Super-activation as a phenomenon in information theory

Janis Nötzel

Beyond IID 4
Barcelona
21.07.2016

Topics of this Talk

1. **Motivation: What makes the difference?**
2. **Historical background of "activation" in Shannon Theory**
   - until '00: Classical "activation" results
   - until '13: Quantum "super-activation"
   - recently : Classical "super-activation"
3. **Introducing the arbitrarily varying wiretap channel (AVWC)**
   - Key idea, some picture, different setups
   - AVWC bridges the gap between i.i.d. and non-i.i.d. world
   - A protocol that super-activates certain AVWCs
4. **Precise formulations**
   - Codes, capacity
   - The recent results + some central ideas in proofs

Results presented in this talk based on joint work with M. Wiese and H. Boche

[NWB16] N., M. Wiese, H. Boche, "The Arbitrarily Varying Wiretap Channel - Secret Randomness, Stability, and Super-Activation", IEEE Trans. Inf. Theory, Vol. 62, No. 6 (2016)

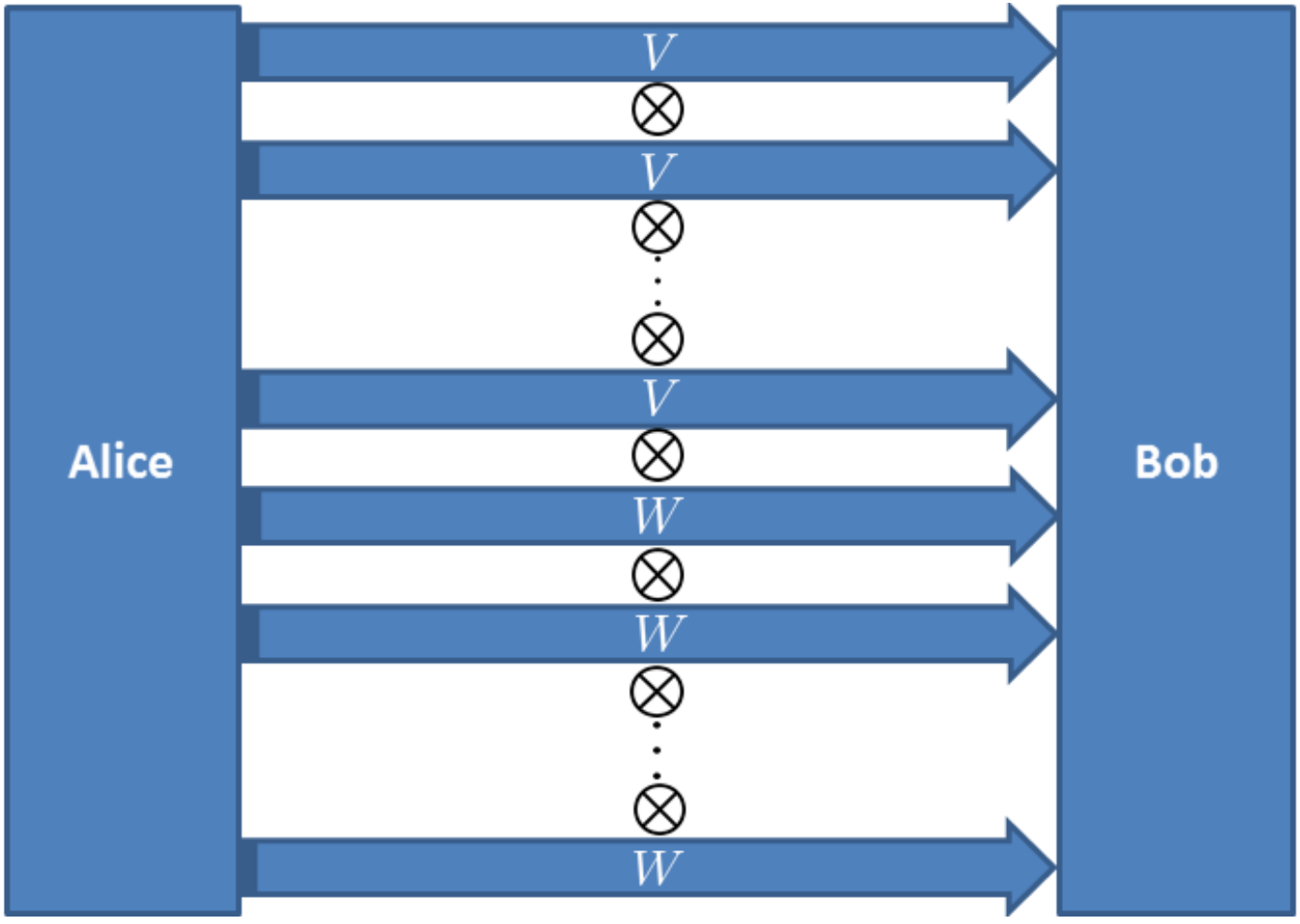
[WNB16] M. Wiese, N., H. Boche, "A channel under simultaneous jamming and eavesdropping attack - Correlated random coding capacities under strong secrecy criteria", IEEE Trans. Inf. Theory, vol. 62, no. 7, pp. 3844 - 3862 (2016)

❶ Motivation: Which ingredients make the difference?

- If I am to build a communication system, with
  - Numerous nodes
  - Many users
  - Many different needs that should be addressed
  - A limited number of different devices and techniques available
  - A limited amount of time (=money) to set up the network

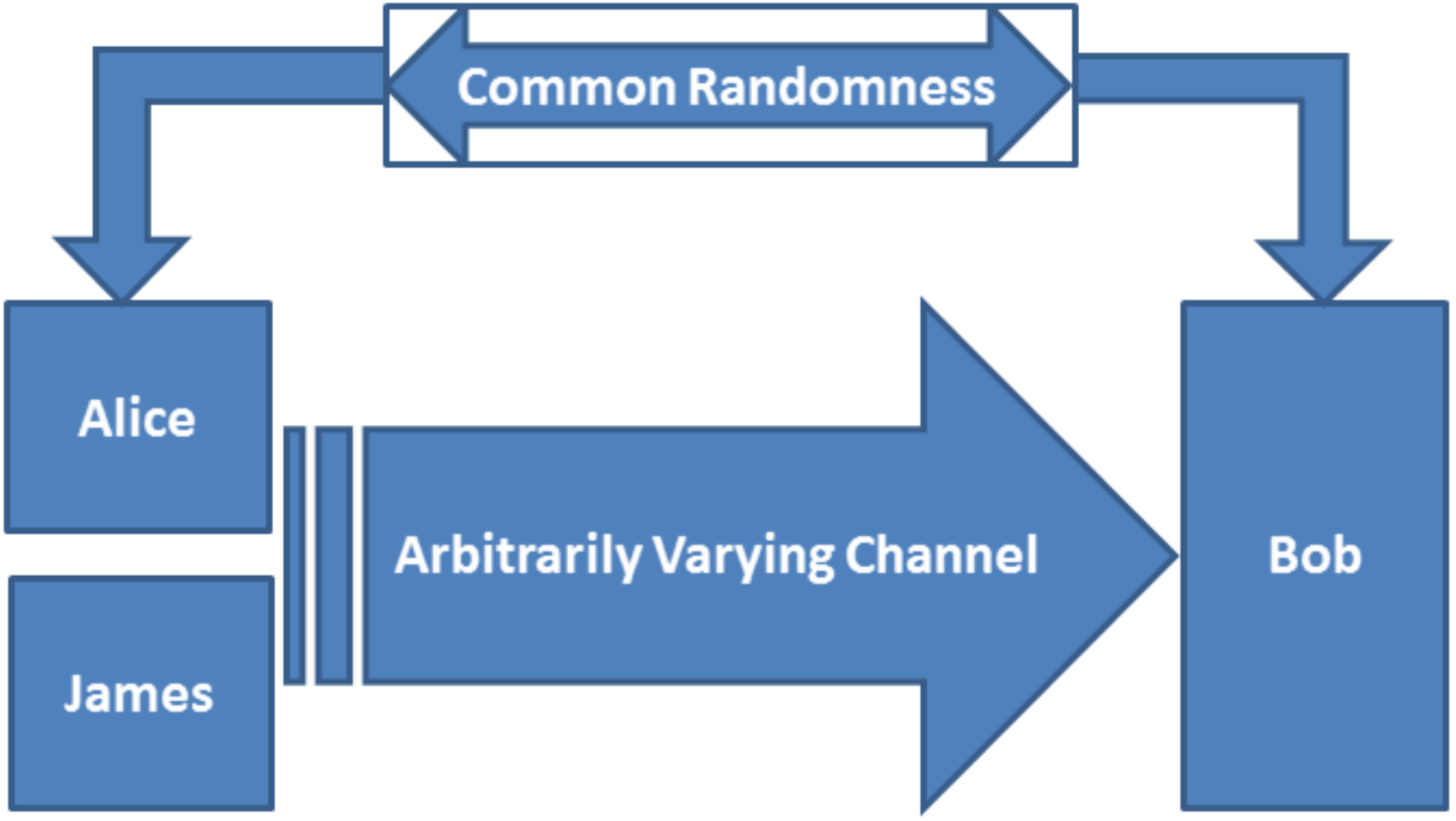
  - what are the key effects that I should worry about?
  - How do I deal with them?
- For example when devices need to work together in order to form an end-to-end link, they only give us certain degrees of freedom.
- Some errors can be compensated for easily (e.g. good coding schemes make the impact of imperfections small), some not.
- General theory of communication chains (resource theory): not yet.
- In particular: Many examples are available that show how using resources together increases efficiency. For example:
  1. When the zero error criterion is used
  2. When shared randomness can be used between Alice and Bob
  3. When public feedback is allowed between them
  4. When different channels can be used in parallel

