Optimal Linear Coding Schemes for the Secure Decentralized Pliable Index Coding Problem

Tang Liu and Daniela Tuninetti,
University of Illinois at Chicago, Chicago, IL 60607 USA,
Email: tliu44, danielat@uic.edu

***Abstract*—This paper studies the secure decentralized Pliable Index CODing (PICOD) problem, where the security constraint forbids users to decode more than one message while the decentralized setting imposes that there is no central transmitter in the system, and thus transmissions occur only among users. A converse bound from the Authors' previous work showed a factor of three difference in optimal code-length between the centralized and the decentralized versions of the problem, under the constraint of linear encoding. This paper first lists all *linearly infeasible cases*, that is, problems where no linear code can simultaneously achieve both correctness/decodability and security. Then, it proposes linear coding schemes for the remaining cases and shows that their code-length is to within an additive constant gap from the converse bound.**

I. Introduction

Index Coding: Pliable Index CODing (PICOD) is a variant of the Index Coding (IC) problem. The traditional IC setting consists of m messages, one central transmitter and n users connected by an error-free broadcast channel. Each user has some messages locally stored as its side information set and has one pre-determined message to decode. The structure of the side information sets and the desired messages are known to the transmitter and all the users. The transmitter broadcasts coded symbols to all users. The users decode based on the received coded symbols and their own side information set. The goal for IC is to find the smallest code-length (i..e, number of transmitted coded symbols) such that all users can decode correctly their desired messages.

Pliable Index Coding: PICOD is a variant of IC motivated by the scenarios where the desired message at the users is not be pre-determined [2], such as for example streaming services and online advertisement systems. In PICOD a user is satisfied whenever it can correctly decode at least one message that is not in its side information set. Therefore, the transmitter can leverage the freedom of choosing the desired messages for the users so as to reduce the code-length. Compared to the IC with the same number of users and side information sets, PICOD needs less transmissions to satisfy all the users [9].

Decentralized Problems: The decentralized IC problem is motivated by peer-to-peer communication systems where there is no central transmitter and instead coded symbols are generated by the users based on their side information set and sent through a common time-sharing noiseless broadcast channel. The goal is again to find the minimal code-length that allows every user to correctly decode its desired message. Under linear encoding constraint, the minimum code-length of the decentralized IC is shown to be no more than twice that of its centralized counterpart [1]. The pliable version of decentralized IC was studied in [4], where information theoretical bounds on the optimal code-length were given for some cases and the multiplicative gap between centralized and decentralized PICOD shown to be less than two in general.

Secure Centralized Problems: Security in IC means that the users can only decode their desired message while all other messages that are not in their side information set must remain unknown to the users. The secure IC problem was first proposed in [7], where private one-time-pad keys were used to meet the security demand. A weaker definition of security, which can be achieved without security keys, was discussed in [7] and later extended to the PICOD setting [8]. Achievable and converse bounds for the case of circular side information structure and linear encoding were derived in [5].

Secure Decentralized Problems: In this paper we are interested in the secure and decentralized setting. Recently, the secure PICOD problem in [5] has been extended to the decentralized setting in [6], where a converse bound under the constraint of linear encoding showed a multiplicative gap of roughly three between the secure centralized and decentralized versions of PICOD. This gap is strictly larger than the one between the centralized and decentralized versions of IC without security, which equals two [1].

Contributions: This paper continues the study of the secure decentralized PICOD problem initiated in [6]. The main contribution is a proof that the proposed linear converse in [6] is tight to within a constant additive gap. Specifically, (i) we provide a complete list of linearly infeasible cases, which shows that most cases when the number of messages m is odd are actually feasible, and (ii) we show linear achievable schemes for all remaining feasible cases. We conclude that the proposed schemes achieve the converse bound in [6] to within an *additive constant gap*. Note that the proposed achievable schemes in this work are not straightforward extensions of the schemes for centralized secure PICOD. The schemes in the decentralized setting are more complicated and we have not yet found a single general scheme working for all cases, as what we did for centralized secure PICOD in [6].

