The Arbitrarily Varying Wiretap Channel – Secret Randomness, Stability and Super-Activation

Janis Nötzel,
Technische Universität München

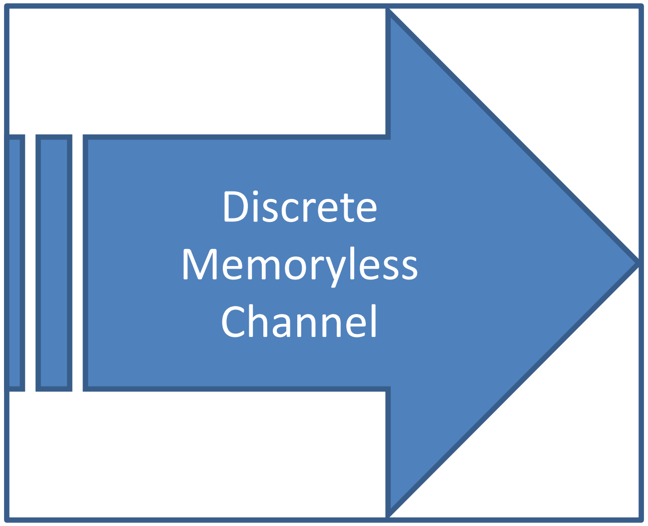
Joint work with Moritz Wiese and Holger Boche

ISIT 2015, Hong Kong - June 18

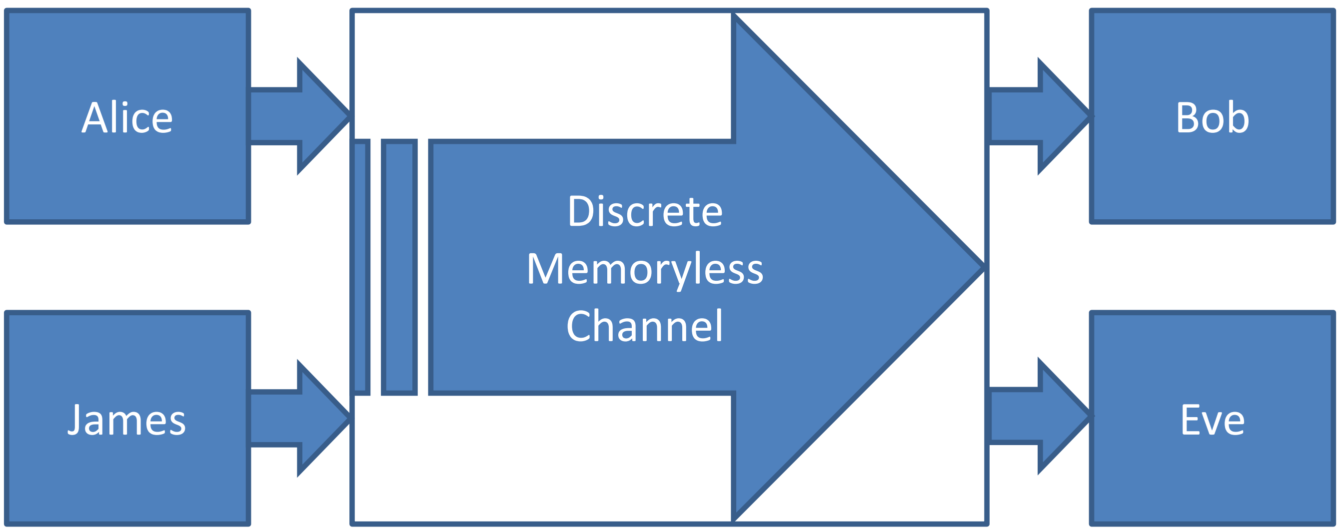
(insights from a multi-letter formula)

