This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

The Capacity Region of Information Theoretic Secure Aggregation with Uncoded Groupwise Keys

Kai Wan, *Member, IEEE,* Hua Sun, *Member, IEEE,* Mingyue Ji, *Member, IEEE,* Tiebin Mi, *Member, IEEE,* and Giuseppe Caire, *Fellow, IEEE*

***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 curious-but-honest 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, in the second round, according to the identity of surviving users after the first round, these surviving users 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, assuming that key sharing has already been performed offline in prior. In this context, Zhao and Sun completely characterized the capacity region under the assumption that the keys can be arbitrary random variables. More recently, an additional constraint, known as "uncoded groupwise keys," has been introduced. This constraint entails the presence of multiple independent keys within the system, with each key being shared by precisely S users, where S is a defined system parameter. The capacity region for the information theoretic secure aggregation problem with uncoded groupwise keys was established in our recent work subject to the condition $\mathsf{S} > \mathsf{K} - \mathsf{U}$, where K is the number of total users and U is the designed minimum number of surviving users (which is another system parameter). In this paper we fully characterize the capacity region for this problem by matching a new converse bound and an achievable scheme. Experimental results over the Tencent Cloud show the improvement on the model aggregation time compared to the original secure aggregation scheme.**

***Index Terms*—Secure aggregation, federated learning, uncoded groupwise keys, information theoretic security**

A short version of this paper was accepted by the 2024 IEEE International Symposium on Information Theory.

K. Wan and T. Mi are with the School of Electronic Information and Communications, Huazhong University of Science and Technology, 430074 Wuhan, China, (e-mail: {kai_wan,mitiebin}@hust.edu.cn). The work of K. Wan and T. Mi was partially funded by the National Natural Science Foundation of China (NSFC-12141107).

M. Ji is with the Electrical and Computer Engineering Department, University of Utah, Salt Lake City, UT 84112, USA (e-mail: mingyue.ji@utah.edu). The work of M. Ji was partially funded by National Science Foundation (NSF) Award 2312227 and CAREER Award 2145835.

H. Sun is with the Department of Electrical Engineering, University of North Texas, Denton, TX 76203, USA (email: hua.sun@unt.edu). The work of H. Sun was supported in part by NSF under Grant CCF-2007108, Grant CCF-2045656, and Grant CCF-2312228.

G. Caire is with the Electrical Engineering and Computer Science Department, Technische Universität Berlin, 10587 Berlin, Germany (e-mail: caire@tu-berlin.de). The work of G. Caire was partially funded by the European Research Council under the ERC Advanced Grant N. 789190, CARENET.

I. Introduction

A. Background on secure aggregation for federated learning

Federated learning is a decentralized machine learning approach that enables multiple devices or users (such as smartphones, edge devices, or Internet of Things devices) to collaboratively train a global model without sharing their local raw data to the central server [1]–[4]. Rather than centralizing all data in a single location, federated learning allows each device training by using its own local data. After initialization, the process of federated learning involves several iterations among the users and the server. In one iteration, each user trains the model using its own local data without sharing it with the central server. 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. Federated learning has two main advantages over traditional centralized and distributed learning: (i) it reduces communication costs and eliminates the need for frequent data transfers; (ii) it preserves data privacy against the server by keeping data local. Despite these advantages, federated learning also suffers from some challenges. On the one hand, assume that the training devices/users are smartphones or edge devices; during the training process of federated learning, the server may lose the connectivity to some users due to user mobility and fluctuating communication quality. Thus an efficient federated learning scenario should be resilient to this unpredictable effect of user dropouts. On the other hand, each user needs to transmit to the server the computed model in terms of the local data; thus the information of local data can be leaked at some level to the server, and this is known as the model inversion attacks in federated learning [5].

To deal with the effect of user dropouts and strengthen local data privacy in federated learning, a new cryptographic problem, referred to as secure aggregation, was originally introduced in [6]. 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,

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

it is called online. Model aggregation follows key sharing, where the users compute, mask, and send their updated models to the server. For the resilience to user dropouts, multi-round communications among the users and server could be used, where in the first round the users send masked updated models and in the remaining rounds the users send some messages composed of keys. The number of rounds depend on the threat models of the server (e.g., the server may be honest-but-curious, or be malicious and lie about the identity of the dropping users, or even collude with some users). The secure aggregation protocol in [6] uses pairwise offline key sharing with Diffie-Hellman key agreement [7] between each two users, where each key is then shared with all other users through Shamir's secret sharing [8] to deal with user dropouts.

Since the original secure aggregation work in [6], intensive efforts have been put forth, introducing more efficient secure aggregation schemes. For example, these include the schemes utilizing common seeds via a homomorphic pseudorandom generator [9], secure multi-party computing [10], non-pairwise keys [11], online key sharing [12]–[14], and improved El Gamal encryption [15]. For further details, readers are encouraged to consult the surveys in [16], [17].

B. Information theoretic secure aggregation

In this paper, we follow the (K,U) information theoretic formulation on secure aggregation with user dropouts and offline key sharing proposed in [11], 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, which contains L uniform and i.i.d. symbols over a finite field.[1] In this model, we aim to determine the optimal transmission in the model aggregation phase with the assumption that enough keys have been shared among the users in a prior key sharing phase, such that the information theoretic security of the users' local data is protected against the server (except the sum of the updated models of the non-dropped users).[2] 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 [11] that to preserve the security of users' local data against the honest-but-curious server with the existence of user dropouts, two-round transmissions 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 according to 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. The objective of this information theoretic 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 normalized by L for $i\in\{1,2\}$. 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 [11] with an achievability strategy based on Minimum Distance Separable (MDS) codes in the key generation and one-time pad coding in the model aggregation. Another secure aggregation scheme which can also achieve capacity was proposed in [19], based on a pairwise coded key generation. Compared to [11], the scheme in [19] significantly reduces the size of keys stored by each user.

There are some other extended information theoretic formulations on secure aggregation in federated learning, following the model in [11]. A weaker information theoretic security constraint compared to the one in [11] was considered in [20], where we only need to preserve the security on a subset of users' input vectors. User collusion was also considered in [11], where the server may collude with up to $\mathsf{T}<\mathsf{U}$ users; to deal with potential user collusion, the capacity region reduces to $\{(\mathsf{R}_1,\mathsf{R}_2):\mathsf{R}_1\geq 1,\mathsf{R}_2\geq 1/(\mathsf{U}-\mathsf{T})\}$, characterized in [11].[3] Information theoretic secure aggregation with cluster federated learning was originally considered in [22], to aggregate the updated models from multiple clusters of users simultaneously, without learning any information about the cluster identities or users' local data.

Recently a modified version of the above problem, referred to as $(\mathsf{K},\mathsf{U},\mathsf{S})$ information theoretic secure aggregation problem with uncoded groupwise keys, was proposed in [23] as illusrated in Fig. 1. An additional constraint on the keys was considered, where the key sharing among the users is "uncoded" and "groupwise". More precisely, 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 distinct users and is also independent of the input vectors.[4] The constraint of uncoded groupwise keys is motivated by the fact that, the uncoded groupwise keys could be directly generated and shared among users by some key agreement protocol such as [24]–[31] 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. An interesting question arises for the $(\mathsf{K},\mathsf{U},\mathsf{S})$ information theoretic secure aggregation with uncoded groupwise keys: does the capacity region remain the same as the secure aggregation problem in [11]? When $\mathsf{S}>\mathsf{K}-\mathsf{U}$, a secure aggregation scheme with groupwise keys was proposed in [23] which achieves the same capacity

[1] Note that the system is designed to tolerate up to $\mathsf{K}-\mathsf{U}$ user dropouts. If more than $\mathsf{K}-\mathsf{U}$ users drop, there is insufficient data for update and the server does not update the model and will ask for a retransmission. In this paper, we directly assume that there are at most $\mathsf{K}-\mathsf{U}$ user dropouts.

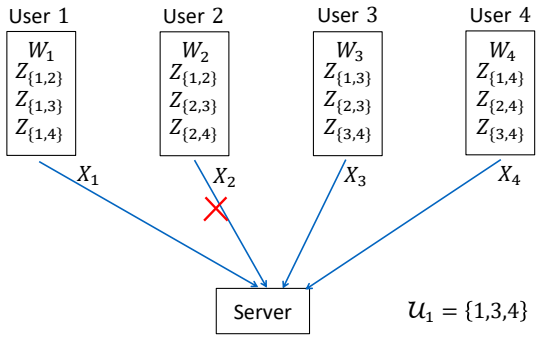
[2] Information theoretic security was proposed in the seminal work by Shannon [18], under which constraint even if the adversary has infinite computation power it still cannot get any information about the data. In the literature of secure aggregation with user dropouts, the secure aggregation schemes proposed in [11], [14], [19] guarantee the information theoretic security constraint.

[3] In this paper we do not consider user collusion; thus we set $\mathsf{T}=0$ in this paper. Secure aggregation with uncoded groupwise keys against user collusion (i.e., $\mathsf{T}>0$) was considered in another paper of ours [21] and characterizing the capacity region is an ongoing work.

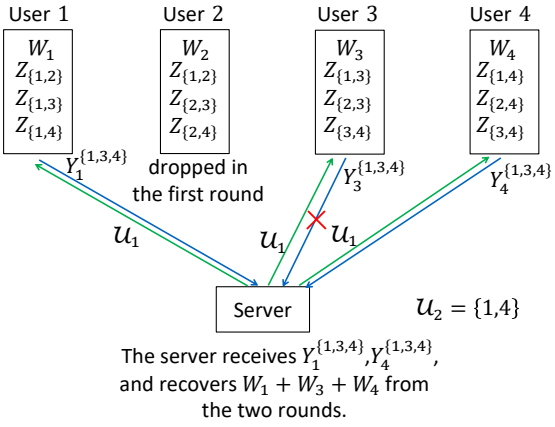
[4] In contrast, coded pairwise keys were used in [6], [19] where the keys shared by the users are not mutually independent.

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740



(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.

region $\{(\mathsf{R}_1, \mathsf{R}_2) : \mathsf{R}_1 \geq 1, \mathsf{R}_2 \geq 1/\mathsf{U}\}$ as in [11]. Hence, in this case, 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 [23] showing that the capacity region in [11] is not achievable. However, the capacity region for the case $\mathsf{S} \leq \mathsf{K} - \mathsf{U}$ still remains open.

C. Main Contribution

The main contribution of this paper is to characterize the capacity region on the rate tuples for the $(\mathsf{K}, \mathsf{U}, \mathsf{S})$ information theoretic secure aggregation problem 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 first derive a new converse bound on the rate of the first round R_1, which is strictly tighter than the converse bound in [23].
- We propose a new secure aggregation scheme based on the interference alignment strategy, which achieves the converse bound. The main difference between the proposed scheme and the secure aggregation scheme in [23] (which works for the case $\mathsf{S} > \mathsf{K} - \mathsf{U}$) is that, when $\mathsf{S} \leq \mathsf{K} - \mathsf{U}$ the optimal rate in the first round R_1 is strictly larger than 1, and in addition to the masked input vector, each user should also transmit some additional messages composed of the keys. Hence, when a whole group of users sharing the same key drops in the second phase, the server can leverage these additional messages transmitted in the first round to decrypt.
- 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 [6].

D. Paper Organization

The rest of this paper is organized as follows. Section II reviews the information theoretic secure aggregation problem with uncoded groupwise keys. Section III introduces the main theorem of the paper, which characterizes the capacity region. Sections IV and V present the converse and achievability proofs of the main theorem, respectively. Section VII concludes the paper, while some proofs are given in the Appendices.

E. Notation Convention

Calligraphic symbols denote sets, bold symbols denote vectors and matrices, and sans-serif symbols denote system parameters. We use $|\cdot|$ to represent the cardinality of a set or the length of a vector; $[a : b] := \{a, a+1, \ldots, b\}$ 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; $\mathbf{A}^{\mathrm{T}}$ and $\mathbf{A}^{-1}$ represent the transpose and the inverse of matrix $\mathbf{A}$, respectively; $\mathrm{rank}(\mathbf{A})$ represents the rank of matrix $\mathbf{A}$; $\mathbf{I}_n$ represents the identity matrix of dimension $n \times n$; $0_{m,n}$ represents all-zero matrix of dimension $m \times n$; $1_{m,n}$ represents all-one matrix of dimension $m \times n$; $(\mathbf{A})_{m\times n}$ explicitly indicates that the matrix $\mathbf{A}$ is of dimension $m \times n$; $< \cdot >_a$ represents the modulo operation with integer quotient $a > 0$ and in this paper we let $< \cdot >_a \in \{1, \ldots, a\}$ (i.e., we let $< b >_a = a$ if a divides b); let $\binom{x}{y} = 0$ if $x < 0$ or $y < 0$ or $x < y$; let $\binom{\mathcal{X}}{y} = \{\mathcal{S} \subseteq \mathcal{X} : |\mathcal{S}| = y\}$ where $|\mathcal{X}| \geq y > 0$. In this paper, for a set of real numbers $\mathcal{S}$, we sort the elements in $\mathcal{S}$ in an increasing order and denote the i^{th} smallest element by $\mathcal{S}(i)$, i.e., $\mathcal{S}(1) < \ldots < \mathcal{S}(|\mathcal{S}|)$. In the rest of the paper, entropies will be in base q, where q represents the field size.

II. System Model

We consider the $(\mathsf{K}, \mathsf{U}, \mathsf{S})$ information theoretic secure aggregation problem with uncoded groupwise keys originally formulated in [23], 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

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

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, i.e.,

$$H\left(\left(Z_{\mathcal{V}} : \mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}\right), (W_1, \ldots, W_{\mathsf{K}})\right) = \sum_{\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}} H(Z_{\mathcal{V}}) + \sum_{k \in [\mathsf{K}]} H(W_k). \tag{1}$$

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.[5] The server aims to aggregate 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 [11] that one transmission round in the model aggregation is not enough. Thus we consider the two-round model aggregation as in [11], [23].

First round. In the 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, i.e,

$$H(X_k | W_k, Z_k) = 0, \quad \text{(Encodability for the first round)}. \tag{2}$$

The transmission rate of the first round R_1 is defined as the largest transmission load among all users normalized by L, i.e.,

$$\mathsf{R}_1 := \max_{k \in [\mathsf{K}]} \frac{H(X_k)}{\mathsf{L}}. \tag{3}$$

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. In the 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, where

$$H(Y_k^{\mathcal{U}_1} | W_k, Z_k, \mathcal{U}_1) = 0, \quad \text{(Encodability for the second round)}. \tag{4}$$

The transmission rate of the second round R_2 is defined as the largest transmission load among all $\mathcal{U}_1$ and all users in $\mathcal{U}_1$ normalized by L, i.e.,

$$\mathsf{R}_2 := \max_{\mathcal{U}_1 \subseteq [\mathsf{K}] : |\mathcal{U}_1| \geq \mathsf{U}} \max_{k \in \mathcal{U}_1} \frac{H\left(Y_k^{\mathcal{U}_1}\right)}{\mathsf{L}}. \tag{5}$$

[5]In this context, the nature of these links is irrelevant. Federated learning is a distributed process running at the application layer, i.e., on top of some possibly heterogeneous networks with possibly different lower protocol layers. In any case, at the application layer, it is reasonable and practical to assume that the server and the users establish end-to-end communication sessions using TCP/IP. In fact, in most practical applications federated learning runs over geographically widely separated users (imagine to run such application on the local picture library of smartphones all over the world).

