Optimal Information Theoretic Secure Aggregation with Uncoded Groupwise Keys

Kai Wan*, Hua Sun†, Mingyue Ji‡, Tiebin Mi*, Giuseppe Caire§
*Huazhong University of Science and Technology, 430074 Wuhan, China, {kai_wan,mitiebin}@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/ISIT57864.2024.10619454

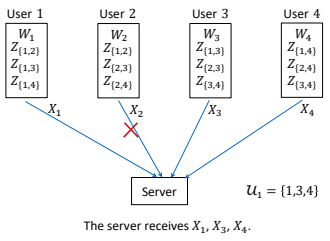
***Abstract*—This paper considers the secure aggregation problem for federated learning under an information theoretic cryptographic formulation, where distributed training nodes (referred to as users) train models based on their own local data and a server aggregates the trained models without retrieving other information about users' local data. Secure aggregation generally contains two phases, namely key sharing phase and model aggregation phase. Due to the common effect of user dropouts in federated learning, the model aggregation phase should contain two rounds, where in the first round the users transmit masked models and according to the identity of surviving users, the surviving users then transmit some further messages to help the server decrypt the sum of users' trained models. The objective of the considered information theoretic formulation is to characterize the capacity region of the communication rates from the users to the server in the two rounds of the model aggregation phase, by assuming that the key sharing have already been done offline in prior. If the keys shared by the users could be any random variables, the capacity was fully characterized in the literature. Recently, an additional constraint on the keys (referred to as uncoded groupwise keys) was added into the problem, where there are several independent keys in the system and each key is shared by exactly S users, where S is a system parameter. In this paper, we fully characterize the capacity region for this problem by matching new converse and achievable bounds.**

I. Introduction

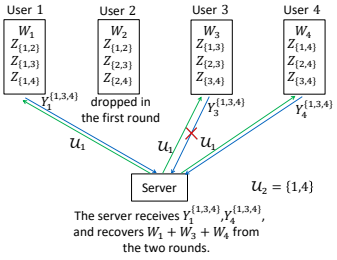
Federated learning is a decentralized machine learning approach that enables multiple devices or users to collaboratively train a global model without sharing their local raw data to the central server [1]. Rather than centralizing all data in a single location, federated learning allows each device training by using its own local data. After training on local data, the users send their model updates (weights or gradients) to the server. Then the central server collects the model updates from all the users and aggregates the updated models to create an updated global model.

To deal with the effect of user dropouts (which is common due to fluctuating connectivity) and strengthen local data privacy in federated learning, a new cryptographic problem, referred to as secure aggregation, was originally introduced in [2]. Except the desired sum of the users' updated models, the server should not learn other information about the users' local data. In order to guarantee the computational or information theoretic security, the key-based encryption could be used, where keys are shared among the users and thus the users' updated models could be masked by the keys. The keys are generated and then shared to the users according to some key generation protocols. If the key generation is independent of the training data, the key sharing is called offline; otherwise, it is called online. Model aggregation follows key sharing, where the users compute, mask, and send their updated models to the server. The secure aggregation protocol in [2] uses the pairwise coded key sharing based on Diffie-Hellman key aggrement [3] and Shamir's secret sharing [4] in order to deal with user dropouts. Following the secure aggregation problem with user dropouts in [2], several works have developed more efficient and/or more secure schemes for aggregation; the readers can refer to the survey for more details [5], [6].

In this paper, we follow the (K,U) information theoretic formulation on secure aggregation with user dropouts and offline key sharing proposed in [7], where K represents the number of users in the system and U represents the minimum number of non-dropped users. The input vector (i.e., updated model) of each user k is denoted by W_k. It is assumed that enough keys have been shared among the users in a prior key sharing phase, and thus each user k has a key Z_k, which can be any random variable independent of $W_1,\ldots,W_{\mathsf{K}}$. It was proved in [7] that to preserve the security of users' local data with the existence of user dropouts, two-round transmission in the model aggregation phase is necessary and also sufficient. In the first round, each user masks its input vector by the stored key and transmits the masked input vector to the server. The server receives and then returns a feedback to the non-dropped users about the identity of the non-dropped users. In the second round, each non-dropped user further transmits a coded message as a function of its local data, key, and the server's feedback. The users may also drop in the second round; the secure aggregation scheme should guarantee that by the two-round transmission the server could recover the sum of the input vectors of the non-dropped users in the first round. Except this computation task, the server should not learn any other information about $W_1,\ldots,W_{\mathsf{K}}$. The objective of this problem is to characterize the region of all possible achievable rate tuples $(\mathsf{R}_1,\mathsf{R}_2)$, where R_i represents the largest number of transmissions in the i^{th} transmission round among all users. The capacity region was proved to be $\{(\mathsf{R}_1,\mathsf{R}_2):\mathsf{R}_1\geq 1,\mathsf{R}_2\geq 1/\mathsf{U}\}$ in [7] with an achievability strategy based on Minimum Distance Separable (MDS) codes in the key generation and one-time pad coding in the model



(a) First round.



(b) Second round.

