Quantenkryptographie

Jürgen Schnack & Frederik Ihorst

Fakultät für Physik – Universität Bielefeld

http://obelix.physik.uni-bielefeld.de/∼schnack/

Preisverleihung – Mathematikolympiade Kreis Gütersloh

Städtisches Gymnasium Gütersloh, 4. Mai 2022

UNIVERSITÄT BIELEFELD
Fakultät für Physik

DFG

Irz

Herzlichen

Glückwunsch

Ihr seid super!

Herzlichen Dank an Herrn Venz,

alle Mathelehrerinnen

und alle Mathelehrer

und einen unendlichen Applaus!

Liebe Eltern (insbesondere die Väter), auch wenn es Ihnen auf der Zunge liegt:

SIE DÜRFEN HEUTE NICHT VORSAGEN!

Kryptographie = Lehre von der Verschlüsselung

Kennt Ihr so etwas?

Einfache Verschlüsselung nach Caesar

Gibt es die absolut sichere Verschlüsselung?

Was braucht man für eine sichere Verschlüsselung?

- einen Schlüssel, der genauso lang ist wie die Botschaft und den man nur einmal verwendet (one-time pad);

- einen Schlüssel, den wirklich nur Sender und Empfänger kennen können;

Was braucht man für eine sichere Verschlüsselung?

- einen Schlüssel, der genauso lang ist wie die Botschaft und den man nur einmal verwendet (one-time pad);
  $\Rightarrow$ Binärzahlen zur Verschlüsselung;

- einen Schlüssel, den wirklich nur Sender und Empfänger kennen können;

Was braucht man für eine sichere Verschlüsselung?

- einen Schlüssel, der genauso lang ist wie die Botschaft und den man nur einmal verwendet (one-time pad);
  $\Rightarrow$ Binärzahlen zur Verschlüsselung;
  $\Rightarrow$ Mathe ist cool!

- einen Schlüssel, den wirklich nur Sender und Empfänger kennen können;

Was braucht man für eine sichere Verschlüsselung?

- einen Schlüssel, der genauso lang ist wie die Botschaft und den man nur einmal verwendet (one-time pad);
  $\Rightarrow$ Binärzahlen zur Verschlüsselung;
  $\Rightarrow$ Mathe ist cool!

- einen Schlüssel, den wirklich nur Sender und Empfänger kennen können;
  $\Rightarrow$ Quantenmechanik zur Erzeugung des Schlüssels;

Was braucht man für eine sichere Verschlüsselung?

- einen Schlüssel, der genauso lang ist wie die Botschaft und den man nur einmal verwendet (one-time pad);
  $\Rightarrow$ Binärzahlen zur Verschlüsselung;
  $\Rightarrow$ Mathe ist cool!

- einen Schlüssel, den wirklich nur Sender und Empfänger kennen können;
  $\Rightarrow$ Quantenmechanik zur Erzeugung des Schlüssels;
  $\Rightarrow$ Physik ist cool!

Binärzahlen
und
Verschlüsselung

Binärzahlen I

Zehnersystem (Dezimalzahlen)
Ziffern $0, 1, \ldots 9$

$$101 = 1 \cdot 100 + 0 \cdot 10 + 1 \cdot 1$$
$$101 = 1 \cdot 10^2 + 0 \cdot 10^1 + 1 \cdot 10^0$$

Binärsystem (Dualzahlen)
Ziffern $0, 1$

$$101 = 1 \cdot 4 + 0 \cdot 2 + 1 \cdot 1$$
$$101 = 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

Binärzahlen II

Zehnersystem (Dezimalzahlen)

Ziffern $0, 1, \ldots 9$

$$101 = 1 \cdot 100 + 0 \cdot 10 + 1 \cdot 1$$
$$101 = 1 \cdot 10^2 + 0 \cdot 10^1 + 1 \cdot 10^0$$

Addition:

$$\begin{array}{r} 101 \\ +101 \\ \hline ??? \end{array}$$

Binärsystem (Dualzahlen)

Ziffern $0, 1$

$$101 = 1 \cdot 4 + 0 \cdot 2 + 1 \cdot 1$$
$$101 = 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

