Secure Identification for Gaussian Channels

Wafa Labidi, Christian Deppe and Holger Boche

Technische Universität München
Lehrstuhl für Theoretische Informationstechnik

ICASSP 2020

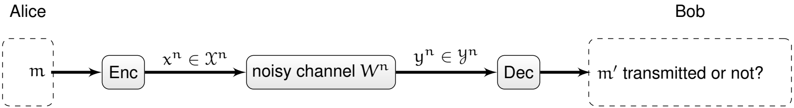
Outline

1. Identification: Overview
2. Identification for the Gaussian Wiretap Channel
3. Conclusions

Outline

1. Identification: Overview
2. Identification for the Gaussian Wiretap Channel
3. Conclusions

What is Identification?



Ahlswede/Dueck Picture 1989

What is Identification?

Shannon Picture 1948

- Receiver's goal: What is the message sent?
- Sender chooses and sends the message $m \in \mathcal{M} = \{1, \ldots, M = 2^{nC}\}$

Ahlswede/Dueck Picture 1989

- Receiver's goal: Is m' the message sent?
- Sender chooses and sends the identity $m \in \mathcal{N} = \{1, \ldots, N = 2^{2^{nC}}\}$

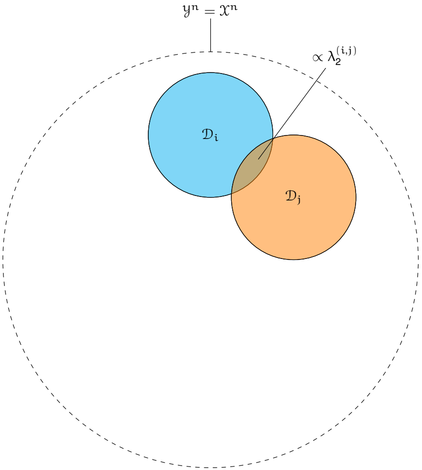
Randomized Identification (ID)-Code

Randomized ID-code

A randomized $(n, N, \lambda_1, \lambda_2)$ ID-code for a discrete memoryless channel (DMC) W is a family of pairs $\{(Q_i, \mathcal{D}_i) | i = 1, \dots, N\}$ with $\lambda_1, \lambda_2 \leqslant \lambda < \frac{1}{2}$ and $\forall i \in \{1, \dots, N\}$:

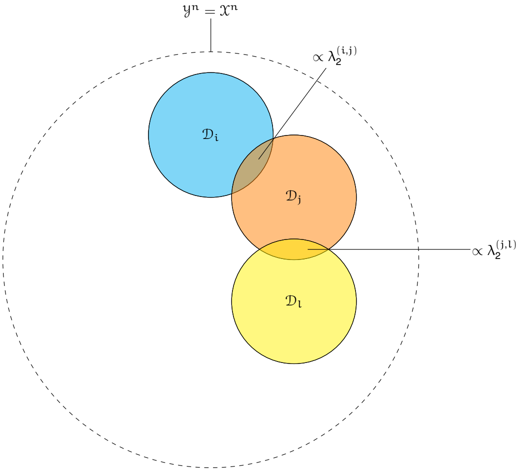
- $Q_i \in \mathcal{P}(\mathcal{X}^n),\ \mathcal{D}_i \subseteq \mathcal{Y}^n$
- $\sum_{x^n \in \mathcal{X}^n} Q_i(x^n) W^n(\mathcal{D}_i^c | x^n) \leqslant \lambda_1 \Longleftarrow$ channel noise
- $\sum_{x^n \in \mathcal{X}^n} Q_j(x^n) W^n(\mathcal{D}_i | x^n) \leqslant \lambda_2 \Longleftarrow$ ID-code

