Appendix of "On the Optimality of Secure Aggregation with Uncoded Groupwise Keys Against User Dropouts and User Collusion"

Appendix A
Proof of Lemma 1

A. Lower bound of the rank.

From the Constraint 3, the matrix $\left[\mathbf{a}_{\mathcal{S}^k_{\overline{\mathcal{T}},1}}([\mathsf{U}-|\mathcal{T}|]),\ldots,\mathbf{a}_{\mathcal{S}^k_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|-1}{\mathsf{S}-1}}}([\mathsf{U}-|\mathcal{T}|])\right]$ in (12) has rank equal to $\mathsf{U}-|\mathcal{T}|$ and is a sub-matrix of the matrix $\left[\mathbf{a}_{\mathcal{S}_{\overline{\mathcal{T}},1}},\ldots,\mathbf{a}_{\mathcal{S}_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|}{\mathsf{S}}}}\right]$ in (13), so the rank of the matrix in (13) has a lower bound of $\mathsf{U}-|\mathcal{T}|$.

B. Upper bound of the rank.

We denote all sets $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$ and $\mathcal{V}\cap\mathcal{T}\neq\emptyset$ by $\mathcal{S}_{\mathcal{T},1},\ldots,\mathcal{S}_{\mathcal{T},\binom{\mathsf{K}}{\mathsf{S}}-\binom{\mathsf{K}-|\mathcal{T}|}{\mathsf{S}}}$.

Recall $Y_k^{\mathcal{U}_1}$ in (11), we define

$$\mathbf{y}_k=\mathbf{s}_k\left[\mathbf{a}_{\mathcal{S}_1},\ldots,\mathbf{a}_{\mathcal{S}_{\binom{\mathsf{K}}{\mathsf{S}}}}\right]=\left[y^k_1\quad\cdots\quad y^k_{\binom{\mathsf{K}}{\mathsf{S}}}\right],\tag{16}$$

where each of them corresponds in turn to the coefficient of the key in the linear combination of $Y_k^{\mathcal{U}_1}$. We can re-write (16) as

$$\mathbf{y}'_k=\left[y^k_{\mathcal{T},1}\quad\cdots\quad y^k_{\mathcal{T},\binom{\mathsf{K}}{\mathsf{S}}-\binom{\mathsf{K}-|\mathcal{T}|}{\mathsf{S}}}\quad y^k_{\overline{\mathcal{T}},1}\quad\cdots\quad y^k_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|}{\mathsf{S}}}\right],\tag{17}$$

where $y^k_{\mathcal{T},i}$ is the coefficient of the key whose set is $\mathcal{S}_{\mathcal{T},i}$, $y^k_{\overline{\mathcal{T}},i}$ is the coefficient of the key whose set is $\mathcal{S}_{\overline{\mathcal{T}},i}$.

From any U users in $\mathcal{U}_2$, the server can recover $F_1,\ldots,F_{\mathsf{U}}$ represented in (10), also assuming $\{k_1,\ldots,k_{\mathsf{U}}\}\in\mathcal{U}_2$, where the first $\mathsf{U}-|\mathcal{T}|$ users are non-colluding and the remaining $|\mathcal{T}|$ are colluding users. We have

$$\begin{bmatrix} y^{k_1}_{\mathcal{T},1} & y^{k_1}_{\overline{\mathcal{T}},1} & \cdots & y^{k}_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|}{\mathsf{S}}}\\ \vdots & \vdots & \ddots & \vdots\\ y^{k_{\mathsf{U}-|\mathcal{T}|}}_{\mathcal{T},1} & y^{k_{\mathsf{U}-|\mathcal{T}|}}_{\overline{\mathcal{T}},1} & \cdots & y^{k_{\mathsf{U}-|\mathcal{T}|}}_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|}{\mathsf{S}}}\\ y^{k_{\mathsf{U}-|\mathcal{T}|+1}}_{\mathcal{T},1} & y^{k_{\mathsf{U}-|\mathcal{T}|+1}}_{\overline{\mathcal{T}},1} & \cdots & y^{k_{\mathsf{U}-|\mathcal{T}|+1}}_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|}{\mathsf{S}}}\\ \vdots & \vdots & \ddots & \vdots\\ y^{k_{\mathsf{U}}}_{\mathcal{T},1} & y^{k_{\mathsf{U}}}_{\overline{\mathcal{T}},1} & \cdots & y^{k_{\mathsf{U}}}_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|}{\mathsf{S}}} \end{bmatrix}\begin{matrix}\\ \\ \mathbf{Y}'_1\\ \\ \mathbf{Y}'_2\\ \\ \end{matrix}\tag{18}$$

$\mathbf{Y}'_1$ is the sub-matrix whose elements correspond to the keys that are not available to the server in the second round of user transmission messages, colluding users cannot send this part of the key information, so all the elements in $\mathbf{Y}'_2$ are 0. The dimension of the matrix $\mathbf{Y}'_1$ is $(\mathsf{U}-|\mathcal{T}|)\times\binom{\mathsf{K}-|\mathcal{T}|}{\mathsf{S}}$ which has rank less than or equal to $\mathsf{U}-|\mathcal{T}|$.

Based on Constraints 1 and 2, from the messages where the coefficients of the keys are present in (18), the server can recover $F_1,\ldots,F_{\mathsf{U}}$, i.e. the matrix $\left[\mathbf{a}_{\mathcal{S}_{\overline{\mathcal{T}},1}},\ldots,\mathbf{a}_{\mathcal{S}_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|}{\mathsf{S}}}}\right]$ is in the linear space spanned by $\mathbf{Y}'_1$. So the rank of the matrix $\left[\mathbf{a}_{\mathcal{S}_{\overline{\mathcal{T}},1}},\ldots,\mathbf{a}_{\mathcal{S}_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|}{\mathsf{S}}}}\right]$ has an upper bound of $\mathsf{U}-|\mathcal{T}|$.