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

$$H\left(\sum_{k \in \mathcal{U}_1} W_k \Big| (X_{k_1} : k_1 \in \mathcal{U}_1), (Y_{k_2}^{\mathcal{U}_1} : k_2 \in \mathcal{U}_2)\right) = 0, \quad \forall \mathcal{U}_1 \subseteq [\mathsf{K}], \mathcal{U}_2 \subseteq \mathcal{U}_1 : |\mathcal{U}_1| \geq |\mathcal{U}_2| \geq \mathsf{U}, \text{(Decodability)}. \tag{6}$$

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, i.e.,

$$I\left(W_1, \ldots, W_{\mathsf{K}}; X_1, \ldots, X_{\mathsf{K}}, (Y_k^{\mathcal{U}_1} : k \in \mathcal{U}_1) \Big| \sum_{k \in \mathcal{U}_1} W_k\right) = 0, \quad \forall \mathcal{U}_1 \subseteq [\mathsf{K}] : |\mathcal{U}_1| \geq \mathsf{U}, \text{(Security)}. \tag{7}$$

It is worth noticing that this mutual information is strictly equal to 0; that is, we consider zero leakage, instead of vanishing leakage as $\mathsf{L} \to \infty$.

Objective. A rate tuple $(\mathsf{R}_1, \mathsf{R}_2)$ is achievable if there exist keys $\left(Z_{\mathcal{V}} : \mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}\right)$ satisfying (1) and a secure aggregation scheme satisfying the decodability and security constraints in (6) and (7), respectively. Our objective is to determine the capacity region (i.e., the closure of all achievable rate tuples), denoted by $\mathcal{R}^\star$.

Existing converse bounds. By removing the uncoded groupwise constraint on the keys from our problem, we obtain the information theoretic aggregation problem in [11]. Hence, the converse bound on the capacity region in [11] is also a converse bound for our problem.

Theorem 1 ([11]). *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*

$$\mathsf{R}_1 \geq 1, \ \mathsf{R}_2 \geq \frac{1}{\mathsf{U}}. \tag{8}$$

□

Considering the uncoded groupwise constraint, an improved converse bound was given in [23] for the case $\mathsf{S} \leq \mathsf{K} - \mathsf{U}$.

Theorem 2 ([23]). *For the* $(\mathsf{K}, \mathsf{U}, \mathsf{S})$ *information theoretic secure aggregation problem with uncoded groupwise keys, when* $1 = \mathsf{S} \leq \mathsf{K} - \mathsf{U}$*, secure aggregation is not possible; when* $2 \leq \mathsf{S} \leq \mathsf{K} - \mathsf{U}$*, any achievable rate tuple* $(\mathsf{R}_1, \mathsf{R}_2)$

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

satisfies

$$\mathsf{R}_1 \geq \frac{\binom{\mathsf{K}-1}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-1}, \mathsf{R}_2 \geq \frac{1}{\mathsf{U}}. \tag{9}$$

□

Existing achievable bound. A secure aggregation scheme with uncoded groupwise keys was proposed in [23] for the case $\mathsf{S} > \mathsf{K}-\mathsf{U}$, achieving the following rates.

Theorem 3 ([23])**.** *For the* $(\mathsf{K},\mathsf{U},\mathsf{S})$ *information theoretic secure aggregation problem with uncoded groupwise keys, when* $\mathsf{S} > \mathsf{K}-\mathsf{U}$*, the following rate tuples are achievable,*

$$\mathsf{R}_1 \geq 1, \mathsf{R}_2 \geq \frac{1}{\mathsf{U}}. \tag{10}$$

□

Comparing the achievable bound in Theorem 3 with the converse bound in Theorem 1, we can characterize the capacity region for the case $\mathsf{S} > \mathsf{K}-\mathsf{U}$, which is

$$\mathcal{R}^\star = \left\{(\mathsf{R}_1,\mathsf{R}_2) : \mathsf{R}_1 \geq 1, \mathsf{R}_2 \geq \frac{1}{\mathsf{U}}\right\}. \tag{11}$$

However, no achievable scheme has been provided in the literature 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 main contribution of this paper is to fully characterize the capacity region for the information theoretic secure aggregation problem with uncoded groupwise keys. This is stated in the following theorem.

Theorem 4. *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*

$$\mathcal{R}^\star = \left\{(\mathsf{R}_1,\mathsf{R}_2) : \mathsf{R}_1 \geq \frac{\binom{\mathsf{K}-1}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}, \mathsf{R}_2 \geq \frac{1}{\mathsf{U}}\right\}. \tag{12}$$

□

The converse proof of Theorem 4 is given in Section IV and the achievability proof is given in Section V. The following remarks on Theorem 4 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 (12) reduces to the one in (11), which is also equal to the capacity region for the information theoretic secure aggregation problem in [11] (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 [11] is only at the first round and is equal to $\frac{\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}$.
- Comparing the proposed converse bound in (12) with the existing converse bound in (9), we can see that the two bounds differ in the first-round transmission rate R_1 and that $\frac{\binom{\mathsf{K}-1}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}} \geq \frac{\binom{\mathsf{K}-1}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-1}$. Hence, the existing converse bound in (9) is strictly loose when $\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1} > 1$ (i.e., when $\mathsf{K} > \mathsf{U}+\mathsf{S}$).
- The secure aggregation scheme proposed in Section V is a new and unified scheme working for all system parameters when $\mathsf{S} > 1$. In constrast, in [23] only the regime $\mathsf{S} > \mathsf{K}-\mathsf{U}$ was considered, where this regime was first divided into three cases and a different secure aggregation scheme was proposed for each case.
- The scheme in Section V uses all the $\binom{\mathsf{K}}{\mathsf{S}}$ keys in the system , where each key contains $\frac{\mathsf{SL}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}$ symbols. In comparison, the secure aggregation in [23] uses at most $\mathcal{O}(\mathsf{K}^2)$ keys, where each key has $\frac{(\mathsf{K}-\mathsf{U}+1)\mathsf{L}}{\mathsf{U}}$ symbols.

IV. Converse Proof of Theorem 4

Since the converse bound for the information theoretic aggregation problem in [11] is also a converse bound for our considered problem, by Theorem 1 we can directly obtain $\mathsf{R}_2 \geq \frac{1}{\mathsf{U}}$. Hence, for Theorem 4 we only need to prove

$$\mathsf{R}_1 \geq \frac{\binom{\mathsf{K}-1}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}, \tag{13}$$

for the case $\mathsf{S} \geq 2$.

Let us focus on user 1 and derive the lower bound of $\frac{H(X_1)}{\mathsf{L}}$. For each set $\mathcal{U} \in \binom{[2:\mathsf{K}]}{\mathsf{U}}$, letting $\mathcal{U}_1 = \{1\} \cup \mathcal{U}$ and $\mathcal{U}_2 = \mathcal{U}$, by the decodability constraint (6) the server can recover $\sum_{i\in\{1\}\cup\mathcal{U}} W_i$ from $(X_k : k \in \{1\}\cup\mathcal{U})$ and $\left(Y_k^{\mathcal{U}_1} : k \in \mathcal{U}\right)$. In addition, for each $k \in \mathcal{U}$, $\left(X_k, Y_k^{\mathcal{U}_1}\right)$ is a function of (Z_k, W_k). Hence, the server can recover $\sum_{i\in\{1\}\cup\mathcal{U}} W_i$ from $(X_1, (Z_k, W_k : k \in \mathcal{U}))$; thus

$$0 = H\left(\sum_{i\in\{1\}\cup\mathcal{U}} W_i \middle| X_1, (Z_k, W_k : k \in \mathcal{U})\right) \tag{14a}$$

$$= H\left(W_1 | X_1, (Z_k, W_k : k \in \mathcal{U})\right) \tag{14b}$$

$$= H\left(W_1 \middle| X_1, \left(Z_{\mathcal{V}} : \mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}, 1 \in \mathcal{V}, \mathcal{U}\cap\mathcal{V} \neq \emptyset\right)\right) \tag{14c}$$

$$= H\left(W_1 \middle| \left(Z_{\mathcal{V}} : \mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}, 1 \in \mathcal{V}, \mathcal{U}\cap\mathcal{V} \neq \emptyset\right)\right) - I\left(X_1; W_1 \middle| \left(Z_{\mathcal{V}} : \mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}, 1 \in \mathcal{V}, \mathcal{U}\cap\mathcal{V} \neq \emptyset\right)\right), \tag{14d}$$

where (14c) comes from (1) and (2). In addition, from (14d) we have

$$I\left(X_1; W_1 \middle| \left(Z_{\mathcal{V}} : \mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}, 1 \in \mathcal{V}, \mathcal{U}\cap\mathcal{V} \neq \emptyset\right)\right)$$

$$= H\left(W_1 \middle| \left(Z_{\mathcal{V}} : \mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}, 1 \in \mathcal{V}, \mathcal{U}\cap\mathcal{V} \neq \emptyset\right)\right) \tag{15a}$$

$$= H(W_1) = \mathsf{L}, \tag{15b}$$

where (15b) follows since W_1 is independent of the keys.

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

By the security constraint (7), we have

$$0 = I\left(W_1,\dots,W_{\mathsf{K}};X_1,\dots,X_{\mathsf{K}},(Y_k^{\mathcal{U}_1}:k\in\mathcal{U}_1)\Big|\sum_{k\in\mathcal{U}_1}W_k\right) \tag{16a}$$

$$\geq I\left(W_1;X_1\Big|\sum_{k\in\mathcal{U}_1}W_k\right) \tag{16b}$$

$$= I\left(W_1;\sum_{k\in\mathcal{U}_1}W_k,X_1\right) - I\left(W_1;\sum_{k\in\mathcal{U}_1}W_k\right) \tag{16c}$$

$$= I\left(W_1;\sum_{k\in\mathcal{U}_1}W_k,X_1\right) \tag{16d}$$

$$\geq I\left(W_1;X_1\right) \tag{16e}$$

$$\iff I\left(W_1;X_1\right)=0, \tag{16f}$$

where (16d) follows since, the elements in $W_1,\dots,W_{\mathsf{K}}$ are i.i.d. over $\mathbb{F}_{\mathsf{q}}$ and thus we can see that W_1 is independent of $\sum_{k\in\mathcal{U}_1}W_k=\sum_{k\in\{1\}\cup\mathcal{U}}W_k$ (recall that $|\mathcal{U}|=\mathsf{U}\geq 1$).

In addition, we have

$$I\left(X_1;\left(Z_{\mathcal{V}}:\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}},1\in\mathcal{V},\mathcal{U}\cap\mathcal{V}\neq\emptyset\right)\Big|W_1\right)$$
$$= I\left(X_1;W_1,\left(Z_{\mathcal{V}}:\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}},1\in\mathcal{V},\mathcal{U}\cap\mathcal{V}\neq\emptyset\right)\right) - I(X_1;W_1) \tag{17a}$$

$$= I\left(X_1;W_1,\left(Z_{\mathcal{V}}:\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}},1\in\mathcal{V},\mathcal{U}\cap\mathcal{V}\neq\emptyset\right)\right) \tag{17b}$$

$$\geq I\left(X_1;W_1\Big|\left(Z_{\mathcal{V}}:\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}},1\in\mathcal{V},\mathcal{U}\cap\mathcal{V}\neq\emptyset\right)\right) \tag{17c}$$

$$= \mathsf{L}, \tag{17d}$$

where (17b) comes from (16f) and (17d) comes from (15b).

We sort the sets $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$ where $1\in\mathcal{V}$ in the lexicographic order, denoted by $\mathcal{S}_{1,1},\dots,\mathcal{S}_{1,\binom{\mathsf{K}-1}{\mathsf{S}-1}}$. Then by the chain rule of mutual information, we have

$$\mathsf{R}_1\mathsf{L}\geq H(X_1) \tag{18a}$$

$$\geq I\left(X_1;Z_{\mathcal{S}_{1,1}},\dots,Z_{\mathcal{S}_{1,\binom{\mathsf{K}-1}{\mathsf{S}-1}}}|W_1\right) \tag{18b}$$

$$= \sum_{i\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}\right]} I(X_1;Z_{\mathcal{S}_{1,i}}|W_1,Z_{\mathcal{S}_{1,1}},\dots,Z_{\mathcal{S}_{1,i-1}}) \tag{18c}$$

$$= \left(\binom{\mathsf{K}-1}{\mathsf{U}}-\binom{\mathsf{K}-\mathsf{S}}{\mathsf{U}}\right) \sum_{i\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}\right]} \frac{1}{\binom{\mathsf{K}-1}{\mathsf{U}}-\binom{\mathsf{K}-\mathsf{S}}{\mathsf{U}}} I(X_1;Z_{\mathcal{S}_{1,i}}|W_1,Z_{\mathcal{S}_{1,1}},\dots,Z_{\mathcal{S}_{1,i-1}}) \tag{18d}$$

$$= \sum_{\mathcal{U}\in\binom{[2:\mathsf{K}]}{\mathsf{U}}} \sum_{i\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}\right]:\mathcal{U}\cap\mathcal{S}_{1,i}\neq\emptyset} \frac{1}{\binom{\mathsf{K}-1}{\mathsf{U}}-\binom{\mathsf{K}-\mathsf{S}}{\mathsf{U}}} I(X_1;Z_{\mathcal{S}_{1,i}}|W_1,Z_{\mathcal{S}_{1,1}},\dots,Z_{\mathcal{S}_{1,i-1}}), \tag{18e}$$

where (18e) follows since for each $i\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}\right]$, there are exactly $\binom{\mathsf{K}-1}{\mathsf{U}}-\binom{\mathsf{K}-\mathsf{S}}{\mathsf{U}}$ sets in $\binom{[2:\mathsf{K}]}{\mathsf{U}}$, each of which intersects $\mathcal{S}_{1,i}$.

From (18e), we have (19) at the top of the next page, where (19c) follows since the uncoded keys and input vectors are independent, (19e) comes from the chain rule of mutual information, and (19f) comes from (17d).

Thus we have

$$\mathsf{R}_1 \geq \frac{\binom{\mathsf{K}-1}{\mathsf{U}}}{\binom{\mathsf{K}-1}{\mathsf{U}}-\binom{\mathsf{K}-\mathsf{S}}{\mathsf{U}}} \tag{20a}$$

$$= \frac{\binom{\mathsf{K}-1}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}, \tag{20b}$$

where (20b) follows since

$$\binom{\mathsf{K}-1}{\mathsf{U}}\binom{(\mathsf{K}-1)-\mathsf{U}}{\mathsf{S}-1} = \binom{\mathsf{K}-1}{\mathsf{S}-1}\binom{(\mathsf{K}-1)-(\mathsf{S}-1)}{\mathsf{U}} \tag{21a}$$

$$= \binom{\mathsf{K}-\mathsf{S}}{\mathsf{U}}\binom{\mathsf{K}-1}{\mathsf{S}-1}. \tag{21b}$$

From (21b), we have

$$\binom{\mathsf{K}-1}{\mathsf{U}}\left(\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}\right) = \binom{\mathsf{K}-1}{\mathsf{S}-1}\left(\binom{\mathsf{K}-1}{\mathsf{U}}-\binom{\mathsf{K}-\mathsf{S}}{\mathsf{U}}\right). \tag{22}$$

Hence, we proved (13) and thus proved the converse bound in Theorem (4).

V. Achievability Proof of Theorem 4

In this section, we describe the proposed secure aggregation scheme achieving the rate region in Theorem 4. For the ease of understanding, while providing the general description of the proposed scheme, we also introduce a running example to illustrate our construction. Note that to design achievable schemes, as explained in [11], by field extension we can assume that q is large enough without loss of generality.

First round. To achieve $\mathsf{R}_1=\frac{\binom{\mathsf{K}-1}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}$ coinciding with the converse bound in Section IV, in the first round we divide each input vector W_i where $i\in[\mathsf{K}]$ into $\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}$ non-overlapping and equal-length pieces, $W_i=\left(W_{i,j}:j\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}\right]\right)$. Hence, each piece contains $\frac{\mathsf{L}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}$ symbols. In addition, for each $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$ we generate a key $Z_{\mathcal{V}}$ with $\frac{\mathsf{SL}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}$ symbols uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}$, shared by the users in $\mathcal{V}$. We further divide each key $Z_{\mathcal{V}}$ into S non-overlapping and equal-length sub-keys, $Z_{\mathcal{V}}=(Z_{\mathcal{V},k}:k\in\mathcal{V})$, where each sub-key $Z_{\mathcal{V},k}$ contains $\frac{\mathsf{L}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}$ symbols uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}$.

