# Optimal Rate Region for Key Efficient Hierarchical Secure Aggregation with User Collusion

Xiang Zhang*, Kai Wan†, Hua Sun‡, Shiqiang Wang§, Mingyue Ji¶, and Giuseppe Caire*
Department of Electrical Engineering and Computer Science, Technical University of Berlin*
School of Electronic Information and Communications, Huazhong University of Science and Technology†
Department of Electrical Engineering, University of North Texas‡
IBM T. J. Watson Research Center§
Department of Electrical and Computer Engineering, University of Florida¶
Email: *{xiang.zhang, caire}@tu-berlin.de, †kai_wan@hust.edu.cn, ‡hua.sun@unt.edu
§wangshiq@us.ibm.com, ¶mingyueji@ufl.edu

***Abstract*—Secure aggregation is concerned with the task of securely uploading the inputs associated with multiple users to an aggregation server without revealing the user inputs to the server besides the summation of all inputs. It finds broad applications in distributed machine learning paradigms such as federated learning (FL). Motivated by practical hierarchical FL systems which utilize the client-edge-cloud network architecture to improve delay performance, we study the hierarchical secure aggregation (HSA) problem in a 3-layer hierarchical network where a total of $UV$ users are connected to an aggregation server through $U$ relay nodes each being associated with a disjoint subset of $V$ users. Security requires that the server learn nothing beyond the desired sum of the inputs (server security), and each relay learn nothing about the user inputs (relay security) even if they collude with up to $T$ users. We characterize the optimal communication and key rate region by proposing a novel secure aggregation scheme and deriving an information-theoretic converse that matches the achievable scheme. In particular, we show that when $T \geq (U-1)V$, the proposed HSA problem is infeasible. Otherwise when $T < (U-1)V$, to securely compute 1 bit of the desired sum, each user needs to upload at least 1 bit to its associating relay, each relay needs to upload at least 1 bit to the server, each user needs to hold at least 1 key bit, and all users need to collectively hold at least $\max\{V+T, \min\{U+T-1, UV-1\}\}$ (source) key bits. The characterization of the source key rate is a major contribution of this work.**

## I. Introduction

Federated learning (FL) has emerged as a powerful decentralized learning paradigm which trains a centralized model using local datasets distributed across many end users [1]–[4]. It finds broad practical applications such as virtual keyboard search suggestion in Google Keyboard [5]. In FL, a set of (possibly many) users, each holding a unique local dataset, wishes to collaboratively learn a shared machine learning model without directly revealing their individual data to the coordination server. More specifically, the training process alternates between local training where each user performs a number of stochastic gradient descent (SGD) on its own dataset, and global aggregation where the users upload their local model parameters to the server for aggregation. In the celebrated FedAvg algorithm [1], the server simply computes a weighted average of the local models, which is then broadcast to the users as an initialization point for a new round of local training. Convergence rates have later been established for FedAvg and related FL algorithms [6], [7].

Despite its potential, FL exposes vulnerability to security and privacy breaches [8]. For example, it was shown that a considerable amount of information of the users' local data can be inferred by the server by observing the local gradients through model inversion attack [9], which poses a threat if the server is not trustworthy. Therefore, a critical consideration in FL is to ensure that the server does not learn the locally trained models of the individual users during aggregation. Moreover, model aggregation should be robust against collusion (server gains access to the local data of some users) and user dropouts due to unreliable connection. Hence, the need for data security and user privacy has stimulated the study of the secure aggregation problem [10]–[12], under a multitude of constraints such as user dropout [13], [14], groupwise keys [15], [16], user selection [17], [18], weak security [19], oblivious servers [20] and malicious users [21]. For example, Bonawitz *et al.* [10] proposed a secure aggregation protocol which relies on pairwise random seed agreement between users to generate zero-sum random keys (masks) that hide individual users' models. When added for aggregation, the keys cancel out and the desired sum of local models can be recovered. Zhao *et al.* [17] proposed an information-theoretic formulation of the secure aggregation problem where the local models are abstracted as i.i.d. inputs. The optimal (upload) communication rate has been characterized under user collusion and dropout. Following this line of work, [15] and [16] considered the use of groupwise keys where multiple users may share an identical key. Weak security was considered in [19] where instead protecting all the inputs against an arbitrary subset of users, protection of a predetermined collection of inputs against a restricted subsets of users was studied. In addition, Sun [20] considered a scenario where the servers are oblivious and characterized the optimal communication and key rates.

Existing information-theoretic secure aggregation proto-

cols focus exclusively on the canonical FL setup with one central server and many distributed users which faces challenges such as excessive communication overhead, latency and substantial user dropouts due to unstable connectivity [8]. To overcome, hierarchical FL [22]–[24] utilizes the client-edge-cloud architecture in edge computing systems to take advantage of the efficient communication between the users and edge servers. Motivated by this architecture, we study the *hierarchical secure aggregation* (HSA) problem in a 3-layer network consisting of a server, $U$ relays and $UV$ users where each relay is connected to a disjoint set of $V$ users (See Fig. 1). In the aggregation phase of HSA, each user uploads a message (as a function of its private input and key) to the associated relay and each relay also uploads a message to the server based on the collected messages from its connected users. Besides the conventional server security which requires that the server learn nothing about the users' inputs beyond the desired sum of inputs, relay security is also enforced. In particular, each relay should not infer anything about the users' inputs even if it colludes with up to $T$ users. Our goal is to design secure aggregation protocols that minimize the communication load and key consumption.

