Transceivers Model–A New Model for Multiterminal Secret Key Agreement

Alireza Poostindouz, and Reihaneh Safavi-Naini

Information Security Talk
Dec. 4, 2020

UNIVERSITY OF CALGARY

Overview

- Motivation
- Intro to Secret Key Agreement (SKA)
- Definitions and Background
- Our results
- Future Work

Paper: Alireza Poostindouz, Reihaneh Safavi-Naini, "A Channel Model of Transceivers for Multiterminal Secret Key Agreement," 2020 International Symposium on Information Theory & Applications (ISITA). Kapolei, Hawai'i, USA, Oct. 2020.

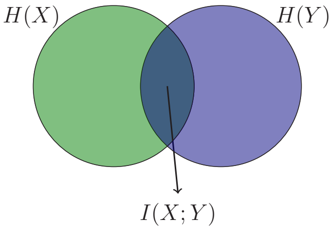
[Full version is available online via arxiv.org:2008.02977]

Why information theoretic key agreement?

- Gives **provable security** guarantee against adversaries with **unlimited computational power**
- Raises many **new insights** and gives a **powerful framework** to study the **fundamental limits of information networks**
- Has **many applications** based on practical physical-layer assumptions
- Enables **quantum-safe communication**

Background

- Entropic Measures of Information



Shannon Entropy

$$H(X) = \sum_{x \in \mathcal{X}} P_X(x) \log_2 \frac{1}{P_X(x)}$$

Joint Entropy

$$H(X,Y) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} P_{XY}(x,y) \log_2 \frac{1}{P_{XY}(x,y)}$$

Conditional Entropy

$$H(X,Y) = H(X) + H(Y|X)$$

Mututal Information

$$I(X;Y) = H(X,Y) - H(X|Y) - H(Y|X)$$

Background - Information theory

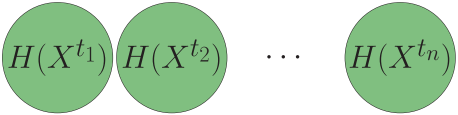
- **IID (Independent and identically distributed) Sources**

$$X^n = (X^{t_1}, X^{t_2}, X^{t_3}, X^{t_4}, \dots, X^{t_n})$$

$\{X^{t_i}\}_{i \leq n}$ are mutually independent

$$P_{X^{t_j}} = P_{X^{t_1}} = P_X \quad \forall j \leq n$$

$$H(X^n) = H(X^{t_1}) + H(X^{t_2}) + \cdots + H(X^{t_n}) = nH(X)$$



Point-to-point Channel

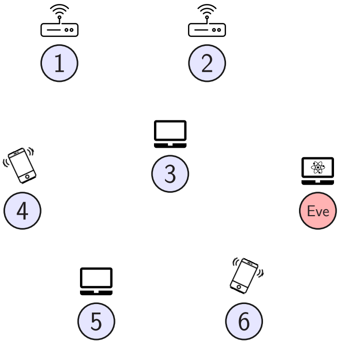
- Consider two parties Alice and Bob.
- Assume that Alice can send signals to Bob, over a *noisy medium*.
- We call such noisy means of signal transmission, "**Channels**."
- A discrete memoryless channel (DMC) is denoted by

$$W = (\mathcal{X}_1, P_{X_2|X_1}, \mathcal{X}_2)$$

or in short $W = P_{X_2|X_1}$.

Multiterminal Channel Model

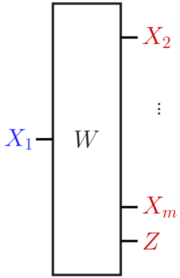
- Set of m terminals.
- E.g. $\mathcal{M} = \{1, 2, 3, 4, 5, 6\}$
- Eve has unlimited computation power
- An underlying noisy channel
- SKA for $\mathcal{A} \subseteq \mathcal{M}$
- E.g. $\mathcal{A} = \{3, 4, 5, 6\}$
- Terminals 1 and 2 are helpers
- Terminals have access to a free and reliable public channel

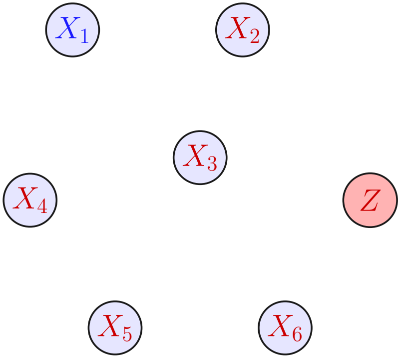


Csiszár and Narayan, "Secrecy Capacities for Multiterminal Channel Models", IEEE Trans. Info. 2008.