Randomized ID-Code



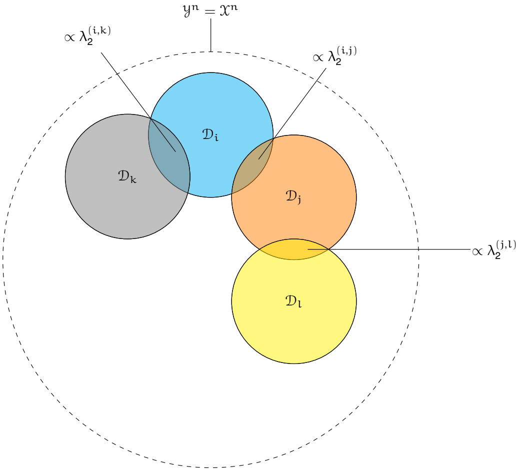
ID-code for a binary noiseless channel

Randomized ID-Code



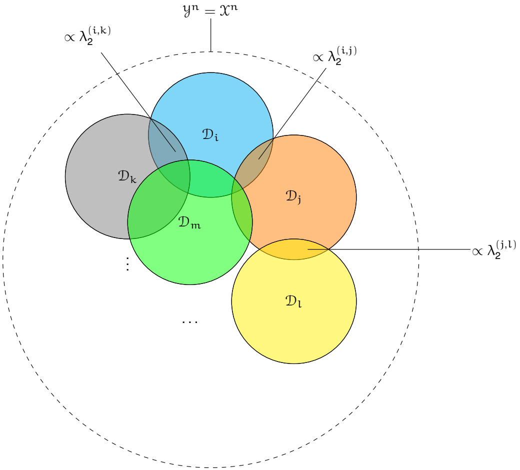
ID-code for a binary noisless channel

Randomized ID-Code



ID-code for a binary noisless channel

Randomized ID-Code



ID-code for a binary noiseless channel

Identification Coding Theorem [1] [2]

Theorem

Let W *be a finite DMC and* $N(n, \lambda)$ *the maximal number s.t. an* $(n, N, \lambda_1, \lambda_2)$ *ID-code for* $W(f, P)$ *exists with* $\lambda_1, \lambda_2 \leqslant \lambda$ *then:*

$$C_{ID}(W) = C(W), \quad \forall \lambda \in (0, \frac{1}{2})$$

$C(W)$ *is the Shannon transmission capacity of* W*,*
$C_{ID}(W) \triangleq \lim_{n\to\infty} \frac{1}{n} \log\log N(n, \lambda)$

[1] R. Ahlswede and G. Dueck, "Identification via channels," in IEEE Transactions on Information Theory, vol. 35, no. 1, pp. 15-29, Jan. 1989

[2] T. S. Han and S. Verdu, "New results in the theory of identification via channels," in IEEE Transactions on Information Theory, vol. 38, no. 1, pp. 14-25, Jan. 1992.

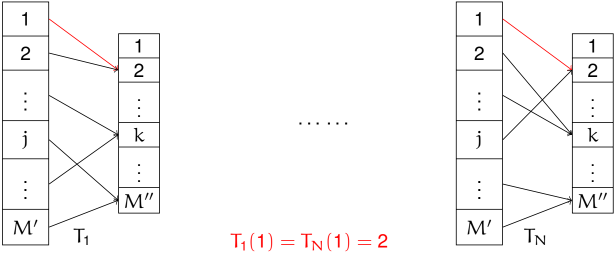
Direct Proof: Coding Scheme

1. To send a message i, we prepare a set of coloring functions T_i known by the sender and the receiver(s)

Direct Proof: Coding Scheme

1. To send a message i, we prepare a set of coloring functions T_i known by the sender and the receiver(s)

$$T_i : \{1, \dots, M'\} \longrightarrow \{1, \dots, M''\}$$
$$: \underbrace{j}_{\text{coloring}} \mapsto \underbrace{T_i(j)}_{\text{color}}$$



$T_1(1) = T_N(1) = 2$

Direct Proof: Coding Scheme

1. To send a message i, we prepare a set of coloring functions T_i known by the sender and the receiver(s)
2. The sender chooses a coloring j randomly and calculates the color of the message i under coloring j denoted by $T_i(j)$

Direct Proof: Coding Scheme

1. To send a message i, we prepare a set of coloring functions T_i known by the sender and the receiver(s)
2. The sender chooses a coloring j randomly and calculates the color of the message i under coloring j denoted by $T_i(j)$
3. Send $(j, T_i(j))$ over the channel

