Hochschule Düsseldorf
University of Applied Sciences

HSD

Kryptographie 2.0

Modul D3.2

Referent: Dr. Jörg Cosfeld

Kryptographie

Was lernen wir in dieser Vorlesung?

Gutes Verständnis für den **Quanten Computer**.

Kryptographie

Alan Turing

* 23. Juni 1912 in London; † 7. Juni 1954 in Wilmslow, Cheshire

Beispielrechnung:

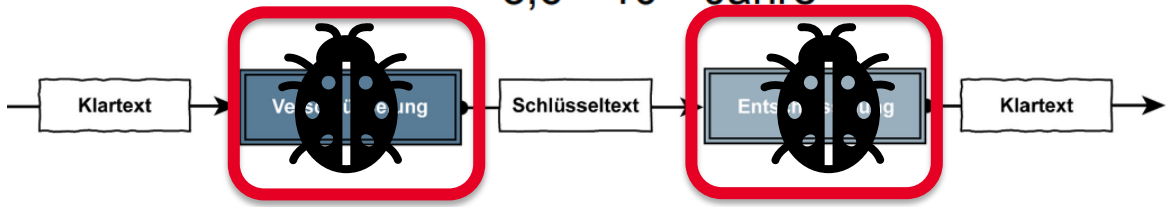
- Schlüssellänge 128 Bit
- Rechner des Angreifers schafft 3mio Schlüsselversuche *a*
- 1000 Rechner stehen dem Angreifer zur Verfügung *b*
- Schlüsselraum $S = 2^{128} \approx 3{,}4 \cdot 10^{38}$
- Ein Jahr hat 31.557.600 Sekunden *c*

Alice

Dauer= S / (a · b · c)

Bob

$3{,}6 \cdot 10^{18}$ Jahre



Kryptographie

Was lernen wir in dieser Vorlesung?

Gutes Verständnis für den **Quanten Computer**.

Wir beamen uns heute nach Las Vegas!

Kryptographie

Was lernen wir in dieser Vorlesung?

Gutes Verständnis für den **Quanten Computer**.

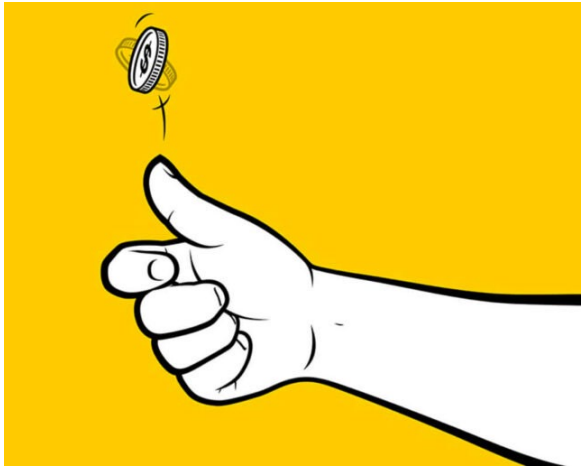
Wir beamen uns heute nach Las Vegas!

Kryptographie

Was lernen wir in dieser Vorlesung?

Gutes Verständnis für den **Quanten Computer**.

Wir beamen uns heute nach Las Vegas!



Warum?

Wir wollen Glückspiele spielen.

Kryptographie

Spielregeln:

Wir spielen gegen einen Computer.

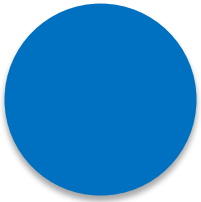
Der Computer ist richtig gut!

Kryptographie

Spielregeln:

Wir spielen gegen einen Computer.

Der Computer ist richtig gut!



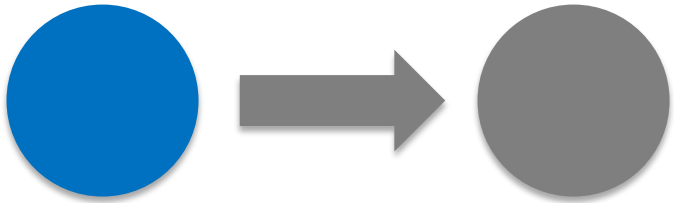
Coin liegt auf blau!

Kryptographie

Spielregeln:

Wir spielen gegen einen Computer.

Der Computer ist richtig gut!



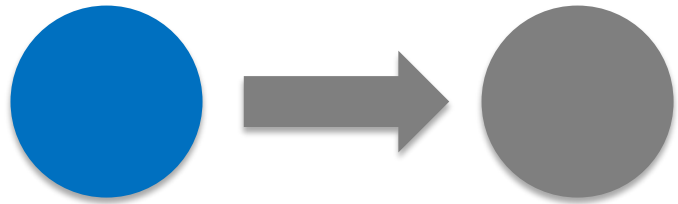
Coin wird von Jörg geflippt.

Kryptographie

Spielregeln:

Wir spielen gegen einen Computer.

Der Computer ist richtig gut!



Coin wird von Jörg geflippt.

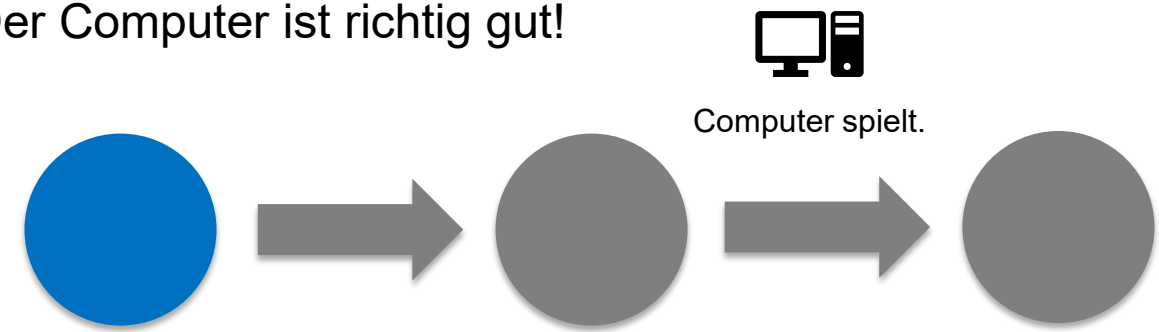
Das Ergebnis bleibt verborgen.

Kryptographie

Spielregeln:

Wir spielen gegen einen Computer.

Der Computer ist richtig gut!

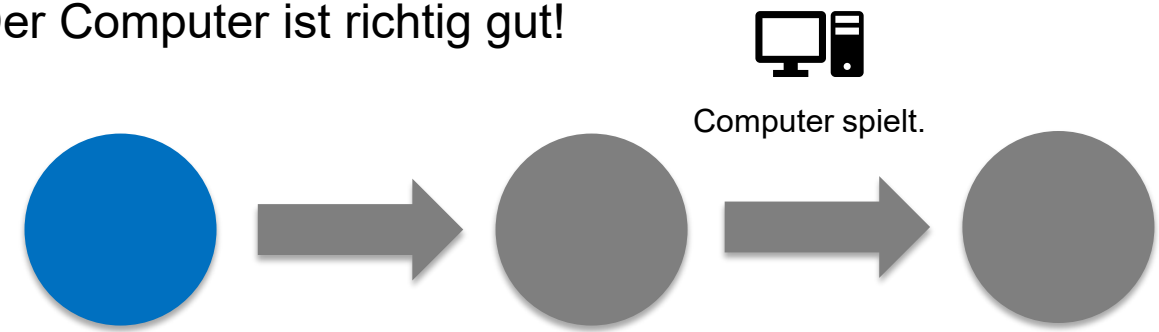


Kryptographie

Spielregeln:

Wir spielen gegen einen Computer.

Der Computer ist richtig gut!

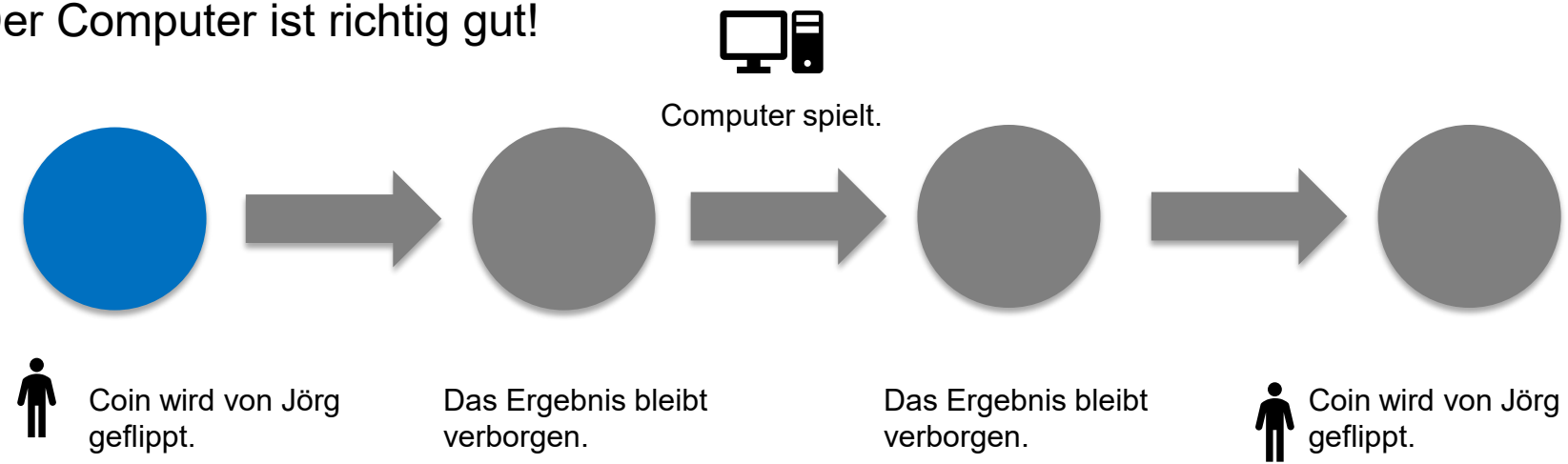


Kryptographie

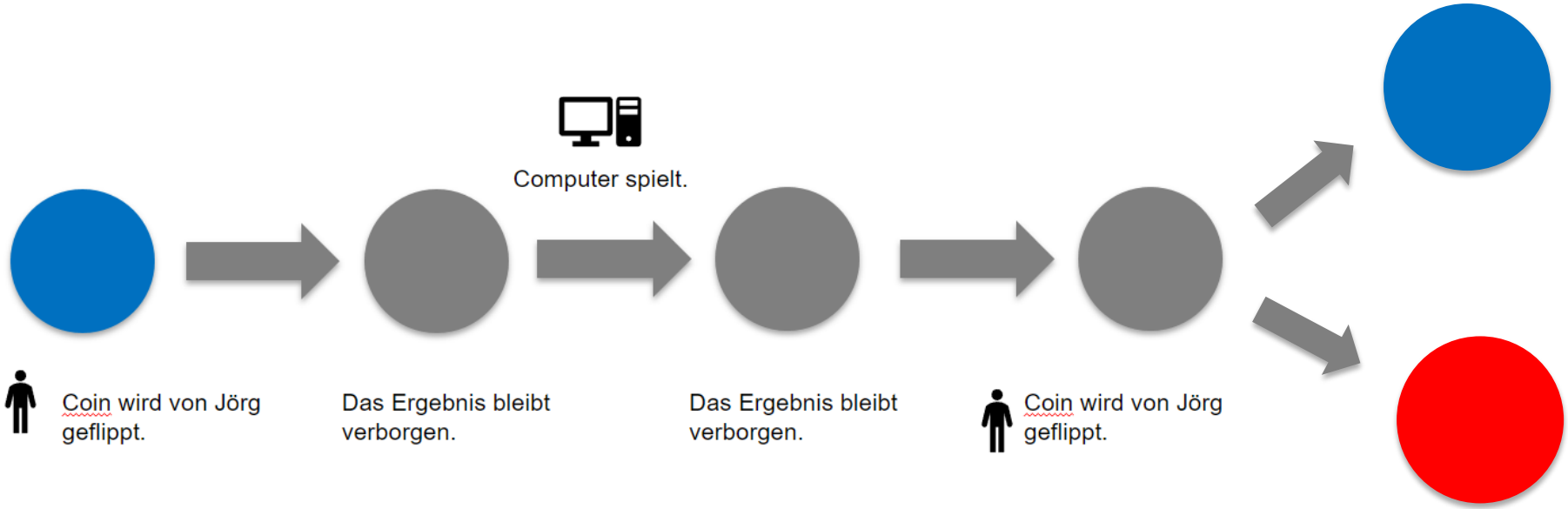
Spielregeln:

Wir spielen gegen einen Computer.

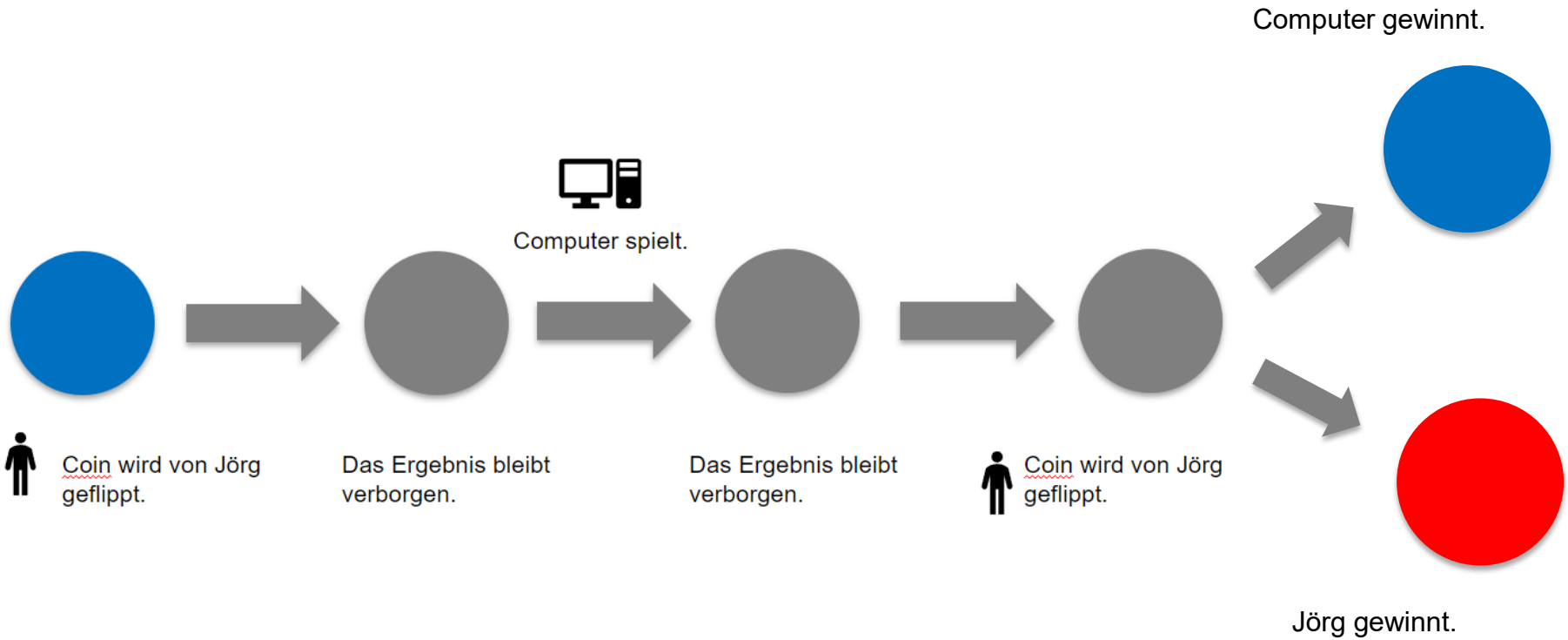
Der Computer ist richtig gut!



