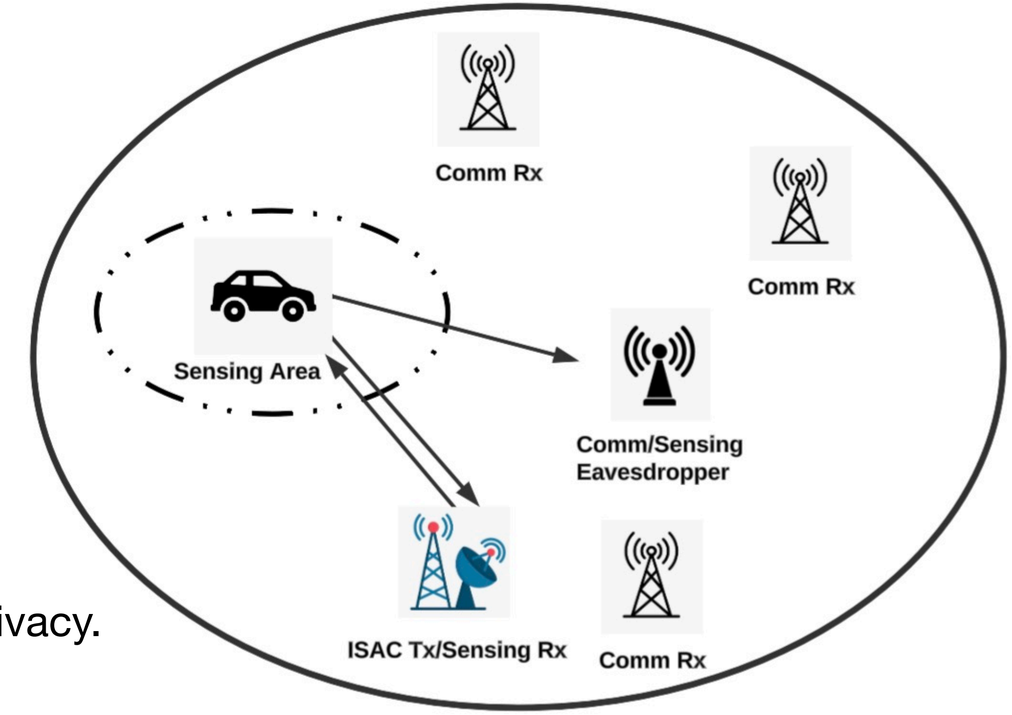
SECURE INTEGRATED SENSING AND COMMUNICATION AGAINST COMMUNICATION AND SENSING EAVESDROPPING

Wednesday July 01, 2026

Sidong Guo, Matthieu R. Bloch

School of Electrical and Computer Engineering

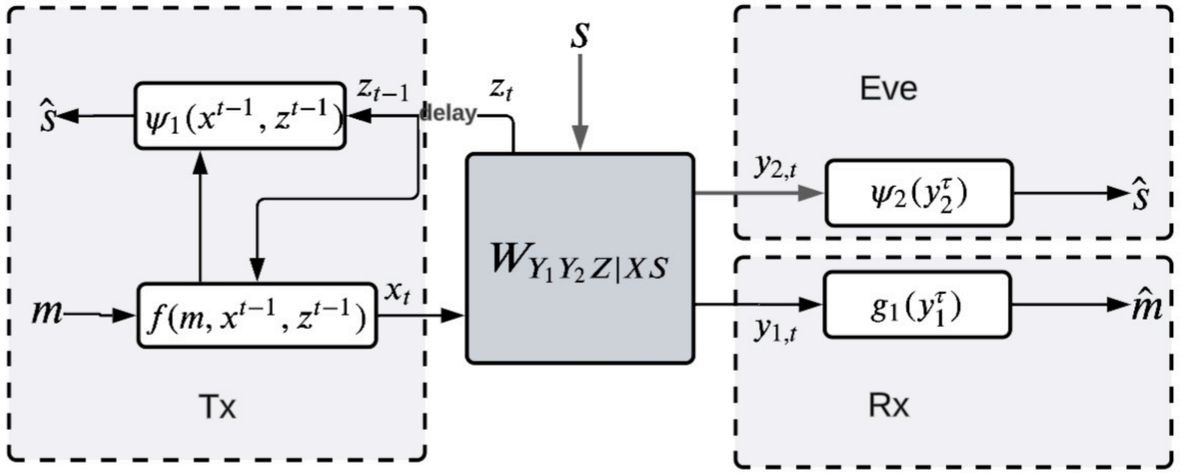
- **BACKGROUND**
  - ISAC architectures unify sensing and communication
    - Common hardware platforms
    - Common waveform
  - Integration creates two vulnerabilities
    - Eavesdropper could decode messages
    - Eavesdropper could infer sensing information



