Pliable Index Coding

Tang Liu
University of Illinois at Chicago

11/19/2019

Content

- Introduction
  - Index Coding problem
  - Pliable Index Coding problem
  - Related past work and summary of contributions
- Contributions
  - Greedy achievability for a constant fraction of satisfied users
  - Complete-S and circular-arc PICOD
  - Decentralized PICOD
  - Individual-message secure PICOD
- Conclusion/Discussion/Future work

Motivation

Broadcast channel with message side information

- Broadcast nature of wireless communication.
  - Wireless communication is a crucial part of wireless communication network.
  - Broadcast Internet services (e.g. video/audio streaming) are popular.

- Receivers have more powerful processor and more storage.
  - Devices (e.g. smartphone) become more and more powerful.
  - Storage becomes cheaper and cheaper.

The coding scheme at the transmitter can leverage the computation and storage resources and the receiver.

Satellite communication

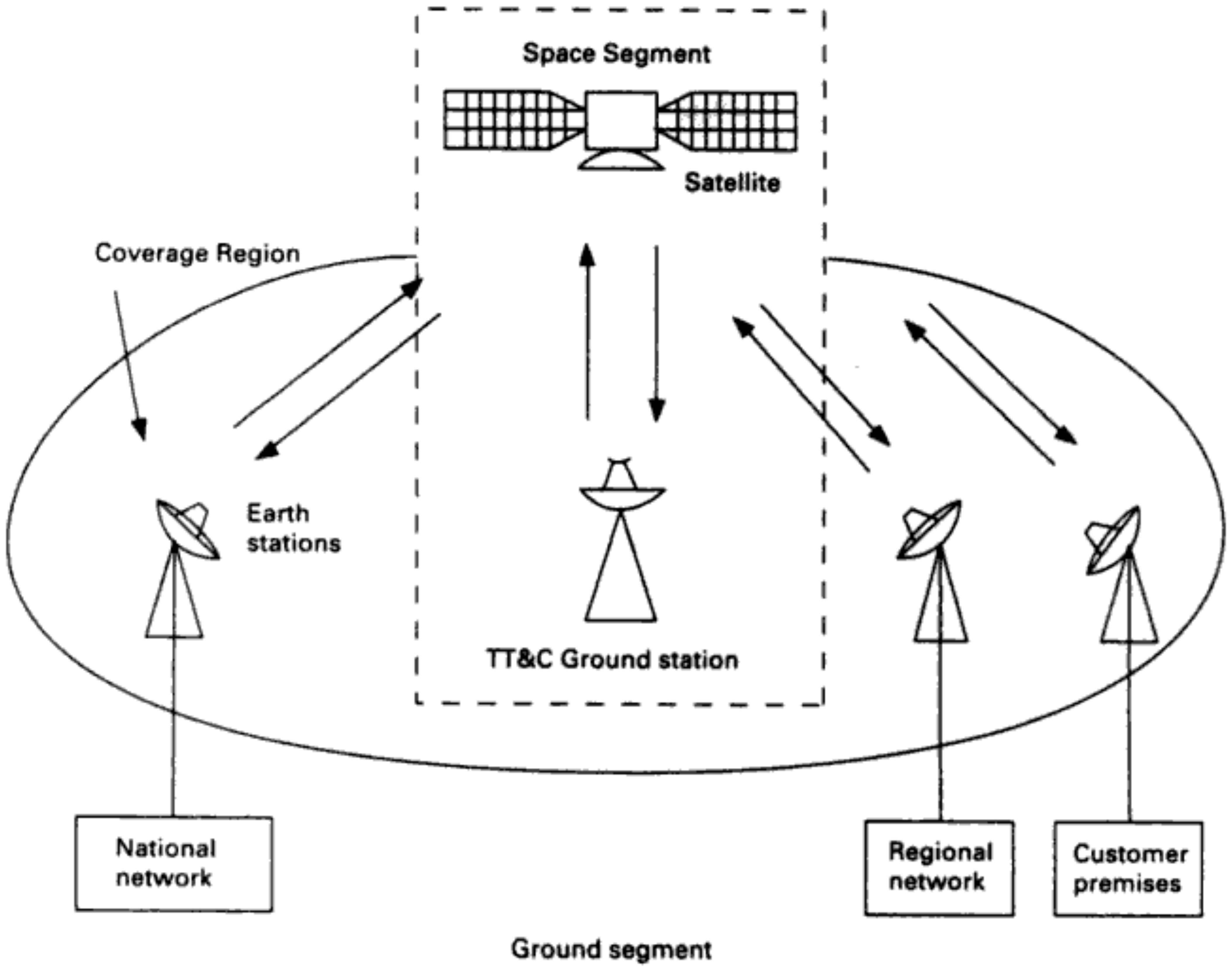


Figure: Satellite communication network with basestations from different

[1] Y. Birk and T. Kol. Coding-on-demand by an informed source (ISCOD) for efficient broadcast of different supplemental data to caching clients. IEEE Transactions on Information Theory, 52(6):2825–2830, 2006. Earlier version appeared in INFOCOM ’98.

Index coding

Notation:

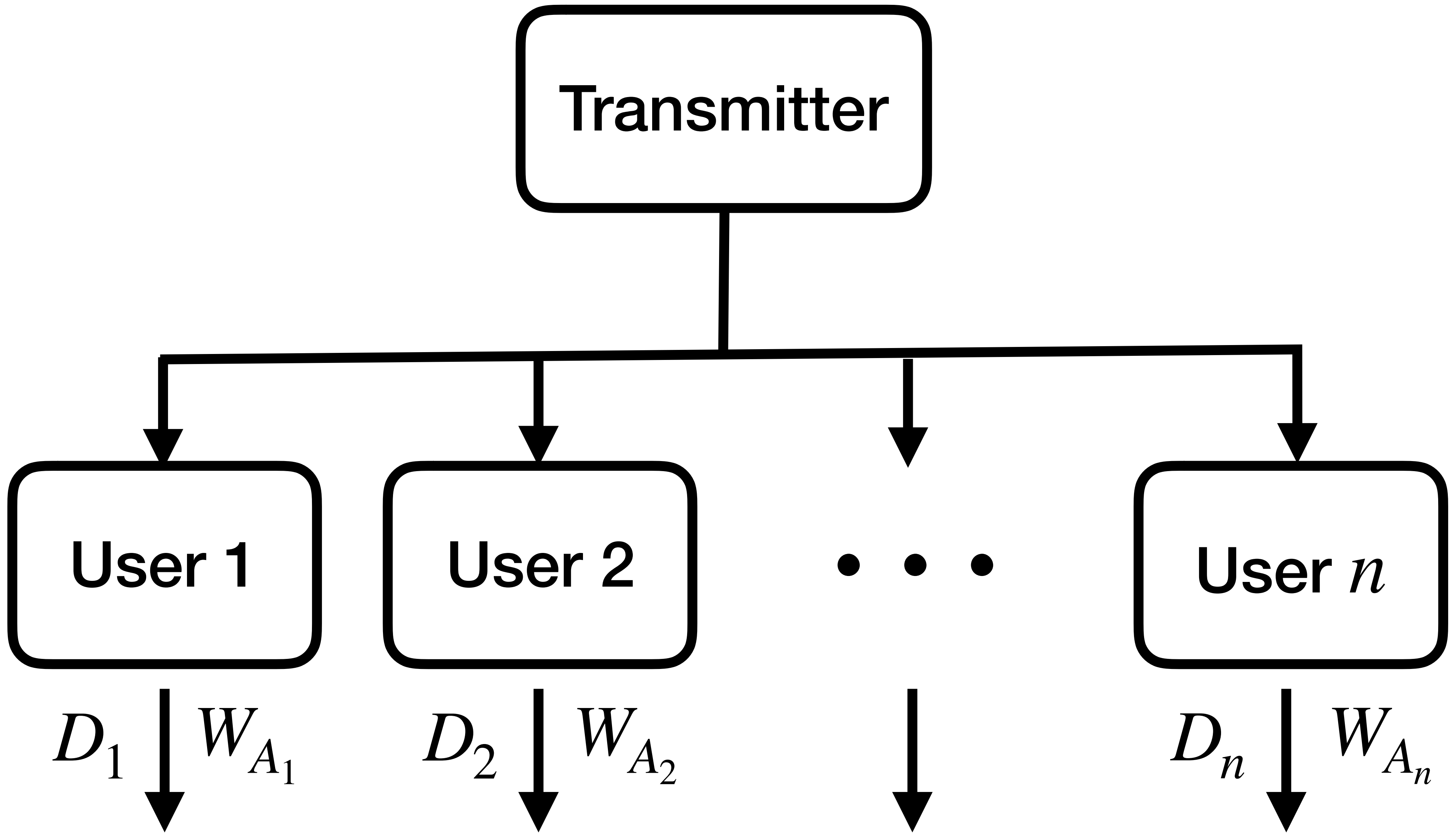
$[m] := \{1,2,\ldots,m\}$;

$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Fixed desired message set: $D_i \subseteq [m] \backslash A_i$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, \mathscr{D} = \{D_1, \ldots, D_n\}$



Index coding

Notation:

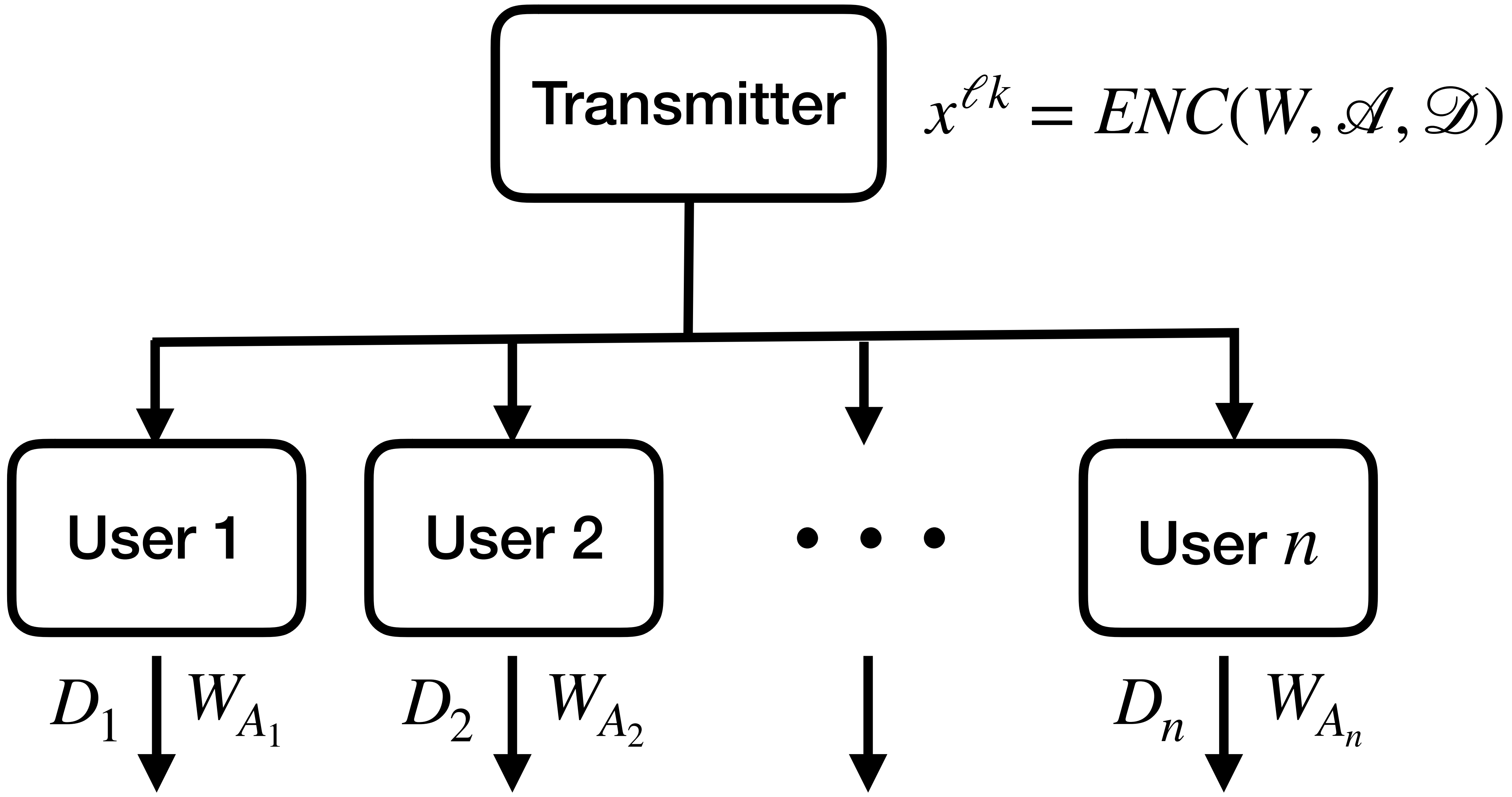
$[m] := \{1,2,\ldots,m\}$;

$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Fixed desired message set: $D_i \subseteq [m] \backslash A_i$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, \mathscr{D} = \{D_1, \ldots, D_n\}$



Index coding

Notation:

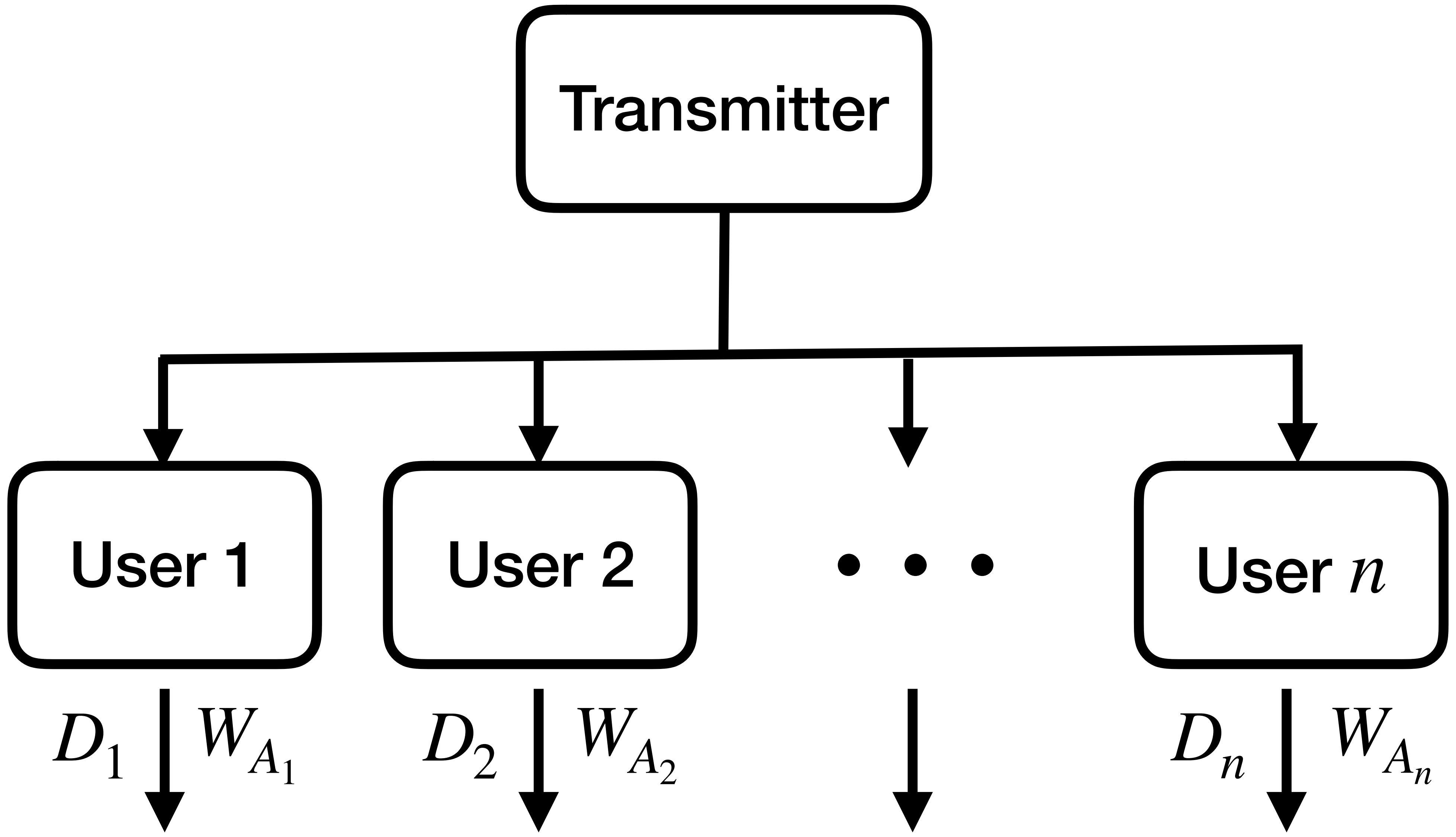
$[m] := \{1,2,\ldots,m\}$;

$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Fixed desired message set: $D_i \subseteq [m] \backslash A_i$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, \mathscr{D} = \{D_1, \ldots, D_n\}$

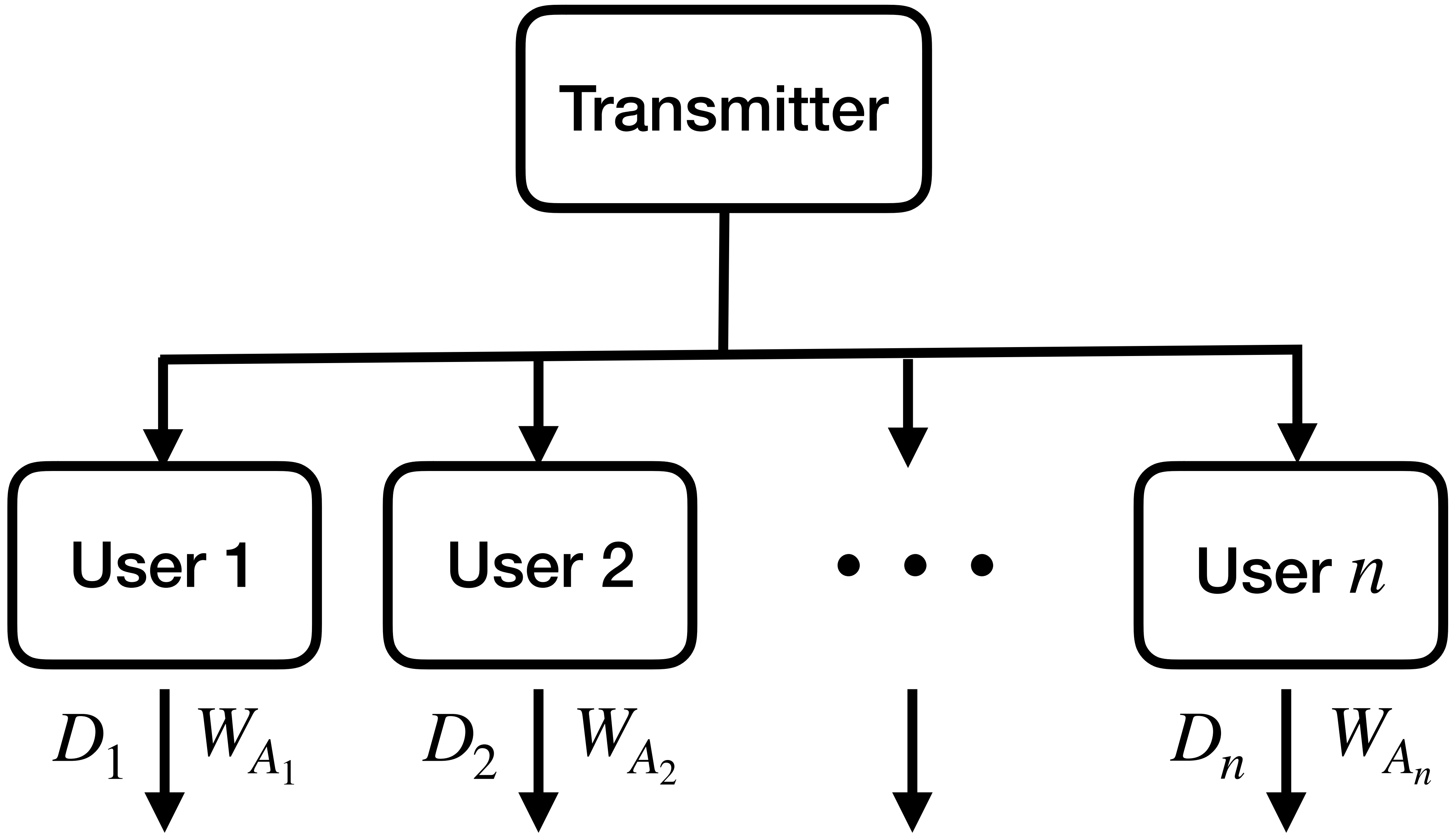


$x^{\ell k} = ENC(W, \mathscr{A}, \mathscr{D})$

Index coding

Notation:
$[m] := \{1,2,\ldots,m\}$;
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;
Side information set: $A_i \subset [m]$;
Fixed desired message set: $D_i \subseteq [m] \backslash A_i$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, \mathscr{D} = \{D_1, \ldots, D_n\}$

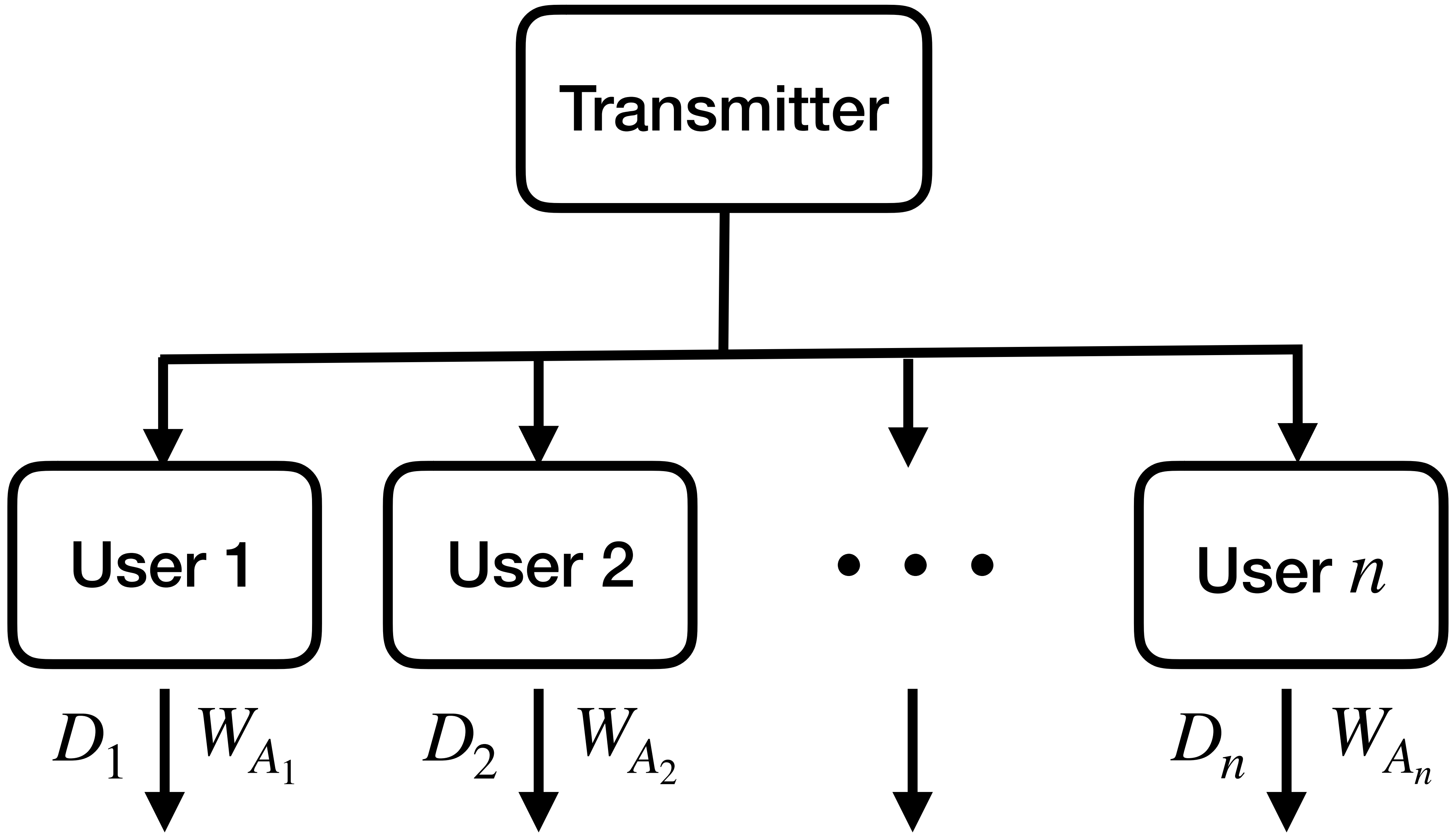


$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k})$

Index coding

Notation:
$[m] := \{1,2,\ldots,m\}$;
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;
Side information set: $A_i \subset [m]$;
Fixed desired message set: $D_i \subseteq [m]\backslash A_i$.