❷ Zero-Error Communication



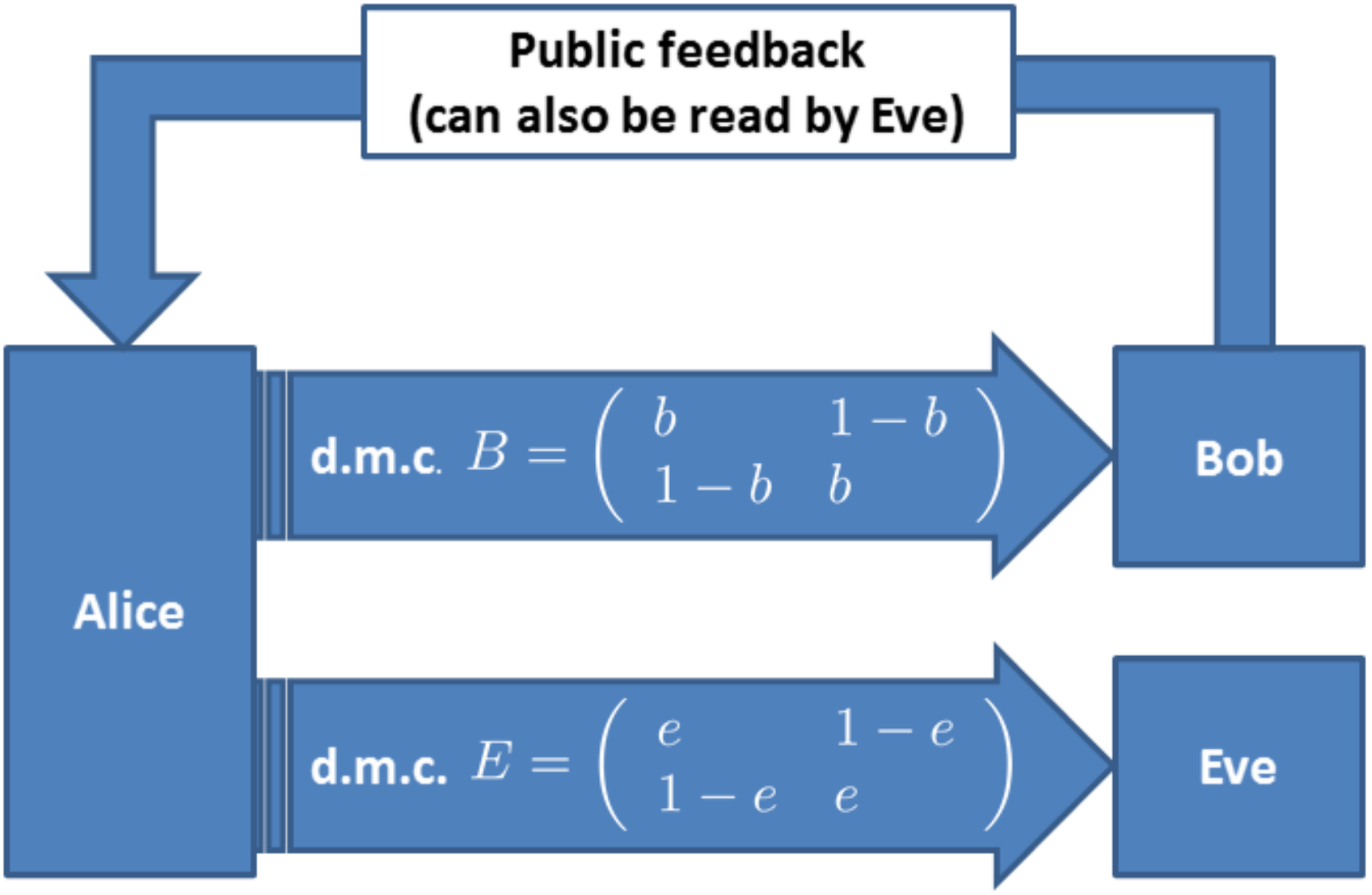
- Conjecture [Sha56]: C_0 is additive.
- $\exists V, W: \ C_0(V \otimes W) > C_0(V) + C_0(W)$ [Hae78,Hae79,Alo98].
- C_0 is connected to AVC under maximal error criterion [Ahl70].

❷ Ahlswede Dichotomy



Common randomness guarantees successful message transmission over the arbitrarily varying channel (under average error criterion) even when it may be impossible without [Ahlswede78].

❷ Secret Key Agreement by Public Discussion



Public feedback enables establishment of a secret key between Alice and Bob even when $b < e$ [Mau93].

❷ Super-activation

- So far, only activation has been mentioned.
- In 2008, Smith & Yard [SY08] discovered that even super-activation is possible.
- The effect was proven by them to occur on specific pairs of quantum channels. A pair $(\mathcal{A}, \mathcal{B})$ of channels is said to show super-activation for the quantum capacity if

$$Q(\mathcal{A}) = Q(\mathcal{B}) = 0 \text{ and } Q(\mathcal{A} \otimes \mathcal{B}) > 0.$$

- Smith & Yard used channels where $\mathcal{B}$ satisfies $\mathcal{P}(\mathcal{B}) > 0$ but $\mathcal{Q}(\mathcal{B}) = 0$ and $\mathcal{A}$ is a 50% erasure channel that satisfies $Q(\mathcal{A}) = 0$.
- Smith & Yard pointed out that the reasons for these two quantum capacities being equal to zero may be different, so that some compensation may become possible.
- According to state of knowledge at that time, super-activation seemed to be a purely quantum effect with no counterpart in classical information theory.
- The phenomenon is still actively researched [KMWY16].

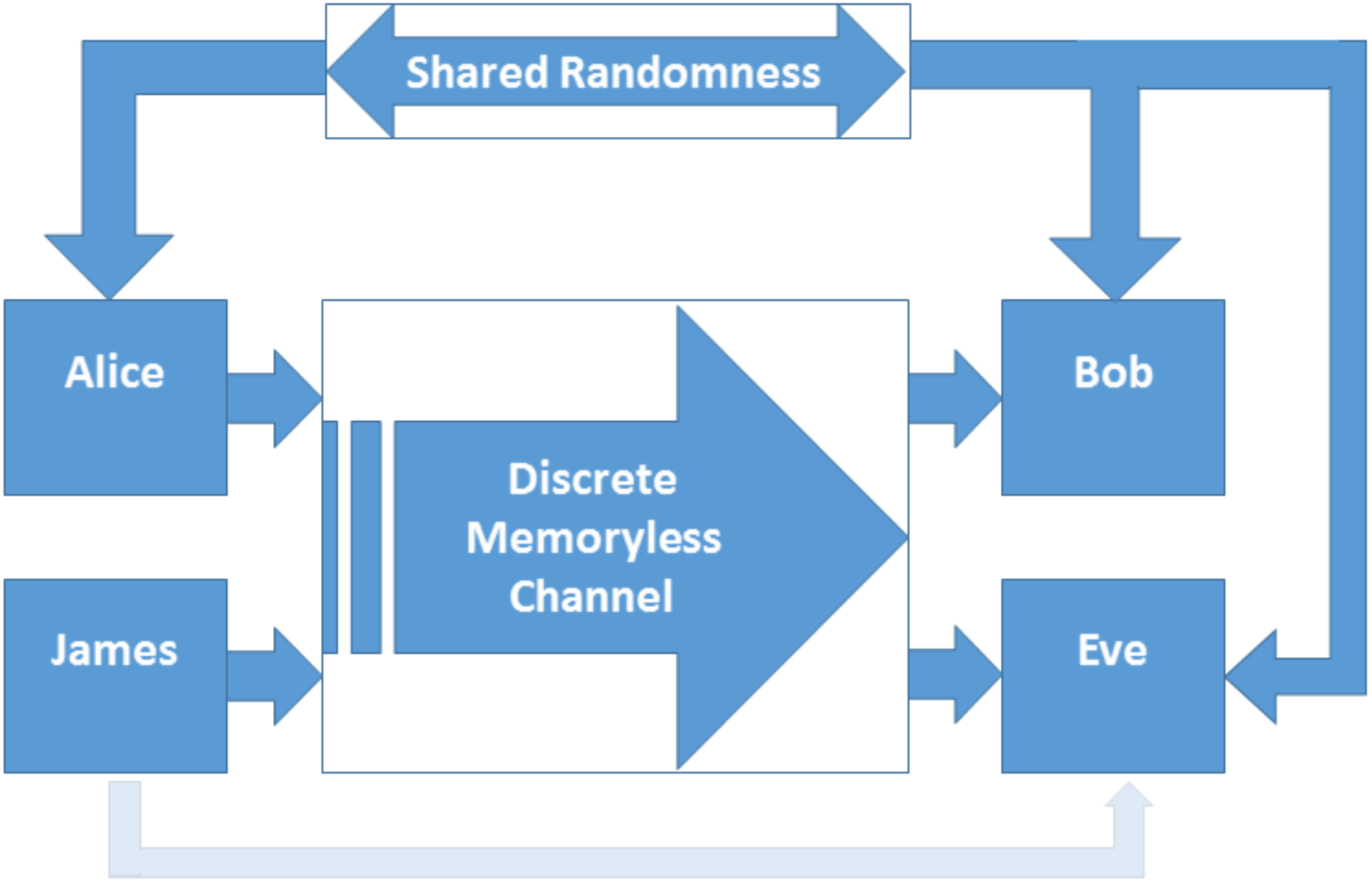
❷ Super-Activation in a Classical System