arXiv : 1501.07439

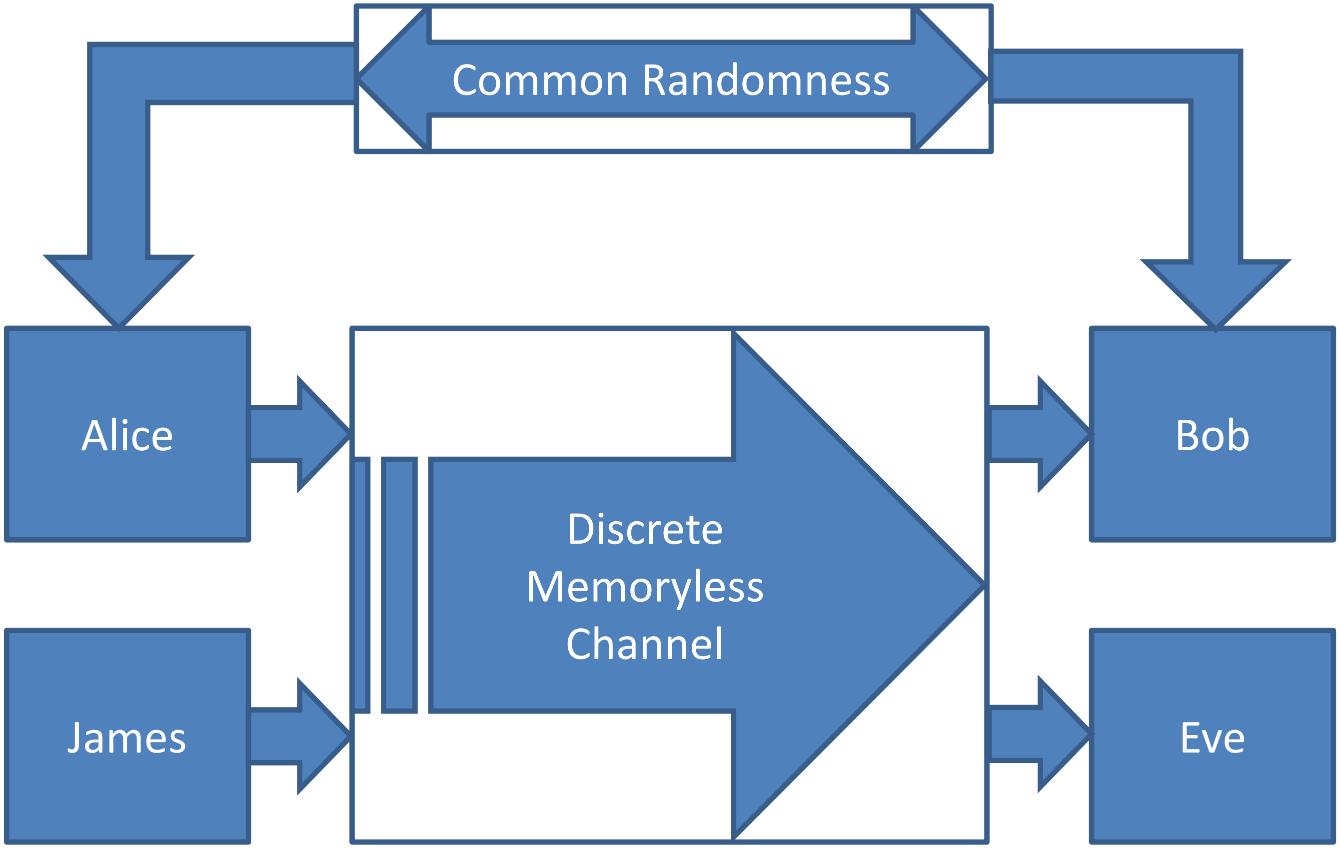
The Model



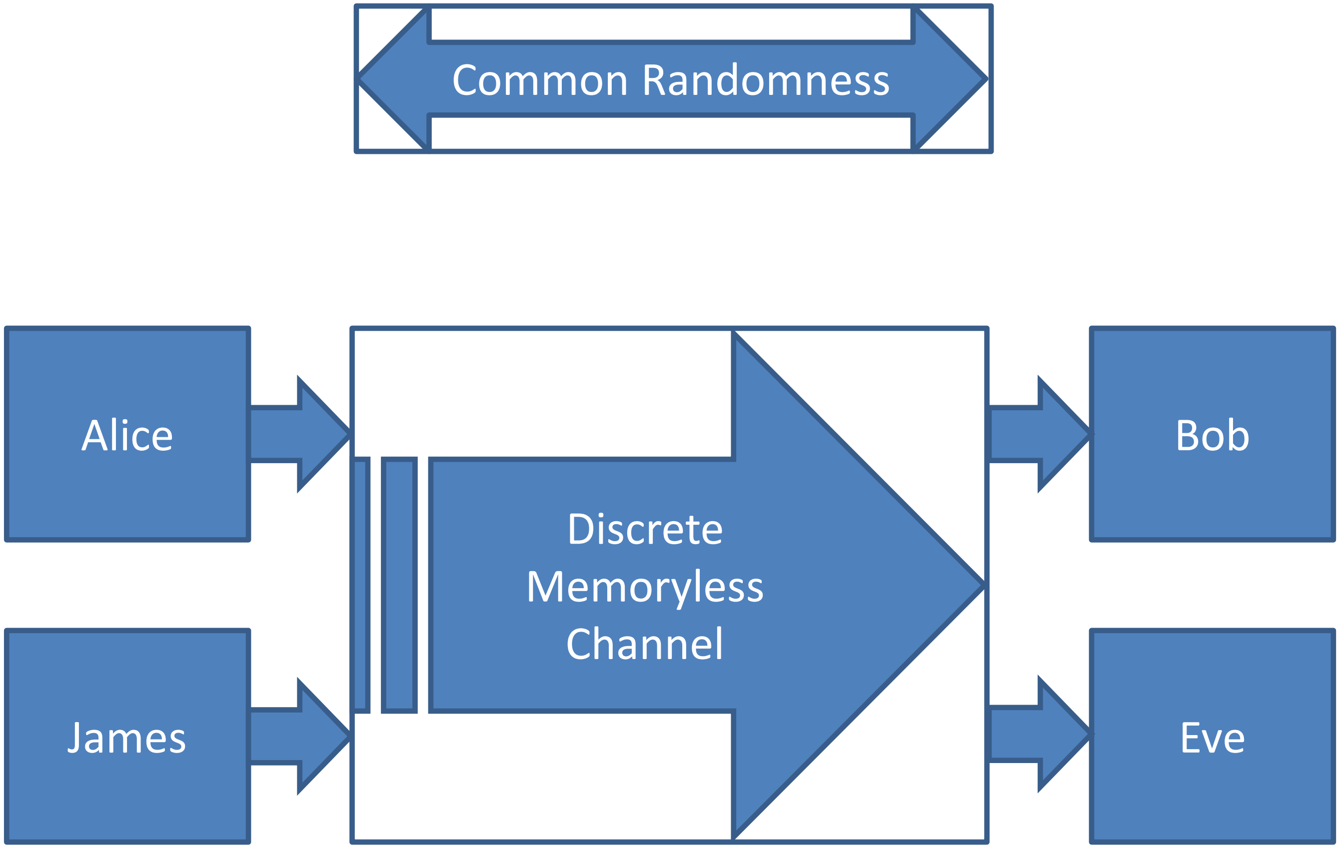
The Model



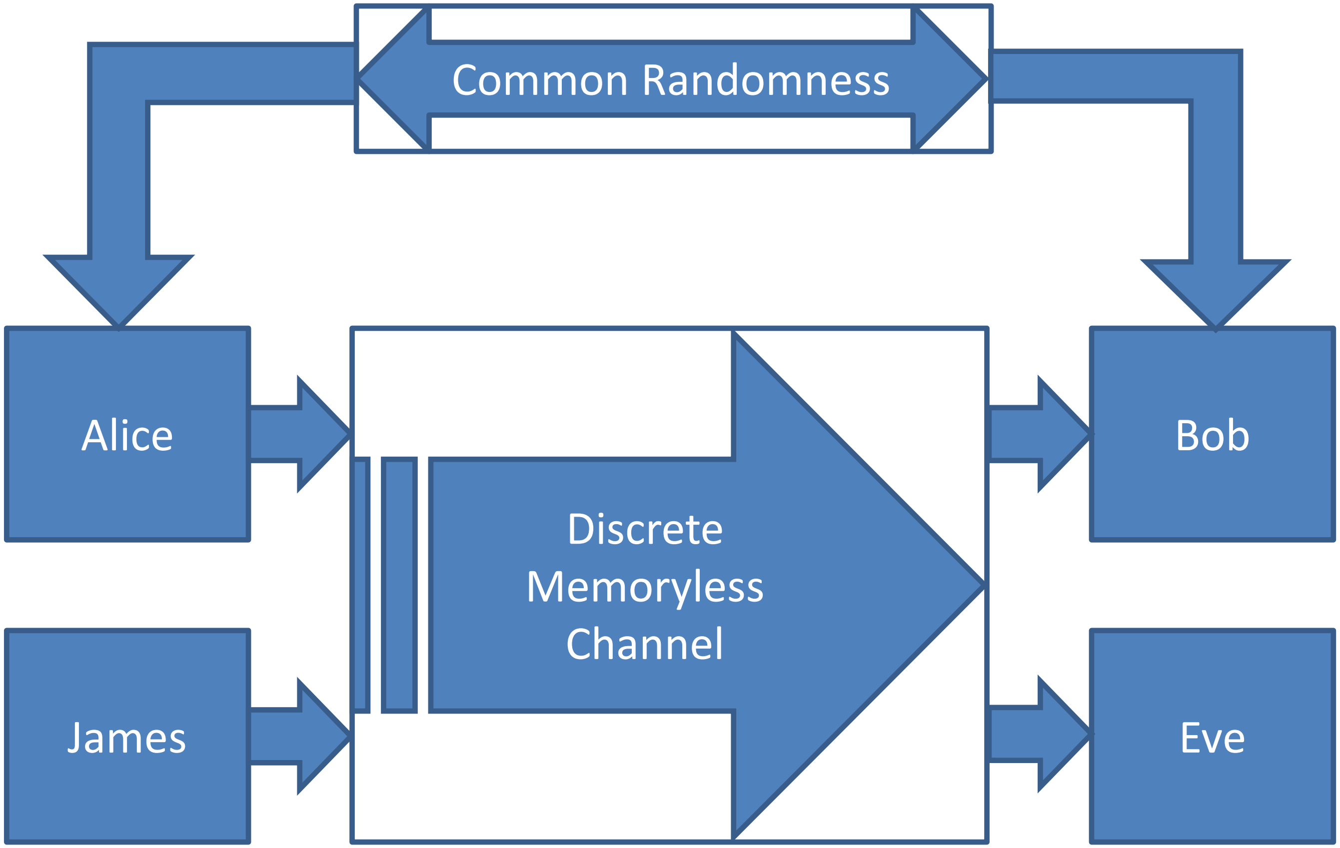
The Model


Common Randomness
Alice
James
Discrete
Memoryless
Channel
Bob
Eve

The Model

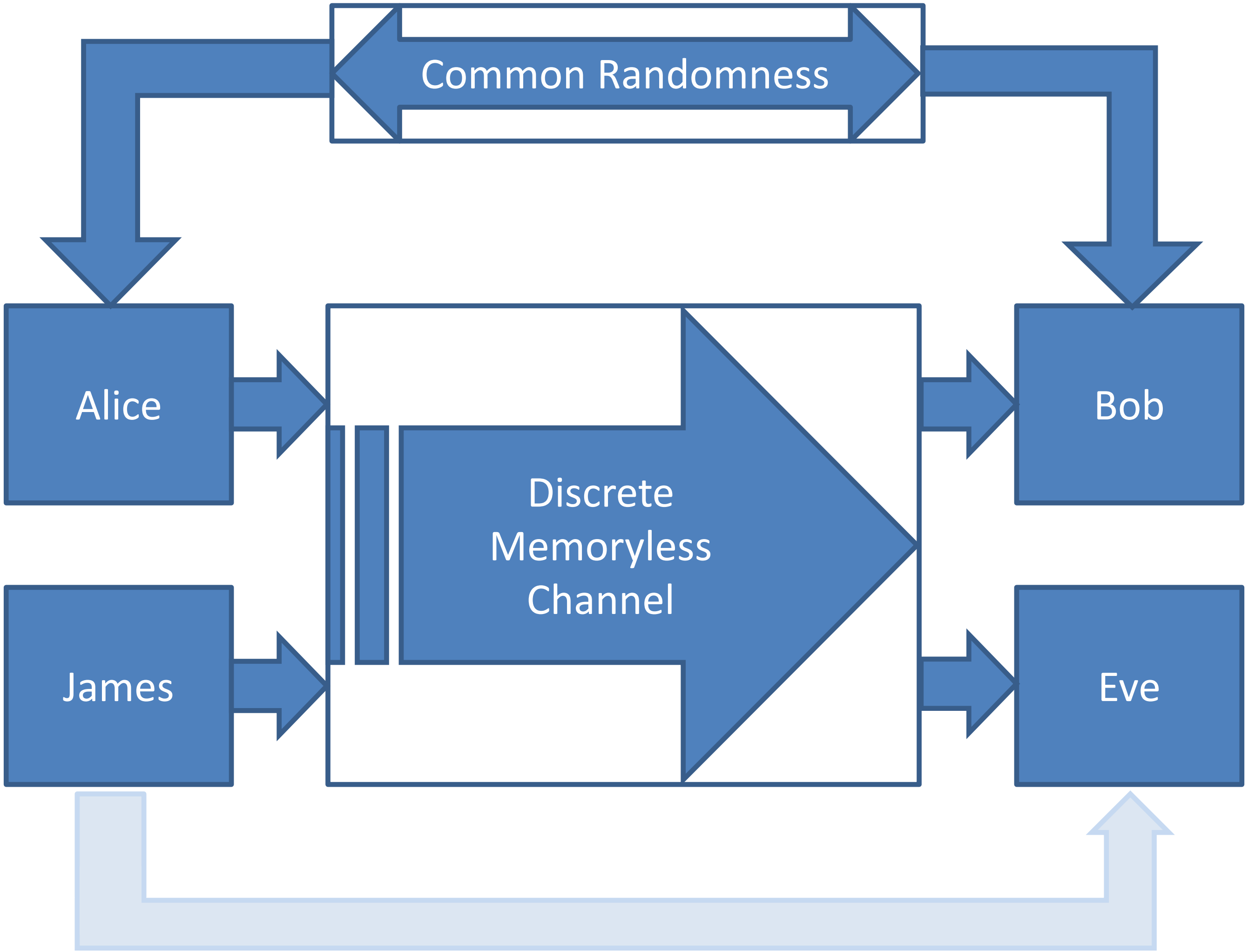

Common Randomness
Alice
James
Discrete
Memoryless
Channel
Bob
Eve

The Model

