On the Optimality of Secure Aggregation with Uncoded Groupwise Keys Against User Dropouts and User Collusion

Ziting Zhang*, Jiayu Liu*, Kai Wan*, Hua Sun†, Mingyue Ji‡, Giuseppe Caire§
*Huazhong University of Science and Technology, 430074 Wuhan, China, {zzting,jiayuliu,kai_wan}@hust.edu.cn
†University of North Texas, Denton, TX 76203, USA, hua.sun@unt.edu
‡University of Utah, Salt Lake City, UT 84112, USA, mingyue.ji@utah.edu
§Technische Universität Berlin, 10587 Berlin, Germany, caire@tu-berlin.de

2024 IEEE International Symposium on Information Theory (ISIT) | 979-8-3503-8284-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISIT57864.2024.10619337

***Abstract*—This paper studies information theoretic secure aggregation in federated learning, involving K distributed users and a central server. "Secure" means that the server can only get aggregated locally trained model updates, with no other information about the local users' data being leaked to the server. In addition, the effect of user dropouts is considered, where at most $\mathsf{K}-\mathsf{U}$ users can drop and the identity of these users cannot be predicted in advance. Users share keys in an offline way independently of the models, and send the encrypted models to the server in the model aggregation phase. The objective of this problem is to minimize the number of transmissions in the model aggregation phase. A secure aggregation scheme with uncoded groupwise keys, where any S users share an independent key, was recently proposed to achieve the same optimal communication cost as the best scheme with coded keys when $\mathsf{S}>\mathsf{K}-\mathsf{U}$. In this paper, we additionally consider the potential impact of user collusion, where up to T users may collude with the server. For this setting, we propose a secure aggregation scheme with uncoded groupwise keys that guarantees secure aggregation with U non-dropped users and T colluding users provided that $\mathsf{K}-\mathsf{U}+1\leq\mathsf{S}\leq\mathsf{K}-\mathsf{T}$, and is proven to achieve the optimality without any constraint on the keys.**

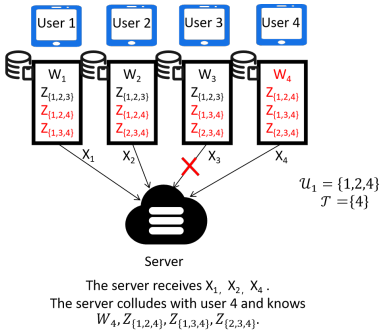
I. Introduction

The emergence of federated learning [1] allows multiple participants to train models collaboratively: instead of centralizing data on a server, models are sent to the users, trained locally based on the local data of users, and only aggregated model updates are shared [2]–[4]. It has been shown that their updated models can still reveal some information about their private data [5]. Secure aggregation was originally introduced in [6] by using cryptographic tools, which guarantees that the server cannot obtain any other information about users' local data, except the sum of the users' updated models. The scheme in [6] is formed by two phases, referred to as key sharing and model aggregation. During the key sharing phase, some keys (unknown to the server) are shared among the users. In the subsequent model aggregation phase, the users mask their updated models by the keys and then send them to the server. Following the seminal work in [6], various cryptographic secure aggregation schemes have been proposed based on different key sharing and model aggregation protocols, according to different threat scenarios; refer to [7], [8] for comprehensive reviews on secure aggregation protocols.

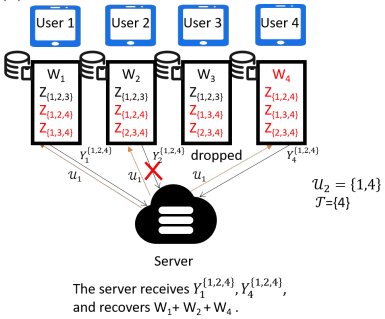
The first information theoretic formulation on secure aggregation was introduced in [9] containing one server and K users, each with some local data. The potential effect of user dropouts and collusion was also considered in [9].[1] The problem in [9] considers one iteration of the learning process, and assumes that the key sharing is performed offline, where the keys could be any random variable independent of the users' local data. In order to guarantee secure aggregation against user dropouts, there should be two-round transmissions in the model aggregation phase, where in the first round each user transmits masked updated models, and then in the second round, according to the identity of the dropped users in the first round, each non-dropped user further transmits some messages for the sake of decryption. The security constraint imposes that, except for the computation task (i.e., the sum of the updated models from the non-dropped users after the first round), the server cannot obtain any other information about the non-colluded users' local data, even if it knows the keys and the input vectors from at most T colluding users. The objective is to characterize the region of all achievable communication rates $(\mathsf{R}_1,\mathsf{R}_2)$, where R_1 (resp. R_2) is defined as the largest first round (resp. second round) transmission load among all users (resp. users in $\mathcal{U}_1$). The capacity region $\{(\mathsf{R}_1,\mathsf{R}_2):\mathsf{R}_1\geq 1,\mathsf{R}_2\geq 1/(\mathsf{U}-\mathsf{T})\}$ was characterized in [9], where U is the minimum number of non-dropped users.

The information theoretic secure aggregation schemes [9], [10] are built on coded keys, where the keys were either assigned by a trusted third party or shared through private links among users. Recently in [11], an additional constraint on the offline keys was considered into the information theoretic secure aggregation problem, referred to as "uncoded groupwise keys", where "groupwise" means that each key is shared among S users and "uncoded" means that the keys

[1]Due to some practical problems such as unstable network connections or delayed transmissions, the effect of user dropouts is common in federated learning, and the identity of the dropped users is always unpredictable in advance. Besides, when the server is an active adversary, it may collude with some users and be able to obtain the keys and updated models of those users.



(a) The transmissions in the first round.



(b) The transmissions in the second round.

Fig. 1: An example of $(\mathsf{K}, \mathsf{U}, \mathsf{S}, \mathsf{T}) = (4, 2, 3, 1)$ information theoretic secure aggregation with uncoded groupwise keys.

are mutually independent. Different from the generation of coded keys, uncoded groupwise keys could be generated by key agreement protocols such as [12]–[15] even in the absence of a trusted third party or private links. Without user collusion (i.e., $\mathsf{T} = 0$), the capacity region of secure aggregation with uncoded groupwise keys was characterized in [11], [16]; note that, the capacity region coincides with that for unconstrained keys in [9] only when $\mathsf{S} > \mathsf{K} - \mathsf{U}$. In [17], we proposed two schemes with uncoded groupwise keys, which can achieve the same capacity region as in [9] when $\mathsf{S} = \mathsf{K} - \mathsf{U} + 1$ and $\mathsf{S} = \mathsf{K} - \mathsf{T}$, respectively.