- In [BS14], Boche and Schaefer presented a protocol that demonstrated how to super-activate certain pairs of arbitrarily varying wiretap channels (AVWCs).
- In [WNB16], we provided (among others) a capacity formula for the AVWC
- In [NWB16], we investigated super-activation of the AVWC further. A complete characterization in terms of the formula from [WNB16] was achieved.

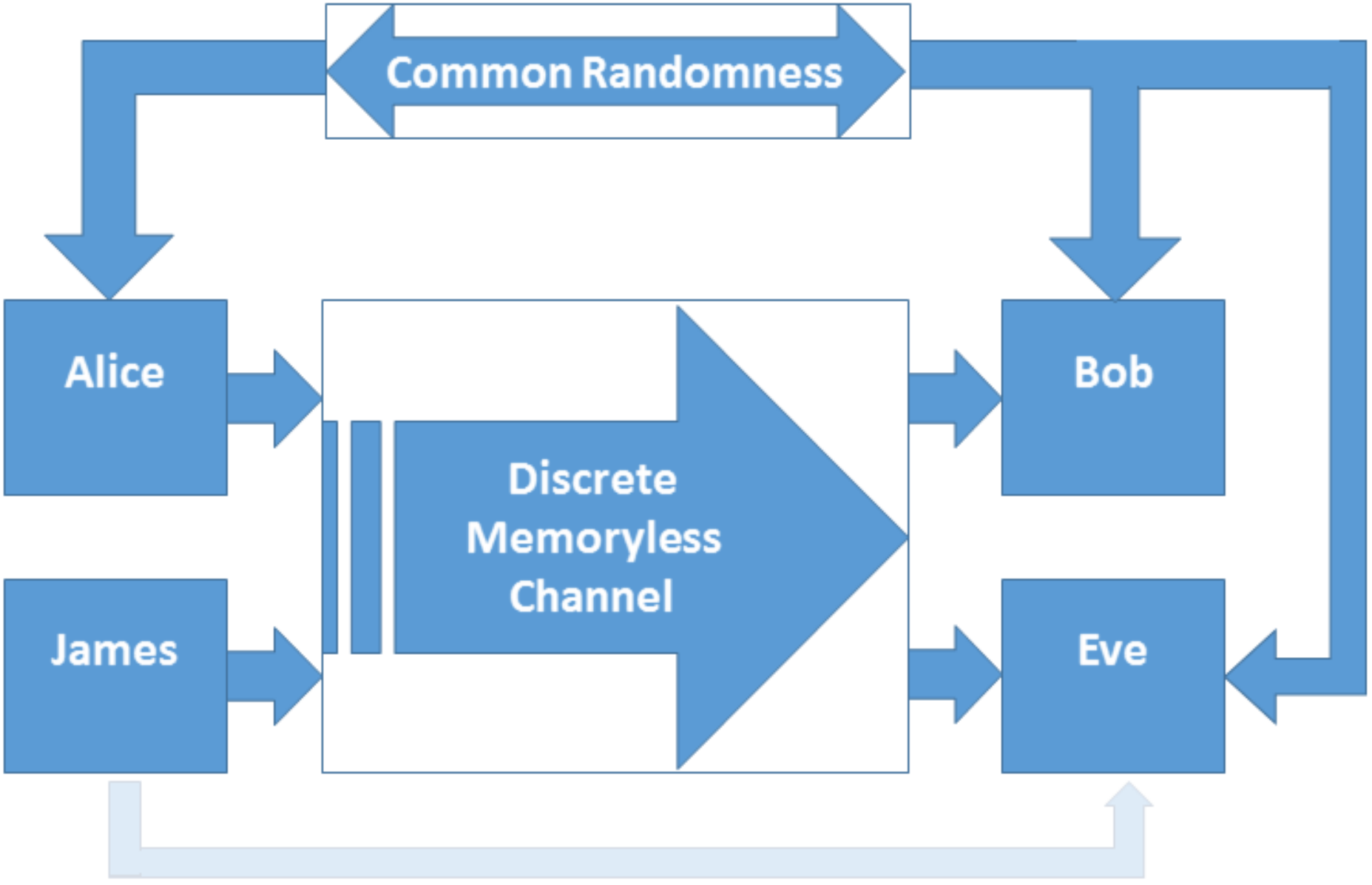
We will now:

1. introduce the AVWC,
2. explain why it is even "strictly beyond IID"
3. explain how it can be super-activated
4. then we present the extended characterization.

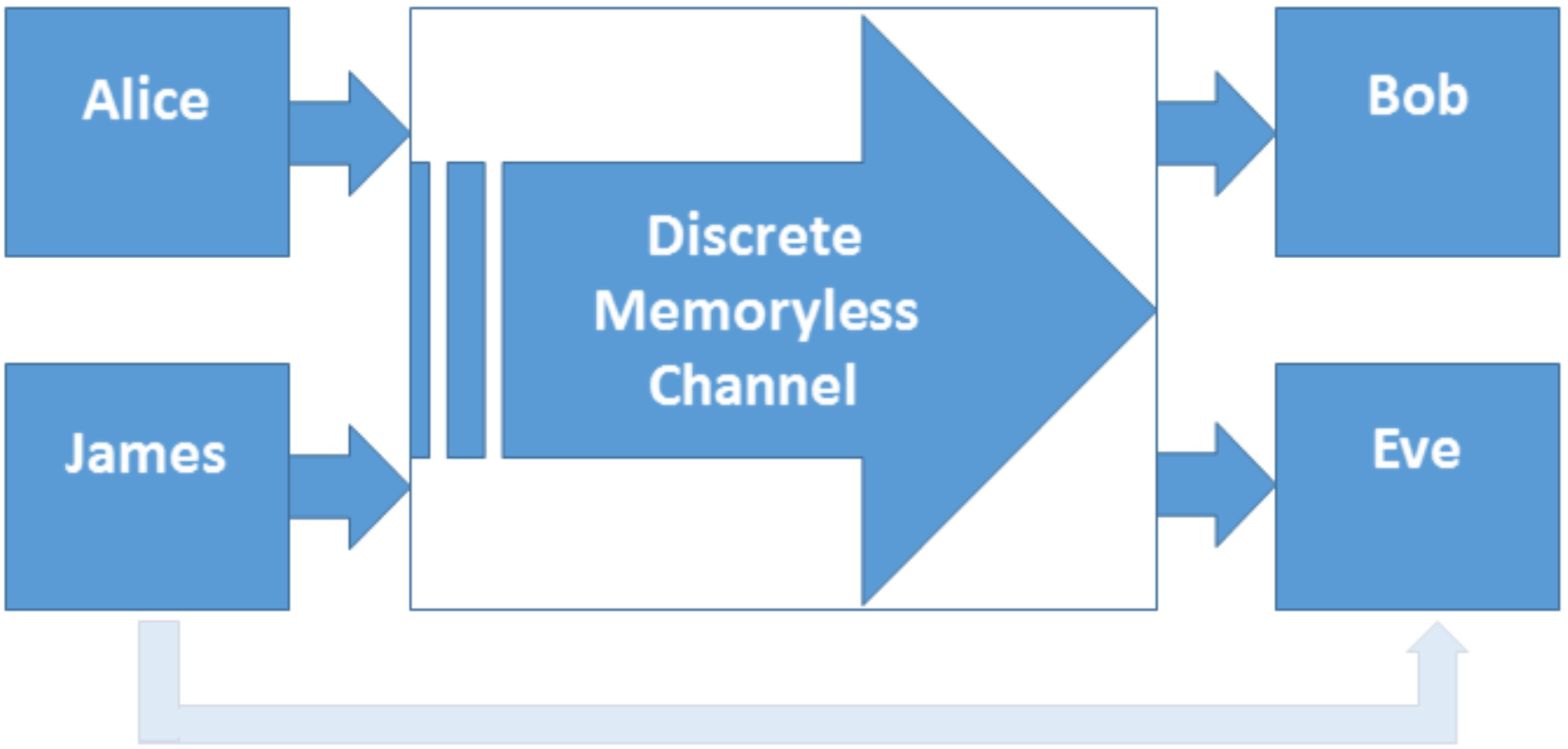
❸ The AVWC: Shared vs. Common Randomness