Note that, by the converse bound in Theorem (4), each user $k\in[\mathsf{K}]$ transmits $\binom{\mathsf{K}-1}{\mathsf{S}-1}$ linear combinations of pieces and keys in the first round, while W_k only contains $\binom{\mathsf{K}-1}{\mathsf{S}-1}-$

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

$$\mathsf{R}_1\mathsf{L} \geq \frac{1}{\binom{\mathsf{K}-1}{\mathsf{U}}-\binom{\mathsf{K}-\mathsf{S}}{\mathsf{U}}} \sum_{\mathcal{U}\in\binom{[2:\mathsf{K}]}{\mathsf{U}}} \sum_{i\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}\right]:\mathcal{U}\cap\mathcal{S}_{1,i}\neq\emptyset} I(X_1; Z_{\mathcal{S}_{1,i}}|W_1, Z_{\mathcal{S}_{1,1}}, \ldots, Z_{\mathcal{S}_{1,i-1}}) \tag{19a}$$

$$= \frac{1}{\binom{\mathsf{K}-1}{\mathsf{U}}-\binom{\mathsf{K}-\mathsf{S}}{\mathsf{U}}} \sum_{\mathcal{U}\in\binom{[2:\mathsf{K}]}{\mathsf{U}}} \sum_{i\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}\right]:\mathcal{U}\cap\mathcal{S}_1(i)\neq\emptyset}$$
$$\Big(I(X_1, (Z_{\mathcal{S}_{1,j}} : j\in[i-1], \mathcal{U}\cap\mathcal{S}_{1,j}=\emptyset); Z_{\mathcal{S}_{1,i}}|W_1, (Z_{\mathcal{S}_{1,j}} : j\in[i-1], \mathcal{U}\cap\mathcal{S}_{1,j}\neq\emptyset))$$
$$- I((Z_{\mathcal{S}_{1,j}} : j\in[i-1], \mathcal{U}\cap\mathcal{S}_{1,j}=\emptyset); Z_{\mathcal{S}_{1,i}}|W_1, (Z_{\mathcal{S}_{1,j}} : j\in[i-1], \mathcal{U}\cap\mathcal{S}_{1,j}\neq\emptyset))\Big) \tag{19b}$$

$$= \frac{1}{\binom{\mathsf{K}-1}{\mathsf{U}}-\binom{\mathsf{K}-\mathsf{S}}{\mathsf{U}}} \sum_{\mathcal{U}\in\binom{[2:\mathsf{K}]}{\mathsf{U}}} \sum_{i\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}\right]:\mathcal{U}\cap\mathcal{S}_{1,i}\neq\emptyset}$$
$$I(X_1, (Z_{\mathcal{S}_{1,j}} : j\in[i-1], \mathcal{U}\cap\mathcal{S}_{1,j}=\emptyset); Z_{\mathcal{S}_{1,i}}|W_1, (Z_{\mathcal{S}_{1,j}} : j\in[i-1], \mathcal{U}\cap\mathcal{S}_{1,j}\neq\emptyset)) \tag{19c}$$

$$\geq \frac{1}{\binom{\mathsf{K}-1}{\mathsf{U}}-\binom{\mathsf{K}-\mathsf{S}}{\mathsf{U}}} \sum_{\mathcal{U}\in\binom{[2:\mathsf{K}]}{\mathsf{U}}} \sum_{i\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}\right]:\mathcal{U}\cap\mathcal{S}_{1,i}\neq\emptyset} I(X_1; Z_{\mathcal{S}_{1,i}}|W_1, (Z_{\mathcal{S}_{1,j}} : j\in[i-1], \mathcal{U}\cap\mathcal{S}_{1,j}\neq\emptyset)) \tag{19d}$$

$$= \frac{1}{\binom{\mathsf{K}-1}{\mathsf{U}}-\binom{\mathsf{K}-\mathsf{S}}{\mathsf{U}}} \sum_{\mathcal{U}\in\binom{[2:\mathsf{K}]}{\mathsf{U}}} I\left(X_1; \left(Z_{\mathcal{S}_{1,j}} : j\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}\right], \mathcal{U}\cap\mathcal{S}_{1,j}\neq\emptyset\right)\Big|W_1\right) \tag{19e}$$

$$\geq \frac{1}{\binom{\mathsf{K}-1}{\mathsf{U}}-\binom{\mathsf{K}-\mathsf{S}}{\mathsf{U}}} \sum_{\mathcal{U}\in\binom{[2:\mathsf{K}]}{\mathsf{U}}} \mathsf{L} \tag{19f}$$

$$= \frac{\binom{\mathsf{K}-1}{\mathsf{U}}}{\binom{\mathsf{K}-1}{\mathsf{U}}-\binom{\mathsf{K}-\mathsf{S}}{\mathsf{U}}}\mathsf{L}, \tag{19g}$$

$\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}$ pieces.[6] Hence, in the first round of the proposed secure aggregation scheme, the first-round transmission by user k, $X_k = \left(X_{k,j} : j\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}\right]\right)$, contains two parts:

- for $j\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}\right]$, we construct

$$X_{k,j} = W_{k,j} + \sum_{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}:k\in\mathcal{V}} a_{\mathcal{V},j} Z_{\mathcal{V},k}; \tag{23}$$

- for $j\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}+1 : \binom{\mathsf{K}-1}{\mathsf{S}-1}\right]$, we construct

$$X_{k,j} = \sum_{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}:k\in\mathcal{V}} a_{\mathcal{V},j} Z_{\mathcal{V},k}. \tag{24}$$

For each $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$, define $\mathbf{a}_{\mathcal{V}} = \left[a_{\mathcal{V},1}, a_{\mathcal{V},2}, \ldots, a_{\mathcal{V},\binom{\mathsf{K}-1}{\mathsf{S}-1}}\right]^{\mathrm{T}}$, where each $a_{\mathcal{V},j}\in\mathbb{F}_{\mathsf{q}}$ is a coefficient to be clarified later.

The selection of $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$ is the most non-trivial design in the proposed secure aggregation scheme, which should satisfy the security constraint (49) and guarantee the encodability and decodability of the second-round transmission. Our selection contains two steps:

- First step. For each $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$ where $1\in\mathcal{V}$, we let $\mathbf{a}_{\mathcal{V}}$ be uniform and i.i.d. over $\mathbb{F}_{\mathsf{q}}^{\binom{\mathsf{K}-1}{\mathsf{S}-1}}$. Thus we have fixed $\binom{\mathsf{K}-1}{\mathsf{S}-1}$ coefficient vectors in random.
- Second step. For each $\mathcal{V}\in\binom{[2:\mathsf{K}]}{\mathsf{S}}$, we let $\mathbf{a}_{\mathcal{V}}$ be a linear combination of some vectors fixed in the first step. More precisely, we let (recall that $\mathcal{V}(i)$ represents the i^{th} smallest element in $\mathcal{V}$)

$$\mathbf{a}_{\mathcal{V}} = \sum_{i\in[\mathsf{S}]} (-1)^{i-1}\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i)\}\cup\{1\}}. \tag{25}$$

The above selection leads to the following lemma, which is crucial for Lemmas 2, 3, 4 (corresponding to the encodability of the second round transmission, decodability, and security of the proposed scheme, respectively).

Lemma 1. *By the above selection of coefficient vectors, for each $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$ and each $k\in[\mathsf{K}]\setminus\mathcal{V}$, denoting the number of elements in $\mathcal{V}$ smaller than k by $n_{\mathcal{V},k}$, we have*

$$\mathbf{a}_{\mathcal{V}} = \sum_{i_1\in[n_{\mathcal{V},k}+1:\mathsf{S}]} (-1)^{i_1-n_{\mathcal{V},k}-1}\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i_1)\}\cup\{k\}} + \sum_{i_2\in[n_{\mathcal{V},k}]} (-1)^{n_{\mathcal{V},k}+i_2}\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i_2)\}\cup\{k\}}; \tag{26}$$

in other words, $\mathbf{a}_{\mathcal{V}}$ is a linear combination of $\mathbf{a}_{\mathcal{V}\setminus\{k_1\}\cup\{k\}}$ where $k_1\in\mathcal{V}$. □

The proof of Lemma 1 could be found in Appendix A.

Due to user dropouts, the server only receives $(X_k : k\in\mathcal{U}_1)$. Hence, for each $j\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}\right]$, the server

[6] This is the main step to deal with the chanllenge arised in the case $\mathsf{S}\leq\mathsf{K}-\mathsf{U}$ compared to the secure aggregation scheme in [23] for the case $\mathsf{S}>\mathsf{K}-\mathsf{U}$. More precisely, when $\mathsf{S}\leq\mathsf{K}-\mathsf{U}$, there may exist some key where the whole group of users knowing that key all drop after the second round. Thus we need to transmit more than one (normalized) linear combinations in the first round to deal with this event, such that even if all the knowing users drop during the transmissions, we can still remove "interference" of this key to recover the task.

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

recovers

$$\sum_{k_1\in\mathcal{U}_1} X_{k_1,j} = \sum_{k_2\in\mathcal{U}_1} W_{k_2,j} + \sum_{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}:\mathcal{V}\cap\mathcal{U}_1\neq\emptyset} a_{\mathcal{V},j} \underbrace{\sum_{k_3\in\mathcal{V}\cap\mathcal{U}_1} Z_{\mathcal{V},k_3}}_{:=Z_{\mathcal{V}}^{\mathcal{U}_1}}; \tag{27}$$

for each $j \in \left[\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1} + 1 : \binom{\mathsf{K}-1}{\mathsf{S}-1}\right]$, the server recovers

$$\sum_{k_1\in\mathcal{U}_1} X_{k_1,j} = \sum_{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}:\mathcal{V}\cap\mathcal{U}_1\neq\emptyset} a_{\mathcal{V},j} Z_{\mathcal{V}}^{\mathcal{U}_1}. \tag{28}$$

Example 1. *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 will be proved later that our proposed scheme generally works for arbitrary field size.*

By the converse bound derived in Section IV, 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* $\mathcal{V}$*. In addition, we further divide each key* $Z_{\mathcal{V}}$ *into* $\mathsf{S} = 3$ *sub-keys,* $Z_{\mathcal{V}} = (Z_{\mathcal{V},k} : k \in \mathcal{V})$*, where each sub-key* $Z_{\mathcal{V},k}$ *has* $\frac{\mathsf{L}}{5}$ *symbols.*

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 [23] 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 key(s) 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 is the most important step in the proposed secure aggregation scheme, which will guarantee the encodability, decodability, and security. 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* $\mathbb{F}_{\mathsf{q}}$*. In this example, we let*

$$\mathbf{a}_{\{1,2,3\}} = [0,1,0,0,1,1]^{\mathrm{T}},\ \mathbf{a}_{\{1,2,4\}} = [1,0,1,1,1,1]^{\mathrm{T}},$$
$$\mathbf{a}_{\{1,2,5\}} = [0,0,0,1,0,1]^{\mathrm{T}},\ \mathbf{a}_{\{1,3,4\}} = [0,1,1,1,0,1]^{\mathrm{T}},$$
$$\mathbf{a}_{\{1,3,5\}} = [1,1,0,1,0,1]^{\mathrm{T}},\ \mathbf{a}_{\{1,4,5\}} = [1,0,0,0,0,1]^{\mathrm{T}}.$$

- *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,*

$$\mathbf{a}_{\{2,3,4\}} = \mathbf{a}_{\{1,3,4\}} - \mathbf{a}_{\{1,2,4\}} + \mathbf{a}_{\{1,2,3\}}. \tag{29}$$

Similarly, for each $\mathcal{V} \in \binom{[2:\mathsf{K}]}{\mathsf{S}}$*, we let* $\mathbf{a}_{\mathcal{V}}$ *be the following linear combination of* $\mathbf{a}_{\mathcal{V}\setminus\{k\}\cup\{1\}}$ *where* $k \in \mathcal{V}$*,*

$$\mathbf{a}_{\mathcal{V}} = \sum_{i\in[3]} (-1)^{i-1} \mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i)\}\cup\{1\}}. \tag{30}$$

The detailed selection on the coefficient vectors is given in Table I.

It can be checked that this selection has the property in Lemma 1, i.e., for each $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ *and each* $k \in [\mathsf{K}] \setminus \mathcal{V}$*,* $\mathbf{a}_{\mathcal{V}}$ *is a linear combination of* $\mathbf{a}_{\mathcal{V}\setminus\{k_1\}\cup\{k\}}$ *where* $k_1 \in \mathcal{V}$*. For example,*

- *let* $\mathcal{V} = \{3,4,5\}$ *and* $k = 1$*, we have*

$$\mathbf{a}_{\{3,4,5\}} = \mathbf{a}_{\{1,4,5\}} - \mathbf{a}_{\{1,3,5\}} + \mathbf{a}_{\{1,3,4\}}; \tag{31}$$

- *let* $\mathcal{V} = \{3,4,5\}$ *and* $k = 2$*, we have*

$$\mathbf{a}_{\{3,4,5\}} = \mathbf{a}_{\{2,4,5\}} - \mathbf{a}_{\{2,3,5\}} + \mathbf{a}_{\{2,3,4\}}; \tag{32}$$

- *let* $\mathcal{V} = \{2,3,5\}$ *and* $k = 1$*, we have*

$$\mathbf{a}_{\{2,3,5\}} = \mathbf{a}_{\{1,3,5\}} - \mathbf{a}_{\{1,2,5\}} + \mathbf{a}_{\{1,2,3\}}; \tag{33}$$

- *let* $\mathcal{V} = \{2,3,5\}$ *and* $k = 4$*, we have*

$$\mathbf{a}_{\{2,3,5\}} = \mathbf{a}_{\{2,3,4\}} - \mathbf{a}_{\{3,4,5\}} + \mathbf{a}_{\{2,4,5\}}. \tag{34}$$

After the selection of the above coefficient vectors, the transmission in the first round by each user $k \in [5]$ *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*

$$X_{k,j} = W_{k,j} + \sum_{\mathcal{V}\in\binom{[5]}{3}:k\in\mathcal{V}} a_{\mathcal{V},j} Z_{\mathcal{V},k}. \tag{35}$$

- *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*

$$X_{k,6} = \sum_{\mathcal{V}\in\binom{[5]}{3}:k\in\mathcal{V}} a_{\mathcal{V},6} Z_{\mathcal{V},k}. \tag{36}$$

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*

$$\sum_{k_1\in[5]} X_{k_1,j} = \sum_{k_2\in[5]} W_{k_2,j} + \sum_{\mathcal{V}\in\binom{[5]}{3}} a_{\mathcal{V},j} \underbrace{\sum_{k_3\in\mathcal{V}} Z_{\mathcal{V},k_3}}_{:=Z_{\mathcal{V}}^{[5]}} \tag{37}$$

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

$$\sum_{k_1\in[5]} X_{k_1,6} = \sum_{\mathcal{V}\in\binom{[5]}{3}} a_{\mathcal{V},6} Z_{\mathcal{V}}^{[5]}. \tag{38}$$

Hence, the server should further recover the second term on the RHS of (37)*,* $\sum_{\mathcal{V}\in\binom{[5]}{3}} a_{\mathcal{V},j} Z_{\mathcal{V}}^{[5]}$ *for* $j \in [5]$*, in the second round.* □

Next we describe the general description on the second round transmission.