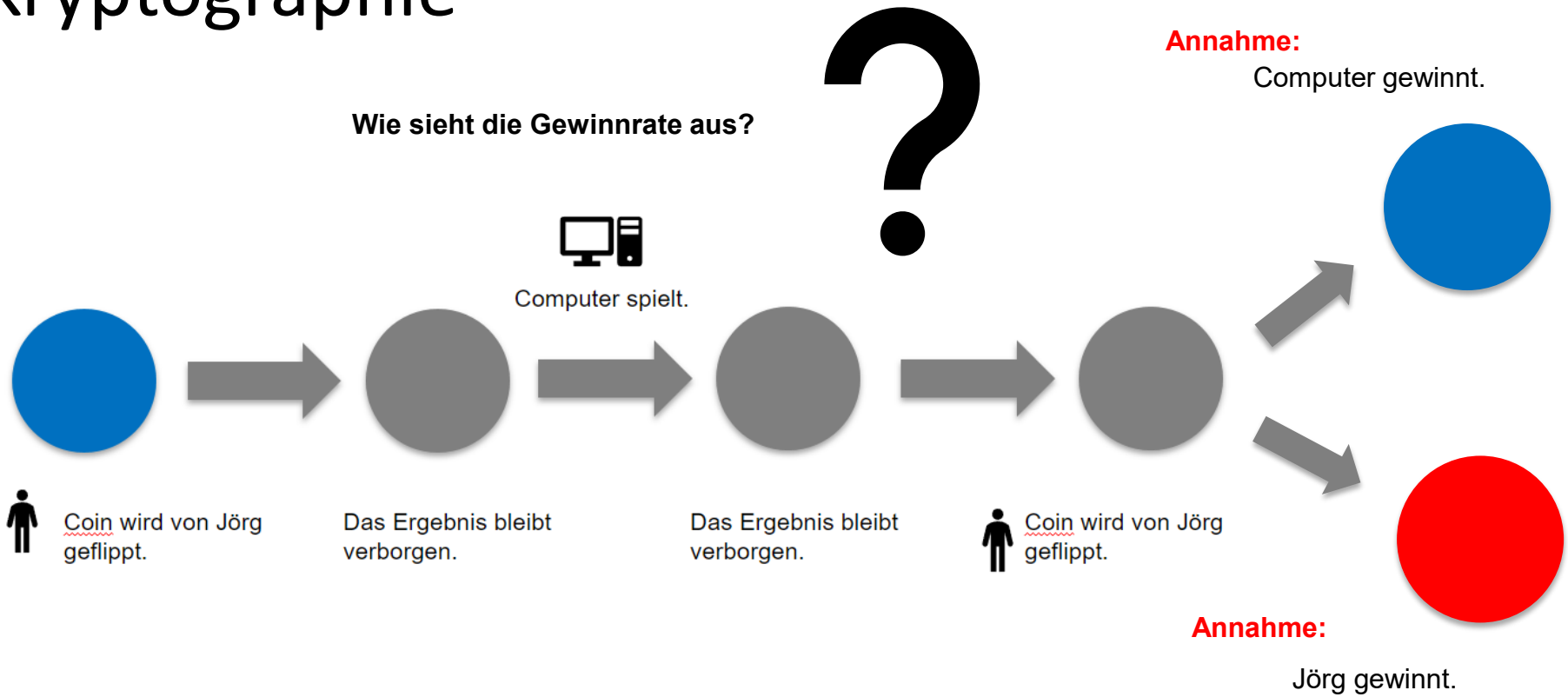
Kryptographie



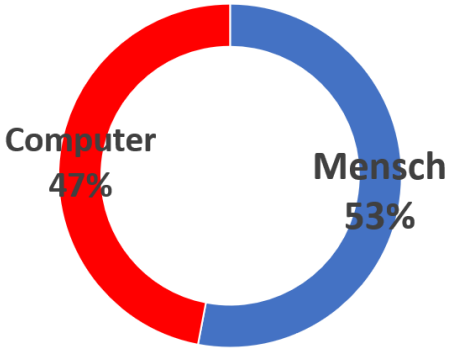
Kryptographie

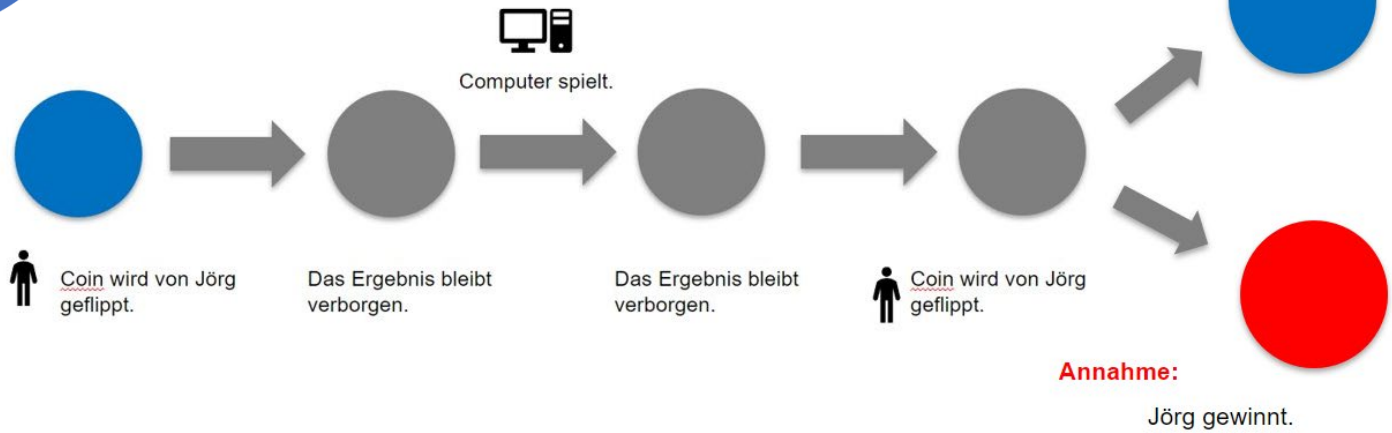


Kryptographie

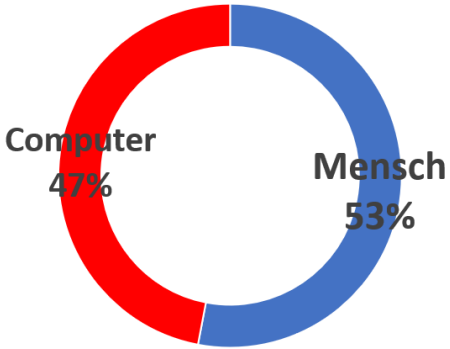


Kryptographie

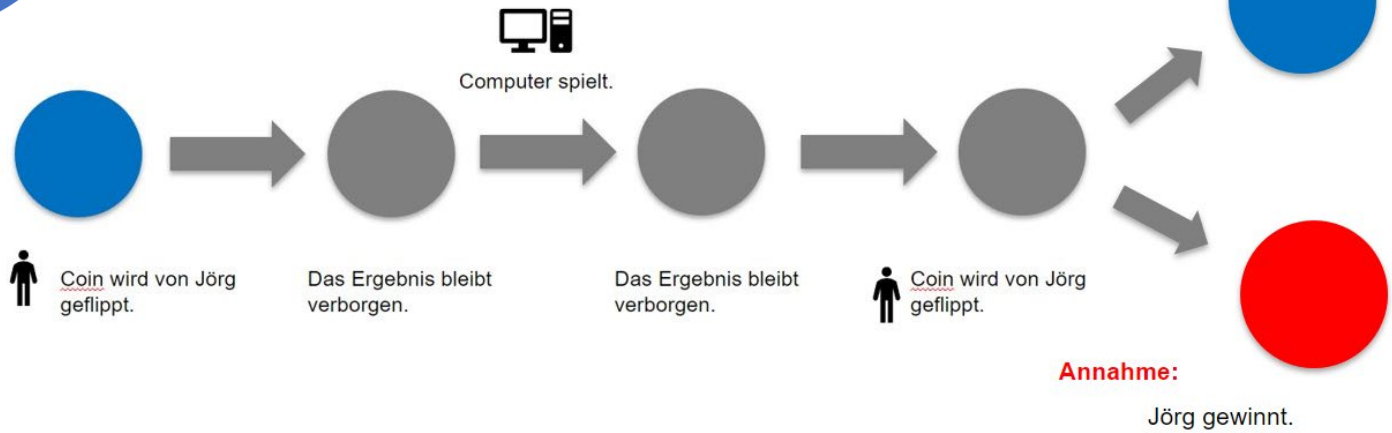




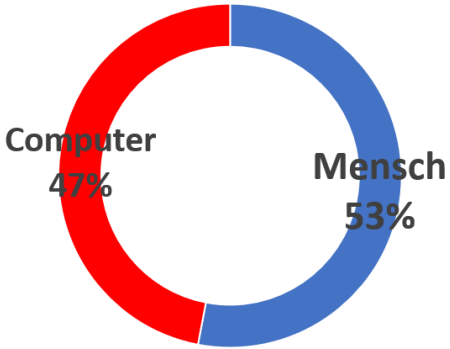
Kryptographie



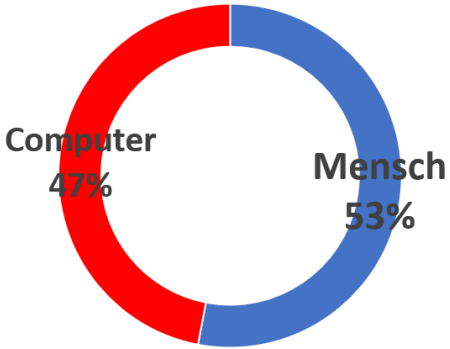
Wir erreichen also einen Wert, der erwartet war.

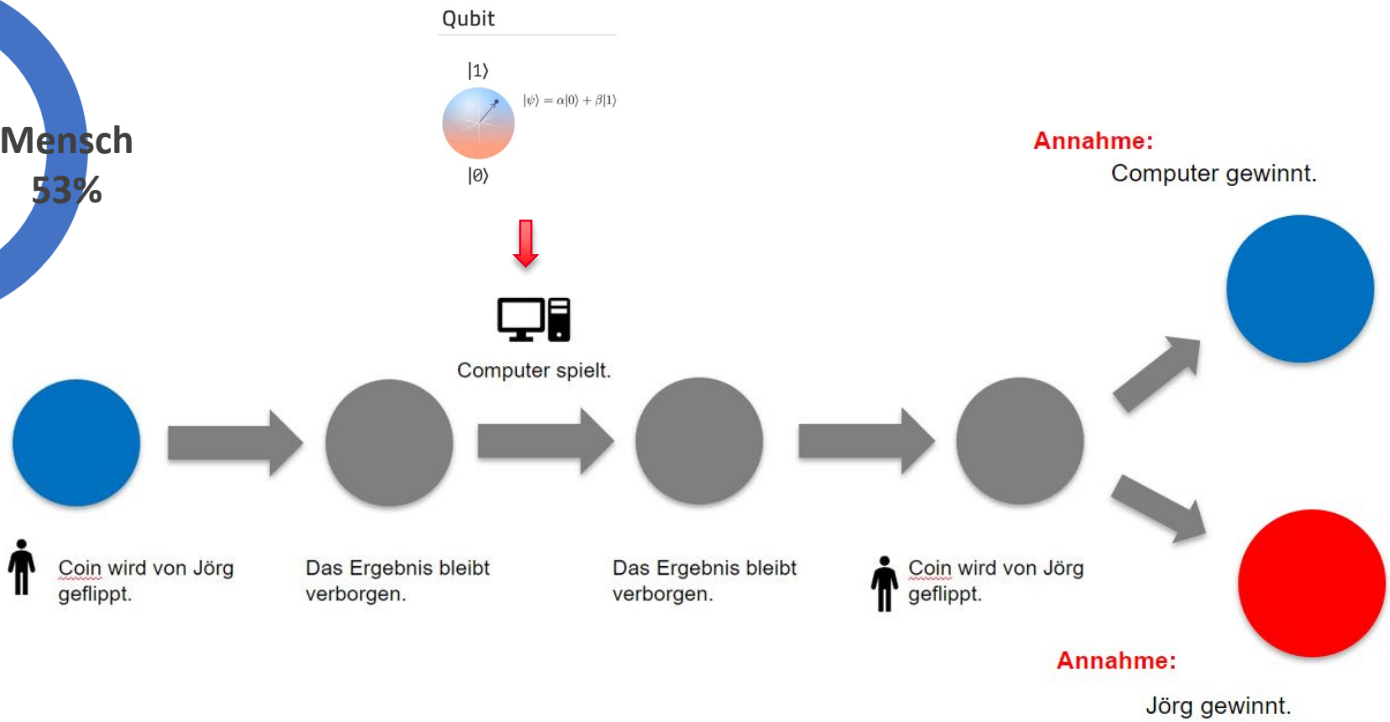


Kryptographie

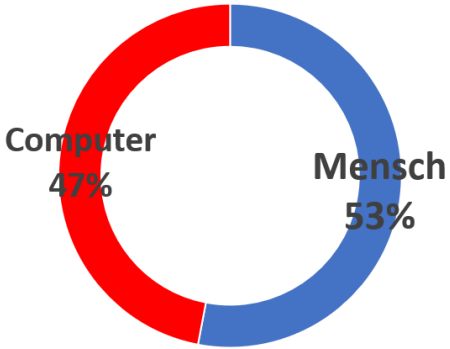


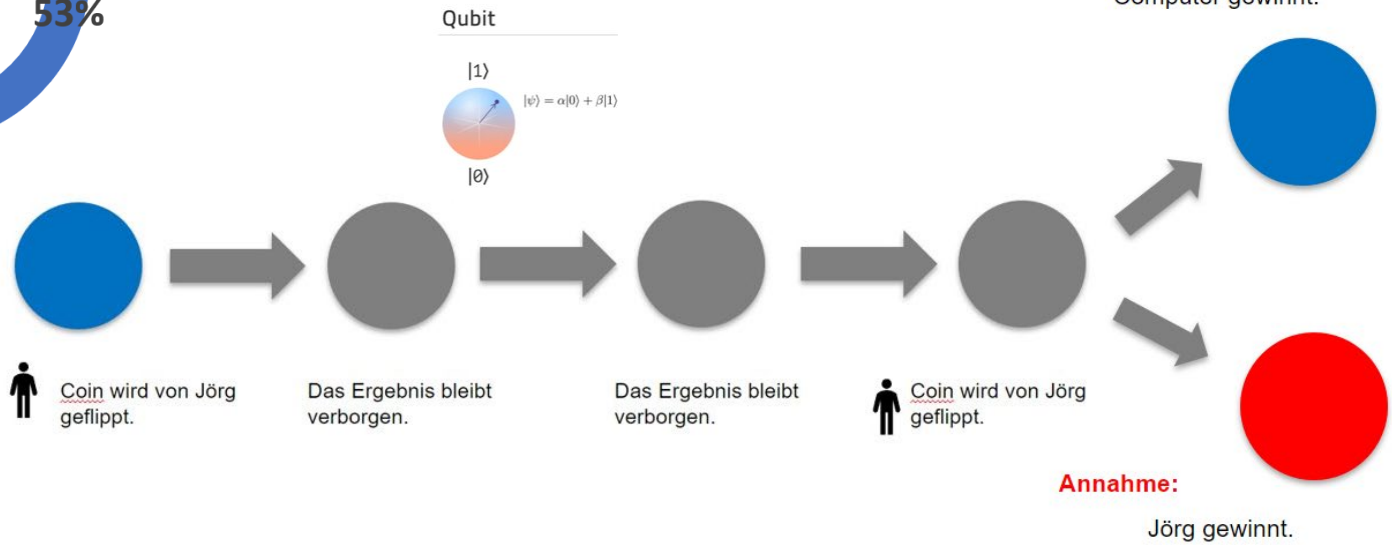
Kryptographie





Kryptographie



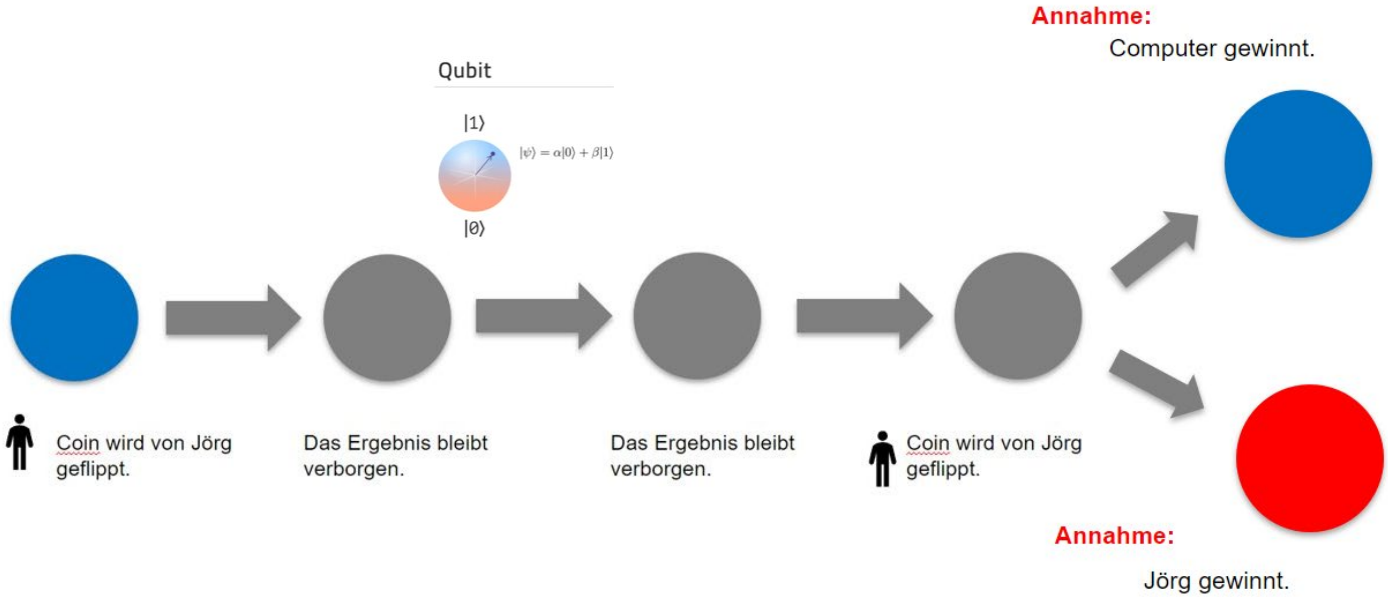


Kryptographie

Start einer Umfrage:

Handzeichen für Blau?

Handzeichen für Rot?

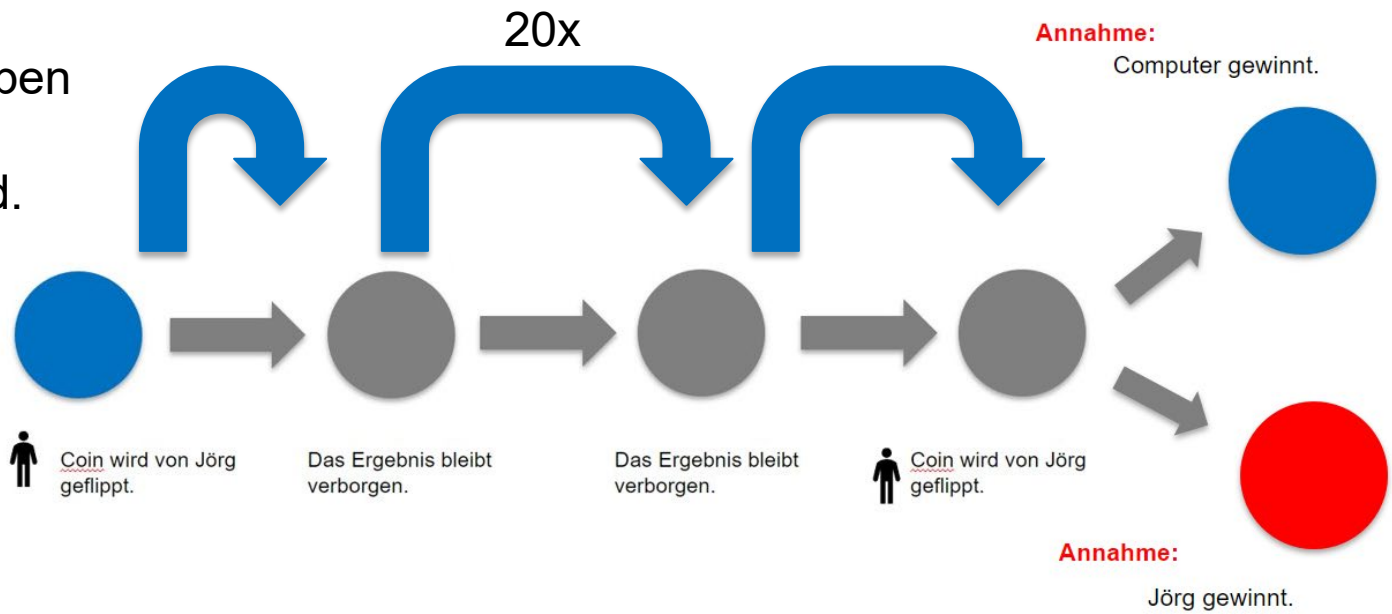


Kryptographie

Start einer Umfrage:

Annahme wir haben 20 flips die auszuführen sind.

