On the Information Theoretic Secure Aggregation with Uncoded Groupwise Keys

Kai Wan, *Member, IEEE,* Xin Yao, Hua Sun, *Member, IEEE,* Mingyue Ji, *Member, IEEE,* and Giuseppe Caire, *Fellow, IEEE*

***Abstract*—Secure aggregation, which is a core component of federated learning, aggregates locally trained models from distributed users at a central server. The "secure" nature of such aggregation consists of the fact that no information about the local users' data must be leaked to the server except the aggregated local models. In order to guarantee security, some keys may be shared among the users (this is referred to as the key sharing phase). After the key sharing phase, each user masks its trained model which is then sent to the server (this is referred to as the model aggregation phase). This paper follows the information theoretic secure aggregation problem originally formulated by Zhao and Sun, with the objective to characterize the minimum communication cost from the K users in the model aggregation phase. Due to user dropouts, which are common in real systems, the server may not receive all messages from the users. A secure aggregation scheme should tolerate the dropouts of at most $\mathsf{K}-\mathsf{U}$ users, where U is a system parameter. The optimal communication cost is characterized by Zhao and Sun, but with the assumption that the keys stored by the users could be any random variables with arbitrary dependency. On the motivation that uncoded groupwise keys are more convenient to be shared and could be used in large range of applications besides federated learning, in this paper we add one constraint into the above problem, namely, that the key variables are mutually independent and each key is shared by a group of S users, where S is another system parameter. To the best of our knowledge, all existing secure aggregation schemes (with information theoretic security or computational security) assign coded keys to the users. We show that if $\mathsf{S}>\mathsf{K}-\mathsf{U}$, a new secure aggregation scheme with uncoded groupwise keys can achieve the same optimal communication cost as the best scheme with coded keys; if $\mathsf{S}\leq\mathsf{K}-\mathsf{U}$, uncoded groupwise key sharing is strictly sub-optimal. Finally, we also implement our proposed secure aggregation scheme into Amazon EC2, which are then compared with the existing secure aggregation schemes with offline key sharing.**

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

A short version of this paper was presented at the 2023 IEEE International Conference on Communications [1].

K. Wan was with the Electrical Engineering and Computer Science Department, Technische Universität Berlin, 10587 Berlin, Germany. He is now with the School of Electronic Information and Communications, Huazhong University of Science and Technology, 430074 Wuhan, China, (e-mail: kai_wan@hust.edu.cn). The work of K. Wan was partially funded by the National Natural Science Foundation of China (NSFC-12141107) and the CCF-Hikvision Open Fund (20210008).

X. Yao and M. Ji are with the Electrical and Computer Engineering Department, University of Utah, Salt Lake City, UT 84112, USA (e-mail: Xin.Yao@utah.edu; mingyue.ji@utah.edu). The work of X. Yao and 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

Federated learning is essentially a distributed machine learning framework, where a central server aims to solve a machine learning problem by the help of distributed users with local data [2]–[5]. A notable advantage of federated learning compared to other distributed learning scenarios, is the security protection on the users' raw local data against the server. Instead of asking the users to directly upload the raw data, federated learning lets each user compute the model updates using its local data and securely aggregates these updates at the server (secure aggregation). In this paper, we use information theoretic tools to focus on two core challenges of the secure aggregation process in federated learning, namely the effect of user dropouts and the communication efficiency [4]. First, in a real environment some users may drop or reply slowly during the training process due to the network connectivity or computational capability. It is non-trivial to let the server recover the aggregated updated models of the surviving users securely while mitigating the effect of potential user dropouts. Second, additional communication among the users and server may be needed to guarantee the perfect security and mitigate the effect of the user dropouts, for example, additional communications on exchanging the keys among the users may be taken. Since a federated learning system usually contains of a massive number of devices, the minimization of the communication cost is crucial.

The secure aggregation problem with user dropouts was originally considered in [6], and generally contains two phases: *offline key sharing* and *model aggregation*, where the user dropouts may happen in either phase or both phases. In the first phase, K users generate random seeds, and secretly share their private random seeds such that some keys are shared among the users. The offline key sharing phase is independent of the users' local training data, and thus can take place during off-peak traffic times when the network is not busy. For example, the secure aggregation schemes in [6]–[10] all make use of offline key sharing protocols.[1] If there is no

[1]Online key sharing protocols (for example the ones proposed in [11]–[13]) which are beyond the scope of this paper, allow users to communicate some information about the updated models and keys among each other, while in offline protocols users can only share keys.

private link among users, the communication among users should go through the central server, and some key agreement protocol such as [14] is needed, whereby two or more parties can agree on a key by communicating some local information through a public link, such that even if some eavesdropper can observe the communication in the public link, it cannot determine the shared key. Once the keys are shared among the users, in the model aggregation phase the users mask the updated models by the keys; then send masked models and masks to the server through multiple rounds. When the server receives the transmissions of a threshold number of users, the server should recover the aggregated updated models of these users without getting any other information about the users' local data, such that the effect of user dropouts could be resolved. The secure aggregation protocol in [6] uses the pairwise offline key sharing based on Diffie-Hellman key agreement [14] between each two users, where each key is then shared to all other users through Shamir's secret sharing [15] in order to deal with user dropouts. By relaxing the resilience on the worst-case dropouts, secure aggregation schemes with probabilistic dropout-resiliency guarantee were proposed in [7], [8], where the number of required keys is further reduced compared to the one in [6]. Following the secure aggregation problem with user dropouts in [6], several works have developed more efficient and/or more secure schemes for aggregation, for example, by using common seeds through homomorphic pseudorandom generator [16], secure multi-party computing [17], non-pairwise keys [9], online key sharing [11]–[13], improved El Gamal encryption [18]. The readers can refer to the survey for more details [19], [20].

Recently, the authors in [9] proposed an information theoretic formulation of the secure aggregation problem with user dropouts originally considered in [6], whose objective is to characterize the fundamental limits of the communication cost while preserving the information theoretic security of the users' local data.[2] Due to the difficulty to characterize the fundamental limits of the communication rates in both two phases, with the assumption that the key sharing phase has been already performed during network off-traffic times and any keys with arbitrary dependency could be used in the model aggregation phase (i.e., we only consider the model aggregation phase and ignore the cost of the key sharing phase), the authors in [9] formulated a (K,U) two-round information theoretic secure aggregation problem for the server-users communication model, where K represents the number of users, U represents the minimum number of surviving users.[3] Each user can communicate with the server while the communication among users is not allowed. The server aims to compute the element-wise sum of the vector inputs (i.e., updated models) of K users, where the input vector of user k is denoted by W_k and contains L uniform and i.i.d. symbols over a finite field $\mathbb{F}_{\mathsf{q}}$.[4] Each user k has stored a key Z_k, which can be any random variable independent of $W_1,\ldots,W_{\mathsf{K}}$. The transmissions (in the model aggregation phase) contains two rounds.[5] In the first round of transmission, each user $k\in\{1,\ldots,\mathsf{K}\}$ sends a coded message X_k as a function of W_k and Z_k to the server. Since some users may drop during its transmission, the server only receives the messages from the users in $\mathcal{U}_1$ where $|\mathcal{U}_1|\geq\mathsf{U}$. Then the server informs the users in the subset $\mathcal{U}_1$ of non-dropped users. In the second round of transmission, after knowing the set $\mathcal{U}_1$, each user $k\in\mathcal{U}_1$ transmits another coded message $Y_k^{\mathcal{U}_1}$ as a function of $(W_k,Z_k,\mathcal{U}_1)$ to the server. Due to the user dropouts in the second round, letting $\mathcal{U}_2$ denote the set of surviving users in the second round with $\mathcal{U}_2\subseteq\mathcal{U}_1$ and $|\mathcal{U}_2|\geq\mathsf{U}$, the server receives $Y_k^{\mathcal{U}_1}$ where $k\in\mathcal{U}_2$. By receiving $(X_k:k\in\mathcal{U}_1)$ and $(Y_k^{\mathcal{U}_1}:k\in\mathcal{U}_2)$, the server should recover the element-wise sum $\sum_{k\in\mathcal{U}_1}W_k$ without getting any other information about $W_1,\ldots,W_{\mathsf{K}}$ even if the server can receive $(X_k:k\in[\mathsf{K}]\backslash\mathcal{U}_1)$, $(Y_k^{\mathcal{U}_1}:k\in\mathcal{U}_1\backslash\mathcal{U}_2)$ (e.g., the users are not really dropped but too slow in the transmission). Since the identity of the dropped users in each round is not known a priori by the users unless they receive the list of surviving users from the server, we should design $(X_k:k\in\{1,\ldots,\mathsf{K}\})$ and $(Y_k^{\mathcal{U}_1}:k\in\mathcal{U}_1)$ for any sets $\mathcal{U}_1,\mathcal{U}_2$ where $\mathcal{U}_2\subseteq\mathcal{U}_1\subseteq\{1,\ldots,\mathsf{K}\}$ and $|\mathcal{U}_1|\geq|\mathcal{U}_2|\geq\mathsf{U}$, while minimizing the communication rates by the users in two rounds. It was shown in [9] that the minimum numbers of symbols that each user needs to send are L over the first round, and L/U over the second round, which can be achieved simultaneously by a novel secure aggregation scheme. Another secure aggregation scheme was proposed in [10] for the above problem, which needs a less amount of generated keys in the system than that of [9].

To the best of our knowledge, all existing secure aggregation schemes with offline key sharing let the users share and store coded keys, through secret sharing (such as [6]–[8]) or Minimum Distance Separable (MDS) codes (such as [9], [10]).[6] In this paper, we follow the information theoretic secure aggregation problem with user dropouts in [9], while adding the additional constraint of uncoded groupwise keys as illustrated in Fig. 1.[7] By defining a system parameter $\mathsf{S}\in\{1,\ldots,\mathsf{K}\}$, for each $\mathcal{V}\subseteq\{1,\ldots,\mathsf{K}\}$ where $|\mathcal{V}|=\mathsf{S}$, there exists a key $Z_{\mathcal{V}}$ shared by the users in $\mathcal{V}$, which is independent of other keys.[8] The uncoded groupwise keys could be directly generated and shared among users by some key agreement

[2]Among the existing secure aggregation schemes with user dropouts, the ones in [9], [10], [13] considered the information theoretic security constraint [21], while the others considered the computational security.

[3]The problem in [9] only considers one epoch of the learning process.

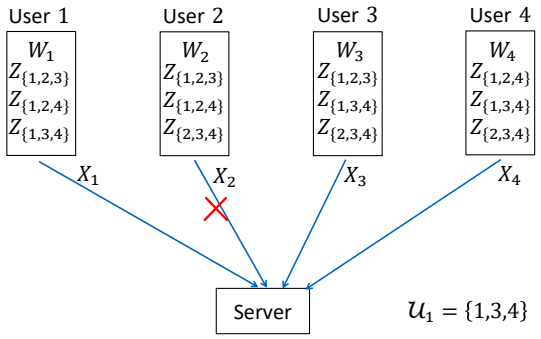
[4]Information theoretic secure aggregation problem with non-i.i.d. input vectors was considered in [22], where the server aims to estimate the empirical frequency of K items each of which is held by a user. Thus by formulating the input vector as a one-hot vector (i.e., a vector with only one element 1 while the others are 0), the required communication cost is much less than the secure aggregation problem for input vectors with i.i.d. elements.

[5]It was shown in [9] that for the sake of security under user dropouts, at least two rounds communications must be taken.

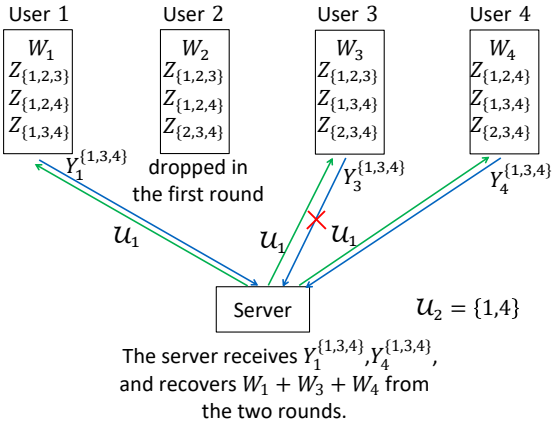
[6]The key sharing protocols in [6]–[8] are designed for the network where no private links exist among users, under the constraint of computational security. The key sharing protocols in [9], [10] lead to information theoretic privacy, but under the constraint that there are private links among users or a trusted server who assigns keys for the key sharing phase.

[7]The constraint of uncoded groupwise keys means that, the keys are independent among each other and each key is stored by a set of users.

[8]Note that all existing secure aggregation schemes fail to satisfy this constraint when $\mathsf{S}<\mathsf{K}$, due to the coded keys shared among users.



(a) First round.



(b) Second round.

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

protocol such as [23]–[30], even if there do not exist private links among users nor a trusted server.In addition, uncoded groupwise keys may be preferred in practice since they can be generated with low complexity and shared conveniently, and find a wide range of applications besides secure aggregation in federated learning.[9] Our objective is to characterize the capacity region of the numbers of transmissions by the users in two rounds of the model aggregation phase (i.e., the rates region).

A. Main Contributions

In this paper, we first formulate the new information theoretic secure aggregation problem with uncoded groupwise keys. Then our main contributions on this new model are as follows:

- When $\mathsf{S} > \mathsf{K} - \mathsf{U}$, we propose a new secure aggregation scheme which achieves exactly the same capacity region as in [9]; this means that, when $\mathsf{S} > \mathsf{K} - \mathsf{U}$, secure aggregation with uncoded groupwise key sharing has no loss on the communication efficiency. It is also interesting to see that by increasing S above $\mathsf{K} - \mathsf{U} + 1$ yields no reduction in the transmission cost; i.e., $\mathsf{S} = \mathsf{K} - \mathsf{U} + 1$ is sufficient and no larger value of S provide improvements. The main technical challenge of the proposed scheme based on linear coding is to determine the coefficients of the keys in the two round transmissions, satisfying the encodability (i.e., the keys cannot appear in the transmitted linear combinations by the users who do not know them), decodability, and security constraints. We overcome these challenges by designing new interference alignment strategies.[10] Note that, to achieve the optimal rates region by our proposed scheme, not all the keys $Z_{\mathcal{V}}$ where $\mathcal{V} \subseteq \{1, \ldots, \mathsf{K}\}$ and $|\mathcal{V}| = \mathsf{S}$ are needed during the transmission. The number of needed keys is either $\mathcal{O}(\mathsf{K})$ or $\mathcal{O}(\mathsf{K}^2)$, where each key has $(\mathsf{K} - \mathsf{U} + 1)\mathsf{L}/\mathsf{U}$ symbols.
- When $\mathsf{S} \leq \mathsf{K} - \mathsf{U}$, we derive a new converse bound to show that the optimal rates region of the considered problem is a strict subset of that in [9] (which is without any constraint on the keys). This implies that in this regime using uncoded keys strictly hurts.
- Experimental results over the Amazon EC2 cloud show that the proposed secure aggregation scheme reduces the communication time in the model aggregation by up to 53% compared to the original secure aggregation scheme in [6], and reduces the key sharing time up to 31.7% compared to the best existing information theoretic secure aggregation scheme with offline key sharing in [10].

B. Paper Organization

The rest of this paper is organized as follows. Section II formulates the considered secure aggregation problem with uncoded groupwise keys. Section III lists the main results of this paper. The proposed secure aggregation scheme is introduced in Section IV. Experimental results are provided in Section V. Section VI concludes the paper, while some proofs can be found in the Appendices.

C. 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; 1_n and 0_n represent the vertical n-dimensional vector whose elements are all 1 and all 0, respectively; $\mathbf{A}^{\mathrm{T}}$ 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

[9]For example, the uncoded pairwise key shared among each two users are independent of the other keys and thus can guarantee the information theoretic secure communication between these two users, while the other users (who may collude) are eavesdropper listening to the communication [21]. However, the pairwise coded keys used in the scheme [10] cannot guarantee secure communication between any two users, because the coded key shared by these two users are correlated to other keys stored by the other users.

[10]Interference alignment was originally proposed in [31] for the wireless interference channel, which aligns the undesired packets (i.e., interference) by each user such that their linear space dimension is reduced.

$n \times n$; $0_{m,n}$ 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 $m \times n$; $\langle\cdot\rangle_a$ represents the modulo operation with integer quotient $a > 0$ and in this paper we let $\langle\cdot\rangle_a \in \{1, \ldots, a\}$ (i.e., we let $\langle b\rangle_a = a$ 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 the rest of the paper entropies will be in base q, where q represents the field size.

II. System Model

We formulate a $(\mathsf{K}, \mathsf{U}, \mathsf{S})$ information theoretic secure aggregation problem with uncoded groupwise keys as illustrated in Fig 1, which contains one epoch of the learning process among K users and one server. For each $k \in [\mathsf{K}]$, user k holds one input vector (i.e., updated model) W_k composed of L uniform and i.i.d. symbols over a finite field $\mathbb{F}_{\mathsf{q}}$. As in [9], we assume that L is large enough. Ideally, the server aims to compute the element-wise sum of input vectors of all users. However, due to the user dropouts, the server may not be able to recover the sum of all input vectors. Hence, we let the server compute the sum of the input vectors from the surviving users, where the number of surviving users is at least U. In this paper, we mainly deal with the user dropouts and thus we assume that $\mathsf{U} \in [\mathsf{K} - 1]$.[11] In addition, by the secure aggregation constraint, the server must not retrieve any other information except the task from the received symbols. In order to guarantee the security, the users must share some secrets (i.e., keys) which are independent of the input vectors. Different from the secure aggregation problem in [9] which assumes that the keys could be any random variables shared among users, in this paper we consider uncoded groupwise keys, where the keys are independent of each other and each key is shared among S users where $\mathsf{S} \in [\mathsf{K}]$, which is shared through private link between each two users or by the key agreement protocols such as [23]–[30]. For each set $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$, there exists a key $Z_{\mathcal{V}}$ independent of other keys. Thus

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

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 the user $k \in [\mathsf{K}]$. The whole secure aggregation procedure contains the following two rounds.

First round. In the first round, each user $k \in [\mathsf{K}]$ generates a message X_k as a function of W_k and Z_k, without knowing the identity of the dropped users. The communication rate of the first round R_1 is defined as the largest transmission load among all users normalized by L, i.e.,

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

[11] When $\mathsf{U} = \mathsf{K}$, it was shown in [32, Theorem 2] (by taking $\mathsf{N}_{\mathrm{r}} = \mathsf{N}$ in [32, Theorem 2]) that one round transmission is enough and that the minimum number of transmitted symbols by each user is L.

User k then sends X_k to the server.

Some users may drop in the first round transmission, and the set of surviving users after the first round is denoted as $\mathcal{U}_1$, where $\mathcal{U}_1 \subseteq [\mathsf{K}]$ and $|\mathcal{U}_1| \geq \mathsf{U}$. Thus the server receives X_k where $k \in \mathcal{U}_1$.

Second round. In the second round, the server first sends the list of the surviving users (i.e., the set $\mathcal{U}_1$) to each user in $\mathcal{U}_1$. Then each user $k \in \mathcal{U}_1$ participates in the second round transmission by generating and sending a message $Y_k^{\mathcal{U}_1}$ as a function of W_k, Z_k, and $\mathcal{U}_1$. The communication 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.,

$$\mathsf{R}_2 := \max_{\mathcal{U}_1\subseteq[\mathsf{K}]:|\mathcal{U}_1|\geq\mathsf{U}} \max_{k\in\mathcal{U}_1} \frac{H(Y_k^{\mathcal{U}_1})}{\mathsf{L}}. \tag{3}$$

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

Decoding. The server should recover $\sum_{k\in\mathcal{U}_1} W_k$ from $(X_{k_1} : k_1 \in \mathcal{U}_1)$ and $(Y_{k_2}^{\mathcal{U}_1} : k_2 \in \mathcal{U}_2)$, i.e.,

$$H\left(\sum_{k\in\mathcal{U}_1} W_k \middle| (X_{k_1} : k_1 \in \mathcal{U}_1), (Y_{k_2}^{\mathcal{U}_1} : k_2 \in \mathcal{U}_2)\right) = 0, \tag{4}$$

for each $\mathcal{U}_1 \subseteq [\mathsf{K}]$ and each $\mathcal{U}_2 \subseteq \mathcal{U}_1 : |\mathcal{U}_1| \geq |\mathcal{U}_2| \geq \mathsf{U}$. Meanwhile, the security constraint imposes that after receiving all messages sent by the users including the dropped users (e.g., the users are not really dropped but too slow in the transmission), the server cannot get any other information about the input vectors except $\sum_{k\in\mathcal{U}_1} W_k$, i.e.,

$$I\left(W_1, \ldots, W_{\mathsf{K}}; X_1, \ldots, X_{\mathsf{K}}, (Y_k^{\mathcal{U}_1} : k \in \mathcal{U}_1) \middle| \sum_{k\in\mathcal{U}_1} W_k\right) = 0, \tag{5}$$

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

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 (4) and (5). Our objective is to determine the capacity region (i.e., the closure of all achievable rate tuples) of the considered problem, denoted by $\mathcal{R}^\star$.

A converse bound from [9]. By removing the uncoded groupwise constraint on the keys in our considered problem, we obtain the information theoretic aggregation problem in [9]. Hence, the converse bound on the capacity region in [9] is also a converse bound for our considered problem, which leads to the following lemma.

Lemma 1 ([9]). *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*

$$\mathsf{R}_1 \geq 1, \ \mathsf{R}_2 \geq \frac{1}{\mathsf{U}}. \tag{6}$$

□

However, the achievable secure aggregation schemes in [9],

TABLE I: Comparison on the information theoretic secure aggregation schemes. Our scheme 1 represents the proposed scheme for the case $2\mathsf{U}-1\leq\mathsf{K}<\mathsf{U}+\mathsf{S}$, while Our scheme 2 reprsents the proposed scheme for the case $\mathsf{K}<\min\{2\mathsf{U}-1,\mathsf{U}+\mathsf{S}\}$.

	[6]	[9]	[10]	Our scheme 1	Our scheme 2
Storage	K^2	$1+\frac{1}{\mathsf{U}}\left(\binom{\mathsf{K}-1}{\mathsf{U}-1}+\cdots+\binom{\mathsf{K}-1}{\mathsf{K}-1}\right)$	$1+\frac{\mathsf{K}}{\mathsf{U}}$	$\frac{\mathsf{K}-\mathsf{U}+1}{\mathsf{U}}\mathsf{S}$	$\mathcal{O}(\frac{\mathsf{K}-\mathsf{U}+1}{\mathsf{U}}\mathsf{SK})$
R_1	1	1	1	1	1
R_2	$\mathcal{O}\left(\frac{\mathsf{K}-\mathsf{U}+1}{\mathsf{U}}\mathsf{K}\right)$	$\frac{1}{\mathsf{U}}$	$\frac{1}{\mathsf{U}}$	$\frac{1}{\mathsf{U}}$	$\frac{1}{\mathsf{U}}$

[10] cannot work in our considered problem with $\mathsf{S}<\mathsf{K}$, since the schemes in [9], [10] assign correlated coded keys to users, while in our considered problem the keys are uncoded, groupwise-sharing and independent.

Another observation is that the capacity region of the $(\mathsf{K},\mathsf{U},\mathsf{S}_1)$ information theoretic secure aggregation problem with uncoded groupwise keys covers that of the $(\mathsf{K},\mathsf{U},\mathsf{S}_2)$ information theoretic secure aggregation problem with uncoded groupwise keys, where $\mathsf{S}_1>\mathsf{S}_2$. This is because, without collusion between the server and the users, having more users knowing the same key will not hurt. So any key $Z_{\mathcal{V}_2}$ could be generated by extracting some symbols from $Z_{\mathcal{V}_1}$ where $\mathcal{V}_2\subseteq\mathcal{V}_1$.

III. Main Results

We first present the main result of our paper.

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

$$\mathcal{R}^\star=\left\{(\mathsf{R}_1,\mathsf{R}_2):\mathsf{R}_1\geq 1,\mathsf{R}_2\geq\frac{1}{\mathsf{U}}\right\}. \tag{7}$$

□

The converse bound for Theorem 1 is directly from Lemma 1. For the achievability, we propose a new secure aggregation scheme based on linear coding and interference alignment, which is described in Section IV.

When $\mathsf{S}>\mathsf{K}-\mathsf{U}$, the proposed scheme for Theorem 1 achieves the same capacity region as the optimal secure aggregation scheme without any constraint on the keys in [9]. It is also interesting to see that increasing S above $\mathsf{K}-\mathsf{U}+1$ will not reduce the communication cost.