$W = \{w_1, \ldots, w_m\}, \mathcal{A} = \{A_1, \ldots, A_n\}, \mathcal{D} = \{D_1, \ldots, D_n\}$



$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k})$ $\quad$ $x^{\ell k} = ENC(W, \mathcal{A}, \mathcal{D})$

Index coding

Notation:

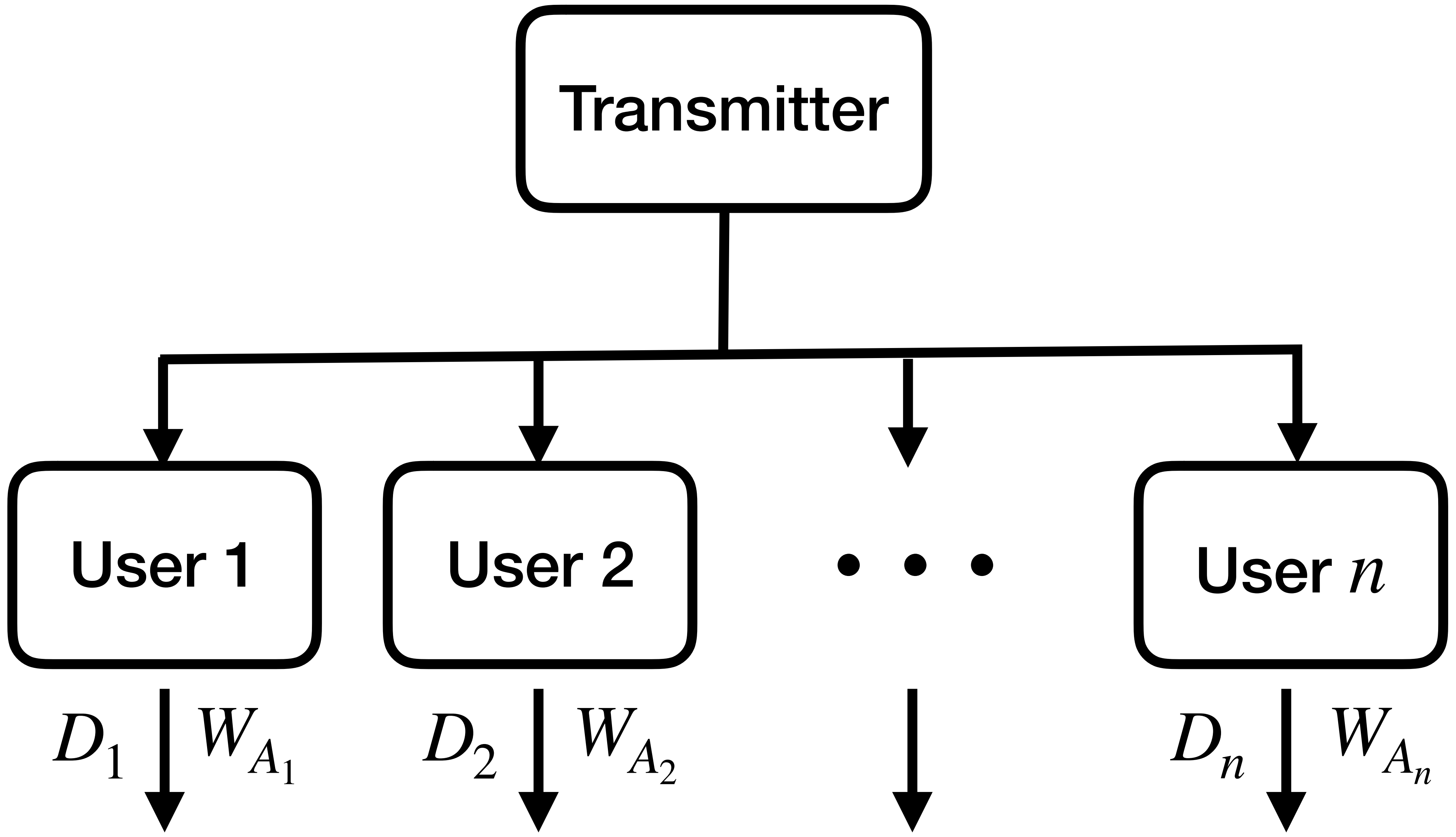
$[m] := \{1,2,\ldots,m\}$;

$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Fixed desired message set: $D_i \subseteq [m] \backslash A_i$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, \mathscr{D} = \{D_1, \ldots, D_n\}$



$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k})$ $\hat{w}_{D_2} = DEC_2(W_{A_2}, x^{\ell k})$

Index coding

Notation:

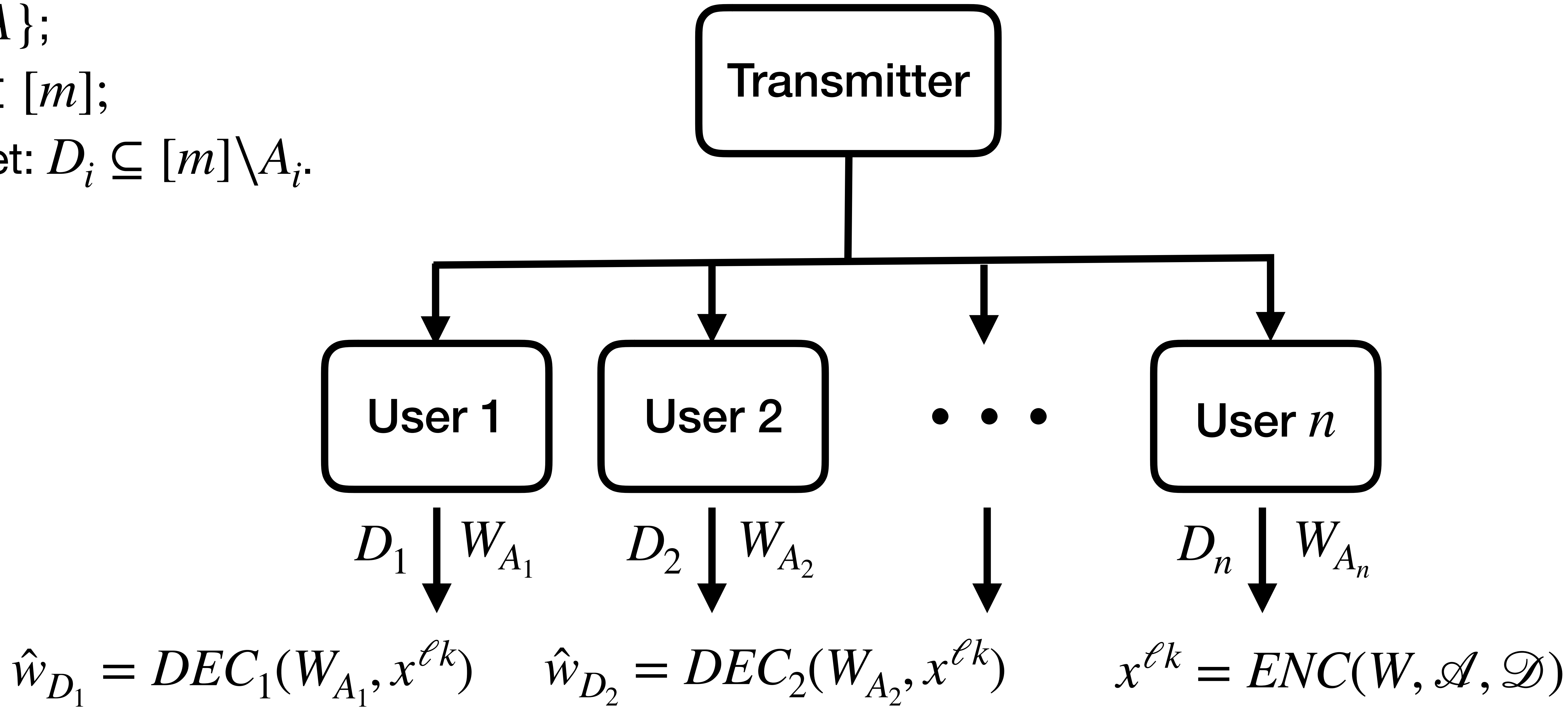
$[m] := \{1,2,\ldots,m\}$;

$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Fixed desired message set: $D_i \subseteq [m] \backslash A_i$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, \mathscr{D} = \{D_1, \ldots, D_n\}$



Index coding

Notation:

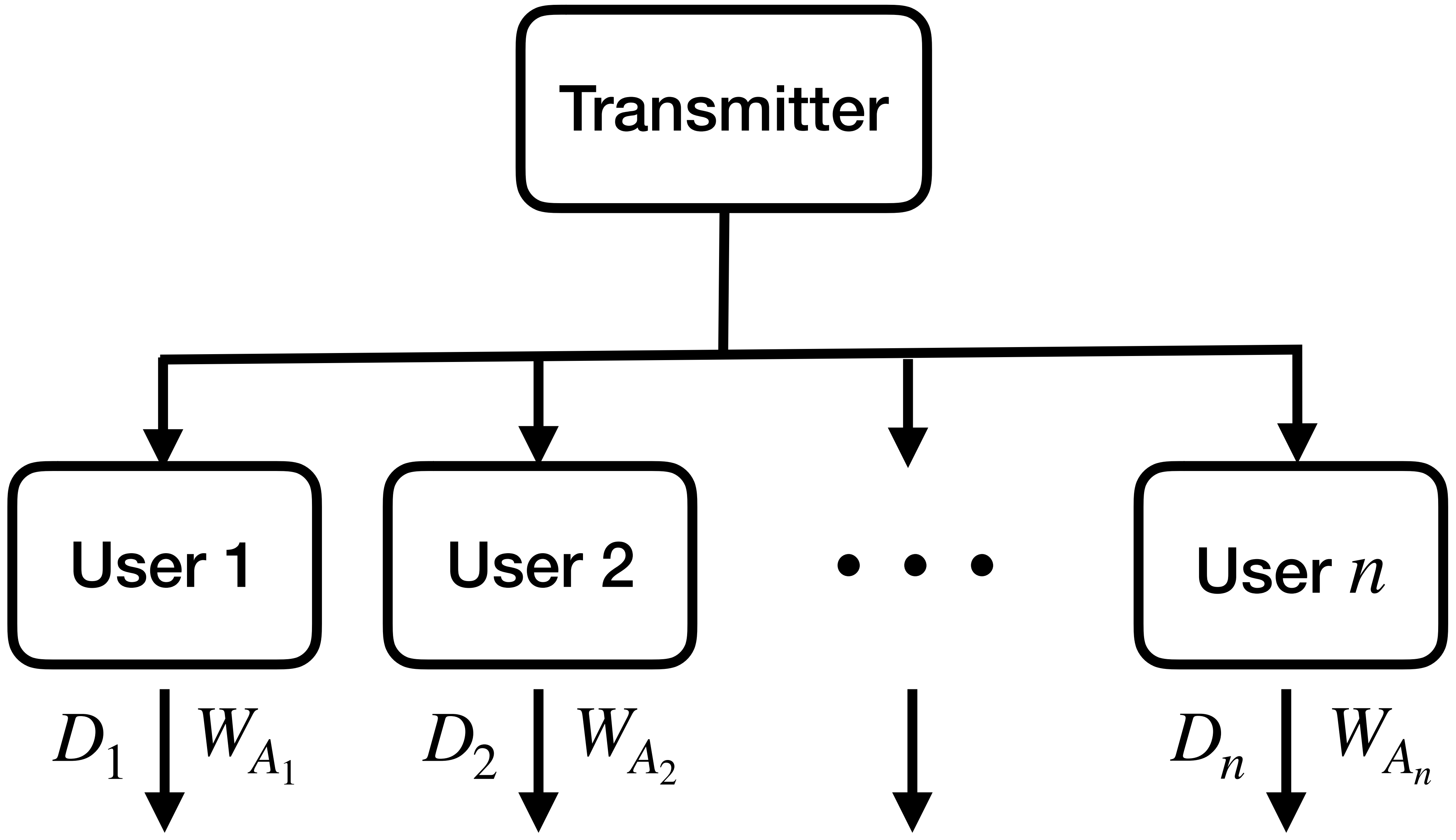
$[m] := \{1,2,\ldots,m\}$;

$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Fixed desired message set: $D_i \subseteq [m] \backslash A_i$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, \mathscr{D} = \{D_1, \ldots, D_n\}$

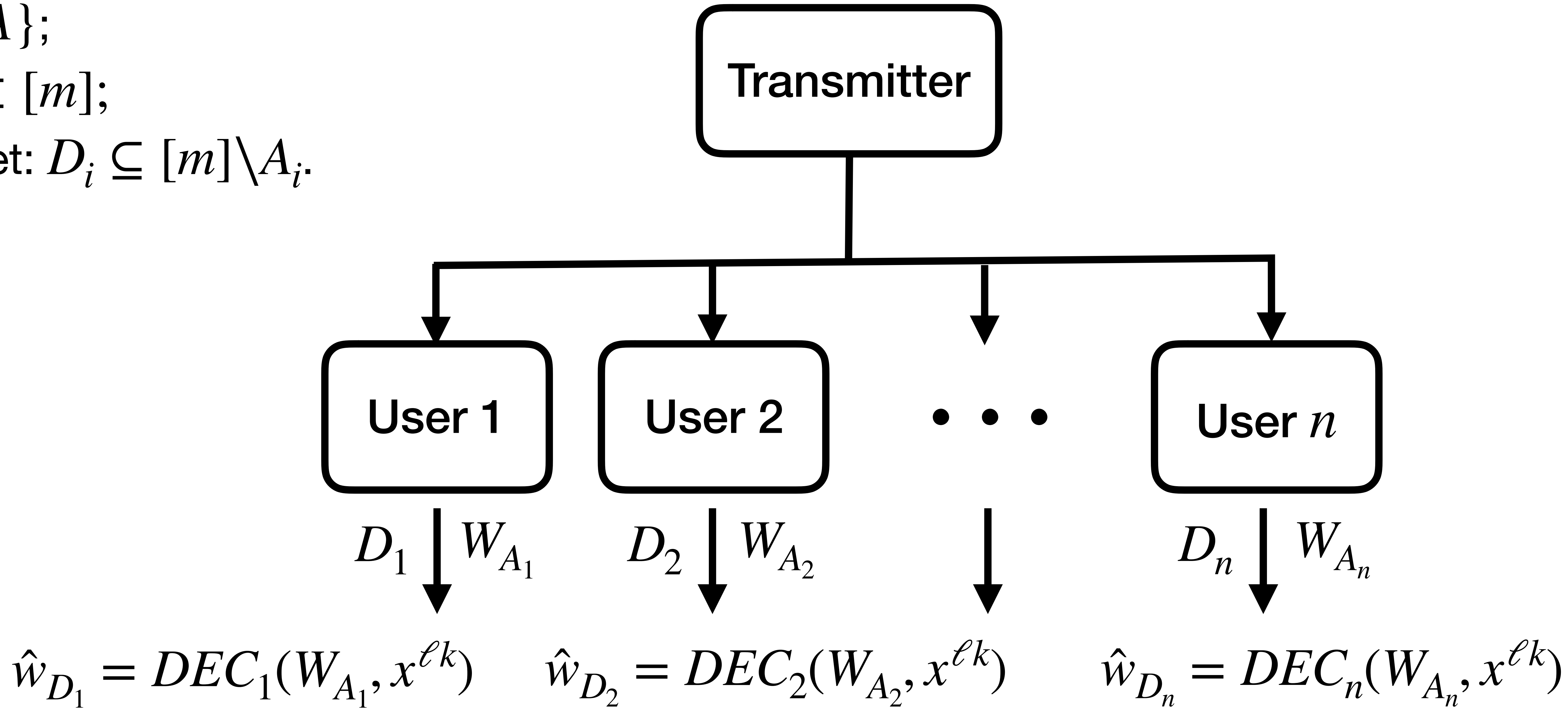


$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k})$ $\hat{w}_{D_2} = DEC_2(W_{A_2}, x^{\ell k})$ $\hat{w}_{D_n} = DEC_n(W_{A_n}, x^{\ell k})$

Index coding

Notation:
$[m] := \{1,2,\ldots,m\}$;
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;
Side information set: $A_i \subset [m]$;
Fixed desired message set: $D_i \subseteq [m] \backslash A_i$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, \mathscr{D} = \{D_1, \ldots, D_n\}$



Goal: find the minimum number of transmission ℓ^* needed by the transmitter such that all users can decode their desired messages

Pliability in the choice of desired message

- There are scenarios where users do not want a specific message.
- The transmitter can choose the desired message for the users to reduce the number of transmissions, as long as users do not have the messages already.
- Goal: find the one with the shortest codelength among all index coding instances with the same users' side information sets.

Application: advertising network

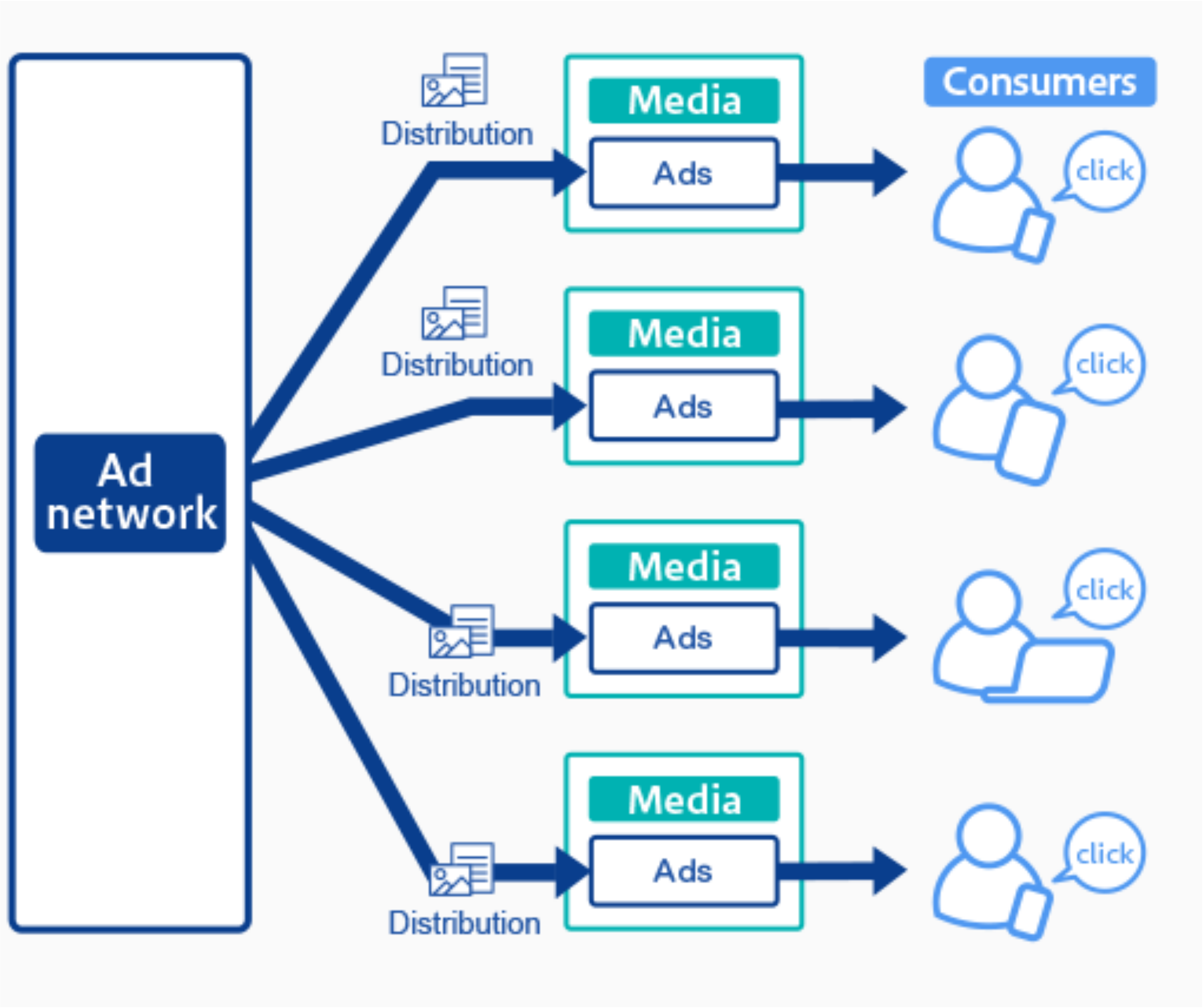


Figure: Advertising network.

- All advertisements are distributed by a single transmitter.
- Consumers may have preference, but do not request a specific ad.
- Distribution/transmission of the ads can leverage this pliability.

Pliable Index CODing (PICOD(t))

Notation:

$[m] := \{1,2,\ldots,m\}$;

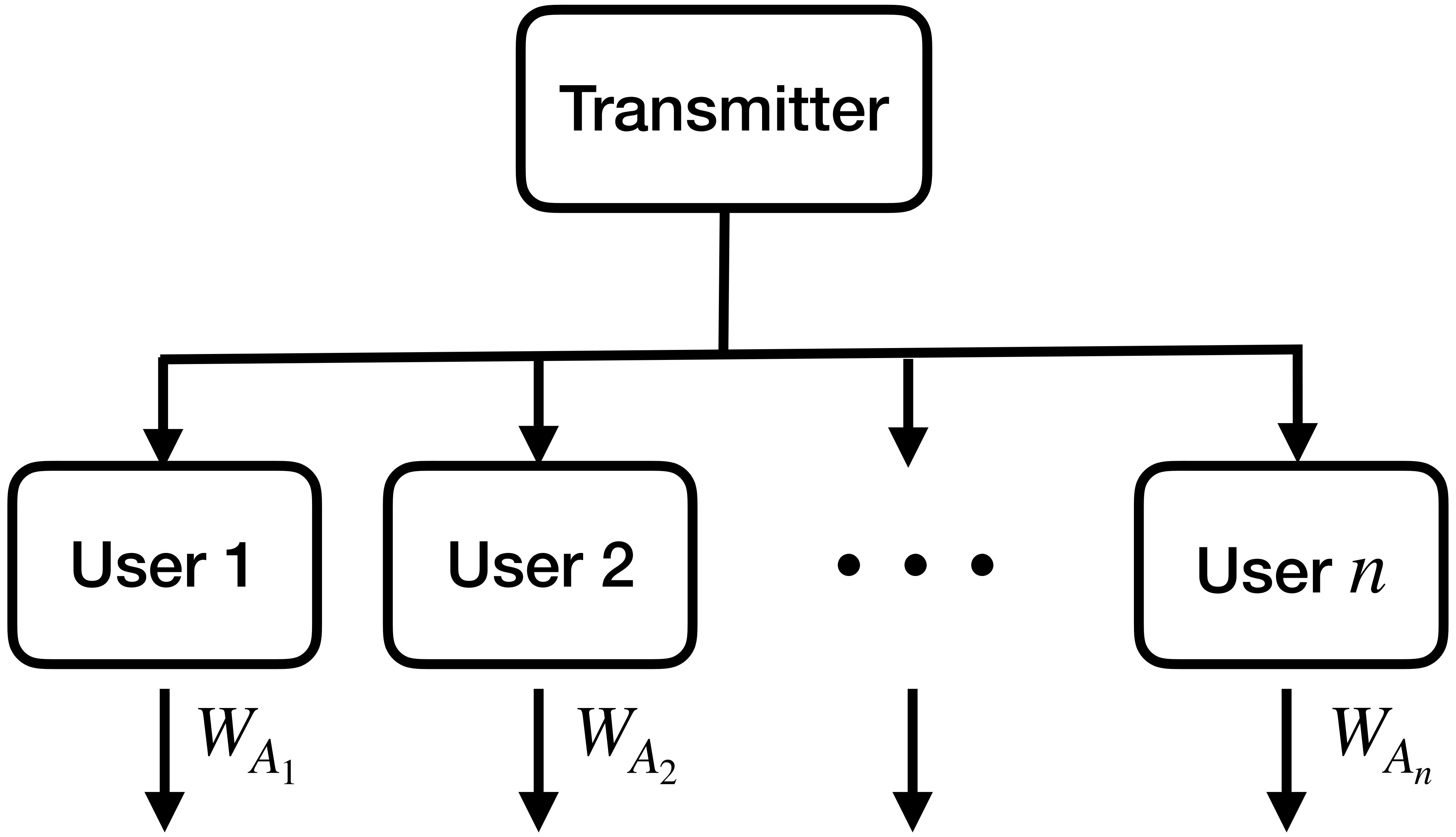
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

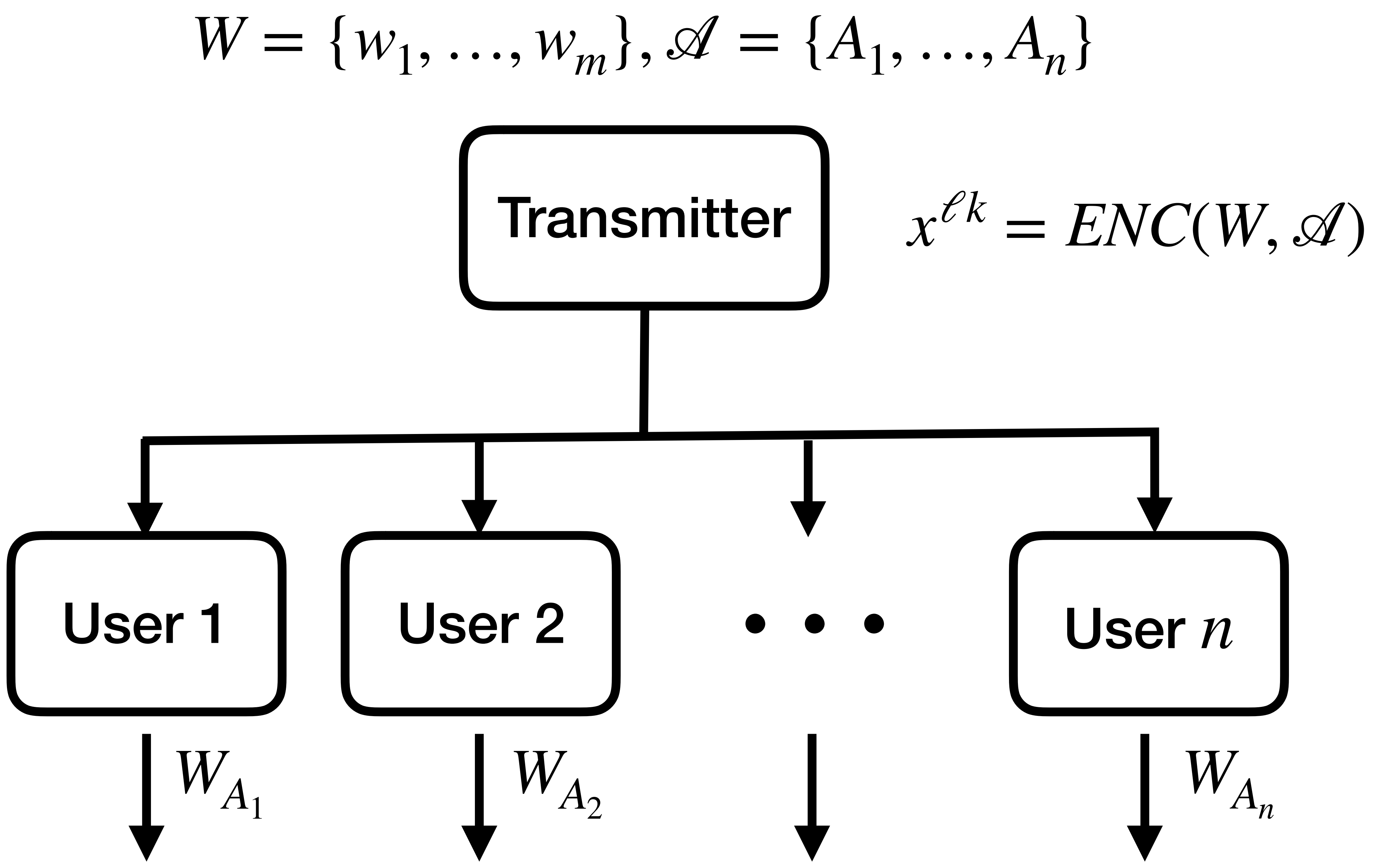
some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}$



Pliable Index CODing (PICOD(t))

Notation:
$[m] := \{1,2,\ldots,m\}$;
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;
Side information set: $A_i \subset [m]$;
Pliable desired message set:
some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.