Appendix B
Realizations of Coefficient vectors in Example 1

The details realizations of coefficient vectors $\mathbf{a}_{\mathcal{V}}$ for Example 1 could be found Table I at the top of the next page.

Appendix C
General Selection on the Coefficient Vectors for the Proposed Scheme In Section IV

In the following, we describe the selection on the coefficient vectors $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$, satisfying Constraints 1-3.

In the coefficient design process, we first allocate the base vectors, and then proceed with the coefficient design. We can summarize the key points as follows:

- *First step.* We generate an $\mathsf{U}\times\mathsf{U}$ matrix $\mathbf{M}=[\mathbf{m}_1,\mathbf{m}_2,\ldots,\mathbf{m}_{\mathsf{U}}]$, whose elements are uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}$.
  For all the sets $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$, we define
  $$\mathcal{M}_{\mathcal{V}}=\{\mathcal{M}_{\mathcal{V}}(1),\ldots,\mathcal{M}_{\mathcal{V}}(|\mathcal{M}_{\mathcal{V}}|)\}:=\mathcal{V}\cap[\mathsf{K}-\mathsf{U}+1:\mathsf{K}],$$
  and $\mathbf{a}_{\mathcal{V}}$ is in the linear space spanned by $\{\mathbf{m}_{\mathcal{M}_{\mathcal{V}}(i)-\mathsf{K}+\mathsf{U}}: i\in|\mathcal{M}_{\mathcal{V}}|\}$, we can have
  $$\begin{aligned}\mathbf{a}_{\mathcal{V}}=&b_{\mathcal{V},1}\ \mathbf{m}_{\mathcal{M}_{\mathcal{V}}(1)-\mathsf{K}+\mathsf{U}}+b_{\mathcal{V},2}\ \mathbf{m}_{\mathcal{M}_{\mathcal{V}}(2)-\mathsf{K}+\mathsf{U}}\\&+\cdots+b_{\mathcal{V},|\mathcal{M}_{\mathcal{V}}|}\ \mathbf{m}_{\mathcal{M}_{\mathcal{V}}(|\mathcal{M}_{\mathcal{V}}|)-\mathsf{K}+\mathsf{U}}.\end{aligned}\tag{19}$$
  where the coefficient vector $\mathbf{b}_{\mathcal{V}}:=(b_{\mathcal{V},1},\ldots,b_{\mathcal{V},|\mathcal{M}_{\mathcal{V}}|})$.
- *Second step.* To ensure the existence of $\mathbf{s}_k$, each coded key $Z^{\mathcal{U}_1}_{\mathcal{V}}$ where $k\notin\mathcal{V}$ can be considered as interference to user k. The coefficients of $Z^{\mathcal{U}_1}_{\mathcal{V}}$ where $k\notin\mathcal{V}$ should be set to 0 in $Y^{\mathcal{U}_1}_k$. We generate a $(\mathsf{K}-\mathsf{U})\times\mathsf{U}$ matrix as $[\mathbf{s}_1;\ldots;\mathbf{s}_{\mathsf{K}-\mathsf{U}}]$ uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}$. For each $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$, we define
  $$\mathcal{B}_{\mathcal{V}}=\{\mathcal{B}_{\mathcal{V}}(1),\ldots,\mathcal{B}_{\mathcal{V}}(|\mathcal{B}_{\mathcal{V}}|)\}:=[\mathsf{K}-\mathsf{U}]\setminus\mathcal{V}.$$
  By define the matrix $\mathbf{A}$ with dimension of $|\mathcal{B}_{\mathcal{V}}|\times|\mathcal{M}_{\mathcal{V}}|$,
  $$\mathbf{A}=\begin{bmatrix}\mathbf{s}_{\mathcal{B}_{\mathcal{V}}(1)}\\ \vdots\\ \mathbf{s}_{\mathcal{B}_{\mathcal{V}}(|\mathcal{B}_{\mathcal{V}}|)}\end{bmatrix}\left[\mathbf{m}_{\mathcal{M}_{\mathcal{V}}(1)-\mathsf{K}+\mathsf{U}},\ldots,\mathbf{m}_{\mathcal{M}_{\mathcal{V}}(|\mathcal{M}_{\mathcal{V}}|)-\mathsf{K}+\mathsf{U}}\right],\tag{20}$$

TABLE I: Coefficient vectors $\mathbf{a}_{\mathcal{V}}$ in the $(\mathsf{K},\mathsf{U},\mathsf{S},\mathsf{T})=(6,4,4,1)$ information theoretic secure aggregation problem.

