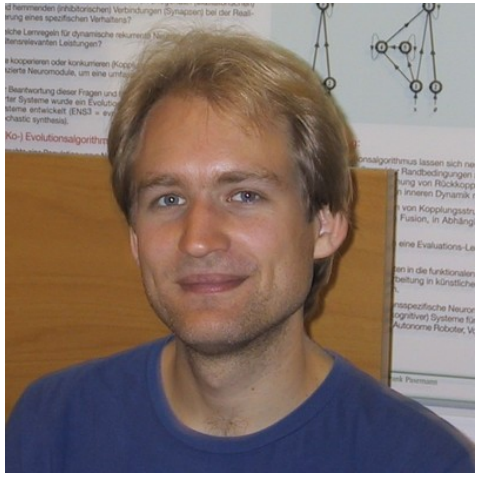
Unique Information and Secret Key Decompositions

Pradeep Kr. Banerjee
MPI MiS
pradeep@mis.mpg.de

IEEE International Symposium on Information Theory (ISIT)
Paris, July 2019

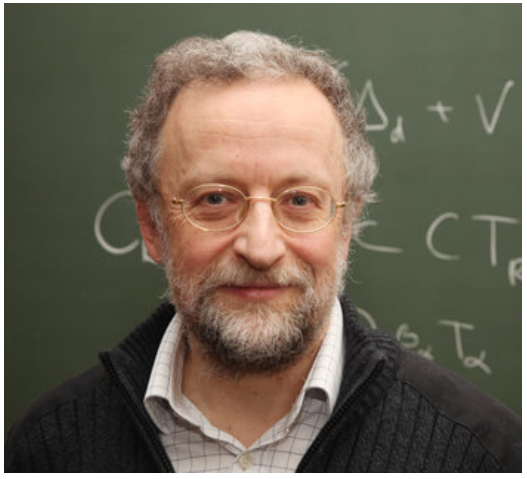
Max-Planck-Institut für
Mathematik
in den Naturwissenschaften

Joint work with



Johannes Rauh

Eckehard Olbrich



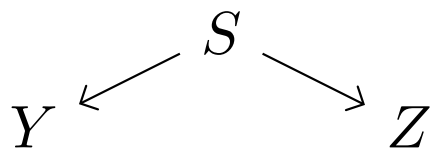
Jürgen Jost

1. Positive information decomposition and the UI
2. UI and secret key decomposition
3. UI-based bounds on secret key rates

Positive information decomposition and the UI

Positive information decomposition

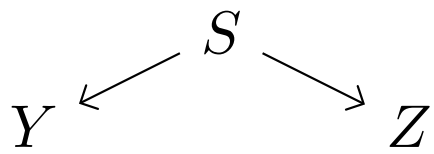
Suppose we want to know S, but can only observe Y and/or Z



How is the information about S distributed?

Positive information decomposition

Suppose we want to know S, but can only observe Y and/or Z



Classify information about S according to *"who knows what"*:

Williams and Beer (2010), "Nonnegative decomposition of multivariate information" [WB10]

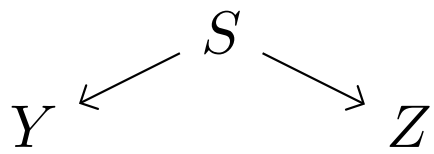
Unique: information *known to* Y*, but unknown to* Z

Redundant: information *known in common to* Y *and* Z

Synergistic: information that *materializes only when* Y *and* Z *act jointly*

Positive information decomposition

Suppose we want to know S, but can only observe Y and/or Z



Classify information about S according to *"who knows what"*:

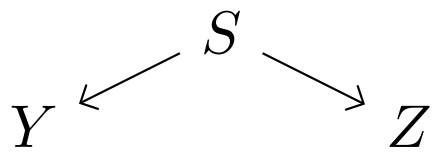
Williams and Beer (2010), "Nonnegative decomposition of multivariate information" [WB10]

Unique: information *known to* Y*, but unknown to* Z
Redundant: information *known in common to* Y *and* Z
Synergistic: information that *materializes only when* Y *and* Z *act jointly*

- Synergy: Y, Z independent binary, $S = \textsc{Xor}(Y, Z)$: $I(S;Y) = I(S;Z) = 0$, but $I(S;YZ) = 1$ bit
- Redundancy: $S = Y = Z$ uniform binary: $I(S;Y) = I(S;Z) = 1$ bit

Positive information decomposition

Suppose we want to know S, but can only observe Y and/or Z



Classify information about S according to *"who knows what"*:

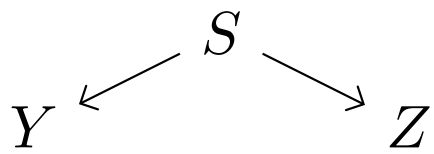
Williams and Beer (2010), "Nonnegative decomposition of multivariate information" [WB10]

Unique: information *known to* Y*, but unknown to* Z
Redundant: information *known in common to* Y *and* Z
Synergistic: information that *materializes only when* Y *and* Z *act jointly*

In general, all three flavors may be present at the same time.
How can we separate them?

Positive information decomposition

Suppose we want to know S, but can only observe Y and/or Z



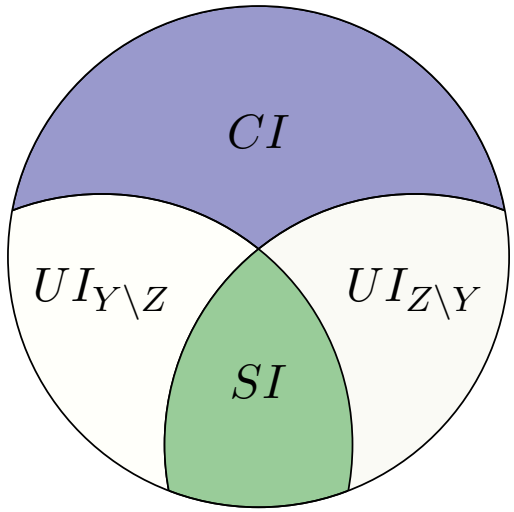
Mathematically, we are looking for a decomposition:

$$I(S;Y,Z) = \underbrace{SI(S;Y,Z)}_{\text{shared information (redundancy)}} + \underbrace{UI(S;Y\backslash Z)}_{\text{unique information of } Y} + \underbrace{UI(S;Z\backslash Y)}_{\text{unique information of } Z} + \underbrace{CI(S;Y,Z)}_{\text{complementary information (synergy)}}$$

$$I(S;Y) = SI(S;Y,Z) + UI(S;Y\backslash Z)$$

$$I(S;Z) = SI(S;Y,Z) + UI(S;Z\backslash Y)$$

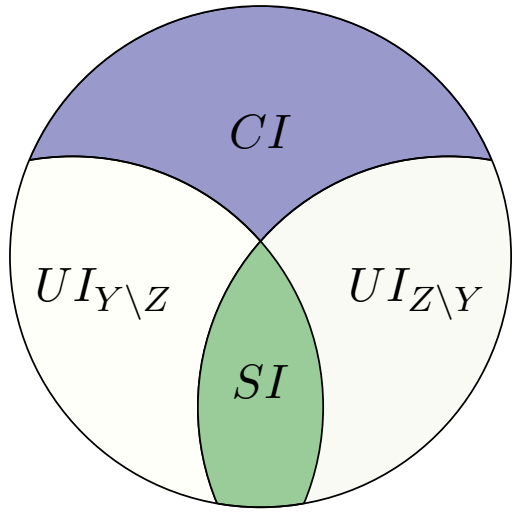
Information decomposition



$I(S;Y,Z)$

Need to fix a degree of freedom

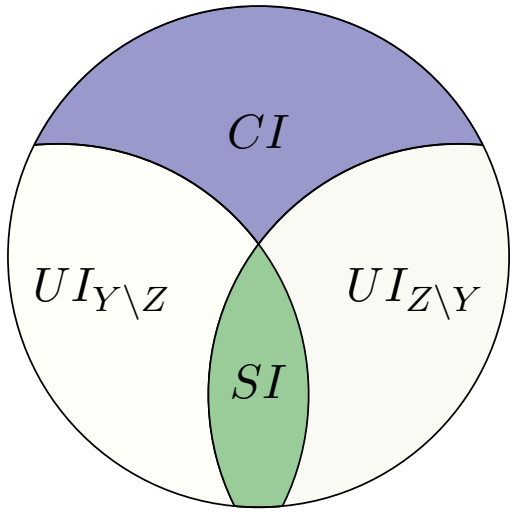
Information decomposition



$I(S;Y,Z)$

Need to fix a degree of freedom

Information decomposition

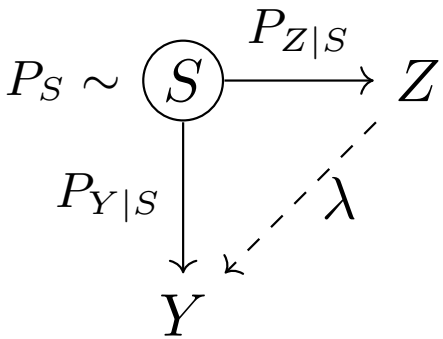


$I(S;Y,Z)$

Need to fix a degree of freedom

The Unique Information (UI)

