Funded by
DFG Deutsche Forschungsgemeinschaft
German Research Foundation

SEITENKANALANGRIFFE: WENN HACKER ZWISCHEN DEN ZEILEN LESEN

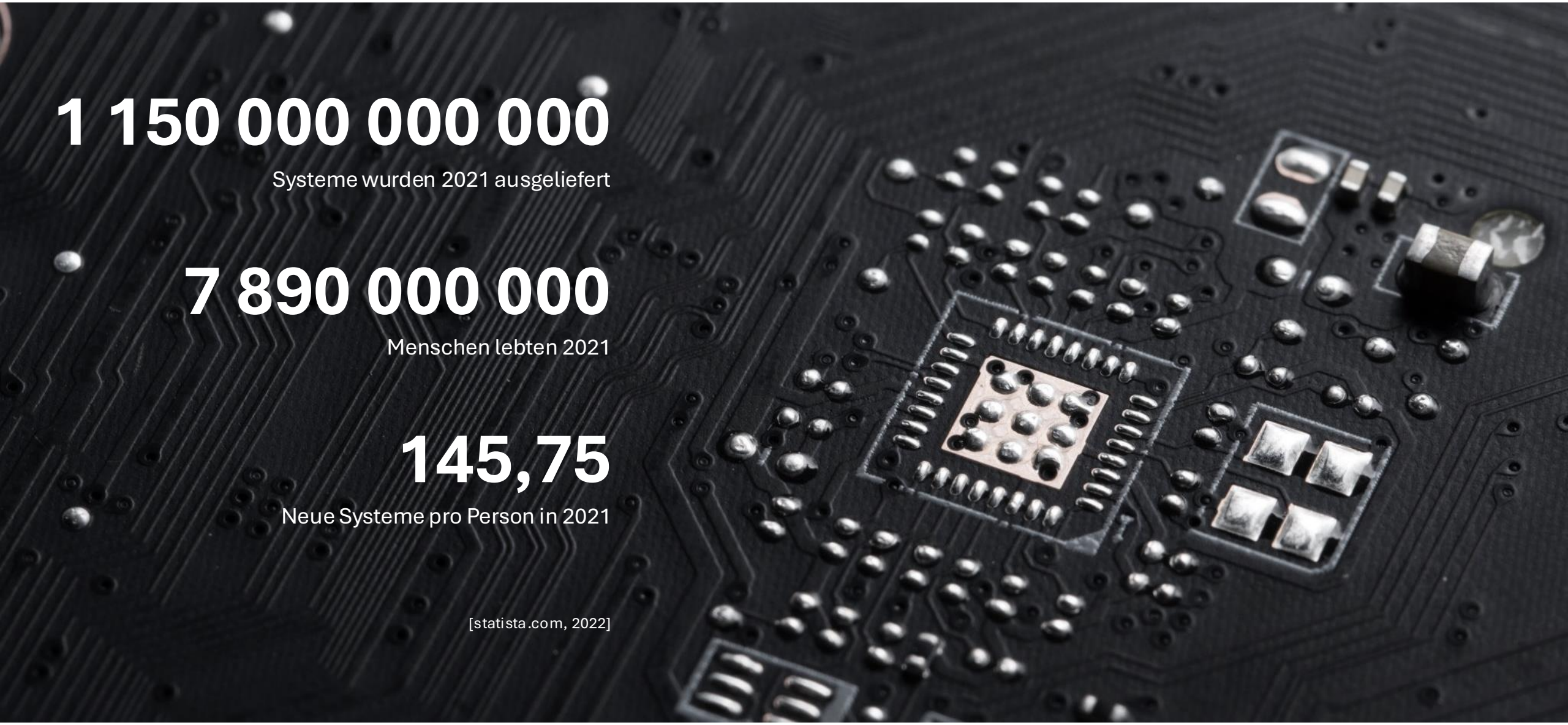
PASCAL SASDRICH

EMMY NOETHER-FORSCHUNGSGRUPPE CAVE
RUHR-UNIVERSITÄT BOCHUM

BITTE WÄHLEN SIE ALLE BILDER MIT EINEM COMPUTER AUS...