$\mathbf{a}_{\mathcal{V}}$	Composition	Constraint	$\mathbf{b}_{\mathcal{V}}$	Value
$\mathbf{a}_{\{1,2,3,4\}}$	$\mathbf{m}_1,\mathbf{m}_2$	None	$[4,1]^\mathsf{T}$	$[6,14,8,8]^\mathsf{T}$
$\mathbf{a}_{\{1,2,3,5\}}$	$\mathbf{m}_1,\mathbf{m}_3$	None	$[4,3]^\mathsf{T}$	$[13,21,7,7]^\mathsf{T}$
$\mathbf{a}_{\{1,2,3,6\}}$	$\mathbf{m}_1,\mathbf{m}_4$	None	$[2,4]^\mathsf{T}$	$[10,18,14,18]^\mathsf{T}$
$\mathbf{a}_{\{1,2,4,5\}}$	$\mathbf{m}_2,\mathbf{m}_3$	None	$[4,3]^\mathsf{T}$	$[17,17,19,19]^\mathsf{T}$
$\mathbf{a}_{\{1,2,4,6\}}$	$\mathbf{m}_2,\mathbf{m}_4$	None	$[1,3]^\mathsf{T}$	$[8,11,13,16]^\mathsf{T}$
$\mathbf{a}_{\{1,2,5,6\}}$	$\mathbf{m}_3,\mathbf{m}_4$	None	$[1,2]^\mathsf{T}$	$[7,9,7,9]^\mathsf{T}$
$\mathbf{a}_{\{1,3,4,5\}}$	$\mathbf{m}_1,\mathbf{m}_2,\mathbf{m}_3$	$\mathbf{s}_2\mathbf{a}_{\{1,3,4,5\}}=0$	$[4,3,-\frac{112}{15}]^\mathsf{T}$	$[-\frac{62}{5},-\frac{22}{5},\frac{128}{15},\frac{128}{15}]^\mathsf{T}$
$\mathbf{a}_{\{1,3,4,6\}}$	$\mathbf{m}_1,\mathbf{m}_2,\mathbf{m}_4$	$\mathbf{s}_2\mathbf{a}_{\{1,3,4,6\}}=0$	$[-\frac{82}{13},2,2]^\mathsf{T}$	$[\frac{22}{13},-\frac{116}{13},\frac{100}{13},\frac{126}{13}]^\mathsf{T}$
$\mathbf{a}_{\{1,3,5,6\}}$	$\mathbf{m}_1,\mathbf{m}_3,\mathbf{m}_4$	$\mathbf{s}_2\mathbf{a}_{\{1,3,5,6\}}=0$	$[3,2,-\frac{23}{7}]^\mathsf{T}$	$[\frac{17}{7},\frac{36}{7},-\frac{34}{7},-\frac{57}{7}]^\mathsf{T}$
$\mathbf{a}_{\{1,4,5,6\}}$	$\mathbf{m}_2,\mathbf{m}_3,\mathbf{m}_4$	$\mathbf{s}_2\mathbf{a}_{\{1,4,5,6\}}=0$	$[4,-\frac{101}{15},1]^\mathsf{T}$	$[-\frac{51}{5},-\frac{46}{5},\frac{184}{15},\frac{199}{15}]^\mathsf{T}$
$\mathbf{a}_{\{2,3,4,5\}}$	$\mathbf{m}_1,\mathbf{m}_2,\mathbf{m}_3$	$\mathbf{s}_1\mathbf{a}_{\{2,3,4,5\}}=0$	$[4,-\frac{10}{3},2]^\mathsf{T}$	$[\frac{10}{3},\frac{34}{3},-\frac{22}{3},-\frac{22}{3}]^\mathsf{T}$
$\mathbf{a}_{\{2,3,4,6\}}$	$\mathbf{m}_1,\mathbf{m}_2,\mathbf{m}_4$	$\mathbf{s}_1\mathbf{a}_{\{2,3,4,6\}}=0$	$[2,-\frac{31}{8},3]^\mathsf{T}$	$[\frac{1}{4},\frac{29}{4},-\frac{9}{2},-\frac{3}{2}]^\mathsf{T}$
$\mathbf{a}_{\{2,3,5,6\}}$	$\mathbf{m}_1,\mathbf{m}_3,\mathbf{m}_4$	$\mathbf{s}_1\mathbf{a}_{\{2,3,5,6\}}=0$	$[-\frac{71}{12},3,1]^\mathsf{T}$	$[\frac{61}{12},-\frac{23}{4},\frac{1}{12},\frac{13}{12}]^\mathsf{T}$
$\mathbf{a}_{\{2,4,5,6\}}$	$\mathbf{m}_2,\mathbf{m}_3,\mathbf{m}_4$	$\mathbf{s}_1\mathbf{a}_{\{2,4,5,6\}}=0$	$[2,1,-\frac{64}{23}]^\mathsf{T}$	$[\frac{33}{23},-\frac{31}{23},\frac{15}{23},-\frac{49}{23}]^\mathsf{T}$
$\mathbf{a}_{\{3,4,5,6\}}$	$\mathbf{m}_1,\mathbf{m}_2,\mathbf{m}_3,\mathbf{m}_4$	$\mathbf{s}_1\mathbf{a}_{\{3,4,5,6\}}=0,\mathbf{s}_2\mathbf{a}_{\{3,4,5,6\}}=0$	$[1,\frac{23}{11},5,-\frac{68}{11}]^\mathsf{T}$	$[\frac{86}{11},\frac{40}{11},-\frac{46}{11},-\frac{114}{11}]^\mathsf{T}$

we select $\mathbf{b}_{\mathcal{V}}$ satisfying $\mathbf{s}_k\mathbf{a}_{\mathcal{V}}=0,\ \forall k\in\mathcal{B}_{\mathcal{V}}$, $\mathbf{a}_{\mathcal{V}}$ is represented in (19),

$$\mathbf{A}\begin{bmatrix} b_{\mathcal{V},1}\\ \vdots\\ b_{\mathcal{V},|\mathcal{M}_{\mathcal{V}}|}\end{bmatrix}=\begin{bmatrix}0\\ \vdots\\ 0\end{bmatrix}. \tag{21}$$

Assume $l_1=\mathcal{V}\cap[\mathsf{K}-\mathsf{U}]$ and $l_2=\mathcal{V}\cap[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]$, then we have $|\mathcal{M}_{\mathcal{V}}|=l_2$, $|\mathcal{B}_{\mathcal{V}}|=\mathsf{K}-\mathsf{U}-l_1$ and $l_1+l_2=\mathsf{S}$. From $\mathsf{S}>\mathsf{K}-\mathsf{U}$, we can obtain $|\mathcal{M}_{\mathcal{V}}|>|\mathcal{B}_{\mathcal{V}}|$, so $\mathbf{b}_{\mathcal{V}}$ can be a null space vector of $\mathbf{A}$.

For $k\in[\mathsf{K}-\mathsf{U}]$, $\mathbf{s}_k$ can be obtained directly from $[\mathbf{s}_1;\ldots;\mathbf{s}_{\mathsf{K}-\mathsf{U}}]$; for $k\in[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]$, $\mathbf{s}_k$ is the left null space vector of $[\mathbf{m}_1,\ldots,\mathbf{m}_{k-\mathsf{K}+\mathsf{U}-1},\mathbf{m}_{k-\mathsf{K}+\mathsf{U}+1},\ldots,\mathbf{m}_{\mathsf{U}}]$.