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

aggregation. Another secure aggregation scheme which can also achieve capacity was proposed in [8], based on a pairwise coded key generation. Compared to [7], the scheme in [8] significantly reduces the size of keys stored by each user.[1]

Recently the authors in [10] considered an additional constraint on the keys into the above problem, where the key sharing among the users is "uncoded" and "groupwise". As illustrated in Fig. 1, given a system parameter S, the system generates $\binom{\mathsf{K}}{\mathsf{S}}$ mutually independent keys, such that each key is shared exactly by one group of S users and is also independent of the input vectors.[2] When $\mathsf{S} > \mathsf{K} - \mathsf{U}$, a secure aggregation scheme with groupwise keys was proposed in [10] which achieves the same capacity region $\{(\mathsf{R}_1, \mathsf{R}_2) : \mathsf{R}_1 \geq 1, \mathsf{R}_2 \geq 1/\mathsf{U}\}$ as in [7]; thus the key group sharing constraint does not involve any loss of optimality. When $\mathsf{S} \leq \mathsf{K} - \mathsf{U}$, a converse bound was proposed in [10] showing that the capacity region in [7] cannot be achieved by secure aggregation schemes with unocded groupwise keys; the capacity region of secure aggregation with uncoded groupwise keys still remains open.

Main Contribution: We characterize the capacity region on the rate tuples for the $(\mathsf{K}, \mathsf{U}, \mathsf{S})$ information theoretic secure aggregation with uncoded groupwise keys, $\left\{(\mathsf{R}_1, \mathsf{R}_2) : \mathsf{R}_1 \geq \frac{\binom{\mathsf{K}-1}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}, \mathsf{R}_2 \geq \frac{1}{\mathsf{U}}\right\}$. More precisely, our focus is on the open case $\mathsf{S} \leq \mathsf{K} - \mathsf{U}$, and we develop the following results.

- We derive a new converse bound on the rates, which is strictly tighter than the converse bound in [10], and propose a new secure aggregation scheme based on interference alignment, which achieves the converse bound.
- We implement the proposed secure aggregation scheme into the Tencent Cloud. Experimental results show that the proposed secure aggregation scheme reduces the model aggregation time by up to 67.2% compared to the original secure aggregation scheme in [2]. Due to the limitation of pages, readers can refer to the extended version of this paper [19, Section VI] for the comparison.

Notation Convention: Calligraphic symbols denote sets, bold symbols denote vectors and matrices, and sans-serif symbols denote system parameters. $[a:b] := \{a, a+1, \ldots, b\}$ and $[n] := [1:n]$; $\mathbb{F}_{\mathsf{q}}$ represents a finite field with order q; $\mathbf{e}_{n,i}$ represents the vertical n-dimensional unit vector whose entry in the i^{th} position is 1 and 0 elsewhere; $\mathbf{A}^{\mathrm{T}}$ represents the transpose of matrix $\mathbf{A}$; $0_{m,n}$ represents all-zero matrix of dimension $m \times n$; let $\binom{\mathcal{X}}{y} = \{\mathcal{S} \subseteq \mathcal{X} : |\mathcal{S}| = y\}$ where $|\mathcal{X}| \geq y > 0$. For each set of integers $\mathcal{S}$, $\mathcal{S}(i)$ denotes the i^{th} smallest element in $\mathcal{S}$. Entropies will be in base q, where q represents the field size.

II. System Model

We consider a $(\mathsf{K}, \mathsf{U}, \mathsf{S})$ information theoretic secure aggregation problem with uncoded groupwise keys in [10], as illustrated in Fig 1. Note that $\mathsf{K}, \mathsf{U}, \mathsf{S}$ are given system parameters, where K represents the number of users in the system, U represents the minimum number of surviving users, and S represents the group-sharing parameter, i.e., the size of the groups uniquely sharing the same key. Each user $k \in [\mathsf{K}]$ holds one input vector W_k containing L uniform and i.i.d. symbols on a finite field $\mathbb{F}_{\mathsf{q}}$, where q is a prime power. In addition, for each set $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$, the users in $\mathcal{V}$ share a common key $Z_{\mathcal{V}}$ with large enough size. Considering that the key sharing is offline, the keys and the input vectors are assumed to be mutually independent. We define $Z_k := \left(Z_{\mathcal{V}} : \mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}, k \in \mathcal{V}\right)$, as the keys accessible by user $k \in [\mathsf{K}]$. A server is connected with the users via dedicated error-free links. The server aims to aggregates the input vectors computed by the users. In this paper, we consider the effect of user dropouts, i.e., the system is designed to tolerate up to $\mathsf{K} - \mathsf{U} > 0$ user dropouts; in this case, it was proved in [7] that two transmission rounds are required in the model aggregation.

