Institut für digitale Kommunikationssysteme
**Prof. Dr. Christoph Ruland**

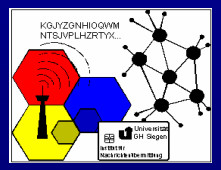
**SELMA Workshop 15./16. Oktober 2003**

# *Einführung in die asymmetrische Kryptographie*


Dipl.-Inform. Mel Wahl

Prof. Dr. Christoph Ruland

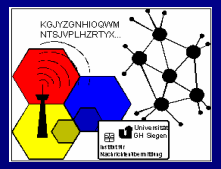
**Universität Siegen**
**Institut für digitale Kommunikationssysteme**

Uni Siegen

# Agenda

- Grundlagen
- Verschlüsselung
- Digitale Signaturen
- Algorithmen
  - RSA
  - DSA
  - EC-DSA



Institut für digitale Kommunikationssysteme
Prof. Dr. Christoph Ruland

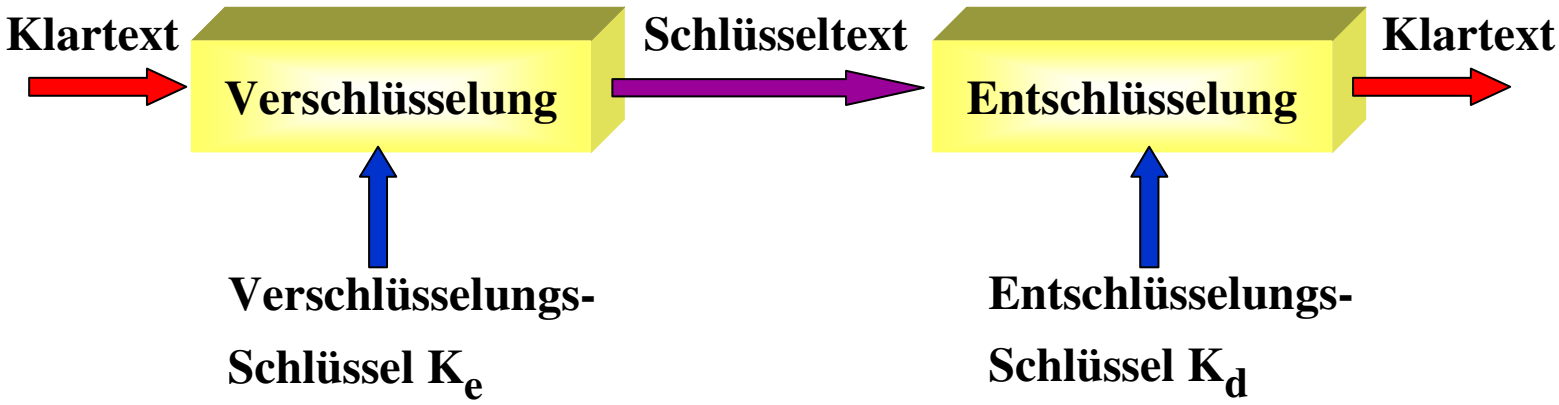
# Sicherheitsdienste und Sicherheitsmechanismen

- Sicherheitsdienste:
  1. Vertraulichkeit
  2. Datenunversehrtheit
  3. Authentikation
  4. Urhebernachweis
     Empfängernachweis
- Sicherheitsmechanismen:
  1. Verschlüsselung
  2. Digitale Signatur
  3. Certification Authority (CA)
  4. Sicherheitsprotokolle
- Realisierung der Sicherheitsdienste:
  1. Vertraulichkeit: Verschlüsselung, Sicherheitsprotokolle
  2. Datenunversehrtheit: Verschlüsselung oder digitale Signatur
  3. Authentikation: eingeschränkt Verschlüsselung, besser digitale Signatur und CA, Sicherheitsprotokolle
  4. Urhebernachweis, Empfängernachweis: digitale Signatur und CA