There are totally $\binom{\mathsf{K}}{\mathsf{S}}$ subsets of $[\mathsf{K}]$ with cardinality S. By the problem setting, we can use at most $\binom{\mathsf{K}}{\mathsf{S}}$ keys each of which is shared by S users. However, we do not need to use generate all these $\binom{\mathsf{K}}{\mathsf{S}}$ keys in our proposed secure scheme for Theorem 1. It will be clarified in Section IV that, the number of needed keys by the proposed secure aggregation scheme for Theorem 1 is K when $\mathsf{U}\leq\mathsf{K}-\mathsf{U}+1$ and is $\mathcal{O}(\mathsf{K}^2)$ when $\mathsf{U}>\mathsf{K}-\mathsf{U}+1$, where each key has $(\mathsf{K}-\mathsf{U}+1)\mathsf{L}/\mathsf{U}$ symbols.[12] Since in our proposed schemes, each key should be stored by K users, the average storage cost normalized by L of each user is $\frac{\mathsf{K}-\mathsf{U}+1}{\mathsf{U}}\mathsf{S}$ when $\mathsf{U}\leq\mathsf{K}-\mathsf{U}+1$, and $\mathcal{O}(\frac{\mathsf{K}-\mathsf{U}+1}{\mathsf{U}}\mathsf{SK})$ when $\mathsf{U}>\mathsf{K}-\mathsf{U}+1$.[13] In Table I, we compare the proposed secure aggregation scheme and the existing information theoretic secure aggregation schemes with offline key sharing in [6], [9], [10], in terms of the storage cost normalized by L at each user, first-round transmission rate R_1, and second-round transmission rate R_2.[14] More precisely,

- The secure aggregation scheme in [6] could be modified to guarantee information theoretic security if each key is generated with i.i.d. symbols (i.e., without using pseudorandom generator). In the rest of this paper, while comparing the performance of the scheme in [6] and the proposed scheme, we consider the modified version of the scheme in [6] which guarantees information theoretic security. Note that if there does not exist any colluding user, the secrete sharing parameter t in [6] could be set to 1 and thus the keys in the secure aggregation scheme in [6] are shared by all users.
- If coded key assignment is allowed, the secure aggregation scheme in [9] needs to generate U coded keys with L/U symbols for each group of users $\mathcal{V}\subseteq[\mathsf{K}]$ where $|\mathcal{V}|\in[\mathsf{U}:\mathsf{K}]$, where each user in the group stores a linear combination of these U coded keys; for each pair of users $\mathcal{V}\subseteq[\mathsf{K}]$ where $|\mathcal{V}|=2$, the secure aggregation scheme in [10] lets each user in the pair generate a coded key with L/U symbols and share it to the other user in the pair.

It can be seen from Table I that, the proposed scheme could significantly reduce the storage cost and the second-round transmission rate of the secure aggregation scheme in [6]; the proposed scheme has lower storage cost than the scheme in [9]; in addition, the proposed scheme has higher storage cost than the scheme in [10]. Furthermore, we want to emphasize that if the constraint of uncoded groupwise keys is imposed, the schemes in [6], [9], [10] can only work when $\mathsf{S}=\mathsf{K}$.

For the case $\mathsf{S}\leq\mathsf{K}-\mathsf{U}$, the following theorem shows that the communication rate of the optimal secure aggregation scheme without any constraint on the keys in [9] cannot be achieved; i.e., the capacity region of the considered problem is a strict subset of the one in [9].

[12]The selection on the keys is done before the model aggregation phase, and only depends on the system parameters K, U, and S, independent of the realizations of sets $\mathcal{U}_1$ and $\mathcal{U}_2$ in the model aggregation phase.

[13]If we require the same storage cost at each user, we can take K cyclic wrap-around permutations on the users and divide the computation task into K non-overlapping and equal-length pieces. Then we use the proposed scheme K times independently to construct the keys and transmissions, where each time we refer to one permutation of users and one piece of computation task (thus the lengths of keys and transmissions in each time are divided by K).

[14]The secure aggregation schemes in [6], [9], [10] can tolerate up to $\mathsf{T}<\mathsf{U}$ users who collude with the server. However, in this paper we do not consider user collusion; thus in our comparison (and also in the later experiments) we set $\mathsf{T}=0$.

Theorem 2. *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* $2\leq\mathsf{S}\leq\mathsf{K}-\mathsf{U}$*, the communication rate of the first round must satisfy that*

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

□

The proof of Theorem 2 can be found in Appendix A. From Theorem 2, when $2\leq\mathsf{S}\leq\mathsf{K}-\mathsf{U}$, it is not enough for each user to transmit one (normalized) linear combination of the input vector and keys. Intuitively, this is because the total number of dropped users after the second round could be larger than or equal to S, which is the number of users sharing each key; thus some key(s) appearing in the transmission of the first round, may not be received in the received packets of the second round due to the user dropouts. Hence, we need to transmit more than one (normalized) linear combination in the first round. It is one of our on-going works to design tight achievable schemes and converse bounds for the case $2\leq\mathsf{S}\leq\mathsf{K}-\mathsf{U}$.

IV. Proof of Theorem 1: New Secure Aggregation Scheme

To present the proposed scheme, we only need to focus on the case where $\mathsf{S}=\mathsf{K}-\mathsf{U}+1$. As we explained at the end of Section II, this is because if $\mathsf{S}>\mathsf{K}-\mathsf{U}+1$, we can generate any key $Z_{\mathcal{V}}$ where $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{K}-\mathsf{U}+1}$ by extracting some symbols from $Z_{\mathcal{V}_1}$ where $\mathcal{V}_1\in\binom{[\mathsf{K}]}{\mathsf{S}}$ and $\mathcal{V}\subseteq\mathcal{V}_1$, while the users in $\mathcal{V}_1\setminus\mathcal{V}$ will not use $Z_{\mathcal{V}}$ even they know it. Thus a secure aggregation scheme for the case $\mathsf{S}=\mathsf{K}-\mathsf{U}+1$ could also work for the case $\mathsf{S}>\mathsf{K}-\mathsf{U}+1$.

The construction structure of the achievable scheme is as follows.

- Since the length of each input vector W_k where $k\in[\mathsf{K}]$ is large enough, as explained in [9], we can consider blocks of symbols of W_k as an element of a suitably large field extension and consider operations such as element wise sum as operations over the field extension. Hence, without loss of generality, in the scheme proposed in this paper we can assume that q is large enough. We then divide each input vector W_k where $k\in[\mathsf{K}]$ into U non-overlapping and equal-length pieces, where the j^{th} piece denoted by $W_{k,j}$ contains L/U symbols on $\mathbb{F}_{\mathsf{q}}$. In addition, for each $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$ and each $k\in\mathcal{V}$,[15] we let $Z_{\mathcal{V},k}$ denote a vector of L/U uniform i.i.d. symbols on $\mathbb{F}_{\mathsf{q}}$. Then, we define a key $Z_{\mathcal{V}}=(Z_{\mathcal{V},k}:k\in\mathcal{V})$ with totally L symbols and let $Z_{\mathcal{V}}$ be shared by all users in $\mathcal{V}$.
- In the first round, each user $k\in[\mathsf{K}]$ sends

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

  where $a_{\mathcal{V},j}\in\mathbb{F}_{\mathsf{q}}$ is a coefficient to be designed.[16] Note that each $X_{k,j}$ contains L/U symbols, and thus $X_k=(X_{k,1},\ldots,X_{k,\mathsf{U}})$ contains L symbols, which leads to $\mathsf{R}_1=1$.
  We let $\mathbf{a}_{\mathcal{V}}:=[a_{\mathcal{V},1},\ldots,a_{\mathcal{V},\mathsf{U}}]^{\mathrm{T}}$. By the security constraint, W_k should be perfectly protected by the keys in $X_k=(X_{k,1},\ldots,X_{k,\mathsf{U}})$; otherwise, the server can retrieve some information about W_k from X_k which hurts the security. Thus, 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 aim to have that the coefficients matrix (whose dimension is $\mathsf{U}\times\binom{\mathsf{K}-1}{\mathsf{S}-1}$)

$$\left[\mathbf{a}_{\mathcal{S}_{k,1}},\ldots,\mathbf{a}_{\mathcal{S}_{k,\binom{\mathsf{K}-1}{\mathsf{S}-1}}}\right]\ \text{ has rank equal to }\mathsf{U},\ \forall k\in[\mathsf{K}]. \tag{10}$$

  If the constraints in (10) are satisfied, we have

$$I(W_1,\ldots,W_{\mathsf{K}};X_1,\ldots,X_{\mathsf{K}})=0, \tag{11}$$

  i.e., the server cannot get any information about $W_1,\ldots,W_{\mathsf{K}}$ even if the server receives all $X_1,\ldots,X_{\mathsf{K}}$ (this will be formally proved in (92) in Appendix C, where we also show that (11) is required for our scheme satisfying the security).
  Since the set of surviving users after the first round is $\mathcal{U}_1$, the server receives X_k where $k\in\mathcal{U}_1$, and thus can recover

$$\begin{aligned}&\sum_{k\in\mathcal{U}_1}X_{k,j}\\ =&\sum_{k\in\mathcal{U}_1}W_{k,j}+\sum_{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}:\mathcal{V}\cap\mathcal{U}_1\neq\emptyset}\left(a_{\mathcal{V},j}\sum_{k_1\in\mathcal{V}\cap\mathcal{U}_1}Z_{\mathcal{V},k_1}\right) &(12)\\ =&\sum_{k\in\mathcal{U}_1}W_{k,j}+\sum_{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}}\left(a_{\mathcal{V},j}\sum_{k_1\in\mathcal{V}\cap\mathcal{U}_1}Z_{\mathcal{V},k_1}\right),\ \forall j\in[\mathsf{U}], &(13)\end{aligned}$$

  where (13) follows since $\mathsf{S}=\mathsf{K}-\mathsf{U}+1>\mathsf{K}-|\mathcal{U}_1|$. Hence, the server still needs to recover $\sum_{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}}\left(a_{\mathcal{V},j}\sum_{k_1\in\mathcal{V}\cap\mathcal{U}_1}Z_{\mathcal{V},k_1}\right)$ for each $j\in[\mathsf{U}]$ in the next round. We can treat

$$Z_{\mathcal{V}}^{\mathcal{U}_1}:=\sum_{k_1\in\mathcal{V}\cap\mathcal{U}_1}Z_{\mathcal{V},k_1},\ \forall\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}, \tag{14}$$

  as one coded key, which can be encoded by all users in $\mathcal{V}\cap\mathcal{U}_1$ and contains L/U uniform and i.i.d. symbols. **Thus by the construction of the first round transmission, we only need to transmit linear combinations of coded keys in the second round, such that the server can recover $\sum_{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}}a_{\mathcal{V},j}Z_{\mathcal{V}}^{\mathcal{U}_1}$ for each $j\in[\mathsf{U}]$.**
- In the second round, we denote the sets in $\binom{[\mathsf{K}]}{\mathsf{S}}$ by $\mathcal{S}_1,\ldots,\mathcal{S}_{\binom{\mathsf{K}}{\mathsf{S}}}$, and for each $k\in[\mathsf{K}]$ denote the sets in $\binom{[\mathsf{K}]\setminus\{k\}}{\mathsf{S}}$ by $\overline{\mathcal{S}}_{k,1},\ldots,\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}$. Thus the server should

[15] Recall that $\binom{\mathcal{X}}{y}=\{\mathcal{S}\subseteq\mathcal{X}:|\mathcal{S}|=y\}$ where $|\mathcal{X}|\geq y>0$.

[16] In this paper, the product $a\mathbf{b}$ where a is a scalar and $\mathbf{b}$ is a vector or a matrix, represents multiplying each element in $\mathbf{b}$ by a.

recover

$$\begin{bmatrix} F_1 \\ \vdots \\ F_{\mathsf{U}} \end{bmatrix} = \left[\mathbf{a}_{\mathcal{S}_1}, \ldots, \mathbf{a}_{\mathcal{S}_{\binom{[\mathsf{K}]}{\mathsf{S}}}} \right] \begin{bmatrix} Z^{\mathcal{U}_1}_{\mathcal{S}_1} \\ \vdots \\ Z^{\mathcal{U}_1}_{\mathcal{S}_{\binom{[\mathsf{K}]}{\mathsf{S}}}} \end{bmatrix}, \tag{15}$$

where each F_j, $j \in [\mathsf{U}]$, contains L/U symbols.

Note that each user $k \in \mathcal{U}_1$ cannot encode $Z^{\mathcal{U}_1}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]\backslash\{k\}}{\mathsf{S}}$. If the U-dimensional vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ satisfy the constraints that

$$\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}}, \ldots, \mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}} \right] \text{ has rank equal to } \mathsf{U}-1, \forall k \in [\mathsf{K}], \tag{16}$$

then the matrix $\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}}, \ldots, \mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}} \right]$ contains exactly one linearly independent left null vector. **To achieve** (16)**, we will propose some interference alignment techniques to align the U-dimensional vectors of the $\binom{\mathsf{K}-1}{\mathsf{S}}$ unknown keys to a linear space spanned by $\mathsf{U}-1$ linearly independent vectors.**

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

$$Y^{\mathcal{U}_1}_k = \mathbf{s}_k \begin{bmatrix} F_1 \\ \vdots \\ F_{\mathsf{U}} \end{bmatrix}, \tag{17}$$

where $\mathbf{s}_k$ represents the left null vector of $\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}}, \ldots, \mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}} \right]$. By construction, in $Y^{\mathcal{U}_1}_k$ the coefficients of the coded keys which cannot be encoded by user k are 0. Note that $Y^{\mathcal{U}_1}_k$ contains L/U symbols, which leads to $\mathsf{R}_2 = 1/\mathsf{U}$.

For the decodability, from any set of surviving users after the second round $\mathcal{U}_2 \subseteq \mathcal{U}_1$ where $|\mathcal{U}_2| \geq \mathsf{U}$, we should recover $F_1, \ldots, F_{\mathsf{U}}$ from the second round transmission; i.e., we aim to have

$$\text{any } \mathsf{U} \text{ vectors in } \{\mathbf{s}_k : k \in \mathcal{U}_1\} \text{ are linearly independent.} \tag{18}$$

Thus from (13) and (18), the server can recover $F_1, \ldots, F_{\mathsf{U}}$ and then recover $\sum_{k \in \mathcal{U}_1} W_{k,j}$ for all $j \in [\mathsf{U}]$; thus it can recover $\sum_{k \in \mathcal{U}_1} W_k$.

In addition, for the security constraint, by construction we have

$$H\left(Y^{\mathcal{U}_1}_k : k \in \mathcal{U}_1 \right) = \mathsf{L}, \tag{19}$$

which follows since each $Y^{\mathcal{U}_1}_k$ where $k \in \mathcal{U}_1$ is in the linear space spanned by $F_1, \ldots, F_{\mathsf{U}}$, where each F_j, $j \in [\mathsf{U}]$, contains L/U symbols. Intuitively, from $(X_k : k \in [\mathsf{K}])$, the server cannot get any information about $W_1, \ldots, W_{\mathsf{K}}$. Together with $(Y^{\mathcal{U}_1}_k : k \in \mathcal{U}_1)$ whose entropy is L, the server can at most get L symbols information about $W_1, \ldots, W_{\mathsf{K}}$, which are exactly the symbols in $\sum_{k \in \mathcal{U}_1} W_k$. Hence, the proposed scheme is secure. The rigorous proof on the security constraint in (5) can be found in Appendix C.

We conclude that the achieved rates are $(\mathsf{R}_1, \mathsf{R}_2) = (1, 1/\mathsf{U})$, coinciding with Theorem 1.

For what said above, it is apparent that the key challenge in the proposed scheme is to design the U-dimensional vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$, such that the constraints in (10)**,** (16)**, and** (18) **are satisfied. As showed above, if such constraints are satisfied, the proposed scheme is decodable and secure.**

Another important observation is that, the constraints in (10), (16) are not related to $\mathcal{U}_1$; in addition, if the constraint in (18) is satisfied for the case $\mathcal{U}_1 = [\mathsf{K}]$, this constraint also holds for any other $\mathcal{U}_1$. **Hence, we only need to consider the case $\mathcal{U}_1 = [\mathsf{K}]$ to design the U-dimensional vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$.**

In the following, we will further divide the considered case $\mathsf{U} < \mathsf{K}$ into three regimes: a) $\mathsf{U} \leq \mathsf{K}-\mathsf{U}+1$; b) $\mathsf{U} > \mathsf{K}-\mathsf{U}+1$ and $\mathsf{U} = \mathsf{K}-1$; c) $\mathsf{U} > \mathsf{K}-\mathsf{U}+1$ and $\mathsf{U} < \mathsf{K}-1$. We will propose our scheme for each regime which achieves the capacity region in Theorem 1. In each regime, we propose a different selection on the U-dimensional vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$, such that the constraints in (10), (16), and (18) are satisfied. For the ease of reading, in Table II we summarize the main parameters and variables used in the proposed scheme.

A. *Case* $\mathsf{U} \leq \mathsf{K} - \mathsf{U} + 1$

We first illustrate the proposed scheme for this case through an example.

Example 1 $((\mathsf{K}, \mathsf{U}, \mathsf{S})) = (3, 2, 2)$**).** Consider the $(\mathsf{K}, \mathsf{U}, \mathsf{S}) = (3, 2, 2)$ information theoretic secure aggregation problem with uncoded groupwise keys. While illustrating the proposed scheme through examples, we perform a field extension on the input vectors to a large enough prime field $\mathbb{F}_{\mathsf{q}}$. In general this assumption on prime field size is not necessary in our proposed scheme.

For each $\mathcal{V} \in \binom{[3]}{2}$, we generate a key $Z_{\mathcal{V}} = (Z_{\mathcal{V},k} : k \in \mathcal{V})$ shared by users in $\mathcal{V}$, where each $Z_{\mathcal{V},k}$ contains $\mathsf{L}/2$ uniform and i.i.d. symbols over $\mathbb{F}_{\mathsf{q}}$. We also divide each input vector W_k where $k \in [3]$ into two pieces, $W_k = (W_{k,1}, W_{k,2})$, where each piece contains $\mathsf{L}/2$ uniform and i.i.d. symbols over $\mathbb{F}_{\mathsf{q}}$.

First round. In the first round, user 1 transmits $X_1 = (X_{1,1}, X_{1,2})$, where

$$X_{1,1} = W_{1,1} + Z_{\{1,2\},1} + Z_{\{1,3\},1};$$
$$X_{1,2} = W_{1,2} + Z_{\{1,2\},1} + 2Z_{\{1,3\},1}.$$

User 2 transmits $X_2 = (X_{2,1}, X_{2,2})$, where

$$X_{2,1} = W_{2,1} + Z_{\{1,2\},2} + Z_{\{2,3\},2};$$
$$X_{2,2} = W_{2,2} + Z_{\{1,2\},2} + 3Z_{\{2,3\},2}.$$

User 3 transmits $X_3 = (X_{3,1}, X_{3,2})$, where

$$X_{3,1} = W_{3,1} + Z_{\{1,3\},3} + Z_{\{2,3\},3};$$
$$X_{3,2} = W_{3,2} + 2Z_{\{1,3\},3} + 3Z_{\{2,3\},3}.$$

In other words, we let

$$\mathbf{a}_{\{1,2\}} = [1,1]^{\mathrm{T}},\ \mathbf{a}_{\{1,3\}} = [1,2]^{\mathrm{T}},\ \mathbf{a}_{\{2,3\}} = [1,3]^{\mathrm{T}}. \tag{20}$$

TABLE II: Notations and main variables used in the proposed scheme.

Notations	Semantics
K	number of users and number of input vectors
U	minimum number of non-dropped users
S	number of users sharing each key
R_1, R_2	first-round and second-round communication rates
$W_k = (W_{k,j} : j \in [\mathsf{U}])$	input vector of user k where $W_{k,j}$ has L/U i.i.d. symbols on $\mathbb{F}_\mathsf{q}$
$X_k = (X_{k,j} : j \in [\mathsf{U}])$, for $k \in [\mathsf{K}]$	first-round transmission of user k, where $X_{k,j}$ defined in (9) has L/U symbols on $\mathbb{F}_\mathsf{q}$
$Z_\mathcal{V} = (Z_{\mathcal{V},k} : k \in \mathcal{V})$, for $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$	key shared by users in $\mathcal{V}$, where $Z_{\mathcal{V},k}$ has L/U i.i.d. symbols on $\mathbb{F}_\mathsf{q}$
$Z_\mathcal{V}^{\mathcal{U}_1}$, for $\mathcal{U}_1 \subseteq [\mathsf{K}]$, $\lvert\mathcal{U}_1\rvert \geq \mathsf{U}$, $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$	$\sum_{k_1 \in \mathcal{V}\cap\mathcal{U}_1} Z_{\mathcal{V},k_1}$, coded key with L/U i.i.d. symbols on $\mathbb{F}_\mathsf{q}$
$\mathbf{a}_\mathcal{V} = [a_{\mathcal{V},1}, a_{\mathcal{V},2}, \ldots, a_{\mathcal{V},\mathsf{U}}]^\mathrm{T}$, for $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$	U-dimensional column vector, which needs to be selected satisfying the constraints in (10), (16), (18)
$\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_{\binom{\mathsf{K}}{\mathsf{S}}}$	sets in $\binom{[\mathsf{K}]}{\mathsf{S}}$
$\mathcal{S}_{k,1}, \mathcal{S}_{k,2}, \ldots, \mathcal{S}_{k,\binom{\mathsf{K}-1}{\mathsf{S}-1}}$, for $k \in [\mathsf{K}]$	sets in $\binom{[\mathsf{K}]}{\mathsf{S}}$ containing k
$\overline{\mathcal{S}}_{k,1}, \overline{\mathcal{S}}_{k,2}, \ldots, \overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}$	sets in $\binom{[\mathsf{K}]\backslash\{k\}}{\mathsf{S}}$
F_j for $j \in [\mathsf{U}]$	L/U symbols on $\mathbb{F}_\mathsf{q}$ defined in (15) which should be recovered by the server in the second round
$\mathbf{s}_k$ for $k \in [\mathsf{K}]$	U-dimensional vector, which is a left null vector of $\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}}, \ldots, \mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}}\right]$
$Y_k^{\mathcal{U}_1}$ for $\mathcal{U}_1 \subseteq [\mathsf{K}]$, $\lvert\mathcal{U}_1\rvert \geq \mathsf{U}$, $k \in \mathcal{U}_1$	second-round transmission of user k defined in (17), containing L/U symbols on $\mathbb{F}_\mathsf{q}$

In X_1, the coefficient matrix of the keys $(Z_{\{1,2\},1}, Z_{\{1,3\},1})$ is $\begin{bmatrix}1 & 1\\ 1 & 2\end{bmatrix}$, which has rank equal to 2 (recall that the field size is large enough), i.e., the constraint in (10) is satisfied for user 1. Thus W_1 is perfectly protected by $(Z_{\{1,2\},1}, Z_{\{1,3\},1})$ from X_1. Similarly, the constraints in (10) are satisfied for user $2, 3$.

Second round. In the second round, we only need to consider the case where $\mathcal{U}_1 = [3]$, as explained before. Since $\mathcal{U}_1 = [3]$, the server should recover $W_1 + W_2 + W_3$. By the definition of coded key in (14), we define the coded keys

$$\begin{aligned} Z_{\{1,2\}}^{[3]} &= Z_{\{1,2\},1} + Z_{\{1,2\},2},\\ Z_{\{1,3\}}^{[3]} &= Z_{\{1,3\},1} + Z_{\{1,3\},3},\\ Z_{\{2,3\}}^{[3]} &= Z_{\{2,3\},2} + Z_{\{2,3\},3}, \end{aligned}$$

each of which contains $\mathsf{L}/2$ uniform and i.i.d. symbols. From the transmission of the first round, the server can recover

$$\begin{aligned} X_{1,1} + X_{2,1} + X_{3,1} &= W_{1,1} + W_{2,1} + W_{3,1}\\ &\quad + Z_{\{1,2\}}^{[3]} + Z_{\{1,3\}}^{[3]} + Z_{\{2,3\}}^{[3]},\\ X_{1,2} + X_{2,2} + X_{3,2} &= W_{1,2} + W_{2,2} + W_{3,2}\\ &\quad + Z_{\{1,2\}}^{[3]} + 2Z_{\{1,3\}}^{[3]} + 3Z_{\{2,3\}}^{[3]}. \end{aligned}$$

Hence, the server should further recover

$$\begin{bmatrix}F_1\\ F_2\end{bmatrix} = [\mathbf{a}_{\{1,2\}}, \mathbf{a}_{\{1,3\}}, \mathbf{a}_{\{2,3\}}] \begin{bmatrix}Z_{\{1,2\}}^{[3]}\\ Z_{\{1,3\}}^{[3]}\\ Z_{\{2,3\}}^{[3]}\end{bmatrix} \tag{21a}$$

$$= \begin{bmatrix}1 & 1 & 1\\ 1 & 2 & 3\end{bmatrix} \begin{bmatrix}Z_{\{1,2\}}^{[3]}\\ Z_{\{1,3\}}^{[3]}\\ Z_{\{2,3\}}^{[3]}\end{bmatrix} \tag{21b}$$

totally L symbols in the second round. Since $\lvert\mathcal{U}_2\rvert \geq \mathsf{S} = 2$, the second round transmission should be designed such that from any two of $Y_1^{[3]}, Y_2^{[3]}, Y_3^{[3]}$, we can recover (21b).