First round. Each user $k \in [\mathsf{K}]$ sends a coded message X_k to the server without knowing which user will drop in the future, where X_k is completely determined by W_k and Z_k,

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

The first round transmission rate is defined as the largest normalized transmission load among all users,

$$\mathsf{R}_1 := \max_{k \in [\mathsf{K}]} H(X_k) / \mathsf{L}. \tag{2}$$

[1]The secure aggregation schemes in [2], [7], [8] can tolerate up to $\mathsf{T} < \mathsf{U}$ users who collude with the server. However, in this paper we do not consider user collusion; thus we set $\mathsf{T} = 0$. Secure aggregation with uncoded groupwise keys against user collusion (i.e., $\mathsf{T} > 0$) was considered in another paper of ours [9] and characterizing the capacity region is an ongoing work.

[2]The uncoded groupwise keys could be directly generated and shared among users by some key agreement protocol such as [11]–[18] even if there do not exist private links among users nor a trusted server, while to share coded keys among users there should exist private links among users or a trusted server who assigns keys for the key sharing phase.

Users may drop during the first round. We denote the set of surviving users after the first round by $\mathcal{U}_1$. Since U represents the minimum number of surviving users, we have $\mathcal{U}_1 \subseteq [\mathsf{K}]$ and $|\mathcal{U}_1| \geq \mathsf{U}$. Hence, the server receives $(X_k : k \in \mathcal{U}_1)$.

Second round. The server first sends the list of the surviving users $\mathcal{U}_1$ to the users in $\mathcal{U}_1$. According to this information, each user $k \in \mathcal{U}_1$ sends another coded message $Y_k^{\mathcal{U}_1}$ to the server,

$$H(Y_k^{\mathcal{U}_1}|W_k, Z_k, \mathcal{U}_1) = 0. \tag{3}$$

The second round transmission rate is defined as the largest normalized transmission load among all $\mathcal{U}_1$, all users in $\mathcal{U}_1$,

$$\mathsf{R}_2 := \max_{\mathcal{U}_1 \subseteq [\mathsf{K}]: |\mathcal{U}_1| \geq \mathsf{U}} \max_{k \in \mathcal{U}_1} H\left(Y_k^{\mathcal{U}_1}\right)/\mathsf{L}. \tag{4}$$

Users may also drop during the second round transmission, and the set of surviving users after the second round is denoted as $\mathcal{U}_2$. By definition, we have $\mathcal{U}_2 \subseteq \mathcal{U}_1$ and $|\mathcal{U}_2| \geq \mathsf{U}$. Thus the server receives $Y_k^{\mathcal{U}_1}$ where $k \in \mathcal{U}_2$.

Decoding. From the two-round transmissions, the server totally receives $(X_{k_1} : k_1 \in \mathcal{U}_1)$ and $(Y_{k_2}^{\mathcal{U}_1} : k_2 \in \mathcal{U}_2)$, from which the server should recover the sum of input vectors by the first round surviving users, i.e., $\sum_{k \in \mathcal{U}_1} W_k$. Thus

$$H\left(\sum_{k \in \mathcal{U}_1} W_k \Big| (X_{k_1} : k_1 \in \mathcal{U}_1), (Y_{k_2}^{\mathcal{U}_1} : k_2 \in \mathcal{U}_2)\right) = 0, \tag{5}$$

for all $\mathcal{U}_1 \subseteq [\mathsf{K}]$ and $\mathcal{U}_2 \subseteq \mathcal{U}_1$ where $|\mathcal{U}_1| \geq |\mathcal{U}_2| \geq \mathsf{U}$.

Security. For the security constraint, we consider the worst-case, where the users may not be really dropped but be too slow in the transmission and thus the server may receive all the possible transmissions by the users. More precisely, it may receive $(X_{k_1} : k_1 \in [\mathsf{K}])$ from the first round and $(Y_{k_2}^{\mathcal{U}_1} : k_2 \in \mathcal{U}_1)$ from the second transmission. By security, from the received messages, the server can only obtain the computation task without retrieving other information about the input vectors. Thus for all $\mathcal{U}_1 \subseteq [\mathsf{K}]$ where $|\mathcal{U}_1| \geq \mathsf{U}$,

$$I\big(W_1, \ldots, W_{\mathsf{K}}; X_1, \ldots, X_{\mathsf{K}}, (Y_k^{\mathcal{U}_1} : k \in \mathcal{U}_1)\big| \sum_{k \in \mathcal{U}_1} W_k\big) = 0. \tag{6}$$

Objective. A rate tuple $(\mathsf{R}_1, \mathsf{R}_2)$ is achievable if there exist uncoded groupwise keys $\left(Z_{\mathcal{V}} : \mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}\right)$ and a secure aggregation scheme satisfying the decodability and security constraints in (5) and (6), respectively. Our objective is to determine the capacity region (i.e., the closure of all achievable rate tuples), denoted by $\mathcal{R}^\star$.

Existing results. By removing the uncoded groupwise constraint on the keys in our problem, we obtain the problem in [7]. Hence, the converse bound on the capacity region in [7] is also a converse bound for our problem.