Main Contribution: When $\mathsf{K} - \mathsf{U} + 1 \leq \mathsf{S} \leq \mathsf{K} - \mathsf{T}$, we propose a secure aggregation scheme that achieves the same capacity region as in [9]. When $\mathsf{S} > \mathsf{K} - \mathsf{T}$, it is proved that secure aggregation is impossible. The proposed scheme with additional tolerance against user collusion is not a direct extension from the scheme in [11], and is built on a new interference alignment strategy.

Notation Convention: Sets are denoted using calligraphic symbols. Vectors and matrices are represented in bold. System parameters are indicated in sans-serif font. The notation $[a : b]$ defines a range as $\{a, a+1, \ldots, b\}$. $[n]$ denotes the set $\{1, 2, \ldots, n\}$. $\mathbb{F}_{\mathsf{q}}$ represents a finite field with order q. For a set $\mathcal{S}$ and an integer $s \leq |\mathcal{S}|$, $\binom{\mathcal{S}}{\mathsf{s}}$ represents the collection of all subsets of $\mathcal{S}$ containing exactly s elements. Entropies are calculated in base q, where q denotes the field size. For a set $\mathcal{S}$, we denote the i^{th} smallest element by $\mathcal{S}(i)$. $\mathbf{a}([b])$ represents the vector composed by the first b elements of $\mathbf{a}$.

II. System Model

We consider the $(\mathsf{K}, \mathsf{U}, \mathsf{S}, \mathsf{T})$ information theoretic secure aggregation problem with uncoded groupwise keys, as illustrated in Fig. 1. The server aims to recover $\sum_{k\in[\mathsf{K}]} W_k$ from $\mathsf{K} > 1$ users, where each input vector W_k can only be computed by user k and contains L uniformly i.i.d. symbols over a finite field $\mathbb{F}_{\mathsf{q}}$. Each group of S users share and store a common key in the key sharing phase. More precisely, for each $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$, the users in $\mathcal{V}$ share a key denoted by $Z_{\mathcal{V}}$, with large enough size. The keys are mutually independent of each other and independent of the data; denote the set of keys stored by user k where $k \in [\mathsf{K}]$ by $Z_k = \{Z_{\mathcal{V}} : k \in \mathcal{V}\}$. After the key sharing phase, the model aggregation phase contains two rounds of transmissions in order to tolerate user dropouts.

First round. Each user $k \in [\mathsf{K}]$ sends the message X_k to the server, which is a function of W_k and Z_k, i.e.,

$$H(X_k | W_k, Z_k) = 0. \tag{1}$$

Due to the user dropouts, the server only receives $(X_k : k \in \mathcal{U}_1)$, where $\mathcal{U}_1 \subseteq [\mathsf{K}]$ and $|\mathcal{U}_1| \geq \mathsf{U}$. The communication rate in the first round R_1 is defined as the maximum transmission load among all users, where $\mathsf{R}_1 := \max_{k\in[\mathsf{K}]} H(X_k)/\mathsf{L}$.

Second round. The server informs the users in $\mathcal{U}_1$ of the set $\mathcal{U}_1$. Each user $k \in \mathcal{U}_1$ then sends the message $Y_k^{\mathcal{U}_1}$ to the server, which is a function of $(Z_k, W_k, \mathcal{U}_1)$, i.e.,

$$H\left(Y_k^{\mathcal{U}_1} | Z_k, W_k, \mathcal{U}_1\right) = 0. \tag{2}$$

Denote the set of non-dropped users after the second round by $\mathcal{U}_2$, where $\mathcal{U}_2 \subseteq \mathcal{U}_1$ and $|\mathcal{U}_2| \geq \mathsf{U}$. So the server receives $\left(Y_k^{\mathcal{U}_1} : k \in \mathcal{U}_2\right)$ from the second round. The communication rate in the second round R_2 is defined as the maximum transmission load among users over all possible sets of $\mathcal{U}_1$, where $\mathsf{R}_2 := \max_{\mathcal{U}_1 \subseteq [\mathsf{K}]: |\mathcal{U}_1| \geq \mathsf{U}} \max_{k\in\mathcal{U}_1} H\left(Y_k^{\mathcal{U}_1}\right)/\mathsf{L}$.

Decodability. The server should recover $\sum_{k\in\mathcal{U}_1} W_k$ from the two-round transmissions $(X_k : k \in \mathcal{U}_1), \left(Y_k^{\mathcal{U}_1} : k \in \mathcal{U}_2\right)$; thus for any $\mathcal{U}_2 \subseteq \mathcal{U}_1 \subseteq [\mathsf{K}]$, where $|\mathcal{U}_1| \geq |\mathcal{U}_2| \geq \mathsf{U}$,

$$H\left(\sum_{k\in\mathcal{U}_1} W_k \middle| (X_k : k \in \mathcal{U}_1), (Y_k^{\mathcal{U}_1} : k \in \mathcal{U}_2)\right) = 0. \tag{3}$$

Security. For any set $\mathcal{T}$ where $\mathcal{T} \subseteq [\mathsf{K}]$ and $|\mathcal{T}| \leq \mathsf{T}$, the server cannot obtain any other information about the input vectors of non-colluding users, except for $\sum_{k\in\mathcal{U}_1} W_k$; for any $\mathcal{U}_1 \subseteq [\mathsf{K}]$ where $|\mathcal{U}_1| \geq \mathsf{U}$, and any $\mathcal{T} \subseteq [\mathsf{K}]$ where $|\mathcal{T}| \leq \mathsf{T}$,

$$I\big((W_k : k \in [K]); (X_k : k \in [\mathsf{K}]), (Y_k^{\mathcal{U}_1} : k \in \mathcal{U}_1)\Big| \sum_{k\in\mathcal{U}_1} W_k, (W_k, Z_k : k \in \mathcal{T})\big) = 0. \tag{4}$$

Objective. If a secure aggregation scheme with uncoded groupwise keys satisfies the encodability constraints in (1) and (2), the decodability constraint in (3), and the security constraint in (4), the rate tuple of the scheme $(\mathsf{R}_1, \mathsf{R}_2)$ is achievable. Our objective is to find the capacity region $\mathcal{R}^\star$, defined as the closure of the set of all achievable rate tuples.