EINGEBETTETE SYSTEME SIND UNSICHTBARE COMPUTER

SCHÄTZEN SIE EINMAL, WIE VIELE SYSTEME 2021 PRODUZIERT WURDEN...



1 150 000 000 000

Systeme wurden 2021 ausgeliefert

7 890 000 000

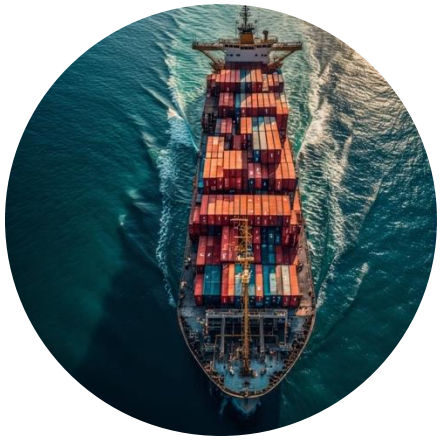
Menschen lebten 2021

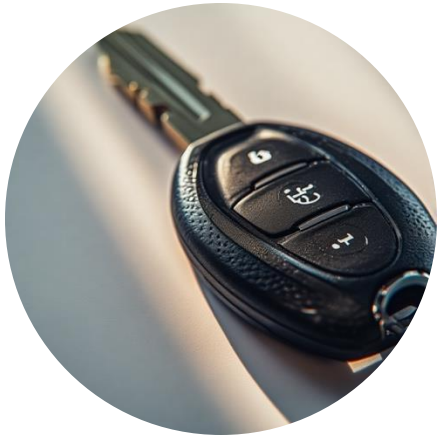
145,75

Neue Systeme pro Person in 2021

[statista.com, 2022]

WAS MACHT EIGENTLICH SO EIN EINGEBETTES SYSTEM?





- STEUERN
- MESSEN
- REGELN
- KOMMUNIZIEREN
- KRYPTOGRAPHIE

Image sources: https://perchance.org/

KRYPTOGRAPHIE – DIE WISSENSCHAFT DER SICHEREN KOMMUNIKATION

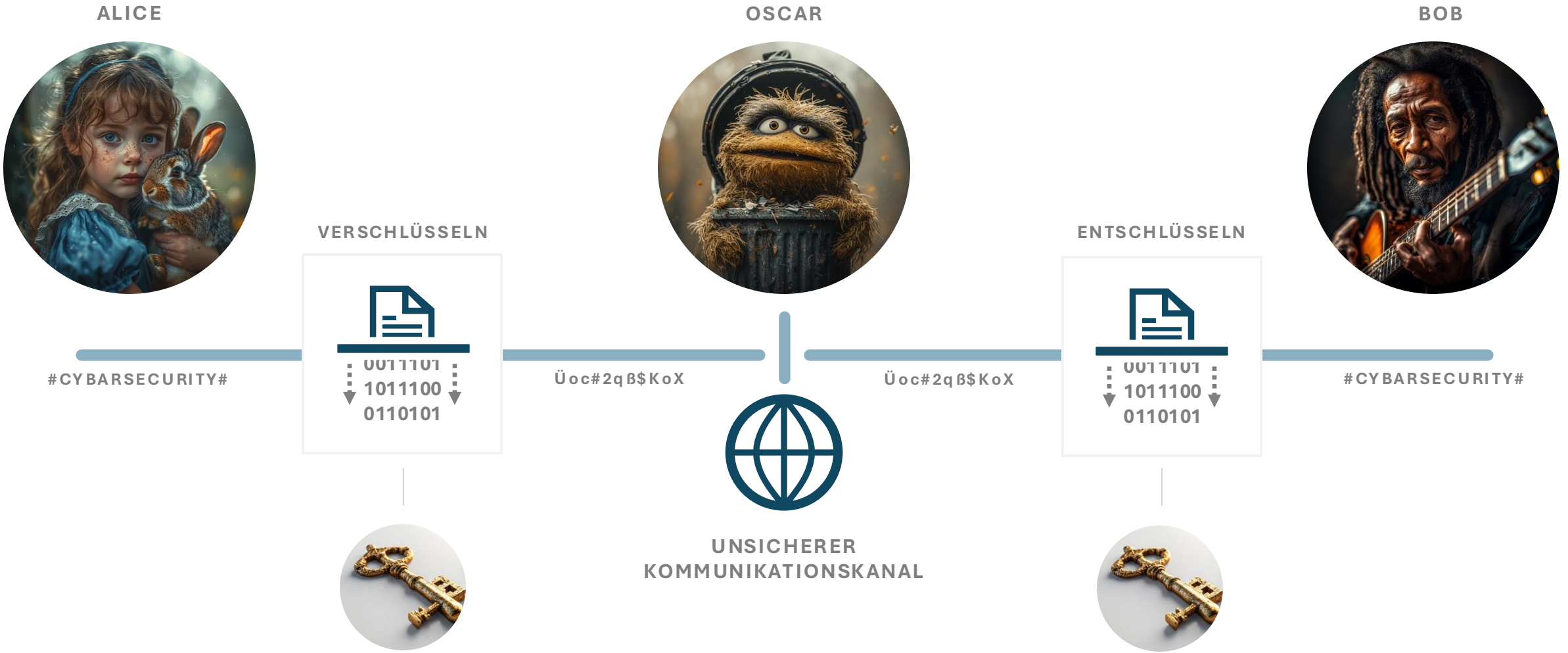
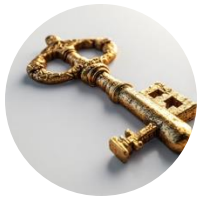


