SESSION 3: PERFORMANCE ANALYSIS: $P_e$

- Probability of Error Analysis for SSM and QIM
- Binary Detection, One sample
- Binary Detection, $N$ samples
- Multiple Codewords
Probability of Error

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

- Conditional error probability: $P_{e|m} = Pr[Y \notin \mathcal{Y}_m \mid m]$
Binary Detection: $\mathcal{M} = \{0, 1\}$

- Binary hypothesis testing:

\[
\begin{cases}
H_0 : Y \sim p_0 \\
H_1 : Y \sim p_1
\end{cases}
\]

- Decision rule: $t(y) \begin{cases} \geq & H_1 \\ < & H_0 \end{cases} T$
- Two types of error: $P_{FA}$ and $P_M$
- $P_e = \frac{1}{2}(P_{FA} + P_M) = \frac{1}{2} \int \min(p_0(y), p_1(y)) \, dy$
SSM, One Sample

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

- **Attack:** \( y = x + w \)

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

- **WNRR:** \( WNRR = \frac{a^2}{\sigma_w^2} \)
SSM (Cont’d)

• Rival pdf’s for $y$:

\[ p_0 = \mathcal{N}(a, \sigma_{\text{noise}}^2), \quad p_1 = \mathcal{N}(-a, \sigma_{\text{noise}}^2) \]

where $\sigma_{\text{noise}}^2 = \begin{cases} 
\sigma_w^2 : \text{private WM} \\
\sigma_s^2 + \sigma_w^2 : \text{blind WM} 
\end{cases}$

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

• 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 $E \sim \mathbb{U}\left[-\frac{(1-\alpha)\Delta}{2\alpha}, \frac{(1-\alpha)\Delta}{2\alpha}\right]$
Scalar QIM (Cont’d)

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

  \[ p_0(\alpha y) \]
  \[ -\frac{5\Delta}{4}, -\frac{\Delta}{4}, \frac{3\Delta}{4} \]

  \[ p_1(\alpha y) \]
  \[ -\frac{3\Delta}{4}, \frac{\Delta}{4}, \frac{5\Delta}{4} \]

- 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 $\tilde{Y} := \alpha Y \mod \Delta$
Scalar QIM (Cont’d)

- Communication model using **Modulo Additive Noise (MAN)** channel:

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

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

- Equivalent hypothesis test:

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

- ML Detector: $\frac{p_1(\tilde{y})}{p_0(\tilde{y})} = \frac{p_V(\tilde{y} - d_1)}{p_V(\tilde{y} - d_0)} > 1$

- $H_1$

- $H_0$

- Probability of error: $\tilde{P}_e = \frac{1}{2} \int \min(p_0(\tilde{y}), p_1(\tilde{y})) \, d\tilde{y}$

- The rival pdf’s $p_0(\tilde{y})$ and $p_1(\tilde{y})$ have means $d_0$ and $d_1$, resp., and common variance

$$\sigma^2_v = (1 - \alpha)^2 \frac{\Delta^2}{12} + \alpha^2 \sigma^2_w$$
Scalar QIM (Cont’d)

- The “generalized SNR” for detection

\[ GSNR := \frac{(d_1 - d_0)^2}{\sigma_v^2} = \frac{\frac{1}{4} \Delta^2}{(1 - \alpha)^2 \frac{\Delta^2}{12} + \alpha^2 \sigma_w^2} \]

is maximized by

\[ \alpha \approx \frac{WNR}{WNR + 1} \]

where \( WNR = \frac{\Delta^2/12}{\sigma_w^2} \)

- Note \( GSNR \) is not necessarily an accurate predictor of detection performance
Scalar QIM (Cont’d)
Scalar QIM (Cont’d)

- $P_e$ is 2–3 times worse than $P_e$ for private SSM
SSM, $N$ Samples

- Embedding & Detection:
  $$x^N = \begin{cases} 
s^N + a^N & : m = 0 \\
  s^N - a^N & : m = 1
  \end{cases}$$

- Attack: $y^N = x^N + w^N$

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

- $WNR = \frac{||a^N||^2}{\sigma_w^2}$

- $P_e = Q(d/2)$ where $d = 2\sqrt{WNR}$ for private WM
Scalar QIM, $N$ Samples

- Apply scalar QIM to each sample, using either vectors $d_0^N$ under $H_0$ and $d_1^N$ under $H_1$.
- W.l.o.g. use $d_{0,n} = -\frac{\Delta}{4}$ and $d_{1,n} = \frac{\Delta}{4}$ for $1 \leq n \leq N$.
- Detector’s problem: choose between two hypotheses

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

\[ H_1 \]

- ML Detector: \( \prod_{n=1}^{N} \frac{p_{V}(\tilde{y}_n - d_{1,n})}{p_{V}(\tilde{y}_n - d_{0,n})} \geq 1 \)

\[ H_0 \]

- Probability of error: \( \tilde{P}_e = \frac{1}{2} \int \min(p_0(\tilde{y}^N), p_1(\tilde{y}^N)) \, d\tilde{y}^N \)

- Hard to evaluate! (integration over \([0, \Delta]^N\))
Gaussian Approximation

- If noise $V^N$ was Gaussian, probability of error would be given by $\tilde{P}_e = Q(\frac{1}{2}\sqrt{GSNR})$ where

$$GSNR = \frac{N\Delta^2/4}{(1 - \alpha)^2 \frac{\Delta^2}{12} + \alpha^2 \sigma_w^2}$$

- However, $V^N$ is non-Gaussian, and this is generally a poor approximation to $\tilde{P}_e$. 
Large Deviations

• Large $N \Rightarrow$ large $GSNR \Rightarrow$ rare events dominate $\tilde{P}_e$

• For all $N$ we have the large-deviations bound

$$\tilde{P}_e \leq \frac{1}{2} e^{-NB(p_0, p_1)}$$

where

$$B(p_0, p_1) = -\ln \int_{-\Delta/2}^{\Delta/2} \sqrt{p_0(\tilde{y})p_1(\tilde{y})} \, d\tilde{y}$$

is the Bhattacharyya coefficient.

• Moreover, $\lim_{N \to \infty} \left[ -\frac{1}{N} \ln \tilde{P}_e \right] = B(p_0, p_1)$

• Conclusion: $B(p_0, p_1)$ is an accurate performance predictor

• Approach is easily generalizable to lattice QIM
Comparison of Probabilities; $D_1 = D_2$; $n=15$

Graph showing the comparison of probabilities $P_{e,\text{actual}}$, $P_{e,\text{Bhat}}$, and $P_{e,\text{CLT}}$ as a function of $\alpha$.
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.

- Let \(d_H\) be minimum Hamming weight of code \(\mathcal{C}\)
- Using the Bhattacharyya bound, we obtain

\[
P_e \leq (|\mathcal{M}| - 1)e^{-d_H B(p_0, p_1)}
\]