Variante: Man-in-the-Middle

	A	B	C	D	E	F	G	H	I	J	K
2			Operator 1	Operator 2	Handlungsschritt	Ergebnis					
3	Beginn Phase 0	Integer			Text erzeugen	Str1 = "Hello World!"	Nachricht Alice-Eve [Alice]	A	1	Alice gibt einen zu verschlüsselnden Text Str1 ein	Beginn Phase 0
4		Bitfolge			Zahl erzeugen	Int1 = 32	Schlüssellänge Alice-Eve [Alice]	A	2	Alice berechnet die Schlüssellänge Int1 basierend auf der Nachricht	
5		Photonen		Int1 = 32	Nachricht über Bitübertragungskanal senden			A	3	Alice sendet die Schlüssellänge Int1 über den Bit-Kanal	
6		Polscha			Zug beenden			A	4	Alice beendet ihren Zug	
7		unscharfe Photonen			Nachricht auf Bitübertragungskanal empfangen	Int1 = 32	Schlüssellänge Alice-Eve [Alice]	E	5	Eve speichert sich die Schlüssellänge Int1	
8		ASCII-Text			Zahl erzeugen	Int2 = 40	Schlüssellänge Eve-Bob [Eve]	E	6	Eve berechnet eigene Schlüssellänge Int2	
9		Verschlüsselter Text		Int2 = 40	Nachricht über Bitübertragungskanal senden		Schlüssellänge Eve-Bob [Eve]	E	7	Eve sendet eigene Schlüssellänge Int2 an Bob	
10		Kommentar Alice			Zug beenden			E	8	Eve beendet ihren Zug	
11		Kommentar Eve			Nachricht auf Bitübertragungskanal empfangen	Int2 = 40	Schlüssellänge Eve-Bob [Eve]	B	9	Bob empfängt die Schlüssellänge Int2	
12		Kommentar Bob			Zug beenden			B	10	Bob beendet seinen Zug	
13	Ende Phase 0				Zug beenden			E	11	Eve ist dran, kann aber eigentlich nichts tun und beendet ihren Zug	Ende Phase 0
14	Beginn Phase 1			Int1 = 32	Bitfolge erzeugen	Bit1 = 0100 1111 1000 0101 1011 1101 0001 0001	Schlüsselbits Alice-Eve [Alice]	A	12	Alice erzeugt zufällige Schlüsselbits Bit1 entsprechend der Länge Int1	Beginn Phase 1
15				Int1 = 32	Polschata erzeugen	Pol1 = xx+x +++x xxx+ +++x x+xx x+++ +++x ++++	Polschata Alice-Eve [Alice]	A	13	Alice erzeugt die gleiche Anzahl zufälliger Polschata Pol1	
16			Bit1 = 0100 1111 1000 0101 1011 1101 0001 0001	Pol1 = xx+x +++x xxx+ +++x x+xx x+++ +++x ++++	Photonen erzeugen	Pho1 = /\\| -|| --|\\| --|\\//| -/-|\\//| --|| \					
17				Pho1 = /\\| --|| --|\\| --|\\//| -/-|\\//| --|| \	Nachricht auf Photonübertragungskanal senden			A	15	Alice überträgt die Photonen Pho1 über den Photonenübertragungskanal	
18					Zug beenden			A	16	Alice beendet ihren Zug	
19				Int1 = 32	Polschata erzeugen	Pol2 = xxx+ x+x+ x+xx +xx+ ++x+ x++x +x++ x++x	Polschata Alice-Eve [Eve]	E	17	Eve erzeugt ihre eigenen Polschata Pol2 anhand der Schlüssellänge Int1	
20				-	-	VPh1 = **********	unscharfe Photonen Alice-Eve	-	18	Auf dem Photonenübertragungskanal befinden sich die Photonen VPh1 unbekannter Polarisation (Für Eve)	
21			Pol2 = xxx+ x+x+ x+xx +xx+ ++x+ x++x +x++ x++x	VPh1 = **********	Nachricht auf Photonenübertragungskanal empfangen	Pho2 = /| /||--/||||\\/||--|\\|\//||/| -/-|\\	Photonen Alice-Eve [Eve]	E	19	Eve liest mithilfe ihrer Polschata Pol2 die unscharfen Photonen VPh1 aus und erhält die Photonen Pho2 (Die Polarisierung einiger Photonen wird geändert)	