Existing converse and achievable bounds on the considered problem. A converse bound for the information theoretic secure aggregation problem against user dropouts and user collusion without the uncoded groupwise keys was proposed in [9], which can be directly applied to our considered problem.

Theorem 1 ([9])**.** *For the* $(\mathsf{K},\mathsf{U},\mathsf{S},\mathsf{T})$ *information theoretic secure aggregation problem with uncoded groupwise keys, if* $\mathsf{U}>\mathsf{T}$*, each achievable rate tuple* $(\mathsf{R}_1,\mathsf{R}_2)$ *satisfies*

$$\mathsf{R}_1\geq 1,\ \mathsf{R}_2\geq 1/(\mathsf{U}-\mathsf{T}). \tag{5}$$

The converse bound in Theorem 1 was shown to be achievable in [9], [10], both with coded keys. It was also proved in [9] that, secure aggregation is possible only when $\mathsf{U}>\mathsf{T}$. The capacity region for the case $\mathsf{T}=0$ was characterized in [11], [16]. **So in the rest of this paper, we will only consider the case** $\mathsf{U}>\mathsf{T}>0$**.**

Theorem 2 ([17])**.** *For the* $(\mathsf{K},\mathsf{U},\mathsf{S},\mathsf{T})$ *information theoretic secure aggregation problem where* $\mathsf{S}=\mathsf{K}-\mathsf{U}+1$*,*

$$\mathcal{R}^\star=\{(\mathsf{R}_1,\mathsf{R}_2):\mathsf{R}_1\geq 1,\mathsf{R}_2\geq 1/(\mathsf{U}-\mathsf{T})\}. \tag{6}$$

When $\mathsf{K}-\mathsf{U}+1\leq\mathsf{S}\leq\mathsf{K}-\mathsf{T}$*,* $(\mathsf{R}_1,\mathsf{R}_2)$ *is achievable if*

$$\mathsf{R}_1\geq 1,\mathsf{R}_2\geq\frac{1}{\mathsf{S}+\mathsf{U}-\mathsf{K}}. \tag{7}$$

It can be seen from (7) that, when $\mathsf{S}=\mathsf{K}-\mathsf{T}$, the scheme in [17] can achieve the capacity region $\{\mathsf{R}_1\geq 1,\mathsf{R}_2\geq\frac{1}{\mathsf{U}-\mathsf{T}}\}$, which coincides with the converse in (5).

III. Main Results

When $\mathsf{S}>\mathsf{K}-\mathsf{T}$, we have $\binom{\mathsf{K}-\mathsf{T}}{\mathsf{S}}=0$ and thus each key is known by at least one user colluding with the server. So the server knows all the keys in the system, and obviously secure aggregation is not possible. Our main contribution in this paper is proposing a scheme with uncoded groupwise keys that achieves the optimal rate when $\mathsf{K}-\mathsf{U}+1\leq\mathsf{S}\leq\mathsf{K}-\mathsf{T}$.

Theorem 3. *For the* $(\mathsf{K},\mathsf{U},\mathsf{S},\mathsf{T})$ *information theoretic secure aggregation problem with uncoded groupwise keys, when* $\mathsf{K}-\mathsf{U}+1\leq\mathsf{S}\leq\mathsf{K}-\mathsf{T}$*, we have*

$$\mathcal{R}^\star=\left\{(\mathsf{R}_1,\mathsf{R}_2):\mathsf{R}_1\geq 1,\mathsf{R}_2\geq\frac{1}{\mathsf{U}-\mathsf{T}}\right\}. \tag{8}$$

The converse bound for Theorem 3 can be derived from Theorem 1. For the achievability, we propose a new secure aggregation scheme with uncoded groupwise keys against user dropouts and user collusion in Section IV. By Theorem 3, it is interesting to see that when $\mathsf{K}-\mathsf{U}+1\leq\mathsf{S}\leq\mathsf{K}-\mathsf{T}$, uncoded groupwise keys can achieve the general optimality characterized in [9]; when $\mathsf{S}>\mathsf{K}-\mathsf{T}$, as explained before, secure aggregation with uncoded groupwise keys is not possible.

Note that the proposed scheme is not a direct extension from the secure aggregation scheme in [11], which works for the case $\mathsf{S}\geq\mathsf{K}-\mathsf{U}+1$ and $\mathsf{T}=0$. The reasons are as follows.

- To guarantee the security against user collusion, a stronger constraint on the security is required. The security proof in this paper is based on a genie-aided method, which is not required for the case $\mathsf{T}=0$.
- For the case $\mathsf{T}=0$, since having more users knowing the same key will not hurt and when $\mathsf{S}\geq\mathsf{K}-\mathsf{U}+1$ the capacity region does not change, it suffices to only consider the case $\mathsf{S}=\mathsf{K}-\mathsf{U}+1$ and propose a secure aggregation scheme, as in [11]. However, for the case $\mathsf{T}>0$, increasing S may lead to a higher threat, since the server will know more keys by colluding with users. So we cannot directly state that the scheme for $\mathsf{S}>\mathsf{K}-\mathsf{U}+1$ could be directly obtained from that for $\mathsf{S}=\mathsf{K}-\mathsf{U}+1$.

IV. Proof of Theorem 3

Recall that when $\mathsf{S}=\mathsf{K}-\mathsf{T}$, the scheme in [17] can achieve the capacity region in (8). In the following, we will propose a secure aggregation scheme for the case $\mathsf{K}-\mathsf{U}+1\leq\mathsf{S}<\mathsf{K}-\mathsf{T}$, which can achieve the capacity region in (8).

For each user $k\in[\mathsf{K}]$, we divide W_k into $\mathsf{U}-\mathsf{T}$ non-overlapping and equal-length pieces, defined as $W_k=(W_{k,1},\ldots,W_{k,\mathsf{U}-\mathsf{T}})$, each containing $\mathsf{L}/(\mathsf{U}-\mathsf{T})$ uniformly i.i.d. symbols on $\mathbb{F}_\mathsf{q}$. Without loss of generality, we can assume that q is large enough as shown in [9].