The Underlying Noisy Channel

Example: Single-Input Multi-output DMC



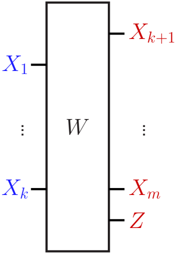


$$W = P_{X_2,\dots,X_m,Z|X_1}$$

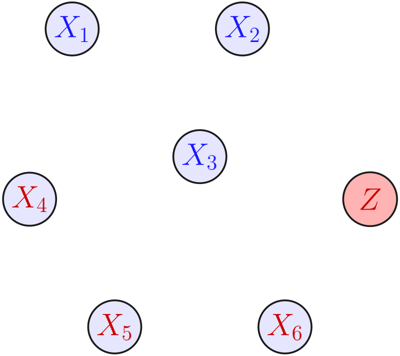
Csiszár and Narayan, "Secrecy Capacities for Multiterminal Channel Models", IEEE Trans. Info. 2008.

The Underlying Noisy Channel

Example: Multiaccess DMC

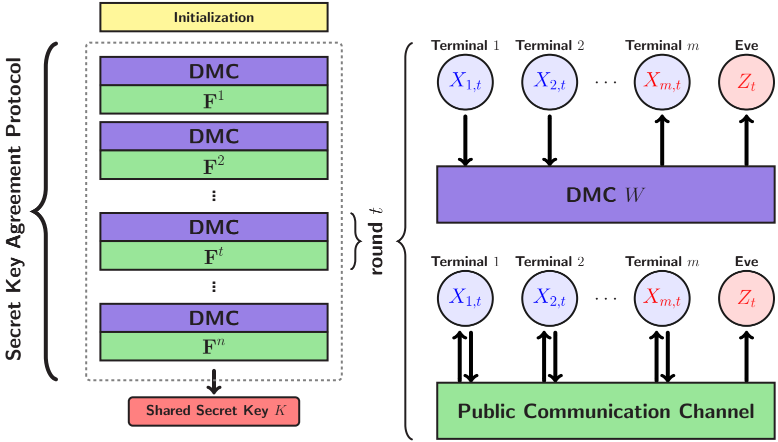


$$W = P_{X_{k+1},\ldots,X_m,Z|X_1,\ldots,X_k}$$



Csiszár and Narayan, "Secrecy Generation for Multiaccess Channel Models", IEEE Trans. Info. 2013.

UNIVERSITY OF CALGARY



Definition: K is an (ϵ, σ)-SK for $\mathcal{A} \subseteq \mathcal{M}$ if

$$\Pr\{K_j = K\} \geq 1 - \epsilon, \forall j \in \mathcal{A} \quad \text{(reliability)}$$

$$\mathbf{SD}((K, \mathbf{F}, Z); (U, \mathbf{F}, Z)) \leq \sigma \quad \text{(secrecy)}$$

where $\mathbf{SD}(X; Y) = \frac{1}{2} \sum_{w \in \mathcal{W}} |P_X(w) - P_Y(w)|$.

Definition - Key Capacity

Definition:

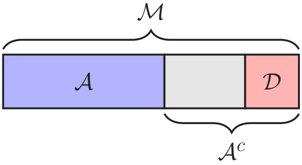
Let $K \in \mathcal{K}$ be an $(\epsilon_n, \sigma_n)-$SK with $\lim_{n\to\infty} \epsilon_n = \lim_{n\to\infty} \sigma_n = 0$.

Then, $\lim_{n\to\infty} \frac{1}{n} \log |\mathcal{K}| = R$ is an achievable **SK rate**.

The largest achievable key rate is called **key capacity**.

- **Adversarial model** (Csiszár & Narayan)

Eve has unbounded computational power, listens to the public communication, $\mathbf{F}$, and has access to random variable Z



1	**Secret Key (SK)**	$Z = \text{const.}$
2	**Private Key (PK)**	$Z = X_{\mathcal{D}}$
3	**Wiretap Secret Key (WSK)**	Any Z

$\mathcal{M}$ is the set of all terminals.