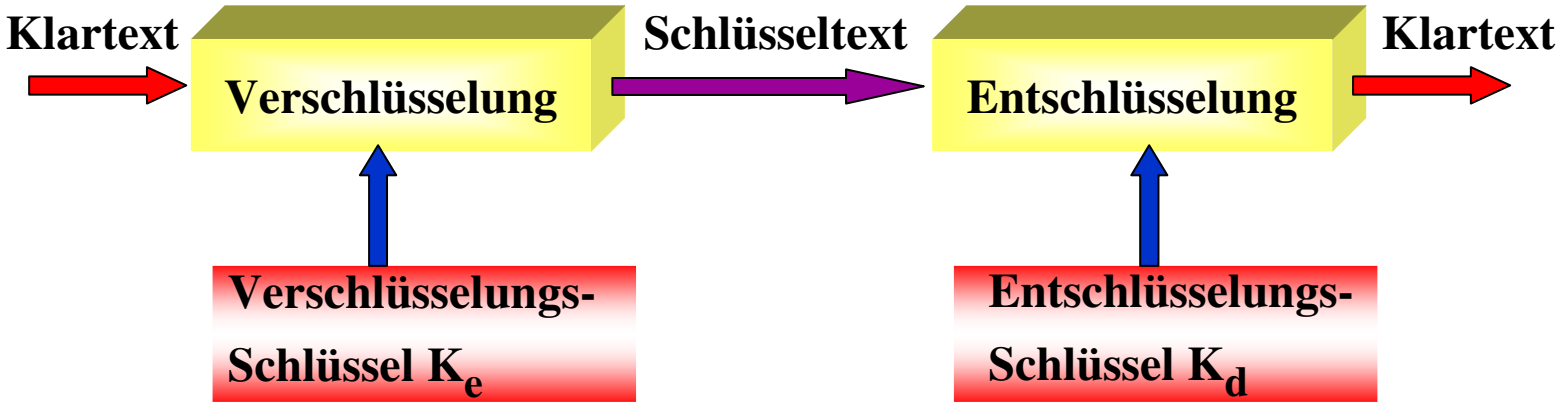
Uni Siegen

Institut für digitale Kommunikationssysteme
Prof. Dr. Christoph Ruland

# Schlüsselgesteuerte Verschlüsselung



# Verschlüsselungsarten




- Symmetrische Verschlüsselung

$$K_d = K_e$$

- Asymmetrische Verschlüsselung

$$K_d \neq K_e$$

Institut für digitale Kommunikationssysteme
Prof. Dr. Christoph Ruland

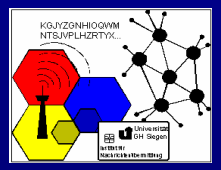
# Symmetrische Verschlüsselung

- Wer verschlüsseln kann, kann auch entschlüsseln
- Je zwei Kommunikationspartner müssen einen geheimen Schlüssel austauschen
- Schlüsselmanagement-Problematik
  - n Kommunikationspartner müssen je n-1 geheime Schlüssel verwalten
  - Insgesamt n(n-1) Schlüssel müssen ausgetauscht werden

Institut für digitale Kommunikationssysteme
Prof. Dr. Christoph Ruland

# Ansatz asymmetrische Verschlüsselung

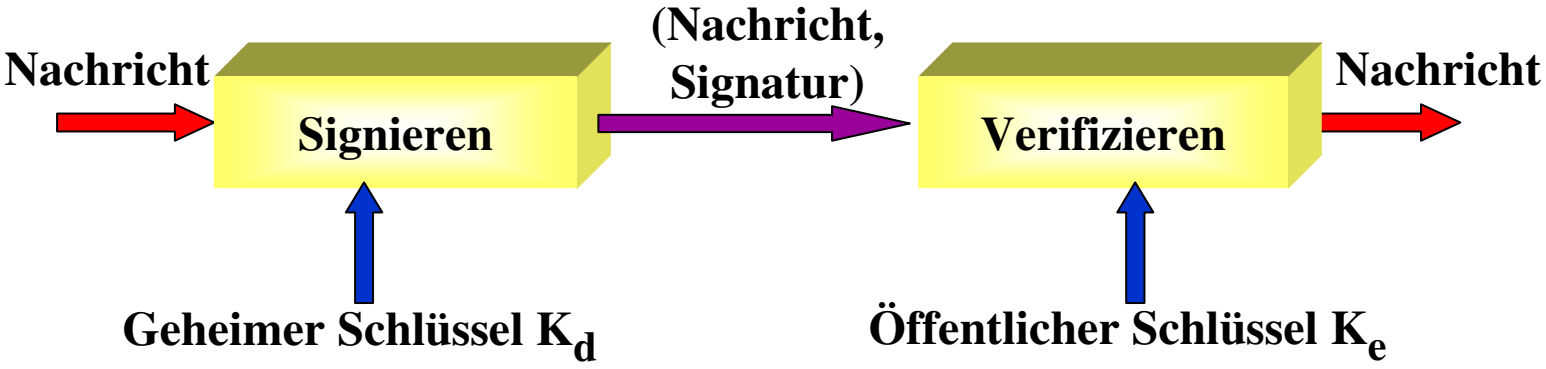
- Teilnehmer kann mit einem Schlüssel entweder ver- oder entschlüsseln
- Schlüsselpaar:
  - öffentlicher Schlüssel:
    kann öffentlich zugänglich gemacht werden
  - privater / geheimer Schlüssel:
    muss geschützt aufbewahrt werden
- Verschlüsseln mit öffentlichem Schlüssel des Empfängers, Entschlüsseln mit privatem Schlüssel des Empfängers