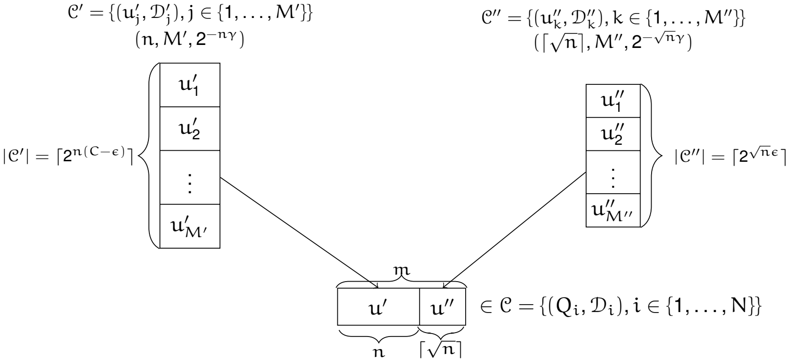
Direct Proof: Coding Scheme

1. To send a message i, we prepare a set of coloring functions T_i known by the sender and the receiver(s)
2. The sender chooses a coloring j randomly and calculates the color of the message i under coloring j denoted by $T_i(j)$
3. Send $(j, T_i(j))$ over the channel
4. The receiver, interested in i', calculates $T_{i'}(\hat{j})$

Direct Proof: Coding Scheme

1. To send a message i, we prepare a set of coloring functions T_i known by the sender and the receiver(s)
2. The sender chooses a coloring j randomly and calculates the color of the message i under coloring j denoted by $T_i(j)$
3. Send $(j, T_i(j))$ over the channel
4. The receiver, interested in i', calculates $T_{i'}(\hat{j})$
5. If $T_i(\hat{j}) = T_{i'}(\hat{j})$, then $i = i'$

Direct Proof: Code Construction

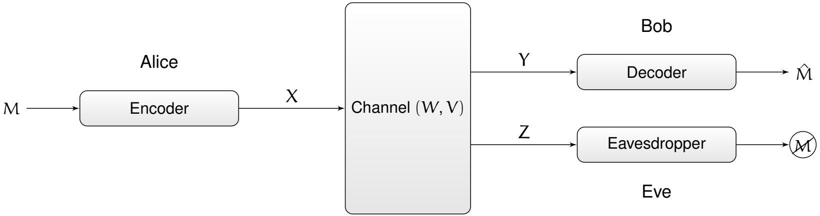


Outline

Wiretap Channel

Requirements:

- Secrecy (here strong): $I(M; Z^n) \leqslant \xi_1, \quad \xi_1 > 0$
- Reliability: $P_e^{(n)} \triangleq \Pr[\hat{M} \neq M] \leqslant \xi_2, \quad \xi_2 > 0$



Dichotomy Theorem [5]

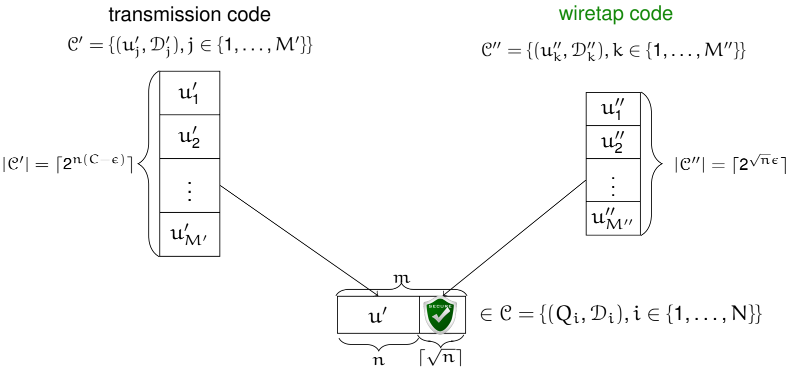
Theorem

We denote by $C(W)$ *the capacity of the channel* W *and by* $C_{SID}(W,V)$ *the identification capacity of the wiretap channel* (W,V) *then:*

$$C_{SID}(W,V) = \begin{cases} C(W) & \text{if } C_S(W,V) > 0 \\ 0 & \text{if } C_S(W,V) = 0 \end{cases}$$

[5] R. Ahlswede and Z. Zhang, "New directions in the theory of identification via channels," in IEEE Transactions on Information Theory, vol. 41, no. 4, pp. 1040-1050, July 1995.

