Common Randomness Generation from Finite Compound Sources

Rami Ezzine, Moritz Wiese, Christian Deppe and Holger Boche

Technical University of Munich, Munich, Germany

Technische Universität Braunschweig, Brunswick, Germany

BMBF Research Hub 6G-life, Germany

Munich Center for Quantum Science and Technology (MCQST)

Munich Quantum Valley (MQV)

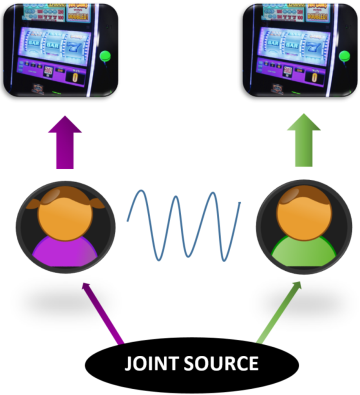
ISIT 2024

Outline

Outline

1. Overview
2. System Model for CR Generation from Finite Compound Sources
3. Single-Letter Bounds on the Compound CR Capacity
4. Proof Sketch of the Bounds
5. Conclusions

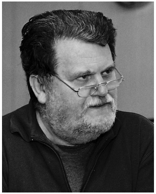
What is Common Randomness (CR)?



- The parties aim to agree on a common random variable with high probability

CR Generation

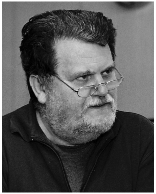
- Introduced by Ahlswede and Csiszár[1]



[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. II. CR capacity," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 225-240, 1998.

CR Generation

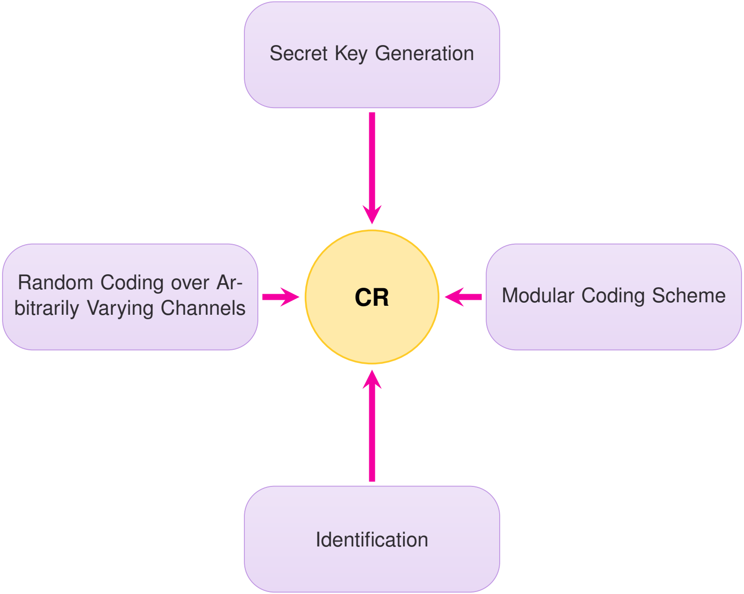
- Introduced by Ahlswede and Csiszár[1]



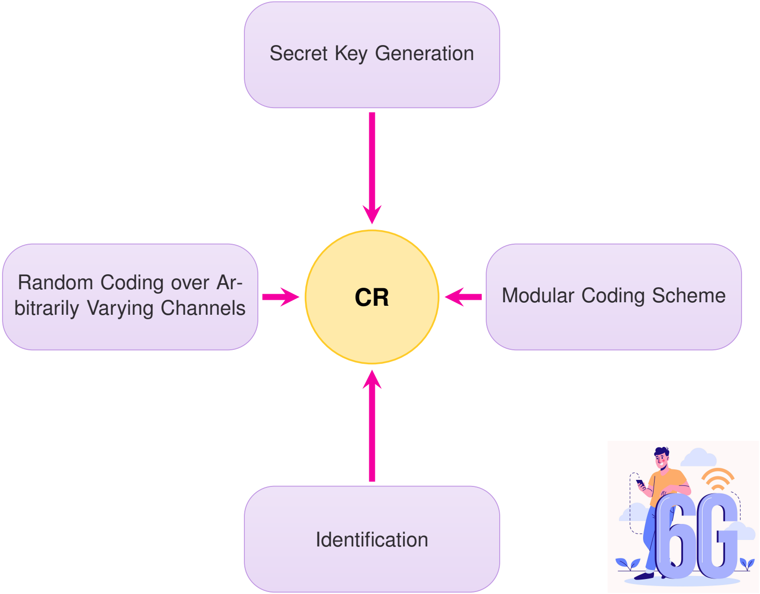
- Ahlswede and Csiszár established the CR capacity of rate-limited perfect channels as well as discrete memroyless channels[1]

[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. II. CR capacity," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 225-240, 1998.