22				Pho2 = /| /||--/||||\\/||--|\\|\//||/| -/-|\\	Photonen zu Bitfolge konvertieren	Bit2 = 1010 0101 0011 0110 1100 1101 0101 1001	Schlüsselbits Alice-Eve [Eve]	E	20	Aus Photonen Pho2 wird der Bitstrom Bit2 erzeugt	
23				Int2 = 40	Bitfolge erzeugen	Bit3 = 0110 1010 1010 1011 1001 1010 1010 0101	Schlüsselbits Eve-Bob [Eve]	E	21	Eve erzeugt so viele zufällige Schlüsselbits Bit3 wie der Wert der Zahl der Schlüssellänge Int2	
24				Int2 = 40	Polschata erzeugen	Pol3 = xx+x +++x xxx+ +++x x+xx x+++ +++x ++++	Polschata Eve-Bob [Eve]	E	22	Eve erzeugt gleich viele zufällige Polschata Pol3	
25			Pol3 = xx+x +++x xxx+ +++x x+xx x+++ +++x ++++	Bit3 = 0110 1010 1010 1011 1001 1010 1010 0101	Photonen erzeugen	Pho3 = /\\| --|| --|\\| --|\\//| -/-|\\//| --|| \	Photonen Eve-Bob [Eve]	E	23	Eve erzeugt aus den Schlüsselbits Bit3 und Polschata Pol3 die Photonen Pho3	
26				Pho3 = /\\| --|| --|\\| --|\\//| -/-|\\//| --|| \	Nachricht auf Photonübertragungskanal senden			E	24	Eve überträgt die Photonen Pho3 über den Photonenübertragungskanal	
27					Zug beenden			E	25	Eve beendet ihren Zug	
28				Int2 = 40	Polschata erzeugen	Pol4 = x+x+ +x+x +++x +x+x +xx+ x+x+ +++x x+xx	Polschata Eve-Bob [Bob]	B	26	Bob erzeugt seine eigene Polschata Pol4 anhand der Schlüssellänge Int2	
29				-	-	VPh2 = **********	unscharfe Photonen Eve-Bob	-	27	Auf dem Photonenübertragungskanal befinden sich die Photonen VPh2 unbekannter Polarisation (Für Bob)	
30			Pol4 = x+x+ +x+x +++x +x+x +xx+ x+x+ +++x x+xx	VPh2 = **********	Nachricht auf Photonübertragungskanal empfangen	Pho4 = /| |--/||/|||/|\\/|--|\\--///-||\\-|-	Photonen Eve-Bob [Bob]	B	28	Bob liest mithilfe seiner Polschata Pol4 die unscharfen Photonen VPh2 aus	
31				Pho4 = /| |--/||/|||/|\\/|--|\\--///-||\\-|-	Photonen zu Bitfolge konvertieren	Bit4 = 0110 1110 1010 1011 0010 1010 1001 0100	Schlüsselbits Eve-Bob [Bob]	B	29	Aus Photonen Pho4 wird der Bitstrom Bit4 erzeugt	
32	Ende Phase 1				Zug beenden			B	30	Bob bestätigt erhalt der Nachricht durch Beenden seines Zuges	Ende Phase 1
33	Beginn Phase 2			Pol1 = xx+x +++x xxx+ +++x x+xx x+++ +++x ++++	Nachricht auf Bitübertragungskanal senden			A	31	Alice gibt über den Bitübertragungskanal ihre Polschata Pol1 preis welche Eve abfängt	Beginn Phase 2
34					Zug beenden			A	32	Alice beendet ihren Zug	
35					Nachricht auf Bitübertragungskanal empfangen	Pol1 = xx+x +++x xxx+ +++x x+xx x+++ +++x ++++	Polschata Alice-Eve [Alice]	E	33	Eve empfängt Alices Polschata Pol1	
36			Pol2 = xxx+ x+x+ x+xx +xx+ ++x+ x++x +x++ x++x	Pol1 = xx+x +++x xxx+ +++x x+xx x+++ +++x ++++	Vergleich Polschata (XOR)	Bit5 = 0011 1011 0101 0101 1001 0001 0110 1001	Bitmaske Alice-Eve [Eve]	E	34	Es entsteht eine Bitmaske Bit5, bei welcher "0" für gleich und "1" für ungleich steht	
37			Bit2 = 1010 0101 0011 0110 1100 1101 0101 1001	Bit5 = 0011 1011 0101 0101 1001 0001 0110 1001	Streichen von Bits aus Bitfolge	Bit6= 0100 1011 0111 0000	Schlüsselbits Alice-Eve 2 [Eve]	E	35	Aus den Schlüsselbits Bit2 löscht Eve mit der Bitmaske Bit5 alle falsch geratenen Stellen	