$\mathcal{A}$ is the target subset.

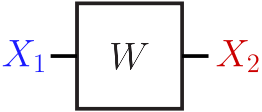
$\mathcal{A}^c$ is the set of helper terminals.

$\mathcal{D}$ is the set of compromised terminals.

Csiszár and Narayan, "Secrecy Capacities for Multiple Terminals," IEEE Trans. Inf. Theory, Dec. 2004.

Past Results

Past Results: Two-Party SKA



Theorem - Two-Party Secret Key (SK) Capacity [AC'93]

The SK capacity for two terminals is $C_{SK}(W) = \max_{P_{X_1}} I(X_1; X_2)$.

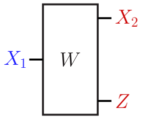
SKA Protocol

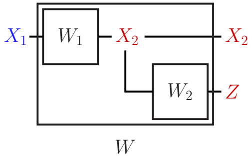
- Alice sends X_1^n, Bob receives X_2^n
- Alice sends message F, Bob recovers X_1^n (using F and X_2^n)
- Both parties extract a key K from X_1^n where $\log |\mathcal{K}| \approx nI(X_1; X_2)$

Ahlswede and Csiszár, "Common randomness in information theory and cryptography. I," IEEE Trans. Inf. Theory, 1993.

Finding a general expression for **WSK capacity**, even for the case of two terminals ($|\mathcal{M}| = 2$) is an **open problem**.

Past Results: Two-Party SKA





Theorem - Two-Party WSK Capacity [AC'93]

The two-party WSK capacity is bounded by

$$C_{WSK}(P_{ZX_2|X_1}) \leq \max_{P_{X_1}} I(X_1; X_2|Z),$$

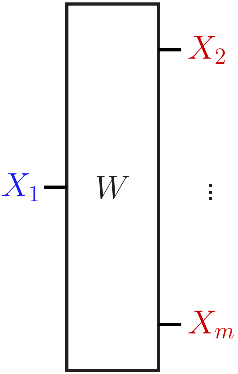
which is tight if $X_1 - X_2 - Z$ (degrade channels). Also, the noninteractive WSK capacity is

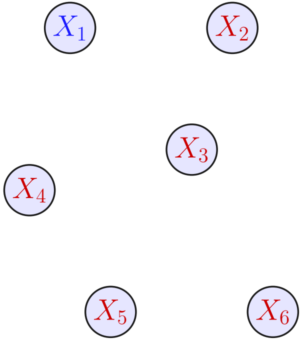
$$C_{NI-WSK} = \max_{P_{X_1}} \{I(X_1; X_2) - I(X_1; Z)\}.$$

Ahlswede and Csiszár, "Common randomness in information theory and cryptography. I," IEEE Trans. Inf. Theory, 1993.

SK and **PK** capacities

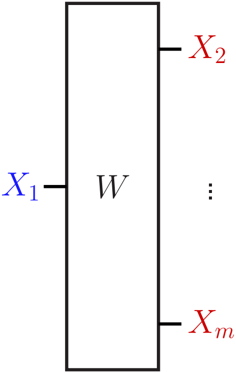
Past Results: Multiterminal SKA





Csiszár and Narayan, "Secrecy Capacities for Multiterminal Channel Models", IEEE Trans. Info. 2008.

Past Results: Multiterminal SKA



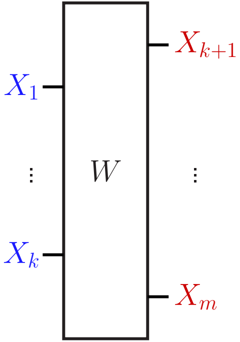
Single-input channel model

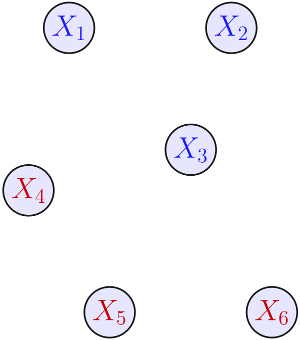
In [CN'08] general expressions for the SK and PK capacity of the single-input multi-output channel model were proved.

