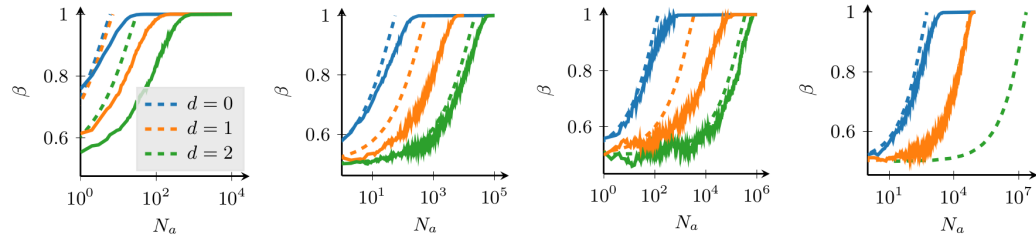


Bitslice masking: $|\mathcal{Y}| = 2$, Leakage model: $\mathbf{L}_i = \text{hw}(\mathbf{Y}_i) + \text{Noise}(0, \sigma^2)$



(a) $\sigma^2 = 1$.

(b) $\sigma^2 = 10$.

(c) $\sigma^2 = 25$.

(d) $\sigma^2 = 100$.

Figure: Success rate of concrete bit recoveries and MI-based upper bounds.