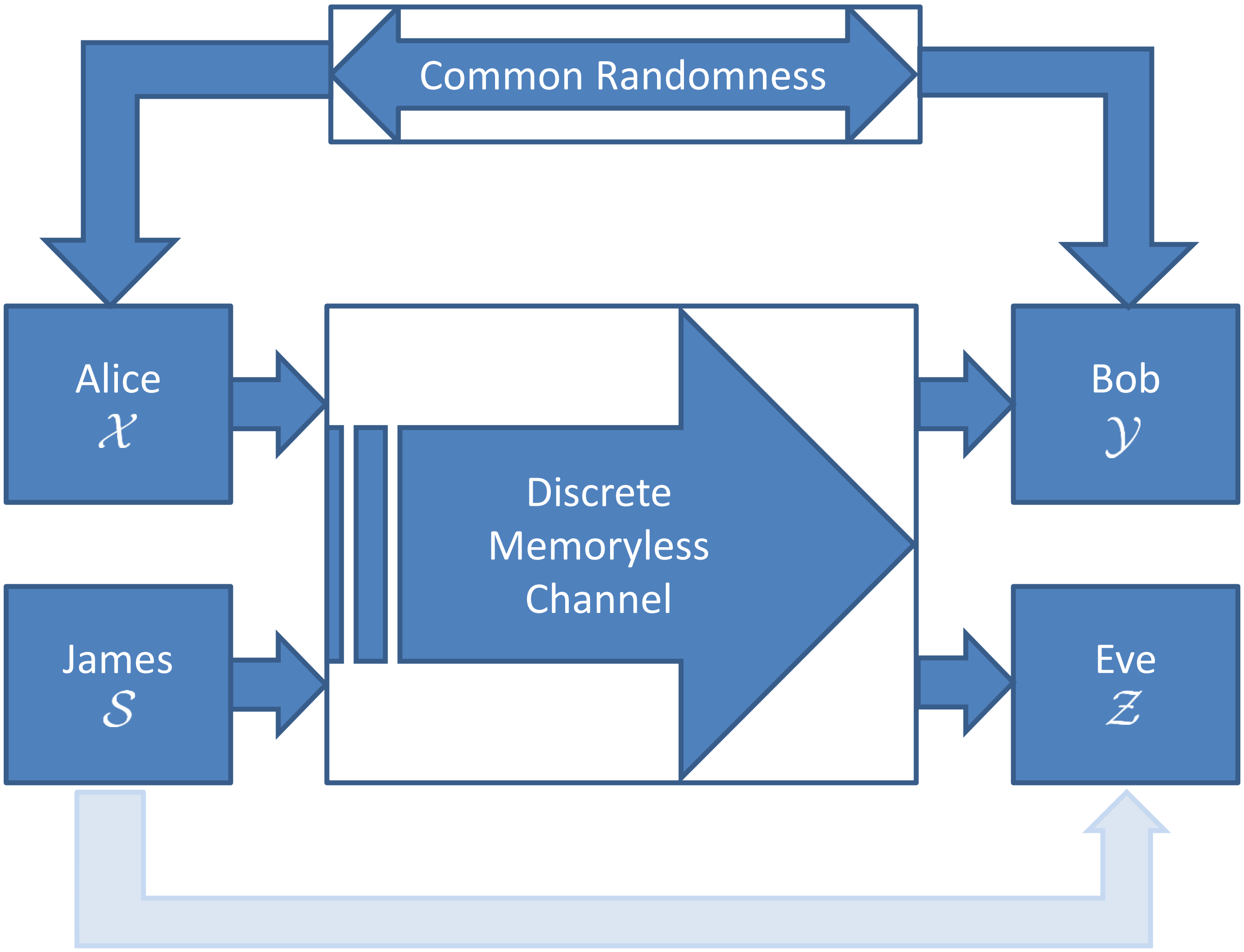


Common Randomness
Alice
Bob
Discrete
Memoryless
Channel
James
Eve

The Model


Common Randomness
Alice
Bob
Discrete
Memoryless
Channel
James
Eve

The Model


Common Randomness
Alice
$\mathcal{X}$
Discrete
Memoryless
Channel
Bob
$\mathcal{Y}$
James
$\mathcal{S}$
Eve
$\mathcal{Z}$

Topics of the talk

- We consider message transmission under two uncoordinated attacks: jamming & eavesdropping.
- This model is called the arbitrarily varying wiretap channel (AVWC).
- We consider the impact of *secret* common randomness (secret CR) as compared to common randomness (CR) which is available at Eve's site as well.
  - ➡ We provide a capacity formula for the scenario with secret CR.
- The capacity of the arbitrarily varying channel has been proven to have discontinuity points.
  - ➡ We prove that this carries over to AVWCs.
  - ➡ We also prove a very positive result: the capacity depends continuously on the channel to Eve!
- The AVWC exhibits super-activation when no CR is used.
  - ➡ We give a precise characterization of the phenomenon.
  - ➡ We provide a link to the (conjectured) super-activation of the CR assisted capacity.

