Information Theoretic Secure Aggregation with User Dropouts

Yizhou Zhao and Hua Sun
Department of Electrical Engineering
University of North Texas, Denton, TX 76203
Email: yizhouzhao@my.unt.edu, hua.sun@unt.edu

2021 IEEE International Symposium on Information Theory (ISIT) | 978-1-5386-8209-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISIT45174.2021.9517953

***Abstract*—In the robust secure aggregation problem, a server wishes to learn and only learn the sum of the inputs of a number of users while some users may drop out (i.e., may not respond). The identity of the dropped users is not known a priori and the server needs to securely recover the sum of the remaining surviving users. We consider the following minimal two-round model of secure aggregation. Over the first round, any set of no fewer than U users out of K users respond to the server and the server wants to learn the sum of the inputs of all responding users. The remaining users are viewed as dropped. Over the second round, any set of no fewer than U users of the surviving users respond (i.e., dropouts are still possible over the second round) and from the information obtained from the surviving users over the two rounds, the server can decode the desired sum. The security constraint is that even if the server colludes with any T users and the messages from the dropped users are received by the server (e.g., delayed packets), the server is not able to infer any additional information beyond the sum in the information theoretic sense. For this information theoretic secure aggregation problem, we characterize the optimal communication cost. When $U \leq T$, secure aggregation is not feasible, and when $U > T$, to securely compute one symbol of the sum, the minimum number of symbols sent from each user to the server is 1 over the first round, and $1/(U-T)$ over the second round.**

I. Introduction

The rapidly increasing volume of data available at massive distributed nodes enables powerful large-scale learning applications. For example, in federated learning [1]–[3], a large number of mobile users wish to collaboratively train a shared global model, coordinated by a central server. While the distributed users are willing to cooperate with the server to learn the shared model, they do not fully trust the server and do not want to reveal any information beyond what is necessary to train the desired model. Specifically, when the local models of the distributed users are aggregated (in the form of summation usually) at the server to produce the global model, each user does not want to reveal any additional information about its local data. Therefore, regarding security, the central technical problem is secure sum computation or secure aggregation [4], [5], i.e., how to compute, with as little communication as possible, the sum of the inputs of a number of users without exposing any information beyond the sum. A particular challenge in secure aggregation brought by federated learning is the phenomenon of user dropouts, i.e., some users whose identities are not known beforehand may drop from the learning procedure (due to unreliable communication connections or limited battery life) and the server needs to be able to robustly recover the sum of the inputs of the remaining surviving users while learning nothing else at the same time. The robustness to dropped users is a key requirement that calls for novel models and analysis. The objective of this work is to understand the fundamental communication limits of information theoretic secure aggregation with user dropouts.

Secure Aggregation with User Dropouts

The secure aggregation problem is comprised of one server and K users. User $k, k \in \{1, 2, \cdots, K\}$ holds an input W_k, which is a vector of L elements from a field. In federated learning, the input W_k may represent the local model, model update, gradient, loss, or parameters of User k, from one iteration of the iterative training optimization process and is typically high-dimensional, i.e., L is large, which matches well with the Shannon theoretic formulation where L is allowed to approach infinity. A randomness variable Z_k, independent of all inputs, is generated offline (before the values of $W_1, \cdots, W_K$ are known) and is available to User k to assist with the secure aggregation task.

The server wishes to compute the element-wise sum of the vector inputs of all users. To do so, each user sends a message X_k, as a function of W_k and Z_k, to the server. However, due to user dropouts, the server may not receive all messages; if only the messages from the set of users $\mathcal{U}_1$ arrive at the server and other messages are dropped, then the server wants to securely compute $\sum_{k\in\mathcal{U}_1} W_k$, i.e., the sum of the inputs of all responding users, from $(X_k : k \in \mathcal{U}_1)$. For example, suppose $K = 4$ and $\mathcal{U}_1 = \{1, 2, 3\}$. Then the server sees only X_1, X_2, X_3 and wants to recover $W_1 + W_2 + W_3$ while learning no other information, e.g., the server cannot infer $W_1 + W_2$. We now observe an inherent deficiency of such a model, caused by the uncertainty of the identity of the dropped users. As it is not known a priori which users will drop, the sent messages X_k cannot depend on the set of dropped users and must enable secure computation for all possible responding users. For example, if $\mathcal{U}_1 = \{1, 2\}$, then the server must be able to decode $W_1 + W_2$ from X_1, X_2, which contradicts the security constraint for the case where $\mathcal{U}_1 = \{1, 2, 3\}$, i.e., from X_1, X_2, X_3, the server can learn only $W_1+W_2+W_3$. Therefore, for the above communication model as the identity of the responding users is unknown beforehand, it is not feasible to learn only the sum of their inputs and nothing else.

