情報理論的暗号の最近の発展と未解決問題

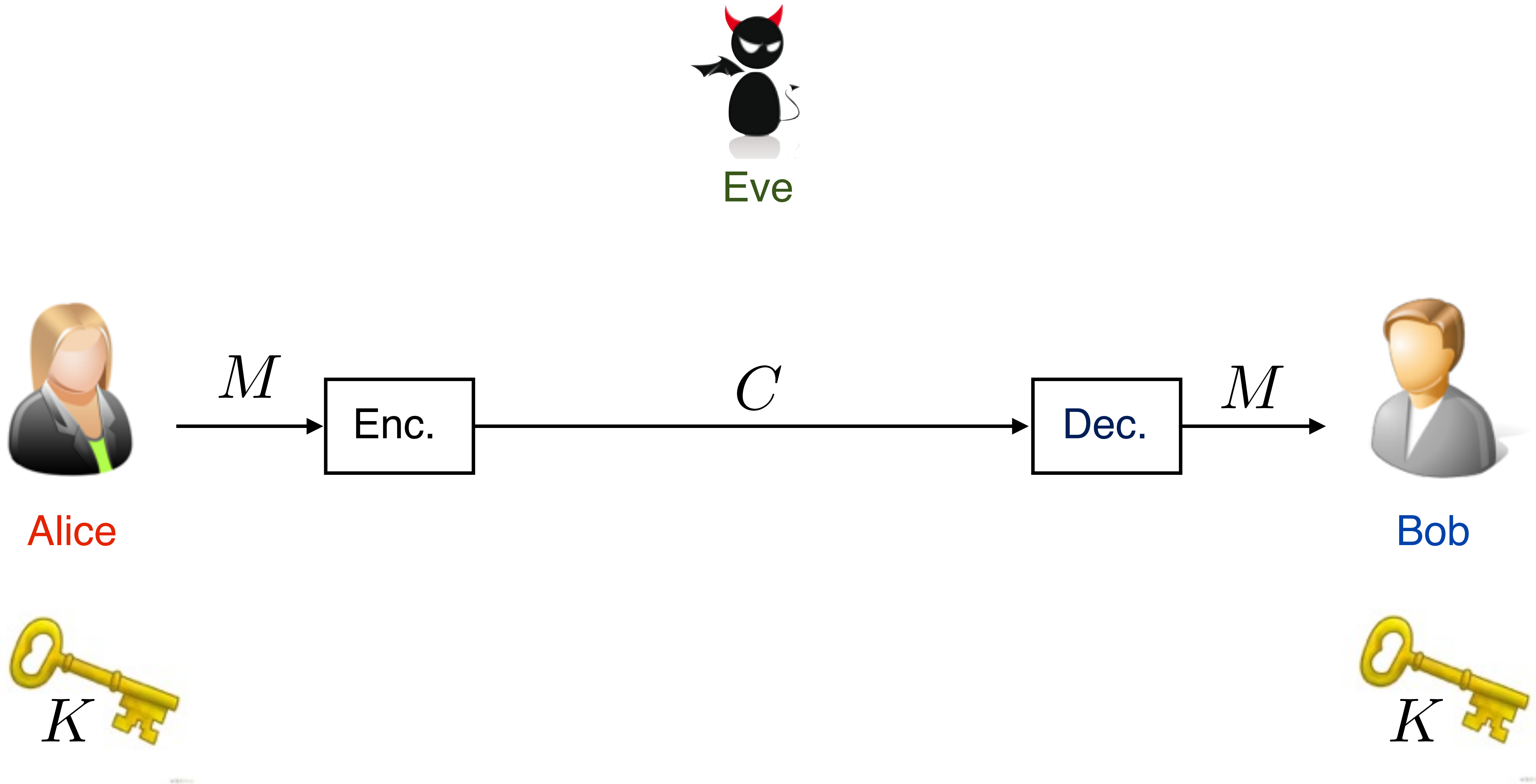
IT研究会＠泉慶

November, 2017

渡辺　峻 (東京農工大)

joint work with Himanshu Tyagi (IISc Bangalore)

Secret Key Cryptography



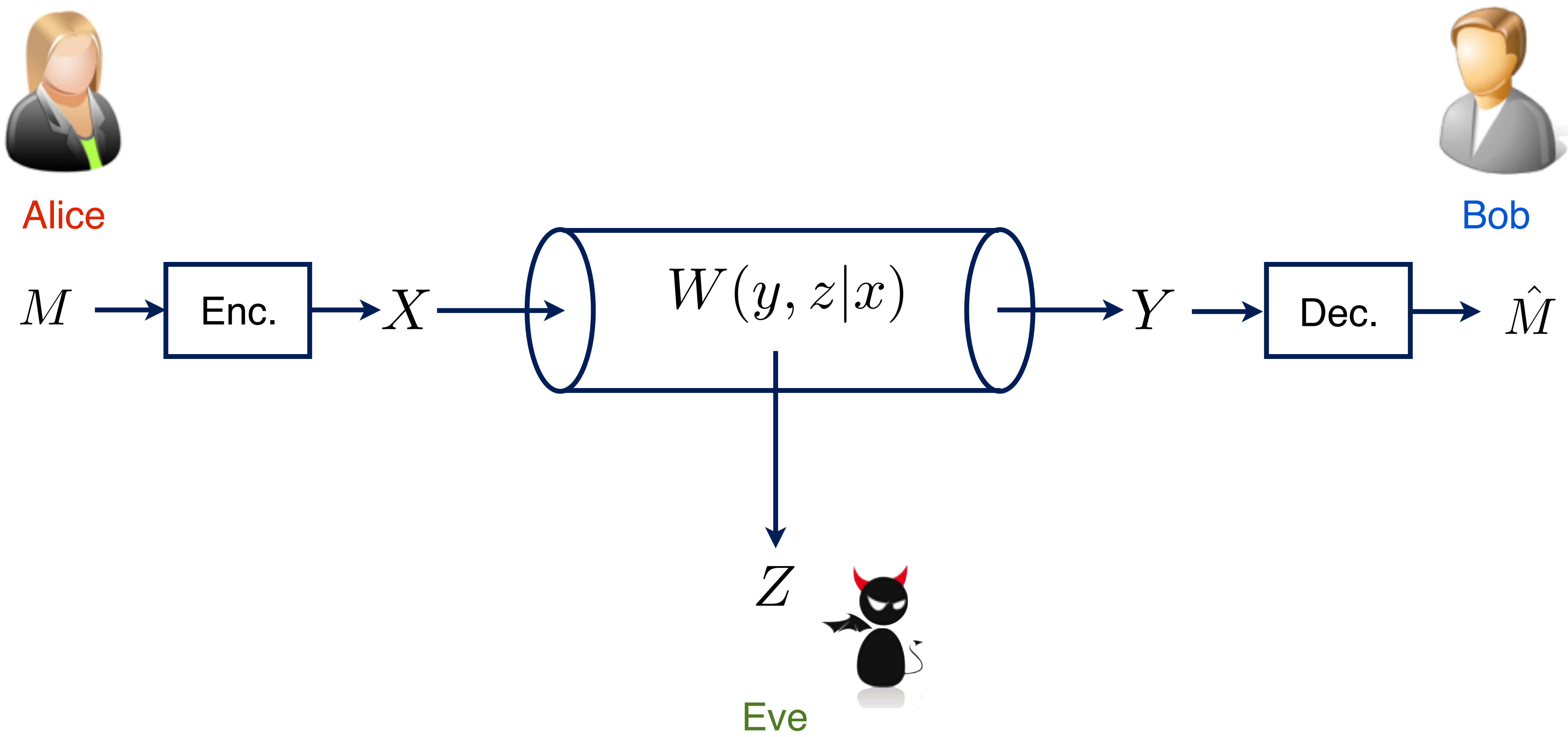
Shannon's Pessimistic Result

A secret key crypto system is secure only if

$$H(K) \geq H(M)$$

Key length must be as large as message length…

Wyner's Wiretap Channel



$W(y,z|x) = W_1(y|x)W_2(z|y)$: Degraded Wiretap Channel [Wyner 75]

General wiretap channel [Csiszár-Körner]

Secret Key Agreement: Model

[Maurer 93, Ahlswede-Csiszár 93]

Eve

Z

Alice

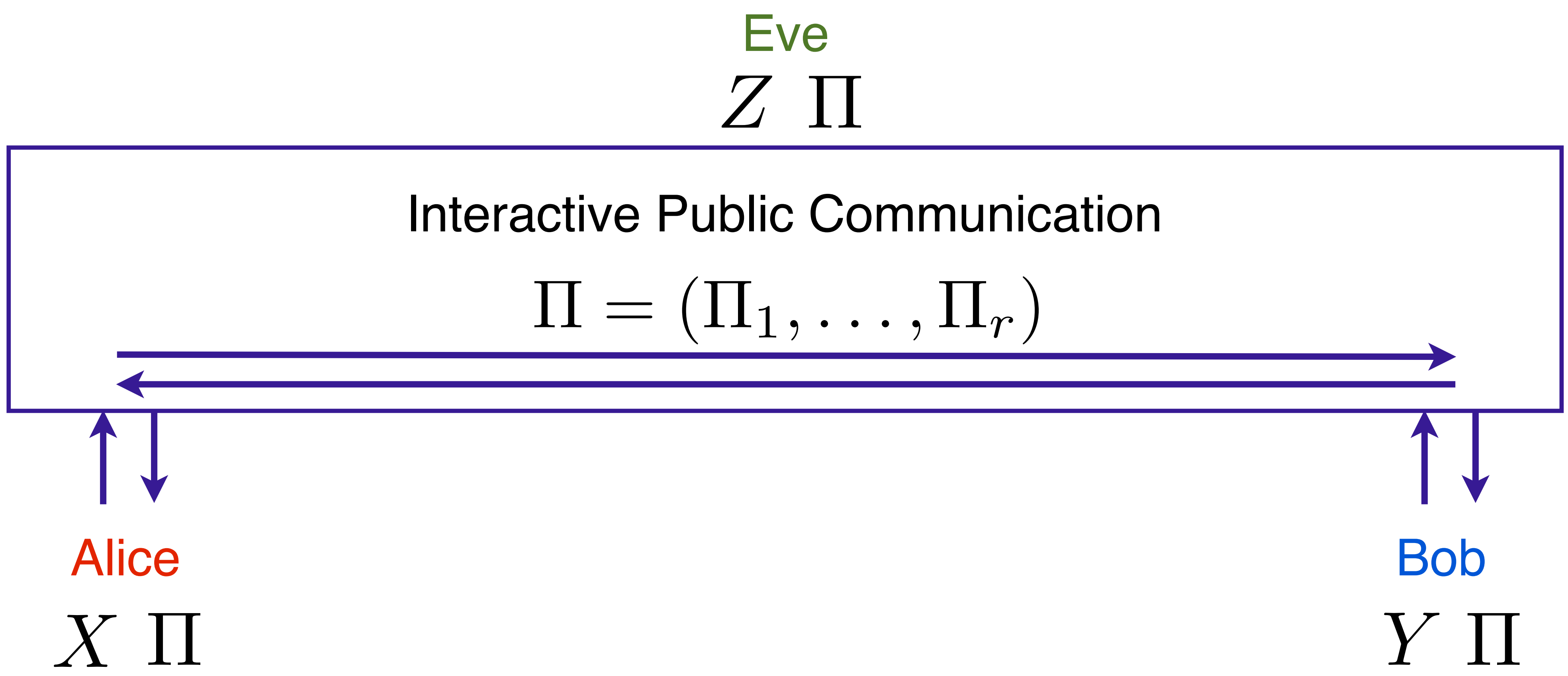
X

Bob

Y

Secret Key Agreement: Protocol

[Maurer 93, Ahlswede-Csiszár 93]