Theorem 1 ([7]). *For the $(\mathsf{K}, \mathsf{U}, \mathsf{S})$ information theoretic secure aggregation problem with uncoded groupwise keys, any achievable rate tuple $(\mathsf{R}_1, \mathsf{R}_2)$ satisfies*

$$\mathsf{R}_1 \geq 1, \ \mathsf{R}_2 \geq 1/\mathsf{U}. \tag{7}$$

A secure aggregation scheme with uncoded groupwise keys was proposed in [10] for the case $\mathsf{S} > \mathsf{K} - \mathsf{U}$, achieving the converse bound in Theorem 1; thus the capacity region for the case $\mathsf{S} > \mathsf{K} - \mathsf{U}$ has been characterized in [10]. An improved converse bound was given in [10] for the case $\mathsf{S} \leq \mathsf{K} - \mathsf{U}$.

Theorem 2 ([10]). *For the $(\mathsf{K}, \mathsf{U}, \mathsf{S})$ information theoretic secure aggregation problem with uncoded groupwise keys, when $\mathsf{S} = 1$, secure aggregation is not possible; when $2 \leq \mathsf{S} \leq \mathsf{K} - \mathsf{U}$, any achievable rate tuple $(\mathsf{R}_1, \mathsf{R}_2)$ satisfies*

$$\mathsf{R}_1 \geq 1 + \frac{1}{\binom{\mathsf{K}-1}{\mathsf{S}-1} - 1}, \mathsf{R}_2 \geq 1/\mathsf{U}. \tag{8}$$

However, no achievable scheme has been provided for the case $\mathsf{S} \leq \mathsf{K} - \mathsf{U}$, and the capacity region for this case remained open until this paper.

III. Main Result

The following theorem fully characterizes the capacity region for the information theoretic secure aggregation problem with uncoded groupwise keys.

Theorem 3. *For the $(\mathsf{K}, \mathsf{U}, \mathsf{S})$ information theoretic secure aggregation problem with uncoded groupwise keys, when $\mathsf{S} = 1$, secure aggregation is not possible; when $\mathsf{S} \geq 2$, we have*

$$\mathcal{R}^\star = \left\{(\mathsf{R}_1, \mathsf{R}_2) : \mathsf{R}_1 \geq \frac{\binom{\mathsf{K}-1}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}, \mathsf{R}_2 \geq \frac{1}{\mathsf{U}}\right\}. \tag{9}$$

The achievability proof is given in Section IV. Due to the limitation of pages, the converse proof could be found in the extended version [19, Section IV]. The following remarks on Theorem 3 are in order:

- When $\mathsf{S} > \mathsf{K} - \mathsf{U}$, we have $\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1} = 0$ and thus the capacity region in (9) reduces to the one in (7), which is also equal to the capacity region for the information theoretic secure aggregation problem in [7] (the one without the constraint on the uncoded groupwise keys). When $2 \leq \mathsf{S} \leq \mathsf{K} - \mathsf{U}$, the additional communication rate from the optimal secure aggregation scheme with uncoded groupwise keys compared to the generally optimal secure aggregation scheme in [7] is only at the first round and is equal to $\frac{\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}$. Note that, the proposed secure aggregation scheme in this paper is a new and unified scheme working for all system parameters when $\mathsf{S} > 1$.
- The converse bound to prove (9) is strictly tighter than the existing one in (8).

IV. Achievability Proof of Theorem 3

Due to the limitation of pages, we illustrate the main ideas of the proposed scheme through the following example; readers can refer to the extended version of this paper [19, Section V] for the general description.

We consider the $(\mathsf{K}, \mathsf{U}, \mathsf{S}) = (5, 2, 3)$ information theoretic secure aggregation problem with uncoded groupwise keys. Note that in this example, for the ease of illustration, we assume that the field size q is a large enough prime; it is

proved in [19, Section V] that our proposed scheme works for arbitrary field size.

By the converse bound in Theorem 3, we have $\mathsf{R}_1 \geq \frac{\binom{\mathsf{K}-1}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}} = \frac{6}{5}$ and $\mathsf{R}_2 \geq \frac{1}{\mathsf{U}} = \frac{1}{2}$. Inspired by the converse bound, we divide each input vector W_i where $i \in [\mathsf{K}]$ into $\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1} = 5$ non-overlapping and equal-length pieces, $W_i = \{W_{i,1}, \ldots, W_{i,5}\}$. For each set $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$, we generate a key $Z_{\mathcal{V}}$ containing $\frac{\mathsf{S}\mathsf{L}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}} = \frac{3\mathsf{L}}{5}$ symbols uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}$; let $Z_{\mathcal{V}}$ be shared by the users in $\mathcal{V}$. We further divide each key $Z_{\mathcal{V}}$ into $\mathsf{S} = 3$ sub-keys (each with $\frac{\mathsf{L}}{5}$ symbols), $Z_{\mathcal{V}} = \{Z_{\mathcal{V},k} : k \in \mathcal{V}\}$.