The remedy is to include additional rounds of communication, and this solution has been taken in prior works on secure aggregation [4]–[8]. In this work, we consider the simplest model of two rounds. We refer to the round that is discussed above and parameterized by $X_1, \cdots, X_K$, as the first round. At the end of the first round, the server informs all responding users about the surviving user set $\mathcal{U}_1$ and the remaining users are viewed as dropped thus no further communication with them is requested. One additional round of messages are requested from the surviving users in $\mathcal{U}_1$. This round is referred to as the second round and the message from User $k \in \mathcal{U}_1$ is denoted as $Y_k^{\mathcal{U}_1}$, where the superscript highlights that the identity of the surviving users over the first round is known when the user decides the second round message (also as a function of W_k and Z_k). User dropouts are still possible over the second round and we denote the set of responding users over the second round by $\mathcal{U}_2$, which is a subset of $\mathcal{U}_1$. We assume that $|\mathcal{U}_2|$, the cardinality of $\mathcal{U}_2$, is at least U, a pre-determined threshold parameter. That is, the server will wait for at least U users, e.g., by setting up a proper time deadline. As $\mathcal{U}_2 \subset \mathcal{U}_1$, we have $|\mathcal{U}_1| \geq U$. The setup of this U parameter is interpreted as the worst case estimate of the number of surviving users. See Figure 1 for an example where $K = 4, U = 2$, and $\mathcal{U}_1 = \{1, 3, 4\}$, $\mathcal{U}_2 = \{1, 4\}$.

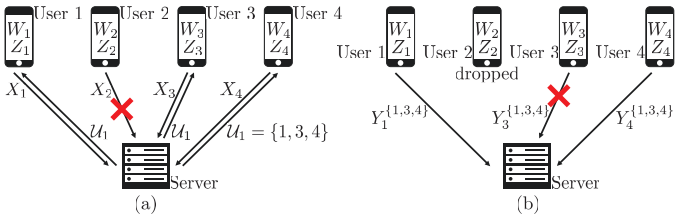

Fig. 1. A secure aggregation problem instance with $K = 4$ users. (a). Over the first round, User 2 is dropped; (b). Over the second round, User 3 is dropped. The server securely computes $W_1 + W_3 + W_4$.

After describing the communication model, we now state the constraints of secure aggregation - correctness and security.

1. *Correctness constraint*: From only the messages received from the surviving users over the two rounds, the server can decode $\sum_{k \in \mathcal{U}_1} W_k$ with no error. For example, in Figure 1, it is required that $W_1 + W_3 + W_4$ can be recovered from $X_1, X_3, X_4, Y_1^{\{1,3,4\}}, Y_4^{\{1,3,4\}}$.

2. *Information theoretic security constraint*: From *all* the messages sent from the users over the two rounds (including those from dropped users as their packets may be merely delayed) and even if the server colludes with any set of at most T users, the server cannot infer any additional information in the information theoretic sense about all inputs $W_1, W_2, \cdots, W_K$ beyond what is already known from the colluding user(s) and the desired sum. For example, suppose $T = 1$ and the colluding user is User 4 in Figure 1, then it is required that from all the messages $X_1, X_2, X_3, X_4, Y_1^{\{1,3,4\}}, Y_3^{\{1,3,4\}}, Y_4^{\{1,3,4\}}$ and colluding user's information W_4, Z_4, no information about W_1, W_2, W_3, W_4 is revealed, except W_4 and $W_1 + W_3 + W_4$. Specifically, while $W_1 + W_3$ can be obtained, nothing more about W_1 or W_3 can be learned.

Importantly, we emphasize that a feasible secure aggregation protocol must satisfy the correctness and security constraints for any first round responding user set $\mathcal{U}_1$ where $|\mathcal{U}_1| \geq U$, any second round responding user set $\mathcal{U}_2$ where $\mathcal{U}_2 \subset \mathcal{U}_1$ and $|\mathcal{U}_2| \geq U$, and any colluding user set $\mathcal{T}$ where $|\mathcal{T}| \leq T$. A secure aggregation protocol specifies a design of the messages $X_k, Y_k^{\mathcal{U}_1}$ and we are interested in characterizing the optimal communication efficiency, i.e., minimizing the number of symbols contained in the messages X_k and $Y_k^{\mathcal{U}_1}$.