Bertschinger, Rauh, Olbrich, Jost, Ay (2014) [BRO$^+$14]

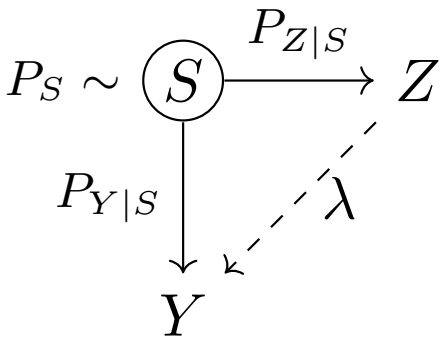


$$UI_P(S;Y\backslash Z) := \min_{Q\in\Delta_P} I_Q(S;Y|Z)$$

$$\Delta_P = \left\{Q_{SYZ} \in \Delta \colon Q_{SY} = P_{SY},\ Q_{SZ} = P_{SZ}\right\}$$

The Unique Information (UI)

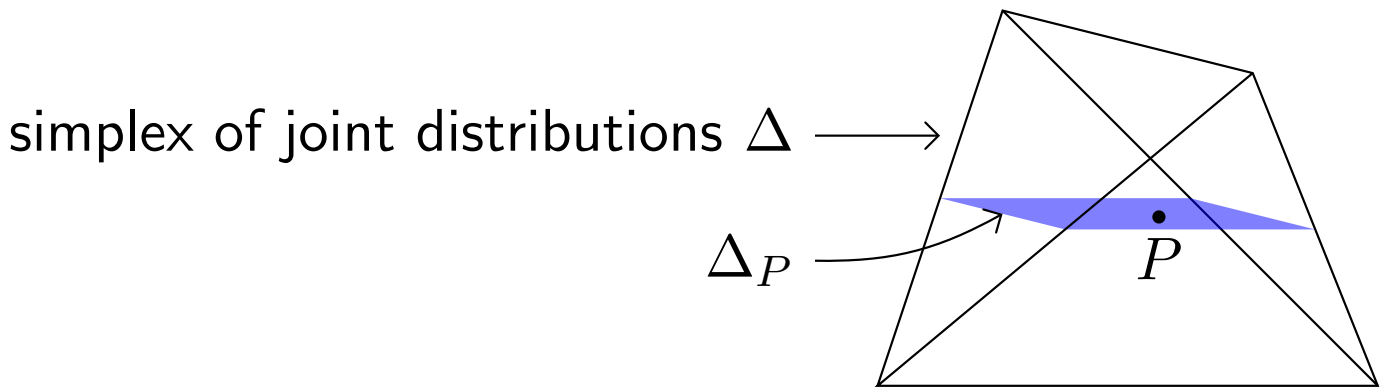
Bertschinger, Rauh, Olbrich, Jost, Ay (2014) [BRO$^+$14]



$$UI_P(S;Y\backslash Z) := \min_{Q\in\Delta_P} I_Q(S;Y|Z)$$

$$\Delta_P = \{Q_{SYZ} \in \Delta \colon Q_{SY} = P_{SY},\ Q_{SZ} = P_{SZ}\}$$

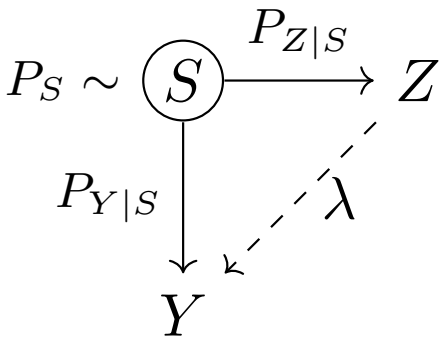
Convex program over a polytope of dimension $|\mathcal{S}|(|\mathcal{Y}|-1)(|\mathcal{Z}|-1)$



Computing the Unique Information, Proc. IEEE ISIT, [BRM18]

The Unique Information (UI)

Bertschinger, Rauh, Olbrich, Jost, Ay (2014) [BRO$^+$14]



$$UI_P(S;Y\backslash Z) := \min_{Q\in\Delta_P} I_Q(S;Y|Z)$$

$$\Delta_P = \left\{Q_{SYZ} \in \Delta \colon Q_{SY} = P_{SY},\ Q_{SZ} = P_{SZ}\right\}$$

Theorem 1 ([BRO$^+$14])

$UI(S;Y\backslash Z) = 0$ *if and only if there is a stochastic matrix* λ *with*

$$P(y|s) = \sum_z \lambda(y|z)P(z|s).$$

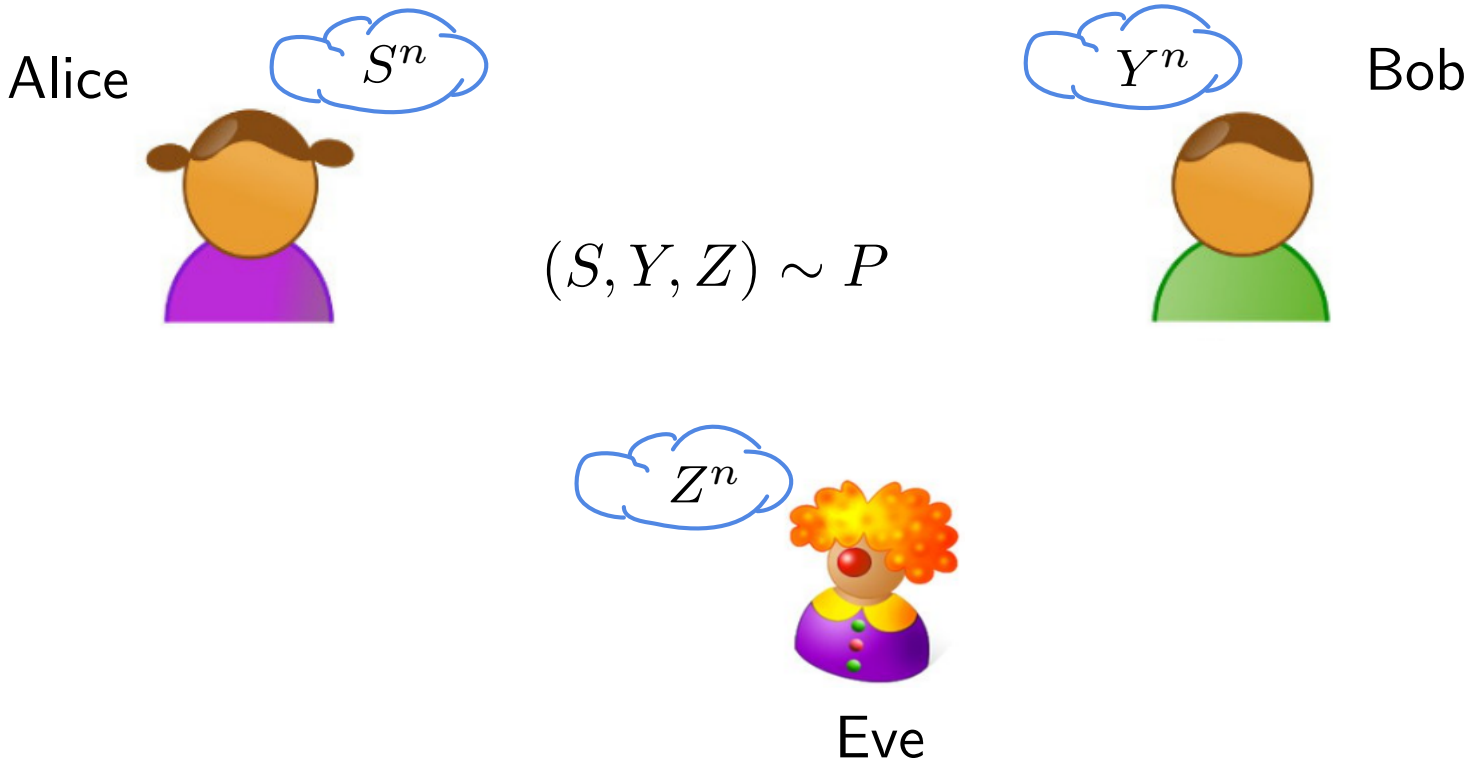
D. Blackwell, "Equivalent comparisons of experiments," Ann. Math. Stat. [Bla53]