Proof: Code Construction



Secure Codes for the Gaussian Channel

Wiretap transmission codes

An (n, M, λ) wiretap code for (W, V, g, g', P) is a family of pairs $\{(Q(\cdot|i), \mathcal{D}_i),\ i = 1, \ldots, M\}$ such that for all $in \in \{1, \ldots, M\}$:

- $Q(\cdot|i) \in \mathcal{P}(\mathcal{X}^n), \quad \mathcal{D}_i \subset \mathcal{Y}^n$
- $\mathcal{D}_i \cap \mathcal{D}_j = \emptyset, \quad \forall i \neq j$
- $\int_{x^n \in \mathcal{X}^n} Q(x^n|i) W^n(\mathcal{D}_i^c|x^n) d^n x^n \leqslant \lambda$
- $I(U; Z^n) \leqslant \lambda$

Secure Codes for the Gaussian Channel

Wiretap ID-codes

A randomized $(n, N, \lambda_1, \lambda_2)$ wiretap ID-code for (V, W, g, g', P) is a family of pairs $\{(Q(\cdot|i), \mathcal{D}_i),\ i = 1, \dots, N\}$ such that for $\lambda_1, \lambda_2 \leqslant \lambda < \frac{1}{2}$, $\forall \mathcal{E} \subset \mathcal{Z}^n$, $\forall i$:

- $Q(\cdot|i) \in \mathcal{P}(\mathcal{X}^n), \quad \mathcal{D}_i \subset \mathcal{Y}^n$
- $\sum_{l=1}^{n} x_l^2 \leqslant n \cdot P,\ \forall x^n \in \mathcal{X}^n$
- $\int_{x^n \in \mathcal{X}^n} Q(x^n|i) W^n(\mathcal{D}_i^c|x^n) d^n x^n \leqslant \lambda_1$
- $\int_{x^n \in \mathcal{X}^n} Q(x^n|j) W^n(\mathcal{D}_i|x^n) d^n x^n \leqslant \lambda_2, \quad \forall i \neq j$
- $\int_{x^n \in \mathcal{X}^n} Q(x^n|j) V^n(\mathcal{E}|x^n) + Q(x^n|i) V^n(\mathcal{E}^c|x^n) d^n x^n \geqslant 1 - \lambda,\ \forall i \neq j$

Extension for the Gaussian Case

- $W: \quad y_i = x_i + n_i, \quad n_i \sim \mathcal{N}(0, N) \triangleq g, \quad 1 \leqslant i \leqslant n$
- $V: \quad z_i = x_i + n_i', \quad n_i' \sim \mathcal{N}(0, N') \triangleq g', \quad 1 \leqslant i \leqslant n$
- Average power constraint: $\frac{1}{n} \sum_{i=1}^{n} x_i^2 \leqslant P$
- $\mathcal{Y} = \mathcal{Z} = \mathbb{R}$

$\Longrightarrow$ We call this channel (W, V, g, g', P)

Extension for the Gaussian Case: Dichotomy Theorem

Theorem (Secure identification capacity)

Let $C_{SID}(g, g', P)$ *be the identification capacity of the wiretap channel* (W, V, g, g', P) *then:*

$$C_{SID}(g, g', P) = \begin{cases} C(g, P) & \text{if } C_S(g, g', P) > 0 \\ 0 & \text{if } C_S(g, g', P) = 0 \end{cases}$$

Outline

Conclusions and Outlook

- We provided a coding scheme for the Gaussian wiretap channel and calculated the corresponding secure identification capacity. ☺
- **Future:**
  - Explore identification and secure identification for the single-user MIMO channel
  - Investigate identification over multi-user MIMO channels