Paper Organization: Section II introduces the problem. Section III summarizes the main results. In Section IV we prove the infeasible cases. In Section V we illustrate the main ideas for the achievable schemes by giving examples that highlight the main ideas for the general schemes. Section VI

concludes the paper. The details of the general achievable schemes can be found in the longer version of this paper at [3].

II. Problem formulation

We consider the (m, s) secure decentralized PICOD problem with circular side information structure at the users. The system consists of m messages and m users. The messages are vectors of length $\kappa \in \mathbb{N}$ independent and uniformly distributed bits. $\mathcal{W} := \{w_1, \ldots, w_m\}$ denotes the set of all messages. $W_A := \{w_i, i \in A\}$ denotes the set of messages with indices in set A. $\mathcal{U} := \{u_1, \ldots, u_m\}$ denotes the set of the users. User u_i has message W_{A_i} as its side information, where $A_i = \{i, i-1 \ldots, i-s+1\}$. The entries in the side information set are intended modulo m. The collection $\mathcal{A} = \{A_1, \ldots, A_m\}$ is globally known to all users. The coded symbols are generated by the users based on their side information sets. The encoding function at user u_i is

$$x^{\kappa \ell_i} := \mathbf{ENC}_i(W_{A_i}, \mathcal{A}),\ i \in [m], \tag{1}$$

where $\ell_i \in \mathbb{N}$ is the code-length. The overall transmission is represented by the vector $x^{\kappa \ell} = (x^{\kappa \ell_1}, \ldots, x^{\kappa \ell_m})$ with the total normalized code-length $\ell := \sum_{i \in [m]} \ell_i$.

Each user must correctly acquire a message that is not in its side information set. The decoding function at user u_i is

$$\widehat{w}_i := \mathbf{DEC}_i(x^{\kappa \ell}, W_{A_i}, \mathcal{A}),\ i \in [m]. \tag{2}$$

The decoding is correct if $\widehat{w}_i = w_{d_i}$ for some $d_i \in [m] \setminus A_i$.

The security constraint requires that user u_i decodes no more than one message. Specifically, we have

$$I(w_j; x^{\kappa \ell}, W_{A_i}) = 0, \forall j \in [m] \setminus \{A_i \cup \{d_i\}\}, \forall i \in [m]. \tag{3}$$

The goal is to find the smallest $\ell := \sum_{i \in [m]} \ell_i$ such that all users meet the correctness and security constraints.

III. Main Contributions

For the (m, s) secure decentralized PICOD with circular side information at the users, the converse bound in [6] gives

$$\ell^* \geq \begin{cases} \frac{m}{s}, & \frac{m}{m-s} \in \mathbb{Z}, \\ \frac{3m}{2s}, & \frac{m}{m-s} \notin \mathbb{Z}, \text{linear encoding}, m > 2s, \\ 2, & \frac{m}{m-s} \notin \mathbb{Z}, \text{linear encoding}, m < 2s. \end{cases} \tag{4}$$

In [6] we found several cases where the problem is *linearly infeasible*, that is, no linear scheme exists such that every user can decode one and only one message outside its side information set. For such linearly infeasible cases, the converse bound in (4) is not tight. In this paper, we first give a complete list of all linearly infeasible cases. We then show schemes that attain the converse bound in (4) to within an additive constant gap for all feasible cases. Specifically, we have the following.

Theorem 1 (All infeasible cases). *The (m, s) secure decentralized PICOD with circular side information sets and linear encoding is infeasible if*

1) $m \geq 2s + 1$, $s = 1$ *or* 2;
2) *Odd* $m \geq 7$, $s = 3$ *or* 4;
3) *Odd* m, $s = m - 2$.