Second round. The task of the second round transmission

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

TABLE I: Selection 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
$\mathbf{a}_{\{1,2,3\}}$	$[0,1,0,0,1,1]^{\mathrm{T}}$	$\mathbf{a}_{\{1,4,5\}}$	$[1,0,0,0,0,1]^{\mathrm{T}}$
$\mathbf{a}_{\{1,2,4\}}$	$[1,0,1,1,1,1]^{\mathrm{T}}$	$\mathbf{a}_{\{2,3,4\}}$	$\mathbf{a}_{\{1,3,4\}}-\mathbf{a}_{\{1,2,4\}}+\mathbf{a}_{\{1,2,3\}}=[-1,2,0,0,0,1]^{\mathrm{T}}$
$\mathbf{a}_{\{1,2,5\}}$	$[0,0,0,1,0,1]^{\mathrm{T}}$	$\mathbf{a}_{\{2,3,5\}}$	$\mathbf{a}_{\{1,3,5\}}-\mathbf{a}_{\{1,2,5\}}+\mathbf{a}_{\{1,2,3\}}=[1,2,0,0,1,1]^{\mathrm{T}}$
$\mathbf{a}_{\{1,3,4\}}$	$[0,1,1,1,0,1]^{\mathrm{T}}$	$\mathbf{a}_{\{2,4,5\}}$	$\mathbf{a}_{\{1,4,5\}}-\mathbf{a}_{\{1,2,5\}}+\mathbf{a}_{\{1,2,4\}}=[2,0,1,0,1,1]^{\mathrm{T}}$
$\mathbf{a}_{\{1,3,5\}}$	$[1,1,0,1,0,1]^{\mathrm{T}}$	$\mathbf{a}_{\{3,4,5\}}$	$\mathbf{a}_{\{1,4,5\}}-\mathbf{a}_{\{1,3,5\}}+\mathbf{a}_{\{1,3,4\}}=[0,0,1,0,0,1]^{\mathrm{T}}$

is to let each user $k\in\mathcal{U}_1$ transmit $Y_k^{\mathcal{U}_1}$ such that from any subset of users $\mathcal{U}_2\subseteq\mathcal{U}_1$ where $|\mathcal{U}_1|\geq|\mathcal{U}_2|\geq\mathsf{U}$, the server can recover

$$\sum_{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}:\mathcal{V}\cap\mathcal{U}_1\neq\emptyset} a_{\mathcal{V},j_1}Z_{\mathcal{V}}^{\mathcal{U}_1},\ \forall j_1\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}\right], \tag{39}$$

from $(Y_{k_1}^{\mathcal{U}_1}:k_1\in\mathcal{U}_2)$ and $\left(\sum_{k_1\in\mathcal{U}_1}X_{k_1,j}:j\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}+1:\binom{\mathsf{K}-1}{\mathsf{S}-1}\right]\right)$ in (28). In other words, from $(Y_{k_1}^{\mathcal{U}_1}:k_1\in\mathcal{U}_2)$ and the linear combinations in (28), the server should recover

$$\sum_{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}:\mathcal{V}\cap\mathcal{U}_1\neq\emptyset} a_{\mathcal{V},j}Z_{\mathcal{V}}^{\mathcal{U}_1},\ \forall j\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}\right]. \tag{40}$$

To achieve $\mathsf{R}_2=1/\mathsf{U}$, we further divide each $Z_{\mathcal{V}}^{\mathcal{U}_1}$ where $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$ and $\mathcal{V}\cap\mathcal{U}_1\neq\emptyset$, into U non-overlapping and equal-length coded keys, $Z_{\mathcal{V}}^{\mathcal{U}_1}=\left(Z_{\mathcal{V},i}^{\mathcal{U}_1}:i\in[\mathsf{U}]\right)$, where each coded key contains $\frac{\mathsf{L}}{\mathsf{U}\left(\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}\right)}$ symbols. We denote the sets in the collection $\left\{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}:\mathcal{V}\cap\mathcal{U}_1\neq\emptyset\right\}$, by $\mathcal{V}_{\mathcal{U}_1,1},\mathcal{V}_{\mathcal{U}_1,2},\ldots,\mathcal{V}_{\mathcal{U}_1,P}$, where with a slight abuse of notation P represents the number of sets in the above collection. Thus the recovery task in (40) could be expressed in the matrix form

$$\mathbf{F}\begin{bmatrix} Z_{\mathcal{V}_{\mathcal{U}_1,1},1}^{\mathcal{U}_1}\\ Z_{\mathcal{V}_{\mathcal{U}_1,2},1}^{\mathcal{U}_1}\\ \vdots\\ Z_{\mathcal{V}_{\mathcal{U}_1,P},1}^{\mathcal{U}_1}\\ Z_{\mathcal{V}_{\mathcal{U}_1,1},2}^{\mathcal{U}_1}\\ \vdots\\ Z_{\mathcal{V}_{\mathcal{U}_1,P},\mathsf{U}}^{\mathcal{U}_1}\end{bmatrix}=\begin{bmatrix} F_1\\ \vdots\\ F_{\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1}}\end{bmatrix} \tag{41}$$

where (recall that $(\mathbf{M})_{m\times n}$ represents the dimension of matrix $\mathbf{M}$ is $m\times n$)

$$\mathbf{F}=\begin{bmatrix} (\mathbf{A})_{\binom{\mathsf{K}-1}{\mathsf{S}-1}\times P} & 0_{\binom{\mathsf{K}-1}{\mathsf{S}-1}\times P} & \cdots & 0_{\binom{\mathsf{K}-1}{\mathsf{S}-1}\times P}\\ 0_{\binom{\mathsf{K}-1}{\mathsf{S}-1}\times P} & (\mathbf{A})_{\binom{\mathsf{K}-1}{\mathsf{S}-1}\times P} & \cdots & 0_{\binom{\mathsf{K}-1}{\mathsf{S}-1}\times P}\\ \vdots & \vdots & \ddots & \vdots\\ 0_{\binom{\mathsf{K}-1}{\mathsf{S}-1}\times P} & 0_{\binom{\mathsf{K}-1}{\mathsf{S}-1}\times P} & \cdots & (\mathbf{A})_{\binom{\mathsf{K}-1}{\mathsf{S}-1}\times P}\end{bmatrix}, \tag{42}$$

with $0_{m\times n}$ representing the zero matrix with dimension $m\times n$ and

$$(\mathbf{A})_{\binom{\mathsf{K}-1}{\mathsf{S}-1}\times P}=\begin{bmatrix} a_{\mathcal{V}_{\mathcal{U}_1,1},1} & a_{\mathcal{V}_{\mathcal{U}_1,2},1} & \cdots & a_{\mathcal{V}_{\mathcal{U}_1,P},1}\\ a_{\mathcal{V}_{\mathcal{U}_1,1},2} & a_{\mathcal{V}_{\mathcal{U}_1,2},2} & \cdots & a_{\mathcal{V}_{\mathcal{U}_1,P},2}\\ \vdots & \vdots & \ddots & \vdots\\ a_{\mathcal{V}_{\mathcal{U}_1,1},\binom{\mathsf{K}-1}{\mathsf{S}-1}} & a_{\mathcal{V}_{\mathcal{U}_1,2},\binom{\mathsf{K}-1}{\mathsf{S}-1}} & \cdots & a_{\mathcal{V}_{\mathcal{U}_1,P},\binom{\mathsf{K}-1}{\mathsf{S}-1}}\end{bmatrix}. \tag{43}$$

Note that $\left(F_{\binom{\mathsf{K}-1}{\mathsf{S}-1}(i-1)+j}:i\in[\mathsf{U}],j\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}+1:\binom{\mathsf{K}-1}{\mathsf{S}-1}\right]\right)$ are the linear combinations in (28), which have already been recovered by the server in the first round.

Thus we can let each user $k\in\mathcal{U}_1$ transmit

$$Y_k^{\mathcal{U}_1}=\mathbf{S}_k\begin{bmatrix} F_1\\ \vdots\\ F_{\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1}}\end{bmatrix}, \tag{44}$$

where $\mathbf{S}_k$ with $\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}$ rows represents the matrix of second-round transmission by user k. The next step is to determine $\mathbf{S}_k$ satisfying that

- (c1) encodability for the second-round transmission: in the second-round transmission by each user $k\in\mathcal{U}_1$, the coefficients of $Z_{\mathcal{V},i}^{\mathcal{U}_1}$ where $\mathcal{V}\in\binom{[\mathsf{K}]\backslash\{k\}}{\mathsf{S}}$ and $i\in[\mathsf{U}]$ are 0, since user k cannot compute such coded keys;
- (c2) decodability: for any set $\mathcal{U}_2\subseteq\mathcal{U}_1$ where $|\mathcal{U}_2|=\mathsf{U}$, the matrix (recall that $\mathbf{e}_{n,i}$ represents the vertical n-dimensional standard unit vector whose i^{th} element is 1)

$$\begin{bmatrix} \mathbf{S}_{\mathcal{U}_{2,1}}\\ \vdots\\ \mathbf{S}_{\mathcal{U}_{2,\mathsf{U}}}\\ \mathbf{e}_{\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1},\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}+1}\\ \mathbf{e}_{\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1},\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}+2}\\ \vdots\\ \mathbf{e}_{\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1},\binom{\mathsf{K}-1}{\mathsf{S}-1}}\\ \mathbf{e}_{\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1},\binom{\mathsf{K}-1}{\mathsf{S}-1}+\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}+1}\\ \vdots\\ \mathbf{e}_{\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1},\binom{\mathsf{K}-1}{\mathsf{S}-1}+\binom{\mathsf{K}-1}{\mathsf{S}-1}}\\ \vdots\\ \mathbf{e}_{\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1},\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1}}\end{bmatrix} \tag{45}$$

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

with dimension $\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1} \times \mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1}$ is full rank.

Note that (c1) guarantees in $Y_k^{\mathcal{U}_1}$, the transmitted linear combinations of the coded keys do not contain the coded keys which user k cannot compute; (c2) guarantees that from the second-round transmissions by any U users in $\mathcal{U}_1$, the server can recover (41) and then the computation task $\sum_{k' \in \mathcal{U}_1} W_{k',j}$ for each $j \in \left[\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}\right]$.

Let us focus on one user $k \in [\mathsf{K}]$ and construct $\mathbf{S}_k$; note that, our construction on $\mathbf{S}_k$ is independent of the value of $\mathcal{U}_1$. Denote the sets in $\binom{[\mathsf{K}]\setminus\{k\}}{\mathsf{S}}$ by $\overline{\mathcal{S}}_{k,1}, \ldots, \overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}$. By the selection of the coefficient vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$, we have the following lemma, whose proof could be found in Appendix B.

Lemma 2 (Interference alignment for encodability)**.** *The matrix*

$$\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}}, \mathbf{a}_{\overline{\mathcal{S}}_{k,2}}, \ldots, \mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}}\right] \tag{46}$$

with dimension $\binom{\mathsf{K}-1}{\mathsf{S}-1} \times \binom{\mathsf{K}-1}{\mathsf{S}}$, has rank equal to $\binom{\mathsf{K}-2}{\mathsf{S}-1}$ with high probability. □

It can be seen from Lemma 2 that, by the selection of the coefficient vectors, the "interferences" to user k (i.e., the coded keys which user k cannot compute) are aligned. Thus with high probability the left null space of the matrix in (46) contains $\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-2}{\mathsf{S}-1} = \binom{\mathsf{K}-2}{\mathsf{S}-2}$ linearly independent vectors, denoted by $\mathbf{s}_{k,1}, \ldots, \mathbf{s}_{k,\binom{\mathsf{K}-2}{\mathsf{S}-2}}$, each with dimension $1 \times \binom{\mathsf{K}-1}{\mathsf{S}-1}$.

Then considering the division of keys in the second-round transmission, we construct the following matrix with dimension $\mathsf{U}\binom{\mathsf{K}-2}{\mathsf{S}-2} \times \mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1}$,

$$\mathbf{S}'_k = \left[\begin{array}{c|c|c|c} \mathbf{s}_{k,1} & 0_{1\times\binom{\mathsf{K}-1}{\mathsf{S}-1}} & \cdots & 0_{1\times\binom{\mathsf{K}-1}{\mathsf{S}-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{s}_{k,\binom{\mathsf{K}-2}{\mathsf{S}-2}} & 0_{1\times\binom{\mathsf{K}-1}{\mathsf{S}-1}} & \cdots & 0_{1\times\binom{\mathsf{K}-1}{\mathsf{S}-1}} \\ \hline 0_{1\times\binom{\mathsf{K}-1}{\mathsf{S}-1}} & \mathbf{s}_{k,1} & \cdots & 0_{1\times\binom{\mathsf{K}-1}{\mathsf{S}-1}} \\ \vdots & \vdots & \ddots & \vdots \\ 0_{1\times\binom{\mathsf{K}-1}{\mathsf{S}-1}} & \mathbf{s}_{k,\binom{\mathsf{K}-2}{\mathsf{S}-2}} & \cdots & 0_{1\times\binom{\mathsf{K}-1}{\mathsf{S}-1}} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline 0_{1\times\binom{\mathsf{K}-1}{\mathsf{S}-1}} & 0_{1\times\binom{\mathsf{K}-1}{\mathsf{S}-1}} & \cdots & \mathbf{s}_{k,1} \\ \vdots & \vdots & \ddots & \vdots \\ 0_{1\times\binom{\mathsf{K}-1}{\mathsf{S}-1}} & 0_{1\times\binom{\mathsf{K}-1}{\mathsf{S}-1}} & \cdots & \mathbf{s}_{k,\binom{\mathsf{K}-2}{\mathsf{S}-2}} \end{array}\right]. \tag{47}$$

Finally, we let $\mathbf{S}_k$ be $\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}$ random linear combinations of the rows in $\mathbf{S}'_k$, where each coefficient in each linear combination is uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}$. These $\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}$ random linear combinations are linearly independent with high probability since

$$\mathsf{U}\binom{\mathsf{K}-2}{\mathsf{S}-2} \geq \binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}, \tag{48}$$

whose proof could be found in Appendix C. Note that it will be also proved in Appendix C that the equality in (48) holds when $\mathsf{K} = \mathsf{S}$.

By construction, the columns in $\mathbf{S}'_k\mathbf{A}$ corresponding to the coded keys $Z^{\mathcal{U}_1}_{\mathcal{V},j}$ where $\mathcal{V} \in \binom{[\mathsf{K}]\setminus\{k\}}{\mathsf{S}}$, $\mathcal{V} \cap \mathcal{U}_1 \neq \emptyset$, and $j \in [\mathsf{U}]$, are all $0_{\mathsf{U}\binom{\mathsf{K}-2}{\mathsf{S}-2}\times 1}$. Since the rows of $\mathbf{S}_k$ are linear combinations of the rows in $\mathbf{S}'_k$, the columns in $\mathbf{S}_k\mathbf{A}$ corresponding to the coded keys $Z^{\mathcal{U}_1}_{\mathcal{V},j}$ where $\mathcal{V} \in \binom{[\mathsf{K}]\setminus\{k\}}{\mathsf{S}}$, $\mathcal{V} \cap \mathcal{U}_1 \neq \emptyset$, and $j \in [\mathsf{U}]$, are also all $0_{\left(\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}\right)\times 1}$. Thus (c1) is satisfied with high probability.

In Appendix D, by using the Schwartz-Zippel lemma [32]–[34], we have the following lemma, which shows that (c2) is satisfied with high probability by the proposed second-round transmission.

Lemma 3 (Decodability)**.** *For any set $\mathcal{U}_2 \subseteq [\mathsf{K}]$ where $|\mathcal{U}_2| = \mathsf{U}$, the matrix in* (45) *is full rank with high probability.* □

Finally, the following lemma shows that the proposed scheme is information theoretically secure.