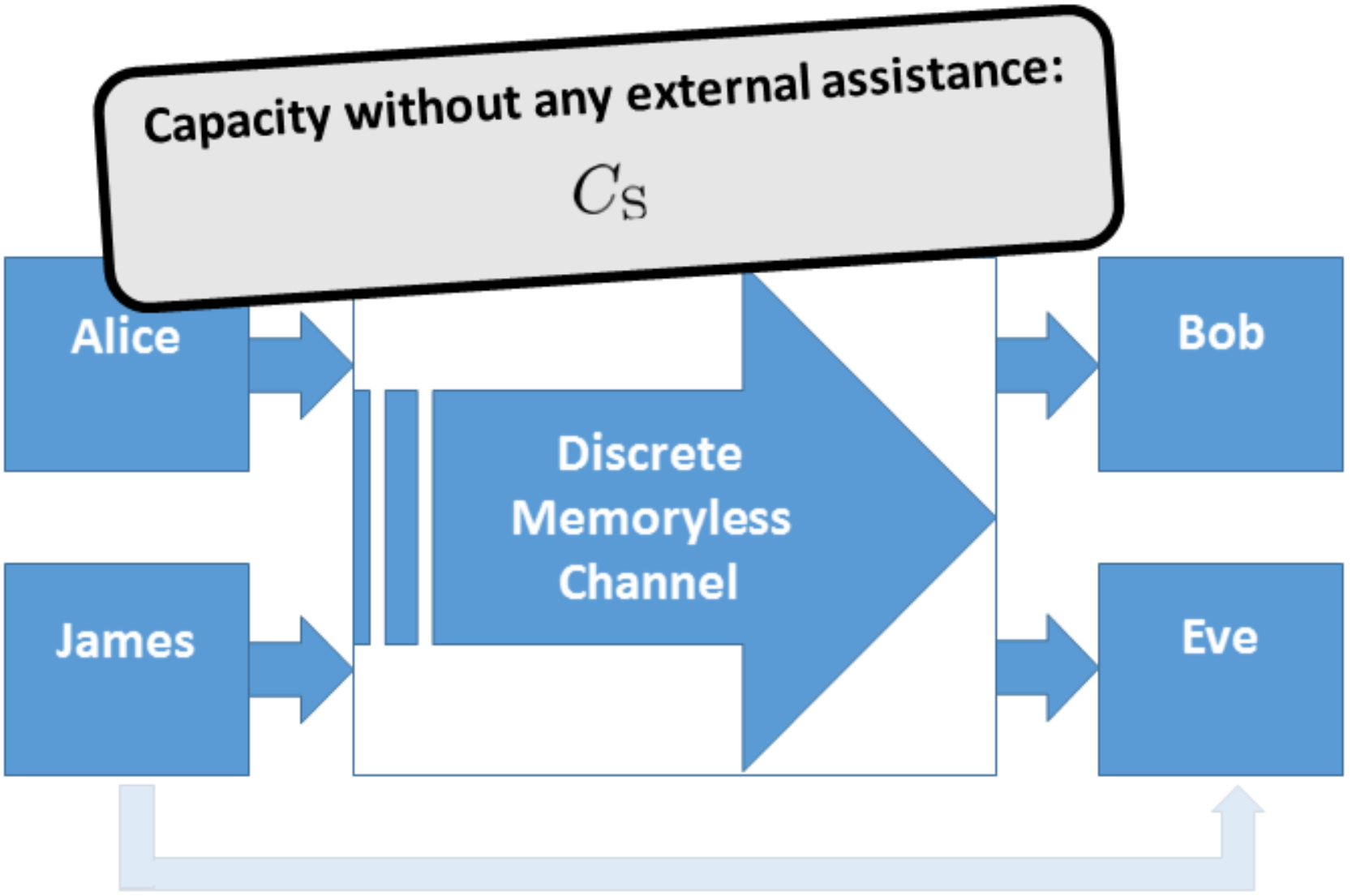
❸ The AVWC: Shared vs. Common Randomness