We show that when $T \geq (U-1)V$, the proposed HSA problem is infeasible. Otherwise when $T < (U-1)V$, we find out that to securely compute 1 bit of the desired sum, each user needs to send at least 1 bit to the associated relay, each relay needs to send at least 1 bit to the server, each user needs to hold at least 1 key bit, and all users need to collectively hold at least $\max\{V+T, \min\{U+T-1, UV-1\}\}$ (source) key bits. The characterization of the minimum source key rate is a major contribution of this work. We propose a novel scheme which achieves the optimal user-to-relay, relay-to-server communication rates, individual and source key rates simultaneously. A tight information-theoretic converse is also derived. Throughout the paper, we use the following notation: $[m:n] \triangleq \{m, \cdots, n\}$ and $[1:n]$ is written as $[n]$ for brevity. Calligraphic letters (e.g., $\mathcal{A}, \mathcal{B}$) represent sets and $\mathcal{A} \backslash \mathcal{B} \triangleq \{x \in \mathcal{A} : x \notin \mathcal{B}\}$. $H(\cdot)$ and $I(\cdot)$ represent entropy and mutual information respectively.

## II. Problem Statement

We study the secure aggregation problem in a hierarchical network consisting of three layers, an aggregation server, an intermediate layer consisting of $U$ relays and a total of $UV$ users at the bottom layer. The network has two hops, i.e., the server is connected to all the relays and each relay is connected to a disjoint subset of $V$ users that form a cluster (See Fig. 1 for an example with $U=2, V=3$). This network structure finds practical applications in distributed machine learning systems such hierarchical Federated Learning (FL) [22]–[24] where the edge servers act as relays and forward the clients' partially aggregated local parameters to the cloud server for model aggregation. All connection links are orthogonal (i.e., no interference among links) and noiseless. The $v^{\text{th}}$ user of the $u^{\text{th}}$ cluster is labelled as

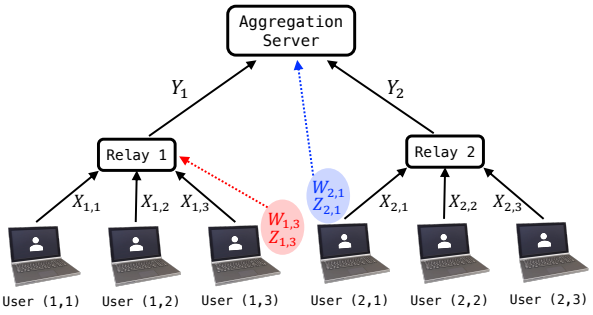


Fig. 1. Hierarchical secure aggregation with $(U,V,T)=(2,3,1)$ where the server and each relay can collude with at most one user. Here the server colludes with User (2,1) and Relay 1 colludes with User (1,3).

user $(u,v) \in [U] \times [V]$. Let $\mathcal{M}_u \triangleq \{(u,v)\}_{v\in[V]}$ denote the $u^{\text{th}}$ cluster. Each user $(u,v)$ is equipped with an input $W_{u,v}$ (e.g., the local gradient or model parameters in FL) of $H(W_{u,v}) = L$ symbols (in $q$-ary units) from some finite field $\mathbb{F}_q$. The inputs of the users are assumed to be uniformly distributed[1] and independent of each other. Each user is also equipped with a key variable $Z_{u,v}$ of $L_Z$ symbols from $\mathbb{F}_q$ which is generated from a source key variable $Z_\Sigma$ containing $H(Z_\Sigma) = L_{Z_\Sigma}$ symbols, i.e.,

$$H\left(\{Z_{u,v}\}_{u\in[U],v\in[V]} | Z_\Sigma\right) = 0. \tag{1}$$

The keys $\mathcal{Z} \triangleq \{Z_{u,v}\}_{u\in[U],v\in[V]}$ are independent of the inputs $\mathcal{W} \triangleq \{W_{u,v}\}_{u\in[U],v\in[V]}$, i.e.,

$$H(\mathcal{Z},\mathcal{W}) = H(\mathcal{Z}) + \sum_{u\in[U],v\in[V]} H(W_{u,v}). \tag{2}$$

The aggregation server wishes to learn the sum of all inputs $\sum_{u\in[U],v\in[V]} W_{u,v}$ and should be prohibited from learning anything about $\mathcal{W}$ more than the sum itself even if it colludes with (i.e., gaining access to the individual inputs and keys) any set of up to $T$ users. The relays are oblivious, that is, each relay should not learn anything about $\mathcal{W}$ even if it colludes with up to $T$ users.

A two-hop communication protocol is used. Over the first hop, User $(u,v)$ sends a message $X_{u,v}$ containing $H(X_{u,v}) = L_X$ symbols to Relay $u$, as a function of $W_{u,v}$ and $Z_{u,v}$. Over the second hop, Relay $u$ sends a message $Y_u$ of $H(Y_u) = L_Y$ symbols to the aggregation server, as a function of the messages $\{X_{u,v}\}_{v\in[V]}$ received from the users in its cluster. Hence,

$$H\left(X_{u,v} | W_{u,v}, Z_{u,v}\right) = 0, \ \forall (u,v) \in [U]\times[V] \tag{3}$$

$$H\left(Y_u | \{X_{u,v}\}_{v\in[V]}\right) = 0, \ \forall u \in [U] \tag{4}$$

From the relay's messages, the server should be able to recover the desired sum of inputs, i.e,

$$H\left(\sum_{u\in[U],v\in[V]} W_{u,v} \Big| \{Y_u\}_{u\in[U]}\right) = 0. \tag{5}$$

[1]The uniformity of the inputs is used to facilitate the converse proof although our proposed scheme works with arbitrary input distributions.