Lemma 4 (Security)**.** *By the proposed scheme, after receiving all the linear combinations in $X_1, \ldots X_{\mathsf{K}}$ and $Y_k^{\mathcal{U}_1}$ where $k \in \mathcal{U}_1$, the server cannot get any information about $W_1, \ldots, W_{\mathsf{K}}$ except $\sum_{k\in\mathcal{U}_1} W_k$.* □

In the following we provide an intuitive proof on Lemma 4, while the formal proof is provided in Appendix E. By the security constraint, as we proved in (16f), the server should not get any information about W_k from X_k, which requires that the rank of the sub-keys in X_k is equal to the dimension of X_k. In other words, by denoting the sets $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ where $k \in \mathcal{V}$ by $\mathcal{S}_{k,1}, \ldots, \mathcal{S}_{k,\binom{\mathsf{K}-1}{\mathsf{S}-1}}$, we need to have that the coefficients matrix (whose dimension is $\binom{\mathsf{K}-1}{\mathsf{S}-1} \times \binom{\mathsf{K}-1}{\mathsf{S}-1}$)

$$\left[\mathbf{a}_{\mathcal{S}_{k,1}}, \ldots, \mathbf{a}_{\mathcal{S}_{k,\binom{\mathsf{K}-1}{\mathsf{S}-1}}}\right] \quad \text{has rank equal to } \binom{\mathsf{K}-1}{\mathsf{S}-1}. \ \forall k \in [\mathsf{K}]. \tag{49}$$

It can be checked that (49) is satisfied by the above selection of coefficient vectors. This is because by Lemma 1, it can be directly seen that for each $k \in [\mathsf{K}]$, from the coefficient vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ and $k \in \mathcal{V}$, we can re-construct all $\binom{\mathsf{K}}{\mathsf{S}}$ coefficient vectors; thus the constraint (49) is satisfied with high probability.[7]

In addition, $(X_1, W_1), \ldots, (X_{\mathsf{K}}, W_{\mathsf{K}})$ are mutually independent in our scheme, because the keys and input vectors are mutually independent and $X_1, \ldots, X_{\mathsf{K}}$ use different sub-keys. Hence, from $X_1, \ldots, X_{\mathsf{K}}$ the server cannot get any information about $W_1, \ldots, W_{\mathsf{K}}$.

In the second round, all the transmissions are in the linear space spanned by $F_1, \ldots F_{\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1}}$, totally $\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1}\frac{\mathsf{L}}{\mathsf{U}\left(\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}\right)} = \mathsf{L}\frac{\binom{\mathsf{K}-1}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}$ symbols. In addition, the server can recover $\left(F_{\binom{\mathsf{K}-1}{\mathsf{S}-1}(i-1)+j} : i \in [\mathsf{U}], j \in \left[\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1} + 1 : \binom{\mathsf{K}-1}{\mathsf{S}-1}\right]\right)$ from the first round.

[7]We generate $\binom{\mathsf{K}-1}{\mathsf{S}-1}$ coefficient vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ and $1 \in \mathcal{V}$, and each vector contains $\binom{\mathsf{K}-1}{\mathsf{S}-1}$ elements uniformly i.i.d. over a large enough finite field. Hence, these $\binom{\mathsf{K}-1}{\mathsf{S}-1}$ coefficient vectors are linearly independent with high probability.

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

Hence, from the second round the server can get at most

$$\mathsf{L}\frac{\binom{\mathsf{K}-1}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}-\mathsf{L}\frac{\mathsf{U}\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}{\mathsf{U}\left(\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}\right)}=\mathsf{L}$$

symbols. Hence, by the Shannon's seminal results in [18], from the second round the server can get at most L symbols information about $W_1,\ldots,W_{\mathsf{K}}$, which are exactly the L symbols in the computation task $\sum_{k\in\mathcal{U}_1}W_k$ by the decodability proof. Hence, the server cannot get any information about $W_1,\ldots,W_{\mathsf{K}}$ except the computation task.

In conclusion, since we show that the constraints (c1), (c2) and in (49) are satisfied with high probability where the randomness is in the selection on coefficients vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$ and $1\in\mathcal{V}$ and on $\mathbf{S}_k$ where $k\in[\mathsf{K}]$;[8] thus there must exist one selection such that all these constraints are satisfied. **So the proposed scheme is decodable and secure satisfying the constraints in** (6) **and** (7)**, with** $\mathsf{R}_1=\frac{\binom{\mathsf{K}-1}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}$ **and** $\mathsf{R}_2\geq\frac{1}{\mathsf{U}}$**.**

Example 1 (cont.) *Let us return to Example 1 with* $(\mathsf{K},\mathsf{U},\mathsf{S})=(5,2,3)$ *and describe the second-round transmission of the proposed scheme. Recall that we consider the case* $\mathcal{U}_1=[5]$*, i.e., no user drops in the first round. The server should further recover* $\sum_{\mathcal{V}\in\binom{[5]}{3}}a_{\mathcal{V},j}Z_{\mathcal{V}}^{[5]}$ *for* $j\in[5]$*, in the second round, where the coefficient vectors* $\mathbf{a}_{\mathcal{V}}$ *where* $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$ *are given in Table I.*

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 matrix form*

$$\begin{bmatrix}F_1\\ \vdots\\ F_{12}\end{bmatrix}=\mathbf{F}\begin{bmatrix}Z_{\{1,2,3\},1}^{[5]}\\ Z_{\{1,2,4\},1}^{[5]}\\ \vdots\\ Z_{\{3,4,5\},1}^{[5]}\\ Z_{\{1,2,3\},2}^{[5]}\\ Z_{\{1,2,4\},2}^{[5]}\\ \vdots\\ Z_{\{3,4,5\},2}^{[5]}\end{bmatrix}\tag{50}$$

where

$$\mathbf{F}=\begin{bmatrix}\mathbf{a}_{\{1,2,3\}},\mathbf{a}_{\{1,2,4\}},\ldots,\mathbf{a}_{\{3,4,5\}} & 0_{6\times 10}\\ 0_{6\times 10} & \mathbf{a}_{\{1,2,3\}},\mathbf{a}_{\{1,2,4\}},\ldots,\mathbf{a}_{\{3,4,5\}}\end{bmatrix}.\tag{51}$$

Note that $F_6=\sum_{\mathcal{V}\in\binom{[5]}{3}}a_{\mathcal{V},6}Z_{\mathcal{V},1}^{[5]}$ *and* $F_{12}=\sum_{\mathcal{V}\in\binom{[5]}{3}}a_{\mathcal{V},6}Z_{\mathcal{V},2}^{[5]}$ *have been already recovered by the server from the first round.*

[8]Recall that $\mathbf{S}_k$ contains $\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}$ random linear combinations of the rows in $\mathbf{S}'_k$, where each coefficient in each linear combination is uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}$.

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*

$$\mathbf{S}_k\begin{bmatrix}F_1\\ \vdots\\ F_{12}\end{bmatrix},\tag{52}$$

where $\mathbf{S}_k$ *is a matrix with dimension* 5×12*. Note that for the encodability, user* k *can only compute the coded keys* $Z_{\mathcal{V},j}^{[5]}$ *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*, given in* (53) *at the top of the next page. 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* (31) *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, 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*

$$\begin{aligned}&(\mathbf{s}_{1,1},0_{1\times 6}),\ (\mathbf{s}_{1,2},0_{1\times 6}),\ (\mathbf{s}_{1,3},0_{1\times 6}),\\ &(0_{1\times 6},\mathbf{s}_{1,1}),\ (0_{1\times 6},\mathbf{s}_{1,2}),\ (0_{1\times 6},\mathbf{s}_{1,3}).\end{aligned}\tag{54}$$

We let each row of $\mathbf{S}_1$ *be one random linear combination of the vectors in* (54)*; in this example, we let*

$$\mathbf{S}_1=\begin{bmatrix}0&-1&-2&0&0&2&0&0&0&0&0&0\\ -2&-1&0&0&4&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&-1&-2&0&0&2\\ 0&0&0&0&0&0&-2&-1&0&0&4&0\\ 0&0&0&1&0&0&0&0&0&1&0&0\end{bmatrix}.\tag{55}$$

For user 2*, the columns of* $\mathbf{S}_2\mathbf{F}$ *with indices in* $\{4,5,6,10,14,15,16,20\}$ *should be* $0_{5\times 1}$*, since these columns correspond to* $Z_{\{1,3,4\},1}$*,* $Z_{\{1,3,5\},1}$*,* $Z_{\{1,4,5\},1}$*,* $Z_{\{3,4,5\},1}$*,* $Z_{\{1,3,4\},2}$*,* $Z_{\{1,3,5\},2}$*,* $Z_{\{1,4,5\},2}$*,* $Z_{\{3,4,5\},2}$*, which cannot be computed by user* 2*. 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*, given in* (56) *at the top of the next page. 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* (32)*. 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,*

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

$$\mathbf{F}_1 = \left[\begin{array}{c:c} \underline{\mathbf{a}_{\{2,3,4\}}, \mathbf{a}_{\{2,3,5\}}, \mathbf{a}_{\{2,4,5\}}, \mathbf{a}_{\{3,4,5\}}} & 0_{6\times 4} \\ 0_{6\times 4} & \mathbf{a}_{\{2,3,4\}}, \mathbf{a}_{\{2,3,5\}}, \mathbf{a}_{\{2,4,5\}}, \mathbf{a}_{\{3,4,5\}} \end{array}\right]. \tag{53}$$

$$\mathbf{F}_2 = \left[\begin{array}{c:c} \underline{\mathbf{a}_{\{1,3,4\}}, \mathbf{a}_{\{1,3,5\}}, \mathbf{a}_{\{1,4,5\}}, \mathbf{a}_{\{3,4,5\}}} & 0_{6\times 4} \\ 0_{6\times 4} & \mathbf{a}_{\{1,3,4\}}, \mathbf{a}_{\{1,3,5\}}, \mathbf{a}_{\{1,4,5\}}, \mathbf{a}_{\{3,4,5\}} \end{array}\right]. \tag{56}$$

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 one random linear combination of the vectors in* (54)*; in this example, we let*

$$\mathbf{S}_2 = \begin{bmatrix} -1 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 & 0 & -2 & 0 & 2 & 0 & 0 \end{bmatrix}. \tag{57}$$

We can also check that

- $\mathbf{a}_{\{2,4,5\}} = \mathbf{a}_{\{1,4,5\}} - \mathbf{a}_{\{1,2,5\}} + \mathbf{a}_{\{1,2,4\}}$*; thus 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*;*
- $\mathbf{a}_{\{2,3,5\}} = \mathbf{a}_{\{1,3,5\}} - \mathbf{a}_{\{1,2,5\}} + \mathbf{a}_{\{1,2,3\}}$*; thus 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*;*
- $\mathbf{a}_{\{2,3,4\}} = \mathbf{a}_{\{1,3,4\}} - \mathbf{a}_{\{1,2,4\}} + \mathbf{a}_{\{1,2,3\}}$*; thus 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*.*

So Lemma 2 holds in this example. Then by a similar way to choose $\mathbf{S}_1$ *and* $\mathbf{S}_2$*, we choose*

$$\mathbf{S}_3 = \begin{bmatrix} -1 & 0 & 1 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{58}$$

$$\mathbf{S}_4 = \begin{bmatrix} 1 & -1 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \end{bmatrix}, \tag{59}$$

$$\mathbf{S}_5 = \begin{bmatrix} -1 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & -1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -2 & -1 & 1 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & -5 & 5 & 0 & 0 \end{bmatrix}. \tag{60}$$

As a summary, constraint (c1) 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. 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 from* (55)-(60) *that the matrix*

$$\begin{bmatrix} \mathbf{S}_{u_1} \\ \mathbf{S}_{u_2} \\ \mathbf{e}_{12,6}^{\mathrm{T}} \\ \mathbf{e}_{12,12}^{\mathrm{T}} \end{bmatrix} \tag{61}$$

whose dimension is 12×12*, is full rank; thus constraint (c2) is satisfied (i.e., Lemma 3 holds in this example). So the server can recover* $F_1, \ldots, F_{12}$ *and then recover* $W_1 + \cdots + W_5$*.*

Lastly, we check the security. Recall that we denote the sets $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ *where* $k \in \mathcal{V}$ *by* $\mathcal{S}_{k,1}, \ldots, \mathcal{S}_{k,\binom{\mathsf{K}-1}{\mathsf{S}-1}}$*. It can be checked from Table I that our selection on the coefficient vectors has the following property:*

$$\left[\mathbf{a}_{\mathcal{S}_{k,1}}, \ldots, \mathbf{a}_{\mathcal{S}_{k,\binom{\mathsf{K}-1}{\mathsf{S}-1}}}\right] \quad \textit{has rank equal to} \quad \binom{\mathsf{K}-1}{\mathsf{S}-1} = 6, \tag{62}$$

for each $k \in [\mathsf{K}]$*.*

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* (62)*, 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*. In addition,* $(X_1, W_1), \ldots, (X_5, W_5)$ *are mutually independent in our scheme, because the keys and input vectors are mutually independent and* $X_1, \ldots, X_5$ *use different sub-keys. Hence, from* $X_1, \ldots, X_5$ *the server cannot get 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 [18] 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* $\mathcal{U}_1 \geq 2$*. For example, consider* $\mathcal{U}_1 = [4]$*. After the first round, the server can recover*

$$\sum_{k_1 \in [4]} X_{k_1,j} = \sum_{k_2 \in [4]} W_{k_2,j} + \sum_{\mathcal{V} \in \binom{[5]}{3}} a_{\mathcal{V},j} \underbrace{\sum_{k_3 \in \mathcal{V} \cap [4]} Z_{\mathcal{V},k_3}}_{:= Z_{\mathcal{V}}^{[4]}} \tag{63}$$

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

$$\sum_{k_1 \in [4]} X_{k_1,6} = \sum_{\mathcal{V} \in \binom{[5]}{3}} a_{\mathcal{V},6} Z_{\mathcal{V}}^{[4]}. \tag{64}$$

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

Hence, the server should further recover in the second round

$$\begin{bmatrix} F_1 \\ \vdots \\ F_{12} \end{bmatrix} = \mathbf{F} \begin{bmatrix} Z^{[4]}_{\{1,2,3\},1} \\ Z^{[4]}_{\{1,2,4\},1} \\ \vdots \\ Z^{[4]}_{\{3,4,5\},1} \\ Z^{[4]}_{\{1,2,3\},2} \\ Z^{[4]}_{\{1,2,4\},2} \\ \vdots \\ Z^{[4]}_{\{3,4,5\},2} \end{bmatrix}, \tag{65}$$

where $\mathbf{F}$ *is given in* (53)*, and* F_6, F_{12} *have been recovered from the first round. By choosing* $\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_3, \mathbf{S}_4$ *as in* (55)-(59)*, we let each user* $k \in [4]$ *transmit* $\mathbf{S}_k\mathbf{F}$ *in the second round. For any set of two users* $\mathcal{U}_2 = \{u_1, u_2\} \subseteq [4]$ *where* $|\mathcal{U}_2| = 2$*, the matrix in* (61) *is full rank; thus the decodability was proved. By the same reason as the case* $\mathcal{U}_1 = [5]$*, we can also prove that the proposed scheme is secure for the case* $\mathcal{U}_1 = [4]$.

As a result, the proposed secure aggregation scheme achieves $\mathsf{R}_1 = 6/5$ *and* $\mathsf{R}_2 = 1/2$*, coinciding with the converse bound in Section IV.* □

Remark 1. *The proposed secure aggregation scheme in this section can also work for the case* $\mathsf{S} > \mathsf{K} - \mathsf{U}$*. In this case,* $\mathsf{R}_1 = \frac{\binom{\mathsf{K}-1}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}} = 1$ *and each input vector is divided into* $\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1} = \binom{\mathsf{K}-1}{\mathsf{S}-1}$ *non-overlapping and equal-length pieces. In the first round transmission, we only transmit the coded messages in* (23)*, while the coded messages in* (24) *does not exist since* $\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1} = 0$*. In other words, since the number of users knowing each key is larger than the maximal number of dropped users, in the first round we do not need to transmit coded messages in* (24) *which are only composed of keys. In addition, in the second round transmission, the proposed scheme also works with the optimal communication rate* $\mathsf{R}_2 = 1/\mathsf{U}$*, while the decodability and security constraints are both satisfied.*

For the case $\mathsf{S} > \mathsf{K}-\mathsf{U}$*, compared to the secure aggregation scheme in [23] with the optimal communication rates, the proposed secure aggregation scheme in this paper achieves the same optimal communication rates. However, the proposed scheme requires all the* $\binom{\mathsf{K}}{\mathsf{S}}$ *keys each of which is shared by a different set of* S *users and has* $\frac{\mathsf{S}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}}$ *symbols; the number of keys required by the scheme in [23] is at most* $\mathcal{O}(\mathsf{K}^2)$*, where each key is shared by* S *users and has* $(\mathsf{K}-\mathsf{U}+1)\mathsf{L}/\mathsf{U}$ *symbols.* □

VI. Experimental Results

We implement our proposed secure aggregation scheme in Python3.11 by using the MPI4py library over the Tencent Cloud, which is then compared to the original secure aggregation scheme in [6] (referred to as SecAgg). Note that, the secure aggregation scheme in [6] is modified to guarantee information theoretic security if each key is generated with i.i.d. symbols instead of being generated by pseudorandom generator. Our comparison focuses on the model aggregation times of the proposed protocol and SecAgg (including encryption, transmission, decryption times), by assuming the offline keys have been already shared.