From the converse bound we see that in the first round each user $k \in [5]$ should send more than L symbols, while input vector W_k contains L symbols. Thus, unlike the secure aggregation scheme in [10] which has $\mathsf{R}_1 = 1$, in the first round besides the encrypted input vector, we also need to transmit some coded messages composed of keys, to cope with the fact that some keys cannot be transmitted in the second round due to user dropouts. For each key $\mathcal{Z}_{\mathcal{V}}$, we select a 6-length vector $\mathbf{a}_{\mathcal{V}} = [a_{\mathcal{V},1}, \ldots, a_{\mathcal{V},6}]^{\mathrm{T}}$ which will serve as the coefficient vector of its sub-keys during the first round. The selection of these coefficient vectors to guarantee the encodability, decodability and security, is the most important step in the proposed secure aggregation scheme. We denote the sets $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ where $k \in \mathcal{V}$ by $\mathcal{S}_{k,1}, \ldots, \mathcal{S}_{k,\binom{\mathsf{K}-1}{\mathsf{S}-1}}$; denote the sets in $\binom{[\mathsf{K}]\backslash\{k\}}{\mathsf{S}}$ by $\overline{\mathcal{S}}_{k,1}, \ldots, \overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}$. For the security and encodability, it will be explained later that the selection has the following two properties respectively: for each $k \in [\mathsf{K}]$,

$$\left[\mathbf{a}_{\mathcal{S}_{k,1}}, \ldots, \mathbf{a}_{\mathcal{S}_{k,\binom{\mathsf{K}-1}{\mathsf{S}-1}}}\right] \text{ has rank } \binom{\mathsf{K}-1}{\mathsf{S}-1} = 6; \tag{10}$$

$$\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}}, \ldots, \mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}}\right] \text{ has rank } \binom{\mathsf{K}-2}{\mathsf{S}-1} = 3. \tag{11}$$

In order to guarantee (10) and (11), we select the coefficient vectors by the following two steps:

- We first select each vector $\mathbf{a}_{\mathcal{V}}$ for each $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ where $1 \in \mathcal{V}$. More precisely, we choose each element in $\mathbf{a}_{\mathcal{V}}$ uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}$, as illustrated in Table I.
- Then we fix each of the remaining vectors by a linear combination of the selected vectors in the first step. More precisely, to fix $\mathbf{a}_{\{2,3,4\}}$, we let $\mathbf{a}_{\{2,3,4\}}$ be a linear combination of $\mathbf{a}_{\{1,3,4\}}$, $\mathbf{a}_{\{1,2,4\}}$, and $\mathbf{a}_{\{1,2,3\}}$, where the coefficients are either $+1$ or -1 and alternated,

$$\mathbf{a}_{\{2,3,4\}} = \mathbf{a}_{\{1,3,4\}} - \mathbf{a}_{\{1,2,4\}} + \mathbf{a}_{\{1,2,3\}}. \tag{12}$$

  Similarly, for each $\mathcal{V} \in \binom{[2:\mathsf{K}]}{\mathsf{S}}$, we let $\mathbf{a}_{\mathcal{V}}$ be the following linear combination of $\mathbf{a}_{\mathcal{V}\backslash\{k\}\cup\{1\}}$ where $k \in \mathcal{V}$, (recall that $\mathcal{V}(i)$ represents the i^{th} smallest element in $\mathcal{V}$)

$$\mathbf{a}_{\mathcal{V}} = \sum_{i\in[3]} (-1)^{i-1} \mathbf{a}_{\mathcal{V}\backslash\{\mathcal{V}(i)\}\cup\{1\}}. \tag{13}$$

The detailed section on the coefficient vectors is given in Table I. It can be checked that this selection has the two properties in (10) and (11). The first property could be directly checked. For the second property, we have

$$\mathbf{a}_{\{3,4,5\}} = \mathbf{a}_{\{2,4,5\}} - \mathbf{a}_{\{2,3,5\}} + \mathbf{a}_{\{2,3,4\}}; \tag{14}$$

thus the rank of $[\mathbf{a}_{\{2,3,4\}}, \mathbf{a}_{\{2,3,5\}}, \mathbf{a}_{\{2,4,5\}}, \mathbf{a}_{\{3,4,5\}}]$ is equal to the rank of $[\mathbf{a}_{\{2,3,4\}}, \mathbf{a}_{\{2,3,5\}}, \mathbf{a}_{\{2,4,5\}}]$ which is equal to 3. In addition, since

$$\mathbf{a}_{\{3,4,5\}} = \mathbf{a}_{\{1,4,5\}} - \mathbf{a}_{\{1,3,5\}} + \mathbf{a}_{\{1,3,4\}}; \tag{15}$$