We next give a general proof of the choice of coefficients that satisfies the Constraints in (1), (2), (3).

Constraint (1)**.** For user $k\in[\mathsf{K}-\mathsf{U}]$, the matrix $\left[\mathbf{a}_{\mathcal{S}_1^{\bar{k}}},\ldots,\mathbf{a}_{\mathcal{S}_{\binom{\mathsf{K}-1}{\mathsf{S}}}^{\bar{k}}}\right]$ with dimension of $\mathsf{U}\times\binom{\mathsf{K}-1}{\mathsf{S}}$ has a non-zero left space $\mathbf{s}_k$, which makes the rank of the matrix less than or equal to $\mathsf{U}-1$. For user $k\in[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]$, each column vector of the matrix $\left[\mathbf{a}_{\mathcal{S}_1^{\bar{k}}},\ldots,\mathbf{a}_{\mathcal{S}_{\binom{\mathsf{K}-1}{\mathsf{S}}}^{\bar{k}}}\right]$ can be seen as a linear combination of $[\mathbf{m}_1,\ldots,\mathbf{m}_{k-\mathsf{K}+\mathsf{U}-1},\mathbf{m}_{k-\mathsf{K}+\mathsf{U}+1},\ldots,\mathbf{m}_{\mathsf{U}}]$, which makes the rank less than or equal to $\mathsf{U}-1$.

Next, we consider the decodability in the transmission, we give the following lemma, whose detailed proof can be found in Appendix D.

Lemma 2. *Any* U *vectors of* $\mathbf{s}_1,\mathbf{s}_2,\ldots,\mathbf{s}_{\mathsf{K}}$ *are linearly independent with high probability.*

Constraint (2)**.** From U linearly independent combinations of $F_1,\ldots,F_{\mathsf{U}}$, the decodability constraint can be proved directly by Lemma 2.

Lemma 3. *By this interference alignment coefficient design, the matrix*

$$\left[\mathbf{a}_{\mathcal{S}^k_{\mathcal{T},1}}([\mathsf{U}-|\mathcal{T}|]),\ldots,\mathbf{a}_{\mathcal{S}^k_{\mathcal{T},\binom{\mathsf{K}-|\mathcal{T}|-1}{\mathsf{S}-1}}}([\mathsf{U}-|\mathcal{T}|])\right] \tag{22}$$

has rank equal to $\mathsf{U}-|\mathcal{T}|$ *with high probability.*[2]

The proof of Lemma 3 could be found in Appendix E.

Constraint (3)**.** By Lemma 3, the security constraint can be proved. It is intuitively evident that the colluding set $\mathcal{T}$ can be expressed as the union of two subsets, namely $\mathcal{T}_1=\mathcal{T}\cap[\mathsf{K}-\mathsf{U}]$ and $\mathcal{T}_2=\mathcal{T}\cap[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]$. Consider the matrix $\left[\mathbf{a}_{\mathcal{S}^k_{\mathcal{T},1}}([\mathsf{U}-|\mathcal{T}|]),\ldots,\mathbf{a}_{\mathcal{S}^k_{\mathcal{T},\binom{\mathsf{K}-|\mathcal{T}|-1}{\mathsf{S}-1}}}([\mathsf{U}-|\mathcal{T}|])\right]$, which are spanned in $\mathbf{M}\setminus\{\mathbf{m}_{i-\mathsf{K}+\mathsf{U}}:i\in\mathcal{T}_2\}$. Simultaneously, the left null space of this matrix contains $\{\mathbf{s}_j:j\in\mathcal{T}_1\}$. With high probability, the rank of the matrix is equal to $\mathsf{U}-|\mathcal{T}_1|-|\mathcal{T}_2|=\mathsf{U}-|\mathcal{T}|$.

In conclusion, all constraints in (1), (2), and (3) are satisfied with high probability; thus there must exist a choice of $\mathbf{a}_{\mathcal{V}}$ where $\mathcal{V}\in\binom{[\mathsf{K}]}{\mathsf{S}}$ and $\mathbf{s}_k$ where $k\in[\mathsf{K}]$ satisfying those constraints. Hence, the proposed scheme is decodable, secure and achieves the optimal rate.

Appendix D
Proof of Lemma 2

For any set $\mathcal{A}\subseteq[\mathsf{K}]$ where $|\mathcal{A}|=\mathsf{U}$, we will prove that the U vectors in $\{\mathbf{s}_k:k\in\mathcal{A}\}$ are linearly independent with high probability by the Schwartz-Zippel Lemma [19]–[21]. Note

[2]Recall that $\mathbf{a}_{\mathcal{S}^k_{\mathcal{T},i}}([\mathsf{U}-|\mathcal{T}|])$ represents the the first $\mathsf{U}-|\mathcal{T}|$ elements of $\mathbf{a}_{\mathcal{S}^k_{\mathcal{T},i}}$, where $\mathcal{S}^k_{\mathcal{T},i}$ represents the i-th set (in a lexicographic order) in $\left\{\mathcal{V}\in\binom{[\mathsf{K}]\setminus\mathcal{T}}{\mathsf{S}}:k\in\mathcal{V}\right\}$.

that each of the above vector is a U-dimensional vector. The determinant of the matrix

$$\begin{bmatrix} \mathbf{s}_{\mathcal{A}(1)} \\ \cdots \\ \mathbf{s}_{\mathcal{A}(\mathsf{U})} \end{bmatrix} \tag{23}$$