SK Capacity:	Yes
PK Capacity:	Yes

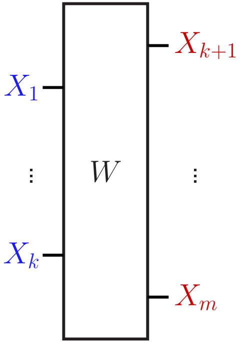
Csiszár and Narayan, "Secrecy Capacities for Multiterminal Channel Models", IEEE Trans. Info. 2008.

Past Results: Multiterminal SKA





Csiszár and Narayan, "Secrecy Generation for Multiaccess Channel Models", IEEE Trans. Info. 2013.



The multiaccess channel model

In [CN'13] upper and lower bounds for the SK and PK capacity of the multiaccess (multi-input multi-output) channel model were proved.

SK Capacity:	Upper and lower bound
PK Capacity:	Upper and lower bound

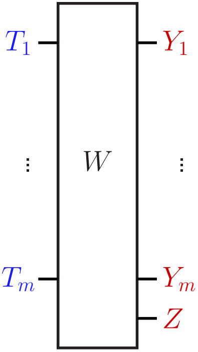
Csiszár and Narayan, "Secrecy Generation for Multiaccess Channel Models", IEEE Trans. Info. 2013.

Our Results

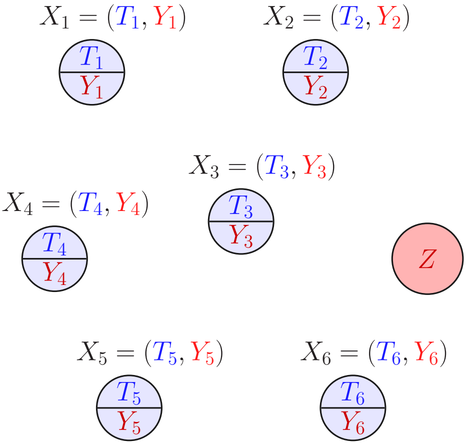
- **Our results:**

1. A **new multiterminal channel model** for SKA
2. General **upper and lower bounds** on **SK** and **PK** capacity
3. The **noninteractive SK capacity**
4. The **noninteractive WSK capacity of Polytree-PIN**

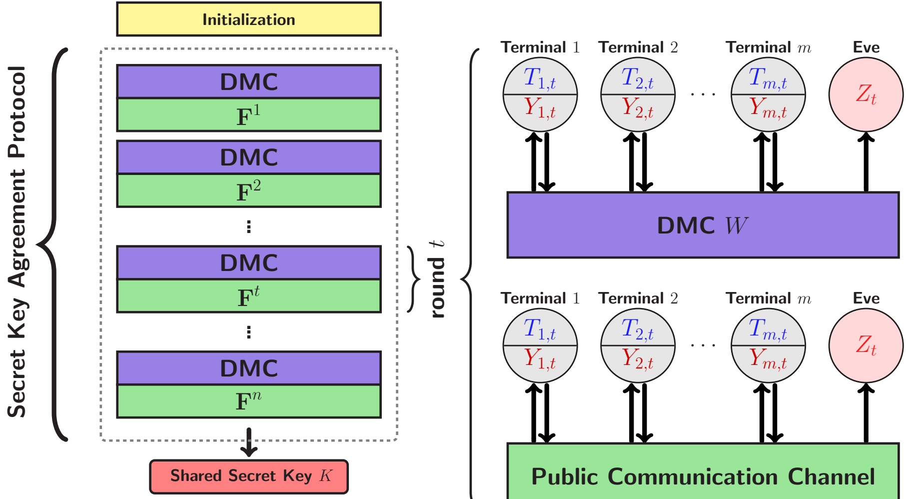
The Channel Model of Transceivers



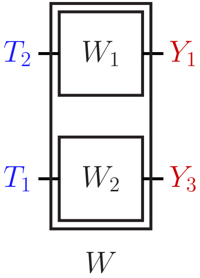
$$W = P_{ZY_{\mathcal{M}}|T_{\mathcal{M}}}$$