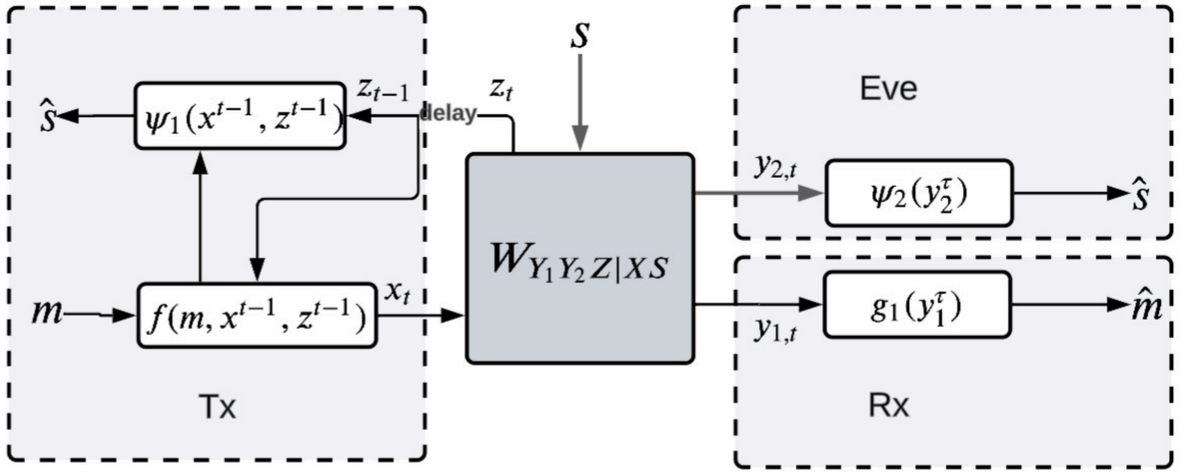
- **OBJECTIVE OF PRESENT WORK**
  - Considers **both** communication confidentiality and sensing privacy.
  - Characterize tradeoff between
    - Secrecy rate
    - Legitimate sensing performance
    - Adversarial sensing performance
  - Develop insight into efficient coding strategies

- **How can an ISAC transmitter simultaneously protect communication content and sensing information from a dual-purpose adversary?**

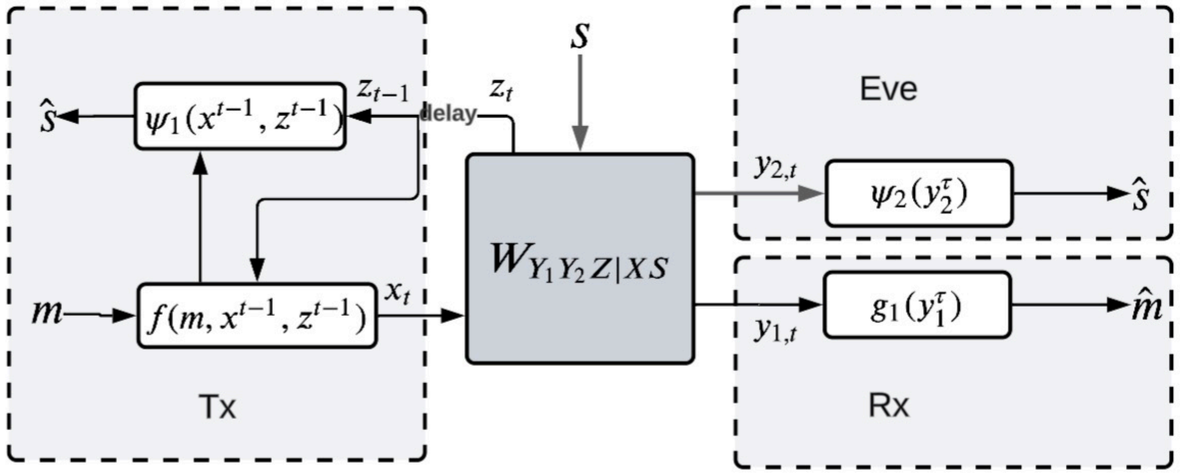
📚 **Integrated Sensing and Communication: Recent Advances and Ten Open Challenges,** Liu, Fan, et al. IEEE journal on selected areas in communications, 2022



- **MODELING ASSUMPTIONS**
  - State-dependent channel with **fixed state** during transmission,
  - One-tap delayed noiseless feedback to transmitter
  - Tx attempts to estimate channel state in mono-static configuration (knows input)
  - Tx attempts to communicate confidential message to eavesdropper
  - Eve attempts to estimate channel state in bi-static configuration (does *not* know input)
  - Both Tx, Rx and Eve have knowledge of the set of kernels $\{W_{Y_1|X,s}, W_{Y_2|X,s}\}_{s\in\mathcal{S}}$
  - Eavesdropper has knowledge of policy but not to realization of channel input
  - Both Tx and Eve use maximum likelihood estimator (MLE) using log likelihood ratio (LLR)



- **TECHNICAL ASSUMPTIONS**
  - The input, output and state spaces $\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2, \mathcal{Z}, \mathcal{S}$ are all finite.
  - $\forall s \neq s' \in \mathcal{S}$ and $\forall x \in \mathcal{X}$, $\forall y_1, y_2 \in \mathcal{Y}_1, \mathcal{Y}_2$, $0 < \mathbb{D}(W_{\cdot|X,s}(\cdot\,|x)\,||\,W_{\cdot|X,s'}(\cdot\,|x)) < \infty$
  - The prior distribution over all hypotheses is uniform