Gegen den IBM Quantum Computer

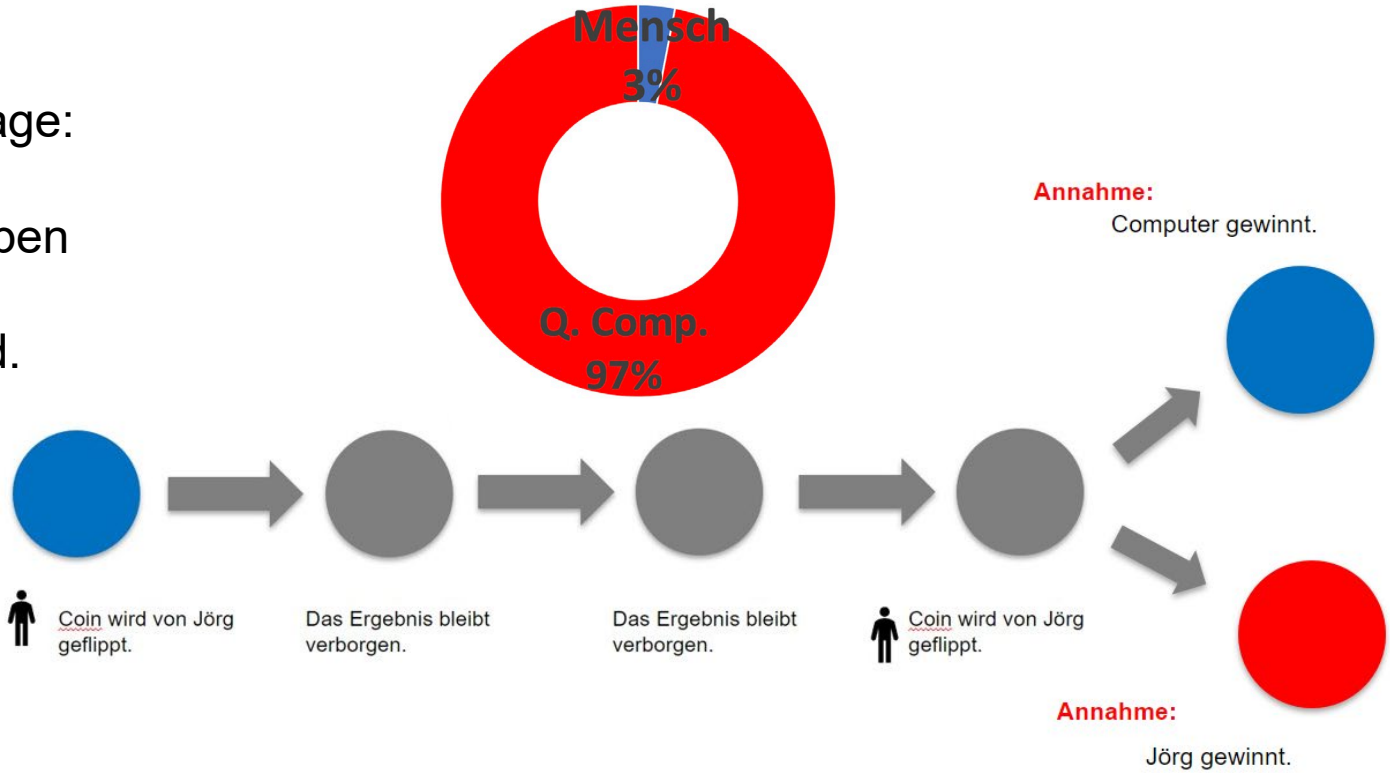


Kryptographie

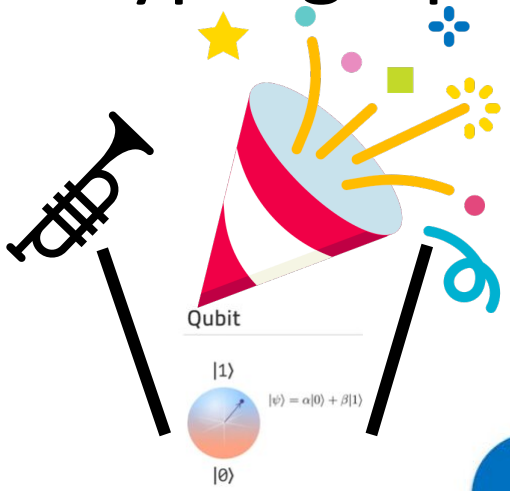
Start einer Umfrage:

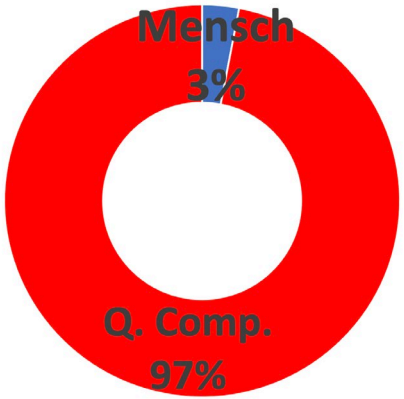
Annahme wir haben 20 flips die auszuführen sind.

Gegen den IBM Quantum Computer



Kryptographie



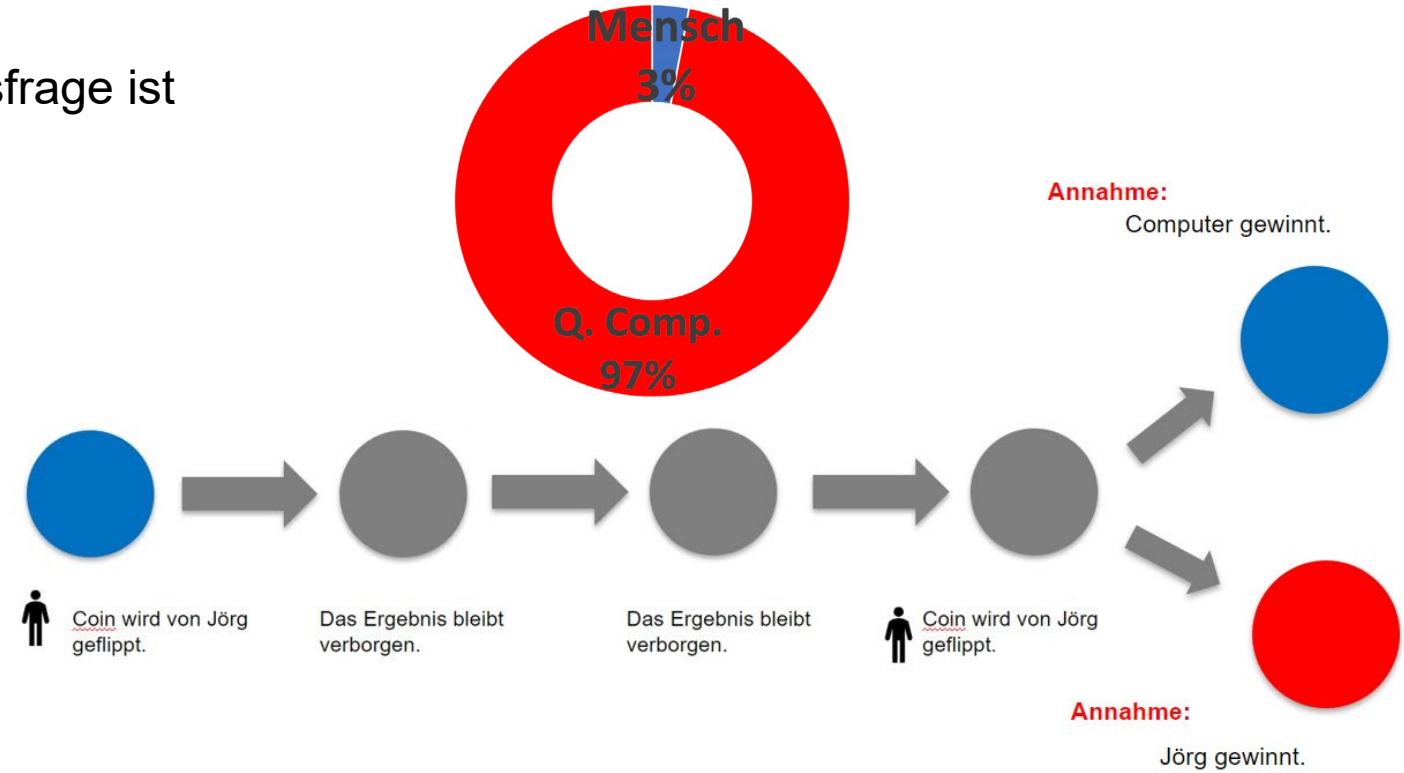


Der Q. Comp. gewinnt mit ordentlich Vorsprung.

Kryptographie

Die Preisfrage ist nun:

Warum?

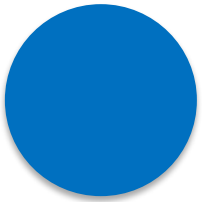


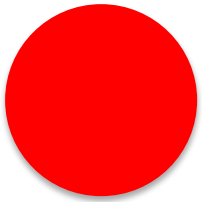
Kryptographie

Die Preisfrage ist nun:

Warum?

Ein Computer codiert den Coin Flip (blau oder rot) in einen Bit.





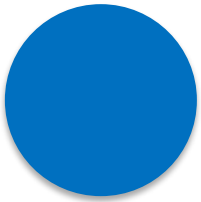
Annahme: 0 1

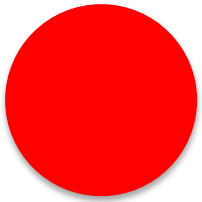
Kryptographie

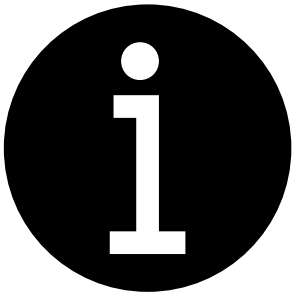
Die Preisfrage ist nun:

Warum?

Ein Computer codiert den Coin Flip (blau oder rot) in einen Bit.

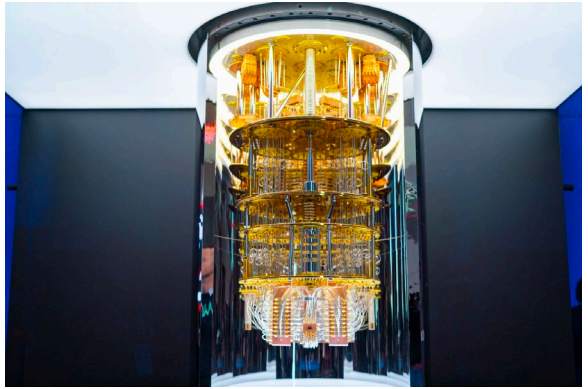






Annahme: 0 1

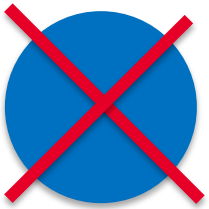
Kryptographie

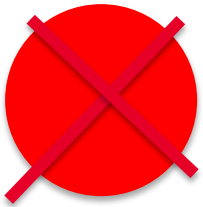


Die Preisfrage ist nun:

Warum?

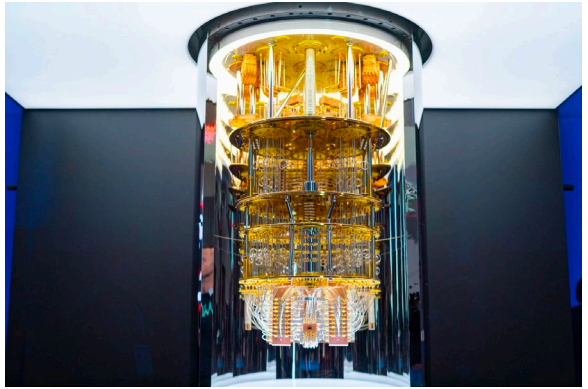
Ein Computer codiert den Coin Flip (blau oder rot) in einen Bit.





Annahme: 0 1

Kryptographie

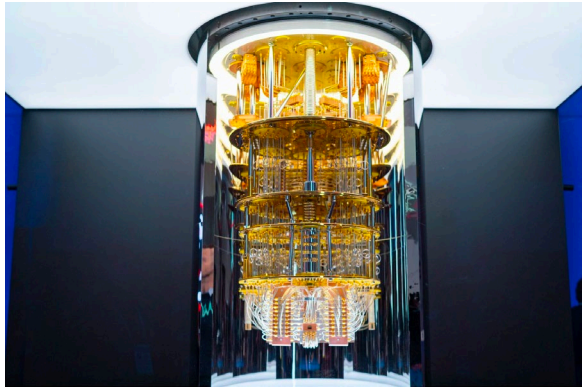


Die Preisfrage ist nun:

Warum?

<u>Ein Quantencomputer codiert in einem fluid</u>.

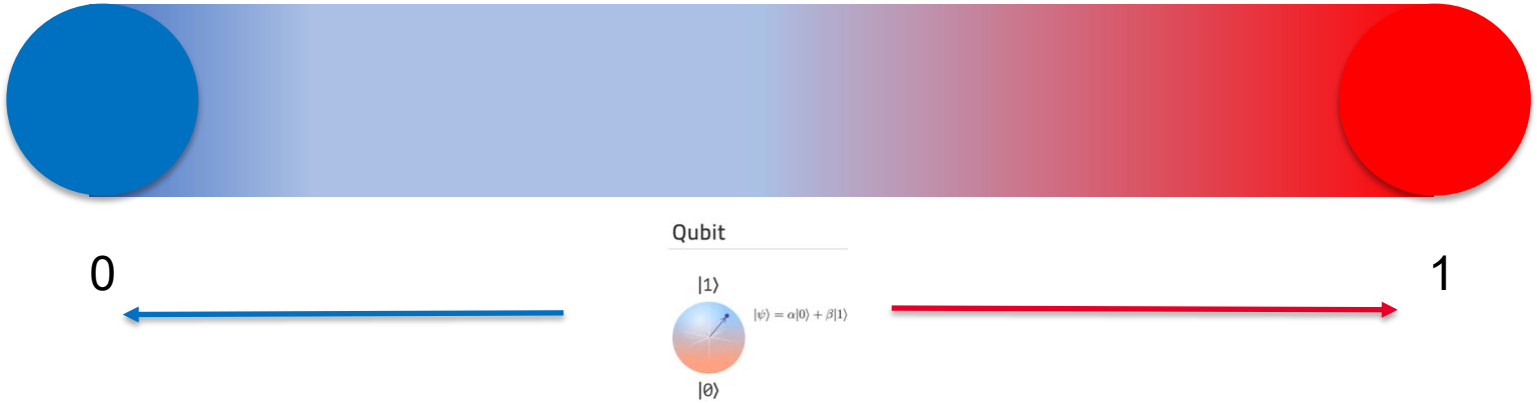
Kryptographie



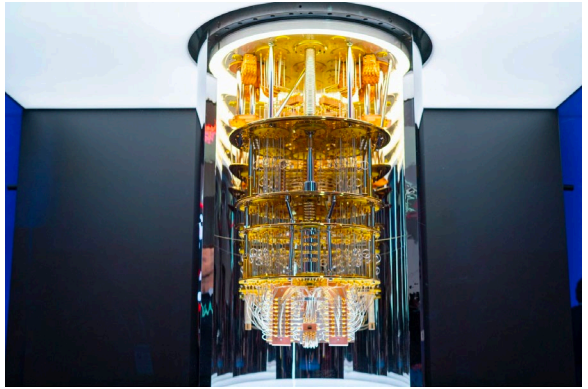
Die Preisfrage ist nun:

Warum?

<u>Ein Quantencomputer codiert in einem fluid</u>.



Kryptographie

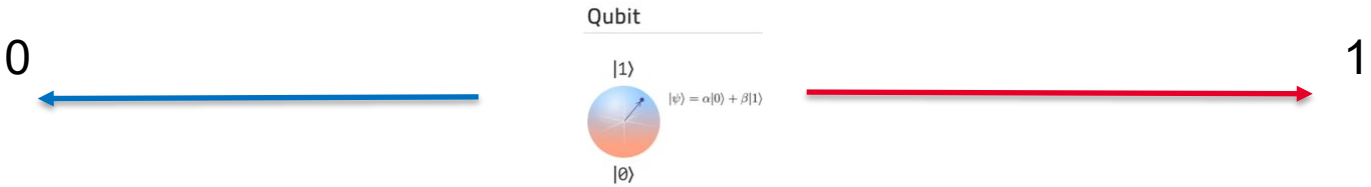


Die Preisfrage ist nun:

Warum?

<u>Ein Quantencomputer codiert in einem fluid</u>.

Ein Qubit ist eine Zustandsfunktion. Sie beschreibt den fluidalen Zustand der Quanten Computer Information.



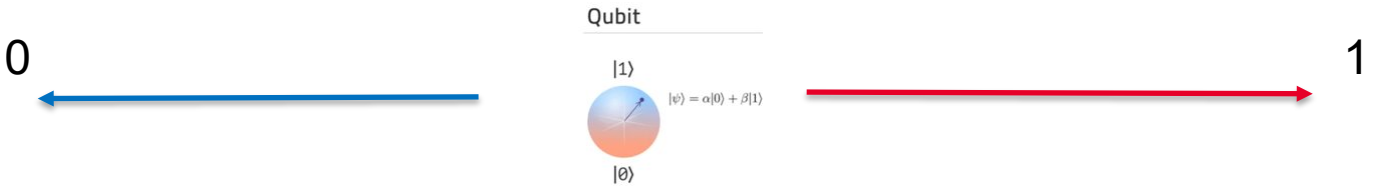
Kryptographie

Die Preisfrage ist nun:

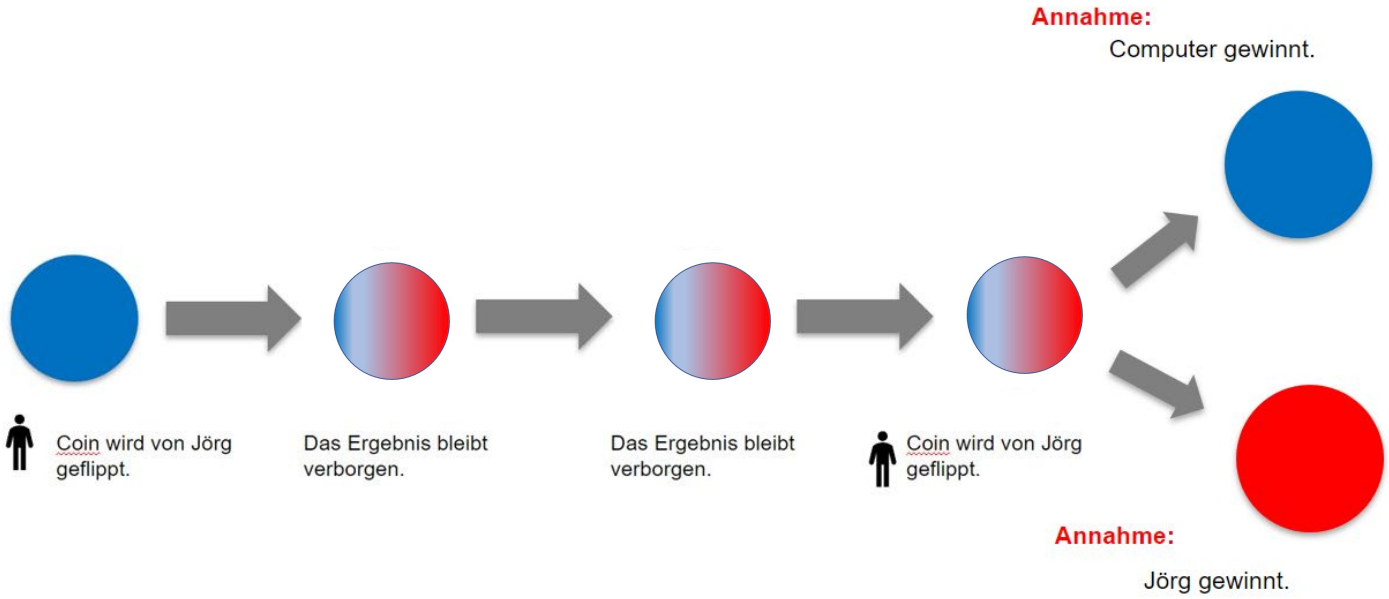
Warum?