For user 1 who cannot encode $Z_{\{2,3\}}^{[3]}$, the sub-matrix $[\mathbf{a}_{\{2,3\}}]$ has rank equal to 1; thus the constraint in (16) is satisfied for user 1. The left null space of $[\mathbf{a}_{\{2,3\}}]$ contains exactly one linearly independent 2-dimensional vector, which could be $[3, -1]$. Thus we let user 1 transmit

$$Y_1^{[3]} = [3, -1] \begin{bmatrix}F_1\\ F_2\end{bmatrix} = 3F_1 - F_2, \tag{22}$$

in which the coefficient of $Z_{\{2,3\}}^{[3]}$ is 0. Similarly, we let user 2 transmit

$$Y_2^{[3]} = [2, -1] \begin{bmatrix}F_1\\ F_2\end{bmatrix} = 2F_1 - F_2, \tag{23}$$

in which the coefficient of $Z_{\{1,3\}}^{[3]}$ is 0, and let user 3 transmit

$$Y_3^{[3]} = [1, -1] \begin{bmatrix}F_1\\ F_2\end{bmatrix} = F_1 - F_2, \tag{24}$$

in which the coefficient of $Z_{\{1,2\}}^{[3]}$ is 0. The constraints in (16) are also satisfied for users $2, 3$.

By construction, any two of $Y_1^{[3]}, Y_2^{[3]}, Y_3^{[3]}$ are linearly

independent. Hence, for any $\mathcal{U}_2 \subseteq [3]$ where $|\mathcal{U}_2| \geq 2$, the server can recover F_1 and F_2; thus the constraint in (18) is satisfied. Hence, from the two round transmissions, the server can recover $W_1 + W_2 + W_3$.

Since the constraints in (10), (16), and (18) are satisfied, by the security proof in Appendix C, the scheme is secure for the case $\mathcal{U}_1 = [3]$.

In conclusion, in the first round, each user transmits L symbols. In the second round, each user in $\mathcal{U}_1$ transmits $\mathsf{L}/2$ symbols. Hence, the achieved rates are $(\mathsf{R}_1, \mathsf{R}_2) = (1, 1/2)$, coinciding with Theorem 1. □

We are now ready to generalize the proposed scheme in Example 1 to the case where $\mathsf{U} \leq \mathsf{K} - \mathsf{U} + 1$. For the sake of simplicity, we directly describe the choice of the U-dimensional vectors and show that such choice satisfies the constraints in (10), (16), and (18).

We use a cyclic key assignment, by defining a collection of cyclic sets

$$\mathcal{C} := \big\{\{i, \langle i+1\rangle_{\mathsf{K}}, \ldots, \langle i+\mathsf{K}-\mathsf{U}\rangle_{\mathsf{K}}\} : i \in [\mathsf{K}]\big\}. \tag{25}$$

For the ease of notation, we sort the sets in $\mathcal{C}$ in an order where the i^{th} set denoted by $\mathcal{C}(i)$ is $\{i, \langle i+1\rangle_{\mathsf{K}}, \ldots, \langle i+\mathsf{K}-\mathsf{U}\rangle_{\mathsf{K}}\}$, for each $i \in [\mathsf{K}]$.[17] It can be seen that each of the sets $\mathcal{C}(k), \mathcal{C}(\langle k-1\rangle_{\mathsf{K}}), \ldots, \mathcal{C}(\langle k-\mathsf{K}+\mathsf{U}\rangle_{\mathsf{K}})$ contains k, for each $k \in [\mathsf{K}]$.

We select the U-dimensional vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ as follows:

- if $\mathcal{V} \in \mathcal{C}$, we let $\mathbf{a}_{\mathcal{V}}$ be uniform and i.i.d. over $\mathbb{F}_{\mathsf{q}}^{\mathsf{U}}$;
- otherwise, we let each element in $\mathbf{a}_{\mathcal{V}}$ be 0.

Next we will show that the above choice of these U-dimensional vectors satisfies the constraints in (10), (16), and (18), with high probability.

Constraints in (10)*:* Since q is large enough and $\mathsf{U} \leq \mathsf{K} - \mathsf{U} + 1$, for each $k \in [\mathsf{K}]$ the matrix

$$\big[\mathbf{a}_{\mathcal{C}(k)}, \mathbf{a}_{\mathcal{C}(\langle k-1\rangle_{\mathsf{K}})}, \ldots, \mathbf{a}_{\mathcal{C}(\langle k-\mathsf{K}+\mathsf{U}\rangle_{\mathsf{K}})}\big]$$

whose dimension is $\mathsf{U} \times (\mathsf{K}-\mathsf{U}+1)$, has rank equal to U with high probability; thus the constraints in (10) are satisfied with high probability.

Constraints in (16)*:* Among the sets in $\mathcal{C}$, each of the sets $\mathcal{C}(\langle k+1\rangle_{\mathsf{K}}), \mathcal{C}(\langle k+2\rangle_{\mathsf{K}}), \ldots, \mathcal{C}(\langle k+\mathsf{U}-1\rangle_{\mathsf{K}})$ does not contain k, where $k \in [\mathsf{K}]$. It can be seen that $[\mathbf{a}_{\mathcal{C}(\langle k+1\rangle_{\mathsf{K}})}, \mathbf{a}_{\mathcal{C}(\langle k+2\rangle_{\mathsf{K}})}, \ldots, \mathbf{a}_{\mathcal{C}(\langle k+\mathsf{U}-1\rangle_{\mathsf{K}})}]$ has dimension equal to $\mathsf{U} \times (\mathsf{U}-1)$, and that its elements are uniformly and i.i.d. over $\mathbb{F}_{\mathsf{q}}$. So the left null space contains $\mathsf{U} - (\mathsf{U}-1) = 1$ linearly independent U-dimensional vector with high probability, and we let $\mathbf{s}_k$ be this vector. Hence, the constraints in (16) are satisfied with high probability.

Constraint in (18)*:* Recall that we only need to consider the case where $\mathcal{U}_1 = [\mathsf{K}]$. In the second round transmission, the server should recover U linear combinations of coded keys,

$$\begin{bmatrix} F_1 \\ \vdots \\ F_{\mathsf{U}} \end{bmatrix} = \big[\mathbf{a}_{\mathcal{C}(1)}, \ldots, \mathbf{a}_{\mathcal{C}(\mathsf{K})}\big] \begin{bmatrix} Z^{[\mathsf{K}]}_{\mathcal{C}(1)} \\ \vdots \\ Z^{[\mathsf{K}]}_{\mathcal{C}(\mathsf{K})} \end{bmatrix},$$

from the answers of any U of the K users, each of whom knows $\mathsf{K}-\mathsf{U}+1$ coded keys in a cyclic way. This problem is equivalent to the distributed linearly separable computation problem in [33], where we aim to compute U linear combinations of K messages (whose coefficients are uniformly and i.i.d. over $\mathbb{F}_{\mathsf{q}}$) through K distributed computing nodes, each of which can stores $\mathsf{K}-\mathsf{U}+1$ messages, such that from the answers of any U nodes we can recover the computing task. From [33, Lemma 2], we have the following lemma.

Lemma 2 ([33])**.** *For any set $\mathcal{A} \in \binom{[\mathsf{K}]}{\mathsf{U}}$, the vectors $\mathbf{s}_n, n \in \mathcal{A}$, are linearly independent with high probability.* □

Thus by Lemma 2, the constraint in (18) is satisfied with high probability.

In conclusion, all constraints in (10), (16), and (18) are satisfied with high probability. Hence, there must exist a choice of $\big[\mathbf{a}_{\mathcal{C}(1)}, \ldots, \mathbf{a}_{\mathcal{C}(\mathsf{K})}\big]$ satisfying those constraints. Thus the proposed scheme is decodable and secure. In this case, we need the keys $Z_{\mathcal{V}}$ where $\mathcal{V} \in \mathcal{C}$, totally K keys each of which is shared by S users.

B. Case $\mathsf{U} > \mathsf{K} - \mathsf{U} + 1$ *and* $\mathsf{U} = \mathsf{K} - 1$

When $\mathsf{U} > \mathsf{S}$, the proposed secure aggregation scheme with cyclic assignment does not work. This is because, among $\mathcal{C}$, the number of sets containing each $k \in [\mathsf{K}]$ is $\mathsf{K}-\mathsf{U}+1 < \mathsf{U}$, which are $\mathcal{C}(k), \mathcal{C}(\langle k-1\rangle_{\mathsf{K}}), \ldots, \mathcal{C}(\langle k-\mathsf{K}+\mathsf{U}\rangle_{\mathsf{K}})$. Hence, the coefficient matrix of keys in X_k, $\big[\mathbf{a}_{\mathcal{C}(k)}, \mathbf{a}_{\mathcal{C}(\langle k-1\rangle_{\mathsf{K}})}, \ldots, \mathbf{a}_{\mathcal{C}(\langle k-\mathsf{K}+\mathsf{U}\rangle_{\mathsf{K}})}\big]$, is with dimension $\mathsf{U} \times (\mathsf{K}-\mathsf{U}+1)$ and with rank strictly less than U. Thus the constraint in (10) is not satisfied. In other words, W_k is not perfectly protected from X_k.

In this subsection, we present our proposed secure aggregation scheme for the case where $\mathsf{U} > \mathsf{K}-\mathsf{U}+1$ and $\mathsf{U} = \mathsf{K}-1$. We first illustrate the main idea through the following example.

Example 2 $((\mathsf{K}, \mathsf{U}, \mathsf{S})) = (4, 3, 2))$**.** Consider the $(\mathsf{K}, \mathsf{U}, \mathsf{S}) = (4, 3, 2)$ information theoretic secure aggregation problem with uncoded groupwise keys. For each $\mathcal{V} \in \binom{[4]}{2}$, we generate a key $Z_{\mathcal{V}} = (Z_{\mathcal{V},k} : k \in \mathcal{V})$ shared by users in $\mathcal{V}$, where each $Z_{\mathcal{V},k}$ contains $\mathsf{L}/3$ uniform and i.i.d. symbols over $\mathbb{F}_{\mathsf{q}}$. We also divide each input vector W_k where $k \in [4]$ into three pieces, $W_k = (W_{k,1}, W_{k,2}, W_{k,3})$, where each piece contains $\mathsf{L}/3$ uniform and i.i.d. symbols over $\mathbb{F}_{\mathsf{q}}$.

In the first round, each user $k \in [4]$ transmits

$$X_{k,j} = W_{k,j} + \sum_{\mathcal{V} \in \binom{[4]}{2} : k \in \mathcal{V}} a_{\mathcal{V},j} Z_{\mathcal{V},k}, \ \forall j \in [3]. \tag{26}$$

Now we select the 3-dimensional vectors $\mathbf{a}_{\{1,2\}}, \mathbf{a}_{\{1,3\}}, \mathbf{a}_{\{1,4\}}, \mathbf{a}_{\{2,3\}}, \mathbf{a}_{\{2,4\}}$, and $\mathbf{a}_{\{3,4\}}$ as follows,

$$\mathbf{a}_{\{1,2\}} = [1,0,0]^{\mathrm{T}}, \ \mathbf{a}_{\{1,3\}} = [0,1,0]^{\mathrm{T}}, \ \mathbf{a}_{\{1,4\}} = [0,0,1]^{\mathrm{T}}, \tag{27a}$$

[17] For example, when $\mathsf{K} = 4$ and $\mathsf{U} = 2$, we have $\mathcal{C}(1) = \{1,2,3\}$, $\mathcal{C}(2) = \{2,3,4\}$, $\mathcal{C}(3) = \{1,3,4\}$, and $\mathcal{C}(4) = \{1,2,4\}$.

$$\mathbf{a}_{\{2,3\}} = \mathbf{a}_{\{1,2\}} - \mathbf{a}_{\{1,3\}} = [1,-1,0]^{\mathsf{T}}, \tag{27b}$$

$$\mathbf{a}_{\{2,4\}} = \mathbf{a}_{\{1,2\}} - \mathbf{a}_{\{1,4\}} = [1,0,-1]^{\mathsf{T}}, \tag{27c}$$

$$\mathbf{a}_{\{3,4\}} = \mathbf{a}_{\{1,3\}} - \mathbf{a}_{\{1,4\}} = [0,1,-1]^{\mathsf{T}}. \tag{27d}$$

We next show that by the above choice the constraints in (10), (16), and (18) are satisfied.

For user 1, the matrix $[\mathbf{a}_{\{1,2\}}, \mathbf{a}_{\{1,3\}}, \mathbf{a}_{\{1,4\}}] = \mathbf{I}_3$ has rank 3, where we recall that $\mathbf{I}_3$ represents the identity matrix with dimension 3×3. Hence, the constraint in (10) is satisfied for user 1. Thus W_1 is perfectly protected by $(Z_{\{1,2\},1}, , Z_{\{1,3\},1}, Z_{\{1,4\},1})$ from X_1. For user 2, the matrix $[\mathbf{a}_{\{1,2\}}, \mathbf{a}_{\{2,3\}}, \mathbf{a}_{\{2,4\}}] = \begin{bmatrix} 1 & 1 & 1 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$ has rank 3. Hence, the constraint in (10) is satisfied for user 2. Thus W_2 is perfectly protected by $(Z_{\{1,2\},2}, , Z_{\{2,3\},2}, Z_{\{2,4\},2})$ from X_2. Similarly, the constraints in (10) are also satisfied for users $3, 4$.

In the second round, we only need to consider the case $\mathcal{U}_1 = [4]$, where the server should recover $W_1 + \cdots + W_4$. By defining the coded keys as in (14), the server needs to further recover

$$\begin{bmatrix} F_1 \\ F_2 \\ F_3 \end{bmatrix} = [\mathbf{a}_{\{1,2\}}, \mathbf{a}_{\{1,3\}}, \mathbf{a}_{\{1,4\}}, \mathbf{a}_{\{2,3\}}, \mathbf{a}_{\{2,4\}}, \mathbf{a}_{\{3,4\}}] \begin{bmatrix} Z^{[4]}_{\{1,2\}} \\ Z^{[4]}_{\{1,3\}} \\ Z^{[4]}_{\{1,4\}} \\ Z^{[4]}_{\{2,3\}} \\ Z^{[4]}_{\{2,4\}} \\ Z^{[4]}_{\{3,4\}} \end{bmatrix} \tag{28a}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 & -1 & -1 \end{bmatrix} \begin{bmatrix} Z^{[4]}_{\{1,2\}} \\ Z^{[4]}_{\{1,3\}} \\ Z^{[4]}_{\{1,4\}} \\ Z^{[4]}_{\{2,3\}} \\ Z^{[4]}_{\{2,4\}} \\ Z^{[4]}_{\{3,4\}} \end{bmatrix}. \tag{28b}$$

For user 1 who cannot encode $Z^{[4]}_{\{2,3\}}, Z^{[4]}_{\{2,4\}}, Z^{[4]}_{\{3,4\}}$, it can be seen that the sub-matrix $[\mathbf{a}_{\{2,3\}}, \mathbf{a}_{\{2,4\}}, \mathbf{a}_{\{3,4\}}]$ has rank 2, equal to the rank of $[\mathbf{a}_{\{2,3\}}, \mathbf{a}_{\{2,4\}}]$, since $\mathbf{a}_{\{2,3\}} - \mathbf{a}_{\{2,4\}} = -\mathbf{a}_{\{3,4\}}$;[18] thus the constraint in (16) is satisfied for user 1. Hence, the left null space of $[\mathbf{a}_{\{2,3\}}, \mathbf{a}_{\{2,4\}}, \mathbf{a}_{\{3,4\}}]$ contains exactly one linearly independent 3-dimensional vector, which could be $[1,1,1]$. Thus we let user 1 compute

$$Y^{[4]}_1 = [1,1,1] \begin{bmatrix} F_1 \\ F_2 \\ F_3 \end{bmatrix} = F_1 + F_2 + F_3. \tag{29}$$

For user 2, who cannot encode $Z^{[4]}_{\{1,3\}}, Z^{[4]}_{\{1,4\}}, Z^{[4]}_{\{3,4\}}$, it can be seen that the sub-matrix $[\mathbf{a}_{\{1,3\}}, \mathbf{a}_{\{1,4\}}, \mathbf{a}_{\{3,4\}}]$ has rank 2, equal to the rank of $[\mathbf{a}_{\{1,3\}}, \mathbf{a}_{\{1,4\}}]$, since $\mathbf{a}_{\{3,4\}} = \mathbf{a}_{\{1,3\}} - \mathbf{a}_{\{1,4\}}$; thus the constraint in (16) is satisfied for user 2. Hence, the left null space of $[\mathbf{a}_{\{1,3\}}, \mathbf{a}_{\{1,4\}}, \mathbf{a}_{\{3,4\}}]$ contains exactly one linearly independent 3-dimensional vector, which could be $[1,0,0]$. Thus we let user 2 compute

$$Y^{[4]}_2 = [1,0,0] \begin{bmatrix} F_1 \\ F_2 \\ F_3 \end{bmatrix} = F_1. \tag{30}$$

Similarly, the constraints in (16) are satisfied for users $3, 4$; thus we let user 3 compute

$$Y^{[4]}_3 = [0,1,0] \begin{bmatrix} F_1 \\ F_2 \\ F_3 \end{bmatrix} = F_2, \tag{31}$$

and let user 4 compute

$$Y^{[4]}_4 = [0,0,1] \begin{bmatrix} F_1 \\ F_2 \\ F_3 \end{bmatrix} = F_3. \tag{32}$$

It can be seen that any 3 of $Y^{[4]}_1, Y^{[4]}_2, Y^{[4]}_3, Y^{[4]}_4$ are linearly independent; thus the constraint in (18) is satisfied. Hence, for any $\mathcal{U}_2 \in \binom{[4]}{3}$, the server can recover F_1, F_2, F_3 from the second round. Thus from the two round transmissions, the server can recover $W_1 + \cdots + W_4$.

Since the constraints in (10), (16), and (18) are satisfied, by the security proof in Appendix C, the scheme is secure for the case $\mathcal{U}_1 = [4]$.

In conclusion, the achieved rates of the proposed scheme are $(\mathsf{R}_1, \mathsf{R}_2) = (1, 1/3)$, coinciding with Theorem 1.

□

We are now ready to generalize the proposed scheme in Example 2 to the case where $\mathsf{U} > \mathsf{K} - \mathsf{U} + 1$ and $\mathsf{U} = \mathsf{K} - 1$. In this case, we have $\mathsf{S} = 2$. As the previous case, we directly describe the choice of the U-dimensional vectors and show that such choice satisfies the constraints in (10), (16), and (18).

Let us first consider the sets $\mathcal{V} \in \binom{[\mathsf{K}]}{2}$ where $1 \in \mathcal{V}$. Each of such sets could be written as $\{1, j\}$, where $j \in [2 : \mathsf{K} - 1]$. We let

$$\mathbf{a}_{\{1,j\}} = \mathbf{e}_{\mathsf{U},j-1}, \ \forall j \in [2 : \mathsf{K}], \tag{33}$$

where $\mathbf{e}_{n,i}$ represents the vertical n-dimensional unit vector whose entry in the i^{th} position is 1 and 0 elsewhere. We then consider the sets $\mathcal{V} \in \binom{[2:\mathsf{K}]}{2}$. Each of such sets could be written as $\{i, j\}$, where $1 < i < j \leq \mathsf{K}$. We let

$$\mathbf{a}_{\{i,j\}} = \mathbf{a}_{\{1,i\}} - \mathbf{a}_{\{1,j\}} = \mathbf{e}_{\mathsf{U},i-1} - \mathbf{e}_{\mathsf{U},j-1}, \ \forall 1 < i < j \leq \mathsf{K}. \tag{34}$$

Next we will show that the above choice of these U-dimensional vectors satisfies the constraints in (10), (16), and (18).

Constraints in (10)*:* For user 1, the matrix $\left[\mathbf{a}_{\{1,2\}}, \mathbf{a}_{\{1,3\}}, \ldots, \mathbf{a}_{\{1,\mathsf{K}\}}\right]$ is the identity matrix $\mathbf{I}_{\mathsf{K}-1} = \mathbf{I}_{\mathsf{U}}$, whose rank is U; thus the constraint in (10) is satisfied for user 1. For each user $k \in [2 : \mathsf{K}]$, by a simple linear transform on the matrix

$$\left[\mathbf{a}_{\{1,k\}}, \mathbf{a}_{\{2,k\}}, \ldots, \mathbf{a}_{\{k-1,k\}}, \mathbf{a}_{\{k,k+1\}}, \mathbf{a}_{\{k,k+2\}}, \ldots \mathbf{a}_{\{k,\mathsf{K}\}}\right], \tag{35}$$

[18] In other words, we align the three vectors $\mathbf{a}_{\{2,3\}}, \mathbf{a}_{\{2,4\}}, \mathbf{a}_{\{3,4\}}$ into the linear space spanned by $\mathbf{a}_{\{2,3\}}$ and $\mathbf{a}_{\{2,4\}}$.

we obtain the matrix

$$\begin{aligned}&[\mathbf{a}_{\{1,k\}}+\mathbf{a}_{\{2,k\}},\mathbf{a}_{\{1,k\}}+\mathbf{a}_{\{3,k\}},\ldots,\mathbf{a}_{\{1,k\}}+\mathbf{a}_{\{k-1,k\}},\\&\mathbf{a}_{\{1,k\}},\mathbf{a}_{\{1,k\}}-\mathbf{a}_{\{k,k+1\}},\mathbf{a}_{\{1,k\}}-\mathbf{a}_{\{k,k+2\}},\\&\ldots,\mathbf{a}_{\{1,k\}}-\mathbf{a}_{\{k,\mathsf{K}\}}]\\&=[\mathbf{e}_{\mathsf{U},1},\mathbf{e}_{\mathsf{U},2},\ldots,\mathbf{e}_{\mathsf{U},k-2},\mathbf{e}_{\mathsf{U},k-1},\mathbf{e}_{\mathsf{U},k},\mathbf{e}_{\mathsf{U},k+1},\ldots,\mathbf{e}_{\mathsf{U},\mathsf{K}-1}],\end{aligned}$$

which is the identity matrix $\mathbf{I}_{\mathsf{K}-1}=\mathbf{I}_{\mathsf{U}}$ with rank equal to U, which is also full rank. Hence, the matrix in (35) is full rank, with rank equal to U; thus the constraint in (10) is satisfied for user k.

Constraints in (16)*:* For user 1, among the sets in $\mathcal{V}\in\binom{[\mathsf{K}]}{2}$, the sets $\{2,3\},\{2,4\},\ldots,\{2,\mathsf{K}\},\{3,4\},\ldots,\{\mathsf{K}-1,\mathsf{K}\}$ do not contain 1. It can be seen that the following $\mathsf{K}-2$ vectors,

$$\begin{aligned}\mathbf{a}_{\{2,3\}}&=\mathbf{e}_{\mathsf{U},1}-\mathbf{e}_{\mathsf{U},2},\ \mathbf{a}_{\{2,4\}} &\text{(36a)}\\&=\mathbf{e}_{\mathsf{U},1}-\mathbf{e}_{\mathsf{U},3},\ \ldots,\ \mathbf{a}_{\{2,\mathsf{K}\}} &\text{(36b)}\\&=\mathbf{e}_{\mathsf{U},1}-\mathbf{e}_{\mathsf{U},\mathsf{K}-1}, &\text{(36c)}\end{aligned}$$

are linearly independent. In addition, for each set $\{i,j\}$ where $2<i<j\leq\mathsf{K}$, we have $\mathbf{a}_{\{i,j\}}=\mathbf{a}_{\{2,j\}}-\mathbf{a}_{\{2,i\}}$. Hence, the matrix $\left[\mathbf{a}_{\overline{\mathcal{S}}_{1,1}},\ldots,\mathbf{a}_{\overline{\mathcal{S}}_{1,\binom{\mathsf{K}-1}{2}}}\right]$ has rank equal to $\mathsf{K}-2=\mathsf{U}-1$,[19] satisfying the constraint in (16).