Theorem 2 (Achievability to within an additive gap of 7). *For the (m, s) secure decentralized PICOD with circular side information sets that are not listed in Theorem 1, the following is attainable*

$$\ell^* \leq \begin{cases} \frac{m}{s}, & \frac{m}{m-s} \in \mathbb{Z}, \\ \frac{3m}{2s} + 3, & \frac{m}{m-s} \notin \mathbb{Z}, \textit{linear encoding}, m > 2s, \\ 2 + 7, & \frac{m}{m-s} \notin \mathbb{Z}, \textit{linear encoding}, m < 2s. \end{cases} \tag{5}$$

IV. Proof of Theorem 1

In this section we prove the only linearly infeasible case in Theorem 1 that has not been proved in [6], namely, odd $m \geq 7$, $s = 4$. The proof is split into two cases.

A. Case Odd $m \geq 9$, $s = 4$

Assume we have an achievable scheme that satisfies all constraints. Since here we have $m > 2s$, from [5, Proposition 1], one transmission involves at least 2 messages. The number of messages in one transmission is either 2 or 3, since involving $s = 4$ consecutive messages in one transmission is insecure as shown in [6]. For a linear code, a user can decode its desired message if there exists one linear combination of the codewords such that all the messages but its desired message that are involved are in the user's side information set. Therefore, if two transmissions do not satisfy one user and involve no messages in common, the linear combination of these two transmissions will not satisfy the user. Each transmission involving 2 or 3 consecutive messages satisfies 2 users. Each transmission involving 2 nonconsecutive messages satisfies 4 users. Thus, if no transmissions have common messages, the total number of satisfied users is even, which contradicts to the condition that m is odd. Therefore, there must exist two transmissions that have messages in common. We consider the following sub-cases.

a) Both transmissions involve 2 messages: There exists a user that can decode the common message by one transmission, then decode another message by the other transmission. Therefore the user can decode two messages, which violates the security constraint.

b) One transmission involves 2 messages and the other 3 messages: Let $g(.)$ denote a linear combination of its argument. We have the following cases:

1) $g_1(W_{\{4,5\}})$ and $g_2(W_{\{4,5,6\}})$: the user with side information $W_{\{1,2,3,4\}}$ can decode $W_{\{5,6\}}$, which is insecure;
2) $g_1(W_{\{4,5\}})$ and $g_2(W_{\{5,6,7\}})$: the user with side information $W_{\{6,7,8,9\}}$ can decode $W_{\{4,5\}}$, which is insecure;
3) $g_1(W_{\{4,6\}})$ and $g_2(W_{\{4,5,6\}})$: the user with side information $W_{\{1,2,3,4\}}$ can decode $W_{\{5,6\}}$, which is insecure;
4) $g_1(W_{\{4,6\}})$ and $g_2(W_{\{5,6,7\}})$: the user with side information $W_{\{6,7,8,9\}}$ can decode $W_{\{4,5\}}$, which is insecure;
5) $g_1(W_{\{3,5\}})$ and $g_2(W_{\{5,6,7\}})$: the user with side information $W_{\{6,7,8,9\}}$ can decode $W_{\{3,5\}}$, which is insecure.

c) Both transmissions involve 3 consecutive messages: We have the following cases:

1) $g_1(W_{\{4,5,6\}})$ and $g_2(W_{\{4,5,6\}})$: a linear combination of these two transmissions can generate a linear combination of $W_{\{4,5\}}$. This case is insecure as shown in case 1 of paragraph IV-A0b;
2) $g_1(W_{\{4,5,6\}})$ and $g_2(W_{\{5,6,7\}})$: the user with side information $W_{\{2,3,4,5\}}$ can decode $W_{\{6,7\}}$, which is insecure;
3) $g_1(W_{\{4,5,6\}})$ and $g_2(W_{\{6,7,8\}})$: a linear combination of these two transmissions can generate a linear combination of $W_{\{4,5,6,7,8\}}$. This is the only case that does not violate the security constraint. However, this case does not allow any new users to decode. Therefore, the number of satisfied users is the the sum of the number of users satisfied by each transmission, which even. This contradicts the condition that m is odd.

This concludes the linearly infeasible proof.