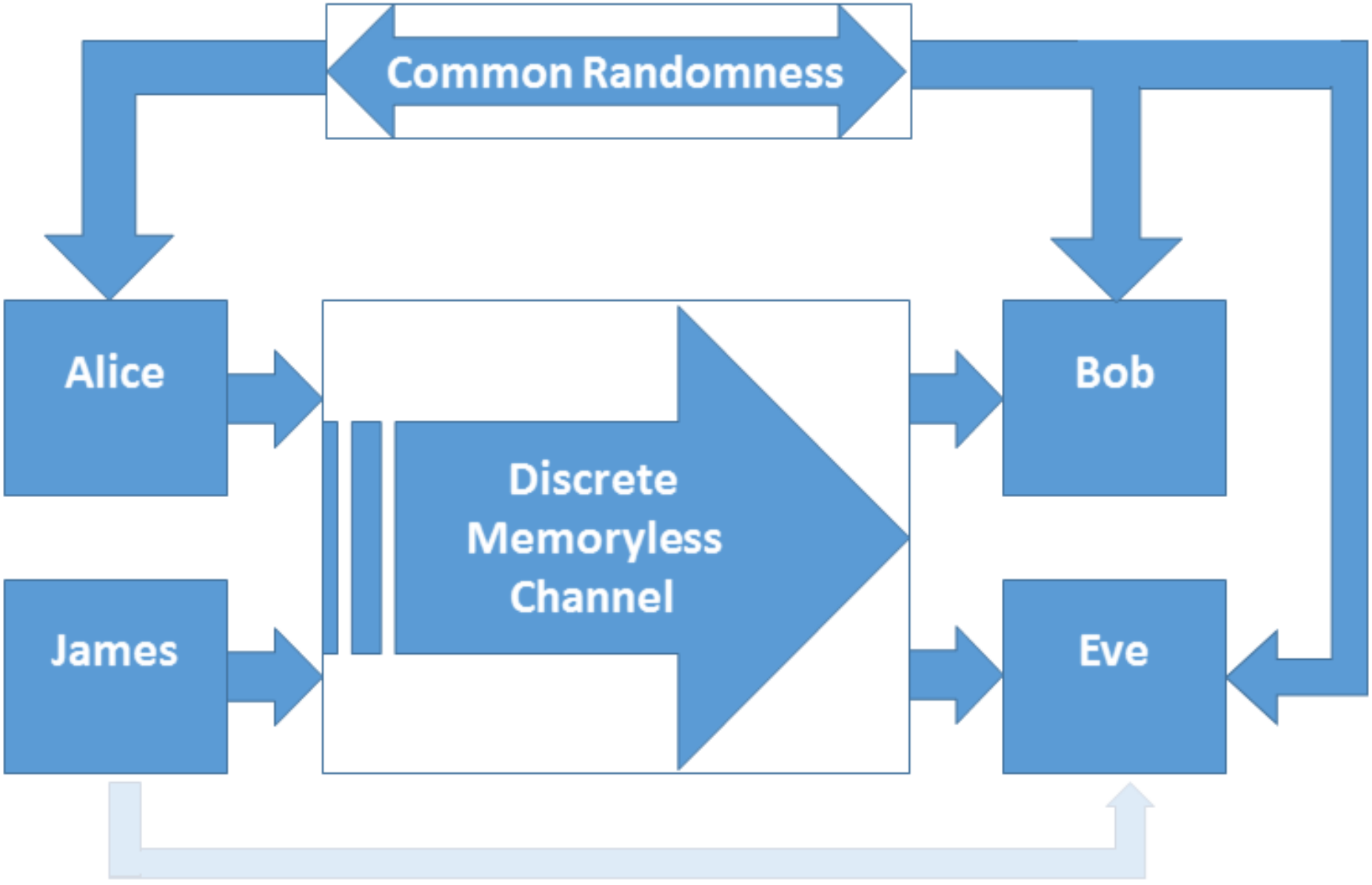
❸ The AVWC: Without External Randomness



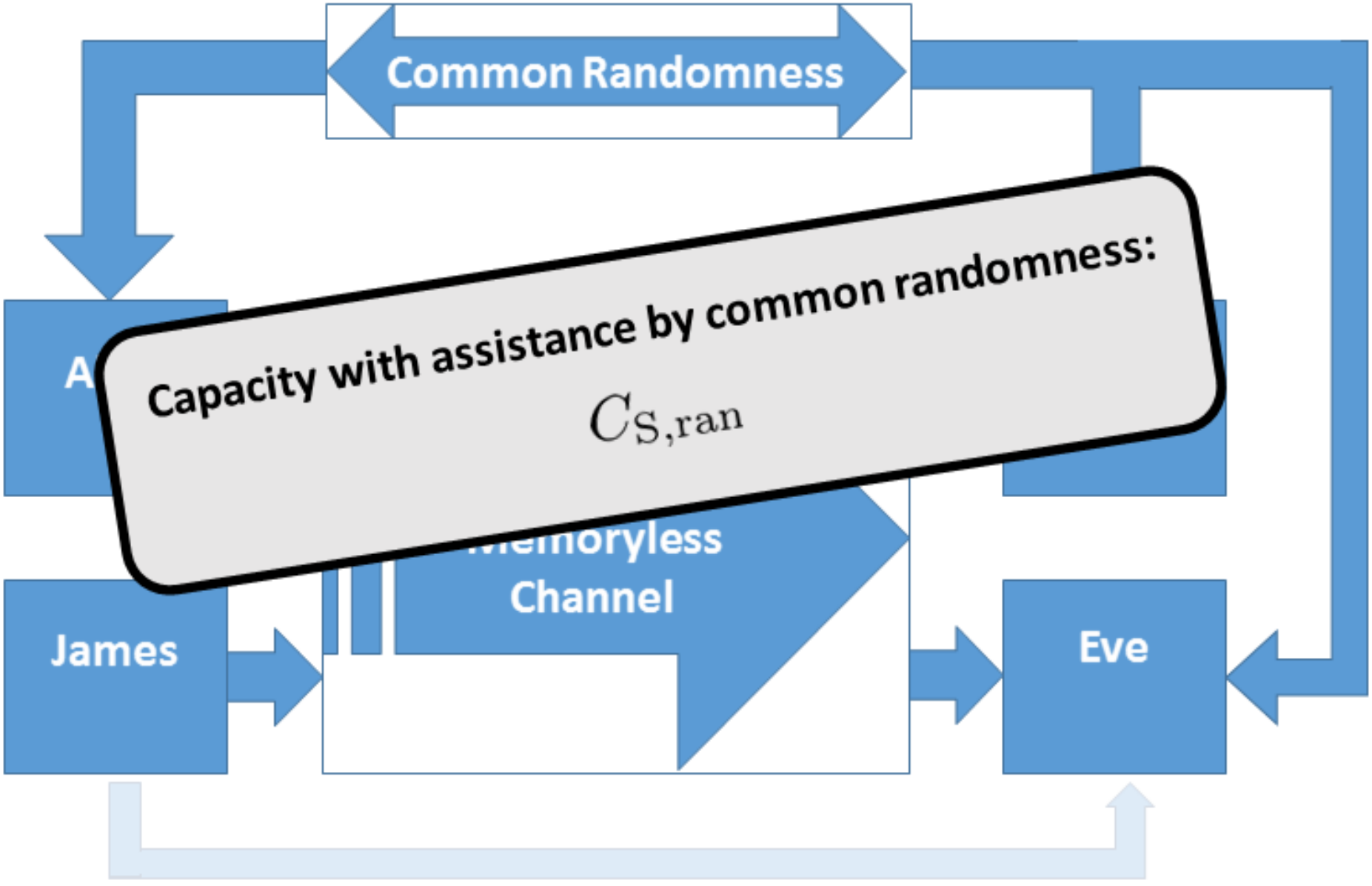
❸ The AVWC: Without External Randomness



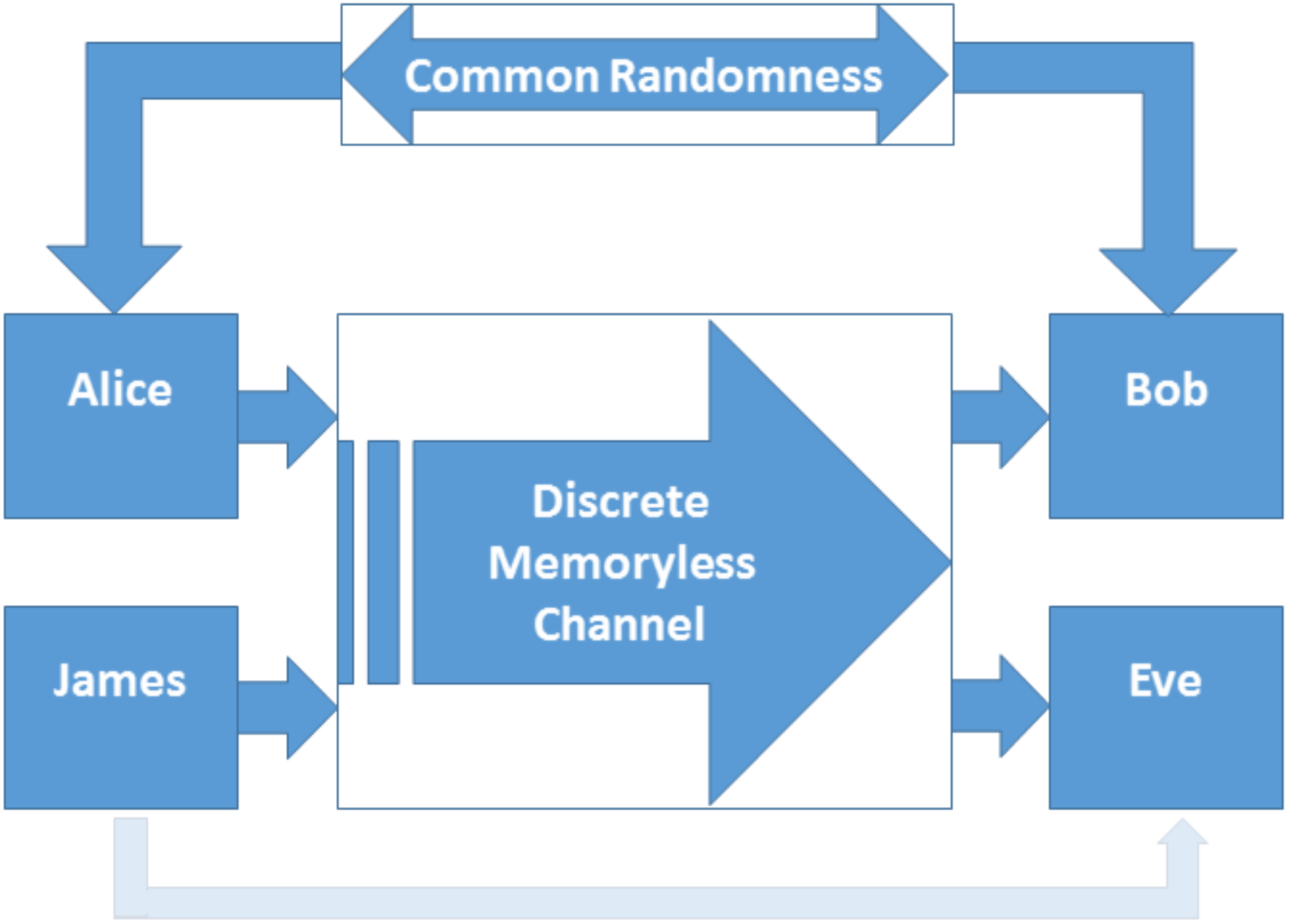
❸ The AVWC: With External Randomness known by Eve



