SICHERHEITSASPEKTE DER DIGITALISIERUNG: WAS CONTROLLER ALLES PREISGEBEN

Microtec Nord 2018

Prof. Dr. Heike Neumann
HAW Hamburg
Fakultät Technik und Informatik, Department Informations- und Elektrotechnik

HAW HAMBURG

Was ich vorhabe ….

- Überblick über Hardware Angriffe
- Kurze Einführung zur Kryptographie
- Zwei Beispiele für Hardware Attacken auf den RSA

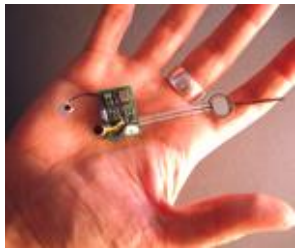
HAW HAMBURG

IT-SICHERHEIT?!

DAS ANGRIFFSSZENARIO

Das Zielobjekt: Elektronisches Gerät mit Sicherheitsfunktion

- **Sicherheit ist durch kryptographische Methoden implementiert**
- **Sicherheit beruht auf der Geheimhaltung eines kryptographischen Schlüssels, der im Gerät gespeichert ist**

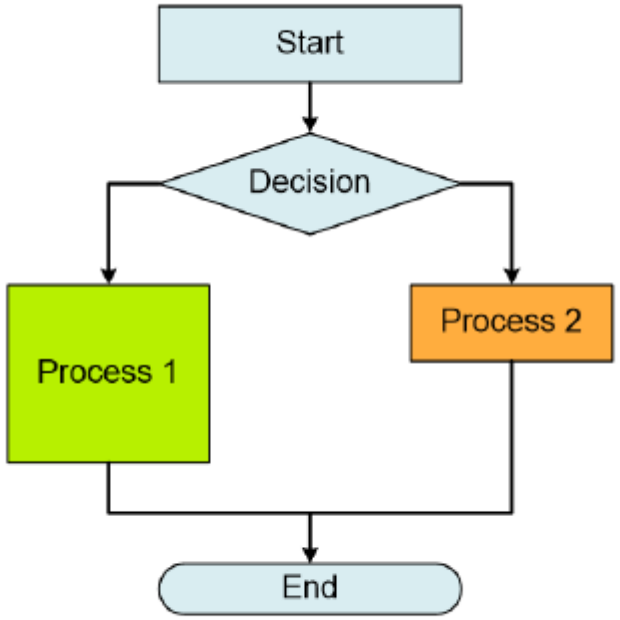


Der Angreifer: der Besitzer des Geräts - oder nur mit Zugriff auf das Gerät

WIE MAN CONTROLLER DIREKT ATTACKIEREN KANN

- Invasive Angriffe
- Semi-invasive Angriffe
- Nicht-invasive Angriffe

NICHT-INVASIVE ANGRIFFE: PERFORMANCE UND STROMPROFILANALYSEN



Die Ausführungszeit hängt von den Daten ab.

Die Laufzeit des Programms gibt das Geheimnis preis.

BEISPIEL 1: PIN VERIFIKATION

- 8 Ziffern PIN Code als Zugangscode
- Annahme: Eingabe der PIN braucht rund eine Minute
- Vollständige Suche:

$$\frac{\frac{1}{2}\cdot 10^8}{60\cdot 24\cdot 365} \approx 95\ years$$

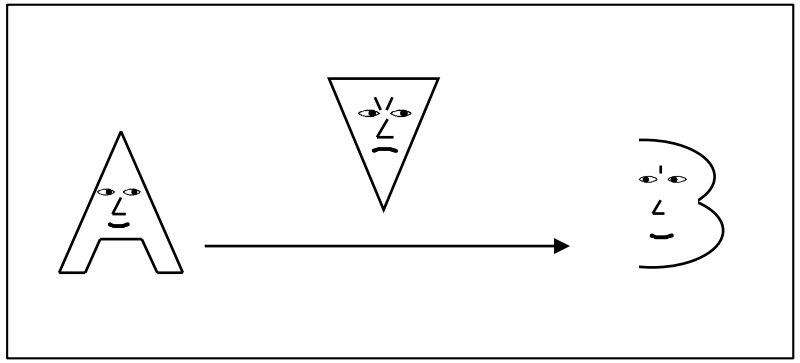
TIMING ANGRIFF AUF NAIVE IMPLEMENTIERUNG