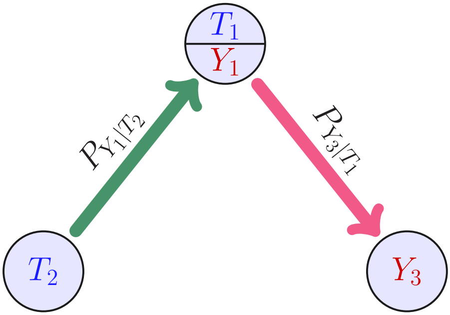


Our Model


Initialization
Secret Key Agreement Protocol
DMC
$\mathbf{F}^1$
DMC
$\mathbf{F}^2$
DMC
$\mathbf{F}^t$
DMC
$\mathbf{F}^n$
Shared Secret Key K
round t
Terminal 1
Terminal 2
Terminal m
Eve
$T_{1,t}$
$Y_{1,t}$
$T_{2,t}$
$Y_{2,t}$
$T_{m,t}$
$Y_{m,t}$
Z_t
DMC W
Terminal 1
Terminal 2
Terminal m
Eve
$T_{1,t}$
$Y_{1,t}$
$T_{2,t}$
$Y_{2,t}$
$T_{m,t}$
$Y_{m,t}$
Z_t
Public Communication Channel

Transceivers Model: examples





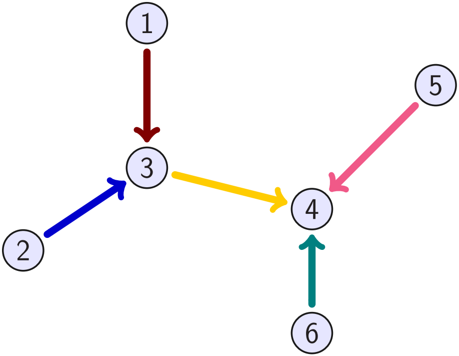
$$
\begin{aligned}
W &= P_{Y_{\mathcal{M}}|T_{\mathcal{M}}} \\
&= P_{Y_1|T_2} \cdot P_{Y_3|T_1}
\end{aligned}
$$

Transceivers Model: examples

Polytree-PIN

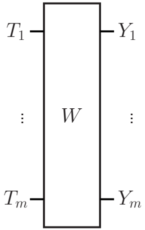
There exists a polytree $G = (\mathcal{M}, \mathcal{E})$ that defines the underlying noisy DMC as a pairwise independent network of point-to-point channels:

$$\begin{aligned} W &= P_{Y_{\mathcal{M}}|T_{\mathcal{M}}} \\ &= \prod_{e_{ij} \in \mathcal{E}} P_{Y_{ij}|T_{ji}} \end{aligned}$$



The Upper Bound

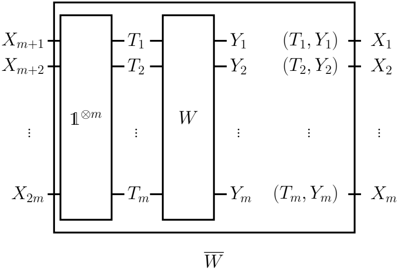
- Consider a given transceivers model $W = P_{Y_{\mathcal{M}}|T_{\mathcal{M}}}$
- Construct an associated multiaccess channel $\overline{W}$



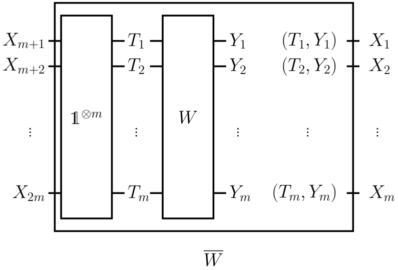
The Upper Bound

- Let $\mathcal{M}' = \{m+1, m+2, \ldots, 2m\}$ be the set of input terminals
- Let $\mathcal{M} = \{1, 2, \ldots, m\}$ be the set of output terminals
- For each $j \in \mathcal{M}$ let $X_j = (T_j, Y_j)$ and let $\overline{W}$ be given as follows:

$$
\begin{aligned}
\overline{W} &= P_{X_{\mathcal{M}}|X_{\mathcal{M}'}} \\
&= P_{Y_{\mathcal{M}}, T_{\mathcal{M}}|X_{\mathcal{M}'}} \\
&= P_{T_{\mathcal{M}}|X_{\mathcal{M}'}} \cdot P_{Y_{\mathcal{M}}|T_{\mathcal{M}}} \\
&= \Big(\prod_{j \in \mathcal{M}} P_{T_j|X_{j+m}} \Big) \cdot W \\
&= \Big(\prod_{j \in \mathcal{M}} \mathbb{1}(T_j = X_{j+m}) \Big) \cdot W
\end{aligned}
$$



