IT-Sicherheit - Schutz der Daten und der Kommunikation

Rouven Dreimann, M. Sc.

Inhalt

Inhaltsverzeichnis

Verschlüsselung

Grundlagen

- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- Hybride Verschlüsselung

Symmetrische Verschlüsselung

- ein Schlüssel
- die Sicherheit ist abhängig von der Sicherheit der Weitergabe
- sehr Schnell

Asymmetrische Verschlüsselung

- basiert immer auf einem mathematischen Problem
- ein öffentlicher Schlüssel
- ein privater Schlüssel
- höhere Sicherheit
- ca. 1000 mal langsamer

Hybride Verschlüsselung

- nutzt den Vorteil beider Verfahren
- nur der symmetrische Schlüssel wird asymmetrisch verschlüsselt
- Standard: Kombination aus RSA und AES

Hybride Verschlüsselung

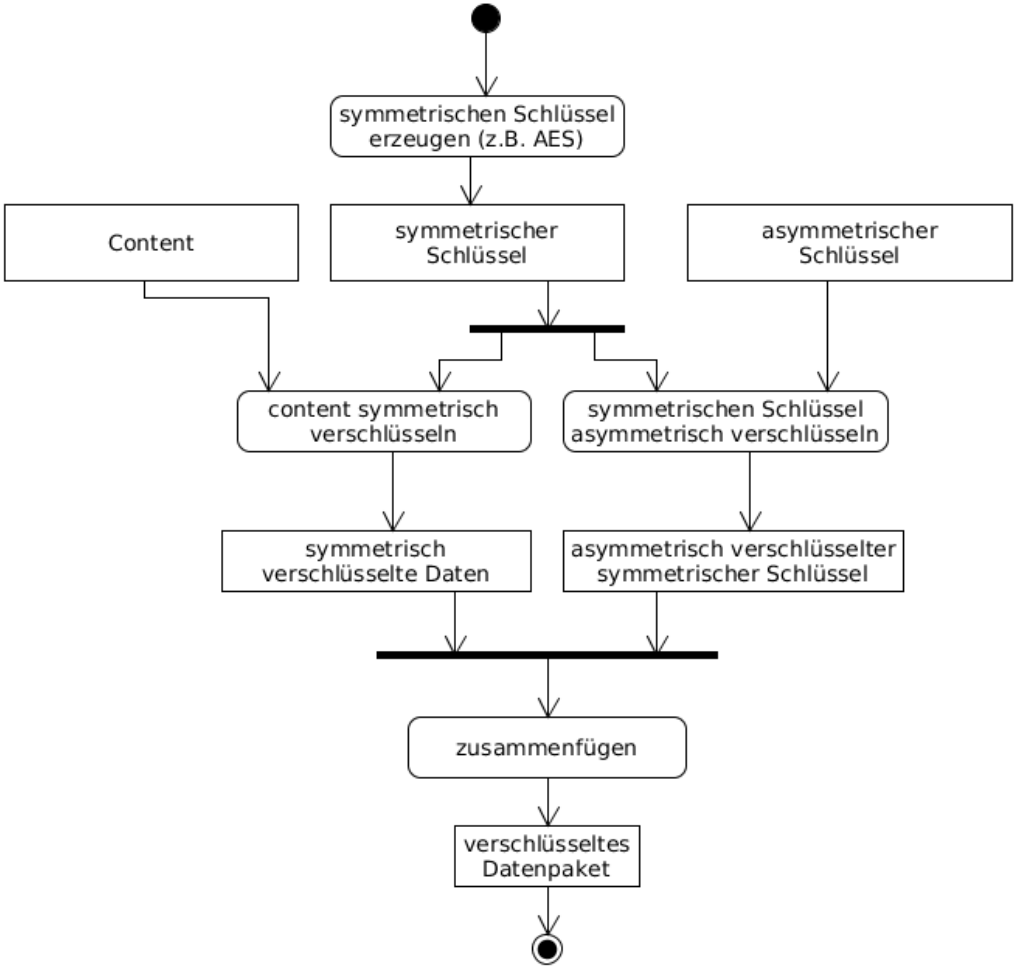


Figure 1: hybride Verschlüsselung

Postquanten-Kryptographie

Motivation

- Wenn es einen ausreichend großen Quantencomputer gibt. . .
- aktuelle asymmetrische Verfahren wäre gebrochen
- zugrunde liegende mathematische Probleme wären effizient zu lösen