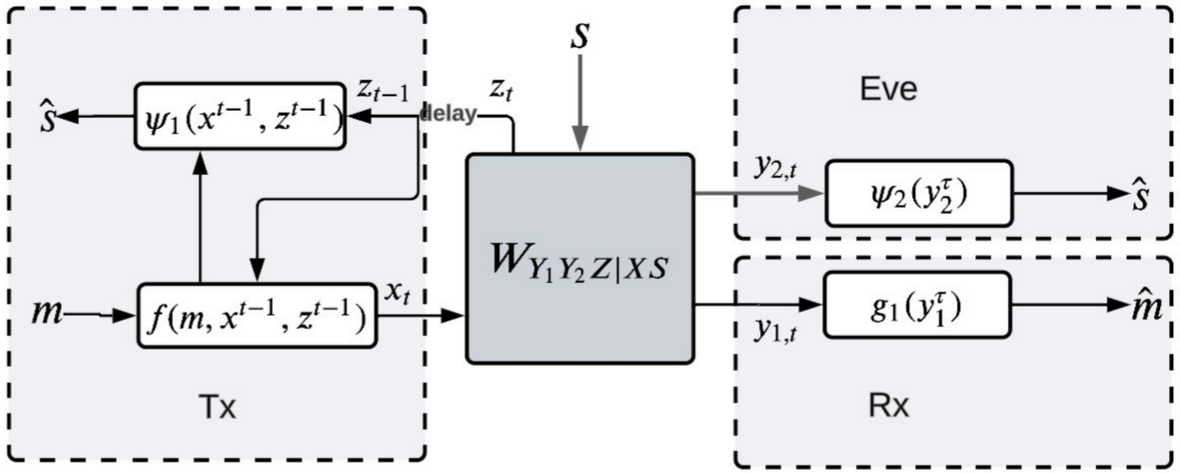
- **SEQUENTIAL ISAC MODEL**
  - Set of message $\mathscr{M} = \cup_{t=1}^{\infty} \mathbb{F}_2^t, \mathbb{F}_2 \triangleq \{0,1\}$, we count message bits M_τ transmitted by stopping time τ
  - Rate becomes a *random variable*
- **PERFORMANCE METRICS**
  - Communication performance quality is measured by (probabilistic) secrecy rate

$$\mathbb{P}\left(\frac{M_\tau}{n} \geqslant R\right) \geqslant 1-\delta \text{ such that } \mathbb{P}(M \neq \widehat{M}) \leqslant \epsilon \text{ and } I(M; Y_{2,\tau}) \leqslant \varepsilon$$

  - Sensing performance captured by detection exponents

$$E_{d_1}^n = -\frac{1}{n}\log P_{d_1} \text{ where } P_{d_1} = \max_{s\in\mathcal{S}} \max_{m\in\mathcal{M}} \mathbb{P}(\psi_1(X^\tau, Y_1^\tau) \neq S | M = m, S = s)$$

$$E_{d_2}^n = -\frac{1}{n}\log P_{d_2} \text{ where } P_{d_2} = \max_{s\in\mathcal{S}} \max_{s\in\mathcal{S}} \mathbb{P}(\psi_2(Y_2^\tau) \neq S | S = s)$$



Definition 1: Achievability

Let $\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6 > 0$, (R, E_1, E_2) tuple is achievable if $\exists n \geq n(\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6)$ such that ISAC policy has vanishing communication error probability $P_c \leq \delta_1$, information leakage $\max_{s \in \mathcal{S}} \mathbb{I}(M; Y_2^\tau) \leq \delta_2$ and probabilistic stopping time $\max_{s \in \mathcal{S}} \max_{w \in \mathscr{M}} \mathbb{P}(\tau > n) \leq \delta_3$ with

$$\min_{s \in \mathcal{S}} \min_{w \in \mathscr{M}} \mathbb{P}(R^n \geq R) \geq 1 - \delta_4,$$

$$E_{d_1}^n \geq E_1 - \delta_5,$$

$$E_{d_2}^n \leq E_2 + \delta_6 .$$

- **CHALLENGE I: SENSING SECURITY LACKS A UNIFIED DEFINITION IN LITERATURE**
  - Notion of sensing security very dependent on what sensing means
  - Prior work used an adversary's detection probability of sensing target **[1]**
  - Sensing security resemble privacy more than confidentiality
    - One can control and minimize leakage of information about message embedded in signals
    - One cannot completely eliminate an adversary's ability to infer environmental information
  - Sensing requires hiding the ***structure*** of transmitted signal

- **PROPOSED APPROACH: SENSING EXPONENTS**
  - Natural asymptotic extension of detection probability **[1]** are detection error exponent
  - Sensing security is characterized by legitimate and eavesdropper's detection error exponent **[2]**

- **CHALLENGE II: RANDOM STOPPING TIME OF SENSING**
  - Sequential estimation is easier to analyze than fixed length estimation
  - Stopping time is random, in contrast with traditional fixed-length communication scheme.

- **PROPOSED APPROACH: SEQUENTIAL ISAC**
  - Achievable policy is based on sub-packetization, where fixed-length coding is adaptive only on a block level.

