, K_{[L]\backslash\{l\}}) - n - \alpha n(L-1) \\
&\overset{(m)}{=} \sum_{l\in[L]} H(S_l) - n - \alpha n(L-1) \\
&\overset{(n)}{=} n(L-1)(1-\alpha),
\end{aligned}$$

其中
(a) 由定义1成立；(b) 成立是因为 $K_{[L]}$ 是 U 的函数；(c) 成立是因为条件化降低熵；(d) 成立是因为 $X_{[L]}$ 是 $(K_{[L]}, S_{[L]})$ 的函数；(e) 成立是因为 $\Sigma_{[L]}$ 是 $S_{[L]}$ 的函数；(f) 由 (3) 及 $\mathcal{T} = 0$ 成立；(g) 由 (1) 成立；(h) 由用户序列的均匀性成立；

(i) 成立是因为条件化降低熵；(j) 成立是因为 $X_{[l-1]}$ 是 $(S_{[L]\setminus\{l\}}, K_{[L]\setminus\{l\}})$ 的函数；(k) 由 (1) 成立，因为 $X_{[L]}$ 可由$(X_l, S_{[L]\setminus\{l\}}, K_{[L]\setminus\{l\}})$ 重构；(l) 由链式法则成立，并且因为 S_l 可由 $(\Sigma_{[L]}, S_{[L]\setminus\{l\}})$ 重构；(m) 由用户序列与局部随机性之间的独立性成立；(n) 由用户序列的均匀性成立。

V. 定理 2的证明

注意到，式（8）和（10）可由定理 1推出，而该定理不需要泄漏对称性（7）。因此，只需在泄漏对称性（9）下证明式（7）。

在下面的引理中，我们首先给出与任意一组合谋用户相关的泄漏的一般刻画。

引理 2. 对于任意 $\mathcal{T} \subseteq [L]$，有

$$C_{|\mathcal{T}|} = n(L - |\mathcal{T}| - \mathbb{1}\{\mathcal{T} \neq [L]\}) - H(S_{\mathcal{T}^c}|X_{[L]}K_{\mathcal{T}}S_{\mathcal{T}}).$$

证明。 见附录C。 ∎

在下面的引理中，我们给出与任意两组仅相差一个成员的合谋用户相关的泄漏之差的刻画。

引理 3. 固定 $l \in [L]$。对于 $t \in [\![0, L-1]\!]$，定义

$$\mathcal{T}_t \triangleq \begin{cases} [\![1, t]\!] & \text{if } t < l \\ [\![1, t+1]\!]\setminus\{l\} & \text{if } t \geqslant l \end{cases},$$

以及 $\mathcal{T}_L \triangleq [L]$。

那么，对于 $t \in [\![0, L-1]\!]$，有

$$\begin{aligned} &C_{t+1} - C_t \\ &= H(K_l, S_l|K_{\mathcal{T}_t}, S_{\mathcal{T}_t}, X_{[L]}) - H(K_l|K_{\mathcal{T}_t}, S_{[L]}, X_{[L]}) \\ &\quad - n\mathbb{1}\{t \neq L-1\}. \end{aligned} \tag{18}$$

证明。 对于 $t \in [\![0, L-2]\!]$，有

$$\begin{aligned} &H(K_l, S_l|K_{\mathcal{T}_t}, S_{\mathcal{T}_t}, X_{[L]}) \\ &\overset{(a)}{=} H(K_l, S_l, S_{\mathcal{T}_t^c}|K_{\mathcal{T}_t}, S_{\mathcal{T}_t}, X_{[L]}) \\ &\quad - H(S_{\mathcal{T}_t^c}|K_{\mathcal{T}_t\cup\{l\}}, S_{\mathcal{T}_t\cup\{l\}}, X_{[L]}) \\ &\overset{(b)}{=} H(S_{\mathcal{T}_t^c}|K_{\mathcal{T}_t}, S_{\mathcal{T}_t}, X_{[L]}) + H(K_l, S_l|K_{\mathcal{T}_t}, S_{[L]}, X_{[L]}) \\ &\quad - H(S_{\mathcal{T}_t^c}|K_{\mathcal{T}_t\cup\{l\}}, S_{\mathcal{T}_t\cup\{l\}}, X_{[L]}) \\ &\overset{(c)}{=} n(L-t-1) - C_t + H(K_l, S_l|K_{\mathcal{T}_t}, S_{[L]}, X_{[L]}) \\ &\quad - H(S_{\mathcal{T}_t^c}|K_{\mathcal{T}_t\cup\{l\}}, S_{\mathcal{T}_t\cup\{l\}}, X_{[L]}) \\ &\overset{(d)}{=} n(L-t-1) - C_t + H(K_l|K_{\mathcal{T}_t}, S_{[L]}, X_{[L]}) \\ &\quad - H(S_{\mathcal{T}_t^c\setminus\{l\}}|K_{\mathcal{T}_t\cup\{l\}}, S_{\mathcal{T}_t\cup\{l\}}, X_{[L]}) \\ &\overset{(e)}{=} n(L-t-1) - C_t + H(K_l|K_{\mathcal{T}_t}, S_{[L]}, X_{[L]}) + C_{t+1} \\ &\quad - n(L-(t+1)-1) \\ &= n + C_{t+1} - C_t + H(K_l|K_{\mathcal{T}_t}, S_{[L]}, X_{[L]}), \end{aligned} \tag{19}$$

