Information Security A.Y. 2024/2025

Lab 2: Implementation of random binning encoding and secrecy rate evaluation

Abdalaziz Zainelabedeen Abdalaziz Abdo (2141828)
Enkeleda Bardhi (2070874) Laura M. Schulze (2122311)
Aitegin Zhamgyrchieva (2144165)

April 27, 2025

In the following report we provide a brief description of how Tasks 1-8 were implemented, ...

2.1 Brief Description of Implementations

Task 1:Uniform Error Channel

We generated 7-bit words and defined legitimate and eavesdropper channels based on Hamming distances (1 and 3 respectively). Sampling was done uniformly to verify conditional independence.

Task 2: The random Binning Encoder

Using a (7,4) Hamming code, we constructed bins of two codewords for each 3-bit message. Codewords were chosen uniformly at random.

Task 3: The random binning decoder

We implemented a legitimate decoder. It selects the nearest codeword (in Hamming distance) and extracts the message bits according to the first bit (directly or complemented)

Task 4: Perfect Secrecy

We evaluated the secrecy by measuring $I(U;Z)$ based on the encoder from Task 2. The observed mutual information was significantly higher than zero, indicating that perfect secrecy was not achieved with the current design. Additionally, we tested a case where the encoder picked codewords independently of u, and mutual information became close to zero, demonstrating perfect secrecy is theoretically achievable.

Task 5: Transmission over a binary symmetric channel

We implemented the wiretap binary symmetric channel (BSC) with independent error probabilities ϵ and δ for Bob and Eve, respectively.

Task 6: Evaluation on the system security over the wiretap BSC

We simulated the full system over the BSC for various (ϵ, δ) pairs. We measured Bob's decoding error rate and Eve's mutual information leakage $I(U;Z)$. We evaluated system reliability and secrecy using these metrics.

Task 7: Transmission over a wiretap AWGN channel

We implemented a simple PAM (Pulse Amplitude Modulation) scheme, where '0' was mapped to -1 and '1' to +1. Transmission over AWGN was simulated by adding Gaussian noise with different SNR values for Bob and Eve.

Task 8: Evaluation on the system security over the wiretap AWGN channel

We evaluated system performance over various Eve SNRs by measuring Bob's decoding error rates and Eve's mutual information. We plotted the resulting secrecy metrics against Eve's SNR values.

2.2 Considerations and Remarks

1. We obtain 3 secret message bits per channel use (transmitted word) since each codeword encodes 3 bits. Therefore, the number of secret bits per transmitted bit is $3/7 \approx 0.43$.

2. It is not possible to obtain 4 secret bits per channel use with the (7,4) Hamming code because its information dimension is 3. To achieve 4 bits, we would need a different code structure with a higher dimension.

3. It is possible to obtain 2 secret bits per channel use by adjusting the binning or using a different coding strategy, but this would reduce the efficiency compared to our current scheme.

4. The evaluation of secrecy through decoding errors is simpler, but less precise. Even if Eve's decoding error rate is high, she may still extract partial information. Therefore, we compute mutual information $I(U;Z)$ to accurately measure information leakage.