$$\Pi_1 = \Pi_1(X)$$

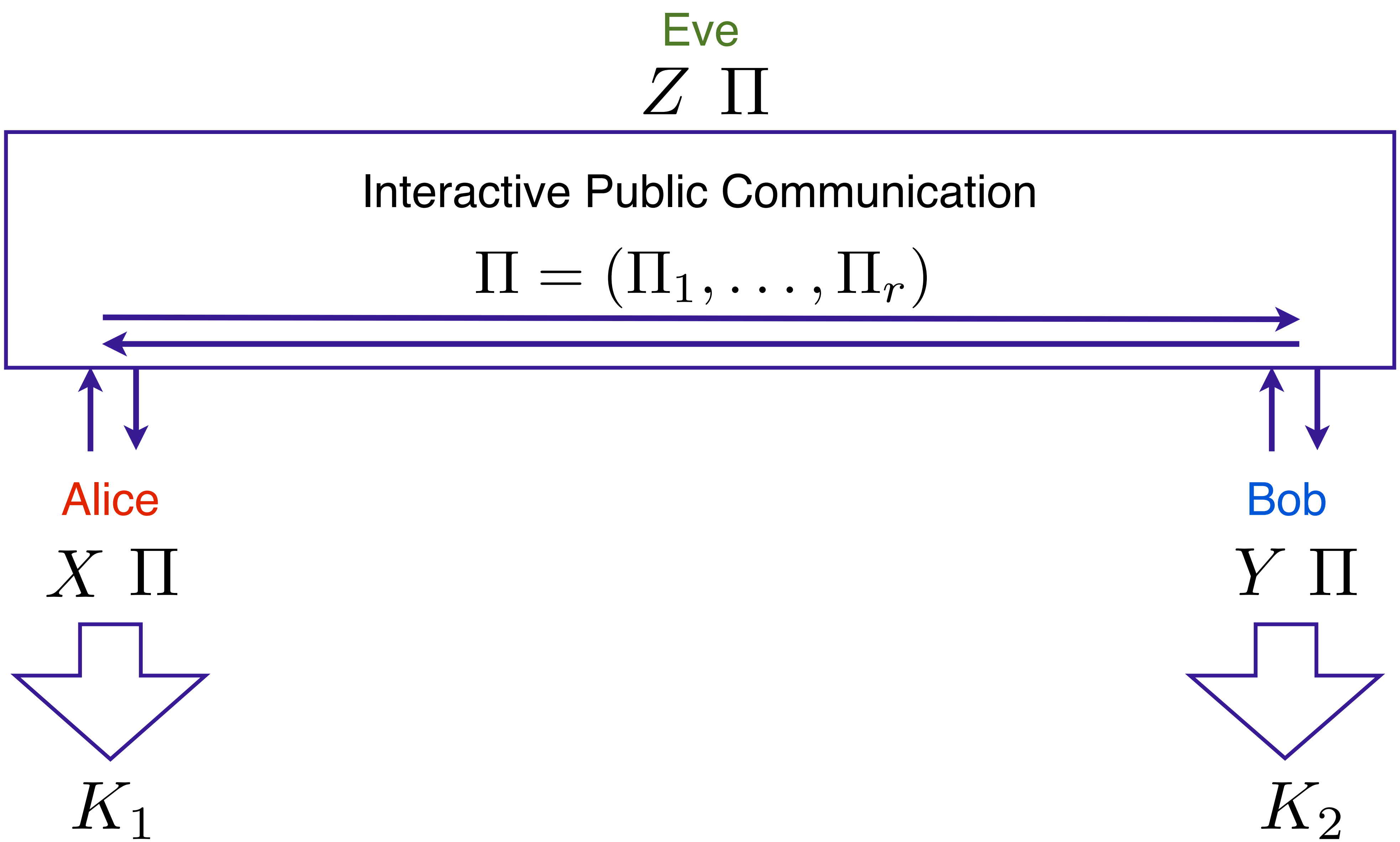
$$\Pi_2 = \Pi_2(Y, \Pi_1)$$

$$\vdots$$

$$\Pi_r = \Pi_r(Y, \Pi_1, \ldots, \Pi_{r-1})$$

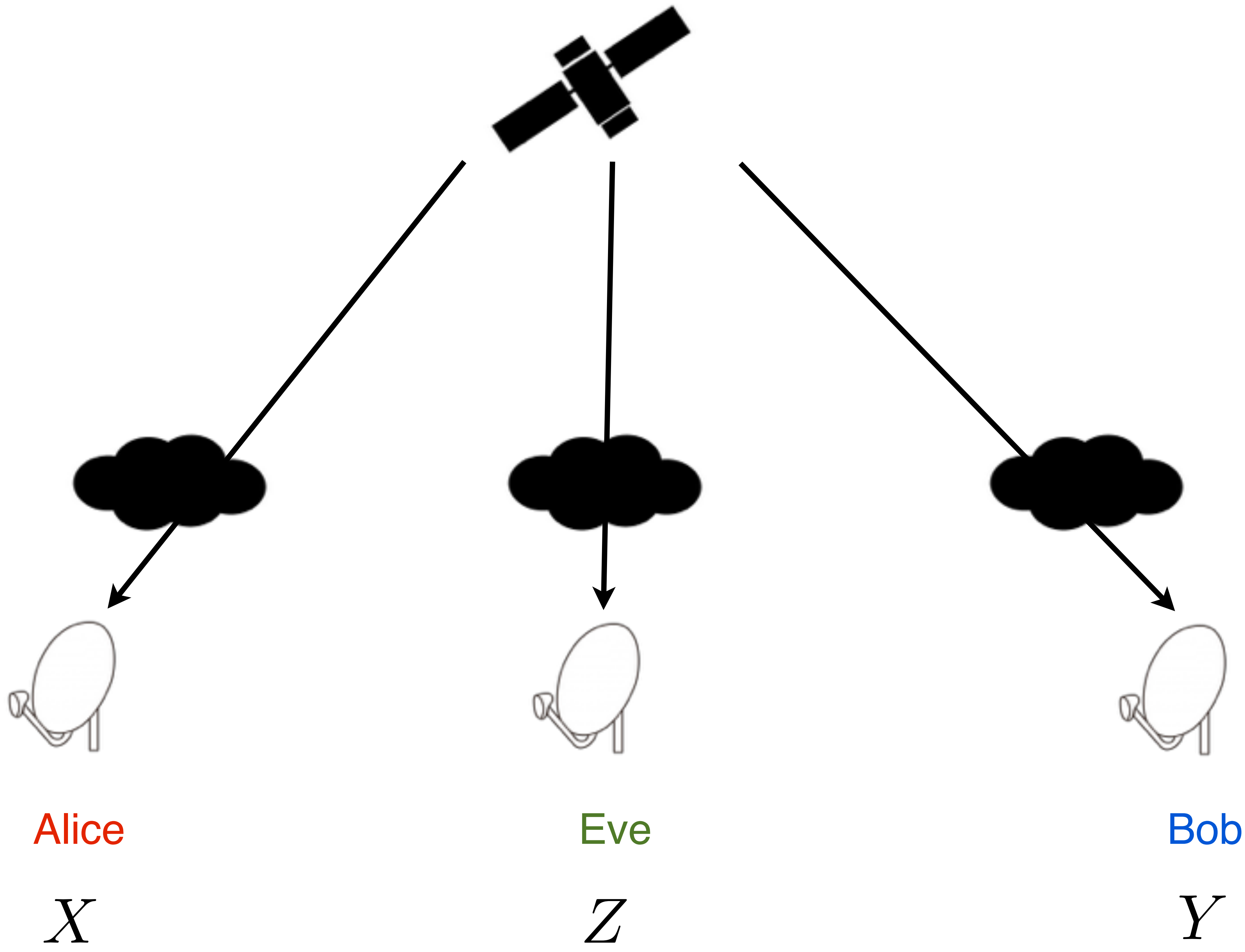
Secret Key Agreement: Protocol

[Maurer 93, Ahlswede-Csiszár 93]

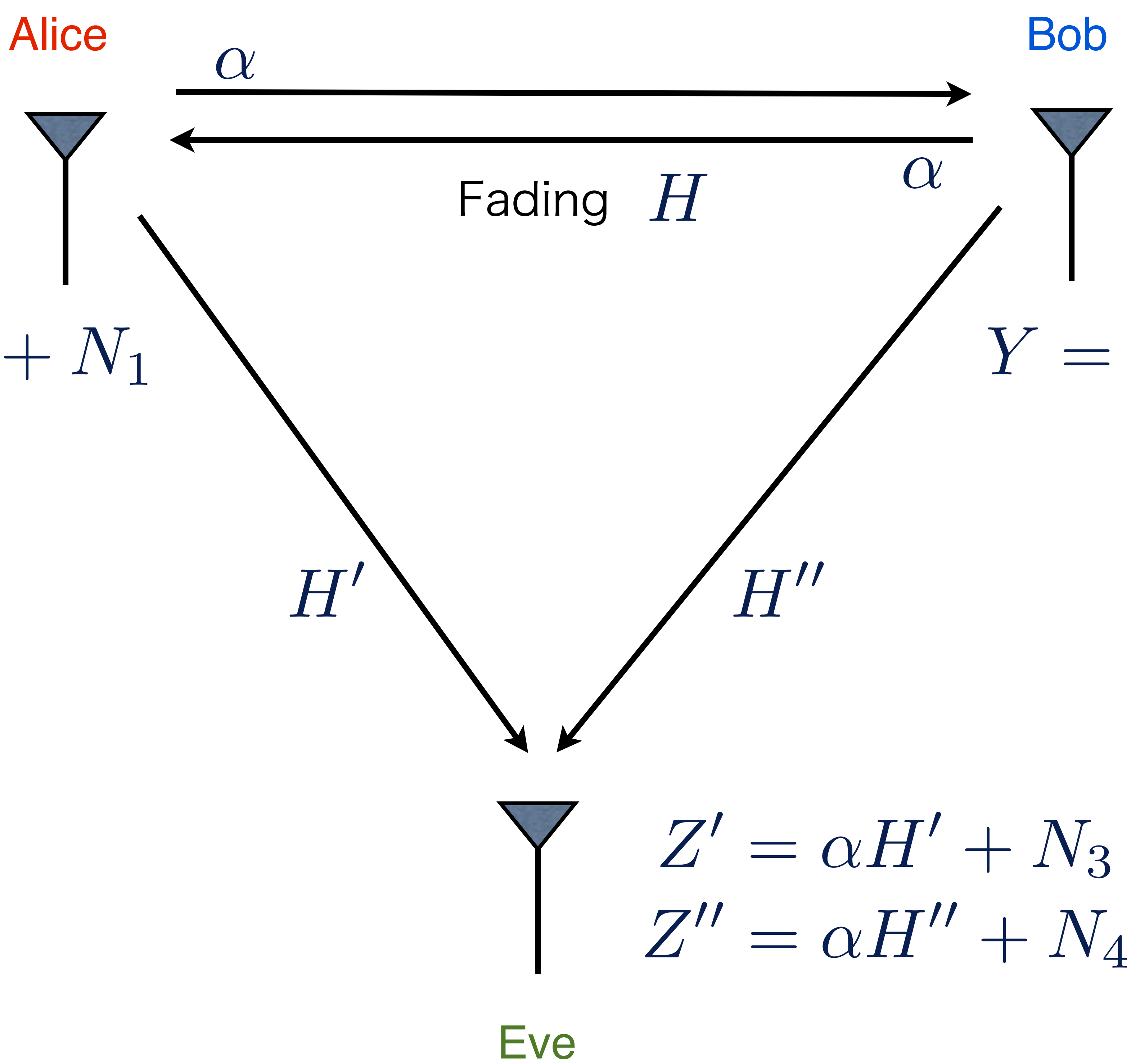


$$K_1 = K_1(X, \Pi) \qquad\qquad K_2 = K_2(Y, \Pi)$$

Example 1: Maurer’s Satellite Model



Example 2: Fading of Wireless Communication



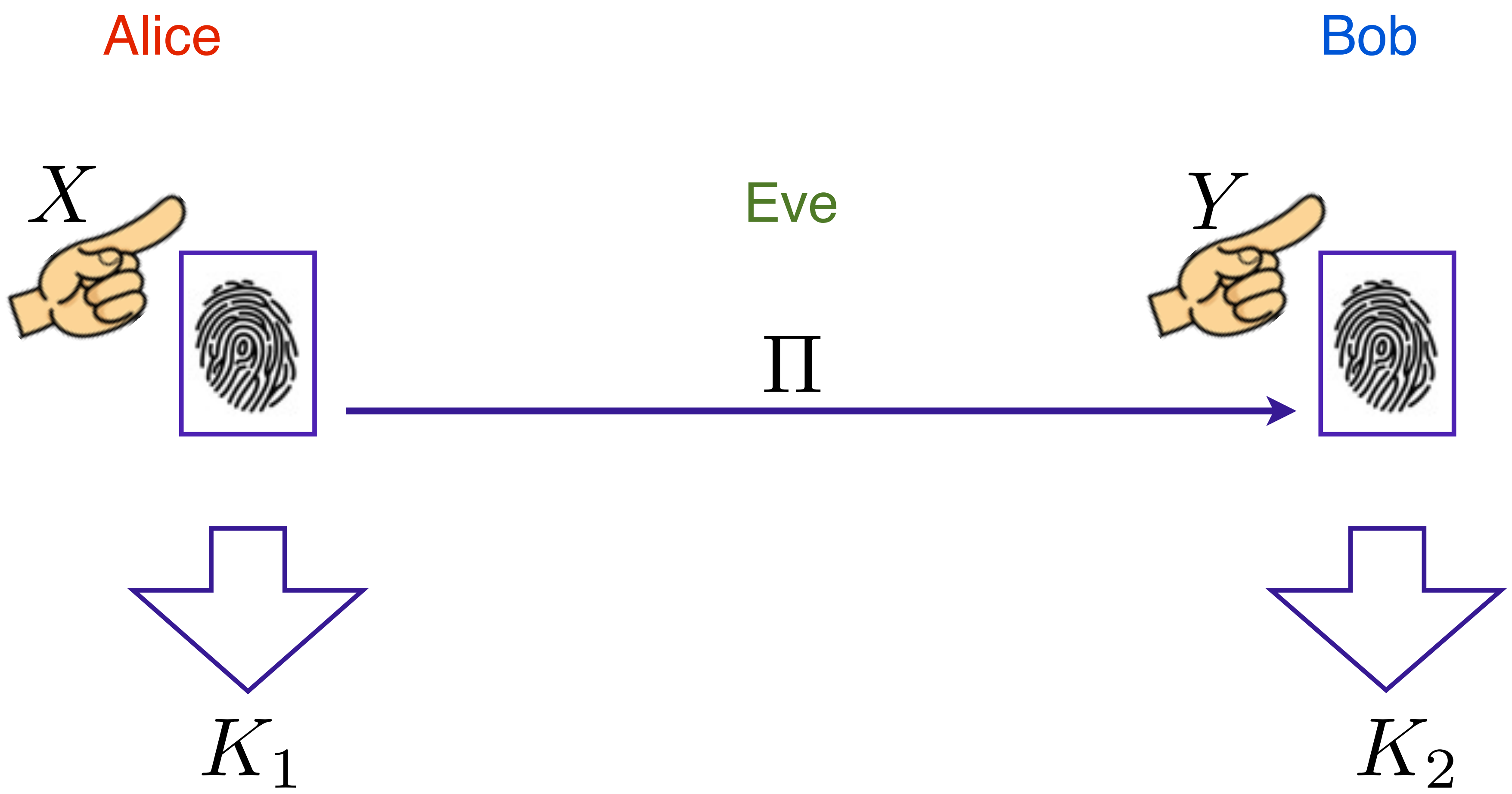
$$X = \alpha H + N_1$$

$$Y = \alpha H + N_2$$

$$Z' = \alpha H' + N_3$$
$$Z'' = \alpha H'' + N_4$$

[Hassan et. al. '96]

Example 3: Fuzzy Extractor (Biometric Security)



[Dodis et. al. 04]

Problem Formulation of SK

The generate key is (ε, δ)-SK $(0 \le \varepsilon, \delta < 1)$ if there exists K such that

Reliability $\Pr\{K_1 = K_2 = K\} \ge 1 - \varepsilon$

Security $d(P_{K\Pi Z}, P_{\mathtt{unif}} \times P_{\Pi Z}) \le \delta$

$$d(P, Q) := \frac{1}{2} \sum_a |P(a) - Q(a)|$$

$P_{\Pi Z}$: marginal of $P_{K\Pi Z}$

$$P_{\text{unif}}(k) = \frac{1}{|\mathcal{K}|}$$

Problem Formulation of SK

The generate key is (ε, δ)-SK $(0 \le \varepsilon, \delta < 1)$ if there exists K such that

Reliability $\Pr\{K_1 = K_2 = K\} \ge 1 - \varepsilon$

Security $d(P_{K\Pi Z}, P_{\mathtt{unif}} \times P_{\Pi Z}) \le \delta$

$$d(P, Q) := \frac{1}{2} \sum_a |P(a) - Q(a)|$$

$P_{\Pi Z}$: marginal of $P_{K\Pi Z}$

$$P_{\mathrm{unif}}(k) = \frac{1}{|\mathcal{K}|}$$

$S_{\varepsilon,\delta}(X, Y|Z)$:maximum $\log |\mathcal{K}|$ such that a protocol generating (ε, δ)-SK exists

Secret Key Capacity

For i.i.d. observations $\{(X^n, Y^n, Z^n)\}_{n=1}^{\infty}$,

$$C(X, Y|Z) := \lim_{\varepsilon,\delta \to 0} \liminf_{n \to \infty} \frac{1}{n} S_{\varepsilon,\delta}(X^n, Y^n|Z^n)$$

Secret Key Capacity

For i.i.d. observations $\{(X^n, Y^n, Z^n)\}_{n=1}^{\infty}$,

$$C(X, Y|Z) := \lim_{\varepsilon,\delta \to 0} \liminf_{n\to\infty} \frac{1}{n} S_{\varepsilon,\delta}(X^n, Y^n|Z^n)$$