其中
(a)、(b) 和 (d) 根据链式法则成立；
(c) 和 (e) 根据引理2。

此外，有

$$\begin{aligned} &H(K_l, S_l|K_{\mathcal{T}_{L-1}}, S_{\mathcal{T}_{L-1}}, X_{[L]}) \\ &\overset{(a)}{=} H(K_l, S_l|K_{\mathcal{T}_{L-1}}, S_{[L]}, X_{[L]}) \\ &= H(K_l|K_{\mathcal{T}_{L-1}}, S_{[L]}, X_{[L]}) \\ &\overset{(b)}{=} C_L - C_{L-1} + H(K_l|K_{\mathcal{T}_{L-1}}, S_{[L]}, X_{[L]}), \end{aligned} \tag{20}$$

其中
（a）成立，因为 $S_{[L]}$ 可以由 $X_{[L]}$ 根据（1）重构；（b）成立，因为 $C_{L-1} = 0 = C_L$。

Hence, (18) holds by (19) and (20). ∎

接下来，我们对用户 $l \in [L]$ 的个体局部随机性给出下界：

$$\begin{aligned} &H(K_l) \\ &\overset{(a)}{\geqslant} H(K_l) + n - H(X_l) \\ &\overset{(b)}{=} H(K_l) + H(S_l) - H(X_l) \\ &\overset{(c)}{=} H(K_l, S_l) - H(X_l) \\ &\overset{(d)}{=} H(K_l, S_l, X_l) - H(X_l) \\ &= H(K_l, S_l|X_l) \\ &\overset{(e)}{\geqslant} H(K_l, S_l|K_{\mathcal{T}_0}, S_{\mathcal{T}_0}, X_{[L]}) \\ &\geqslant H(K_l, S_l|K_{\mathcal{T}_0}, S_{\mathcal{T}_0}, X_{[L]}) \\ &\quad - H(K_l, S_l|K_{\mathcal{T}_{L-1}}, S_{\mathcal{T}_{L-1}}, X_{[L]}) \\ &= \sum_{i=0}^{L-2}[H(K_l, S_l|K_{\mathcal{T}_i}, S_{\mathcal{T}_i}, X_{[L]}) \\ &\qquad - H(K_l, S_l|K_{\mathcal{T}_{i+1}}, S_{\mathcal{T}_{i+1}}, X_{[L]})] \\ &\overset{(f)}{=} \sum_{i=0}^{L-3}[C_{i+1} - C_i - C_{i+2} + C_{i+1} + H(K_l|K_{\mathcal{T}_i}, S_{[L]}, X_{[L]}) \\ &\quad - H(K_l|K_{\mathcal{T}_{i+1}}, S_{[L]}, X_{[L]})] \\ &\quad + [n + C_{L-1} - C_{L-2} + H(K_l|K_{\mathcal{T}_{L-2}}, S_{[L]}, X_{[L]}) \\ &\qquad - C_L + C_{L-1} - H(K_l|K_{\mathcal{T}_{L-1}}, S_{[L]}, X_{[L]})] \\ &\overset{(g)}{\geqslant} n + \sum_{i=0}^{L-2}[C_{i+1} - C_i - C_{i+2} + C_{i+1}] \\ &= n + C_1 - C_0 - C_L + C_{L-1} \\ &\overset{(h)}{=} C_1 - C_0 + n \\ &\overset{(i)}{\geqslant} n(1-\alpha), \end{aligned}$$

其中
（a）由（4）得证；（b）由用户序列的均匀性得证；
（c）由用户序列与局部随机性之间的独立性得证；（d）由定义1得证；（e）因为条件化降低熵而得证；（f）由引理3得证；

（g）成立是因为，对于任意 $i \in [\![0,\ L-2]\!]$，

$$H(K_l|K_{\mathcal{T}_i}, S_{[L]}, X_{[L]}) \geqslant H(K_l|K_{\mathcal{T}_{i+1}}, S_{[L]}, X_{[L]})$$

因为条件化降低熵；
(h) 由 $C_{L-1} = 0 = C_L$ 得出；(i) 根据性质3成立。

VI. 证明：定理 3

为证明定理 3，只需证明下述可达性结果，该结果证明第 III-B 节的逆定理界是紧的。

命题 1（可达性）。对任意 $\alpha \in [0,1] \cap \mathbb{Q}$，存在一个$(L,\ n,\ (R_l^{(X)})_{l\in[L]},\ R^{(U)},\ (R_l^{(K)})_{l\in[L]})$ 私有求和计算协议，它是 $(\delta = \alpha(L-1)\ T)$-私有的，并且满足

$$\begin{aligned} R_l^{(K)} &= (1-\alpha), \forall l \in [L], \\ R_l^{(X)} &= 1, \forall l \in [L], \\ R^{(U)} &= (1-\alpha)(L-1). \end{aligned}$$

