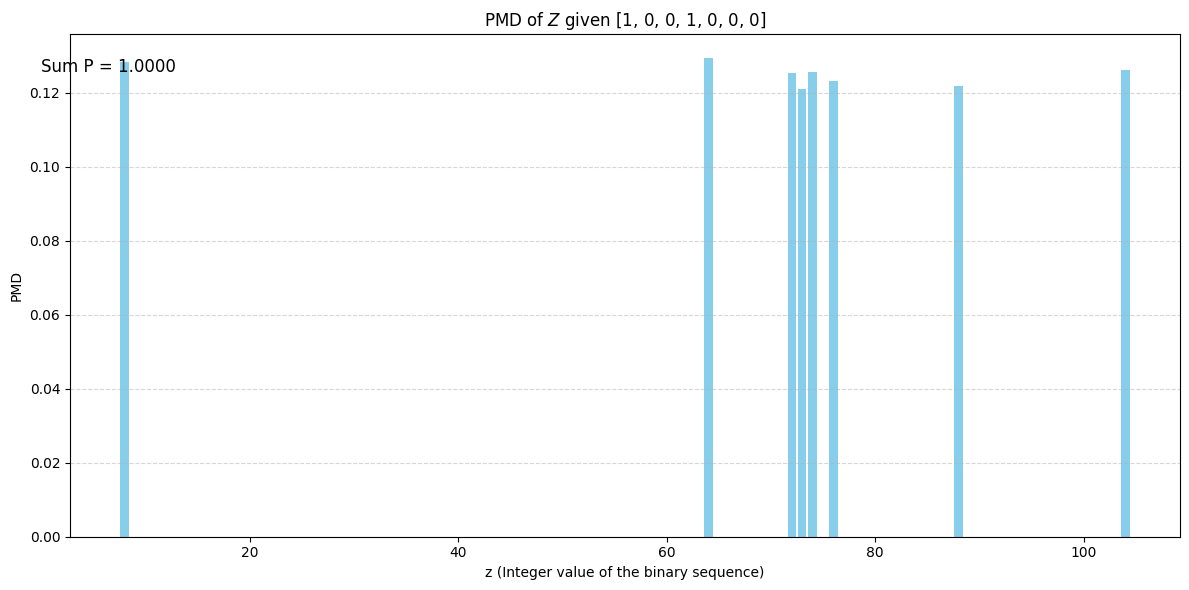
Report sudormrf

Students: Sassone Rodolfo, Vettorello Massimo

1. Brief description of Tasks 1-7:

* Task 1: We implemented the wiretap and checked the uniformity of the output given



* Task 2: We implemented a simulation of the *forward information reconciliation* process using a (7,4) Hamming code for error correction. We defined the parity-check matrix **H** and used it to detect and correct single-bit errors in transmitted messages. The core components included the *error\_correction* function, which identifies the error pattern based on the syndrome and corrects the received vector, and the *information\_reconciliation* function, which uses the syndrome and a correction vector **c** to recover the original message. Finally, we simulated the communication over a noisy channel using *simulate\_forward\_information\_reconciliation*, where a sender transmits a 7-bit message and both a legitimate receiver and an eavesdropper attempt to reconstruct it. The success rates of both parties were measured to assess the exact learning of the original message by Eve and Bob.



* Task 3: In Task 3, we implemented a simulation of the *reverse information reconciliation* process, again utilizing the (7,4) Hamming code. Unlike Task 2, here the receiver computes the syndrome c from the received message y and sends it back to the sender. The sender and a potential eavesdropper then use this syndrome to correct their own versions of the message. We introduced the simulate\_reverse\_information\_reconciliation function to measure how well the sender (Alice) and the eavesdropper (Eve) can reconstruct the receiver’s message. The information\_reconciliation function was reused to perform error correction based on the received syndrome. The success rates of both Alice and Eve were recorded over multiple runs to evaluate the reliability and potential information leakage of the reverse reconciliation protocol.

