

---

# PLS: VISION, MYTHS, AND LOOKING AHEAD

---

MATTHIEU R BLOCH

NSF NextG Security Workshop - Physical Layer Panel

# VISION FOR NEXTG: SECURITY AS A SYSTEM LEVEL METRIC

## SWaPS: Size, Weight and Power, Security

- Systems are designed to *trade off* performance and cost
- Traditionally: size, weight, power consumption, etc.
- Can security be incorporated into the design?

**Challenge:** security is digital while cost metrics are analog.

**Information theory to the rescue:**

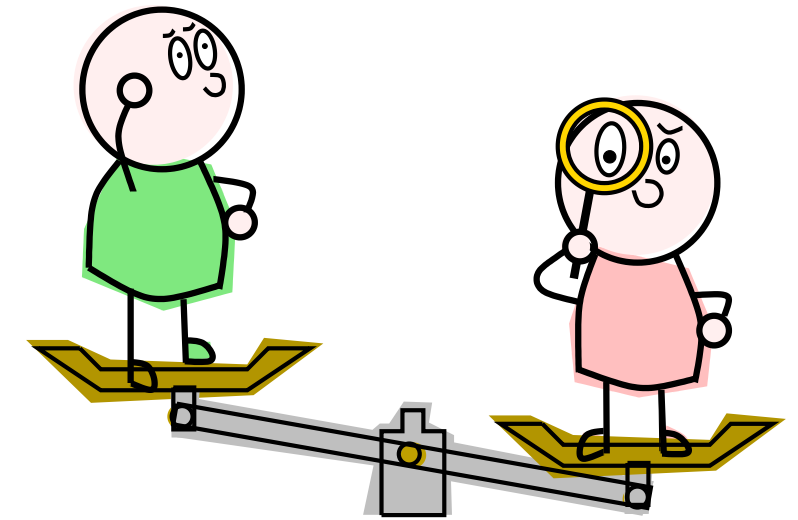
$$C_s = \log(1 + \text{SNR}_B) - \log(1 + \text{SNR}_E)$$

- Information theory provides *metrics* to measure information leakage

$$\max_{f, M} \left( \max_{\mathcal{A}} \mathbb{P}(\mathcal{A}(\mathbf{Z}) = f(M)) - \max_W \mathbb{P}(W = f(M)) \right) \quad \mathcal{L}(X \rightarrow Y) = \sup_{U-X-Y-\hat{U}} \frac{\mathbb{P}(U \neq \hat{U})}{\max_{u \in \mathcal{U}} P_U(u)}$$

- Coding and communication theory provides *algorithms* to control information leakage in signals

**Applications:** Privacy, integrity, authentication, LPI/LPD, confidentiality for edge devices and CPSs

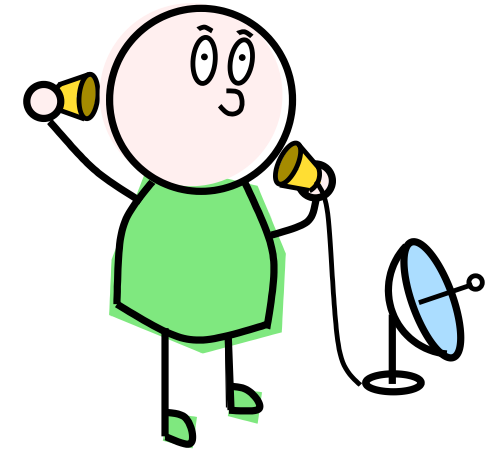


# MYTH: COMMUNICATIONS ENGINEERING AS USUAL

---

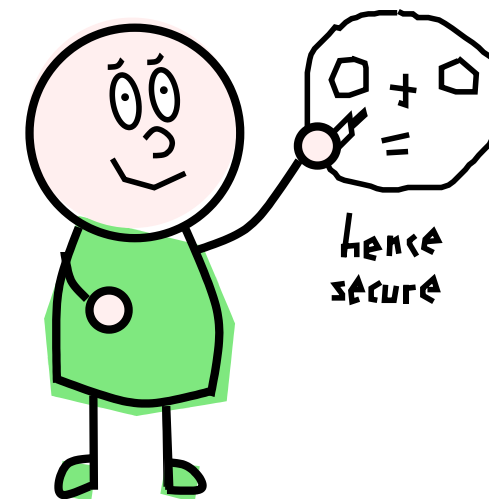
## Traditional communications systems engineering

- “Just put a convolutional/Turbo/LDPC code”
- Resource allocation with information-theoretic formulas sort of works
- Results are *robust* to modeling assumptions (channel estimation)
- The proof is in the *simulation* (BER estimates, etc.)



## Secure communication systems engineering

- Codes are more complicated: our favorite code may not work
- Secrecy capacity *only makes sense* if using specific coding schemes
- Basic results are *fragile* w.r.t. modeling assumptions
- The proof is in the *proof* (can't simulate security)



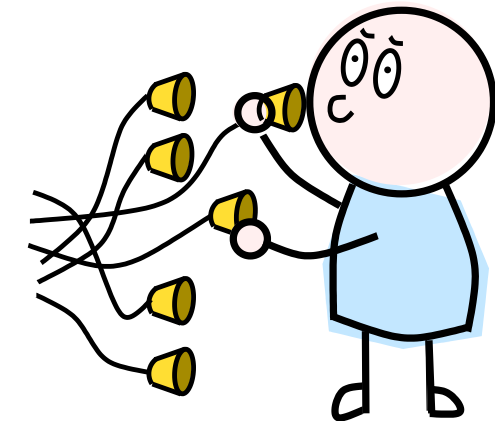
## Some good news: there are solutions to this problem

- Integrate ML ideas to learn what you do not know
- Use techniques from crypto (invertible extractors)
- Include *uncertainty* in the models

# LOOKING AHEAD: CODING, LEARNING, AND CIRCUITS

## Embrace noisy observation structures and coding for security

- We can *engineer* noisy observations structures
- Coding is the *glue* that ties system-level metrics to security
- Coding applies at all layers (PHY, MAC, Network)
- Coding helps for privacy, integrity, confidentiality
- If done well, coding will yield good secrecy/performance trade-off

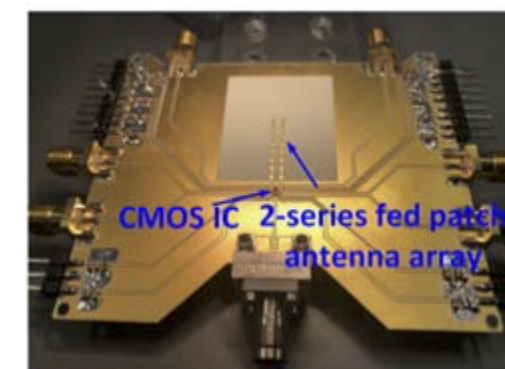


## Leverage ML

- Many NextG issues are at the *edge*: liabilities and opportunities
- If the adversary can learn, so can legitimate parties
- Sensing (feedback from the environment) is becoming easier and cheaper

## Engage with device colleagues

- The proof is in the *proof* pudding: build systems!
- Jianjun Ma et al., Security and eavesdropping in terahertz wireless links, Nature, (2018)
- X. Lu et al., Space-Time Modulated 71-to-76GHz mm-Wave Transmitter Array for Physically Secure Directional Wireless Links, Proc. of IEEE International Solid- State Circuits Conference, (2020)



Lu et al., ISSCC 2020