Corollary 2 (by Blackwell's theorem)

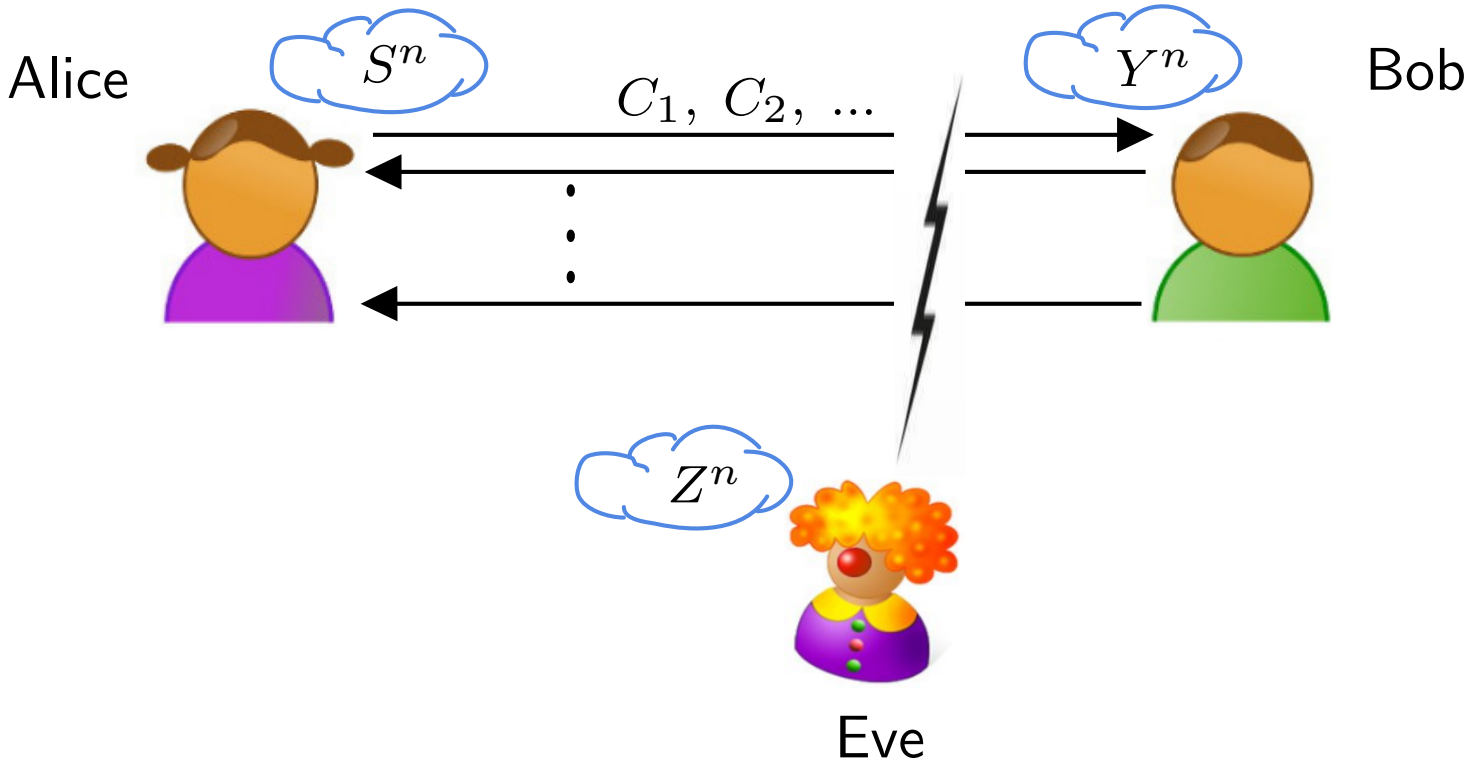
$UI(S;Y\backslash Z) = 0 \iff$ *Z performs better than Y in any decision problem.*

UI and secret key decomposition

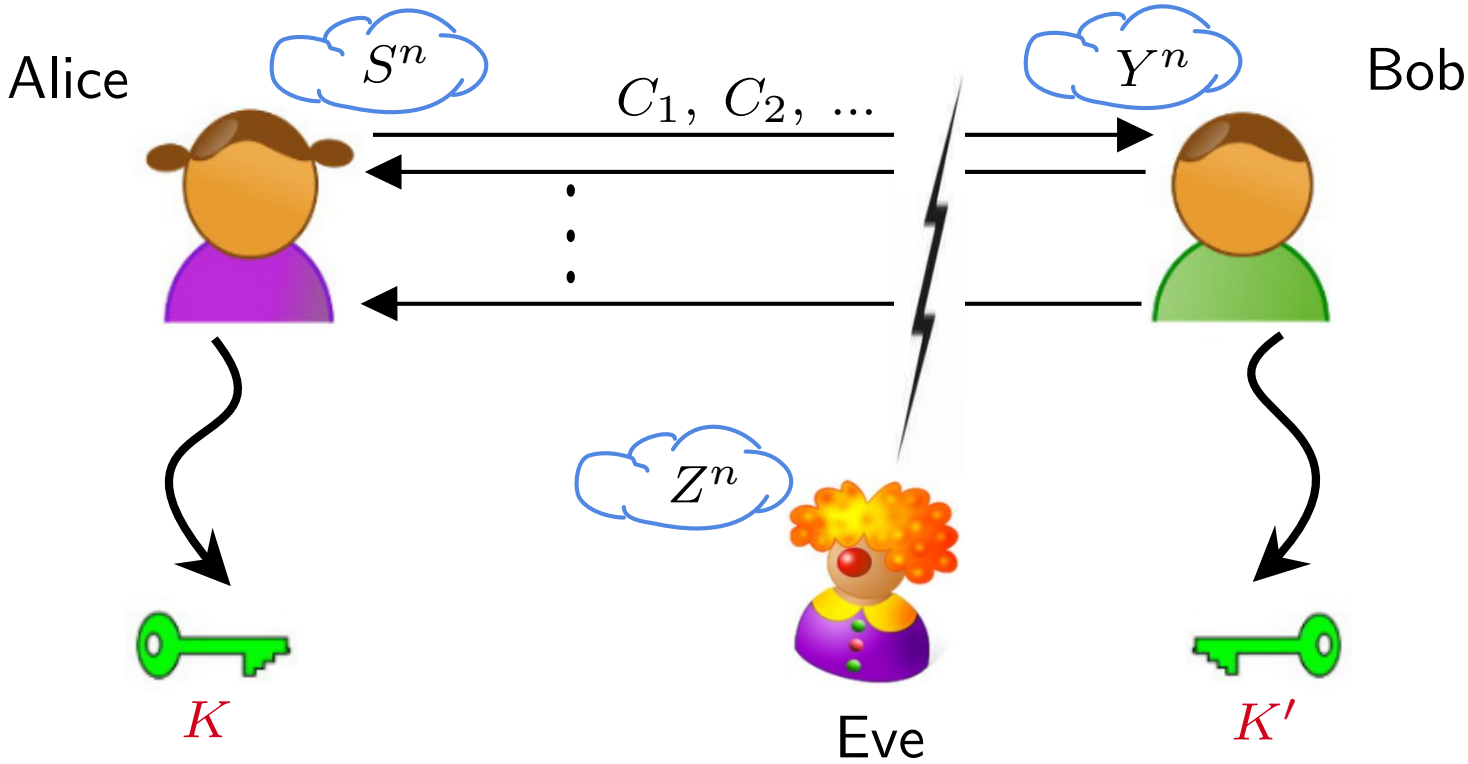
The secret key agreement problem



The secret key agreement problem



The secret key agreement problem



$$\Pr[K = K'] \approx 1$$

$$I(K; Z^n, \vec{C}) \approx 0$$

$$\frac{1}{n} H(K)$$

The one-way secret key rate ($S_{\rightarrow}$)

- The protocol is *one-way* if Alice is allowed to send only one message and Bob none
- Ahlswede and Csiszár [AC93] showed:

$$S_{\rightarrow}(S;Y|Z) = \max_{P_{UV|SYZ}:V-U-S-YZ} I(U;Y|V) - I(U;Z|V)$$

where it suffices to restrict the range of U and V resp. to $|\mathcal{S}|^2$ and $|\mathcal{S}|$

The one-way secret key rate ($S_{\rightarrow}$)

- The protocol is *one-way* if Alice is allowed to send only one message and Bob none
- Ahlswede and Csiszár [AC93] showed:

$$S_{\rightarrow}(S;Y|Z) = \max_{P_{UV|SYZ}:V-U-S-YZ} I(U;Y|V) - I(U;Z|V)$$

  where it suffices to restrict the range of U and V resp. to $|\mathcal{S}|^2$ and $|\mathcal{S}|$