38				Bit5 = 0011 1011 0101 0101 1001 0001 0110 1001	Nachricht auf Bitübertragungskanal senden			E	36	Eve schickt die Bitmaske Bit5 über den Bitübertragungskanal zu Alice	
39				Pol3 = xx+x +++x xxx+ +++x x+xx x+++ +++x ++++	Nachricht auf Bitübertragungskanal senden			E	37	Eve schickt ihre Polschata Pol3 an Bob	
40					Zug beenden			E	38	Eve beendet ihren Zug	
41					Nachricht auf Bitübertragungskanal empfangen	Pol3 = xx+x +++x xxx+ +++x x+xx x+++ +++x ++++	Polschata Eve-Bob [Eve]	B	39	Bob empfängt die Polschata Pol3 von "Alice"	
42		Pol4 = x+x+ +x+x +++x +x+x +xx+ x+x+ +++x x+xx	Bit4 = 0110 1110 1010 1011 0010 1010 1001 0100	Pol3 = xx+x +++x xxx+ +++x x+xx x+++ +++x ++++	Vergleich Polschata (XOR)	Bit7 = 1011 0101 0011 0001 1001 0110 0101 1001	Bitmaske Eve-Bob [Bob]	B	40	Durch Vergleichen der Polschata Pol3 und Pol4 entsteht eine Bitmaske Bit7, bei welcher "0" für gleich und "1" für ungleich steht	
43				Bit7 = 1011 0101 0011 0001 1001 0110 0101 1001	Streichen von Bits aus Bitfolge	Bit8 = 0101 0101 0111 0100 1011	Schlüsselbits Eve-Bob 2 [Bob]	B	41	Der daraus entstandene Bitstrom Bit8 stell die gekürzten Schlüsselbits dar	
44				Bit7 = 1011 0101 0011 0001 1001 0110 0101 1001	Nachricht auf Bitübertragungskanal senden			B	42	Bob schickt die Bitmaske Bit7 über den Bitübertragungskanal zu "Alice"	
45					Zug beenden			B	43	Bob beendet seinen Zug	
46					Nachricht auf Bitübertragungskanal empfangen	Bit7 = 1011 0101 0011 0001 1001 0110 0101 1001	Bitmaske Eve-Bob [Bob]	E	43	Eve empfängt die Bitmaske Bit7 von Bob	
47			Bit7 = 1011 0101 0011 0001 1001 0110 0101 1001	Bit3 = 0110 1010 1010 1011 1001 1010 1010 0101	Streichen von Bits aus Bitfolge	Bit9 = 0011 0110 1100 1101 0101 1001	Schlüsselbits Eve-Bob 2 [Eve]	E	44	Eve streicht die Stellen an Hand der Bitmaske Bit7 die Bob gelöscht hat aus ihren Schlüsselbits Bit3 und erhält somit ihre neuen Schlüsselbits Bit9	
48					Zug beenden			E	45	Eve beendet ihren Zug	
49					Nachricht auf Bitübertragungskanal empfangen	Bit5 = 0011 1011 0101 0101 1001 0001 0110 1001	Bitmaske Alice-Eve [Eve]	A	46	Alice empfängt die Bitmaske Bit 5 von "Bob"	
50	Ende Phase 2		Bit1 = 0100 1111 1000 0101 1011 1101 0001 0001	Bit5 = 0011 1011 0101 0101 1001 0001 0110 1001	Streichen von Bits aus Bitfolge	Bit10 = 1111 0000 1111 0000	Schlüsselbits Alice-Eve 2 [Alice]	A	47	Alice streicht die Stellen an denen "Bob" falsch geraten hat aus ihren Schlüsselbits Bit1 und erhält die neuen Schlüsselbits Bit10	Ende Phase 2
51	Beginn Phase 3				Zahl erzeugen	Int3 = 5	Prüfbitanzahl Alice-Eve [Alice]	A	48	Alice ermittelt aus der Länge der neuen Schlüsselbit Bit10 die Zahl Int3 der Bits, die angefordert werden sollen	Beginn Phase 3
52				Bit10 = 1111 0000 1111 0000	Zahl erzeugen	Int4 = 16	Länge Prüfmaske Alice-Eve [Alice]	A	49	Alice bestimmt die Länge der Bitmaske Int4 anhand ihrer Schlüsselbits Bit10	
53			Int4 = 16	Int3 = 5	Bitmaske erzeugen	Bit11 = 0110 0010 0100 1000	Prüfmaske Alice-Eve [Alice]	A	50	Alice generiert nun eine Bitmaske Bit11, welche angibt, welche Bits Bob schicken soll Ihre Länge ist bestimmt durch Int4 und die Anzahl der zu prüfenden Bits durch Int3	