Applications of CR Generation



Applications of CR Generation



Applications of CR Generation

Secret Key Generation

Random Coding over Arbitrarily Varying Channels

CR

Modular Coding Scheme

Identification

CR Generation with One-Way Communication

Source Type	Channel Type	Known Result
finite	Gaussian	Single-letter CR capacity Formula[1]

[1] R. Ezzine, W. Labidi, H. Boche and C. Deppe, "Common Randomness Generation and Identification over Gaussian Channels," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, Taipei, Taiwan, 2020.

[2] R. Ezzine, M. Wiese, C. Deppe and H. Boche, "Common Randomness Generation over Slow Fading Channels," 2021 IEEE International Symposium on Information Theory (ISIT), Melbourne, Australia, 2021.

[3] R. Ezzine, M. Wiese, C. Deppe and H. Boche, "A General Formula for Uniform Common Randomness Capacity," 2022 IEEE Information Theory Workshop (ITW), Mumbai, India, 2022.

[4] R. Ezzine, M. Wiese, C. Deppe and H. Boche, "A Lower and Upper Bound on the Epsilon-Uniform Common Randomness Capacity," 2023 IEEE International Symposium on Information Theory (ISIT), Taipei, Taiwan, 2023.

CR Generation with One-Way Communication

Source Type	Channel Type	Known Result
finite	Gaussian	Single-letter CR capacity Formula[1]
finite	Slow Fading with arbitrary state distribution	Single-letter outage CR capacity Formula[2]

[1] R. Ezzine, W. Labidi, H. Boche and C. Deppe, "Common Randomness Generation and Identification over Gaussian Channels," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, Taipei, Taiwan, 2020.

[2] R. Ezzine, M. Wiese, C. Deppe and H. Boche, "Common Randomness Generation over Slow Fading Channels," 2021 IEEE International Symposium on Information Theory (ISIT), Melbourne, Australia, 2021.

[3] R. Ezzine, M. Wiese, C. Deppe and H. Boche, "A General Formula for Uniform Common Randomness Capacity," 2022 IEEE Information Theory Workshop (ITW), Mumbai, India, 2022.

[4] R. Ezzine, M. Wiese, C. Deppe and H. Boche, "A Lower and Upper Bound on the Epsilon-Uniform Common Randomness Capacity," 2023 IEEE International Symposium on Information Theory (ISIT), Taipei, Taiwan, 2023.

CR Generation with One-Way Communication

Source Type	Channel Type	Known Result
finite	Gaussian	Single-letter CR capacity Formula[1]
finite	Slow Fading with arbitrary state distribution	Single-letter outage CR capacity Formula[2]
finite	Arbitrary	General Formula/Bounds on the Uniform CR Capacity[3]/ϵ-Uniform CR Capacity[4].

1 R. Ezzine, W. Labidi, H. Boche and C. Deppe, "Common Randomness Generation and Identification over Gaussian Channels," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, Taipei, Taiwan, 2020.

2 R. Ezzine, M. Wiese, C. Deppe and H. Boche, "Common Randomness Generation over Slow Fading Channels," 2021 IEEE International Symposium on Information Theory (ISIT), Melbourne, Australia, 2021.

3 R. Ezzine, M. Wiese, C. Deppe and H. Boche, "A General Formula for Uniform Common Randomness Capacity," 2022 IEEE Information Theory Workshop (ITW), Mumbai, India, 2022.

4 R. Ezzine, M. Wiese, C. Deppe and H. Boche, "A Lower and Upper Bound on the Epsilon-Uniform Common Randomness Capacity," 2023 IEEE International Symposium on Information Theory (ISIT), Taipei, Taiwan, 2023.

