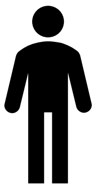
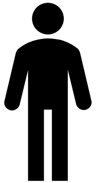
Kryptographie

Bob



Beispiel: Multiplikation von Primzahlen.

Eve

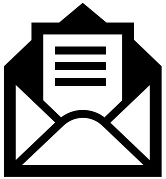


Substitution: vorlesung

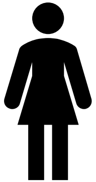
Eve kann ohne die 143 nur raten.

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

$$5\ 8\ 12\ 15\ 87\ 55\ 21\ 32\ 73\ 52\ 44 \times \underbrace{11 \times 13}_{143} = \beta$$



Alice



Kryptographie

Frage aus der Vorlesung (Nachtrag):
Die Zahl 143 kann man beim RSA Verfahren doch einfach abfangen und zum entschlüsseln nutzen?

Richtig! Was ich in der Vorlesung vergessen habe zu zeigen, ist dass die Rechnung auf der rechten Seite der Gleichung eine andere ist.

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

Frage aus der Vorlesung (Nachtrag):
Die Zahl 143 kann man beim RSA Verfahren doch einfach abfangen und zum entschlüsseln nutzen?

Richtig! Was ich in der Vorlesung vergessen habe zu zeigen, ist dass die Rechnung auf der rechten Seite der Gleichung eine andere ist.

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

$$\times \underbrace{\underset{p}{\boxed{11}} \times \underset{q}{\boxed{13}}}_{n} = \beta$$

Kryptographie

Frage aus der Vorlesung (Nachtrag):
Die Zahl 143 kann man beim RSA Verfahren doch einfach abfangen und zum entschlüsseln nutzen?

Richtig! Was ich in der Vorlesung vergessen habe zu zeigen, ist dass die Rechnung auf der rechten Seite der Gleichung eine andere ist.

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

$$\times \underbrace{\boxed{11}_{p} \times \boxed{13}_{q}}_{n} = \beta$$

Freie Wahl einer Zahl *e*

Zahlenpaar *(e,n)* ist der public key

Kryptographie

Frage aus der Vorlesung (Nachtrag):
Die Zahl 143 kann man beim RSA Verfahren doch einfach abfangen und zum entschlüsseln nutzen?

Richtig! Was ich in der Vorlesung vergessen habe zu zeigen, ist dass die Rechnung auf der rechten Seite der Gleichung eine andere ist.

Berechnung der Zahl *d nach der euklidischen Norm.*

Beispiel: Multiplikation von Primzahlen.

Substitution: vorlesung

$$e \cdot d \stackrel{!}{=} 1 \qquad mod(p-1)\cdot(q-1)$$

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

$$\times \underbrace{\boxed{11}_{p} \times \boxed{13}_{q}}_{n} = \beta$$

Die Zahl *d* ist der private key.

Freie Wahl einer Zahl *e*

Zahlenpaar *(e,n)* ist der public key

Kryptographie

Frage aus der Vorlesung (Nachtrag):
Die Zahl 143 kann man beim RSA Verfahren doch einfach abfangen und zum entschlüsseln nutzen?

Richtig! Was ich in der Vorlesung vergessen habe zu zeigen, ist dass die Rechnung auf der rechten Seite der Gleichung eine andere ist.

Beispiel: Multiplikation von Primzahlen.

Substitution: vorlesung

Freie Wahl einer Zahl *e*

Zahlenpaar *(e,n)* ist der public key

$$\underbrace{\underset{p}{\boxed{11}} \times \underset{q}{\boxed{13}}}_{n} = \beta$$

Berechnung der Zahl *d nach der euklidischen Norm.*

$$e \cdot d \overset{!}{=} 1 \qquad mod(p-1)\cdot(q-1)$$

Die Zahl *d* ist der private key.

Rechenvorschrift zur Verschlüsselung:

$$c = m^e \qquad \mathrm{mod}(n)$$

Rechenvorschrift zur Entschlüsselung:

$$m = c^d \qquad \mathrm{mod}(n)$$

Kryptographie

Frage aus der Vorlesung (Nachtrag):
Die Zahl 143 kann man beim RSA Verfahren doch einfach abfangen und zum entschlüsseln nutzen?

Richtig! Was ich in der Vorlesung vergessen habe zu zeigen, ist dass die Rechnung auf der rechten Seite der Gleichung eine andere ist.

Beispiel: Multiplikation von Primzahlen.

$$e \cdot d \overset{!}{=} 1 \qquad mod(p-1)\cdot(q-1)$$

$$c = m^e \qquad \mathrm{mod}(n)$$

$$m = c^d \qquad \mathrm{mod}(n)$$

Wahl des Paares *(e,n)*
auf (5,14)

Text: *B*

Kryptographie

Frage aus der Vorlesung (Nachtrag):
Die Zahl 143 kann man beim RSA Verfahren doch einfach abfangen und zum entschlüsseln nutzen?

Richtig! Was ich in der Vorlesung vergessen habe zu zeigen, ist dass die Rechnung auf der rechten Seite der Gleichung eine andere ist.