Pliable Index CODing (PICOD(t))

Notation:

$[m] := \{1,2,\ldots,m\}$;

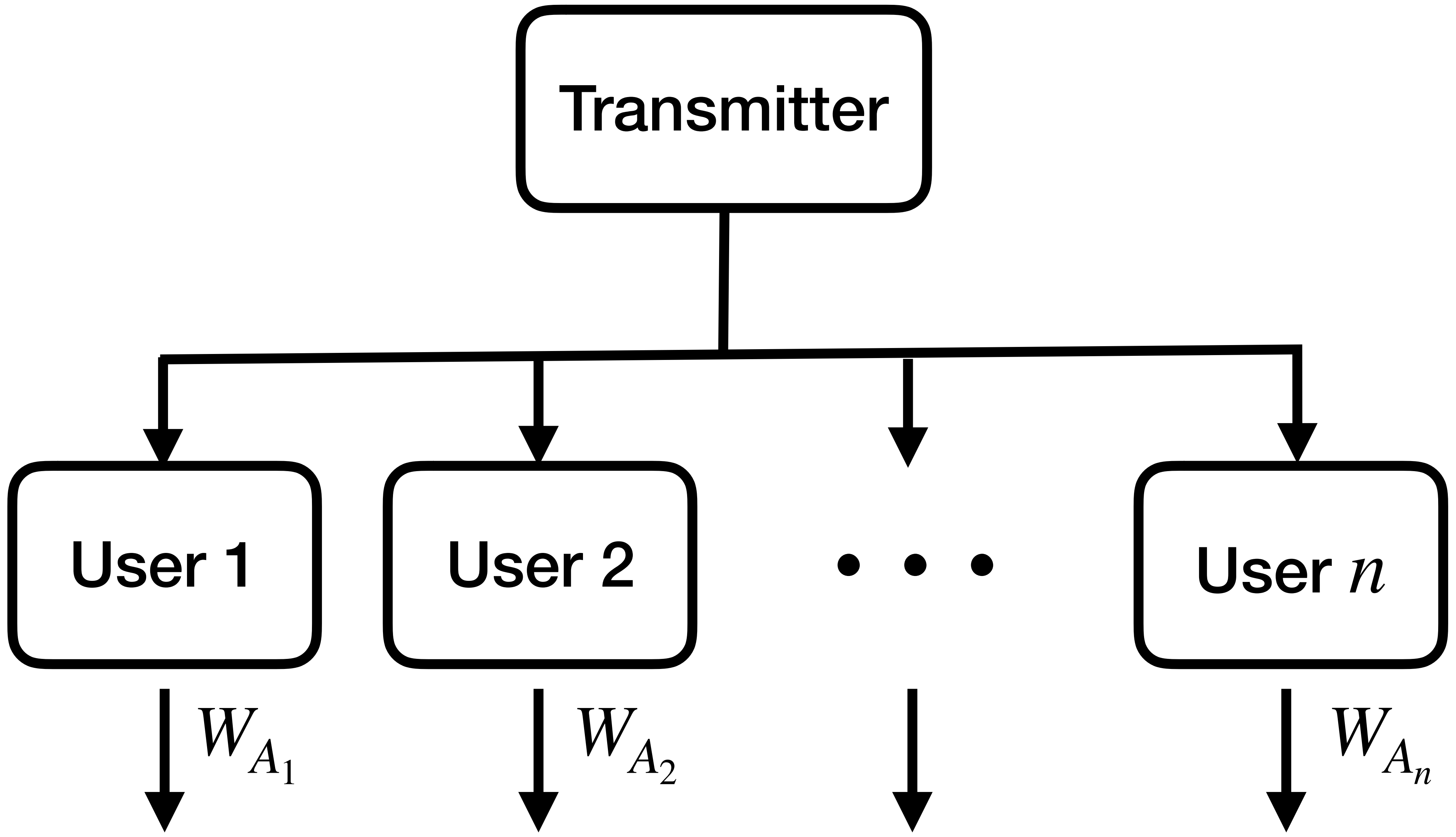
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m]\backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}$



$x^{\ell k} = ENC(W, \mathscr{A})$

Pliable Index CODing (PICOD(t))

Notation:

$[m] := \{1,2,\ldots,m\}$;

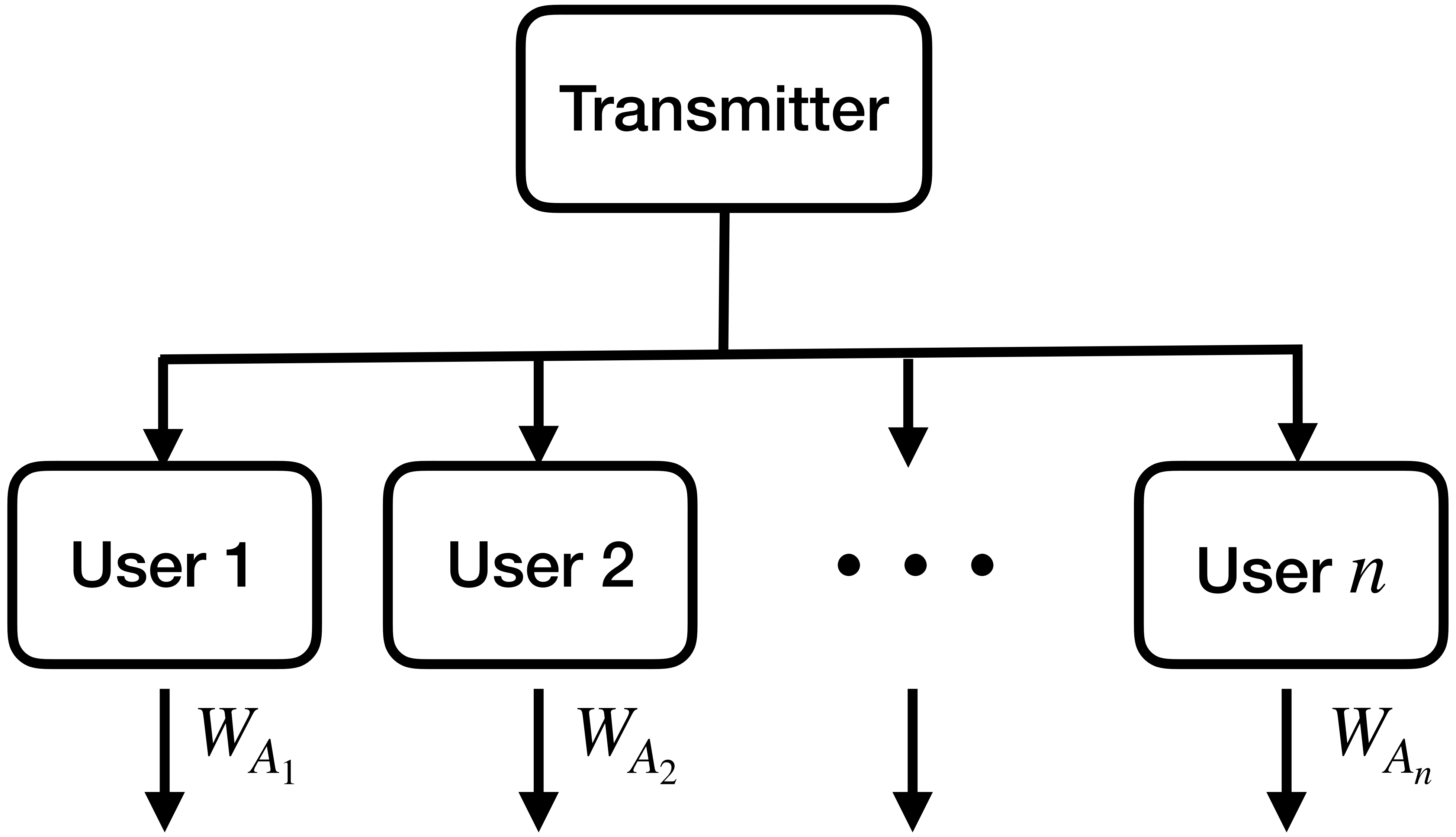
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}$



$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k})$

Pliable Index CODing (PICOD(t))

Notation:

$[m] := \{1,2,\ldots,m\}$;

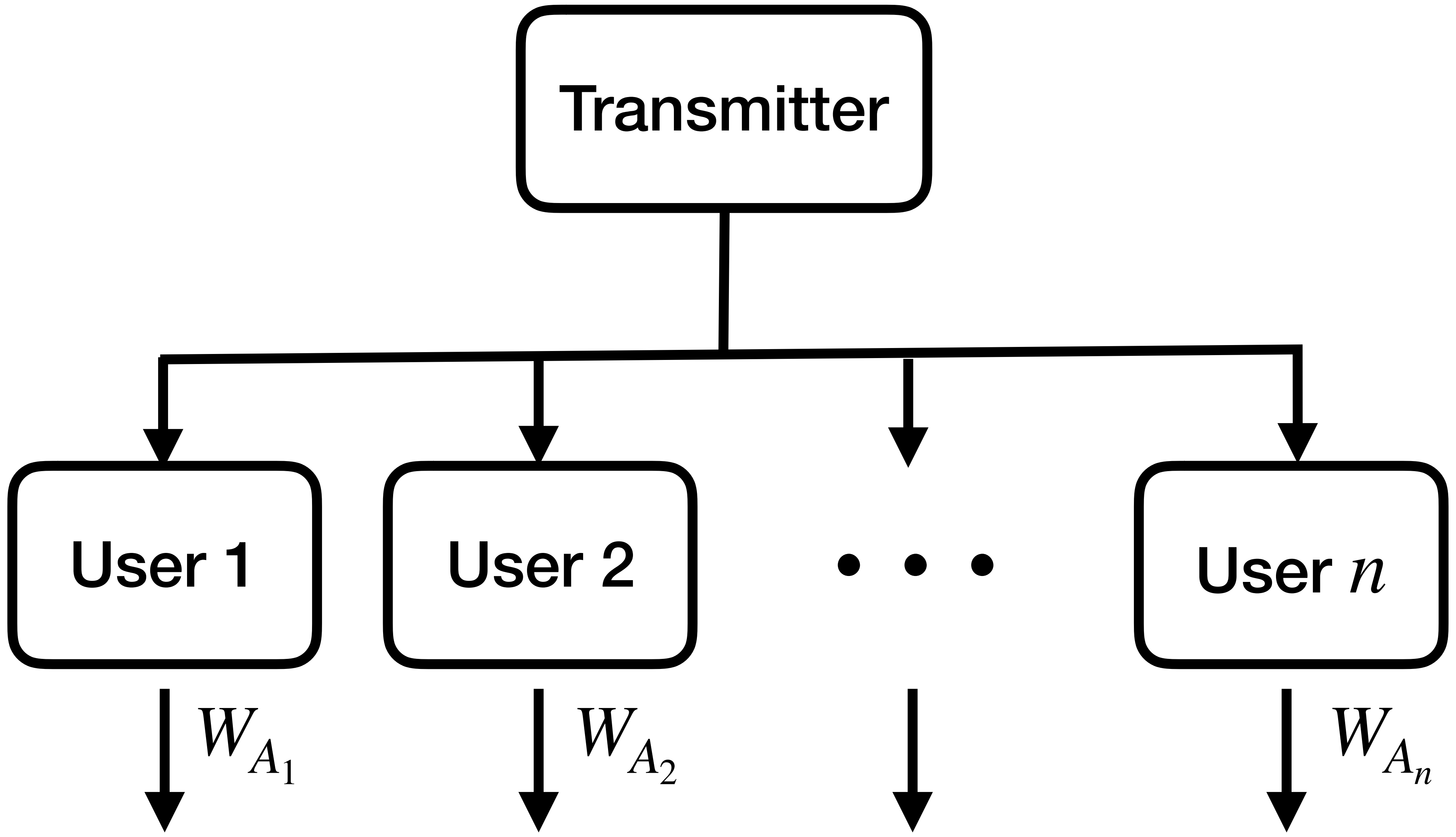
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m]\backslash A_i$ s.t. $|D_i| = t$.

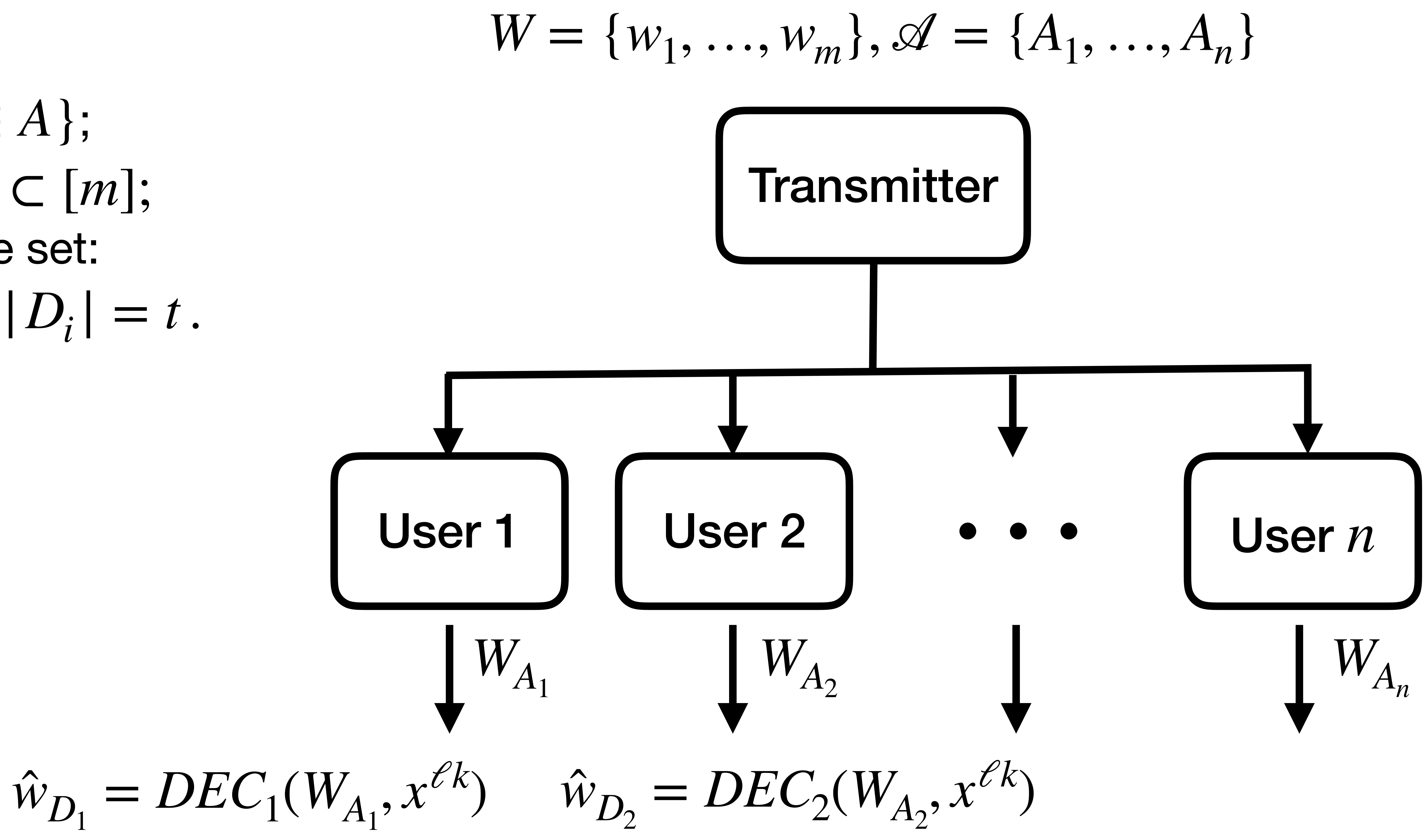
$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}$



$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k})$ $x^{\ell k} = ENC(W, \mathscr{A})$

Pliable Index CODing (PICOD(t))

Notation:
$[m] := \{1,2,\ldots,m\}$;
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;
Side information set: $A_i \subset [m]$;
Pliable desired message set:
some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.



Pliable Index CODing (PICOD(t))

Notation:

$[m] := \{1,2,\ldots,m\}$;

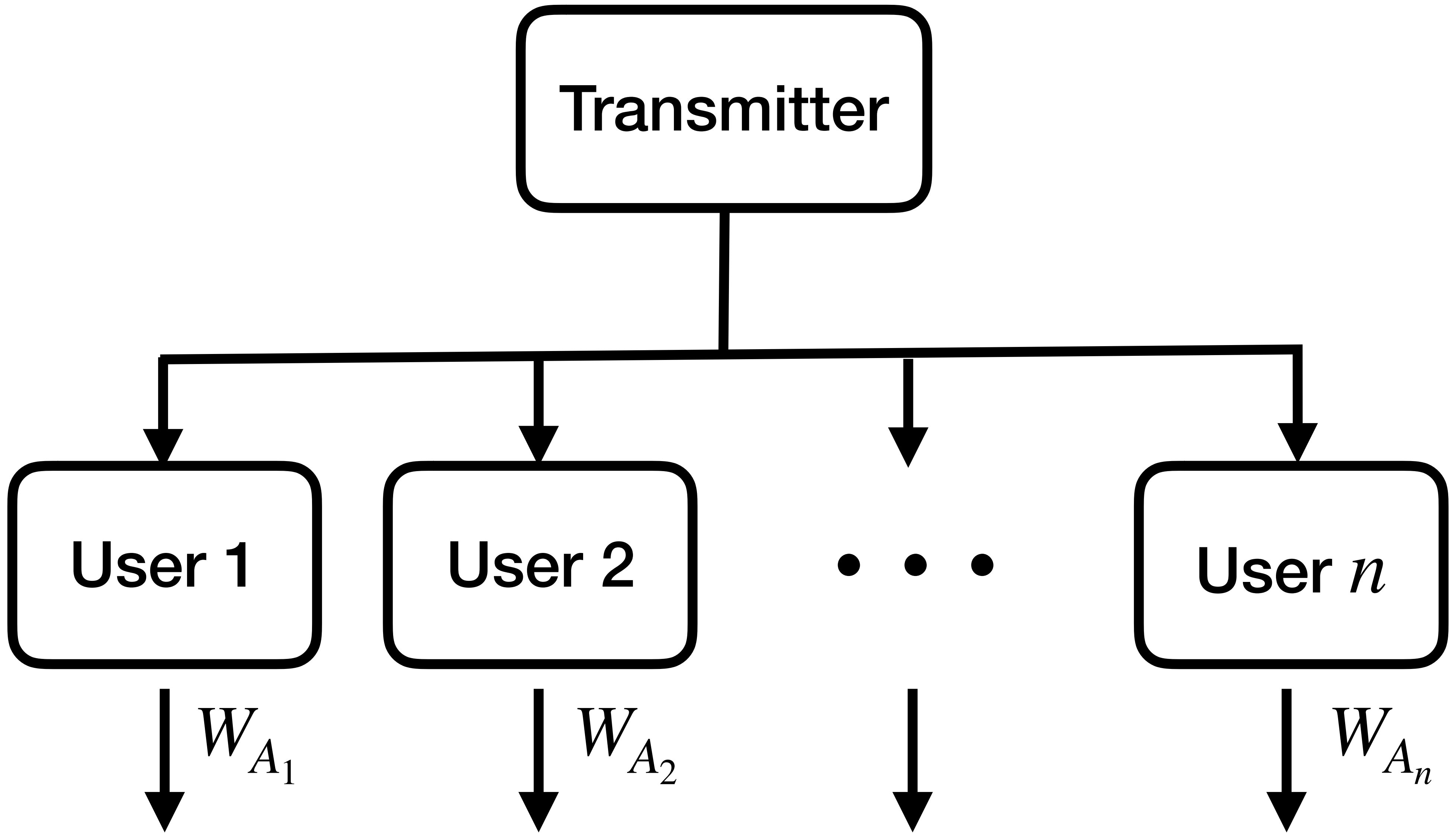
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}$



$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k})$ $\hat{w}_{D_2} = DEC_2(W_{A_2}, x^{\ell k})$ $x^{\ell k} = ENC(W, \mathscr{A})$

Pliable Index CODing (PICOD(t))

Notation:

$[m] := \{1,2,\ldots,m\}$;

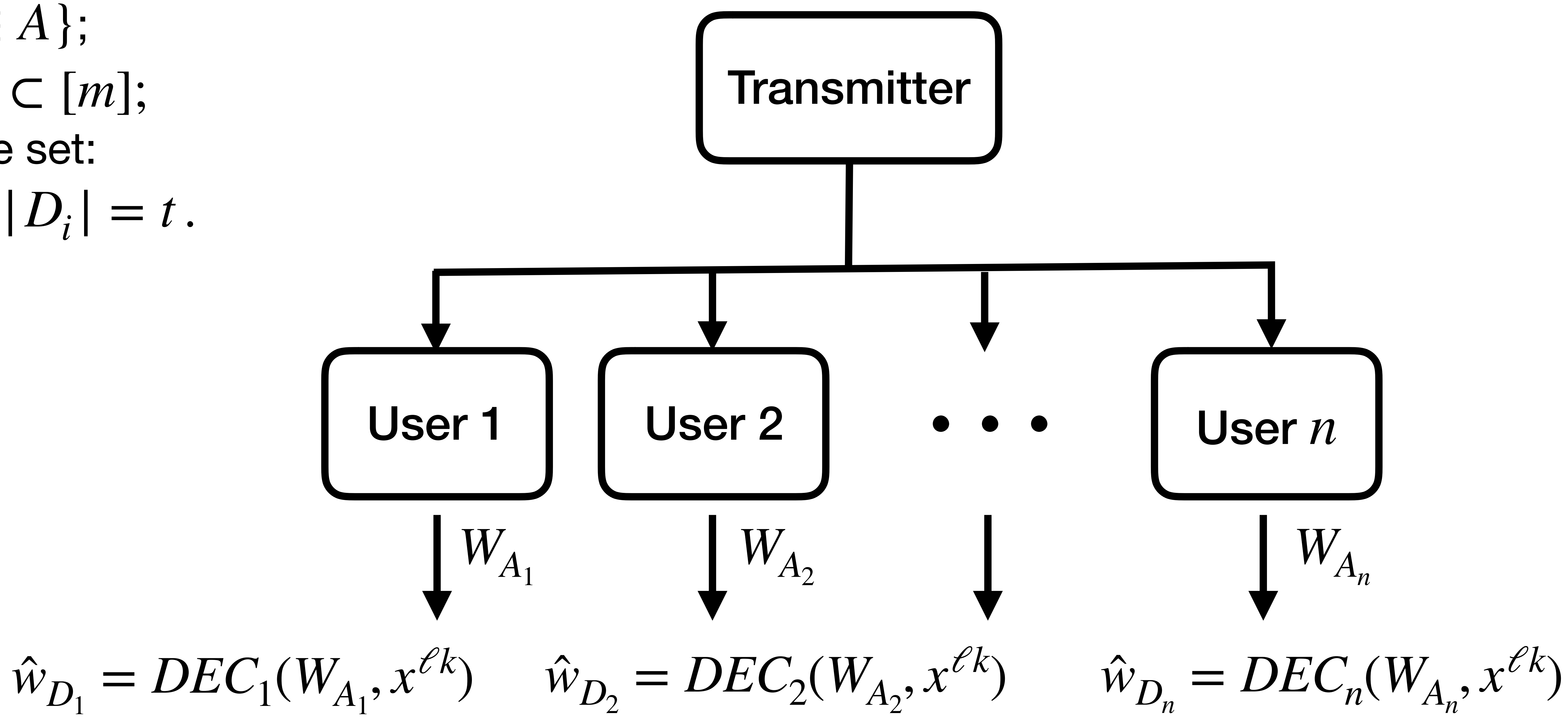
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

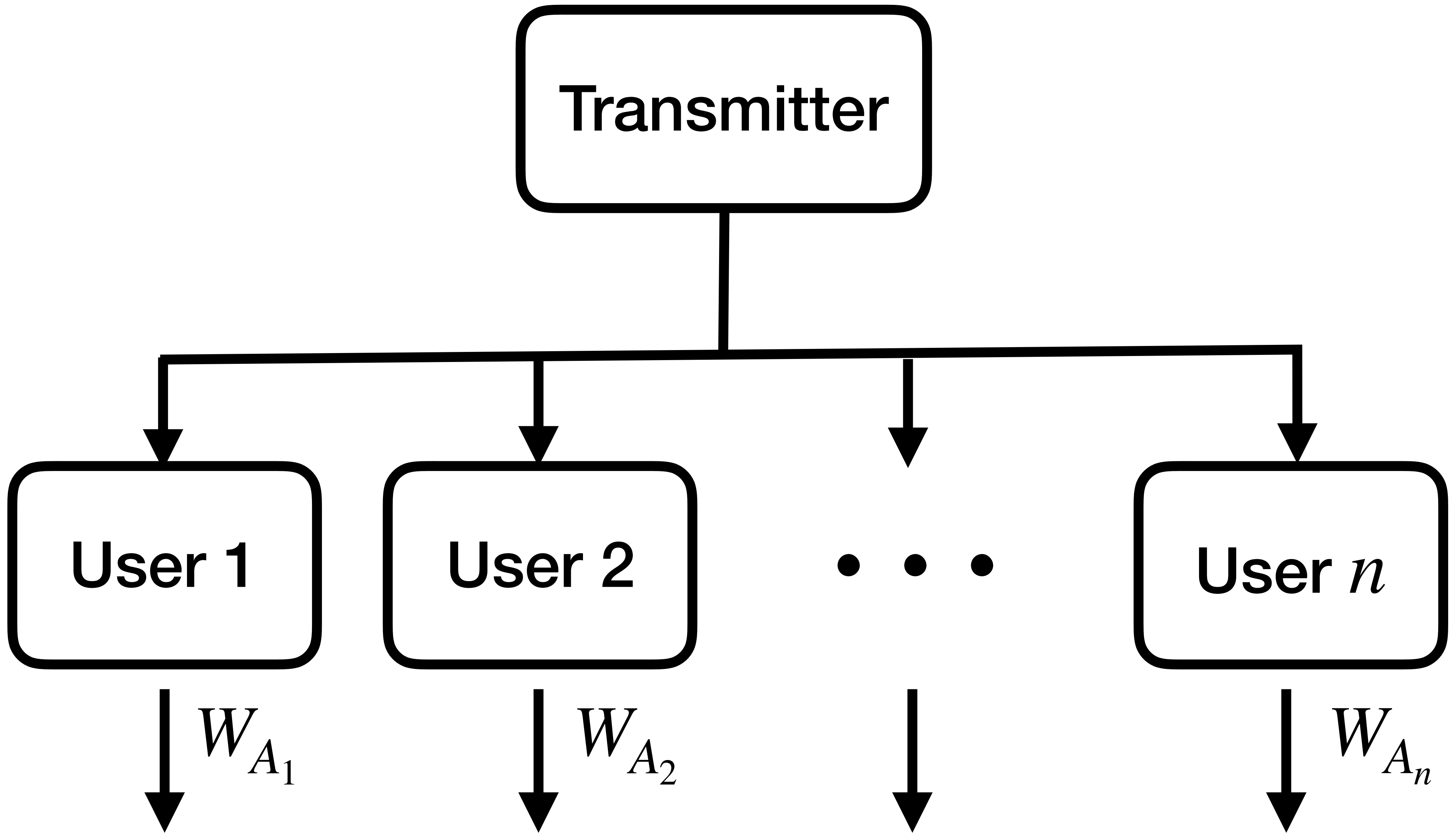
$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}$



Pliable Index CODing (PICOD(t))

Notation:
$[m] := \{1,2,\ldots,m\}$;
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;
Side information set: $A_i \subset [m]$;
Pliable desired message set:
some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathcal{A} = \{A_1, \ldots, A_n\}$



$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k})$ $\hat{w}_{D_2} = DEC_2(W_{A_2}, x^{\ell k})$ $\hat{w}_{D_n} = DEC_n(W_{A_n}, x^{\ell k})$

Goal: find the minimum number of transmission ℓ^* needed by the transmitter such that each user can decode t messages outside its side information set.

