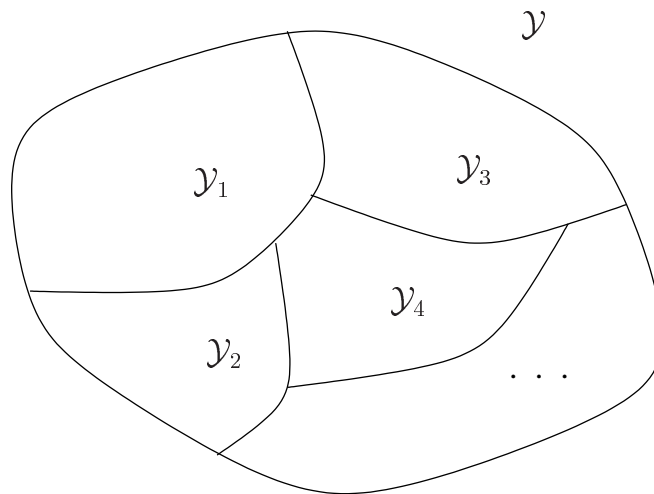


SESSION 4: PERFORMANCE ANALYSIS: P_e

- 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 decoder outputs m 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:

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

- Attack: $\mathbf{y} = \mathbf{x} + \mathbf{w}$

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

- Sufficient Statistic: $t = \begin{cases} \langle \mathbf{y}, \mathbf{a} \rangle & : \text{blind WM} \\ \langle \mathbf{y} - \mathbf{s}, \mathbf{a} \rangle & : \text{nonblind WM} \end{cases}$

SSM (Cont'd)

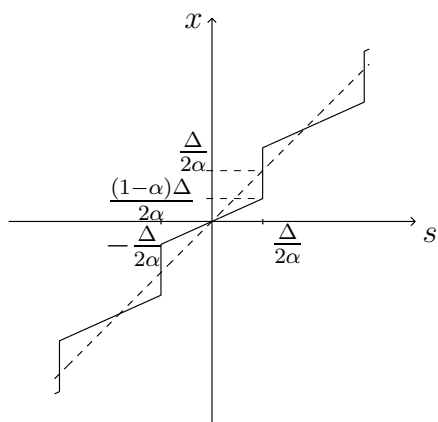
- Noise variance at decoder:

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

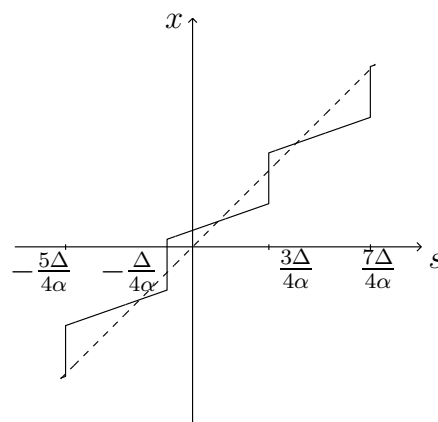
- $P_e = Q(d/2)$ where $d = \frac{2\|\mathbf{a}\|}{\sigma_{noise}}$
- Performance is typically **much worse** for blind WM.

Scalar QIM, One Sample

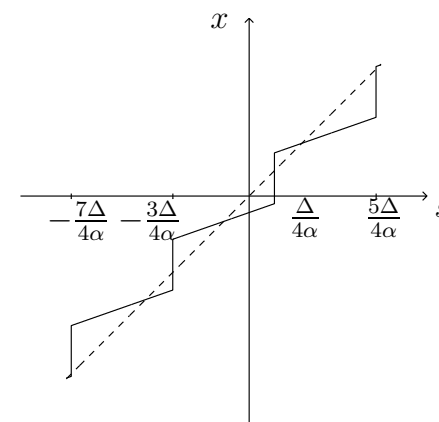
- Blind watermarking, 1-bit embedding:



Prototype $X_{sym}(s)$



$m = 0$

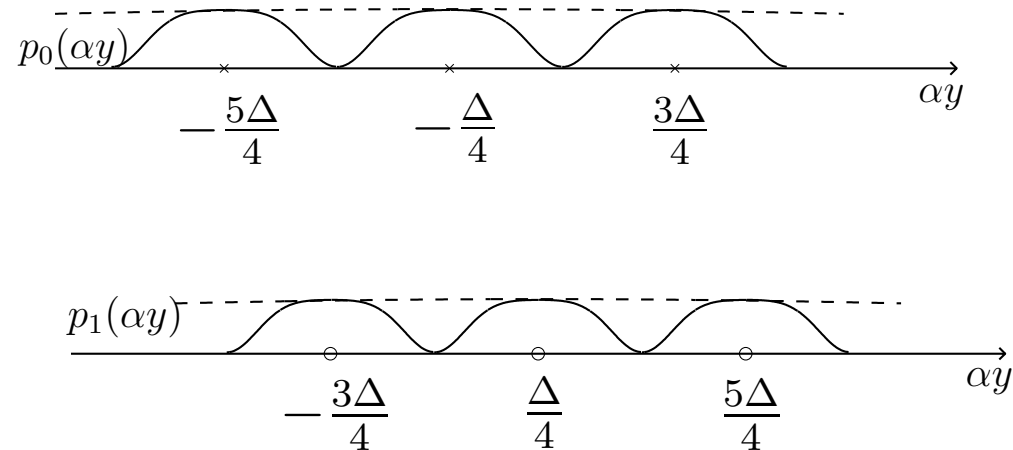


$m = 1$

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

Scalar QIM (Cont'd)

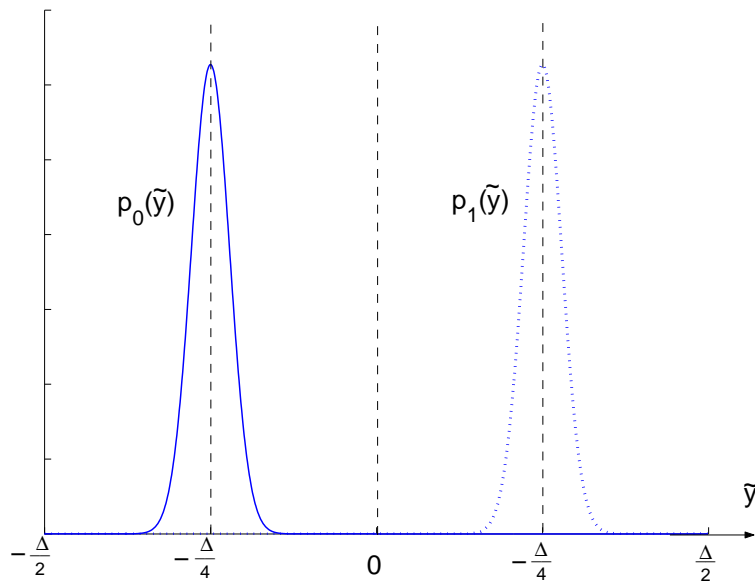
- Rival pdf's are quasi-periodic, with period $\frac{\Delta}{\alpha}$:



- “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 $\mathcal{N}(0, \sigma_w^2)$

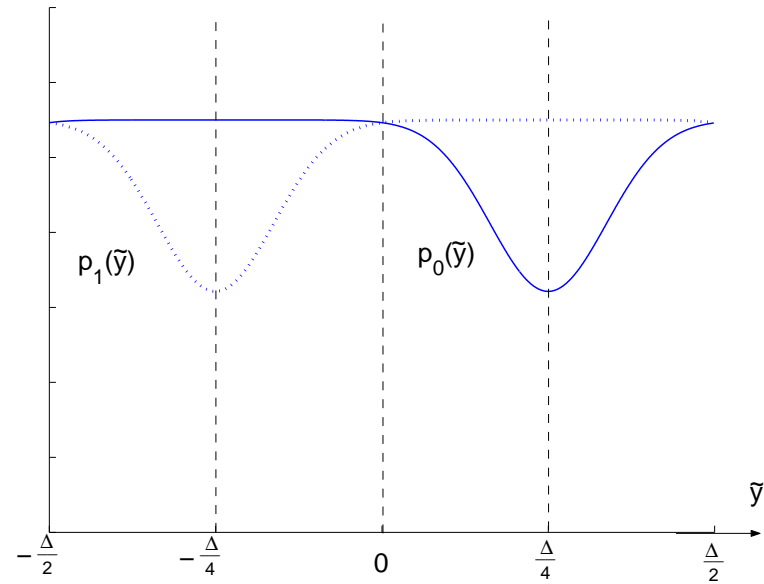
Scalar QIM (Cont'd)