证明。该可达方案可视为 [18] 中编码方案的时分复用版本。令 $n_1, n_2 \in \mathbb{N}^*$，并定义 $n \triangleq n_1 + n_2, \alpha \triangleq n_1/n$。对于 $l \in [L]$，序列 S_l 写为 $S_l = (S_l^{(1)}, S_l^{(2)})$，其中 $|S_l^{(1)}| = n_1$ 且 $|S_l^{(2)}| = n_2$。用户 $l \in [L]$ 发送 $X_l \triangleq (S_l^{(1)}, K_l + S_l^{(2)})$，其中 $(K_l)_{l\in[L-1]}$ 是 n_2 比特的联合均匀序列，与 $S_{[L]}$ 独立，并且 $K_L \triangleq \sum_{l\in[L-1]} K_l$。因此，对任意 $l \in [L]$，$R_l^{(K)} = \frac{n_2}{n} = 1-\alpha$ $R_l^{(X)} = \frac{n}{n} = 1$ $R^{(U)} = \frac{(L-1)\ n_2}{n} =$，，以及 $()(L-1)(1-\alpha)$，我们有。然后，对任意满足 $|\mathcal{T}| = T$ 的 $\mathcal{T} \subset [L]$，我们有

$$\begin{aligned} &I(S_{[L]}; X_{[L]}|\Sigma_{[L]}, S_{\mathcal{T}}, K_{\mathcal{T}}) \\ &\overset{(a)}{=} I(S_{\mathcal{T}^c}; X_{\mathcal{T}^c}|\Sigma_{\mathcal{T}^c}, S_{\mathcal{T}}, K_{\mathcal{T}}) \\ &= H(X_{\mathcal{T}^c}|\Sigma_{\mathcal{T}^c}, S_{\mathcal{T}}, K_{\mathcal{T}}) - H(X_{\mathcal{T}^c}|S_{[L]}, \Sigma_{\mathcal{T}^c}, K_{\mathcal{T}}) \\ &\overset{(b)}{=} H(X_{\mathcal{T}^c}|\textstyle\sum_{l\in\mathcal{T}^c} X_l, \Sigma_{\mathcal{T}^c}, S_{\mathcal{T}}, K_{\mathcal{T}}) \\ &\quad - H(X_{\mathcal{T}^c}|S_{[L]}, \Sigma_{\mathcal{T}^c}, K_{\mathcal{T}}) \\ &\overset{(c)}{\leqslant} H(X_{\mathcal{T}^c}|\textstyle\sum_{l\in\mathcal{T}^c} X_l) - H(X_{\mathcal{T}^c}|S_{[L]}, \Sigma_{\mathcal{T}^c}, K_{\mathcal{T}}) \\ &\overset{(d)}{=} H(X_{\mathcal{T}^c}|\textstyle\sum_{l\in\mathcal{T}^c} X_l) - H(K_{\mathcal{T}^c}|S_{[L]}, \Sigma_{\mathcal{T}^c}, K_{\mathcal{T}}) \\ &\overset{(e)}{=} H(X_{\mathcal{T}^c}|\textstyle\sum_{l\in\mathcal{T}^c} X_l) - H(K_{\mathcal{T}^c}|K_{\mathcal{T}}) \\ &= (L-|\mathcal{T}|-1)n - (L-|\mathcal{T}|-1)n(1-\alpha) \\ &= (L-|\mathcal{T}|-1)n\alpha \\ &\leqslant (L-1)n\alpha, \end{aligned}$$

其中
（a）由链式法则成立，因为可以从（$S_{\mathcal{T}}$，$K_{\mathcal{T}}$）恢复 $X_{\mathcal{T}}$，并且（$\Sigma_{\mathcal{T}^c}$，$S_{\mathcal{T}}$）与（$\Sigma_{[L]}$，$S_{\mathcal{T}}$）之间存在一一映射；

（b）成立，因为根据 K_L 的定义，可以由 $K_{\mathcal{T}}$ 计算出 $\sum_{\in\mathcal{T}^c} K_l$，即 $\sum_{\in\mathcal{T}^c} K_l = \sum_{\in\mathcal{T}} K_l$；
(c) 成立，因为条件化降低熵；
(d) 成立，因为

$$\begin{aligned} &H(X_{\mathcal{T}^c}|S_{[L]}, \Sigma_{\mathcal{T}^c}, K_{\mathcal{T}}) \\ &= H(X_{\mathcal{T}^c}, S_{[L]}|S_{[L]}, \Sigma_{\mathcal{T}^c}, K_{\mathcal{T}}) \\ &= H(K_{\mathcal{T}^c}, S_{[L]}|S_{[L]}, \Sigma_{\mathcal{T}^c}, K_{\mathcal{T}}) \\ &= H(K_{\mathcal{T}^c}|S_{[L]}, \Sigma_{\mathcal{T}^c}, K_{\mathcal{T}}) \end{aligned}$$