Addition:

$$\begin{array}{r} 101 \\ +101 \\ \hline ??? \end{array}$$

Binärzahlen III

Zehnersystem (Dezimalzahlen)

Ziffern $0, 1, \ldots 9$

$$101 = 1 \cdot 100 + 0 \cdot 10 + 1 \cdot 1$$
$$101 = 1 \cdot 10^2 + 0 \cdot 10^1 + 1 \cdot 10^0$$

Addition:

$$\begin{array}{r} 101 \\ +101 \\ \hline 202 \end{array}$$

Binärsystem (Dualzahlen)

Ziffern $0, 1$

$$101 = 1 \cdot 4 + 0 \cdot 2 + 1 \cdot 1$$
$$101 = 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

Addition:

$$\begin{array}{r} 101 \\ +101 \\ \hline 1010 \end{array}$$

Binärzahlen IV

Dez	Hex	Okt	ASCII	Dez	Hex	Okt	ASCII	Dez	Hex	Okt	ASCII	Dez	Hex	Okt	ASCII
0	00	000	NUL	32	20	040	SP	64	40	100	@	96	60	140	`
1	01	001	SOH	33	21	041	!	65	41	101	A	97	61	141	a
2	02	002	STX	34	22	042	"	66	42	102	B	98	62	142	b
3	03	003	ETX	35	23	043	#	67	43	103	C	99	63	143	c
4	04	004	EOT	36	24	044	$	68	44	104	D	100	64	144	d
5	05	005	ENQ	37	25	045	%	69	45	105	E	101	65	145	e
6	06	006	ACK	38	26	046	&	70	46	106	F	102	66	146	f
7	07	007	BEL	39	27	047	'	71	47	107	G	103	67	147	g
8	08	010	BS	40	28	050	(	72	48	110	H	104	68	150	h
9	09	011	HT	41	29	051	)	73	49	111	I	105	69	151	i
10	0A	012	LF	42	2A	052	*	74	4A	112	J	106	6A	152	j
11	0B	013	VT	43	2B	053	+	75	4B	113	K	107	6B	153	k
12	0C	014	FF	44	2C	054	,	76	4C	114	L	108	6C	154	l
13	0D	015	CR	45	2D	055	-	77	4D	115	M	109	6D	155	m
14	0E	016	SO	46	2E	056	.	78	4E	116	N	110	6E	156	n
15	0F	017	SI	47	2F	057	/	79	4F	117	O	111	6F	157	o
16	10	020	DLE	48	30	060	0	80	50	120	P	112	70	160	p
17	11	021	DC1	49	31	061	1	81	51	121	Q	113	71	161	q
18	12	022	DC2	50	32	062	2	82	52	122	R	114	72	162	r
19	13	023	DC3	51	33	063	3	83	53	123	S	115	73	163	s
20	14	024	DC4	52	34	064	4	84	54	124	T	116	74	164	t
21	15	025	NAK	53	35	065	5	85	55	125	U	117	75	165	u
22	16	026	SYN	54	36	066	6	86	56	126	V	118	76	166	v
23	17	027	ETB	55	37	067	7	87	57	127	W	119	77	167	w
24	18	030	CAN	56	38	070	8	88	58	130	X	120	78	170	x
25	19	031	EM	57	39	071	9	89	59	131	Y	121	79	171	y
26	1A	032	SUB	58	3A	072	:	90	5A	132	Z	122	7A	172	z
27	1B	033	ESC	59	3B	073	;	91	5B	133	[	123	7B	173	{
28	1C	034	FS	60	3C	074	<	92	5C	134	\	124	7C	174	|
29	1D	035	GS	61	3D	075	=	93	5D	135	]	125	7D	175	}
30	1E	036	RS	62	3E	076	>	94	5E	136	^	126	7E	176	~
31	1F	037	US	63	3F	077	?	95	5F	137	_	127	7F	177	DEL