Basic lower (achievability) bound:

$$C(X, Y|Z) \geq H(X|Z) - H(X|Y)$$

Basic upper (converse) bound:

$$C(X, Y|Z) \leq I(X \wedge Y|Z)$$

Secret Key Capacity

For i.i.d. observations $\{(X^n, Y^n, Z^n)\}_{n=1}^{\infty}$,

$$C(X,Y|Z) := \lim_{\varepsilon,\delta\to 0} \liminf_{n\to\infty} \frac{1}{n} S_{\varepsilon,\delta}(X^n, Y^n|Z^n)$$

Basic lower (achievability) bound:

$$C(X,Y|Z) \geq H(X|Z) - H(X|Y)$$

Basic upper (converse) bound:

$$C(X,Y|Z) \leq I(X \wedge Y|Z)$$

Theorem [Maurer 93, Ahlswede-Csiszár 93]

When $X -\!\!\circ\!\!- Y -\!\!\circ\!\!- Z$ holds,

$$C(X,Y|Z) = I(X \wedge Y|Z)$$

In particular,

$$C(X,Y) = I(X \wedge Y)$$

Idea of achievability

- Information reconciliation

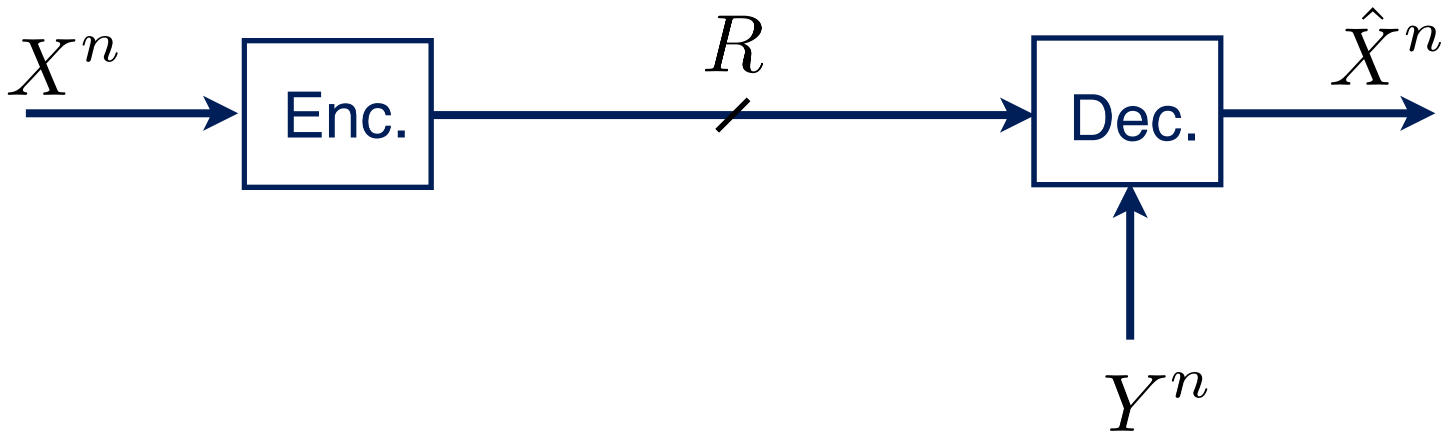
  share a common random variable

- Privacy amplification

  extract a secret key

Information Reconciliation

Use Slepian-Wolf coding:



If $R > H(X|Y)$, there exists a code such that $\Pr\{X^n \neq \hat{X}^n\} \to 0$

Privacy Amplification

Alice and Bob shall generate secret key from X when Z is known to Eve.

Definition (2-Universal hash family)

A random function $F : \mathcal{X} \to \{0,1\}^l$ is called 2-UHF if

$$\mathrm{P}\big(F(x) = F(x')\big) \leq \frac{1}{2^l}, \quad \forall x \neq x' \in \mathcal{X}$$

eg)

- the set of all functions from $\mathcal{X}$ to $\{0,1\}^l$
- the set of all linear functions from $\mathcal{X}$ to $\{0,1\}^l$

Privacy Amplification

Definition (Conditional min-entropy)

For P_{XZ} and Q_Z, the conditional min-entropy of P_{XZ} given Q_Z is

$$H_{\min}(P_{XZ}|Q_Z) := \min_{x \in \mathcal{X}, z \in \mathtt{supp}(Q_Z)} \log \frac{Q_Z(z)}{P_{XZ}(x,z)}$$

Then, the conditional min-entropy of P_{XZ} given Z is

$$H_{\min}(P_{XZ}|Z) := \max_{Q_Z} H_{\min}(P_{XZ}|Q_Z)$$

Privacy Amplification

Definition (Conditional min-entropy)

For P_{XZ} and Q_Z, the conditional min-entropy of P_{XZ} given Q_Z is

$$H_{\min}(P_{XZ}|Q_Z) := \min_{x \in \mathcal{X}, z \in \mathtt{supp}(Q_Z)} \log \frac{Q_Z(z)}{P_{XZ}(x,z)}$$

Then, the conditional min-entropy of P_{XZ} given Z is

$$H_{\min}(P_{XZ}|Z) := \max_{Q_Z} H_{\min}(P_{XZ}|Q_Z)$$

The closed form (-log of success guessing probability):

$$H_{\min}(P_{XZ}|Z) = -\log \sum_z P_Z(z) \max_x P_{X|Z}(x|z)$$

$$Q_Z^*(z) \propto P_Z(z) \max_x P_{X|Z}(x|z)$$

Leftover Hash Lemma

The following bound is useful (cf. [Impagliazzo-Levin-Luby 89, Renner 05]).

Theorem (Leftover Hash Lemma)

For 2-UHF F , $K = F(X)$ satisfies

$$d(P_{KZF}, P_{\mathtt{unif}} \times P_Z \times P_F) \leq \frac{1}{2}\sqrt{2^{l - H_{\min}(P_{XZ}|Z)}}$$

Leftover Hash Lemma

The following bound is useful (cf. [Impagliazzo-Levin-Luby 89, Renner 05]).

Theorem (Leftover Hash Lemma)

For 2-UHF F , $K = F(X)$ satisfies

$$d(P_{KZF}, P_{\mathtt{unif}} \times P_Z \times P_F) \leq \frac{1}{2}\sqrt{2^{l - H_{\min}(P_{XZ}|Z)}}$$

δ -secure secret key of length

$$H_{\min}(P_{XZ}|Z) - 2\log(1/2\delta)$$

can be generated.

Leftover Hash Lemma

The following bound is useful (cf. [Impagliazzo-Levin-Luby 89, Renner 05]).

Theorem (Leftover Hash Lemma)

For 2-UHF F , $K = F(X)$ satisfies

$$d(P_{KZF}, P_{\mathtt{unif}} \times P_Z \times P_F) \le \frac{1}{2}\sqrt{2^{l - H_{\min}(P_{XZ}|Z)}}$$

δ -secure secret key of length

$$H_{\min}(P_{XZ}|Z) - 2\log(1/2\delta)$$

can be generated.

Typically, this bound is loose…; for i.i.d.,

$$\frac{1}{n}H_{\min}(P^n_{XZ}|Z^n) = H_{\min}(P_{XZ}|Z) < H(X|Z)$$

Smoothing

Smoothing: $P_{XZ} \to \tilde{P}_{XZ}$ under the condition $d(\tilde{P}_{XZ}, P_{XZ}) \le \delta$

(allow sub-normalized distribution)

We allow sub-normalized distribution since we typically choose truncated distribution

$$\tilde{P}_{XZ}(x,z) = P_{XZ}(x,z)\mathbf{1}[(x,z) \in \mathcal{T}]$$

for some $\mathcal{T}$ with

$$P_{XZ}(\mathcal{T}) \ge 1 - 2\delta$$

Smooth Conditional Min-Entropy

Definition (Smooth conditional min-entropy)

For P_{XZ} and Q_Z, the smooth conditional min-entropy of P_{XZ} given Q_Z is

$$H_{\min}^{\delta}(P_{XZ}|Q_Z) := \max_{\tilde{P}_{XZ} \in \mathcal{B}_\delta(P_{XZ})} H_{\min}(\tilde{P}_{XZ}|Q_Z)$$

$$\mathcal{B}_\delta(P_{XZ}) := \{\tilde{P}_{XZ} \in \mathcal{P}_{\mathsf{sub}}(\mathcal{X} \times \mathcal{Z}) : d(\tilde{P}_{XZ}, P_{XZ}) \leq \delta\}$$

Then, the smooth conditional min-entropy of P_{XZ} given Z is

$$H_{\min}^{\delta}(P_{XZ}|Z) := \max_{Q_Z} H_{\min}^{\delta}(P_{XZ}|Q_Z)$$

Leftover Hash Lemma with Smoothing

Apply triangular inequality for smoothed distribution…

Theorem (Leftover Hash Lemma with smoothing)

For 2-UHF F , $K = F(X)$ satisfies

$$d(P_{KZF}, P_{\mathtt{unif}} \times P_Z \times P_F) \leq 2\delta + \frac{1}{2}\sqrt{2^{l - H_{\min}^{\delta}(P_{XZ}|Z)}}$$

Leftover Hash Lemma with Smoothing

Apply triangular inequality for smoothed distribution…

Theorem (Leftover Hash Lemma with smoothing)

For 2-UHF F , $K = F(X)$ satisfies

$$d(P_{KZF}, P_{\mathtt{unif}} \times P_Z \times P_F) \le 2\delta + \frac{1}{2}\sqrt{2^{l - H_{\min}^{\delta}(P_{XZ}|Z)}}$$

δ -secure secret key of length

$$H_{\min}^{(\delta-\eta)/2}(P_{XZ}|Z) - 2\log(1/2\eta) - 1$$

can be generated for $0 < \eta \le \delta$.

Leftover Hash Lemma with Smoothing

Apply triangular inequality for smoothed distribution…

Theorem (Leftover Hash Lemma with smoothing)

For 2-UHF F , $K = F(X)$ satisfies

$$d(P_{KZF}, P_{\mathtt{unif}} \times P_Z \times P_F) \le 2\delta + \frac{1}{2}\sqrt{2^{l - H_{\min}^{\delta}(P_{XZ}|Z)}}$$

δ -secure secret key of length

$$H_{\min}^{(\delta-\eta)/2}(P_{XZ}|Z) - 2\log(1/2\eta) - 1$$

can be generated for $0 < \eta \le \delta$.

For i.i.d. observation,

$$\lim_{n\to\infty} \frac{1}{n} H_{\min}^{(\delta-\eta)/2}(P_{XZ}^n|Z^n) = H(X|Z)$$

for $0 < \eta < \delta$.

Leftover Hash Lemma with Extra Message

The following variant of LHL for P_{XZV} is useful for later application:

Theorem (Leftover Hash Lemma with extra message)

For 2-UHF F , $K = F(X)$ satisfies

$$d(P_{KVZF}, P_{\mathtt{unif}} \times P_{VZ} \times P_F) \leq 2\delta + \frac{1}{2}\sqrt{|\mathcal{V}| 2^{l - H^{\delta}_{\min}(P_{XZ}|Z)}}$$

Leftover Hash Lemma with Extra Message

The following variant of LHL for P_{XZV} is useful for later application:

Theorem (Leftover Hash Lemma with extra message)

For 2-UHF F , $K = F(X)$ satisfies

$$d(P_{KVZF}, P_{\mathtt{unif}} \times P_{VZ} \times P_F) \le 2\delta + \frac{1}{2}\sqrt{|\mathcal{V}| 2^{l - H_{\min}^{\delta}(P_{XZ}|Z)}}$$

δ -secure secret key of length

$$H_{\min}^{(\delta-\eta)/2}(P_{XZ}|Z) - 2\log(1/2\delta) - 1 - \log|\mathcal{V}|$$

for $0 < \eta \le \varepsilon$; extra message reduces key length at most $\log|\mathcal{V}|$.

Composition of IR and PA

When message of rate R is revealed to Eve in IR

Alice and Bob can generate SK at rate

$$H(X|Z) - R$$

$\Longrightarrow H(X|Z) - H(X|Y)$ is attainable

Composition of IR and PA

When message of rate R is revealed to Eve in IR

Alice and Bob can generate SK at rate

$$H(X|Z) - R$$

$\Longrightarrow H(X|Z) - H(X|Y)$ is attainable

More generally,

(Randomness unknown to Eve initially) — (Rate revealed in IR)

Idea of Converse: a property of interactive communication

Interactive communication

Alice

Bob

$$\Pi_1 = \Pi_1(X)$$

$$\Pi_2 = \Pi_2(Y, \Pi_1)$$

$$\Pi_3 = \Pi_3(X, \Pi_1, \Pi_2)$$

$$\vdots$$

Idea of Converse: a property of interactive communication

Interactive communication

Alice Bob

$$\Pi_1 = \Pi_1(X) \longrightarrow$$

$$\longleftarrow \Pi_2 = \Pi_2(Y, \Pi_1)$$

$$\Pi_3 = \Pi_3(X, \Pi_1, \Pi_2) \longrightarrow$$

$$\vdots$$

Lemma [Maurer 93, Ahlswede-Csiszár 93]
For any protocol $\Pi = (\Pi_1, \ldots, \Pi_r)$,

$$I(X \wedge Y | Z, \Pi) \leq I(X \wedge Y | Z)$$

In particular,

$$P_{XYZ} = P_{X|Z} P_{Y|Z} P_Z \implies P_{XYZ\Pi} = P_{X|Z\Pi} P_{Y|Z\Pi} P_{Z\Pi}$$

A Basic Converese Bound

By the Fano inequality argument,…

Theorem [Maurer 93, Ahlswede-Csiszár 93]

For every $0 \le \varepsilon, \delta < 1$ with $\varepsilon + \delta < 1$,

$$S_{\varepsilon,\delta}(X, Y|Z) \le \frac{I(X \wedge Y|Z) + h(\varepsilon) + h(\delta)}{1 - \varepsilon - \delta}$$

A Basic Converese Bound

By the Fano inequality argument,…

Theorem [Maurer 93, Ahlswede-Csiszár 93]

For every $0 \leq \varepsilon, \delta < 1$ with $\varepsilon + \delta < 1,$

$$S_{\varepsilon,\delta}(X, Y|Z) \leq \frac{I(X \wedge Y|Z) + h(\varepsilon) + h(\delta)}{1 - \varepsilon - \delta}$$

For i.i.d. observations,

$$C(X, Y|Z) = \lim_{\varepsilon,\delta \to 0} \liminf_{n \to \infty} \frac{1}{n} S_{\varepsilon,\delta}(X^n, Y^n|Z^n) \leq I(X \wedge Y|Z)$$

It is tight when (X, Y, Z) form Markov chain (degraded):

$$I(X \wedge Y|Z) = H(X|Z) - H(X|Y)$$

Conditional Independence Testing Bound

By relating SK and hypothesis testing,…

Theorem [Tyagi-W. 14]

For every $0 \leq \varepsilon, \delta < 1$ and $0 < \eta < 1 - \varepsilon - \delta$, we have

$$S_{\varepsilon,\delta}(X, Y|Z) \leq -\log \beta_{\varepsilon+\delta+\eta}(P_{XYZ}, Q_{XYZ}) + 2\log(1/\eta)$$

for any $Q_{XYZ} = Q_{X|Z} Q_{Y|Z} Q_Z$.