B. Case $m = 7,\ s = 4$

Assume we have an achievable scheme that satisfies all the constraints. If all the transmissions are linear combinations of at least 2 messages, the argument for the case $s = 4$, odd $m \geq 9$ in the previous subsection holds and thus the case is infeasible. Therefore, it is enough to show that the case $s = 4, m = 7$ is insecure if there is one transmission that involves only one message. Without loss of generality, assume one transmission is a linear function of w_4. Users u_1, u_2, u_3 will decode w_4 since they do not have it in their side information set. User u_3 has the same side information of user u_4 after decoding. Therefore, the desired message of user u_4 needs to be inside the side information of u_3. The desired message of u_4 can only be w_7. The the argument applies to u_7 and its desired message can only be w_1. Thus, only the desired message of user u_5 and user u_6 are not fixed yet. Consider the following cases for the desired message of user u_5.

a) $d_5 = 1$: User u_5 can mimic u_4 and decode w_7.

b) $d_5 = 7$: There must exists a linear combination of codewords that is a linear combination of messages $W_{\{2,3,5,7\}}$ by the decoding condition of the linear index code, where w_7 has non-zero coefficient. Let $k \in \{2, 3, 5\}$ be the largest index in $\{2, 3, 5\}$ so that w_k has non-zero coefficient in said linear combination. User u_{k-1} can decode w_k when $k = 2, 3$, user u_3 can decode w_5 when $k = 5$. Since these users already have other decoded message, the security constraint is violated.

c) $d_5 = 6$: There must exist a linear combination of codewords that is a linear combination of messages $W_{\{2,3,5,6\}}$ by the decoding condition of the linear index code, where the coefficient of w_6 is non-zero. Therefore, there exists one transmission involving w_6. We consider all possible linear combinations that involve w_6.

- Linear combination of w_6, or $W_{\{4,6\}}$, or $W_{\{1,6\}}$, or $W_{\{6,7\}}$, or $W_{\{1,6,7\}}$. User u_3 can decode parts of w_6.
- Linear combination of $W_{\{5,6\}}$ or $W_{\{4,5,6\}}$. User u_2 can decode parts w_5.

Therefore, the case $s = 4, m = 7$ is infeasible.

Overall, we conclude that the case $s = 4$, odd $m \geq 7$ is infeasible. This completes the proof of Theorem 1.

V. Proof of Theorem 2

In this section, we give examples to demonstrate the key ideas of our achievable scheme in Theorem 2. This is because, unlike the centralized setting, we have not found a general scheme that works for all decentralized secure PICODs. Therefore, our achievability contains multiple schemes targeting different cases. We choose several cases as the examples to show the similarity and difference among the schemes. The details on the schemes can be found in [3].

The converse bound in (5) includes three regimes, which we shall address separately. Some intuitions of the general schemes are provided in the remarks at the end of each subsection.

A. Case $\frac{m}{m-s} \in \mathbb{Z}$: $\ell^* = \frac{m}{s}$

The information theoretical converse was derived in [6] for the centralized case. The achievable scheme is the one for the decentralized PICOD without security constraint discussed in [4], which satisfies the security constraint because for each user, among all the messages that are involved in the encoding function, there is one and only one message that is not in its side information set. Therefore, the scheme is also information theoretically optimal with an additional security constraint.

B. Case $\frac{m}{m-s} \notin \mathbb{Z}, m > 2s$: $\ell \leq \frac{3m}{2s} + 3$

The converse bound in this regime is $\frac{3m}{2s}$. Therefore, in order to have an achievable scheme that is optimal within an additive constant gap, we aim to satisfy on average $\frac{2s}{3}$ users in one transmission. It has been shown that, for the cases where $\frac{m}{2s} \in \mathbb{Z}$, an optimal secure centralized scheme is $\{w_{1+2sk} + w_{2+2sk}, w_{3+2sk} + w_{s-2+2sk}, w_{s-3+2sk} + w_{s-4+2sk}\}, k \in \{0, 1, \ldots, \frac{m}{2s} - 1\}$, for a total $\frac{3m}{2s}$ transmissions [6]. In this section, by ways of examples, we show how this scheme can be extended to all feasible cases in the regime $\frac{m}{m-s} \notin \mathbb{Z}, m > 2s$. The detailed proof is in [3, Appendix A].