As a recap, our information theoretic secure aggregation formulation contains 3 parameters, K (the number of users), U (a threshold parameter on the minimum number of responding users), and T (a threshold parameter on the maximum number of colluding users). We assume that $1 \leq U \leq K - 1$, so there may exist dropped users; otherwise $U = K$ and the problem becomes degraded as all users must respond. We also assume that $0 \leq T \leq K - 2$; otherwise $T = K - 1$ or K, then when the colluding user set contains at least $K - 1$ users, there is nothing to hide, as from the desired sum and $K-1$ inputs from the colluding users, the server can decode all K inputs. For this model, our main goal is to answer the following question - *to compute one symbol of the desired sum function securely, what is the minimum number of symbols that must be sent from the users over the first round and over the second round, as a function of* K, U, T?

Summary of Results

We obtain a complete answer to the above question, i.e., the exact characterization of the optimal communication efficiency of secure aggregation. Specially, we show that

- when $U \leq T$, secure aggregation is not feasible in the information theoretic sense;
- when $U > T$, the minimum number of symbols that each user needs to send is 1 symbol over the first round, and $1/(U - T)$ symbols over the second round, per symbol of desired sum.

The proofs of the above result are fairly standard. The protocol design uses and adapts elements that are frequently encountered in secure (sum) computation literature [9]–[13]. The entropy based proof of impossibility claims uses Shannon's information theoretic security framework [14], which will be adapted to robust secure aggregation and is conceptually similar to that in (symmetric) private information retrieval context [15]–[20]. Due to space limitations, most detailed proofs are deferred to the full version of this paper [21].

Let us conclude the introduction section by summarizing the major differences between our work and existing works on secure aggregation for federated learning, which has attracted tremendous recent attention [4]–[8], [22]–[32]. First of all, to the best of our knowledge, our work is the only one that considers information theoretic security, i.e., unconditional security based on statistical independence; while all prior works focus on cryptographic security, i.e., conditional security against computationally bounded adversaries. Second, we first define the system parameters (e.g., allowed user dropouts and collusions), and then study the fundamental limits (i.e.,

the best possible protocols) given the specified parameters; while most existing works first propose a specific protocol and then analyze its performance (e.g., allowed user dropouts and collusions). Last but not least, we assume that the randomness variables of certain joint distribution are distributed to the users by a trusted third-party before the communication protocol starts (i.e., offline); while most prior works jointly consider randomness generation/distribution and message transmission (i.e., online). We view interactive randomness generation among the users as a separate problem to be studied in a future work (along with the comparison of overall communication and computation cost to existing protocols in [4]–[8]).

II. Problem Statement

The secure aggregation problem involves a server and K users, where $K \geq 2$ and User $k \in \{1, 2, \cdots, K\} \triangleq [K]$ holds an input vector W_k and a randomness variable Z_k. The input vectors $(W_k)_{k\in[K]}$ are independent. Each W_k is an $L \times 1$ column vector and the L elements are i.i.d. uniform symbols from the finite field $\mathbb{F}_q$. $(W_k)_{k\in[K]}$ is independent of $(Z_k)_{k\in[K]}$.

$$\begin{aligned} & H\left((W_k)_{k\in[K]}, (Z_k)_{k\in[K]}\right) \\ = & \sum_{k\in[K]} H(W_k) + H\left((Z_k)_{k\in[K]}\right), \quad (1) \\ & H(W_k) = L \text{ (in } q\text{-ary units)}, \forall k \in [K]. \quad (2) \end{aligned}$$

The communication protocol between the server and the users has two rounds. Over the first round, User k sends a message $X_k, k \in [K]$ to the server. The message X_k is a function of W_k, Z_k and consists of L_X symbols from $\mathbb{F}_q$.

$$H(X_k|W_k, Z_k) = 0, \forall k \in [K]. \quad (3)$$

Some users may drop and the set of surviving users after the first round is denoted as $\mathcal{U}_1$, which can be any set of at least U users, and $1 \leq U \leq K-1$. The server receives the messages $(X_k)_{k\in\mathcal{U}_1}$ and wishes to securely compute $\sum_{k\in\mathcal{U}_1} W_k$, where the vector summation is defined as the element-wise addition over $\mathbb{F}_q$. To do so, the server informs all surviving users about $\mathcal{U}_1$ and requests a second round of messages from them. The second round message sent from User $k \in \mathcal{U}_1$ is denoted as $Y_k^{\mathcal{U}_1}$, which is a function of W_k, Z_k and consists of L_Y symbols from $\mathbb{F}_q$.

$$H(Y_k^{\mathcal{U}_1}|W_k, Z_k) = 0, \forall k \in \mathcal{U}_1, \forall \mathcal{U}_1 \subset [K], |\mathcal{U}_1| \geq U. \quad (4)$$

Some users may drop and the set of surviving users after the second round is denoted as $\mathcal{U}_2$, where $\mathcal{U}_2 \subset \mathcal{U}_1$ and $|\mathcal{U}_2| \geq U$. Then the server receives the messages $\left(Y_k^{\mathcal{U}_1}\right)_{k\in\mathcal{U}_2}$ over the second round.

