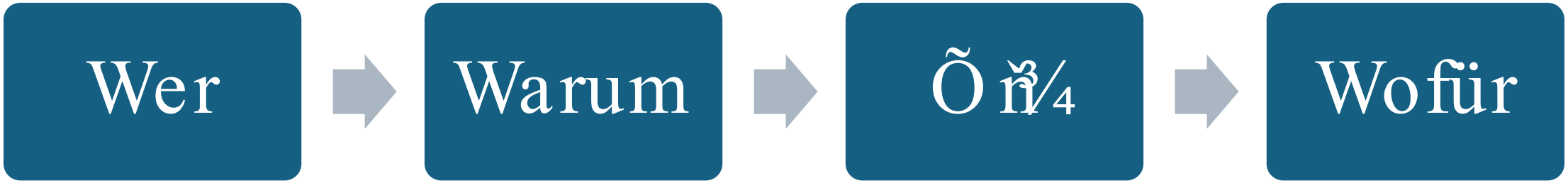
Radio Key Generation

Wie man symmetrische Schlüssel aus Funkkanaleigenschaften generiert

Jakob Heigl-Auer

Inhalt



Wer (hat daran gearbeitet)

FH-Prof. Univ.-Doz. Dipl.-Ing. Dr. Ernst Piller
Ernst.piller@fhstp.ac.at

Jakob Heigl-Auer, Bsc.
is241501@fhstp.ac.at

Dipl.-Ing. Dr. Henri Ruotsalainen
henri.ruotsalainen@fhstp.ac.at

Warum


Forbes
Are We Ready For Post-Quantum Cryptography?


built in
Cryptographers Are Racing Against Quantum Computers
Today's security schemes will soon be obsolete.


DIGITAL JOURNAL
Quantum dilemma: Cybersecurity risks are accelerating

Warum

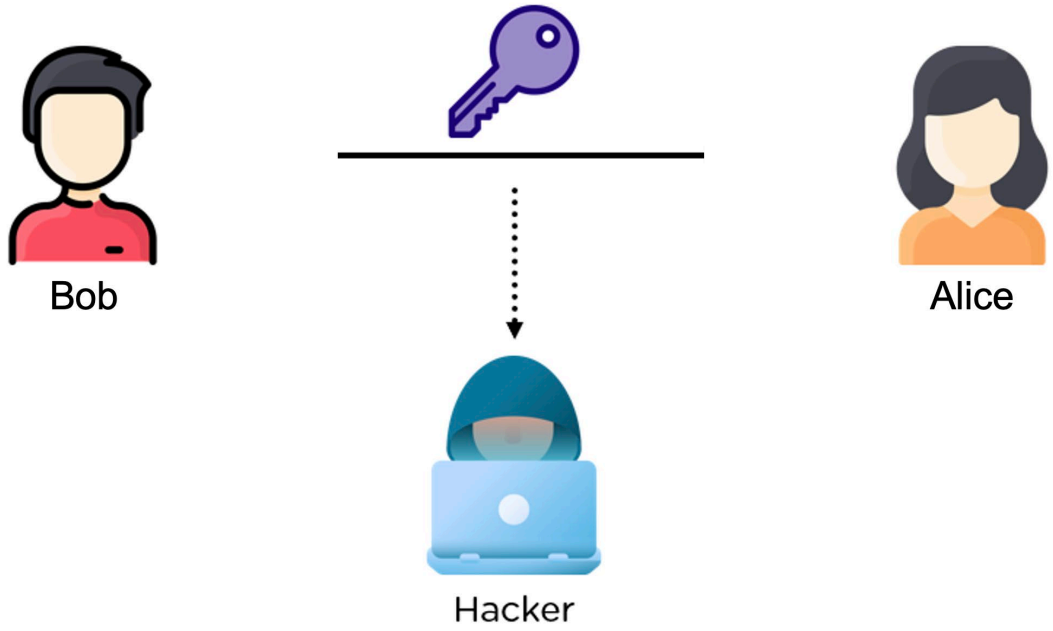
[1] *Dr. Dilip Kumar Yadav Sandeep Kumar Rao Dindayal Mahto, „The AES-256 Cryptosystem Resists Quantum Attacks“, International Journal of Advanced Research in Computer Science, Jg. 8, Nr. 3, S. 404–408, Apr. 2017. DOI: 10 . 26483 / ijarcs . v8i3 . 3025.*

Warum

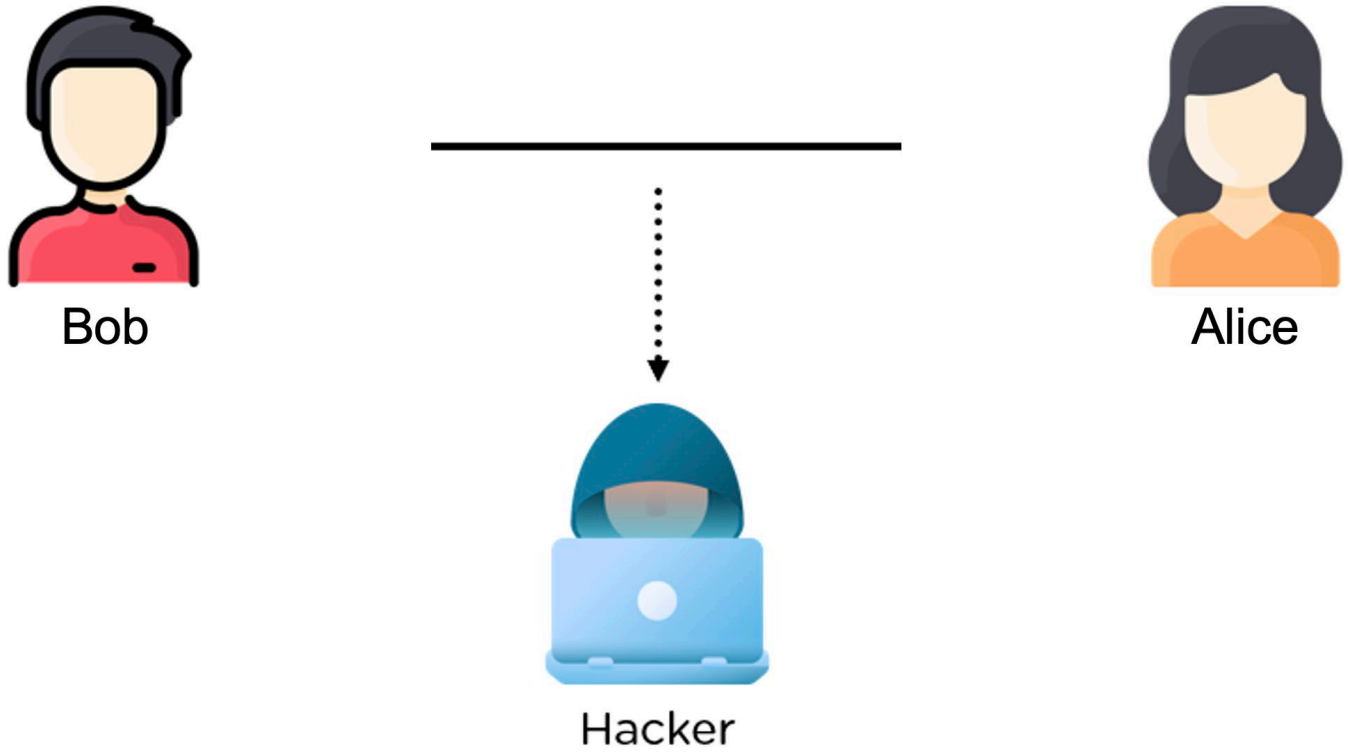
$256\text{Bit} \rightarrow 128\text{Bit}$ [1]

[1] *Dr. Dilip Kumar Yadav Sandeep Kumar Rao Dindayal Mahto, „The AES-256 Cryptosystem Resists Quantum Attacks“, International Journal of Advanced Research in Computer Science, Jg. 8, Nr. 3, S. 404–408, Apr. 2017. DOI: 10 . 26483 / ijarcs . v8i3 . 3025.*

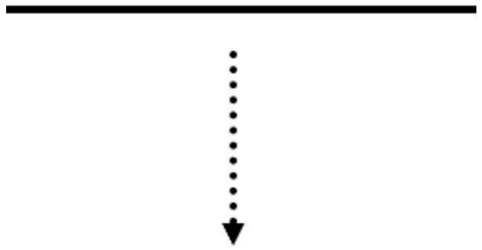
õ ï ╬



Warum



Warum



Wie

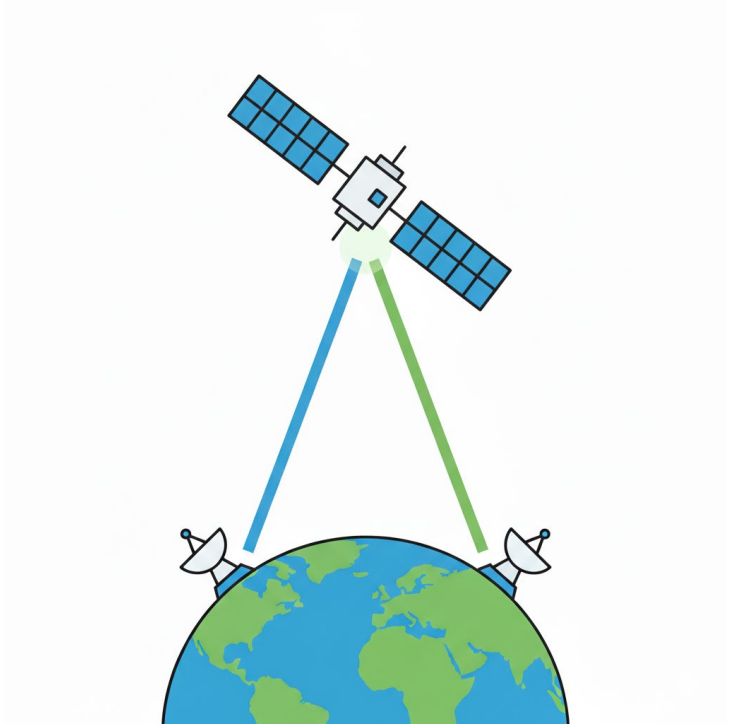
Reziproke Kanaleigenschaften:

- Signalstärke
- Phasenwinkel
- Reflektionen / Multipath Propagation
- Laufzeit
- Uvm.