Uni Siegen

# Digitale Signaturen

- Signaturgesetz, § 2 Begriffsbestimmungen:
  *1. elektronische Signatur: elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung, also der Feststellung der Identität des Signators, dienen*




- Oft wird nicht die Nachricht selbst sondern ein Hashwert signiert
- Trusted Third Party (CA) zur sicheren Zuordnung der öffentlichen Schlüssel zu ihren Besitzern (üblicherweise durch signierte Zertifikate)

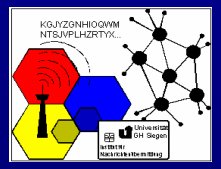
Institut für digitale Kommunikationssysteme
Prof. Dr. Christoph Ruland

# Algorithmen der asymmetrischen Kryptographie

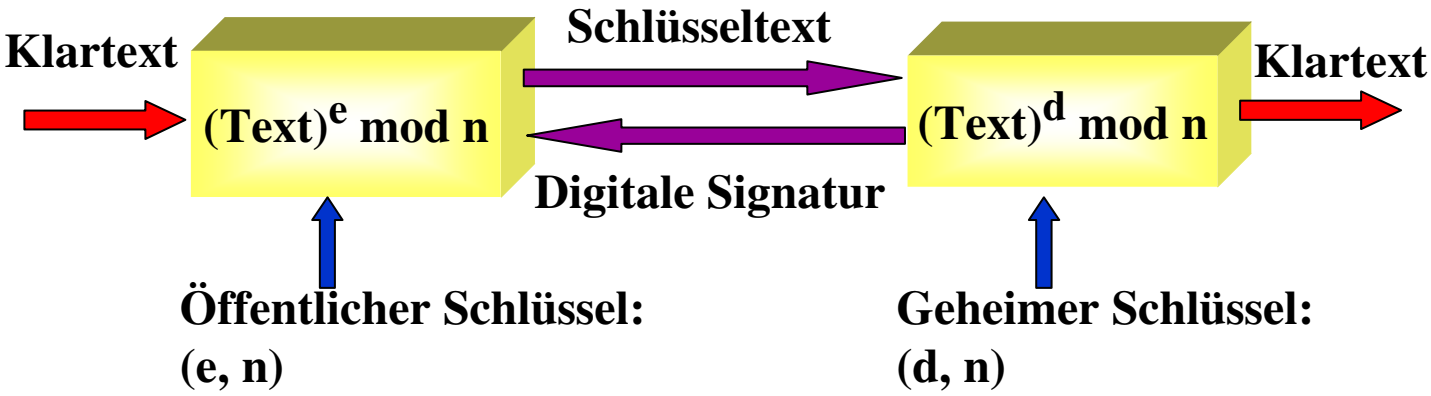
- Algorithmen basieren auf Einwegfunktion mit Geheimnis (one-way-trapdoor-function)
  - Funktion f leicht berechenbar
  - Umkehrfunktion $f^{-1}$ praktisch nicht berechenbar
  - Mit speziellem Geheimnis g (Geheimtür, Trapdoor) kann $f^{-1}$ leicht berechnet werden
  - Aber: komplexer als symmetrische Verschlüsselung → meist langsamer

# Faktorisierungsproblem

- Faktorisierungsproblem: Schwierigkeit, eine große Zahl n in ihre Primfaktoren p,q zu zerlegen (n = p * q)
- Kryptographische Verfahren basierend auf dem Faktorisierungsproblem nutzen die Schwierigkeit, aus n die (geheimen) Faktoren p und q zu berechnen



# RSA




- Nach seinen Erfindern benannt: R. Rivest, A. Shamir und Adleman
- Basierend auf dem Faktorisierungsproblem, d. h. es wird angenommen, dass die Gewinnung des Klartextes aus dem öffentlichen Schlüssel und dem Schlüsseltext genauso schwierig ist wie die Faktorisierung des Produkts zweier Primzahlen