Conditional Independence Testing Bound

By relating SK and hypothesis testing,…

Theorem [Tyagi-W. 14]

For every $0 \le \varepsilon, \delta < 1$ and $0 < \eta < 1 - \varepsilon - \delta$, we have

$$S_{\varepsilon,\delta}(X, Y|Z) \le -\log \beta_{\varepsilon+\delta+\eta}(P_{XYZ}, Q_{XYZ}) + 2\log(1/\eta)$$

for any $Q_{XYZ} = Q_{X|Z}Q_{Y|Z}Q_Z$.

For i.i.d. observations,

$$C_{\varepsilon,\delta}(X, Y|Z) = \liminf_{n\to\infty} \frac{1}{n} S_{\varepsilon,\delta}(X^n, Y^n|Z^n) \le I(X \wedge Y|Z)$$

strong converse can be proved.

It is also tight up to the second-order term for degraded case.

Second-Order Rate of Secret Key Agreement

Second-Order Rate of Secret Key Agreement

The standard protocol with

- information reconciliation
- privacy amplification

no interaction

achieves the secrecy capacity: $H(X|Z) - H(X|Y) = I(X \wedge Y|Z)$

The standard protocol is always optimal? Does interaction help in some case?

Second-Order Rate of Secret Key Agreement

The standard protocol with

- information reconciliation
- privacy amplification

no interaction

achieves the secrecy capacity: $H(X|Z) - H(X|Y) = I(X \wedge Y|Z)$

The standard protocol is always optimal? Does interaction help in some case?

Theorem [Hayashi-Tyagi-W. 14]

For $0 < \varepsilon, \delta < 1$ with $\varepsilon + \delta < 1$,

$$S_{\varepsilon,\delta}(X^n, Y^n|Z^n) = nI(X \wedge Y|Z) - \sqrt{nV}Q^{-1}(\varepsilon + \delta) + \mathcal{O}(\log n)$$

where

$$V := \mathrm{Var}\left[\log \frac{P_{XY|Z}(X,Y|Z)}{P_{X|Z}(X|Z)P_{Y|Z}(Y|Z)}\right]$$

$$Q(a) := \int_a^\infty \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{t^2}{2}\right) dt$$

Does Standard Protocol Work?

- information reconciliation

- privacy amplification

Does Standard Protocol Work?

- information reconciliation

$$nH(X|Y) + \sqrt{nV_{X|Y}}Q^{-1}(\varepsilon) + \mathcal{O}(\log n)$$

$$V_{X|Y} = \mathrm{Var}\left[\log \frac{1}{P_{X|Y}(X|Y)}\right]$$

- privacy amplification

Does Standard Protocol Work?

- information reconciliation

$$nH(X|Y) + \sqrt{nV_{X|Y}}Q^{-1}(\varepsilon) + \mathcal{O}(\log n)$$

$$V_{X|Y} = \mathrm{Var}\left[\log \frac{1}{P_{X|Y}(X|Y)}\right]$$

- privacy amplification

$$nH(X|Z) - \sqrt{nV_{X|Z}}Q^{-1}(\delta) + \mathcal{O}(\log n)$$

$$V_{X|Z} = \mathrm{Var}\left[\log \frac{1}{P_{X|Z}(X|Z)}\right]$$

Does Standard Protocol Work?

- information reconciliation

$$nH(X|Y) + \sqrt{nV_{X|Y}}Q^{-1}(\varepsilon) + \mathcal{O}(\log n)$$

$$V_{X|Y} = \mathrm{Var}\left[\log \frac{1}{P_{X|Y}(X|Y)}\right]$$

- privacy amplification

$$nH(X|Z) - \sqrt{nV_{X|Z}}Q^{-1}(\delta) + \mathcal{O}(\log n)$$

$$V_{X|Z} = \mathrm{Var}\left[\log \frac{1}{P_{X|Z}(X|Z)}\right]$$

$$nI(X \wedge Y|Z) - \sqrt{nV_{X|Y}}Q^{-1}(\varepsilon) - \sqrt{nV_{X|Z}}Q^{-1}(\delta) + \mathcal{O}(\log n)$$

The standard protocol does not achieve the optimal second-order rate.

Does Standard Protocol Work?

- information reconciliation

$$nH(X|Y) + \sqrt{nV_{X|Y}}Q^{-1}(\varepsilon) + \mathcal{O}(\log n)$$

$$V_{X|Y} = \mathrm{Var}\left[\log \frac{1}{P_{X|Y}(X|Y)}\right]$$

- privacy amplification

$$nH(X|Z) - \sqrt{nV_{X|Z}}Q^{-1}(\delta) + \mathcal{O}(\log n)$$

$$V_{X|Z} = \mathrm{Var}\left[\log \frac{1}{P_{X|Z}(X|Z)}\right]$$

$$nI(X \wedge Y|Z) - \sqrt{nV_{X|Y}}Q^{-1}(\varepsilon) - \sqrt{nV_{X|Z}}Q^{-1}(\delta) + \mathcal{O}(\log n)$$

The standard protocol does not achieve the optimal second-order rate.

The optimal second-order rate is achieved by an interactive protocol.

Achievability Idea

Use interactive Slepian-Wolf coding (cf. [Draper 04, Feder-Schulman 02, Yang-He 10])

Achievability Idea

Use interactive Slepian-Wolf coding (cf. [Draper 04, Feder-Schulman 02, Yang-He 10])

Basic ideas are…

- Alice should communicate at small rate if $h_{P_{X|Y}}(X|Y) = \log \frac{1}{P_{X|Y}(X|Y)}$ is small;

Achievability Idea

Use interactive Slepian-Wolf coding (cf. [Draper 04, Feder-Schulman 02, Yang-He 10])

Basic ideas are…

- Alice should communicate at small rate if $h_{P_{X|Y}}(X|Y) = \log \frac{1}{P_{X|Y}(X|Y)}$ is small;
- But neither party know the realization of $h_{P_{X|Y}}(X|Y)$;

Achievability Idea

Use interactive Slepian-Wolf coding (cf. [Draper 04, Feder-Schulman 02, Yang-He 10])

Basic ideas are…

- Alice should communicate at small rate if $h_{P_{X|Y}}(X|Y) = \log \frac{1}{P_{X|Y}(X|Y)}$ is small;
- But neither party know the realization of $h_{P_{X|Y}}(X|Y)$;
- Alice gradually increase rate until Bob is able to decode X;

Achievability Idea

Use interactive Slepian-Wolf coding (cf. [Draper 04, Feder-Schulman 02, Yang-He 10])

Basic ideas are…

- Alice should communicate at small rate if $h_{P_{X|Y}}(X|Y) = \log \frac{1}{P_{X|Y}(X|Y)}$ is small;
- But neither party know the realization of $h_{P_{X|Y}}(X|Y)$;
- Alice gradually increase rate until Bob is able to decode X;
- Bob return Ack/Nack until it decode X.

Achievability Idea

Use interactive Slepian-Wolf coding (cf. [Draper 04, Feder-Schulman 02, Yang-He 10])

Basic ideas are…

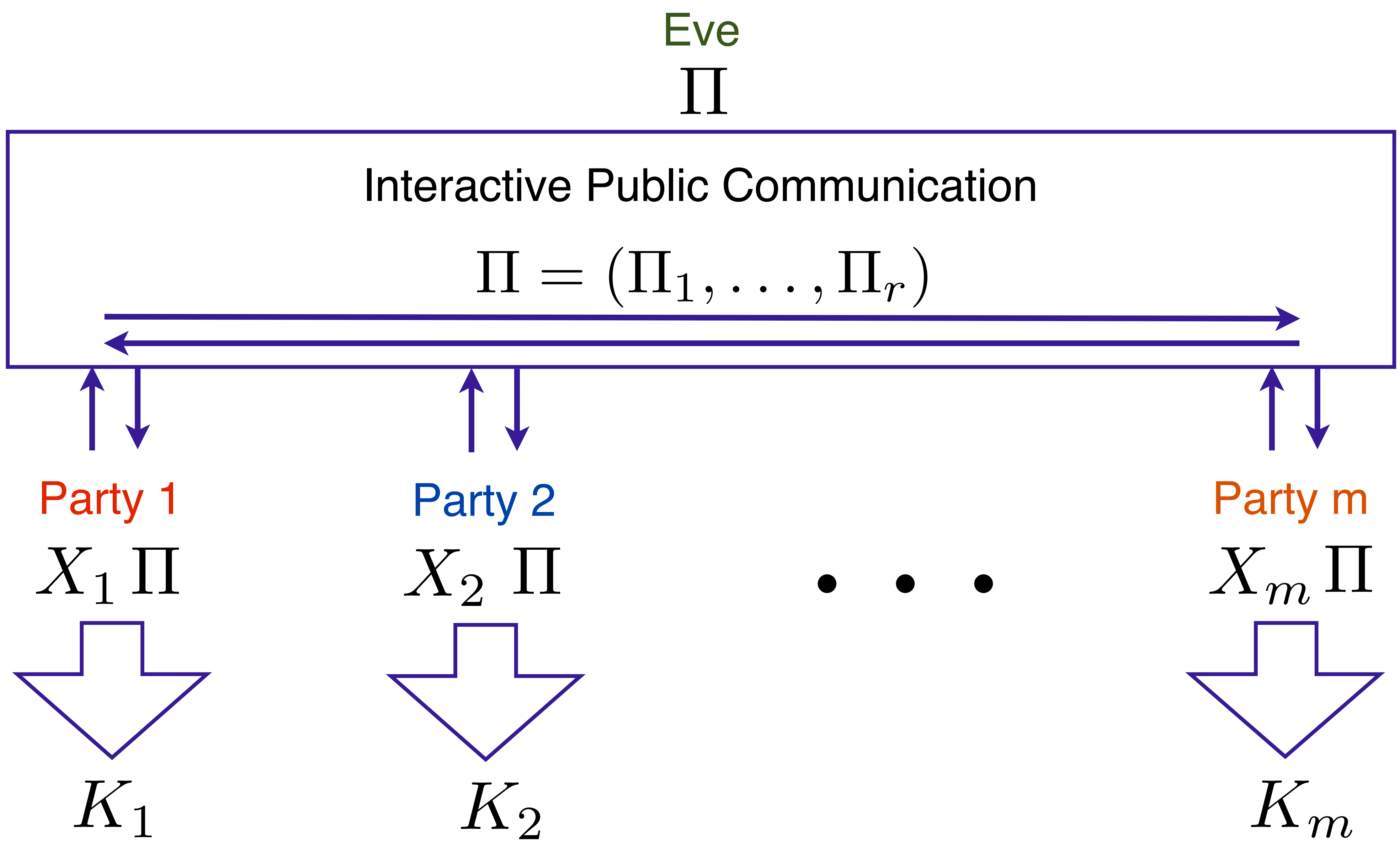
- Alice should communicate at small rate if $h_{P_{X|Y}}(X|Y) = \log \frac{1}{P_{X|Y}(X|Y)}$ is small;
- But neither party know the realization of $h_{P_{X|Y}}(X|Y)$;
- Alice gradually increase rate until Bob is able to decode X;
- Bob return Ack/Nack until it decode X.

The usage of interaction decreases information revealed to Eve…

Multi-Party Secret Key Agreement

Multi-Party Setting

[Csiszár-Narayan 04]



$A \subset \mathcal{M} := \{1, \ldots, M\}$

$X_A := (X_i : i \in A)$

$X_{\mathcal{M}} := (X_1, \ldots, X_m)$

$K_{\mathcal{M}} := (K_1, \ldots, K_m)$

Problem Formulation of Multi-Party SK

The generate key is (ε, δ)-SK $\quad (0 \leq \varepsilon, \delta < 1)$ if there exists K such that

Reliability $\quad \Pr\{K_1 = \cdots = K_m = K\} \geq 1 - \varepsilon$

Security $\quad d(P_{K\Pi Z}, P_{\mathtt{unif}} \times P_{\Pi Z}) \leq \delta$

$S_{\varepsilon,\delta}(X_{\mathcal{M}})$:maximum $\log|\mathcal{K}|$ such that a protocol generating (ε, δ)-SK exists

$$C(X_{\mathcal{M}}) := \lim_{\varepsilon,\delta \to 0} \liminf_{n \to \infty} \frac{1}{n} S_{\varepsilon,\delta}(X^n_{\mathcal{M}})$$

2 Party Revisited

(Randomness unknown to Eve initially) — (Rate revealed in IR)