For each user $k\in[2:\mathsf{K}]$, among the sets in $\mathcal{V}\in\binom{[\mathsf{K}]}{2}$, the sets $\{1,2\},\{1,3\},\ldots,\{1,k-1\},\{1,k+1\},\ldots,\{1,\mathsf{K}\}$ and the sets $\{i,j\}$ where $1<i<j\leq\mathsf{K}$ and $i,j\neq k$, do not contain k. It can be seen that the following $\mathsf{K}-2$ vectors,

$$\begin{aligned}\mathbf{a}_{\{1,2\}}&=\mathbf{e}_{\mathsf{U},1},\mathbf{a}_{\{1,3\}}=\mathbf{e}_{\mathsf{U},2},\ldots,\mathbf{a}_{\{1,k-1\}} &\text{(37a)}\\&=\mathbf{e}_{\mathsf{U},k-2},\mathbf{a}_{\{1,k+1\}}=\mathbf{e}_{\mathsf{U},k},\ldots,\mathbf{a}_{\{1,\mathsf{K}\}} &\text{(37b)}\\&=\mathbf{e}_{\mathsf{U},\mathsf{K}-1}, &\text{(37c)}\end{aligned}$$

are linearly independent. In addition, for each set $\{i,j\}$ where $1<i<j\leq\mathsf{K}$ and $i,j\neq k$, we have $\mathbf{a}_{\{i,j\}}=\mathbf{a}_{\{1,i\}}-\mathbf{a}_{\{1,j\}}$. Hence, the matrix $\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}},\ldots,\mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{2}}}\right]$ has rank equal to $\mathsf{K}-2=\mathsf{U}-1$, satisfying the constraint in (16).

Constraint in (18)*:* For user 1, recall that $\mathbf{s}_1$ is a left null vector of the matrix $\left[\mathbf{a}_{\overline{\mathcal{S}}_{1,1}},\ldots,\mathbf{a}_{\overline{\mathcal{S}}_{1,\binom{\mathsf{K}-1}{2}}}\right]$, whose rank is $\mathsf{U}-1$. The left null space of $\left[\mathbf{a}_{\overline{\mathcal{S}}_{1,1}},\ldots,\mathbf{a}_{\overline{\mathcal{S}}_{1,\binom{\mathsf{K}-1}{2}}}\right]$ is the same as that of its column-wise sub-matrix $\left[\mathbf{a}_{\{2,3\}},\mathbf{a}_{\{2,4\}},\ldots,\mathbf{a}_{\{2,\mathsf{K}\}}\right]$, whose rank is also $\mathsf{U}-1$ and dimension is $\mathsf{U}\times(\mathsf{U}-1)$. Since

$$\begin{aligned}&\left[\mathbf{a}_{\{2,3\}},\mathbf{a}_{\{2,4\}},\ldots,\mathbf{a}_{\{2,\mathsf{K}\}}\right]=\left[\mathbf{a}_{\{2,3\}},\mathbf{a}_{\{2,4\}},\ldots,\mathbf{a}_{\{2,\mathsf{K}\}}\right]\\&=[\mathbf{e}_{\mathsf{U},1}-\mathbf{e}_{\mathsf{U},2},\mathbf{e}_{\mathsf{U},1}-\mathbf{e}_{\mathsf{U},3},\ldots,\mathbf{e}_{\mathsf{U},1}-\mathbf{e}_{\mathsf{U},\mathsf{K}-1}]\end{aligned}$$

contains exactly one linearly independent left null vector, which could be (recall that 1_n represents the vertical n-dimensional vector whose elements are all 1)

$$1_{\mathsf{U}}=\mathbf{s}_1. \tag{38}$$

[19]Recall that for each $k\in[\mathsf{K}]$, the sets $\mathcal{V}\in\binom{[\mathsf{K}]\setminus\{k\}}{\mathsf{S}}$ are $\overline{\mathcal{S}}_{k,1},\ldots,\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}$.

For each user $k\in[2:\mathsf{K}]$, $\mathbf{s}_k$ is a left null vector of the matrix $\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}},\ldots,\mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{2}}}\right]$, whose rank is $\mathsf{U}-1$. The left null space of $\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}},\ldots,\mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{2}}}\right]$ is the same as that of its column-wise sub-matrix $\left[\mathbf{a}_{\{1,2\}},\mathbf{a}_{\{1,3\}},\ldots,\mathbf{a}_{\{1,k-1\}},\mathbf{a}_{\{1,k+1\}},\ldots,\mathbf{a}_{\{1,\mathsf{K}\}}\right]$, whose rank is also $\mathsf{U}-1$ and dimension is $\mathsf{U}\times(\mathsf{U}-1)$. Since

$$\begin{aligned}&\left[\mathbf{a}_{\{1,2\}},\mathbf{a}_{\{1,3\}},\ldots,\mathbf{a}_{\{1,k-1\}},\mathbf{a}_{\{1,k+1\}},\ldots,\mathbf{a}_{\{1,\mathsf{K}\}}\right]\\&=[\mathbf{e}_{\mathsf{U},1},\mathbf{e}_{\mathsf{U},2},\ldots,\mathbf{e}_{\mathsf{U},k-2},\mathbf{e}_{\mathsf{U},k},\ldots,\mathbf{e}_{\mathsf{U},\mathsf{K}-1}]\end{aligned}$$

contains exactly one linearly independent left null vector, which could be

$$\mathbf{e}_{\mathsf{U},k-1}=\mathbf{s}_k. \tag{39}$$

From (38) and (39), it can be seen that any U vectors of $\mathbf{s}_1,\ldots,\mathbf{s}_{\mathsf{K}}$ are linearly independent; thus the constraint in (18) is satisfied.

In conclusion, all constraints in (10), (16), and (18) are satisfied; thus the proposed scheme is decodable and secure. In this case, we need the keys $Z_{\mathcal{V}}$ where $\mathcal{V}\in\binom{[\mathsf{K}]}{2}$, totally $\mathsf{K}(\mathsf{K}-1)/2$ keys each of which is shared by 2 users.

C. Case $\mathsf{U}>\mathsf{K}-\mathsf{U}+1$ and $\mathsf{U}<\mathsf{K}-1$

Finally, we focus on the most involved case where $\mathsf{U}>\mathsf{K}-\mathsf{U}+1$ and $\mathsf{U}<\mathsf{K}-1$. In this case, we have $\mathsf{S}>2$ and $2\mathsf{U}>\mathsf{K}+1$. Recall that our objective is to determine the U-dimensional vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$, such that the constraints in (10), (16), and (18) are satisfied. We start by illustrating the main idea through an example.

Example 3 $((\mathsf{K},\mathsf{U},\mathsf{S}))=(6,4,3)$**).** Consider the $(\mathsf{K},\mathsf{U},\mathsf{S})=(6,4,3)$ information theoretic secure aggregation problem with uncoded groupwise keys. We determine the 4-dimensional vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V}\in\binom{[6]}{3}$ following three steps.

- **Step 1: Select base unit vectors.** We first consider each $\mathbf{a}_{\mathcal{V}}$ where $[2]\subseteq\mathcal{V}$ and let $\mathbf{a}_{\mathcal{V}}$ be a distinct vertical unit vector; i.e., we let

$$\begin{aligned}&\mathbf{a}_{[3]}=\mathbf{e}_{4,1},\ \mathbf{a}_{\{1,2,4\}}=\mathbf{e}_{4,2},\ \mathbf{a}_{\{1,2,5\}}=\mathbf{e}_{4,3}, &\text{(40a)}\\&\mathbf{a}_{\{1,2,6\}}=\mathbf{e}_{4,4}. &\text{(40b)}\end{aligned}$$

  Define that $\mathcal{G}_1=\{[3],\{1,2,4\},\{1,2,5\},\{1,2,6\}\}$.
- **Step 2: Determine the composition of each coefficient vector $\mathbf{a}_{\mathcal{V}}$.** For any $\mathcal{V}\in\binom{[6]}{3}$, we let $\mathbf{a}_{\mathcal{V}}$ be a linear combination of some base unit vectors; the composition of $\mathbf{a}_{\mathcal{V}}$ represents the set of base unit vectors involved in the linear combination. For each $i\in[3:6]\cap\mathcal{V}$, $\mathbf{e}_{4,i-2}$ is in the composition of $\mathbf{a}_{\mathcal{V}}$. After fixing the composition of $\mathbf{a}_{\mathcal{V}}$, we can write

$$\mathbf{a}_{\mathcal{V}}=\sum_{i\in[3:6]\cap\mathcal{V}}b_{\mathcal{V},i-2}\mathbf{e}_{4,i-2}, \tag{41}$$

  where $\mathbf{b}_{\mathcal{V}}:=(b_{\mathcal{V},1},\ldots,b_{\mathcal{V},|[3:6]\cap\mathcal{V}|})$ is an $|[3:6]\cap\mathcal{V}|$-dimensional vector to be designed. By this rule, we determine the composition of each $\mathbf{a}_{\mathcal{V}}$ (i.e., the base vertical unit vectors which compose $\mathbf{a}_{\mathcal{V}}$) where $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$, as illustrated in Table III.

- **Step 3: Determine the vector $\mathbf{b}_{\mathcal{V}}$ for each $\mathbf{a}_{\mathcal{V}}$.** Next we need to determine the coefficient vector of the vertical base unit vectors $\mathbf{b}_{\mathcal{V}}$ for each $\mathcal{V} \in \binom{[6]}{3} \setminus \mathcal{G}_1$.
  For each set $\mathbf{a}_{\mathcal{V}}$ where $\{3,4\} \subseteq \mathcal{V}$, we choose each element of $\mathbf{b}_{\mathcal{V}}$ uniformly and i.i.d. over $\mathbb{F}_{\mathsf{q}}$. For example, by choosing $\mathbf{b}_{\{1,3,4\}} = [1,4]$, we have

$$\mathbf{a}_{\{1,3,4\}} = \mathbf{a}_{[3]} + 4\mathbf{a}_{\{1,2,4\}} = \mathbf{e}_{4,1} + 4\mathbf{e}_{4,2}. \tag{42}$$

  Similarly, by choosing $\mathbf{b}_{\{2,3,4\}} = [1,8]$, $\mathbf{b}_{\{3,4,5\}} = [1,1,1]$, and $\mathbf{b}_{\{3,4,6\}} = [1,2,1]$, we have

$$\mathbf{a}_{\{2,3,4\}} = \mathbf{a}_{[3]} + 8\mathbf{a}_{\{1,2,4\}} = \mathbf{e}_{4,1} + 8\mathbf{e}_{4,2}, \tag{43a}$$
$$\mathbf{a}_{\{3,4,5\}} = \mathbf{a}_{[3]} + \mathbf{a}_{\{1,2,4\}} + \mathbf{a}_{\{1,2,5\}} = \mathbf{e}_{4,1} + \mathbf{e}_{4,2} + \mathbf{e}_{4,3}, \tag{43b}$$
$$\mathbf{a}_{\{3,4,6\}} = \mathbf{a}_{[3]} + 2\mathbf{a}_{\{1,2,4\}} + \mathbf{a}_{\{1,2,6\}} = \mathbf{e}_{4,1} + 2\mathbf{e}_{4,2} + \mathbf{e}_{4,4}. \tag{43c}$$

  Define that $\mathcal{G}_2 = \{\{1,3,4\},\{2,3,4\},\{3,4,5\},\{3,4,6\}\}$.
  We then define $\mathcal{G}_3$ as the collection of the sets in $\binom{[6]}{3} \setminus (\mathcal{G}_1 \cup \mathcal{G}_2)$ where $3 \in \mathcal{V}$; thus $\mathcal{G}_3 = \{\{1,3,5\},\{1,3,6\},\{2,3,5\},\{2,3,6\},\{3,5,6\}\}$. For each set $\mathcal{V} \in \mathcal{G}_3$, we search for the minimum subset of $\mathcal{G}_2$ the union of whose elements is a super-set of $\mathcal{V}$; we denote this minimum subset by $\mathcal{M}'_{\mathcal{V}}$. We let $\mathbf{a}_{\mathcal{V}}$ be a linear combination of $\mathbf{a}_{\mathcal{V}_2}$ where $\mathcal{V}_2 \in \mathcal{M}'_{\mathcal{V}}$. For example, if $\mathcal{V} = \{1,3,5\}$, the minimum subset of $\mathcal{G}_2$ the union of whose elements is a super-set of $\{1,3,5\}$, is $\mathcal{M}'_{\{1,3,5\}} = \{\{1,3,4\},\{3,4,5\}\}$. We let $\mathbf{a}_{\{1,3,5\}}$ be a linear combination of $\mathbf{a}_{\{1,3,4\}} = \mathbf{e}_{4,1} + 4\mathbf{e}_{4,2}$ and $\mathbf{a}_{\{3,4,5\}} = \mathbf{e}_{4,1} + \mathbf{e}_{4,2} + \mathbf{e}_{4,3}$. Recall from (41) that, the base unit vectors of $\mathbf{a}_{\{1,3,5\}}$ are $\mathbf{e}_{4,1}$ and $\mathbf{e}_{4,3}$, which do not contain $\mathbf{e}_{4,2}$. Hence, we let

$$\mathbf{a}_{\{1,3,5\}} = 4\mathbf{a}_{\{3,4,5\}} - \mathbf{a}_{\{1,3,4\}} = 3\mathbf{e}_{4,1} + 4\mathbf{e}_{4,3}, \tag{44}$$

  to 'zero-force' the term $\mathbf{e}_{4,2}$. Similarly, we let

$$\mathbf{a}_{\{1,3,6\}} = 2\mathbf{a}_{\{3,4,6\}} - \mathbf{a}_{\{1,3,4\}} = \mathbf{e}_{4,1} + 2\mathbf{e}_{4,4}, \tag{45a}$$
$$\mathbf{a}_{\{2,3,5\}} = 8\mathbf{a}_{\{3,4,5\}} - \mathbf{a}_{\{2,3,4\}} = 7\mathbf{e}_{4,1} + 8\mathbf{e}_{4,3}, \tag{45b}$$
$$\mathbf{a}_{\{2,3,6\}} = 4\mathbf{a}_{\{3,4,6\}} - \mathbf{a}_{\{2,3,4\}} = 3\mathbf{e}_{4,1} + 4\mathbf{e}_{4,4}, \tag{45c}$$
$$\mathbf{a}_{\{3,5,6\}} = 2\mathbf{a}_{\{3,4,5\}} - \mathbf{a}_{\{3,4,6\}} = \mathbf{e}_{4,1} + 2\mathbf{e}_{4,3} - \mathbf{e}_{4,4}, \tag{45d}$$

  to 'zero-force' the term $\mathbf{e}_{4,2}$.
  It will be checked soon that by using the above coefficient vectors, the full rank constraint in (10) can be satisfied, and thus we can let all the remaining coefficient vectors be zero vectors, in order to reduce the number of required keys. More precisely, for each set $\mathcal{V} \in \binom{[6]}{3} \setminus (\mathcal{G}_1 \cup \mathcal{G}_2 \cup \mathcal{G}_3)$, we let $\mathbf{a}_{\mathcal{V}} = 0_4$, where 0_n represents the vertical n-dimensional vector whose elements are all 0.

As a result, we have determined $\mathbf{a}_{\mathcal{V}}$ for each $\mathcal{V} \in \binom{[6]}{3}$ as illustrated in Table III. We then show the such choice satisfies the constraints in (10), (16), and (18).

Constraints in (10)*:* For users $1,2$, the matrix $\left[\mathbf{a}_{[3]}, \mathbf{a}_{\{1,2,4\}}, \mathbf{a}_{\{1,2,5\}}, \mathbf{a}_{\{1,2,6\}}\right]$ is the identity matrix $\mathbf{I}_4$ whose rank is 4. For users $3,4$, the matrix $\left[\mathbf{a}_{\{1,3,4\}}, \mathbf{a}_{\{2,3,4\}}, \mathbf{a}_{\{3,4,5\}}, \mathbf{a}_{\{3,4,6\}}\right]$ has rank equal to 4. For user 5, the matrix $\left[\mathbf{a}_{\{1,3,5\}}, \mathbf{a}_{\{2,3,5\}}, \mathbf{a}_{\{3,4,5\}}, \mathbf{a}_{\{3,5,6\}}\right]$ has rank equal to 4. For user 6, the matrix $\left[\mathbf{a}_{\{1,3,6\}}, \mathbf{a}_{\{2,3,6\}}, \mathbf{a}_{\{3,4,6\}}, \mathbf{a}_{\{3,5,6\}}\right]$ has rank equal to 4. Hence, the constraints in (10) are satisfied.

Constraints in (16)*:* For user 1, we first remove the columns of 0's from the matrix $\left[\mathbf{a}_{\overline{\mathcal{S}}_{1,1}}, \ldots, \mathbf{a}_{\overline{\mathcal{S}}_{1,\binom{\mathsf{K}-1}{3}}}\right]$, to obtain

$$\left[\mathbf{a}_{\{2,3,4\}}, \mathbf{a}_{\{2,3,5\}}, \mathbf{a}_{\{2,3,6\}}, \mathbf{a}_{\{3,4,5\}}, \mathbf{a}_{\{3,4,6\}}, \mathbf{a}_{\{3,5,6\}}\right]. \tag{46}$$

By construction, we have $\mathbf{a}_{\{2,3,5\}}, \mathbf{a}_{\{2,3,6\}}, \mathbf{a}_{\{3,5,6\}}$ are linear combinations of $\mathbf{a}_{\{2,3,4\}}, \mathbf{a}_{\{3,4,5\}}, \mathbf{a}_{\{3,4,6\}}$. In addition, $\mathbf{a}_{\{2,3,4\}}, \mathbf{a}_{\{3,4,5\}}, \mathbf{a}_{\{3,4,6\}}$ are linearly independent. Hence, the rank of the matrix in (46) is 3, equal to the rank of $[\mathbf{a}_{\{2,3,4\}}, \mathbf{a}_{\{3,4,5\}}, \mathbf{a}_{\{3,4,6\}}]$. Hence, the constraint in (16) is satisfied for user 1. Similarly, this constraint is also satisfied for user 2.

For user 3, by construction, in each $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[6]\setminus\{3\}}{3}$, the coefficient of $\mathbf{e}_{4,1}$ is 0. In addition, $\mathbf{a}_{\{1,2,4\}}, \mathbf{a}_{\{1,2,5\}}, \mathbf{a}_{\{1,2,6\}}$ are linearly independent. Thus the matrix $\left[\mathbf{a}_{\overline{\mathcal{S}}_{3,1}}, \ldots, \mathbf{a}_{\overline{\mathcal{S}}_{3,\binom{\mathsf{K}-1}{3}}}\right]$ has rank equal to 3, equal to the rank of $[\mathbf{a}_{\{1,2,4\}}, \mathbf{a}_{\{1,2,5\}}, \mathbf{a}_{\{1,2,6\}}]$. Hence, the constraint in (16) is satisfied for user 3. Similarly, this constraint is also satisfied for each user in $\{4,5,6\}$.

Constraint in (18)*:* For user 1, recall that $\mathbf{s}_1$ is a left null vector of the matrix $\left[\mathbf{a}_{\overline{\mathcal{S}}_{1,1}}, \ldots, \mathbf{a}_{\overline{\mathcal{S}}_{1,\binom{\mathsf{K}-1}{3}}}\right]$, whose rank is 3. As explained before, its column-wise submatrix $[\mathbf{a}_{\{2,3,4\}}, \mathbf{a}_{\{3,4,5\}}, \mathbf{a}_{\{3,4,6\}}]$ has the same rank. Hence, the left null space of $[\mathbf{a}_{\{2,3,4\}}, \mathbf{a}_{\{3,4,5\}}, \mathbf{a}_{\{3,4,6\}}]$ is the same as that of $\left[\mathbf{a}_{\overline{\mathcal{S}}_{1,1}}, \ldots, \mathbf{a}_{\overline{\mathcal{S}}_{1,\binom{\mathsf{K}-1}{3}}}\right]$. So we let $\mathbf{s}_1$ be a left null vector of $[\mathbf{a}_{\{2,3,4\}}, \mathbf{a}_{\{3,4,5\}}, \mathbf{a}_{\{3,4,6\}}]$, which could be $\mathbf{s}_1 = [-8,1,7,6]^{\mathrm{T}}$. Similarly, we let $\mathbf{s}_2$ be a left null vector of $[\mathbf{a}_{\{1,3,4\}}, \mathbf{a}_{\{3,4,5\}}, \mathbf{a}_{\{3,4,6\}}]$, which could be $\mathbf{s}_2 = [-4,1,3,2]^{\mathrm{T}}$; we let $\mathbf{s}_3$ be a left null vector of $[\mathbf{a}_{\{1,2,4\}}, \mathbf{a}_{\{1,2,5\}}, \mathbf{a}_{\{1,2,6\}}]$, which could be $\mathbf{s}_3 = \mathbf{e}_{4,1}$; we let $\mathbf{s}_4$ be a left null vector of $[\mathbf{a}_{\{1,2,3\}}, \mathbf{a}_{\{1,2,5\}}, \mathbf{a}_{\{1,2,6\}}]$, which could be $\mathbf{s}_4 = \mathbf{e}_{4,2}$; we let $\mathbf{s}_5$ be a left null vector of $[\mathbf{a}_{\{1,2,3\}}, \mathbf{a}_{\{1,2,4\}}, \mathbf{a}_{\{1,2,6\}}]$, which could be $\mathbf{s}_5 = \mathbf{e}_{4,3}$; we let $\mathbf{s}_6$ be a left null vector of $[\mathbf{a}_{\{1,2,3\}}, \mathbf{a}_{\{1,2,4\}}, \mathbf{a}_{\{1,2,5\}}]$, which could be $\mathbf{s}_6 = \mathbf{e}_{4,4}$.

Since any two rows of $[\mathbf{s}_1, \mathbf{s}_2]$ are linearly independent and $[\mathbf{s}_3, \mathbf{s}_4, \mathbf{s}_5, \mathbf{s}_6] = \mathbf{I}_4$, we can see that any 4 vectors of $\mathbf{s}_1, \mathbf{s}_2, \mathbf{s}_3, \mathbf{s}_4, \mathbf{s}_5, \mathbf{s}_6$ are linearly independent. Hence, the constraint in (18) is satisfied.

In conclusion, all constraints in (10), (16), and (18) are satisfied; thus the proposed scheme is decodable and secure. □

To summarize Example 3, our selection on the U-dimensional vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$, contains the following steps from a high-level viewpoint:

- **Step 1: Select base unit vectors:** choose $\mathbf{a}_{\mathcal{V}}$ where $[\mathsf{K}-\mathsf{U}] \subseteq \mathcal{V}$ as the base vertical unit vectors.
- **Step 2: Determine the composition of each coefficient vector $\mathbf{a}_{\mathcal{V}}$:** fix the composition of each $\mathbf{a}_{\mathcal{V}}$ where $[\mathsf{K}-\mathsf{U}] \nsubseteq \mathcal{V}$.

TABLE III: Choice of 4-dimensional vectors $\mathbf{a}_{\mathcal{V}}$ in the $(\mathsf{K},\mathsf{U},\mathsf{S})=(6,4,3)$ information theoretic secure aggregation problem.