54			Bit11 = 0110 0010 0100 1000	Bit10 = 1111 0000 1111 0000	Streichen von Bits aus Bitfolge	Bit12 = 1 0101	Prüfbits Alice-Eve [Alice]	A	51	Alice erhält die Prüfbits Bit12 durch streichen der Schlüsselstellen aus Bit10	
55			Bit11 = 0110 0010 0100 1000	Bit10 = 1111 0000 1111 0000	Streichen von Bits aus Bitfolge	Bit13 = 001 1110 1010	Schlüssel Alice-Eve [Alice]	A	52	Alice erhält den Schlüssel Bit13 durch streichen der Prüfmaske Bit11	
56				Bit11 = 0110 0010 0100 1000	Nachricht auf Bitübertragungskanal senden			A	53	Alice sendet die Prüfmaske Bit11 an "Bob"	
57					Zug beenden			A	54	Alice beendet ihren Zug	
58					Nachricht auf Bitübertragungskanal empfangen	Bit11 = 0110 0010 0100 1000	Prüfmaske Alice-Eve [Alice]	E	55	Eve erhält die Prüfmaske Bit11 von Alice	
59			Bit11 = 0110 0010 0100 1000	Bit6= 0100 1011 0111 0000	Streichen von Bits aus Bitfolge	Bit14 = 0 1111	Prüfbits Alice-Eve [Eve]	E	56	Eve erzeugt aus ihrem Schlüsselbits Bit6 und der Prüfmaske Bit11 von Alice die Prüfbits Bit14	
60			Bit11 = 0110 0010 0100 1000	Bit6= 0100 1011 0111 0000	Streichen von Bits aus Bitfolge	Bit15 = 0110 1010 0001 0100	Schlüssel Alice-Eve [Eve]	E	57	Eve streicht die Stellen aus ihrem Schlüssel Bit6 die angefordert wurden	
61				Bit14 = 0 1111	Nachricht auf Bitübertragungskanal senden			E	58	Eve sendet die berechneten Prüfbits Bit14 an Alice	
62					Zahl erzeugen	Int5 = 7	Prüfbitanzahl Eve-Bob [Eve]	E	59	Eve ermittelt die Anzahl der Prüfbits Int5 anhand der Länge des Schlüssels Bit15	
63				Bit9 = 0011 0110 1100 1101 0101 1001	Zahl erzeugen	Int6 = 20	Länge Prüfmaske Eve-Bob [Eve]	E	60	Eve erzeugt die Länge der Bitmaske Int6 anhand ihrer Schlüsselbits Bit9	
64			Int5 = 7	Int6 = 20	Bitmaske erzeugen	Bit16 = 1111 1110 0000 0000 0000	Prüfmaske Eve-Bob [Eve]	E	61	Eve erzeugt die Prüfmaske Bit16	
65			Bit16 = 1111 1110 0000 0000 0000	Bit9 = 0011 0110 1100 1101 0101 1001	Streichen von Bits aus Bitfolge	Bit17 = 101 0111	Prüfbits Eve-Bob [Eve]	E	62	Eve erhält die Prüfbits Bit17 durch streichen der Schlüsselbits Bit9	
66			Bit16 = 1111 1110 0000 0000 0000	Bit9 = 0011 0110 1100 1101 0101 1001	Streichen von Bits aus Bitfolge	Bit18 = 1 0101 0101 0110	Schlüssel Eve-Bob [Eve]	E	63	Eve erhält den Schlüssel Bit18 durch streichen der Prüfbitstellen Bit16	
67				Bit16 = 1111 1110 0000 0000 0000	Nachricht auf Bitübertragungskanal senden			E	62	Eve sendet ihre Prüfmaske Bit16 an Bob	
68					Zug beenden			E	63	Eve beendet ihren Zug	
69					Nachricht auf Bitübertragungskanal empfangen	Bit16 = 1111 1110 0000 0000 0000	Prüfmaske Eve-Bob [Eve]	B	64	Bob erhält die Prüfmaske Bit16 von "Alice"	
70			Bit16 = 1111 1110 0000 0000 0000	Bit8 = 0101 0101 0111 0100 1011	Streichen von Bits aus Bitfolge	Bit19 = 101 0111	Prüfbits Eve-Bob [Bob]	B	65	Bob streicht die Stellen aus seinem Schlüssel Bit8 die nicht angefordert wurden und erhält seine Prüfbits Bit19	