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 $\mathbf{s}_1, \ldots, \mathbf{s}_{\mathsf{K}-\mathsf{U}}$, $\mathbf{m}_1, \ldots, \mathbf{m}_{\mathsf{K}-\mathsf{U}}$, and $\mathbf{b}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ and $[\mathsf{K}-\mathsf{U}] \subseteq \mathcal{V}$; each element in the above vectors is uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}$ where q is large enough. Hence, by the Schwartz-Zippel Lemma [19]–[21], 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 $\mathbf{s}_1, \ldots, \mathbf{s}_{\mathsf{K}-\mathsf{U}}$, $\mathbf{m}_1, \ldots, \mathbf{m}_{\mathsf{U}}$, and $\mathbf{b}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ and $[\mathsf{K}-\mathsf{U}] \subseteq \mathcal{V}$, goes to 0 when q goes to infinity, and thus the matrix in (23) is full rank with high probability. So in the following, we need to show that $P_{\mathcal{A}} = D_{\mathcal{A}} Q_{\mathcal{A}}$ is non-zero by finding out a realization of $\mathbf{s}_1, \ldots, \mathbf{s}_{\mathsf{K}-\mathsf{U}}$, $\mathbf{m}_1, \ldots, \mathbf{m}_{\mathsf{U}}$, and $\mathbf{b}_{\mathcal{V}}$ where $\mathcal{V} \in \binom{[\mathsf{K}]}{\mathsf{S}}$ and $[\mathsf{K}-\mathsf{U}] \subseteq \mathcal{V}$, such that $D_{\mathcal{A}} \neq 0$ and $Q_{\mathcal{A}} \neq 0$.

To guarantee $Q_{\mathcal{A}} \neq 0$, the selected realization should satisfy that $\mathbf{s}_{\mathcal{A}(1)}, \ldots, \mathbf{s}_{\mathcal{A}(\mathsf{U})}$ exist. Each $\mathbf{s}_{k_1}$ where $k_1 \in ([\mathsf{K}-\mathsf{U}] \cap \mathcal{A})$ exists since its elements are selected uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}$. Each $\mathbf{s}_{k_2}$ where $k_2 \in ([\mathsf{K}-\mathsf{U}+1:\mathsf{K}] \cap \mathcal{A})$ is a left null vector of $\begin{bmatrix} \mathbf{a}_{\mathcal{S}_1^{\overline{k}}}, \ldots, \mathbf{a}_{\mathcal{S}_{\binom{\mathsf{K}-1}{\mathsf{S}}}^{\overline{k}}} \end{bmatrix}$, whose has rank is no more than $\mathsf{U}-1$ as we proved Constraint (1). Hence, $\mathbf{s}_{k_2}$ also exists.

To guarantee $D_{\mathcal{A}} \neq 0$, under the selected realization, the matrix in (23) should be full rank. We select that $\mathbf{m}_i = \mathbf{e}_{\mathsf{U},i}$, representing the column-wise unit vector with dimension U where the i^{th} element is 1 and the other elements are 0.

For each $k \in ([\mathsf{K}-\mathsf{U}+1:\mathsf{K}] \cap \mathcal{A})$, we focus on the set $[\mathsf{K}-\mathsf{U}+1:\mathsf{K}] \backslash \{k\}$ and retrieve $\mathsf{S}-(\mathsf{K}-\mathsf{U})$ elements in a cyclic wrap around way in this set. This is possible because $\mathsf{U}-1 > \mathsf{S}-(\mathsf{K}-\mathsf{U})$ (recall that $\mathsf{S} < \mathsf{K}-\mathsf{T}$ and $\mathsf{T} > 0$). Thus there are $\mathsf{U}-1$ possible retrievable sets (each containing $\mathsf{S}-(\mathsf{K}-\mathsf{U})$ elements), denoted by $\mathcal{V}_{\overline{k},1}, \mathcal{V}_{\overline{k},2}, \ldots, \mathcal{V}_{\overline{k},\mathsf{U}-1}$. Next note that the compositions of $\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k},1}}, \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k},2}}, \ldots, \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k},\mathsf{U}-1}}$ are also in a cyclic wrap around way.[3] Then we can prove by the Schwartz-Zippel Lemma [19]–[21] that, the matrix $[\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k},1}}, \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k},2}}, \ldots, \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k},\mathsf{U}-1}}]$ is full rank with high probability.[4]

By our construction, $\mathbf{s}_k$ is a left null vector of the matrix $[\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k},1}}, \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k},2}}, \ldots, \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k},\mathsf{U}-1}}]$, where this matrix is spanned by the base vectors $\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_{k-1-(\mathsf{K}-\mathsf{U})}, \mathbf{m}_{k+1-(\mathsf{K}-\mathsf{U})}, \ldots, \mathbf{m}_{\mathsf{U}}$. By the choice of $\mathbf{m}_i = \mathbf{e}_{\mathsf{U},i}$ for each $i \in [\mathsf{U}]$, it can be seen that $\mathbf{s}_k$ could be $\mathbf{e}_{\mathsf{U},k-(\mathsf{K}-\mathsf{U})}$.

As a result, the vectors in $\{\mathbf{s}_k : k \in ([\mathsf{K}-\mathsf{U}+1:\mathsf{K}] \cap \mathcal{A})\}$ are linearly independent. In addition, each $\mathbf{s}_k$ where $k \in ([\mathsf{K}-\mathsf{U}] \cap \mathcal{A})$ has uniformly i.i.d. elements on a large enough field $\mathbb{F}_{\mathsf{q}}$. Hence, the matrix in (23) is full rank with high probability.