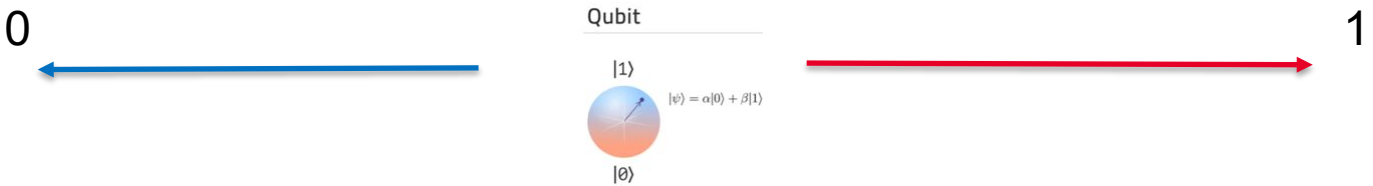
Ein Quantencomputer codiert in einem fluid.

https://www.youtube.com/watch?v=p08_KITKP50&ab_channel=UNMPhysicsandAstronomy

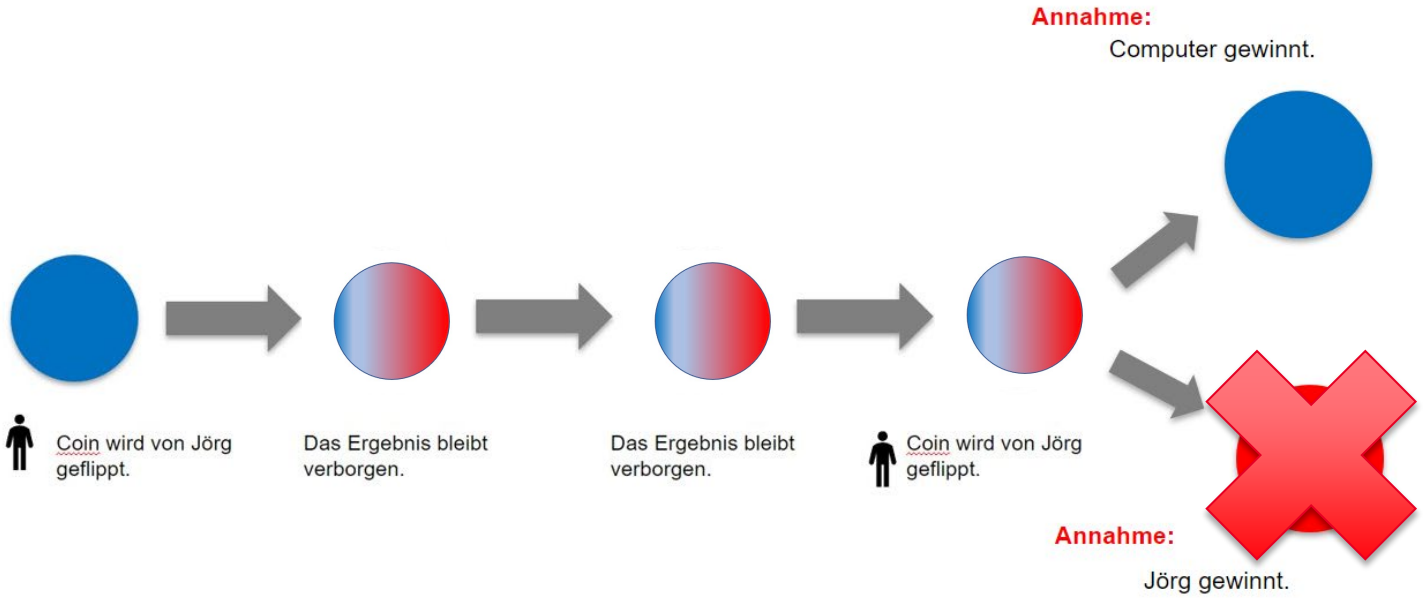


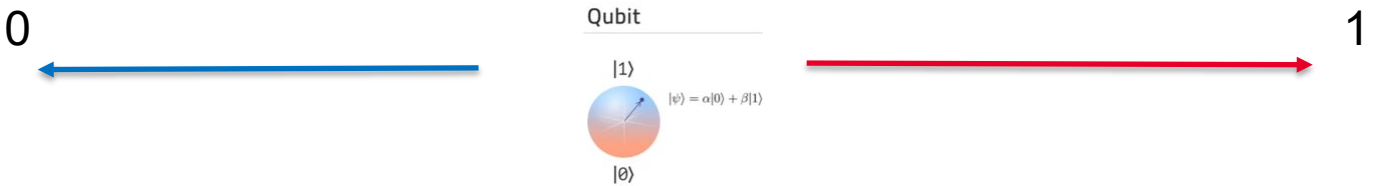
Kryptographie



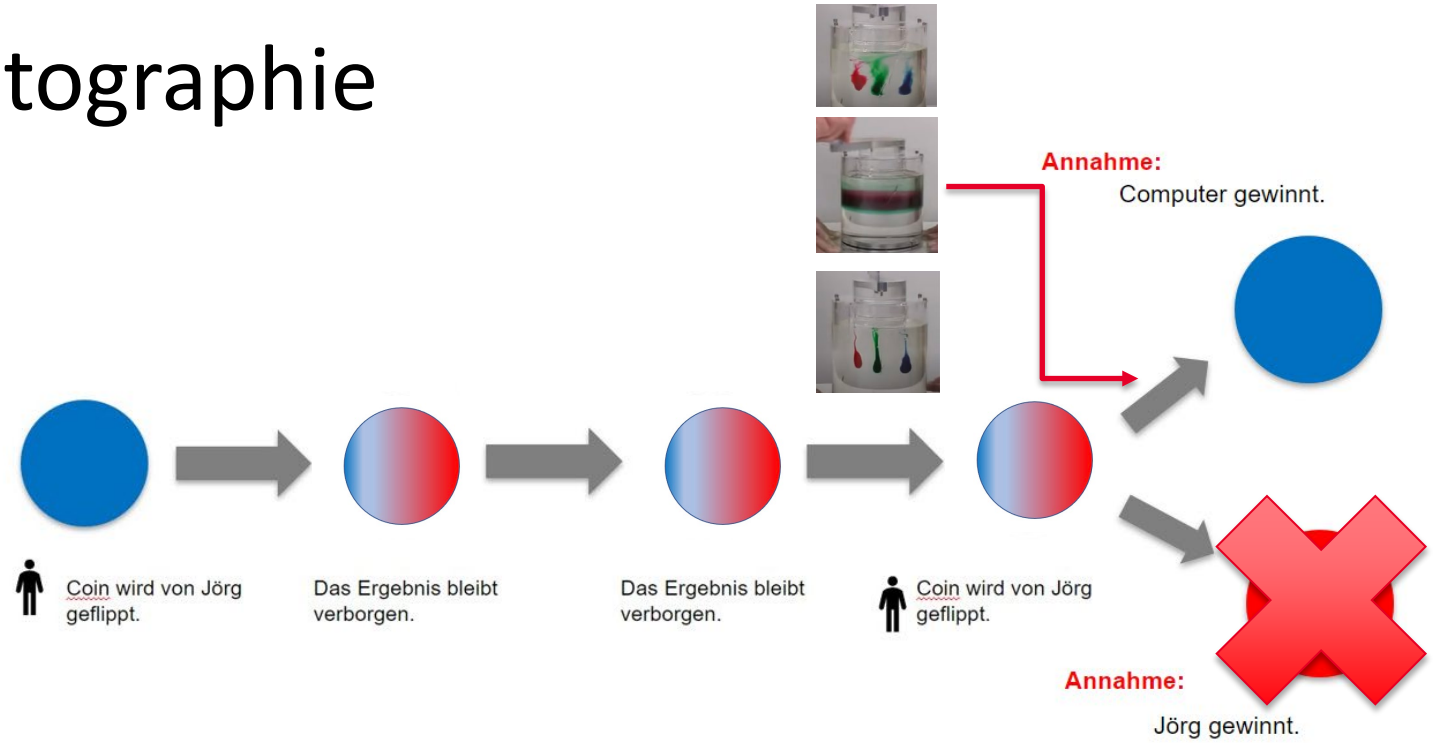


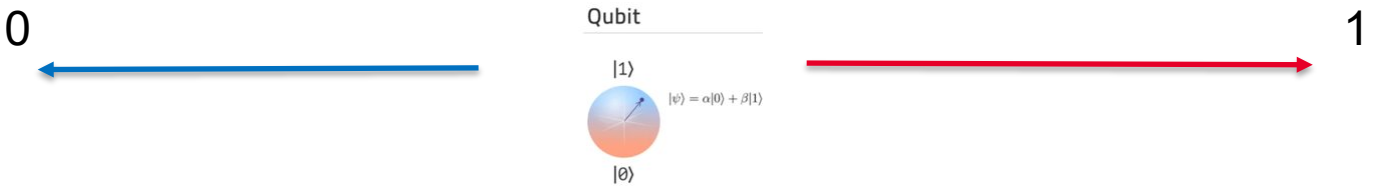
Kryptographie





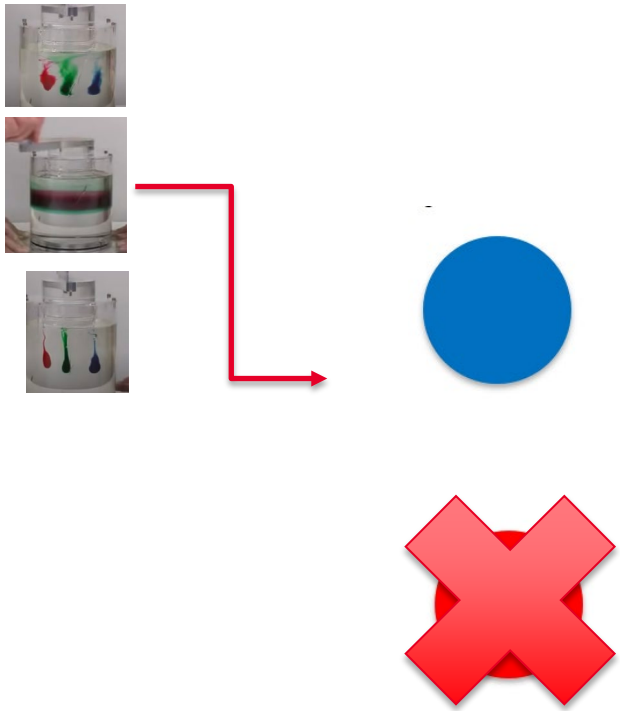
Kryptographie

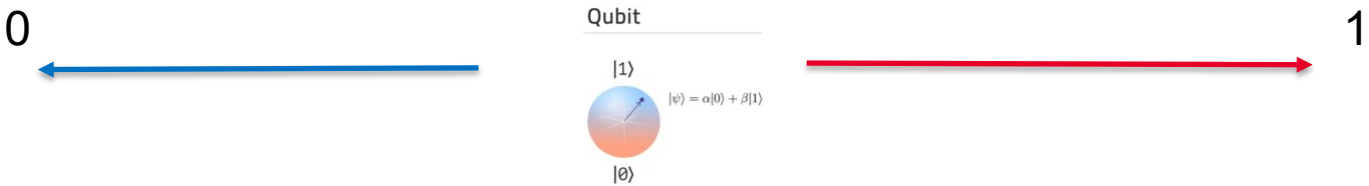




Kryptographie

Der Q. Computer kann sich aus dem fluidalen Zustand, dass richtige aussuchen.





Kryptographie

Ein kurzer Rückblick:

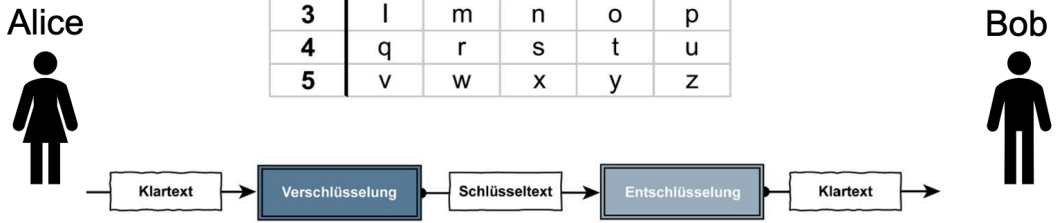
Verschlüsselung durch Substitution

Substitution: vorlesung → 513442311543453322

Was ist der Schlüssel?

$$E : A_1^1 \rightarrow A_2^2$$

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z



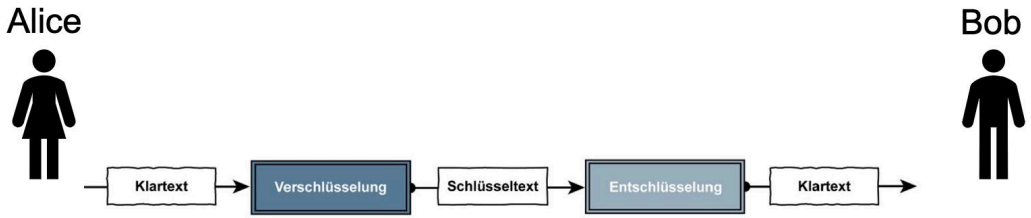
Kryptographie

Ein kurzer Rückblick:

Verschlüsselung durch Substitution

Permutation: $f : A^n \rightarrow A^n$ $\quad A_1 = A_2 = \{a, b, ..., z\}$

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
N	E	W	Y	O	R	K	A	B	C	D	F	G	H	I	J	L	M	P	Q	S	T	U	V	X	Z



Kryptographie

Ein kurzer Rückblick:

Funktion **Permutation:** $f : A^n \rightarrow A^n$ $\quad A_1 = A_2 = \{a, b, ..., z\}$

Kryptographie

Ein kurzer Rückblick:

Funktion **Permutation:** $f : A^n \rightarrow A^n$ $\quad A_1 = A_2 = \{a, b, ..., z\}$

Eine Funktion sollte möglichst irreversibel sein. Und nur mit dem Schlüssel umkehrbar sein.

Kryptographie

Ein kurzer Rückblick:

Funktion **Permutation:** $f : A^n \rightarrow A^n$ $\quad A_1 = A_2 = \{a, b, ..., z\}$

Eine Funktion sollte möglichst irreversibel sein. Und nur mit dem Schlüssel umkehrbar sein.

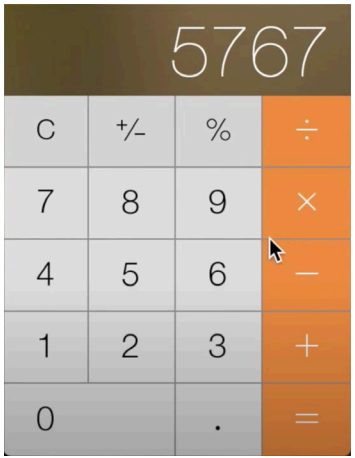
Beispiel: Multiplikation von Primzahlen.

Kryptographie

Beispiel: Multiplikation von Primzahlen.

Multiplikation von

79 x 73

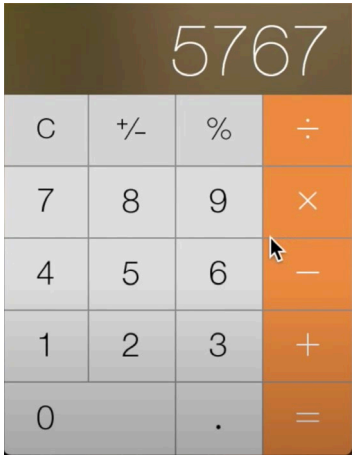


Kryptographie

Beispiel: Multiplikation von Primzahlen.

Multiplikation von

79 x 73



Wir wollen diesen Code knacken. Durch ausprobieren.

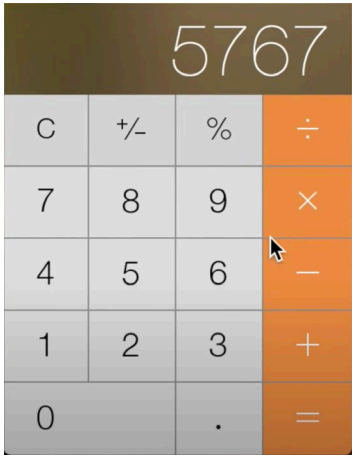
5767 / 2 =

Kryptographie

Beispiel: Multiplikation von Primzahlen.

Multiplikation von

79 x 73



Wir brauchen mehr als eine Rechenoperation.

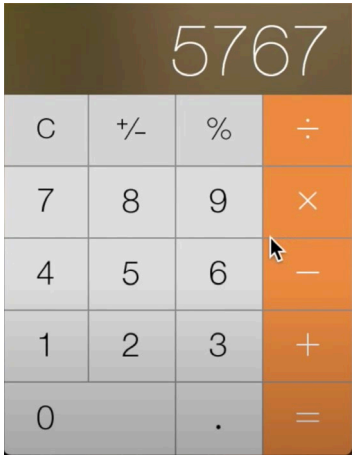
5767 / 2 =

Kryptographie

Beispiel: Multiplikation von Primzahlen.

Multiplikation von

79 x 73



Wir brauchen mehr als eine Rechenoperation.

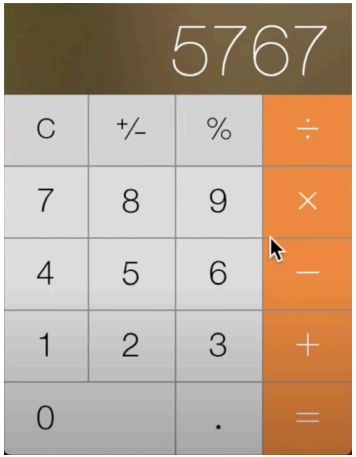
5767 / 2 =

Kryptographie

Beispiel: Multiplikation von Primzahlen.

Multiplikation von

79 x 73



Wir brauchen mehr als eine Rechenoperation.

5767 / 2 =

Wir brauchen also ganz schön viele Versuche und Tippvorgänge.

Kryptographie

Beispiel: Multiplikation von Primzahlen.

Was ist die größte Primzahl die nachgewiesen werden kann?