- **Naive Implementation der PIN VerifiKation:**

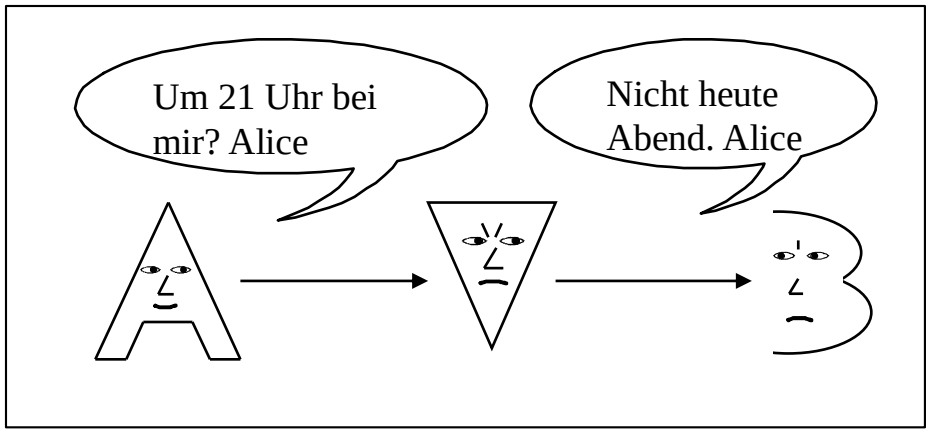
```
for i=0 to 7{
  if PIN[i] != userInput[i]{
    return error;
  }
}
return ok;
```

- **Der Angriff:**
  - **Teste alle 10 Möglichkeiten für die erste Ziffer und messe die Ausführungszeit**
  - **Bei der korrekten ersten Ziffer ist die Ausführungszeit länger**
  - **Teste alle 10 Möglichkeiten für die zweite Ziffer …**
  - **Dauer des Angriffs: maximal 80 Minuten**

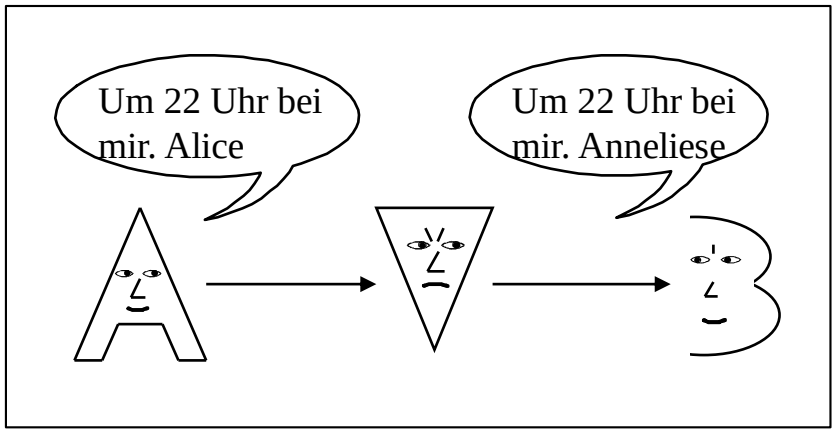
SCHUTZZIELE MIT KRYPTOGRAPHISCHEN METHODEN