From the messages received from surviving users, the server must be able to decode the desired sum $\sum_{k\in\mathcal{U}_1} W_k$ with no error, i.e., the following correctness constraint must be satisfied for any $\mathcal{U}_1, \mathcal{U}_2$, where $\mathcal{U}_2 \subset \mathcal{U}_1 \subset [K], |\mathcal{U}_2| \geq U$.

$$\text{[Correctness]} \ H\left(\sum_{k\in\mathcal{U}_1} W_k \middle| (X_k)_{k\in\mathcal{U}_1}, \left(Y_k^{\mathcal{U}_1}\right)_{k\in\mathcal{U}_2}\right) = 0. \quad (5)$$

We impose that security must be guaranteed even if the messages sent from all surviving *and dropped* users are received by the server and the server may collude with any set of at most T users, where $0 \leq T \leq K-2$. Specifically, security refers to the constraint that the server cannot infer any additional information about $(W_k)_{k\in[K]}$ beyond that contained in $\sum_{k\in\mathcal{U}_1} W_k$ and known from the colluding users. That is, the following security constraint must be satisfied for any $\mathcal{U}_1, \mathcal{T}$, where $\mathcal{U}_1, \mathcal{T} \subset [K], |\mathcal{U}_1| \geq U, |\mathcal{T}| \leq T$.

$$\begin{aligned} \text{[Security]} \quad & I\Bigg((W_k)_{k\in[K]}; (X_k)_{k\in[K]}, \left(Y_k^{\mathcal{U}_1}\right)_{k\in\mathcal{U}_1} \Bigg| \cdots \\ & \cdots \sum_{k\in\mathcal{U}_1} W_k, (W_k, Z_k)_{k\in\mathcal{T}}\Bigg) = 0. \end{aligned} \quad (6)$$

The communication *rate* characterizes how many symbols each message contains per input symbol, and is defined as

$$R_1 \triangleq \frac{L_X}{L}, \ R_2 \triangleq \frac{L_Y}{L} \quad (7)$$

where R_1 is the first round message rate and R_2 is the second round message rate.

A rate tuple (R_1, R_2) is said to be achievable if there exists a secure aggregation scheme (i.e., a design of the correlated randomness variables $(Z_k)_{k\in[K]}$ and the messages $(X_k)_{k\in[K]}, \left(Y_k^{\mathcal{U}_1}\right)_{k\in\mathcal{U}_1}$), for which the correctness and security constraints (5), (6) are satisfied, and the first round and second round message rates are smaller than or equal to R_1 and R_2, respectively. The closure of the set of all achievable rate tuples is called the optimal rate region, denoted as $\mathcal{R}^*$.

III. Optimal Rate Region of Secure Aggregation

Theorem 1 states the main result.

Theorem 1: For the information theoretic secure aggregation problem with K users, at least U responding users, and at most T colluding users, where $1 \leq U \leq K-1, 0 \leq T \leq K-2$, the optimal rate region is

$$\mathcal{R}^* = \begin{cases} \emptyset & \text{when } U \leq T, \\ \left\{(R_1, R_2) : R_1 \geq 1, R_2 \geq \frac{1}{U-T}\right\} & \text{when } U > T. \end{cases} \quad (8)$$

We have the following observations.

1. When $U \leq T$, i.e., the minimum number of responding users is no greater than the maximum number of colluding users, the information theoretic secure aggregation problem is not feasible, i.e., it is not possible to simultaneously satisfy the correctness constraint (5) and the security constraint (6).

2. When $U > T$, the optimal communication-wise strategy is such that each user sends 1 symbol over the first round, and $1/(U-T)$ symbols over the second round, for each input symbol (i.e., to compute one symbol of the desired sum).

3. While the input length L is allowed to approach infinity in the rate definition (7), the achievable scheme only requires $L = U - T$ when the field size q satisfies $q \geq K + U$, and for any field size, it suffices to have $L = B(U-T)$, where B is any integer such that $q^B \geq K + U$.

In the following two sections, we give one example of the achievable scheme and the converse proof when $U \leq T$, respectively, to illustrate the proof ideas. Due to limited space, the remaining detailed achievability and converse proofs, are deferred to the full paper available online [21], which also includes discussions and further results on field size versus input length, integer ring versus finite field (the result of this work holds when inputs are from $\mathbb{Z}_n$), the uniformity and independence of the inputs (which is required for the converse proof, but not essential for achievability), and randomness cost (which remains an open problem in general).