W	o	r	t	
87	111	114	116	
01010111	01101111	01110010	01110100	

Verschlüsseln: Schlüssel addieren*

01010111	01101111	01110010	01110100	T
+10101010	10101010	10101010	10101010	S
11111101	11000101	11011000	11011110	C

Entschlüsseln: Schlüssel noch einmal addieren*

11111101	11000101	11011000	11011110	C
+10101010	10101010	10101010	10101010	S
01010111	01101111	01110010	01110100	T

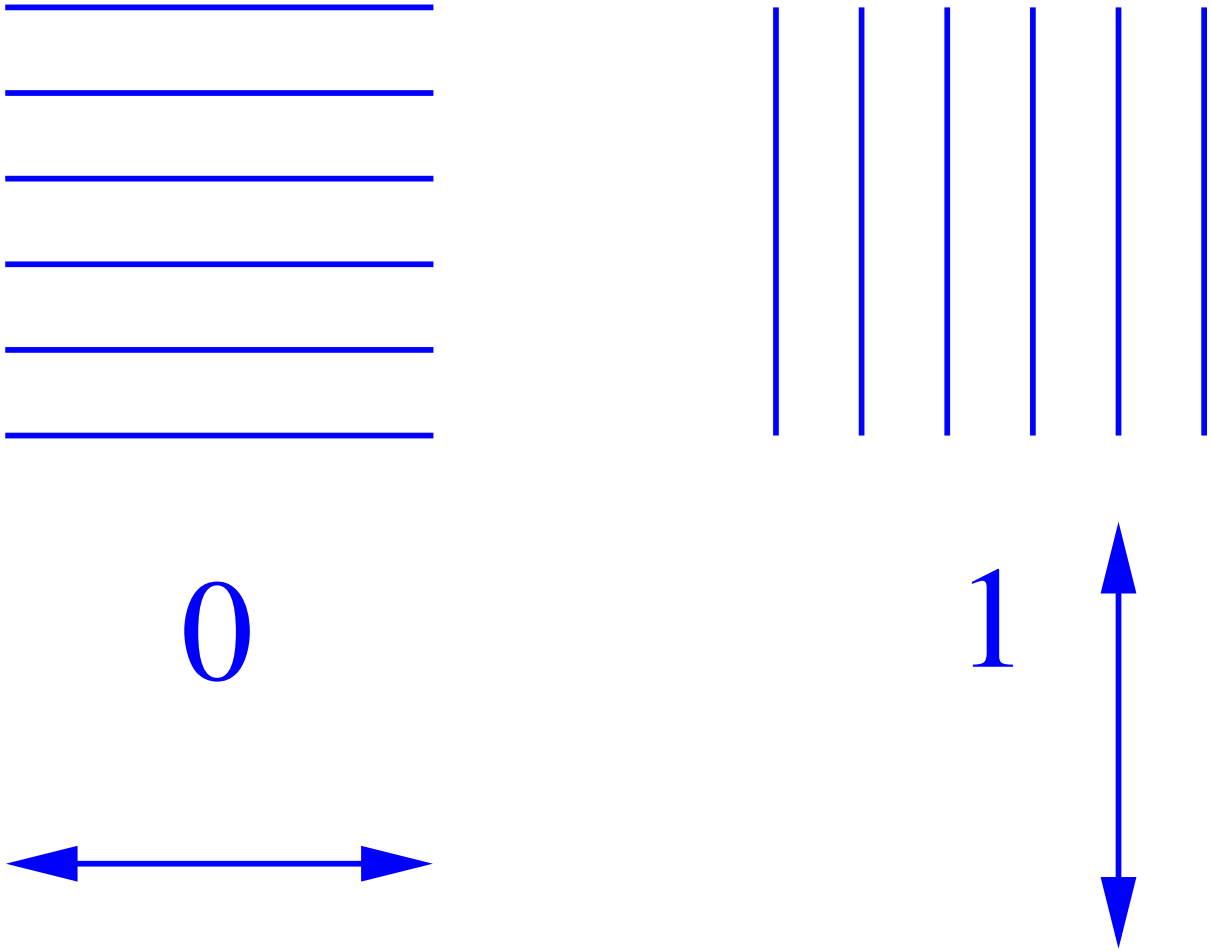
* ohne Übertrag (bitweise)