$\mathbf{a}_{\mathcal{V}}$	Composition	Value	$\mathbf{a}_{\mathcal{V}}$	Composition	Value
$\mathbf{a}_{[3]}$	$\mathbf{e}_{4,1}$	$\mathbf{e}_{4,1}$	$\mathbf{a}_{\{2,3,4\}}$	$\mathbf{e}_{4,1},\mathbf{e}_{4,2}$	$\mathbf{e}_{4,1}+8\mathbf{e}_{4,2}$
$\mathbf{a}_{\{1,2,4\}}$	$\mathbf{e}_{4,2}$	$\mathbf{e}_{4,2}$	$\mathbf{a}_{\{2,3,5\}}$	$\mathbf{e}_{4,1},\mathbf{e}_{4,3}$	$7\mathbf{e}_{4,1}+8\mathbf{e}_{4,3}$
$\mathbf{a}_{\{1,2,5\}}$	$\mathbf{e}_{4,3}$	$\mathbf{e}_{4,3}$	$\mathbf{a}_{\{2,3,6\}}$	$\mathbf{e}_{4,1},\mathbf{e}_{4,4}$	$3\mathbf{e}_{4,1}+4\mathbf{e}_{4,4}$
$\mathbf{a}_{\{1,2,6\}}$	$\mathbf{e}_{4,4}$	$\mathbf{e}_{4,4}$	$\mathbf{a}_{\{2,4,5\}}$	$\mathbf{e}_{4,2},\mathbf{e}_{4,3}$	0_4
$\mathbf{a}_{\{1,3,4\}}$	$\mathbf{e}_{4,1},\mathbf{e}_{4,2}$	$\mathbf{e}_{4,1}+4\mathbf{e}_{4,2}$	$\mathbf{a}_{\{2,4,6\}}$	$\mathbf{e}_{4,2},\mathbf{e}_{4,4}$	0_4
$\mathbf{a}_{\{1,3,5\}}$	$\mathbf{e}_{4,1},\mathbf{e}_{4,3}$	$3\mathbf{e}_{4,1}+4\mathbf{e}_{4,3}$	$\mathbf{a}_{\{2,5,6\}}$	$\mathbf{e}_{4,3},\mathbf{e}_{4,4}$	0_4
$\mathbf{a}_{\{1,3,6\}}$	$\mathbf{e}_{4,1},\mathbf{e}_{4,4}$	$\mathbf{e}_{4,1}+2\mathbf{e}_{4,4}$	$\mathbf{a}_{\{3,4,5\}}$	$\mathbf{e}_{4,1},\mathbf{e}_{4,2},\mathbf{e}_{4,3}$	$\mathbf{e}_{4,1}+\mathbf{e}_{4,2}+\mathbf{e}_{4,3}$
$\mathbf{a}_{\{1,4,5\}}$	$\mathbf{e}_{4,2},\mathbf{e}_{4,3}$	0_4	$\mathbf{a}_{\{3,4,6\}}$	$\mathbf{e}_{4,1},\mathbf{e}_{4,2},\mathbf{e}_{4,4}$	$\mathbf{e}_{4,1}+2\mathbf{e}_{4,2}+\mathbf{e}_{4,4}$
$\mathbf{a}_{\{1,4,6\}}$	$\mathbf{e}_{4,2},\mathbf{e}_{4,4}$	0_4	$\mathbf{a}_{\{3,5,6\}}$	$\mathbf{e}_{4,1},\mathbf{e}_{4,3},\mathbf{e}_{4,4}$	$\mathbf{e}_{4,1}+2\mathbf{e}_{4,3}-\mathbf{e}_{4,4}$
$\mathbf{a}_{\{1,5,6\}}$	$\mathbf{e}_{4,3},\mathbf{e}_{4,4}$	0_4	$\mathbf{a}_{\{4,5,6\}}$	$\mathbf{e}_{4,2},\mathbf{e}_{4,3},\mathbf{e}_{4,4}$	0_4

- **Step 3: Determine the vector $\mathbf{b}_{\mathcal{V}}$ for each $\mathbf{a}_{\mathcal{V}}$:** for each $\mathbf{a}_{\mathcal{V}}$ where $[\mathsf{K}-\mathsf{U}]\nsubseteq\mathcal{V}$, determine the coefficients of the base vertical unit vectors which compose $\mathbf{a}_{\mathcal{V}}$.

In the following, we describe the three-step vector selection for the general case where $\mathsf{U}>\mathsf{K}-\mathsf{U}+1$ and $\mathsf{U}<\mathsf{K}-1$ in detail.

Step 1. For each $j\in[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]$, we let

$$\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{j\}}=\mathbf{e}_{\mathsf{U},j-\mathsf{K}+\mathsf{U}}. \tag{47}$$

In other words, we let

$$[\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{\mathsf{K}-\mathsf{U}+1\}},\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{\mathsf{K}-\mathsf{U}+2\}},\ldots,\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{\mathsf{K}\}}]$$

be the identity matrix $\mathbf{I}_{\mathsf{U}}$.

For the ease of notation, we define that[20]

$$\mathcal{G}_1:=\{[\mathsf{K}-\mathsf{U}]\cup\{j\}:j\in[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]\}.$$

It can be seen that

$$|\mathcal{G}_1|=\mathsf{U}. \tag{48}$$

Step 2. For each $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}\setminus\mathcal{G}_1$, we let $\mathbf{a}_{\mathcal{V}}$ be a linear combination of some base unit vectors; the composition of $\mathbf{a}_{\mathcal{V}}$ represents the set of base unit vectors involved in the linear combination. For each $i\in[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]\cap\mathcal{V}$, $\mathbf{e}_{\mathsf{U},i-(\mathsf{K}-\mathsf{U})}$ is in the composition of $\mathbf{a}_{\mathcal{V}}$. After fixing the composition of $\mathbf{a}_{\mathcal{V}}$, we can write

$$\mathbf{a}_{\mathcal{V}}=\sum_{i\in[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]\cap\mathcal{V}}b_{\mathcal{V},i-(\mathsf{K}-\mathsf{U})}\mathbf{e}_{\mathsf{U},i-(\mathsf{K}-\mathsf{U})}, \tag{49}$$

where $\mathbf{b}_{\mathcal{V}}:=(b_{\mathcal{V},1},\ldots,b_{\mathcal{V},|[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]\cap\mathcal{V}|})$ is an $|[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]\cap\mathcal{V}|$-dimensional vector to be designed. For the ease of notation, we define $\mathcal{M}_{\mathcal{V}}:=[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]\cap\mathcal{V}$.

Step 3. We divide the sets in $\binom{[\mathsf{K}]}{\mathsf{S}}\setminus\mathcal{G}_1$ into three classes, which are then considered sequentially. In short, for each set $\mathcal{V}$ in the first class (denoted by $\mathcal{G}_2$ to be clarified later), we choose $\mathbf{b}_{\mathcal{V}}$ uniformly and i.i.d. over $\mathbb{F}_{\mathsf{q}}^{|\mathcal{M}_{\mathcal{V}}|}$; for each set $\mathcal{V}$ in the second class (denoted by $\mathcal{G}_3$ to be clarified later), we choose $\mathbf{b}_{\mathcal{V}}$ such that $\mathbf{a}_{\mathcal{V}}$ is also a linear combination of some vectors $\mathbf{a}_{\mathcal{V}_1}$ where $\mathcal{V}_1\in\mathcal{G}_2$; for each set $\mathcal{V}$ in the third class (i.e., $\binom{[\mathsf{K}]}{\mathsf{S}}\setminus(\mathcal{G}_1\cup\mathcal{G}_2\cup\mathcal{G}_3)$), we let $\mathbf{b}_{\mathcal{V}}$ be a all-zero vector.

More precisely,

- We first consider the sets in[21]

$$\mathcal{G}_2:=\big\{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\}:j\in([\mathsf{K}-\mathsf{U}]\cup[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}])\big\}.$$

Recall that $2\mathsf{U}>\mathsf{K}+1$, thus $\mathsf{K}>2\mathsf{K}-2\mathsf{U}+1$ and $[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}]$ is not empty. Since $\mathsf{U}<\mathsf{K}-1$, we have $\mathsf{K}-\mathsf{U}\geq 2$ and thus $\mathcal{G}_1\cap\mathcal{G}_2=\emptyset$. It can be seen that

$$|\mathcal{G}_2|=\mathsf{K}-\mathsf{U}+(\mathsf{K}-2\mathsf{K}+2\mathsf{U})=\mathsf{U}. \tag{50}$$

For each $\mathcal{V}\in\mathcal{G}_2$, we choose $\mathbf{b}_{\mathcal{V}}$ uniformly and i.i.d. over $\mathbb{F}_{\mathsf{q}}^{|\mathcal{M}_{\mathcal{V}}|}$. More precisely,

  - for each $j\in[\mathsf{K}-\mathsf{U}]$, by assuming $\mathcal{V}=[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\}$, it can be seen that

$$\mathcal{M}_{\mathcal{V}}=\{\mathsf{K}-\mathsf{U}+1,\mathsf{K}-\mathsf{U}+2,\ldots,2\mathsf{K}-2\mathsf{U}\},$$

and thus from (49), $\mathbf{a}_{\mathcal{V}}$ is with the form

$$\mathbf{a}_{\mathcal{V}}=b_{\mathcal{V},1}\ \mathbf{e}_{\mathsf{U},1}+\cdots+b_{\mathcal{V},\mathsf{K}-\mathsf{U}}\ \mathbf{e}_{\mathsf{U},\mathsf{K}-\mathsf{U}}. \tag{51}$$

We let each $b_{\mathcal{V},i}$, $i\in[\mathsf{K}-\mathsf{U}]$, be chosen uniformly and i.i.d. over $\mathbb{F}_{\mathsf{q}}$;

  - for each $j\in[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}]$, by assuming $\mathcal{V}=[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\}$, it can be seen that

$$\mathcal{M}_{\mathcal{V}}=\{\mathsf{K}-\mathsf{U}+1,\mathsf{K}-\mathsf{U}+2,\ldots,2\mathsf{K}-2\mathsf{U},j\},$$

and thus from (49), $\mathbf{a}_{\mathcal{V}}$ is with the form

$$\begin{aligned}\mathbf{a}_{\mathcal{V}}=&\,b_{\mathcal{V},1}\ \mathbf{e}_{\mathsf{U},1}+\cdots+b_{\mathcal{V},\mathsf{K}-\mathsf{U}}\ \mathbf{e}_{\mathsf{U},\mathsf{K}-\mathsf{U}}\\&+b_{\mathcal{V},\mathsf{K}-\mathsf{U}+1}\ \mathbf{e}_{\mathsf{U},j-\mathsf{K}+\mathsf{U}}.\end{aligned} \tag{52}$$

We let each $b_{\mathcal{V},i}$, $i\in[\mathsf{K}-\mathsf{U}+1]$, be chosen uniformly and i.i.d. over $\mathbb{F}_{\mathsf{q}}$.

- We then consider the sets in[22]

$$\mathcal{G}_3:=\Big\{\mathcal{T}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}-1]:\mathcal{T}\in\binom{[\mathsf{K}-\mathsf{U}]\cup[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}]}{2},\mathcal{T}\cap[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}]\neq\emptyset\Big\}.$$

Since $\mathsf{K}-\mathsf{U}\geq 2$, we have $\mathcal{G}_3\cap\mathcal{G}_1=\emptyset$; since the integer $2\mathsf{K}-2\mathsf{U}$ appears in each set in $\mathcal{G}_2$ and does not appear

[20] In Example 3, when $(\mathsf{K},\mathsf{U},\mathsf{S})=(6,4,3)$, we have $\mathcal{G}_1=\{[3],\{1,2,4\},\{1,2,5\},\{1,2,6\}\}$.

[21] In Example 3, when $(\mathsf{K},\mathsf{U},\mathsf{S})=(6,4,3)$, we have $\mathcal{G}_2=\{\{1,3,4\},\{2,3,4\},\{3,4,5\},\{3,4,6\}\}$.

[22] In Example 3, when $(\mathsf{K},\mathsf{U},\mathsf{S})=(6,4,3)$, we have $\mathcal{G}_3=\{\{1,3,5\},\{1,3,6\},\{2,3,5\},\{2,3,6\},\{3,5,6\}\}$.

in any set in $\mathcal{G}_3$, we have $\mathcal{G}_3 \cap \mathcal{G}_2 = \emptyset$. It can be seen that

$$|\mathcal{G}_3| = \binom{\mathsf{K}-(\mathsf{K}-\mathsf{U})}{2} - \binom{\mathsf{K}-\mathsf{U}}{2} \tag{53a}$$

$$= \frac{\mathsf{K}(2\mathsf{U}-\mathsf{K}+1)}{2} - \mathsf{U}. \tag{53b}$$

For each $\mathcal{V} \in \mathcal{G}_3$, we search for the minimum subset of $\mathcal{G}_2$ the union of whose elements is a super-set of $\mathcal{V}$; we denote this minimum subset by $\mathcal{M}'_{\mathcal{V}}$. We let $\mathbf{a}_{\mathcal{V}}$ be a linear combination of $\mathbf{a}_{\mathcal{V}_2}$ where $\mathcal{V}_2 \in \mathcal{M}'_{\mathcal{V}}$.
More precisely, for each $\mathcal{T} \in \binom{[\mathsf{K}-\mathsf{U}]\cup[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}]}{2}$ where $\mathcal{T} \cap [2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}] \neq \emptyset$,

– if $\mathcal{T} = \{i, j\}$ where $i \in [\mathsf{K}-\mathsf{U}]$ and $j \in [2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}]$, by assuming $\mathcal{V} = [\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}-1]\cup\{i,j\}$, we have

$$\mathcal{M}'_{\mathcal{V}} = \big\{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{i\}, [\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\}\big\}.$$

Define $\mathcal{M}'_{\mathcal{V}}(1) = [\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{i\}$ and $\mathcal{M}'_{\mathcal{V}}(2) = [\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\}$. Hence, we aim to let $\mathbf{a}_{\mathcal{V}}$ be a linear combination of

$$\mathbf{a}_{\mathcal{M}'_{\mathcal{V}}(1)} = b_{\mathcal{M}'_{\mathcal{V}}(1),1}\ \mathbf{e}_{\mathsf{U},1} + \cdots + b_{\mathcal{M}'_{\mathcal{V}}(1),\mathsf{K}-\mathsf{U}}\ \mathbf{e}_{\mathsf{U},\mathsf{K}-\mathsf{U}}, \tag{54a}$$

and $\mathbf{a}_{\mathcal{M}'_{\mathcal{V}}(2)} = b_{\mathcal{M}'_{\mathcal{V}}(2),1}\ \mathbf{e}_{\mathsf{U},1} + \cdots + b_{\mathcal{M}'_{\mathcal{V}}(2),\mathsf{K}-\mathsf{U}}\ \mathbf{e}_{\mathsf{U},\mathsf{K}-\mathsf{U}} + b_{\mathcal{M}'_{\mathcal{V}}(2),\mathsf{K}-\mathsf{U}+1}\ \mathbf{e}_{\mathsf{U},j-\mathsf{K}+\mathsf{U}}$, (54b)

where (54a) and (54b) come from (51) and (52), respectively. Recall that each element in $\mathbf{b}_{\mathcal{M}'_{\mathcal{V}}(1)}$ and $\mathbf{b}_{\mathcal{M}'_{\mathcal{V}}(2)}$ is chosen uniformly and i.i.d. over $\mathbb{F}_{\mathsf{q}}$.
In addition, we have

$$\mathcal{M}_{\mathcal{V}} = \{\mathsf{K}-\mathsf{U}+1, \mathsf{K}-\mathsf{U}+2, \ldots, 2\mathsf{K}-2\mathsf{U}-1, j\}.$$

Hence, from (49), $\mathbf{a}_{\mathcal{V}}$ is with the form

$$\mathbf{a}_{\mathcal{V}} = b_{\mathcal{V},1}\ \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{\mathsf{K}-\mathsf{U}+1\}} + \cdots + b_{\mathcal{V},\mathsf{K}-\mathsf{U}-1}\ \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{2\mathsf{K}-2\mathsf{U}-1\}} + b_{\mathcal{V},\mathsf{K}-\mathsf{U}}\ \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{j\}} \tag{55a}$$

$$= b_{\mathcal{V},1}\ \mathbf{e}_{\mathsf{U},1} + \cdots + b_{\mathcal{V},\mathsf{K}-\mathsf{U}-1}\ \mathbf{e}_{\mathsf{U},\mathsf{K}-\mathsf{U}-1} + b_{\mathcal{V},\mathsf{K}-\mathsf{U}}\ \mathbf{e}_{\mathsf{U},j-\mathsf{K}+\mathsf{U}}. \tag{55b}$$

By comparing (54) with the form of $\mathbf{a}_{\mathcal{V}}$ in (55b), we need to 'zero-force' $\mathbf{e}_{\mathsf{U},\mathsf{K}-\mathsf{U}}$, which could be done by letting

$$\mathbf{a}_{\mathcal{V}} = b_{\mathcal{M}'_{\mathcal{V}}(2),\mathsf{K}-\mathsf{U}}\ \mathbf{a}_{\mathcal{M}'_{\mathcal{V}}(1)} - b_{\mathcal{M}'_{\mathcal{V}}(1),\mathsf{K}-\mathsf{U}}\ \mathbf{a}_{\mathcal{M}'_{\mathcal{V}}(2)}. \tag{56}$$

– if $\mathcal{T} = \{i, j\}$ where $2\mathsf{K}-2\mathsf{U}+1 \leq i < j \leq \mathsf{K}$, by assuming $\mathcal{V} = [\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}-1]\cup\{i,j\}$, it can be seen that

$$\mathcal{M}'_{\mathcal{V}} = \big\{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{i\}, [\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\}\big\}.$$

Hence, we aim to let $\mathbf{a}_{\mathcal{V}}$ be a linear combination of

$$\mathbf{a}_{\mathcal{M}'_{\mathcal{V}}(1)} = b_{\mathcal{M}'_{\mathcal{V}}(1),1}\ \mathbf{e}_{\mathsf{U},1} + \cdots + b_{\mathcal{M}'_{\mathcal{V}}(1),\mathsf{K}-\mathsf{U}}\ \mathbf{e}_{\mathsf{U},\mathsf{K}-\mathsf{U}} + b_{\mathcal{M}'_{\mathcal{V}}(1),\mathsf{K}-\mathsf{U}+1}\ \mathbf{e}_{\mathsf{U},i-\mathsf{K}+\mathsf{U}}, \tag{57a}$$

and $\mathbf{a}_{\mathcal{M}'_{\mathcal{V}}(2)} = b_{\mathcal{M}'_{\mathcal{V}}(2),1}\ \mathbf{e}_{\mathsf{U},1} + \cdots + b_{\mathcal{M}'_{\mathcal{V}}(2),\mathsf{K}-\mathsf{U}}\ \mathbf{e}_{\mathsf{U},\mathsf{K}-\mathsf{U}} + b_{\mathcal{M}'_{\mathcal{V}}(2),\mathsf{K}-\mathsf{U}+1}\ \mathbf{e}_{\mathsf{U},j-\mathsf{K}+\mathsf{U}}$, (57b)

where (57a) and (57b) come from (52).
In addition, we have

$$\mathcal{M}_{\mathcal{V}} = \{\mathsf{K}-\mathsf{U}+1, \mathsf{K}-\mathsf{U}+2, \ldots, 2\mathsf{K}-2\mathsf{U}-1, i, j\}.$$

Hence, from (49), $\mathbf{a}_{\mathcal{V}}$ is with the form

$$\mathbf{a}_{\mathcal{V}} = b_{\mathcal{V},1}\ \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{\mathsf{K}-\mathsf{U}+1\}} + \cdots + b_{\mathcal{V},\mathsf{K}-\mathsf{U}-1}\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{2\mathsf{K}-2\mathsf{U}-1\}} + b_{\mathcal{V},\mathsf{K}-\mathsf{U}}\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{i\}} + b_{\mathcal{V},\mathsf{K}-\mathsf{U}+1}\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{j\}} \tag{58a}$$

$$= b_{\mathcal{V},1}\ \mathbf{e}_{\mathsf{U},1} + \cdots + b_{\mathcal{V},\mathsf{K}-\mathsf{U}-1}\ \mathbf{e}_{\mathsf{U},\mathsf{K}-\mathsf{U}-1} + b_{\mathcal{V},\mathsf{K}-\mathsf{U}}\ \mathbf{e}_{\mathsf{U},i-\mathsf{K}+\mathsf{U}} + b_{\mathcal{V},\mathsf{K}-\mathsf{U}+1}\ \mathbf{e}_{\mathsf{U},j-\mathsf{K}+\mathsf{U}}. \tag{58b}$$

By comparing (57) with the form of $\mathbf{a}_{\mathcal{V}}$ in (58b), we need to 'zero-force' $\mathbf{e}_{\mathsf{U},\mathsf{K}-\mathsf{U}}$, which could be done by letting

$$\mathbf{a}_{\mathcal{V}} = b_{\mathcal{M}'_{\mathcal{V}}(2),\mathsf{K}-\mathsf{U}}\ \mathbf{a}_{\mathcal{M}'_{\mathcal{V}}(1)} - b_{\mathcal{M}'_{\mathcal{V}}(1),\mathsf{K}-\mathsf{U}}\ \mathbf{a}_{\mathcal{M}'_{\mathcal{V}}(2)}. \tag{59}$$

– Finally, for each $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}} \setminus (\mathcal{G}_1 \cup \mathcal{G}_2 \cup \mathcal{G}_3)$, we let

$$\mathbf{a}_{\mathcal{V}} = 0_{\mathsf{U}}. \tag{60}$$

This concludes our selection on $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$. Next we will show that the above choice of these U-dimensional vectors satisfies the constraints in (10), (16), and (18), with high probability.

Constraints in (10)*:* For each user $k \in [\mathsf{K}-\mathsf{U}]$, the matrix

$$\big[\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{\mathsf{K}-\mathsf{U}+1\}}, \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{\mathsf{K}-\mathsf{U}+2\}}, \ldots, \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{\mathsf{K}\}}\big]$$

is the identity matrix $\mathbf{I}_{\mathsf{U}}$, whose rank is U.

For each user $k \in [\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]$, let us focus on the matrix

$$\big[\mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{1\}}, \ldots, \mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{\mathsf{K}-\mathsf{U}\}}, \mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{2\mathsf{K}-2\mathsf{U}+1\}}, \ldots, \mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{\mathsf{K}\}}\big], \tag{61}$$

whose dimension is $\mathsf{U}\times\mathsf{U}$. By our construction, for each $j \in [\mathsf{K}-\mathsf{U}]$, by (51) we have (assume $\mathcal{V} = [\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\}$)

$$\mathbf{a}_{\mathcal{V}} = b_{\mathcal{V},1}\ \mathbf{e}_{\mathsf{U},1} + \cdots + b_{\mathcal{V},\mathsf{K}-\mathsf{U}}\ \mathbf{e}_{\mathsf{U},\mathsf{K}-\mathsf{U}}, \tag{62}$$

where $b_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\},i}$, $i \in [\mathsf{K}-\mathsf{U}]$, is chosen uniformly and i.i.d. over $\mathbb{F}_{\mathsf{q}}$. In addition, for each $j \in [2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}]$, by (52) we have (assume $\mathcal{V} = [\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\}$)

$$\mathbf{a}_{\mathcal{V}} = b_{\mathcal{V},1}\mathbf{e}_{\mathsf{U},1} + \cdots + b_{\mathcal{V},\mathsf{K}-\mathsf{U}}\mathbf{e}_{\mathsf{U},\mathsf{K}-\mathsf{U}} + b_{\mathcal{V},\mathsf{K}-\mathsf{U}+1}\mathbf{e}_{\mathsf{U},j-\mathsf{K}+\mathsf{U}}, \tag{63}$$

where each $b_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\},i}$, $i \in [\mathsf{K}-\mathsf{U}+1]$, is chosen uniformly and i.i.d. over $\mathbb{F}_{\mathsf{q}}$. Since q is large enough, from (62) and (63), it can be seen that the matrix in (61) has rank equal to U with high probability.

For each user $k \in [2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}]$, let us focus on the

matrix

$$\big[\mathbf{a}_{\{1\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}-1]\cup\{k\}}, \mathbf{a}_{\{2\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}-1]\cup\{k\}}, \ldots, \mathbf{a}_{\{\mathsf{K}-\mathsf{U}\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}-1]\cup\{k\}}, \mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}-1]\cup\{2\mathsf{K}-2\mathsf{U},k\}}, \mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}-1]\cup\{2\mathsf{K}-2\mathsf{U}+1,k\}}, \ldots, \mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}-1]\cup\{k-1,k\}}, \mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}-1]\cup\{k,k+1\}}, \ldots, \mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}-1]\cup\{k,\mathsf{K}\}}\big], \tag{64}$$

whose dimension is $\mathsf{U}\times\mathsf{U}$. For each $j\in[\mathsf{K}-\mathsf{U}]$, by (56), we have

$$\begin{aligned}&\mathbf{a}_{\{j\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}-1]\cup\{k\}}\\&= b_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{k\},\mathsf{K}-\mathsf{U}}\ \mathbf{a}_{\{j\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]}\\&- b_{\{j\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}],\mathsf{K}-\mathsf{U}}\ \mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{k\}},\end{aligned} \tag{65}$$

where $b_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{k\},\mathsf{K}-\mathsf{U}}$ and $b_{\{j\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}],\mathsf{K}-\mathsf{U}}$ are chosen uniformly and i.i.d. over $\mathbb{F}_\mathsf{q}$. For each $j\in[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}]\setminus\{k\}$, by (59), we have (66) at the top of the next page, where $b_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{k\},\mathsf{K}-\mathsf{U}}$ and $b_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\},\mathsf{K}-\mathsf{U}}$ are chosen uniformly and i.i.d. over $\mathbb{F}_\mathsf{q}$. In addition, as we showed before, $\mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{1\}},\ldots,\mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{\mathsf{K}-\mathsf{U}\}}$, $\mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{2\mathsf{K}-2\mathsf{U}+1\}},\ldots,\mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{\mathsf{K}\}}$ which are the columns of the matrix in (61), are linearly independent with high probability. Hence, by (65), (66), and the fact that $\mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}-1]\cup\{2\mathsf{K}-2\mathsf{U},k\}}=\mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{k\}}$ is in the matrix in (64), we can see that the matrix in (64) is full rank with high probability.

Hence, the constraints in (10) are satisfied with high probability.