To make the exposition easier, we shall use the case $m = 26$ in the following examples and represent the scheme in a "matrix" form in the figures. In the figures, a row with **X**'s represents a transmission that is a linear combination of the messages marked by the **X**. A row with **U**'s shows the users that are satisfied by the transmission shown by the row right above with **X**'s. The user represented by the **U** in position i is the user with side information set $W_{A_i} = \{w_{i-s+1}, \ldots, w_i\}$.

a) Case $m = 26, s = 6$: The scheme is illustrated in Fig. 1. We have two groups of $2s = 12$ users each. Six transmissions are used to satisfy the 24 users in these groups. The transmissions are $w_1 + w_2,\ w_3 + w_7,\ w_8 + w_9,\ w_{13} + w_{14},\ w_{15} + w_{19},\ w_{20} + w_{21}$. The two remaining users are satisfied by the last transmission $w_{22} + w_{23} + w_{24} + w_{25} + w_{26}$. The total number of transmissions is $\ell = 7$.

b) Case $m = 26, s = 10$: We have one group of $2s = 20$ users, and 6 remaining users. The transmissions and the users that are satisfied by each transmission are illustrated in Fig. 2. Three transmissions satisfy the 20 users' group. The transmissions are $w_1 + w_2,\ w_3 + w_{12},\ w_{13} + w_{14}$. For the remaining users, we use two transmissions $w_{15} + w_{17} + w_{18} +$

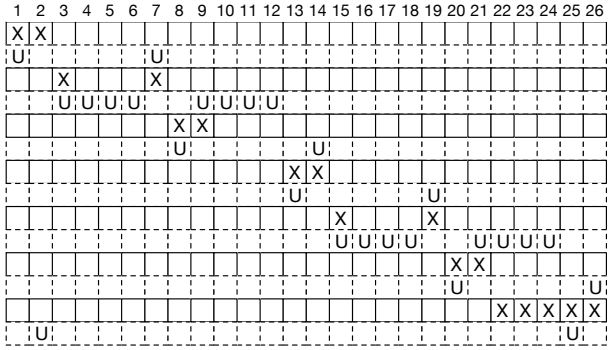

Fig. 1: Achievable scheme for $m = 26, s = 6$.

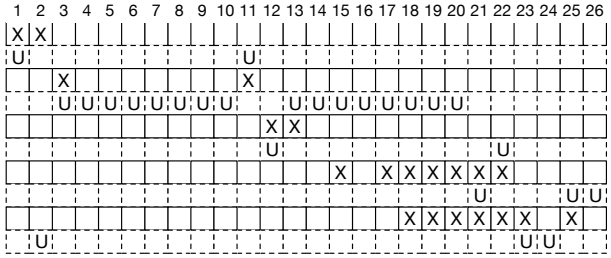

Fig. 2: Achievable scheme for $m = 26, s = 10$.

$w_{19} + w_{20} + w_{21} + w_{22}$ and $w_{18} + w_{19} + w_{20} + w_{21} + w_{22} + w_{23} + w_{25}$, each satisfying three of the remaining users. The total number of transmissions is $\ell = 5$.

Remark 1. *In the regime $m > 2s$ we use the scheme that satisfies $2s$ users by using three transmissions. In the first step, we group the users into disjoint groups of size $2s$ and satisfy the users in each group with 3 transmissions. In the second step, we satisfy the remaining users, which are less than $2s$. Our scheme guarantees that the number of transmissions needed to satisfy the remaining users is a constant that does not grow with the system parameter (m, s). Therefore, the proposed scheme can achieve the converse bound to within an additive constant gap that equals the number of transmissions in the second step.*

C. Case $\frac{m}{m-s} \notin \mathbb{Z}, s < m < 2s$: $\ell \leq 9$

In this regime the scheme in [6] does not work because the number of users is $m < 2s$, thus no group of size $2s$ users can be formed. Here we aim to satisfy all users with a constant number of transmissions that does not grow with the system parameters (m, s). We treat two sub-cases separately.