CR Generation from Compound Sources

- **Compound source**: the source derives from a defined uncertainty set, and the latter remains unchanged during the observation time scale
- The concept of generating shared randomness from compound sources was introduced solely in the context of secret key generation[1][2][3]
- No secrecy requirements are imposed in our work

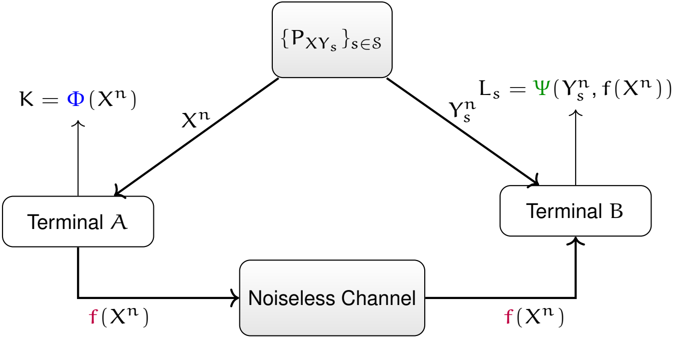
[1] H. Boche and R. F. Wyrembelski, "Secret key generation using compound sources - optimal key-rates and communication costs," in 9th International ITG Conference on Systems, Communication and Coding, pp. 1-6, 2013.

[2] N. Tavangaran, S. Baur, A. Grigorescu and H. Boche, "Compound Biometric Authentication Systems with Strong Secrecy," in 11th International ITG Conference on Systems, Communications and Coding, pp. 1-5, 2017.

[3] N. Tavangaran, H. Boche and R. F. Schaefer, Secret-Key Generation Using Compound Sources and One-Way Public Communication," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 227-241, 2017.

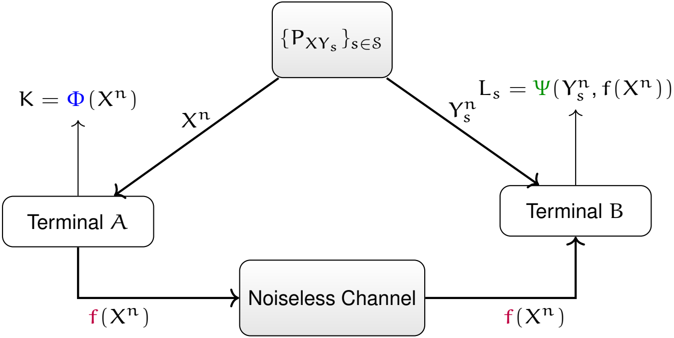
Outline

System Model



- $\{P_{XY_s}\}_{s\in\mathcal{S}}$ is a compound discrete memoryless multiple source (CDMMS)
- $\mathcal{S}$: Finite set of source states
- both terminals know the set of source states as well as their statistics with probability distributions $\{P_{XY_s}\}_{s\in\mathcal{S}}$ but they don't know the actual state $s \in \mathcal{S}$

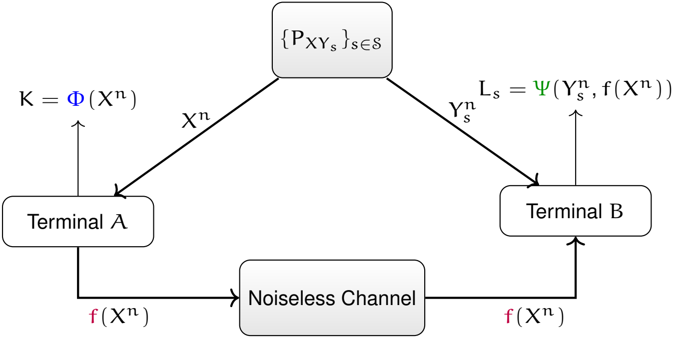
System Model



- The CDMMS emits i.i.d. samples of (X, Y_s)
- Communication over a noiseless channel with capacity $R > 0$

No other resources are available!

System Model



- (K, L_s) is called permissible pair
- **Question**: How much CR can we generate in one-way communication such that $\mathbb{P}[K \neq L_s]$ is small for every $s \in \mathcal{S}$?