📚**[1] Secure Cell-Free ISAC in the Presence of Information and Sensing Eavesdropper,** Ren, Zixiang, et al. IEEE journal on selected areas in communications, 2024
📚**[2] Evasive Hypothesis Testing,** Chang, Meng-Che, and Matthieu R. Bloch. IEEE journal on selected areas in information theory, 2021
📚**[3] Sequential Joint Communication and Sensing of Fixed States,** Chang, Meng-Che, and Matthieu R. Bloch. Proc. of IEEE Information Theory Workshop. IEEE, 2023.

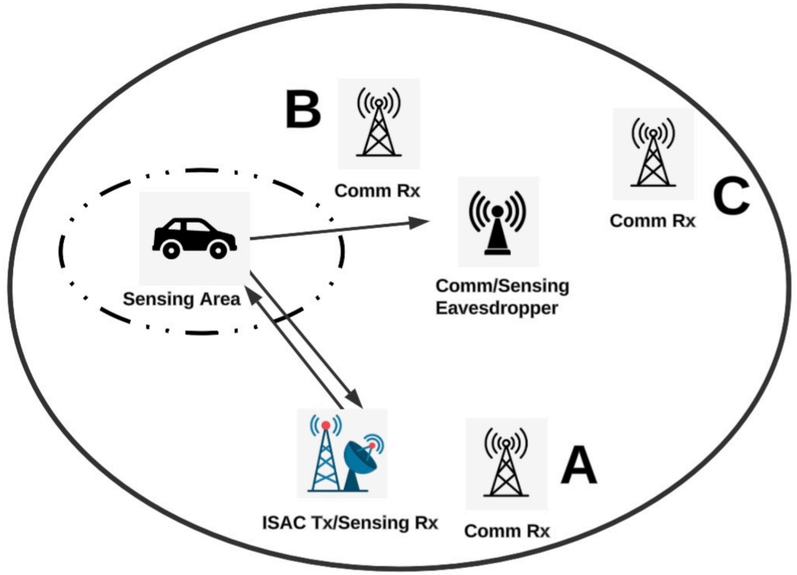
- Block-based adaptation structure: For some n, choose block length $N = \sqrt{n}$
- Tx and Rx first agree on a set of policies for each possible state $\{P_{X,s}\}_{s\in\mathcal{S}}$ (An off-line adaptive policy for each possible environmental state).
- For each block (Initial n^β blocks) : Tx use an universal policy $\tilde{P}_X = \arg\max_{P_X} \min_{s,s'\neq s} \mathbb{D}(W_{Y_1|X,s} \,||\, W_{Y_1|X,s'} | P_X)$ for sensing only
- For each block:
  - Tx first estimate the state s based on previous blocks and feedback (mono-static sensing)
  - Tx selects a stochastic encoder $P_{X,s}$ at the beginning of the block based on the ***estimated state*** s and knowledge of the kernels $\{W_{Y_1|X,s}, W_{Y_2|X,s}\}_{s\in\mathcal{S}}$
  - With perfect feedback, Tx and Rx distill a set of shared keys.
  - Tx employs policy $P_{X,s}$ and $(1-\gamma)N$ block length to transmit message and γN to transmit state information (using an universal code), with help of the shared keys.
  - Rx first recovers state information, then decode the message with shared keys.

- **Case A:** $\mathbb{I}(P_{X,s}; W_{Y_1|X,s}) \geq \mathbb{I}(P_{X,s}; W_{Y_2|X,s})$
  - Note that encoder decides based on estimated state $\hat{s}$, but it can be shown that with high probability $\hat{s} = s$
  - **Interpretation:** The legitimate receiver's channel has a larger capacity than Eavesdropper's channel
  - By resolvability argument, output mixture distribution at Eve behave like i.i.d distribution. Mixture distribution

$$\frac{1}{2^{M_\tau}} \sum_{m=1}^{2^{M_\tau}} \left[P_{X,s}\big(x_1(m)\big) \prod_{k=1}^{\tau-1} P_{X,s}\big(x_{k+1}(m) \mid x^k(m)\big) \times \prod_{k=1}^{\tau-1} W_{Y_2|X,s}\big(y_{2,k} \mid x_k(m)\big) \right]$$

Approximates product distribution $\prod_{k=1}^{\tau-1} \left(P_{X,s} \circ W_{Y_2|X,s} \right)$