- No analogous formula for the two-way secret key rate, $S_{\leftrightarrow}(S;Y|Z)$
- Value of $S_{\leftrightarrow}$ is known only for a handful of distributions

Bounds on the two-way secret key rate

Trivial upper bound [Mau93]

$$S_{\leftrightarrow}(S;Y|Z) \leq \min\{I(S;Y), I(S;Y|Z)\}$$

Intrinsic information [MW99]

$$I_{\downarrow}(S;Y|Z) := \min_{P_{Z'|Z}} I(S;Y|Z'),\ |\mathcal{Z}'| \leq |\mathcal{Z}|$$

Reduced intrinsic information [RW03]

$$I_{\downarrow\downarrow}(S;Y|Z) := \inf_{P_{U|SYZ}} I_{\downarrow}(S;Y|ZU) + H(U)$$

Bounds on the two-way secret key rate

Trivial upper bound [Mau93]

$$S_{\leftrightarrow}(S;Y|Z) \leq \min\{I(S;Y), I(S;Y|Z)\}$$

Intrinsic information [MW99]

$$I_{\downarrow}(S;Y|Z) := \min_{P_{Z'|Z}} I(S;Y|Z'),\ |\mathcal{Z}'| \leq |\mathcal{Z}|$$

Reduced intrinsic information [RW03]

$$I_{\downarrow\downarrow}(S;Y|Z) := \inf_{P_{U|SYZ}} I_{\downarrow}(S;Y|ZU) + H(U)$$

Secret key decomposition-based bounds [GA10, GA17]

$$B_1(S;Y|Z) := \min_{P_{Z'|SYZ}} I(S;Y|Z') + I(SY;Z'|Z),\ |\mathcal{Z}'| \leq |\mathcal{S}||\mathcal{Y}||\mathcal{Z}|$$

Bounds on the two-way secret key rate

Trivial upper bound [Mau93]

$$S_{\leftrightarrow}(S;Y|Z) \leq \min\{I(S;Y), I(S;Y|Z)\}$$

Intrinsic information [MW99]

$$I_{\downarrow}(S;Y|Z) := \min_{P_{Z'|Z}} I(S;Y|Z'),\ |\mathcal{Z}'| \leq |\mathcal{Z}|$$

Reduced intrinsic information [RW03]

$$I_{\downarrow\downarrow}(S;Y|Z) := \inf_{P_{U|SYZ}} I_{\downarrow}(S;Y|ZU) + H(U)$$

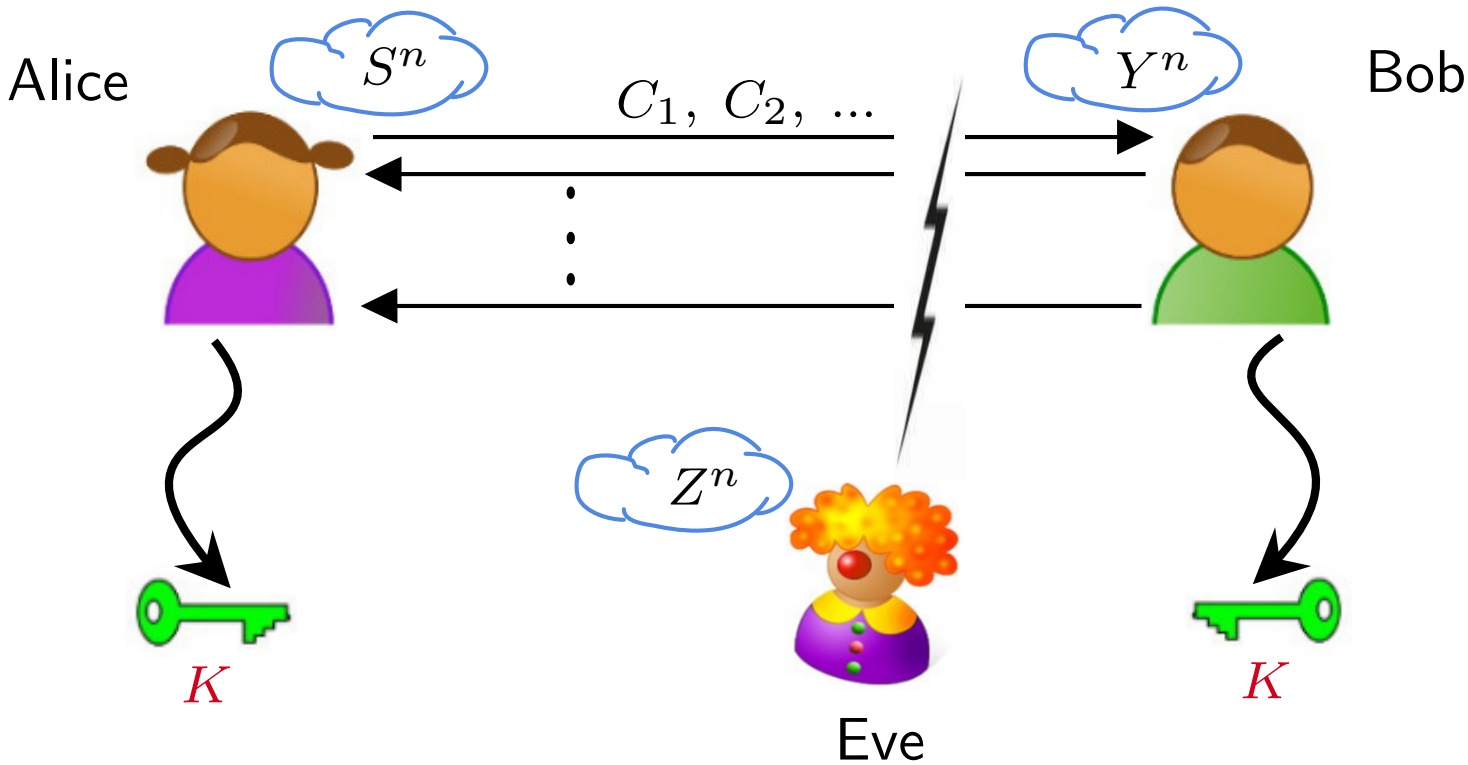
Secret key decomposition-based bounds [GA10, GA17]

$$B_1(S;Y|Z) := \min_{P_{Z'|SYZ}} I(S;Y|Z') + I(SY;Z'|Z),\ |\mathcal{Z}'| \leq |\mathcal{S}||\mathcal{Y}||\mathcal{Z}|$$

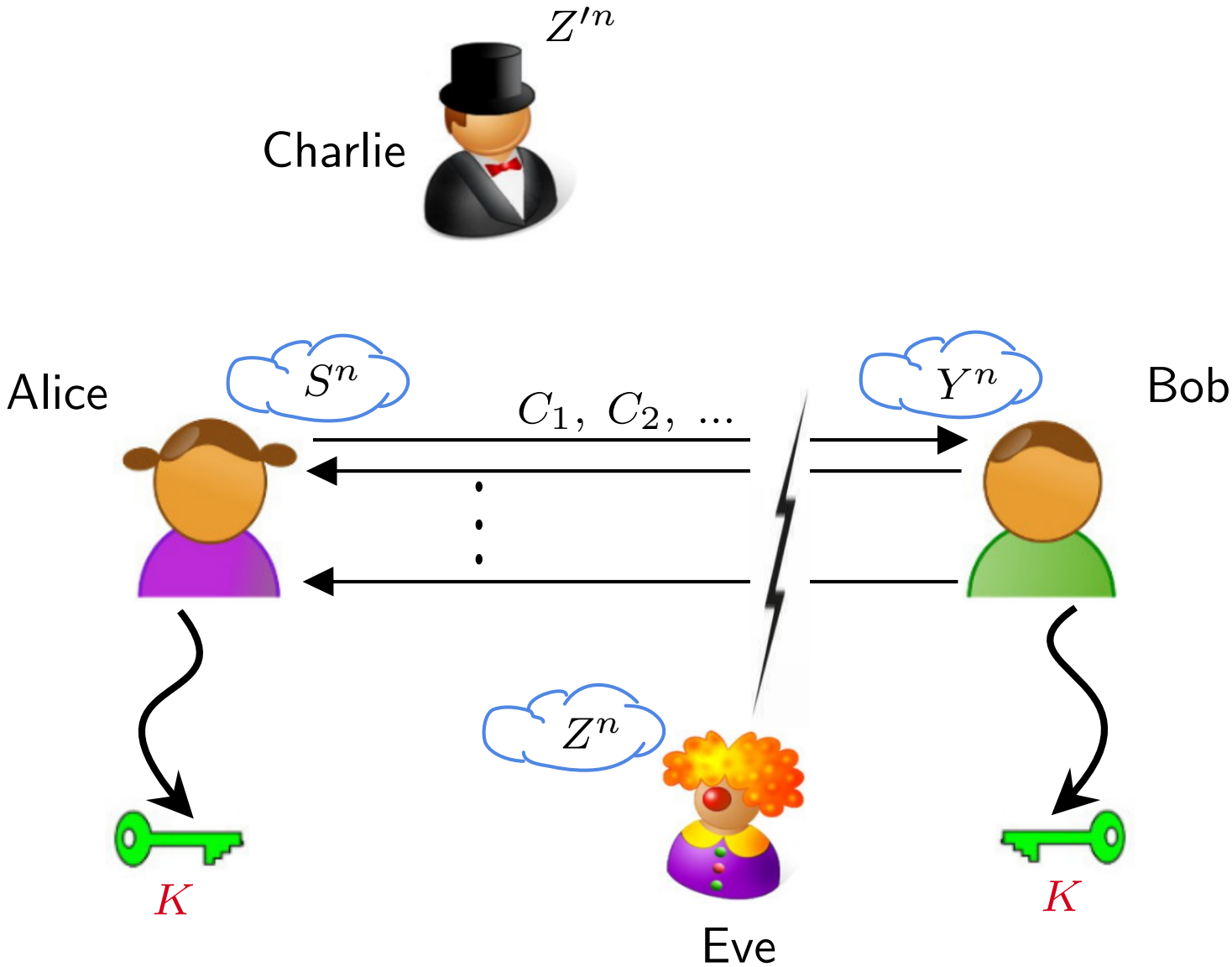
Full chain of bounds on $S_{\leftrightarrow}$