Achievable Compound CR Rate

A number H is called an achievable compound CR rate if for every $\alpha, \delta > 0$ and for sufficiently large n there exists a permissible pair of random variables (K, L_s) for every $s \in \mathcal{S}$ such that

$$\forall s \in \mathcal{S} : \mathbb{P}[K \neq L_s] \leqslant \alpha$$

and

$$\frac{1}{n} H(K) > \mathrm{H} - \delta$$

Compound CR Capacity

The compound CR capacity $C_{CCR}(R)$ is the maximum achievable compound CR rate

Outline

Lower Bound on the Compound CR Capacity

Theorem

The compound CR capacity $C_{CCR}(R)$ *satisfies*

$$C_{CCR}(R) \geqslant \max_{\substack{U \\ \forall s \in \mathcal{S}: U \multimap X \multimap Y_s \\ I(U;X) - \min_{s \in \mathcal{S}} I(U;Y_s) \leqslant R}} I(U;X)$$

- *The alphabet* $\mathcal{U}$ *of* U *is subject to the cardinality bound*

$$|\mathcal{U}| \leqslant |\mathcal{X}| + |\mathcal{S}| - 1$$

Upper Bound on the Compound CR Capacity

Theorem

The compound CR capacity $C_{CCR}(R)$ *satisfies*

$$C_{CCR}(R) \leqslant \min_{s \in \mathcal{S}} \max_{\substack{U_s \\ U_s \multimap X \multimap Y_s \\ I(U_s;X) - I(U_s;Y_s) \leqslant R}} I(U_s;X)$$

- *For every* $s \in \mathcal{S}$, *the alphabet* $\mathcal{U}_s$ *of* U_s *is subject to the cardinality bound*

$$|\mathcal{U}_s| \leqslant |\mathcal{X}|$$

Facts

- $C_{CCR}(R) \leqslant H(X)$

Facts

- $C_{CCR}(R) \leqslant H(X)$
- For $R \geqslant \max_{s \in \mathcal{S}} H(X|Y_s)$, the bounds are both equal to $H(X)$

Facts

- $C_{CCR}(R) \leqslant H(X)$
- For $R \geqslant \max_{s \in \mathcal{S}} H(X|Y_s)$, the bounds are both equal to $H(X)$
- If there exists $s' \in \mathcal{S}$ such that for every $s \in \mathcal{S}$, $X \multimap Y_s \multimap Y_{s'}$ forms a Markov chain, then, the bounds are equal

Facts

- $C_{CCR}(R) \leqslant H(X)$
- For $R \geqslant \max_{s \in \mathcal{S}} H(X|Y_s)$, the bounds are both equal to $H(X)$
- If there exists $s' \in \mathcal{S}$ such that for every $s \in \mathcal{S}$, $X \multimap Y_s \multimap Y_{s'}$ forms a Markov chain, then, the bounds are equal
- For $R < \max_{s \in \mathcal{S}} H(X|Y_s)$,

$$\max_{\substack{U \\ \forall s \in \mathcal{S}: U \multimap X \multimap Y_s \\ I(U;X) - \min_{s \in \mathcal{S}} I(U;Y_s) \leqslant R}} I(U;X) \geqslant R$$

The lower-bound is not tight. **Example:** Consider $\mathcal{S} = \{s_0\}$ and $X = Y_{s_0}$ then for all $R > 0$

$$\max_{\substack{U \\ \forall s \in \mathcal{S}: U \multimap X \multimap Y_s \\ I(U;X) - \min_{s \in \mathcal{S}} I(U;Y_s) \leqslant R}} I(U;X) = H(X)$$

Outline

Proof Sketch of the Lower Bound

Extend the scheme provided by Ahslwede and Csiszár [1] to compound sources:

- Generation of nearly uniform random variables K and L_s for every $s \in \mathcal{S}$, s.t for sufficiently large n such that for every $\alpha > 0$

$$\forall s \in \mathcal{S} : \mathbb{P}\left[K \neq L_s\right] \leqslant \alpha \checkmark$$

$$\frac{1}{n}H(K) > I(U;X) - \delta \checkmark$$

for any U satisfying $\forall s \in \mathcal{S} : U \multimap X \multimap Y_s$ and $I(U;X) - \min_{s \in \mathcal{S}} I(U;Y_s) < R$

[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. II. CR capacity," in IEEE Transactions on Information Theory, vol. 44, no. 1, pp. 225-240, Jan. 1998.