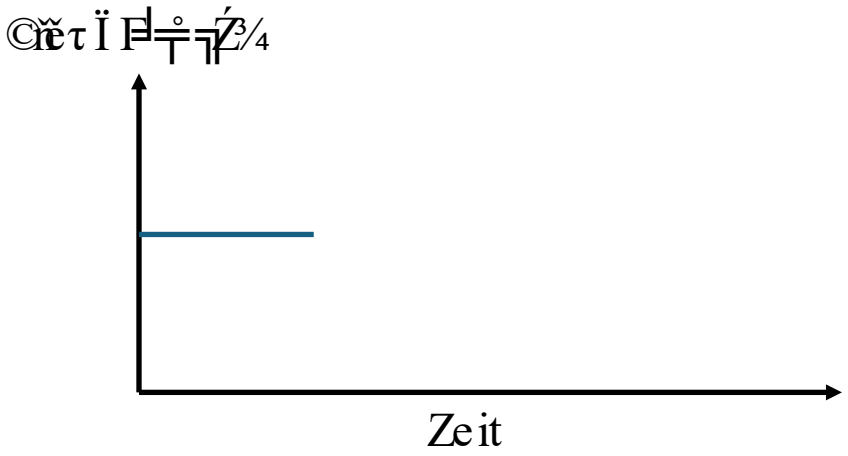
Dynamik:

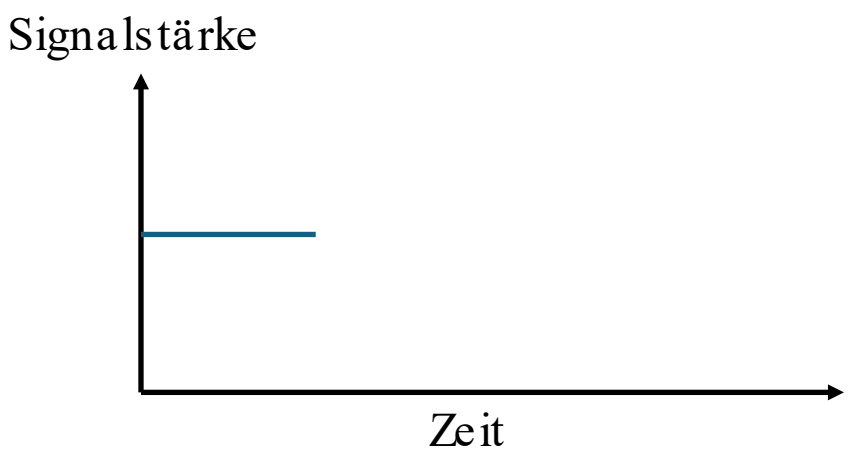
- Satellitenumlauf
- Antennenbewegung
- Reflektoränderung
- Fortbewegung (gehen, fahren, fliegen)

- Fortbewegung (in einem Publikum herumreichen)