$$S_{\rightarrow} \leq S_{\leftrightarrow} \leq B_1 \leq I_{\downarrow\downarrow} \leq I_{\downarrow} \leq I$$

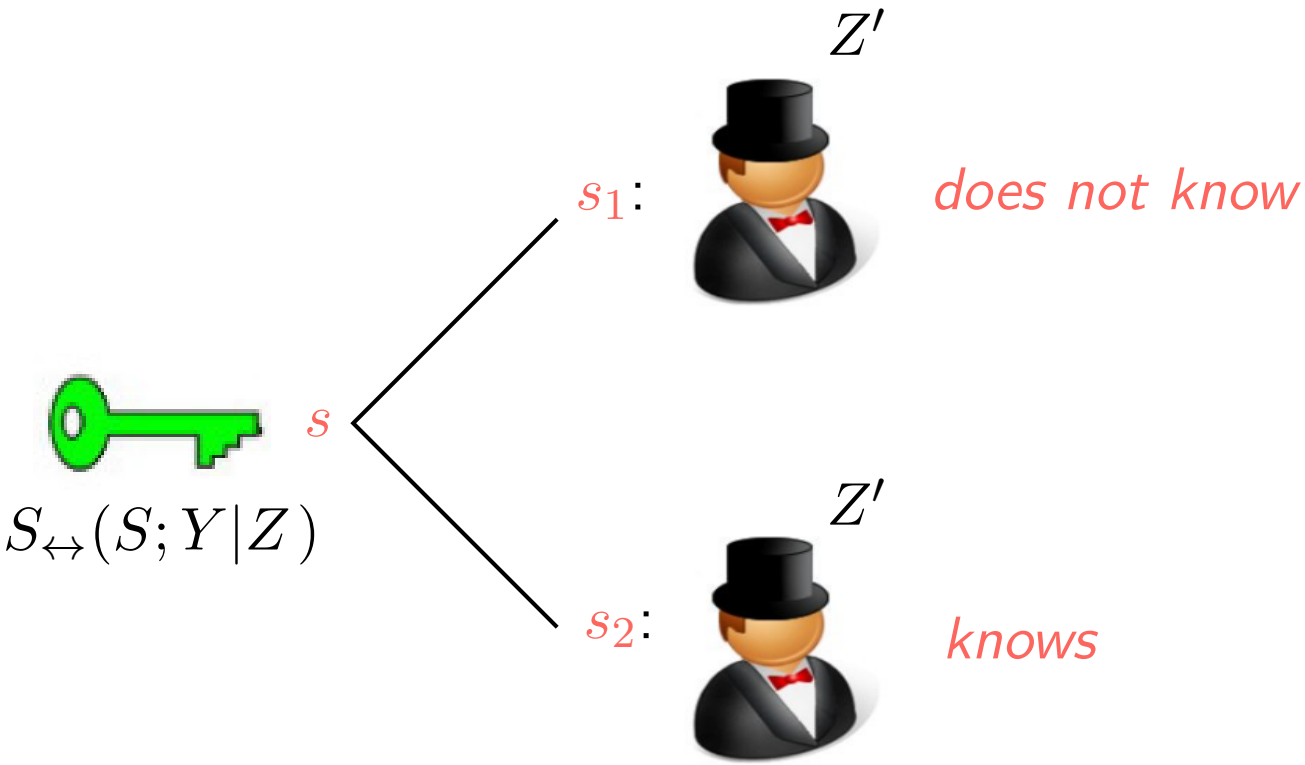
Secret key decomposition



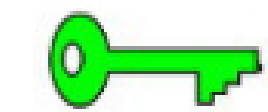
Secret key decomposition



Secret key decomposition



Secret key decomposition



$S_{\leftrightarrow}(S;Y|Z)$

s

s_1:

Z'

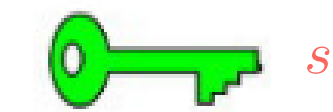
does not know $\leq \underbrace{S_{\leftrightarrow}(S;Y|Z')}_{\text{unique (w.r.t. } Z')}$

s_2:

Z'

knows $\leq \underbrace{S_{\rightarrow}(SY;Z'|Z)}_{\text{shared (with } Z')}$

Secret key decomposition



$S_{\leftrightarrow}(S;Y|Z)$

s

s_1:

Z'

does not know $\leq \underbrace{S_{\leftrightarrow}(S;Y|Z')}_{\text{unique (w.r.t. } Z')}$

s_2:

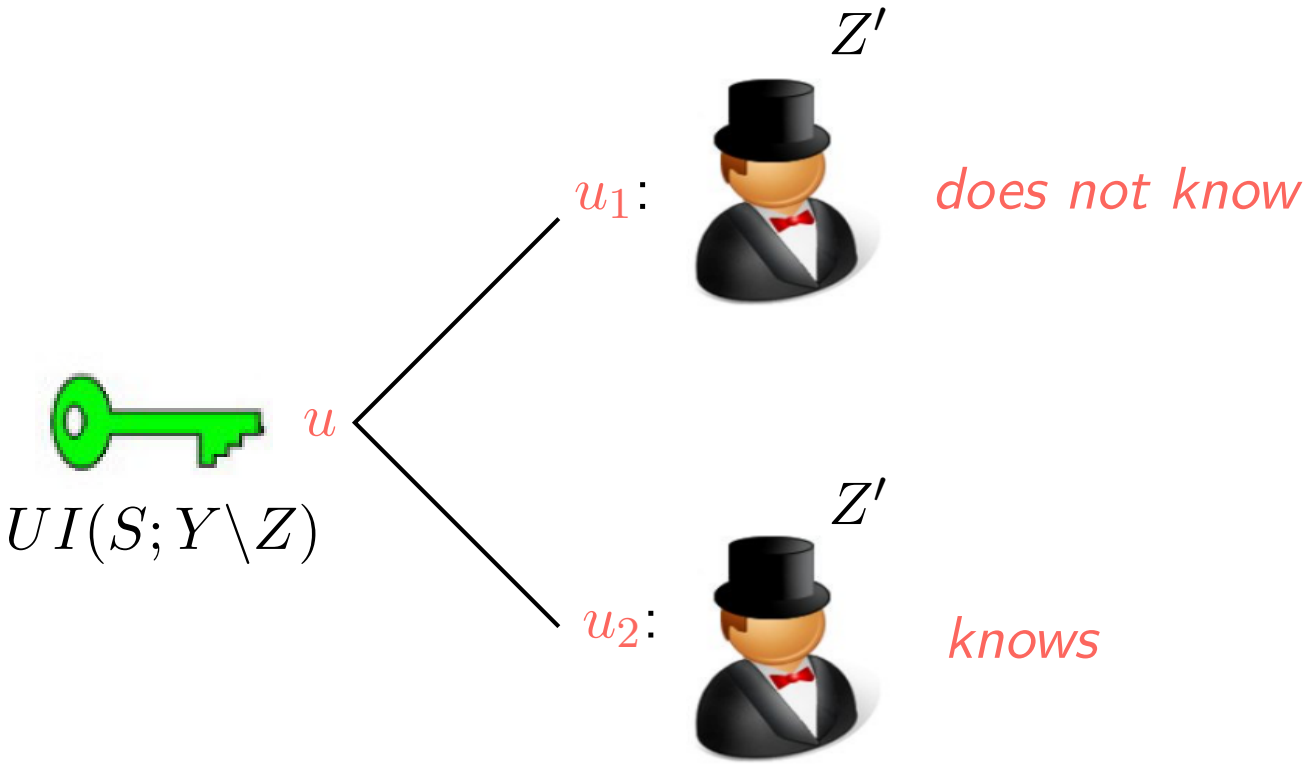
Z'