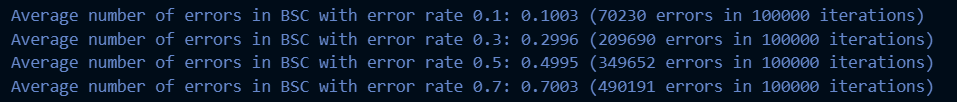


* Task 4: The implementation of the deterministic privacy amplification is straight forward. About the uniform and the independence:

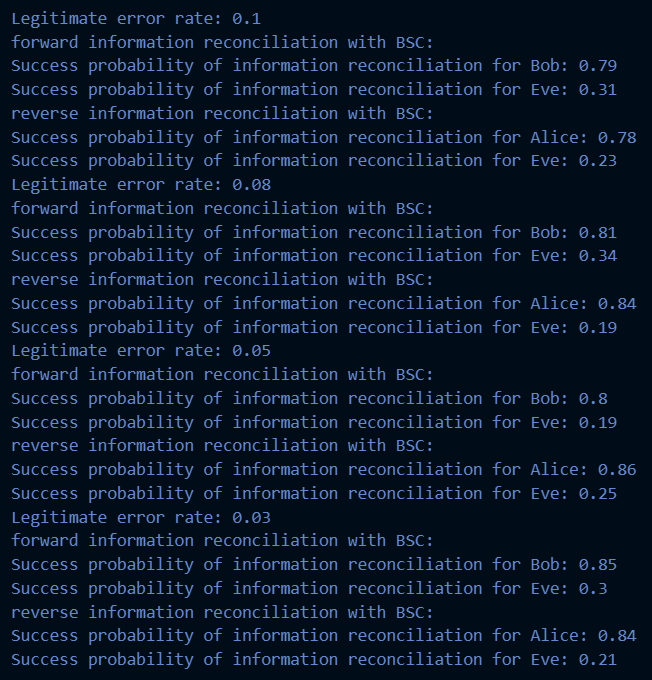
Immagine che contiene testo, Carattere, schermata, nero

Il contenuto generato dall'IA potrebbe non essere corretto.

* Task 5: To assess the effectiveness of the probabilistic privacy amplification method, we defined *eval\_prob\_privacy\_amplification*, which simulates the wiretap scenario multiple times and estimates the joint distribution of the final key, the syndrome **c**, and the eavesdropper's observation **z**. We then calculated the *mutual information* between the key and the pair (**c**, **z**) using the *mutual\_information* function. A low mutual information value indicates that the key is nearly independent of what Eve observes, thus confirming the strength of the privacy amplification step.
  + In this case, the lowest (empirical) mutual information is obtained by .
* Task 6: In Task 6, we implemented the *wiretap binary symmetric channel (BSC)* model, allowing configurable error rates for both the legitimate receiver (ε) and the eavesdropper (δ). The *binary\_symmetric\_channel* function simulates the bit-flipping behavior of a BSC, and wiretap\_bsc applies it independently to both the receiver and eavesdropper paths.
  + To verify correctness, we transmitted a known all-zero 7-bit message over the BSC for many iterations and counted the bit flips to estimate the empirical error rate. This confirmed that the channel introduces noise as expected for different values of ε.



* + Next, we integrated the wiretap BSC with the complete *information-theoretic key agreement protocol*, using either forward or reverse information reconciliation. The function *key\_agreement* coordinates this process by simulating message transmission, performing reconciliation using the chosen syndrome direction, and applying privacy amplification with a random binary matrix.
  + Finally, we ran simulations across various legitimate error rates to observe how often Bob or Alice (depending on the direction) successfully reconstructs the message compared to Eve. Results showed that perfect reliability and secrecy are not guaranteed—multiple bit errors can occur in a single message, and Eve's error distribution is not uniform.



* Task 7: In Task 7, we numerically evaluated the performance of the complete key agreement protocol over a wiretap BSC by simulating multiple runs across different values of the parameters: legitimate error rate (ε), eavesdropper error rate (δ), and key length after privacy amplification (ℓ).
  + The results were visualized in heatmaps to analyze the impact of each parameter on security and reliability, highlighting the trade-offs between noise tolerance and key strength.

Immagine che contiene schermata, Policromia, quadrato, Rettangolo

Il contenuto generato dall'IA potrebbe non essere corretto.