IFE nutzt NTRU

- Resistent gegen Quantencomputer
- Hoffnungsträger unter den postquantensicheren Kryptoalgorithmen
- Verfahren in der Theorie schnell genug
- Praxistauglichkeit muss sich erst noch herausstellen

IFE

Übersicht

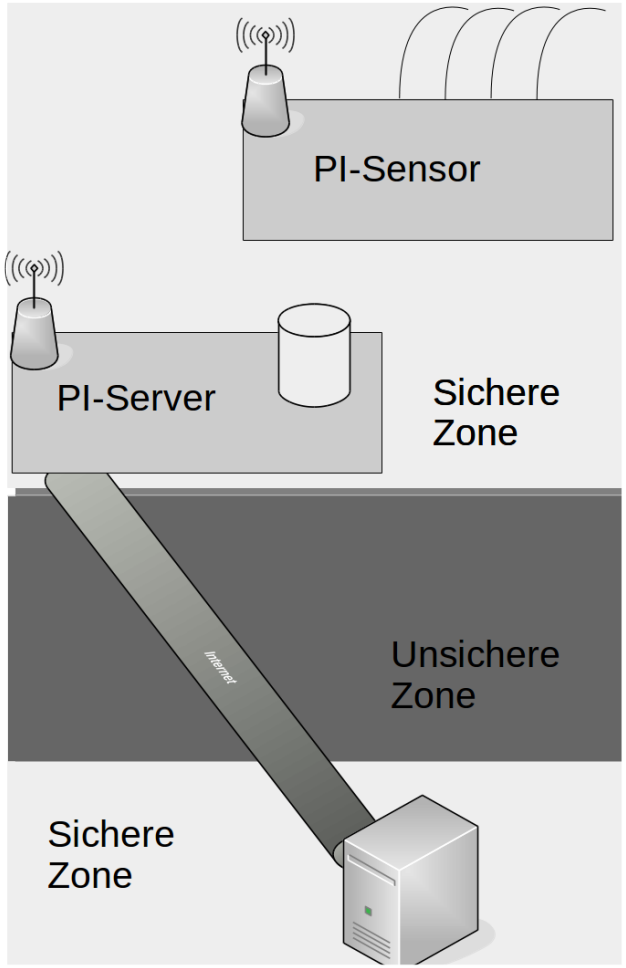


Figure 2: IFE Verschlüsselung

IFE Verschlüsselungstechnik