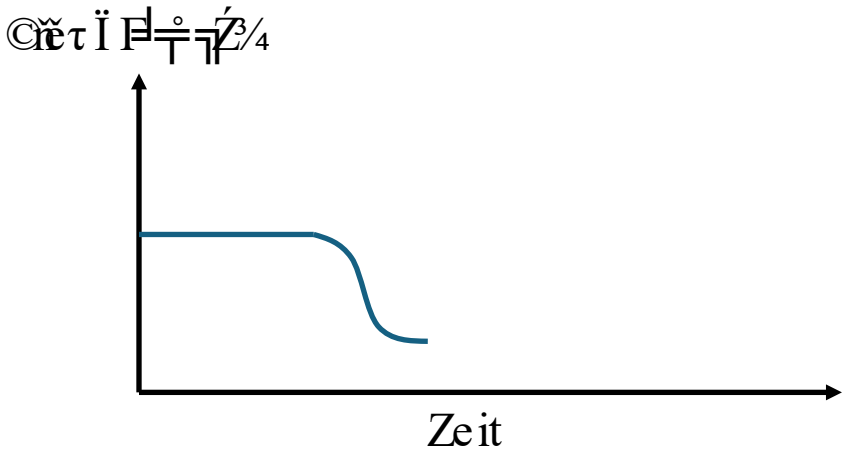


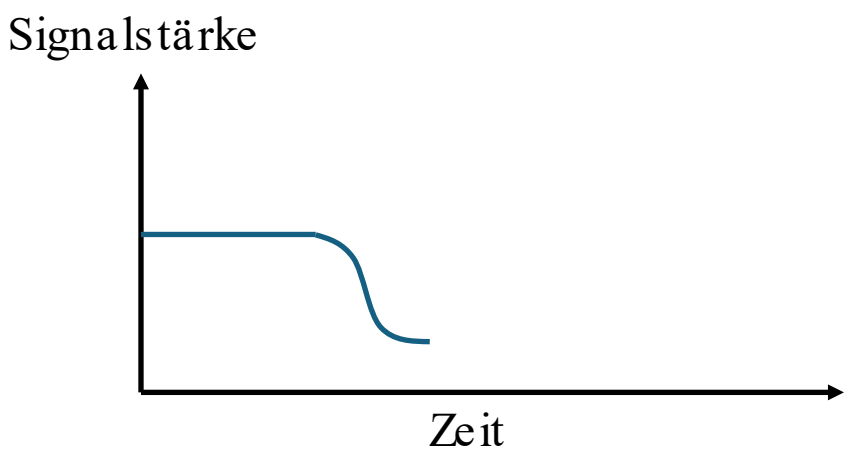
Wie Signalstärke





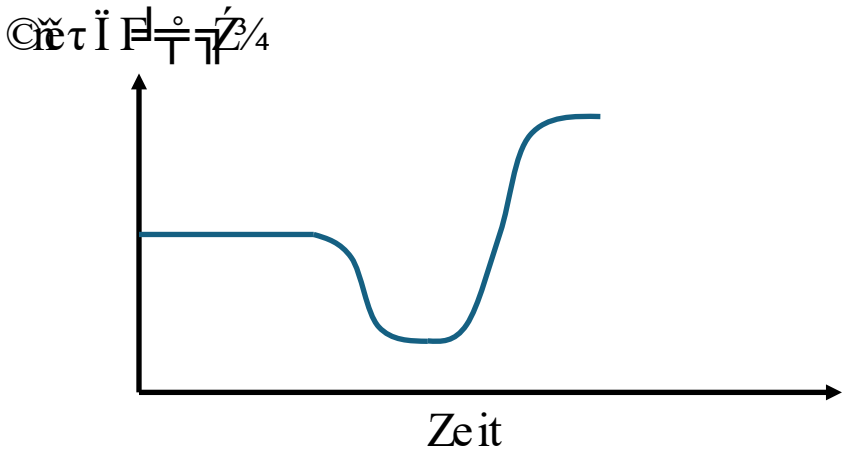
Wie Signalstärke



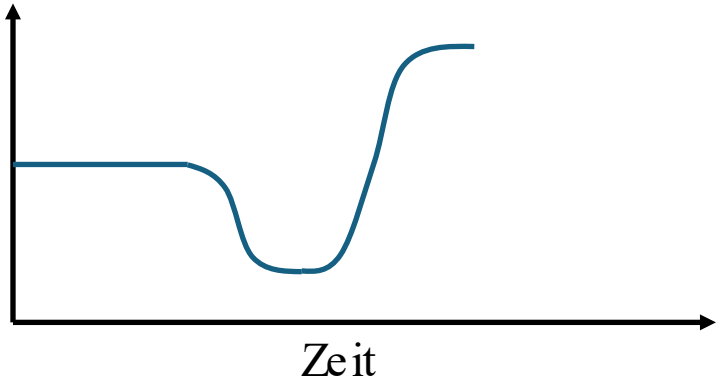


Wie

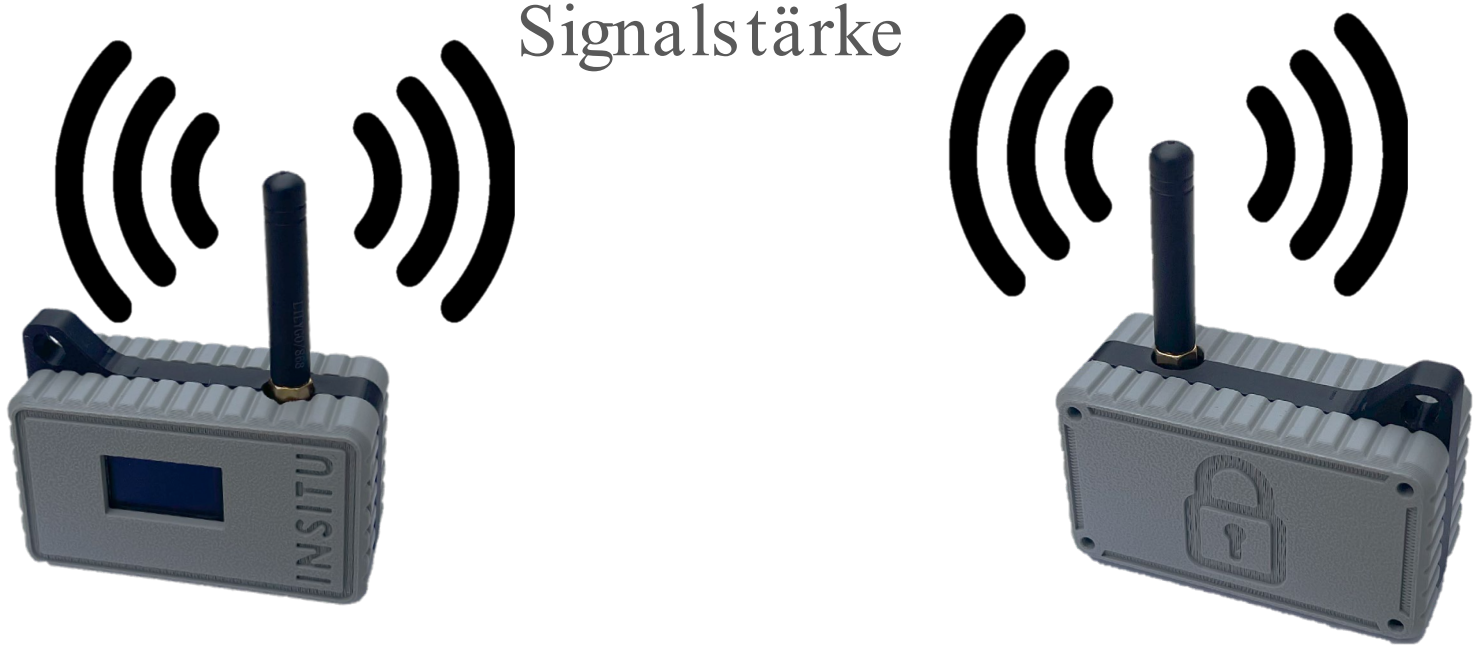
Signalstärke