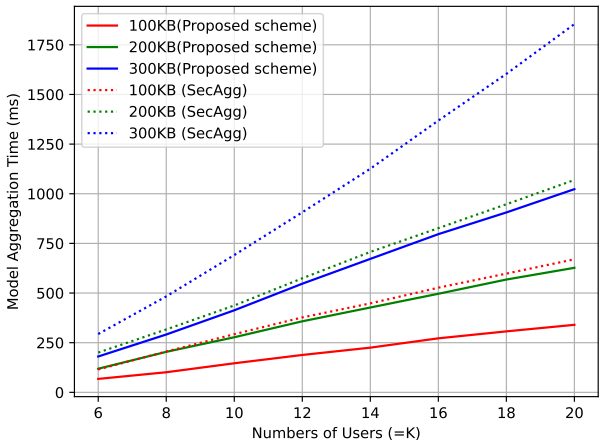


Fig. 2: Model aggregation times of the proposed scheme and `SecAgg` for $\mathsf{U} = \lfloor(\mathsf{K}+1)/2\rfloor$ and $\mathsf{S} = \mathsf{K} - \mathsf{U}$.

Tencent Cloud Setup. We choose Tencent Cloud instances, specifically `S6.LARGE16` and `S6.MEDIUM2`. Of these, one `S6.LARGE16` instance plays the role of the server and all the users. These Tencent Cloud instances are equipped with Intel Xeon Ice Lake processors running at a base clock speed of 2.7 GHz with a turbo frequency of 3.3 GHz. All instances used in our experiment are identical in terms of computing power, memory and network resources. The communication speed between the server and the users is a fast 100MB/s. To generate our input vectors, we set the field size q to 7 and generate vectors that are uniformly i.i.d. over $\mathbb{F}_7$. We also consider three different sizes for each input vector: 100KB, 200KB, and 300KB, following the suggestions in [6]. In the system configuration represented by $(\mathsf{K}, \mathsf{U}, \mathsf{S})$, we use Monte Carlo methods with 100 samples and then average the resulting times over these 100 samples.

Proposed scheme v.s. `SecAgg`. We compare the model aggregation times of our proposed scheme and SecAgg, for $\mathsf{U} = \lfloor(\mathsf{K}+1)/2\rfloor$ and $\mathsf{S} = \mathsf{K} - \mathsf{U}$, as shown in Fig. 2. We can see that the proposed scheme outperforms SecAgg by reducing model aggregation time, where the reduction percent ranges from 29.7% to 67.2%. This improvement coincides with the theoretical perspective that the proposed scheme achieves the optimal communication cost during the model aggregation phase, while SecAgg does not.

VII. Conclusions and Discussions

In this paper, we aimed to minimize the communication rates in the two-round transmissions of the model aggregation phase, for the information theoretic secure aggregation problem with uncoded groupwise keys. While preserving the security on the users' local data, the secure aggregation scheme should also be able to tolerate user dropouts. By

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

proposing a new and tight converse bound coinciding with the achievable rates by the new secure aggregation scheme based on interference alignment, we fully characterized the region of all possible rates tuples for the considered problem.

There are several interesting and important future directions on secure aggregation with uncoded groupwise keys. First, when the total size of keys or the storage cost on keys by each user is limited by a value, it is important to characterize the optimal tradeoff between this value and the communication rates.[9] Second, it is important to consider the threat model where the server can collude with some users; thus secure aggregation with uncoded groupwise keys against user collusion can be one of the future works. Third, the extension of the secure aggregation scheme with uncoded groupwise keys to the scenario of clustered federated learning is another promising direction.

Appendix A
Proof of Lemma 1

Consider one set $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ and one $k \in [\mathsf{K}] \setminus \mathcal{V}$. Recall that $n_{\mathcal{V},k}$ represents the number of elements in $\mathcal{V}$ which are smaller than k.

When $k = 1$, we have $n_{\mathcal{V},1} = 0$ and thus the equation to be proved, (26), becomes

$$\mathbf{a}_{\mathcal{V}} = \sum_{i_1 \in [\mathsf{S}]} (-1)^{i_1 - 1} \mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i_1)\} \cup \{1\}}, \tag{66}$$

which is exactly (25) and thus is proved.

When $1 \in \mathcal{V}$ and $k \neq 1$, assume that $\mathcal{V} \setminus \{1\} = \mathcal{V}'$ where $|\mathcal{V}'| = \mathsf{S} - 1$. Hence, (26) becomes

$$\begin{aligned} \mathbf{a}_{\mathcal{V}' \cup \{1\}} &= \sum_{i_1 \in [n_{\mathcal{V},k}+1:\mathsf{S}]} (-1)^{i_1 - n_{\mathcal{V},k} - 1} \mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i_1)\} \cup \{k\}} \\ &+ (-1)^{n_{\mathcal{V},k}+1} \mathbf{a}_{\mathcal{V}' \cup \{k\}} + \sum_{i_2 \in [2:n_{\mathcal{V},k}]} (-1)^{n_{\mathcal{V},k}+i_2} \mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i_2)\} \cup \{k\}}, \end{aligned} \tag{67a}$$

$$\begin{aligned} &\iff (-1)^{n_{\mathcal{V},k}} \mathbf{a}_{\mathcal{V}' \cup \{k\}} = \\ &\sum_{i_1 \in [n_{\mathcal{V},k}+1:\mathsf{S}]} (-1)^{i_1 - n_{\mathcal{V},k} - 1} \mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i_1)\} \cup \{k\}} \\ &+ \sum_{i_2 \in [2:n_{\mathcal{V},k}]} (-1)^{n_{\mathcal{V},k}+i_2} \mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i_2)\} \cup \{k\}} - \mathbf{a}_{\mathcal{V}' \cup \{1\}}, \end{aligned} \tag{67b}$$

$$\begin{aligned} &\iff \mathbf{a}_{\mathcal{V}' \cup \{k\}} = \sum_{i_2 \in [2:n_{\mathcal{V},k}]} (-1)^{i_2} \mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i_2)\} \cup \{k\}} \\ &+ (-1)^{n_{\mathcal{V},k}+1} \mathbf{a}_{\mathcal{V}' \cup \{1\}} + \sum_{i_1 \in [n_{\mathcal{V},k}+1:\mathsf{S}]} (-1)^{i_1 - 1} \mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i_1)\} \cup \{k\}}, \end{aligned} \tag{67c}$$

$$\begin{aligned} &\iff \mathbf{a}_{\mathcal{V}' \cup \{k\}} = \sum_{i_4 \in [1:n_{\mathcal{V},k}-1]} (-1)^{i_4 - 1} \mathbf{a}_{\mathcal{V} \cup \{k\} \setminus \{\mathcal{V}'(i_4)\}} \\ &+ (-1)^{n_{\mathcal{V},k}-1} \mathbf{a}_{\mathcal{V}' \cup \{1\}} + \sum_{i_3 \in [n_{\mathcal{V},k}:\mathsf{S}-1]} (-1)^{i_3} \mathbf{a}_{\mathcal{V} \cup \{k\} \setminus \{\mathcal{V}'(i_3)\}}, \end{aligned} \tag{67d}$$

where (67a) follows since $\mathcal{V}(1) = 1$ and (67d) follows since we let $i_3 = i_1 - 1$ and $i_4 = i_2 - 1$. It can be seen that (67d) can be derived by directly expanding $\mathbf{a}_{\mathcal{V}' \cup \{k\}}$ according to (25).

Finally, we consider the most involved case where $k \neq 1$ and $1 \notin \mathcal{V}$. We first expand the LHS of (26) as in (25); that is,

$$\mathbf{a}_{\mathcal{V}} = \sum_{i \in [\mathsf{S}]} (-1)^{i-1} \mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{1\}}. \tag{68}$$

Then for each $i \in [\mathsf{S}]$, we will show in the following that the RHS of (26) also contains the term $(-1)^{i-1} \mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{1\}}$. We also expand each term on the RHS of (26) by using (25). Note that $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{1\}}$ can only appear in $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{k\}}$. We consider two cases:

- $\mathcal{V}(i) > k$. The coefficient of $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{k\}}$ on the RHS of (26) is $(-1)^{i - n_{\mathcal{V},k} - 1}$. We expand $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{k\}}$ by using (25). Since the number of elements in $\mathcal{V}$ smaller than k is $n_{\mathcal{V},k}$ and $\mathcal{V}(i) > k$, the number of elements in $\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{k\}$ smaller than k is also $n_{\mathcal{V},k}$; thus by using (25), the coefficient of $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{1\}}$ in $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{k\}}$ is $(-1)^{n_{\mathcal{V},k}}$. Hence, the coefficient of $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{1\}}$ on the RHS of (26) is $(-1)^{i - n_{\mathcal{V},k} - 1} (-1)^{n_{\mathcal{V},k}} = (-1)^{i-1}$.
- $\mathcal{V}(i) < k$. The coefficient of $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{k\}}$ on the RHS of (26) is $(-1)^{n_{\mathcal{V},k} + i}$. We expand $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{k\}}$ by using (25). Since the number of elements in $\mathcal{V}$ smaller than k is $n_{\mathcal{V},k}$ and $\mathcal{V}(i) < k$, the number of elements in $\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{k\}$ smaller than k is $n_{\mathcal{V},k} - 1$; thus by using (25), the coefficient of $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{1\}}$ in $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{k\}}$ is $(-1)^{n_{\mathcal{V},k} - 1}$. Hence, the coefficient of $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{1\}}$ on the RHS of (26) is $(-1)^{n_{\mathcal{V},k} + i} (-1)^{n_{\mathcal{V},k} - 1} = (-1)^{i-1}$.

After expanding each $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{k\}}$ where $i \in [\mathsf{S}]$ on the RHS of (26) by using (25), the RHS of (26) may only contain $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i)\} \cup \{1\}}$ where $i \in [\mathsf{S}]$ and $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i'), \mathcal{V}(i'')\} \cup \{1,k\}}$ where $1 \leq i' < i'' \leq \mathsf{S}$. Next we will prove that the coefficient of each term $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i'), \mathcal{V}(i'')\} \cup \{1,k\}}$ where $1 \leq i' < i'' \leq \mathsf{S}$, is 0.

$\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i'), \mathcal{V}(i'')\} \cup \{1,k\}}$ appears in the expansions of $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i')\} \cup \{k\}}$ and $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i'')\} \cup \{k\}}$. We consider three cases:

- $\mathcal{V}(i') < \mathcal{V}(i'') < k$. The coefficient of $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i')\} \cup \{k\}}$ on the RHS of (26) is $(-1)^{n_{\mathcal{V},k} + i'}$; the coefficient of $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i'), \mathcal{V}(i'')\} \cup \{1,k\}}$ in the expansion of $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i')\} \cup \{k\}}$ is $(-1)^{i'' - 1 - 1} = (-1)^{i''}$, since the number of elements in $\mathcal{V} \setminus \{\mathcal{V}(i')\} \cup \{k\}$ smaller than $\mathcal{V}(i'')$ is $i'' - 1 - 1$. Similarly, the coefficient of $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i'')\} \cup \{k\}}$ on the RHS of (26) is $(-1)^{n_{\mathcal{V},k} + i''}$; the coefficient of $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i'), \mathcal{V}(i'')\} \cup \{1,k\}}$ in the expansion of $\mathbf{a}_{\mathcal{V} \setminus \{\mathcal{V}(i'')\} \cup \{k\}}$ is $(-1)^{i' - 1}$, since the number of elements in $\mathcal{V} \setminus \{\mathcal{V}(i'')\} \cup \{k\}$ smaller than $\mathcal{V}(i')$ is $i' - 1$. Hence, the coefficient of

[9] Without the constraint of uncoded groupwise keys, it was proved in [11, Theorem 2] that the total size of keys and the communication rates can simultaneously reach the minimum; i.e., there is no "tradeoff" between them. However, with the constraint of uncoded groupwise keys, the problem on the tradeoff among the total size of keys and the communication rates becomes more complicated. If the value S is not a fixed system parameter, the best scheme is to trivially let $\mathsf{S} = \mathsf{K}$ and thus this constraint of uncoded groupwise keys is actually meaningless (since we can directly use the scheme in [11]). So the non-trivial setting is that S is a fixed system parameter, as formulated in this paper, where we need to choose which of the keys $(Z_{\mathcal{V}} : \mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}})$ should be generated and then how to use them in the secure aggregation. Furthermore, for the optimal tradeoff among the storage cost and the communication rates, it remains open even without the constraint of uncoded groupwise keys.

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

$\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i'),\mathcal{V}(i'')\}\cup\{1,k\}}$ on the RHS of (26) is

$$(-1)^{n_{\mathcal{V},k}+i'}(-1)^{i''}+(-1)^{n_{\mathcal{V},k}+i''}(-1)^{i'-1}=0.$$

- $k<\mathcal{V}(i')<\mathcal{V}(i'')$. The coefficient of $\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i')\}\cup\{k\}}$ on the RHS of (26) is $(-1)^{i'-n_{\mathcal{V},k}-1}$; the coefficient of $\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i'),\mathcal{V}(i'')\}\cup\{1,k\}}$ in the expansion of $\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i')\}\cup\{k\}}$ is $(-1)^{i''-1}$, since the number of elements in $\mathcal{V}\setminus\{\mathcal{V}(i')\}\cup\{k\}$ smaller than $\mathcal{V}(i'')$ is $i''-1$. Similarly, the coefficient of $\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i'')\}\cup\{k\}}$ on the RHS of (26) is $(-1)^{i''-n_{\mathcal{V},k}-1}$; the coefficient of $\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i'),\mathcal{V}(i'')\}\cup\{1,k\}}$ in the expansion of $\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i'')\}\cup\{k\}}$ is $(-1)^{i'}$, since the number of elements in $\mathcal{V}\setminus\{\mathcal{V}(i'')\}\cup\{k\}$ smaller than $\mathcal{V}(i')$ is i'. Hence, the coefficient of $\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i'),\mathcal{V}(i'')\}\cup\{1,k\}}$ on the RHS of (26) is

$$(-1)^{i'-n_{\mathcal{V},k}-1}(-1)^{i''-1}+(-1)^{i''-n_{\mathcal{V},k}-1}(-1)^{i'}=0.$$

- $\mathcal{V}(i')<k<\mathcal{V}(i'')$. The coefficient of $\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i')\}\cup\{k\}}$ on the RHS of (26) is $(-1)^{n_{\mathcal{V},k}+i'}$; the coefficient of $\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i'),\mathcal{V}(i'')\}\cup\{1,k\}}$ in the expansion of $\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i')\}\cup\{k\}}$ is $(-1)^{i''-1}$, since the number of elements in $\mathcal{V}\setminus\{\mathcal{V}(i')\}\cup\{k\}$ smaller than $\mathcal{V}(i'')$ is $i''-1$. In addition, the coefficient of $\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i'')\}\cup\{k\}}$ on the RHS of (26) is $(-1)^{i''-n_{\mathcal{V},k}-1}$; the coefficient of $\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i'),\mathcal{V}(i'')\}\cup\{1,k\}}$ in the expansion of $\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i'')\}\cup\{k\}}$ is $(-1)^{i'-1}$, since the number of elements in $\mathcal{V}\setminus\{\mathcal{V}(i'')\}\cup\{k\}$ smaller than $\mathcal{V}(i')$ is $i'-1$. Hence, the coefficient of $\mathbf{a}_{\mathcal{V}\setminus\{\mathcal{V}(i'),\mathcal{V}(i'')\}\cup\{1,k\}}$ on the RHS of (26) is

$$(-1)^{n_{\mathcal{V},k}+i'}(-1)^{i''-1}+(-1)^{i''-n_{\mathcal{V},k}-1}(-1)^{i'-1}=0.$$

As a result, we proved (26).

