Aufgabenblatt 02
Einführung in die Kryptographie PS

Andreas Schlager

March 12, 2025

1 Aufgabe 6

Erklären sie, warum bei Hamming ECC (Error Correction Code) die Parity Bits zwischen den Datenbits eingefügt werden und nicht einfach alle geschlossen den Datenbits vorangestellt oder angehängt werden. Illustrieren sie das anhand eines Beispiels unter Verwendung eines (15,11)-Hamming Codes.

In einer Hamming-codierten Nachricht befinden sich die Paritätsbits nicht am Anfang oder Ende der Nachricht, sondern an speziellen Positionen, die Zweierpotenzen entsprechen (z.B. $1, 2, 4, 8, \ldots$). Diese Positionen haben in der Binärdarstellung die Form einer einzelnen Eins, umgeben von Nullen:

Position	**Binärdarstellung**
1	000001
2	000010
4	000100
8	001000
16	010000
32	100000

Diese Eigenschaft ermöglicht eine effiziente Fehlererkennung und -korrektur durch eine XOR-Verknüpfung. Da die Einsen an unterschiedlichen Positionen sind, beeinflussen sie sich später in der Berechnung nicht gegenseitig. Wird eine entsprechende Wahl der Paritätsbits getroffen (odd oder even), dann ergibt die XOR-Verknüpfung aller Positionen, an denen eine Eins steht, stets null wenn kein Fehler aufgetreten ist. Ansonsten ist das Ergebnis die Position des Bits, welches fehlerhaft übertragen wurde. Falls mehrere Bits gekippt sind, entsteht zumindest ein unerwartetes Ergebnis. Dadurch ist zwar erkennbar, dass ein Fehler vorliegt, er kann jedoch nicht behoben werden.

1.1 Beispiel Hamming(15,11)

Angenommen man möchte das Datenwort 10110111011_2 übertragen und durch einen Hamming ECC absichern, dann würde die ganze Nachricht mit den Paritätsbits wie folgt aussehen:

Position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Nachricht	P_1	P_2	1	P_3	0	1	1	P_4	0	1	1	1	0	1	1