Security refers to the constraint that each relay should not infer any information about the inputs $\mathcal{W}$ (*relay security*) and the server should not obtain any information about $\mathcal{W}$ beyond the knowledge of the desired sum $\sum_{u,v} W_{u,v}$ (*server security*), even if each relay and the server can respectively collude with any set $\mathcal{T}$ of no more than $T$ users, i.e., $|\mathcal{T}| \leq T$. More specifically, relay security can be expressed in terms of mutual information as

$$I\left(\{X_{u,v}\}_{v\in[V]}; \mathcal{W} \,\middle|\, \{W_{i,j}, Z_{i,j}\}_{(i,j)\in\mathcal{T}}\right) = 0, \forall u \in [U] \quad (6)$$

for any $\mathcal{T}$. Server security requires that

$$I\left(\{Y_u\}_u; \mathcal{W} \,\middle|\, \sum_{u,v} W_{u,v}, \{W_{i,j}, Z_{i,j}\}_{(i,j)\in\mathcal{T}}\right) = 0, \forall \mathcal{T} \quad (7)$$

The communication rate $R_X$ ($R_Y$) characterizes how many symbols that each message $X_{u,v}$ ($Y_u$) contains per input symbol and the individual (source) key rate $R_Z$ ($R_{Z_\Sigma}$) characterizes how many symbols that each key variable $Z_{u,v}$ ($Z_\Sigma$) contains per input symbol, i.e.,

$$R_X \triangleq \frac{L_X}{L}, R_Y \triangleq \frac{L_Y}{L}, R_Z \triangleq \frac{L_Z}{L}, R_{Z_\Sigma} \triangleq \frac{L_{Z_\Sigma}}{L}. \quad (8)$$

A rate tuple $(R_X, R_Y, R_Z, R_{Z_\Sigma})$ is said to be achievable if there exists a secure aggregation scheme (i.e., the design of the keys $\{Z_{u,v}\}_{u,v}, Z_\Sigma$ and messages $\{X_{u,v}\}_{u,v}, \{Y_u\}_u$ subject to (3) and (4)) with communication rates $R_X, R_Y$ and key rates $R_Z, R_{Z_\Sigma}$ for which the correctness constraint (5) and the security constraints (6), (7) are satisfied. The optimal rate region $\mathcal{R}^*$ is defined as the closure of the set of all achievable rate tuples. For ease of notation, let $\mathcal{C}_\mathcal{T} \triangleq \{W_{u,v}, Z_{u,v}\}_{(u,v)\in\mathcal{T}}$ denote the collection of inputs and keys at the colluding users $\mathcal{T}$. Also denote $W^\Sigma \triangleq \sum_{u,v} W_{u,v}$ and $W_u^\Sigma \triangleq \sum_v W_{u,v}, u \in [U]$ as the sum of inputs of all users and the $u^{\text{th}}$ cluster respectively.

## III. Main Result

*Theorem 1:* For the hierarchical secure aggregation problem with $U$ relays, $V$ users per cluster and a maximum of $T$ colluding users, the optimal rate region is given by

$$\mathcal{R}^* = \left\{ \begin{array}{l} R_X \geq 1, R_Y \geq 1, R_Z \geq 1, \\ R_{Z_\Sigma} \geq \max\{V+T, \min\{UV-1, U+T-1\}\} \end{array} \right\}$$

if $T < (U-1)V$ and $\mathcal{R}^* = \emptyset$ if $T \geq (U-1)V$.

We highlight the implications of Theorem 1 as follows:

1) *Infeasible regime*: When $T \geq (U-1)V$, the secure aggregation problem is not feasible. Intuitively, when $T \geq (U-1)V$, each relay can collude with all inter-cluster users so that it is able to recover the sum of all inputs because it has access to all the information necessary to construct the relay-to-server messages $\{Y_u\}_{u\in[U]}$. This violates the relay security constraint (6).
2) *Source key rate*: The optimal $R_{Z_\Sigma}$ takes the maximum of $V+T$ and $\min\{U+T-1, UV-1\}$. An intuitive explanation to this formula is provided as follows. When $T < (U-1)V$, for any relay, in addition to the $V$ intra-cluster users, we need $T$ more independent keys to tackle user collusion with that relay, resulting in the $V+T$ term. The second term is mainly due to server security. When $T \leq U(V-1)$, we have $\min\{U+T-1, UV-1\} = U+T-1$. In this case, we need $U-1$ keys to protect the relay-to-server messages and $T$ additional independent keys against user collusion for the sake of server security. Otherwise when $T > U(V-1)$, we have $\min\{U+T-1, UV-1\} = UV-1$, i.e., the source key rate will not exceed $UV-1$ (the total number of users minus one) and it does not depend on $T$ in this regime. In Section V, the above intuitions are formalized through an information-theoretic converse proof.
3) *Impact of network hierarchy*: Ignoring the boundary cases of $T \geq U(V-1)$, the optimal source key rate can be written as $\max\{V+T, U+T-1\}$. Comparing with the basic one-hop secure aggregation setting [15] where the minimum source key rate is $UV-1$, we make two interesting observations. First, the total number of users $UV$ is (approximately) replaced by the maximum value of $U$ and $V$, i.e., a smaller amount source key consumption is required in HSA. This highlights the benefits of employing a hierarchical network structure where there exists a natural separation between the relays and the (inter-cluster) users, and also between the server and the users. Second, the collusion level $T$ comes into play explicitly which necessitates more complicated design strategies than [15].