VERTRAULICHKEIT

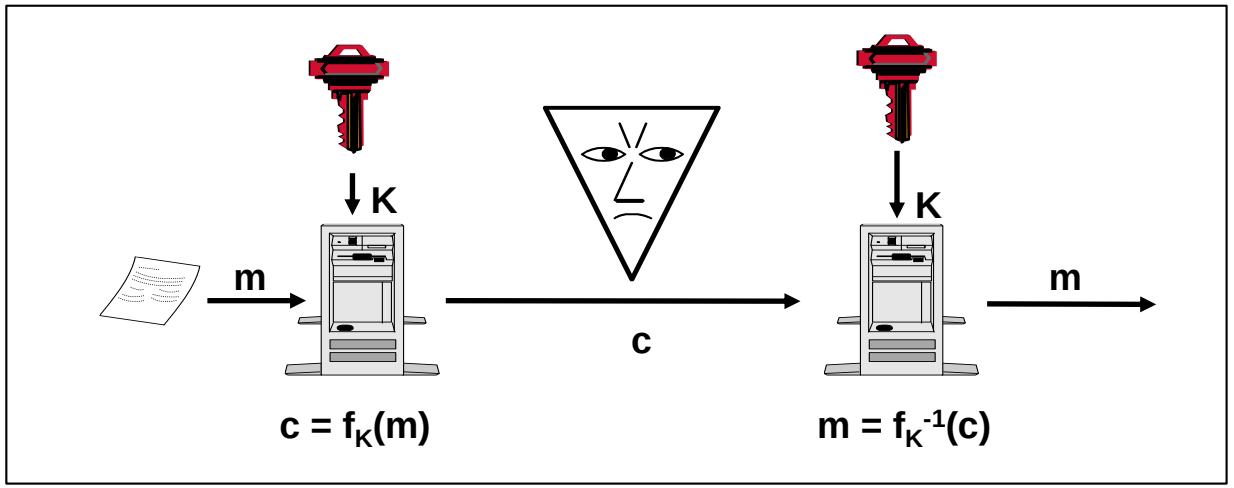


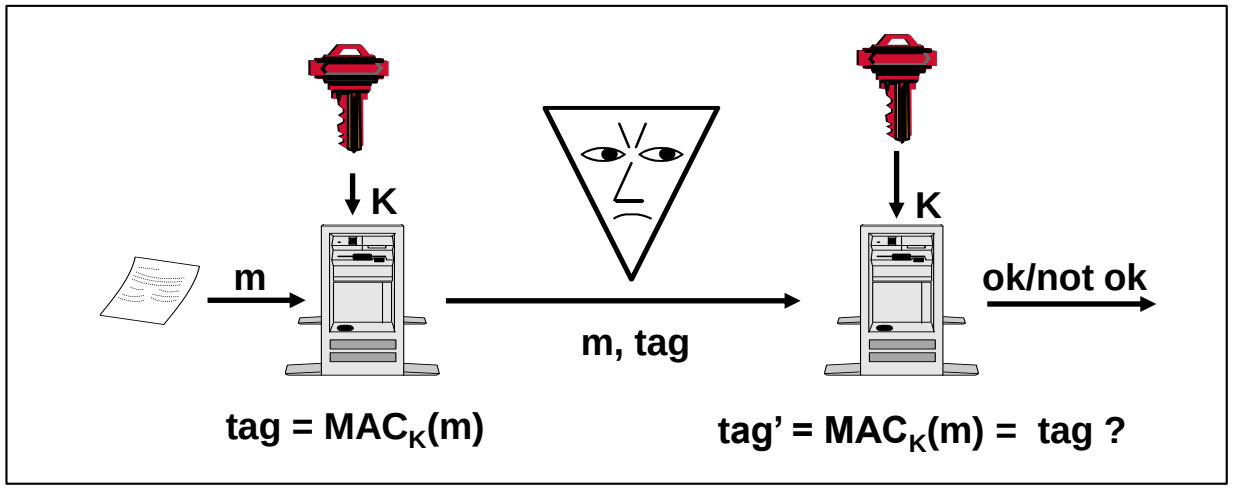
NACHRICHTENINTEGRITÄT



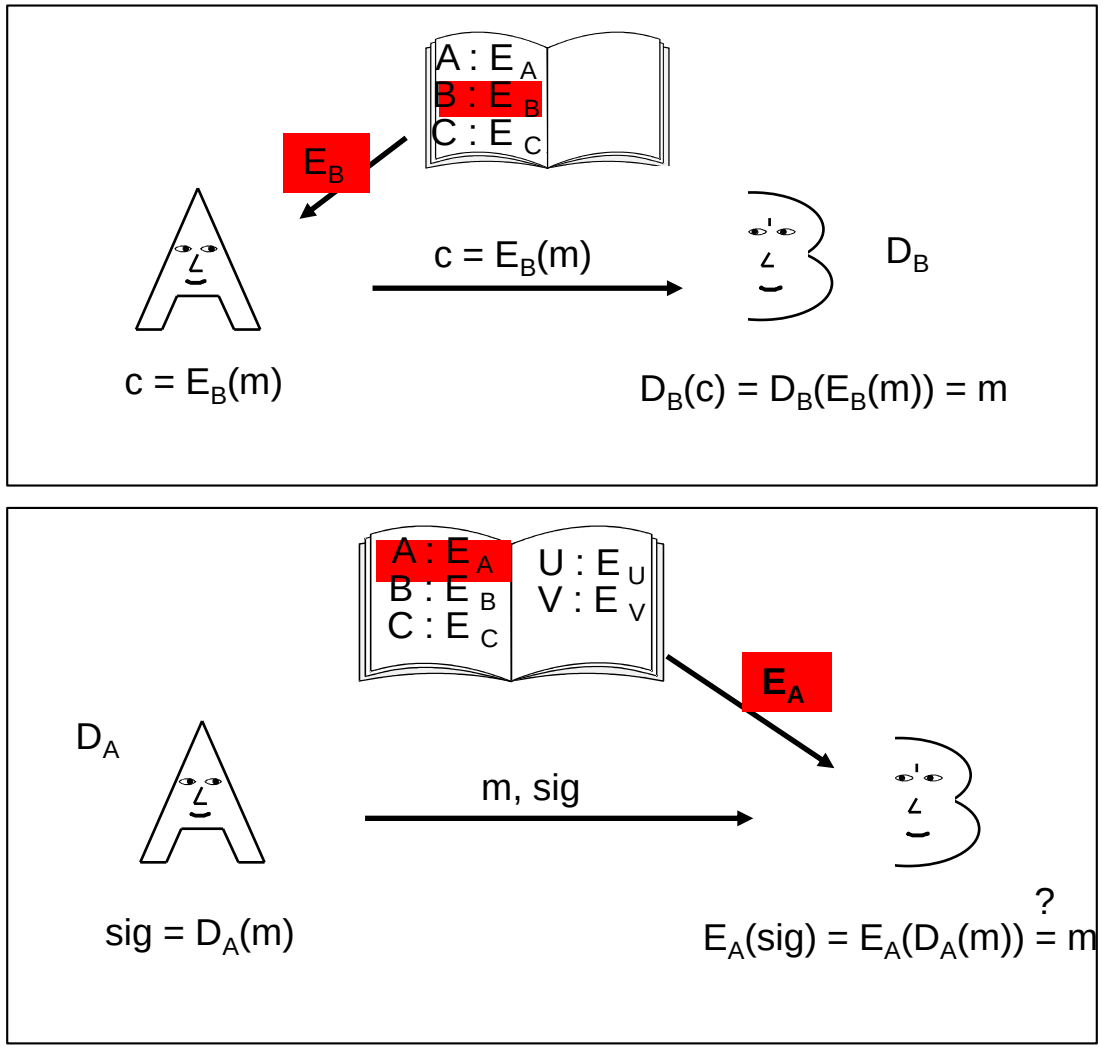
AUTHENTIZITÄT

DAS SYMMETRISCHE SHANNON-MODELL