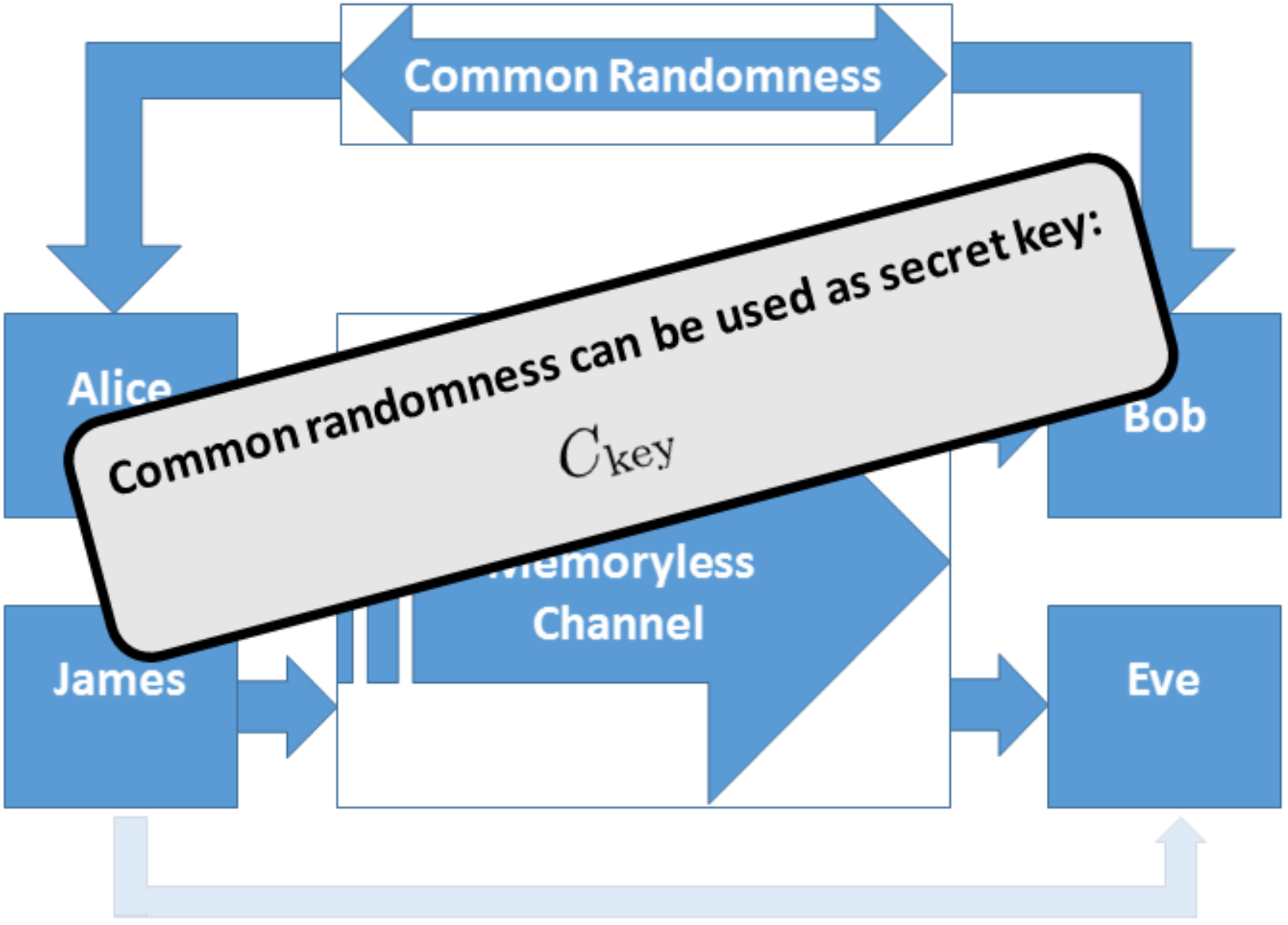
❸ The AVWC: With External Randomness known by Eve



❸ The AVWC: External Randomness used as Secret Key



❸ The AVWC: External Randomness used as Secret Key



❸ Why is this "beyond IID"?

- Forget about Eve (for the moment)
- The choices of James are not limited in any form.
- Thus, no probability distribution can be said to govern his choices, especially no i.i.d. distribution.
- Any code between Alice and Bob has to work reliably both under such extreme type of error and, simultaneously, under "usual" i.i.d. noise.
- One may think of the sources of the noise as split into two parts:
  1. One where e.g. a car can cross the communication link (James being the driver). Over the (short) time of communication, it may not be suitable to model such rare events as random variables.
  2. One where noise happens e.g. in a receive antenna. When the communication link is disturbed by a large obstacle (e.g. a car), the lower SNR increases the noise level in the antenna.
- Only the influence of e.g. common randomness allows to transform the model into the i.i.d. realm.
- We will give a short sketch of the respective mechanism:

❸ Why is this "beyond IID"?

Consider an AVC (W_1, W_2). How can Alice and Bob transform the AVWC to something more IID?

- Alice and Bob agree on any code. Let it have length 10.
- In addition, they choose (uniformly random) from the set of permutations on $\{1, \ldots, 10\}$.
- Consider James sending $s^{10} = (1, 1, 1, 1, 1, 2, 2, 2, 2, 2)$. The type of this is $10^{-1} \cdot N(1|s^{10}) = 5/10$.
- Alice and Bob's random code effectively transforms James' choice:

$$\frac{1}{10!} \sum_{\pi} \delta_{\pi(s^{10})} = |T_N|^{-1} \cdot \mathbb{1}_{T_N} \approx \left(\frac{1}{10} N(\cdot|s^{10}) \right)^{\otimes 10} = (\tfrac{1}{2}\mathbb{1})^{\otimes 10}.$$

- The communication cost of this is super-exponential, but may be brought down to roughly log of the number of channel uses.
- An external communication link is necessary for this, and James has to be kept ignorant of the exact permutation!
- This transforms the AVC to a compound channel.

❸ How super-activation occurs for AVWCs

- The effect is based on two observations:
  1. symmetrizability. A symmetrizable AVWC cannot transmit messages, but the defect can be repaired by using an external resource like e.g. shared randomness (Ahlswede dichotomy)
  2. There are AVWCs that allow for reliable but insecure transmission of data.
- Key idea:
  1. Take one symmetrizable AVWC which is secure when assisted by common randomness (CR).
  2. Take a second AVWC which is non-symmetrizable but not secure.
  3. Use the insecure AVWC to transmit messages to Bob.
  4. Use these messages as CR for the symmetrizable AVWC.
  5. Benefit from the positive CR-assisted secrecy capacity of the first AVWC.
- Immediate question: Is this the whole story?
- Answer: Still not known.
- One step on the way: see the next slides.

❹ 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 AVWCs by $(\mathfrak{W}, \mathfrak{V})$ in what follows.

❹ 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

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

❹ 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

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

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

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

❹ Definition of Capacities

DEF IV. Let $G > 0$. $C_{\text{key}}(\mathfrak{W}, \mathfrak{V}, G)$ 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. $C_{\text{S}}(\mathfrak{W}, \mathfrak{V})$ is the supremum over all $R \geq 0$ such that there is a secure deterministic coding scheme $\mathcal{K}$ at rate R.

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

❹ Results

RESULT 0. ([WNB16] Capacity with CR known by Eve) It holds

$$C_{\mathrm{S,ran}}(\mathfrak{W},\mathfrak{V}) = \lim_{n\to\infty} \frac{1}{n} \max_{p\in\mathcal{P}(\mathcal{U}_n)} \max_{U\in C(\mathcal{U}_n,\mathcal{X}^n)} \left(\min_{q\in\mathcal{P}(\mathcal{S})} I(p; W_q^{\otimes n}\circ U) - \max_{s^n\in\mathcal{S}^n} I(p; V_{s^n}\circ U) \right)$$

RESULT I. (Capacity with secret CR*) It holds

$$C_{\mathrm{key}}(\mathfrak{W},\mathfrak{V},G) = \min\{\ C_{\mathrm{S,ran}}(\mathfrak{W},\mathfrak{V}) + G,\ \ C_{\mathrm{S,ran}}(\mathfrak{W},\mathfrak{T})\ \},$$