Decentralized system

- No centralized controller/distributer/transmitter. All transmissions are done by the users in the system.
- The codewords are generated by the users based on their side information set. Decentralized system is “weaker” compared to centralized system in terms of transmission rate.
- Examples: ad-hoc network, p2p network, distributed storage…

Application of decentralized system

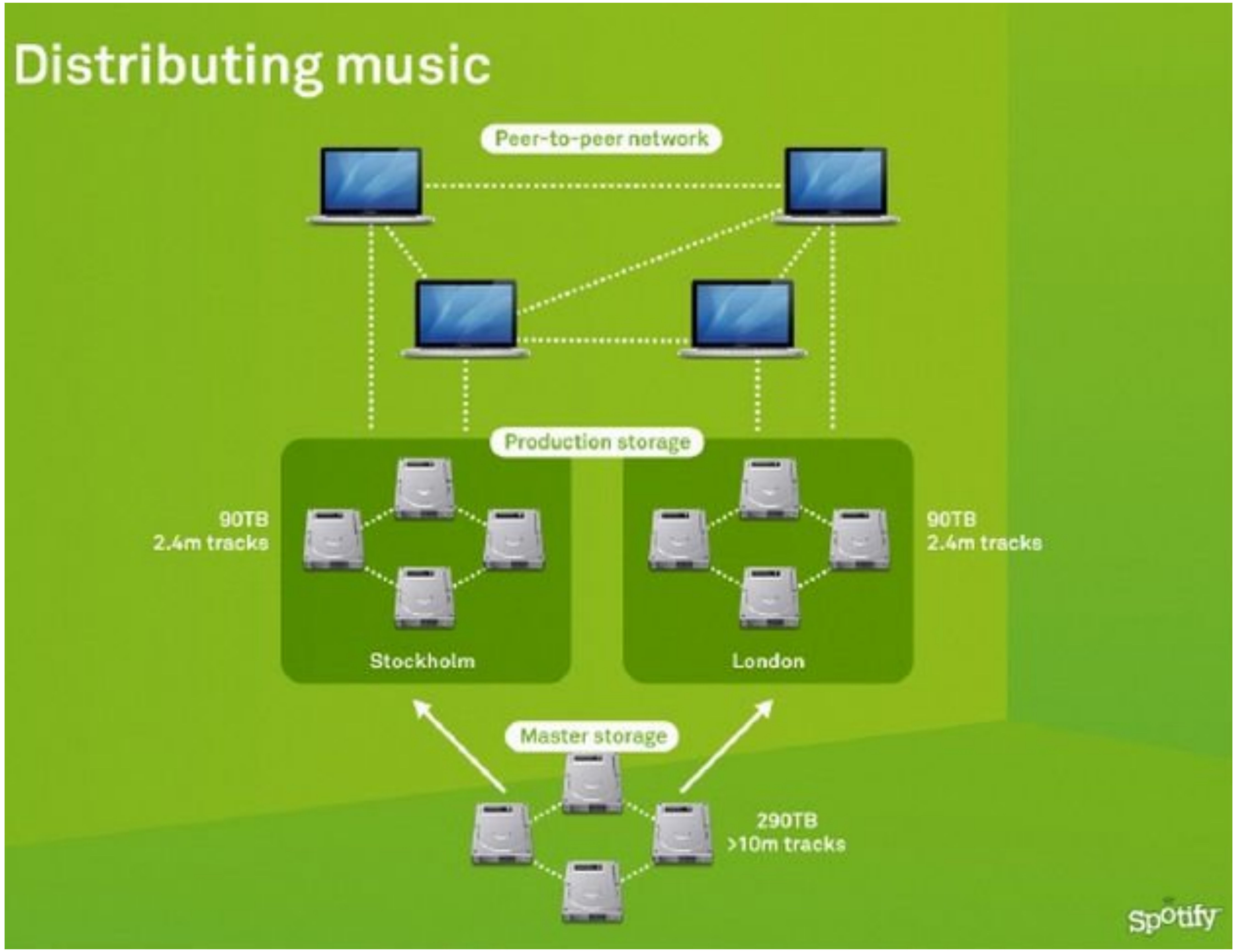
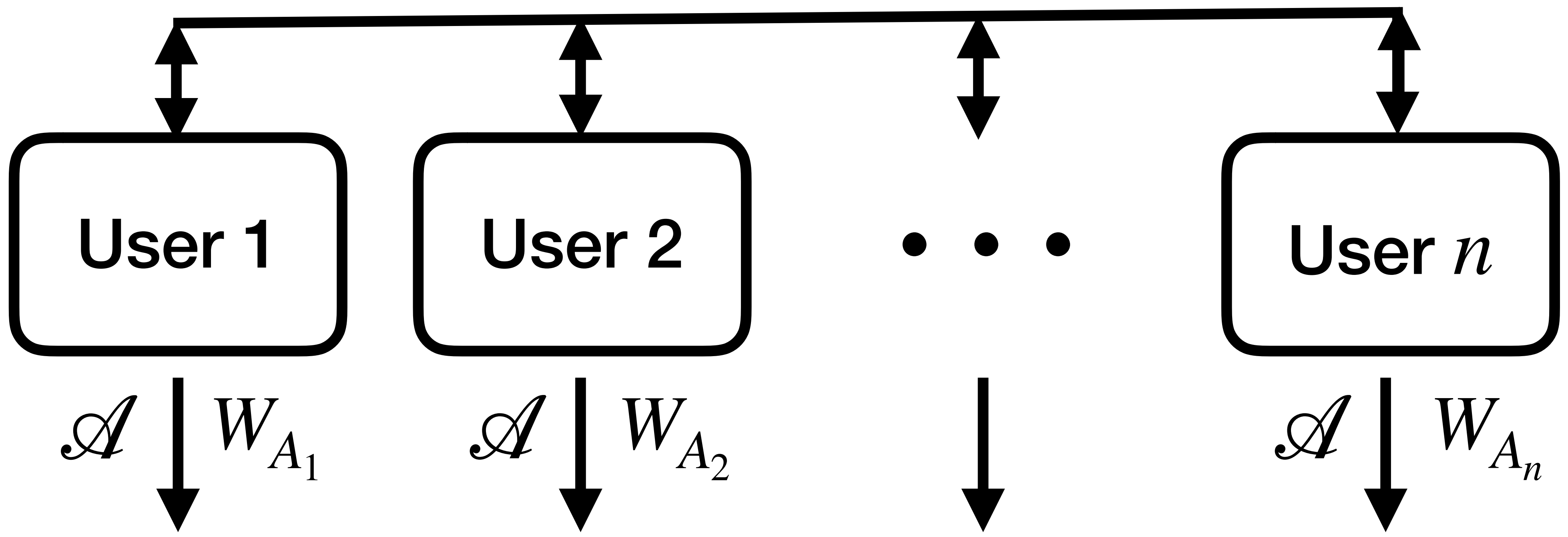


Figure: Distributed music by Spotify

Decentralized PICOD(t)

Notation:
$[m] := \{1,2,\ldots,m\}$;
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;
Side information set: $A_i \subset [m]$;
Pliable desired message set:
some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, x^{\ell k} = \{x^{\ell_1 k}, \ldots, x^{\ell_n k}\}$



Decentralized PICOD(t)

Notation:

$[m] := \{1,2,\ldots,m\}$;

$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

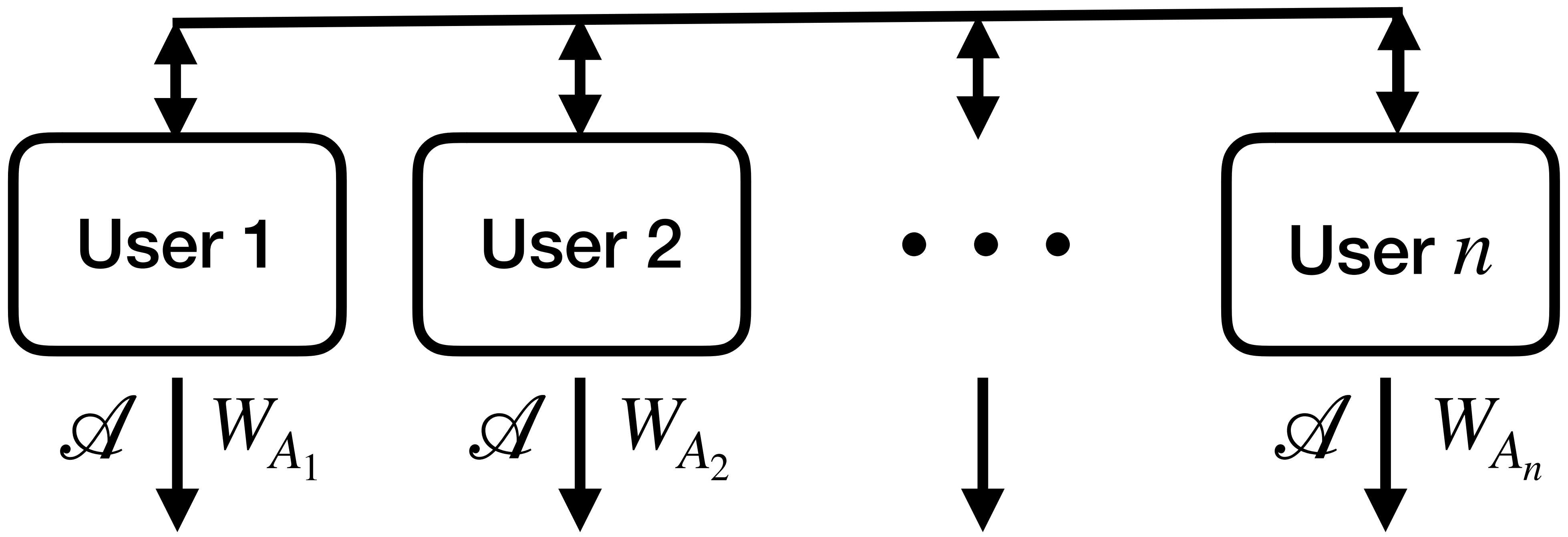
Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, x^{\ell k} = \{x^{\ell_1 k}, \ldots, x^{\ell_n k}\}$$

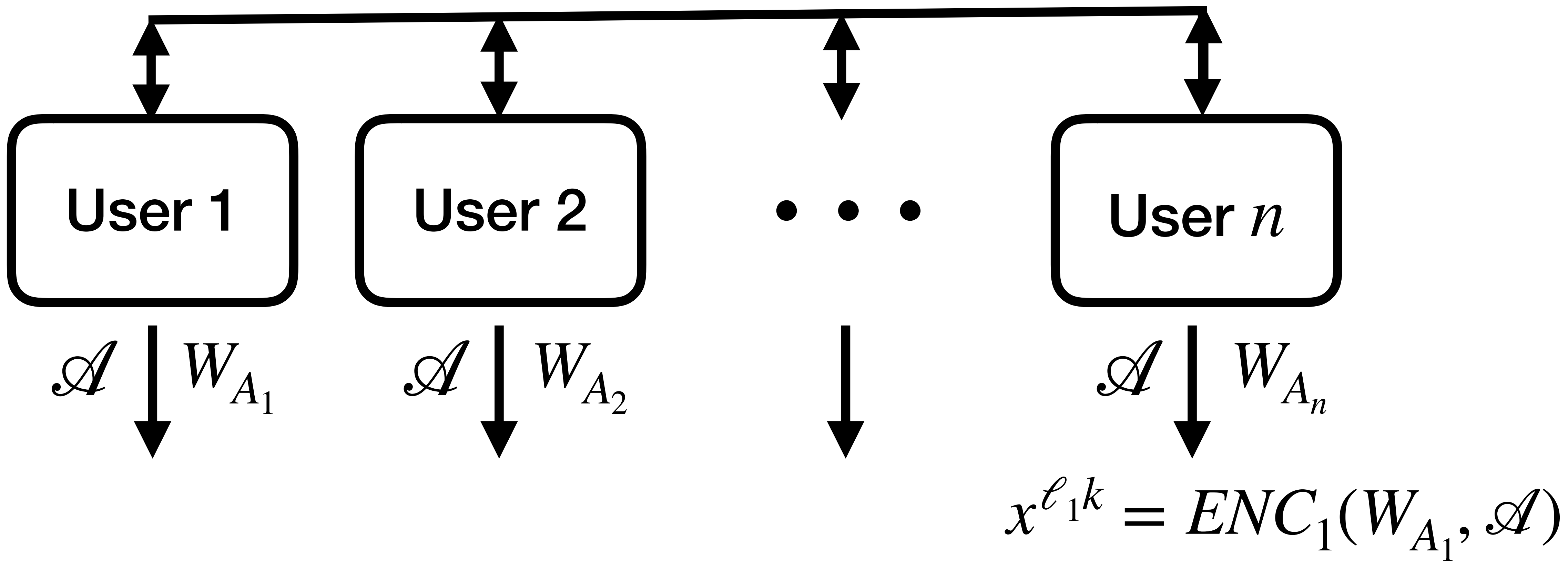
$$x^{\ell_1 k} = ENC_1(W_{A_1}, \mathscr{A})$$



Decentralized PICOD(t)

Notation:
$[m] := \{1,2,\ldots,m\}$;
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;
Side information set: $A_i \subset [m]$;
Pliable desired message set:
some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

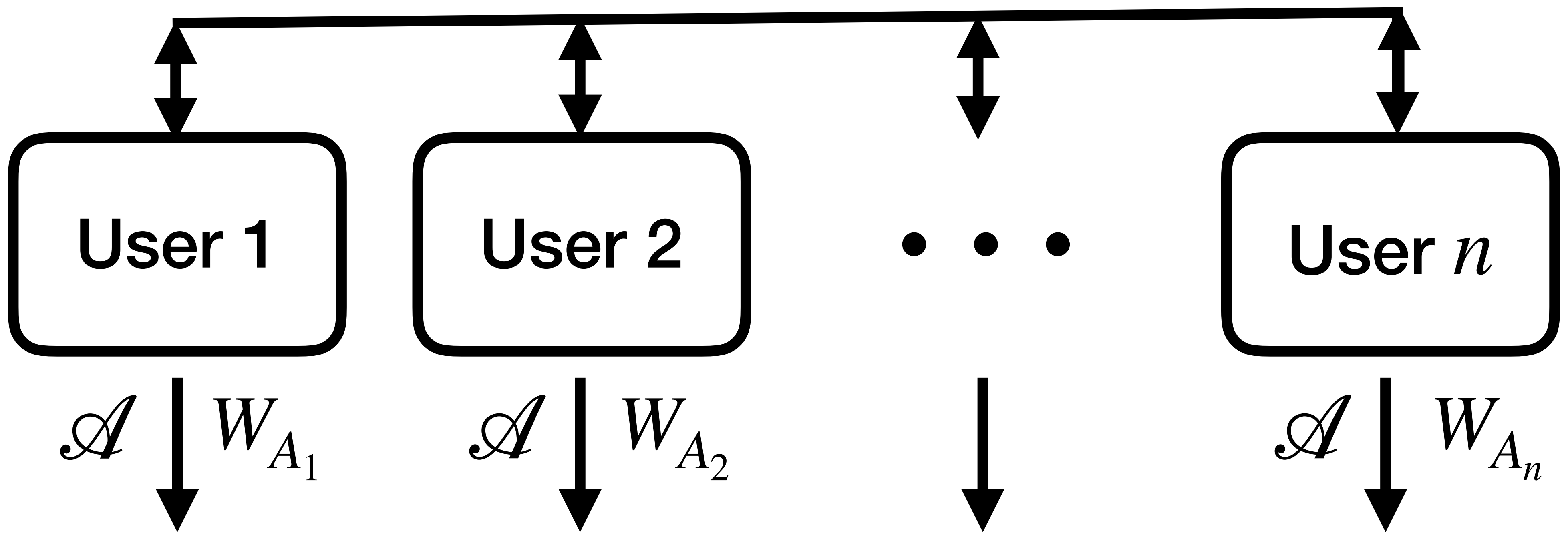
$$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, x^{\ell k} = \{x^{\ell_1 k}, \ldots, x^{\ell_n k}\}$$



Decentralized PICOD(t)

Notation:
$[m] := \{1,2,\ldots,m\}$;
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;
Side information set: $A_i \subset [m]$;
Pliable desired message set:
some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, x^{\ell k} = \{x^{\ell_1 k}, \ldots, x^{\ell_n k}\}$

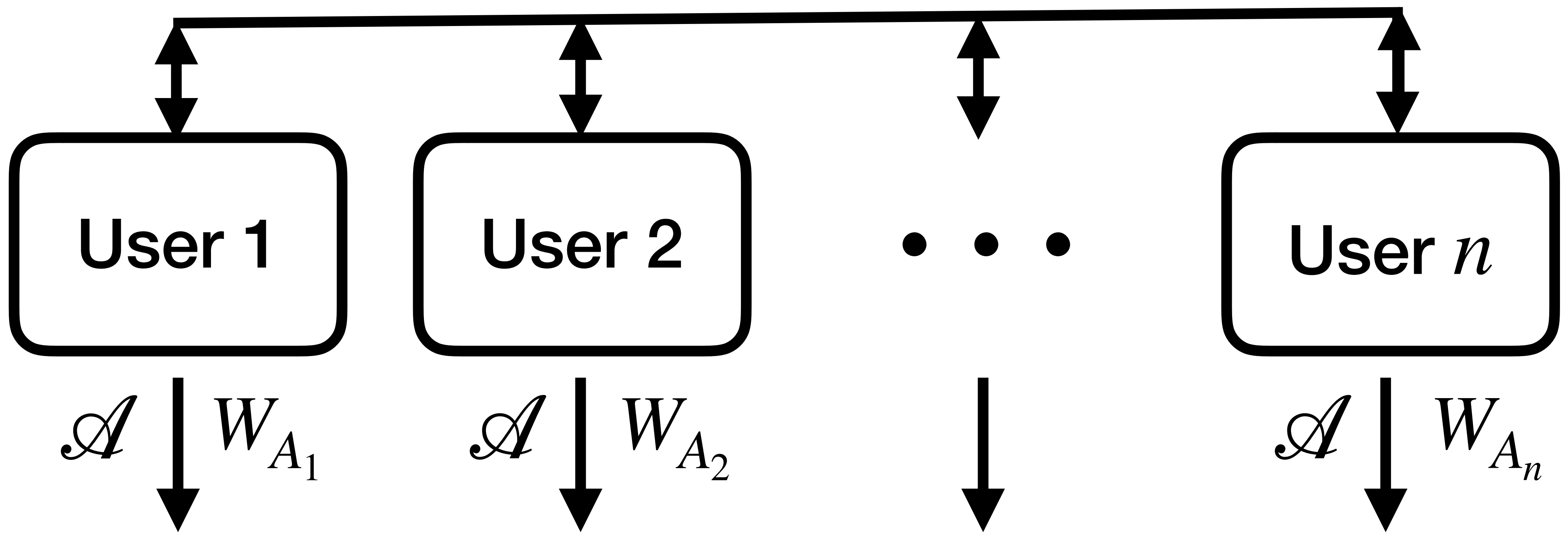


Decentralized PICOD(t)

Notation:
$[m] := \{1,2,\ldots,m\}$;
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;
Side information set: $A_i \subset [m]$;
Pliable desired message set:
some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, x^{\ell k} = \{x^{\ell_1 k}, \ldots, x^{\ell_n k}\}$

$x^{\ell_2 k} = ENC_2(W_{A_2}, \mathscr{A})$



Decentralized PICOD(t)

Notation:

$[m] := \{1,2,\ldots,m\}$;

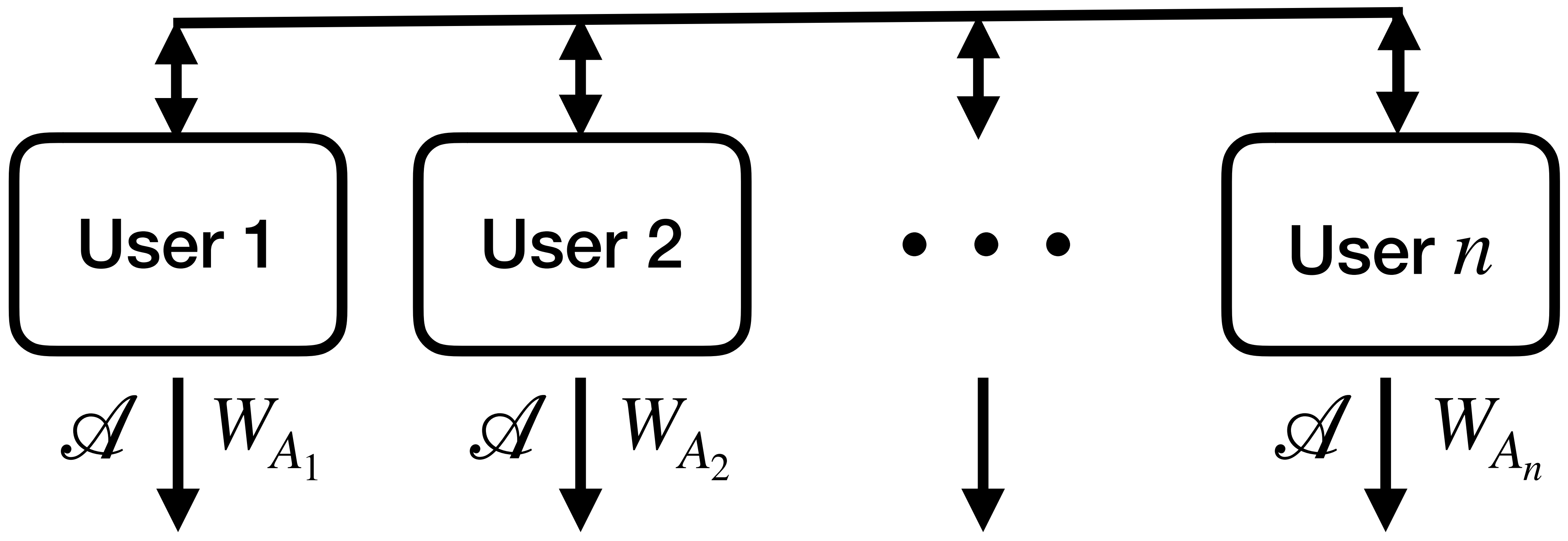
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, x^{\ell k} = \{x^{\ell_1 k}, \ldots, x^{\ell_n k}\}$

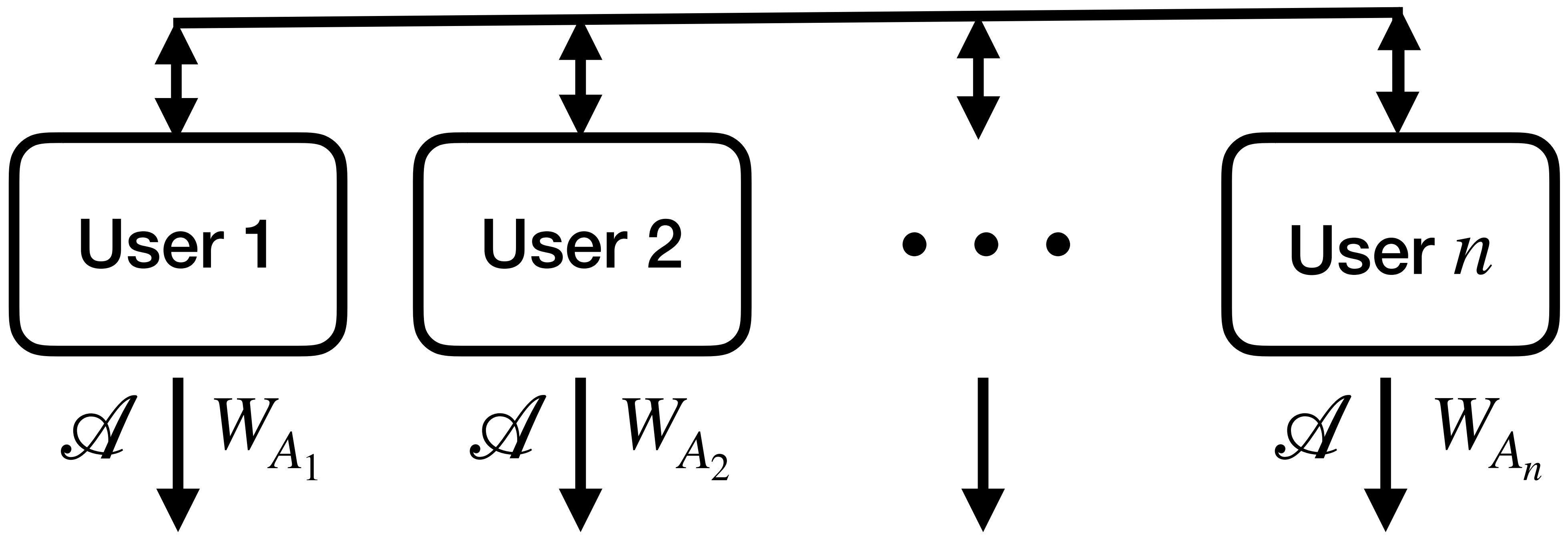


$x^{\ell_2 k} = ENC_2(W_{A_2}, \mathscr{A})$

Decentralized PICOD(t)

Notation:
$[m] := \{1,2,\ldots,m\}$;
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;
Side information set: $A_i \subset [m]$;
Pliable desired message set:
some $D_i \subseteq [m]\backslash A_i$ s.t. $|D_i| = t$.