根据 X_l、$l \in [L]$ 的定义；
(e) 由 $K_{[L]}$ 与 $S_{[L]}$ 的独立性成立。

■

VII. 定理 4 的证明

我们首先在以下引理中推导任意一组用户所需最少联合通信量的下界。

引理 4. 对于 $\mathcal{T} \subseteq [L]$，我们有

$$H(X_{\mathcal{T}}) \geqslant n|\mathcal{T}|.$$

证明。对于满足 $|\mathcal{T}| \geqslant 1$ 和 $t \in \mathcal{T}$ 的 $\mathcal{T} \subseteq [L]$，我们有

$$\begin{aligned} &H(X_{\mathcal{T}}) \\ &\overset{(a)}{\geqslant} H(X_{\mathcal{T}}|S_{[L]\setminus\mathcal{T}}, K_{[L]\setminus\mathcal{T}}) \\ &\geqslant I(X_{\mathcal{T}}; \Sigma_{[L]}, X_{\mathcal{T}\setminus\{t\}}|S_{[L]\setminus\mathcal{T}}, K_{[L]\setminus\mathcal{T}}) \\ &= H(\Sigma_{[L]}, X_{\mathcal{T}\setminus\{t\}}|S_{[L]\setminus\mathcal{T}}, K_{[L]\setminus\mathcal{T}}) \\ &\quad - H(\Sigma_{[L]}, X_{\mathcal{T}\setminus\{t\}}|X_{\mathcal{T}}, S_{[L]\setminus\mathcal{T}}, K_{[L]\setminus\mathcal{T}}) \\ &\overset{(b)}{=} H(\Sigma_{[L]}, X_{\mathcal{T}\setminus\{t\}}|S_{[L]\setminus\mathcal{T}}, K_{[L]\setminus\mathcal{T}}) \\ &= H(X_{\mathcal{T}\setminus\{t\}}|S_{[L]\setminus\mathcal{T}}, K_{[L]\setminus\mathcal{T}}) \\ &\quad + H(\Sigma_{[L]}|X_{\mathcal{T}\setminus\{t\}}, S_{[L]\setminus\mathcal{T}}, K_{[L]\setminus\mathcal{T}}) \\ &\overset{(c)}{\geqslant} H(X_{\mathcal{T}\setminus\{t\}}|S_{[L]\setminus(\mathcal{T}\setminus\{t\})}, K_{[L]\setminus(\mathcal{T}\setminus\{t\})}) \\ &\quad + H(\Sigma_{[L]}|X_{\mathcal{T}\setminus\{t\}}, S_{[L]\setminus\{t\}}, K_{[L]\setminus\{t\}}) \\ &\overset{(d)}{=} H(X_{\mathcal{T}\setminus\{t\}}|S_{[L]\setminus(\mathcal{T}\setminus\{t\})}, K_{[L]\setminus(\mathcal{T}\setminus\{t\})}) \\ &\quad + H(\Sigma_{[L]}|S_{[L]\setminus\{t\}}, K_{[L]\setminus\{t\}}) \\ &\overset{(e)}{\geqslant} H(X_{\mathcal{T}\setminus\{t\}}|S_{[L]\setminus(\mathcal{T}\setminus\{t\})}, K_{[L]\setminus(\mathcal{T}\setminus\{t\})}) + n \\ &\overset{(f)}{\geqslant} n|\mathcal{T}|, \end{aligned} \tag{21, 22}$$

其中
(a) 成立是因为条件化降低熵；
(b) 成立是因为

$$\begin{aligned} &H(\Sigma_{[L]}, X_{\mathcal{T}\setminus\{t\}}|X_{\mathcal{T}}, S_{[L]\setminus\mathcal{T}}, K_{[L]\setminus\mathcal{T}}) \\ &= H(\Sigma_{[L]}|X_{\mathcal{T}}, S_{[L]\setminus\mathcal{T}}, K_{[L]\setminus\mathcal{T}}) \\ &\leqslant H(\Sigma_{[L]}|X_{[L]}) \\ &= 0, \end{aligned}$$

其中，不等式成立是因为 $X_{[L]\setminus\mathcal{T}}$ 是 $(S_{[L]\setminus\mathcal{T}}, K_{[L]\setminus\mathcal{T}})$ 的函数，等式则由式（1）得出；
（c）成立是因为条件化降低熵；
(d) 成立，因为可以从 $(S_{\mathcal{T}\setminus\{t\}},\ K_{\mathcal{T}\setminus\{t\}})$ 恢复 $X_{\mathcal{T}\setminus\{t\}}$；

（e）成立是因为

$$\begin{aligned}
&H(\Sigma_{[L]}|S_{[L]\setminus\{t\}}, K_{[L]\setminus\{t\}})\\
&= H(\Sigma_{[L]}, S_t|S_{[L]\setminus\{t\}}, K_{[L]\setminus\{t\}})\\
&\quad - H(S_t|\Sigma_{[L]}, S_{[L]\setminus\{t\}}, K_{[L]\setminus\{t\}})\\
&= H(\Sigma_{[L]}, S_t|S_{[L]\setminus\{t\}}, K_{[L]\setminus\{t\}})\\
&= H(S_t|S_{[L]\setminus\{t\}}, K_{[L]\setminus\{t\}})\\
&= H(S_t)\\
&= n,
\end{aligned}$$

其中第二个等式成立，是因为可以从 $(S_{[L]\setminus\{t\}},\ \Sigma_{[L]})$ 恢复 S_t，第三个等式根据链式法则成立，并且因为可以从 $(S_{[L]\setminus\{t\}},\ S_t)$ 恢复 $\Sigma_{[L]}$，第四个等式根据用户序列与局部随机性之间的独立性成立，最后一个等式根据用户序列的均匀性成立；

（f）通过重复 $|\mathcal{T}|-1$ 次与（22）之间的步骤而成立。(21)

