SESSION 4: PERFORMANCE ANALYSIS: $P_e$

- Probability of Error Analysis for SSM and QIM
- Two Codewords
- Multiple Codewords
Probability of Error

- Decoding regions $\mathcal{Y}_m, m \in \mathcal{M}$
  \[ \Rightarrow \text{ decoder outputs } m \text{ for all } y \in \mathcal{Y}_m \]

- Conditional error probability: $P_{e|m} = Pr[Y \notin \mathcal{Y}_m \mid m]$
SSM – Two Codewords

• Embedding & Detection:

\[ x = \begin{cases} 
  s + a & : m = 0 \\
  s - a & : m = 1 
\end{cases} \]

• Attack: \( y = x + w \)

• Statistical model: \( S \sim \mathcal{N}(0, \sigma_s^2 I_N) \) and \( W \sim \mathcal{N}(0, \sigma_w^2 I_N) \)

• Sufficient Statistic: \( t = \begin{cases} 
  \langle y, a \rangle & : \text{blind WM} \\
  \langle y - s, a \rangle & : \text{nonblind WM} 
\end{cases} \)
SSM (Cont’d)

• Noise variance at decoder:

\[ \sigma^2_{\text{noise}} = \begin{cases} 
\sigma^2_s + \sigma^2_w & : \text{blind WM} \\
\sigma^2_w & : \text{nonblind WM} 
\end{cases} \]

• \( P_e = Q(d/2) \) where \( d = \frac{2\|a\|}{\sigma_{\text{noise}}} \)

• Performance is typically much worse for blind WM.
Scalar QIM, One Sample

- Blind watermarking, 1-bit embedding:

Prototype $X_{sym}(s)$

$m = 0$  

$m = 1$

- Can make quantization noise $E \sim \mathbb{U}\left[-\frac{(1-\alpha)\Delta}{2\alpha}, \frac{(1-\alpha)\Delta}{2\alpha}\right]$ and independent of $S$ using dithered quantization
Scalar QIM (Cont’d)

- Rival pdf’s are quasi-periodic, with period \( \frac{\Delta}{\alpha} \):

\[
p_0(\alpha y) \quad p_1(\alpha y)
\]

- “Pulses” are due to total noise \( E + W \)

- Pulse = convolution of \( \mathbb{U} \left[ -\frac{(1-\alpha)\Delta}{2\alpha}, \frac{(1-\alpha)\Delta}{2\alpha} \right] \) with \( \mathcal{N}(0, \sigma_w^2) \)
Scalar QIM (Cont’d)

- Use test statistic \( \tilde{Y} := \alpha Y \mod \Delta \)

\[
WNR = D_1 / \sigma_w^2 = 100
\]
\[
\alpha = 0.99
\]

\[
WNR = 0.01
\]
\[
\alpha = 0.01
\]
Scalar QIM (Cont’d)

• Communication model using Modulo Additive Noise (MAN) channel:

\[
\begin{align*}
V & \quad \downarrow \\
+ \mod \Lambda & \\
\downarrow \\
\tilde{Y} & \quad D
\end{align*}
\]

where \(d_0 = -\frac{\Delta}{4} = -d_1\), and \(V = E + W \mod \Delta\)

• Equivalent hypothesis test:

\[
\begin{aligned}
H_0 & : \quad \tilde{Y} = d_0 + V \\
H_1 & : \quad \tilde{Y} = d_1 + V
\end{aligned}
\]
Scalar QIM (Cont’d)

- $P_e$ is just 2–3 times worse than $P_e$ for private SSM
Scalar QIM, \( N \) Samples

- Apply scalar QIM to each sample, using dither vectors \(-d\) under \( H_0 \) and \( d \) under \( H_1 \).
- W.l.o.g. use \( d_n = \frac{\Delta}{4} \) for \( 1 \leq n \leq N \)
- Detector chooses between two hypotheses
  \[
  \begin{cases}
  H_0 : \tilde{Y} = -d + V \\
  H_1 : \tilde{Y} = d + V
  \end{cases}
  \]
- Evaluate \( P_e \) via Monte-Carlo simulations or Bhattacharyya bounds
Example: $WNR = 1, \ N = 15$

Error Probabilities with varying $\alpha; D_1 = D_2$

- $P_{e,\text{actual}}$
- $P_{e,\text{bhat}}$
- $P_{e,\text{Gauss}}$

Graph showing the relationship between $\alpha$ and error probabilities.
Multiple Codewords: $|\mathcal{M}| > 2$

- Computation of $P_e = \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} Pr[Y \notin \mathcal{Y}_m | m]$ is difficult
- For linear codes, we have $P_e = Pr[Y \notin \mathcal{Y}_0 | m = 0]$
- Union bound:
  \[
P_e \leq (|\mathcal{M}| - 1) \max_{i \neq 0 \in \mathcal{M}} P_e|i,0
  \]
  which is tight at low rates.