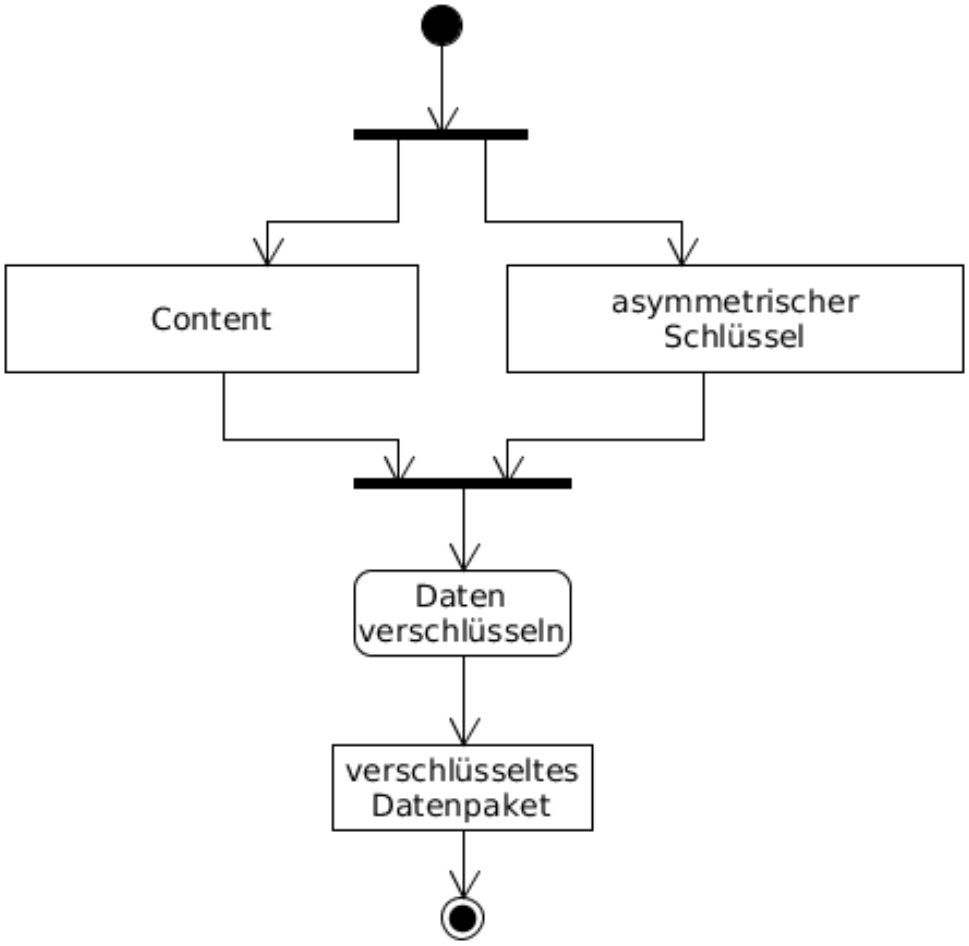
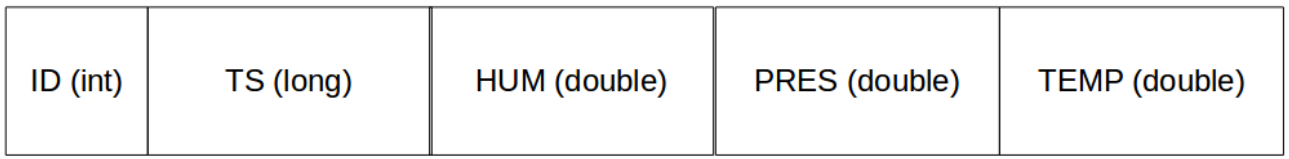


Figure 3: IFE Verschlüsselung

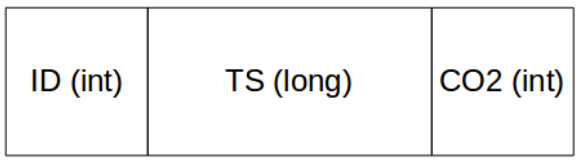
Abwandlungen IFE

- ein rein asymmetrisches Verfahren
- kleine zu verschlüsselnde Datenpakte

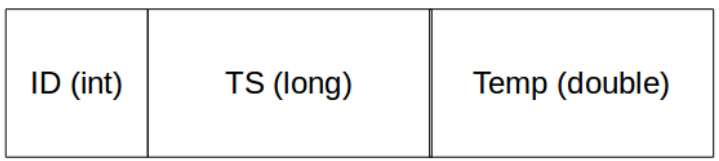
BME 280 (36 Bytes)



T6613 CO2 (16 Bytes)



DS18b20 (20 Bytes)