Beispiel: Multiplikation von Primzahlen.

Wahl des Paares *(e,n)*
auf (5,14)

Text: *B* $\longrightarrow$ *2*

$$e \cdot d \stackrel{!}{=} 1 \qquad mod(p-1)\cdot(q-1)$$

$$c = m^e \qquad \mathrm{mod}(n)$$

$$m = c^d \qquad \mathrm{mod}(n)$$

Kryptographie

Frage aus der Vorlesung (Nachtrag):
Die Zahl 143 kann man beim RSA Verfahren doch einfach abfangen und zum entschlüsseln nutzen?

Richtig! Was ich in der Vorlesung vergessen habe zu zeigen, ist dass die Rechnung auf der rechten Seite der Gleichung eine andere ist.

Beispiel: Multiplikation von Primzahlen.

$$e \cdot d \overset{!}{=} 1 \qquad mod(p-1)\cdot(q-1)$$

$$c = m^e \qquad \mod(n)$$

$$m = c^d \qquad \mod(n)$$

Wahl des Paares *(e,n)* auf (5,14)

Text: *B* ⟶ *2*

$$\begin{aligned} 2^5 \mod(14) &= 32 \mod(14) \\ &= 4 \mod(14) \end{aligned}$$

Kryptographie

Frage aus der Vorlesung (Nachtrag):
Die Zahl 143 kann man beim RSA Verfahren doch einfach abfangen und zum entschlüsseln nutzen?

Richtig! Was ich in der Vorlesung vergessen habe zu zeigen, ist dass die Rechnung auf der rechten Seite der Gleichung eine andere ist.

Beispiel: Multiplikation von Primzahlen.

$$e \cdot d \overset{!}{=} 1 \qquad mod(p-1)\cdot(q-1)$$

$$c = m^e \qquad \mathrm{mod}(n)$$

$$m = c^d \qquad \mathrm{mod}(n)$$

Wahl des Paares *(e,n)* auf (5,14)

Text: *B* $\longrightarrow$ *2*

$$2^5 \mod(14) = 32 \mod(14) = \underbrace{4}_{c} \mod(14)$$

Kryptographie

Frage aus der Vorlesung (Nachtrag):
Die Zahl 143 kann man beim RSA Verfahren doch einfach abfangen und zum entschlüsseln nutzen?

Richtig! Was ich in der Vorlesung vergessen habe zu zeigen, ist dass die Rechnung auf der rechten Seite der Gleichung eine andere ist.

Beispiel: Multiplikation von Primzahlen.

$$e \cdot d \stackrel{!}{=} 1 \qquad mod(p-1) \cdot (q-1)$$

$$c = m^e \qquad \mathrm{mod}(n)$$

$$m = c^d \qquad \mathrm{mod}(n)$$

Wahl des Paares *(e,n)* auf (5,14)

Text: *B* → *2*

$$2^5 \mod(14) = 32 \mod(14)$$
$$= \underline{4} \mod(14)$$

Text: 4 → D

Kryptographie

Frage aus der Vorlesung (Nachtrag):
Die Zahl 143 kann man beim RSA Verfahren doch einfach abfangen und zum entschlüsseln nutzen?

Richtig! Was ich in der Vorlesung vergessen habe zu zeigen, ist dass die Rechnung auf der rechten Seite der Gleichung eine andere ist.

Beispiel: Multiplikation von Primzahlen.

Wahl des Paares *(e,n)* auf (5,14)

Text: *B* → *2*

$$2^5 \mod(14) = 32 \mod(14)$$
$$= 4 \mod(14)$$

Text: 4 → D

$$e \cdot d \stackrel{!}{=} 1 \qquad mod(p-1)\cdot(q-1)$$
$$c = m^e \qquad \mod(n)$$
$$m = c^d \qquad \mod(n)$$

Entschlüsseln mit (11,14)

$$4^{(11)} \mod(14) = 4104304 \mod(14)$$
$$= 299.593,1428571429 \mod(14)$$
$$\approx 2 \mod(14) \qquad | - 299.593 \text{ and } \cdot 14$$

Kryptographie

Frage aus der Vorlesung (Nachtrag):
Die Zahl 143 kann man beim RSA Verfahren doch einfach abfangen und zum entschlüsseln nutzen?

Richtig! Was ich in der Vorlesung vergessen habe zu zeigen, ist dass die Rechnung auf der rechten Seite der Gleichung eine andere ist.

Beispiel: Multiplikation von Primzahlen.

$$e \cdot d \stackrel{!}{=} 1 \qquad mod(p-1)\cdot(q-1)$$

$$c = m^e \qquad \mathrm{mod}(n)$$

$$m = c^d \qquad \mathrm{mod}(n)$$

Wahl des Paares *(e,n)* auf (5,14)

Text: *B* → *2*

$$2^5 \mod(14) = 32 \mod(14)$$
$$= 4 \mod(14)$$

Text: 4 → D

Entschlüsseln mit (11,14)

$$4^{(11)} \mod(14) = 4104304 \mod(14)$$
$$= 299.593,1428571429 \mod(14)$$
$$\approx 2 \mod(14) \qquad | - 299.593 \text{ and } \cdot 14$$

Kryptographie

Frage aus der Vorlesung (Nachtrag):
Die Zahl 143 kann man beim RSA Verfahren doch einfach abfangen und zum entschlüsseln nutzen?