Appendix E
Proof of Lemma 3

We focus on one $k \in [\mathsf{K}]$ and one $\mathcal{T} \subseteq [\mathsf{K}] \setminus \{k\}$ where $|\mathcal{T}| \leq \mathsf{T}$. Denote $\mathcal{T}_1 = \mathcal{T} \cap [\mathsf{K}-\mathsf{U}]$ and $\mathcal{T}_2 = \mathcal{T} \cap [\mathsf{K}-\mathsf{U}+1:\mathsf{K}]$; thus $\mathsf{T} = |\mathcal{T}_1| + |\mathcal{T}_2|$. We will prove that

$$\left[\mathbf{a}_{\mathcal{S}^k_{\overline{\mathcal{T}},1}}([\mathsf{U}-|\mathcal{T}|]), \ldots, \mathbf{a}_{\mathcal{S}^k_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|-1}{\mathsf{S}-1}}}([\mathsf{U}-|\mathcal{T}|])\right] \tag{24}$$

has rank equal to $\mathsf{U}-|\mathcal{T}|$ with high probability, by considering two cases, $k \in [\mathsf{K}-\mathsf{U}]$ and $k \in [\mathsf{K}-\mathsf{U}+1:\mathsf{K}]$, respectively.

Let us first consider the case where $k \in [\mathsf{K}-\mathsf{U}]$. Among the vectors of non-colluding keys $\mathbf{a}_{\mathcal{S}^k_{\overline{\mathcal{T}},1}}([\mathsf{U}-|\mathcal{T}|]), \ldots, \mathbf{a}_{\mathcal{S}^k_{\overline{\mathcal{T}},\binom{\mathsf{K}-|\mathcal{T}|-1}{\mathsf{S}-1}}}([\mathsf{U}-|\mathcal{T}|])$, we want to prove that $\mathsf{U}-|\mathsf{T}|$ of them are linearly independent with high probability. We focus on the set $[\mathsf{K}-\mathsf{U}+1:\mathsf{K}] \setminus \mathcal{T}$, and retrieve $\mathsf{S}-(\mathsf{K}-\mathsf{U}-|\mathcal{T}_1|)$ elements in a cyclic wrap around way in this set, which is possible because $\mathsf{U}-|\mathcal{T}_2| = \mathsf{U}-|\mathcal{T}|+|\mathcal{T}_1| > \mathsf{S}-(\mathsf{K}-\mathsf{U}-|\mathcal{T}_1|)$ (recall that $\mathsf{S} < \mathsf{K}-\mathsf{T} \leq \mathsf{K}-|\mathcal{T}|$). Thus there are $\mathsf{U}-|\mathcal{T}_2| = \mathsf{U}-|\mathcal{T}|+|\mathcal{T}_1|$ possible retrievable sets (each containing $\mathsf{S}-(\mathsf{K}-\mathsf{U}-|\mathcal{T}_1|)$ elements), denoted by $\mathcal{V}_{k,1}, \mathcal{V}_{k,2}, \ldots, \mathcal{V}_{k,\mathsf{U}-|\mathcal{T}|+|\mathcal{T}_1|}$.

Note that the compositions of $\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{k,1}}, \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{k,2}}, \ldots, \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{k,\mathsf{U}-|\mathcal{T}|}}$ are also in a cyclic wrap around way. Since the elements of $\mathbf{b}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{k,1}}, \ldots, \mathbf{b}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{k,\mathsf{U}-|\mathcal{T}|}}$ and $\mathbf{m}_1, \ldots, \mathbf{m}_{\mathsf{U}}$ are uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}$, the matrix $[\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{k,1}}([\mathsf{U}-|\mathcal{T}|]), \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{k,2}}([\mathsf{U}-|\mathcal{T}|]), \ldots, \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{k,\mathsf{U}-|\mathcal{T}|}}([\mathsf{U}-|\mathcal{T}|])]$ is full rank with high probability (i.e., rank $\mathsf{U}-|\mathcal{T}|$), by a similar proof as in Footnote 4.

We then consider the case where $k \in [\mathsf{K}-\mathsf{U}+1:\mathsf{K}]$. We focus on the set $[\mathsf{K}-\mathsf{U}+1:\mathsf{K}] \setminus (\mathcal{T} \cup \{k\})$, and retrieve $\mathsf{S}-(\mathsf{K}-\mathsf{U}-|\mathcal{T}_1|)-1$ elements in a cyclic wrap around way in this set, which is possible because $\mathsf{U}-|\mathcal{T}_2|-1 = \mathsf{U}-|\mathcal{T}|+|\mathcal{T}_1|-1 > \mathsf{S}-(\mathsf{K}-\mathsf{U}-|\mathcal{T}_1|)-1$. Thus there are $\mathsf{U}-|\mathcal{T}_2|-1 = \mathsf{U}-|\mathcal{T}|+|\mathcal{T}_1|-1$ possible retrievable sets (each containing $\mathsf{S}-(\mathsf{K}-\mathsf{U}-|\mathcal{T}_1|)-1$ elements), denoted by $\mathcal{V}'_{k,1}, \mathcal{V}'_{k,2}, \ldots, \mathcal{V}'_{k,\mathsf{U}-|\mathcal{T}|+|\mathcal{T}_1|-1}$.

Next consider the case $|\mathcal{T}_1| \geq 1$ and $k \in [\mathsf{K}-\mathsf{U}+1:\mathsf{K}]$. The composition of each vector in $\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{k\}\cup\mathcal{V}'_{k,1}}, \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{k\}\cup\mathcal{V}'_{k,2}}, \ldots, \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{k\}\cup\mathcal{V}'_{k,\mathsf{U}-|\mathcal{T}|}}$ contains $\mathbf{m}_{k-(\mathsf{K}-\mathsf{U})}$, after removing $\mathbf{m}_{k-(\mathsf{K}-\mathsf{U})}$, the compositions of the above $\mathsf{U}-|\mathcal{T}|$ vectors are in a cyclic

[3] Let us go back to Table I. If $k=4$, we have $\mathcal{V}_{4,1} = \{3,5\}$, $\mathcal{V}_{4,2} = \{5,6\}$, $\mathcal{V}_{4,3} = \{6,3\}$. The compositions of $\mathbf{a}_{\{1,2,3,5\}}$, $\mathbf{a}_{\{1,2,5,6\}}$, and $\mathbf{a}_{\{1,2,3,6\}}$ are $(\mathbf{m}_1, \mathbf{m}_3)$, $(\mathbf{m}_3, \mathbf{m}_4)$, and $(\mathbf{m}_1, \mathbf{m}_4)$ respectively; thus we can see that the compositions are also in a cyclic wrap around way.