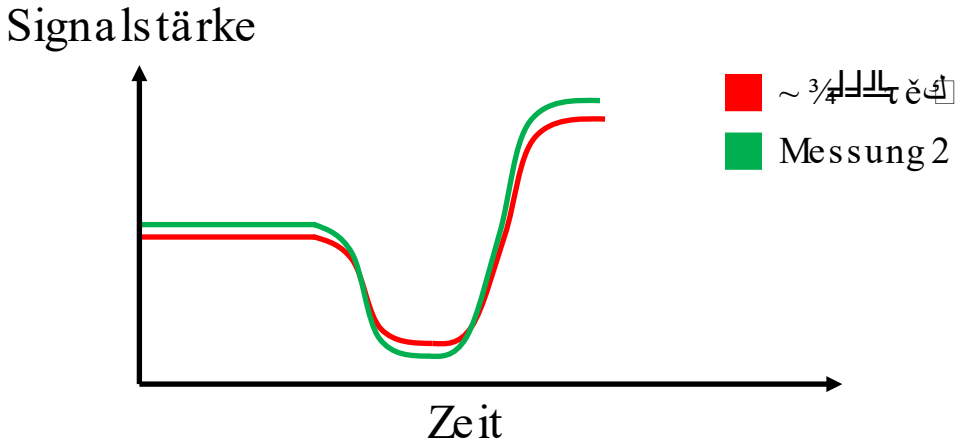


Signalstärke

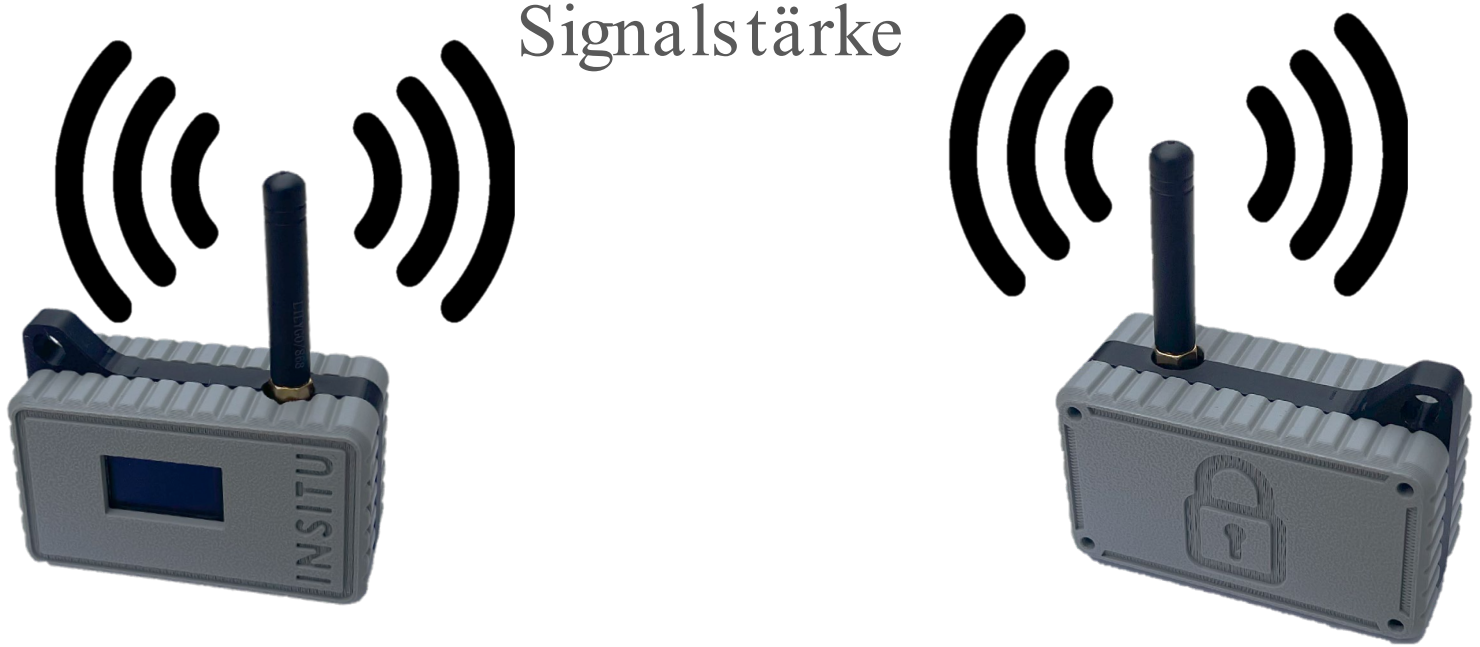


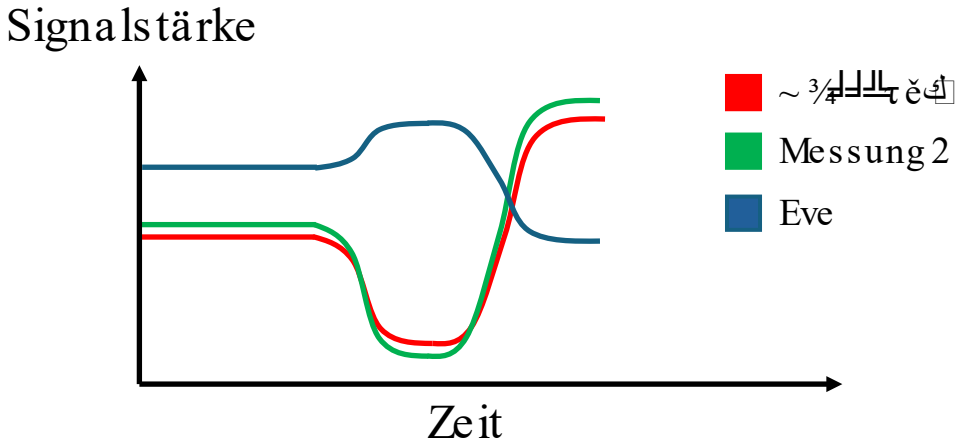
Wie Signalstärke





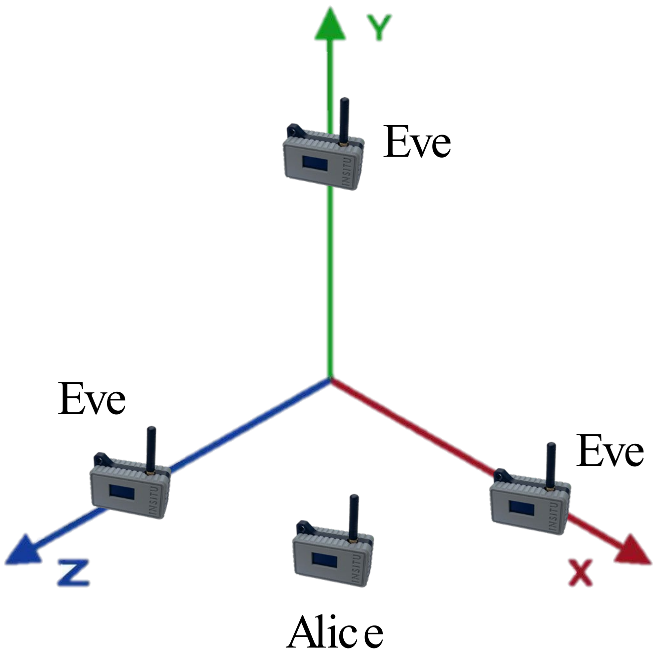
Wie Signalstärke





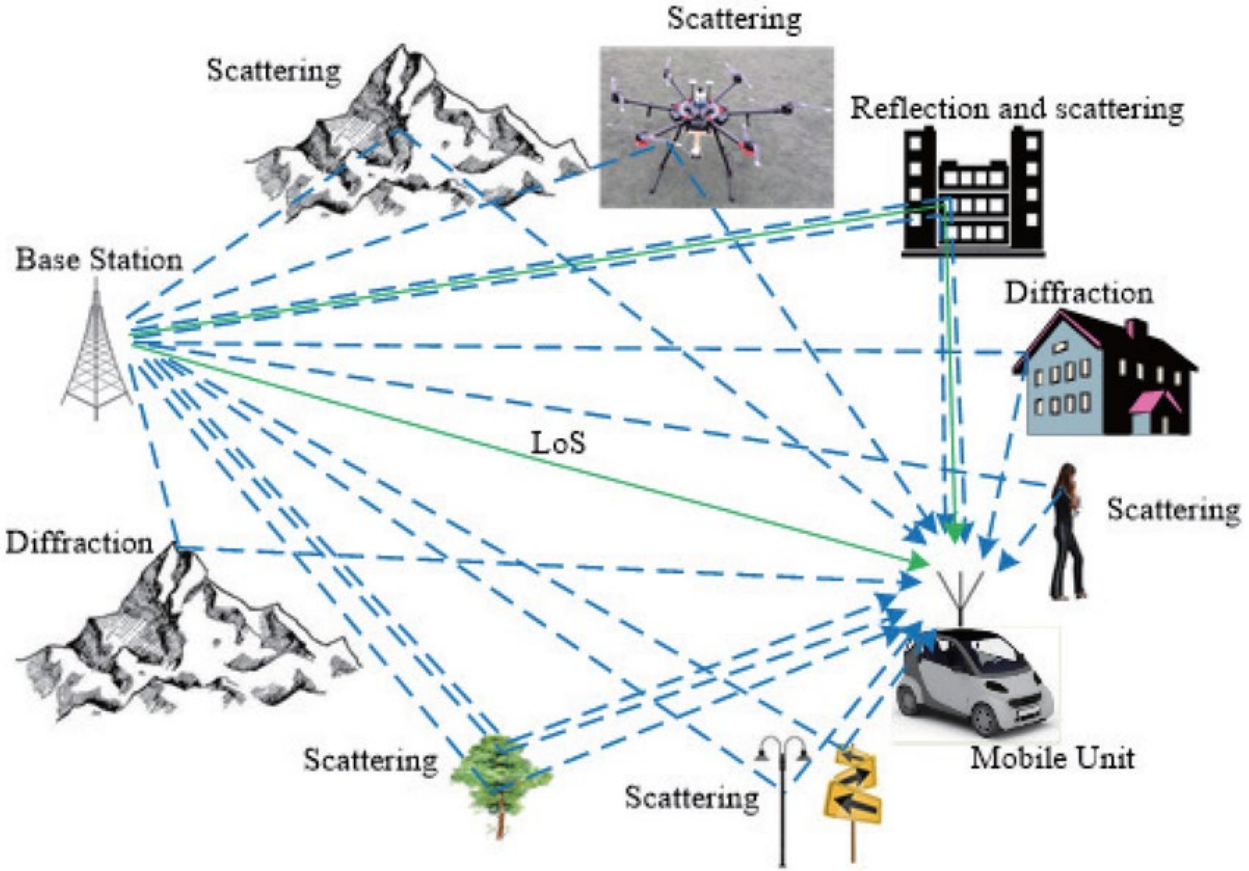
Wie

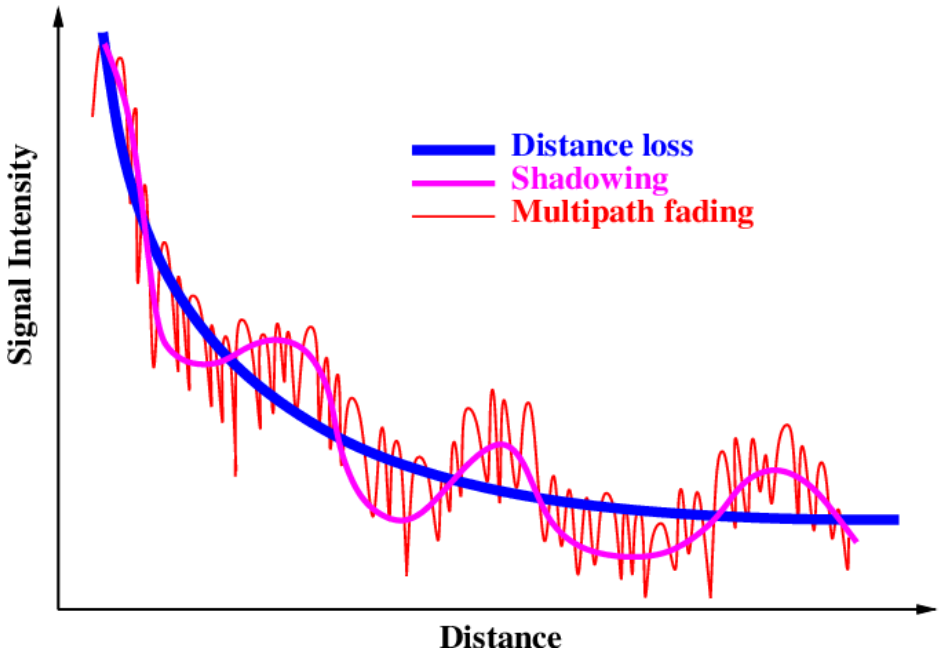