Richtig! Was ich in der Vorlesung vergessen habe zu zeigen, ist dass die Rechnung auf der rechten Seite der Gleichung eine andere ist.

Beispiel: Multiplikation von Primzahlen.

$$e \cdot d \overset{!}{=} 1 \qquad mod(p-1)\cdot(q-1)$$

$$c = m^e \qquad \mathrm{mod}(n)$$

$$m = c^d \qquad \mathrm{mod}(n)$$

Wahl des Paares *(e,n)* auf (5,14)

$\boxed{\text{Text: } B} \rightarrow$ *2*

$$2^5 \mod(14) = 32 \mod(14)$$
$$= 4 \mod(14)$$

Text: 4 $\rightarrow$ D

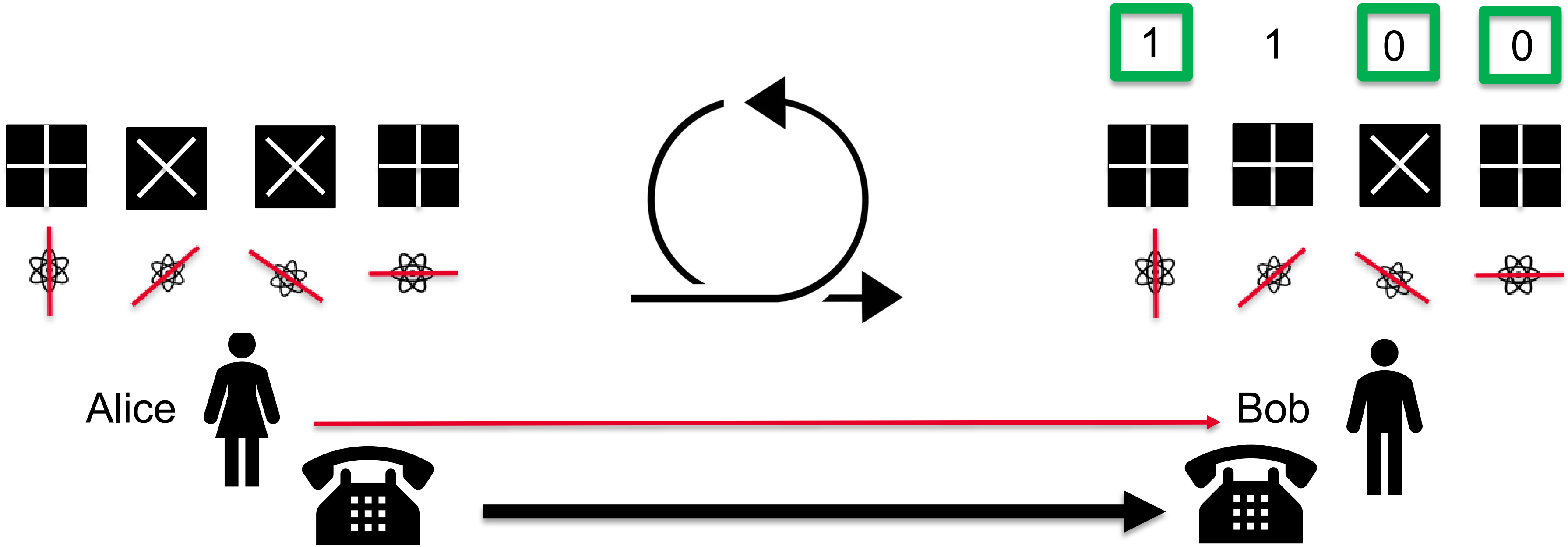
Entschlüsseln mit (11,14)

$$4^{(11)} \mod(14) = 4104304 \mod(14)$$
$$= 299.593,1428571429 \mod(14) \qquad | -299.593 \text{ and } \cdot 14$$
$$\approx 2 \mod(14)$$

$\boxed{B}$

Kryptographie

Frage aus der Vorlesung (Nachtrag):
Wie sehen die Leitungen bei der Übertragung aus?



Kryptographie

Frage aus der Vorlesung (Nachtrag):
Wie sehen die Leitungen bei der Übertragung aus?

Photonen werden transportiert. Diese Leiter laufen über Glasfaser oder über Lasersysteme.

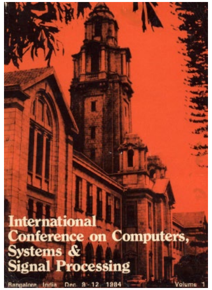
Kryptographie

Frage aus der Vorlesung (Nachtrag):
Wie sehen die Leitungen bei der Übertragung aus?

Photonen werden transportiert. Diese Leiter laufen über Glasfaser oder über Lasersysteme.