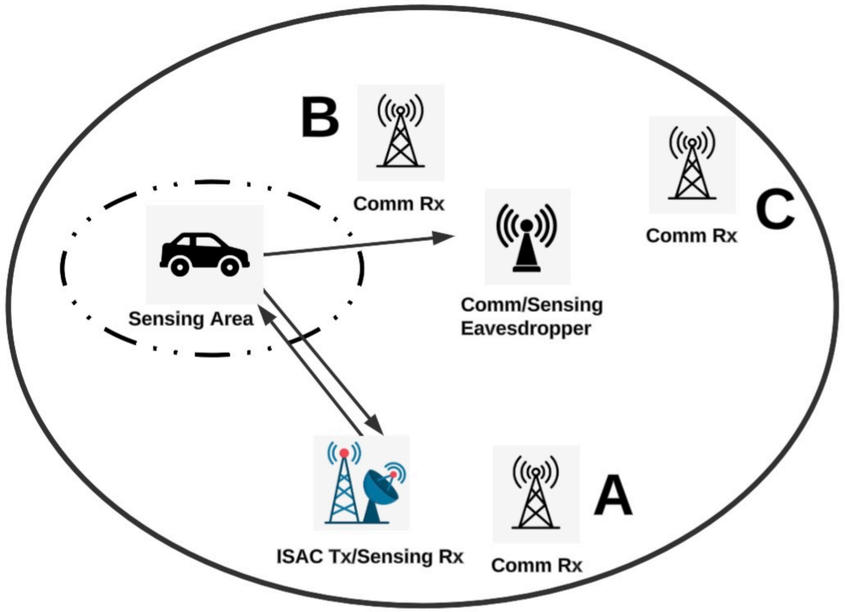
  - Dual-security policy: Tx uses all available keys for secure communication. Standard wiretap coding with feedback for each set of policies $\{P_{X,s}\}_{s \in \mathcal{S}}$ **[1][2]**
  - Tx's and Eve's detection exponent are in KL divergence and Chernoff information, respectively. Tx has control over stopping time while Eve functionally operates in fixed length.



Case A: Legitimate communication receiver A has channel advantage over Eavesdropper

[1] **Transmission, identification and common randomness capacities for wire-tape channels with secure feedback from the decoder,** Ahlswede, Rudolf, and Ning Cai. General Theory of Information Transfer and Combinatorics, 2008.
[2] **Physical-layer security: from information theory to security engineering,** Bloch, Matthieu, and Joao Barros. Cambridge University Press, 2011.

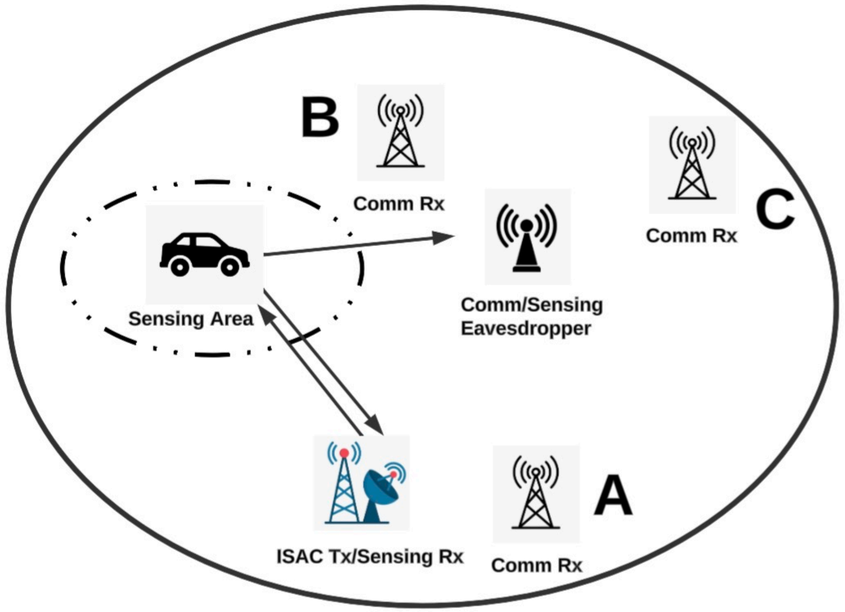
- **Case B:**
$$(\mathbb{I}(P_{X,s}; W_{Y_2|X,s}) - \mathbb{H}_{P_{X,s} \circ W_{Y_1,Y_2|X,s}}(Y_1 \,|\, X, Y_2))^+ < \mathbb{I}(P_{X,s}; W_{Y_1|X,s}) < \mathbb{I}(P_{X,s}; W_{Y_2|X,s})$$
  - **Interpretation:** The legitimate receiver's channel has a lower capacity than Eavesdropper's channel, but the channel quality gap can be bridged by key rate (obtained from feedback)
  - Transmitter may choose to balance communication security and sensing security:
    - Communication-secure policy: Uses all generated keys for one-time-pad
    - Sensing-secure policy: Uses part of keys to construct a resolvability code to induce i.i.d distribution at Eve, use remaining keys for one-time-pad **[1]**



Case B: Legitimate communication receiver B has a moderately worse channel than Eavesdropper

[1] **Covert communication over noisy channels: A resolvability perspective,** Bloch, Matthieu R. IEEE Transactions on Information Theory, 2016.

- **Case C:** $(\mathbb{I}(P_{X,s}; W_{Y_2|X,s}) - \mathbb{H}_{P_{X,s} \circ W_{Y_1,Y_2|X,s}}(Y_1 \,|\, X, Y_2))^+ > \mathbb{I}(P_{X,s}; W_{Y_1|X,s})$
  - **Interpretation:** The legitimate receiver's channel has a lower capacity than Eavesdropper's channel, and the channel quality gap is substantial such that feedback cannot help
  - Analyzing this regime is challenging, since no closed-form expression exists for Chernoff information between mixtures.
  - Since Transmitter cannot induce i.i.d output distribution at Eve, Eve may infer policy distribution from the ***structure*** of the codewords.
  - Transmitter may choose to balance communication security and sensing security:
    - Communication-secure policy: Uses all generated keys for one-time-pad and use adaptive policy $\{P_{X,s}\}_{s \in \mathcal{S}}$
    - Sensing-secure policy: Uses all generated keys for one-time-pad and use open-loop policy $\{P_{X,s} = P_X\}_{s \in \mathcal{S}}$.