knows $\leq \underbrace{S_{\rightarrow}(SY;Z'|Z)}_{\text{shared (with } Z')}$

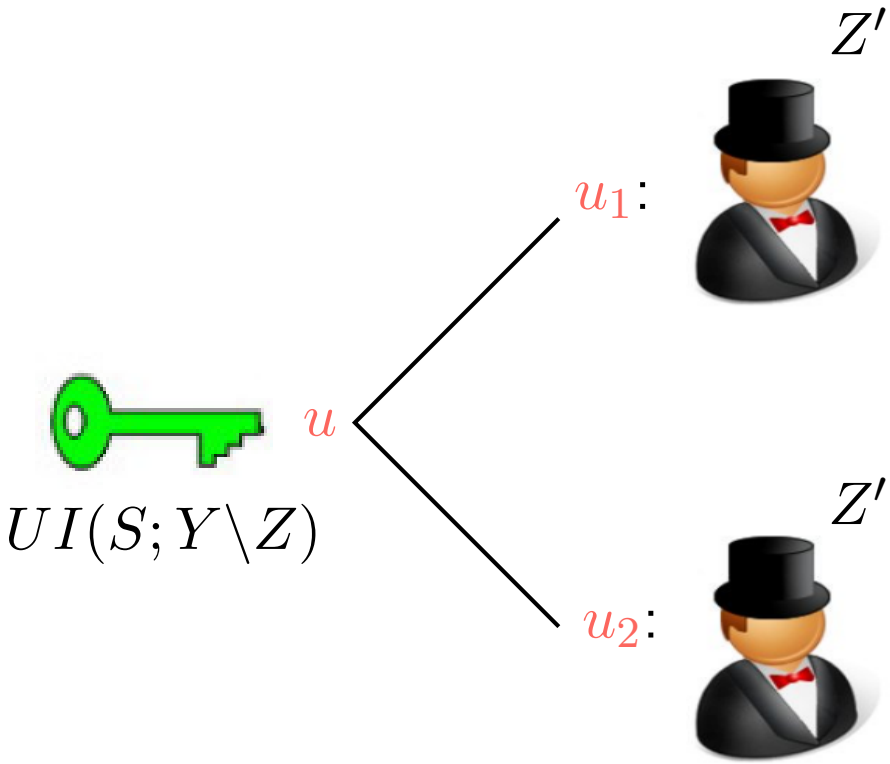
Secret key decomposition property [GA10, GA17]

$$\forall\,(S,Y,Z,Z'):\ S_{\leftrightarrow}(S;Y|Z) \leq \underbrace{S_{\leftrightarrow}(S;Y|Z')}_{\text{unique (w.r.t. } Z')} + \underbrace{S_{\rightarrow}(SY;Z'|Z)}_{\text{shared (with } Z')}$$

Unique information decomposition



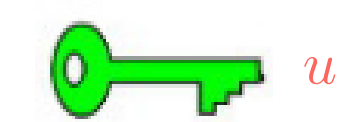
Unique information decomposition



does not know $UI(S;Y\backslash Z,Z')$ $\leq \underbrace{UI(S;Y\backslash Z')}_{\text{unique (w.r.t. } Z')}$

knows $\leq \underbrace{UI(S;Z'\backslash Z)}_{\text{shared (with } Z')}$

Unique information decomposition



$UI(S;Y\backslash Z)$

u

u_1: Z'

does not know $UI(S;Y\backslash Z,Z')$ $\leq \underbrace{UI(S;Y\backslash Z')}_{\text{unique (w.r.t. } Z')}$

u_2: Z'

knows $\leq \underbrace{UI(S;Z'\backslash Z)}_{\text{shared (with } Z')}$

Triangle inequality for the UI [RBOJ19]

$$\forall\,(S,Y,Z,Z'):\ UI(S;Y\backslash Z) \leq \underbrace{UI(S;Y\backslash Z')}_{\text{unique (w.r.t. } Z')} + \underbrace{UI(S;Z'\backslash Z)}_{\text{shared (with } Z')}$$

UI and Secret key decomposition

Unique information decomposition property [RBOJ19]

$$\forall\,(S,Y,Z,Z'):\ UI(S;Y\backslash Z)\leq UI(S;Y\backslash Z')+UI(SY;Z'\backslash Z)$$

$$UI\leq B_1\leq I_{\downarrow\downarrow}\leq I_{\downarrow}\leq I$$

Secret key decomposition property [GA10, GA17]

$$\forall\,(S,Y,Z,Z'):\ S_{\leftrightarrow}(S;Y|Z)\leq S_{\leftrightarrow}\big(S;Y\big|Z'\big)+S_{\rightarrow}\big(SY;Z'|Z\big)$$

$\longrightarrow$ Key takeaway: The UI is similar in spirit to the secret key rates

- $UI(S;Y\backslash Z)$: *Information about S known to Y but unknown to Z*
- $S_{\leftrightarrow}(S;Y|Z)$: *Information common to S and Y that is unique w.r.t. Z*

UI-based bounds on secret key rates

UI is a secrecy monotone

Key property: UI is *nonincreasing* under local operations (LO) of Alice and Bob and one-way public communication (PC) by Alice

Theorem 3

$$S_{\rightarrow} \leq UI$$

UI is a secrecy monotone

Key property: UI is *nonincreasing* under local operations (LO) of Alice and Bob and one-way public communication (PC) by Alice

Theorem 3

$$S_{\rightarrow} \leq UI$$

Theorem 4

Let (S, Y, Z) be a triple of random variables such that $S_{\leftrightarrow}(S;Y|Z) > 0$. If either $UI(S;Y\backslash Z)$ or $UI(Y;S\backslash Z)$ vanishes, then the secret key rate in the active adversary scenario vanishes, or else it equals $S_{\leftrightarrow}(S;Y|Z)$.

UI-based bounds on secret key rates

Theorem 5

$$S_{\rightarrow} \leq UI \leq B_1 \leq I_{\downarrow\downarrow} \leq I_{\downarrow} \leq I$$

Full chain of bounds on $S_{\leftrightarrow}$

$$S_{\rightarrow} \leq S_{\leftrightarrow} \leq B_1 \leq I_{\downarrow\downarrow} \leq I_{\downarrow} \leq I$$

UI-based bounds on secret key rates

Theorem 5

$$S_{\rightarrow} \leq UI \leq B_1 \leq I_{\downarrow\downarrow} \leq I_{\downarrow} \leq I$$

Full chain of bounds on $S_{\leftrightarrow}$

$$S_{\rightarrow} \leq S_{\leftrightarrow} \leq B_1 \leq I_{\downarrow\downarrow} \leq I_{\downarrow} \leq I$$

Given $(S, Y, Z) \sim P$, let

$$\begin{aligned} Q^* &\in \operatorname{argmin}_{Q \in \Delta_P} I_Q(S;Y|Z) \\ CI_P(S;Y,Z) &= I_P(S;Y|Z) - UI(S;Y\backslash Z) \\ &= I_P(S;Y|Z) - I_{Q^*}(S;Y|Z) \end{aligned}$$

Q^* is called a *minimum synergy distribution*, as

$$CI_P(S;Y,Z) = 0 \text{ if and only if } P = Q^*$$

UI-based bounds on secret key rates

Theorem 5

$$S_{\rightarrow} \leq UI \leq B_1 \leq I_{\downarrow\downarrow} \leq I_{\downarrow} \leq I$$

Full chain of bounds on $S_{\leftrightarrow}$

$$S_{\rightarrow} \leq S_{\leftrightarrow} \leq B_1 \leq I_{\downarrow\downarrow} \leq I_{\downarrow} \leq I$$

Given $(S, Y, Z) \sim P$, let

$$\begin{aligned} Q^* &\in \operatorname{argmin}_{Q \in \Delta_P} I_Q(S;Y|Z) \\ CI_P(S;Y,Z) &= I_P(S;Y|Z) - UI(S;Y\backslash Z) \\ &= I_P(S;Y|Z) - I_{Q^*}(S;Y|Z) \end{aligned}$$