ðŃلكÏ╛ك╥ĭ τ ě╧Ĭŋ¾╗¾ŏŃﻣ



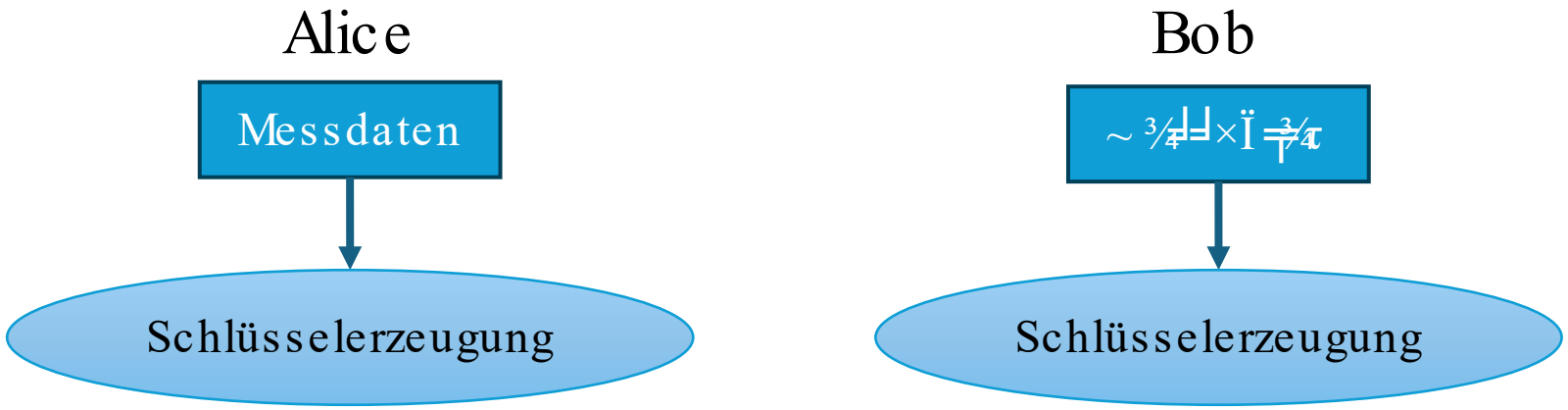
Wie

Good Luck



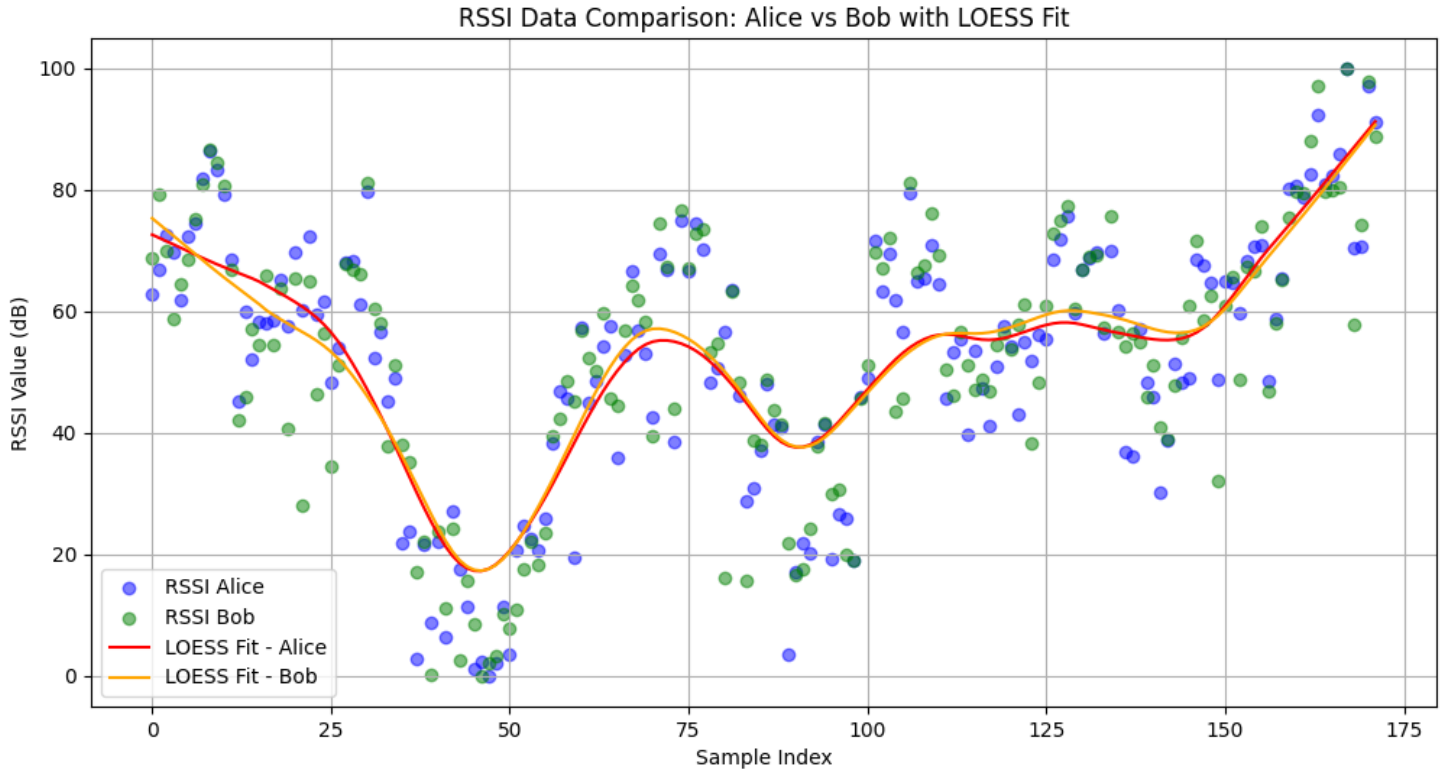


Wie


Alice
Messdaten
Schlüsselerzeugung
Bob
Schlüsselerzeugung

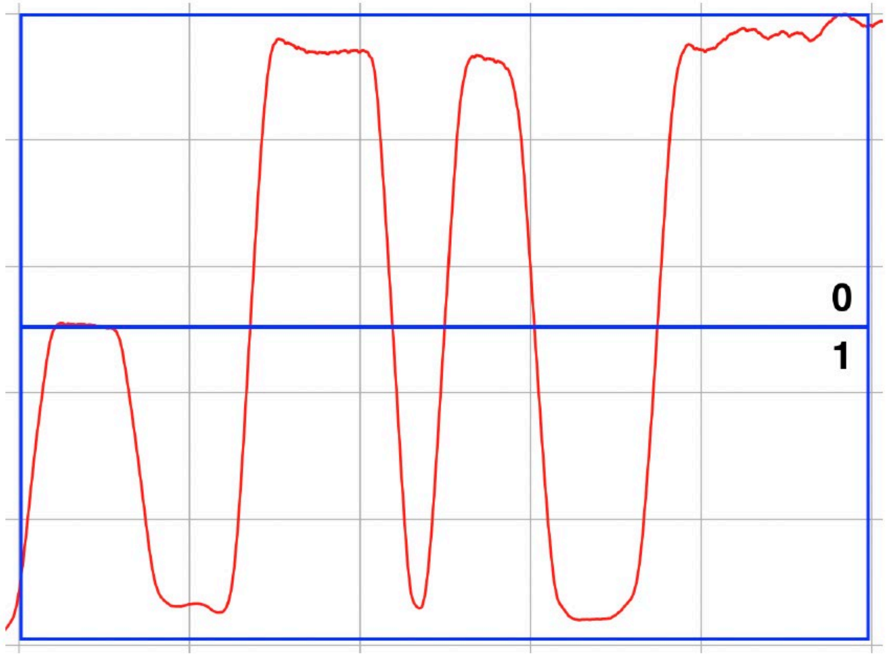
Wie

Schlüsselerzeugung