■

接下来，我们利用引理 4 证明如下引理，给出任意一组用户所需局部随机性的联合总量下界。

引理 5。对于任意 $\mathcal{T}\subseteq[L]$，有

$$H(K_{\mathcal{T}}) \geqslant n(|\mathcal{T}|-\mathbb{1}\{\mathcal{T}=[L]\})(1-\alpha).$$

证明。固定满足 $|\mathcal{T}|\leqslant L-2$ 的 $\mathcal{T}\subseteq[L]$，将其补集记为 $\mathcal{T}^c=(a_t)^{t\in[L-|\mathcal{T}|]}$，并对 $t\in[L-|\mathcal{T}|]$ $\mathcal{A}_t\triangleq(a_i)^{i\in[t]}$ 作如下定义。于是，对于 $t=1$，有

$$\begin{aligned}
&H(K_{\mathcal{T}})\\
&\overset{(a)}{\geqslant} H(K_{\mathcal{T}}) + |\mathcal{T}|n - H(X_{\mathcal{T}})\\
&\overset{(b)}{=} H(K_{\mathcal{T}}) + H(S_{\mathcal{T}}) - H(X_{\mathcal{T}})\\
&\overset{(c)}{=} H(K_{\mathcal{T}}, S_{\mathcal{T}}) - H(X_{\mathcal{T}})\\
&\overset{(d)}{=} H(K_{\mathcal{T}}, S_{\mathcal{T}}, X_{\mathcal{T}}) - H(X_{\mathcal{T}})\\
&= H(K_{\mathcal{T}}, S_{\mathcal{T}}|X_{\mathcal{T}})\\
&\overset{(e)}{\geqslant} H(K_{\mathcal{T}}, S_{\mathcal{T}}|K_{\mathcal{A}_t}, S_{\mathcal{A}_t}, X_{[L]})\\
&= H(K_{\mathcal{T}}, S_{\mathcal{T}}, S_{\mathcal{A}_t^c}|K_{\mathcal{A}_t}, S_{\mathcal{A}_t}, X_{[L]})\\
&\quad - H(S_{\mathcal{A}_t^c}|K_{\mathcal{A}_t\cup\mathcal{T}}, S_{\mathcal{A}_t\cup\mathcal{T}}, X_{[L]})\\
&\geqslant H(S_{\mathcal{A}_t^c}|K_{\mathcal{A}_t}, S_{\mathcal{A}_t}, X_{[L]}) - H(S_{\mathcal{A}_t^c}|K_{\mathcal{A}_t\cup\mathcal{T}}, S_{\mathcal{A}_t\cup\mathcal{T}}, X_{[L]})\\
&\overset{(f)}{=} H(S_{\mathcal{A}_t^c}|K_{\mathcal{A}_t}, S_{\mathcal{A}_t}, X_{[L]})\\
&\quad - H(S_{(\mathcal{A}_t\cup\mathcal{T})^c}|K_{\mathcal{A}_t\cup\mathcal{T}}, S_{\mathcal{A}_t\cup\mathcal{T}}, X_{[L]})\\
&\overset{(g)}{=} n(L-t-1) - C_t - n(L-(t+|\mathcal{T}|)-1) + C_{t+|\mathcal{T}|}\\
&\overset{(h)}{\geqslant} n|\mathcal{T}|(1-\alpha),
\end{aligned} \tag{23}$$

其中
(a) 由引理4得出；(b) 由用户序列的均匀性得出；(c) 由用户序列与局部随机性的独立性得出；
(d) 成立，因为可以从 $(K_{\mathcal{T}}, S_{\mathcal{T}})$ 中恢复 $X_{\mathcal{T}}$；(e) 成立，因为条件化会降低熵；(f) 成立，因为 $(\mathcal{A}_t^c\cap\mathcal{T}^c)\cup(\mathcal{A}_t^c\cap\mathcal{T})$，并根据链式法则；
(g) 根据引理2成立；
(h) 成立，因为 $C_{t+|\mathcal{T}|}-C_t=-\Delta|\mathcal{T}|$ 根据性质 1，并根据性质 3。

那么，对于满足 $|\mathcal{T}|=L-1$ 的 $\mathcal{T}\subseteq[L]$，我们有

$$\begin{aligned}
H(K_{\mathcal{T}}) &\overset{(a)}{\geqslant} H(K_{\mathcal{T}}, S_{\mathcal{T}}|X_{\mathcal{T}})\\
&\overset{(b)}{\geqslant} H(S_{\mathcal{T}}|X_{[L]})\\
&\overset{(c)}{=} H(S_{\mathcal{T}}, \Sigma_{[L]}|X_{[L]})\\
&\overset{(d)}{=} H(S_{[L]}|X_{[L]})\\
&\overset{(e)}{=} n(L-1) - C_0\\
&\overset{(f)}{\geqslant} n(L-1)(1-\alpha),
\end{aligned} \tag{24}$$

其中
（a）类似于（23）成立；
（b）成立，因为条件化降低熵；（c）根据（1）成立；（d）成立，因为 $|\mathcal{T}|=L-1$；
（e）根据引理2成立；（f）根据性质3成立。

最后，我们有

$$\begin{aligned}
H(K_{[L]}) &\geqslant H(K_{[L-1]})\\
&\geqslant n(L-1)(1-\alpha),
\end{aligned}$$