thus the rank of $[\mathbf{a}_{\{1,3,4\}}, \mathbf{a}_{\{1,3,5\}}, \mathbf{a}_{\{1,4,5\}}, \mathbf{a}_{\{3,4,5\}}]$ is equal to the rank of $[\mathbf{a}_{\{1,3,4\}}, \mathbf{a}_{\{1,3,5\}}, \mathbf{a}_{\{1,4,5\}}]$ which is equal to 3. Similarly, we can also check that the rank of $[\mathbf{a}_{\{1,2,4\}}, \mathbf{a}_{\{1,2,5\}}, \mathbf{a}_{\{1,4,5\}}, \mathbf{a}_{\{2,4,5\}}]$ is equal to the rank of $[\mathbf{a}_{\{1,2,4\}}, \mathbf{a}_{\{1,2,5\}}, \mathbf{a}_{\{1,4,5\}}]$ which is equal to 3; the rank of $[\mathbf{a}_{\{1,2,3\}}, \mathbf{a}_{\{1,2,5\}}, \mathbf{a}_{\{1,3,5\}}, \mathbf{a}_{\{2,3,5\}}]$ is equal to the rank of $[\mathbf{a}_{\{1,2,3\}}, \mathbf{a}_{\{1,2,5\}}, \mathbf{a}_{\{1,3,5\}}]$ which is equal to 3; the rank of $[\mathbf{a}_{\{1,2,3\}}, \mathbf{a}_{\{1,2,4\}}, \mathbf{a}_{\{1,3,4\}}, \mathbf{a}_{\{2,3,4\}}]$ is equal to the rank of $[\mathbf{a}_{\{1,2,3\}}, \mathbf{a}_{\{1,2,4\}}, \mathbf{a}_{\{1,3,4\}}]$ which is equal to 3. Thus the property is satisfied. We will show later that this selection guarantees the encodability, decodability and security.

After the selection of the above coefficient vectors, the transmission in the first round by each user $k \in [\mathsf{K}]$ can be divided into two parts (as explained before):

- The first part contains $\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1} = 5$ linear combinations of pieces and sub-keys, where each linear combination contains $\mathsf{L}/5$ symbols. For each $j \in [5]$, let user k transmit $X_{k,j} = W_{k,j} + \sum_{\mathcal{V}\in\binom{[5]}{3}:k\in\mathcal{V}} a_{\mathcal{V},j} Z_{\mathcal{V},k}$.
- The second part contains $\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1} = 1$ linear combination of sub-keys with $\mathsf{L}/5$ symbols; let user k transmit $X_{k,6} = \sum_{\mathcal{V}\in\binom{[5]}{3}:k\in\mathcal{V}} a_{\mathcal{V},6} Z_{\mathcal{V},k}$.

Hence, user k transmits $X_k = (X_{k,1}, \ldots, X_{k,6})$, totally $6\mathsf{L}/5$ symbols in the first round. Since the selection of the coefficient vectors has the property in (10), the rank of the sub-keys in X_k is equal to the dimension of X_k and thus from X_k the server cannot get any information about W_k (see [10, Appendix C] for the formal proof).

Now we consider the case $\mathcal{U}_1 = [5]$, i.e., no user drops in the first round. From the first round, the server can recover

$$\sum_{k_1\in[5]} X_{k_1,j} = \sum_{k_2\in[5]} W_{k_2,j} + \sum_{\mathcal{V}\in\binom{[5]}{3}} a_{\mathcal{V},j} \underbrace{\sum_{k_3\in\mathcal{V}} Z_{\mathcal{V},k_3}}_{:=Z_{\mathcal{V}}^{[5]}} \tag{16}$$

for each $j \in [5]$, and can also recover

$$\sum_{k_1\in[5]} X_{k_1,6} = \sum_{\mathcal{V}\in\binom{[5]}{3}} a_{\mathcal{V},6} Z_{\mathcal{V}}^{[5]}. \tag{17}$$

The server should further recover the second term on the RHS of (16), $\sum_{\mathcal{V}\in\binom{[5]}{3}} a_{\mathcal{V},j} Z_{\mathcal{V}}^{[5]}$ for $j \in [5]$, in the second round.

In the second round, to achieve $\mathsf{R}_2 = 1/2$, we divide each $Z_{\mathcal{V}}^{[5]}$ where $\mathcal{V} \in \binom{[5]}{3}$ into 2 non-overlapping and equal-length coded keys, $Z_{\mathcal{V}}^{[5]} = \left\{Z_{\mathcal{V},1}^{[5]}, Z_{\mathcal{V},2}^{[5]}\right\}$, where each coded key contains $\frac{\mathsf{L}}{10}$ symbols. Hence, we can write the recovery task of the second round in the ma-

TABLE I: Choice of 6-dimensional vectors $\mathbf{a}_{\mathcal{V}}$ in the $(\mathsf{K},\mathsf{U},\mathsf{S}))=(5,2,3)$ information theoretic secure aggregation problem.