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

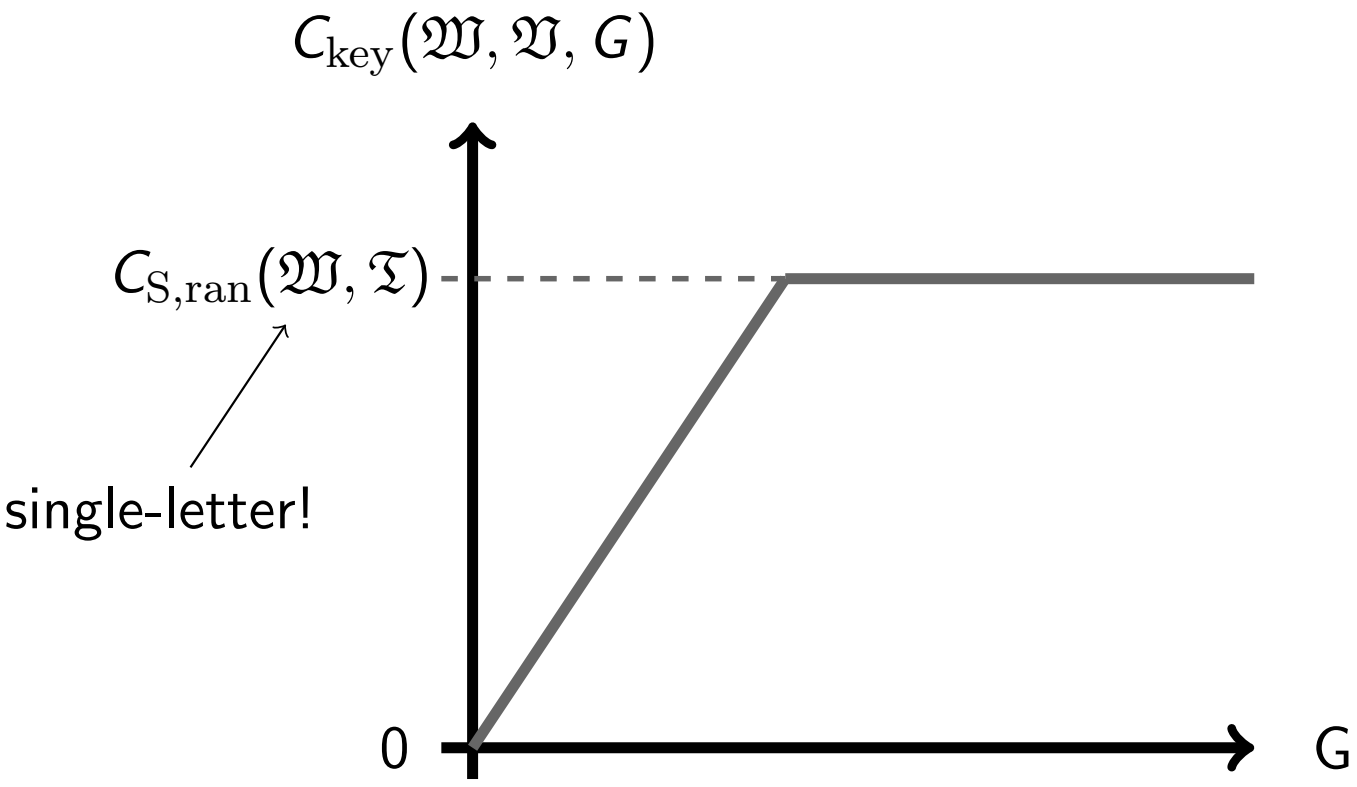
* Slightly sidestepping here, but it is important to see that searching for a simpler expression for the capacities of an AVWC is not a hopeless task.

❹ Results

RESULT I. (Capacity with secret CR) It holds

$$C_{\text{key}}(\mathfrak{W}, \mathfrak{V}, G) = \min\{\ C_{\text{S,ran}}(\mathfrak{W}, \mathfrak{V}) + G,\ \ C_{\text{S,ran}}(\mathfrak{W}, \mathfrak{T})\ \},$$

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



❹ Results

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

REMARK. The proof is based on [CN88], + additional tricks that account for the randomization that is necessary at the encoder in order to keep Eve obfuscated

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

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

❹ 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,

$$C_{\mathrm{S}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2) \geq C_{\mathrm{S}}(\mathfrak{W}_1, \mathfrak{V}_1) + C_{\mathrm{S}}(\mathfrak{W}_2, \mathfrak{V}_2)$$

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

$$C_{\mathrm{S}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2) > C_{\mathrm{S}}(\mathfrak{W}_1, \mathfrak{V}_1) + C_{\mathrm{S}}(\mathfrak{W}_2, \mathfrak{V}_2)$$

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

$$\begin{aligned} C_{\mathrm{S}}(\mathfrak{W}_1, \mathfrak{V}_1) = C_{\mathrm{S}}(\mathfrak{W}_2, \mathfrak{V}_2) = 0, \\ C_{\mathrm{S}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2) > 0 \end{aligned}$$

we speak of *super-activation*.

❹ Super-activation: results

RESULT III. (Super-activation) Let $(\mathfrak{W}_i, \mathfrak{V}_i)_{i=1,2}$ be AVWCs.
1) Assume that $C_{\mathrm{S}}(\mathfrak{W}_1, \mathfrak{V}_1) = C_{\mathrm{S}}(\mathfrak{W}_2, \mathfrak{V}_2) = 0$. Then

$$C_{\mathrm{S}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2) > 0$$

if and only if $\mathfrak{W}_1 \otimes \mathfrak{W}_2$ is not symmetrizable and
$C_{\mathrm{S,ran}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2) > 0$.
If $(\mathfrak{W}_i, \mathfrak{V}_i)_{i=1,2}$ can be super-activated it holds

$$C_{\mathrm{S}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2) = C_{\mathrm{S,ran}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2).$$

2) If $C_{\mathrm{S,ran}}$ shows super-activation for $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$, then C_{S} shows 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.
3) If $C_{\mathrm{S,ran}}$ shows no super-activation for $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$ then super-activation of C_{S} happens if and only if $\mathfrak{W}_1$ is non- symmetrizable and $\mathfrak{W}_2$ is symmetrizable and $C_{\mathrm{S,ran}}(\mathfrak{W}_1, \mathfrak{V}_1) = 0$ and $C_{\mathrm{S,ran}}(\mathfrak{W}_2, \mathfrak{V}_2) > 0$.

There exist pairs of AVWCs satisfying all inequalities in **1)** [BS13].

❹ Key ideas

- In [CN88] the following was proven: If $R < C(\mathfrak{W})$, and $\mathfrak{W}$ is non-symmetrizable, there exists $N \in \mathbb{N}$ such that for all $n \geq N$ we have $\mathbb{P}(\exists \text{ reliable code at rate } R) \geq 1 - \exp(2^{-n \cdot c'})$.
- Use [CN88] and add secrecy results on top. Exponential number of choices for James is OK because of double-exponentials in reliability and secrecy results.
- Requires heavy use of Chernoff-Hoeffding bound.
- That way, you get a on-shot coding result (Res1) without pre-coding U.
- Idea: keep using Res1, but for many copies of the channel (this makes use of a second characterization of $C_{\mathrm{S,ran}}$ from [WNB16]).
- Problem: pre-coding may turn a non-symmetrizable channel symmetrizable. Thus, the optimal rates may not be achievable using Res1!
- We now demonstrate that it may indeed happen that pre-coding makes a channel symmetrizable.
- Then, we explain the way out.

❹ Example: Calculations

For $x \in [0,1]$ set $x' := 1 - x$. Define $\mathfrak{W} \subset C(\{x_1, x_2\}, \{1,2,3\})$ by

$$w(\cdot|s_1, x_2) := 0.4\delta_1 + 0.5\delta_2 + 0.1\delta_3,$$
$$w(\cdot|s_1, x_1) := \delta_1, \;\; w(\cdot|s_2, x_1) := \delta_2, w(\cdot|s_2, x_2) := \delta_3$$

Then W is non-symmetrizable: If $\lambda, \mu \in [0,1]$, the equation

$$\lambda \cdot w(\cdot|s_1, x_1) + \lambda' \cdot w(\cdot|s_2, x_1) = \mu \cdot w(\cdot|s_1, x_2) + \mu' \cdot w(\cdot|s_2, x_2)$$

has no solution. With pre-coding by BSC N_p ($W'_s := W_s \circ N_p$):