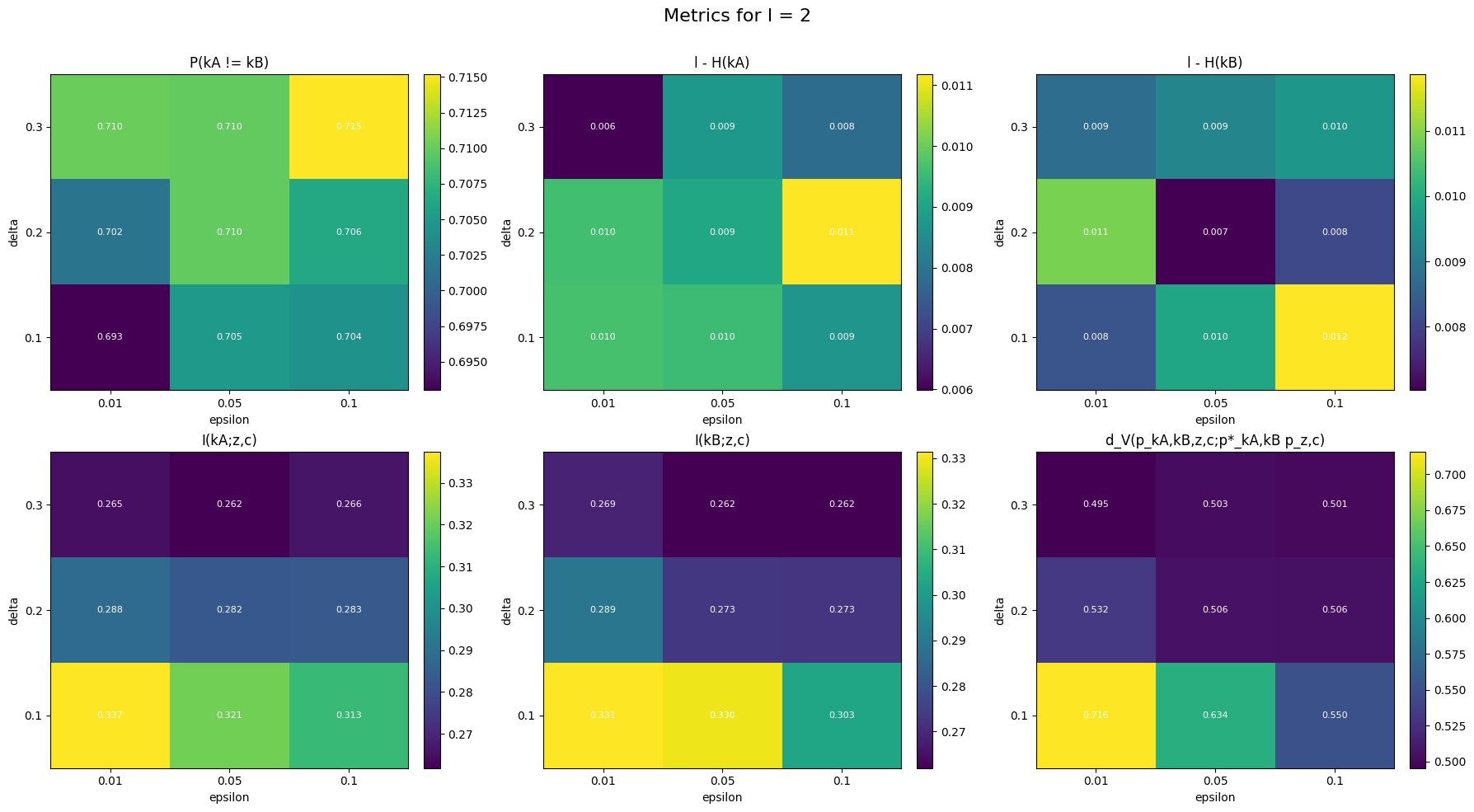


Immagine che contiene schermata, Policromia, quadrato, Rettangolo

Il contenuto generato dall'IA potrebbe non essere corretto.

Comparison Between the Obtained Secret Key Rate and the Secret Key Capacity

From the experimental results, the best estimated secret key rate is obtained for , particularly with **ε = 0.05** and **δ = 0.1**, where the information leakage is approximately 0.115 and the entropy of the key is close to 1. In this case, the SKR can be estimated as:

This value is relatively close to the theoretical **secret key capacity**, which is bounded by:

assuming and are the observations of the legitimate parties and is the adversary’s observation. Without a precise model of the source and channels, we consider this estimated SKR as approaching capacity in the best case.

However, for  and , the secret key rate significantly drops due to:

* Higher disagreement rates
* Increased information leakage ,
* Greater variational distances between the real and ideal distributions.

Thus, **the system performs better with small ℓ, low δ, and low ε**, and only under these conditions does the secret key rate come close to the system’s secret key capacity.