2.3 Evaluation of Proper Security Metrics

Task 1: Conditional PMF $p_{Z|X}(\cdot|1001000)$

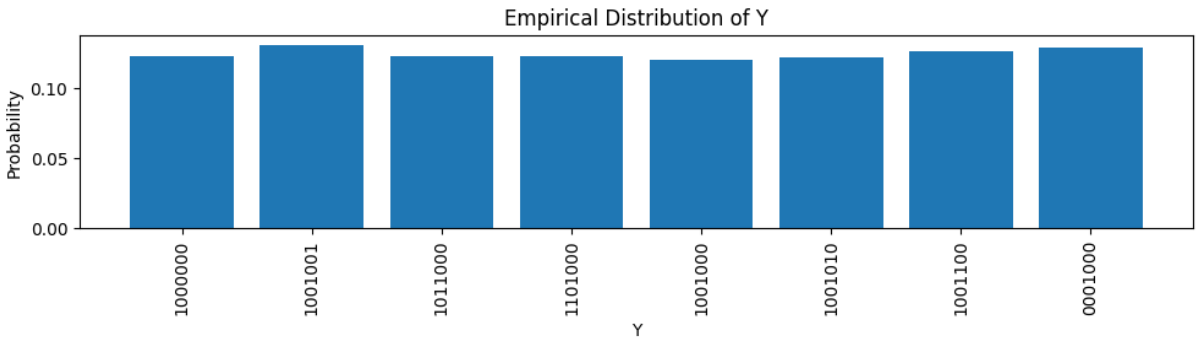

Figure 1: Empirical Distribution of Y for $X = 1001000$

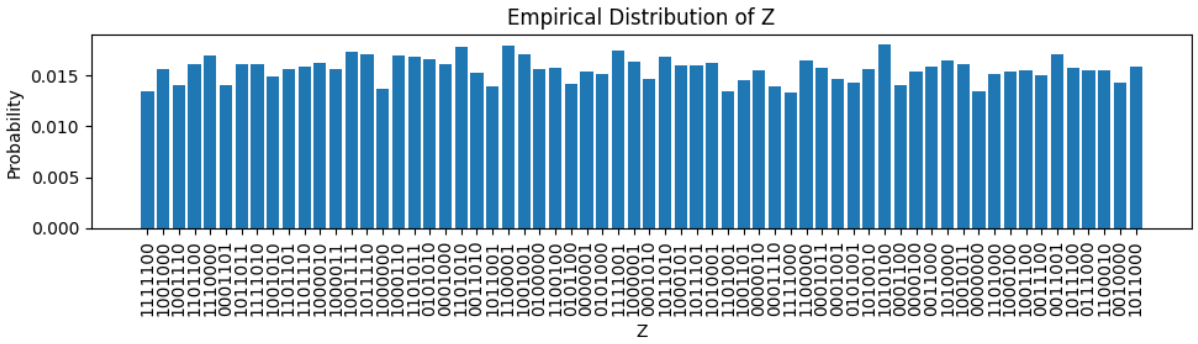

Figure 2: Empirical Distribution of Z for $X = 1001000$

The distribution of Y is concentrated around a few neighbors of $X = 1001000$ because only one bit error is allowed. In contrast, Z is much more uniform due to up to three bit errors. This explains the small mutual information $I(Y; Z|X)$ observed.