2 Party Revisited

(Randomness unknown to Eve initially) — (Rate revealed in IR)

$$C(X_1, X_2) = I(X_1 \wedge X_2)$$

$$= H(X_1) - H(X_1|X_2)$$

it is asymmetric…

2 Party Revisited

(Randomness unknown to Eve initially) — (Rate revealed in IR)

$$C(X_1, X_2) = I(X_1 \wedge X_2)$$

$$= H(X_1) - H(X_1|X_2)$$

it is asymmetric…

$$= H(X_1, X_2) - H(X_1|X_2) - H(X_2|X_1)$$

2 Party Revisited

(Randomness unknown to Eve initially) — (Rate revealed in IR)

$$C(X_1, X_2) = I(X_1 \wedge X_2)$$

$$= H(X_1) - H(X_1|X_2)$$

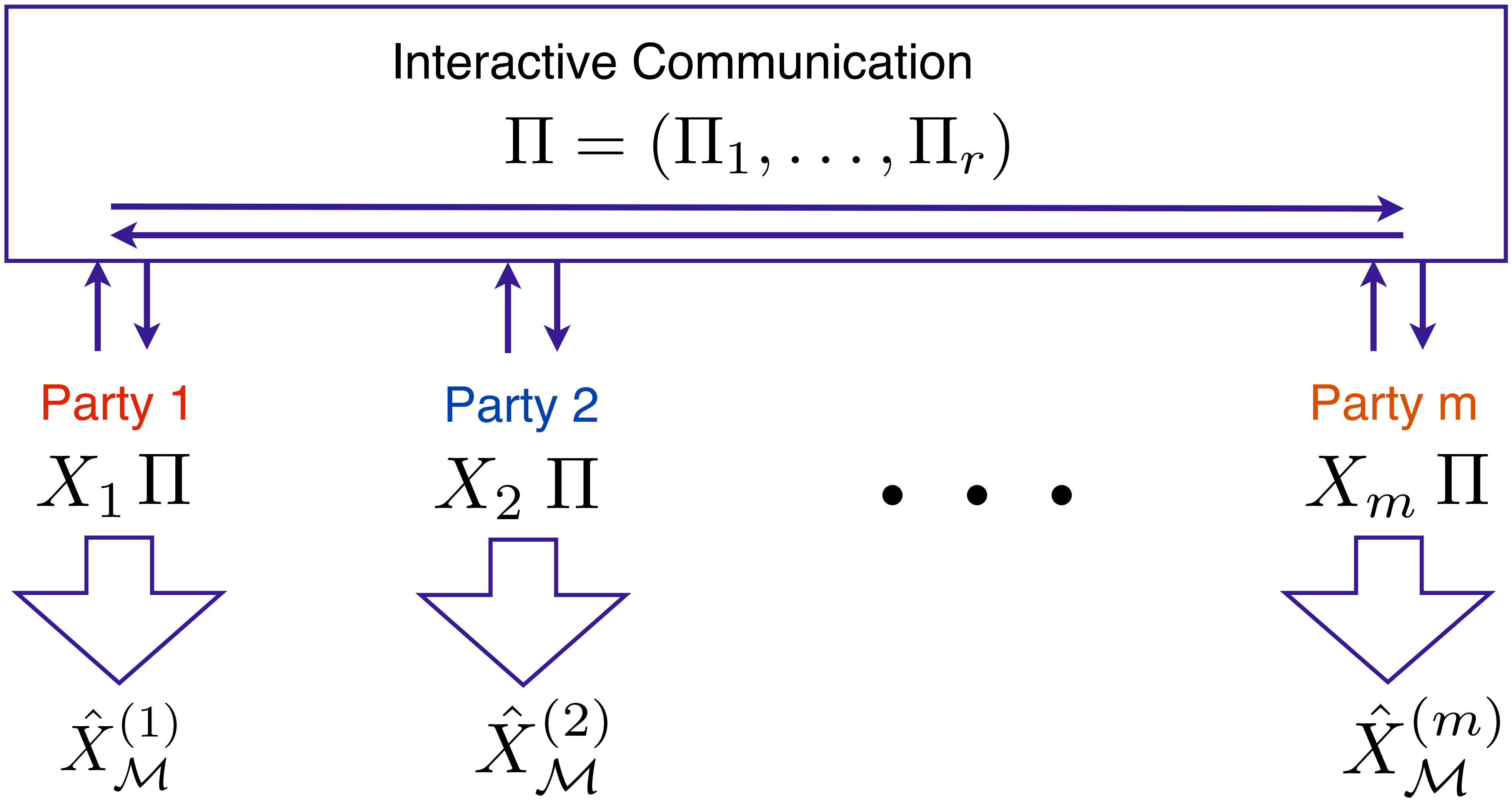
it is asymmetric…

$$= H(X_1, X_2) - H(X_1|X_2) - H(X_2|X_1)$$

$H(X_{\mathcal{M}})-$ communication rate needed to agree on $X_{\mathcal{M}}$

Omniscience (Data Exchange) Problem

[Csiszár-Narayan 04]



$L_\epsilon(X_{\mathcal{M}})$: minimum sum-rate for omniscience with

$$\mathrm{P}\big(X^{(i)}_{\mathcal{M}} = X_{\mathcal{M}},\ \forall 1 \le i \le m\big) \ge 1 - \epsilon$$

Asymptotic Omniscience Rate

$$R(\mathrm{P}_{X_{\mathcal{M}}}) = \lim_{\epsilon \to 0} \limsup_{n \to \infty} \frac{1}{n} L_\epsilon(X_{\mathcal{M}}^n)$$

Asymptotic Omniscience Rate

$$R(\mathrm{P}_{X_{\mathcal{M}}}) = \lim_{\epsilon \to 0} \limsup_{n \to \infty} \frac{1}{n} L_\epsilon(X_{\mathcal{M}}^n)$$

$$R(\mathrm{P}_{X_{\mathcal{M}}}) = \min \left\{ \sum_{i=1}^{m} R_i : \sum_{i \in B} R_i \geq H(X_B | X_{B^c}), \quad \forall B \subsetneq \mathcal{M} \right\}$$

[Csiszár-Narayan 04]

Achieved by Slepian-Wolf coding; interaction not needed.

Asymptotic Omniscience Rate

$$R(\mathrm{P}_{X_\mathcal{M}}) = \lim_{\epsilon \to 0} \limsup_{n\to\infty} \frac{1}{n} L_\epsilon(X_\mathcal{M}^n)$$

$$R(\mathrm{P}_{X_\mathcal{M}}) = \min\left\{\sum_{i=1}^m R_i : \sum_{i\in B} R_i \geq H(X_B|X_{B^c}), \quad \forall B \subsetneq \mathcal{M}\right\}$$

[Csiszár-Narayan 04]

$$\overset{\geq}{=} \max_{\sigma\in\Sigma(\mathcal{M})} \mathbb{H}_\sigma(\mathcal{M}|\mathrm{P}_{X_\mathcal{M}})$$

[Chan 08]

Achieved by Slepian-Wolf coding; interaction not needed.

$$\mathbb{H}_\sigma(\mathcal{M}|\mathrm{P}_{X_\mathcal{M}}) := \frac{1}{|\sigma|-1}\sum_{i=1}^{|\sigma|} H(X_\mathcal{M}|X_{\sigma_i})$$

σ :partition of $\mathcal{M}$

Asymptotic Omniscience Rate

$$R(\mathrm{P}_{X_{\mathcal{M}}}) = \lim_{\epsilon \to 0} \limsup_{n \to \infty} \frac{1}{n} L_\epsilon(X_{\mathcal{M}}^n)$$

$$R(\mathrm{P}_{X_{\mathcal{M}}}) = \min \left\{ \sum_{i=1}^{m} R_i : \sum_{i \in B} R_i \geq H(X_B | X_{B^c}), \quad \forall B \subsetneq \mathcal{M} \right\}$$

[Csiszár-Narayan 04]

$$\overset{\geq}{=} \max_{\sigma \in \Sigma(\mathcal{M})} \mathbb{H}_\sigma(\mathcal{M} | \mathrm{P}_{X_{\mathcal{M}}})$$

[Chan 08]

Achieved by Slepian-Wolf coding; interaction not needed.

$$\mathbb{H}_\sigma(\mathcal{M} | \mathrm{P}_{X_{\mathcal{M}}}) := \frac{1}{|\sigma| - 1} \sum_{i=1}^{|\sigma|} H(X_{\mathcal{M}} | X_{\sigma_i})$$

σ :partition of $\mathcal{M}$

$$m = 2 \qquad \Sigma(\mathcal{M}) = \{\{1|2\}\}$$

$$R(\mathrm{P}_{X_{\mathcal{M}}}) = H(X_1 | X_2) + H(X_2 | X_1)$$

Asymptotic Omniscience Rate

$$R(\mathrm{P}_{X_\mathcal{M}}) = \lim_{\epsilon\to 0}\limsup_{n\to\infty} \frac{1}{n} L_\epsilon(X_\mathcal{M}^n)$$

$$R(\mathrm{P}_{X_\mathcal{M}}) = \min\left\{\sum_{i=1}^m R_i : \sum_{i\in B} R_i \geq H(X_B|X_{B^c}),\quad \forall B \subsetneq \mathcal{M}\right\}$$

[Csiszár-Narayan 04]

$$\underset{=}{\geq} \max_{\sigma\in\Sigma(\mathcal{M})} \mathbb{H}_\sigma(\mathcal{M}|\mathrm{P}_{X_\mathcal{M}})$$

[Chan 08]

Achieved by Slepian-Wolf coding; interaction not needed.

$$\mathbb{H}_\sigma(\mathcal{M}|\mathrm{P}_{X_\mathcal{M}}) := \frac{1}{|\sigma|-1}\sum_{i=1}^{|\sigma|} H(X_\mathcal{M}|X_{\sigma_i})$$

σ :partition of $\mathcal{M}$

$$m = 3 \qquad \Sigma(\mathcal{M}) = \{\{1|23\},\{12|3\},\{23|1\},\{1|2|3\}\}$$

$$R(\mathrm{P}_{X_\mathcal{M}}) = \max\Big\{H(X_1|X_2,X_3)+H(X_2,X_3|X_1), H(X_3|X_1,X_2)+H(X_1,X_2|X_3),$$
$$H(X_2|X_1,X_3)+H(X_1,X_3|X_2), \frac{H(X_2,X_3|X_1)+H(X_1,X_3|X_2)+H(X_1,X_2|X_3)}{2}\Big\}$$

Multi-Party Secrecy Capacity

Theorem [Csiszár-Narayan 04]

$$C(X_{\mathcal{M}}) = H(X_{\mathcal{M}}) - R(\mathrm{P}_{X_{\mathcal{M}}})$$

Multi-Party Secrecy Capacity

Theorem [Csiszár-Narayan 04, Chan 08]

$$C(X_{\mathcal{M}}) = H(X_{\mathcal{M}}) - R(\mathrm{P}_{X_{\mathcal{M}}})$$

$$= \min_{\sigma \in \Sigma(\mathcal{M})} \frac{1}{|\sigma| - 1} D\left(\mathrm{P}_{X_{\mathcal{M}}} \middle\| \prod_{i=1}^{|\sigma|} \mathrm{P}_{X_{\sigma_i}}\right)$$

Multi-Party Secrecy Capacity

Theorem [Csiszár-Narayan 04, Chan 08]

$$C(X_{\mathcal{M}}) = H(X_{\mathcal{M}}) - R(\mathrm{P}_{X_{\mathcal{M}}})$$

$$= \min_{\sigma \in \Sigma(\mathcal{M})} \frac{1}{|\sigma| - 1} D\left(\mathrm{P}_{X_{\mathcal{M}}} \middle\| \prod_{i=1}^{|\sigma|} \mathrm{P}_{X_{\sigma_i}}\right)$$

A single-shot converse can be proved via hypothesis testing [Tyagi-W. 14]

Universal Protocol

Universal Protocol

We shall construct a SK/Data exchange protocol that does not rely on knowledge of $\mathrm{P}_{X_{\mathcal{M}}}$.

It suffices to construct a universal data exchange protocol.

Universal Protocol

We shall construct a SK/Data exchange protocol that does not rely on knowledge of $\mathrm{P}_{X_{\mathcal{M}}}$.

It suffices to construct a universal data exchange protocol.

In fact, it works for a given individual sequence…

Theorem [Tyagi-W. 16]

There exists a universal data exchange protocol such that, for a given $\mathbf{x}_{\mathcal{M}}$, it communicates

$$nR^*(\mathrm{P}_{\mathbf{x}_{\mathcal{M}}}) + \mathcal{O}(\sqrt{n})$$

where $\mathrm{P}_{\mathbf{x}_{\mathcal{M}}}$ is the joint type.

The universal protocol is called recursive data exchange (RDE) protocol.

Universal RDE Protocol

Two-step coding for single-terminal source coding:

(1) Send the type $\mathcal{O}(\log n)$

(2) Send the index among the type class $nH(\mathrm{P}_{\mathbf{x}}) + \mathcal{O}(\log n)$

Universal RDE Protocol

Two-step coding for single-terminal source coding:

(1) Send the type $\mathcal{O}(\log n)$

(2) Send the index among the type class $nH(\mathrm{P}_{\mathbf{x}}) + \mathcal{O}(\log n)$

In the data exchange problem, observations are distributed over the parties…

Universal RDE Protocol

Two-step coding for single-terminal source coding:

(1) Send the type $\mathcal{O}(\log n)$

(2) Send the index among the type class $nH(\mathrm{P}_{\mathbf{x}}) + \mathcal{O}(\log n)$

In the data exchange problem, observations are distributed over the parties…

Use interactive Slepian-Wolf coding [Draper 04, Yang-He 10]

- The encoder gradually increment rate until the decoder recovers $\mathbf{x}$
- The decoder return Ack/Nack until it recovers $\mathbf{x}$

Universal RDE Protocol

Two-step coding for single-terminal source coding:

(1) Send the type $\mathcal{O}(\log n)$

(2) Send the index among the type class $nH(\mathrm{P}_{\mathbf{x}}) + \mathcal{O}(\log n)$

In the data exchange problem, observations are distributed over the parties…

Use interactive Slepian-Wolf coding [Draper 04, Yang-He 10]

- The encoder gradually increment rate until the decoder recovers $\mathbf{x}$
- The decoder return Ack/Nack until it recovers $\mathbf{x}$

The decoder looks for joint type $\mathrm{P}_{\overline{XY}}$ s.t. there exists a unique $\hat{\mathbf{x}}$ satisfying

1) $\mathrm{P}_{\hat{\mathbf{x}}\mathbf{y}} = \mathrm{P}_{\overline{XY}}$

2) $R_t \geq H(\overline{X}|\overline{Y}) + \Delta$

3) Hash values (bin indices) of $\hat{\mathbf{x}}$ up to round t are compatible.

Decoding Rule for Local Omniscience

Local omniscience region for $A \subseteq \mathcal{M}$:

$$\mathcal{R}_{\mathsf{CO}}^{\Delta}(A|\mathrm{P}_{\overline{X}_A}) = \left\{ (R_i : i \in A) : \sum_{i \in B} R_i \geq H(\overline{X}_B|\overline{X}_{A \setminus B}) + |B|\Delta, \ \forall B \subseteq A \right\}$$

Decoding Rule for Local Omniscience

Local omniscience region for $A \subseteq \mathcal{M}$:

$$\mathcal{R}_{\mathsf{CO}}^{\Delta}(A|\mathrm{P}_{\overline{X}_A}) = \left\{ (R_i : i \in A) : \sum_{i \in B} R_i \geq H(\overline{X}_B | \overline{X}_{A \setminus B}) + |B|\Delta, \ \forall B \subseteq A \right\}$$

i th party looks for maximal $i \in A \subseteq \mathcal{M}$ and $\mathrm{P}_{\overline{X}_A}$ s.t. there exists a unique $\hat{\mathbf{x}}_A$ satisfying

1) $\hat{\mathbf{x}}_i = \mathbf{x}_i$, $\mathrm{P}_{\hat{\mathbf{x}}_A} = \mathrm{P}_{\overline{X}_A}$

2) $(R_i^{(t)} : i \in A) \in \mathcal{R}_{\mathsf{CO}}^{\Delta}(A|\mathrm{P}_{\overline{X}_A})$

3) Hash values (bin indices) of $\hat{\mathbf{x}}_A$ up to round t are compatible.