For each $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$, the users in $\mathcal{V}$ share a key $Z_\mathcal{V}$ with $\mathsf{L}/(\mathsf{U}-\mathsf{T})$ uniformly i.i.d. symbols on $\mathbb{F}_\mathsf{q}$, next we generate a U-length vertical coefficient vector $\mathbf{a}_\mathcal{V}:=[a_{\mathcal{V},1},\ldots,a_{\mathcal{V},\mathsf{U}}]^\mathsf{T}$, where $a_{\mathcal{V},i}\in\mathbb{F}_\mathsf{q}$ for each $i\in[\mathsf{U}]$. Note that the selection of $\mathbf{a}_\mathcal{V}$ is the non-trivial step in the proposed scheme, we adopt a new coefficient vector design different from that in [17] (which cannot guarantee the security and decodability for the regime $\mathsf{S}>\mathsf{K}-\mathsf{U}+1$). The selection will be clarified later, which is based on a new interference alignment method.

First round. In the first round of transmission, each user $k\in[\mathsf{K}]$ sends $X_k=(X_{k,1},\ldots,X_{k,\mathsf{U}-\mathsf{T}})$ to the server,

$$X_{k,j}=W_{k,j}+\sum_{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}:k\in\mathcal{V}}a_{\mathcal{V},j}Z_{\mathcal{V},k},\ \forall j\in[\mathsf{U}-\mathsf{T}], \tag{9}$$

where the vector X_k contains L symbols, leading to $\mathsf{R}_1=1$. Since $\mathsf{S}\geq\mathsf{K}-\mathsf{U}+1$, all sets $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$ satisfy $\mathcal{V}\cap\mathcal{U}_1\neq\emptyset$. Hence, after receiving $(X_k:k\in\mathcal{U}_1)$, the server recovers

$$\begin{aligned}\sum_{k\in\mathcal{U}_1}X_{k,j}&=\sum_{k\in\mathcal{U}_1}W_{k,j}+\sum_{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}:\mathcal{V}\cap\mathcal{U}_1\neq\emptyset}\left(a_{\mathcal{V},j}\sum_{k_1\in\mathcal{V}\cap\mathcal{U}_1}Z_{\mathcal{V},k_1}\right)\\&=\sum_{k\in\mathcal{U}_1}W_{k,j}+\sum_{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}}a_{\mathcal{V},j}Z_\mathcal{V}^{\mathcal{U}_1},\ \forall j\in[\mathsf{U}-\mathsf{T}],\end{aligned}$$

where we define a coded key as $Z_\mathcal{V}^{\mathcal{U}_1}:=\sum_{k_1\in\mathcal{V}\cap\mathcal{U}_1}Z_{\mathcal{V},k_1}$, for each $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$. Thus to obtain $\sum_{k\in\mathcal{U}_1}W_k$, the server should further recover $\sum_{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}}a_{\mathcal{V},j}Z_\mathcal{V}^{\mathcal{U}_1},\ \forall j\in[\mathsf{U}-\mathsf{T}]$ in the second round. We denote the sets in $\binom{[\mathsf{K}]}{\mathsf{S}}$ by $\mathcal{S}_1,\ldots,\mathcal{S}_{\binom{\mathsf{K}}{\mathsf{S}}}$, and for each $k\in[\mathsf{K}]$ denote the sets in $\binom{[\mathsf{K}]\backslash\{k\}}{\mathsf{S}}$ by $\mathcal{S}_1^{\overline{k}},\ldots,\mathcal{S}_{\binom{\mathsf{K}-1}{\mathsf{S}}}^{\overline{k}}$.

Second round. In the second round, we let the server recover U-dimensional keys,

$$\begin{bmatrix} F_1 \\ \vdots \\ F_{\mathsf{U}} \end{bmatrix} = \left[\mathbf{a}_{\mathcal{S}_1}, \ldots, \mathbf{a}_{\mathcal{S}_{\binom{\mathsf{K}}{\mathsf{S}}}}\right] \begin{bmatrix} Z^{\mathcal{U}_1}_{\mathcal{S}_1} \\ \vdots \\ Z^{\mathcal{U}_1}_{\mathcal{S}_{\binom{\mathsf{K}}{\mathsf{S}}}} \end{bmatrix}, \tag{10}$$

where each $F_j, j \in [\mathsf{U}]$ contains $\mathsf{L}/(\mathsf{U}-\mathsf{T})$ symbols. We let each user transmit one linear combination of $F_1, \ldots, F_{\mathsf{U}}$; thus user $k \in \mathcal{U}_1$ sends

$$Y^{\mathcal{U}_1}_k = \mathbf{s}_k \begin{bmatrix} F_1 \\ \vdots \\ F_{\mathsf{U}} \end{bmatrix} = \mathbf{s}_k \left[\mathbf{a}_{\mathcal{S}_1}, \ldots, \mathbf{a}_{\mathcal{S}_{\binom{\mathsf{K}}{\mathsf{S}}}}\right] \begin{bmatrix} Z^{\mathcal{U}_1}_{\mathcal{S}_1} \\ \vdots \\ Z^{\mathcal{U}_1}_{\mathcal{S}_{\binom{\mathsf{K}}{\mathsf{S}}}} \end{bmatrix}, \tag{11}$$

where $\mathbf{s}_k$ is a row vector with U elements. $\mathbf{s}_k$ should be a left null space vector of $\left[\mathbf{a}_{\mathcal{S}^{\overline{k}}_1}, \ldots, \mathbf{a}_{\mathcal{S}^{\overline{k}}_{\binom{\mathsf{K}-1}{\mathsf{S}}}}\right]$, corresponding to the coded keys which user k cannot compute. Each $Y^{\mathcal{U}_1}_k$ consists of $\mathsf{L}/(\mathsf{U}-\mathsf{T})$ symbols, which leads to $\mathsf{R}_2 = 1/(\mathsf{U}-\mathsf{T})$.

We can treat each coded key which user k cannot compute as an interference to user k. To guarantee the existence of $\mathbf{s}_k$, the following constraint should be satisfied.