Constraints in (16)*:* For each user $k\in[\mathsf{K}-\mathsf{U}]$, the sets in $\mathcal{V}\in\binom{[\mathsf{K}]\setminus\{k\}}{\mathsf{S}}$ do not contain k. By our construction, it can be seen that

$$\binom{[\mathsf{K}]\setminus\{k\}}{\mathsf{S}}\cap\mathcal{G}_1=\emptyset, \tag{67a}$$

$$\binom{[\mathsf{K}]\setminus\{k\}}{\mathsf{S}}\cap\mathcal{G}_2=\{\{j\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]:\ j\in[\mathsf{K}]\setminus(\{k\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}])\}, \tag{67b}$$

$$\binom{[\mathsf{K}]\setminus\{k\}}{\mathsf{S}}\cap\mathcal{G}_3=\Big\{\mathcal{T}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}-1]:\ \mathcal{T}\in\binom{([\mathsf{K}-\mathsf{U}]\cup[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}])\setminus\{k\}}{2},\ \mathcal{T}\cap[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}]\neq\emptyset\Big\}. \tag{67c}$$

Focus on the sets in (67b). Since the matrix in (61) is full rank with high probability, the $\mathsf{U}-1$ vectors in

$$\{\mathbf{a}_{\{j\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]}:\ j\in[\mathsf{K}]\setminus(\{k\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}])\} \tag{68}$$

are linearly independent with high probability.

Focus on the sets in (67c). For each $\mathcal{T}\in\binom{([\mathsf{K}-\mathsf{U}]\cup[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}])\setminus\{k\}}{2}$ where $\mathcal{T}\cap[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}]\neq\emptyset$, by assuming that $\mathcal{V}=\mathcal{T}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}-1]$ and $\mathcal{T}=\{i,j\}$ where $i<j$, it can be seen from (56) and (59) that

$$\begin{aligned}\mathbf{a}_\mathcal{V}&= b_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\},\mathsf{K}-\mathsf{U}}\ \mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{i\}}\\&- b_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{i\},\mathsf{K}-\mathsf{U}}\ \mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\}},\end{aligned} \tag{69}$$

where both $\mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{i\}}$ and $\mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\}}$ are in (68).

Recall that for each set $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}\setminus(\mathcal{G}_1\cup\mathcal{G}_2\cup\mathcal{G}_3)$, from (60) we have $\mathbf{a}_\mathcal{V}=0_\mathsf{U}$. As a result, the matrix $\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}},\ldots,\mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}}\right]$ has rank equal to $\mathsf{U}-1$ with high probability, which is the same as its column-wise sub-matrix (whose dimension is $\mathsf{U}\times(\mathsf{U}-1)$)

$$\begin{aligned}&[\mathbf{a}_{\{1\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]},\ldots,\mathbf{a}_{\{k-1\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]},\\&\mathbf{a}_{\{k+1\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]},\ldots,\mathbf{a}_{\{\mathsf{K}-\mathsf{U}\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]},\\&\mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{\mathsf{K}-\mathsf{U}+1\}},\ldots,\mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{\mathsf{K}\}}],\end{aligned} \tag{70}$$

where $\mathbf{a}_{\{j_1\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]}$, $j_1\in[\mathsf{K}-\mathsf{U}]\setminus\{k\}$ is given in (62) and $\mathbf{a}_{\{j_2\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]}$, $j_2\in[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}]$ is given in (63).

For each user $k\in[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]$, among the sets in $\mathcal{V}\in\binom{[\mathsf{K}]\setminus\{k\}}{\mathsf{S}}$ which do not contain k, we can see that in $\mathbf{a}_\mathcal{V}$ the coefficient of $\mathbf{e}_{\mathsf{U},k-\mathsf{K}+\mathsf{U}}$ is 0. This could be directly checked from the second step to select the U-dimensional vectors, where we fix the composition of $\mathbf{a}_\mathcal{V}$ in (49). Thus the rank of $\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}},\ldots,\mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}}\right]$ is no more than $\mathsf{U}-1$. In addition, its column-wise sub-matrix

$$\begin{aligned}&[\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{\mathsf{K}-\mathsf{U}+1\}},\ldots,\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{k-1\}},\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{k+1\}},\ldots,\\&\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{\mathsf{K}\}}]\\&=[\mathbf{e}_{\mathsf{U},1},\ldots,\mathbf{e}_{\mathsf{U},k-\mathsf{K}+\mathsf{U}-1},\mathbf{e}_{\mathsf{U},k-\mathsf{K}+\mathsf{U}+1},\ldots,\mathbf{e}_{\mathsf{U},\mathsf{U}}],\end{aligned} \tag{71}$$

has rank equal to $\mathsf{U}-1$. Hence, the rank of $\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}},\ldots,\mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}}\right]$ is $\mathsf{U}-1$.

Hence, the constraints in (16) are satisfied with high probability.

Constraint in (18)*:* For each user $k\in[\mathsf{K}-\mathsf{U}]$, as we showed before, the matrix $\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}},\ldots,\mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}}\right]$ has the same rank equal to $\mathsf{U}-1$, as its column-wise sub-matrix in (70). Hence, the left null space of the matrix $\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}},\ldots,\mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}}\right]$ is the same as that of its column-wise sub-matrix in (70). Since the matrix in (70) has dimension $\mathsf{U}\times(\mathsf{U}-1)$ and rank $\mathsf{U}-1$ with high probability, its left null space contains exactly one linearly independent left null vector (with dimension $1\times\mathsf{U}$). Let $\mathbf{s}_k$ be one left null vector of the matrix in (70).

For each user $k\in[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]$, the matrix $\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}},\ldots,\mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}}\right]$ has the same rank equal to $\mathsf{U}-1$, as its column-wise sub-matrix in (71). Hence, the left null space of the matrix $\left[\mathbf{a}_{\overline{\mathcal{S}}_{k,1}},\ldots,\mathbf{a}_{\overline{\mathcal{S}}_{k,\binom{\mathsf{K}-1}{\mathsf{S}}}}\right]$ is the same as that of its column-wise sub-matrix in (71), which contains exactly one linearly independent left null vector. One possible choice of the left null vector could be

$$\mathbf{s}_k=\mathbf{e}_{\mathsf{U},k-\mathsf{K}+\mathsf{U}}^\mathsf{T}. \tag{72}$$

The most difficult part in the proof of the constraint in (18) is the following lemma, which will be proved in Appendix D

$$\mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}-1]\cup\{j,k\}} = \begin{cases} b_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{k\},\mathsf{K}-\mathsf{U}}\ \mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\}} - b_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\},\mathsf{K}-\mathsf{U}}\ \mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{k\}}, & \text{if } j<k; \\ b_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\},\mathsf{K}-\mathsf{U}}\ \mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{k\}} - b_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{k\},\mathsf{K}-\mathsf{U}}\ \mathbf{a}_{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\}}, & \text{if } j>k, \end{cases} \tag{66}$$

by the Schwartz-Zippel lemma [34]–[36].

Lemma 3. *For any $\mathcal{A} \subseteq [\mathsf{K}]$ where $|\mathcal{A}| = \mathsf{U}$, the U-dimensional vectors $\mathbf{s}_k$ where $k \in \mathcal{A}$ are linearly independent with high probability.* □

Directly from Lemma 3, it can be seen that the constraint in (18) is satisfied with high probability.

In conclusion, all constraints in (10), (16), and (18) are satisfied with high probability. Hence, there must exist a choice of $\mathbf{b}_{\mathcal{V}}$ where $\mathcal{V} \in \mathcal{G}_2$ satisfying those constraints. Thus the proposed scheme is decodable and secure. In this case, we need the keys $Z_{\mathcal{V}}$ where $\mathcal{V} \in (\mathcal{G}_1 \cup \mathcal{G}_2 \cup \mathcal{G}_3)$. It can be seen from (48), (50), and (53b) that there are totally

$$\mathsf{U} + \mathsf{U} + \frac{\mathsf{K}(2\mathsf{U}-\mathsf{K}+1)}{2} - \mathsf{U} = \mathsf{U} + \frac{\mathsf{K}(2\mathsf{U}-\mathsf{K}+1)}{2}$$

keys each of which is shared by S users.

V. Experimental Results

We implement our proposed secure aggregation scheme (which is referred to as `Group` for the sake of simplicity) in Python2.7 by using the MPI4py library over the Amazon EC2 cloud, which is then compared to the original secure aggregation scheme in [6] (referred to as `Sec`), and the best existing information theoretic secure aggregation scheme with offline key sharing in [10] (referred to as `Light`). We compare the key sharing times of `Group` and `Light`, since the communication costs in the model aggregation phase of these two schemes are the same. In addition, since `Sec` provides computational security instead of information theoretic security, the total size of needed keys is much smaller in `Sec`. Thus we compare the model aggregation times of `Group` and `Sec`. Note that in the experiments, we only record the the communication time as the running time in each procedure; the detail of running times in each procedure of `Group`, `Light`, and `Sec` could be found in Appendix E.

Amazon EC2 Setup. The Amazon EC2 `t2.large` and `t2.xlarge` instances are selected, where we take one specific `t2.xlarge` instance as the server and all the other instances are users. The Amazon EC2 T2 instances have a 3.0 GHz Intel Scalable Processor, and all instances which we use in this experiment have the same capacity of computation, memory and network resources. The transmission speed is up to 100MB/s between the server and users. By setting the field size q as 7, we generate the input vectors uniformly i.i.d. over $\mathbb{F}_7$, and consider the three sizes of each input vector (100KB, 200KB, 300KB) as suggested in [6]. In the offline key sharing phase, we consider that each two users have a private link to communicate as in [10];[23] thus between each two users, we use the `MPI.send` command. For each considered system with $(\mathsf{K}, \mathsf{U}, \mathsf{S})$, we use Monte-Carlo methods with 20 samples and take the average times over these 20 samples.

[23]In this framework, to generate an uncoded groupwise key shared among S users, we need $\mathsf{S}-1$ pairwise key sharing communications.

`Group` v.s. `Light`. We first compare our `Group` with `Light`, by considering the two cases where $\mathsf{U} = (\mathsf{K}+1)/2$ illustrated in Fig. 2a and $\mathsf{U} = \mathsf{K}-1$ illustrated in Fig. 2b, respectively. For each case, our `Group` needs $\mathsf{S} = \mathsf{K}-\mathsf{U}+1$.

In Fig. 2a, since $\mathsf{U} = (\mathsf{K}+1)/2$, we have $\mathsf{U} = \mathsf{K}-\mathsf{U}+1$ and thus our secure aggregation scheme is the one in Section IV-A. We use the cyclic key assignment; more precisely, for each $i \in [\mathsf{K}]$, we let user i randomly generate a key $Z_{\mathcal{C}(i)}$ with $(\mathsf{K}-\mathsf{U}+1)\mathsf{L}/\mathsf{U} = \mathsf{L}$ symbols, and transmit $Z_{\mathcal{C}(i)}$ to the other $\mathsf{U}-1$ users in $\mathcal{C}(i)$, where $\mathcal{C}$ is defined in (25). Compared to `Light`, `Group` reduces the key sharing time by at least 16.5% and at most 31.7% in Fig. 2a. The improvement of `Group` is mainly because the number of keys is smaller than that of `Light`, and thus less number of connections is needed to build among users.

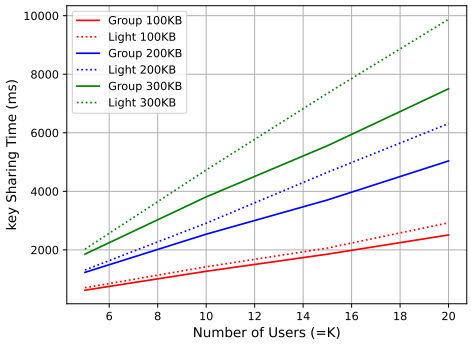
In Fig. 2b, since $\mathsf{U} = \mathsf{K}-1$, our secure aggregation scheme is the one in Section IV-B. In this case, for each pair of users $\mathcal{V} = \{\mathcal{V}(1), \mathcal{V}(2)\}$ where $\mathcal{V} \subseteq [\mathsf{K}]$, $|\mathcal{V}| = 2$, and $\mathcal{V}(1) < \mathcal{V}(2)$, there is one key $Z_{\mathcal{V}} = \{Z_{\mathcal{V},\mathcal{V}(1)}, Z_{\mathcal{V},\mathcal{V}(2)}\}$ with $(\mathsf{K}-\mathsf{U}+1)\mathsf{L}/\mathsf{U} = 2\mathsf{L}/\mathsf{U}$ symbols shared by users in $\mathcal{V}$. We consider two ways of key sharing: (i) "`Group`" in Fig. 2b: user $\mathcal{V}(1)$ randomly generates $Z_{\mathcal{V}}$ and sends $Z_{\mathcal{V}}$ to user $\mathcal{V}(2)$; (ii) "`Group_1`" in Fig. 2b: user $\mathcal{V}(1)$ randomly generates $Z_{\mathcal{V},\mathcal{V}(1)}$ and sends $Z_{\mathcal{V},\mathcal{V}(1)}$ to user $\mathcal{V}(2)$, while user $\mathcal{V}(2)$ randomly generates $Z_{\mathcal{V},\mathcal{V}(2)}$ and sends $Z_{\mathcal{V},\mathcal{V}(2)}$ to user $\mathcal{V}(1)$. Compared to `Light`, `Group` increase the key sharing time by at least 11.2% and at most 23.7% in Fig. 2b, while the key sharing time of `Group_1` is close to that of `Light`. The reason that the key sharing time of `Group` is more than that of `Light` is because the transmissions of users in Amazon EC2 are parallel, and in `Group` the users with smaller indices transmit more keys in the key sharing phase. In `Group_1`, we "balance" the numbers of user transmissions which reduce key sharing time.

`Group` v.s. `Sec`. We then compare our `Group` with `Sec`, by considering the two cases where $\mathsf{U} = (\mathsf{K}+1)/2$ illustrated in Fig. 2c and $\mathsf{U} = \mathsf{K}-1$ illustrated in Fig. 2d, respectively. Compared to `Sec`, `Group` reduces the model aggregation time by at least 48% and at most 53% in Fig. 2c, and reduces the model aggregation time by at least 33% and at most 44% in Fig. 2d. From the theoretic viewpoint, this improvement is because our `Group` achieves the optimal communication cost in the model aggregation phase, while `Sec` is sub-optimal.

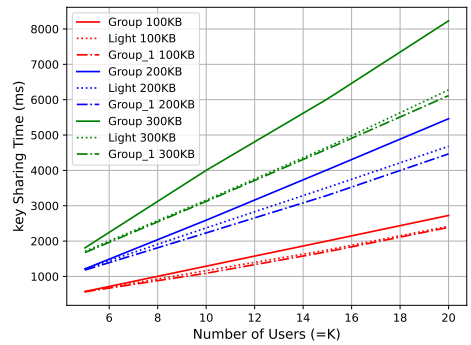
VI. Conclusions

In this paper, we formulated the information theoretic secure aggregation problem with uncoded groupwise keys, where the

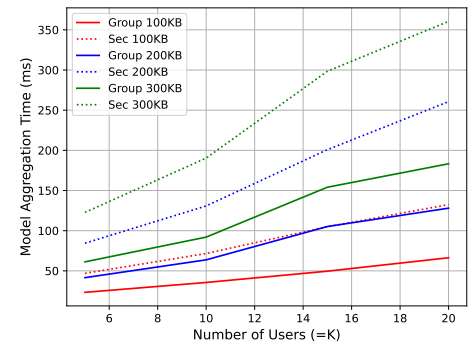
This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3422087



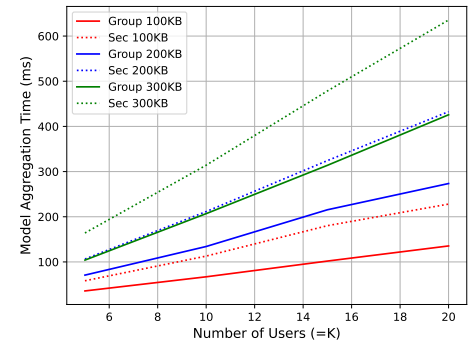
(a) Group v.s. Light: $\mathsf{U} = (\mathsf{K}+1)/2$



(b) Group (Group_1) v.s. Light: $\mathsf{U} = \mathsf{K}-1$



(c) Group v.s. Sec: $\mathsf{U} = (\mathsf{K}+1)/2$



(d) Group v.s. Sec: $\mathsf{U} = \mathsf{K}-1$

Fig. 2: The key sharing time and the model aggregation time of Group versus Light and Sec, respectively.

keys are independent of each other and each of them is shared by a group of users. For the case $\mathsf{S} > \mathsf{K}-\mathsf{U}$, we proposed a new secure aggregation scheme, which is the first scheme with uncoded keys. Quite surprisingly, the proposed scheme with uncoded groupwise keys achieves the same capacity region of the communication rates in the two-round transmissions as the optimal scheme with any possible keys. In addition, to achieve the capacity region, we showed that not all keys shared by S users are needed; instead, the number of keys used in the proposed scheme is no more than $\mathcal{O}(\mathsf{K}^2)$. When $\mathsf{S} \leq \mathsf{K}-\mathsf{U}$, by proposing a new converse bound under the constraint of uncoded groupwise keys, we showed that uncoded groupwise keys sharing is strictly sub-optimal compared to coded keys sharing.

Ongoing work includes the characterization of the capacity region for the case $\mathsf{S} \leq \mathsf{K}-\mathsf{U}$ and the extension of the proposed secure aggregation scheme to tolerate the collusion between the server and the users.

Appendix A
Proof of Theorem 2

We first consider the case $1 = \mathsf{S} \leq \mathsf{K}-\mathsf{U}$. In this case, it can be seen that $\mathsf{U} \leq \mathsf{K}-1$. We will show by contradiction that there does not exist any feasible secure aggregation scheme.

Assume that there exists one feasible secure aggregation scheme. When $\mathcal{U}_1 = [\mathsf{U}+1]$ and $\mathcal{U}_2 = [2:\mathsf{U}+1]$, the server can recover $\sum_{k\in[\mathsf{U}+1]} W_k$; thus

$$0 = H\left(W_1+\cdots+W_{\mathsf{U}+1}|X_1,(X_{k_1},Y_{k_1}^{[\mathsf{U}+1]}:k_1\in[2:\mathsf{U}+1])\right) \tag{73a}$$

$$\geq H\left(W_1+\cdots+W_{\mathsf{U}+1}|X_1,(W_{k_1},Z_{\{k_1\}}:k_1\in[2:\mathsf{U}+1])\right) \tag{73b}$$

$$= H\left(W_1|X_1,(W_{k_1},Z_{\{k_1\}}:k_1\in[2:\mathsf{U}+1])\right) \tag{73c}$$

$$= H(W_1|X_1), \tag{73d}$$

where (73b) follows since $(X_{k_1},Y_{k_1}^{[\mathsf{U}+1]}:k_1\in[2:\mathsf{U}+1])$ is a function of $(W_{k_1},Z_{\{k_1\}}:k_1\in[2:\mathsf{U}+1])$ and condition does not increase entropy, (73d) follows since X_k is a function of $(W_1,Z_{\{1\}})$ and $(W_1,Z_{\{1\}})$ is independent of $(W_2,\ldots,W_{\mathsf{U}+1},Z_{\{2\}},\ldots,Z_{\{\mathsf{U}+1\}})$. However, by the security constraint in (5), we should have $I(X_1;W_1)=0$, which leads (recall that W_1 contains L uniform and i.i.d. symbols over $\mathbb{F}_\mathsf{q}$)

$$H(W_1|X_1) = H(W_1) - I(X_1;W_1) = \mathsf{L}. \tag{74}$$

Hence, (74) contradicts to (73d).

In the rest of this proof, we consider the case where $2 \leq \mathsf{S} \leq \mathsf{K}-\mathsf{U}$. By the converse bound in Lemma 1, we have $\mathsf{R}_1 \geq 1$. Hence, for any feasible secure aggregation scheme, we can assume that it achieves $\mathsf{R}_1 = 1+\mathsf{a}$, where $\mathsf{a}\geq 0$. Then in the following, we focus on this scheme.

For each $k\in[\mathsf{K}]$, when $|\mathcal{U}_1|\geq \mathsf{U}+1$, $k\in\mathcal{U}_1$, and $\mathcal{U}_2 = \mathcal{U}_1\setminus\{k\}$, the server can recover $\sum_{k_1\in\mathcal{U}_1} W_{k_1}$; thus we have

$$0 = H\left(\sum_{k_1\in\mathcal{U}_1} W_{k_1}\Big|X_k,(X_{k_2},Y_{k_2}^{\mathcal{U}_1}:k_2\in\mathcal{U}_2)\right) \tag{75a}$$

$$\geq H\left(\sum_{k_1\in\mathcal{U}_1} W_{k_1}\Big|X_k, Z_k, (W_{k_2}, Z_{k_2} : k_2 \in \mathcal{U}_2)\right) \quad (75b)$$
$$= H(W_k|X_k, Z_k, (W_{k_2}, Z_{k_2} : k_2 \in \mathcal{U}_2)), \quad (75c)$$

where (75b) follows since $(X_{k_2}, Y_{k_2}^{\mathcal{U}_1} : k_2 \in \mathcal{U}_2)$ is a function of $(W_{k_2}, Z_{k_2} : k_2 \in \mathcal{U}_2)$, and condition does not increase entropy. From (75c), we have

$$H(X_k|Z_k) \geq H(X_k|Z_k, (W_{k_2}, Z_{k_2} : k_2 \in \mathcal{U}_2)) \quad (76a)$$
$$= I(W_k; X_k|Z_k, (W_{k_2}, Z_{k_2} : k_2 \in \mathcal{U}_2))$$
$$+ H(X_k|W_k, Z_k, (W_{k_2}, Z_{k_2} : k_2 \in \mathcal{U}_2)) \quad (76b)$$
$$= I(W_k; X_k|Z_k, (W_{k_2}, Z_{k_2} : k_2 \in \mathcal{U}_2)) \quad (76c)$$
$$= H(W_k|Z_k, (W_{k_2}, Z_{k_2} : k_2 \in \mathcal{U}_2))$$
$$- H(W_k|X_k, Z_k, (W_{k_2}, Z_{k_2} : k_2 \in \mathcal{U}_2)) \quad (76d)$$
$$\overset{(75c)}{\geq} H(W_k|Z_k, (W_{k_2}, Z_{k_2} : k_2 \in \mathcal{U}_2)) \quad (76e)$$
$$= H(W_k) = \mathsf{L}, \quad (76f)$$

where (76c) follows since X_k is a function of (W_k, Z_k). From (76f), we have

$$I(W_k; X_k|Z_k) = H(X_k|Z_k) - H(X_k|Z_k, W_k) \quad (77a)$$
$$= H(X_k|Z_k) \quad (77b)$$
$$\overset{(76f)}{\geq} \mathsf{L}. \quad (77c)$$

From (77c), we have

$$H(X_k|Z_k) = I(W_k; X_k|Z_k) + H(X_k|Z_k, W_k) \geq \mathsf{L}. \quad (78)$$

In addition, from (77c) we also have

$$H(W_k|Z_k, X_k) = H(W_k|Z_k) - I(W_k; X_k|Z_k) \quad (79a)$$
$$\overset{(77c)}{\leq} H(W_k|Z_k) - \mathsf{L} = 0. \quad (79b)$$

We define that $\mathcal{V}_k' := \left\{\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}} : k \in \mathcal{V}\right\}$, and sort the sets in $\mathcal{V}_k'$ in a lexicographic order. $\mathcal{V}_k'(j)$ represents the j^{th} set in $\mathcal{V}_k'$, where $j \in \left[\binom{\mathsf{K}-1}{\mathsf{S}-1}\right]$. Since $2 \leq \mathsf{S} \leq \mathsf{K}-\mathsf{U}$, we can see that $\binom{\mathsf{K}-1}{\mathsf{S}-1} \geq 2$. For any set $\mathcal{S} \subseteq \mathcal{V}_k'$, from (78) we have

$$\mathsf{L} \overset{(78)}{\leq} H(X_k|Z_k) \leq H(X_k|(Z_{\mathcal{V}} : \mathcal{V} \in \mathcal{S}))$$
$$\leq H(X_k) \leq \mathsf{R}_1 = \mathsf{L}(1+\mathsf{a}).$$

Hence, we have

$$\mathsf{L} \leq H(X_k|(Z_{\mathcal{V}} : \mathcal{V} \in \mathcal{S})) \leq \mathsf{L}(1+\mathsf{a}). \quad (80)$$