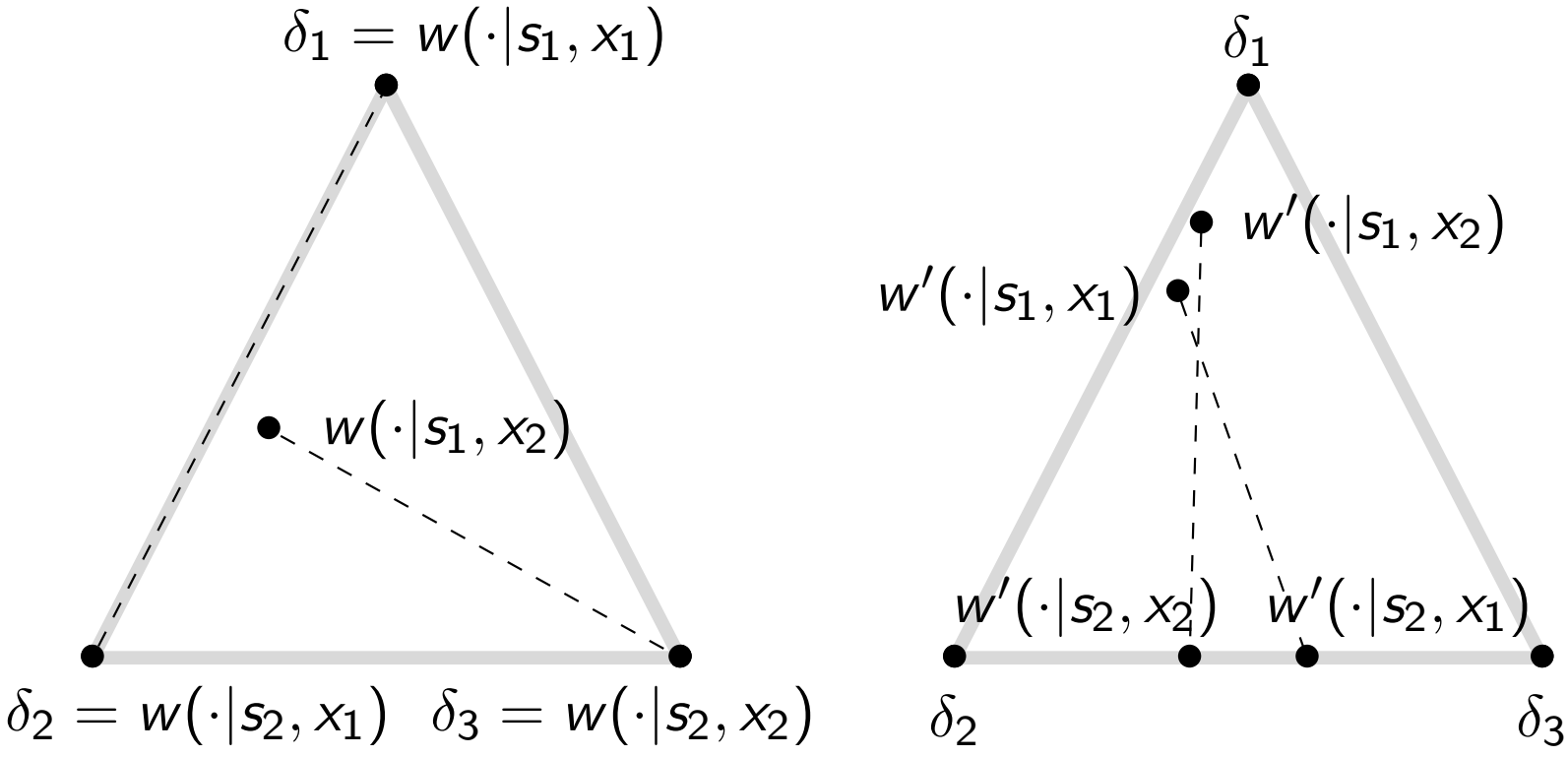
$$w'(\cdot|s_1, x_1) = p\delta_1 + p'(0.4\delta_1 + 0.5\delta_2 + 0.1\delta_3),$$
$$w'(\cdot|s_1, x_2) = p(0.4\delta_1 + 0.5\delta_2 + 0.1\delta_3) + p'\delta_1,$$
$$w'(\cdot|s_2, x_1) = p\delta_2 + p'\delta_3, \quad w'(\cdot|s_2, x_2) = p\delta_3 + p'\delta_2.$$

For $p = 0.4$, $\lambda = 38/45$, $\mu = 32/45$, the following holds:

$$\lambda \cdot w'(\cdot|s_1, x_1) + \lambda' \cdot w'(\cdot|s_2, x_1) = \mu \cdot w'(\cdot|s_1, x_2) + \mu' \cdot w'(\cdot|s_2, x_2).$$

Thus $\mathfrak{W}' = \mathfrak{W} \circ \mathfrak{N}_{0.4}$ is symmetrizable.

❹ Example: Pictures



Black dots denote probability distributions. Light gray lines are the edges of the probability simplex $\mathcal{P}(\{1, 2, 3\})$. The sets $\text{conv}(\{w(\cdot|s_1, x_i), w(\cdot|s_2, x_i)\})$ where $i = 1, 2$ are visualized as dashed lines. The intersection of the dashed lines in the right picture shows that $\mathfrak{W}'$ is symmetrizable.

❹ The way out of the symmetrizability trap

- Use sub-optimal encodings:
  1. Take the optimal U_n for the n-th term in the capacity formula.
  2. Set $\tilde{U}_{n+1} := \mathbb{1} \otimes U_n$.
  3. Define $\hat{\mathfrak{W}}$ by $(\hat{W}_{s^{n+1}} \circ \tilde{U}_{n+1})_{s^{n+1} \in \mathcal{S}^{n+1}}$, $\hat{\mathfrak{V}}$ accordingly.
  4. This definition ensures that $\hat{\mathfrak{W}}$ is non-symmetrizable.
  5. Use one-shot coding results for $(\hat{\mathfrak{W}}, \hat{\mathfrak{V}})$.
- Prove that this incurs a negligible deviation from optimal the n-th term in the capacity formula of order c/n for some constant c.
- As the capacity formula is regularized, the term c/n becomes insignificant for increasing n.
- This strategy automatically lets one achieve capacity for any non-symmetrizable AVWC, including those made up from pairs!
- Much more general than the activation protocol [BS13].
- Only one channel use is "insecure" (as compared to $\approx \log n$ in [BS13]). One may think of this slot as the one where the CR is transmitted.

❹ Conclusion

- AVWC is an example of a channel where super-activation happens.
- The effect can be explained in a very practical way.

- We provided an additional and complete characterization in terms of symmetrizability and $C_{\mathrm{S,ran}}$.

- Super-activation of $C_{\mathrm{S,ran}}$ remains an open problem. It is not clear whether the situation underlying the BS protocol is the only way to super-activate an AVWC.
- The expressions for $C_{\mathrm{S,ran}}$ look intractable.
- We provided some hope that $C_{\mathrm{S,ran}}$ could be single-letterizable when analyzing C_{key}.

- Further results include:
- Characterization of discontinuity points
- Stronger ("maximum") secrecy metric analyzed as well [WNB16]

THANKS FOR YOUR ATTENTION

Related work

[Ahl70] R. 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", Ann. Math. Stat., Vol. 41, No. 3, pp. 1027–1033 (1970)

[Ahl78] R. Ahlswede "Elimination of correlation for arbitrarily varying channels", Z. Wahrscheinlichkeitstheorie verw. Gebiete, Vol. 44, pp. 159–175 (1978)

[Alo98] N. Alon, "The Shannon capacity of a union", Combinatorica, Vol. 18, No. 3, pp. 301–310 (1998)

[BS13] H. Boche, R. Schaefer "Capacity results and super-activation for wiretap channels with active wiretappers" IEEE Trans. Inf. For. Sec., Vol. 8, No. 9, pp. 1482–1496(2013)

[CN88] I. Csiszar, P. Narayan "The capacity of the arbitrarily varying channel revisited: positivity, constraints" IEEE Trans. Inf. Theory, Vol. 34, No. 2, pp 181–193 (1988)

[Hae78] W. Haemers, "An upper bound for the Shannon capacity of a graph", Algebraic Methods in Graph Theory, (L. Lovasz and V. T. Sos), Colloq. Math. Soc. Janos Bolyai, 25, Szeged, Hungary, pp. 267–272, (1978)

[Hae79] W. Haemers, "On some problems of Lovasz concerning the Shannon capacity of a graph", IEEE Trans. Inf. Theory, Vol. 25, pp. 231–232 (1979)

[KMWY16] S. Karumanchi, S. Mancini, A. Winter, D. Yang, "Quantum Channel Capacities With Passive Environment Assistance", IEEE Trans. Inf. Theory, Vol. 62, No. 4, pp. 1733–1747 (2016)

[Mau93] U. Maurer, "Secret key agreement by public discussion from common information", IEEE Trans. Inf. Theory, Vol. 39, No. 3, pp. 733–742 (1993)

[NWB16] N., M. Wiese, H. Boche, "The Arbitrarily Varying Wiretap Channel - Secret Randomness, Stability, and Super-Activation", IEEE Trans. Inf. Theory, Vol. 62, No. 6 (2016)

[SY08] G. Smith and J. Yard. Quantum communication with zero-capacity channels. Science, 321:1812 (2008)

[Sha56] C. Shannon, "The zero error capacity of a noisy channel", IRE Trans. Inf. Theory, Vol. IT-2, pp. 8–19 (1956)

[WNB16] M. Wiese, N., H. Boche, "A channel under simultaneous jamming and eavesdropping attack - Correlated random coding capacities under strong secrecy criteria", IEEE Trans. Inf. Theory, vol. 62, no. 7, pp. 3844–3862 (2016)

Backup: Continuity

DEFINITION. Let $M_{\mathrm{f}} := \{M \subset C(\mathcal{X}, \mathcal{Y}) : |M| < \infty\}$. Define

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

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

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 $C_d(\mathfrak{W}', \mathfrak{V}') > 0$.