Q^* is called a *minimum synergy distribution*, as

$$CI_P(S;Y,Z) = 0 \text{ if and only if } P = Q^*$$

$\longrightarrow$ Choosing $P = Q^*$, all upper bounds on $S_{\leftrightarrow}$ collapse to the UI

A conjecture

UI *cannot* be an upper bound on the two-way rate:

- If the pairs (S, Y) and (S, Z) have the same distribution, then $UI(S; Y \backslash Z) = UI(S; Z \backslash Y) = 0$
- $S_{\leftrightarrow}$ can still be positive in such a situation [GA17]

Conjecture 6

$UI(S; Y \backslash Z) \leq S_{\leftrightarrow}(S; Y|Z)$

A conjecture

UI *cannot* be an upper bound on the two-way rate:

- If the pairs (S, Y) and (S, Z) have the same distribution, then $UI(S; Y \backslash Z) = UI(S; Z \backslash Y) = 0$
- $S_{\leftrightarrow}$ can still be positive in such a situation [GA17]

Conjecture 6

$UI(S; Y \backslash Z) \leq S_{\leftrightarrow}(S; Y|Z)$

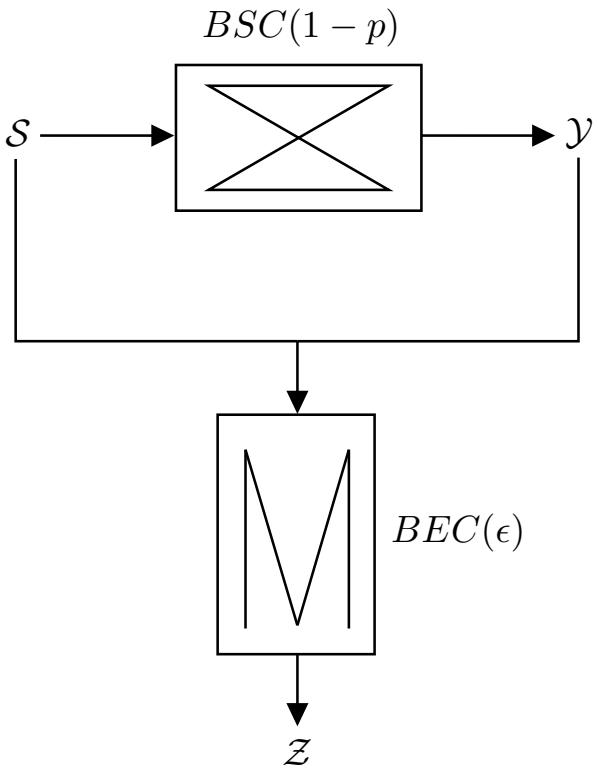
Sandwich bound on $S_{\leftrightarrow}(S; Y|Z)$: If Conjecture 6 is true, then

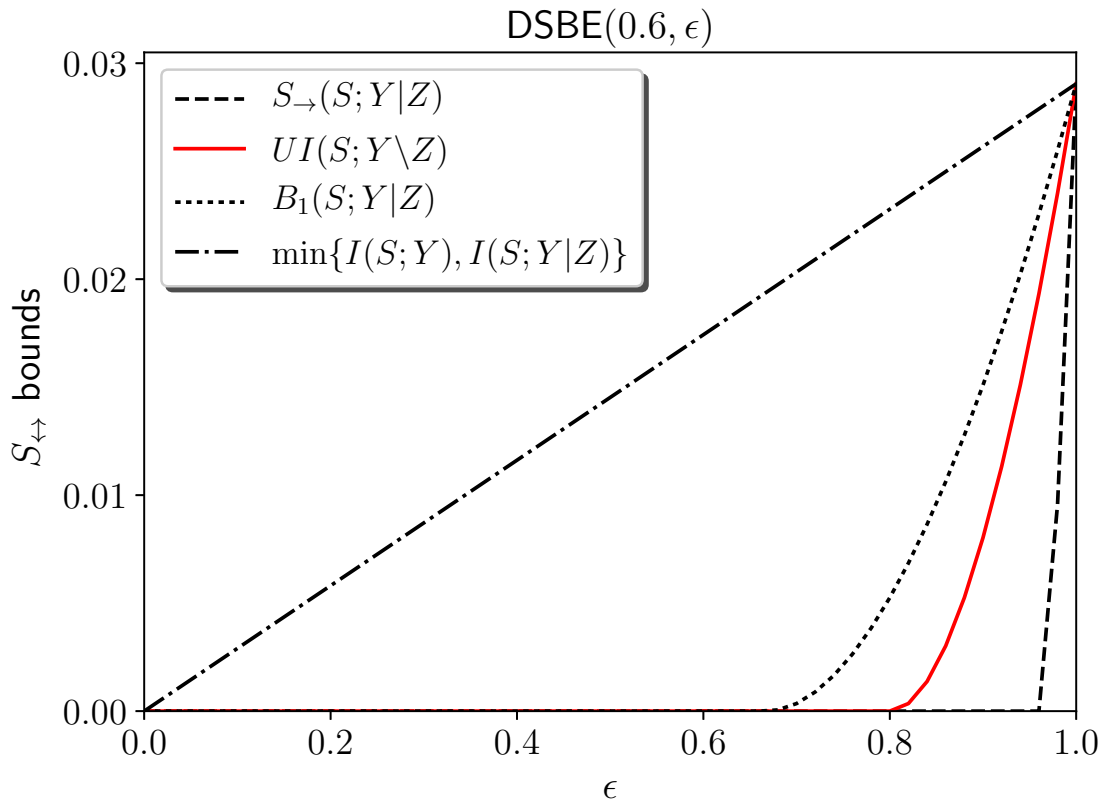
$$UI(S; Y \backslash Z) = I_{Q^*}(S; Y|Z) \leq S_{\leftrightarrow}(S; Y|Z) \leq I_P(S; Y|Z)$$

The set of all Q^* is a set of distributions for which the UI equals $S_{\leftrightarrow}$

$\longrightarrow$ **Operationalizes the** UI

DSBE source example





- $S_{\leftrightarrow} = 0 \iff \epsilon \leq \frac{1-p}{p}$
- $UI = 0 \iff \epsilon \leq 2(1-p)$

References I

Rudolf Ahlswede and Imre Csiszár.
Common randomness in information theory and cryptography. I. Secret sharing.
IEEE Transactions on Information Theory, 39(4):1121–1132, 1993.

David Blackwell.
Equivalent comparisons of experiments.
The Annals of Mathematical Statistics, 24(2):265–272, 1953.

Pradeep Kr. Banerjee, Eckehard Olbrich, Jürgen Jost, and Johannes Rauh.
Unique informations and deficiencies.
In *Proceedings of the 56th Annual Allerton Conference on Communication, Control and Computing*, pages 32–38, 2018.

Pradeep Kr. Banerjee, Johannes Rauh, and Guido Montúfar.
Computing the unique information.
In *Proc. IEEE ISIT*, pages 141–145. IEEE, 2018.

Nils Bertschinger, Johannes Rauh, Eckehard Olbrich, Jürgen Jost, and Nihat Ay.
Quantifying unique information.
Entropy, 16(4):2161–2183, 2014.

Amin Aminzadeh Gohari and Venkat Anantharam.
Information-theoretic key agreement of multiple terminals–Part I.
IEEE Transactions on Information Theory, 56(8):3973–3996, 2010.

Amin Aminzadeh Gohari and Venkat Anantharam.
Comments on "Information-theoretic key agreement of multiple terminals–Part I".
IEEE Transactions on Information Theory, 63(8):5440–5442, 2017.

Amin Aminzadeh Gohari, Onur Günlü, and Gerhard Kramer.
Coding for positive rate in the source model key agreement problem.
arXiv preprint arXiv:1709.05174, 2018.

References II

Ueli M Maurer.

Secret key agreement by public discussion from common information.
IEEE Transactions on Information Theory, 39(3):733–742, 1993.

Ueli M. Maurer and Stefan Wolf.

Unconditionally secure key agreement and the intrinsic conditional information.
IEEE Transactions on Information Theory, 45(2):499–514, 1999.

Ueli M. Maurer and Stefan Wolf.

Secret-key agreement over unauthenticated public channels II: the simulatability condition.
IEEE Transactions on Information Theory, 49(4):832–838, 2003.

Johannes Rauh, Pradeep Kr. Banerjee, Eckehard Olbrich, and Jürgen Jost.

Unique information and secret key decompositions.
In *Proc. IEEE ISIT (to appear)*. IEEE, 2019.

Renato Renner and Stefan Wolf.