UNIVERSITY OF CALGARY



Theorem - Upper Bound

For any given transceivers model $W = P_{Y_{\mathcal{M}}|T_{\mathcal{M}}}$ we have

$$C_{SK}^{\mathcal{A}}(W) \leq C_{SK}^{\mathcal{A}}(\overline{W}), \quad (1)$$

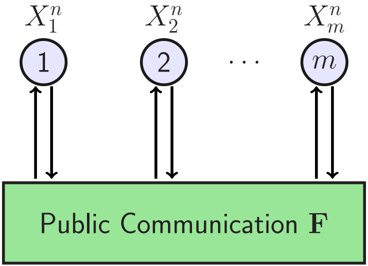
$$C_{PK}^{\mathcal{A}|\mathcal{D}}(W) \leq C_{PK}^{\mathcal{A}|\mathcal{D}}(\overline{W}). \quad (2)$$

Proof Idea:

Let Π be an SKA protocol that achieves an SK K in W. The SKA protocol Π can also be used in $\overline{W}$ to achieves the same SK K.

Recall: Source Model

- Correlated samples are observed
- Samples are IID with distribution $P_{X^n_{\mathcal{M}}} = (P_{X_{\mathcal{M}}})^n$
- The joint distribution $P_{X_{\mathcal{M}}}$ is known publicly
- Terminals use the public communication to establish the secret key K
- Largest achievable key rate is given by the source model key capacity



UNIVERSITY OF CALGARY

Recall: Source Model

- Largest achievable key rate is given by the source model key capacity

Theorem - Source model key capacity [CN'04]

In a given source model $P_{X_\mathcal{M}}$, the PK capacity is

$$C_{PK}^{\mathcal{A}|\mathcal{D}}(P_{X_\mathcal{M}}) = H(P_{X_\mathcal{M}}|P_{X_\mathcal{D}}) - R_{CO}^{\mathcal{A}|\mathcal{D}}(P_{X_\mathcal{M}}),$$

where $R_{CO}^{\mathcal{A}|\mathcal{D}}(P_{X_\mathcal{M}}) = \min_{R_{\mathcal{D}^c} \in \mathcal{R}_{CO}} \mathsf{sum}(R_{\mathcal{D}^c})$ and
$\mathcal{R}_{CO} = \{R_{\mathcal{D}^c} | \mathsf{sum}(R_\mathcal{B}) \geq H(P_{X_\mathcal{M}}|P_{X_{\mathcal{B}^c}}),\ \forall \mathcal{B} \subset \mathcal{D}^c, \mathcal{A} \nsubseteq \mathcal{B}\}$.

[CN'04] Csiszár and Narayan, "Secrecy Capacities for Multiple Terminals," IEEE Trans. Inf. Theory, Dec. 2004.

The Lower Bound

Theorem - Lower Bound

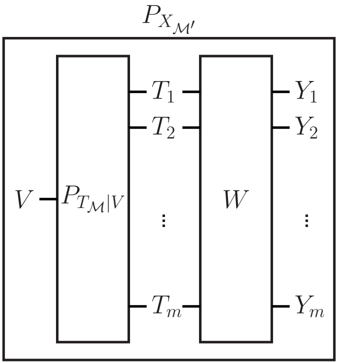
For any given transceivers model W, and for any random variable V satisfying $P_{V,T_{\mathcal{M}}} = P_V \Pi_{j \in \mathcal{M}} P_{T_j|V}$, we have

$$C_{SK}^{\mathcal{A}}(W) \geq C_{SK}^{\mathcal{A}|\{0\}}(P_{X_{\mathcal{M}'}}), \qquad (3)$$