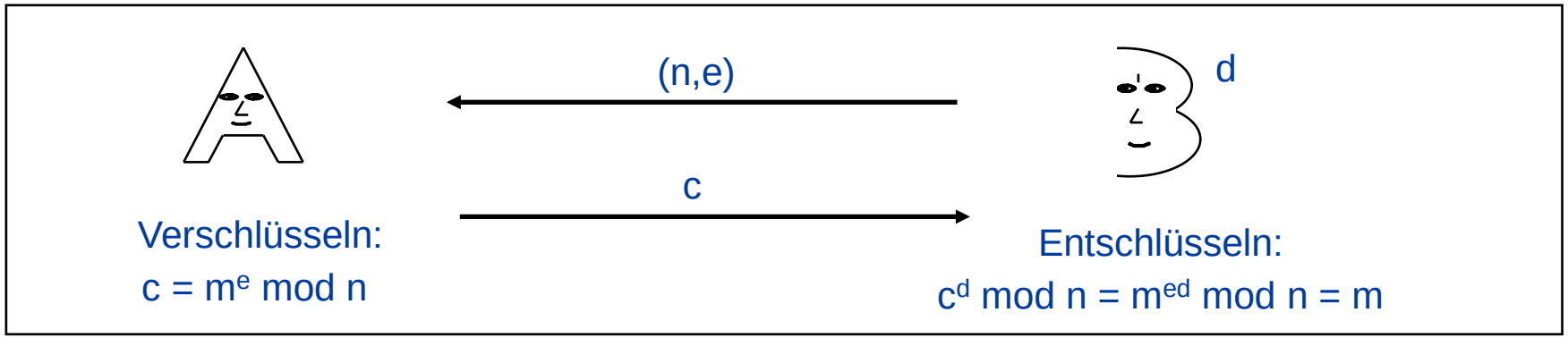




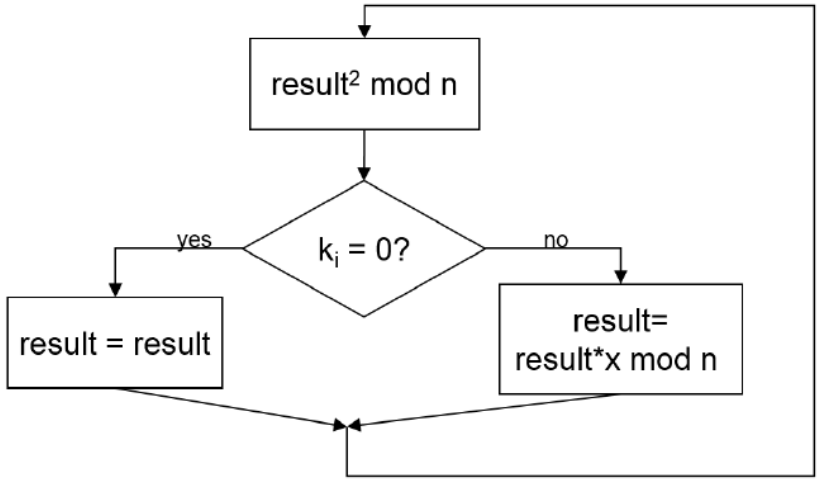
DAS ASYMMETRISCHE MODELL



DER RSA IM ÜBERBLICK

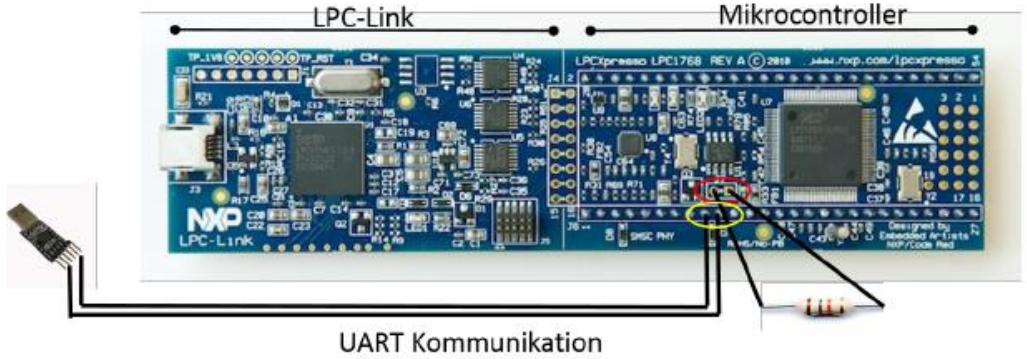


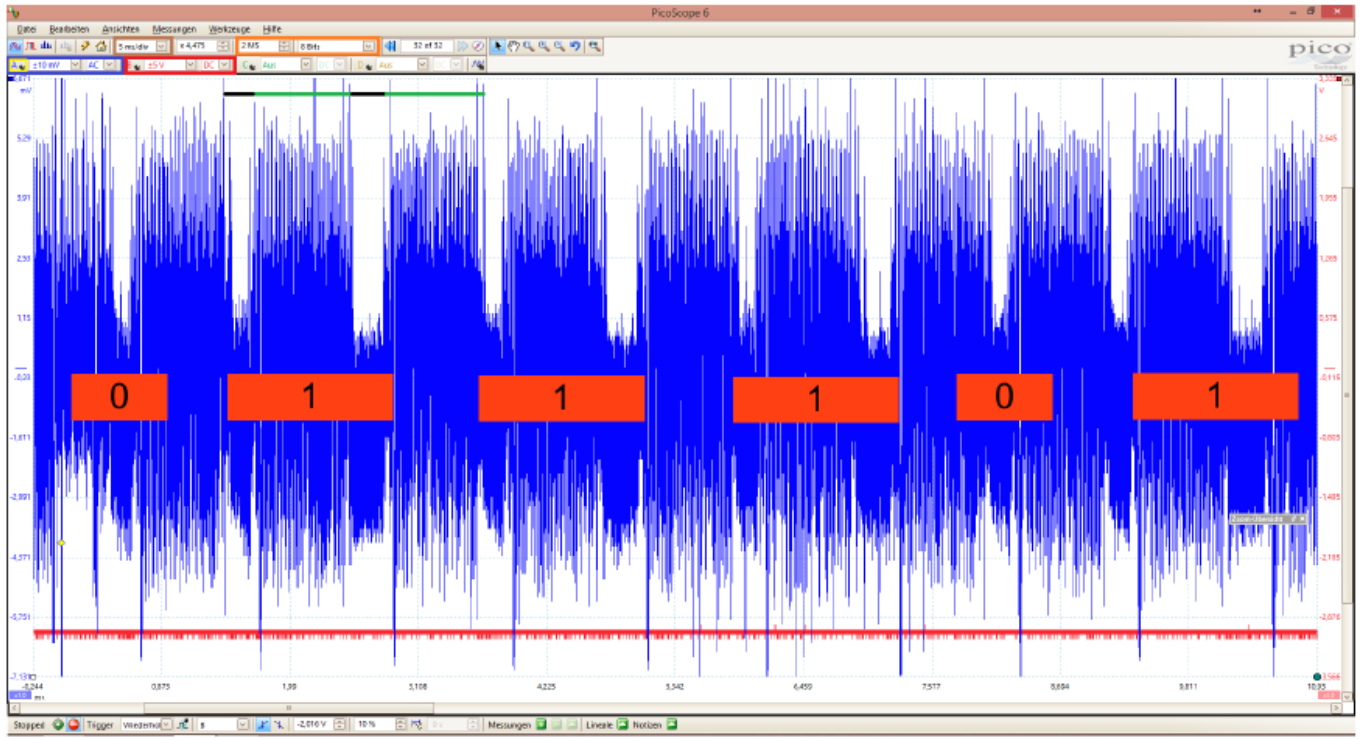
- Zu berechnen ist $x^k \mod n$
- Schreibe den Exponenten k als Binärzahl: $(k_s, k_{s-1}, ..., k_1, k_0)$
- Setze $result := 1$
- for $i = s$ downto 0 do



SEITENKANALANGRIFF AUF DEN RSA

Ergebnis nach 10 Stunden Praktikum: Single Trace Power Analysis (SPA)