New bounds in secret-key agreement: The gap between formation and secrecy extraction.
In *Advances in Cryptology - EUROCRYPT 2003, Warsaw, Poland*, pages 562–577, 2003.

Claude Elwood Shannon.

A mathematical theory of communication.
Bell System Technical Journal, 27(3):379–423, 1948.

Paul Williams and Randall Beer.

Nonnegative decomposition of multivariate information.
arXiv:1004.2515v1, 2010.

Unique information and deficiencies

Output deficiency

$$\mathcal{S} \xrightarrow{\kappa} \mathcal{Y}$$

$$\mathcal{S} \xrightarrow{\mu} \mathcal{Z} \overset{\lambda}{\dashrightarrow} \mathcal{Y}$$

$$\delta_o^{\pi}(\mu, \kappa) := \min_{\lambda \in \mathsf{M}(\mathcal{Z};\mathcal{Y})} D(\kappa \| \lambda \circ \mu | \pi_S)$$

Input deficiency

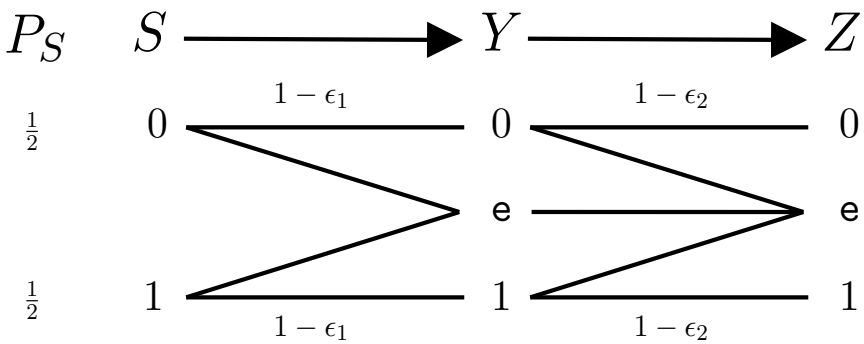
$$\mathcal{Y} \xrightarrow{\bar{\kappa}} \mathcal{S}$$

$$\mathcal{Y} \overset{\bar{\lambda}}{\dashrightarrow} \mathcal{Z} \xrightarrow{\bar{\mu}} \mathcal{S}$$

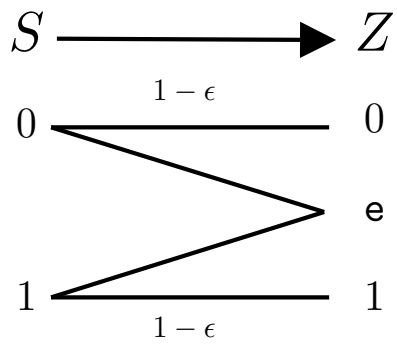
$$\delta_i^{\pi}(\bar{\mu}, \bar{\kappa}) := \min_{\bar{\lambda} \in \mathsf{M}(\mathcal{Y};\mathcal{Z})} D(\bar{\kappa} \| \bar{\mu} \circ \bar{\lambda} | \pi_Y)$$

Unique informations and deficiencies, Proc. IEEE Allerton, [BOJR18]

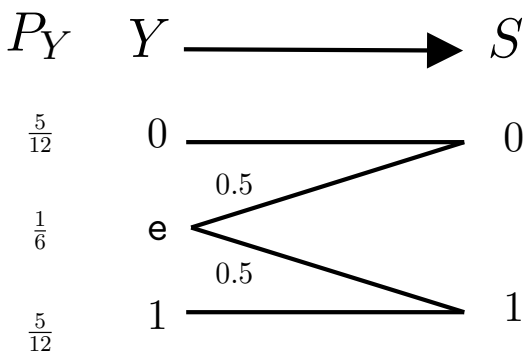
Vanishing sets of UI and δ_i^π are different

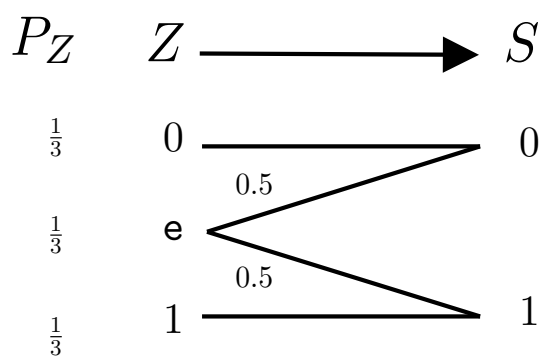


$\epsilon_1 = \frac{1}{6}$ $\epsilon_2 = \frac{1}{5}$



$\epsilon = 1-(1-\epsilon_1)(1-\epsilon_2) = \frac{1}{3}$





$UI = \frac{1}{6}$ $\delta_i^\pi = 0$

Properties of the UI

Non-locking and monotonicity under LO of Eve

The secret key rate is non-locking:

$$\forall\ (S,Y,Z,U):\ S_{\leftrightarrow}(S;Y|ZU)\geq S_{\leftrightarrow}(S;Y|Z)-H(U)$$

P.1 *UI is non-locking*

$$\forall\ (S,Y,Z,U):\ UI(S;Y\backslash ZU)\geq UI(S;Y\backslash Z)-H(U)$$

Properties of the UI

Non-locking and monotonicity under LO of Eve

The secret key rate is non-locking:

$$\forall\ (S,Y,Z,U):\ S_{\leftrightarrow}(S;Y|ZU)\geq S_{\leftrightarrow}(S;Y|Z)-H(U)$$

P.1 *UI is non-locking*

$$\forall\ (S,Y,Z,U):\ UI(S;Y\backslash ZU)\geq UI(S;Y\backslash Z)-H(U)$$

If Eve sends Z through a channel $P_{Z'|Z}$, then the key rate cannot decrease:

$$S_{\leftrightarrow}(S;Y|Z)\leq S_{\leftrightarrow}\big(S;Y\big|Z'\big)\ \text{ for any } P_{Z'|Z}$$

P.2 *Monotonicity under local operation (LO) of Eve*

$$\forall\ (S,Y,Z,Z'):\ SY-Z-Z',\ \text{we have } UI(S;Y\backslash Z)\leq UI(S;Y\backslash Z')$$

A consequence of Properties **P.1** and **P.2**:

$$UI\leq I_{\downarrow\downarrow}\leq I_{\downarrow}$$

Properties of the UI

Monotonicity under LOPC

P.3 *Monotonicity under local operation (LO) of Alice and Bob*

$$\forall\ (S, S', Y, Z) : YZ - S - S',\ \text{we have } UI(S; Y \backslash Z) \geq UI(S'; Y \backslash Z)$$

and likewise for local operations on Y

P.4 *Monotonicity under (one-way) public communication (PC) by Alice*
For all (S, Y, Z) and functions f over the support of S, we have

$$UI(S; Y \backslash Z) \geq UI((S, f(S)); (Y, f(S)) \setminus (Z, f(S)))$$

Properties of the UI

Monotonicity under LOPC

P.3 *Monotonicity under local operation (LO) of Alice and Bob*

$$\forall\ (S, S', Y, Z) : YZ - S - S',\ \text{we have}\ UI(S; Y \backslash Z) \geq UI(S'; Y \backslash Z)$$

and likewise for local operations on Y

P.4 *Monotonicity under (one-way) public communication (PC) by Alice*
For all (S, Y, Z) and functions f over the support of S, we have

$$UI(S; Y \backslash Z) \geq UI((S, f(S)); (Y, f(S)) \setminus (Z, f(S)))$$

$UI(S; Y \backslash Z)$ is a monotone under LO of Alice and Bob and one-way PC of Alice

Properties of the UI

Additivity and asymptotic continuity

P.5 *Normalization* For a perfect secret bit $\Phi(s, y, z) := \frac{1}{2}\delta_{s,y} \times Q_Z(z)$,

$$UI_\Phi(S, Y \backslash Z) = 1$$

P.6 *Additivity on tensor products* For n i.i.d. copies of $(S, Y, Z) \sim P$,

$$UI(S^n; Y^n \backslash Z^n) = n \cdot UI(S; Y \backslash Z)$$

P.7 *Asymptotic continuity*

For any $P, P' \in \mathbb{P}_{\mathcal{S}\times\mathcal{Y}\times\mathcal{Z}}$, and $\epsilon \in [0, 1]$, if $\|P - P'\|_1 = \epsilon$, then

$$UI_{P'}(S; Y \backslash Z) - UI_P(S; Y \backslash Z) \leq \zeta(\epsilon) + \tfrac{5}{2}\epsilon \log \min\{|\mathcal{S}|, |\mathcal{Y}|\}$$

for some bounded, continuous function $\zeta : [0, 1] \to \mathbb{R}_+$ s.t. $\zeta(0) = 0$.