Image sources: https://perchance.org/

BEISPIEL: SYMMETRISCHE KRYPTOGRAPHIE IM AUTOSCHLÜSSEL

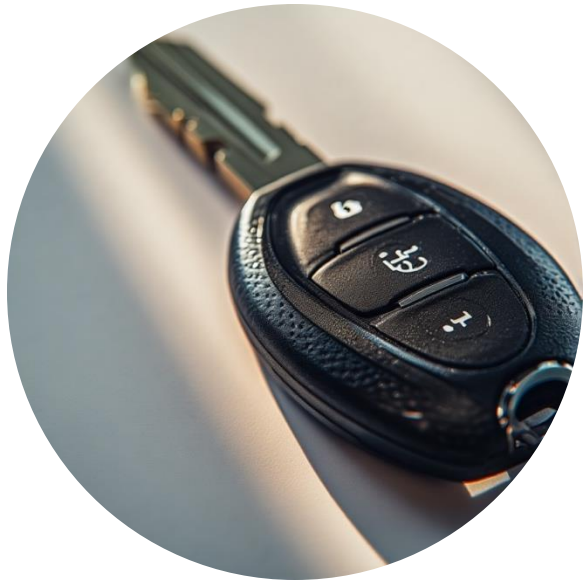
SPORTWAGEN



ZUFALLSZAHL (NONCE) UND ZEITSTEMPEL

VERSCHLÜSSELTE ZUFALLSZAHL UND ZEITSTEMPEL

AUTOSCHLÜSSEL



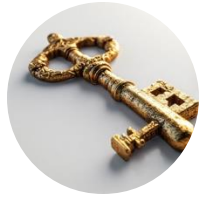


Image sources: https://perchance.org/

MODERNE KRYPTOGRAPHIE IST MATHEMATISCH HART ZU KNACKEN...

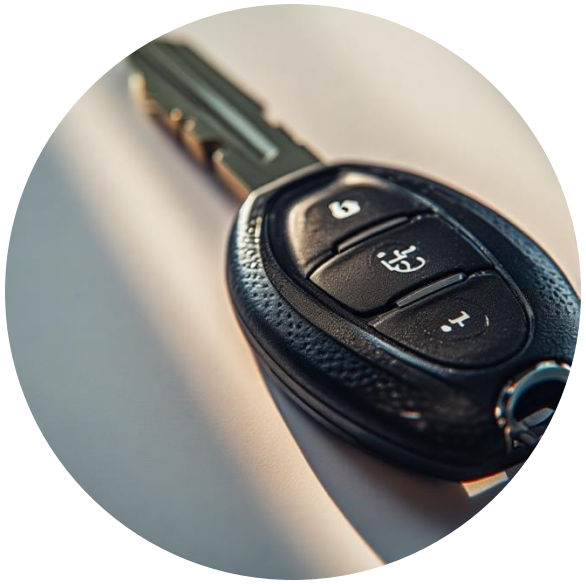
MATHEMATIKER:IN

ZIEL: GEHEIMEN SCHLÜSSEL LERNEN

SENDET BELIEBIGE ANFRAGEN

BEOBACHTET ALLE ANTWORTEN

KRYPTOGRAPHISCHES GERÄT



MODERNE KRYPTOGRAPHIE IST
MATHEMATISCH HART ZU BRECHEN.