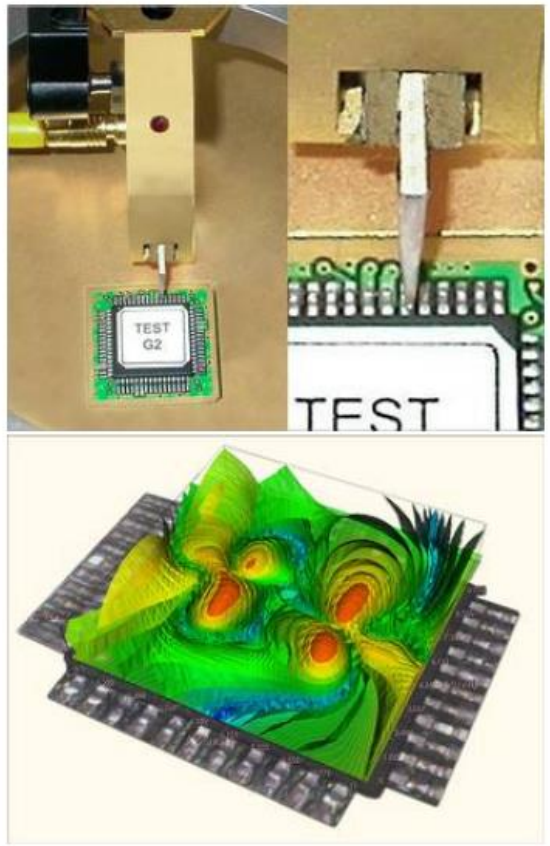




DAS PROBLEM IST LEICHT GELÖST?!?

- **Simple Gegenmaßnahme: Square-and-Always-Multiply**

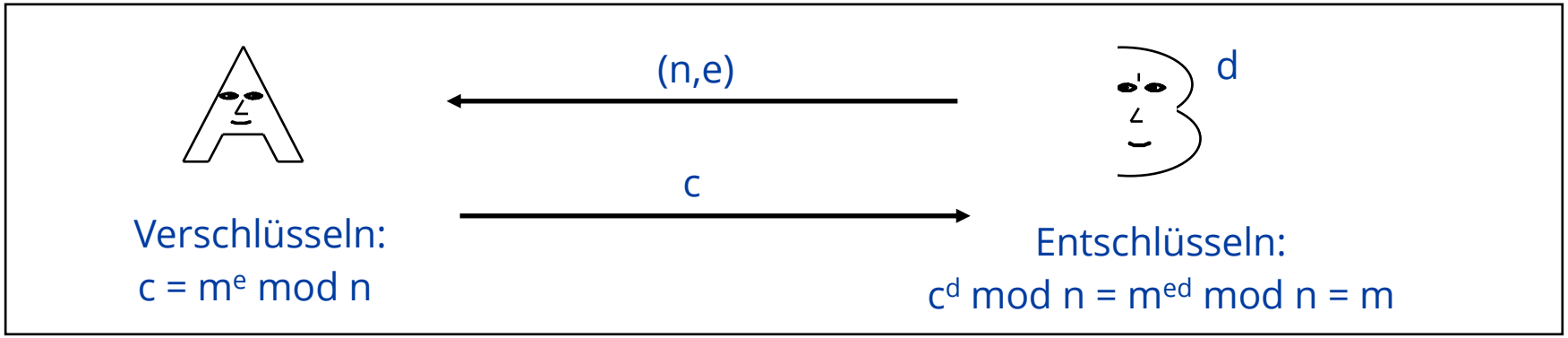
- **Messen der elektromagnetischen Abstrahlung: Single Trace Electromagnetic Radiation Analysis (SEMA)**

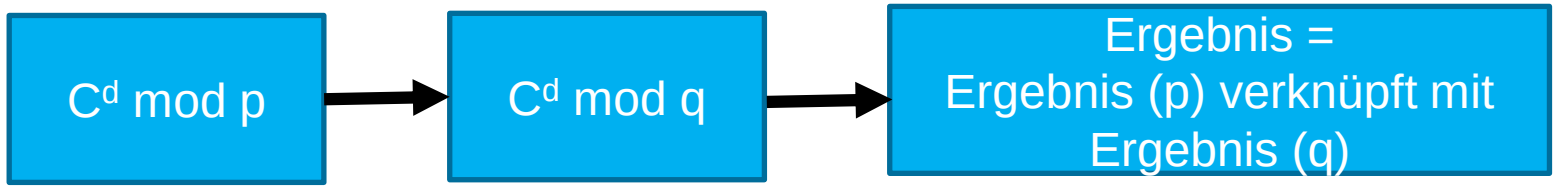


SEMI-INVASIVE ANGRIFFE

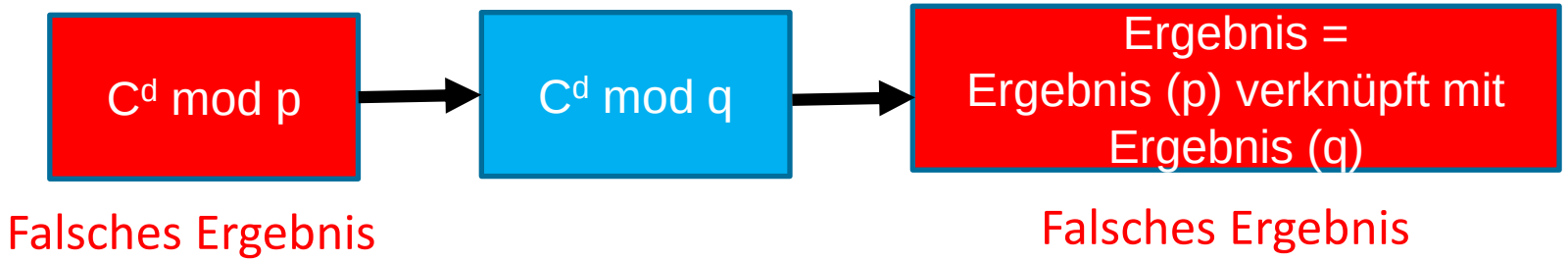
- Angriffe ändern das Verhalten des Controllers
- Ziele des Angriffs:
  - Schwächung von kryptographischen Schlüsseln
  - Manipulation von kritischen Tests auf dem Controller
- Angriffe durch
  - Zusätzliche Energie
  - Verwendung außerhalb der spezifizierten Parameter