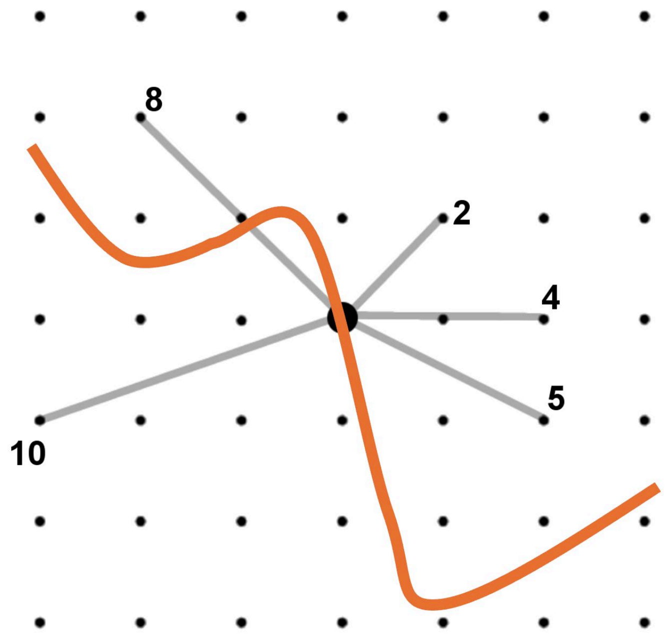


Wie ©ǒŃ▀╝╛¾Ґ¾╗ç¾╩ě╧τ ě

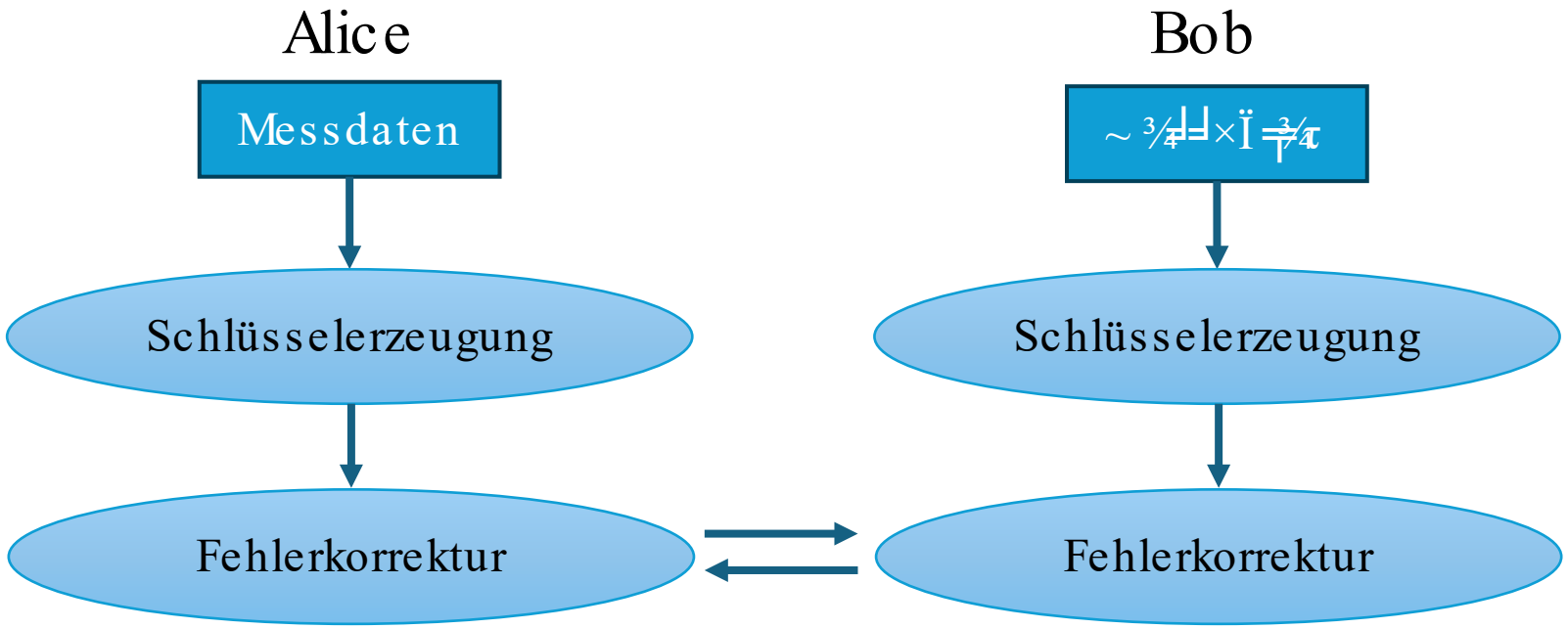
1	0	0	1	0



(a) 1-Bit Auflösung

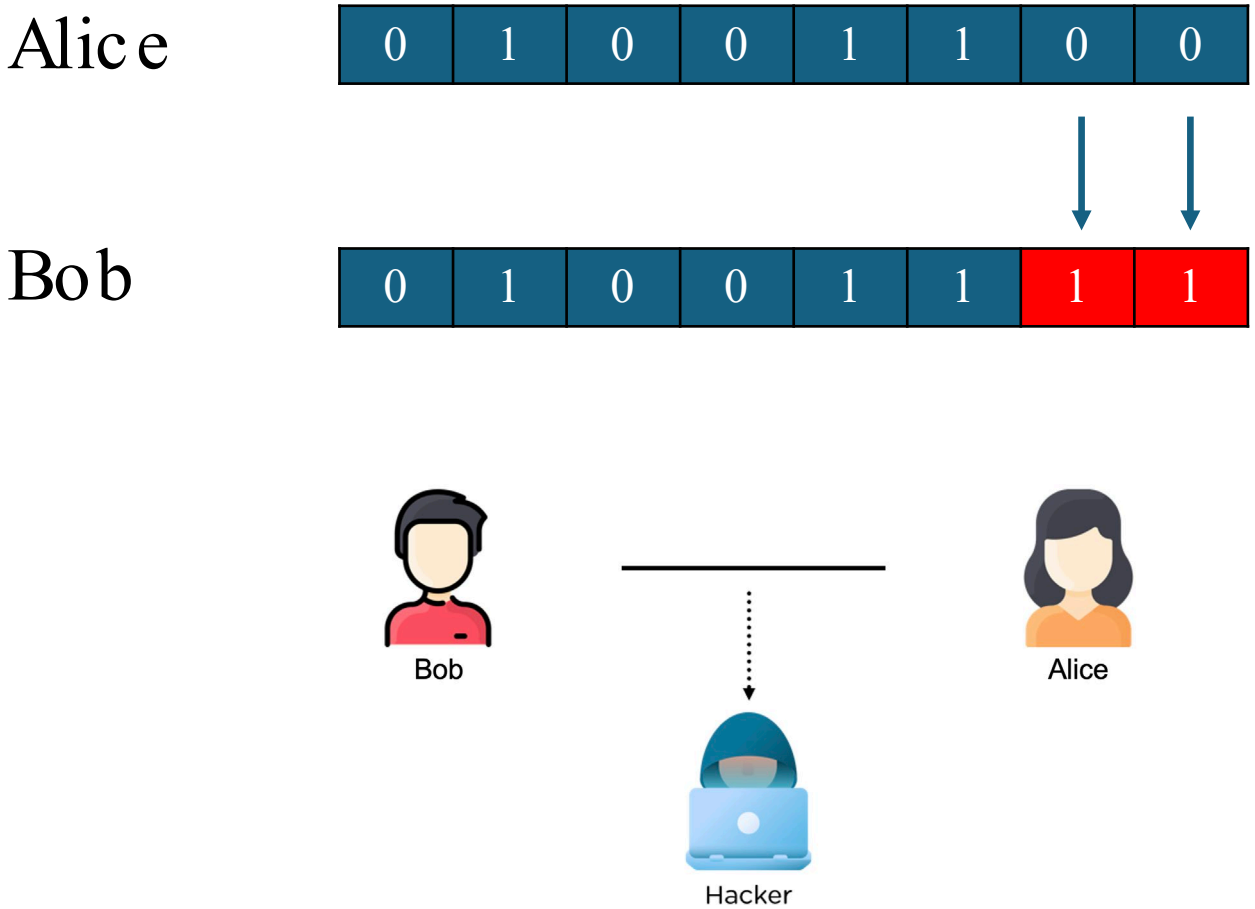


Wie


Alice
Bob
Messdaten
~ ¾╩═×Ï═¾τ
Schlüsselerzeugung
Schlüsselerzeugung
Fehlerkorrektur
Fehlerkorrektur