Proof Sketch of the Lower Bound

1. Let $s \in \mathcal{S}$ be fixed arbitrarily. Let (x^n, y_s^n) be any realization of (X^n, Y_s^n)

Proof Sketch of the Lower Bound

1. Let $s \in \mathcal{S}$ be fixed arbitrarily. Let (x^n, y_s^n) be any realization of (X^n, Y_s^n)

2. Consider a set of sequences $\mathbf{U}_{i,j}, i = 1 \dots N_1, j = 1 \dots N_2$, uniformly distributed on $\mathcal{T}_\sigma^n(P_U)$ and let $\mathbf{u}_{i,j}$ some realization of $\mathbf{U}_{i,j}, i = 1 \dots N_1, j = 1 \dots N_2$,

    - $\mathcal{T}_\sigma^n(P_U)$: Set of σ-strongly typical sequences with respect to $P_U(\cdot)$

Proof Sketch of the Lower Bound

1. Let $s \in \mathcal{S}$ be fixed arbitrarily. Let (x^n, y_s^n) be any realization of (X^n, Y_s^n)

2. Consider a set of sequences $\mathbf{U}_{i,j}, i = 1 \ldots N_1, j = 1 \ldots N_2$, uniformly distributed on $\mathcal{T}_\sigma^n(P_U)$ and let $\mathbf{u}_{i,j}$ some realization of $\mathbf{U}_{i,j}, i = 1 \ldots N_1, j = 1 \ldots N_2$,

   - $\mathcal{T}_\sigma^n(P_U)$: Set of σ-strongly typical sequences with respect to $P_U(\cdot)$

3. $x^n \xrightarrow{\Phi} \mathbf{u}_{i,j} : (\mathbf{u}_{i,j}, x^n) \in \mathcal{T}_\sigma^n(P_{UX})$

   - $\mathcal{T}_\sigma^n(P_{UX})$: Set of σ-strongly typical sequences with respect to $P_{UX}(\cdot)$

Proof Sketch of the Lower Bound

1. Let $s \in \mathcal{S}$ be fixed arbitrarily. Let (x^n, y_s^n) be any realization of (X^n, Y_s^n)

2. Consider a set of sequences $\mathbf{U}_{i,j}, i = 1 \dots N_1, j = 1 \dots N_2$, uniformly distributed on $\mathcal{T}_\sigma^n(P_U)$ and let $\mathbf{u}_{i,j}$ some realization of $\mathbf{U}_{i,j}, i = 1 \dots N_1, j = 1 \dots N_2$,

   - $\mathcal{T}_\sigma^n(P_U)$: Set of σ-strongly typical sequences with respect to $P_U(\cdot)$

3. $x^n \xrightarrow{\Phi} \mathbf{u}_{i,j} : (\mathbf{u}_{i,j}, x^n) \in \mathcal{T}_\sigma^n(P_{UX})$

   - $\mathcal{T}_\sigma^n(P_{UX})$: Set of σ-strongly typical sequences with respect to $P_{UX}(\cdot)$

4. $(y_s^n, i) \xrightarrow{\Psi} \mathbf{u}_{i,\tilde{j}}$:
   - The index i is sent over the noiseless channel
   - $y_s^n \xrightarrow{E_i} \tilde{j}$ if there exists $s^\star \in \mathcal{S}$ such that $(\mathbf{u}_{i,\tilde{j}}, y_s^n) \in \mathcal{T}_\sigma^n(P_{UY_{s^\star}})$
     - $\mathcal{T}_\sigma^n(P_{UY_{s^\star}})$: Set of σ-strongly typical sequences with respect to $P_{UY_{s^\star}}(\cdot)$

Proof Sketch of the Lower Bound

1. Let $s \in \mathcal{S}$ be fixed arbitrarily. Let (x^n, y_s^n) be any realization of (X^n, Y_s^n)

2. Consider a set of sequences $\mathbf{U}_{i,j}, i = 1 \ldots N_1, j = 1 \ldots N_2$, uniformly distributed on $\mathcal{T}_\sigma^n(P_U)$ and let $\mathbf{u}_{i,j}$ some realization of $\mathbf{U}_{i,j}, i = 1 \ldots N_1, j = 1 \ldots N_2$,

   - $\mathcal{T}_\sigma^n(P_U)$: Set of σ-strongly typical sequences with respect to $P_U(\cdot)$

3. $x^n \xrightarrow{\Phi} \mathbf{u}_{i,j} : (\mathbf{u}_{i,j}, x^n) \in \mathcal{T}_\sigma^n(P_{UX})$

   - $\mathcal{T}_\sigma^n(P_{UX})$: Set of σ-strongly typical sequences with respect to $P_{UX}(\cdot)$