## IV. Achievable Scheme

In this section, we illustrate the proposed secure aggregation scheme through an example. A brief sketch of the general scheme is provided due to space limit. We refer the readers to [25] for a detailed description.

*Example 1:* Consider $(U, V, T) = (2, 3, 1)$ as shown in Fig. 1. Each input $W_{u,v}$ contains one symbol from $\mathbb{F}_3$. The source key $Z_\Sigma = (N_1, N_2, N_3, N_4)$ contains 4 i.i.d. uniform random variables from $\mathbb{F}_3$. The individual keys are chosen as

$$\begin{aligned} &Z_{1,1} = N_1, Z_{1,2} = N_2, Z_{1,3} = N_3, Z_{2,1} = -N_1 + N_4, \\ &Z_{2,2} = -N_2 + N_4, Z_{2,3} = -(N_3 + 2N_4). \end{aligned} \quad (9)$$

User $(u, v)$ sends $X_{u,v} = W_{u,v} + Z_{u,v}$ to Relay $u$ and Relay $u$ sends $Y_u = \sum_{v=1}^3 X_{u,v}$ to the server. In particular,

$$\begin{aligned} Y_1 &= W_{1,1} + W_{1,2} + W_{1,3} + N_1 + N_2 + N_3, \\ Y_2 &= W_{2,1} + W_{2,2} + W_{2,3} - (N_1 + N_2 + N_3). \end{aligned} \quad (10)$$

Since $L_X = L_Y = L_Z = 1, L_{Z_\Sigma} = 4$, the achieved rates are $R_X = R_Y = R_Z = 1, R_{Z_\Sigma} = 4$ which matches the lower bound in Theorem 1. Correctness is straightforward because $Y_1 + Y_2 = \sum_{u,v} W_{u,v}$. Security is proved as follows.

**Relay security**. An important property of the key design (9) is that *any 4 out of the total 6 keys are mutually independent.* This means that for any relay $u$, even if it colludes with some inter-cluster user $(u', v')$ where $u' \neq u$ and gains

access to $Z_{u',v'}$, it cannot infer the inputs $\{W_{u,v}\}_{v=1}^3$ from the messages $\{W_{u,v}+Z_{u,v}\}_{v=1}^3$ due to the independence of $\{Z_{u,v}\}_{v=1}^3$ and $Z_{u',v'}$. Therefore, relay security is achieved. We formalize the above intuition as follows. Consider Relay 1 colluding with $\mathcal{T}=\{(2,1)\}$ so that $\mathcal{C}_{\mathcal{T}}=\{W_{2,1},Z_{2,1}\}$:

$$
\begin{aligned}
&I\left(\{X_{1,v}\}_{v=1}^3;\mathcal{W}|\mathcal{C}_{\mathcal{T}}\right)\\
&=H\left(\{X_{1,v}\}_{v=1}^3|\mathcal{C}_{\mathcal{T}}\right)-H\left(\{X_{1,v}\}_{v=1}^3|\mathcal{C}_{\mathcal{T}},\mathcal{W}\right) && \text{(11a)}\\
&\le H\left(\{X_{1,v}\}_{v=1}^3\right)-H\left(\{X_{1,v}\}_{v=1}^3|\mathcal{C}_{\mathcal{T}},\mathcal{W}\right) && \text{(11b)}\\
&\le 3-H\left(\{X_{1,v}\}_{v=1}^3|\mathcal{C}_{\mathcal{T}},\mathcal{W}\right) && \text{(11c)}\\
&=3-H\left(\{W_{1,v}+Z_{1,v}\}_{v=1}^3|Z_{2,1},\mathcal{W}\right) && \text{(11d)}\\
&=3-H\left(\{Z_{1,v}\}_{v=1}^3|Z_{2,1},\mathcal{W}\right) && \text{(11e)}\\
&\overset{(2)}{=}3-H\left(\{Z_{1,v}\}_{v=1}^3|Z_{2,1}\right) && \text{(11f)}\\
&=3-H\left(N_1,N_2,N_3|-N_1+N_4\right) && \text{(11g)}\\
&=3-H\left(N_1,N_2,N_3,N_4\right)+H\left(-N_1+N_4\right)=0 && \text{(11h)}
\end{aligned}
$$

where (11c) is because each $X_{1,v}$ contains one symbol and uniform distribution maximizes entropy; (11f) is due to the independence of the inputs and the keys; In (11g) we plugged in the key design (9) and the last step is because $N_1,\cdots,N_4$ are i.i.d. and uniform. Since mutual information is non-negative, we have proved $I(\{X_{1,v}\}_{v=1}^3;\mathcal{W}|\mathcal{C}_{\mathcal{T}})=0$.