Schlüsselerzeugung

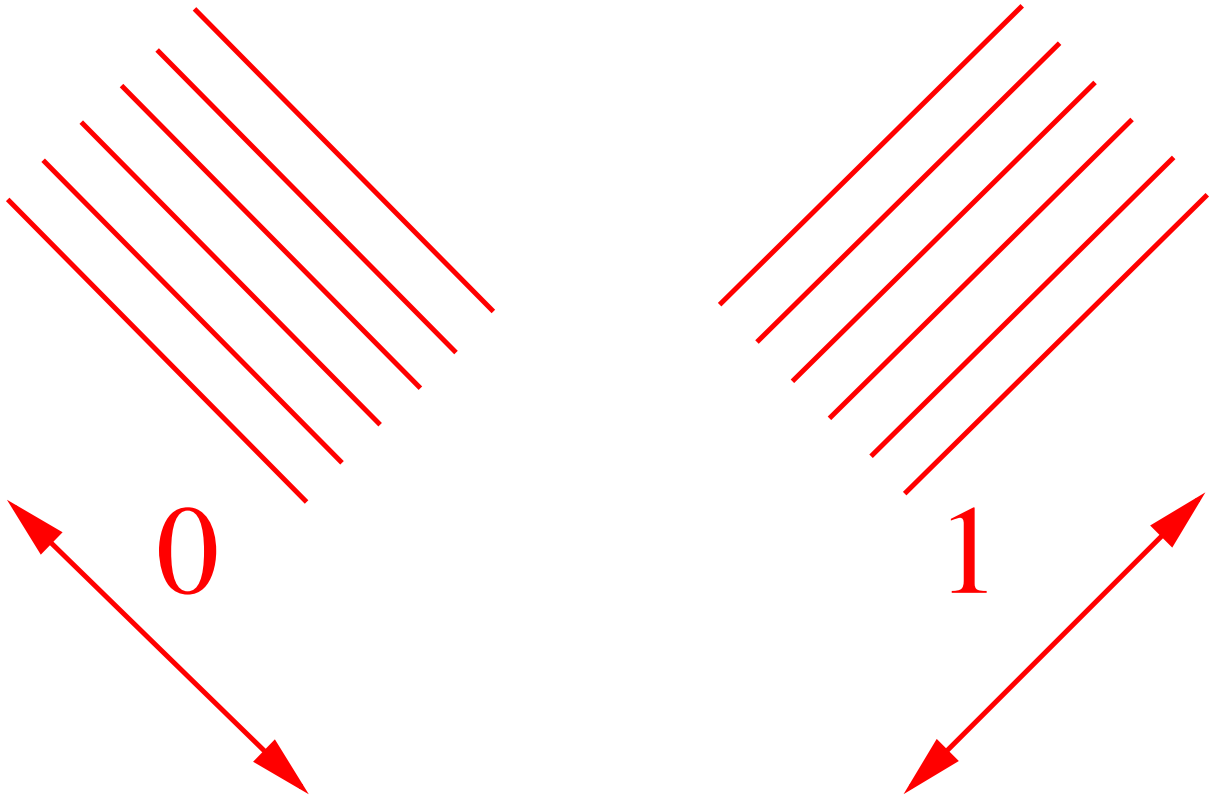
(mit Polarisatoren und einzelnen Photonen)

Polarisatoren

Quantenschlüssel I



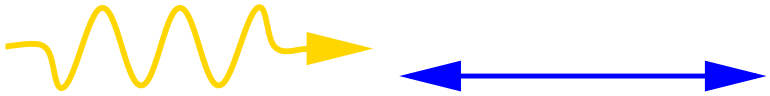
Quantenschlüssel II



Quantenschlüssel – Regeln I

Sender (Alice)

Empfänger (Bob)

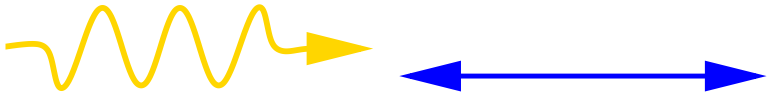


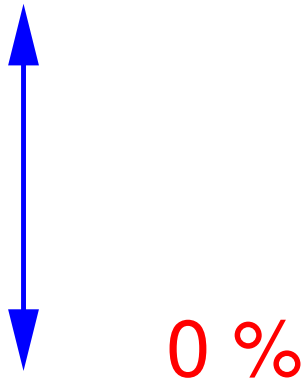
100 %

Quantenschlüssel – Regeln II

Sender (Alice)