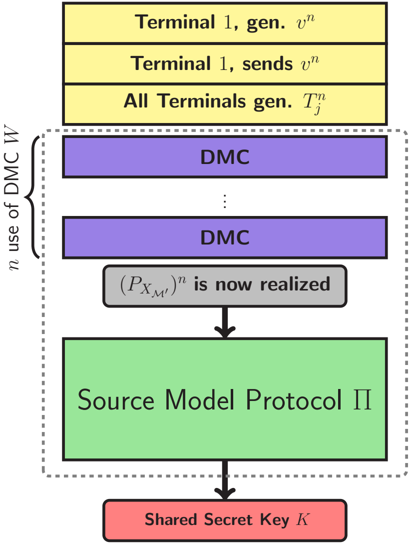
and

$$C_{PK}^{\mathcal{A}|\mathcal{D}}(W) \geq C_{PK}^{\mathcal{A}|\mathcal{D}'}(P_{X_{\mathcal{M}'}}), \qquad (4)$$

where $P_{X_{\mathcal{M}'}} = P_{VT_{\mathcal{M}}} P_{Y_{\mathcal{M}}|T_{\mathcal{M}}}$ denotes the associated source model with $m+1$ terminals, $\mathcal{M}' = \{0, 1, \ldots, m\}$, where $\mathcal{D}' = \mathcal{D} \cup \{0\}$, and $X_0 = V$.



UNIVERSITY OF CALGARY



Proof Idea: Source Emulation

Let Π be a source model SKA protocol that achieves the source model key capacity of $P_{X_{\mathcal{M}'}}$. We emulate (realize) $(P_{X_{\mathcal{M}'}})^n$, and use protocol Π to achieve a secret key $K \in \mathcal{K}$ such that, the key rate, $\frac{1}{n} \log |\mathcal{K}|$, approaches the source model capacity of $P_{X_{\mathcal{M}'}}$ as $n \to \infty$.

UNIVERSITY OF CALGARY

Definition - The Noninteractive Capacity

Consider the following limitations

(a) Noninteractive Communication. Only after all symbol transmissions over the DMC, terminals each send a single message over the public channel in one round. In this case, $\mathbf{F} = \mathbf{F}^n = (F_1, \ldots, F_m)$, where F_j denotes the public message of terminal j which is only a function of X_j^n (not other messages).

(b) Independent Inputs. Terminals are locally controlling their input variables, and the input variables are independent, i.e., $P_{T_{\mathcal{M}}} = \Pi_{j \in \mathcal{M}} P_{T_j}$.

The **noninteractive secret key capacity**, is defined as the largest achievable key rate of all SKA protocols satisfying (a) and (b), above; and is denoted by $C_{NI-SK}^{\mathcal{A}}(P_{Y_{\mathcal{M}}|T_{\mathcal{M}}})$.

Definition - The Noninteractive Capacity

Consider the following limitations

(a) Noninteractive Communication.

(b) Independent Inputs.

$P_{T_\mathcal{M}} = \Pi_{j \in \mathcal{M}} P_{T_j}$.

The **noninteractive secret key capacity**, is defined as the largest achievable key rate of all SKA protocols satisfying (a) and (b), above; and is denoted by $C^{\mathcal{A}}_{NI-SK}(P_{Y_\mathcal{M}|T_\mathcal{M}})$.

UNIVERSITY OF CALGARY

Theorem - Noninteractive capacity

Given any transceivers model $W = P_{Y_{\mathcal{M}}|T_{\mathcal{M}}}$, we have

$$C^{\mathcal{A}}_{NI-SK}(W) = \max_{P_{T_{\mathcal{M}}}} C^{\mathcal{A}}_{SK}(P_{T_{\mathcal{M}}} P_{Y_{\mathcal{M}}|T_{\mathcal{M}}}). \tag{5}$$

Proof Idea:

Converse: By our upper bound, the capacity of W is upper bounded by the capacity of an associated multiaccess model. We, then, use the upper bound given in [CN'13] for multiaccess models, and simplify it to RHS of Eq.(5) using the noninteractivity assumptions (a) and (b).

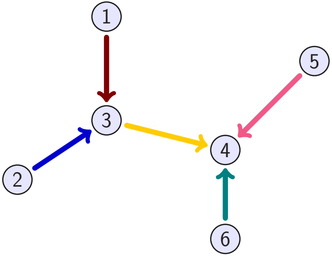
Achievability: Use the source emulation approach with $V = \text{constant}$.