其中，最后一个不等式根据（24）成立。 ■

利用引理 5，现在我们刻画任意严格用户子集的局部随机性给定条件下的全局随机性熵。

引理 6。对于任意 $\mathcal{T}\subsetneq[L]$，我们有

$$H(U|K_{\mathcal{T}}) = n(L-|\mathcal{T}|-1)(1-\alpha), \tag{25}$$

证明。对于任意 $\mathcal{T}\subsetneq[L]$，我们有

$$\begin{aligned}
H(U|K_{\mathcal{T}}) &\overset{(a)}{=} H(U) - H(K_{\mathcal{T}})\\
&\overset{(b)}{=} n(L-1)(1-\alpha) - H(K_{\mathcal{T}})\\
&\overset{(c)}{=} n(L-1)(1-\alpha) - n|\mathcal{T}|(1-\alpha)\\
&= n(L-|\mathcal{T}|-1)(1-\alpha),
\end{aligned}$$

其中
(a) 成立，因为 $K_{\mathcal{T}}$ 是 U 的函数；(b) 由私有求和计算协议的最优性成立；(c) 成立，因为 $H(K_{\mathcal{T}})\leqslant\sum_{t\in\mathcal{T}}H(K_t)=n|\mathcal{T}|(1-\alpha)$ 由私有求和计算协议的最优性成立，并且因为 $H(K_{\mathcal{T}})\geqslant n|\mathcal{T}|(1-\alpha)$ 由引理 5 成立。

■

我们现在证明定理 4 ，利用引理 6 如下进行。对于任意 $\mathcal{T} \subsetneq [L]$，我们有

$$\begin{aligned}\frac{I(U;K_{\mathcal{T}})}{H(U)} &= \frac{H(U)-H(U|K_{\mathcal{T}})}{H(U)} \\ &= \frac{n(L-1)(1-\alpha)-n(L-|\mathcal{T}|-1)(1-\alpha)}{n(L-1)(1-\alpha)} \\ &= \frac{|\mathcal{T}|}{L-1}, \end{aligned} \tag{26}$$

其中第二个等号由引理6以及私有求和计算协议的最优性得出。此外，我们有

$$\begin{aligned}\frac{I(U;K_{[L]})}{H(U)} &= \frac{H(U)-H(U|K_{[L]})}{H(U)} \\ &= 1, \end{aligned} \tag{27}$$

其中第二个等号成立是因为，根据引理6,

$$H(U|K_{[L]}) \leqslant H(U|K_{[L-1]}) = 0.$$

因此，根据（26）和（27），我们有

$$\frac{I(U;K_{\mathcal{T}})}{H(U)} = \begin{cases} 0 & \text{if } |\mathcal{T}|=0 \\ \frac{|\mathcal{T}|}{L-1} & \text{if } |\mathcal{T}|\in[\![1,L-1]\!] \\ 1 & \text{if } |\mathcal{T}|=L \end{cases},$$

根据（14），这意味着 $(K_l)^{l\in[L]}$ 是一个 $(L-1,L-1,L)$ 坡道秘密共享方案的份额，其中 U 是秘密。

VIII. 总结

我们研究了分布式用户通过单向、公开且无噪声信道进行隐私求和的问题。我们的设定将安全求和问题推广为：允许针对给定的一组合谋用户发生受控程度的信息泄漏。对于固定的信息泄漏量，我们刻画了所需通信量、全局随机性以及用户局部随机性的最优值。在泄漏对称条件下，该条件确保所有用户在获取其他用户私有序列信息的能力方面不可区分，我们还推导出了每个用户局部随机性的最优个体速率。此外，我们通过证明生成用户的局部随机性需要秘密共享，建立了秘密共享与隐私求和之间的联系。

附录 A 性质的证明(3)

对于任意 $\mathcal{T} \subset [L]$，我们有

$$\begin{aligned} &I(S_{[L]};X_{[L]}|\Sigma_{[L]},S_{\mathcal{T}},K_{\mathcal{T}}) \\ &\leqslant H(S_{[L]}|\Sigma_{[L]},S_{\mathcal{T}},K_{\mathcal{T}}) \\ &\overset{(a)}{\leqslant} H(S_{[L]}|\Sigma_{[L]}) \\ &\overset{(b)}{=} H(S_L|S_{[L-1]},\Sigma_{[L]}) + \sum_{l\in[L-1]} H(S_l|S_{[l-1]},\Sigma_{[L]}) \\ &\overset{(c)}{=} \sum_{l\in[L-1]} H(S_l|S_{[l-1]},\Sigma_{[L]}) \\ &\overset{(d)}{\leqslant} \sum_{l\in[L-1]} H(S_l) \\ &\overset{(e)}{=} n(L-1), \end{aligned}$$

其中
(a) 成立是因为条件化降低熵；(b) 根据链式法则成立；(c) 成立是因为可以从 S_L 中恢复$(S_{[L-1]},\ \Sigma_{[L]})$；(d) 成立是因为条件化降低熵；(e) 根据定义1成立。

因此，(3) 的左侧总是不超过$n(L-1)$。

Appendix B
Proof of Properties 1–3

A. 性质*1* 的证明

令 $l \in [\![0,\ L-1]\!]$。令 $\mathcal{T} \subseteq [L]$，使得 $|\mathcal{T}|= l$ 且$\mathcal{T} =(t_i)^{i\in[l]}$。于是，我们有

$$l\Delta = \sum_{j\in[l]} [\mathbb{L}((t_i)_{i\in[j-1]}) - \mathbb{L}((t_i)_{i\in[j]})] = \mathbb{L}(\emptyset) - \mathbb{L}(\mathcal{T}).$$