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)



In more detail one user ('Alice') chooses a random bit string and a random sequence of polarization bases (rectilinear or diagonal). She then sends the other user (Bob) a train of photons, each

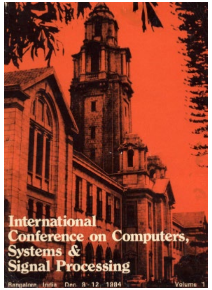
Kryptographie

Frage aus der Vorlesung (Nachtrag):
Wie sehen die Leitungen bei der Übertragung aus?

Photonen werden transportiert. Diese Leiter laufen über Glasfaser oder über Lasersysteme.

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)



In more detail one user ('Alice') chooses a random bit string and a random sequence of polarization bases (rectilinear or diagonal). She then sends the other user (Bob) a train of photons, each

Alice

Bob

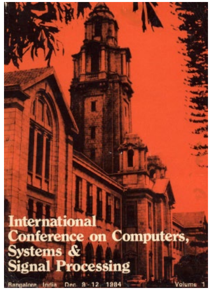
Kryptographie

Frage aus der Vorlesung (Nachtrag):
Wie sehen die Leitungen bei der Übertragung aus?

Photonen werden transportiert. Diese Leiter laufen über Glasfaser oder über Lasersysteme.

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)



J Wie sieht eine Leitung bei der Quantum Key Distribution aus?

Bei der Quantum Key Distribution (QKD) wird eine Leitung verwendet, um die Photonen, die als Träger der verschlüsselten Informationen dienen, von einem Sender zu einem Empfänger zu übertragen. Diese Leitung kann auf verschiedene Arten realisiert werden, zum Beispiel mithilfe von Glasfaserkabeln oder Luftwellenleitungen.

Alice

Bob

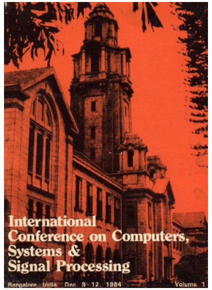
Kryptographie

Frage aus der Vorlesung (Nachtrag):
Wie sehen die Leitungen bei der Übertragung aus?

Photonen werden transportiert. Diese Leiter laufen über Glasfaser oder über Lasersysteme.

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)



J Erkläre mit die erste technische Umsetzung nach QKD

Die erste technische Umsetzung von QKD fand 1991 statt, als das Quantenkryptographie-Experiment (QKD-Experiment) von ID Quantique (IDQ) durchgeführt wurde. Das QKD-Experiment von IDQ war das erste experimentelle System, das QKD zur sicheren Übertragung von Nachrichten verwendete.

Alice

Bob

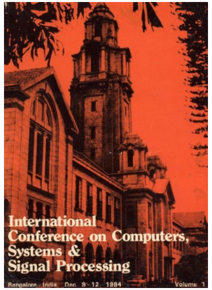
Kryptographie

Frage aus der Vorlesung (Nachtrag):
Wie sehen die Leitungen bei der Übertragung aus?

Photonen werden transportiert. Diese Leiter laufen über Glasfaser oder über Lasersysteme.