[4] Recall that the elements of $\mathbf{b}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k},1}}, \mathbf{b}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k},2}}, \ldots, \mathbf{b}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k},\mathsf{U}-1}}$ are uniformly i.i.d. over $\mathbb{F}_{\mathsf{q}}$, and that by (19)

$$\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k},i}} = \sum_{j \in |\mathcal{V}_{\overline{k},i}|} b_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k}},j}\ \mathbf{m}_{\mathcal{V}_{\overline{k},i}(j)-(\mathsf{K}-\mathsf{U})}.$$

We can select one realization of $\mathbf{b}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k},i}} = \mathbf{e}^{\mathsf{T}}_{\mathsf{U}-1,i}$ for $i \in [\mathsf{U}-1]$, and it can be easily seen that the resulting $[\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k},1}}, \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k},2}}, \ldots, \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{V}_{\overline{k},\mathsf{U}-1}}]$ is an identity matrix after some row permutation.

wrap around way. Hence, by a similar proof as in Footnote 4, the matrix $[\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{k\}\cup\mathcal{V}'_{k,1}}([\mathsf{U}-|\mathcal{T}|]), \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{k\}\cup\mathcal{V}'_{k,2}}([\mathsf{U}-|\mathcal{T}|]), \ldots, \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{k\}\cup\mathcal{V}'_{k,\mathsf{U}-|\mathcal{T}|}}([\mathsf{U}-|\mathcal{T}|])]$ is full rank (i.e., rank $\mathsf{U}-|\mathcal{T}|$) with high probability.

Finally, consider the case $|\mathcal{T}_1|=0$ and $k\in[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]$. In this case, we have $\mathsf{U}-|\mathcal{T}|+|\mathcal{T}_1|-1=\mathsf{U}-|\mathcal{T}|-1$ and thus there are only $\mathsf{U}-|\mathcal{T}|-1$ sets in $\mathcal{V}'_{k,1},\mathcal{V}'_{k,2},\ldots,\mathcal{V}'_{k,\mathsf{U}-|\mathcal{T}|+|\mathcal{T}_1|-1}$. So besides the $\mathsf{U}-|\mathcal{T}|-1$ vectors in

$$\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{k\}\cup\mathcal{V}'_{k,1}}([\mathsf{U}-|\mathcal{T}|]), \mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{k\}\cup\mathcal{V}'_{k,2}}([\mathsf{U}-|\mathcal{T}|]), \ldots, \tag{25}$$

$$\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{k\}\cup\mathcal{V}'_{k,\mathsf{U}-|\mathcal{T}|-1}}([\mathsf{U}-|\mathcal{T}|]),$$

we need to consider another vector in $\mathbf{a}_{\mathcal{S}^k_{\mathcal{T},1}}([\mathsf{U}-|\mathcal{T}|]), \ldots, \mathbf{a}_{\mathcal{S}^k_{\mathcal{T},\binom{\mathsf{K}-|\mathcal{T}|-1}{\mathsf{S}-1}}}([\mathsf{U}-|\mathcal{T}|])$, such that this vector is linearly independent with all the $\mathsf{U}-|\mathcal{T}|-1$ vectors in (25). For this purpose, we consider one vector $\mathbf{a}_{[2:\mathsf{K}-\mathsf{U}]\cup\{k\}\cup\mathcal{V}}([\mathsf{U}-|\mathcal{T}|])$, where $\mathcal{V}$ is a set in $\binom{[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]\setminus(\{k\}\cup\mathcal{T})}{\mathsf{S}-(\mathsf{K}-\mathsf{U})}$. Note that $\mathcal{V}$ must exist since $\mathsf{S}<\mathsf{K}-\mathsf{T}$, which leads $\mathsf{U}-1-|\mathcal{T}|\geq\mathsf{S}-(\mathsf{K}-\mathsf{U})$.

At the end of this Appendix, we will prove that the matrix

$$[\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{k\}\cup\mathcal{V}'_{k,1}}([\mathsf{U}-|\mathcal{T}|]), \ldots, \tag{26}$$

$$\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{k\}\cup\mathcal{V}'_{k,\mathsf{U}-|\mathcal{T}|-1}}([\mathsf{U}-|\mathcal{T}|]), \mathbf{a}_{[2:\mathsf{K}-\mathsf{U}]\cup\{k\}\cup\mathcal{V}}([\mathsf{U}-|\mathcal{T}|])]$$

with dimension $(\mathsf{U}-|\mathcal{T}|)\times(\mathsf{U}-|\mathcal{T}|)$, is full rank with high probability, by using the Schwartz-Zippel Lemma [19]–[21].

After considering the above cases, Lemma 3 is proved.

Finally, we prove that the matrix in (26) is full rank with high probability. Recall that $\mathcal{V}$ is a set in $\binom{[\mathsf{K}-\mathsf{U}+1:\mathsf{K}]\setminus(\{k\}\cup\mathcal{T})}{\mathsf{S}-(\mathsf{K}-\mathsf{U})}$. Denote $\{k\}\cup\mathcal{V}=\mathcal{Q}$, we have $|\mathcal{Q}|=\mathsf{S}-(\mathsf{K}-\mathsf{U})+1$ and

$$\mathbf{a}_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q}}=\sum_{i\in|\mathcal{Q}|} b_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q},i}\ \mathbf{m}_{\mathcal{Q}(i)-(\mathsf{K}-\mathsf{U})}, \tag{27}$$

by the composition of $\mathbf{a}_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q}}$.