Image sources: https://perchance.org/

… ABER KRYPTOGRAPHIE AUF EINGEBETTETE SYSTEME KANN PRAKTISCH GEBROCHEN WERDEN!

TÜFTLER:IN

ZIEL: GEHEIMEN SCHLÜSSEL LERNEN

SENDET BELIEBIGE ANFRAGEN

BEOBACHTET DAS VERHALTEN DES GERÄTS

KRYPTOGRAPHISCHES GERÄT

DIE UMSETZUNG (IMPLEMENTIERUNG) DER KRYPTOGRAPHISCHEN FUNKTIONEN WEISST SCHWACHSTELLEN AUF.

Image sources: https://perchance.org/

SEITENKANALANGRIFFE – WENN DER HACKER ZWISCHEN DEN ZEILEN LIEST

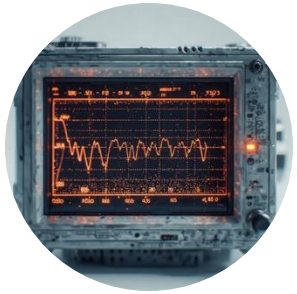
ZEIT

KRYPTOGRAPHISCHES GERÄT

WÄRME

JEGLICHE MESSBARE PHYSIKALISCHE GRÖSSE KANN GEHEIME INFORMATIONEN TRANSPORTIEREN

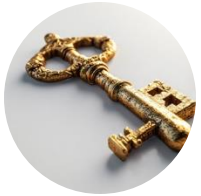
STROM



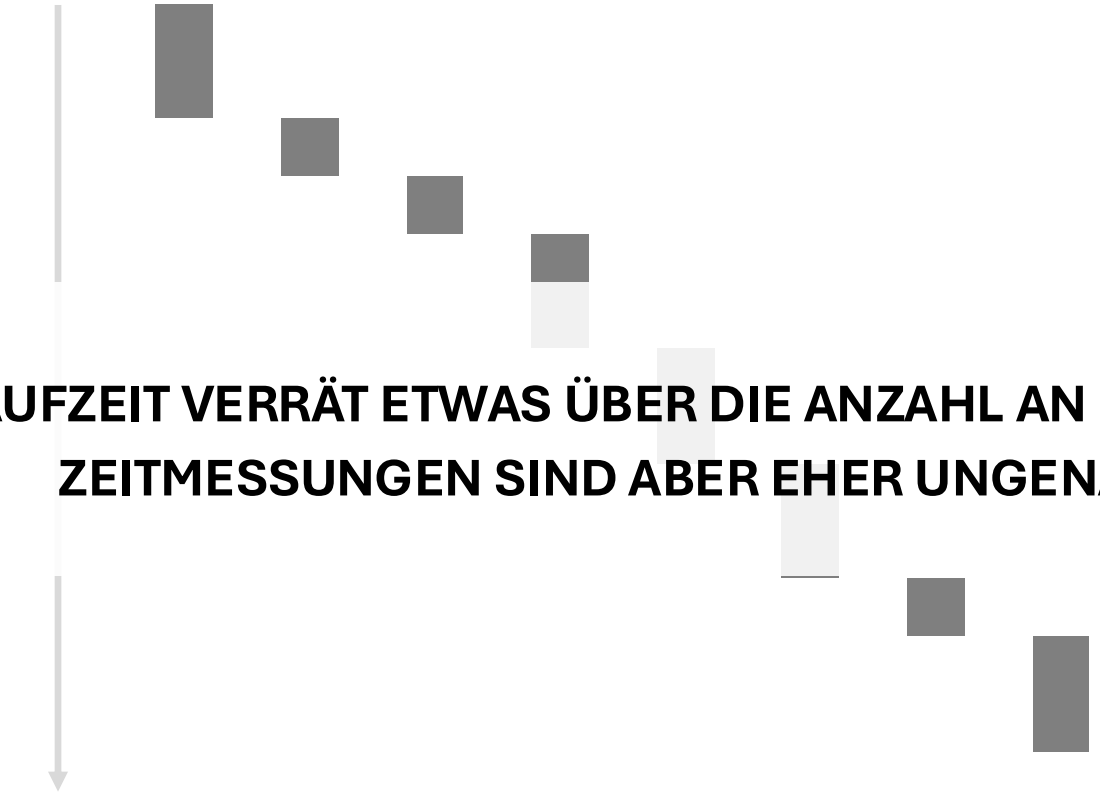
MAGNETISMUS

Image sources: https://perchance.org/

SEITENKANALANGRIFFE – WENN'S LÄNGER DAUERT...



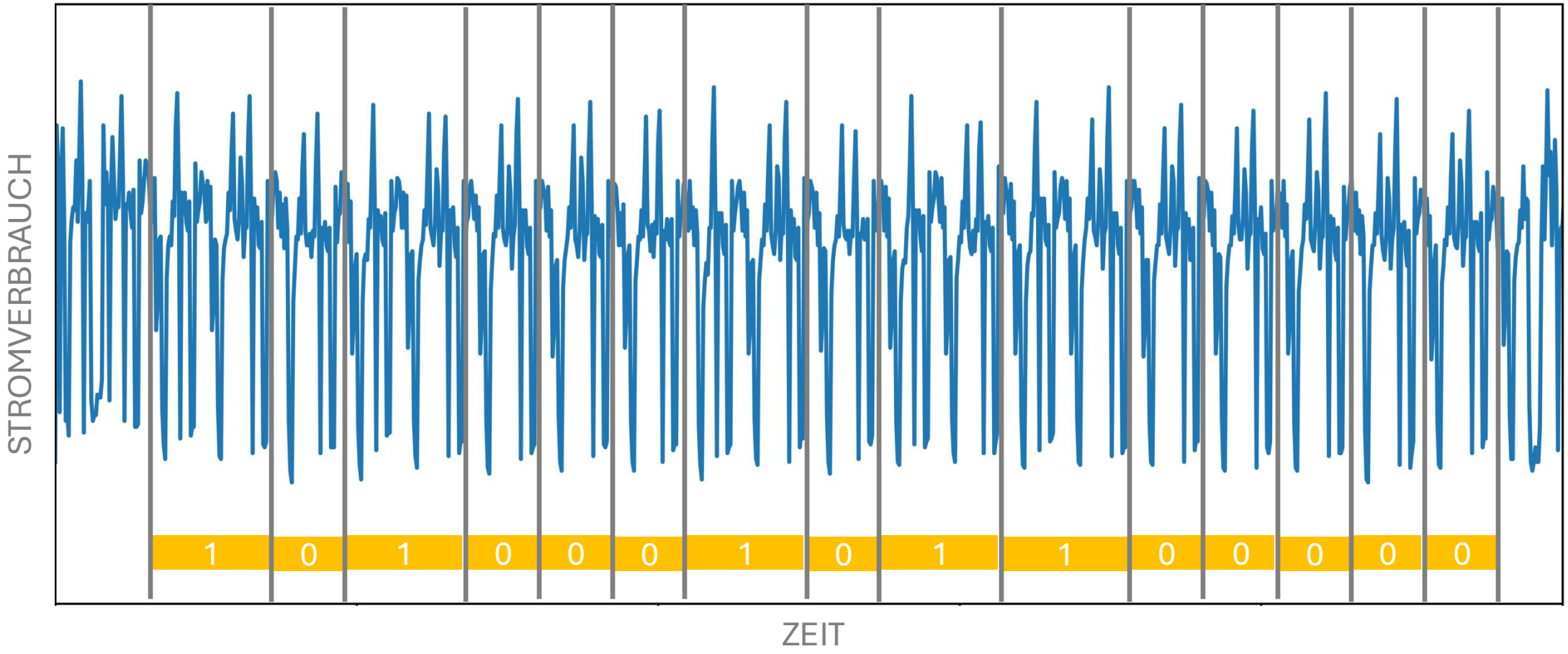
... 1 0 0 1 1 1 0 1 ...