因此，对于任意满足 $|\mathcal{T}|= l$ 的 $\mathcal{T} \subseteq [L-1]$，我们有 $C_l = \mathbb{L}(\emptyset) - l\Delta$。

B. 性质*2*的证明

Since $C_{L-1} = 0$, we have

$$(L-1)\Delta = \sum_{l\in[L-1]} (C_{l-1}-C_l) = C_0 - C_{L-1} = C_0 = \mathbb{L}(\emptyset) \geqslant 0, \tag{28}$$

因此，对于 $l \in [\![0,\ L-2]\!]$, $0 \leqslant \Delta = C_l - C_{l+1}$。注意到 $C_{L-1} = 0 = C_L$，即可得出该性质成立。

C. 性质*3*的证明

由（28），可得

$$\Delta = \frac{C_0}{L-1} \leqslant n\alpha.$$

Appendix C
Proof of Lemma 2

对于任意 $\mathcal{T} \subseteq [L]$，我们有

$$\begin{aligned} C_{|\mathcal{T}|} &\overset{(a)}{=} I(S_{[L]};X_{[L]}|\Sigma_{[L]},S_{\mathcal{T}},K_{\mathcal{T}}) \\ &= I(S_{[L]};X_{[L]},K_{\mathcal{T}}|\Sigma_{[L]},S_{\mathcal{T}}) - I(S_{[L]};K_{\mathcal{T}}|\Sigma_{[L]},S_{\mathcal{T}}) \\ &\overset{(b)}{=} I(S_{[L]};X_{[L]},K_{\mathcal{T}}|\Sigma_{[L]},S_{\mathcal{T}}) \\ &= H(S_{[L]}|\Sigma_{[L]},S_{\mathcal{T}}) - H(S_{[L]}|X_{[L]},K_{\mathcal{T}},\Sigma_{[L]},S_{\mathcal{T}}) \\ &\overset{(c)}{=} H(S_{\mathcal{T}^c}|\Sigma_{\mathcal{T}^c},S_{\mathcal{T}}) - H(S_{\mathcal{T}^c}|X_{[L]},K_{\mathcal{T}},\Sigma_{[L]},S_{\mathcal{T}}) \\ &\overset{(d)}{=} H(S_{\mathcal{T}^c}|\Sigma_{\mathcal{T}^c},S_{\mathcal{T}}) - H(S_{\mathcal{T}^c}|X_{[L]},K_{\mathcal{T}},S_{\mathcal{T}}) \\ &\overset{(e)}{=} H(S_{\mathcal{T}^c}|\Sigma_{\mathcal{T}^c}) - H(S_{\mathcal{T}^c}|X_{[L]},K_{\mathcal{T}},S_{\mathcal{T}}) \\ &\overset{(f)}{=} H(S_{\mathcal{T}^c}) - H(\Sigma_{\mathcal{T}^c}) - H(S_{\mathcal{T}^c}|X_{[L]},K_{\mathcal{T}},S_{\mathcal{T}}) \\ &\overset{(g)}{=} n(L-|\mathcal{T}|) - n\mathbb{1}\{\mathcal{T}^c \neq \emptyset\} - H(S_{\mathcal{T}^c}|X_{[L]},K_{\mathcal{T}},S_{\mathcal{T}}), \end{aligned}$$

其中
（a）由性质1成立；
（b）成立是因为

$$I(S_{[L]}; K_{\mathcal{T}}|\Sigma_{[L]}, S_{\mathcal{T}}) \leqslant I(S_{[L]}, \Sigma_{[L]}, S_{\mathcal{T}}; K_{\mathcal{T}}) = 0,$$

等式成立是因为用户序列与局部随机性相互独立；(c) 根据链式法则成立，且$(\Sigma_{[L]}, S_{\mathcal{T}})$与$(\Sigma_{\mathcal{T}^c}, S_{\mathcal{T}})$之间存在一一映射；(d) 成立是因为根据 (1)，可以从 $X_{[L]}$ 中重构出 $\Sigma_{[L]}$；(e) 根据$(S_{\mathcal{T}^c}, \Sigma_{\mathcal{T}^c})$与 $S_{\mathcal{T}}$的独立性成立；(f) 成立是因为 $H(S_{\mathcal{T}^c}, \Sigma_{\mathcal{T}^c}) = H(S_{\mathcal{T}^c})$；(g) 根据用户序列的均匀性成立。