For any collections of sets $\mathcal{S}, \mathcal{S}' \subseteq \mathcal{V}_k'$ we have (which will be proved in Appendix B)

$$H(W_k|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{S})) + H(W_k|X_k, (Z_{\mathcal{V}_2} : \mathcal{V}_2 \in \mathcal{S}'))$$
$$\geq H(W_k|X_k, (Z_{\mathcal{V}_0} : \mathcal{V}_0 \in \mathcal{S} \cup \mathcal{S}'))$$
$$+ H(W_k|X_k, (Z_{\mathcal{V}_5} : \mathcal{V}_5 \in \mathcal{S} \cap \mathcal{S}')) - I\big((Z_{\mathcal{V}_4} : \mathcal{V}_4 \in \mathcal{S} \setminus \mathcal{S}');$$
$$(Z_{\mathcal{V}_3} : \mathcal{V}_3 \in \mathcal{S}' \setminus \mathcal{S})|X_k, (Z_{\mathcal{V}_5} : \mathcal{V}_5 \in \mathcal{S} \cap \mathcal{S}')\big). \quad (81)$$

In addition, we have

$$I\big((Z_{\mathcal{V}_4} : \mathcal{V}_4 \in \mathcal{S} \setminus \mathcal{S}');$$
$$(Z_{\mathcal{V}_3} : \mathcal{V}_3 \in \mathcal{S}' \setminus \mathcal{S})|X_k, (Z_{\mathcal{V}_5} : \mathcal{V}_5 \in \mathcal{S} \cap \mathcal{S}')\big) \quad (82a)$$
$$\leq I((Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{S}); (Z_{\mathcal{V}_3} : \mathcal{V}_3 \in \mathcal{S}' \setminus \mathcal{S})|X_k) \quad (82b)$$
$$= H((Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{S})|X_k) + H((Z_{\mathcal{V}_3} : \mathcal{V}_3 \in \mathcal{S}' \setminus \mathcal{S})|X_k)$$
$$- H((Z_{\mathcal{V}_0} : \mathcal{V}_0 \in \mathcal{S} \cup \mathcal{S}')|X_k) \quad (82c)$$
$$\leq H(Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{S}) + H(Z_{\mathcal{V}_3} : \mathcal{V}_3 \in \mathcal{S}' \setminus \mathcal{S})$$
$$- H((Z_{\mathcal{V}_0} : \mathcal{V}_0 \in \mathcal{S} \cup \mathcal{S}')|X_k) \quad (82d)$$
$$= H(Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{S}) + H(Z_{\mathcal{V}_3} : \mathcal{V}_3 \in \mathcal{S}' \setminus \mathcal{S})$$
$$- H(Z_{\mathcal{V}_0} : \mathcal{V}_0 \in \mathcal{S} \cup \mathcal{S}') + I((Z_{\mathcal{V}_0} : \mathcal{V}_0 \in \mathcal{S} \cup \mathcal{S}'); X_k) \quad (82e)$$
$$= I((Z_{\mathcal{V}_0} : \mathcal{V}_0 \in \mathcal{S} \cup \mathcal{S}'); X_k) \quad (82f)$$
$$= H(X_k) - H(X_k|(Z_{\mathcal{V}_0} : \mathcal{V}_0 \in \mathcal{S} \cup \mathcal{S}')) \quad (82g)$$
$$\overset{(80)}{\leq} \mathsf{L}(1+\mathsf{a}) - \mathsf{L} = \mathsf{aL}. \quad (82h)$$

By taking (82h) into (81), we have

$$H(W_k|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{S})) + H(W_k|X_k, (Z_{\mathcal{V}_2} : \mathcal{V}_2 \in \mathcal{S}'))$$
$$\geq H(W_k|X_k, (Z_{\mathcal{V}_0} : \mathcal{V}_0 \in \mathcal{S} \cup \mathcal{S}'))$$
$$+ H(W_k|X_k, (Z_{\mathcal{V}_5} : \mathcal{V}_5 \in \mathcal{S} \cap \mathcal{S}')) - \mathsf{aL}. \quad (83)$$

Hence, by using (83) iteratively, we have

$$\sum_{j\in\left[\binom{\mathsf{K}-1}{\mathsf{S}-1}\right]} H(W_k|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{S}_k' \setminus \{\mathcal{S}_k'(j)\}))$$
$$\geq H(W_k|X_k) - \left(\binom{\mathsf{K}-1}{\mathsf{S}-1} - 1\right)\mathsf{aL} \quad (84a)$$
$$= \left(1 - \left(\binom{\mathsf{K}-1}{\mathsf{S}-1} - 1\right)\mathsf{a}\right)\mathsf{L}, \quad (84b)$$

where (84b) comes from the security constraint $I(W_k; X_k) = 0$ and $H(W_k) = \mathsf{L}$.[24]

For each set $\mathcal{V} \in \mathcal{V}_k'$, we have

$$H\Big(W_k\Big|X_k, (W_{k_1} : k_1 \in [\mathsf{K}] \setminus \{k\}),$$
$$\Big(Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \binom{[\mathsf{K}]}{\mathsf{S}}, \mathcal{V}_1 \neq \mathcal{V}\Big)\Big)$$
$$\geq I\Big(W_k; Z_{\mathcal{V}}\Big|X_k, (W_{k_1} : k_1 \in [\mathsf{K}] \setminus \{k\}),$$
$$\Big(Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \binom{[\mathsf{K}]}{\mathsf{S}}, \mathcal{V}_1 \neq \mathcal{V}\Big)\Big) \quad (85a)$$
$$= I(W_k; Z_{\mathcal{V}}|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{V}_k' \setminus \{\mathcal{V}\})) \quad (85b)$$
$$= H(W_k|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{V}_k' \setminus \{\mathcal{V}\}))$$
$$- H(W_k|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{V}_k')) \quad (85c)$$
$$= H(W_k|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{V}_k' \setminus \{\mathcal{V}\})), \quad (85d)$$

[24]To make the derivation of (84a) more clear, we first consider the first two terms on the LHS of (84a). We can see that $\big(\mathcal{V}_k' \setminus \{\mathcal{V}_k'(1)\}\big) \cup \big(\mathcal{V}_k' \setminus \{\mathcal{V}_k'(2)\}\big) = \mathcal{V}_k'$, and $\big(\mathcal{V}_k' \setminus \{\mathcal{V}_k'(1)\}\big) \cap \big(\mathcal{V}_k' \setminus \{\mathcal{V}_k'(2)\}\big) = \mathcal{V}_k' \setminus \{\mathcal{V}_k'(1), \mathcal{V}_k'(2)\}$. From (83), we have $\sum_{j\in[2]} H(W_k|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{V}_k' \setminus \{\mathcal{V}_k'(j)\})) \geq H(W_k|X_k, Z_k) + H(W_k|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{V}_k' \setminus \{\mathcal{V}_k'(1), \mathcal{V}_k'(2)\})) - \mathsf{aL}$, and we recall that $H(W_k|X_k, Z_k) = 0$. Next, from (83) again, we can lower bound the sum of $H(W_k|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{V}_k' \setminus \{\mathcal{V}_k'(1), \mathcal{V}_k'(2)\}))$ and $H(W_k|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{V}_k' \setminus \{\mathcal{V}_k'(3)\}))$, by $H(W_k|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{V}_k' \setminus \{\mathcal{V}_k'(1), \mathcal{V}_k'(2), \mathcal{V}_k'(3)\})) - \mathsf{aL}$. We repeat this iteratively. The last (i.e., $\left(\binom{\mathsf{K}-1}{\mathsf{S}-1} - 1\right)^{\text{th}}$) step is to lower bound the sum of $H(W_k|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{V}_k' \setminus \{\mathcal{V}_k'(1), \ldots, \mathcal{V}_k'(\binom{\mathsf{K}-1}{\mathsf{S}-1} - 1)\}))$ and $H(W_k|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{V}_k' \setminus \{\mathcal{V}_k'(\binom{\mathsf{K}-1}{\mathsf{S}-1})\}))$, by $H(W_k|X_k) - \mathsf{aL}$. In conclusion, we can obtain (84a).

where (85b) follows since $(W_{k_1} : k_1 \in [\mathsf{K}] \setminus \{k_1\})$ and $\left(Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \binom{[\mathsf{K}]\setminus\{k\}}{\mathsf{S}}\right)$ are independent of (X_k, Z_k, W_k), (85d) comes from (79b).

On the other hand, when $\mathcal{U}_1 = ([\mathsf{K}] \setminus \mathcal{V}) \cup \{k\}$ and $\mathcal{U}_2 = [\mathsf{K}] \setminus \mathcal{V}$,[25] we have

$$0 = H\left(\sum_{k_1\in\mathcal{U}_1} W_{k_1}\Big|X_k, (X_{k_2}, Y_{k_2}^{\mathcal{U}_1} : k_2 \in \mathcal{U}_2)\right) \tag{86a}$$

$$\geq H\left(\sum_{k_1\in\mathcal{U}_1} W_{k_1}\Big|X_k, (W_{k_2}, Z_{k_2} : k_2 \in \mathcal{U}_2)\right) \tag{86b}$$

$$= H(W_k|X_k, (W_{k_2}, Z_{k_2} : k_2 \in \mathcal{U}_2)) \tag{86c}$$

$$\geq H\Big(W_k\Big|X_k, (W_{k_1} : k_1 \in [\mathsf{K}] \setminus \{k\}), \Big(Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \binom{[\mathsf{K}]}{\mathsf{S}}, \mathcal{V}_1 \neq \mathcal{V}\Big)\Big), \tag{86d}$$

where (86b) follows since $(X_{k_2}, Y_{k_2}^{\mathcal{U}_1})$ is a function of (W_{k_2}, Z_{k_2}), and (86d) follows since $k \notin \mathcal{U}_2$ and $\mathcal{V} \cap \mathcal{U}_2 = \emptyset$.

From (85d) and (86d), we have

$$H(W_k|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{V}_k' \setminus \mathcal{V})) \leq 0. \tag{87}$$

By taking (87) into (84b), we have

$$1 - \left(\binom{\mathsf{K}-1}{\mathsf{S}-1} - 1\right)\mathsf{a} \leq 0, \tag{88a}$$

$$\iff \mathsf{a} \geq \frac{1}{\binom{\mathsf{K}-1}{\mathsf{S}-1} - 1}. \tag{88b}$$

Hence, Theorem 2 can be proved from $\mathsf{R}_1 = 1 + \mathsf{a}$ and (88b).

Appendix B
Proof of (81)

The proof of (81) follows the proof of [37, Proposition 3] (which shows a generalized version of the submodularity of entropy). More precisely, we have

$$\begin{aligned}
&H(W_k|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{S})) - H(W_k|X_k, \\
&(Z_{\mathcal{V}_0} : \mathcal{V}_0 \in \mathcal{S} \cup \mathcal{S}')) + H(W_k|X_k, (Z_{\mathcal{V}_2} : \mathcal{V}_2 \in \mathcal{S}')) \\
&= I(W_k; (Z_{\mathcal{V}_3} : \mathcal{V}_3 \in \mathcal{S}' \setminus \mathcal{S})|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{S})) \\
&+ H(W_k|X_k, (Z_{\mathcal{V}_2} : \mathcal{V}_2 \in \mathcal{S}')) \qquad (89a)\\
&= I(W_k; (Z_{\mathcal{V}_3} : \mathcal{V}_3 \in \mathcal{S}' \setminus \mathcal{S})|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{S})) \\
&+ H(W_k|X_k, (Z_{\mathcal{V}_0} : \mathcal{V}_0 \in \mathcal{S} \cup \mathcal{S}')) \\
&+ I(W_k; (Z_{\mathcal{V}_4} : \mathcal{V}_4 \in \mathcal{S} \setminus \mathcal{S}')|X_k, (Z_{\mathcal{V}_2} : \mathcal{V}_2 \in \mathcal{S}')). \qquad (89b)
\end{aligned}$$

In addition, we have (90) at the top of the next page. By taking (90d) into (89b), we have

$$\begin{aligned}
&H(W_k|X_k, (Z_{\mathcal{V}_1} : \mathcal{V}_1 \in \mathcal{S})) - H(W_k|X_k, (Z_{\mathcal{V}_0} : \mathcal{V}_0 \in \mathcal{S} \cup \mathcal{S}')) \\
&+ H(W_k|X_k, (Z_{\mathcal{V}_2} : \mathcal{V}_2 \in \mathcal{S}')) \\
&\geq H(W_k|X_k, (Z_{\mathcal{V}_5} : \mathcal{V}_5 \in \mathcal{S} \cap \mathcal{S}')) - I\big((Z_{\mathcal{V}_4} : \mathcal{V}_4 \in \mathcal{S} \setminus \mathcal{S}'); \\
&(Z_{\mathcal{V}_3} : \mathcal{V}_3 \in \mathcal{S}' \setminus \mathcal{S})|X_k, (Z_{\mathcal{V}_5} : \mathcal{V}_5 \in \mathcal{S} \cap \mathcal{S}')\big), \qquad (91)
\end{aligned}$$

which coincides with (81).

[25] This case is possible because, $|\mathcal{V}| = \mathsf{S} \leq \mathsf{K} - \mathsf{U}$, and thus $|[\mathsf{K}] \setminus \mathcal{V}| \geq \mathsf{U}$.

Appendix C
Proof of the Security Constraint in (5) for the Proposed Secure Aggregation Scheme

Assume that in the proposed secure aggregation scheme for Theorem 1, the U-dimensional vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ are determined, such that the constraints in (10), (16), and (18) are satisfied.

Let us then prove that the scheme is secure. By our construction, since the constraint in (10) is satisfied, we have

$$I(X_1, \ldots, X_{\mathsf{K}}; W_1, \ldots, W_{\mathsf{K}}) = \sum_{k\in[\mathsf{K}]} I(X_k; W_k) \tag{92a}$$

$$= \sum_{k\in[\mathsf{K}]} (H(X_k) - H(X_k|W_k)) \tag{92b}$$

$$= \sum_{k\in[\mathsf{K}]} (\mathsf{L} - H(X_k|W_k)) \tag{92c}$$

$$= \sum_{k\in[\mathsf{K}]} (\mathsf{L} - \mathsf{L}) = 0, \tag{92d}$$

where (92a) follows since $(X_1, W_1), \ldots, (X_{\mathsf{K}}, W_{\mathsf{K}})$ are mutually independent in our scheme (Recall (1) and that $X_1, \ldots, X_{\mathsf{K}}$ use different keys), (92c) follows since each W_k contains L uniform and i.i.d. symbols over $\mathbb{F}_{\mathsf{q}}$ and the keys are independent of W_k, and (92d) follows since (recall that each $Z_{\mathcal{V},k}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ and $k \in \mathcal{V}$ contains L/U uniform and i.i.d. symbols over $\mathbb{F}_{\mathsf{q}}$)

$$H(X_k|W_k) = H\left(\left(W_{k,j} + \sum_{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}:k\in\mathcal{V}} a_{\mathcal{V},j} Z_{\mathcal{V},k} : j \in [\mathsf{U}]\right)\Big|(W_{k,j} : j \in [\mathsf{U}])\right) \tag{93a}$$

$$\overset{(1)}{=} H\left(\sum_{\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}:k\in\mathcal{V}} a_{\mathcal{V},j} Z_{\mathcal{V},k} : j \in [\mathsf{U}]\right) \tag{93b}$$

$$\overset{(10)}{=} \mathsf{L}. \tag{93c}$$

By (92d), we can immediately obtain

$$0 = I(X_1, \ldots, X_{\mathsf{K}}; W_1, \ldots, W_{\mathsf{K}}) \tag{94a}$$

$$= I\left(X_1, \ldots, X_{\mathsf{K}}; W_1, \ldots, W_{\mathsf{K}}, \sum_{k\in\mathcal{U}_1} W_k\right) \tag{94b}$$

$$\implies I\left(X_1, \ldots, X_{\mathsf{K}}; W_1, \ldots, W_{\mathsf{K}}|\sum_{k\in\mathcal{U}_1} W_k\right) = 0, \tag{94c}$$

where (94b) follows since $\sum_{k\in\mathcal{U}_1} W_k$ is a function of $W_1, \ldots, W_{\mathsf{K}}$ and (94c) follows since the non-negativity of mutual information.

Hence, we have

$$I\left(W_1, \ldots, W_{\mathsf{K}}; X_1, \ldots, X_{\mathsf{K}}, (Y_k^{\mathcal{U}_1} : k \in \mathcal{U}_1)\Big|\sum_{k\in\mathcal{U}_1} W_k\right) = I\left(W_1, \ldots, W_{\mathsf{K}}; (Y_k^{\mathcal{U}_1} : k \in \mathcal{U}_1)\Big|\sum_{k\in\mathcal{U}_1} W_k, X_1, \ldots, X_{\mathsf{K}}\right) \tag{95a}$$

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.2024.3422087

$$
\begin{aligned}
&I(W_k;(Z_{\mathcal{V}_3}:\mathcal{V}_3\in\mathcal{S}'\setminus\mathcal{S})|X_k,(Z_{\mathcal{V}_1}:\mathcal{V}_1\in\mathcal{S}))+I(W_k;(Z_{\mathcal{V}_4}:\mathcal{V}_4\in\mathcal{S}\setminus\mathcal{S}')|X_k,(Z_{\mathcal{V}_2}:\mathcal{V}_2\in\mathcal{S}'))\\
&=I(W_k,(Z_{\mathcal{V}_4}:\mathcal{V}_4\in\mathcal{S}\setminus\mathcal{S}');(Z_{\mathcal{V}_3}:\mathcal{V}_3\in\mathcal{S}'\setminus\mathcal{S})|X_k,(Z_{\mathcal{V}_5}:\mathcal{V}_5\in\mathcal{S}\cap\mathcal{S}'))\\
&-I\left((Z_{\mathcal{V}_4}:\mathcal{V}_4\in\mathcal{S}\setminus\mathcal{S}');(Z_{\mathcal{V}_3}:\mathcal{V}_3\in\mathcal{S}'\setminus\mathcal{S})|X_k,(Z_{\mathcal{V}_5}:\mathcal{V}_5\in\mathcal{S}\cap\mathcal{S}')\right)\\
&+I(W_k;(Z_{\mathcal{V}_4}:\mathcal{V}_4\in\mathcal{S}\setminus\mathcal{S}')|X_k,(Z_{\mathcal{V}_2}:\mathcal{V}_2\in\mathcal{S}')) \qquad (90a)\\
&\geq H(W_k,(Z_{\mathcal{V}_4}:\mathcal{V}_4\in\mathcal{S}\setminus\mathcal{S}')|X_k,(Z_{\mathcal{V}_5}:\mathcal{V}_5\in\mathcal{S}\cap\mathcal{S}'))-H(W_k|X_k,(Z_{\mathcal{V}_2}:\mathcal{V}_2\in\mathcal{S}'))\\
&-I\left((Z_{\mathcal{V}_4}:\mathcal{V}_4\in\mathcal{S}\setminus\mathcal{S}');(Z_{\mathcal{V}_3}:\mathcal{V}_3\in\mathcal{S}'\setminus\mathcal{S})|X_k,(Z_{\mathcal{V}_5}:\mathcal{V}_5\in\mathcal{S}\cap\mathcal{S}')\right)\\
&+I(W_k;(Z_{\mathcal{V}_4}:\mathcal{V}_4\in\mathcal{S}\setminus\mathcal{S}')|X_k,(Z_{\mathcal{V}_2}:\mathcal{V}_2\in\mathcal{S}')) \qquad (90b)\\
&=H(W_k,(Z_{\mathcal{V}_4}:\mathcal{V}_4\in\mathcal{S}\setminus\mathcal{S}')|X_k,(Z_{\mathcal{V}_5}:\mathcal{V}_5\in\mathcal{S}\cap\mathcal{S}'))-H(W_k|X_k,(Z_{\mathcal{V}_0}:\mathcal{V}_0\in\mathcal{S}\cup\mathcal{S}'))\\
&-I\left((Z_{\mathcal{V}_4}:\mathcal{V}_4\in\mathcal{S}\setminus\mathcal{S}');(Z_{\mathcal{V}_3}:\mathcal{V}_3\in\mathcal{S}'\setminus\mathcal{S})|X_k,(Z_{\mathcal{V}_5}:\mathcal{V}_5\in\mathcal{S}\cap\mathcal{S}')\right) \qquad (90c)\\
&\geq H(W_k|X_k,(Z_{\mathcal{V}_5}:\mathcal{V}_5\in\mathcal{S}\cap\mathcal{S}'))-H(W_k|X_k,(Z_{\mathcal{V}_0}:\mathcal{V}_0\in\mathcal{S}\cup\mathcal{S}'))\\
&-I\left((Z_{\mathcal{V}_4}:\mathcal{V}_4\in\mathcal{S}\setminus\mathcal{S}');(Z_{\mathcal{V}_3}:\mathcal{V}_3\in\mathcal{S}'\setminus\mathcal{S})|X_k,(Z_{\mathcal{V}_5}:\mathcal{V}_5\in\mathcal{S}\cap\mathcal{S}')\right). \qquad (90d)
\end{aligned}
$$

$$
\leq I\left(W_1,\ldots,W_{\mathsf{K}};F_1,\ldots,F_{\mathsf{U}}\Big|\sum_{k\in\mathcal{U}_1}W_k,X_1,\ldots,X_{\mathsf{K}}\right) \qquad (95b)
$$

$$
=0, \qquad (95c)
$$

where (95a) comes from (94c), (95b) comes from $(Y_k^{\mathcal{U}_1}:k\in\mathcal{U}_1)$ are in the linear space spanned by $F_1,\ldots,F_{\mathsf{U}}$ and thus are determined by $F_1,\ldots,F_{\mathsf{U}}$, (95c) follows since $F_1,\ldots,F_{\mathsf{U}}$ can be recovered from $\sum_{k\in\mathcal{U}_1}W_k$ and $\sum_{k\in\mathcal{U}_1}X_k$. Hence, the security constraint in (5) is satisfied.

Appendix D
Proof of Lemma 3

Consider one set $\mathcal{A}\subseteq[\mathsf{K}]$ where $|\mathcal{A}|=\mathsf{U}$. Assume that $\mathcal{A}=\{\mathcal{A}(1),\ldots,\mathcal{A}(\mathsf{U})\}$ where $\mathcal{A}(1)<\cdots<\mathcal{A}(\mathsf{U})$. We also assume that the sets in $\mathcal{G}_2=\big\{[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\}:j\in([\mathsf{K}-\mathsf{U}]\cup[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}])\big\}$ are $\mathcal{G}_{2,1},\ldots,\mathcal{G}_{2,\mathsf{K}-\mathsf{U}},\mathcal{G}_{2,2\mathsf{K}-2\mathsf{U}+1},\ldots,\mathcal{G}_{2,\mathsf{K}}$, where $\mathcal{G}_{2,j}=[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]\cup\{j\}$ for each $j\in([\mathsf{K}-\mathsf{U}]\cup[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}])$.

Recall that by our construction, for each user $k\in[\mathsf{K}-\mathsf{U}]$, $\mathbf{s}_k$ is a left null vector of the matrix in (70). Note that each column of the matrix in (70) is $\mathbf{a}_{\{j\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]}$ where $j\in([\mathsf{K}-\mathsf{U}]\setminus\{k\})\cup[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}]$. In addition, it can be seen that $\{j\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]$ is in $\mathcal{G}_2$; thus each element of $\mathbf{b}_{\{j\}\cup[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]}$ is chosen uniformly and i.i.d. over $\mathbb{F}_{\mathsf{q}}$. For each user $k\in[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]$, from (72) we have that $\mathbf{s}_k=\mathbf{e}^{\mathrm{T}}_{\mathsf{U},k-\mathsf{K}+\mathsf{U}}$.