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

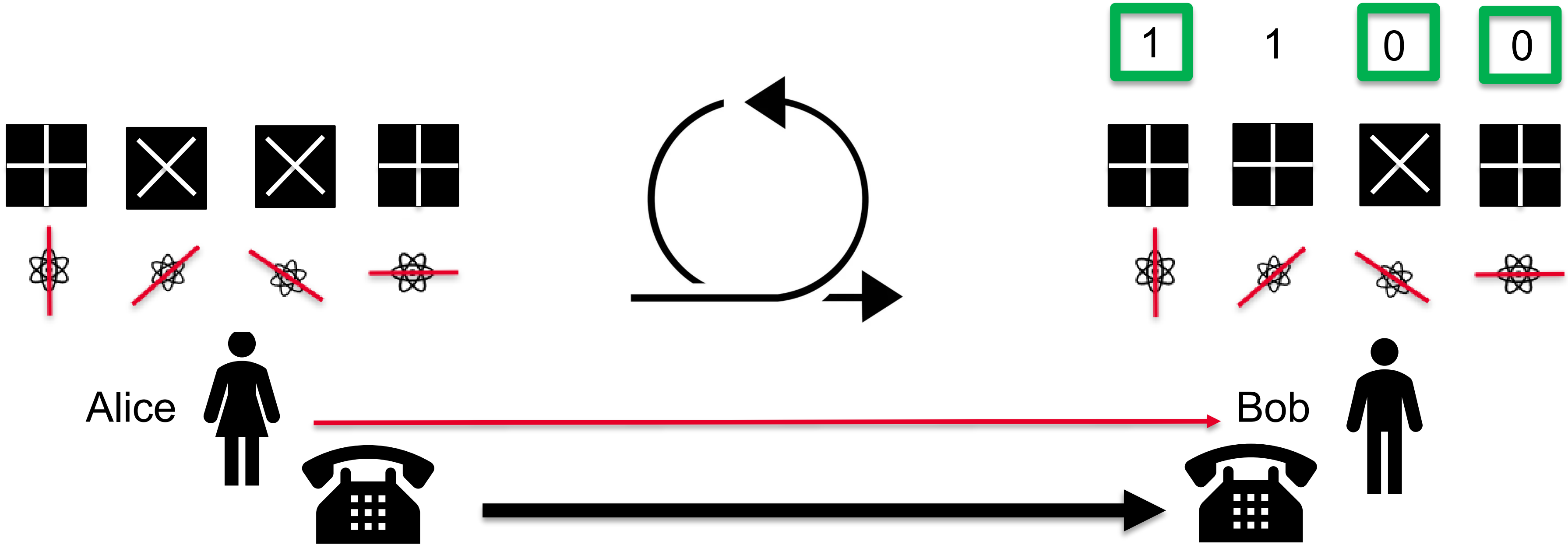


J Wie sah der Leiter in dieser Umestzung aus?

In der ersten technischen Umsetzung von QKD, dem Quantenkryptographie-Experiment (QKD-Experiment) von ID Quantique (IDQ) aus dem Jahr 1991, wurde eine Glasfaserleitung als Leiter für die Photonen verwendet, die als Träger der verschlüsselten Informationen dienten. Die Glasfaserleitung verlief direkt zwischen dem Sender und dem Empfänger und diente als Übertragungsmethode für die Photonen.

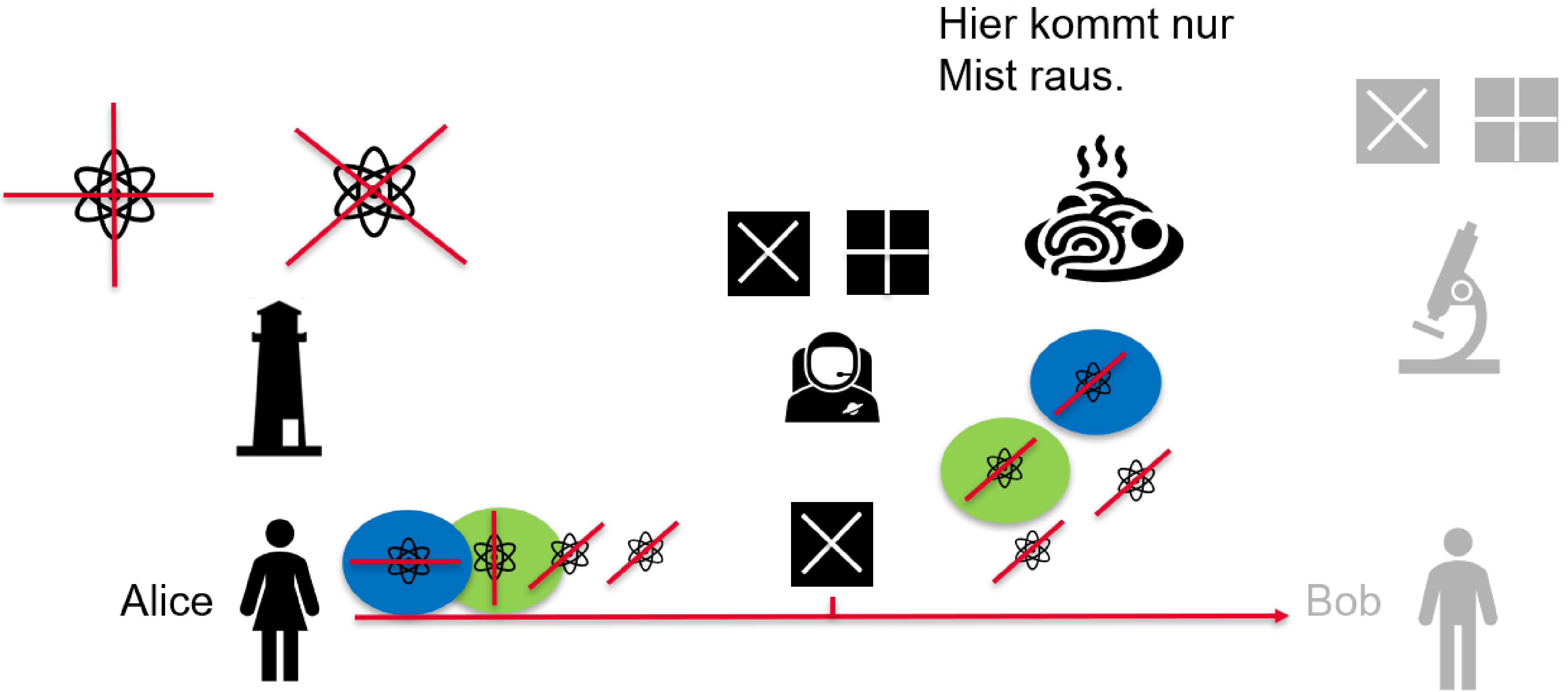
Kryptographie

Frage aus der Vorlesung (Nachtrag):
Warum übermittelt Alice nicht die Filterreihenfolge direkt an Bob?