Notation

- $\mathcal{P}(\mathcal{A})$ - the probability distributions on $\mathcal{A}$.
- $\mathcal{A}^n := \{(a_1, \ldots, a_n) : a_i \in \mathcal{A}\ \forall i \in \{1, \ldots, n\}\ \}$.
- The set of channels from $\mathcal{A}$ to $\mathcal{B}$ is $C(\mathcal{A}, \mathcal{B})$. $w \in C(\mathcal{A}, \mathcal{B})$ is identified with the transition probabilities $(w(b|a))_{a\in\mathcal{A}, b\in\mathcal{B}}$.
- $w \in C(\mathcal{A}, \mathcal{B})$, $w' \in C(\mathcal{A}', \mathcal{B}') \Rightarrow w \otimes w' \in C(\mathcal{A} \times \mathcal{A}', \mathcal{B} \times \mathcal{B}')$ via $(w \otimes w')((b, b')|(a, a')) := w(b|a)w'(b'|a')$ $(\forall a, b, a', b')$.
- The mutual information of a bipartite random variable (X, Y) is denoted $I(X; Y)$.
- For the remainder of the talk, fix $\mathcal{S}$, $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$. The channel to Bob is $w \in C(\mathcal{S} \times \mathcal{X}, \mathcal{Y})$. The channel to Eve is $v \in C(\mathcal{S} \times \mathcal{X}, \mathcal{Z})$.
- w and v incorporate all the necessary details for this model.
- Equivalent representation: $\mathfrak{W} := (w(\cdot|s, \cdot))_{s\in\mathcal{S}} \in C(\mathcal{X}, \mathcal{Y})^{|\mathcal{S}|}$ and $\mathfrak{V} := (v(\cdot|s, \cdot))_{s\in\mathcal{S}} \in C(\mathcal{X}, \mathcal{Z})^{|\mathcal{S}|}$. Denote the AVWC by $(\mathfrak{W}, \mathfrak{V})$.

Definition of codes

DEF I. Let $n \in \mathbb{N}$. A CR assisted code $\mathcal{K}_n$ for n uses of $(\mathfrak{W}, \mathfrak{V})$ consists of: $K, \Gamma \in \mathbb{N}$, a set of encoders $\{E^\gamma\}_{\gamma=1}^{\Gamma} \subset C(\{1, \dots, K\}, \mathcal{X}^n)$ and a collection $(D_k^\gamma)_{k,\gamma=1}^{K,\Gamma}$ of subsets D_k^γ of $\mathcal{Y}^n$ satisfying $D_k^\gamma \cap D_{k'}^\gamma = \emptyset$ for all $\gamma \in [\Gamma]$, whenever $k \neq k'$. Every such code defines the random variables $S_{s^n} := (\mathfrak{K}_n, \mathfrak{K}'_n, \mathfrak{d}_n, \mathfrak{X}_n, \mathfrak{Y}_{s^n}, \mathfrak{Z}_{s^n})$ $(s^n \in \mathcal{S}^n)$ via

$$\begin{aligned}\mathbb{P}(&S_{s^n} = (k, k', \gamma, x^n, y^n, z^n)) \\ &:= \frac{1}{\Gamma \cdot K} E^\gamma(x^n|k) \mathbb{1}_{D_{k'}^\gamma}(y^n) w^{\otimes n}(y^n|s^n, x^n) v^{\otimes n}(z^n|s^n, x^n).\end{aligned}$$

The average error of $\mathcal{K}_n$ is

$$e(\mathcal{K}_n) = 1 - \max_{s^n \in \mathcal{S}^n} \frac{1}{K\Gamma} \sum_{k,\gamma=1}^{K,\Gamma} \sum_{x^n} E^\gamma(x^n|k) w^{\otimes n}(D_k^\gamma|s^n, x^n).$$

Definition of coding schemes

DEF II. A CR assisted secure coding scheme for $(\mathfrak{W}, \mathfrak{V})$ operating at rate R consists of a sequence $(\mathcal{K}_n)_{n\in\mathbb{N}}$ of CR assisted codes such that

$$\lim_{n\to\infty} e(\mathcal{K}_n) = 0, \qquad \liminf_{n\to\infty} \frac{1}{n}\log(K_n) = R,$$
$$\text{and} \qquad \limsup_{n\to\infty} \max_{s^n\in\mathcal{S}^n} I(\mathfrak{K}_n; \mathfrak{Z}_{s^n}|\mathfrak{d}_n) = 0.$$

If $\Gamma_n = 1$ for all $n \in \mathbb{N}$, $(\mathcal{K}_n)_{n\in\mathbb{N}}$ is called deterministic coding scheme.