Wie

Fehlerkorrektur

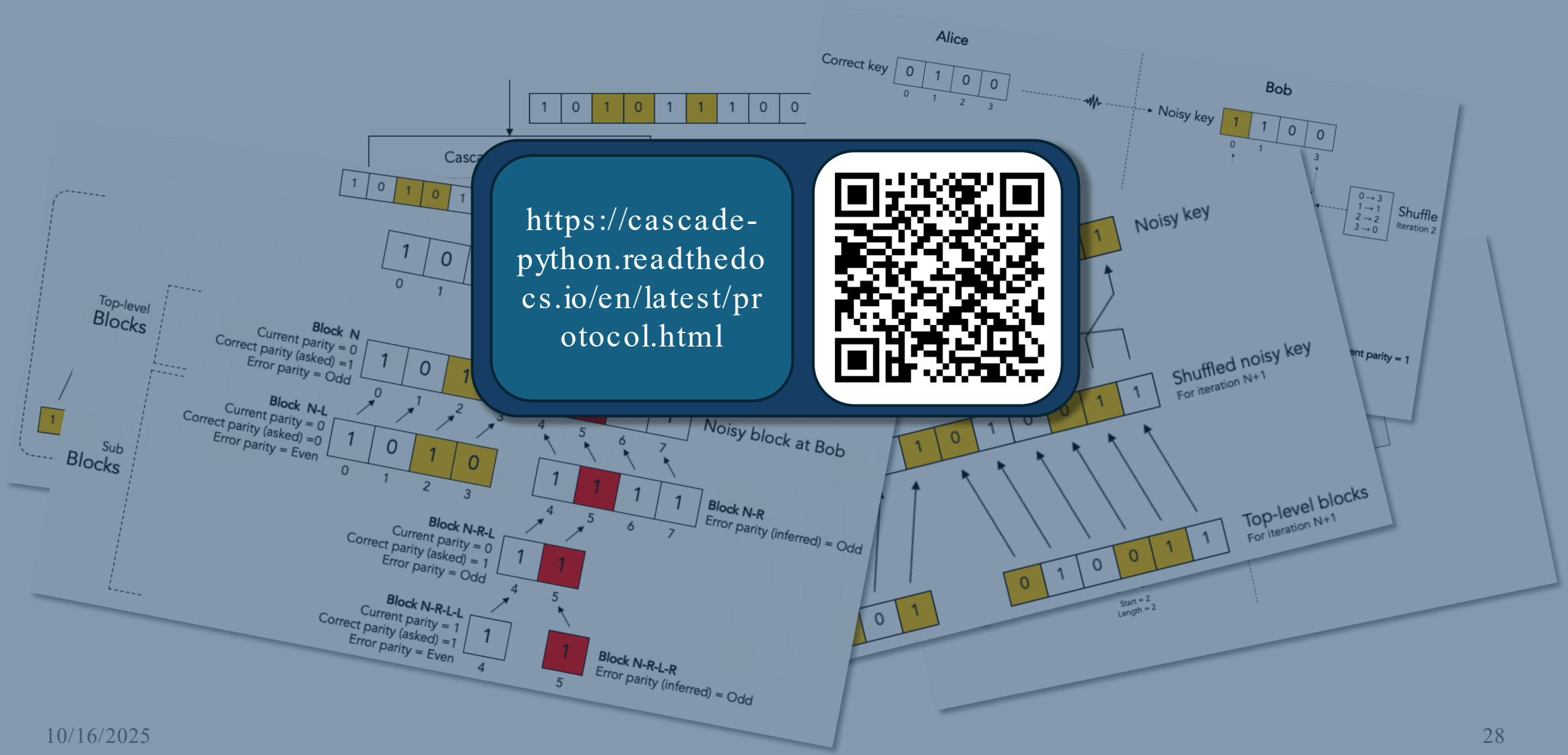


Wie

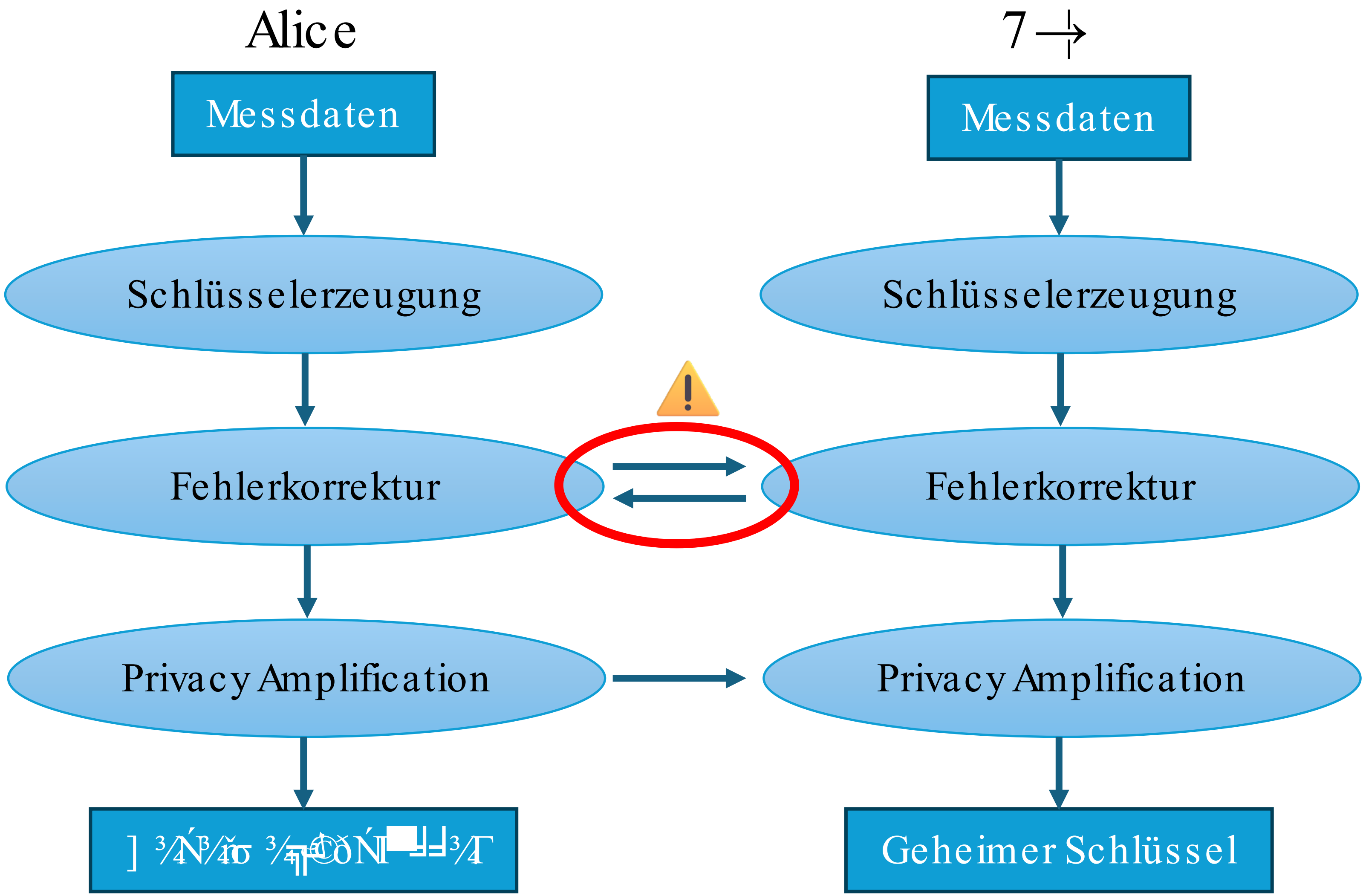
Cascade Error Correction

Wie

Cascade Error Correction

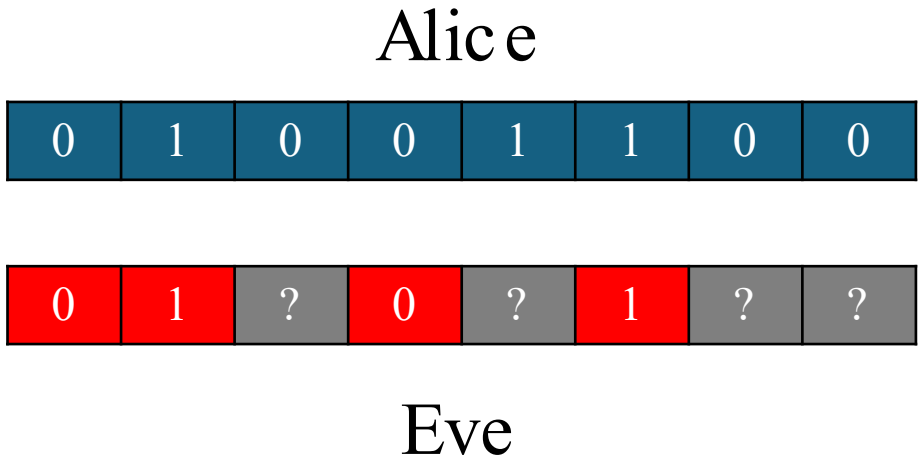


Õ ň¾


Alice
Messdaten
Messdaten
Schlüsselerzeugung
Schlüsselerzeugung
Fehlerkorrektur
Fehlerkorrektur
Privacy Amplification
Privacy Amplification
Geheimer Schlüssel

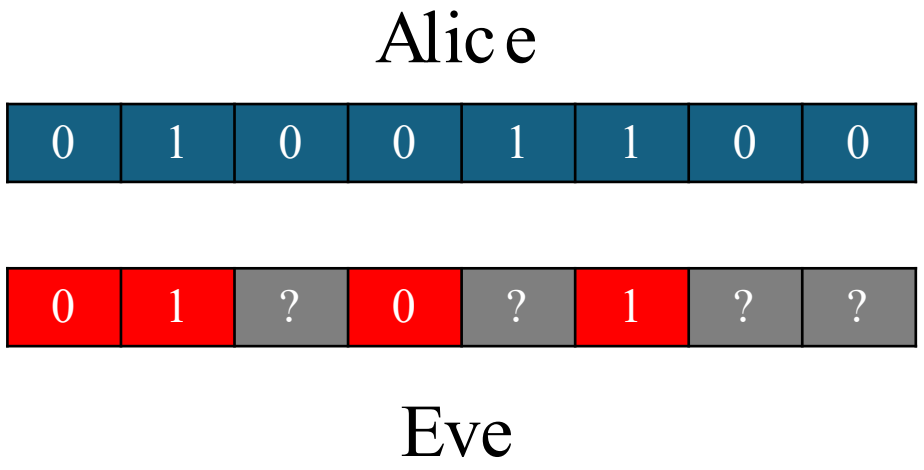
Wie

Privacy Amplification



Wie

Privacy Amplification



Leftover Hash Lemma:

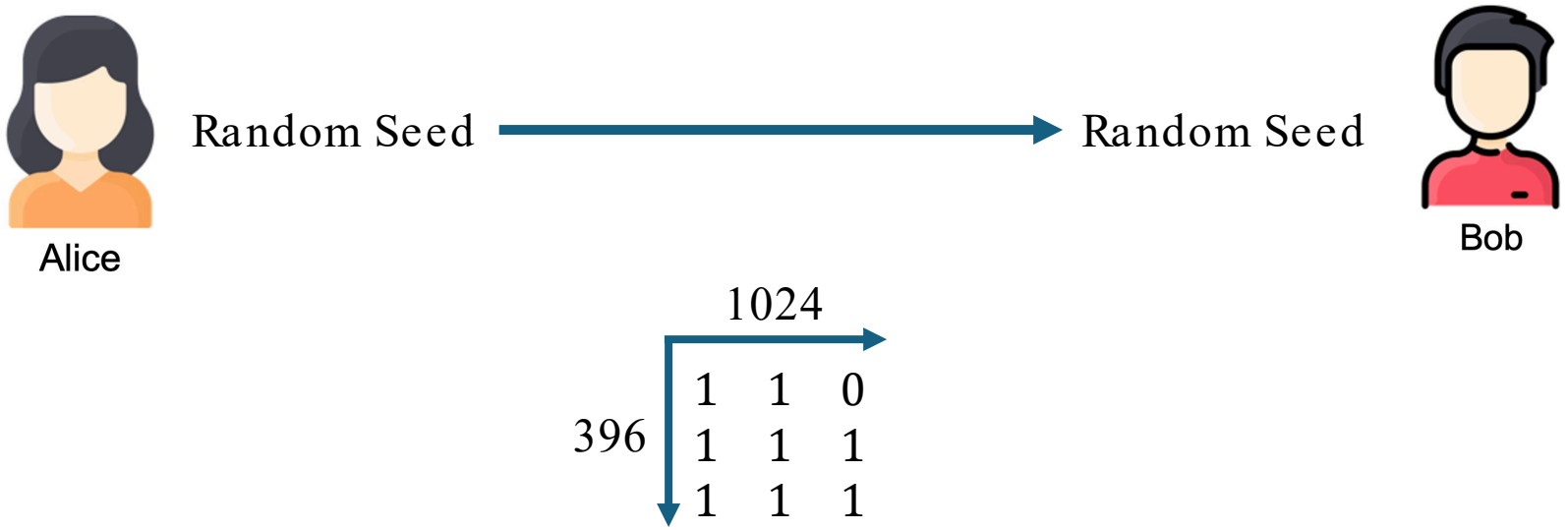
$Roher\ Schlüssel = X$
$Schlüssel\ Bits = n = 1024\ Bits$
$Leaked\ Bits = t = 500\ Bits$
$Sicherheitsmarge = □ = 128\ Bits$

$Sicherer\ Schlüssel = n - t - □ = 396\ Bits$

Wie

Privacy Amplification

$Schlüssel\ Bits = n = 1024\ Bits$
$Sicherer\ Schlüssel = s = 396\ Bits$



Wie

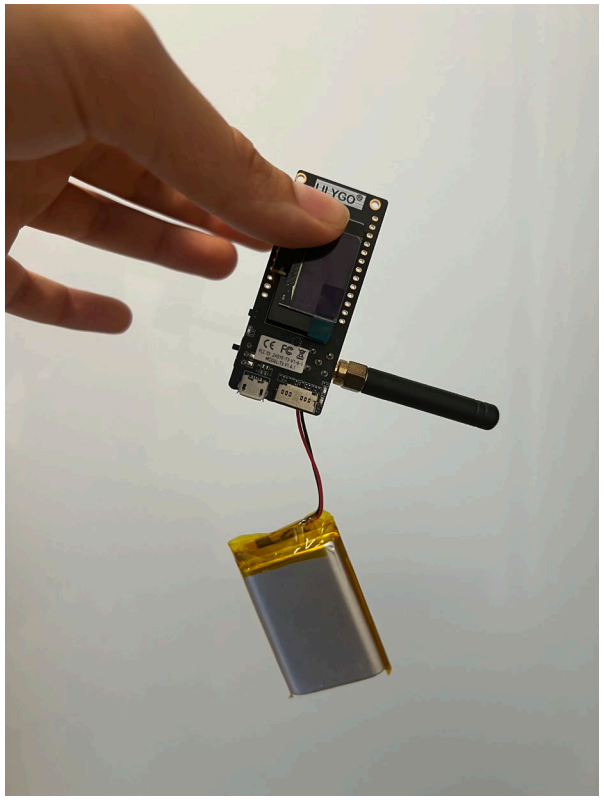
Privacy Amplification

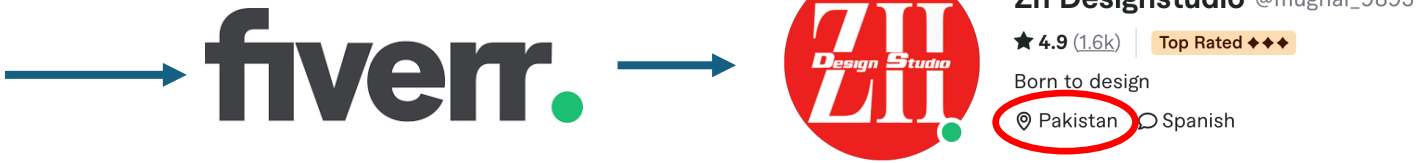
$Schlüssel\ Bits = n = 1024\ Bits$
$Sicherer\ Schlüssel = s = 396\ Bits$

$$1\ \ 0\ \ 1\ \ldots \times \begin{matrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{matrix} = 0\ \ 1\ \ldots$$