$\mathbf{a}_{\mathcal{V}}$	Value	$\mathbf{a}_{\mathcal{V}}$	Value
$\mathbf{a}_{\{1,2,3\}}$	$[0,1,0,0,1,1]^{\mathrm{T}}$	$\mathbf{a}_{\{1,4,5\}}$	$[1,0,0,0,0,1]^{\mathrm{T}}$
$\mathbf{a}_{\{1,2,4\}}$	$[1,0,1,1,1,1]^{\mathrm{T}}$	$\mathbf{a}_{\{2,3,4\}}$	$\mathbf{a}_{\{1,3,4\}}-\mathbf{a}_{\{1,2,4\}}+\mathbf{a}_{\{1,2,3\}}=[-1,2,0,0,0,1]^{\mathrm{T}}$
$\mathbf{a}_{\{1,2,5\}}$	$[0,0,0,1,0,1]^{\mathrm{T}}$	$\mathbf{a}_{\{2,3,5\}}$	$\mathbf{a}_{\{1,3,5\}}-\mathbf{a}_{\{1,2,5\}}+\mathbf{a}_{\{1,2,3\}}=[1,2,0,0,1,1]^{\mathrm{T}}$
$\mathbf{a}_{\{1,3,4\}}$	$[0,1,1,1,0,1]^{\mathrm{T}}$	$\mathbf{a}_{\{2,4,5\}}$	$\mathbf{a}_{\{1,4,5\}}-\mathbf{a}_{\{1,2,5\}}+\mathbf{a}_{\{1,2,4\}}=[2,0,1,0,1,1]^{\mathrm{T}}$
$\mathbf{a}_{\{1,3,5\}}$	$[1,1,0,1,0,1]^{\mathrm{T}}$	$\mathbf{a}_{\{3,4,5\}}$	$\mathbf{a}_{\{1,4,5\}}-\mathbf{a}_{\{1,3,5\}}+\mathbf{a}_{\{1,3,4\}}=[0,0,1,0,0,1]^{\mathrm{T}}$

trix form $\begin{bmatrix} F_1 \\ \vdots \\ F_{12} \end{bmatrix} = \mathbf{F} \begin{bmatrix} Z^{[5]}_{\{1,2,3\},1} \\ \vdots \\ Z^{[5]}_{\{3,4,5\},1} \\ Z^{[5]}_{\{1,2,3\},2} \\ \vdots \\ Z^{[5]}_{\{3,4,5\},2} \end{bmatrix}$ where $\mathbf{F} = \left[\begin{array}{ccc|ccc} & \mathbf{a}_{\{1,2,3\}},\ldots,\mathbf{a}_{\{3,4,5\}} & & & 0_{6\times 10} & \\ \hline & 0_{6\times 10} & & & \mathbf{a}_{\{1,2,3\}},\ldots,\mathbf{a}_{\{3,4,5\}} & \end{array}\right]$. Note that F_6 and F_{12} have been already recovered by the server from the first round.

We focus on each user $k \in [5]$, who should transmit $\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}=5$ linear combinations of $F_1,\ldots,F_{12}$ in the second round; in the matrix form these 5 linear combinations are $\mathbf{S}_k[F_1;\ldots,F_{12}]$, where $\mathbf{S}_k$ is a matrix with dimension 5×12. Note that for the encodability, user k can only compute the coded keys $Z^{[5]}_{\mathcal{V},j}$ where $k\in\mathcal{V}$; thus in the transmitted linear combinations the coefficients of the coded keys which user k cannot compute should be equal to 0.

For user 1, the columns of $\mathbf{S}_1\mathbf{F}$ with indices in $[7:10]\cup[17:20]$ should be $0_{5\times 1}$, since these columns correspond to $Z_{\{2,3,4\},1}, Z_{\{2,3,5\},1}, Z_{\{2,4,5\},1}, Z_{\{3,4,5\},1}, Z_{\{2,3,4\},2}, Z_{\{2,3,5\},2}$, $Z_{\{2,4,5\},2}, Z_{\{3,4,5\},2}$, which cannot be computed by user 1. Assume that the column-wise sub-matrix of $\mathbf{F}$ including the columns with indices in $[7:10]\cup[17:20]$ is $\mathbf{F}_1$ with dimension 12×8. We need to find 5 linearly independent left null vectors of $\mathbf{F}_1$, and let $\mathbf{S}_1$ be the matrix of these 5 vectors. Note that if $\mathbf{F}_1$ is full rank, the left null space of $\mathbf{F}_1$ only contains $12-8=4$ linearly independent vectors. However, by our construction, it has been shown in (14) that $\mathbf{a}_{\{3,4,5\}}=\mathbf{a}_{\{2,4,5\}}-\mathbf{a}_{\{2,3,5\}}+\mathbf{a}_{\{2,3,4\}}$; in other words, **the coefficient vectors corresponding to the unknown coded keys of user** 1 **are aligned.** Thus by this interference alignment-like construction leading to (11), the rank of $\mathbf{F}_1$ is 6, and thus the left null space of $\mathbf{F}_1$ contains $12-6=6$ linearly independent vectors. More precisely, the left null space of $[\mathbf{a}_{\{2,3,4\}},\mathbf{a}_{\{2,3,5\}},\mathbf{a}_{\{2,4,5\}}]$ is the linear space spanned by $\mathbf{s}_{1,1}=(0,-1,-2,0,0,2),\mathbf{s}_{1,2}=(-2,-1,0,0,4,0),\mathbf{s}_{1,3}=(0,0,0,1,0,0)$. Hence, the left null space of $\mathbf{F}_1$ is the linear space spanned by $(\mathbf{s}_{1,1},0_{1\times 6}),(\mathbf{s}_{1,2},0_{1\times 6}),(\mathbf{s}_{1,3},0_{1\times 6}),(0_{1\times 6},\mathbf{s}_{1,1}),(0_{1\times 6},\mathbf{s}_{1,2})$, $(0_{1\times 6},\mathbf{s}_{1,3})$. We let each row of $\mathbf{S}_1$ be a random vector in the the null space of $\mathbf{F}_1$.