It can be seen from (21) that $\mathbf{b}_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q}}=(b_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q},i},\ldots,b_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q},|\mathcal{Q}|})$ should satisfy the constraint that $\mathbf{s}_1\mathbf{a}_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q}}=0$. This can be done by choosing $b_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q},1},\ldots,b_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q},|\mathcal{Q}|-1}$ uniformly i.i.d. over $\mathbb{F}_\mathsf{q}$ and then solve $b_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q},|\mathcal{Q}|}$ by the equation $\mathbf{s}_1\mathbf{a}_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q}}=0$. For the ease of following description, we assume that k is not the largest number in $\mathcal{Q}$.[5]

In order to prove the matrix in (26) is full rank with high probability, we need to find out one realization of the uniformly i.i.d. elements in $\mathbf{m}_1,\ldots,\mathbf{m}_\mathsf{U}$, $\mathbf{b}_{[\mathsf{K}-\mathsf{U}]\cup\{k\}\cup\mathcal{V}'_{k,1}},\ldots,\mathbf{b}_{[\mathsf{K}-\mathsf{U}]\cup\{k\}\cup\mathcal{V}'_{k,\mathsf{U}-|\mathcal{T}|-1}}, b_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q},1},\ldots,$ $b_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q},|\mathcal{Q}|-1}$, and $\mathbf{s}_1$, such that the matrix in (26) exists and full rank. Note that

$$\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{k\}\cup\mathcal{V}'_{k,1}}([\mathsf{U}-|\mathcal{T}|]),\ldots,\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\{k\}\cup\mathcal{V}'_{k,\mathsf{U}-|\mathcal{T}|-1}}([\mathsf{U}-|\mathcal{T}|])$$

exist since by (19), we have for each $i\in[\mathsf{U}-|\mathcal{T}|-1]$ (denoting $\{k\}\cup\mathcal{V}'_{k,i}=\mathcal{Q}_{k,i}$)

$$\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{Q}_{k,i}}=\sum_{j\in|\mathcal{Q}_{k,i}|} b_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{Q}_{k,i},j}\ \mathbf{m}_{\mathcal{Q}_{k,i}(j)-(\mathsf{K}-\mathsf{U})}, \tag{28}$$

where the elements in $\mathbf{b}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{Q}_{k,i}}$ and $\mathbf{m}_1,\ldots,\mathbf{m}_\mathsf{U}$ are uniformly i.i.d. over $\mathbb{F}_\mathsf{q}$. Hence, the existence of the matrix in (26) is satisfied if $\mathbf{s}_1\mathbf{a}_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q}}=0$ has solution, which only requires that $\mathbf{s}_1\mathbf{m}_{\mathcal{Q}(|\mathcal{Q}|)-(\mathsf{K}-\mathsf{U})}\neq 0$.

We next choose a realization of $\mathbf{m}_1,\ldots,\mathbf{m}_\mathsf{U}$, $\mathbf{b}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{Q}_{k,1}},\ldots,\mathbf{b}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{Q}_{k,\mathsf{U}-|\mathcal{T}|-1}}, b_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q},1},\ldots,$ $b_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q},|\mathcal{Q}|-1}$, and $\mathbf{s}_1$, such that $\mathbf{s}_1\mathbf{m}_{\mathcal{Q}(|\mathcal{Q}|)-(\mathsf{K}-\mathsf{U})}\neq 0$ and the matrix in (26) is full rank.

We let $[\mathbf{m}_1,\ldots,\mathbf{m}_\mathsf{U}]$ be an MDS matrix with dimension $\mathsf{U}\times\mathsf{U}$. In addition, for each $j\in[|\mathcal{Q}|-1]$, we let $b_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q},j}=1$ if $\mathcal{Q}(j)=k$, and $b_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q},j}=0$ otherwise. Moreover, select $\mathbf{s}_1$ such that $\mathbf{s}_1\mathbf{m}_{k-(\mathsf{K}-\mathsf{U})}=0$ and $\mathbf{s}_1\mathbf{m}_{\mathcal{Q}(|\mathcal{Q}|)-(\mathsf{K}-\mathsf{U})}\neq 0$. Hence, by such selection, we can solve $b_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q},|\mathcal{Q}|}=0$ and thus $\mathbf{a}_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q}}=\mathbf{m}_{k-(\mathsf{K}-\mathsf{U})}$. Then the matrix in (26) becomes

$$[\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{Q}_{k,1}}([\mathsf{U}-|\mathcal{T}|]),\ldots,\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{Q}_{k,\mathsf{U}-|\mathcal{T}|-1}}([\mathsf{U}-|\mathcal{T}|]), \tag{29}$$

$$\mathbf{m}_{k-(\mathsf{K}-\mathsf{U})}([\mathsf{U}-|\mathcal{T}|])]$$

where $\mathbf{m}_{k-(\mathsf{K}-\mathsf{U})}([\mathsf{U}-|\mathcal{T}|])$ represents the first $\mathsf{U}-|\mathcal{T}|$ elements of $\mathbf{m}_{k-(\mathsf{K}-\mathsf{U})}$. Note that after removing $\mathbf{m}_{k-(\mathsf{K}-\mathsf{U})}$, the compositions of $\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{Q}_{k,1}},\ldots,\mathbf{a}_{[\mathsf{K}-\mathsf{U}]\cup\mathcal{Q}_{k,\mathsf{U}-|\mathcal{T}|-1}}$ are in a cyclic wrap around way. So by a similar proof as in Footnote 4, the matrix in (29) is full rank (i.e., rank $\mathsf{U}-|\mathcal{T}|$) with high probability.

[5]If k is the largest number, we can random select $b_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q},2},\ldots,b_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q},|\mathcal{Q}|}$ and solve $b_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q},1}$ by $\mathbf{s}_1\mathbf{a}_{[2:\mathsf{K}-\mathsf{U}]\cup\mathcal{Q}}=0$, and the following proofs could be correspondingly modified.