Kryptographie

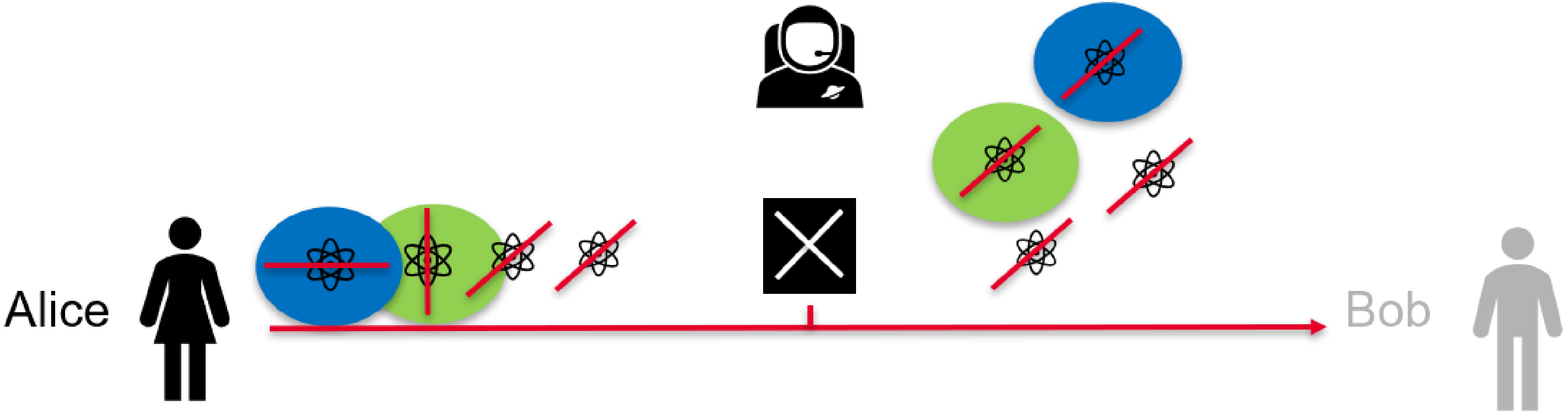
Frage aus der Vorlesung (Nachtrag):
Warum übermittelt Alice nicht die



Kryptographie

Frage aus der Vorlesung (Nachtrag):
Warum übermittelt Alice nicht die Filterreihenfolge direkt an Bob?

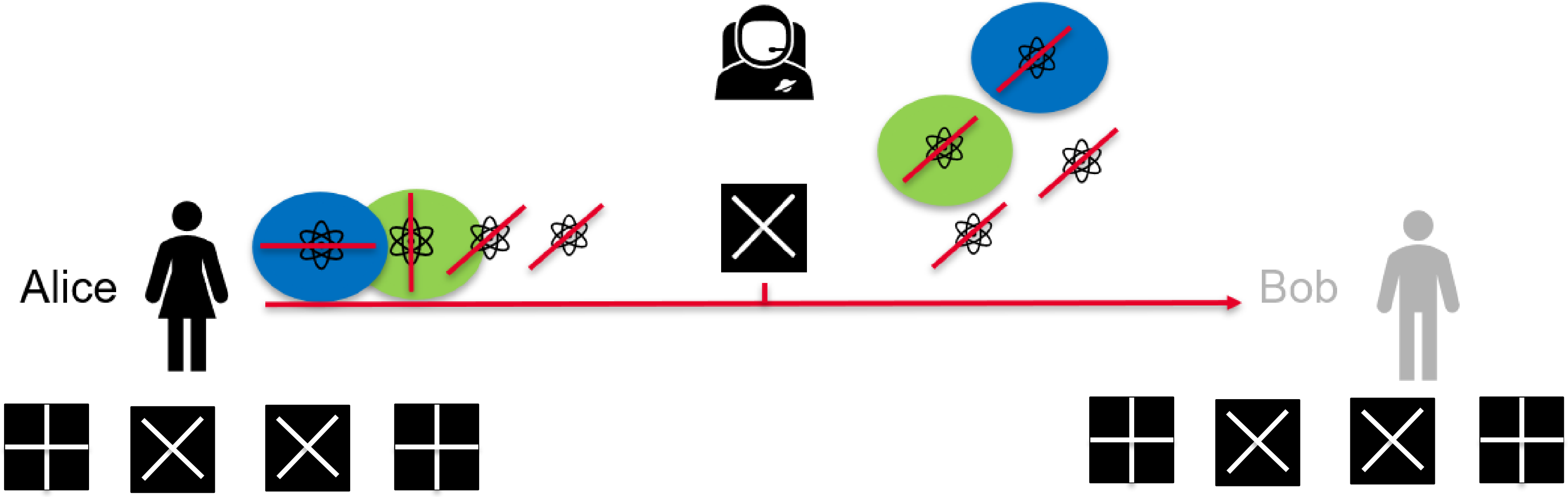
Ja, hier ist es möglich. Denn Alice verändert die Werte, bzw. die Polarisation der Photonen.