Case C: Legitimate communication receiver C has substantially worse channel than Eavesdropper

Theorem 1: Achievable Region

The following region is achievable

$$\bigcup_{\substack{\rho \in [0,1], \\ \{P_{X,s}\}_{s\in\mathcal{S}} \in (\mathscr{P}_{\mathcal{X}})^{|\mathcal{S}|}}} \bigcap_{s\in\mathcal{S}} \{(R, E_1, E_2) \in \mathbb{R}_+^3\}$$

$$R \leq \min(\rho R_{\mathsf{key}}(s) + (1-\rho)[R_1(s) - R_2(s) + R_{\mathsf{key}}(s)]^+, R_1(s)),$$

$$E_1 \leq \min_{s'\neq s} \mathbb{D}(W_{Y_1|X,s} \,||\, W_{Y_1|X,s'} \,|\, P_{X,s}),$$

$$E_2 \geq \min_{s'\neq s} \mathbf{1}_{\{P_{X,s},P_{X,s'}\in\mathscr{P}_{res}\}}\{\rho\mathbb{C}(W_{Y_2|X,s} \,||\, W_{Y_2|X,s'} \,|\, P_{X,s}) + (1-\rho)\mathbb{C}(P_{X,s}\circ W_{Y_2|X,s} \,||\, P_{X,s'}\circ W_{Y_2|X,s'})\} + \mathbf{1}_{\{P_{X,s},P_{X,s'}\notin\mathscr{P}_{res}\}}\{\mathbb{C}(W_{Y_2|X,s} \,||\, W_{Y_2|X,s'} \,|\, P_{X,s})\}$$

Where $R_{\mathsf{key}}(s) = \mathbb{H}_{P_{X,s}\circ W_{Y_1,Y_2|X,s}}(Y_1 \,|\, X, Y_2)$, $R_1(s) = \mathbb{I}(P_{X,s}; W_{Y_1|X,s})$, $R_2(s) = \mathbb{I}(P_{X,s}; W_{Y_2|X,s})$. $\mathscr{P}_{res}$ is the resolvability region defined as

$$\mathscr{P}_{res}(P_{X,s}, P_{X,s'}) = \left\{ \begin{matrix} P_{X,s} \\ P_{X,s'} \end{matrix} \in \mathscr{P}_{\mathcal{X}} : \; R_1(s) - R_2(s) + R_{\mathsf{key}}(s) \geq 0, \mathbb{C}\left(P_{X,s}\circ W_{Y_2|X,s} \,\middle\|\, P_{X,s'}\circ W_{Y_2|X,s'}\right) < \min_{s''\in\{s,s'\}} E_{SC}(P_{X,s''}, W_{Y_2|X,s''}), \right\},$$

$$E_{SC}(P_X, W_{Y|X}) = \min_{Q_{Y|X}\in\mathscr{P}_{\mathcal{Y}|\mathcal{X}}} \left\{ \mathbb{D}(P_X Q_{Y|X} \,||\, P_X W_{Y|X}) + \frac{1}{2}[R - \mathbb{D}(P_X Q_{Y|X} \,||\, P_X Q_Y)]^+ \right\}$$

Is the soft covering exponent **[1]**.

📚**[1] Exact exponent for soft covering.** Yagli, Semih, and Paul Cuff. IEEE Transactions on Information Theory, 2019.

- We present a result for channel condition B:
$$(\mathbb{I}(P_{X,s}; W_{Y_2|X,s}) - \mathbb{H}_{P_{X,s}\circ W_{Y_1,Y_2|X,s}}(Y_1 \,|\, X, Y_2))^+ < \mathbb{I}(P_{X,s}; W_{Y_1|X,s}) < \mathbb{I}(P_{X,s}; W_{Y_2|X,s})$$
- We use binary symmetric channel to reduce the tuple (E_1, E_2, R) to a 2-D plot. In BSC, it is known that there is no tradeoff between Tx's detection exponent E_1 and rate R **[1]**
- Region I is perfect sensing security condition also possible in condition A, for a class of channels including BSC.
- Region III characterizes condition C in which sensing security cannot be guaranteed.