Constraint 1 (Encodability constraint)**.** *For each user $k \in [\mathsf{K}]$, $\left[\mathbf{a}_{\mathcal{S}^{\overline{k}}_1}, \ldots, \mathbf{a}_{\mathcal{S}^{\overline{k}}_{\binom{\mathsf{K}-1}{\mathsf{S}}}}\right]$ has rank no more than $\mathsf{U}-1$.*

In other words, Constraint 1 imposes that the dimension of the interferences to user k should be no more than $\mathsf{U}-1$.

For the decodability, we let the server can recover $F_1, F_2, \ldots, F_{\mathsf{U}}$ from any U users in the second round. So we have the following constraint.

Constraint 2 (Decodability constraint)**.** *Any U vectors in $\{\mathbf{s}_k : k \in [\mathsf{K}]\}$ are linearly independent.*

We denote all sets $\mathcal{V} \in \binom{[\mathsf{K}]\setminus\mathcal{T}}{\mathsf{S}}$ by $\mathcal{S}_{\overline{\mathcal{T}},1}, \ldots, \mathcal{S}_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|}{\mathsf{S}}}$ and all sets $\mathcal{V} \in \binom{[\mathsf{K}]\setminus\mathcal{T}}{\mathsf{S}}$ where $k \in \mathcal{V}$ by $\mathcal{S}^k_{\overline{\mathcal{T}},1}, \ldots, \mathcal{S}^k_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|-1}{\mathsf{S}-1}}$. Finally, we generate the following constraint for the information theoretic security against user collusion.

Constraint 3 (Security constraint)**.** *For each $k \in [\mathsf{K}]$ and each $\mathcal{T} \subseteq [\mathsf{K}]\setminus\{k\}$ where $|\mathcal{T}| \le \mathsf{T}$, we have (recall $\mathbf{a}([b])$ represents the vector containing the first b elements of $\mathbf{a}$)*

$$\left[\mathbf{a}_{\mathcal{S}^k_{\overline{\mathcal{T}},1}}([\mathsf{U}-|\mathcal{T}|]), \ldots, \mathbf{a}_{\mathcal{S}^k_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|-1}{\mathsf{S}-1}}}([\mathsf{U}-|\mathcal{T}|])\right] \tag{12}$$

has rank equal to $\mathsf{U}-|\mathcal{T}|$.

If Constraints 1-3 are satisfied, the resulting secure aggregation scheme has the property in the following lemma, whose proof is given in Appendix A of [18].

Lemma 1. *If Constraints 1-3 are satisfied, then for any $\mathcal{T} \subseteq [\mathsf{K}]$ where $|\mathcal{T}| \le \mathsf{T}$, we have*

$$\left[\mathbf{a}_{\mathcal{S}_{\overline{\mathcal{T}},1}}, \ldots, \mathbf{a}_{\mathcal{S}_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|}{\mathsf{S}}}}\right] \text{ has rank equal to } \mathsf{U}-|\mathcal{T}|. \tag{13}$$

We provide an intuitive proof on the security if Constraints 1-3 are satisfied.

Consider the case $|\mathcal{T}| = \mathsf{T}$. For each $k \in [\mathsf{K}]\setminus\mathcal{T}$, the matrix $\left[\mathbf{a}_{\mathcal{S}^k_{\overline{\mathcal{T}},1}}([\mathsf{U}-|\mathcal{T}|]), \ldots, \mathbf{a}_{\mathcal{S}^k_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|-1}{\mathsf{S}-1}}}([\mathsf{U}-|\mathcal{T}|])\right]$ in (12), which is the coefficient matrix of the keys in $X_{k,1}, \ldots, X_{k,\mathsf{U}-\mathsf{T}}$ unknown to the users in $\mathcal{T}$, has rank $\mathsf{U}-\mathsf{T}$. In addition, the keys are independent of W_k. Hence, from $X_k = (X_{k,1}, \ldots, X_{k,\mathsf{U}-\mathsf{T}})$ and the keys known by the users in $\mathcal{T}$, the server cannot get any information about W_k. In addition, the matrix $\left[\mathbf{a}_{\mathcal{S}_{\overline{\mathcal{T}},1}}, \ldots, \mathbf{a}_{\mathcal{S}_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|}{\mathsf{S}}}}\right]$ in (13) has rank equal to $\mathsf{U}-\mathsf{T}$, thus the server can additionally recover $\frac{\mathsf{U}-\mathsf{T}}{\mathsf{U}-\mathsf{T}}\mathsf{L} = \mathsf{L}$ symbols from the second round transmission. By the seminal result by Shannon [19], the server can at most recover L symbols on $(W_k : k \in [\mathsf{K}]\setminus\mathcal{T})$, which is exactly $\sum_{k\in\mathcal{U}_1\setminus\mathcal{T}} W_k$ by the decodability.

Consider the case $|\mathcal{T}| < \mathsf{T}$. A genie-aided method is used to prove the security. We consider a genie-aided system, in the first round each user $k \in [\mathsf{K}]$ also sends $X_{k,j} = W_{k,j} + \sum_{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}:k\in\mathcal{V}} a_{\mathcal{V},j} Z_{\mathcal{V},k}$, $\forall j \in [\mathsf{U}-\mathsf{T}+1 : \mathsf{U}-|\mathcal{T}|]$, where $W_{k,j}$ for $j \in [\mathsf{U}-\mathsf{T}+1 : \mathsf{U}-|\mathcal{T}|]$ represents the virtual input vector piece uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}^{\frac{\mathsf{L}}{\mathsf{U}-\mathsf{T}}\times(\mathsf{T}-|\mathcal{T}|)}$. Since the matrix $\left[\mathbf{a}_{\mathcal{S}^k_{\overline{\mathcal{T}},1}}([\mathsf{U}-|\mathcal{T}|]), \ldots, \mathbf{a}_{\mathcal{S}^k_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|-1}{\mathsf{S}-1}}}([\mathsf{U}-|\mathcal{T}|])\right]$ in (12) has rank to $\mathsf{U}-|\mathcal{T}|$, from $X_{k,1}, \ldots, X_{k,\mathsf{U}-|\mathcal{T}|}$ and the keys known by the users in $\mathcal{T}$ the server cannot get any information about $W_{k,1}, \ldots, W_{k,\mathsf{U}-|\mathcal{T}|}$. In addition, the matrix $\left[\mathbf{a}_{\mathcal{S}_{\overline{\mathcal{T}},1}}, \ldots, \mathbf{a}_{\mathcal{S}_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|}{\mathsf{S}}}}\right]$ in (13) has rank equal to $\mathsf{U}-|\mathcal{T}|$; thus the server can recover $\frac{\mathsf{U}-|\mathcal{T}|}{\mathsf{U}-\mathsf{T}}\mathsf{L}$ symbols from the second round transmission, which are $\{\sum_{k\in\mathcal{U}_1\setminus\mathcal{T}} W_{k,j} : j \in [\mathsf{U}-|\mathcal{T}|]\}$ by the decodability. Moreover, the virtual pieces of the input vectors are independent of the real pieces; thus from $\{\sum_{k\in\mathcal{U}_1\setminus\mathcal{T}} W_{k,j} : j \in [\mathsf{U}-|\mathcal{T}|]\}$, the server can only obtain $\sum_{k\in\mathcal{U}_1\setminus\mathcal{T}} W_k$ about the real pieces.