**Server security**. It can be seen from (10) that $Y_1$ and $Y_2$ are protected by $\pm(N_1+N_2+N_3)$ respectively. By the key design (9), colluding with any user will not eliminate the key component contained in $Y_1$ and $Y_2$ so that the inputs are still protected and the server security is guaranteed. Due to space limit, the rigorous proof of server security is omitted. $\Diamond$

*Remark 1 (Key efficiency):* A naive key generation method [13] suggests using $UV-1=5$ i.i.d. variables $N_1,\cdots,N_5$ each being assigned to one user and assigning $-(N_1+\cdots+N_5)$ to the last user. Our scheme uses a smaller number of i.i.d. variables and thus improving the source key.

*Remark 2 (Sketch of the general scheme):* Given the source key $Z_\Sigma=(N_1,\cdots,N_{R_{Z_\Sigma}^*})$ where $R_{Z_\Sigma}^*=\max\{V+T,\min\{UV-1,U+T-1\}\}$, the individual keys are generated as $(Z_{u,v})_{u\in[U],v\in[V]}^T=\mathbf{H}Z_\Sigma$ where $\mathbf{H}\in\mathbb{F}_q^{UV\times R_{Z_\Sigma}^*}$ is the coefficient matrix to be designed. The communication protocol is that $X_{u,v}=W_{u,v}+Z_{u,v}, Y_u=\sum_{v=1}^V X_{u,v},\forall u,v$ (thus $R_X=R_Y=1$). The server adds up the messages from the relays and obtains $Y_1+\cdots+Y_U=\sum_{u,v}W_{u,v}+\sum_{u,v}Z_{u,v}$. To recover the input sum, the aggregated individual keys must cancel out, i.e., $\sum_{u,v}Z_{u,v}=\sum_{i=1}^K\mathbf{h}_iZ_\Sigma^T=0$ ($\mathbf{h}_i$ denotes the $i^{\text{th}}$ row of $\mathbf{H}$) which implies that $\sum_{i=1}^K\mathbf{h}_i=\mathbf{0}$, i.e., the rows of $\mathbf{H}$ add up to zero. Moreover, the security constraints require statistical independence among subsets of up to $R_{Z_\Sigma}^*$ individual keys which entails linear independence of every $R_{Z_\Sigma}^*$ rows of $\mathbf{H}$. We propose a specific construction of $\mathbf{H}$ utilizing a novel matrix structure called *extended Vandermonde matrix* which satisfies the zero-sum-of-rows and linear independence properties.

## V. Converse

In this section, we derive lower bounds on the communication and key rates $R_X,R_Y,R_Z$ and $R_{Z_\Sigma}$. Because these bounds match the achievable rates in Section IV, the optimality of the proposed scheme is established. For ease of presentation, we denote $W^\Sigma\triangleq\sum_{u,v}W_{u,v}$ and $\mathcal{W}_\mathcal{A}\triangleq\{W_{u,v}\}_{(u,v)\in\mathcal{A}}$, $\mathcal{Z}_\mathcal{A}\triangleq\{Z_{u,v}\}_{(u,v)\in\mathcal{A}}$, $\mathcal{Y}_\mathcal{U}\triangleq\{Y_u\}_{u\in\mathcal{U}}$ for any $\mathcal{A}\subseteq[U]\times[V]$, $\mathcal{U}\subseteq[U]$.

### A. Infeasible Regime: $T\ge(U-1)V$

When $T\ge(U-1)V$, each relay can collude with all inter-cluster users and it is impossible to avoid leakage to this relay so that relay security is violated.

### B. Feasible Regime: $T<(U-1)V$

We start with a useful lemma which states that each message $X_{u,v}$ and $Y_u$ should contain at least $L$ symbols even if all other inputs are known.

*Lemma 1: For any $u\in[U],v\in[V]$, we have*

$$H\left(X_{u,v}|\{W_{i,j},Z_{i,j}\}_{(i,j)\in[U]\times[V]\backslash\{(u,v)\}}\right)\ge L, \quad \text{(12a)}$$

$$H\left(Y_u|\{W_{i,j},Z_{i,j}\}_{(i,j)\in[U]\times[V]\backslash\{(u,v)\}}\right)\ge L. \quad \text{(12b)}$$

With Lemma 1, the converse bounds on $R_X,R_Y$ and $R_Z$ follow immediately. We elaborate on the derivation of the lower bound on $R_{Z_\Sigma}$ which is major novelty of this work.

**Proof of** $R_X\ge1$: For any $u\in[U],v\in[V]$, we have $L_X=H(X_{u,v})\ge L$ due to (12a), so $R_X=L_X/L\ge1$.

**Proof of** $R_Y\ge1$: For any $u\in[U]$, we have $L_Y=H(Y_u)\ge L$ due to (12b), so $R_Y=L_Y/L\ge1$.

**Proof of** $R_Z\ge1$: The proof of the individual key rate relies on (12a). Intuitively, to protect any individual input, the key must be at least the size of the input size. The detailed proof is omitted due to space limit.

**Proof of** $R_{Z_\Sigma}\ge\max\{V+T,\min\{U+T-1,UV-1\}\}$. This converse bound is given as the maximum of two terms, where the first term $V+T$ is due to relay security and the second term $\min\{U+T-1,UV-1\}$ is mainly due to server security while relay security is also needed. We first show that for any relay, the joint entropy of the keys at any set of intra-cluster users $\mathcal{V}$ is at least $|\mathcal{V}|L$ as stated in Lemma 2.