DEF III. A secure CR assisted secure coding scheme $\mathcal{K}$ for $(\mathfrak{W}, \mathfrak{V})$ operating at rate R and using an amount $G > 0$ of secret CR consists of a sequence $(\mathcal{K}_n)_{n\in\mathbb{N}}$ of CR assisted codes satisfying

$$\lim_{n\to\infty} \frac{1}{n}\log\Gamma_n = G, \qquad \liminf_{n\to\infty} \frac{1}{n}\log(K_n) = R,$$
$$\lim_{n\to\infty} e(\mathcal{K}_n) = 0, \qquad \limsup_{n\to\infty} \max_{s^n\in\mathcal{S}^n} I(\mathfrak{K}_n; \mathfrak{Z}_{s^n}) = 0.$$

Definition of capacities

DEF IV. Let $G > 0$. $C_s(\mathfrak{W}, \mathfrak{V}, G)$ is the supremum over all $R \geq 0$ such that there is a secure coding scheme $\mathcal{K}$ for $(\mathfrak{W}, \mathfrak{V})$ operating at rate R and using an amount G of secret CR.

DEF V. $C_d(\mathfrak{W}, \mathfrak{V})$ is the supremum over all $R \geq 0$ such that there is a secure deterministic coding scheme $\mathcal{K}$ at rate R.

DEF VI. $C_r(\mathfrak{W}, \mathfrak{V})$ is the supremum over all $R \geq 0$ such that there exists a secure CR assisted coding scheme $\mathcal{K}$ at rate R.

Results

RESULT I. (Capacity with secret CR) It holds

$$C_s(\mathfrak{W}, \mathfrak{V}, G) = \min\{\ C_r(\mathfrak{W}, \mathfrak{V}) + G,\ \ C_r(\mathfrak{W}, \mathfrak{T})\ \},$$

where $\mathfrak{T} = \{t\}$ and $t(z|x,s) = 1/|\mathcal{Z}|\ \forall\ s \in \mathcal{S}$, $x \in \mathcal{X}$, $z \in \mathcal{Z}$.

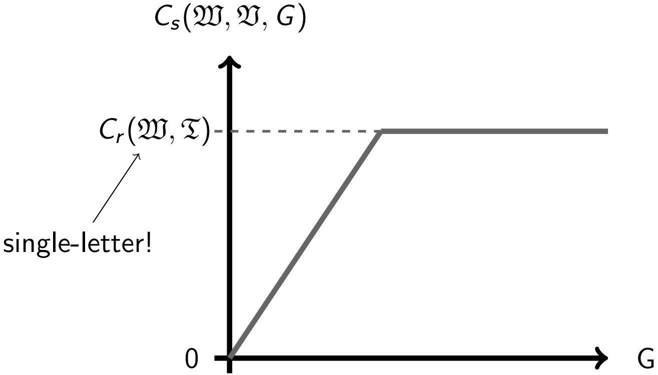
REMARK. Recent (*arXiv:1410.8078*, this ISIT, paper number 2395) work by Wiese, Nötzel and Boche provided a multi-letter formula for C_r.

Results

RESULT I. (Capacity with secret CR) It holds

$$C_s(\mathfrak{W}, \mathfrak{V}, G) = \min\{\ C_r(\mathfrak{W}, \mathfrak{V}) + G,\ \ C_r(\mathfrak{W}, \mathfrak{T})\ \},$$

where $\mathfrak{T} = \{t\}$ and $t(z|x,s) = 1/|\mathcal{Z}|\ \forall\ s \in \mathcal{S},\ x \in \mathcal{X},\ z \in \mathcal{Z}$.



Results

RESULT II. (Symmetrizability)
1) If $\mathfrak{W}$ is symmetrizable, then $C_d(\mathfrak{W}, \mathfrak{V}) = 0$.
2) If $\mathfrak{W}$ is non-symmetrizable, then $C_d(\mathfrak{W}, \mathfrak{V}) = C_r(\mathfrak{W}, \mathfrak{V})$.

REMARK. The proof is based on [Csiszar,Narayan'78].

REMARK. An AVC $\mathfrak{W}$ is symmetrizable if there is a conditional probability distribution $(u(s|x))_{s\in\mathcal{S},x\in\mathcal{X}}$ such that

$$\forall x, \hat{x} \in \mathcal{X} : \qquad \sum_{s\in\mathcal{S}} u(s|x)w(\cdot|s,\hat{x}) = \sum_{s\in\mathcal{S}} u(s|\hat{x})w(\cdot|s,x).$$

DEFINITION. Let $M_{\mathrm{f}} := \{M \subset C(\mathcal{X}, \mathcal{Y}) : |M| < \infty\}$. Define $F : M_{\mathrm{f}} \to \mathbb{R}_+$ by

$$F(\mathfrak{W}) := \max_{x\neq x'} \min_{u} \| \sum_{s} (u(s|x)w(\cdot|s,\hat{x}) - u(s|\hat{x})w(\cdot|s,x))\|_1.$$

Then '$F(\mathfrak{W}) = 0$' is equivalent to 'the AVC $\mathfrak{W}$ is symmetrizable'.