LAUFZEIT VERRÄT ETWAS ÜBER DIE ANZAHL AN EINSEN.
ZEITMESSUNGEN SIND ABER EHER UNGENAU.

PANZERKNACKER:IN

SEITENKANALANGRIFFE – DER STROMVERBRAUCH VERRÄT (FAST) ALLES…

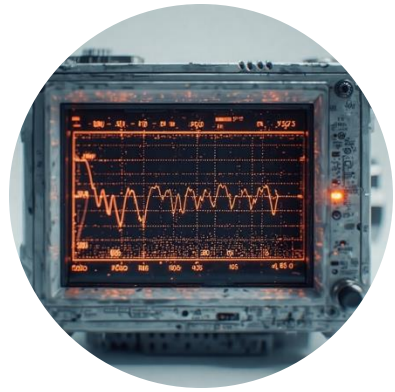


UND WIE FUNKTIONIERT DAS JETZT IN DER PRAXIS?

STROMVERSORGUNG

MESSAUFBAU

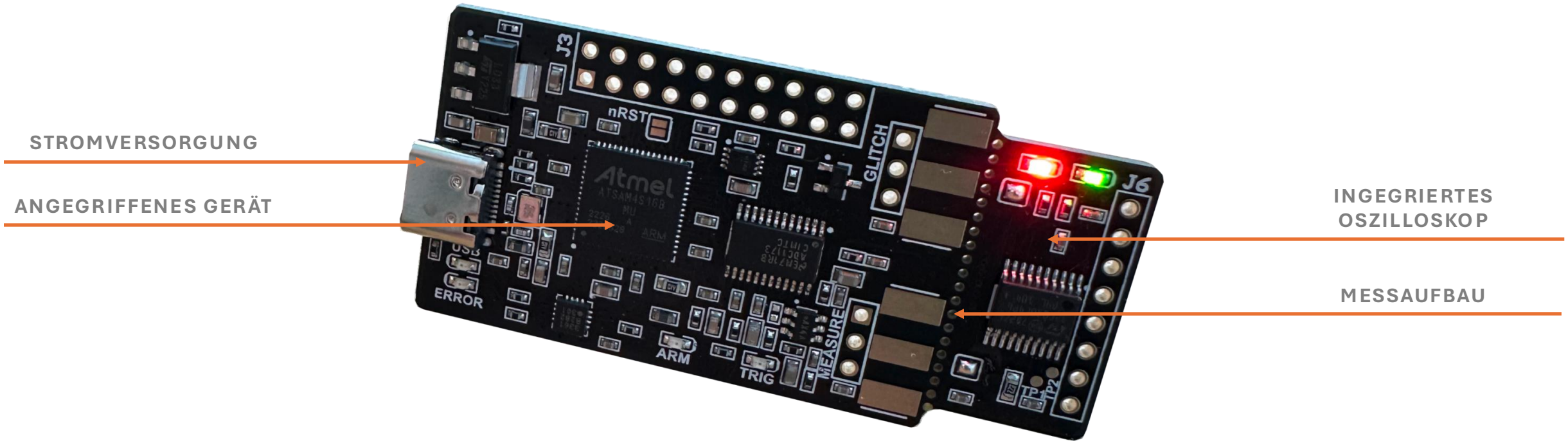
DIGITALES OSZILLOSKOP



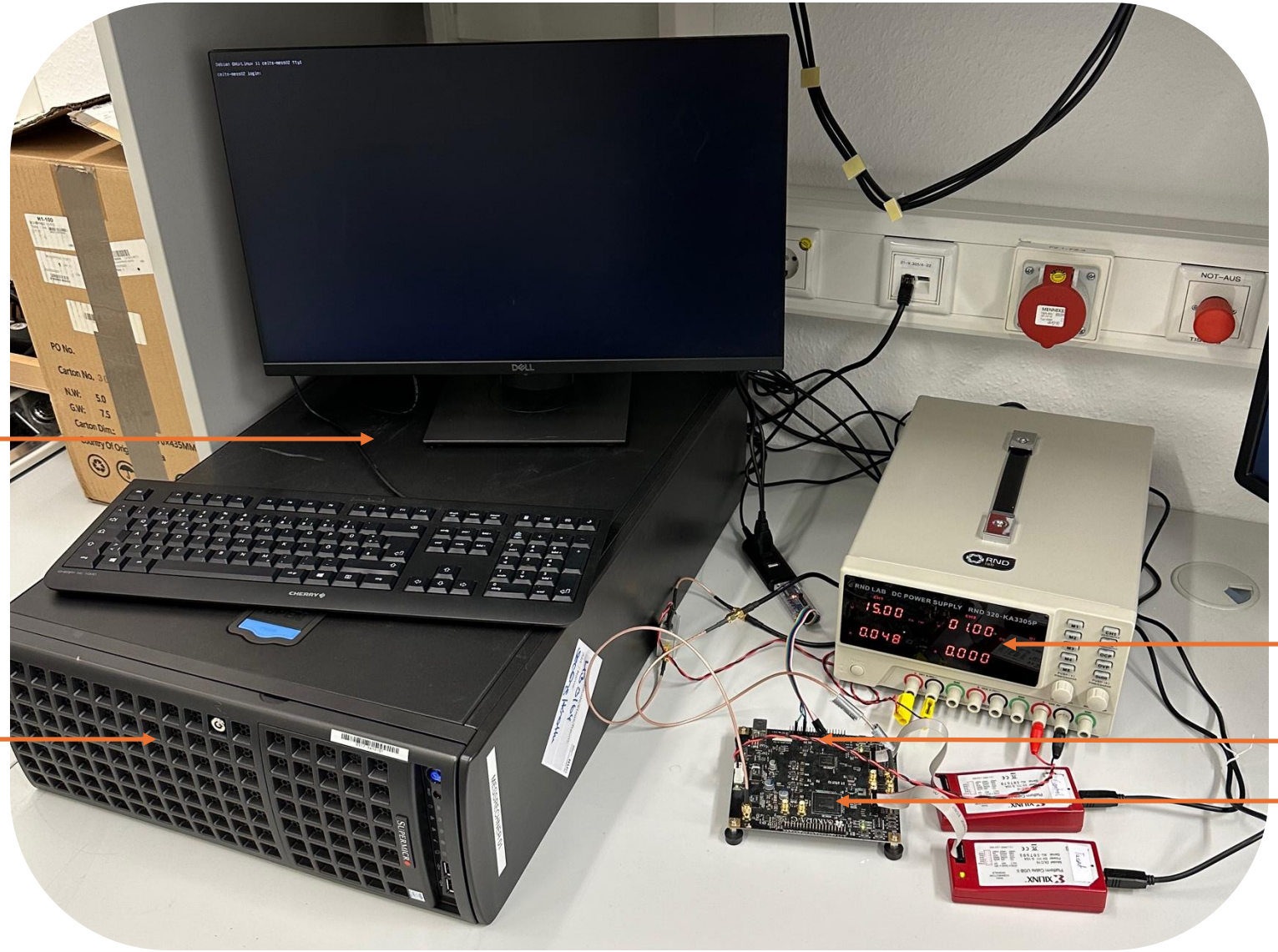
ANGEGRIFFENES SYSTEM

MESSRECHNER

BEISPIEL: EIN EINSTEIGER-SETUP...



BEISPIEL: HIGH-PERFORMANCE MESSAUFBAU



ZUSAMMENFASSUNG UND FORSCHUNGSTHEMEN

SEITENKANALANGRIFFE SIND SEIT 1996 BEKANNT.

Seitdem wird u. a. an folgenden Fragen und Themen geforscht:

- *Wie können Angriffe verstanden und verbessert werden?*
- *Wie kann Maschinelles Lernen bei Angriffen helfen?*
- *Wie können wir unsere eingebetteten Systeme gegen Seitenkananalgriffe schützen?*
- *Wie können wir zeigen und beweisen, dass Systeme sicher und geschützt sind?*
- ...

HABEN SIE FRAGEN?

PASCAL SASDRICH
pascal.sasdrich@rub.de