IV. Achievability when $K = 3, U = 2, T = 1$

Consider $K = 3$ users, where at least $U = 2$ users will respond, and the server could collude with any $T = 1$ user.

Suppose $L = U - T = 1$, i.e., $W_k \in \mathbb{F}_q$ and $q \geq 5$. The achievable scheme is based on generic vector linear codes and is described as follows.

Randomness Assignment: Consider 7 i.i.d. uniform symbols over $\mathbb{F}_q$, denoted as $S_1, S_2, S_3,\ N_1, N_2, N_3, N_4$ and yield the following generic linear combinations of the sum of some subsets of $\{S_1, S_2, S_3\}$ and some additional noise variable N_i.

$$\begin{bmatrix} Z_1^{\{1,2,3\}} \\ Z_2^{\{1,2,3\}} \\ Z_3^{\{1,2,3\}} \end{bmatrix} \triangleq \mathbf{C}_{3\times 2} \begin{bmatrix} \sum_{i=1}^{3} S_i \\ N_4 \end{bmatrix}, \begin{bmatrix} Z_1^{\{1,2\}} \\ Z_2^{\{1,2\}} \end{bmatrix} \triangleq \mathbf{C}_{2\times 2} \begin{bmatrix} S_1 + S_2 \\ N_1 \end{bmatrix},$$
$$\begin{bmatrix} Z_1^{\{1,3\}} \\ Z_3^{\{1,3\}} \end{bmatrix} \triangleq \mathbf{C}_{2\times 2} \begin{bmatrix} S_1 + S_3 \\ N_2 \end{bmatrix}, \begin{bmatrix} Z_2^{\{2,3\}} \\ Z_3^{\{2,3\}} \end{bmatrix} \triangleq \mathbf{C}_{2\times 2} \begin{bmatrix} S_2 + S_3 \\ N_3 \end{bmatrix} \quad (9)$$

where $\mathbf{C}_{a\times b}$ denotes a Cauchy matrix of dimension $a \times b$, i.e., the element in the i-th row and j-column is set as

$$c_{ij} = \frac{1}{\alpha_i - \beta_j},\ \alpha_i, \beta_j, i \in [a], j \in [b] \text{ are distinct over } \mathbb{F}_q.$$

Note that $q \geq 5$, so distinct elements as required above exist over $\mathbb{F}_q$. Intuitively, Cauchy matrices may ensure that the independent noise variables N_i are fully mixed with the sum of S_k variables to avoid any unwanted leakage. Then we set

$$Z_k = \left(S_k, \left(Z_k^{\mathcal{U}_1} \right)_{\mathcal{U}_1 : k \in \mathcal{U}_1 \subset \{1,2,3\}, |\mathcal{U}_1| \geq 2} \right), \forall k \in \{1,2,3\}. \quad (10)$$

Message Generation: For the first round, we set

$$X_1 = W_1 + S_1,\ X_2 = W_2 + S_2,\ X_3 = W_3 + S_3, \quad (11)$$

i.e., each input is mixed with an independent noise variable. For the second round, we set

$$\forall \mathcal{U}_1 \subset \{1,2,3\}, |\mathcal{U}_1| \geq 2 :\ Y_k^{\mathcal{U}_1} = Z_k^{\mathcal{U}_1},\ \forall k \in \mathcal{U}_1, \quad (12)$$

i.e., generic linear combinations of the sum of the noise variables from first round responding users are sent to decode the desired sum. Further, additional noise variables N_i are included in the combinations to prevent leakage under collusion.

Proof of Correctness: For any $\mathcal{U}_1$ such that $|\mathcal{U}_1| \geq 2$, due to the randomness and message design (see (9) and (12)), the server can recover $\sum_{k\in\mathcal{U}_1} S_k$ from any set of second round messages where $|\mathcal{U}_2| \geq 2$. Then from $\sum_{k\in\mathcal{U}_1} X_k = \sum_{k\in\mathcal{U}_1} W_k + \sum_{k\in\mathcal{U}_1} S_k$, the server can decode the desired sum aggregation $\sum_{k\in\mathcal{U}_1} W_k$ with no error.