Csiszár and Narayan, "Secrecy Generation for Multiaccess Channel Models", IEEE Trans. Info. 2013.

Polytree-PIN

There exists a polytree $G = (\mathcal{M}, \mathcal{E})$ that defines the underlying noisy DMC as:

$$W = P_{Y_{\mathcal{M}}|T_{\mathcal{M}}} = \prod_{e_{ij} \in \mathcal{E}} P_{Y_{ij}|T_{ji}}$$



Corollary - Noninteractive Capacity of Polytree-PIN

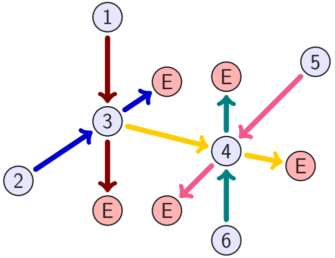
Given any Polytree-PIN model W, we have

$$C^{\mathcal{A}}_{NI-SK}(W) = \max_{P_{T_{\mathcal{M}}}} \min_{\substack{i,j \in \mathcal{M} \\ \text{s.t. } e_{ij} \in \mathcal{E}}} I(T_{ij}; Y_{ji}). \tag{6}$$

Wiretapped Polytree-PIN

There exists a polytree $G = (\mathcal{M}, \mathcal{E})$ that defines the underlying noisy DMC as:

$$\begin{aligned} W &= P_{ZY_{\mathcal{M}}|T_{\mathcal{M}}} \\ &= \prod_{e_{ij} \in \mathcal{E}} P_{Y_{ij}|T_{ji}} P_{Z_{ij}|Y_{ji}} \end{aligned}$$

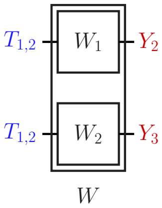


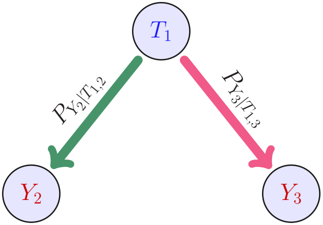
Theorem - Noninteractive WSK Capacity of Polytree-PIN

Given any Wiretapped Polytree-PIN model W, we have

$$C^{\mathcal{A}}_{NI-WSK}(W) = \max_{P_{T_{\mathcal{M}}}} \min_{\substack{i,j \in \mathcal{M} \\ \text{s.t. } e_{ij} \in \mathcal{E}}} I(T_{ij}; Y_{ji} | Z_{ij}). \tag{7}$$

Polytree-PIN Example 1: Single-input Model



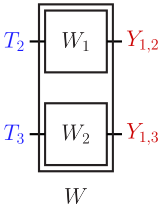


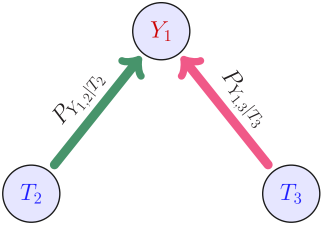
Capacity	Results [CN'08]
SK	Exact
PK	Exact
NI-SK	Exact

Csiszár and Narayan, "Secrecy Capacities for Multiterminal Channel Models", IEEE Trans. Info. 2008.

UNIVERSITY OF CALGARY

Polytree-PIN Example 2: Multiaccess Model

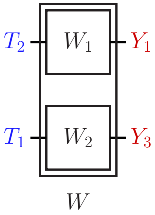


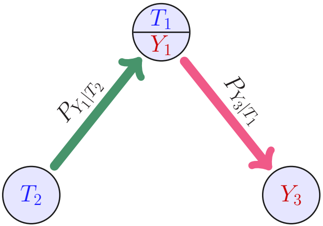


Capacity	Results [CN'13]
SK	Bounds
PK	Bounds
NI-SK	Exact

Csiszár and Narayan, "Secrecy Generation for Multiaccess Channel Models", IEEE Trans. Info. 2013.

Polytree-PIN Example 3: Transceivers Model





Capacity	Our Results
SK	Bounds
PK	Bounds
NI-SK	Exact
NI-WSK	Polytree-PINs

Future Directions

- Finding tighter bounds for the SK and PK capacities
- Finding the WSK capacity of wiretapped Polytree-PIN
- Investigating interactive SKA protocols

Thanks for your attention!