Appendix B
Proof of Lemma 2

For each $k\in[\mathsf{K}]$, we want to prove that the matrix in (46), which is

$$\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}},\mathbf{a}_{\overline{\mathcal{S}}_{k,2}},\ldots,\mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}}\right], \tag{69}$$

has rank $\binom{\mathsf{K}-2}{\mathsf{S}-1}$ with high probability, where $\overline{\mathcal{S}}_{k,1},\overline{\mathcal{S}}_{k,2},\ldots,\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}$ denote the vectors $\mathcal{V}\in\binom{[\mathsf{K}]\setminus\{k\}}{\mathsf{S}}$.

We select one user $k'\in[\mathsf{K}]\setminus\{k\}$. Denote the sets $\mathcal{V}\in\binom{[\mathsf{K}]\setminus\{k\}}{\mathsf{S}}$ where $k'\in\mathcal{V}$ by $\overline{\mathcal{S}}_{k,k',1},\ldots,\overline{\mathcal{S}}_{k,k',\binom{\mathsf{K}-2}{\mathsf{S}-1}}$. It can be seen from Lemma 1 that, for each $\mathcal{V}\in\binom{[\mathsf{K}]\setminus\{k,k'\}}{\mathsf{S}}$ we can re-construct the vector $\mathbf{a}_{\mathcal{V}}$ by a linear combination of the vectors $\mathbf{a}_{\mathcal{V}\setminus\{k''\}\cup\{k'\}}$ where $k''\in\mathcal{V}$. Hence, all the vectors $\mathbf{a}_{\overline{\mathcal{S}}_{k,1}},\mathbf{a}_{\overline{\mathcal{S}}_{k,2}},\ldots,\mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}}$ are linear combinations of $\mathbf{a}_{\overline{\mathcal{S}}_{k,k',1}},\ldots,\mathbf{a}_{\overline{\mathcal{S}}_{k,k',\binom{\mathsf{K}-2}{\mathsf{S}-1}}}$. Hence, the rank of the matrix in (69) is equal to the rank of

$$\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,k',1}},\ldots,\mathbf{a}_{\overline{\mathcal{S}}_{k,k',\binom{\mathsf{K}-2}{\mathsf{S}-1}}}\right]. \tag{70}$$

By construction, all the vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$ are located in the linear space spanned by $\mathbf{a}_{\mathcal{V}_1}$ where $\mathcal{V}_1\in\binom{[\mathsf{K}]}{\mathsf{S}}$ and $1\in\mathcal{V}_1$. Since each vector $\mathbf{a}_{\mathcal{V}_1}$ where $\mathcal{V}_1\in\binom{[\mathsf{K}]}{\mathsf{S}}$ and $1\in\mathcal{V}_1$, is uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}^{\binom{\mathsf{K}-1}{\mathsf{S}-1}}$ with large enough q, the above linear space has dimension $\binom{\mathsf{K}-1}{\mathsf{S}-1}$ with high probability. In addition by Lemma 1, the vectors $\mathbf{a}_{\mathcal{V}_2}$ where $\mathcal{V}_2\in\binom{[\mathsf{K}]}{\mathsf{S}}$ and $k'\in\mathcal{V}_2$ can re-construct each vector in this $\binom{\mathsf{K}-1}{\mathsf{S}-1}$-dimensional linear space. Hence, the $\binom{\mathsf{K}-1}{\mathsf{S}-1}$ vectors $\mathcal{V}_2\in\binom{[\mathsf{K}]}{\mathsf{S}}$ and $k'\in\mathcal{V}_2$ are linearly independent with high probability. Hence, we proved that the matrix in (70) is full rank with high probability, with rank $\binom{\mathsf{K}-2}{\mathsf{S}-1}$. As a result, we proved that the rank of the matrix in (69) is $\binom{\mathsf{K}-2}{\mathsf{S}-1}$ with high probability.

Appendix C
Proof of (48)

We prove (48) by induction.

First consider the case $\mathsf{U}=1$. We need to prove

$$\binom{\mathsf{K}-2}{\mathsf{S}-2}\geq\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-2}{\mathsf{S}-1}, \tag{71}$$

which directly holds from Pascal's triangle $\binom{\mathsf{K}-2}{\mathsf{S}-2}=\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-2}{\mathsf{S}-1}$.

Then for any $\mathsf{U}\in[i]$, we assume that

$$i\binom{\mathsf{K}-2}{\mathsf{S}-2}\geq\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-i}{\mathsf{S}-1} \tag{72}$$

holds, and will prove

$$(i+1)\binom{\mathsf{K}-2}{\mathsf{S}-2}\geq\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-i-2}{\mathsf{S}-1}. \tag{73}$$

Note that

$$\binom{\mathsf{K}-2}{\mathsf{S}-2}>\binom{\mathsf{K}-i-2}{\mathsf{S}-2}=\binom{\mathsf{K}-i-1}{\mathsf{S}-1}-\binom{\mathsf{K}-i-2}{\mathsf{S}-1}. \tag{74}$$

By summing (72) and (74), we can prove (73).

Appendix D
Proof of Lemma 3

Consider one set $\mathcal{U}_2\subseteq[\mathsf{K}]$ where $|\mathcal{U}_2|=\mathsf{U}$. We want to prove that the matrix in (45) with dimension $\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1}\times\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1}$ is full rank with high probability; i.e., the determinant of the matrix in (45) is not zero with high probability. Note that the determinant could be written as $D_{\mathcal{A}}=\frac{P_{\mathcal{A}}}{Q_{\mathcal{A}}}$. $P_{\mathcal{A}}$ and $Q_{\mathcal{A}}$ are multivariate polynomials whose variables are the elements in $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}},1\in\mathcal{V}$ and the coefficients in the $\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}$ random linear combinations of the rows in $\mathbf{S}'_k$ for each $k\in\mathcal{U}_2$. Since the matrix in (45) exists with high probability by Lemma 2 and (48), $Q_{\mathcal{A}}$ is not zero with high probability. Hence, it remains to prove that $P_{\mathcal{A}}$ is not zero with high probability neither. Since the variables in $P_{\mathcal{A}}$ are uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}$ where q is large enough, by the Schwartz-Zippel Lemma [32]–[34], if the multivariate polynomial $P_{\mathcal{A}}$ is non-zero (i.e., a multivariate polynomial whose coefficients are not all 0), the probability that $P_{\mathcal{A}}$ is equal to 0 over all possible realizations of variables goes to 0 when q goes to infinity, and thus the matrix in (45) is full rank with high probability. So in the following, we need to show that $P_{\mathcal{A}}$ is a non-zero polynomial; i.e., we want to find out one realization of the variables in $P_{\mathcal{A}}$, such that the matrix

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

in (45) exists and is full rank (in this way, $P_{\mathcal{A}} = D_{\mathcal{A}} Q_{\mathcal{A}}$ is not zero).

We pick one integer $u \in [\mathsf{K}] \setminus \mathcal{U}_2$. We first select the elements in $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}, 1 \in \mathcal{V}$. Note that the dimension of $\mathbf{a}_{\mathcal{V}}$ is $\binom{\mathsf{K}-1}{\mathsf{S}-1}$. We want to let $[\mathbf{a}_{\mathcal{V}} : \mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}, u \in \mathcal{V}]$ be an identity matrix with dimension $\binom{\mathsf{K}-1}{\mathsf{S}-1} \times \binom{\mathsf{K}-1}{\mathsf{S}-1}$. More precisely, we define a collection of sets $\mathcal{C}_1 = \left\{\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}} : u \in \mathcal{V}, \mathcal{V} \cap \mathcal{U}_2 \neq \emptyset\right\}$ and sort its sets as $\mathcal{C}_{1,1}, \ldots, \mathcal{C}_{1,\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}$. Let

$$\mathbf{a}_{\mathcal{C}_{1,i}} = \mathbf{e}_{\binom{\mathsf{K}-1}{\mathsf{S}-1},i}, \ \forall i \in \left[\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}\right]. \quad (75)$$

In addition, we also define a collection of sets $\mathcal{C}_2 = \left\{\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}} : u \in \mathcal{V}, \mathcal{V} \cap \mathcal{U}_2 = \emptyset\right\}$ and sort its sets as $\mathcal{C}_{2,1}, \ldots, \mathcal{C}_{2,\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}$. Let

$$\mathbf{a}_{\mathcal{C}_{2,i}} = \mathbf{e}_{\binom{\mathsf{K}-1}{\mathsf{S}-1},\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}+i}, \ \forall i \in \left[\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}\right]. \quad (76)$$

There must exist a selection of $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}, 1 \in \mathcal{V}$ which leads (75) and (76). This is because by Lemma 1, we can obtain $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}, 1 \in \mathcal{V}$ from the vectors $\mathbf{a}_{\mathcal{V}'}$ where $\mathcal{V}' \in \binom{[\mathsf{K}]}{\mathsf{S}}, u \in \mathcal{V}$. Hence, those resulting vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}, 1 \in \mathcal{V}$ can in turn lead (75) and (76).

Focus on each user $k \in \mathcal{U}_2$. Recall that the sets in $\binom{[\mathsf{K}]\setminus\{k\}}{\mathsf{S}}$ are denoted by $\overline{\mathcal{S}}_{k,1}, \ldots, \overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}$. By Lemma 1, $\mathbf{a}_{\overline{\mathcal{S}}_{k,1}}, \mathbf{a}_{\overline{\mathcal{S}}_{k,2}}, \ldots, \mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}}$ are in the linear space spanned by $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]\setminus\{k\}}{\mathsf{S}}$ and $u \in \mathcal{V}$. Hence, the rank of the matrix $[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}}, \mathbf{a}_{\overline{\mathcal{S}}_{k,2}}, \ldots, \mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}}]$ is $\binom{\mathsf{K}-2}{\mathsf{S}-1}$; thus this matrix with dimension $\binom{\mathsf{K}-1}{\mathsf{S}-1} \times \binom{\mathsf{K}-1}{\mathsf{S}}$ contains $\binom{\mathsf{K}-2}{\mathsf{S}-2}$ linearly independent left null vectors, which are $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ and $\{u, k\} \subseteq \mathcal{V}$. Let $\mathbf{s}_{k,1}, \ldots, \mathbf{s}_{k,\binom{\mathsf{K}-2}{\mathsf{S}-2}}$ be these $\binom{\mathsf{K}-2}{\mathsf{S}-2}$ vectors, we can obtain $\mathbf{S}'_k$ in (47). Since $\mathbf{S}'_k$ exists, $\mathbf{S}_k$, which are $\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}$ random linear combinations of the rows in $\mathbf{S}'_k$, also exists and thus the matrix in (45) exists.

Let us then select the coefficients in the $\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}$ random linear combinations of the $\mathsf{U}\binom{\mathsf{K}-2}{\mathsf{S}-2}$ rows in $\mathbf{S}'_k$ for each $k \in \mathcal{U}_2$. More precisely, we directly select $\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}$ rows from $\mathbf{S}'_k$ to compose $\mathbf{S}_k$; i.e., in each linear combination, the coefficient vector contains $\mathsf{U}\binom{\mathsf{K}-2}{\mathsf{S}-2} - 1$ zeros and 1 one. This is possible because of (48). Hence, $\mathbf{S}_k$ contains $\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}$ unit vectors, where these vectors are selected from $\mathbf{e}_{\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1},j\binom{\mathsf{K}-1}{\mathsf{S}-1}+i}$, for all $j \in [0 : \mathsf{U}-1]$, $i \in \left[\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}\right]$, and $k \in \mathcal{C}_{1,i}$, totally $\mathsf{U}\binom{\mathsf{K}-2}{\mathsf{S}-2}$ unit vectors. Recall that the users in $\mathcal{U}_2$ are denoted by $\mathcal{U}_2(1), \ldots, \mathcal{U}_2(\mathsf{U})$, where $\mathcal{U}_2(1) < \cdots < \mathcal{U}_2(\mathsf{U})$. Our objective on the selection is that the $\mathsf{U}\left(\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}\right)$ rows in $\begin{bmatrix}\mathbf{S}_{\mathcal{U}_2(1)} \\ \vdots \\ \mathbf{S}_{\mathcal{U}_2(\mathsf{U})}\end{bmatrix}$ are exactly $\mathbf{e}_{\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1},j\binom{\mathsf{K}-1}{\mathsf{S}-1}+i}$, where $j \in [0 : \mathsf{U}-1]$ and $i \in \left[\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}\right]$; thus the matrix in (45) is an identity matrix (with some row permutation) and is full rank.

The existence of the above selection is equivalent to the following combinatorial problem:

(p1). There are $\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}$ urns, where each urn is with the index $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ where $\mathcal{U}_2 \cap \mathcal{V} \neq \emptyset$ and $u \in \mathcal{V}$. There are U colors of balls, where the number of balls for each color with index $k \in \mathcal{U}_2$ is $\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}$. A ball with color k can be only put into an urn with index $\mathcal{V}$ where $k \in \mathcal{V}$. We want to put the balls into the urns such that each urn contains U balls (not necessarily with the different colors).

If there exists a solution for Problem (p1), we can treat each color as one user in our problem and each urn as a set in $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ where $\mathcal{U}_2 \cap \mathcal{V} \neq \emptyset$ and $u \in \mathcal{V}$. Assume the urn with index $\mathcal{V}$ contains x_1 balls with color k_1, x_2 balls with color k_2, etc. Then for user k_1, we select $\mathbf{e}_{\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1},j\binom{\mathsf{K}-1}{\mathsf{S}-1}+i}$ where $j \in [k_1]$ and $\mathcal{C}_{1,i} = \mathcal{V}$ and put them into $\mathbf{S}_{k_1}$; for user k_2, we select $\mathbf{e}_{\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1},j\binom{\mathsf{K}-1}{\mathsf{S}-1}+i}$ where $j \in [k_1+1 : k_2]$ and $\mathcal{C}_{1,i} = \mathcal{V}$ and put them into $\mathbf{S}_{k_2}$, etc. Thus we can see that from the solution for Problem (p1), we can design the selection of the coefficients satisfying the matrix in (45) is full rank.

At the end of this section, we provide one solution for Problem (p1), which is based the Pascal's triangle

$$\begin{aligned}&\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1} \\ &= \binom{\mathsf{K}-2}{\mathsf{S}-2} + \binom{\mathsf{K}-3}{\mathsf{S}-2} + \cdots + \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-2}. \end{aligned} \quad (77)$$

Let us focus on the $\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}$ balls in color $k \in \mathcal{U}_2$, and put these balls into urns by the following U step:

Step $t \in [\mathsf{U}]$. We put one ball in color k into each urn with index $\mathcal{V}$ where $\mathcal{V} \in \binom{[\mathsf{K}]\setminus\{\mathcal{U}_2(<k+1>_{\mathsf{U}}), \mathcal{U}_2(<k+2>_{\mathsf{U}}), \ldots, \mathcal{U}_2(<k+t-1>_{\mathsf{U}})\}}{\mathsf{S}}$, $\mathcal{U}_2 \cap \mathcal{V} \neq \emptyset$, and $\{u, k\} \subseteq \mathcal{V}$. Thus in this step, we have put $\binom{\mathsf{K}-1-t}{\mathsf{S}-2}$ balls in color k into urns.