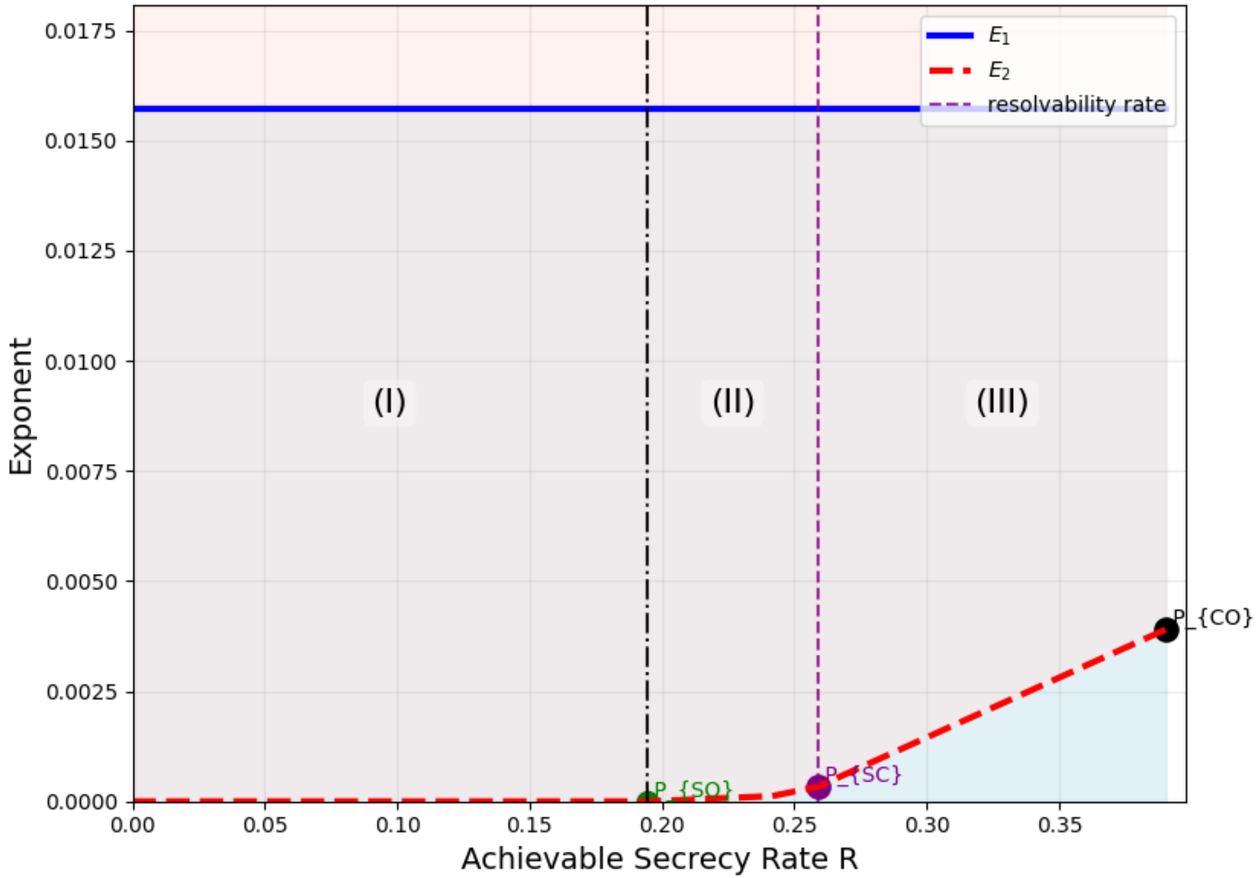


TABLE I: Table for BSC $W_{Y_2|X,S}(y_2|x,s), W_{Y_1|X,S}(y_1|x,s)$ and $S \in \{0,1\}$

S \ X	$W_{Y_1\|X,S}(y_1 = 1\|x = 0, s)$	$W_{Y_2\|X,S}(y_2 = 1\|x = 0, s)$
0	0.1	0.06
1	0.15	0.03

[1] **Rate and detection-error exponent tradeoff for joint communication and sensing of fixed channel states.** Meng-Che Chang, et al. IEEE Journal on Selected Areas in Information Theory, 2023.

- Case B:

$$(\mathbb{I}(P_{X,s}; W_{Y_2|X,s}) - \mathbb{H}_{P_{X,s} \circ W_{Y_1,Y_2|X,s}}(Y_1 \,|\, X, Y_2))^+ < \mathbb{I}(P_{X,s}; W_{Y_1|X,s}) < \mathbb{I}(P_{X,s}; W_{Y_2|X,s})$$

- Region (I): Tx selects input distribution $\{P_{X,s}\}_{s \in \mathcal{S}}$ that satisfies

$$\mathbb{C}\left(P_{X,s} \circ W_{Y_2|X,s} \,\middle\|\, P_{X,s'} \circ W_{Y_2|X,s'} \right) = 0, \forall s, s' \in \mathcal{S}$$

- Region (II): Tx deviates from the sensing-security-optimal tuple to one that maximizes the secrecy rate.
- Region (III): Tx employs open-loop strategy in order to not leak state information through adaptation, Eve's exponent is now conditional Chernoff $\mathbb{C}(W_{Y_2|X,s} \,||\, W_{Y_2|X,s'} \,|\, P_{X,s})$