1) Subcase $\frac{m}{m-s} \notin \mathbb{Z}, s < m \leq \frac{3s}{2}$: In this case we consider the complement of the side information set of every user, which is of size $m-s$. The proposed scheme guarantees that among every consecutive $m-s$ messages, the codewords contain one and only one message that is linearly independent of the remaining $m-s-1$ messages. In the following, we provide examples to demonstrate the scheme. The detailed proof can be found in [3, Appendix B].

a) Case $m = 26, s = 20$: The codewords, which are the linear combinations of the messages, contain two parts:

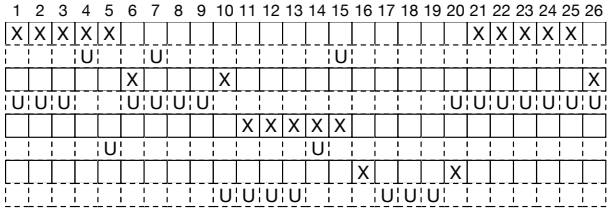

Fig. 3: Achievable scheme for $m = 26, s = 20$.

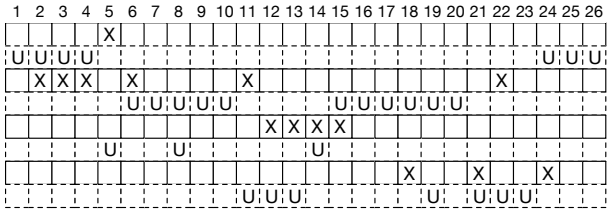

Fig. 4: Achievable scheme for $m = 26, s = 19$.

- Part A are $w_{i+1} + \ldots + w_{i+(m-s-1)}$ and $w_{i+(m-s)} + w_{i+2(m-s-1)}$. The involved messages are in a range of $2k_1(m-s-1)$, where $k_1 \geq 2, k_1 \in \mathbb{Z}$.
- Part B are $w_j, w_{j+1} + \ldots + w_{j+(m-s-1)}$. The involved messages are in a range of $k_2(m-s)$, where $k_2 \in \mathbb{N}$.

The messages the these two parts do not overlap. Therefore, this scheme works for the case $m = k_1 2(m-s-1) + k_2(m-s)$, where $k_1 \geq 2, k_2 \geq 0, k_1, k_2 \in \mathbb{N}$. In the case of $s = 20, m = 26 = 2(10) + 6$, the proposed scheme takes 4 transmissions: $w_1 + w_2 + w_3 + w_4 + w_5 + w_{21} + w_{22} + w_{23} + w_{24} + w_{25}$, $w_6 + w_10 + w_{26}$, $w_{11} + w_{12} + w_{13} + w_{14} + w_{15}$, and $w_{16} + w_{20}$, as shown in Fig. 3.

For the cases where $m \neq k_1 2(m-s-1) + k_2(m-s), \forall k_1 \geq 2, k_2 \geq 0, k_1, k_2 \in \mathbb{Z}$, we propose the following examples to show how the scheme can be modified.

b) Case $m = 26, s = 19$: In this case the proposed scheme takes 4 transmissions: w_5, $w_2 + w_3 + w_4 + w_6 + w_{11} + w_{22}$, $w_{12} + w_{13} + w_{14} + w_{15}$, and $w_{18} + w_{21} + w_{24}$, as shown in Fig. 4. Every $7 = m - s$ consecutive messages are in two linear combinations where one contains one message and the other contains all the other messages with nonzero coefficients. The scheme can be seen as a modified version of the scheme in Section V-C1a: the part from w_6 to w_{17} is a modified Part A; the part from w_{25} to w_5 is a modified Part B; and the rest is a new structure that combines these two pieces.