Task 2: Conditional PMFs $p_{Z|U}(\cdot|u)$ for all values of u

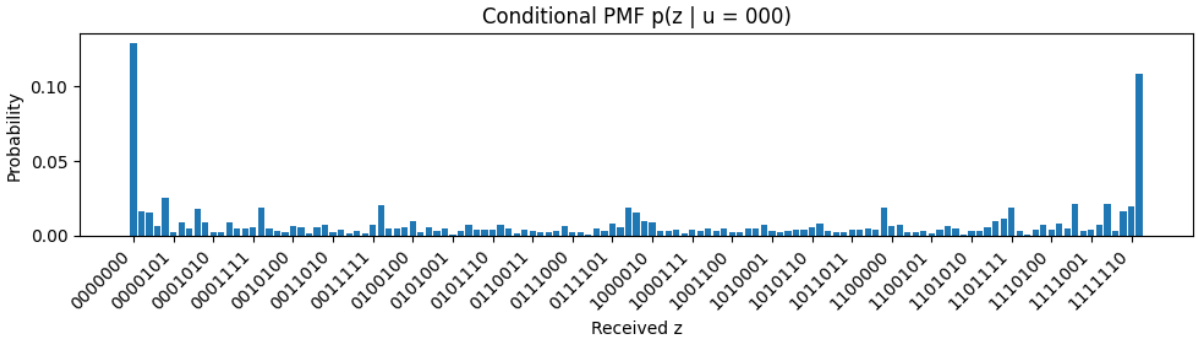

Figure 3: Conditional PMF $p(z|u = 000)$

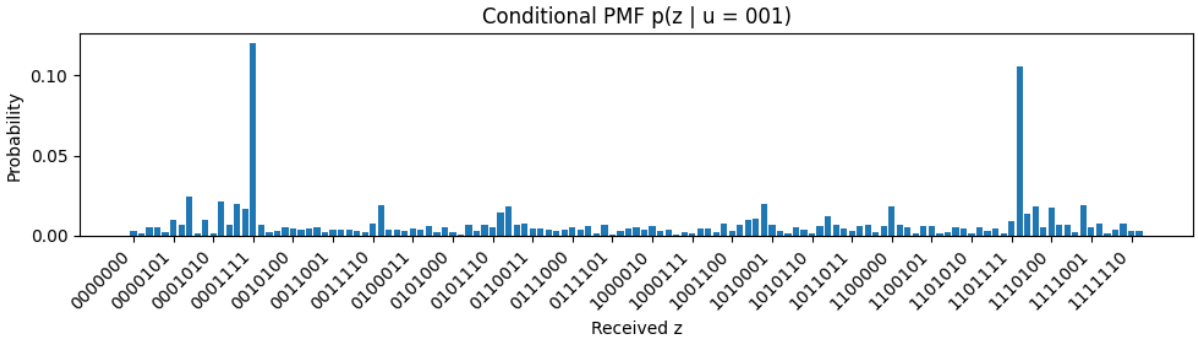

Figure 4: Conditional PMF $p(z|u = 001)$

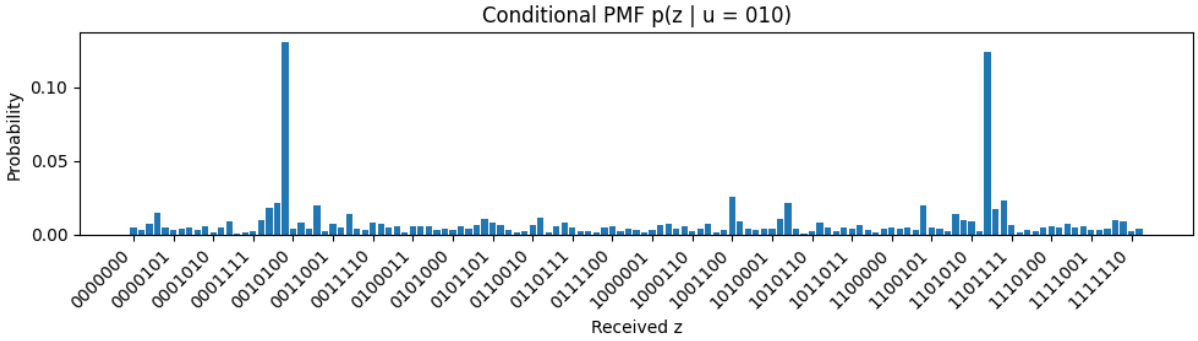

Figure 5: Conditional PMF $p(z|u = 010)$

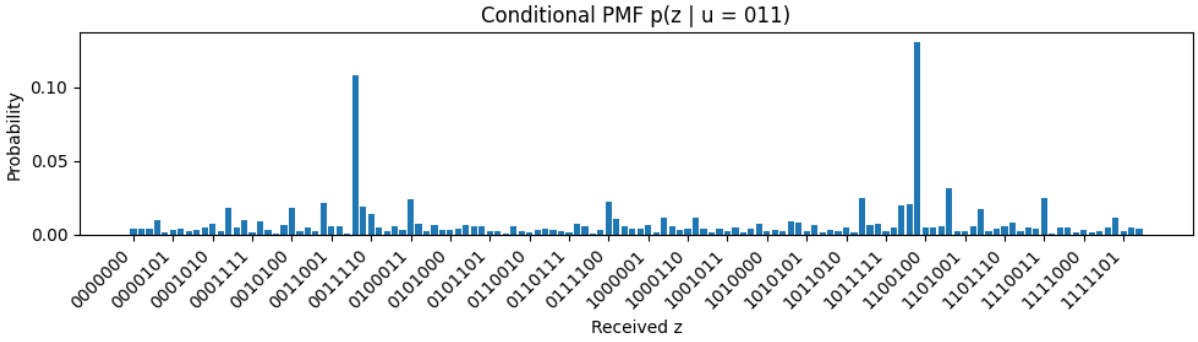

Figure 6: Conditional PMF $p(z|u = 011)$

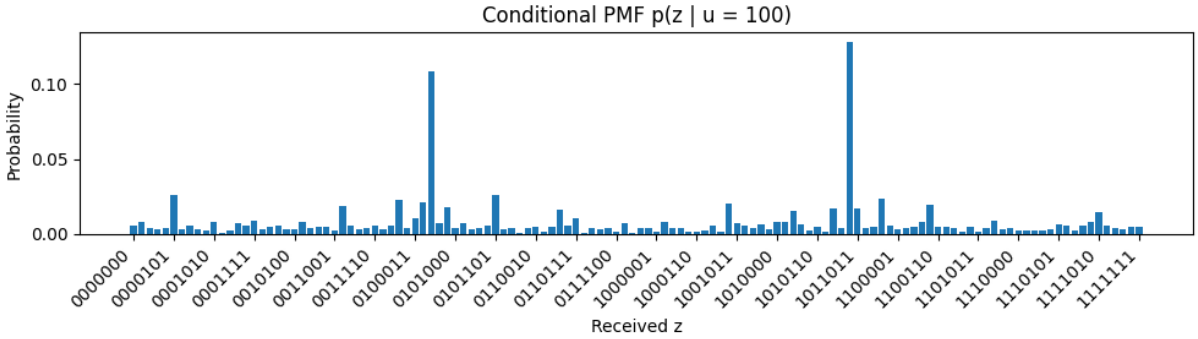