Kryptographie

Frage aus der Vorlesung (Nachtrag):
Warum übermittelt Alice nicht die Filterreihenfolge direkt an Bob?

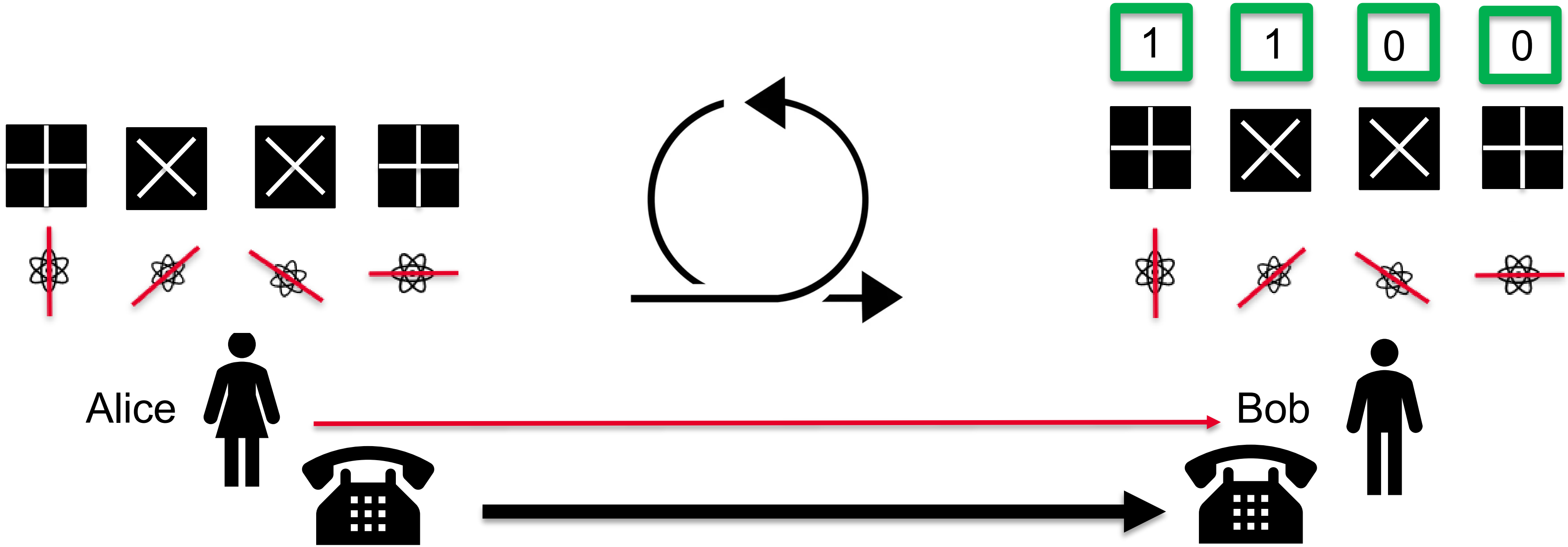
Ja, hier ist es möglich. Denn Alice verändert die Werte, bzw. die Polarisation der Photonen.



Kryptographie

Frage aus der Vorlesung (Nachtrag):
Warum übermittelt Alice nicht die Filterreihenfolge direkt an Bob?

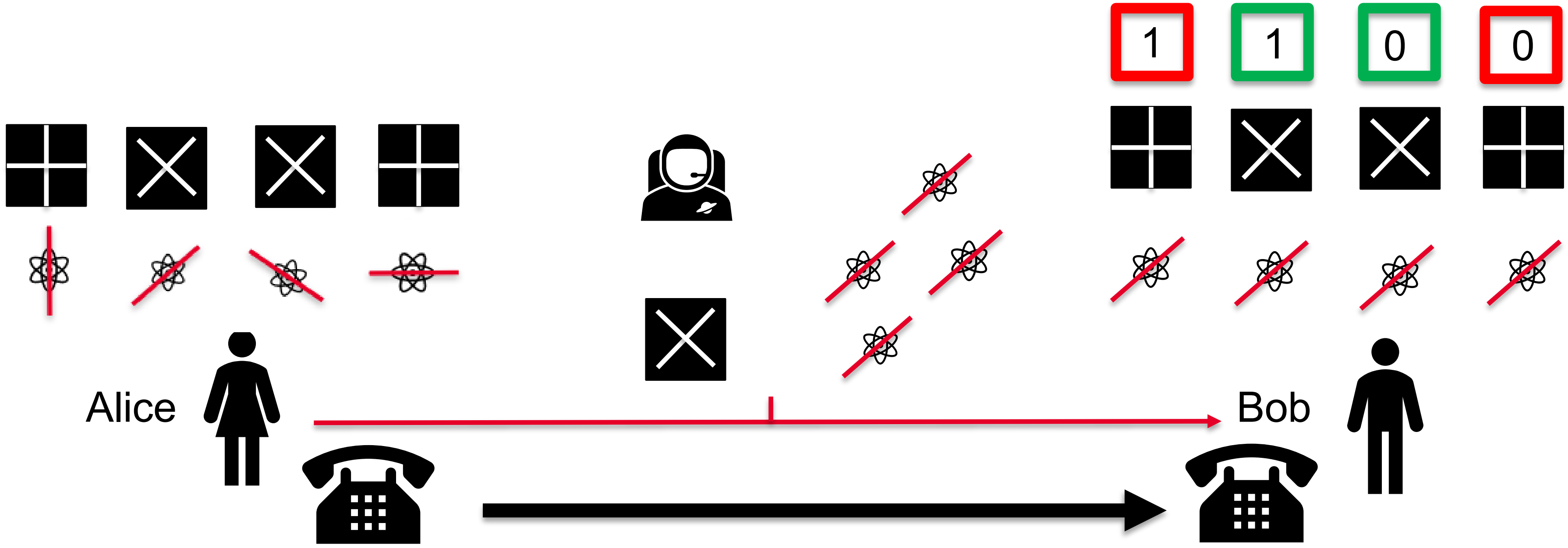
Ja, hier ist es möglich. Denn Alice verändert die Werte, bzw. die Polarisation der Photonen.