*Lemma 2: For any $u\in[U]$, $\mathcal{V}\subseteq[V]$, and any $\mathcal{T}\subset([U]\backslash\{u\})\times[V]$ where $|\mathcal{T}|\le T$, we have*

$$H\left(\{Z_{u,v}\}_{v\in\mathcal{V}}|\{Z_{i,j}\}_{(i,j)\in\mathcal{T}}\right)\ge|\mathcal{V}|L. \quad \text{(13)}$$

*Proof of* $R_{Z_\Sigma}\ge V+T$: Suppose $T=mV+n$ where $m,n$ are non-negative integers and $n\le V-1$. We apply Lemma 2 repeatedly on different colluding set $\mathcal{T}$ with decreasing sizes as follows:

$$
\begin{aligned}
&L_{Z_\Sigma}=H(Z_\Sigma) && \text{(14a)}\\
&\overset{(1)}{=}H\left(Z_\Sigma,\mathcal{Z}_{[m+1]\times[V]},\{Z_{m+2,v}\}_{v\in[n]}\right) && \text{(14b)}\\
&\ge H\left(\mathcal{Z}_{[m+1]\times[V]},\{Z_{m+2,v}\}_{v\in[n]}\right) && \text{(14c)}\\
&=H\left(\{Z_{1,v}\}_{v\in[V]}|\mathcal{Z}_{[2:m+1]\times[V]},\{Z_{m+2,v}\}_{v\in[n]}\right)\\
&\quad+H\left(\mathcal{Z}_{[2:m+1]\times[V]},\{Z_{m+2,v}\}_{v\in[n]}\right) && \text{(14d)}
\end{aligned}
$$

$$\overset{(13)}{\geq} VL + H\left(\mathcal{Z}_{[2:m+1]\times[V]}, \{Z_{m+2,v}\}_{v\in[n]}\right) \tag{14e}$$
$$= VL + H\left(\{Z_{2,v}\}_{v\in[V]}|\mathcal{Z}_{[3:m+1]\times[V]}, \{Z_{m+2,v}\}_{v\in[n]}\right) + H\left(\mathcal{Z}_{[3:m+1]\times[V]}, \{Z_{m+2,v}\}_{v\in[n]}\right) \tag{14f}$$
$$\geq \cdots$$
$$\overset{(13)}{\geq} mVL + H\left(\{Z_{m+1,v}\}_{v\in[V]}|\{Z_{m+2,v}\}_{v\in[n]}\right) + H\left(\{Z_{m+2,v}\}_{v\in[n]}\right) \tag{14g}$$
$$\overset{(13)}{\geq} (m+1)VL + H\left(\{Z_{m+2,v}\}_{v\in[n]}\right) \tag{14h}$$
$$\overset{(13)}{\geq} (m+1)VL + nL \tag{14i}$$
$$= (V+T)L \tag{14j}$$

where from (14e) to (14g) we applied Lemma 2 with $u = 1, \mathcal{V} = [V], \mathcal{T} = ([2:m+1]\times[V]) \cup (\{m+2\}\times[n])$, $u = 2, \mathcal{V} = [V], \mathcal{T} = ([3:m+1]\times[V]) \cup (\{m+2\}\times[n]), \cdots, u = m$. In (14h) we applied Lemma 2 with $u = m+1, \mathcal{V} = [V]$ and $\mathcal{T} = \{m+2\}\times[n]$; in (14i) we applied Lemma 2 with $u = m+2, \mathcal{V} = [n]$ and $\mathcal{T} = \emptyset$. As a result, we proved $R_{Z_\Sigma} = L_{Z_\Sigma}/L \geq V + T$.

*Proof of* $R_{Z_\Sigma} \geq \min\{U+T-1, UV-1\}$: This bound is mainly due to server security. First note that $\min\{U+T-1, UV-1\} = U+T-1$ if $T \leq U(V-1)$ and $UV-1$ if $T \geq U(V-1)$. So we need to prove 1) $R_{Z_\Sigma} \geq U+T-1$ when $T \leq U(V-1)$ and 2) $R_{Z_\Sigma} \geq UV-1$ when $T \geq U(V-1)$. 1) suggests $R_{Z_\Sigma} \geq U + U(V-1) - 1 = UV - 1$ with $U(V-1)$ colluding users. Since increasing $T$ can only possibly increase the source key rate, we have $R_{Z_\Sigma} \geq UV-1$ when $T \geq U(V-1)$, i.e., 2) is implied by 1). Hence, we only need to prove 1) which is shown as follows:

Choose $\mathcal{T}$ so that $|\mathcal{T}| = T$ and for any cluster $u \in [U]$, there is at least one user $(u, v_u) \in \mathcal{M}_u$ that is not in $\mathcal{T}$.[2] Note that such $\mathcal{T}$ exists because $T \leq U(V-1)$. We have

$$\begin{aligned} L_{Z_\Sigma} = H(Z_\Sigma) &\overset{(1)}{=} H\left(Z_\Sigma, \mathcal{Z}, \mathcal{Z}_\mathcal{T}\right) \\ &\geq H\left(\mathcal{Z}, \mathcal{Z}_\mathcal{T}\right) \\ &= H\left(\mathcal{Z}|\mathcal{Z}_\mathcal{T}\right) + H\left(\mathcal{Z}_\mathcal{T}\right). \end{aligned} \tag{15}$$

We find lower bounds for the two terms in (15) respectively.