Hence, the security of the proposed scheme is proved. If we can select the coefficient vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ satisfying Constraints 1-3, the proposed scheme is achievable with $\mathsf{R}_1 = 1$ and $\mathsf{R}_2 = 1/(\mathsf{U}-\mathsf{T})$. Next we introduce our selection on the U-dimension vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ through an example to illustrate the main idea, the general description is given in Appendix C of [18].

Example 1 $((\mathsf{K},\mathsf{U},\mathsf{S},\mathsf{T}) = (6,4,4,1))$**.** For each $\mathcal{V} \in \binom{[6]}{4}$, we aim to choose a coefficient vector $\mathbf{a}_{\mathcal{V}} = [a_{\mathcal{V},1}, a_{\mathcal{V},2}, a_{\mathcal{V},3}, a_{\mathcal{V},4}]^{\mathsf{T}}$, satisfying Constraints 1-3.

We generate a 4×4 matrix $[\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3, \mathbf{m}_4] = \begin{bmatrix} 1 & 2 & 3 & 2 \\ 3 & 2 & 3 & 3 \\ 1 & 4 & 1 & 3 \\ 1 & 4 & 1 & 4 \end{bmatrix}$, whose elements are uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}$.

Recall $\mathcal{S}(i)$ represents the i^{th} smallest element in $\mathcal{S}$. For each $\mathcal{V} \in \binom{[6]}{4}$ we define

$$\mathcal{M}_{\mathcal{V}} = \{\mathcal{M}_{\mathcal{V}}(1), \ldots, \mathcal{M}_{\mathcal{V}}(|\mathcal{M}_{\mathcal{V}}|)\} := \mathcal{V} \cap [3:6].$$

Our main strategy is to let $\mathbf{a}_{\mathcal{V}}$ be a vector in the linear space spanned by $\mathbf{m}_{\mathcal{M}_{\mathcal{V}}(1)-2}, \mathbf{m}_{\mathcal{M}_{\mathcal{V}}(2)-2}, \ldots, \mathbf{m}_{\mathcal{M}_{\mathcal{V}}(|\mathcal{M}_{\mathcal{V}}|)-2}$,

$$\begin{aligned}\mathbf{a}_{\mathcal{V}} &= [\mathbf{m}_{\mathcal{M}_{\mathcal{V}}(1)-2}, \mathbf{m}_{\mathcal{M}_{\mathcal{V}}(2)-2}, \ldots, \mathbf{m}_{\mathcal{M}_{\mathcal{V}}(|\mathcal{M}_{\mathcal{V}}|)-2}]\mathbf{b}_{\mathcal{V}} \\ &= b_{\mathcal{V},1}\mathbf{m}_{\mathcal{M}_{\mathcal{V}}(1)-2} + \cdots + b_{\mathcal{V},|\mathcal{M}_{\mathcal{V}}|}\ \mathbf{m}_{\mathcal{M}_{\mathcal{V}}(|\mathcal{M}_{\mathcal{V}}|)-2}, \quad (14)\end{aligned}$$

where $\mathbf{b}_{\mathcal{V}} := [b_{\mathcal{V},1}, \ldots, b_{\mathcal{V},|\mathcal{M}_{\mathcal{V}}|}]^{\mathsf{T}}$ is a column vector to be designed. For example, $\mathbf{a}_{\{2,3,4,6\}}$ is in the linear space spanned by $\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_4$.

After determining the composition of each vector $\mathbf{a}_{\mathcal{V}}$ in (14), we next select the vector $\mathbf{b}_{\mathcal{V}}$. We generate two 4-dimensional row vectors $\mathbf{s}_1$ and $\mathbf{s}_2$, whose elements are uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}$. For example, let $\mathbf{s}_1 = (2,2,3,1)$ and $\mathbf{s}_2 = (1,3,2,1)$. Recall that $\mathbf{s}_1$ and $\mathbf{s}_2$ represent the second-round coding vectors for users 1 and 2, respectively, as defined in (11).

For all sets $\mathcal{V} \in \binom{[6]}{4}$, we divide them into three classes: $|\mathcal{V} \cap [\mathsf{K}-\mathsf{U}]| = |\mathcal{V} \cap [2]| = 2$, $|\mathcal{V} \cap [2]| = 1$, and $|\mathcal{V} \cap [2]| = 0$.