c) Case $m = 26, s = 18$: In this case the proposed scheme takes 4 transmissions: $w_1 + w_4 + w_5 + w_6 + w_7$, $w_8 + w_{13}$, $w_{15} + w_{16} + w_{17} + w_{18} + w_{19}$, and $w_{22} + w_{26}$, as shown in Fig. 5. One can check that for every $8 = m - s$ consecutive messages are in two linear combinations where one contains one message and the other contains all the other messages with nonzero coefficients. The scheme can be seen as a modified version of the scheme used in Section V-C1a: the part from w_1 to w_{14} is a modified Part A; the part from w_{15} to w_{26} is a modified and shrunk Part A.

Remark 2. *In this regime our proposed scheme is designed*

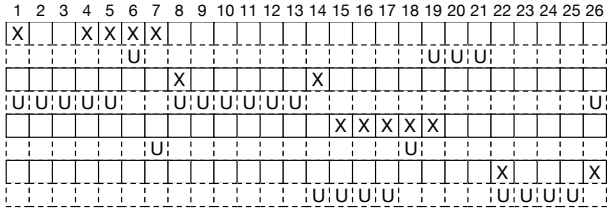

Fig. 5: Achievable scheme for $m = 26, s = 18$.

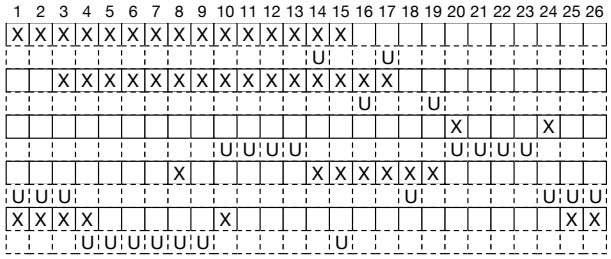

Fig. 6: Achievable scheme for $m = 26, s = 16$.

such that every consecutive $m - s$ messages have one and only one message that is linearly independent of the rest. The scheme treats the m users as "sliding windows" of size $m-s$ on the m messages. The "sliding window" thus satisfies both decodability and security. The scheme for case $m > 2s$ can not be extended straightforwardly in this case because to satisfy users less than $2s$ the scheme has transmissions that take more than $2s$ consecutive messages. This is not an issue in the case $m > 2s$. But when $m < 2s$ this means the transmissions will have messages in common as the indices of the messages are intended modulo m. The common messages among the transmissions could allow one user to decode more than one message so the security constraint thus does not hold anymore.

2) Subcase $\frac{m}{m-s} \notin \mathbb{Z}, \frac{3s}{2} < m < 2s$: Here we propose a scheme that can be seen as a combination of the ideas we presented in Sections V-B and V-C1. That is, we first use a finite number (less than a constant) of transmissions to satisfy a finite number of users with the scheme in [6]. Then, we use a scheme similar to the one proposed for the case $m > 2s$ in Sections V-B for the remaining users. The total number of transmissions is thus finite and the scheme achieves the converse bound to within a constant gap. The following example illustrates the proposed scheme. The detailed proof can be found in [3, Appendix C].

a) Case $m = 26, s = 16$: The first two transmissions are: $w_1 + \cdots + w_{15}$ and $w_3 + w_{17}$. Four users are satisfied by these two transmissions. The remaining users are grouped into 6 groups and are satisfied by 3 transmissions, where each transmission aims to satisfy 2 groups. The transmissions are: $w_{20} + w_{24}$, $w_8 + w_{14} + \cdots + w_{19}$, and $w_1 + \cdots + 4 + w_{10} + w_{25} + w_{26}$. The transmissions and the corresponding satisfied users are shown in Fig. 6. The scheme uses 5 transmissions.

We thus proposed schemes that are to within a constant gap from the converse bound in (4). All cases and the corresponding bounds are summarized in Table I.

TABLE I: All cases and the corresponding achievable schemes. $m_{|a}$ represents $m \bmod a$, where a is an integer; "infea." is the abbreviation of "infeasible".