Proof of Security: We show that the noise variables N_i help to guarantee the security constraint (6). For example, suppose $\mathcal{U}_1 = \{1,2\}$ and the colluding user set is $\mathcal{T} = \{1\}$. Then

$$\begin{aligned} & I\Big(W_1, W_2, W_3; X_1, X_2, X_3, Y_1^{\{1,2\}}, Y_2^{\{1,2\}} \Big| \dots \\ & \quad \dots, W_1 + W_2, W_1, Z_1\Big) \\ =\ & H\left(X_1, X_2, X_3, Y_1^{\{1,2\}}, Y_2^{\{1,2\}} \middle| W_1 + W_2, W_1, Z_1\right) \\ & - H\left(X_1, X_2, X_3, Y_1^{\{1,2\}}, Y_2^{\{1,2\}} \middle| W_1, W_2, W_3, Z_1\right) \quad (13) \\ =\ & H(W_1 + S_1, W_2 + S_2, W_3 + S_3, S_1 + S_2, N_1 | W_1 + W_2, \\ & W_1, Z_1) - H(S_1, S_2, S_3, N_1 | W_1, W_2, W_3, Z_1) \quad (14) \\ \overset{(1)}{=}\ & H(S_1, W_2 + S_2, W_3 + S_3, N_1 | W_1 + W_2, W_1, Z_1) \\ & - H(S_1, S_2, S_3, N_1 | Z_1) \quad (15) \\ =\ & H(W_2 + S_2, W_3 + S_3 | W_1 + W_2, W_1, Z_1) \\ & + \underbrace{H(N_1 | W_2 + S_2, W_3 + S_3, W_1 + W_2, W_1, Z_1)}_{=0} \\ & - H(S_2, S_3 | Z_1) - \underbrace{H(N_1 | Z_1, S_2, S_3)}_{=0} \quad (16) \\ \leq\ & 2 - 2 = 0 \quad (17) \end{aligned}$$

where (16) is due to the fact that S_1 is contained in Z_1 (see (10)) and N_1 can be obtained from $Z_1^{\{1,2\}}$ (contained in Z_1), when $S_1 + S_2$ is known (obtained from Z_1, S_2, refer to (9), (10)). In the last step, the first term follows from the property that uniform random variables are entropy maximizers, and the second term is due to the independence of (S_2, S_3) and Z_1, whose proof is rather involved and is deferred to [21] (along with the security proof for other choices of $\mathcal{U}_1$ and $\mathcal{T}$).

Rate Calculation: As $L_X = L_Y = 1$ symbol, we have $R_1 = R_2 = 1$, as desired for this case.

V. Converse when $U \leq T$: Proof of $\mathcal{R}^* = \emptyset$

Let us start with a simple consequence of the independence of inputs $(W_k)_{k\in[K]}$ and $(Z_k)_{k\in[K]}$, and the uniformity of $(W_k)_{k\in[K]}$, which will be used in the converse proof.

Lemma 1: For any $V_2 < V_1 < K$, we have

$$I\left(\sum_{k\in[V_1]} W_k; \sum_{k\in[V_1+1]} W_k, (W_k, Z_k)_{k\in[V_2]}\right) = 0. \quad (18)$$

Proof of Lemma 1:

$$\begin{aligned} & I\left(\sum_{k\in[V_1]} W_k; \sum_{k\in[V_1+1]} W_k, (W_k, Z_k)_{k\in[V_2]}\right) \\ \overset{(1)}{=}\ & I\left(\sum_{k\in[V_1]} W_k; \sum_{k\in[V_1+1]} W_k, (W_k)_{k\in[V_2]}\right) \quad (19) \\ =\ & L - H\left(\sum_{k\in[V_1]} W_k \middle| \sum_{k\in[V_1+1]} W_k, (W_k)_{k\in[V_2]}\right) \quad (20) \end{aligned}$$

$$0 \overset{(6)}{=} I\left((W_k)_{k\in[K]}; (X_k)_{k\in[K]}, \left(Y_k^{[U+2]}\right)_{k\in[U+2]} \middle| \sum_{k\in[U+2]} W_k, (W_k, Z_k)_{k\in[U]}\right) \tag{23}$$

$$\geq I\left(\sum_{k\in[U+1]} W_k; (X_k)_{k\in[U+1]} \middle| \sum_{k\in[U+2]} W_k, (W_k, Z_k)_{k\in[U]}\right) \tag{24}$$

$$\overset{(4)}{=} I\left(\sum_{k\in[U+1]} W_k; (X_k)_{k\in[U+1]}, \left(Y_k^{[U+1]}\right)_{k\in[U]} \middle| \sum_{k\in[U+2]} W_k, (W_k, Z_k)_{k\in[U]}\right) \tag{25}$$

$$= I\left(\sum_{k\in[U+1]} W_k; (X_k)_{k\in[U+1]}, \left(Y_k^{[U+1]}\right)_{k\in[U]}, \sum_{k\in[U+2]} W_k, (W_k, Z_k)_{k\in[U]}\right)$$