Kryptographie

Beispiel: Multiplikation von Primzahlen.

Was ist die größte Primzahl die nachgewiesen werden kann?

148894445742041325547806458472397916603026273992795324185271289425213239361064475310309971132180337174752834401423587560 ...

(24,861,808 digits skipped)

... 06210755794795829753159520880719269367652178218447252664007691211435530831196948763376645782369507403795121032521790259[6]

Kryptographie

Beispiel: Multiplikation von Primzahlen.

Was ist die größte Primzahl die nachgewiesen werden kann?

Rank	Number	Discovered	Digits	Form	Ref
1	$2^{82589933} - 1$	2018-12-07	24,862,048	Mersenne	[1]
2	$2^{77232917} - 1$	2017-12-26	23,249,425	Mersenne	[18]
3	$2^{74207281} - 1$	2016-01-07	22,338,618	Mersenne	[19]
4	$2^{57885161} - 1$	2013-01-25	17,425,170	Mersenne	[20]
5	$2^{43112609} - 1$	2008-08-23	12,978,189	Mersenne	[21]
6	$2^{42643801} - 1$	2009-06-04	12,837,064	Mersenne	[22]
7	$2^{37156667} - 1$	2008-09-06	11,185,272	Mersenne	[21]
8	$2^{32582657} - 1$	2006-09-04	9,808,358	Mersenne	[23]
9	$10223 \times 2^{31172165} + 1$	2016-10-31	9,383,761	Proth	[24]
10	$2^{30402457} - 1$	2005-12-15	9,152,052	Mersenne	[25]
11	$2^{25964951} - 1$	2005-02-18	7,816,230	Mersenne	[26]
12	$2^{24036583} - 1$	2004-05-15	7,235,733	Mersenne	[27]
13	$1963736^{1048576} + 1$	2022-09-24	6,598,776	Generalized Fermat	[28]
14	$1951734^{1048576} + 1$	2022-08-09	6,595,985	Generalized Fermat	[29]
15	$202705 \times 2^{21320516} + 1$	2021-12-01	6,418,121	Proth	[30]
16	$2^{20996011} - 1$	2003-11-17	6,320,430	Mersenne	[31]
17	$1059094^{1048576} + 1$	2018-10-31	6,317,602	Generalized Fermat	[32]
18	$919444^{1048576} + 1$	2017-08-29	6,253,210	Generalized Fermat	[33]
19	$7 \times 2^{20267500} + 1$	2022-07-21	6,101,127	Proth	[34]
20	$168451 \times 2^{19375200} + 1$	2017-09-17	5,832,522	Proth	[35]

Kryptographie

Beispiel: Multiplikation von Primzahlen.

Was ist die größte Primzahl die nachgewiesen werden kann?

Rank	Number	Discovered	Digits	Form	Ref
1	$2^{82589933} - 1$	2018-12-07	24,862,048	Mersenne	[1]
2	$2^{77232917} - 1$	2017-12-26	23,249,425	Mersenne	[18]

Kryptographie

Beispiel: Multiplikation von Primzahlen.

Was ist die größte Primzahl die nachgewiesen werden kann?

Rank	Number	Discovered	Digits	Form	Ref
1	$2^{82589933} - 1$	2018-12-07	24,862,048	Mersenne	[1]
2	$2^{77232917} - 1$	2017-12-26	23,249,425	Mersenne	[18]

Multiplikation

Rank 1 x Rank 2

Kryptographie

Beispiel: Multiplikation von Primzahlen.

Was ist die größte Primzahl die nachgewiesen werden kann?

Rank	Number	Discovered	Digits	Form	Ref
1	$2^{82589933} - 1$	2018-12-07	24,862,048	Mersenne	[1]
2	$2^{77232917} - 1$	2017-12-26	23,249,425	Mersenne	[18]

Multiplikation

Rank 1 x Rank 2

Kryptographie

Beispiel: Multiplikation von Primzahlen.

Substitution: vorlesung → 513442311543453322

Kryptographie

Beispiel: Multiplikation von Primzahlen.

Substitution: vorlesung

v	o	r	l	e	s	u	n	g	_	!						
5	8	12	15	87	55	21	32	73	52	44	✖	11	✖	13	〓	β

Kryptographie

Beispiel: Multiplikation von Primzahlen.

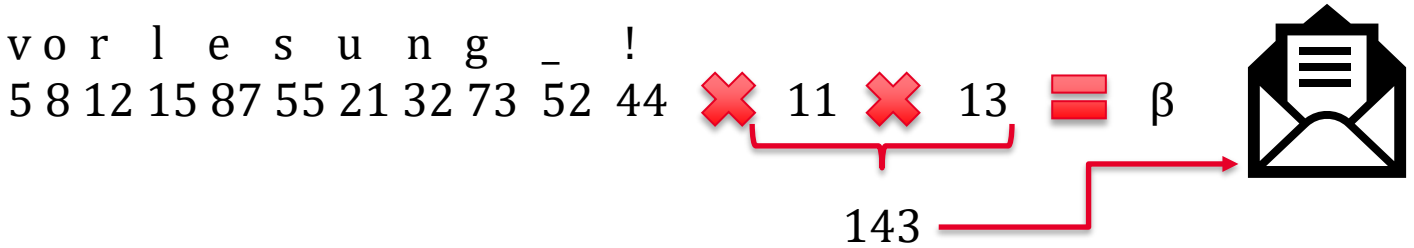
Substitution: vorlesung

v o r l e s u n g _ !
5 8 12 15 87 55 21 32 73 52 44 ✖ 11 ✖ 13 = β

Kryptographie

Beispiel: Multiplikation von Primzahlen.

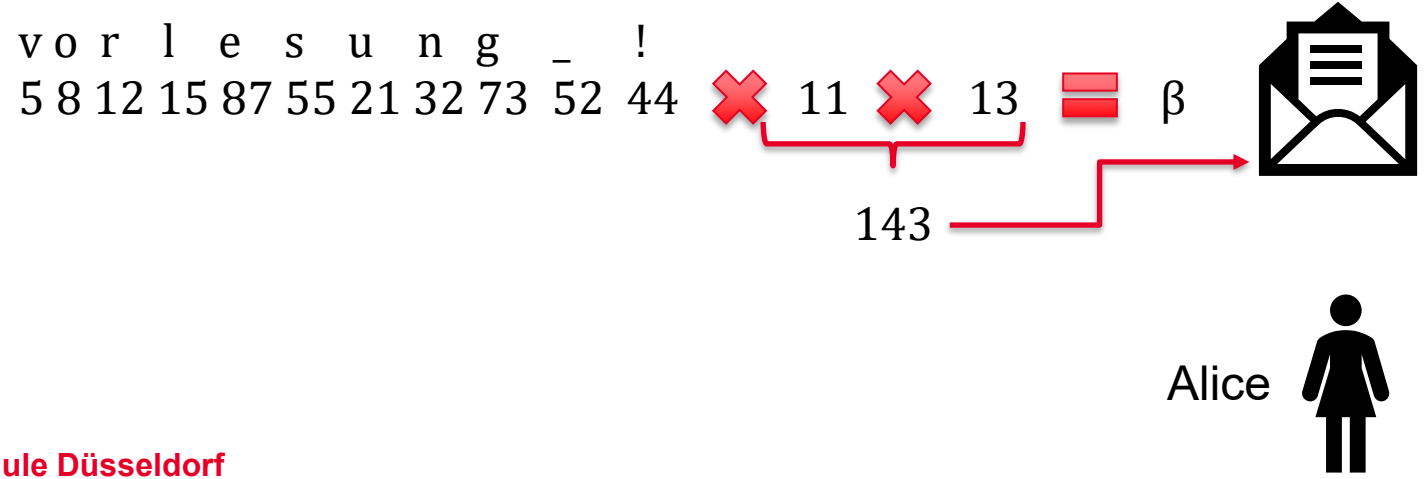
Substitution: vorlesung



Kryptographie

Beispiel: Multiplikation von Primzahlen.

Substitution: vorlesung

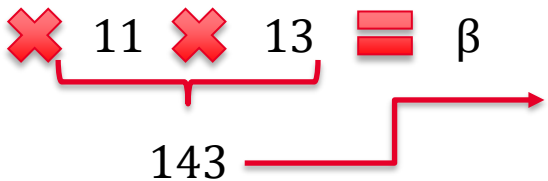


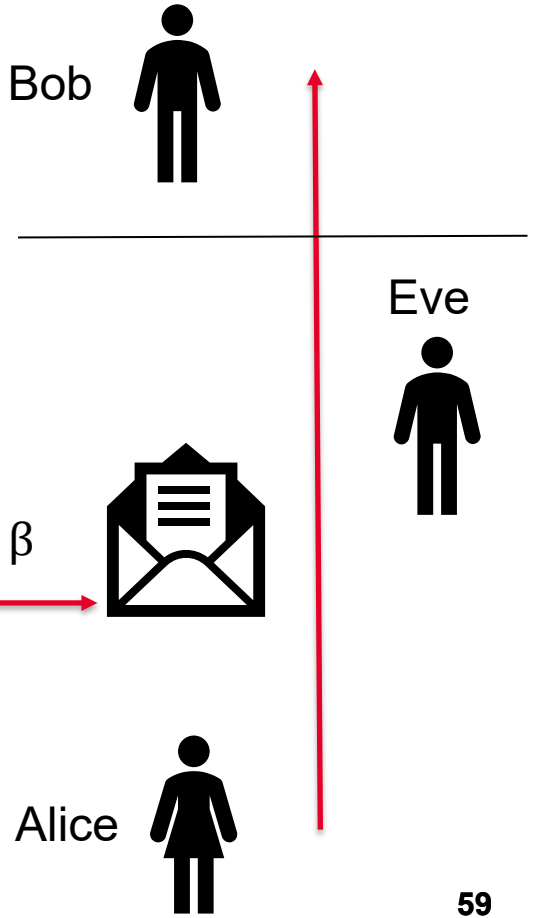
Kryptographie

Beispiel: Multiplikation von Primzahlen.

Substitution: vorlesung

v	o	r	l	e	s	u	n	g	_	!
5	8	12	15	87	55	21	32	73	52	44



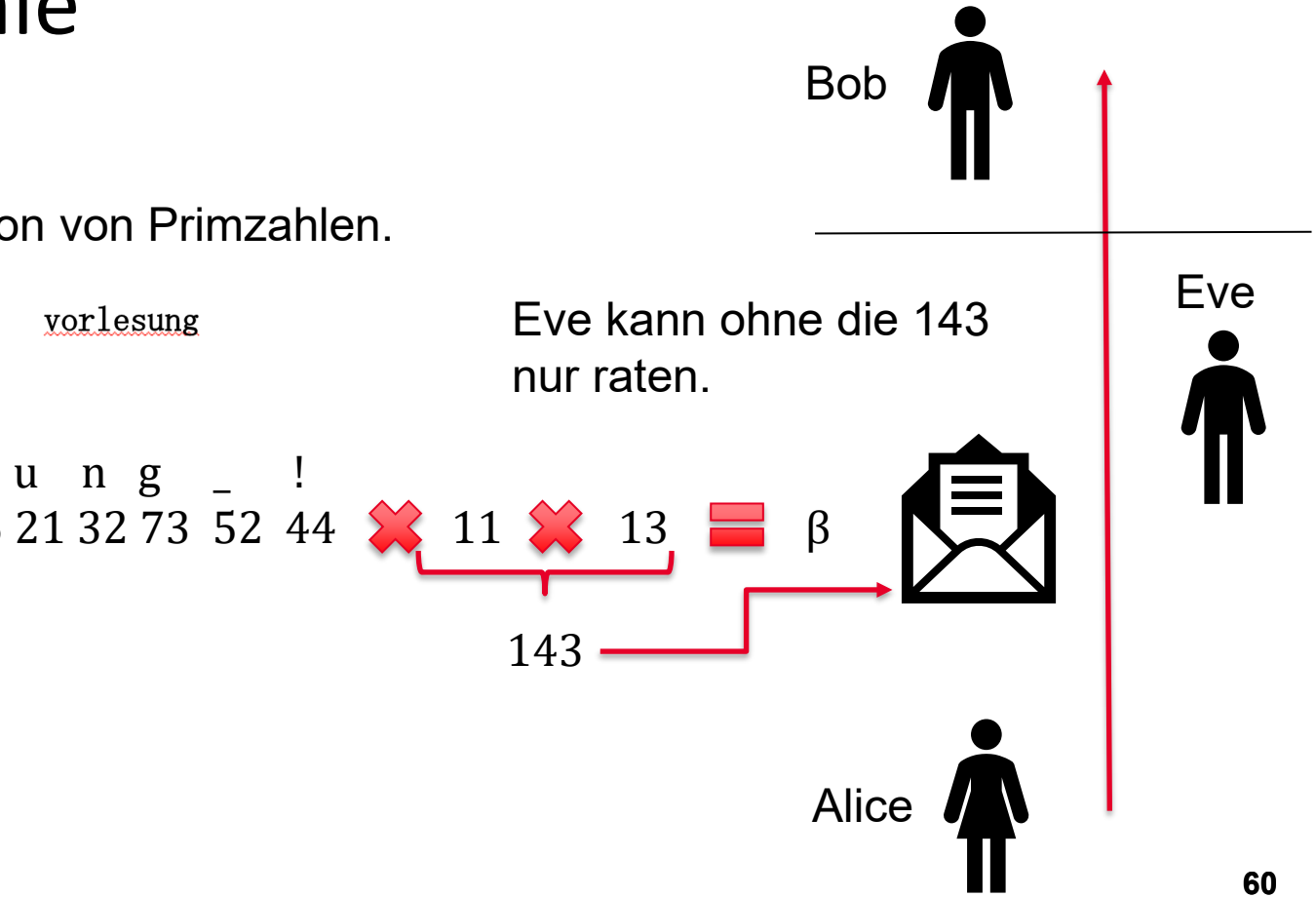


Kryptographie

Beispiel: Multiplikation von Primzahlen.

Substitution: vorlesung

Eve kann ohne die 143 nur raten.



Kryptographie

Beispiel: Multiplikation von Primzahlen.

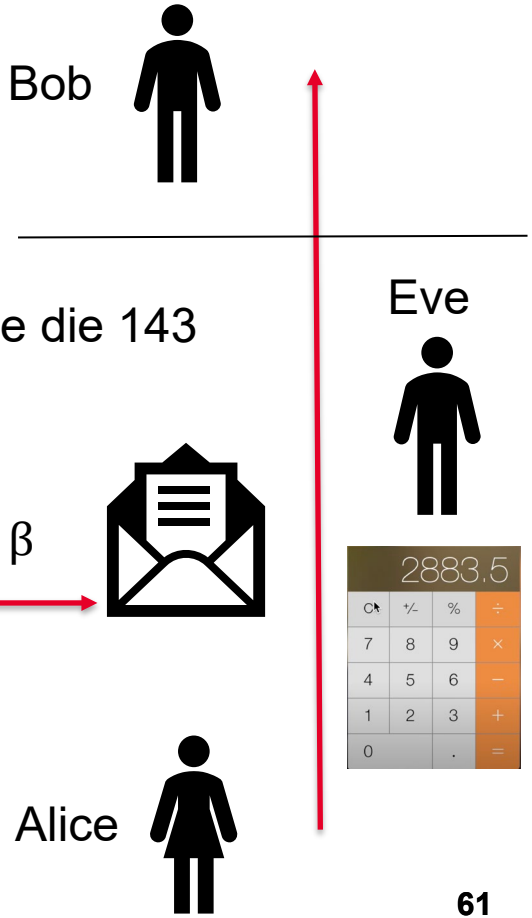
Substitution: vorlesung

v o r l e s u n g _ !
5 8 12 15 87 55 21 32 73 52 44

11 × 13 = β

143

Eve kann ohne die 143 nur raten.

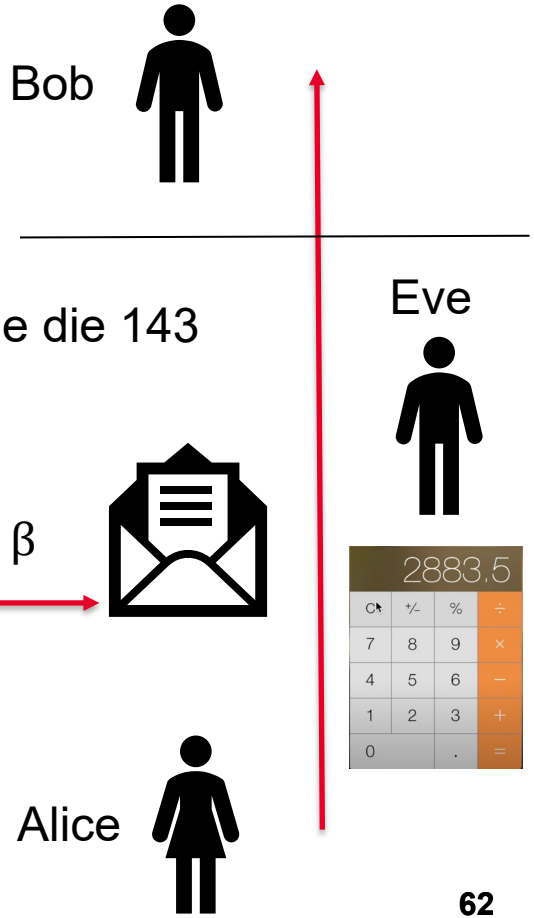


Kryptographie

Beispiel: Multiplikation von Primzahlen.

Substitution: vorlesung

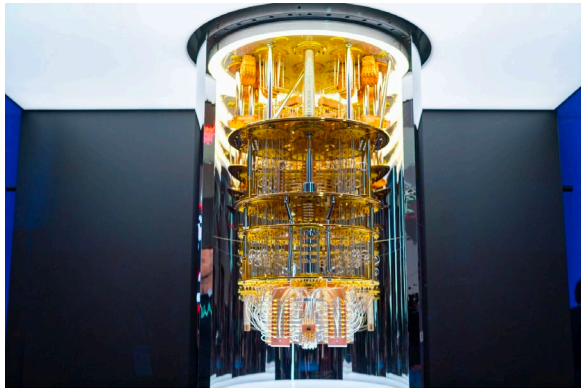
v o r l e s u n g _ !
5 8 12 15 87 55 21 32 73 52 44 ✖ 11 ✖ 13 = β

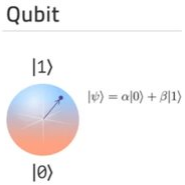


Eve kann ohne die 143 nur raten.

Rank	Number	Discovered	Digits	Form	Re
1	$2^{82589933} - 1$	2018-12-07	24,862,048	Mersenne	[1]
2	$2^{77232917} - 1$	2017-12-26	23,249,425	Mersenne	[18]

Kryptographie

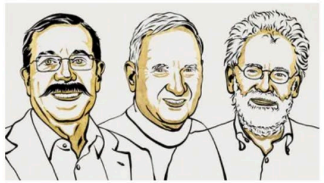




Kryptographie

Mindmap

Vorlesung 1



Nobelpreis

Physik-Nobelpreis geht an drei Quantenforscher

Alain Aspect, John F. Clauser und Anton Zeilinger werden für ihre Forschung in der Quantenphysik ausgezeichnet. Ihre Arbeit ist die Basis für ganz neue Technologien.