Figure 7: Conditional PMF $p(z|u = 100)$

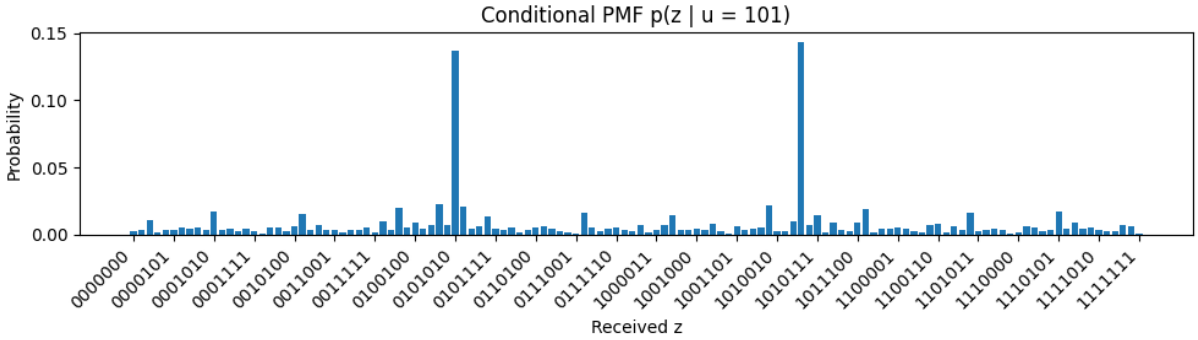

Figure 8: Conditional PMF $p(z|u = 101)$

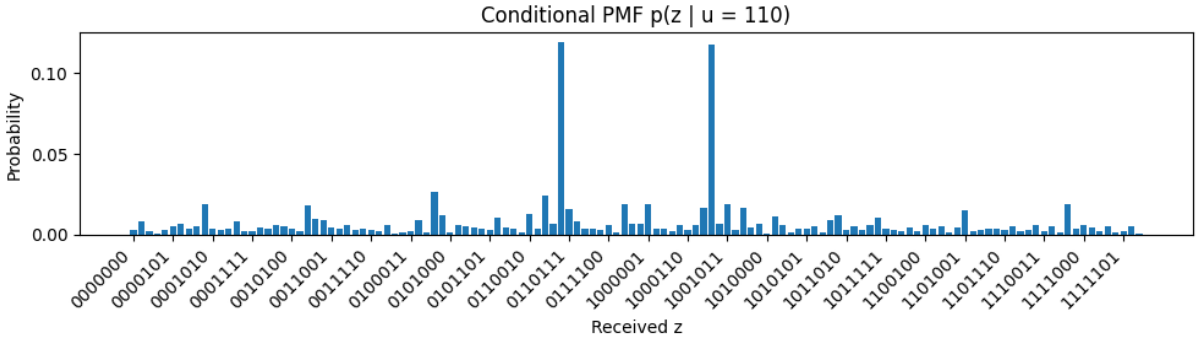

Figure 9: Conditional PMF $p(z|u = 110)$

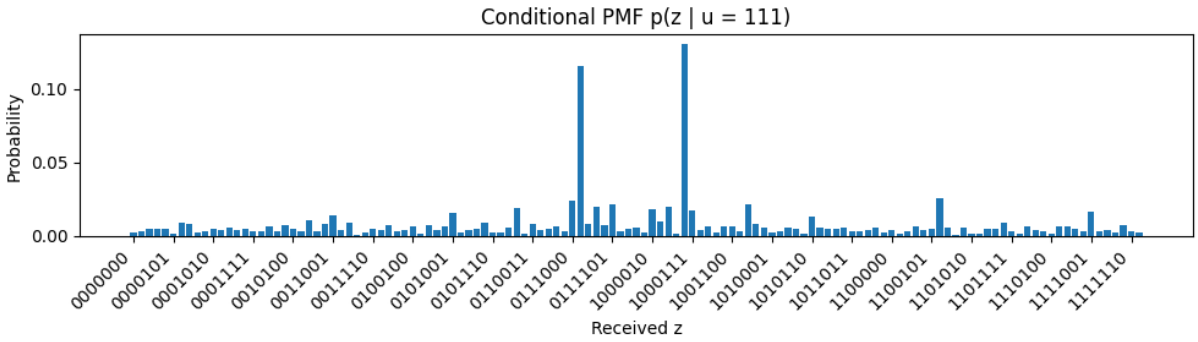

Figure 10: Conditional PMF $p(z|u = 111)$

Each $p(z|u)$ is concentrated around few outputs, reflecting the encoder structure and limited noise.