$$- \underbrace{I\left(\sum_{k\in[U+1]} W_k; \sum_{k\in[U+2]} W_k, (W_k, Z_k)_{k\in[U]}\right)}_{=0} \tag{26}$$

$$\geq I\left(\sum_{k\in[U+1]} W_k; (X_k)_{k\in[U+1]}, \left(Y_k^{[U+1]}\right)_{k\in[U]}\right) \tag{27}$$

$$= H\left(\sum_{k\in[U+1]} W_k\right) - H\left(\sum_{k\in[U+1]} W_k \middle| (X_k)_{k\in[U+1]}, \left(Y_k^{[U+1]}\right)_{k\in[U]}\right) \tag{28}$$

$$\overset{(5)}{=} L - 0 = L \quad \Rightarrow \quad 0 \geq L \tag{29}$$

$$= L - H\left(W_{V_1+1} \middle| \sum_{k\in[V_1+1]} W_k, (W_k)_{k\in[V_2]}\right) \tag{21}$$

$$= L - \big((V_2+2)L - (V_2+1)L\big) = 0 \tag{22}$$

where in (20) and the last step, we use the uniformity of $(W_k)_{k\in[K]}$. ■

Next, we present the converse proof, where the key is to judiciously choose $\mathcal{U}_1, \mathcal{U}_2, \mathcal{T}$ to produce the desired bounds from the correctness and security constraints (5), (6).

We show that when $U \leq T$, the system constraints are self-contradictory, so they cannot be satisfied by any secure aggregation scheme, i.e., $\mathcal{R}^* = \emptyset$. To see why we have a contradiction, consider $\mathcal{U}_1 = [U+2]$ and $\mathcal{T} = [U]$. Note that $U \leq T \leq K-2$, so this choice of $\mathcal{U}_1$ and $\mathcal{T}$ is feasible.

From the security constraint (6), we have the inequalities shown at the top of this page, where in (25), we use the fact that $Y_k^{[U+1]}$ is a function of W_k, Z_k (see (4)); note that here the choice of the superscript of $Y_k^{[U+1]}$ is crucial (i.e., the first round responding user set). The second term of (26) is zero because of Lemma 1, where we set $V_1 = U+1, V_2 = U$ in (18). In (28), the first term is L because the inputs are independent and uniform so that the sum is also uniform; the second term is zero because of the correctness constraint (5), when $\mathcal{U}_1 = [U+1]$ and $\mathcal{U}_2 = [U]$. In the final step, where $0 \geq L$, we arrive at a contradiction, i.e., the constraints used in the above derivation cannot hold simultaneously. The proof of $\mathcal{R}^* = \emptyset$ is thus complete.

Remark: The intuition of the above proof is as follows. When $\mathcal{U}_1 = [U+2], \mathcal{T} = [U]$, the security constraint requires that nothing beyond $W_{U+1} + W_{U+2}$ shall be learned, given all the messages and the information from colluding users. However, such messages and colluding information can fully recover all responding messages when $\mathcal{U}_1 = [U+1], \mathcal{U}_2 = [U]$, so from the correctness constraint, $\sum_{k\in[U+1]} W_k$ can be decoded and then W_{U+1} can be obtained (given the colluding information), which violates that only $W_{U+1} + W_{U+2}$ shall be learned. The above proof formalizes this intuition.

VI. Conclusion

Motivated by robust secure aggregation in federated learning, we consider a secure sum computation problem with user dropouts and characterize the optimal communication efficiency under information theoretic security (while a number of relevant problems remain widely open, e.g., the minimum randomness consumption. Refer to the full paper [21] for related results and more discussions). This work represents a promising step towards using information and coding theory tools to understand diverse relevant challenges brought by new machine learning paradigms.

Acknowledgement

This work is supported in part by NSF grant CCF-2007108.

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] 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," *arXiv preprint arXiv:1912.04977*, 2019.

[3] 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.

[4] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical secure aggregation for federated learning on user-held data," *arXiv preprint arXiv:1611.04482*, 2016.

[5] ——, "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.

[6] J. H. Bell, K. A. Bonawitz, A. Gascón, T. Lepoint, and M. Raykova, "Secure single-server aggregation with (poly) logarithmic overhead," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, pp. 1253–1269.

[7] J. So, B. Guler, and A. S. Avestimehr, "Turbo-aggregate: Breaking the quadratic aggregation barrier in secure federated learning," *arXiv preprint arXiv:2002.04156*, 2020.

[8] S. Kadhe, N. Rajaraman, O. O. Koyluoglu, and K. Ramchandran, "Fastsecagg: Scalable secure aggregation for privacy-preserving federated learning," *arXiv preprint arXiv:2009.11248*, 2020.