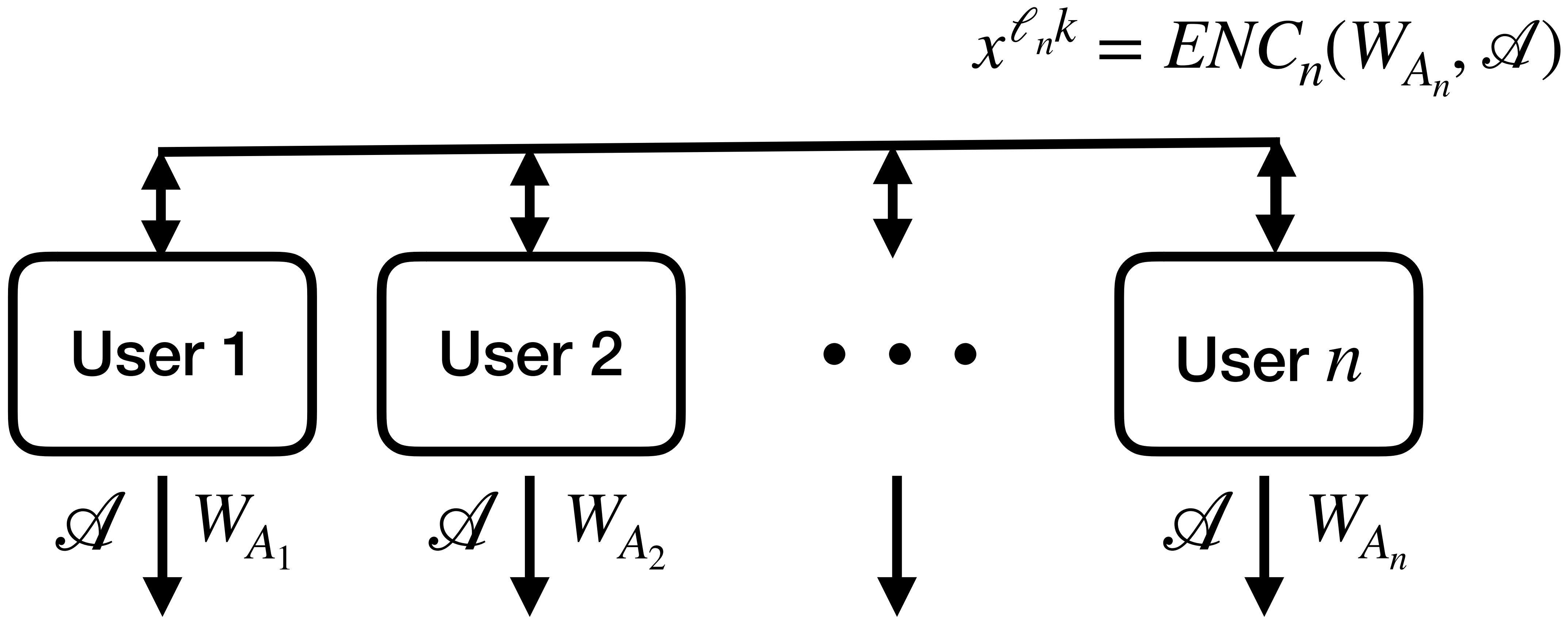
$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, x^{\ell k} = \{x^{\ell_1 k}, \ldots, x^{\ell_n k}\}$



Decentralized PICOD(t)

Notation:
$[m] := \{1,2,\ldots,m\}$;
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;
Side information set: $A_i \subset [m]$;
Pliable desired message set:
some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

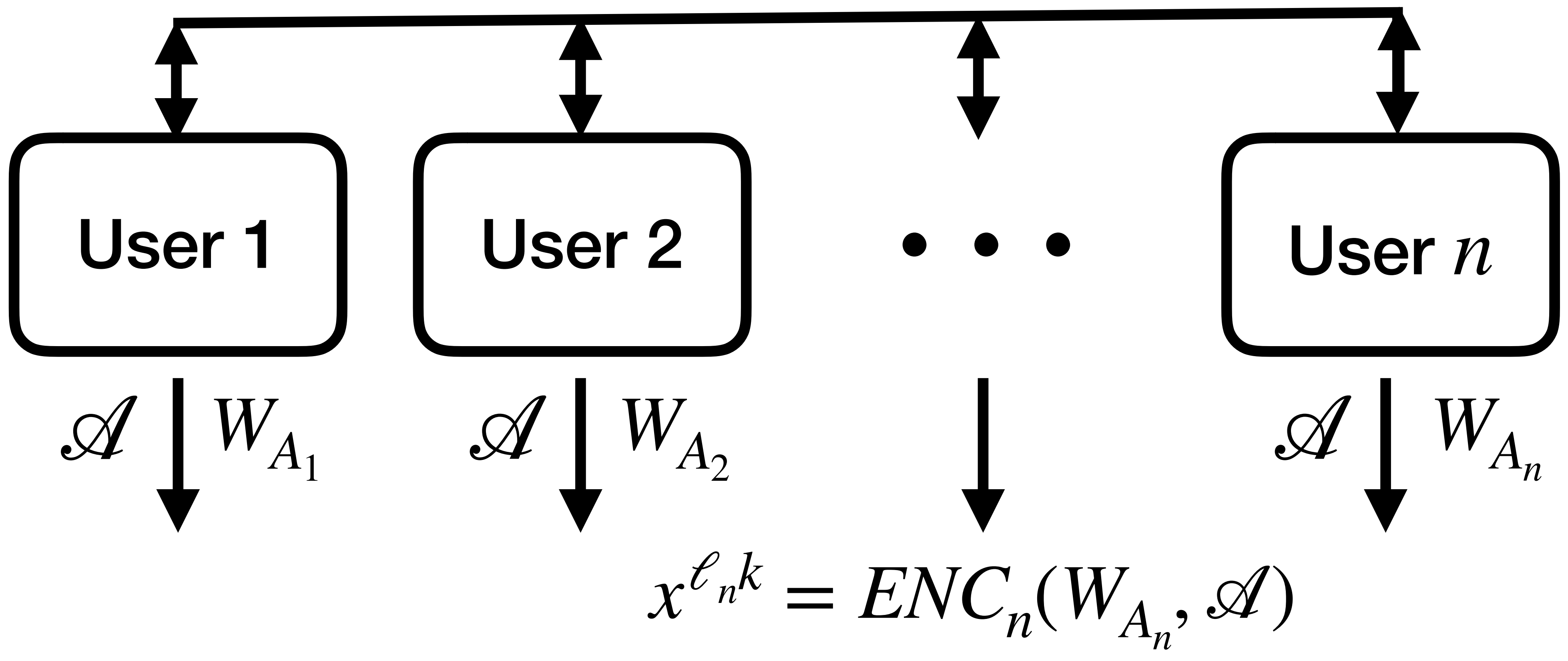
$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, x^{\ell k} = \{x^{\ell_1 k}, \ldots, x^{\ell_n k}\}$



Decentralized PICOD(t)

Notation:
$[m] := \{1,2,\ldots,m\}$;
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;
Side information set: $A_i \subset [m]$;
Pliable desired message set:
some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

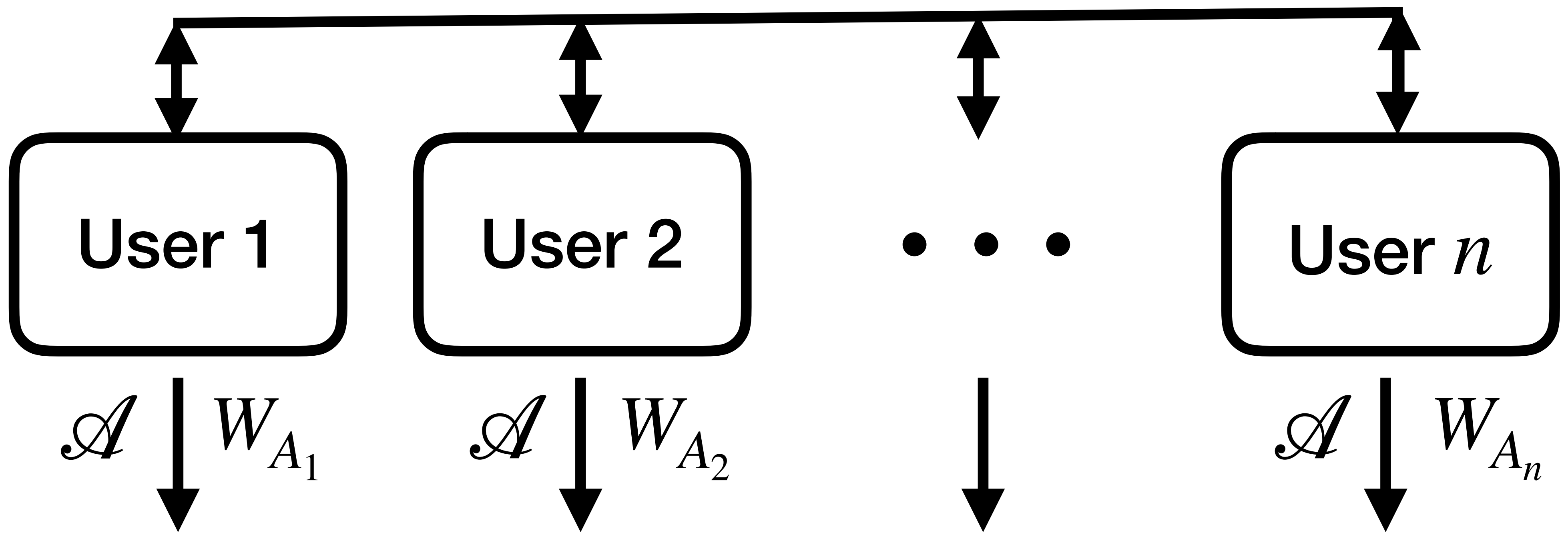
$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, x^{\ell k} = \{x^{\ell_1 k}, \ldots, x^{\ell_n k}\}$



Decentralized PICOD(t)

Notation:
$[m] := \{1,2,\ldots,m\}$;
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;
Side information set: $A_i \subset [m]$;
Pliable desired message set:
some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, x^{\ell k} = \{x^{\ell_1 k}, \ldots, x^{\ell_n k}\}$



Tang Liu, PhD thesis defense, Nov 19th 2019, UIC

Decentralized PICOD(t)

Notation:

$[m] := \{1,2,\ldots,m\}$;

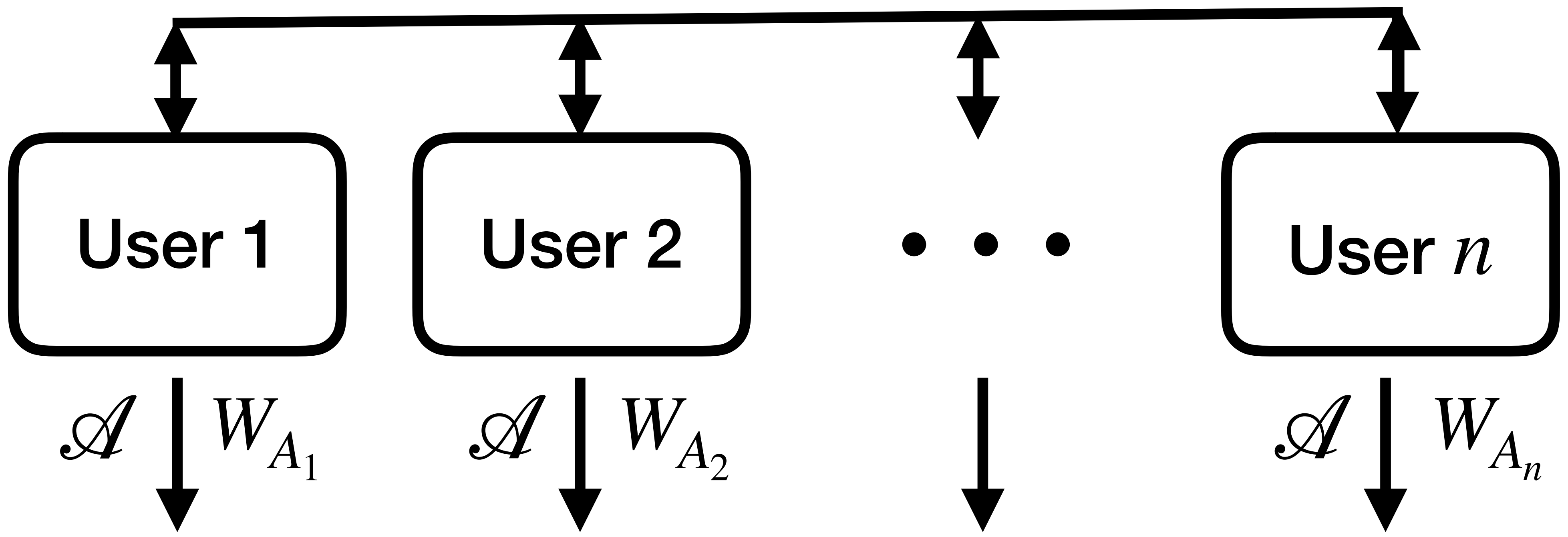
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, x^{\ell k} = \{x^{\ell_1 k}, \ldots, x^{\ell_n k}\}$



$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k})$

Decentralized PICOD(t)

Notation:

$[m] := \{1,2,\ldots,m\}$;

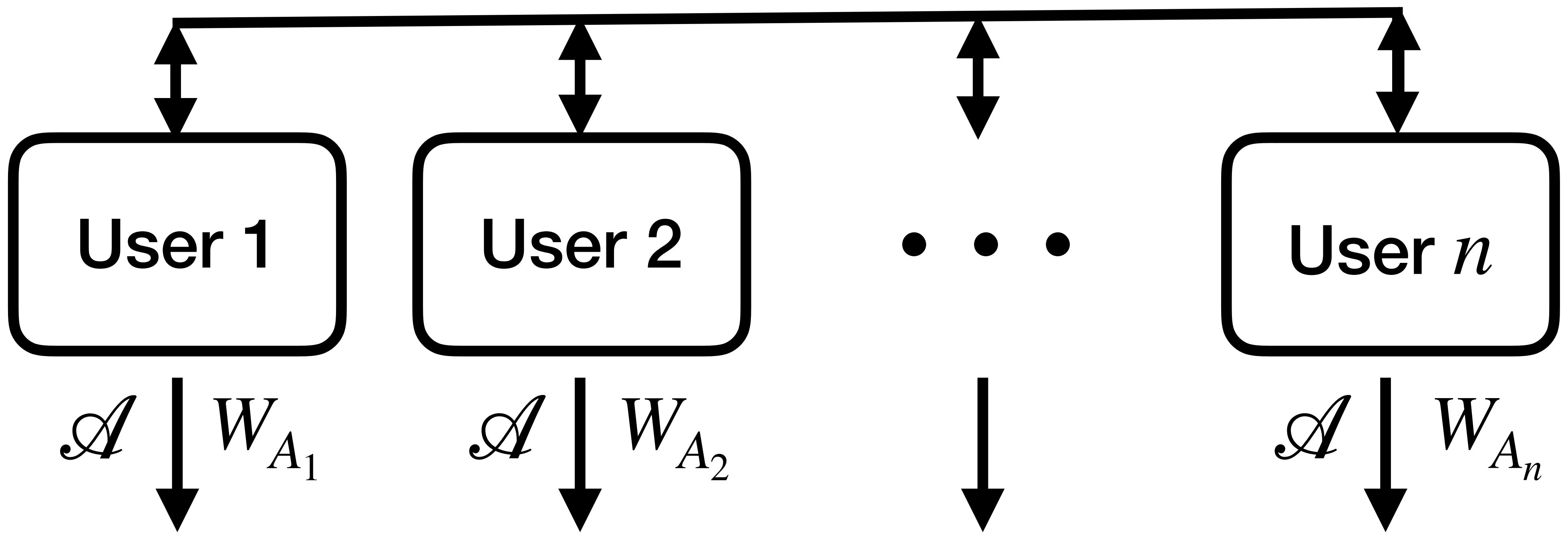
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, x^{\ell k} = \{x^{\ell_1 k}, \ldots, x^{\ell_n k}\}$$



$$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k}) \qquad \hat{w}_{D_2} = DEC_2(W_{A_2}, x^{\ell k})$$

Decentralized PICOD(t)

Notation:

$[m] := \{1,2,\ldots,m\}$;

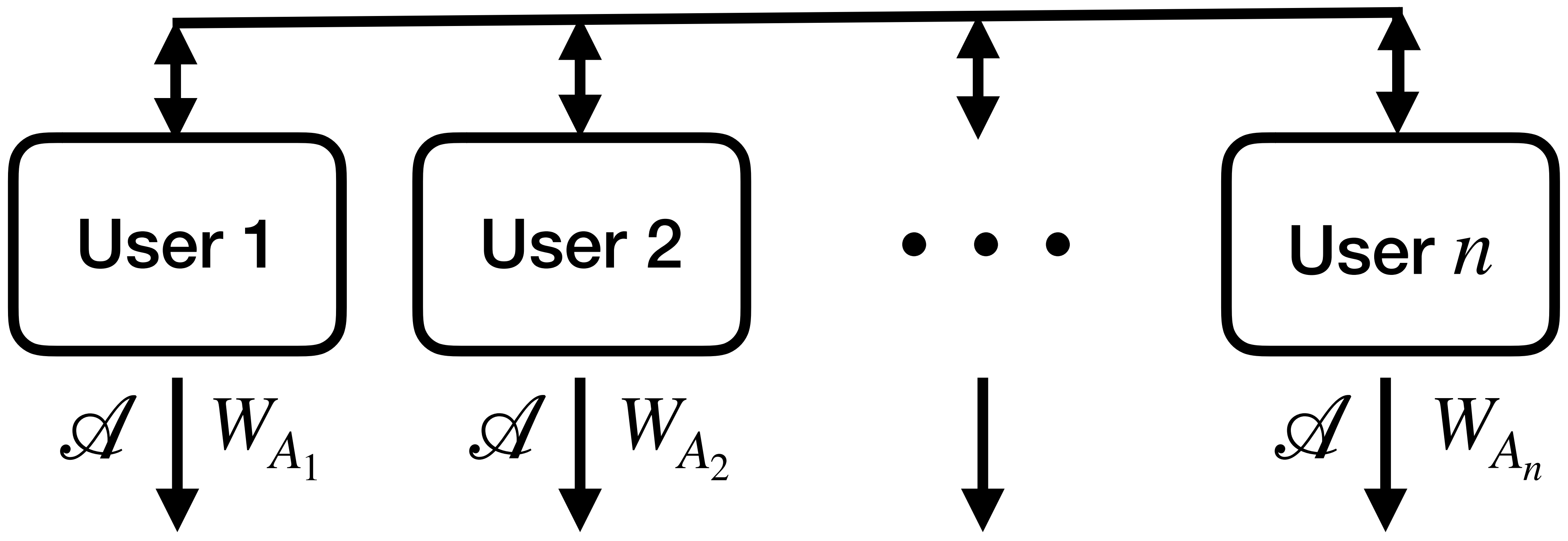
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m]\backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, x^{\ell k} = \{x^{\ell_1 k}, \ldots, x^{\ell_n k}\}$



$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k})$ $\hat{w}_{D_2} = DEC_2(W_{A_2}, x^{\ell k})$ $\hat{w}_{D_n} = DEC_n(W_{A_n}, x^{\ell k})$

Decentralized PICOD(t)

Notation:

$[m] := \{1,2,\ldots,m\}$;

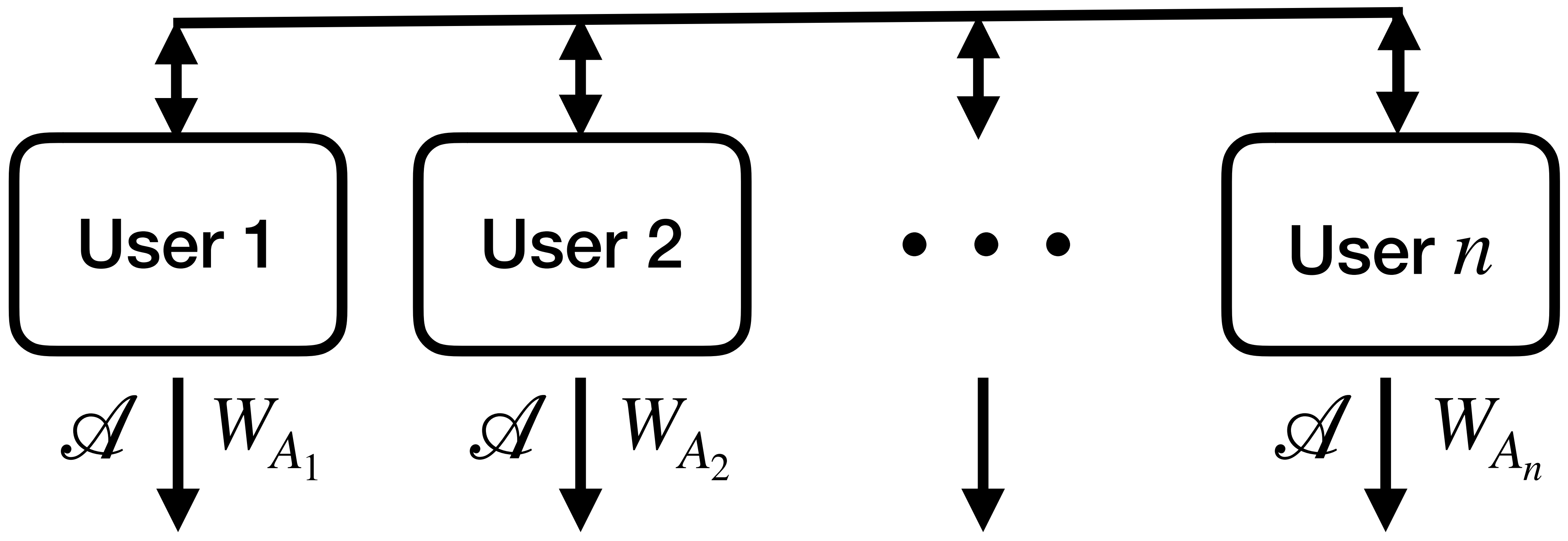
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}, x^{\ell k} = \{x^{\ell_1 k}, \ldots, x^{\ell_n k}\}$$



$$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k}) \quad \hat{w}_{D_2} = DEC_2(W_{A_2}, x^{\ell k}) \quad \hat{w}_{D_n} = DEC_n(W_{A_n}, x^{\ell k})$$

- The codewords are generated by the users based on their side information sets and globally known side information structure.

- **Goal**: determine the minimum number of transmissions that allow each user to decode t messages outside its side information.