Condition	Subcase	Converse	ℓ
$\frac{m}{m-s} \in \mathbb{Z}$	all	m/s	m/s
$\frac{m}{m-s} \notin \mathbb{Z}$, $m-4 \geq s \geq 5$, $m > 2s$	$m_{\|2s} = 0$	$\frac{3m}{2s}$	$\frac{3m}{2s}$
	$m_{\|2s} = 1$		$\frac{3m}{2s} + \frac{4s-3}{2s}$
	$m_{\|2s} = 2$		$\frac{3m}{2s} + \frac{s-3}{s}$
	$m_{\|2s} = 3$		$\frac{3m}{2s} + \frac{6s-3}{2s}$
	$m_{\|2s} \in [4:s]$		$\frac{3m}{2s} + \frac{4s-3m_{\|2s}}{2s}$
	$m_{\|2s} \in [s+1:2s-2]$		$\frac{3m}{2s} + \frac{6s-3m_{\|2s}}{2s}$
	$m_{\|2s} = 2s-1$		$\frac{3m}{2s} + \frac{2s+3}{2s}$
$\frac{m}{m-s} \notin \mathbb{Z}$, $m-4 \geq s \geq 5$, $m < 2s$	$s < m \leq 3s/2$	2	≤ 4
	$3s/2 < m < 2s$		≤ 9
$s \leq 4$, $\frac{m}{m-s} \notin \mathbb{Z}$	$s = 1$	infea.	∞
	$s = 2$	infea.	∞
	$s = 3$, even m	$\frac{m}{2}$	$\frac{m}{2}$
	$s = 3$, odd m	infea.	∞
	$s = 4$, even m	$\frac{3m}{8}$	$3\lfloor \frac{m}{8} \rfloor + \frac{m_{\|8}}{2}$
	$s = 4$, odd m	infea.	∞
$s \geq m-3$, $\frac{m}{m-s} \notin \mathbb{Z}$	$m - s = 2$, odd m	infea.	∞
	$m - s = 3$, even m	$\frac{3}{2} + \frac{9}{2s}$	3
	$m - s = 3$, odd m	$\frac{3}{2} + \frac{9}{2s}$	4

VI. Conclusion

In this paper we studied the secure decentralized PICOD with circular side information at the users. We first proved the infeasible case that has not been studied in the prior work. Then for all the remaining cases, we proposed achievable schemes that use the same number of transmissions as predicted by our converse bound under the constraint of linear encoding up to a constant additive gap. Ongoing work includes extending the setting to other types of side information structures.

Acknowledgment

The work of the Authors was partially funded by NSF Awards 1527059 and 1910309.

References

[1] M. W. Alexandra Porter, "Embedded index coding," *Information Theory Workshop*, 2019. arXiv:1904.02179.

[2] S. Brahma and C. Fragouli, "Pliable index coding," *IEEE Trans. on Information Theory*, vol. 61, no. 11, pp. 6192–6203, Nov 2015.

[3] T. Liu and D. Tuninetti, "Optimal linear coding schemes for the secure decentralized pliable index," *arXiv:2010.10494*.

[4] ——, "Decentralized pliable index coding," *Proc. Int. Symp. Inf. Theory*, 2019.

[5] ——, "Private pliable index coding," *arXiv:1904.04468*, 2019.

[6] ——, "Secure decentralized pliable index coding," *Proc. Int. Symp. Inf. Theory*, 2020.

[7] V. Narayanan, J. Ravi, V. K. Mishra, B. K. Dey, N. Karamchandani, and V. M. Prabhakaran, "Private index coding," *Proc. Int. Symp. Inf. Theory*, 2018.

[8] S. Sasi and B. S. Rajan, "On pliable index coding," *arXiv:1901.05809*, 2019.

[9] L. Song and C. Fragouli, "A deterministic algorithm for pliable index coding," in *Proc. Int. Symp. Inf. Theory*, July 2016.