- Use test statistic $\tilde{Y} := \alpha Y \bmod \Delta$



$$WNR = D_1/\sigma_w^2 = 100$$

$$\alpha = 0.99$$

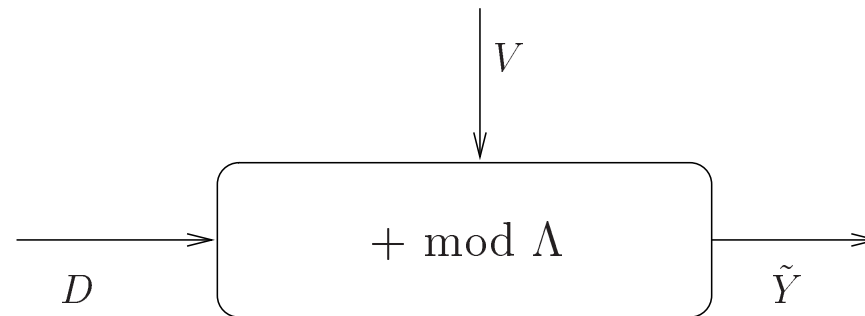


$$WNR = 0.01$$

$$\alpha = 0.01$$

Scalar QIM (Cont'd)

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

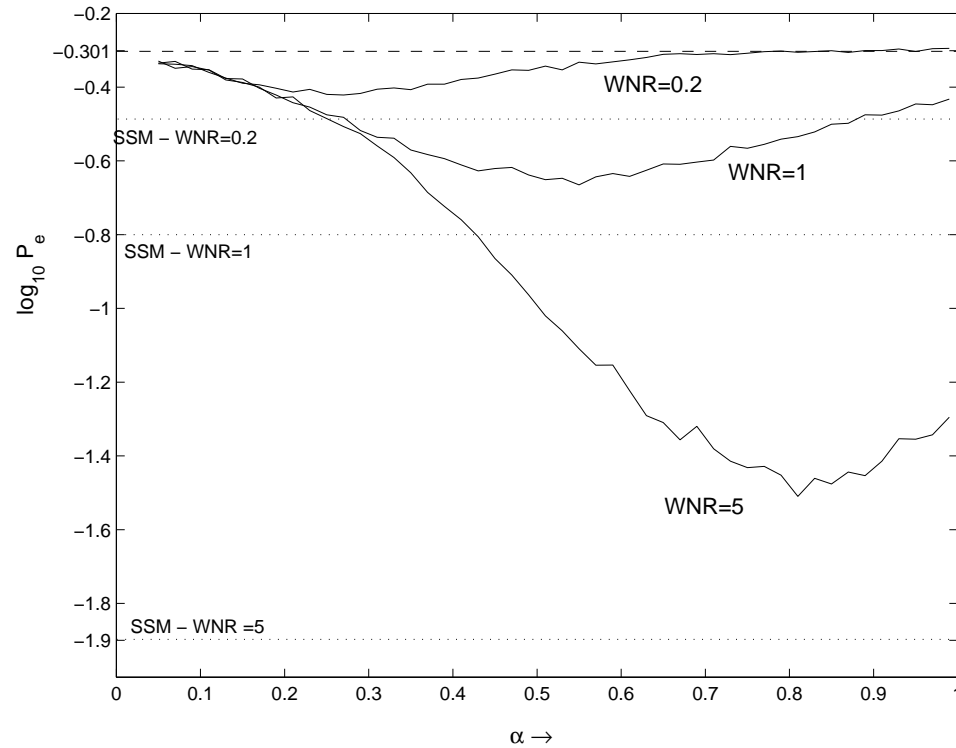


where $d_0 = -\frac{\Delta}{4} = -d_1$, and $V = E + W \bmod \Delta$

- Equivalent hypothesis test:

$$\begin{cases} H_0 : \tilde{Y} = d_0 + V \\ H_1 : \tilde{Y} = d_1 + V \end{cases}$$