Decoding Rule for Local Omniscience

Local omniscience region for $A \subseteq \mathcal{M}$:

$$\mathcal{R}_{\mathsf{CO}}^{\Delta}(A|\mathrm{P}_{\overline{X}_A}) = \left\{ (R_i : i \in A) : \sum_{i \in B} R_i \geq H(\overline{X}_B | \overline{X}_{A \setminus B}) + |B|\Delta,\ \forall B \subseteq A \right\}$$

i th party looks for maximal $i \in A \subseteq \mathcal{M}$ and $\mathrm{P}_{\overline{X}_A}$ s.t. there exists a unique $\hat{\mathbf{x}}_A$ satisfying

1) $\hat{\mathbf{x}}_i = \mathbf{x}_i$, $\mathrm{P}_{\hat{\mathbf{x}}_A} = \mathrm{P}_{\overline{X}_A}$

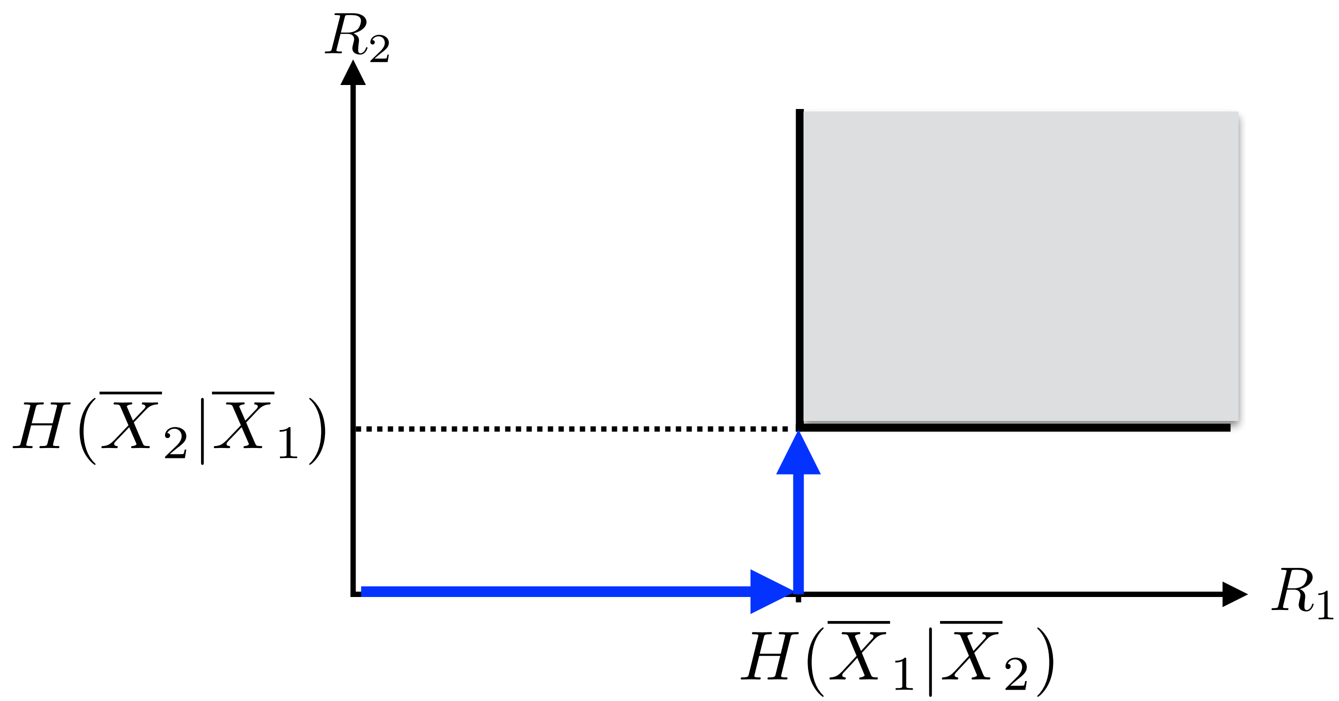
2) $(R_i^{(t)} : i \in A) \in \mathcal{R}_{\mathsf{CO}}^{\Delta}(A|\mathrm{P}_{\overline{X}_A})$

3) Hash values (bin indices) of $\hat{\mathbf{x}}_A$ up to round t are compatible.

Once accumulated rate vector enters a local omniscience region, local omniscience occur automatically. Difficulty is how to increment rates…

Rate Increment Rule

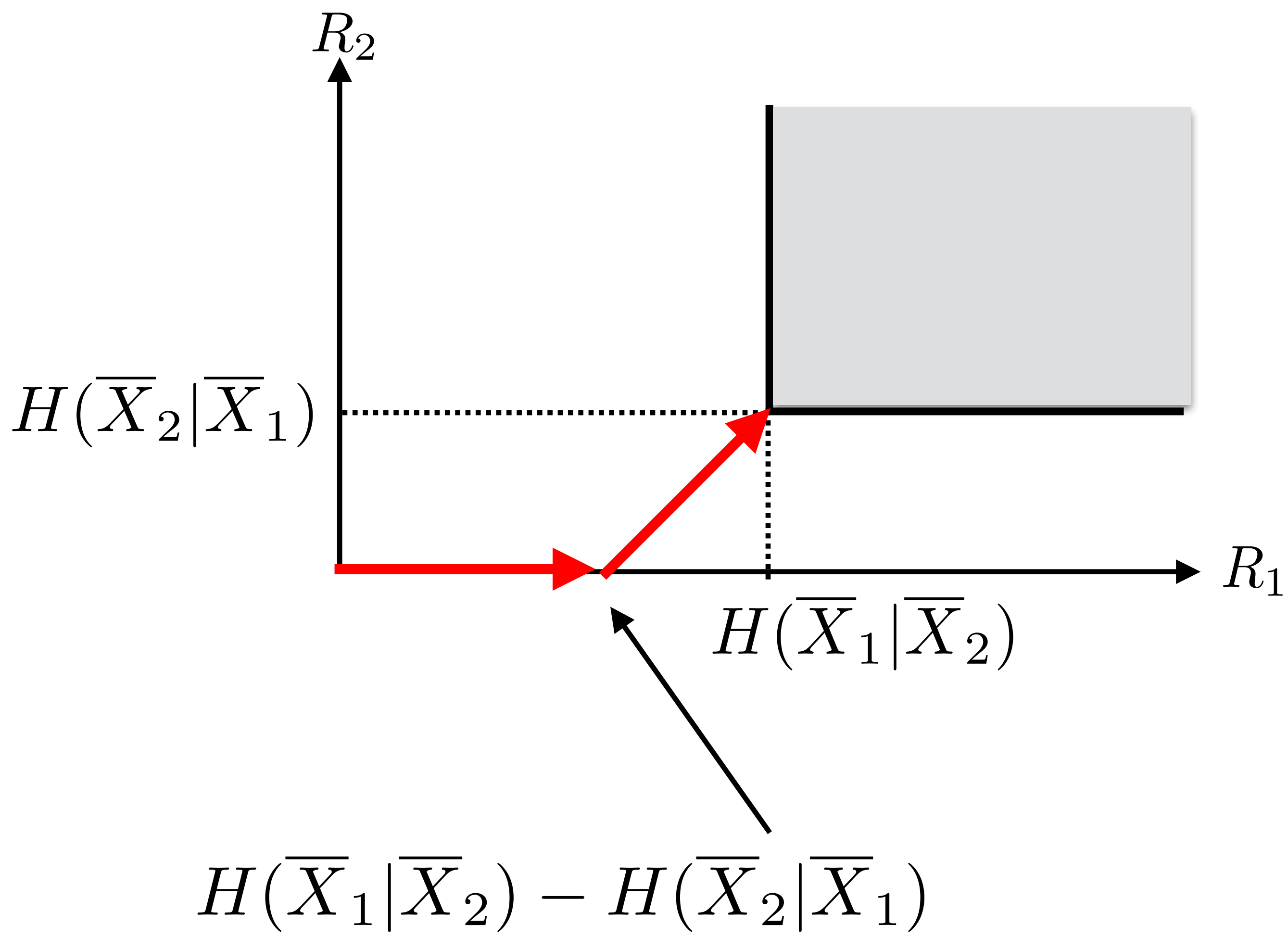
Two-party case:



It is asymmetric…

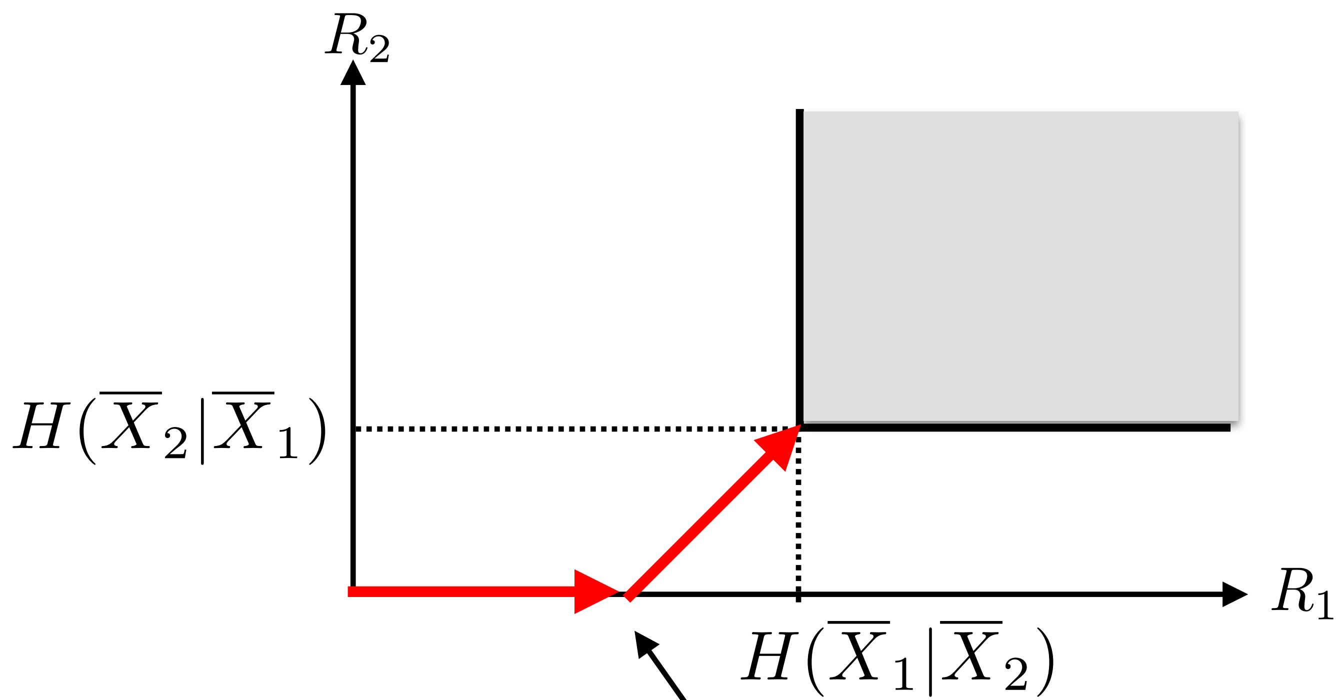
Rate Increment Rule

Two-party case:



Rate Increment Rule

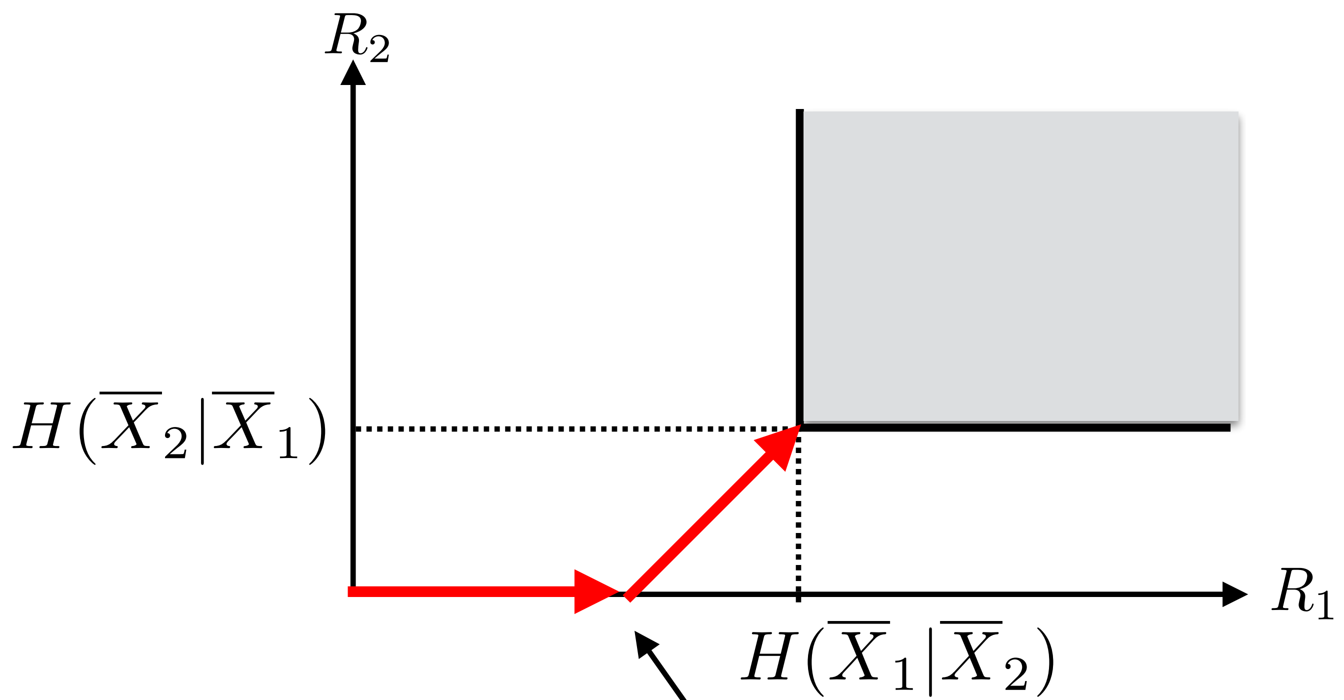
Two-party case:



$$H(\overline{X}_1|\overline{X}_2) - H(\overline{X}_2|\overline{X}_1) = H(\overline{X}_1) - H(\overline{X}_2)$$

Rate Increment Rule

Two-party case:

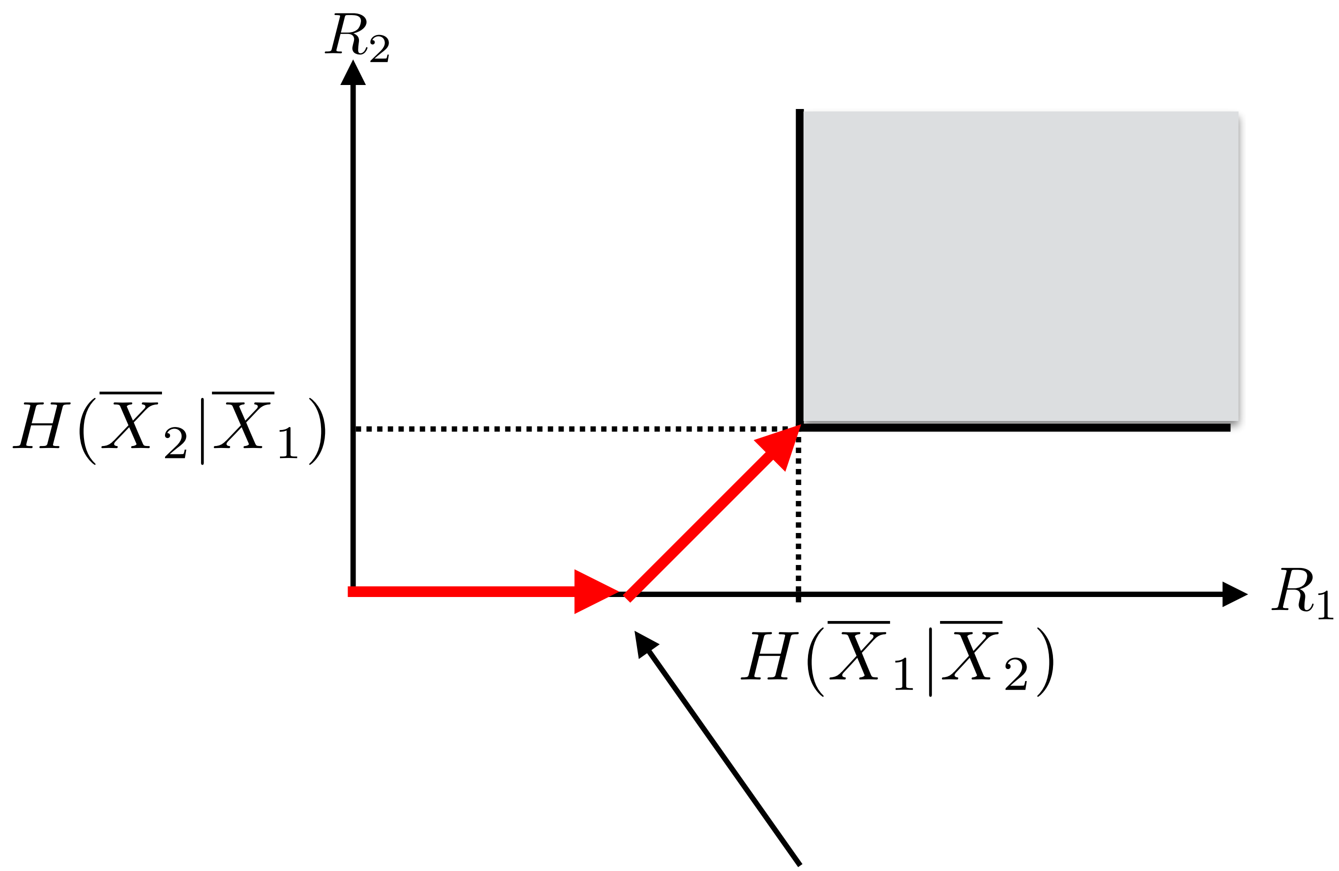


$$H(\overline{X}_1|\overline{X}_2) - H(\overline{X}_2|\overline{X}_1) = H(\overline{X}_1) - H(\overline{X}_2)$$

W.L.G., assume $H(\overline{X}_1) \geq H(\overline{X}_2)$

Rate Increment Rule

Two-party case:



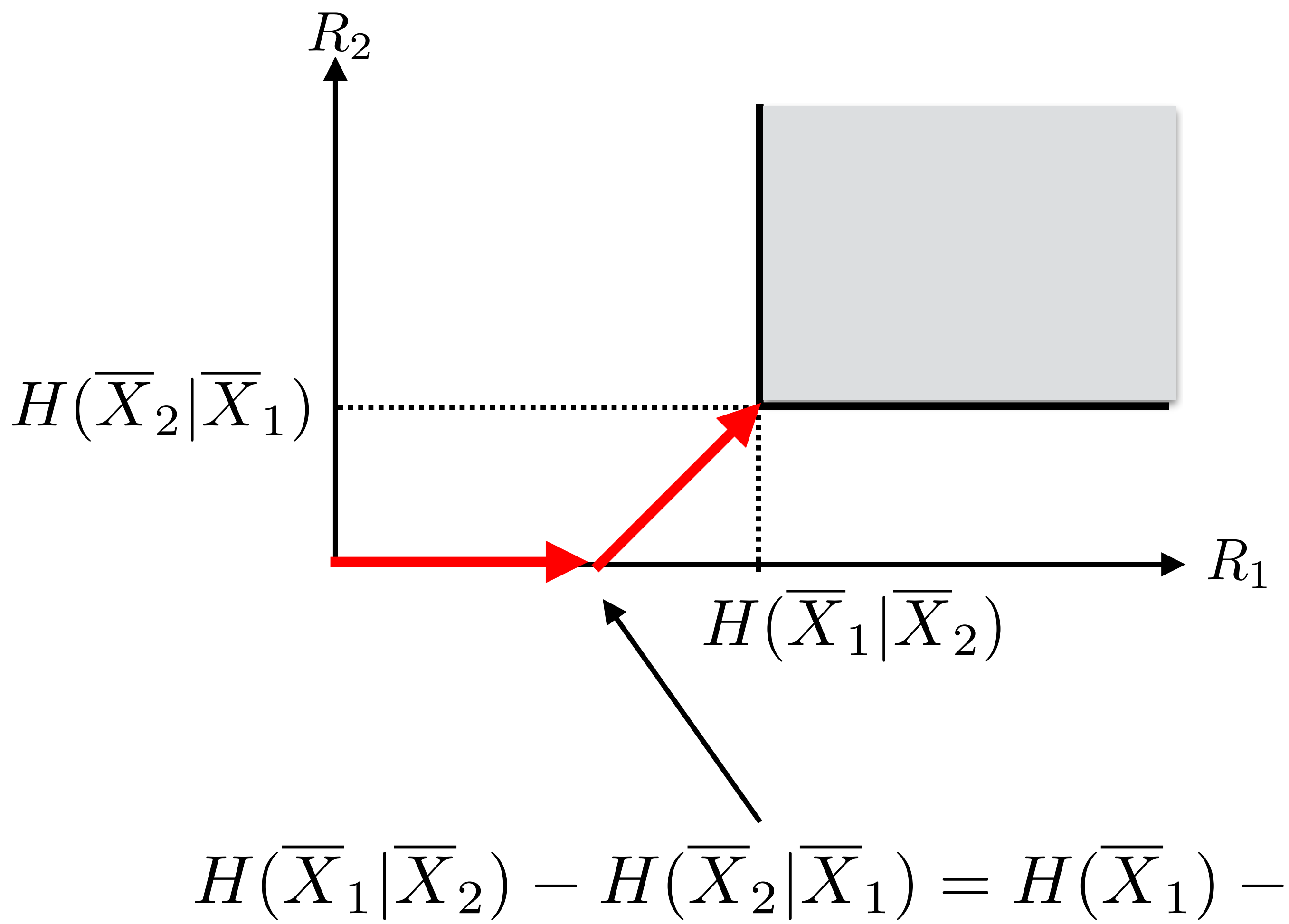
$$H(\overline{X}_1|\overline{X}_2) - H(\overline{X}_2|\overline{X}_1) = H(\overline{X}_1) - H(\overline{X}_2)$$

W.L.G., assume $H(\overline{X}_1) \geq H(\overline{X}_2)$

Party 1: $R_1^{(0)} = 0\,;\; R_1^{(t+1)} := R_1^{(t)} + \Delta$

Rate Increment Rule

Two-party case:



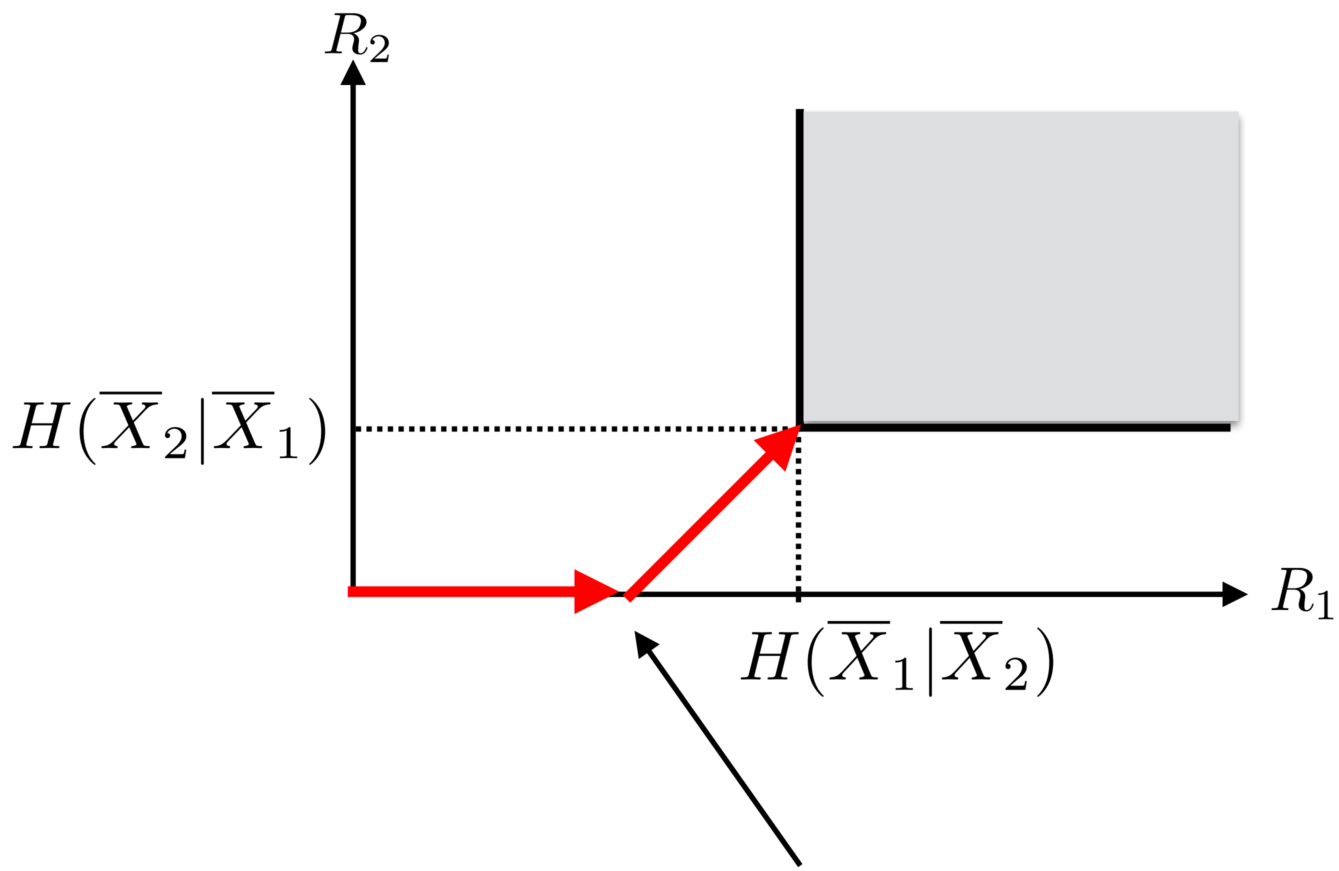
W.L.G., assume $H(\overline{X}_1) \geq H(\overline{X}_2)$

Party 1: $R_1^{(0)} = 0$; $R_1^{(t+1)} := R_1^{(t)} + \Delta$

Party 2: start communication if $R_1^{(t)} \geq H(\overline{X}_1) - H(\overline{X}_2)$;

Rate Increment Rule

Two-party case:



$$H(\overline{X}_1|\overline{X}_2) - H(\overline{X}_2|\overline{X}_1) = H(\overline{X}_1) - H(\overline{X}_2)$$

W.L.G., assume $H(\overline{X}_1) \geq H(\overline{X}_2)$

Party 1: $R_1^{(0)} = 0\,;\; R_1^{(t+1)} := R_1^{(t)} + \Delta$

Party 2: start communication if $R_1^{(t)} \geq H(\overline{X}_1) - H(\overline{X}_2)\,;\; R_2^{(0)} = 0\,;\; R_2^{(t+1)} = R_2^{(t)} + \Delta$

Rate Increment Rule

Multi-party case:

W.L.G., assume $H(\overline{X}_1) \geq H(\overline{X}_2) \geq \cdots \geq H(\overline{X}_m)$

Rate Increment Rule

Multi-party case:

W.L.G., assume $H(\overline{X}_1) \geq H(\overline{X}_2) \geq \cdots \geq H(\overline{X}_m)$

Party 1: $R_1^{(0)} = 0$; $R_1^{(t+1)} := R_1^{(t)} + \Delta$

Rate Increment Rule

Multi-party case:

W.L.G., assume $H(\overline{X}_1) \geq H(\overline{X}_2) \geq \cdots \geq H(\overline{X}_m)$

Party 1: $R_1^{(0)} = 0$; $R_1^{(t+1)} := R_1^{(t)} + \Delta$

Party 2: start communication if $R_1^{(t)} \geq H(\overline{X}_1) - H(\overline{X}_2)$; $R_2^{(0)} = 0$; $R_2^{(t+1)} = R_2^{(t)} + \Delta$

Rate Increment Rule

Multi-party case:

W.L.G., assume $H(\overline{X}_1) \geq H(\overline{X}_2) \geq \cdots \geq H(\overline{X}_m)$

Party 1: $R_1^{(0)} = 0\,;\; R_1^{(t+1)} := R_1^{(t)} + \Delta$

Party 2: start communication if $R_1^{(t)} \geq H(\overline{X}_1) - H(\overline{X}_2)\,;\; R_2^{(0)} = 0\,;\; R_2^{(t+1)} = R_2^{(t)} + \Delta$

Party 3: start communication if $R_1^{(t)} \geq H(\overline{X}_1) - H(\overline{X}_3)\,;\; R_3^{(0)} = 0; R_3^{(t+1)} = R_3^{(t)} + \Delta$

$\vdots$

Rate Increment Rule

Multi-party case:

W.L.G., assume $H(\overline{X}_1) \geq H(\overline{X}_2) \geq \cdots \geq H(\overline{X}_m)$

Party 1: $R_1^{(0)} = 0$; $R_1^{(t+1)} := R_1^{(t)} + \Delta$

Party 2: start communication if $R_1^{(t)} \geq H(\overline{X}_1) - H(\overline{X}_2)$; $R_2^{(0)} = 0$; $R_2^{(t+1)} = R_2^{(t)} + \Delta$

Party 3: start communication if $R_1^{(t)} \geq H(\overline{X}_1) - H(\overline{X}_3)$; $R_3^{(0)} = 0$; $R_3^{(t+1)} = R_3^{(t)} + \Delta$

$\vdots$

Rate assignment for the tipping

$$\sum_{i \in A \setminus \{j\}} R_i^*(A) = H(\overline{X}_A | \overline{X}_j), \ j \in A$$

Property:

$$R_i^*(A) - R_j^*(A) = H(\overline{X}_i) - H(\overline{X}_j)$$

Recursive Structure

Theorem (rough statement)

At some point, $(R_i^{(t)} : i \in A)$ for some $A \subseteq \mathcal{M}$ reaches $\mathcal{R}_{\mathtt{CO}}^{\Delta}(A|\mathrm{P}_{\overline{X}_A})$ at

$$(R_i^*(A) : i \in A) \qquad \text{modulo} \quad \mathcal{O}(\Delta)$$

Recursive Structure

Theorem (rough statement)

At some point, $(R_i^{(t)} : i \in A)$ for some $A \subseteq \mathcal{M}$ reaches $\mathcal{R}_{\texttt{CO}}^{\Delta}(A|\mathrm{P}_{\overline{X}_A})$ at

$$(R_i^*(A) : i \in A) \qquad \text{modulo } \mathcal{O}(\Delta)$$

Parties in A attain local omniscience.