Observation: When u and z are independent, the distribution $p(z|u)$ becomes approximately uniform across all outputs.

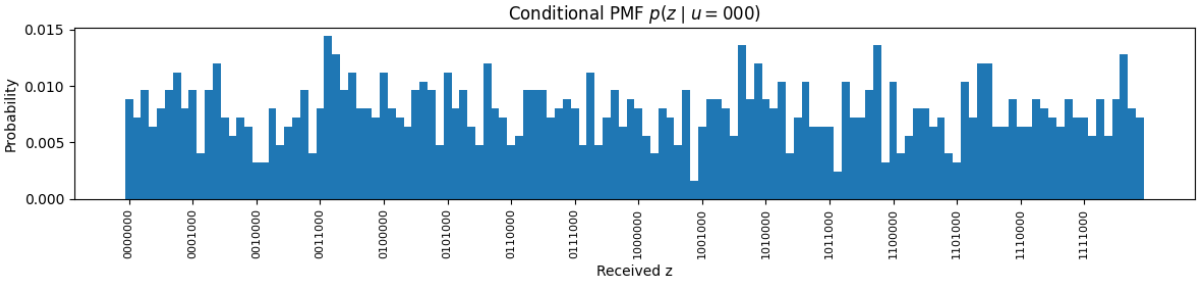

Figure 11: Empirical conditional PMF $p(z|u = 000)$ under independent encoding

Task 3: Estimates of $H(U)$ and $I(U;Z)$ from Task 4

When using the random binning encoder from Task 2:

$$H(U) \approx 3.00 \text{ bits} \quad I(U;Z) \approx 0.84 \text{ bits}$$

When using an encoder independent of u: $I(U;Z) \approx 0.06$ bits