A lower bound on the first term can be derived as follows:

$$H\left(\mathcal{Z}|\mathcal{W}_\mathcal{T}, \mathcal{Z}_\mathcal{T}\right)$$
$$\geq H\left(\mathcal{Z}|\mathcal{W}, \mathcal{W}_\mathcal{T}, \mathcal{Z}_\mathcal{T}\right) \tag{16a}$$
$$\geq I\left(\mathcal{Z}; \mathcal{Y}_{[U]}|\mathcal{W}, \mathcal{W}_\mathcal{T}, \mathcal{Z}_\mathcal{T}\right) \tag{16b}$$
$$\overset{(3),(4)}{\geq} H\left(\mathcal{Y}_{[U]}|\mathcal{W}, \mathcal{W}_\mathcal{T}, \mathcal{Z}_\mathcal{T}\right) \tag{16c}$$
$$= H\left(\mathcal{Y}_{[U]}|\mathcal{W}_\mathcal{T}, \mathcal{Z}_\mathcal{T}\right) - I\left(\mathcal{Y}_{[U]}; \mathcal{W}|\mathcal{W}_\mathcal{T}, \mathcal{Z}_\mathcal{T}\right) \tag{16d}$$
$$\geq \sum_{k=1}^{U} H\left(\mathcal{Y}_k|\mathcal{Y}_{[U]\setminus\{k\}}, \mathcal{W}_\mathcal{T}, \mathcal{Z}_\mathcal{T}\right) - I\left(\mathcal{Y}_{[U]}; \mathcal{W}, W^\Sigma|\mathcal{W}_\mathcal{T}, \mathcal{Z}_\mathcal{T}\right) \tag{16e}$$
$$\geq \sum_{k=1}^{U} H\left(\mathcal{Y}_k|\mathcal{Y}_{[U]\setminus\{k\}}, \mathcal{W}_{\widetilde{\mathcal{T}}_k}, \mathcal{Z}_{\widetilde{\mathcal{T}}_k}\right) - I\left(\mathcal{Y}_{[U]}; W^\Sigma|\mathcal{W}_\mathcal{T}, \mathcal{Z}_\mathcal{T}\right) - \underbrace{I\left(\mathcal{Y}_{[U]}; \mathcal{W}|W^\Sigma, \mathcal{W}_\mathcal{T}, \mathcal{Z}_\mathcal{T}\right)}_{=0} \tag{16f}$$
$$\overset{(3),(4)}{\geq} \sum_{k=1}^{U} H\left(\mathcal{Y}_k|\mathcal{W}_{([U]\times[V])\setminus\{(k,v_k)\}}, \mathcal{Z}_{([U]\times[V])\setminus\{(k,v_k)\}}\right) - H\left(W^\Sigma|\mathcal{W}_\mathcal{T}, \mathcal{Z}_\mathcal{T}\right) + \underbrace{H\left(W^\Sigma|\mathcal{Y}_{[U]}, \mathcal{W}_\mathcal{T}, \mathcal{Z}_\mathcal{T}\right)}_{=0} \tag{16g}$$
$$\overset{(12b),(2)}{\geq} UL - H\Bigg(\sum_{(u,v)\in([U]\times[V])\setminus\mathcal{T}} W_{u,v}\Bigg) \tag{16h}$$
$$= (U-1)L \tag{16i}$$

where we denote $\widetilde{\mathcal{T}}_k \triangleq \mathcal{T} \cup ([U]\setminus\{k\}\times[V])$ in (16f). (16c) is because $H(\mathcal{Y}_{[U]}|\mathcal{W}, \mathcal{W}_\mathcal{T}, \mathcal{Z}_\mathcal{T}, \mathcal{Z}) = 0$ since the message set $\mathcal{Y}_{[U]}$ is a function of the input and key sets $\mathcal{W}, \mathcal{Z}$; (16f) is due to server security (7); in (16g), the first term is because $\mathcal{T} \cup (([U]\setminus\{k\})\times[V]) \subseteq ([U]\times[V])\setminus\{(k, v_k)\}$ and the third term is due to the correctness constraint (5); (16i) is due to the uniformity of the inputs.

We then derive a lower bound for $H\left(\mathcal{Z}_\mathcal{T}\right)$. Write $\mathcal{T} = \mathcal{T}_1 \cup \cdots \cup \mathcal{T}_U$ where $\mathcal{T}_k = \mathcal{T} \cap \mathcal{M}_k$ and $|\mathcal{T}_k| \leq V-1, \forall k \in [U]$.

$$H\left(\mathcal{Z}_\mathcal{T}\right) = H\left(\mathcal{Z}_{\mathcal{T}_1}, \cdots, \mathcal{Z}_{\mathcal{T}_U}\right) \tag{17a}$$
$$= \sum_{k=1}^{U} H\left(\mathcal{Z}_{\mathcal{T}_k}|\,\mathcal{Z}_{\mathcal{T}_1}, \cdots, \mathcal{Z}_{\mathcal{T}_{k-1}}\right) \tag{17b}$$
$$\overset{(13)}{\geq} \sum_{k=1}^{U} |\mathcal{T}_k| L = TL \tag{17c}$$

where in (17b) we used the chain rule of entropy and the last line is due to Lemma 2. Finally, by combining (16) and (17) in (15), we obtain $L_{Z_\Sigma} \geq H\left(\mathcal{Z}_\mathcal{T}\right) + H\left(\mathcal{Z}|\mathcal{Z}_\mathcal{T}\right) \geq (U+T-1)L$, i.e., $R_{Z_\Sigma} = L_{Z_\Sigma}/L \geq U+T-1$, completing the converse proof.