Hence, the determinant of the matrix

$$
\begin{bmatrix}\mathbf{s}_{\mathcal{A}(1)}\\ \cdots\\ \mathbf{s}_{\mathcal{A}(\mathsf{U})}\end{bmatrix} \qquad (96)
$$

could be seen as $D_{\mathcal{A}}=\frac{P_{\mathcal{A}}}{Q_{\mathcal{A}}}$, where $P_{\mathcal{A}}$ and $Q_{\mathcal{A}}$ are multivariate polynomials whose variables are the elements in $\mathbf{b}_{\mathcal{V}}$ where $\mathcal{V}\in\mathcal{G}_2$. Since each element in $\mathbf{b}_{\mathcal{V}}$ where $\mathcal{V}\in\mathcal{G}_2$ is uniformly and i.i.d. over $\mathbb{F}_{\mathsf{q}}$ where q is large enough, by the Schwartz-Zippel Lemma [34]–[36], if we can further show that the multivariate polynomial $P_{\mathcal{A}}$ is non-zero (i.e., a multivariate polynomial whose coefficients are not all 0), the probability that this multivariate polynomial is equal to 0 over all possible realization of the elements in $\mathbf{b}_{\mathcal{V}}$ where $\mathcal{V}\in\mathcal{G}_2$ goes to 0 when q goes to infinity, and thus the matrix in (96) is full rank with high probability. So in the following, we need to show that $P_{\mathcal{A}}$ is non-zero. For the matrix $\mathbf{G}$ in (97) whose dimension is $\mathsf{U}\times\mathsf{U}$, where $r_1,\ldots,r_{\mathsf{U}}$ denote the labels of rows, $c_1,\ldots,c_{\mathsf{U}}$ denote the labels of columns, and each '$*$' denotes a symbol uniformly and i.i.d. over $\mathbb{F}_{\mathsf{q}}$. With a slight abuse of notation, we define that $\mathbf{G}\setminus\mathbf{a}_{\mathcal{G}_{2,j}}$ where $j\in[\mathsf{K}-\mathsf{U}]\cup[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}]$ as the column-wise sub-matrix of $\mathbf{G}$ by removing the column $\mathbf{a}_{\mathcal{G}_{2,j}}$. For each $k\in(\mathcal{A}\cap[\mathsf{K}-\mathsf{U}])$, by our construction, $\mathbf{s}_k$ is a left null vector of $\mathbf{G}\setminus\mathbf{a}_{\mathcal{G}_{2,k}}$. Hence, to show that $P_{\mathcal{A}}$ is non-zero, we need to find one realization of the '$*$'s in $\mathbf{G}$ such that

1) $\mathbf{G}\setminus\mathbf{a}_{\mathcal{G}_{2,k}}$ has rank equal to $\mathsf{U}-1$ for each $k\in(\mathcal{A}\cap[\mathsf{K}-\mathsf{U}])$ (such that $\mathbf{s}_k$ exists by using the Cramer's rule and thus $Q_{\mathcal{A}}$ is not zero);
2) the U rows of the matrix in (96), including $\mathbf{s}_k$ where $k\in(\mathcal{A}\cap[\mathsf{K}-\mathsf{U}])$ and $\mathbf{e}^{\mathrm{T}}_{\mathsf{U},j-\mathsf{K}+\mathsf{U}}$ where $j\in(\mathcal{A}\cap[\mathsf{K}-\mathsf{U}+1:\mathsf{K}])$, are linearly independent (such that $D_{\mathcal{A}}$ is not zero).

We divide the set $\mathcal{A}\cap[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]$ into two subsets, $\mathcal{A}_1=\mathcal{A}\cap[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]$ where

$$
x=|\mathcal{A}_1|=|\mathcal{A}\cap[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]|\leq\mathsf{K}-\mathsf{U}, \qquad (98)
$$

and $\mathcal{A}_2=\mathcal{A}\cap[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}]$ where

$$
y=|\mathcal{A}_2|=|\mathcal{A}\cap[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}]|\leq 2\mathsf{U}-\mathsf{K}. \qquad (99)
$$

For each user $j_1\in\mathcal{A}_1$, we have $j_1-\mathsf{K}+\mathsf{U}\in[\mathsf{K}-\mathsf{U}]$; for each user $j_2\in\mathcal{A}_2$, we have $j_2-\mathsf{K}+\mathsf{U}\in[\mathsf{K}-\mathsf{U}+1:\mathsf{U}]$. Since $x+y=|\mathcal{A}\cap[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]|$ and $|\mathcal{A}|=\mathsf{U}$, we have

$$
\mathsf{U}-(\mathsf{K}-\mathsf{U})\leq x+y\leq\mathsf{U}. \qquad (100)
$$

If $x+y=\mathsf{U}$, we can see that the matrix in (96) is the identity matrix $\mathbf{I}_{\mathsf{U}}$ which is full rank. Hence, in the rest of the proof, we focus on the case where $2\mathsf{U}-\mathsf{K}\leq x+y<\mathsf{U}$.

By symmetry, we only need to consider the case where $\mathcal{A}\cap[\mathsf{K}-\mathsf{U}]=[\mathsf{U}-x-y]$, $\mathcal{A}_1=\mathcal{A}\cap[\mathsf{K}-\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}]=[\mathsf{K}-\mathsf{U}+1:\mathsf{K}-\mathsf{U}+x]$ and $\mathcal{A}_2=\mathcal{A}\cap[2\mathsf{K}-2\mathsf{U}+1:\mathsf{K}]=[2\mathsf{K}-2\mathsf{U}+1:2\mathsf{K}-2\mathsf{U}+y]$, and find one realization of the '$*$'s in $\mathbf{G}$ satisfying the constraints 1) and 2). Thus the last

$$\mathbf{G} = \left[\mathbf{a}_{\mathcal{G}_{2,1}}, \ldots, \mathbf{a}_{\mathcal{G}_{2,\mathsf{K}-\mathsf{U}}}, \mathbf{a}_{\mathcal{G}_{2,2\mathsf{K}-2\mathsf{U}+1}}, \ldots, \mathbf{a}_{\mathcal{G}_{2,\mathsf{K}}}\right] \tag{97a}$$

$$= \begin{array}{c} \\ r_1 \\ r_2 \\ \vdots \\ r_{\mathsf{K}-\mathsf{U}} \\ r_{\mathsf{K}-\mathsf{U}+1} \\ r_{\mathsf{K}-\mathsf{U}+2} \\ \vdots \\ r_{\mathsf{U}} \end{array} \begin{array}{c} \begin{array}{ccccccc} c_1 & c_2 & \cdots & c_{\mathsf{K}-\mathsf{U}} & c_{\mathsf{K}-\mathsf{U}+1} & c_{\mathsf{K}-\mathsf{U}+2} & \cdots & c_{\mathsf{U}} \end{array} \\ \begin{bmatrix} * & * & \cdots & * & * & * & \cdots & * \\ * & * & \cdots & * & * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * & * & * & \cdots & * \\ 0 & 0 & \cdots & 0 & * & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & * & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & * \end{bmatrix} \end{array} \tag{97b}$$

$|\mathcal{A} \setminus [\mathsf{K}-\mathsf{U}]| = x + y$ rows of the matrix in (96) includes $\mathbf{e}_{\mathsf{U},i}^{\mathrm{T}}$ where $i \in ([x] \cup [\mathsf{K}-\mathsf{U}+1 : \mathsf{K}-\mathsf{U}+y])$. To determine the first $\mathsf{U}-x-y$ rows of the matrix in (96), we select a realization of $\mathbf{G}$ in (101) at the top of the next page, where $0_{m,n}$ and $1_{m,n}$ represents all-zero matrix and all-one matrix of dimension $m \times n$, respectively. Note that $g_1 := \mathsf{K}-\mathsf{U}-x$, $g_2 := x+y-2\mathsf{U}+\mathsf{K}$, $r_{[i:j]}$ represents $r_i, r_{i+1}, \ldots, r_j$, and $c_{[i:j]}$ represents $c_i, c_{i+1}, \ldots, c_j$. Let us then derive $\mathbf{s}_k$ for each user $k \in (\mathcal{A} \cap [\mathsf{K}-\mathsf{U}]) = [\mathsf{U}-x-y]$.

For each user $k \in [g_1]$, the matrix $\mathbf{G} \setminus \mathbf{a}_{\mathcal{G}_{2,k}}$ has rank equal to $\mathsf{U}-1$, since one can easily check that the columns in $\mathbf{G}$ are linearly independent. Thus $\mathbf{G} \setminus \mathbf{a}_{\mathcal{G}_{2,k}}$ contains exactly one linearly independent left null vector. We can check that this vector could be (recall that 1_n and 0_n represent the vertical n-dimensional vector whose elements are all 1 and all 0, respectively)

$$\mathbf{s}_k = [1_{2\mathsf{U}-\mathsf{K}-y}^{\mathrm{T}},\ 1_{g_2}^{\mathrm{T}},\ \mathbf{e}_{g_1,k}^{\mathrm{T}},\ -1_y^{\mathrm{T}},\ 0_{2\mathsf{U}-\mathsf{K}-y}^{\mathrm{T}}], \tag{102}$$

for each $k \in [g_1]$.

For each user $k \in [g_1+1 : \mathsf{U}-x-y]$, since the columns in $\mathbf{G}$ are linearly independent, the matrix $\mathbf{G} \setminus \mathbf{a}_{\mathcal{G}_{2,k}}$ has rank equal to $\mathsf{U}-1$. Thus $\mathbf{G} \setminus \mathbf{a}_{\mathcal{G}_{2,k}}$ contains exactly one linearly independent left null vector. We can check that this vector could be

$$\mathbf{s}_k = [\mathbf{e}_{2\mathsf{U}-\mathsf{K}-y,k-g_1}^{\mathrm{T}},\ 0_{g_2}^{\mathrm{T}},\ 0_{g_1}^{\mathrm{T}},\ 0_y^{\mathrm{T}},\ \mathbf{e}_{2\mathsf{U}-\mathsf{K}-y,k-g_1}^{\mathrm{T}}], \tag{103}$$

for each $k \in [g_1+1 : \mathsf{U}-x-y]$.

Recall that the last $x+y$ rows of the matrix in (96) include $\mathbf{e}_{\mathsf{U},i}^{\mathrm{T}}$ where $i \in ([x] \cup [\mathsf{K}-\mathsf{U}+1 : \mathsf{K}-\mathsf{U}+y])$. Hence, together with the first $\mathsf{U}-x-y$ rows as shown in (102) and (103), we can see that the matrix in (96) is (104) at the top of the next page, which is full rank. Thus we proved that with the choice of $\mathbf{G}$ in (101), the constraints 1) and 2) are satisfied; thus $P_{\mathcal{A}}$ is a non-zero polynomial. This completes the proof of Lemma 3.

APPENDIX E
DATA TABLES OF THE EXPERIMENTAL RESULTS IN SECTION V

In the following, we consider the cases where $\mathsf{U} = (\mathsf{K}+1)/2$ and $\mathsf{U} = \mathsf{K}-1$, and list the running times of each procedure in our experiments. In the tables provided in this Section, we use "IPS" to represent the size of each input vector; use "KST" to represent key sharing time; use "R1AT" and "R2AT" to represent the running times in the first and second rounds of model aggregation, respectively; use 'R3AT" and "R4AT" to represent the running times in the third and fourth rounds of model aggregation (only needed by `Sec`), respectively; use "TMA" to represent the total model aggregation time.

1) Case $\mathsf{U} = (\mathsf{K}+1)/2$: `Group` vs. `Light` vs. `Sec`:

Running Times (ms): $\mathsf{K}=5, \mathsf{U}=3$					
Scheme	IPS	KST	R1AT	R2AT	TMA
`Group`	10^5	622.70	19.42	4.45	23.88
`Light`	10^5	707.12	19.26	4.16	23.42
`Group`	2×10^5	1232.11	31.66	9.90	41.56
`Light`	2×10^5	1313.31	32.79	9.71	42.50
`Group`	3×10^5	1854.66	42.62	19.11	61.73
`Light`	3×10^5	2024.43	41.30	23.46	64.76

Running Times (ms): $\mathsf{K}=5, \mathsf{U}=3$						
Scheme	IPS	R1AT	R2AT	R3AT	R4AT	TMA
`Sec`	10^5	7.41	3.53	38.51	0.94	47.75
`Sec`	2×10^5	13.74	3.15	77.50	0.87	84.84
`Sec`	3×10^5	27.02	3.16	116.57	0.82	124.07

Running Times (ms): $\mathsf{K}=10, \mathsf{U}=5$					
Scheme	IPS	KST	R1AT	R2AT	TMA
`Group`	10^5	1268.69	27.843	7.26	35.10
`Light`	10^5	1422.05	29.9577	7.31	37.27
`Group`	2×10^5	2536.10	49.15	12.40	61.55
`Light`	2×10^5	2911.85	54.28	11.75	66.03
`Group`	3×10^5	3810.15	74.56	18.79	93.34
`Light`	3×10^5	4729.24	73.53	18.63	92.17

Running Times (ms): $\mathsf{K}=10, \mathsf{U}=5$						
Scheme	IPS	R1AT	R2AT	R3AT	R4AT	TMA
`Sec`	10^5	10.65	4.13	59.22	0.88	71.91
`Sec`	2×10^5	12.15	4.52	118.30	1.23	133.91
`Sec`	3×10^5	9.47	4.10	179.67	1.10	191.94

$$\mathbf{G} = \left[\mathbf{a}_{\mathcal{G}_{2,1}}, \ldots, \mathbf{a}_{\mathcal{G}_{2,\mathsf{K}-\mathsf{U}}}, \mathbf{a}_{\mathcal{G}_{2,2\mathsf{K}-2\mathsf{U}+1}}, \ldots, \mathbf{a}_{\mathcal{G}_{2,\mathsf{K}}}\right] \tag{101a}$$

$$= \begin{array}{c} \\ r_{[2\mathsf{U}-\mathsf{K}-y]} \\ r_{[2\mathsf{U}-\mathsf{K}-y+1:x]} \\ r_{[x+1:\mathsf{K}-\mathsf{U}]} \\ r_{[\mathsf{K}-\mathsf{U}+1:\mathsf{K}-\mathsf{U}+y]} \\ r_{[\mathsf{K}-\mathsf{U}+y+1:\mathsf{U}]} \end{array} \begin{array}{c} \begin{array}{cccccc} c_{[g_1]} & & c_{[g_1+1:\mathsf{U}-x-y]} & & c_{[\mathsf{U}-x-y+1:\mathsf{K}-\mathsf{U}]} & c_{[\mathsf{K}-\mathsf{U}+1:\mathsf{K}-\mathsf{U}+y]} & c_{[\mathsf{K}-\mathsf{U}+y+1:\mathsf{U}]} \end{array} \\ \begin{bmatrix} 0_{2\mathsf{U}-\mathsf{K}-y,g_1} & & \mathbf{I}_{2\mathsf{U}-\mathsf{K}-y} & & 0_{2\mathsf{U}-\mathsf{K}-y,g_2} & 0_{2\mathsf{U}-\mathsf{K}-y,y} & -\mathbf{I}_{2\mathsf{U}-\mathsf{K}-y} \\ 0_{g_2,g_1} & & 0_{g_2,2\mathsf{U}-\mathsf{K}-y} & & \mathbf{I}_{g_2} & 0_{g_2,y} & 0_{g_2,2\mathsf{U}-\mathsf{K}-y} \\ \mathbf{I}_{g_1} & & -1_{g_1,2\mathsf{U}-\mathsf{K}-y} & & -1_{g_1,g_2} & 1_{g_1,y} & 1_{g_1,2\mathsf{U}-\mathsf{K}-y} \\ 0_{y,g_1} & & 0_{y,2\mathsf{U}-\mathsf{K}-y} & & 0_{y,g_2} & \mathbf{I}_y & 0_{y,2\mathsf{U}-\mathsf{K}-y} \\ 0_{2\mathsf{U}-\mathsf{K}-y,g_1} & & 0_{2\mathsf{U}-\mathsf{K}-y,2\mathsf{U}-\mathsf{K}-y} & & 0_{2\mathsf{U}-\mathsf{K}-y,g_2} & 0_{2\mathsf{U}-\mathsf{K}-y,y} & \mathbf{I}_{2\mathsf{U}-\mathsf{K}-y} \end{bmatrix} \end{array} \tag{101b}$$

$$\begin{array}{c} \\ r_{[g_1]} \\ r_{[g_1+1:\mathsf{U}-x-y]} \\ r_{[\mathsf{U}-x-y+1:\mathsf{U}-y]} \\ r_{[\mathsf{U}-y+1:\mathsf{U}]} \end{array} \begin{array}{c} \begin{array}{cccc} c_{[x]} & c_{[x+1:\mathsf{K}-\mathsf{U}]} & c_{[\mathsf{K}-\mathsf{U}+1:\mathsf{K}-\mathsf{U}+y]} & c_{[\mathsf{K}-\mathsf{U}+y+1:\mathsf{U}]} \end{array} \\ \begin{bmatrix} 1_{g_1,x} & \mathbf{I}_{g_1} & -1_{g_1,y} & 0_{g_1,2\mathsf{U}-\mathsf{K}-y} \\ (\mathbf{I}_{2\mathsf{U}-\mathsf{K}-y},\ 0_{2\mathsf{U}-\mathsf{K}-y,g_2}) & 0_{2\mathsf{U}-\mathsf{K}-y,g_1} & 0_{2\mathsf{U}-\mathsf{K}-y,y} & \mathbf{I}_{2\mathsf{U}-\mathsf{K}-y} \\ \mathbf{I}_x & 0_{x,\mathsf{K}-\mathsf{U}-x} & 0_{x,y} & 0_{x,2\mathsf{U}-\mathsf{K}-y} \\ 0_{y,x} & 0_{y,\mathsf{K}-\mathsf{U}-x} & \mathbf{I}_y & 0_{y,2\mathsf{U}-\mathsf{K}-y} \end{bmatrix} \end{array}, \tag{104}$$

Running Times (ms): $\mathsf{K}=15, \mathsf{U}=8$					
Scheme	IPS	KST	R1AT	R2AT	TMA
`Group`	10^5	1853.25	45.97	10.52	56.49
`Light`	10^5	2061.42	40.46	10.44	50.90
`Group`	2×10^5	3704.39	90.76	18.58	109.34
`Light`	2×10^5	4650.02	92.16	16.35	108.51
`Group`	3×10^5	5556.72	140.93	22.20	163.13
`Light`	3×10^5	7346.74	130.83	22.80	153.63

Running Times (ms): $\mathsf{K}=15, \mathsf{U}=8$						
Scheme	IPS	R1AT	R2AT	R3AT	R4AT	TMA
`Sec`	10^5	12.78	6.64	90.32	1.41	107.59
`Sec`	2×10^5	12.02	7.27	182.66	1.40	199.31
`Sec`	3×10^5	13.62	6.59	279.89	1.32	298.55

Running Times (ms): $\mathsf{K}=20, \mathsf{U}=10$					
Scheme	IPS	KST	R1AT	R2AT	TMA
`Group`	10^5	2510.21	51.54	14.43	65.97
`Light`	10^5	2925.39	53.71	13.91	67.62
`Group`	2×10^5	5038.56	110.70	20.68	131.37
`Light`	2×10^5	6314.36	111.00	20.78	131.78
`Group`	3×10^5	7501.90	165.40	29.39	194.79
`Light`	3×10^5	9878.07	158.98	28.13	187.10

Running Times (ms): $\mathsf{K}=20, \mathsf{U}=10$						
Scheme	IPS	R1AT	R2AT	R3AT	R4AT	TMA
`Sec`	10^5	18.06	8.77	112.25	1.53	133.58
`Sec`	2×10^5	20.30	8.65	236.04	1.61	260.71
`Sec`	3×10^5	34.58	8.10	330.95	1.89	359.95

2) Case $\mathsf{U}=\mathsf{K}-1$*:* `Group (Group_1)` *vs.* `Light` *vs.* `Sec`*:*

Running Times (ms): $\mathsf{K}=5, \mathsf{U}=4$					
Scheme	IPS	KST	R1AT	R2AT	TMA
`Group`	10^5	573.52	32.09	4.55	36.64
`Group1`	10^5	565.96	32.09	4.55	36.64
`Light`	10^5	571.29	31.42	4.51	35.93
`Group`	2×10^5	1212.92	61.32	9.82	71.14
`Group1`	2×10^5	1180.77	61.32	9.82	71.14
`Light`	2×10^5	1215.37	61.66	9.89	71.55
`Group`	3×10^5	1808.52	92.88	14.32	107.20
`Group1`	3×10^5	1674.90	92.88	14.32	107.20
`Light`	3×10^5	1714.31	90.65	15.02	105.68

Running Times (ms): $\mathsf{K}=5, \mathsf{U}=4$						
Scheme	IPS	R1AT	R2AT	R3AT	R4AT	TMA
`Sec`	10^5	8.04	2.39	52.24	0.85	63.53
`Sec`	2×10^5	6.03	4.52	99.12	0.96	110.62
`Sec`	3×10^5	13.33	2.48	148.46	0.85	165.12

Running Times (ms): $\mathsf{K}=10, \mathsf{U}=9$					
Scheme	IPS	KST	R1AT	R2AT	TMA
`Group`	10^5	1290.11	60.14	6.58	66.71
`Group1`	10^5	1090.28	60.14	6.58	66.71
`Light`	10^5	1165.68	61.82	6.13	67.95
`Group`	2×10^5	2590.86	119.60	13.55	133.15
`Group1`	2×10^5	2231.25	119.60	13.55	133.15
`Light`	2×10^5	2372.63	122.31	12.76	135.07
`Group`	3×10^5	4000.38	189.28	16.93	206.21
`Group1`	3×10^5	3122.44	189.28	16.93	206.21
`Light`	3×10^5	3159.10	192.45	17.07	209.52

Running Times (ms): $\mathsf{K}=10, \mathsf{U}=9$						
Scheme	IPS	R1AT	R2AT	R3AT	R4AT	TMA
`Sec`	10^5	6.50	5.39	101.61	1.28	114.78
`Sec`	2×10^5	6.14	5.70	202.90	1.34	216.08
`Sec`	3×10^5	5.50	5.00	303.92	1.19	315.62

Running Times (ms): $\mathsf{K}=15, \mathsf{U}=14$					
Scheme	IPS	KST	R1AT	R2AT	TMA
Group	10^5	2003.57	99.94	2.68	102.62
Group1	10^5	1699.15	99.94	2.68	102.62
Light	10^5	1748.13	98.91	2.89	101.80
Group	2×10^5	4017.40	201.35	13.69	215.05
Group1	2×10^5	3293.68	201.35	13.69	215.05
Light	2×10^5	3514.38	196.78	14.78	211.57
Group	3×10^5	6020.53	285.31	21.70	307.01
Group	3×10^5	4605.54	285.31	21.70	307.01
Light	3×10^5	4657.34	299.46	19.53	318.99

Running Times (ms): $\mathsf{K}=15, \mathsf{U}=14$						
Scheme	IPS	R1AT	R2AT	R3AT	R4AT	TMA
Sec	10^5	17.82	8.34	153.16	1.58	180.90
Sec	2×10^5	10.62	7.61	303.97	1.68	323.87
Sec	3×10^5	9.14	8.31	459.96	1.78	479.20

Running Times (ms): $\mathsf{K}=20, \mathsf{U}=19$					
Scheme	IPS	KST	R1AT	R2AT	TMA
Group	10^5	2724.81	132.58	4.03	136.61
Group1	10^5	2387.80	132.58	4.03	136.61
Light	10^5	2419.75	128.80	3.71	132.51
Group	2×10^5	5460.64	263.68	16.17	279.86
Group1	2×10^5	4466.25	263.68	16.17	279.86
Light	2×10^5	4680.18	260.38	14.64	275.02
Group	3×10^5	8230.29	404.78	24.86	429.64
Group1	3×10^5	6114.46	404.78	24.86	429.64
Light	3×10^5	6277.13	400.43	25.45	425.88

Running Times (ms): $\mathsf{K}=20, \mathsf{U}=19$						
Scheme	IPS	R1AT	R2AT	R3AT	R4AT	TMA
Sec	10^5	10.17	11.63	204.31	2.04	228.15
Sec	2×10^5	11.14	11.81	406.37	2.51	431.83
Sec	3×10^5	10.24	12.28	611.32	2.10	635.94

REFERENCES

[1] K. Wan, Y. Yao, H. Sun, M. Ji, and G. Caire, "Groupsecagg: Information theoretic secure aggregation with uncoded groupwise keys," *in IEEE Intern. Conf. Commun. (ICC)*, pp. 3890–3895, May 2023.

[2] 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.

[3] 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.

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

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

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

[8] B. Choi, J.-y. Sohn, D.-J. Han, and J. Moon, "Communication-computation efficient secure aggregation for federated learning," *arXiv:2012.05433*, Dec. 2020.

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

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

[11] 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.

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

[13] 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.

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

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

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

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

[22] W.-N. Chen, A. Ozgur, G. Cormode, and A. Bharadwaj, "The communication cost of security and privacy in federated frequency estimation," in *International Conference on Artificial Intelligence and Statistics*. PMLR, 2023, pp. 4247–4274.

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

[24] 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.

[25] 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.

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

[27] 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.

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

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

[30] ——, "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.

[31] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the k-user interference channel," *IEEE Trans. Infor. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.

[32] K. Wan, H. Sun, M. Ji, and G. Caire, "On secure distributed linearly separable computation," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 3, pp. 912–926, Mar. 2022.

[33] ——, "Distributed linearly separable computation," *IEEE Trans. Inf. Theory*, vol. 68, no. 2, pp. 1259–1278, Feb. 2022.

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

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

[36] 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.

[37] K. Wan, D. Tuninetti, M. Ji, and P. Piantanida, "Combination networks with end-user-caches: Novel achievable and converse bounds under uncoded cache placement," *IEEE Trans. Inf. Theory*, vol. 68, no. 2, pp. 806–827, Feb. 2022.

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.

Xin Yao received the B.E. degree in Electrical and Computer Engineering from Tianjin University of Science and Technology, Tianjin, China, in 2019, the M.Sc. degree in Wireless Communications from George Washington University, District of Columbia, US, in 2021. He is currently a PhD student at University of Utah, Salt Lake City, US. His research focus on Wireless Communication and the Privacy in Federated Learning.

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.

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.