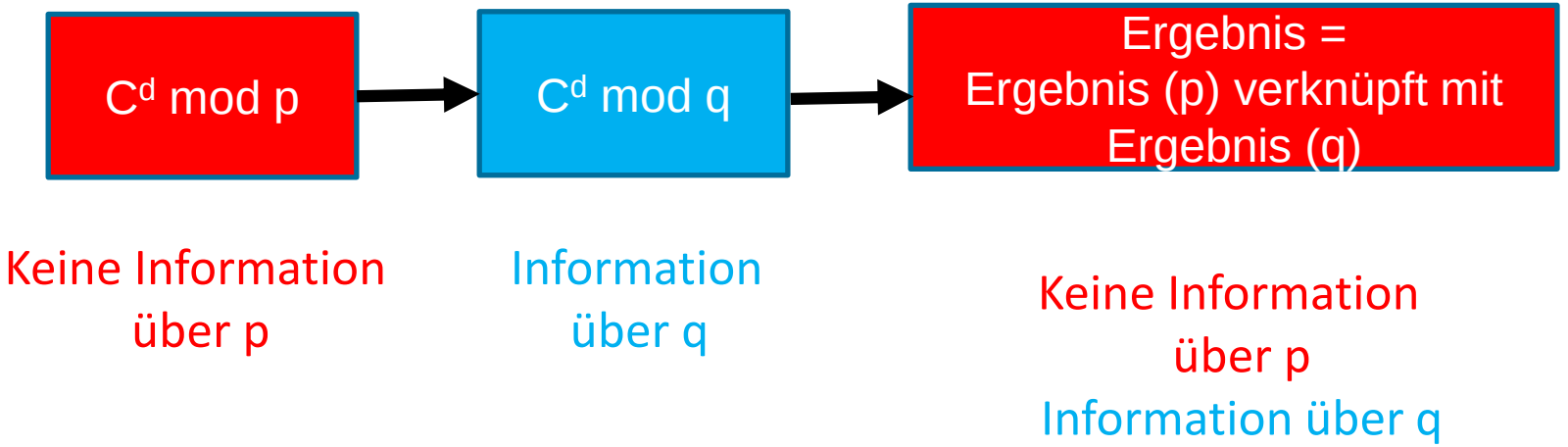
EIN EFFIZIENZTRICK FÜR DEN RSA





FEHLERINDUZIERUNG BEIM RSA





FEHLERINDUZIERUNG BEIM RSA 2

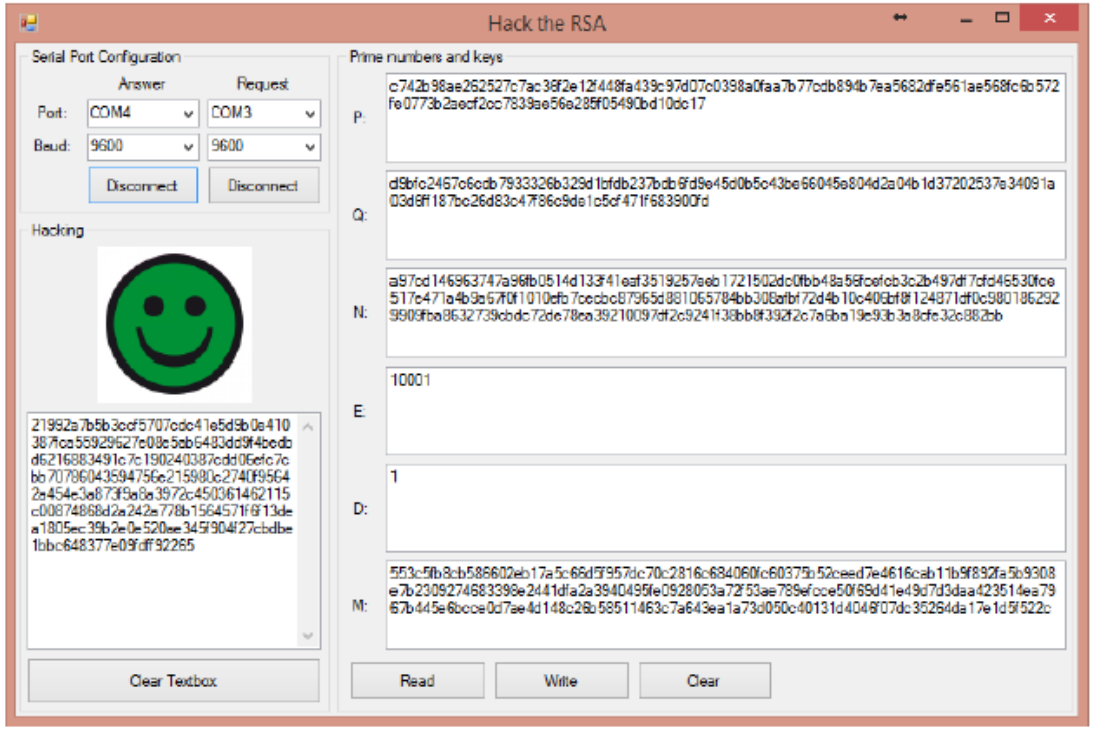
Bedrohlichkeit des Angriffs: Man braucht nur eine falsche Signatur