## VI. Conclusion

We studied the hierarchical secure aggregation problem where communication takes place on a 3-layer hierarchical network consisting of clustered users connected to an aggregation server via intermediate relay nodes. We characterized the optimal communication and key rate region under user collusion. Future directions may include extension to deeper network hierarchies, allowing user dropouts and more complicated connection patterns between the users and relays.


## Acknowledgement

The work of X. Zhang and G. Caire was partially funded by the European Research Council under the ERC Advanced Grant N. 789190, CARENET. The work of K. Wan was partially funded by the National Natural Science Foundation of China (NSFC-12141107). The work of H. Sun was supported in part by NSF under Grant CCF-2045656 and Grant CCF-2312228. The work of M. Ji was supported by the National Science Foundation (NSF) Award 2312227 and CAREER Award 2145835.


[2]Because the security constraints have to be satisfied for every possible $\mathcal{T}$, the converse derived for a specific choice of $\mathcal{T}$ is also a valid converse.

## 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] J. Konecnỳ, 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*, vol. 8, 2016.

[3] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings *et al.*, "Advances and open problems in federated learning," *Foundations and trends® in machine learning*, vol. 14, no. 1–2, pp. 1–210, 2021.

[4] N. Rieke, J. Hancox, W. Li, F. Milletari, H. R. Roth, S. Albarqouni, S. Bakas, M. N. Galtier, B. A. Landman, K. Maier-Hein *et al.*, "The future of digital health with federated learning," *NPJ digital medicine*, vol. 3, no. 1, pp. 1–7, 2020.

[5] T. Yang, G. Andrew, H. Eichner, H. Sun, W. Li, N. Kong, D. Ramage, and F. Beaufays, "Applied federated learning: Improving google keyboard query suggestions," *arXiv preprint arXiv:1812.02903*, 2018.

[6] S. P. Karimireddy, S. Kale, M. Mohri, S. Reddi, S. Stich, and A. T. Suresh, "Scaffold: Stochastic controlled averaging for federated learning," in *International conference on machine learning*. PMLR, 2020, pp. 5132–5143.

[7] W. Liu, L. Chen, Y. Chen, and W. Zhang, "Accelerating federated learning via momentum gradient descent," *IEEE Transactions on Parallel and Distributed Systems*, vol. 31, no. 8, pp. 1754–1766, 2020.

[8] N. Bouacida and P. Mohapatra, "Vulnerabilities in federated learning," *IEEE Access*, vol. 9, pp. 63 229–63 249, 2021.

[9] 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.

[10] 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 *proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1175–1191.

[11] K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farokhi, S. Jin, T. Q. Quek, and H. V. Poor, "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE transactions on information forensics and security*, vol. 15, pp. 3454–3469, 2020.

[12] P. Kairouz, Z. Liu, and T. Steinke, "The distributed discrete gaussian mechanism for federated learning with secure aggregation," in *International Conference on Machine Learning*. PMLR, 2021, pp. 5201–5212.

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

[14] 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," *Proceedings of Machine Learning and Systems*, vol. 4, pp. 694–720, 2022.

[15] Y. Zhao and H. Sun, "Secure summation: Capacity region, groupwise key, and feasibility," *IEEE Transactions on Information Theory*, 2023.

[16] K. Wan, H. Sun, M. Ji, T. Mi, and G. Caire, "The capacity region of information theoretic secure aggregation with uncoded groupwise keys," *IEEE Transactions on Information Theory*, 2024.

[17] Y. Zhao and H. Sun, "Mds variable generation and secure summation with user selection," *arXiv preprint arXiv:2211.01220*, 2022.

[18] ——, "The optimal rate of mds variable generation," in *2023 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2023, pp. 832–837.

[19] Z. Li, Y. Zhao, and H. Sun, "Weakly secure summation with colluding users," in *2023 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2023, pp. 2398–2403.

[20] H. Sun, "Secure aggregation with an oblivious server," *arXiv preprint arXiv:2307.13474*, 2023.

[21] F. Karakoç, M. Önen, and Z. Bilgin, "Secure aggregation against malicious users," in *Proceedings of the 26th ACM Symposium on Access Control Models and Technologies*, 2021, pp. 115–124.

[22] L. Liu, J. Zhang, S. Song, and K. B. Letaief, "Client-edge-cloud hierarchical federated learning," in *ICC 2020-2020 IEEE international conference on communications (ICC)*. IEEE, 2020, pp. 1–6.

[23] T. Castiglia, A. Das, and S. Patterson, "Multi-level local sgd: Distributed sgd for heterogeneous hierarchical networks," in *International Conference on Learning Representations*, 2020.

[24] J. Wang, S. Wang, R.-R. Chen, and M. Ji, "Demystifying why local aggregation helps: Convergence analysis of hierarchical sgd," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 36, no. 8, 2022, pp. 8548–8556.

[25] X. Zhang, K. Wan, H. Sun, S. Wang, M. Ji, and G. Caire, "Optimal communication and key rate region for hierarchical secure aggregation with user collusion," 2024. [Online]. Available: https://arxiv.org/abs/2410.14035