参考文献

[1] R. A. Chou、J. Kliewer 和 A. Yener，《私密求和计算：共享随机性与隐私之间的权衡》，载于 IEEE国际信息论研讨会 (ISIT)，2024。[2] K. Bonawitz、V. Ivanov、B. Kreuter、A. Marcedone、H. B. McMahan、S. Patel、D. Ramage、A. Segal 和 K. Seth，《面向隐私保护机器学习的实用安全聚合》，载于 2017 年 ACM SIGSAC计算机与通信安全会议论文集，2017 年，第 1175–1191 页。[3] J. H. Bell、K. A. Bonawitz、A. Gasc´on、T. Lepoint 和 M. Raykova，《具有（多项式）对数开销的安全单服务器聚合》，载于 2020 年 ACM SIGSAC计算机与通信安全会议论文集，2020 年，第 1253–1269 页。[4] J. So、B. G¨uler 和 A. S. Avestimehr，《Turbo-aggregate：突破安全联邦学习中的二次聚合障碍》，IEEE信息论选题期刊，第 2 卷，489，2021 1，479，第 – 页。[5] S. Kadhe、N. Rajaraman、O. O. Koyluoglu 和 K. Ramchandran，《Fast-secagg：面向隐私保护联邦学习的可扩展安全聚合》，arXiv 预印本 arXiv:2009.11248，2020。[6] Y. Zhao 和 H. Sun，《支持用户掉线的信息论安全聚合》，IEEE信息论汇刊，第 68 卷，第 11 期，第 7471–7484 页，2022。[7] J. So、C. He、C.-S. Yang、S. Li、Q. Yu、R. E Ali、B. Guler 和 S. Avestimehr，《Lightsecagg：用于联邦学习安全聚合的轻量且通用设计》，机器学习与系统会议论文集，第 4 卷，第 694–720 页，2022。[8] T. Jahani-Nezhad、M. A. Maddah-Ali、S. Li 和 G. Caire，《Swiftagg+：实现联邦学习安全聚合中渐近最优的通信负载》，IEEE通信选题期刊，第 41 卷，第 4 期，第 977–989 页，2023。[9] K. Wan、H. Sun、M. Ji 和 G. Caire，《使用非编码分组密钥的信息论安全聚合》，arXiv 预印本 arXiv:2204.11364，2022。[10] 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，2023。[11] Z. Liu、J. Guo、K.-Y. Lam 和 J. Zhao，《面向隐私保护机器学习的高效抗掉线聚合》，IEEE信息取证与安全汇刊，第 18 卷，第 1839–1854 页，2022。[12] B. Chor 和 E. Kushilevitz，《模加法中的通信-隐私权衡》，信息处理快报，第 45 卷，第 4 期，第 205–210 页，1993。[13] M. Hayashi 和 T. Koshiba，《作为密码学资源的安全模零和随机性》，密码学电子预印本档案，2018。[14] Y. Zhao 和 H. Sun，《Expand-and-randomize：一种安全计算的代数方法》，Entropy，第 23 卷，第 11 期，第 1461 页，2021。[15] K. Wan、H. Sun、M. Ji 和 G. Caire，《论安全分布式线性可分计算》，IEEE通信选题期刊，第 40 卷，第 3 期，第 912–926 页，2022。[16] G. R. Blakley 和 C. Meadows，《斜坡方案的安全性》，载于密码技术理论与应用研讨会。Springer，1984 年，第 242–268 页。[17] H. Yamamoto，《使用 (k, l, n) 门限方案的秘密共享系统》，日本电子与通信（第一部分：通信），第 69 卷，第 9 期，第 46–54 页，1986。[18] Y. Zhao 和 H. Sun，《安全求和：容量区域、组间密钥与可行性》，*IEEE*信息论汇刊，2023。[19] H. Tyagi，《具有机密性的分布式函数计算》，*IEEE*通信选题期刊，第 31 卷，第 4 期，第 691–701 页，2013。[20] D. Data、G. R. Kurri、J. Ravi 和 V. M. Prabhakaran，《交互式安全函数计算》，*IEEE*信息论汇刊，第 66 卷，第 9 期，第 5492–5521 页，2020。[21] D. Data、V. M. Prabhakaran 和 M. M. Prabhakaran，《安全计算的通信与随机性下界》，*IEEE*信息论汇刊，第 62 卷，第 7 期，第 3901–3929 页，2016。[22] H. Tyagi、P. Narayan 和 P. Gupta，《何时能够安全计算一个函数？》，*IEEE*信息论汇刊，第 57 卷，第 10 期，第 6337–6350 页，2011。[23] W. Tu 和 L. Lai，《具有隐私与保密约束的函数计算》，*IEEE*信息论汇刊，第 65 卷，第 10 期，第 6716–6733 页，2019。[24] R. A. Chou 和 J. Kliewer，《无安全链路的函数计算：信息与泄漏速率》，载于*IEEE*国际信息论研讨会 *(ISIT)*，2022 年，第 1223–1228 页。[25] D. R. Stinson，密码学：理论与实践。Chapman and Hall/CRC，2005。[26] M. Yoshida、T. Fujiwara 和 M. P. Fossorier，《最优均匀秘密共享》，*IEEE*信息论汇刊，第 65 卷，第 1 期，第 436–443 页，2018。[27] M. Yoshida、T. Fujiwara 和 M. Fossorier，《最优一般门限秘密共享》，载于国际信息论安全会议，*ICITS*。Springer，2012 年，第 187–204 页。[28] R. Chou 和 J. Kliewer，《安全分布式存储：存储速率-隐私权衡与基于异或的编码方案》，载于*IEEE*国际信息论研讨会 *(ISIT)*，2020 年，第 605–610 页。[29] R. A. Chou 和 J. Kliewer，《安全分布式存储：存储速率与隐私泄露之间的最优权衡》，*IEEE*信息论汇刊，第 70 卷，第 5 期，第 3658–3668 页，2024。