Empfänger (Bob)



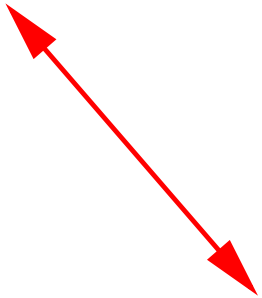


0 %

Quantenschlüssel – Regeln III

Sender (Alice)

Empfänger (Bob)

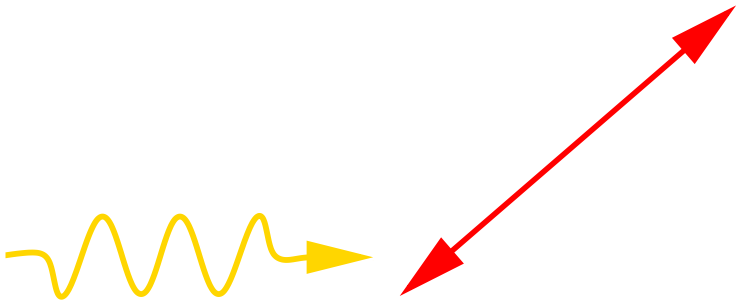


50 %

Quantenschlüssel – Verstanden?

Sender (Alice)

Empfänger (Bob)

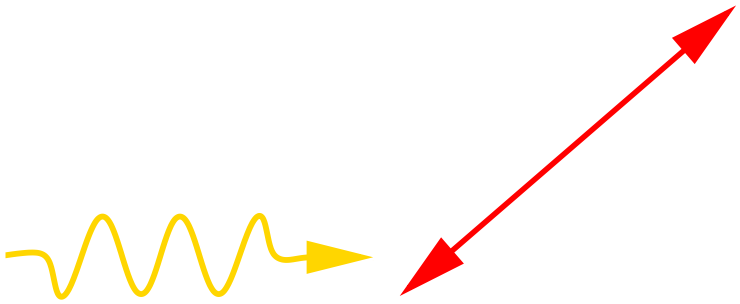


? %

Quantenschlüssel – Verstanden!

Sender (Alice)

Empfänger (Bob)



50 %

Erzeugung des Quantenschlüssels – Protokoll BB84

1. Alice wählt zufällig eine der 4 Polarisationsrichtungen: 
2. Bob wählt zufällig eine der 4 Polarisationsrichtungen: 
3. Alice sendet das Photon mit ihrer Polarisationsrichtung:
4. Bob empfängt ein Photon oder nicht.
5. Alice sagt Bob, ob sie blau oder rot genommen hat.
6. Hatten beide das gleiche System, weiß Bob, welche Richtung Alice gewählt hatte.
   Warum???
   Er sagt o.k.; das Bit zählt und beide fügen es zum Schlüssel hinzu.
7. Das machen sie so lange, bis der Schlüssel lang genug ist.

Erzeugung des Quantenschlüssels – Beispiel

Alice	Bob	Bob sieht Photon	Alice sagt	Bob sagt	neues Bit	Schlüssel
		ja	blau	o.k.	0	0
		nein	blau	o.k.	1	01
		ja oder nein	rot	nicht o.k.	-	01
		nein	rot	o.k.	0	010
		?	?	?	?	?
		?	?	?	?	?

Erzeugung des Quantenschlüssels – Beispiel

Alice	Bob	Bob sieht Photon	Alice sagt	Bob sagt	neues Bit	Schlüssel
		ja	blau	o.k.	0	0
		nein	blau	o.k.	1	01
		ja oder nein	rot	nicht o.k.	-	01
		nein	rot	o.k.	0	010
		ja oder nein	rot	nicht o.k.	-	010
		nein	rot	o.k.	1	0101

Schlüsselerzeugung ist zufällig, und kann nicht berechnet werden.

Nur Alice und Bob kennen den Schlüssel!

Die Erzeugung kann nicht abgehört werden!

Warum?

Ihr könnt es herausfinden!

Denn Ihr mögt Mathematik!

Damit könnt Ihr vieles studieren, z.B.

Physik!

Vielen Dank für Eure Aufmerksamkeit