Geschwindigkeit

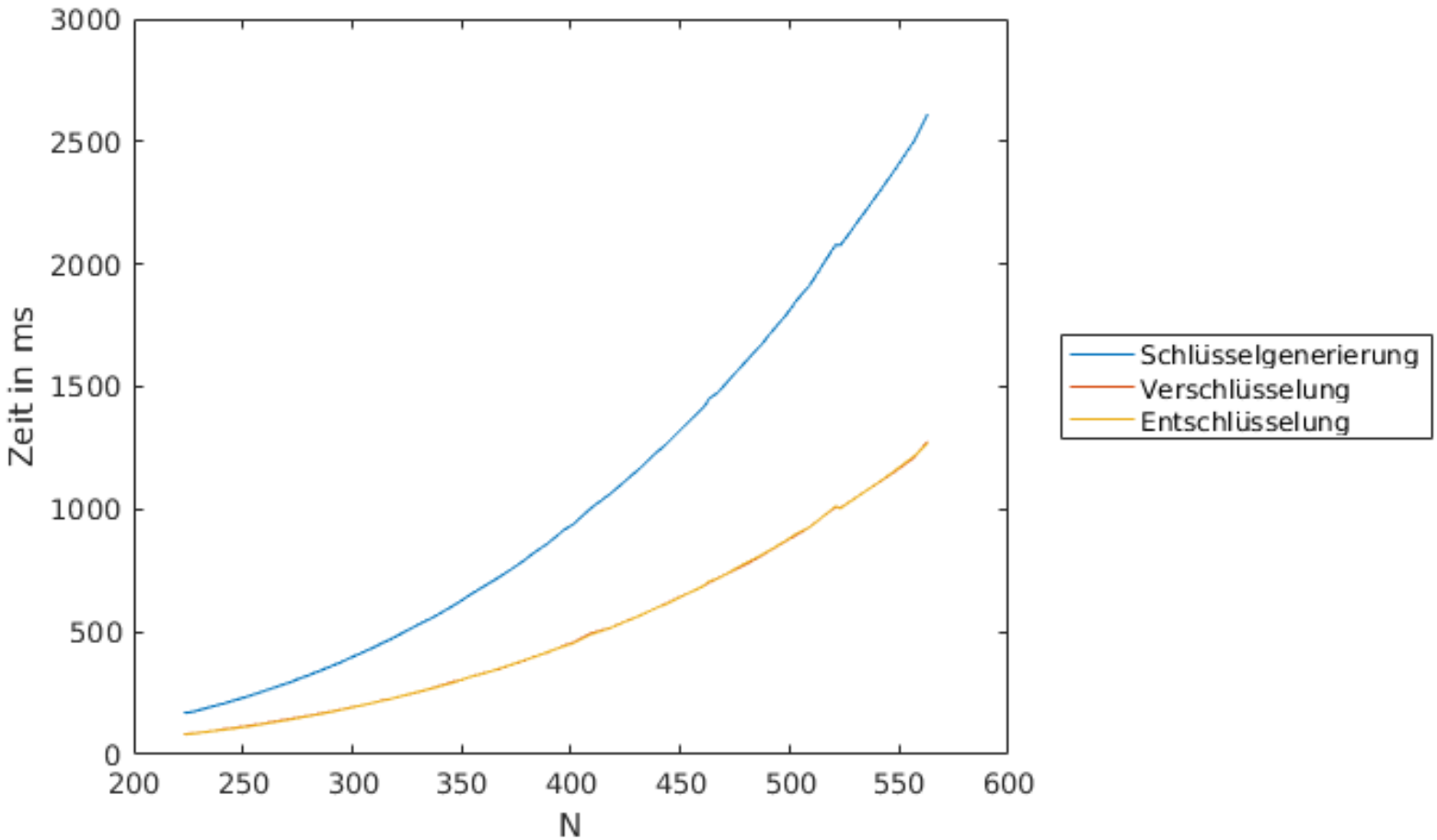


Figure 5: Geschwindigkeit