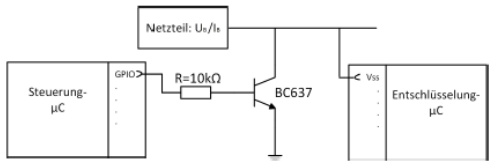
Fehlerquellen:

- **Kurzzeitiger Spannungsabfall**
- **Kurzzeitige Frequenzänderung**
- **Bestrahlung durch (Laser-)Licht**
- **Bestrahlung durch α-Partikel**

FEHLERINDUZIERUNG MIT SPANNUNGSABFALL

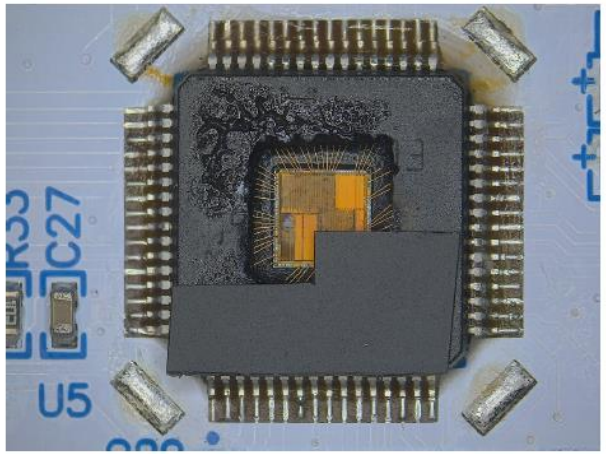
Ergebnis nach 15 Stunden Praktikum

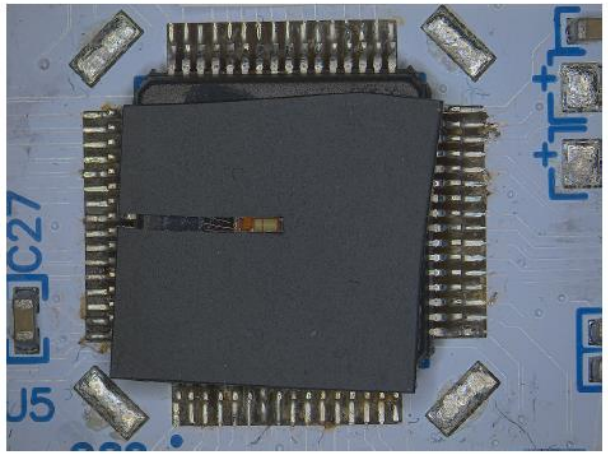


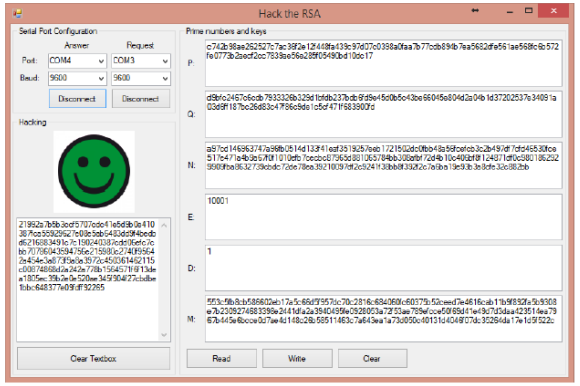


FEHLERINDUZIERUNG MIT LICHT

Ergebnis nach 20 Stunden Praktikum







ZUSAMMENFASSUNG

- **Sichere kryptographische Algorithmen allein reichen nicht aus, um sichere Systeme zu bauen.**

- **Nichtinvasive Angriffe:**
  - **Timing Angriffe**
  - **Stromprofilanalysen**
  - **Analyse der elektromagnetischen Abstrahlung**

- **Semi-invasive Angriffe:**
  - **Fehlerinduzierung mit Spannungsabfall oder Licht**

Vielen Dank für Ihre Aufmerksamkeit!

HAW HAMBURG