Vor 1 Tag • 189 Kommentare

Mr. Beam

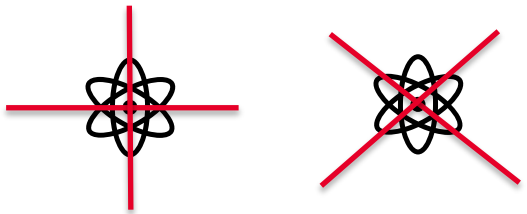
- Blockchain
- Klassische Verfahren
- Quanten Computer
- Vergleiche zu anderen Hochschulen

Kryptographie

Kryptographie

Kryptographie

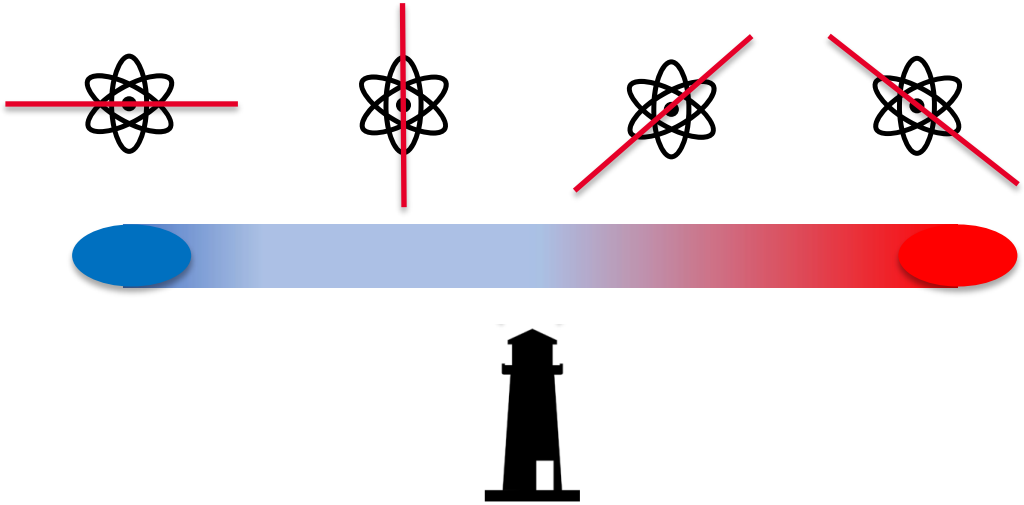
Kryptographie



Alice

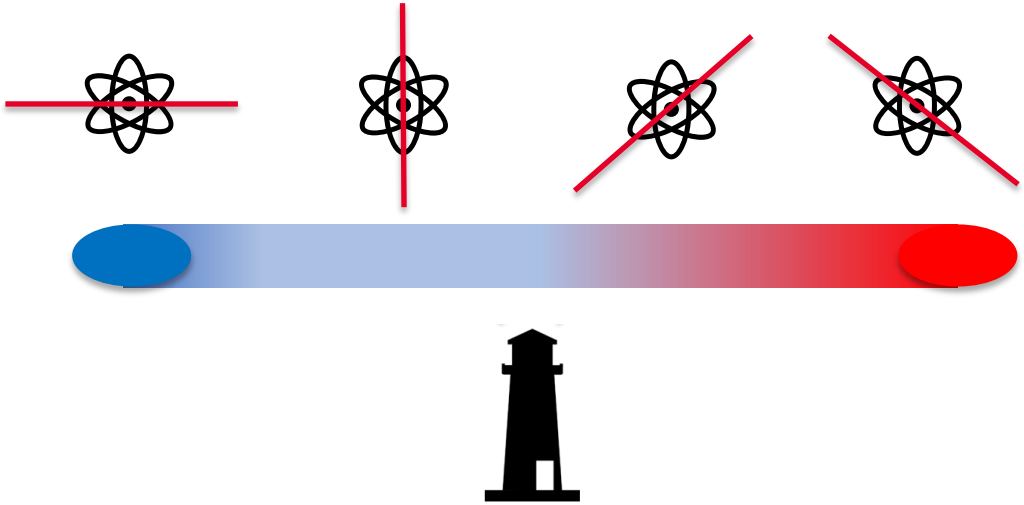
Bob

Kryptographie



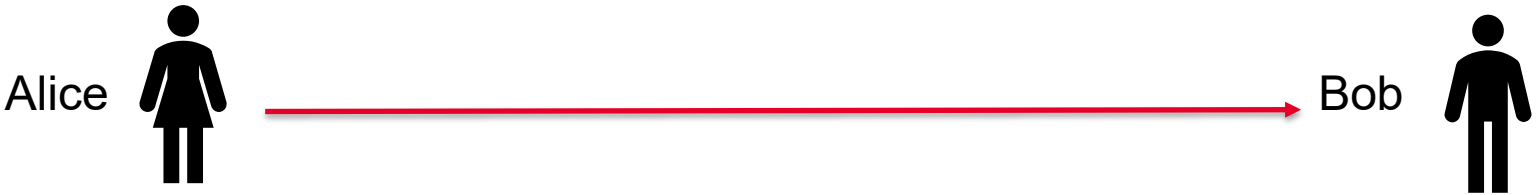
Alice darf sich einen dieser Zustände aussuchen.

Kryptographie



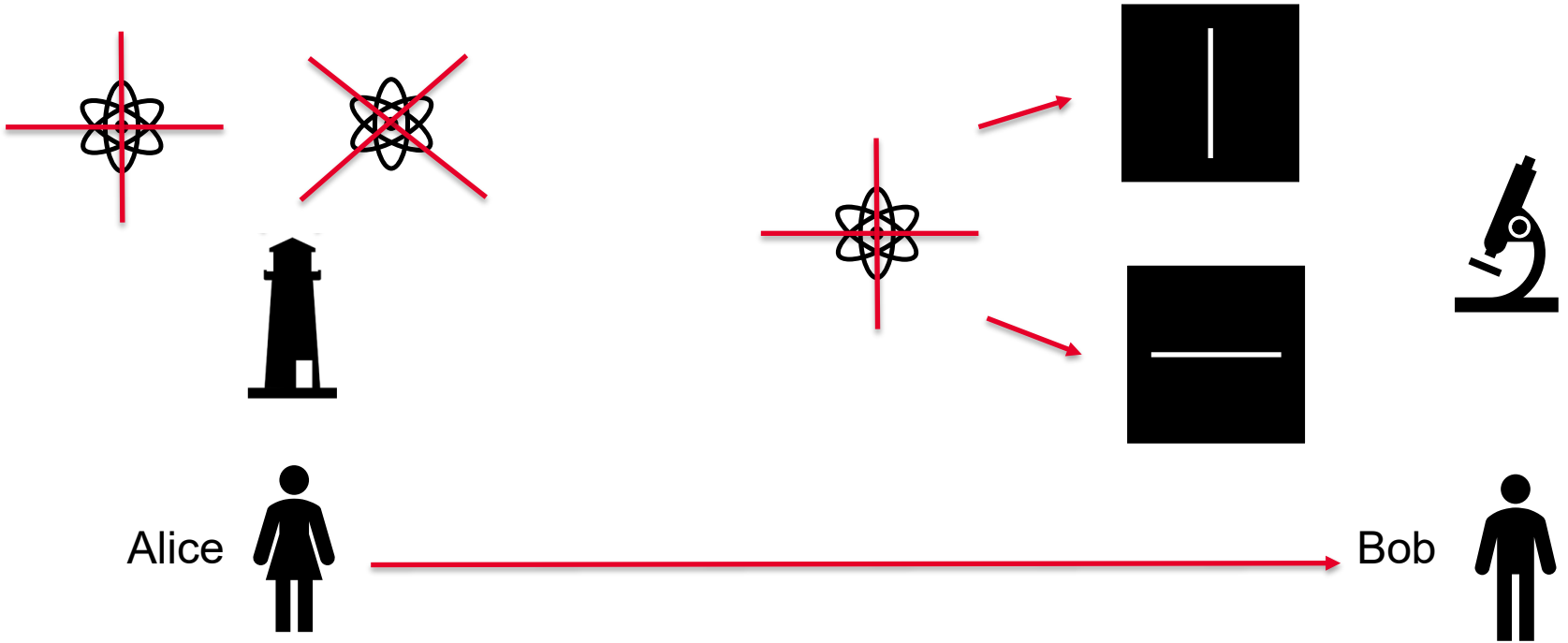
Alice darf sich einen dieser Zustände aussuchen.

Bob muss diesen versuchen zu detektieren.

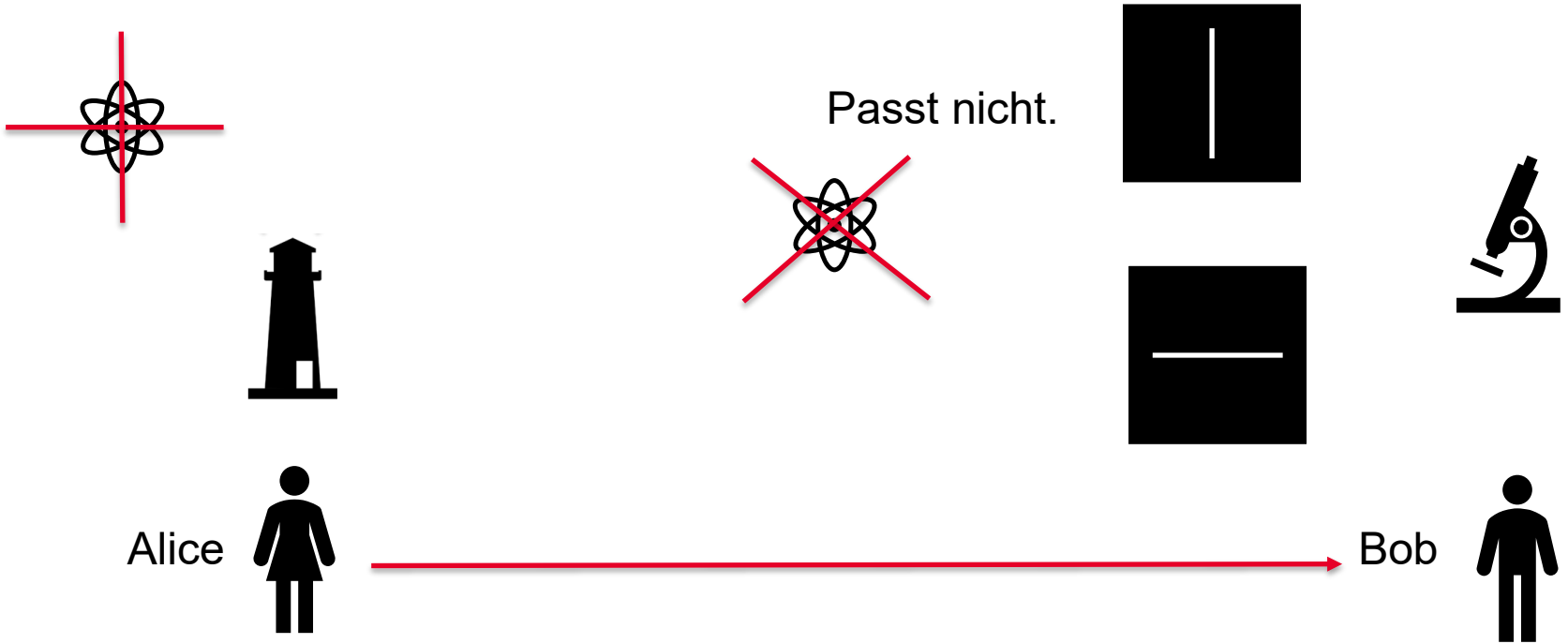


Kryptographie

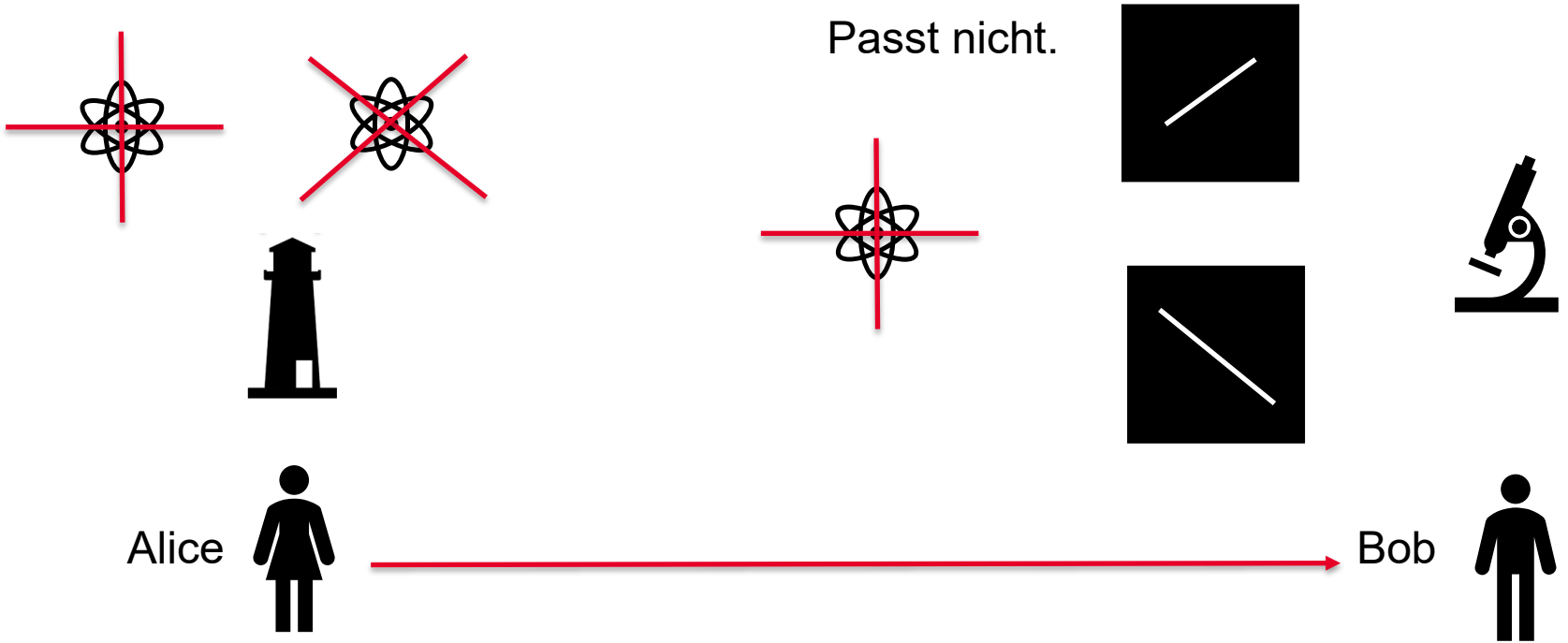
Kryptographie



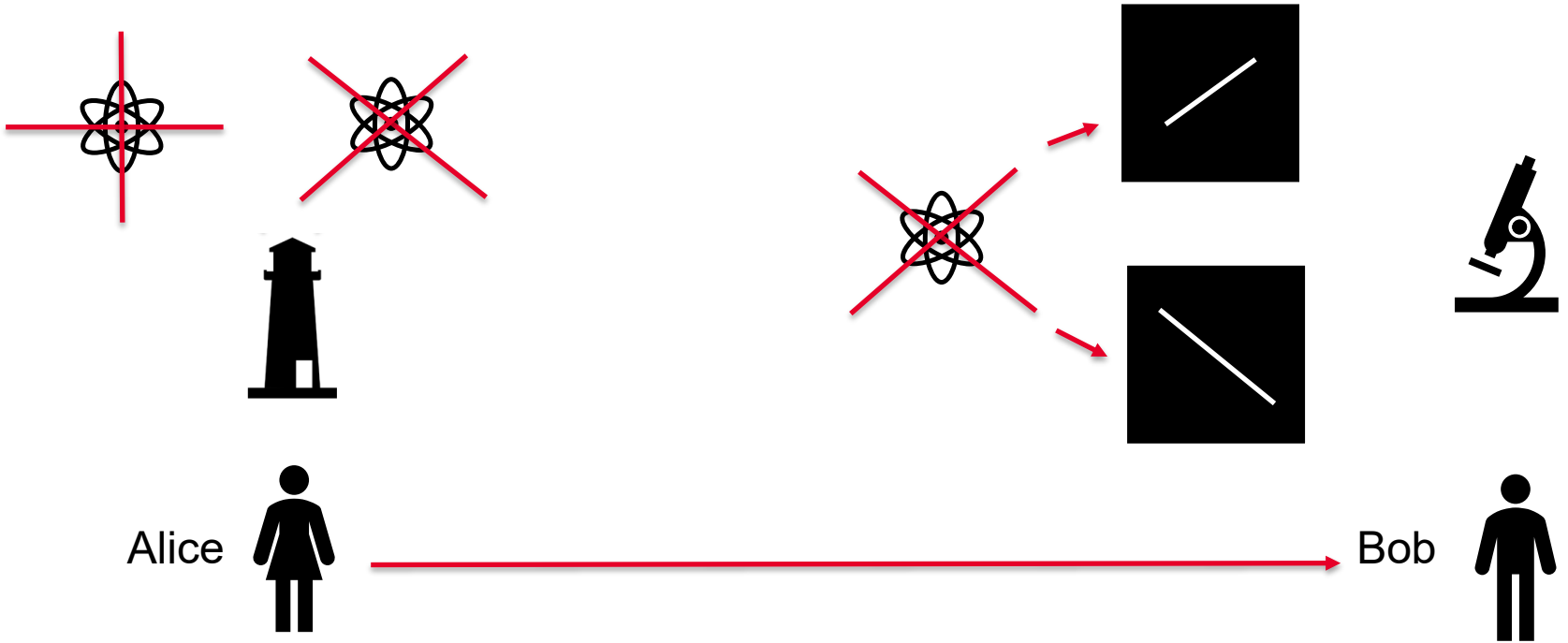
Kryptographie



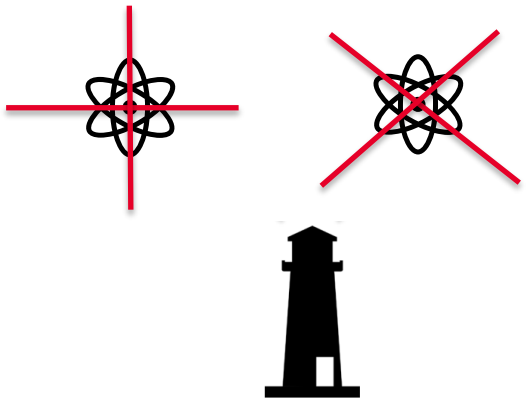
Kryptographie

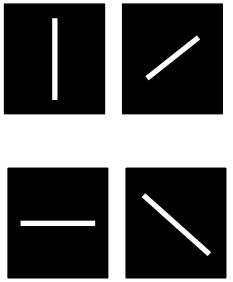


Kryptographie



Kryptographie





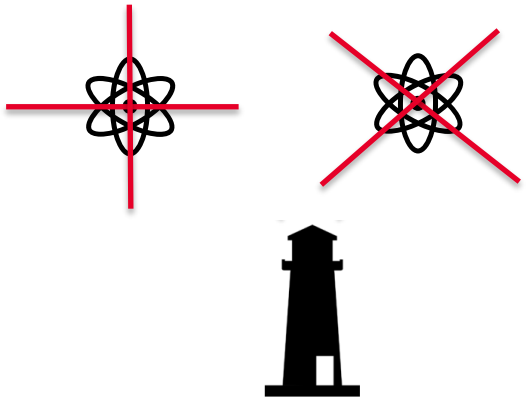
Wichtig!