4. $(y_s^n, i) \xrightarrow{\Psi} \mathbf{u}_{i,\tilde{j}}$:
   - The index i is sent over the noiseless channel
   - $y_s^n \xrightarrow{E_i} \tilde{j}$ if there exists $s^\star \in \mathcal{S}$ such that $(\mathbf{u}_{i,\tilde{j}}, y_s^n) \in \mathcal{T}_\sigma^n(P_{UY_{s^\star}})$
     - $\mathcal{T}_\sigma^n(P_{UY_{s^\star}})$: Set of σ-strongly typical sequences with respect to $P_{UY_{s^\star}}(\cdot)$

No state estimation is required at Terminal B!

Proof Sketch of the Lower Bound

- Proof of the cardinality bound $|\mathcal{U}| \leqslant |\mathcal{X}| + |\mathcal{S}| - 1$ based on a direct application of the support lemma

Support Lemma [1]

Let $\mathcal{P}(X)$ be the family of all probability distributions on the set X, and let f_j, $j = 1, \ldots, k$ be real-valued continuous functions on $\mathcal{P}(X)$. Then to any probability measure μ on the Borel σ-algebra of $\mathcal{P}(X)$ there exist k elements P_i of $\mathcal{P}(X)$ and non-negative numbers $\alpha_1, \ldots, \alpha_k$ with $\sum_{i=1}^{k} \alpha_i = 1$ such that for every $j = 1, \ldots, k$:

$$\int_{\mathcal{P}(X)} f_j(P)\, \mu(dP) = \sum_{i=1}^{k} \alpha_i f_j(P_i)$$

[1] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*," 2nd ed. Cambridge University Press, 2011.

Proof Sketch of the Upper Bound

We prove that for every $s \in \mathcal{S}: \frac{H(K)}{n} \leqslant \max_{\substack{U_s \\ U_s \circ\!\!-\, X \circ\!\!-\, Y_s \\ I(U_s;X) - I(U_s;Y_s) \leqslant R + \zeta(n)}} I(U_s; X)$, for

$\zeta(n) > 0$ where $\lim_{n \to \infty} \zeta(n)$ can be made arbitrarily small ✓

Proof Sketch of the Upper Bound

We prove that for every $s \in \mathcal{S}$: $\frac{H(K)}{n} \leqslant \max_{\substack{U_s \\ U_s \multimap X \multimap Y_s \\ I(U_s;X)-I(U_s;Y_s)\leqslant R+\zeta(n)}} I(U_s;X)$, for $\zeta(n) > 0$ where $\lim_{n\to\infty} \zeta(n)$ can be made arbitrarily small ✓

1. Consider an arbitrary $s \in \mathcal{S}$ and define J to be uniformly distributed on $\{1, \ldots, n\}$ and $U_s = KX_1 \ldots X_{J-1}Y_{s,J+1} \ldots Y_{s,n}J$, where
   - $U_s \multimap X_J \multimap Y_{s,J}$
   - The joint distribution of X_J and $Y_{s,J}$ is equal to P_{XY_s}

Proof Sketch of the Upper Bound

We prove that for every $s \in \mathcal{S}: \frac{H(K)}{n} \leqslant \max_{\substack{U_s \\ U_s \multimap X \multimap Y_s \\ I(U_s;X)-I(U_s;Y_s) \leqslant R+\zeta(n)}} I(U_s;X)$, for $\zeta(n) > 0$ where $\lim_{n\to\infty} \zeta(n)$ can be made arbitrarily small ✓

1. Consider an arbitrary $s \in \mathcal{S}$ and define J to be uniformly distributed on $\{1,\dots,n\}$ and $U_s = KX_1 \dots X_{J-1} Y_{s,J+1} \dots Y_{s,n} J$, where
   - $U_s \multimap X_J \multimap Y_{s,J}$
   - The joint distribution of X_J and $Y_{s,J}$ is equal to P_{XY_s}
2. Show that $\frac{H(K)}{n} \leqslant I(U_s;X_J)$

Proof Sketch of the Upper Bound

We prove that for every $s \in \mathcal{S}: \frac{H(K)}{n} \leqslant \max_{\substack{U_s \\ U_s \multimap X \multimap Y_s \\ I(U_s;X)-I(U_s;Y_s)\leqslant R+\zeta(n)}} I(U_s;X)$, for $\zeta(n) > 0$ where $\lim_{n\to\infty} \zeta(n)$ can be made arbitrarily small ✓