Results

DEFINITION. As metric on the set of AVWCs (and AVCs) we use the Hausdorff-distance which is inherited from the one-norm (variational distance) on probability distributions. Let this distance be denoted by d.

RESULT III. (Discontinuity)
1) C_d is discontinuous in $(\mathfrak{W}, \mathfrak{V})$ iff: $C_r(\mathfrak{W}, \mathfrak{V}) > 0$, $F(\mathfrak{W}) = 0$ but: $\forall\ \epsilon > 0\ \exists\ \mathfrak{W}_\epsilon$ such that $d(\mathfrak{W}, \mathfrak{W}_\epsilon) < \epsilon$ and $F(\mathfrak{W}_\epsilon) > 0$.
2) If C_d is discontinuous in the point $(\mathfrak{W}, \mathfrak{V})$ then it is discontinuous for all $\hat{\mathfrak{V}}$ for which $C_r(\mathfrak{W}, \hat{\mathfrak{V}}) > 0$.

RESULT IV. (Stability) If $C_d(\mathfrak{W}, \mathfrak{V}) > 0$ then there is $\epsilon > 0$ such that $d((\mathfrak{W}, \mathfrak{V}), (\mathfrak{W}', \mathfrak{V}')) \leq \epsilon$ implies $C_d(\mathfrak{W}', \mathfrak{V}') > 0$.

Super-activation: preliminaries

For two AVWCs $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$, we define $(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2)$ to equal

$$((w_1(\cdot|\cdot, s) \otimes w_2(\cdot|\cdot, s'))_{s,s' \in \mathcal{S}}, (v_1(\cdot|\cdot, s) \otimes v_2(\cdot|\cdot, s'))_{s,s' \in \mathcal{S}}),$$

Since all state alphabets are assumed to be finite, there is no loss of generality in this definition. Then,

$$C_d(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2) \geq C_d(\mathfrak{W}_1, \mathfrak{V}_1) + C_d(\mathfrak{W}_2, \mathfrak{V}_2)$$

follows trivially from the definition of C_d. In contrast, if

$$C_d(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2) > C_d(\mathfrak{W}_1, \mathfrak{V}_1) + C_d(\mathfrak{W}_2, \mathfrak{V}_2)$$

holds, we speak of *super-additivity* and if even

$$\begin{aligned} C_d(\mathfrak{W}_1, \mathfrak{V}_1) = C_d(\mathfrak{W}_2, \mathfrak{V}_2) &= 0, \\ C_d(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2) &> 0 \end{aligned}$$

we speak of *super-activation*.

Super-activation: results

There exist AVWCs which exhibit super-activation [Boche,Schaefer'14].
We give a precise characterization of the effect.

RESULT III. (Super-activation) Let $(\mathfrak{W}_i, \mathfrak{V}_i)_{i=1,2}$ be AVWCs.
...
3) If C_r shows super-activation for $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$, then C_d can show super-activation for $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$ if and only if at least one of $\mathfrak{W}_1$ or $\mathfrak{W}_2$ is non-symmetrizable.
4) If C_r shows no super-activation for $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$ then super-activation of C_d can only happen if $\mathfrak{W}_1$ is non-symmetrizable and $\mathfrak{W}_2$ is symmetrizable and $C_r(\mathfrak{W}_1, \mathfrak{V}_1) = 0$ and $C_r(\mathfrak{W}_2, \mathfrak{V}_2) > 0$.

Conclusions

- We provided a complete characterization of the secrecy capacity of AVWCs
  - This characterization uses a multi-letter formula
  - nonetheless, we were able to make nontrivial statements:
  - Complete characterization of discontinuity points in terms of functions which are continuous themselves
  - Complete characterization of super-activation of C_d
  - Single-letterization is an open and potentially hard problem

- Compare to zero-error capacity which [Ahlswede'70] is deeply connected to AVCs

- It was conjectured [Shannon'56] that the zero-error capacity of a DMC is additive. This conjecture was proven to be wrong [Alon'98]
  - ➡ Super-additivity can occur for the zero-error capacity

THANKS FOR YOUR ATTENTION

Related work

- [Boche,Schaefer'14] Boche and Schaefer "Capacity results and super-activation for wiretap channels with active wiretappers"(2014)
- [Csiszar,Narayan'88] Csiszar and Narayan "The arbitrarily varying channel revisited: positivity, constraints" (1988)
- [Ahlswede'78] Ahlswede "Elimination of correlation for arbitrarily varying channels" (1978)
- [Shannon'56] Shannon, "The zero-error capacity of a noisy channel" (1956)
- [Ahlswede'70] Ahlswede, "A Note on the Existence of the Weak Capacity for Channels with Arbitrarily Varying Channel Probability Functions and Its Relation to Shannon's Zero Error Capacity" (1970)
- [Alon'98] Alon, "The Shannon capacity of a union" (1998)