First class. For each $\mathcal{V} \in \binom{[6]}{4}$ where $|\mathcal{V} \cap [2]| = 2$, by definition we have $\mathbf{b}_{\mathcal{V}} = [b_{\mathcal{V},1}, b_{\mathcal{V},2}]^{\mathsf{T}}$. We choose each of $b_{\mathcal{V},1}, b_{\mathcal{V},2}$ uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}$. For example, we let

$$\mathbf{a}_{\{1,2,3,4\}} = 4\mathbf{m}_1 + \mathbf{m}_2,\ \mathbf{a}_{\{1,2,3,5\}} = 4\mathbf{m}_1 + 3\mathbf{m}_3, \quad (15a)$$

$$\mathbf{a}_{\{1,2,3,6\}} = 2\mathbf{m}_1 + 4\mathbf{m}_4,\ \mathbf{a}_{\{1,2,4,5\}} = 4\mathbf{m}_2 + 3\mathbf{m}_3, \quad (15b)$$

$$\mathbf{a}_{\{1,2,4,6\}} = \mathbf{m}_2 + 3\mathbf{m}_4,\ \mathbf{a}_{\{1,2,5,6\}} = \mathbf{m}_3 + 2\mathbf{m}_4. \quad (15c)$$

Second class. For each $\mathcal{V} \in \binom{[6]}{4}$ where $|\mathcal{V} \cap [2]| = 1$, by definition we have $\mathbf{b}_{\mathcal{V}} = [b_{\mathcal{V},1}, b_{\mathcal{V},2}, b_{\mathcal{V},3}]^{\mathsf{T}}$. We fix $\mathbf{b}_{\mathcal{V}}$ by solving a linear equation. More precisely,

- if $\mathcal{V} \cap [2] = \{1\}$, the set $\mathcal{V}$ does not contain 2; thus for the encodability of the second-round transmission by user 2, we should have $\mathbf{s}_2\mathbf{a}_{\mathcal{V}} = 0$, satisfying which we choose the value of $\mathbf{b}_{\mathcal{V}}$. For example, when $\mathcal{V} = \{1,3,4,5\}$, we choose $\mathbf{b}_{\{1,3,4,5\}}$ satisfying $\mathbf{s}_2\mathbf{a}_{\{1,3,4,5\}} = 0$. We first randomly choose $b_{\{1,3,4,5\},1} = 4$ and $b_{\{1,3,4,5\},2} = 3$, which leads $\mathbf{a}_{\{1,3,4,5\}} = 4\mathbf{m}_1 + 3\mathbf{m}_2 + b_{\{1,3,4,5\},3}\ \mathbf{m}_3$; and then solve $b_{\{1,3,4,5\},3} = -\frac{112}{15}$ by $\mathbf{s}_2\mathbf{a}_{\{1,3,4,5\}} = 0$;
- if $\mathcal{V} \cap [2] = \{2\}$, the set $\mathcal{V}$ does not contain 1; thus for the encodability of the second-round transmission by user 1, we should have $\mathbf{s}_1\mathbf{a}_{\mathcal{V}} = 0$, satisfying which we choose the value of $\mathbf{b}_{\mathcal{V}}$.

Third class. Finally, for each set $\mathcal{V} \in \binom{[6]}{4}$ where $|\mathcal{V} \cap [2]| = 0$; in this example, only $\{3,4,5,6\}$ is in the third class. By (14), $\mathbf{a}_{\{3,4,5,6\}}$ is a linear combination of $\mathbf{m}_1, \ldots, \mathbf{m}_4$, and thus we have $\mathbf{b}_{\{3,4,5,6\}} := [b_{\{3,4,5,6\},1}, b_{\{3,4,5,6\},2}, b_{\{3,4,5,6\},3}, b_{\{3,4,5,6\},4}]^{\mathsf{T}}$. Since $\{3,4,5,6\}$ does not contain 1 nor 2, for the encodability of the second-round transmission by users 1 and 2, we should have $\mathbf{s}_1\mathbf{a}_{\{3,4,5,6\}} = 0$ and $\mathbf{s}_2\mathbf{a}_{\{3,4,5,6\}} = 0$, satisfying which we choose $\mathbf{b}_{\{3,4,5,6\}}$. We can first choose two elements of $\mathbf{b}_{\{3,4,5,6\}}$ uniformly and i.i.d. over $\mathbb{F}_{\mathsf{q}}$, and then solve the remaining two elements by $\mathbf{s}_1\mathbf{a}_{\{3,4,5,6\}} = 0$ and $\mathbf{s}_2\mathbf{a}_{\{3,4,5,6\}} = 0$; for example we choose $\mathbf{b}_{\{3,4,5,6\}} = [1, \frac{23}{11}, 5, -\frac{68}{11}]^{\mathsf{T}}$.

In conclusion, the selection on $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[6]}{4}$ is given in Table I of [18], which can be found in Appendix B of [18]. Next, we show that this selection satisfies Constraints 1-3.

Constraint 1. For user 1, Constraint 1 imposes that the matrix $[\mathbf{a}_{\{2,3,4,5\}}, \mathbf{a}_{\{2,3,4,6\}}, \mathbf{a}_{\{2,3,5,6\}}, \mathbf{a}_{\{2,4,5,6\}}, \mathbf{a}_{\{3,4,5,6\}}]$ has rank no more than $\mathsf{U}-1 = 3$. This constraint is satisfied because by construction the matrix has a non-zero left null vector $\mathbf{s}_1$ while the dimension of this matrix is 4×5. Similarly, Constraint 1 is satisfied for user 2. Then for user 3, Constraint 1 imposes that $[\mathbf{a}_{\{1,2,4,5\}}, \mathbf{a}_{\{1,2,4,6\}}, \mathbf{a}_{\{1,2,5,6\}}, \mathbf{a}_{\{1,4,5,6\}}, \mathbf{a}_{\{2,4,5,6\}}]$ has rank no more than $\mathsf{U}-1 = 3$. This constraint is satisfied because by construction each column of the matrix is a linear combination of $\mathbf{m}_2, \mathbf{m}_3, \mathbf{m}_4$. Similarly, Constraint 1 is also satisfied for users $4,5,6$.

Constraint 2. By our construction, we can check that $\mathbf{s}_1 = (2,2,3,1)$, $\mathbf{s}_2 = (1,3,2,1)$, $\mathbf{s}_3 = (1,-1,-1,1)$, $\mathbf{s}_4 = (0,1,-9,6)$, $\mathbf{s}_5 = (-5,1,1,1)$, $\mathbf{s}_6 = (0,0,-1,1)$, where any $\mathsf{U} = 4$ of them are linearly independent.