Kryptographie

Frage aus der Vorlesung (Nachtrag):
Warum übermittelt Alice nicht die
Filterreihenfolge direkt an Bob?

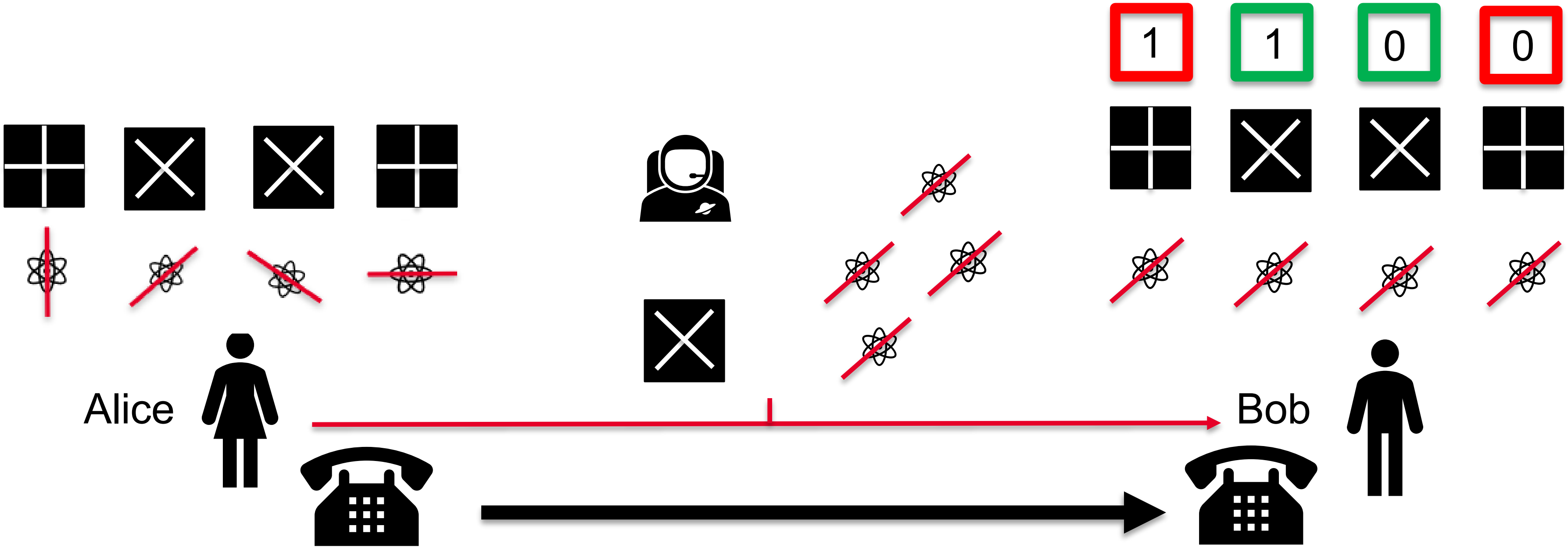
Ja, hier ist es möglich. Denn Alice verändert die Werte, bzw. die
Polarisation der Photonen.



Kryptographie

Frage aus der Vorlesung (Nachtrag):
Warum übermittelt Alice nicht die Filterreihenfolge direkt an Bob?

Dieser Schlüssel wird verworfen.



Kryptographie

Frage aus der Vorlesung (Nachtrag):
Warum übermittelt Alice nicht die Filterreihenfolge direkt an Bob?

Erkläre mir die Physik hinter der Quantum Key Distribution, Alice und Bob.

Die QKD basiert auf der Tatsache, dass es in der Quantenphysik unmöglich ist, bestimmte Eigenschaften von Quantenpartikeln ohne eine signifikante Störung zu messen. Diese Eigenschaften umfassen zum Beispiel die Impuls-, Orts- oder Energieverteilung von Photonen. Aufgrund dieser Eigenschaft ist es unmöglich, die übertragenen Photonen abzuhören oder zu verändern, ohne dass dies bemerkt wird.