1. Consider an arbitrary $s \in \mathcal{S}$ and define J to be uniformly distributed on $\{1, \dots, n\}$ and $U_s = KX_1 \dots X_{J-1} Y_{s,J+1} \dots Y_{s,n} J$, where
   - $U_s \multimap X_J \multimap Y_{s,J}$
   - The joint distribution of X_J and $Y_{s,J}$ is equal to P_{XY_s}
2. Show that $\frac{H(K)}{n} \leqslant I(U_s;X_J)$
3. Show that $\frac{H(K|Y_s^n)}{n} = I(U_s;X_J) - I(U_s;Y_{s,J})$

Proof Sketch of the Upper Bound

We prove that for every $s \in \mathcal{S}$: $\frac{H(K)}{n} \leqslant \max_{\substack{U_s \\ U_s \multimap X \multimap Y_s \\ I(U_s;X) - I(U_s;Y_s) \leqslant R + \zeta(n)}} I(U_s;X)$, for $\zeta(n) > 0$ where $\lim_{n \to \infty} \zeta(n)$ can be made arbitrarily small ✓

1. Consider an arbitrary $s \in \mathcal{S}$ and define J to be uniformly distributed on $\{1, \ldots, n\}$ and $U_s = KX_1 \ldots X_{J-1} Y_{s,J+1} \ldots Y_{s,n} J$, where
   - $U_s \multimap X_J \multimap Y_{s,J}$
   - The joint distribution of X_J and $Y_{s,J}$ is equal to P_{XY_s}
2. Show that $\frac{H(K)}{n} \leqslant I(U_s;X_J)$
3. Show that $\frac{H(K|Y_s^n)}{n} = I(U_s;X_J) - I(U_s;Y_{s,J})$
4. Show that $\frac{H(K|Y_s^n)}{n} \leqslant R + \zeta(n)$

Proof Sketch of the Upper Bound

We prove that for every $s \in \mathcal{S}$: $\frac{H(K)}{n} \leqslant \max_{\substack{U_s \\ U_s \multimap X \multimap Y_s \\ I(U_s;X)-I(U_s;Y_s)\leqslant R+\zeta(n)}} I(U_s;X)$, for $\zeta(n) > 0$ where $\lim_{n\to\infty} \zeta(n)$ can be made arbitrarily small ✓

1. Consider an arbitrary $s \in \mathcal{S}$ and define J to be uniformly distributed on $\{1, \ldots, n\}$ and $U_s = KX_1 \ldots X_{J-1}Y_{s,J+1} \ldots Y_{s,n}J$, where
   - $U_s \multimap X_J \multimap Y_{s,J}$
   - The joint distribution of X_J and $Y_{s,J}$ is equal to P_{XY_s}
2. Show that $\frac{H(K)}{n} \leqslant I(U_s;X_J)$
3. Show that $\frac{H(K|Y_s^n)}{n} = I(U_s;X_J) - I(U_s;Y_{s,J})$
4. Show that $\frac{H(K|Y_s^n)}{n} \leqslant R + \zeta(n)$

- Proof of the cardinality bound $|\mathcal{U}_s| \leqslant |\mathcal{X}|$ is based on a direct application of the support lemma.

Outline

Conclusions

- ☺ We established a single-letter lower and upper bound on the compound CR capacity for our proposed model
- ☺ We considered two special scenarios where the established bounds coincide
- ☺ **Open Problem**: Derivation of a single-letter formula of the compound CR capacity for our system model

Acknowledgements

Thank You !

- The authors acknowledge the financial support by the Federal Ministry of Education and Research of Germany in the program of “Souverän. Digital. Vernetzt.”. Joint project 6G-life, project identification number: 16KISK002
- Holger Boche and Christian Deppe further gratefully acknowledge the financial support by the BMBF Quantum Programm QD-CamNetz, Grant 16KISQ077, QuaPhySI, Grant 16KIS1598K, and QUIET, Grant 16KISQ093
- Christian Deppe was supported by the Bundesministerium für Bildung und Forschung (BMBF) through Grant 16KIS1005 and Rami Ezzine was supported by the BMBF through Grant 16KIS1003K
- Moritz Wiese was further supported by the Bavarian Ministry of Economic Affairs, Regional Development and Energy as part of the project 6G Future Lab Bavaria