[9] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation," in *Proceedings of the twentieth annual ACM symposium on Theory of computing*. ACM, 1988, pp. 1–10.

[10] D. Chaum, C. Crépeau, and I. Damgard, "Multiparty Unconditionally Secure Protocols," in *Proceedings of the twentieth annual ACM symposium on Theory of computing*. ACM, 1988, pp. 11–19.

[11] B. Chor and E. Kushilevitz, "A communication-privacy tradeoff for modular addition," *Information Processing Letters*, vol. 45, no. 4, pp. 205–210, 1993.

[12] E. Kushilevitz and A. Rosén, "A randomness-rounds tradeoff in private computation," *SIAM Journal on Discrete Mathematics*, vol. 11, no. 1, pp. 61–80, 1998.

[13] Y. Zhou, H. Sun, and S. Fu, "On the Randomness Cost of Linear Secure Computation," in *2019 53rd Annual Conference on Information Sciences and Systems (CISS)*, March 2019, pp. 1–6.

[14] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[15] H. Sun and S. A. Jafar, "The Capacity of Symmetric Private Information Retrieval," *IEEE Transactions on Information Theory*, vol. 65, no. 1, pp. 322–329, 2019.

[16] Z. Jia, H. Sun, and S. A. Jafar, "Cross Subspace Alignment and the Asymptotic Capacity of X–Secure T–Private Information Retrieval," *IEEE Transactions on Information Theory*, vol. 65, no. 9, pp. 5783–5798, 2019.

[17] T. Guo, R. Zhou, and C. Tian, "On the information leakage in private information retrieval systems," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2999–3012, 2020.

[18] J. Cheng, N. Liu, and W. Kang, "The capacity of symmetric private information retrieval under arbitrary collusion and eavesdropping patterns," *arXiv preprint arXiv:2010.08249*, 2020.

[19] Q. Wang, H. Sun, and M. Skoglund, "The ϵ-Error Capacity of Symmetric PIR with Byzantine Adversaries," in *2018 IEEE Information Theory Workshop (ITW)*. IEEE, 2018, pp. 1–5.

[20] ——, "Symmetric Private Information Retrieval with Mismatched Coded Messages and Randomness," in *2019 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2019, pp. 365–369.

[21] Y. Zhao and H. Sun, "Information Theoretic Secure Aggregation with User Dropouts," *arXiv preprint arXiv:2101.07750*, 2021.

[22] K. Bonawitz, F. Salehi, J. Konečnỳ, B. McMahan, and M. Gruteser, "Federated learning with autotuned communication-efficient secure aggregation," in *2019 53rd Asilomar Conference on Signals, Systems, and Computers*. IEEE, 2019, pp. 1222–1226.

[23] B. Choi, J. yong Sohn, D.-J. Han, and J. Moon, "Communication-Computation Efficient Secure Aggregation for Federated Learning," *arXiv preprint arXiv:2012.05433*, 2020.

[24] K. Pillutla, S. M. Kakade, and Z. Harchaoui, "Robust aggregation for federated learning," *arXiv preprint arXiv:1912.13445*, 2019.

[25] R. Xu, N. Baracaldo, Y. Zhou, A. Anwar, and H. Ludwig, "Hybridalpha: An efficient approach for privacy-preserving federated learning," in *Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security*, 2019, pp. 13–23.

[26] C. Beguier and E. W. Tramel, "Safer: Sparse secure aggregation for federated learning," *arXiv preprint arXiv:2007.14861*, 2020.

[27] J. So, B. Guler, and A. S. Avestimehr, "Byzantine-resilient secure federated learning," *arXiv preprint arXiv:2007.11115*, 2020.

[28] A. R. Elkordy and A. S. Avestimehr, "Secure aggregation with heterogeneous quantization in federated learning," *arXiv preprint arXiv:2009.14388*, 2020.

[29] J. Guo, Z. Liu, K.-Y. Lam, J. Zhao, Y. Chen, and C. Xing, "Secure weighted aggregation in federated learning," *arXiv preprint arXiv:2010.08730*, 2020.

[30] A. B. Alexandru and G. J. Pappas, "Private weighted sum aggregation," *arXiv preprint arXiv:2010.10640*, 2020.

[31] D. Lia and M. Togan, "Privacy-preserving machine learning using federated learning and secure aggregation," in *2020 12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*. IEEE, 2020, pp. 1–6.

[32] N. Truong, K. Sun, S. Wang, F. Guitton, and Y. Guo, "Privacy preservation in federated learning: Insights from the gdpr perspective," *arXiv preprint arXiv:2011.05411*, 2020.