Hence, by the Pascal's triangle in (77), consider all the U steps for the balls in color k, we have put all the $\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}$ balls in color k into urns.

Let us then show that after considering the balls in all colors, each urn has exactly U balls. Consider an urn with index $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ where $\mathcal{U}_2 \cap \mathcal{V} \neq \emptyset$ and $u \in \mathcal{V}$. Assume that $\mathcal{U}_2 \cap \mathcal{V} = \mathcal{B} = \{\mathcal{U}_2(i_1), \mathcal{U}_2(i_2), \ldots, \mathcal{U}_2(i_{|\mathcal{B}|})\}$, where $i_1 < i_2 < \cdots < i_{|\mathcal{B}|}$. We consider two cases:

- $|\mathcal{B}| = 1$. By construction, in each of the U steps for color $\mathcal{B}(1)$, we put one ball in color $\mathcal{B}(1)$ into the urn with index $\mathcal{V}$. Hence, this urn totally contains U balls.
- $|\mathcal{B}| > 1$. By construction, for each $s \in [|\mathcal{B}|]$, in each of the first $< i_{<s+1>_{|\mathcal{B}|}} - i_s >_{\mathsf{U}}$ steps for color $\mathcal{U}_2(s)$, we put one ball in color $\mathcal{U}_2(s)$ into the urn with index $\mathcal{V}$. Hence, considering all $s \in [|\mathcal{B}|]$, the number of balls in this urn is

$$\begin{aligned}&< i_2 - i_1 >_{\mathsf{U}} + < i_3 - i_2 >_{\mathsf{U}} + \cdots + \\ &< i_{|\mathcal{B}|} - i_{|\mathcal{B}|-1} >_{\mathsf{U}} + < i_1 - i_{|\mathcal{B}|} >_{\mathsf{U}} \\ &= i_{|\mathcal{B}|} - i_1 + < i_1 - i_{|\mathcal{B}|} >_{\mathsf{U}} \\ &= \mathsf{U}.\end{aligned}$$

As a result, we proved that each urn has exactly U balls. Thus the proposed solution is indeed a solution for Problem (p1).

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

Hence, we showed that $P(\mathcal{A})$ is a non-zero polynomial and proved Lemma 3.

Appendix E
Proof of Lemma 4

Recall that we have shown in Section V that the proposed scheme satisfies that

$$\left[\mathbf{a}_{\mathcal{S}_{k,1}},\ldots,\mathbf{a}_{\mathcal{S}_{k,\binom{\mathsf{K}-1}{\mathsf{S}-1}}}\right] \text{ has rank equal to } \binom{\mathsf{K}-1}{\mathsf{S}-1}, \quad (78)$$

for each $k\in[\mathsf{K}]$, and recall that each $\mathbf{a}_{\mathcal{S}_{k,j}}$ where $j\in[\binom{\mathsf{K}-1}{\mathsf{S}-1}]$ is a $\binom{\mathsf{K}-1}{\mathsf{S}-1}$-dimensional column-wise vector. Then for each $k\in[\mathsf{K}]$, we have (79) at the top of the next page, where (79c) follows since the keys and input vectors are independently, and (79d) follows since the proposed schemes satisfies the constraint in (78) and each sub-key $Z_{\mathcal{S}_{k,i},k}$ where $i\in[\binom{\mathsf{K}-1}{\mathsf{S}-1}]$ contains $\frac{\mathsf{L}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}$ uniformly i.i.d. symbols on $\mathbb{F}_{\mathsf{q}}$. Hence, we have

$$I(X_k;W_k)=H(X_k)-H(X_k|W_k) \quad (80a)$$

$$=\frac{\binom{\mathsf{K}-1}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}\mathsf{L}-\frac{\binom{\mathsf{K}-1}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}\mathsf{L}=0. \quad (80b)$$

By (80b), we have

$$I(X_1,\ldots,X_{\mathsf{K}};W_1,\ldots,W_{\mathsf{K}})$$
$$=I(X_1;W_1)+I(X_2;W_2)+\cdots+I(X_{\mathsf{K}};W_{\mathsf{K}}) \quad (81a)$$
$$=0, \quad (81b)$$

where (81a) follows since the keys and input vectors are mutually independent and $X_1,\ldots,X_{\mathsf{K}}$ use different sub-keys. In other words, (81b) shows that in the proposed scheme $(X_1,\ldots,X_{\mathsf{K}})$ and $(W_1,\ldots,W_{\mathsf{K}})$ are independent; thus we also have

$$0=I\left(X_1,\ldots,X_{\mathsf{K}};W_1,\ldots,W_{\mathsf{K}},\sum_{k\in\mathcal{U}_1}W_k\right) \quad (82a)$$

$$=I\left(X_1,\ldots,X_{\mathsf{K}};W_1,\ldots,W_{\mathsf{K}}\Big|\sum_{k\in\mathcal{U}_1}W_k\right). \quad (82b)$$

Considering all transmissions which may be received by the server, we have

$$I\left(W_1,\ldots,W_{\mathsf{K}};X_1,\ldots,X_{\mathsf{K}},(Y_k^{\mathcal{U}_1}:k\in\mathcal{U}_1)\Big|\sum_{k\in\mathcal{U}_1}W_k\right)$$
$$=I\left(W_1,\ldots,W_{\mathsf{K}};(Y_k^{\mathcal{U}_1}:k\in\mathcal{U}_1)\Big|\sum_{k\in\mathcal{U}_1}W_k,X_1,\ldots,X_{\mathsf{K}}\right) \quad (83a)$$
$$\le I\left(W_1,\ldots,W_{\mathsf{K}};F_1,\ldots,F_{\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1}}\Big|\sum_{k\in\mathcal{U}_1}W_k,X_1,\ldots,X_{\mathsf{K}}\right) \quad (83b)$$
$$=0, \quad (83c)$$

where (83a) comes from (82b), (83b) follows since $(Y_k^{\mathcal{U}_1}:k\in\mathcal{U}_1)$ are linear combinations of $F_1,\ldots,F_{\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1}}$, and (83c) follows since by our construction $F_1,\ldots,F_{\mathsf{U}\binom{\mathsf{K}-1}{\mathsf{S}-1}}$ can be recovered from $\sum_{k\in\mathcal{U}_1}W_k$ and $\sum_{k\in\mathcal{U}_1}X_k$. Hence, we prove that the proposed scheme satisfies the security constraint in (7).

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] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, no. 2, p. 12, 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.

[4] H. B. McMahan *et al.*, "Advances and open problems in federated learning," *Foundations and Trends® in Machine Learning*, vol. 14, no. 1, 2021.

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

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

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

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

[9] Z. Liu, J. Guo, K. Y. Lam, and J. Zhao, "Efficient dropout-resilient aggregation for privacy-preserving machine learning," *IEEE Trans. on Information Forensics and Security*, vol. 18, pp. 1839–1854, 2023.

[10] A. R. Elkordy and A. S. Avestimehr, "Heterosag: Secure aggregation with heterogeneous quantization in federated learning," *IEEE Transactions on Communications*, vol. 70, no. 4, pp. 2372–2386, 2022.

[11] 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.

[12] J. So, B. Güler, and A. S. Avestimehr, "Turbo-aggregate: Breaking the quadratic aggregation barrier in secure federated learning," *IEEE Journal on Selected Areas in Info. Theory*, vol. 2, no. 1, pp. 479–489, 2021.

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

[14] T. Jahani-Nezhad, M. A. Maddah-Ali, S. Li, and G. Caire, "SwiftAgg+: Achieving asymptotically optimal communication load in secure aggregation for federated learning," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 4, pp. 977–989, Apr. 2023.

[15] X. Yang, Z. Liu, X. Tang, R. Lu, and B. Liu, "An efficient and multi-private key secure aggregation for federated learning," *arXiv:2306.08970*, Jun. 2023.

[16] 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.

[17] 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.

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

[19] 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.

[20] Z. Li, Y. Zhao, and H. Sun, "Weakly secure summation with colluding users," *arXiv:2304.09771*, Apr. 2023.

[21] 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.

[22] H. U. Sami and B. Güler, "Secure aggregation for clustered federated learning," *in IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 186–191, Jul. 2023.

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

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

$$H(X_k|W_k) = H\Bigg(\Big(W_{k,j} + \sum_{i\in[\binom{\mathsf{K}-1}{\mathsf{S}-1}]} a_{\mathcal{S}_{k,i},j} Z_{\mathcal{S}_{k,i},k} : j \in \Big[\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}\Big]\Big),$$

$$\Big(\sum_{i\in[\binom{\mathsf{K}-1}{\mathsf{S}-1}]} a_{\mathcal{S}_{k,i},j} Z_{\mathcal{S}_{k,i},k} : j \in \Big[\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1} + 1 : \binom{\mathsf{K}-1}{\mathsf{S}-1}\Big]\Big)\Big| W_{k,1}, \ldots, W_{k,\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}\Bigg) \tag{79a}$$

$$= H\left(\Big(\sum_{i\in[\binom{\mathsf{K}-1}{\mathsf{S}-1}]} a_{\mathcal{S}_{k,i},j} Z_{\mathcal{S}_{k,i},k} : j \in \Big[\binom{\mathsf{K}-1}{\mathsf{S}-1}\Big]\Big)\Big| W_{k,1}, \ldots, W_{k,\binom{\mathsf{K}-1}{\mathsf{S}-1}-\binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}\right) \tag{79b}$$

$$= H\left(\Big(\sum_{i\in[\binom{\mathsf{K}-1}{\mathsf{S}-1}]} a_{\mathcal{S}_{k,i},j} Z_{\mathcal{S}_{k,i},k} : j \in \Big[\binom{\mathsf{K}-1}{\mathsf{S}-1}\Big]\Big)\right) \tag{79c}$$

$$= \frac{\binom{\mathsf{K}-1}{\mathsf{S}-1}}{\binom{\mathsf{K}-1}{\mathsf{S}-1} - \binom{\mathsf{K}-1-\mathsf{U}}{\mathsf{S}-1}}\mathsf{L}, \tag{79d}$$

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

[25] 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.

[26] 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.

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

[28] 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.

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

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

[31] ——, "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.

[32] J. T. Schwartz, "Fast probabilistic algorithms for verification of polynomial identities," *Journal of the ACM (JACM)*, vol. 27, no. 4, pp. 701–717, 1980.

[33] R. Zippel, "Probabilistic algorithms for sparse polynomials," in *International symposium on symbolic and algebraic manipulation*. Springer, 1979, pp. 216–226.

[34] R. A. Demillo and R. J. Lipton, "A probabilistic remark on algebraic program testing," *Information Processing Letters*, vol. 7, no. 4, pp. 193–195, 1978.

Kai Wan (S '15 – M '18) received the B.E. degree in Optoelectronics from Huazhong University of Science and Technology, China, in 2012, the M.Sc. and Ph.D. degrees in Communications from Université Paris-Saclay, France, in 2014 and 2018. He subsequently was a post-doctoral researcher with the Communications and Information Theory Chair (CommIT) at Technische Universität Berlin, Berlin, Germany. He is now a Professor with the School of Electronic Information and Communications, Huazhong University of Science and Technology. His research interests include information theory, coding techniques, and their applications on coded caching, index coding, distributed storage, distributed computing, wireless communications, privacy and security. He received the Best Young Scientist Award in the 8th International Conference on Computer and Communication Systems, 2023. He has served as an Associate Editors for IEEE Transactions on Communications since Mar. 2024 and IEEE Communications Letters since Aug. 2021.

Hua Sun (S '12 – M '17) received the B.E. degree in Communications Engineering from Beijing University of Posts and Telecommunications, China, in 2011, and the M.S. and Ph.D. degrees in Electrical and Computer Engineering from University of California Irvine, USA, in 2013 and 2017, respectively. He is an Associate Professor in the Department of Electrical Engineering at the University of North Texas, USA. His research interests include information theory and its applications to communications, privacy, security, and storage.

Dr. Sun is a recipient of the NSF CAREER award in 2021, the UNT College of Engineering Junior Faculty Research Award in 2021, and the UNT College of Engineering Distinguished Faculty Fellowship in 2023. His co-authored papers received the IEEE Jack Keil Wolf ISIT Student Paper Award in 2016, an IEEE GLOBECOM Best Paper Award in 2016, and the 2020-2021 IEEE Data Storage Best Student Paper Award.

Mingyue Ji (S '09 – M '15) received the Ph.D. degree from the Ming Hsieh Department of Electrical and Computer Engineering at the University of Southern California in 2015, where he received the USC Annenberg Fellowship from 2010 to 2014. He subsequently was a Staff II System Design Scientist with Broadcom Inc. from 2015 to 2016. He is currently an Associate Professor in the Department of Electrical and Computer Engineering and an Adjunct Associate Professor in the Kahlert School of Computing at the University of Utah. His research interests span a broad spectrum, including cloud and edge computing, distributed machine learning, and 5G and beyond wireless communications, networking, and sensing. Mingyue Ji's research activities cover fundamental theory study, algorithm design and analysis, and practical system implementation and experimentation. He received the NSF CAREER Award in 2022, the IEEE Communications Society Leonard G. Abraham Prize for the Best IEEE Journal on Selected Areas in Communications (JSAC) Paper in 2019, the Best Paper Awards at 2021 IEEE GLOBECOM Conference, 2015 IEEE ICC Conference and 2024 IEEE ISICN Conference, the Best Student Paper Award at 2010 IEEE European Wireless Conference, the 2022 Outstanding ECE Teaching Award and the 2023 Outstanding ECE Research Award at the University of Utah. He has been serving as Associate Editors for IEEE Transactions on Information Theory since 2022 and IEEE Transactions on Communications since 2020.

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3393740

Tiebin Mi (Member, IEEE) received the B.E. degree in computer science from Xidian University, China, in 2002, and the Ph.D. degree in electrical engineering from the Institute of Acoustics, Chinese Academy of Sciences, China, in 2010. Currently, he holds the position of a Lecturer (Assistant Professor) at the School of Electronic Information and Communications, Huazhong University of Science and Technology, China. His research interests include wireless communications, high-dimensional signal processing, random matrix theory, and reconfigurable intelligent surfaces.

Giuseppe Caire (S '92 – M '94 – SM '03 – F '05) was born in Torino in 1965. He received the B.Sc. in Electrical Engineering from Politecnico di Torino in 1990, the M.Sc. in Electrical Engineering from Princeton University in 1992, and the Ph.D. from Politecnico di Torino in 1994. He has been a post-doctoral research fellow with the European Space Agency (ESTEC, Noordwijk, The Netherlands) in 1994-1995, Assistant Professor in Telecommunications at the Politecnico di Torino, Associate Professor at the University of Parma, Italy, Professor with the Department of Mobile Communications at the Eurecom Institute, Sophia-Antipolis, France, a Professor of Electrical Engineering with the Viterbi School of Engineering, University of Southern California, Los Angeles, and he is currently an Alexander von Humboldt Professor with the Faculty of Electrical Engineering and Computer Science at the Technical University of Berlin, Germany.

He received the Jack Neubauer Best System Paper Award from the IEEE Vehicular Technology Society in 2003, the IEEE Communications Society and Information Theory Society Joint Paper Award in 2004 and in 2011, the Okawa Research Award in 2006, the Alexander von Humboldt Professorship in 2014, the Vodafone Innovation Prize in 2015, an ERC Advanced Grant in 2018, the Leonard G. Abraham Prize for best IEEE JSAC paper in 2019, the IEEE Communications Society Edwin Howard Armstrong Achievement Award in 2020, and he is a recipient of the 2021 Leibinz Prize of the German National Science Foundation (DFG). Giuseppe Caire is a Fellow of IEEE since 2005. He has served in the Board of Governors of the IEEE Information Theory Society from 2004 to 2007, and as officer from 2008 to 2013. He was President of the IEEE Information Theory Society in 2011. His main research interests are in the field of communications theory, information theory, channel and source coding with particular focus on wireless communications.

Authorized licensed use limited to: The University of Utah. Downloaded on July 30,2024 at 03:01:43 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.