Security in PICOD

- Security is a major concern in today's communication. A message should not be decoded at the users for which the message is not intended for.
- Information theoretical security provides guarantee regardless of the computational power of the attacker/eavesdropper/non-intended party.
- In broadcast channels, without explicitly imposing security constraints, the information is likely to be overheard by multiple users.
- Strong security constraint: $H(W_{[m]\backslash(A_i \cup D_i)} | x^{\ell k}, W_{A_i}) \geq H(W_{[m]\backslash(A_i \cup D_i)}) - \epsilon_k, \forall i \in [n]$
- Individual-message security constraint: $H(w_j | x^{\ell k}, W_{A_i}) \geq H(w_j) - \epsilon_k, \forall i \in [n], \forall j \in [m]\backslash(A_i \cup D_i)$

Secure PICOD(t)

Notation:

$[m] := \{1,2,\ldots,m\}$;

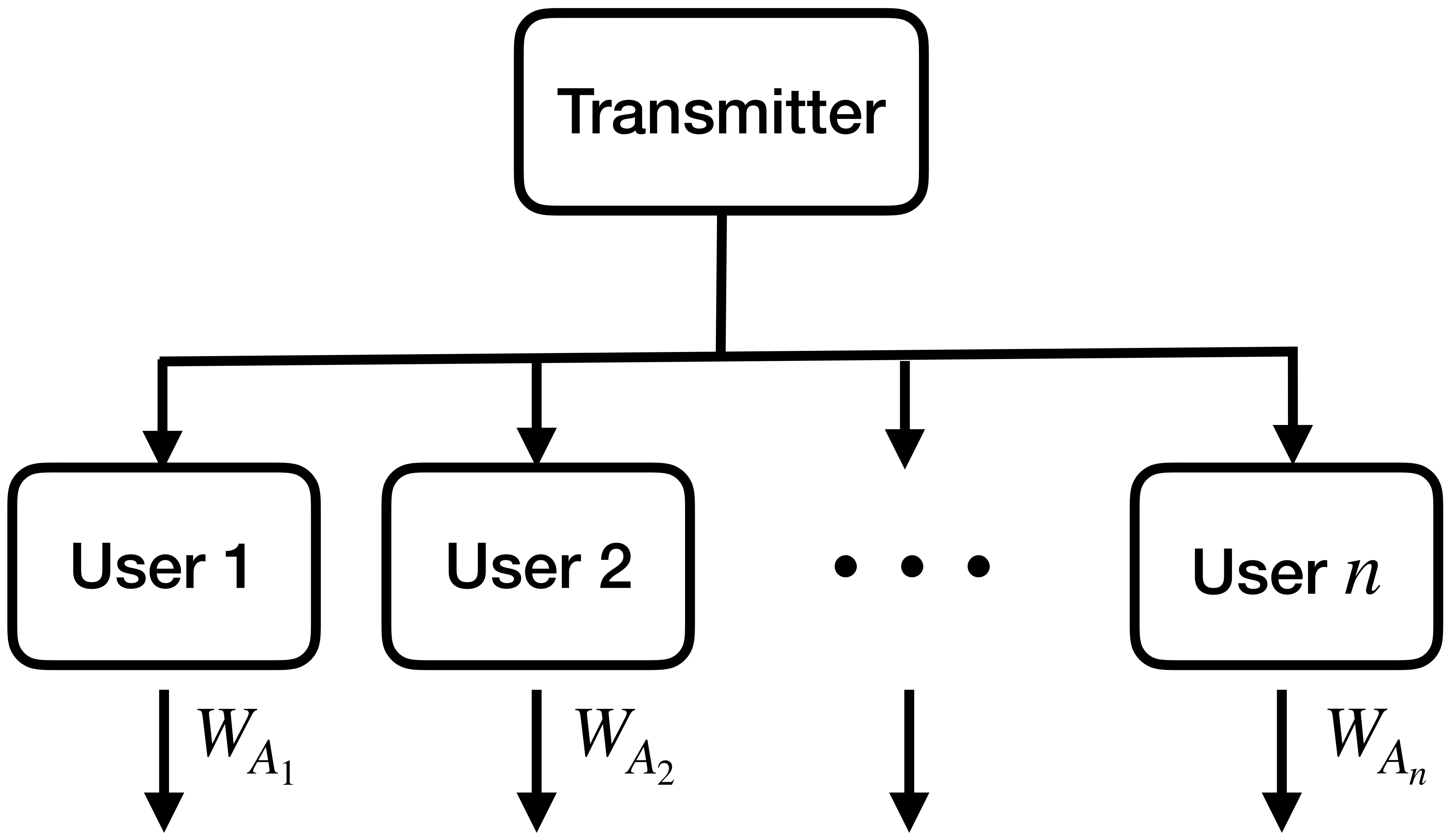
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

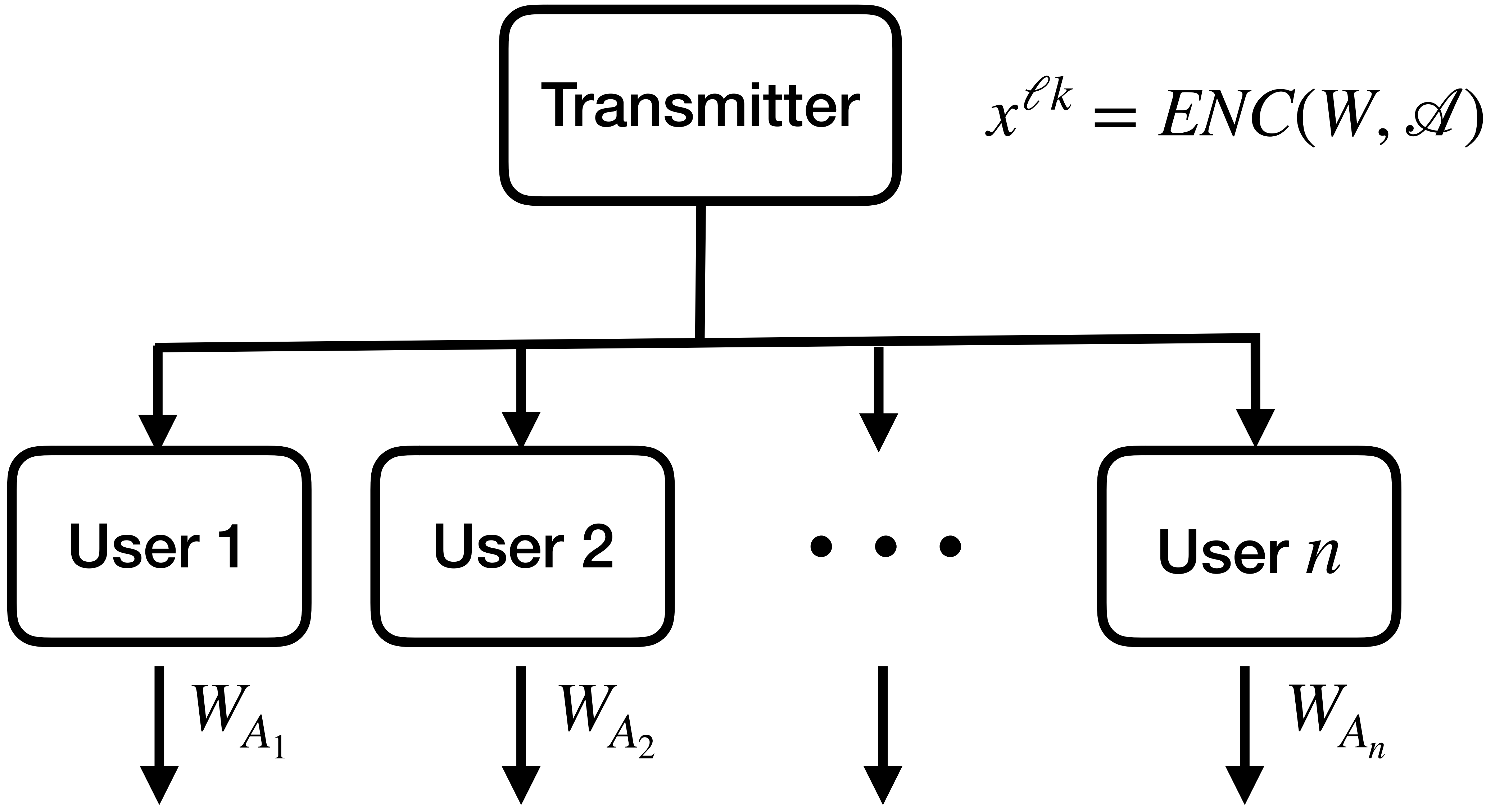
$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}$



Secure PICOD(t)

Notation:
$[m] := \{1,2,\ldots,m\}$;
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;
Side information set: $A_i \subset [m]$;
Pliable desired message set:
some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}$



Secure PICOD(t)

Notation:

$[m] := \{1,2,\ldots,m\}$;

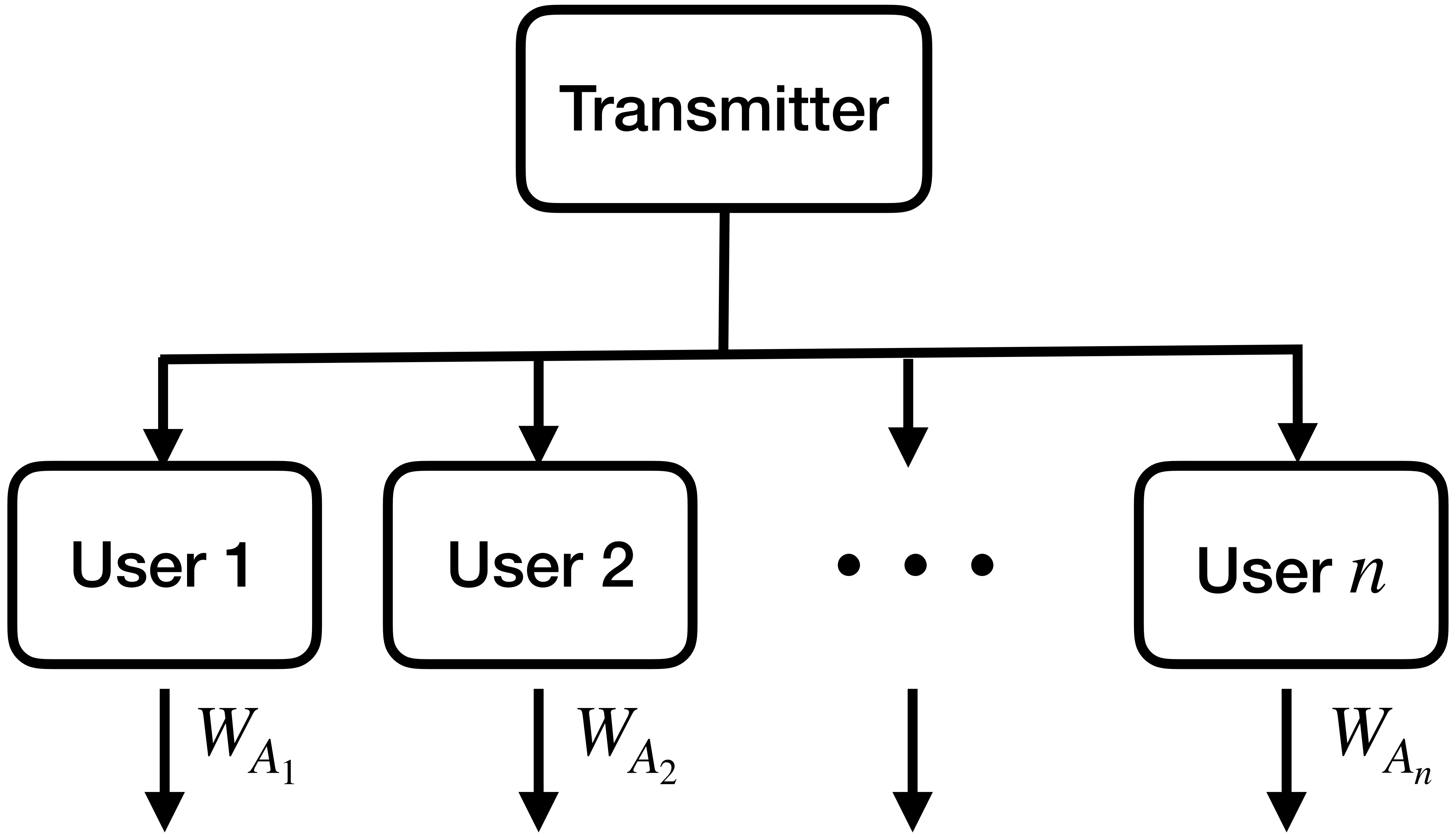
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}$



$x^{\ell k} = ENC(W, \mathscr{A})$

Secure PICOD(t)

Notation:

$[m] := \{1,2,\ldots,m\}$;

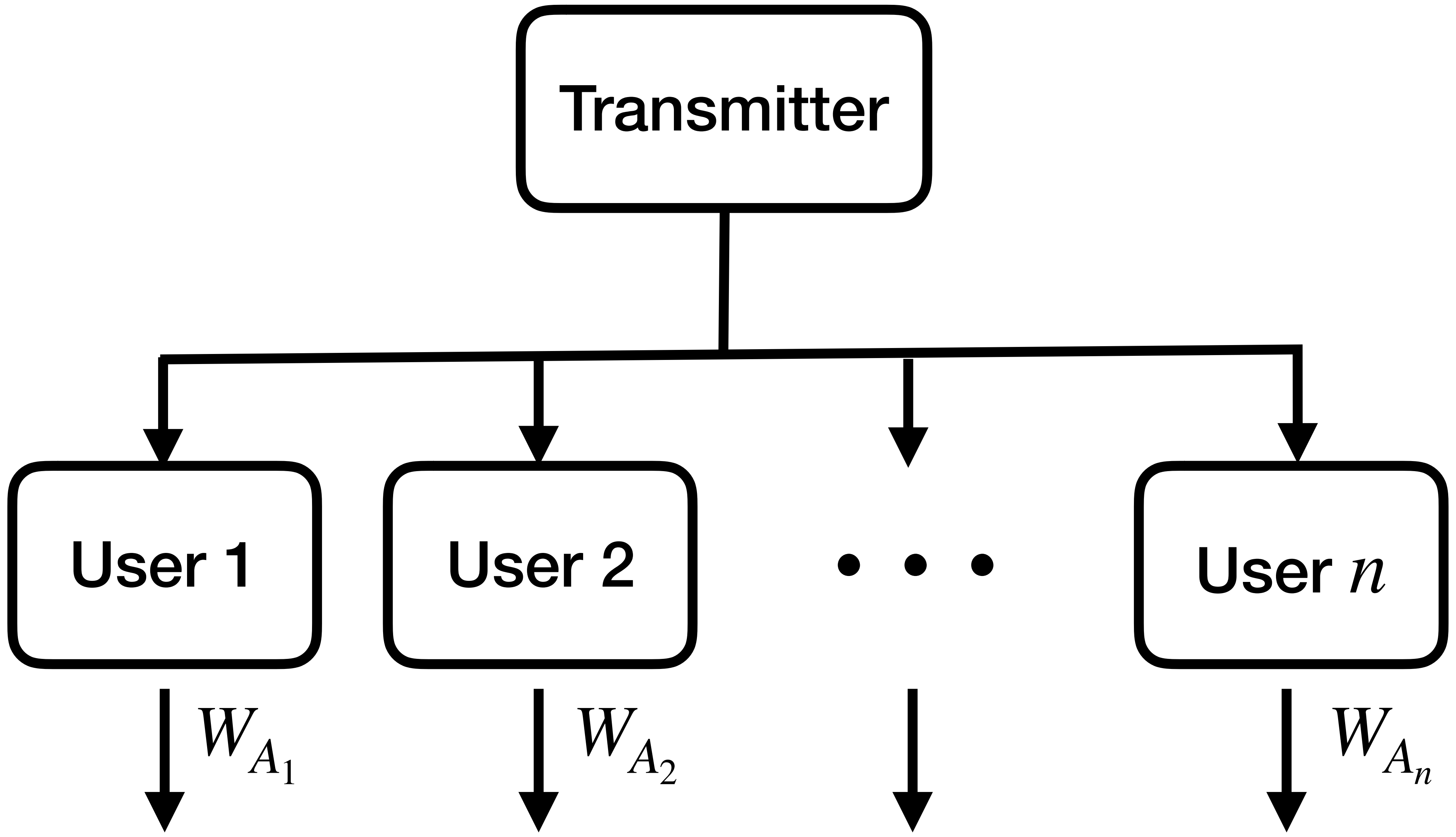
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}$



$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k})$

Secure PICOD(t)

Notation:

$[m] := \{1,2,\ldots,m\}$;

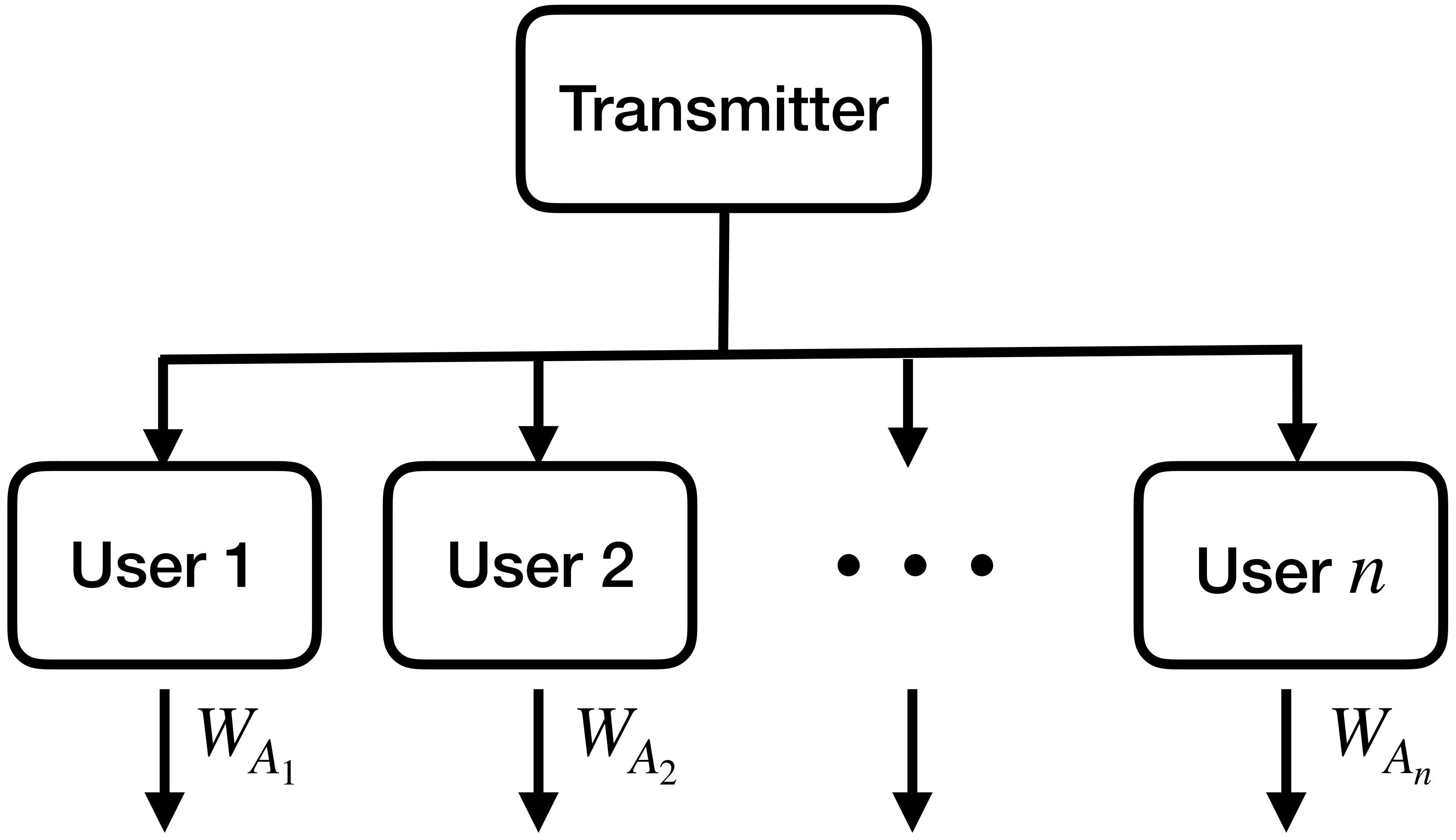
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}$

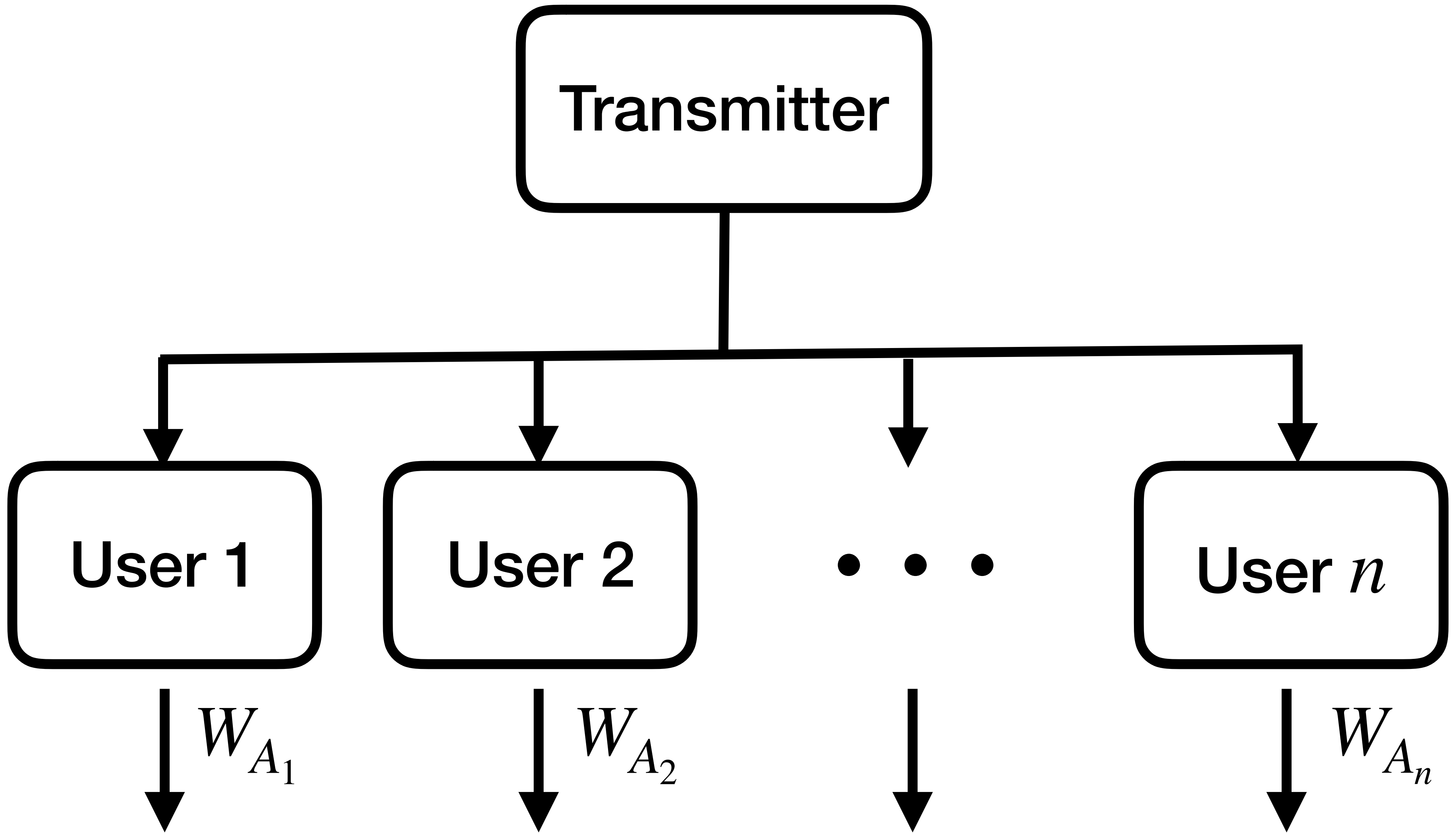


$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k})$ $x^{\ell k} = ENC(W, \mathscr{A})$

Secure PICOD(t)

Notation:
$[m] := \{1,2,\ldots,m\}$;
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;
Side information set: $A_i \subset [m]$;
Pliable desired message set:
some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}$



$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k})$ $\hat{w}_{D_2} = DEC_2(W_{A_2}, x^{\ell k})$

Secure PICOD(t)

Notation:

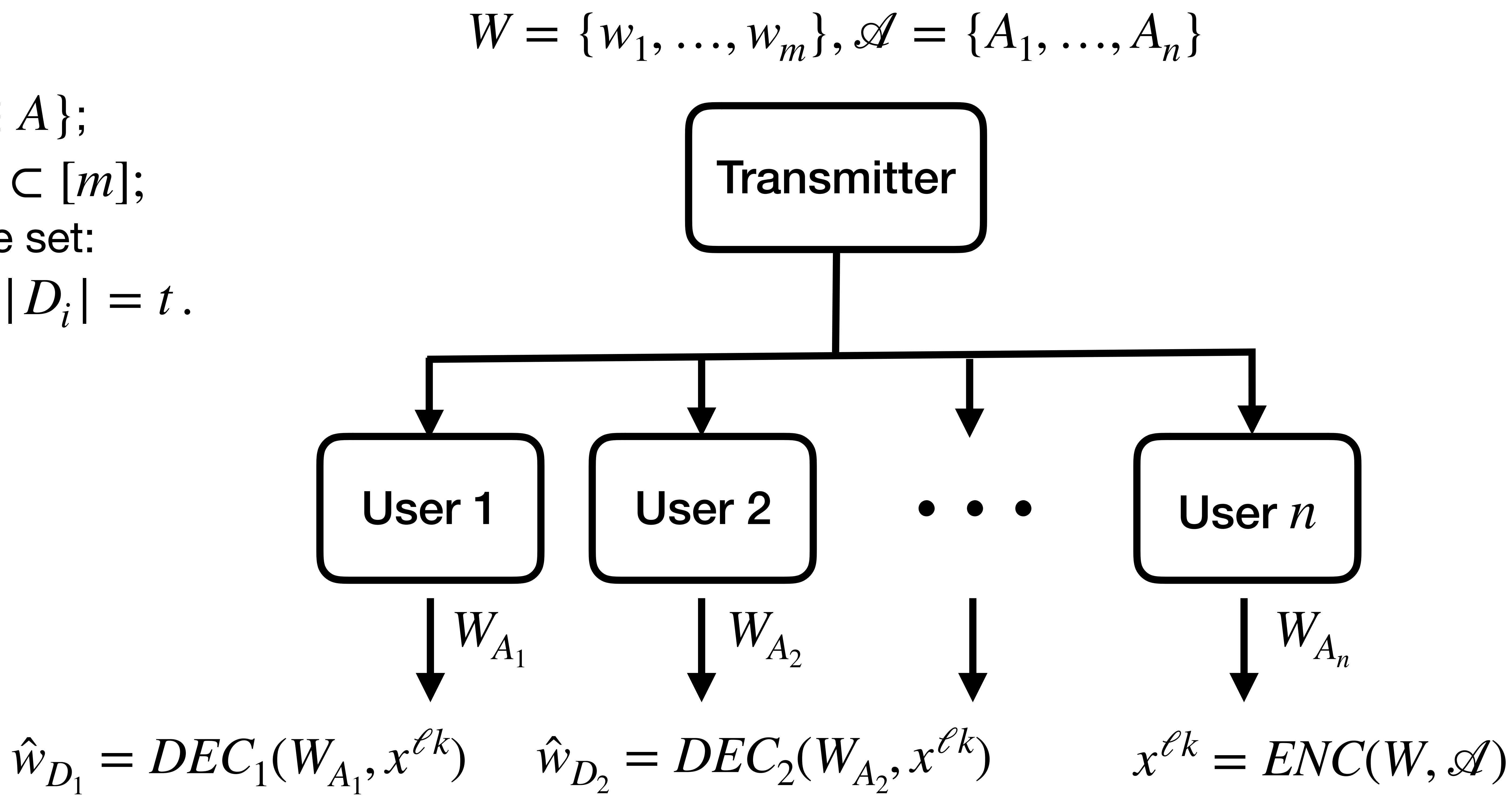
$[m] := \{1,2,\ldots,m\}$;

$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m]\backslash A_i$ s.t. $|D_i| = t$.



