Anhang C) Messprotokolle und Binärcode-Tabelle

Messprotokoll zur Schlüsselerzeugung – ALICE

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Ba																		
Bi																		

	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Ba																		
Bi																		

	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
Ba																
Bi																

Ba = Basis (+ oder x) Bi = Bit (0 oder 1)

Winkeleinstellung (Erinnerung)	Basis +	Basis x
Bit 0	0°	-45°
Bit 1	90°	45°

Erzeugter Schlüssel:

— —

Tabelle zur Verschlüsselung der Nachricht – ALICE

Bu																				
D																				
S																				
V																				

Bu = Buchstabe, D = Datenbit (Buchstabe in binärer Darstellung, 4 x 5 Bit)
S = Schlüsselbit, V = Verschlüsseltes Bit zum Senden

Messprotokoll zur Schlüsselerzeugung – BOB

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Ba																		
Bi																		
Bi(E)																		

	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Ba																		
Bi																		
Bi(E)																		

	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
Ba																
Bi																
Bi(E)																

Ba = Basis (+ oder x) Bi = Bit (0 oder 1)
Bi(E): Bits mit eingebauter Eve

Erinnerung	transmittiert	reflektiert
Basis + (=0°)	0	1
Basis x (=45°)	0	1

Erzeugter Schlüssel:

— — — — — — — — — — — — — — — — — — — —

Tabelle zur Entschlüsselung der Nachricht – BOB

E																				
S																				
D																				
Bu																				

E = Empfanges Bit, S = Schlüsselbit, D = Datenbit (4 x 5 Bit), Bu = Buchstabe

Basiswahl – EVE

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Ba																		

	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Ba																		

	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
Ba																

Binäre Darstellung des Alphabets

A	0	0	0	0	0
B	0	0	0	0	1
C	0	0	0	1	0
D	0	0	0	1	1
E	0	0	1	0	0
F	0	0	1	0	1
G	0	0	1	1	0
H	0	0	1	1	1
I	0	1	0	0	0
J	0	1	0	0	1
K	0	1	0	1	0
L	0	1	0	1	1
M	0	1	1	0	0
N	0	1	1	0	1
O	0	1	1	1	0
P	0	1	1	1	1
Q	1	0	0	0	0
R	1	0	0	0	1
S	1	0	0	1	0
T	1	0	0	1	1
U	1	0	1	0	0
V	1	0	1	0	1
W	1	0	1	1	0
X	1	0	1	1	1
Y	1	1	0	0	0
Z	1	1	0	0	1