Errata List 2nd Edition (April 2025)

Chapter	Page	Section	Figure	Comment
2	56	2.4	56	In the text of "Core function of Salsa20", y_i should state u_i
3	80	3.3	3.6	Bit 50 should be mapped to position 2 and bit 58 to position 1, not vice versa
2	61	2.4		In the second round of the QR function, the arguments should be u_i instead of v_i
13	477	13.3.4		"The result of this XOR operation is finally multiplied with the output of the encryption of the first counter value CTR0." Should state: "The result of this XOR operation is multiplied with the subkey and finally XORed with the output of the encryption of the first counter value CTR0."
12	397	12.2		c_aux is (56,35,33) instead of (2,25,6)