For user 2, the columns of $\mathbf{S}_2\mathbf{F}$ with indices in $\{4,5,6,10,14,15,16,20\}$ should be $0_{5\times 1}$. Assume that the column-wise sub-matrix of $\mathbf{F}$ including the columns with indices in $\{4,5,6,10,14,15,16,20\}$ is $\mathbf{F}_2$ with dimension 12×8. By construction we have $\mathbf{a}_{\{3,4,5\}}=\mathbf{a}_{\{1,4,5\}}-\mathbf{a}_{\{1,3,5\}}+\mathbf{a}_{\{1,3,4\}}$ as shown in (15). The left null space of $[\mathbf{a}_{\{2,3,4\}},\mathbf{a}_{\{2,3,5\}},\mathbf{a}_{\{2,4,5\}}]$ is the linear space spanned by $\mathbf{s}_{2,1}=(-1,0,-1,0,0,1),\mathbf{s}_{2,2}=(0,0,0,0,1,0),\mathbf{s}_{2,3}=(0,-1,0,1,0,0)$. Hence, the left null space of $\mathbf{F}_2$ is the linear space spanned by $(\mathbf{s}_{2,1},0_{1\times 6}),(\mathbf{s}_{2,2},0_{1\times 6}),(\mathbf{s}_{2,3},0_{1\times 6}),(0_{1\times 6},\mathbf{s}_{2,1}),(0_{1\times 6},\mathbf{s}_{2,2})$, $(0_{1\times 6},\mathbf{s}_{2,3})$. We let each row of $\mathbf{S}_2$ be a random vector in the the null space of $\mathbf{F}_2$.

Similarly, we can select $\mathbf{S}_3,\ldots,\mathbf{S}_5$. Note that the detailed selection on $\mathbf{S}_1,\ldots,\mathbf{S}_5$ is given in [19, Example 1]. As a summary, the constraint (11) is satisfied by the interference alignment-like construction, while satisfying this constraint leads to the successful encoding of each user.

Then we check the decodability. Note that F_6 and F_{12} have been recovered by the server from the first round. Recall that $\mathbf{e}_{n,i}$ represents the vertical n-dimensional standard unit vector whose i^{th} element is 1. For any set of two users $\mathcal{U}_2=\{u_1,u_2\}\subseteq[\mathsf{K}]$ where $|\mathcal{U}_2|=2$, one can check that that the matrix $\begin{bmatrix} \mathbf{S}_{u_1} \\ \mathbf{S}_{u_2} \\ \mathbf{e}^{\mathrm{T}}_{12,6} \\ \mathbf{e}^{\mathrm{T}}_{12,12} \end{bmatrix}$ whose dimension is 12×12, is full rank; thus the server can recover $F_1,\ldots,F_{12}$ and then recover $W_1+\cdots+W_5$.

For the security, from the first round the server cannot obtain any information about $W_1,\ldots,W_5$. In the second round, all the transmissions by all users are linear combinations of $F_1,\ldots,F_{12}$, where F_6 and F_{12} can be recovered from the first round. Since each F_i, where $i\in[12]\setminus\{6,12\}$ contains $\mathsf{L}/10$ symbols, by [20] the server can only obtain additional $10\mathsf{L}/10=\mathsf{L}$ symbols about $W_1,\ldots,W_5$ from the second round, which are exactly the symbols in $W_1+\cdots+W_5$. Hence, the proposed secure aggregation scheme is secure.

The above scheme could be directly extended to other $\mathcal{U}_1\subseteq[5]$ where $|\mathcal{U}_1|\geq 2$. So it achieves $\mathsf{R}_1=6/5$ and $\mathsf{R}_2=1/2$, coinciding with the proposed converse bound.

Acknowledgement: The work of K. Wan and T. Mi 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, 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.

[3] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Infor. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[4] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[5] 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.

[6] A. R. Elkordy, Y. H. Ezzeldin, S. Han, S. Sharma, C. He, S. Mehrotra, and S. Avestimehr, "Federated analytics: A survey," *APSIPA Transactions on Signal and Information Processing*, 2023.

[7] 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.

[8] 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.

[9] 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.

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

[11] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Infor. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[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] ——, "Information-theoretic key agreement of multiple terminals—part II: Channel model," *IEEE Trans. Infor. Theory*, vol. 56, no. 8, pp. 3997–4010, Aug. 2010.

[17] H. Sun, "Secure groupcast with shared keys," *IEEE Trans. Infor. Theory*, vol. 68, no. 7, pp. 4681–4699, Mar. 2022.

[18] ——, "Compound secure groupcast: Key assignment for selected broadcasting," *IEEE Journal on Selected Areas in Information Theory*, vol. 3, no. 2, pp. 379–389, Jun. 2022.

[19] K. Wan, H. Sun, M. Ji, T. Mi, and G. Caire, "The capacity region of information theoretic secure aggregation with uncoded groupwise keys," *arXiv:2310.09889v2*, Nov. 2023.

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