Wie

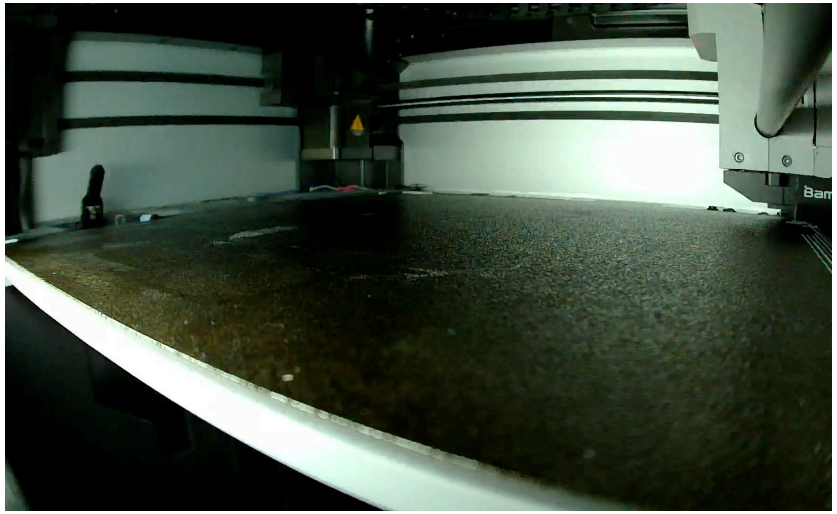
Gehäuse

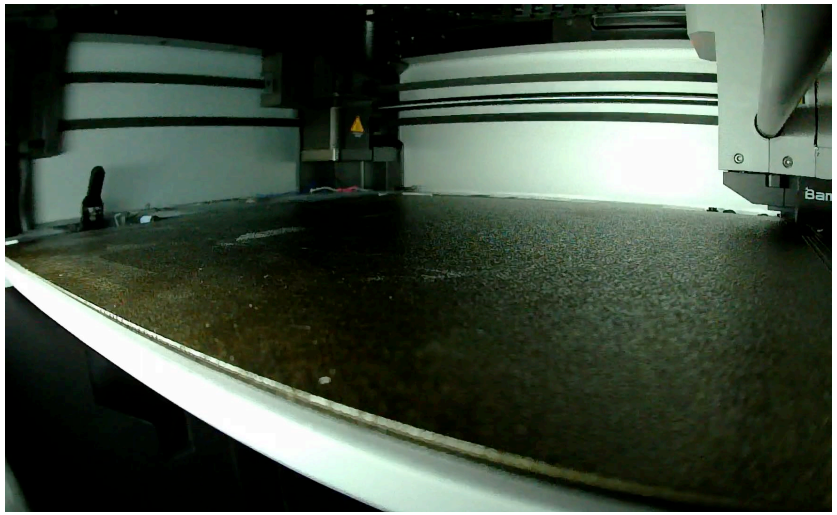



fiverr.
Zh Designstudio @mughal_9895
4.9 (1.6k)
Top Rated
Born to design
Pakistan
Spanish

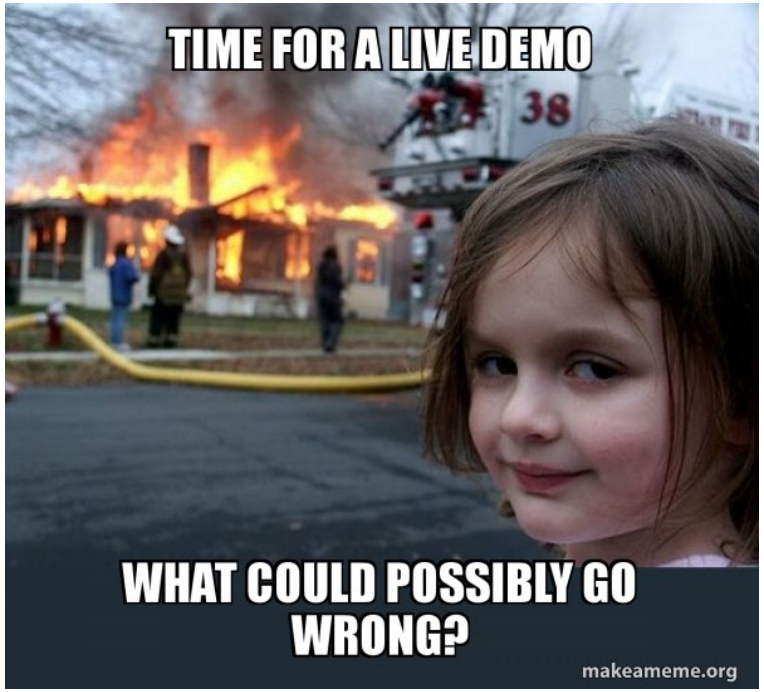
Õ ñ¼

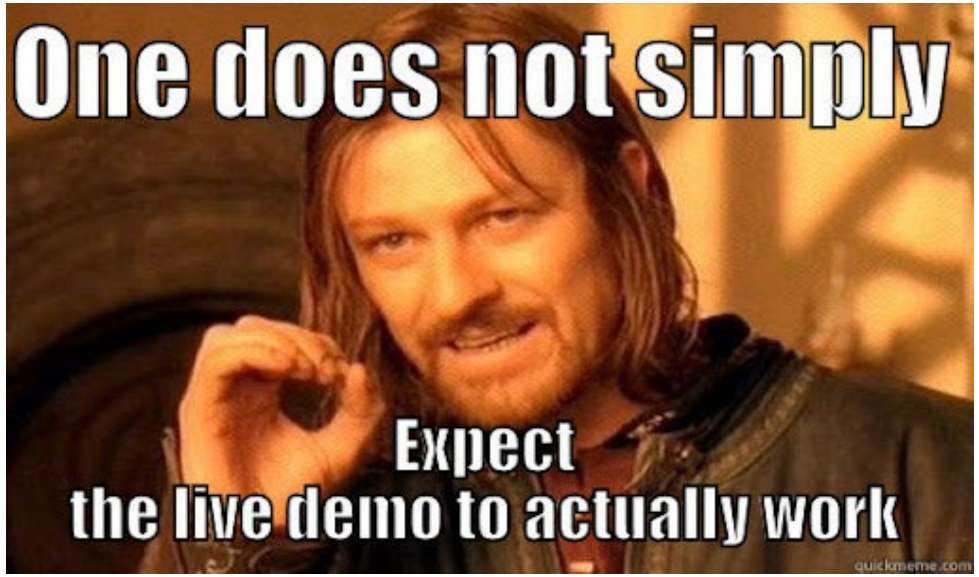
Gehäuse

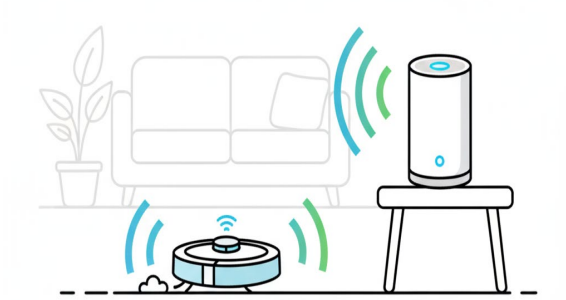


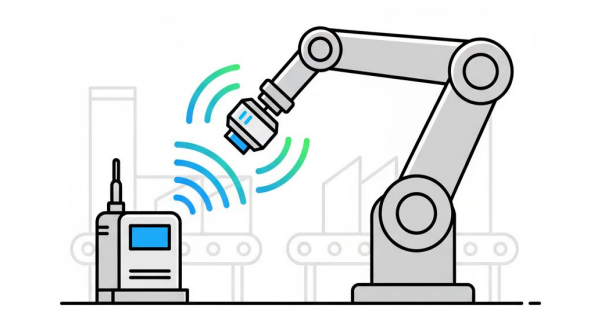


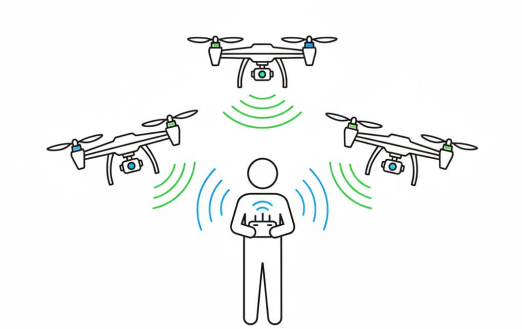
Live Demo


TIME FOR A LIVE DEMO
WHAT COULD POSSIBLY GO WRONG?
makeameme.org


One does not simply
Expect
the live demo to actually work
quickmeme.com







Wofür

Umfeld mit unvermeidbarer Dynamik