Scalar QIM (Cont'd)



- P_e is just 2–3 times worse than P_e for private SSM

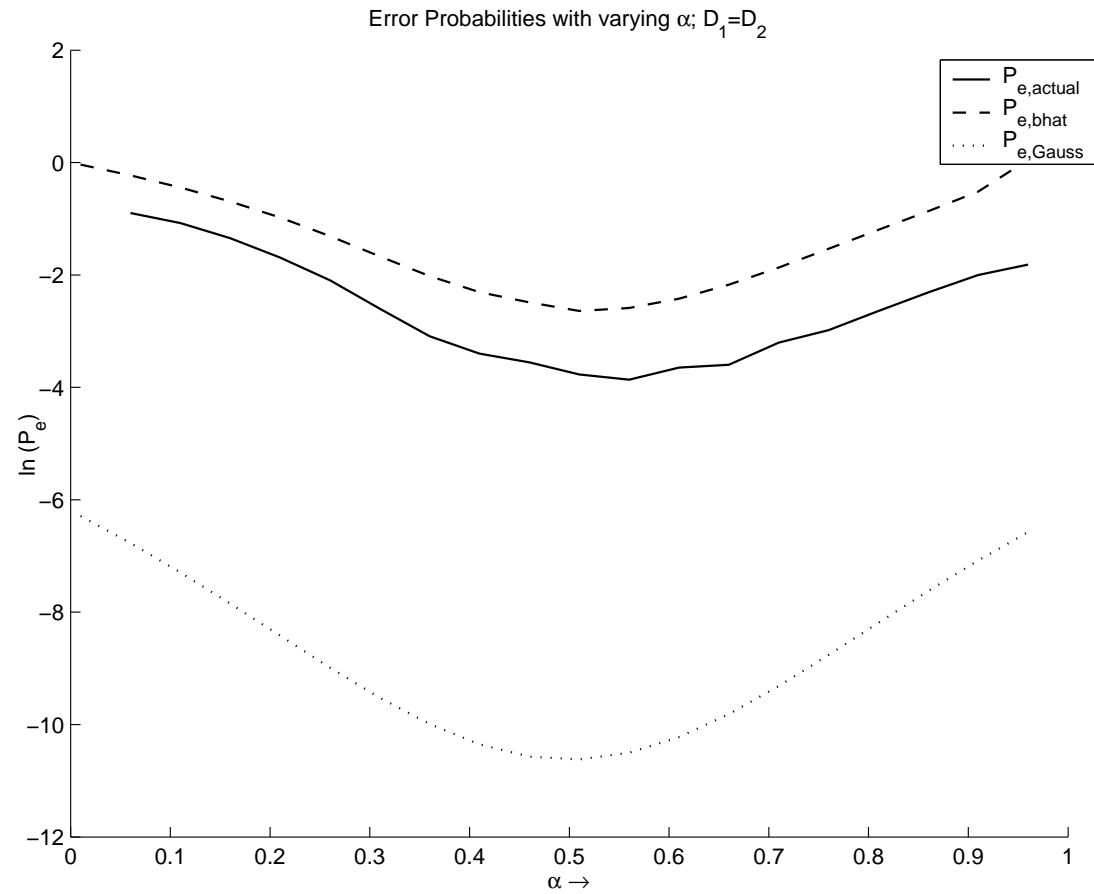
Scalar QIM, N Samples

- Apply scalar QIM to each sample, using dither vectors $-\mathbf{d}$ under H_0 and \mathbf{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

$$\begin{cases} H_0 : \tilde{\mathbf{Y}} = -\mathbf{d} + \mathbf{V} \\ H_1 : \tilde{\mathbf{Y}} = \mathbf{d} + \mathbf{V} \end{cases}$$

- Evaluate P_e via Monte-Carlo simulations or Bhattacharyya bounds

Example: $WNR = 1, N = 15$



Multiple Codewords: $|\mathcal{M}| > 2$

- Computation of $P_e = \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} Pr[\mathbf{Y} \notin \mathcal{Y}_m | m]$ is difficult
- For linear codes, we have $P_e = Pr[\mathbf{Y} \notin \mathcal{Y}_0 | m = 0]$
- 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.