<u>Der Spin wird nach der Passage eines Filters gewechselt.</u>

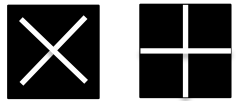
Alice

Bob

Kryptographie



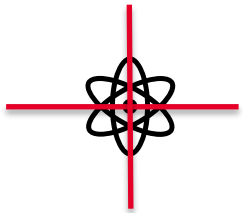
Reduktion der
Filter.

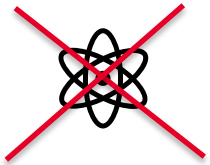


Alice

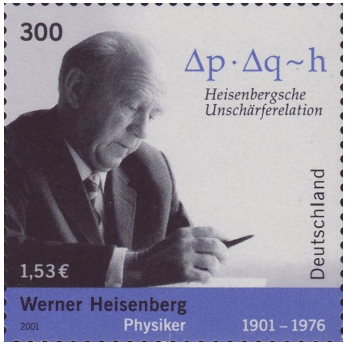
Bob

Kryptographie

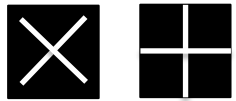




Wichtig!



Der Spin wird nach der Passage eines Filters gewechselt.



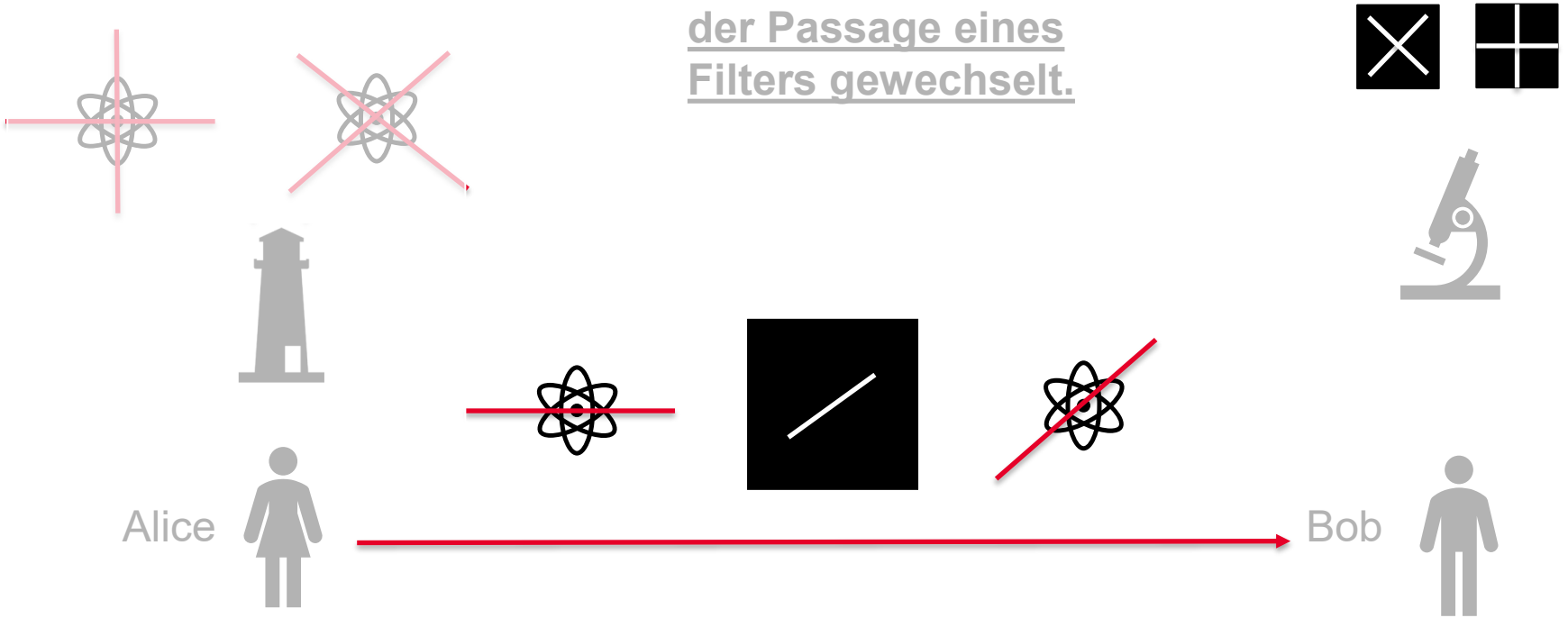
Alice

Bob

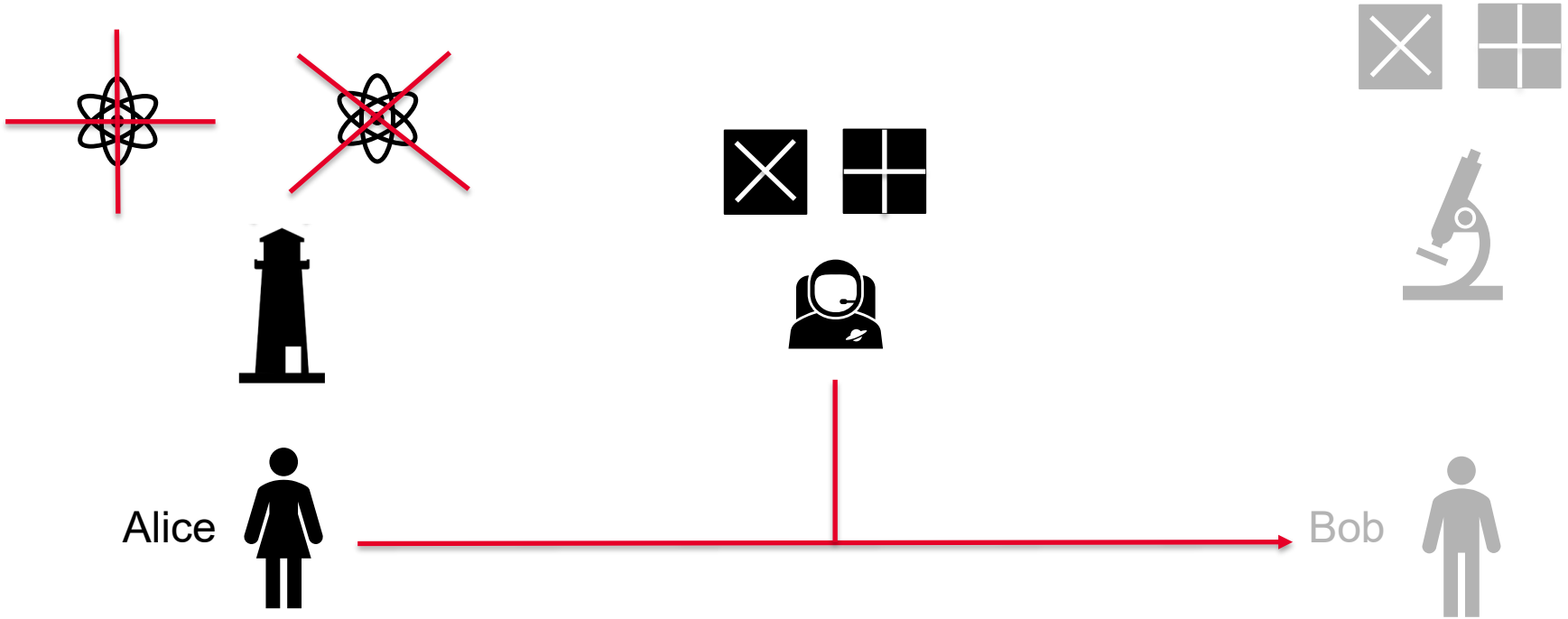
Kryptographie

Wichtig!

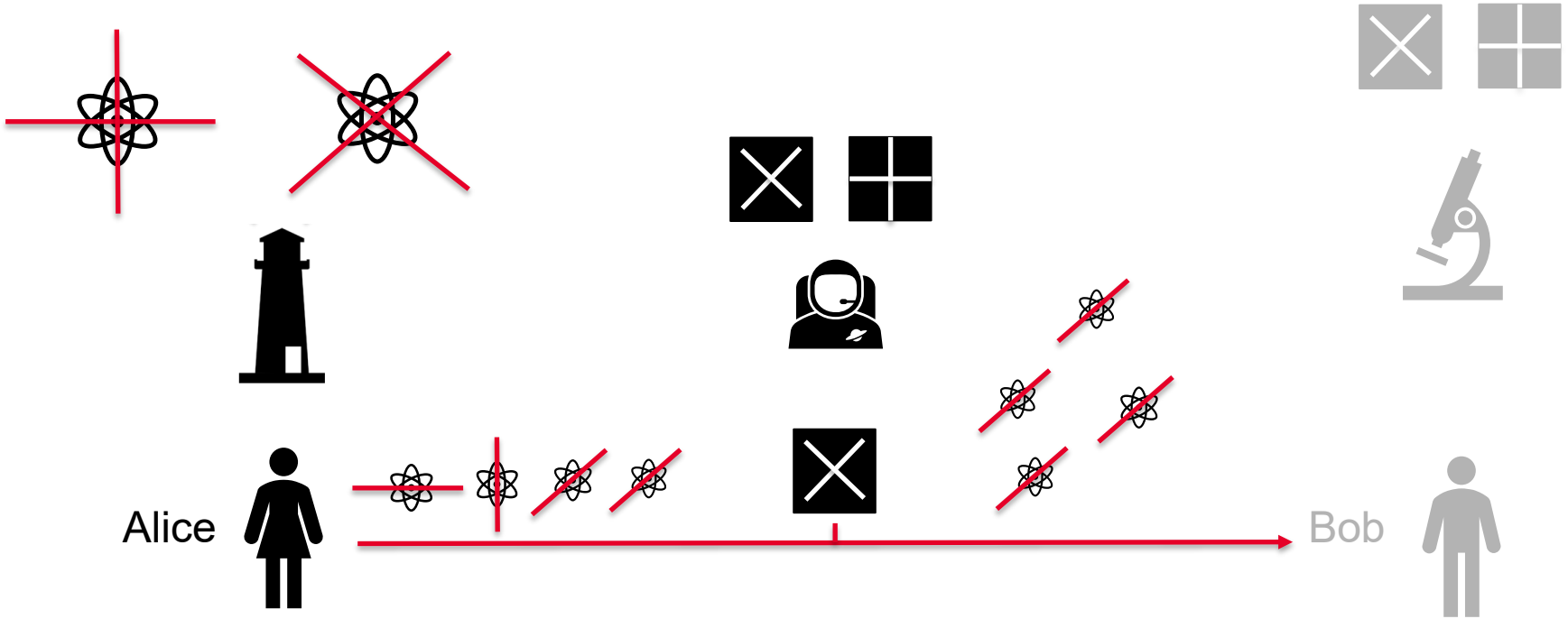
Der Spin wird nach der Passage eines Filters gewechselt.



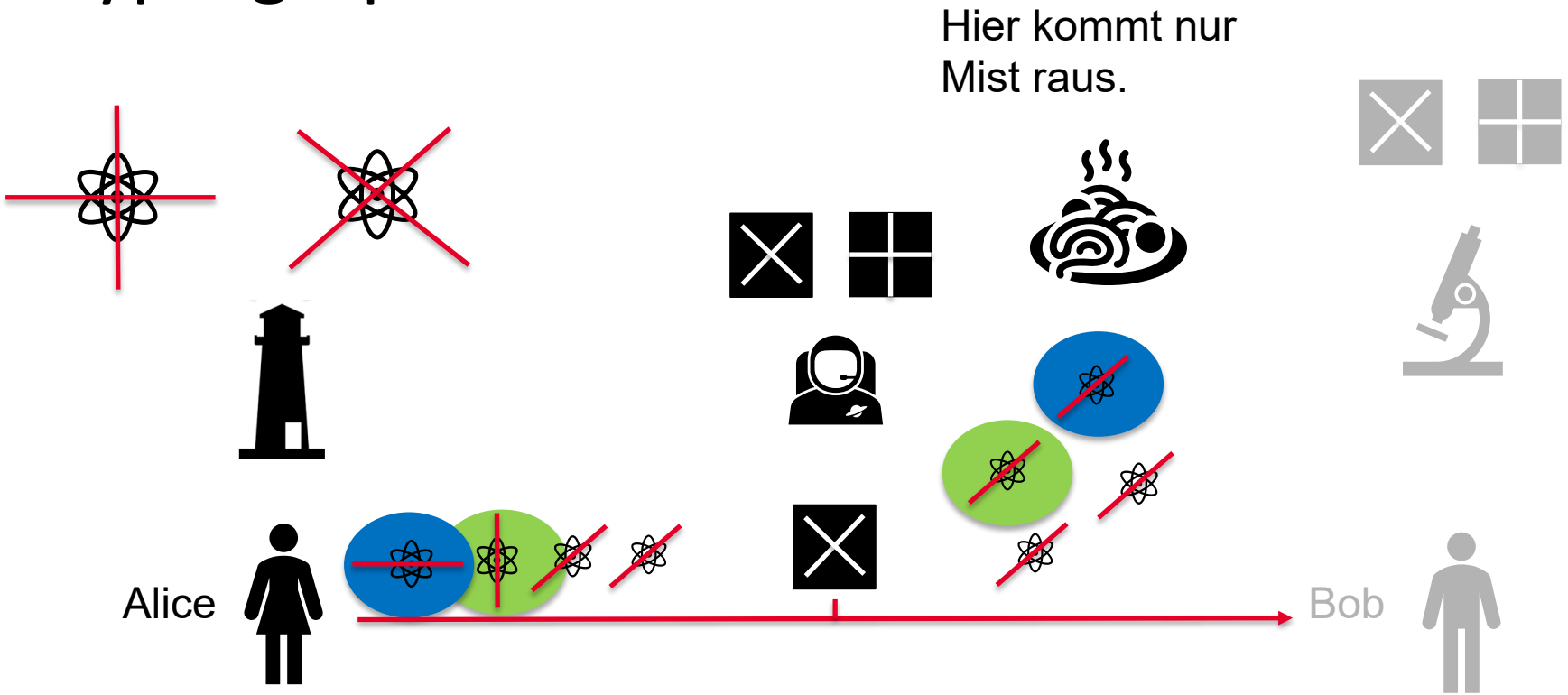
Kryptographie



Kryptographie

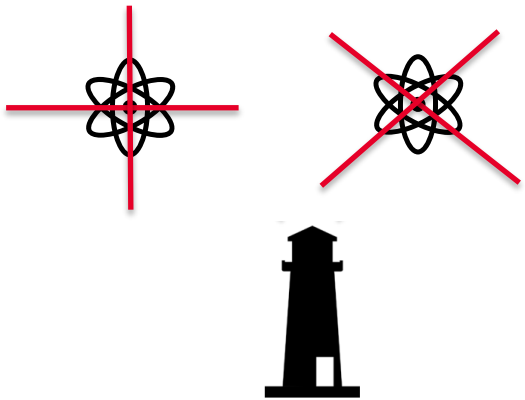


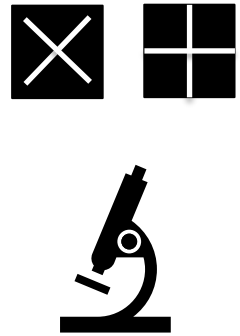
Kryptographie



Kryptographie

Wie kann sich Bob vor Eve's Schicksal schützen?

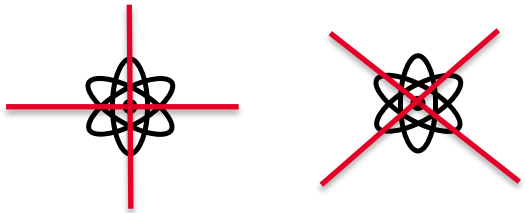




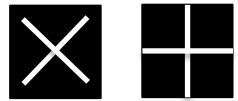
Alice

Bob

Kryptographie

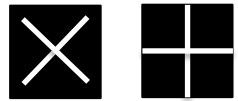


Wie kann sich Bob vor Eve's Schicksal schützen?



Kryptographie

Wie kann sich Bob vor Eve's Schicksal schützen?