Secure PICOD(t)

Notation:

$[m] := \{1,2,\ldots,m\}$;

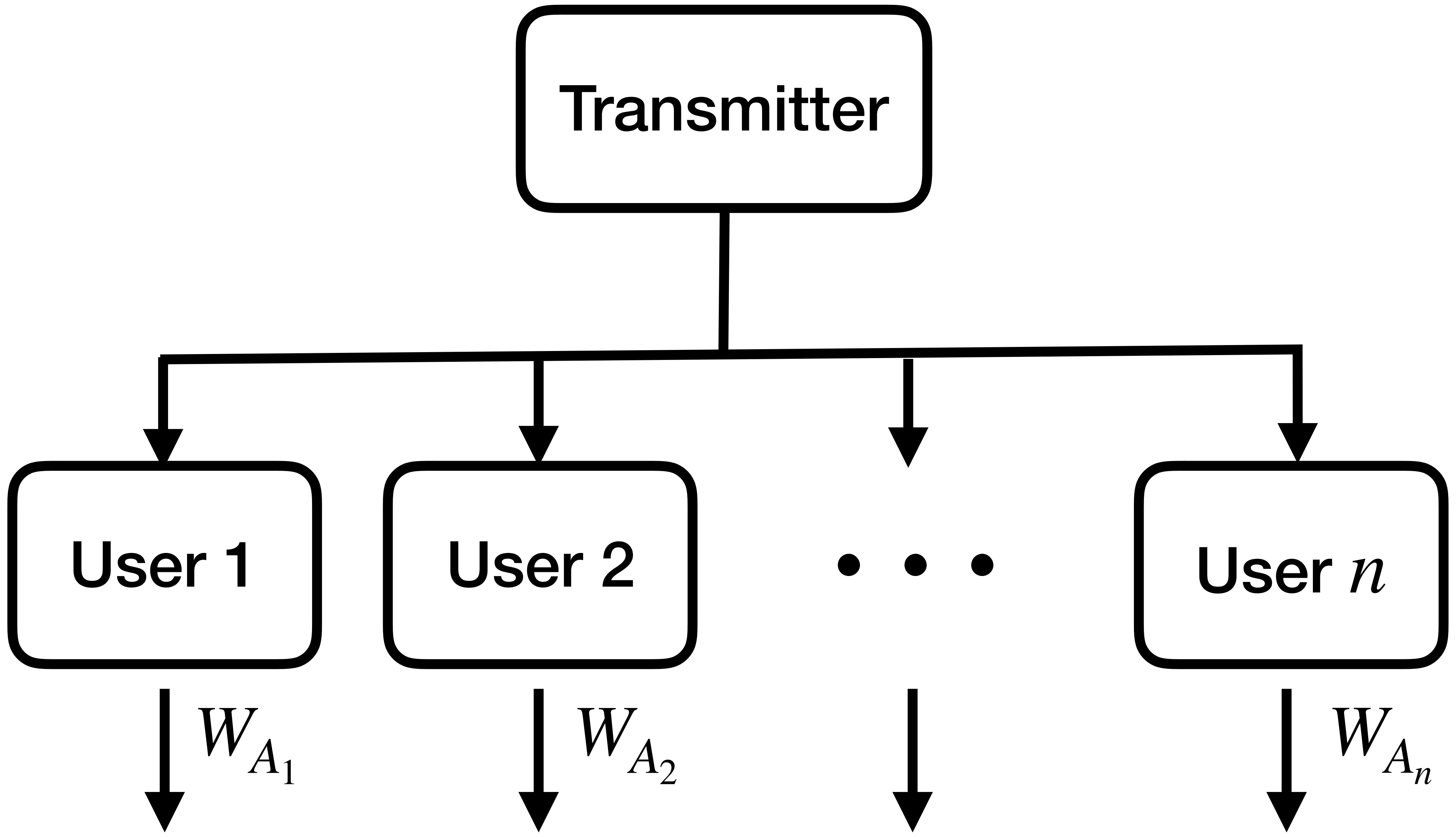
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}$



$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k})$ $\hat{w}_{D_2} = DEC_2(W_{A_2}, x^{\ell k})$ $\hat{w}_{D_n} = DEC_n(W_{A_n}, x^{\ell k})$

Secure PICOD(t)

Notation:

$[m] := \{1,2,\ldots,m\}$;

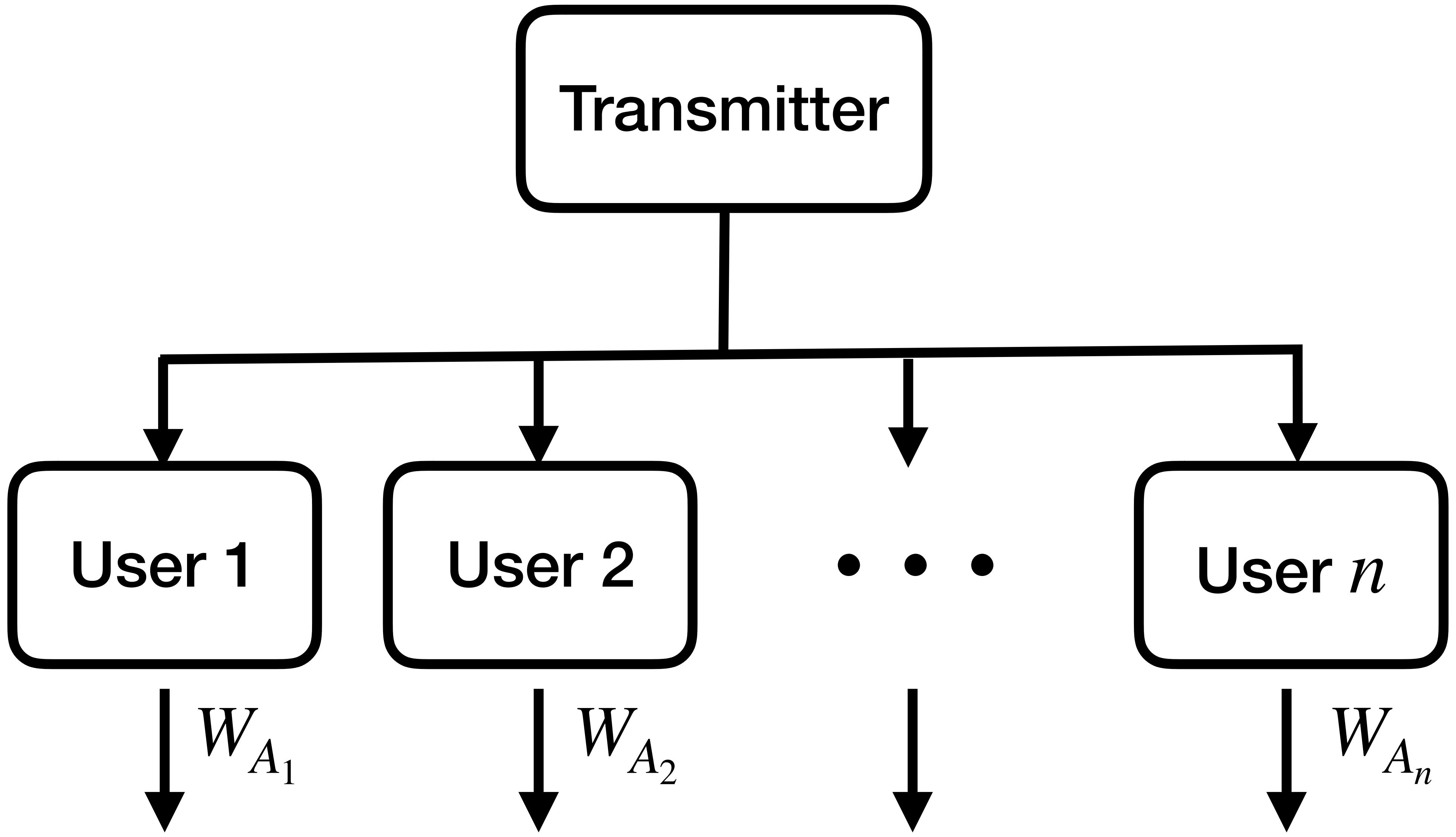
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}$



$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k})$ $\hat{w}_{D_2} = DEC_2(W_{A_2}, x^{\ell k})$ $\hat{w}_{D_n} = DEC_n(W_{A_n}, x^{\ell k})$

$I(w_j; x^{\ell k}, W_{A_i}) \leq \epsilon_k, \forall i \in [n], \forall j \in [m] \backslash (A_i \cup \{d_i\})$

Secure PICOD(t)

Notation:

$[m] := \{1,2,\ldots,m\}$;

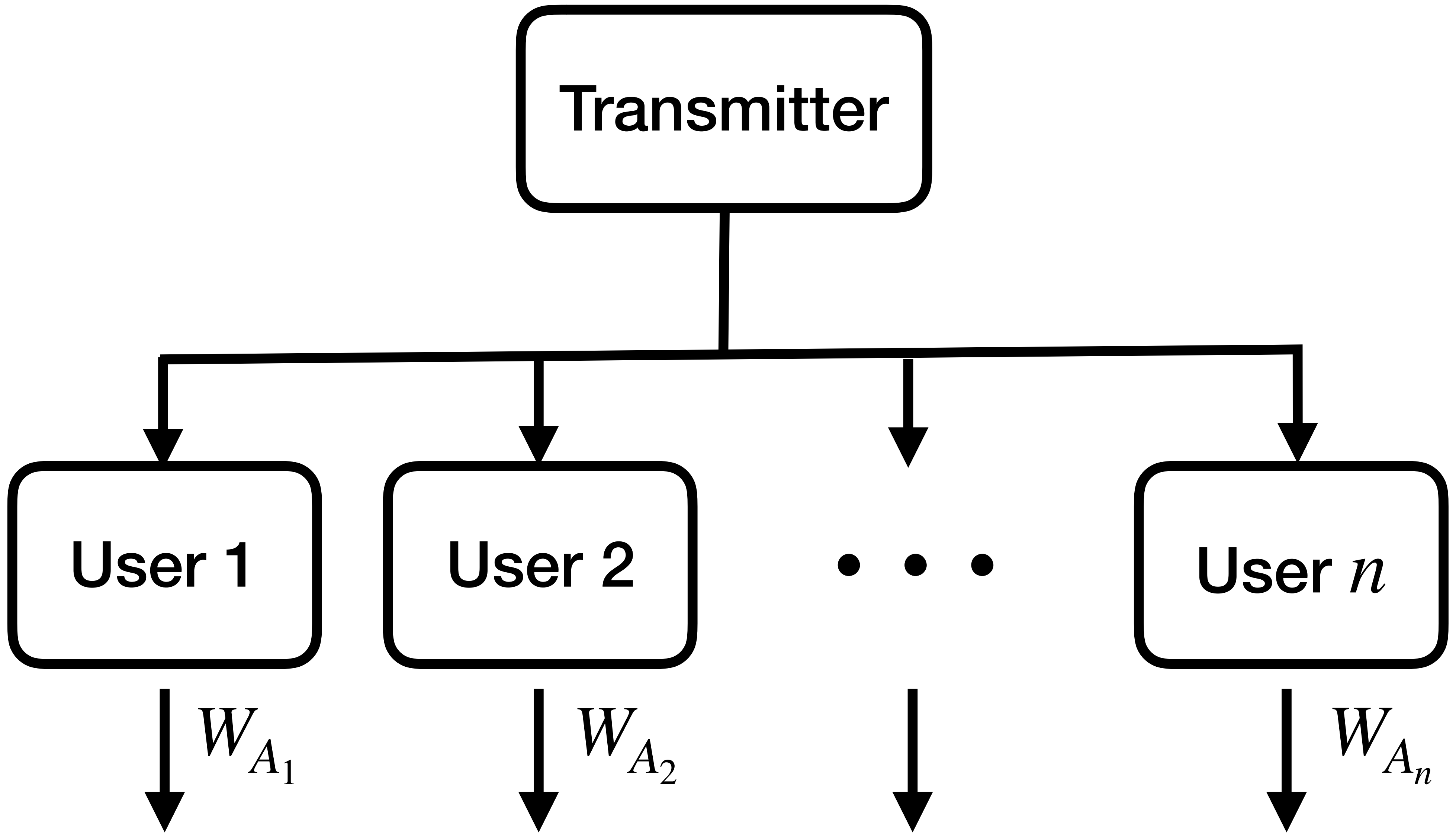
$w \in \mathbb{F}_{2^k}, W_A = \{w_i, i \in A\}$;

Side information set: $A_i \subset [m]$;

Pliable desired message set:

some $D_i \subseteq [m] \backslash A_i$ s.t. $|D_i| = t$.

$W = \{w_1, \ldots, w_m\}, \mathscr{A} = \{A_1, \ldots, A_n\}$



$\hat{w}_{D_1} = DEC_1(W_{A_1}, x^{\ell k})$ $\hat{w}_{D_2} = DEC_2(W_{A_2}, x^{\ell k})$ $\hat{w}_{D_n} = DEC_n(W_{A_n}, x^{\ell k})$

$I(w_j; x^{\ell k}, W_{A_i}) \leq \epsilon_k, \forall i \in [n], \forall j \in [m] \backslash (A_i \cup \{d_i\})$

Goal: find the minimum number of transmission ℓ^* needed by the transmitter such that each user can decode t messages outside its side information and no more than t.

Index coding

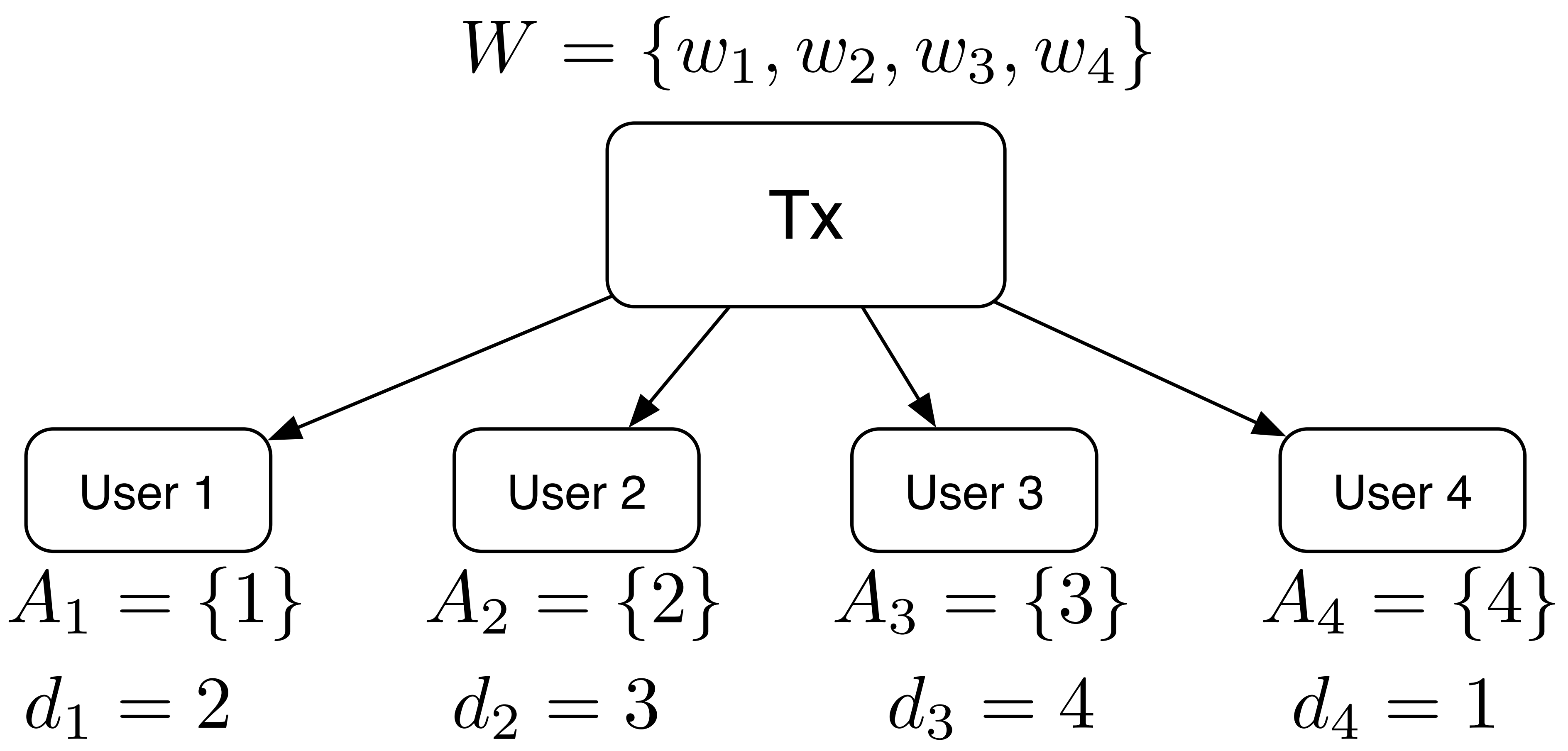
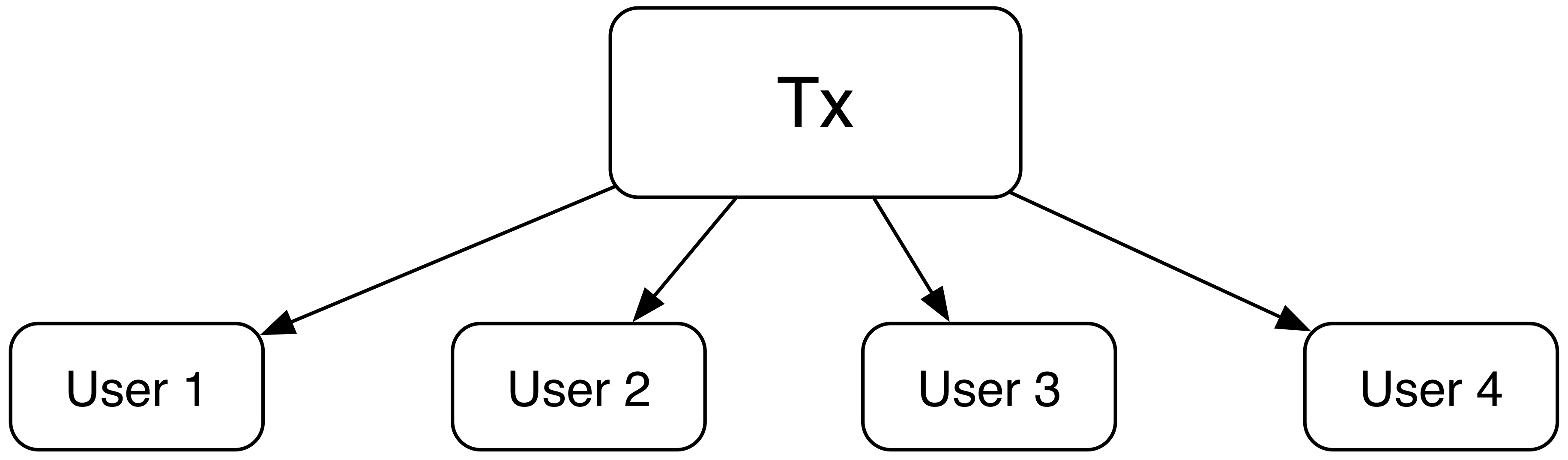


Figure: One optimal code is $\{w_1 + w_2, w_2 + w_3, w_3 + w_4\}$.

Index coding

$W = \{w_1, w_2, w_3, w_4\}$



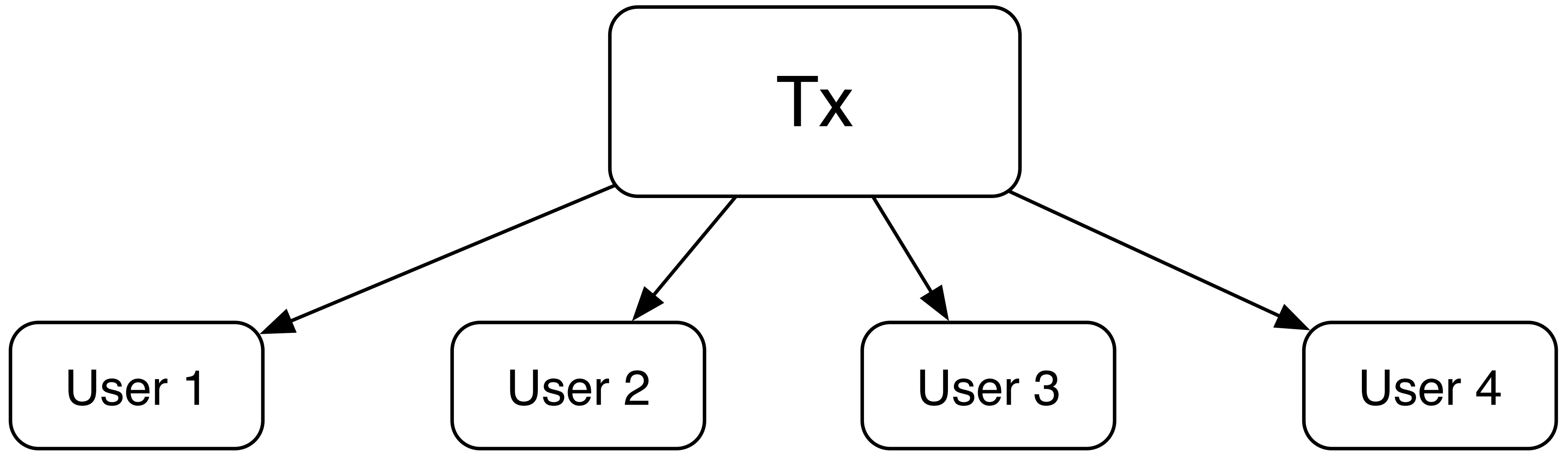
$A_1 = \{1\}$ $A_2 = \{2\}$ $A_3 = \{3\}$ $A_4 = \{4\}$

$d_1 = 2$ $d_2 = 3$ $d_3 = 4$ $d_4 = 1$

Figure: One optimal code is $\{w_1 + w_2, w_2 + w_3, w_3 + w_4\}$.

PICOD

$W = \{w_1, w_2, w_3, w_4\}$



$A_1 = \{1\}$ $A_2 = \{2\}$ $A_3 = \{3\}$ $A_4 = \{4\}$

$d_1 \in \{2, 3, 4\}$ $d_2 \in \{1, 3, 4\}$ $d_3 \in \{1, 2, 4\}$ $d_4 \in \{1, 2, 3\}$

Figure: $\{w_1, w_3\}$ and $\{w_1 + w_2, w_3 + w_4\}$ are optimal.

PICOD

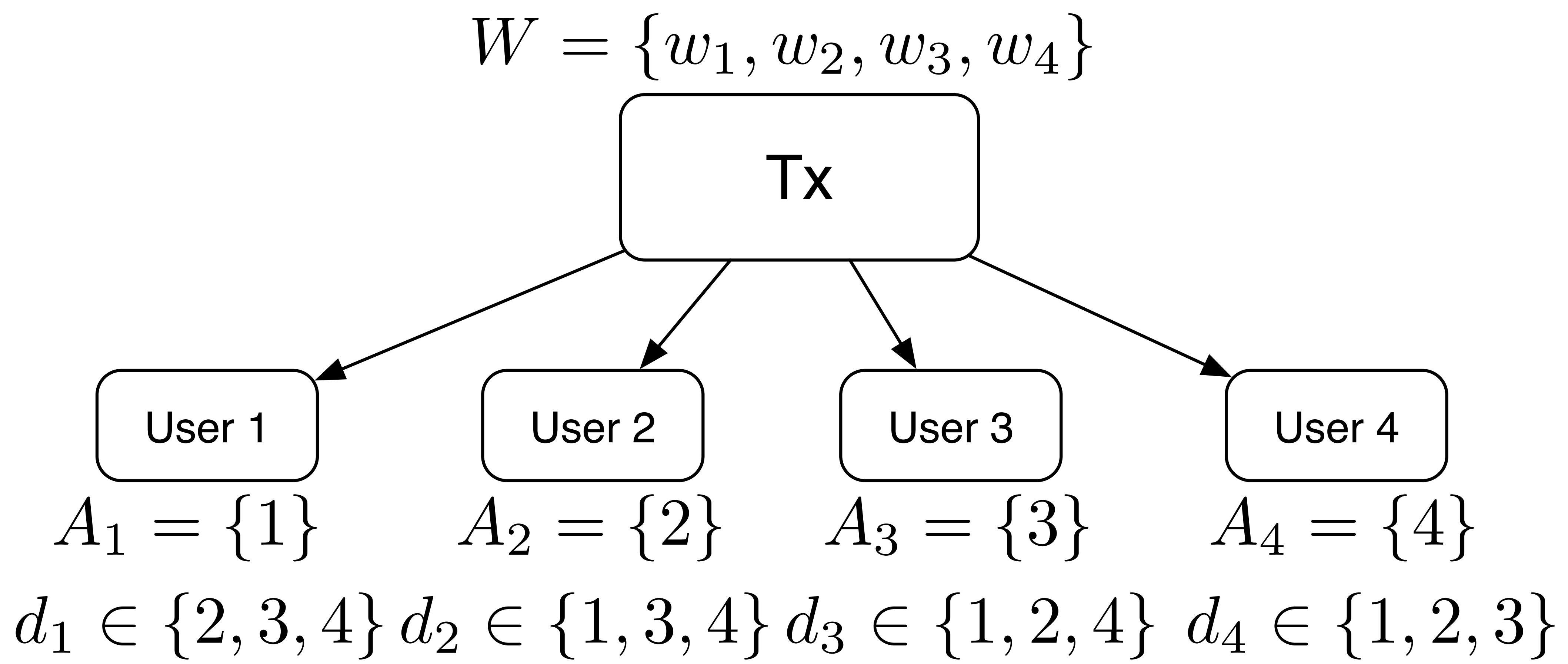


Figure: $\{w_1, w_3\}$ and $\{w_1 + w_2, w_3 + w_4\}$ are optimal.

PICOD

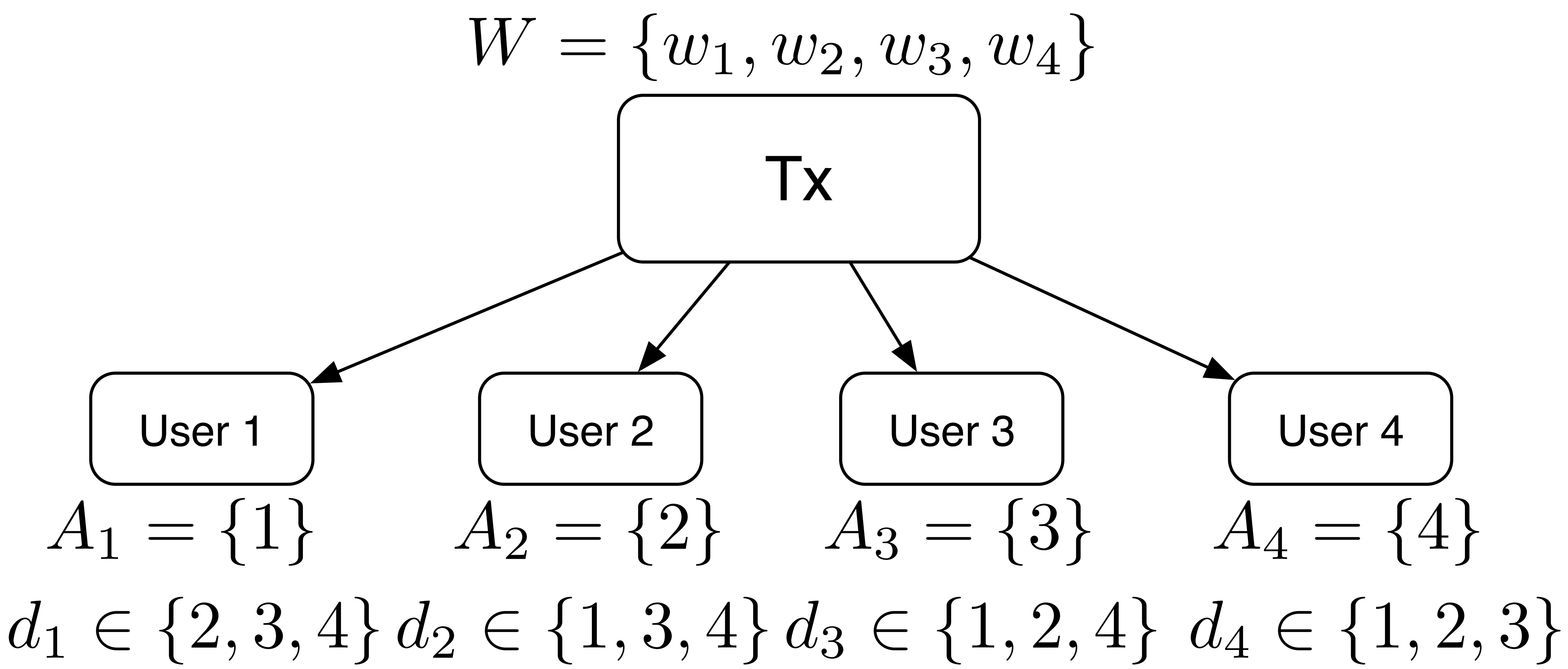


Figure: $\{w_1, w_3\}$ and $\{w_1 + w_2, w_3 + w_4\}$ are optimal.