From that point, the parties in A behaves as if one large party: increment rule is

$$R_i^{(t+1)} = R_i^{(t)} + \frac{\Delta}{|A|},\ i \in A \qquad (R_A^{(t+1)} = R_A^{(t)} + \Delta)$$

Recursive Structure

Theorem (rough statement)

At some point, $(R_i^{(t)} : i \in A)$ for some $A \subseteq \mathcal{M}$ reaches $\mathcal{R}_{\mathsf{CO}}^{\Delta}(A|\mathrm{P}_{\overline{X}_A})$ at

$$(R_i^*(A) : i \in A) \qquad \text{modulo } \mathcal{O}(\Delta)$$

Parties in A attain local omniscience.

From that point, the parties in A behaves as if one large party: increment rule is

$$R_i^{(t+1)} = R_i^{(t)} + \frac{\Delta}{|A|},\ i \in A \qquad (R_A^{(t+1)} = R_A^{(t)} + \Delta)$$

Theorem (rough statement)

The protocol proceed as if A were one party from the begin with…

Recursive Structure

P2

X_2

P1

X_1

P3

X_3

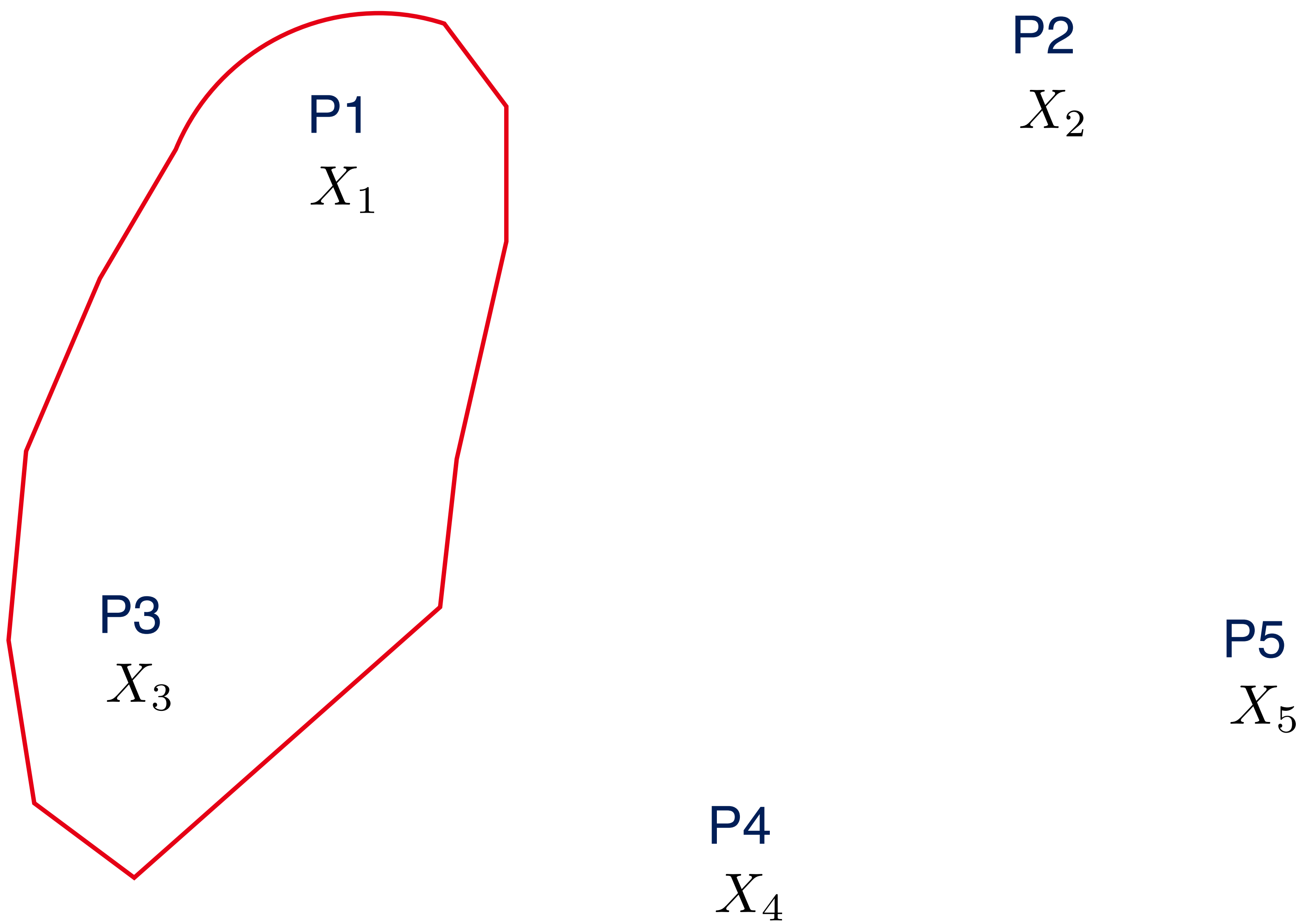
P5

X_5

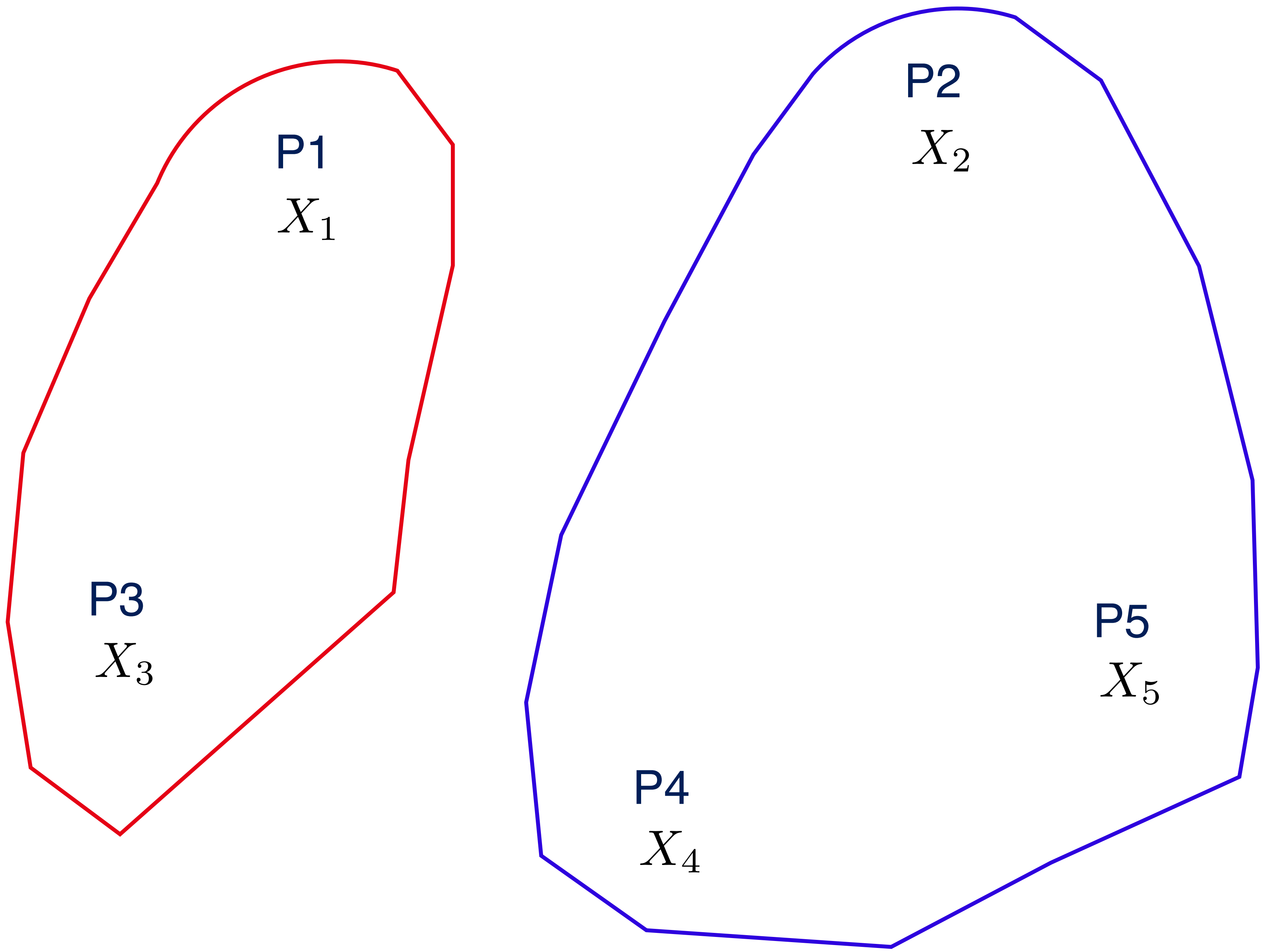
P4

X_4

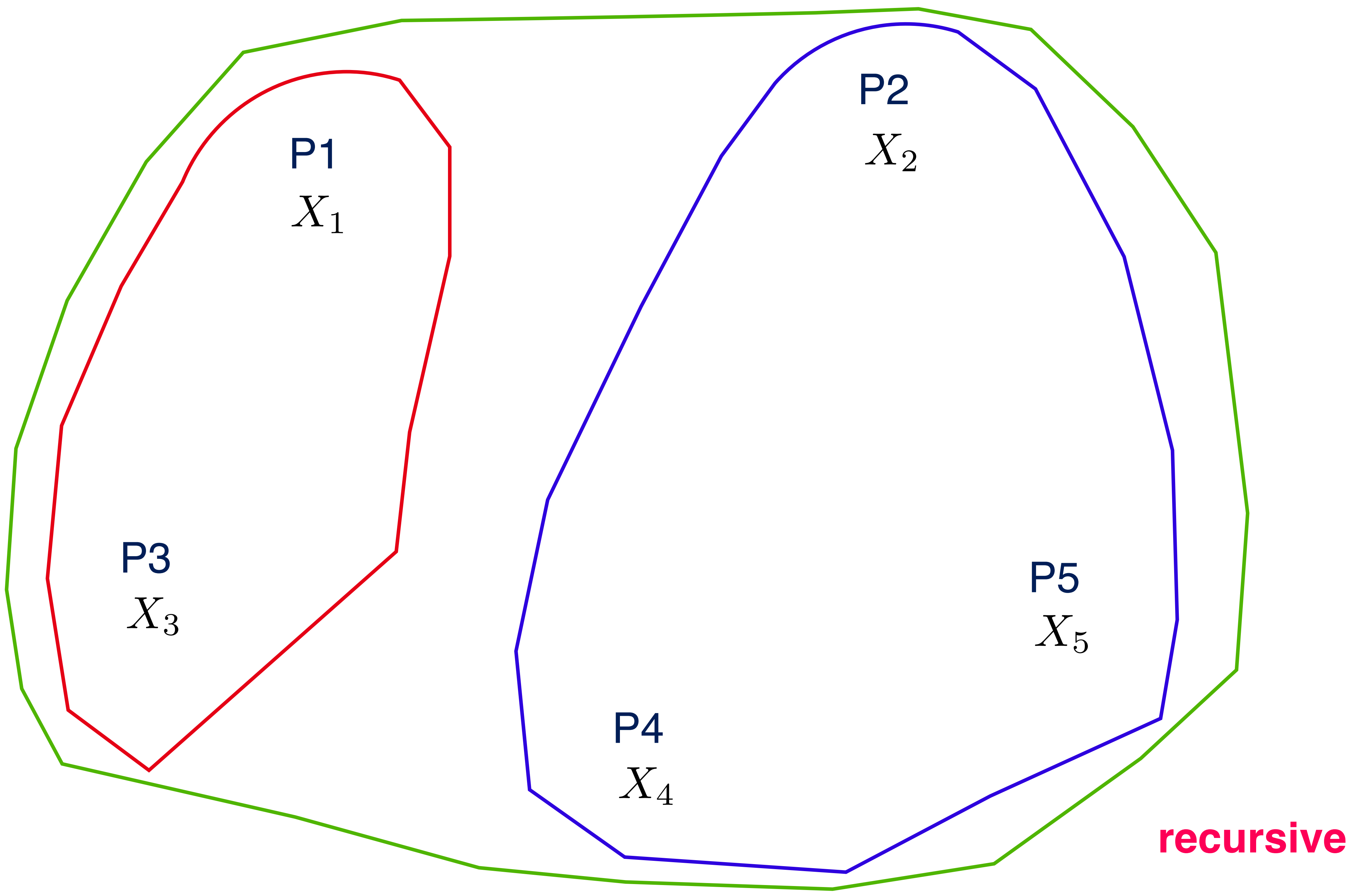
Recursive Structure



Recursive Structure



Recursive Structure



Performance of Universal RDE

Corollary (rough statement)

The protocol recursively attain omniscience with rate

$$R(\mathrm{P}_{\mathbf{x}_{\mathcal{M}}}) + \mathcal{O}(\Delta) + \mathcal{O}\left(\frac{1}{n\Delta}\right) + \mathcal{O}\left(\frac{\log n}{n}\right)$$

slack of rate increment

rate for Ack/Nack
proportional to #rounds $\mathcal{O}(1/\Delta)$

Some Open Problems

Some Open Problems

(1) Non-degraded case:

- Even the first-order capacity is not known in general.
- When interaction is not allowed, capacity is known but involves auxiliary RVs.
- What is the second-order rate when the capacity is known?

Some Open Problems

(1) Non-degraded case:

- Even the first-order capacity is not known in general.
- When interaction is not allowed, capacity is known but involves auxiliary RVs.
- What is the second-order rate when the capacity is known?

(2) Necessity of interaction to attain the optimal second-order rate

- Even for the degraded case, the standard protocol does not attain the optimal second-order rate.

- How about other non-interactive protocols? Interaction is necessary?

Some Open Problems

(1) Non-degraded case:

- Even the first-order capacity is not known in general.
- When interaction is not allowed, capacity is known but involves auxiliary RVs.
- What is the second-order rate when the capacity is known?

(2) Necessity of interaction to attain the optimal second-order rate

- Even for the degraded case, the standard protocol does not attain the optimal second-order rate.
- How about other non-interactive protocols? Interaction is necessary?

(3) Universal protocol for the case with helpers

- When only subset $\mathcal{A} \subset \mathcal{M}$ try to attain omniscience, is there universal protocol?
- Slepian-Wolf coding is known to be optimal, but the rate formula is more involved.

Thank you for listening.