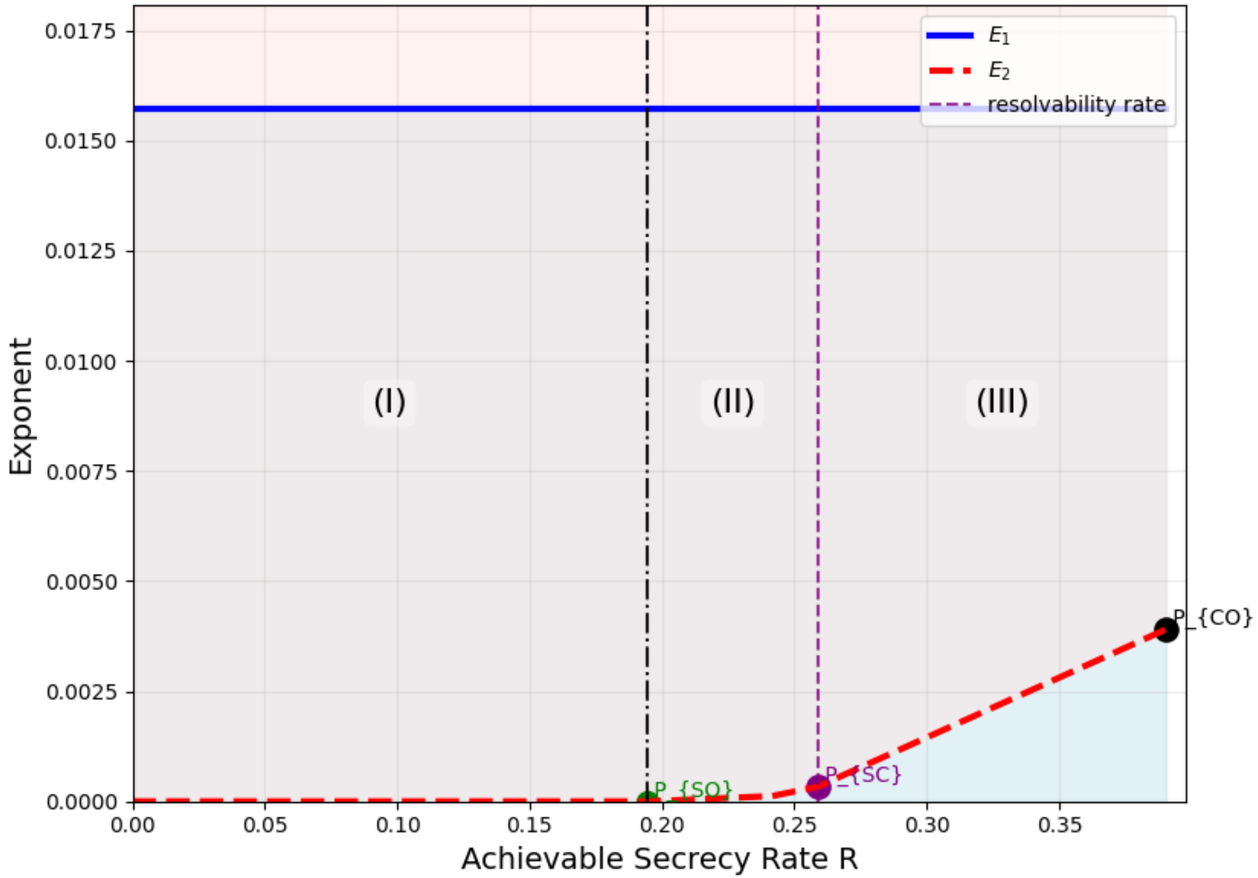


TABLE I: Table for BSC $W_{Y_2|X,S}(y_2|x,s), W_{Y_1|X,S}(y_1|x,s)$ and $S \in \{0,1\}$

S \ X	$W_{Y_1\|X,S}(y_1 = 1\|x = 0, s)$	$W_{Y_2\|X,S}(y_2 = 1\|x = 0, s)$
0	0.1	0.06
1	0.15	0.03

- **Stopping Time**
  - After the initial state-learning phase, every pairwise log-likelihood ratio $L^{(1)}_{s,s';t} = \log \frac{\mathbb{P}_s(X_t, Y_{1,t})}{\mathbb{P}_{s'}(X_t, Y_{1,t})}$ has positive KL drift under the true hypothesis. Concentration of the bounded-increment LLR martingales using Azuma's inequality.
- **Detection Exponent**
  - Known result for symbol-level adaptation. Same techniques applies to block-wise adaptation **[1].**
- **Eve's Detection Exponent**
  - Eve only observes the sensing output. Soft covering makes the induced output law close to the target mixture whenever the soft covering rate exceeds Eve's sensing exponent.
  - Thus Eve is limited to the Chernoff information of the corresponding mixture distributions $E_2 \leq \mathbb{C}\left(P_{X,s} \circ W_{Y_2|X,s} \| P_{X,s'} \circ W_{Y_2|X,s'}\right)$; however, without sufficient covering, the open-loop Chernoff exponent $\mathbb{C}(W_{Y_2|X,s} \,||\, W_{Y_2|X,s'} \,|\, P_{X,s})$ is used as a valid upper bound.
- **Reliability**
  - Use union bound to isolate communication error, initial estimation error and estimation error in each block. Using standard typicality techniques from wiretap code.
- **Secrecy**
  - Show that both within-block and cross-block leakage vanish; **see the conference paper for details.**

📚**[1] Controlled Sensing for Multi-hypothesis Testing.** S. Nitinawarat, G. K. Atia, and V. V. Veeravalli. IEEE Transactions on Automatic Control, 2013.

- **Future Works**
  - A more explicit characterization when soft-covering does not provide sufficient randomness to induce i.i.d distribution
  - Converse in ISAC setting with adaptive feedback

THANK YOU!