Decentralized PICOD

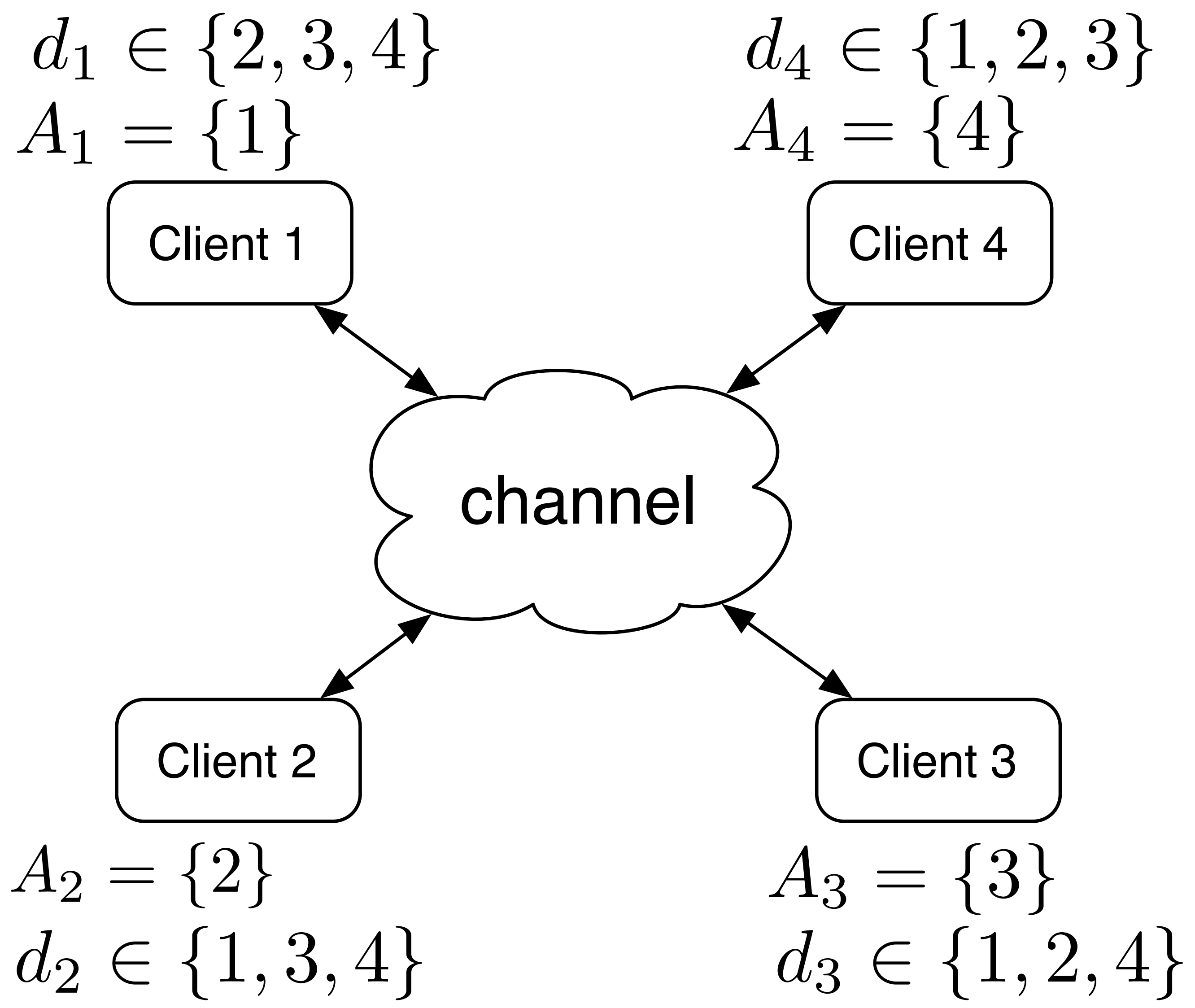


Figure: $\{w_1 + w_2, w_3 + w_4\}$ is not a decentralized code.
$\{w_1, w_3\}$ is decentralized code.

PICOD

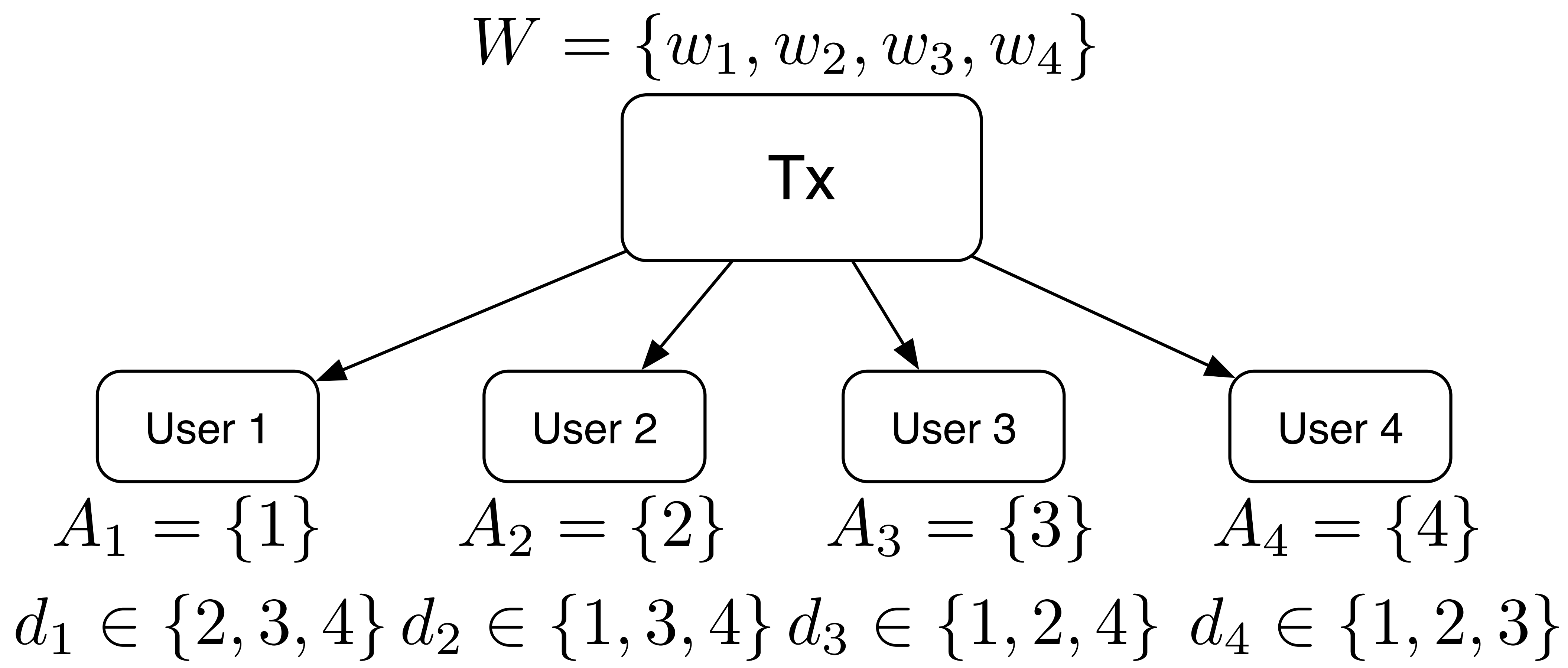


Figure: $\{w_1, w_3\}$ and $\{w_1 + w_2, w_3 + w_4\}$ are optimal.

Secure PICOD

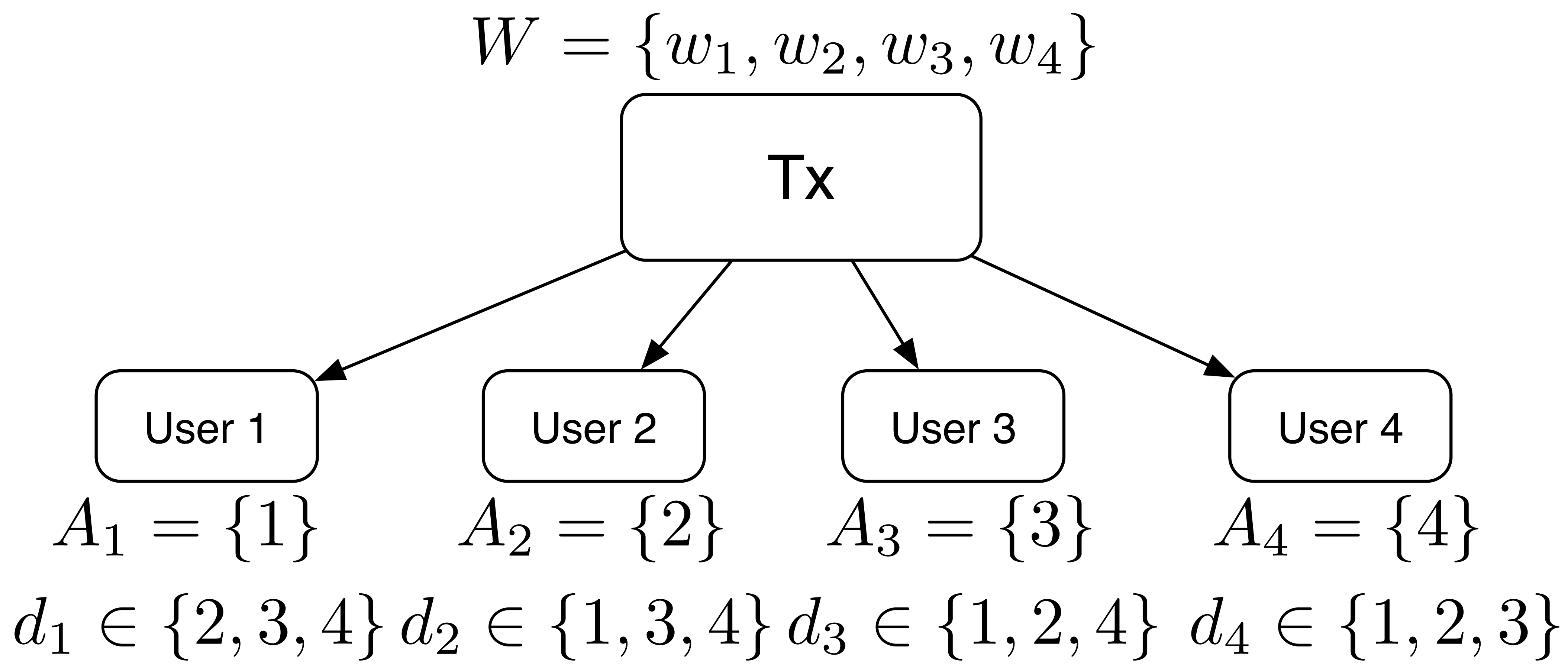


Figure: $\{w_1 + w_2, w_3 + w_4\}$ is secured code. $\{w_1, w_3\}$ is not secure code.

Decentralized PICOD

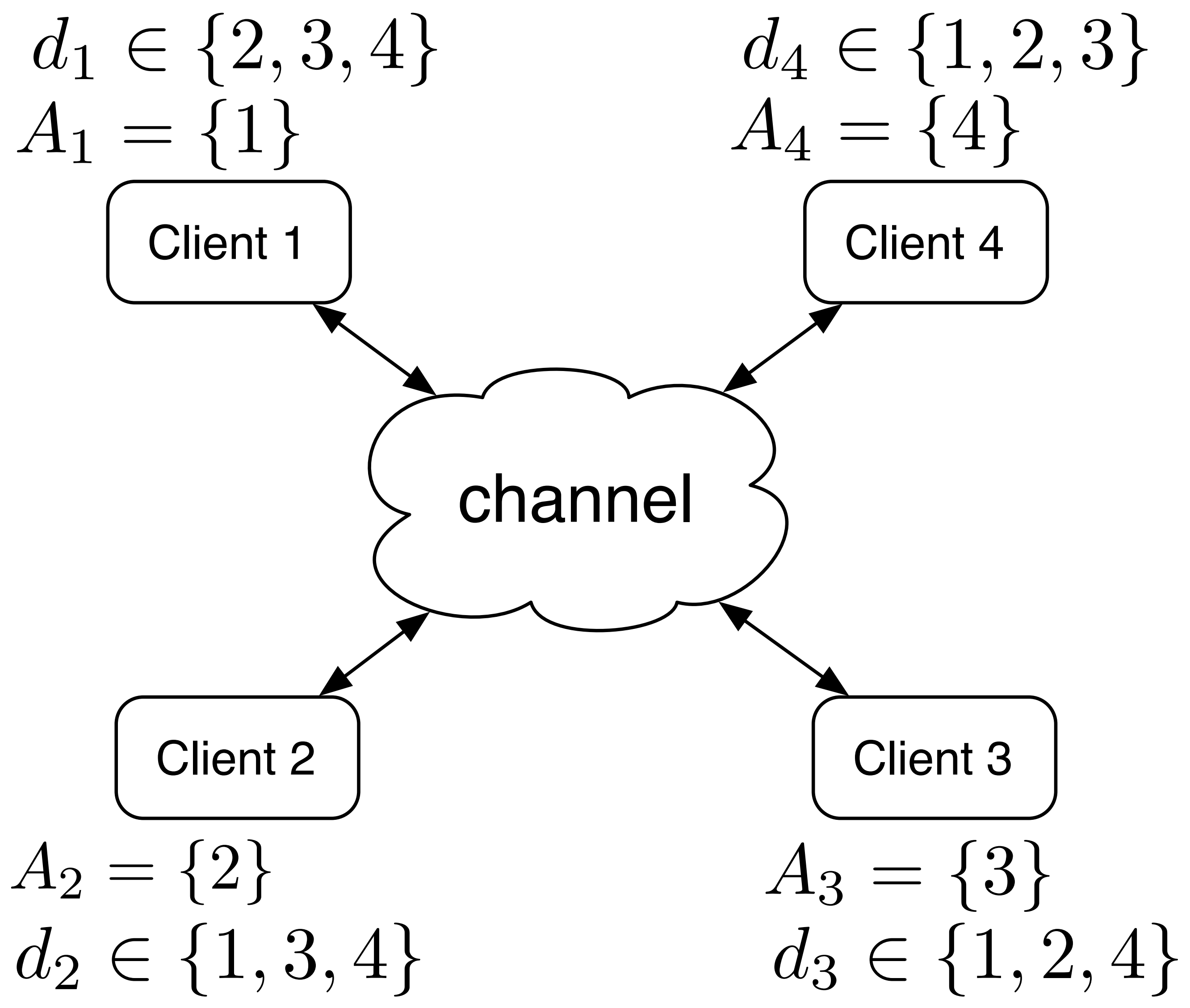


Figure: $\{w_1 + w_2, w_3 + w_4\}$ is not a decentralized code. $\{w_1, w_3\}$ is decentralized code.

Relevant past work

Index Coding

- General index coding problem is open.
- Index coding is equivalent to network coding[1].
- There are index coding instances that require non-Shannon type of inequalities[2] (non-negativity of conditional mutual information).
- There are index coding instances where nonlinear schemes strictly outperforms all linear schemes[3].

We do not solve PICOD by solving the corresponding family of IC.

[1] M. Effros, S. E. Rouayheb, M. Langberg, "An Equivalence Between Network Coding and Index Coding," IEEE Trans. Information Theory, May 2015.
[2] H. Sun, S. A. Jafar, "Index Coding Capacity: How Far Can One Go With Only Shannon Inequalities?" IEEE Trans. Information Theory, June 2015.
[3] E. Lubetzky, U. Stav, "Nonlinear Index Coding Outperforming the Linear Optimum," IEEE Trans. Information Theory, Aug 2009.

PICOD(t)

m = # of messages; $s_{\max}/s_{\min}$ = maximum/minimum size of side information set; t = # of desired message per user.

- **Past work**
  - Achievability:
    - Sufficiency of $O(\log n)$ transmissions for PICOD(1) if each user has side information set of the same size ($|A_i| = s, \forall i$)[1].
    - Sufficiency of $O(t\log(n) + \log^2(n))$ transmissions for PICOD(t)[2].
  - Linear converse:
    - Necessity of $\min\{s_{\max} + t, m - s_{\min}\}$ transmissions for linear scheme in PICOD(t) where transmitter only knows side information size range $[s_{\min} : s_{\max}]$[1].
    - Necessity of $\log(n)$ transmissions for linear scheme in a construction of PICOD(1)[2].
- **Our contributions**
  - For PICOD(1) with same size of side information at the users, one transmission satisfies at least $\max\{(1-\frac{s}{m})^{\frac{m}{s}-1}e(1-\frac{1}{s})^{s-1}, \frac{s}{m}\} \geq 1/e$ fraction of unsatisfied users in the system[3].
  - Information theoretical optimality for some complete-S PICOD(t) and PICOD(1) with circular-arc side information[4,5,6].

[1] S. Brahma and C. Fragouli, "Pliable index coding," IEEE Trans. Information Theory, Nov 2015.
[2] L. Song and C. Fragouli, "A Polynomial-Time Algorithm for Pliable Index Coding," IEEE Trans. Information Theory, Feb 2018.
[3] T. Liu and D. Tuninetti, "Pliable Index Coding: Novel Lower Bound on the Fraction of Satisfied Clients with a Single Transmission and its Application," ITW, 2016.
[4] T. Liu and D. Tuninetti, "Information Theoretic Converse Proofs for Some PICOD Problems," ITW, 2017.
[5] T. Liu and D. Tuninetti, "An Information Theoretic Converse for the "Consecutive CompleteS" PICOD Problem," ITW, 2018.
[6] T. Liu and D. Tuninetti, "Tight Information Theoretic Converse Results for some Pliable Index Coding Problems," IEEE Trans. on Information Theory, 2019.

Decentralized PICOD(t)

- **Past work (decentralized IC)**
  - IC with multiple transmitters/distributed IC[1]: capacity up to 3 messages.
  - Decentralized/embedded IC[2]: multiplicative gap 2 to the centralized version.
  - Data exchange problem[3]: users request all messages that are not in the side information.
- **Our contributions**[4,5]
  - Achievability scheme based on vector index coding and decentralized MDS code for decentralized complete—S PICOD(t) and PICOD(1) with circular-arc side information.

[1] Y. Liu, P. Sadeghi, F. Arbabjolfaei, and Y.-H. Kim, "Capacity theorems for distributed index coding," arXiv:1801.09063, 2018.
[2] M. W. Alexandra Porter, "Embedded index coding," Information Theory Workshop, 2019. arXiv:1904.02179.
[3] N. Milosavljevic, S. Pawar, S. E. Rouayheb, M. Gastpar, and K. Ramchandran, ``Efficient algorithms for the data exchange problem,'' IEEE Trans. Information Theory, vol. 62, no. 4, pp. 1878 – 1896, April 2016.
[4] T. Liu and D. Tuninetti, "Decentralized pliable index coding." ISIT, 2019.
[5] T. Liu and D. Tuninetti, "Decentralized Pliable Index Coding." Submitted to IEEE Trans. on Information Theory.

Secure PICOD(1)

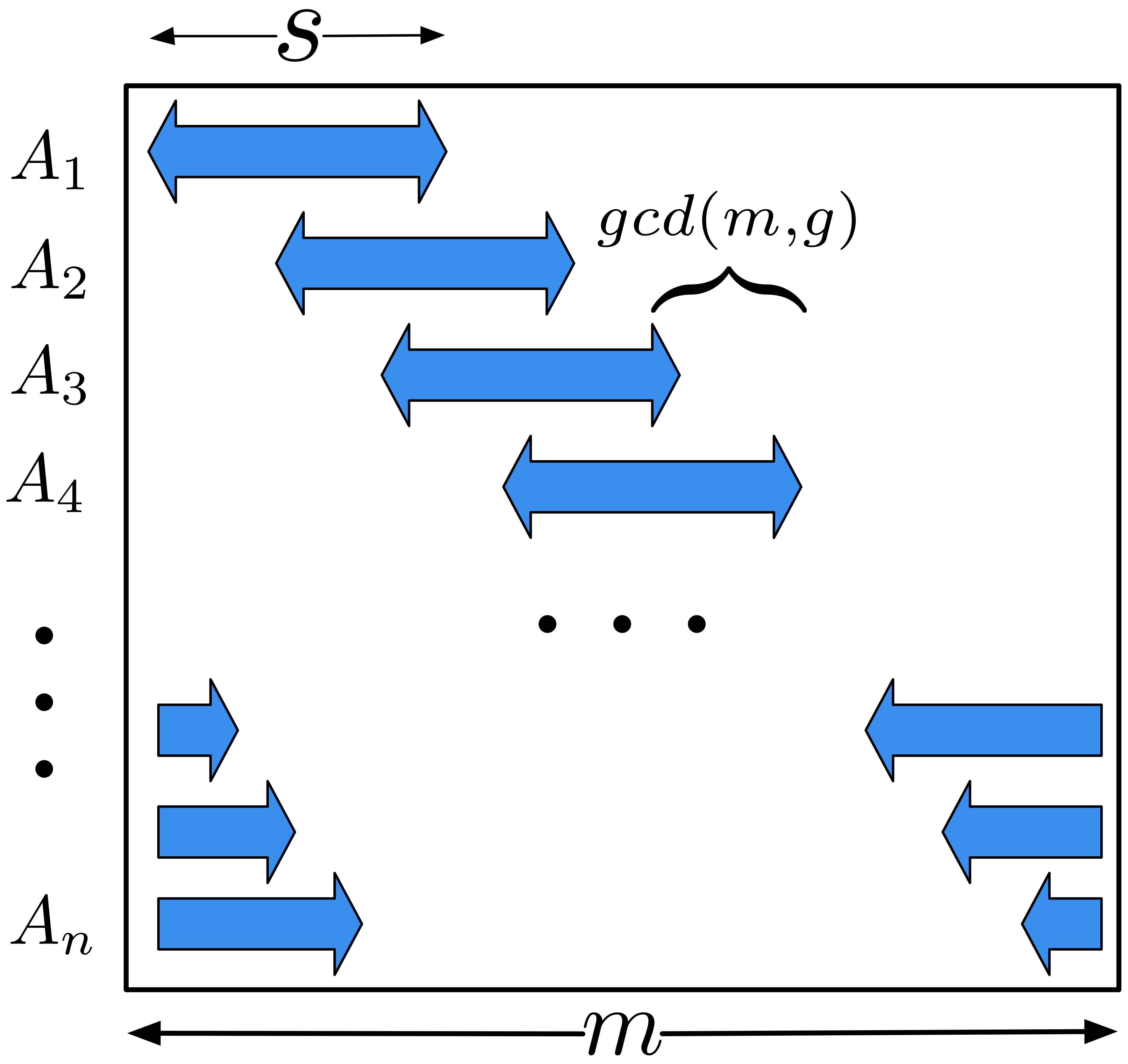


Figure: Circular shift side

- **Past work**[1]
  - # of messages = # of users = m; side information size = s; side information shift = 1.
  - Under linear encoding constraint
    - Unfeasible cases.
    - Optimality for $s > m/2$.
- **Our contributions**[2,3]
  - Generalized model: # of messages = m, side information size = s, side information shift = g.
  - Information theoretical converse tight for some cases.
  - Universal achievable scheme that differ from optimality by one transmission under the linear encoding constraint.

[1] Shanuja Sasi, B. Sundar Rajan, ``On Pliable Index Coding,'' ISIT 2019.
[2] T. Liu and D. Tuninetti, "Private pliable index coding." ITW, 2019.
[3] T. Liu and D. Tuninetti, "Individually Secure Pliable Index Coding." Under preparation.

Our contributions

Our contributions

1. For PICOD(1) where all users have the same size of side information, there exists a scheme that satisfies at least a constant fraction of unsatisfied users at each transmission [1]. **Deterministic construction and better faction guarantee.**
2. Information theoretical optimality for some complete-S PICOD(t) and PICOD(1) with circular-arc side information [2,3,4]. **Novel converse bound rooted in combinatorics.**
3. Information theoretical optimality for some decentralized complete-S PICOD(t) and PICOD(1) with circular-arc side information [5,6]. **First to pose and study the problem.**
4. Linear near optimality for individual message secure PICOD(1) with circular-arc side information [7,8]. **Improved scheme and information theoretic optimality in some cases.**

[1] T. Liu and D. Tuninetti, "Pliable Index Coding: Novel Lower Bound on the Fraction of Satisfied Clients with a Single Transmission and its Application," ITW, 2016.
[2] T. Liu and D. Tuninetti, "Information Theoretic Converse Proofs for Some PICOD Problems," ITW, 2017.
[3] T. Liu and D. Tuninetti, "An Information Theoretic Converse for the "Consecutive CompleteS" PICOD Problem," ITW, 2018.
[4] T. Liu and D. Tuninetti, "Tight Information Theoretic Converse Results for some Pliable Index Coding Problems," IEEE Trans. on Information Theory, 2019.
[5] T. Liu and D. Tuninetti, "Decentralized pliable index coding." ISIT, 2019.
[6] T. Liu and D. Tuninetti, "Decentralized Pliable Index Coding." Submitted to IEEE Trans. on Information Theory.
[7] T. Liu and D. Tuninetti, "Private pliable index coding." ITW, 2019.
[8] T. Liu and D. Tuninetti, "Individually Secure Pliable Index Coding." Under preparation.

Proofs in a longer version on these slides. See also PICOD ieeexplore 8871209

d-PICOD arXiv 1904.05272

s-PICOD arXiv 1904.04468

Future work

- Combine our method with others (e.g., absent user[1], weighted alignment chain[2]) for improved converse bounds.

- Understand fundamental differences between PICOD and decentralized or secure version.

- Secure vs Privacy[3] in PICOD.

[1] L. Ong, B. N. Vellambi, J. Kliewer, "Optimal-Rate Characterisation for Pliable Index Coding using Absent Receivers," ISIT 2019.
[2] Y. Liu and P. Sadeghi, "From Alignment to Acyclic Chains: Lexicographic Performance Bounds for Index Coding," Allerton 2019.
[3] M. Karmoose, L. Song, M. Cardone and C. Fragouli, Privacy in Index Coding: Improved Bounds and Coding Schemes, in: IEEE International Symposium on Information Theory (ISIT), 2018

THANK YOU!