Constraint 3. Consider the case $|\mathcal{T}| = 0$. For each user $k \in [6]$, we can pick 4 vectors $\mathbf{a}_{\mathcal{V}}$ where $k \in \mathcal{V}$ such that these vectors are linearly independent. For users $1,2$, $\mathbf{a}_{\{1,2,3,4\}}, \mathbf{a}_{\{1,2,3,6\}}, \mathbf{a}_{\{1,2,4,5\}}, \mathbf{a}_{\{1,2,5,6\}}$ are linearly independent. For user 3, $\mathbf{a}_{\{1,2,3,4\}}, \mathbf{a}_{\{1,3,4,5\}}, \mathbf{a}_{\{1,3,4,6\}}, \mathbf{a}_{\{1,3,5,6\}}$ are linearly independent; similarly for user $4,5,6$.

Consider the case $|\mathcal{T}| = 1$. For each user $k \in [2]$, for example for user 1, if $\mathcal{T} = \{2\}$, $\mathbf{a}_{\{1,3,4,5\}}([3])$, $\mathbf{a}_{\{1,3,4,6\}}([3])$, $\mathbf{a}_{\{1,3,5,6\}}([3])$ are linearly independent; if $\mathcal{T} = \{i\}$ where $i \in [3:6]$, for example $i = 3$, $\mathbf{a}_{\{1,2,4,5\}}([3])$, $\mathbf{a}_{\{1,2,4,6\}}([3])$, $\mathbf{a}_{\{1,2,5,6\}}([3])$ are linearly independent. For each user $k \in [3:6]$, for example for user 3, if $\mathcal{T} = \{i\}$ where $i \in [2]$, for example $i = 1$, $\mathbf{a}_{\{2,3,4,5\}}([3])$, $\mathbf{a}_{\{2,3,4,6\}}([3])$, $\mathbf{a}_{\{2,3,5,6\}}([3])$ are linearly independent; if $\mathcal{T} = \{i\}$ where $i \in [4:6]$, for example $i = 4$, $\mathbf{a}_{\{1,2,3,5\}}([3])$, $\mathbf{a}_{\{1,2,3,6\}}([3])$, $\mathbf{a}_{\{1,3,5,6\}}([3])$ are linearly independent. Hence, Constraint 3 is satisfied. □

Remark 1. *To design a secure aggregation scheme against user collusion, the construction structure on the coefficient vectors* $\mathbf{a}_{\mathcal{V}}$ *where* $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ *satisfying Constraints 1-3 was originally proposed in [17]. Under this structure, a selection on the coefficient vectors was proposed in [17] for the case* $\mathsf{S} = \mathsf{K} - \mathsf{U} + 1$*, which heavily depends on the fact that each coded key is unknown to exactly* $\mathsf{K} - \mathsf{S} = \mathsf{U} - 1$ *users. In this paper, the selection on the coefficient vectors are more flexible in terms of the system parameters; that is, by the new proposed strategy on the generation of the coefficient vectors in* (14)*, we can cancel the interference of each coded key in the transmissions by less than* $\mathsf{U} - 1$ *users.*

Acknowledgement: The work of Z. Zhang, J. Liu, and K. Wan was partially funded by NSFC-12141107. The work of H. Sun was supported in part by NSF under Grant CCF-2007108, Grant CCF-2045656, and Grant CCF-2312228. The work of M. Ji was partially funded by NSF Award 2312227 and CAREER Award 2145835. The work of G. Caire was partially funded by the ERC Advanced Grant N. 789190, CARENET.

REFERENCES

[1] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Artificial intelligence and statistics*. PMLR, 2017, pp. 1273–1282.

[2] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konečnỳ, S. Mazzocchi, B. McMahan *et al.*, "Towards federated learning at scale: System design," *Proceedings of machine learning and systems*, vol. 1, pp. 374–388, 2019.

[3] J. Konečnỳ, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," *arXiv preprint arXiv:1610.05492*, 2016.

[4] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE signal processing magazine*, vol. 37, no. 3, pp. 50–60, 2020.

[5] J. Geiping, H. Bauermeister, H. Dröge, and M. Moeller, "Inverting gradients-how easy is it to break privacy in federated learning?" *Advances in Neural Information Processing Systems*, vol. 33, pp. 16 937–16 947, 2020.

[6] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical secure aggregation for privacy-preserving machine learning," in *2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1175–1191.

[7] Z. Liu, J. Guo, W. Yang, J. Fan, K.-Y. Lam, and J. Zhao, "Privacy-preserving aggregation in federated learning: A survey," *IEEE Transactions on Big Data*, 2022.

[8] A. R. Elkordy, Y. H. Ezzeldin, S. Han, S. Sharma, C. He, S. Mehrotra, S. Avestimehr *et al.*, "Federated analytics: A survey," *APSIPA Transactions on Signal and Information Processing*, vol. 12, no. 1, 2023.

[9] Y. Zhao and H. Sun, "Information theoretic secure aggregation with user dropouts," *IEEE Trans. Inf. Theory*, vol. 68, no. 11, pp. 7471–7484, Nov. 2022.

[10] J. So, C. He, C.-S. Yang, S. Li, Q. Yu, R. E. Ali, B. Guler, and S. Avestimehr, "LightSecAgg: a lightweight and versatile design for secure aggregation in federated learning," *arXiv:2109.14236*, Feb. 2022.

[11] K. Wan, H. Sun, M. Ji, and G. Caire, "On the information theoretic secure aggregation with uncoded groupwise keys," *arXiv:2204.11364*, App. 2022.

[12] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Infor. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[13] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. secret sharing," *IEEE Trans. Infor. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[14] I. Csiszar and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Infor. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[15] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals—part I," *IEEE Trans. Infor. Theory*, vol. 56, no. 8, pp. 3973–3996, Aug. 2010.

[16] K. Wan, H. Sun, M. Ji, T. Mi, and G. Caire, "The capacity region of information theoretic secure aggregation with uncoded groupwise keys," *arXiv preprint arXiv:2310.09889*, 2023.

[17] Z. Zhang, K. Wan, H. Sun, M. Ji, and G. Caire, "Secure aggregation with uncoded groupwise keys against user collusion," in *2023 8th International Conference on Computer and Communication Systems (ICCCS)*, 2023, pp. 559–564.

[18] Z. Zhang, K. Wan, H. Sun, M. Ji, and G. Caire, "Appendix of on the optimality of secure aggregation with uncoded groupwise keys against user dropouts and user collusion," https://github.com/zztqqq/Collusion, 2024.

[19] C. E. Shannon, "Communication theory of secrecy systems," *in The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.