71			Bit16 = 1111 1110 0000 0000 0000	Bit8 = 0101 0101 0111 0100 1011	Streichen von Bits aus Bitfolge	Bit20 = 11 01101 0010	Schlüssel Eve-Bob [Bob]	B	66	Bob streicht die angefragten Prüfbits Bit16 aus seinem Schlüssel Bit8	
72				Bit19 = 101 0111	Nachricht auf Bitübertragungskanal senden			B	67	Bob sendet die berechneten Prüfbits Bit19 an "Alice"	
73					Zug beenden			B	68	Bob beendet seinen Zug	
74					Nachricht auf Bitübertragungskanal empfangen	Bit19 = 101 0111	Prüfbits Eve-Bob [Bob]	E	69	Eve empfängt die von Bob gesendeten Prüfbits Bit19	
75			Bit17 = 101 0111	Bit19 = 101 0111	Bitfolgen auf Gleichheit prüfen (XOR)	Bit21 = 000 0000	Ergebnisbits Prüfung Eve-Bob [Eve]	E	70	Falls die Prüfbits Bit17 und Bit19 nicht übereinstimmen, so weiß Eve, dass gegen sie ein Mitm-Angriff durchgeführt wurde und sie kann den Austausch abbrechen	
76					Zug beenden			E	71	Eve beendet ihren Zug	
77					Nachricht auf Bitübertragungskanal empfangen	Bit14 = 0 1111	Prüfbits Alice-Eve [Eve]	A	72	Alice empfängt die von "Bob" gesendeten Prüfbits Bit14	
78	Ende Phase 3		Bit12 = 1 0101	Bit14 = 0 1111	Bitfolgen auf Gleichheit prüfen (XOR)	Bit22 = 0 0000	Ergebnisbits Prüfung Alice-Eve [Alice]	A	73	Alice prüft ihre berechneten Prüfbits Bit12 mit den von "Bob" erhaltenen Prüfbits Bit14 auf Gleichheit	Ende Phase 3
79	Beginn Phase 4		Str1 = "Hello World!"	Bit13 = 001 1110 1010	Nachricht verschlüsseln	Cif1 = **********	Chiffre Alice-Eve [Alice]	A	74	Alice verschlüsselt den String Str1 mit ihrem Schlüssel Bit13 und erhält dadurch die Chiffre Chif1	Beginn Phase 4
80				Cif1 = **********	Nachricht auf Bitübertragungskanal senden			A	75	Alice sendet die Chiffre Cif1 über den Bitübertragungskanal an "Bob"	
81					Zug beenden			A	76	Alice beendet ihren Zug	
82					Nachricht auf Bitübertragungskanal empfangen	Cif1 = **********	Chiffre Alice-Eve [Alice]	E	77	Eve hört die Chiffre Chif1 ab	
83			Cif1 = **********	Bit15 = 0110 1010 0001 0100	Nachricht entschlüsseln	Str1 = "Hello World!"	Nachricht Alice-Eve [Alice]	E	78	Eve entschlüsselt die Chiffre Chif1 mit dem Schlüssel Bit15	
84					Text erzeugen	Str2 = "Bye World!"	Nachricht Eve-Bob [Eve]	E	79	Eve erzeugt einen eigenen String Str2, welcher mit Str1 identisch sein kann	
85			Str2 = "Bye World!"	Bit18 = 1 0101 0101 0110	Nachricht verschlüsseln	Cif2 = **********	Chiffre Eve-Bob [Eve]	E	80	Eve verschlüsselt den String Str2 mit ihrem Schlüssel Bit18 und erhält dadurch die Chiffre Chif2	
86				Cif2 = **********	Nachricht auf Bitübertragungskanal senden			E	81	Eve sendet die Chifre Chif2 über den Bitübertragungskanal an Bob	
87					Zug beenden			E	82	Eve beendet ihren Zug	
88					Nachricht auf Bitübertragungskanal empfangen	Cif2 = **********	Chiffre Eve-Bob [Eve]	B	83	Bob empfängt die Chiffre Cif2	
89	Ende Phase 4		Cif2 = **********	Bit20 = 11 01101 0010	Nachricht entschlüsseln	Str2 = "Bye World!"	Nachricht Eve-Bob [Bob]	B	84	Bob entschlüsselt mithilfe seines Schlüssels Bit20 die Chiffre Cif2 und erhält dadurch den String Str2	Ende Phase 4