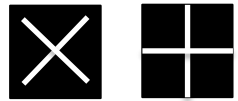


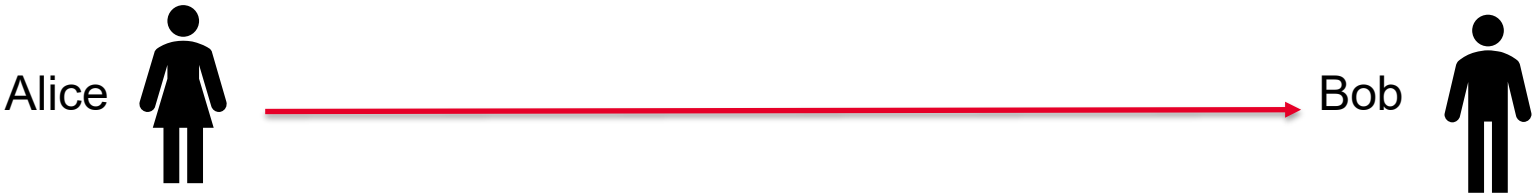
Alice

Bob

Kryptographie

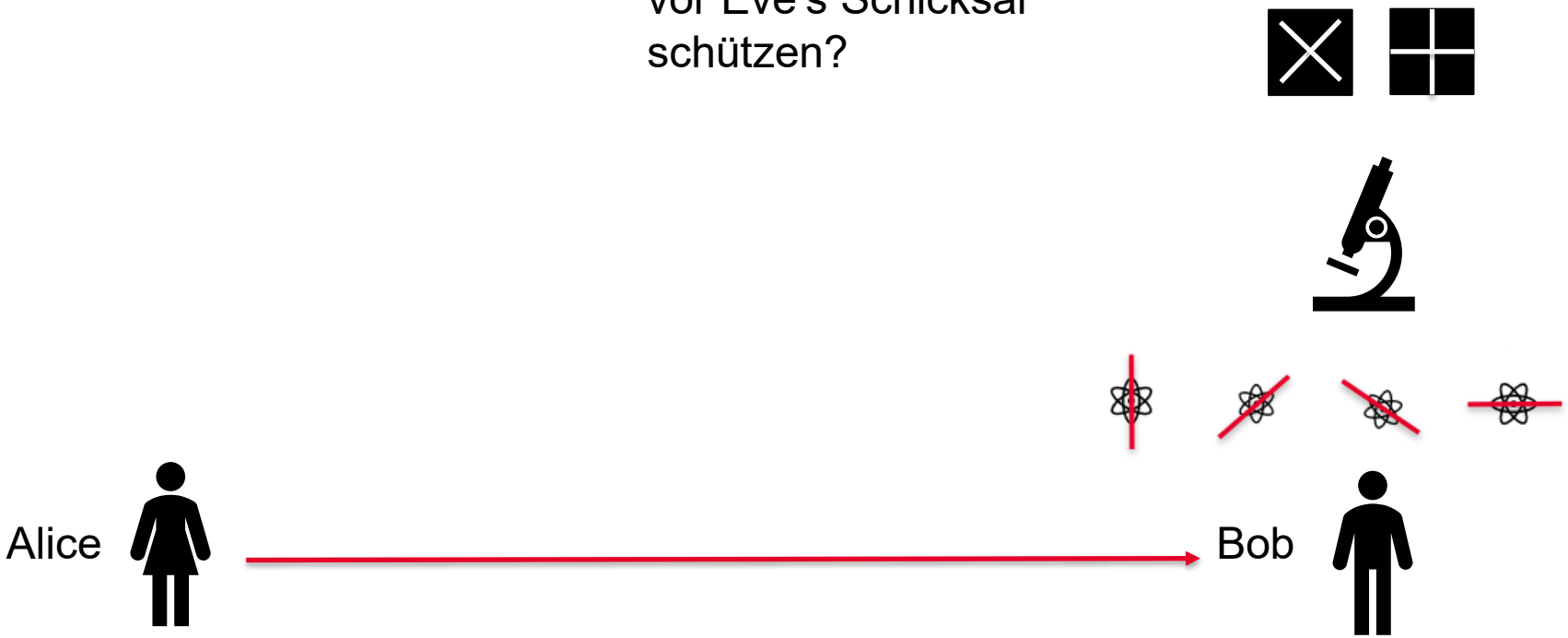
Wie kann sich Bob vor Eve's Schicksal schützen?





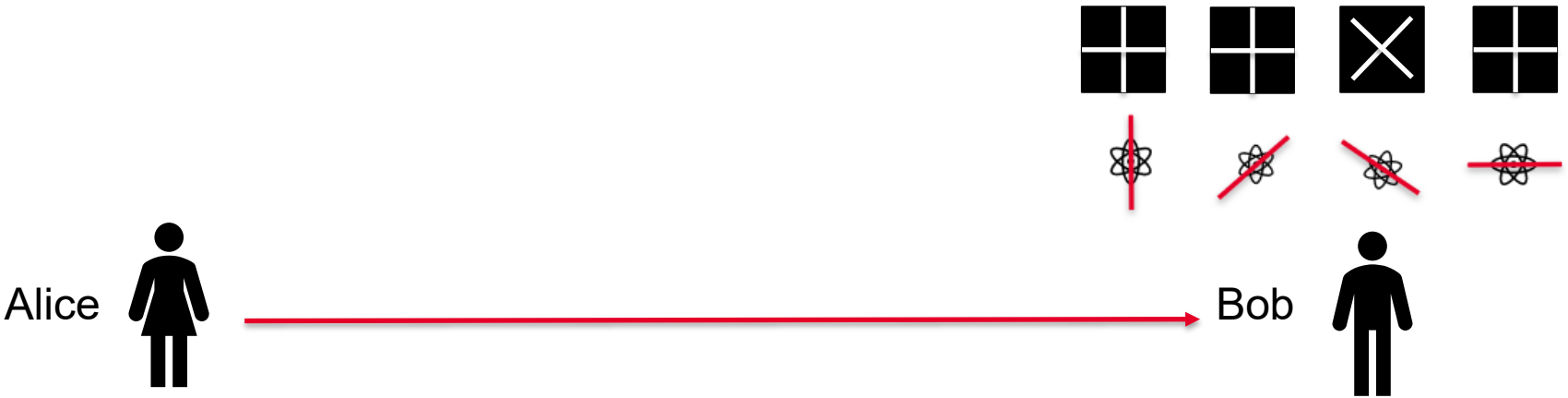
Kryptographie

Wie kann sich Bob vor Eve's Schicksal schützen?



Kryptographie

Wie kann sich Bob vor Eve's Schicksal schützen?

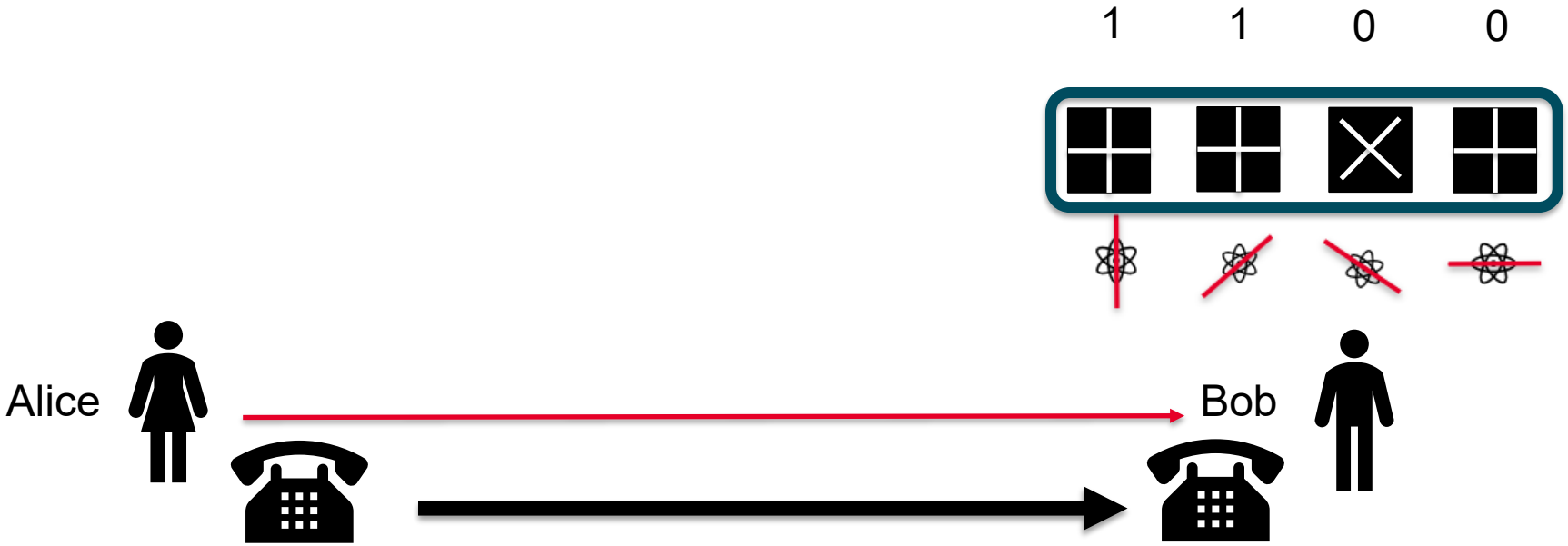


Kryptographie

Wie kann sich Bob vor Eve's Schicksal schützen?

Kryptographie

Wie kann sich Bob vor Eve's Schicksal schützen?



Kryptographie

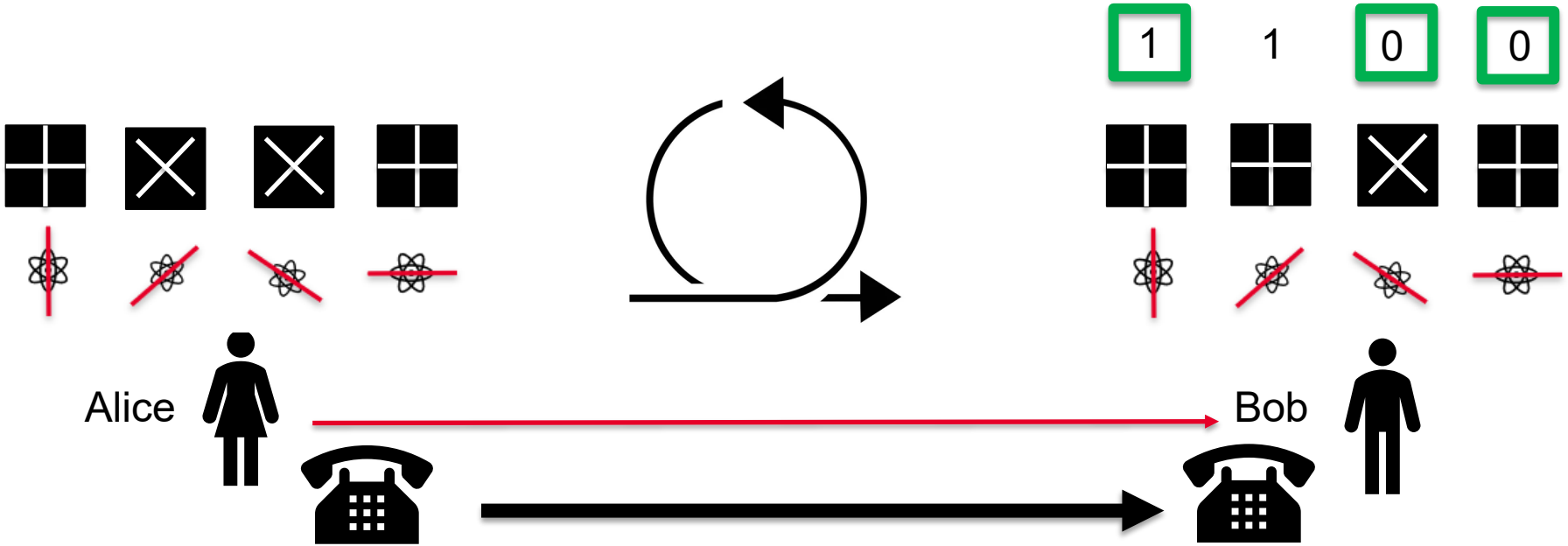
Wie kann sich Bob vor Eve's Schicksal schützen?

Kryptographie

Wie kann sich Bob vor Eve's Schicksal schützen?

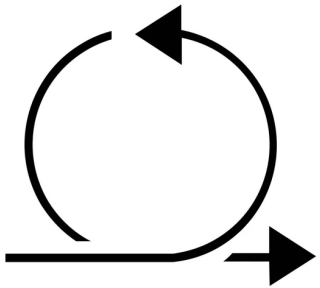
Kryptographie

Wie kann sich Bob vor Eve's Schicksal schützen?



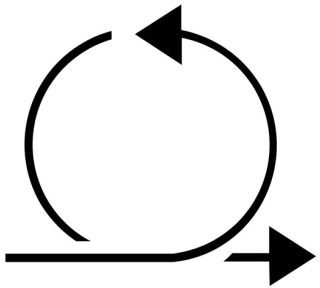
Kryptographie

Wie kann sich Bob vor Eve's Schicksal schützen?



Kryptographie

Wie kann sich Bob vor Eve's Schicksal schützen?



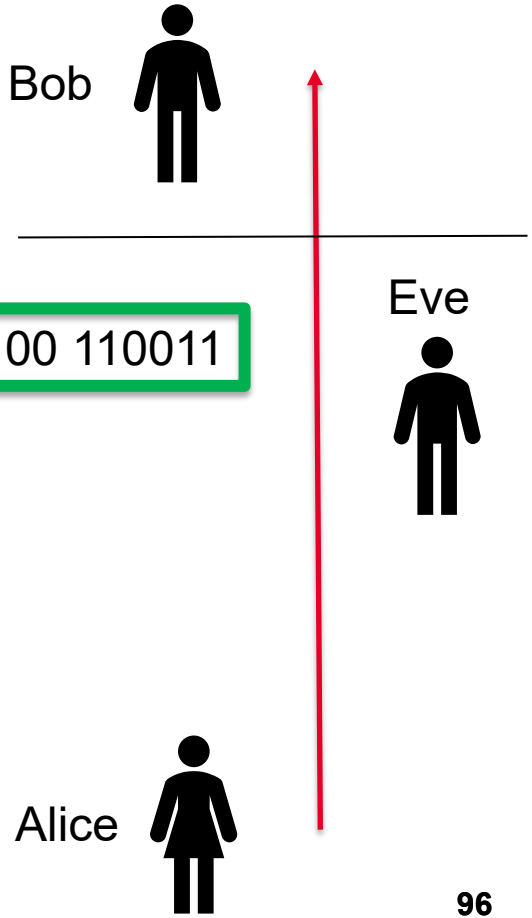
110001 110100 110011

Kryptographie

Beispiel: Multiplikation von Primzahlen.

Substitution: vorlesung

v o r l e s u n g _ !
5 8 12 15 87 55 21 32 73 52 44 ✖ 11 ✖ 13



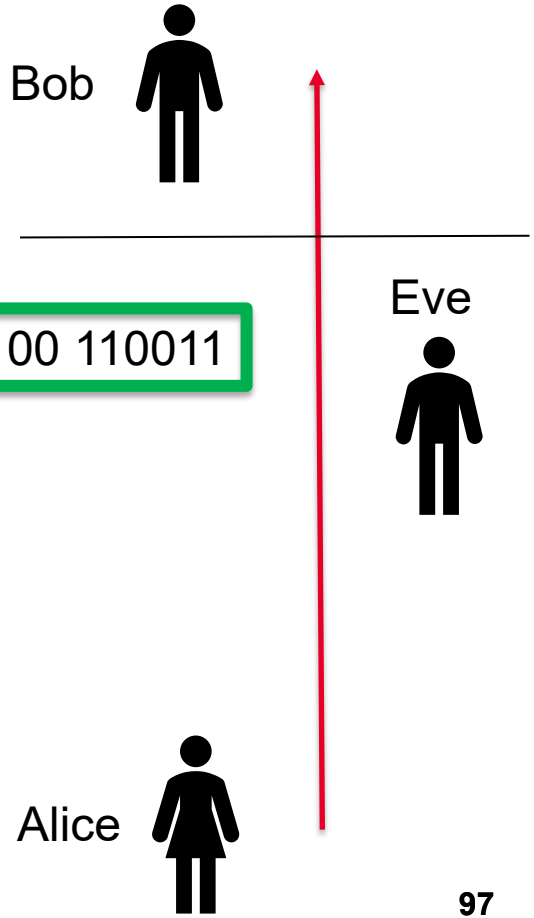
Kryptographie

Beispiel: Multiplikation von Primzahlen.

Substitution: vorlesung

v o r l e s u n g _ !
5 8 12 15 87 55 21 32 73 52 44 ✖ 11 ✖ 13

143

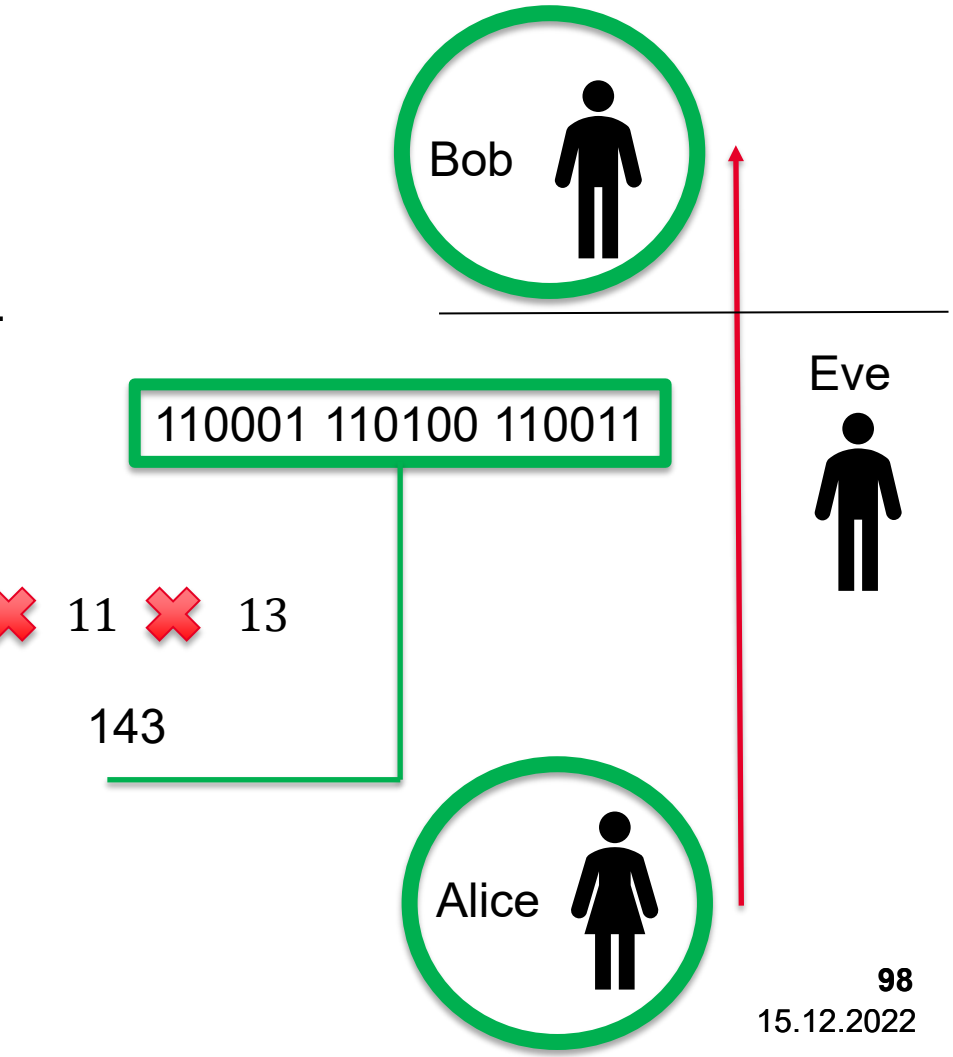


Kryptographie

Beispiel: Multiplikation von Primzahlen.

Substitution: vorlesung

v	o	r	l	e	s	u	n	g	_	!
5	8	12	15	87	55	21	32	73	52	44

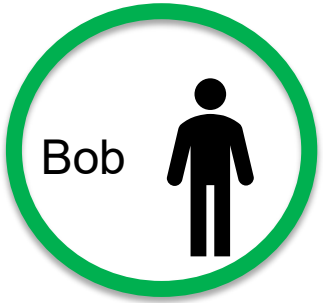


Kryptographie

Beispiel: Multiplikation v

Substitution: vo

v o r l e s u
5 8 12 15 87 55 21



110001 110100 110011