# Diskretes Logarithmusproblem

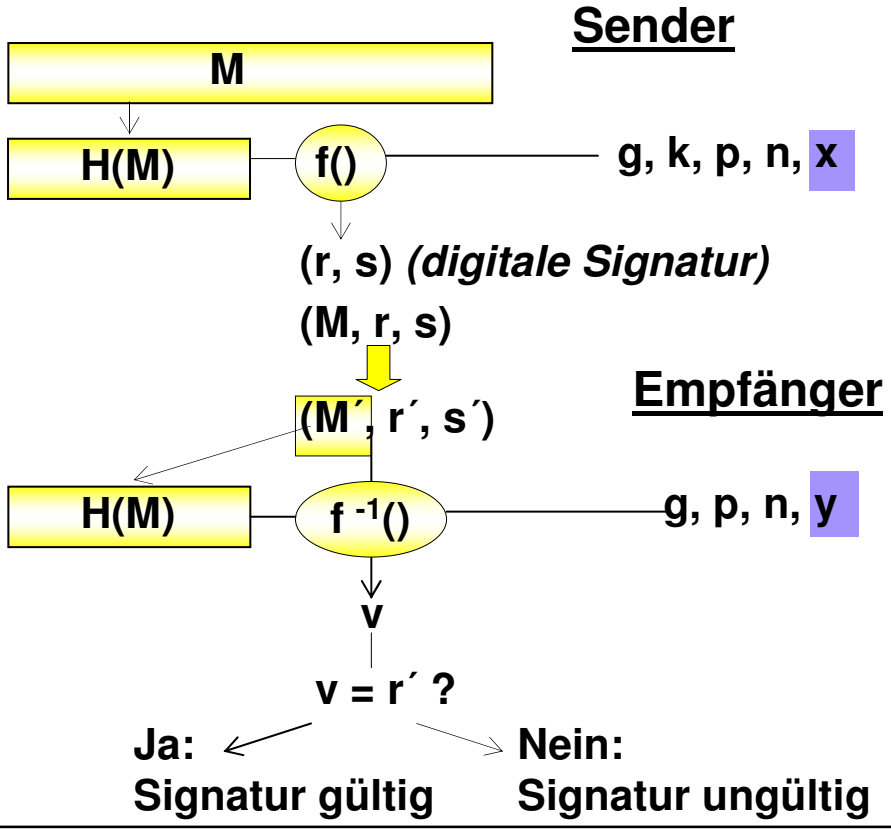
- Sei GF(p) ein endlicher Körper und g $\epsilon$ GF(p) ein Generator von GF(p), dann erfüllt ein Element y $\epsilon$ GF(p) die Gleichung

  $$y = g^x \bmod p$$

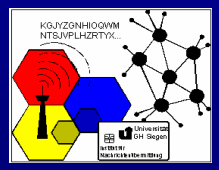
  für x genau dann, wenn $y^p = 1 \bmod p$
- Der Exponent x wird als diskreter Logarithmus von y (bzgl. der Basis g) bezeichnet
- Das diskrete Logarithmusproblem ist das Finden von x zu einem y (d. h. die Berechnung des diskreten Logarithmus)
- Kryptographische Verfahren basierend auf dem diskreten Logarithmusproblem nutzen die Schwierigkeit, den diskreten Logarithmus zu berechnen

# Digital Signature Standard (DSS) / Digital Signature Algorithm (DSA)

- DSA wurde von NIST im DSS vorgeschlagen
- Basierend auf dem diskreten Logarithmus Problem
- Ablauf Signatur erstellen und verifizieren:



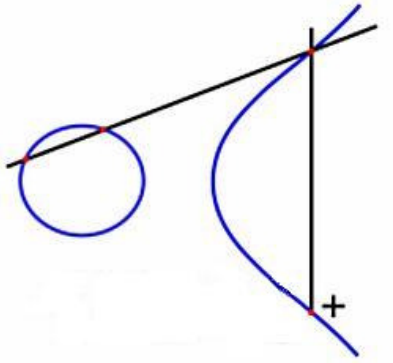

*M* *Klartext*
*H(M)* *Hashwert von M*
*x* *geheimer Schlüssel des Signators* *(1 ≤ x ≤ n-1)*
*y* *öffentlicher Schlüssel des Signators* *($y = g^x \bmod p$)*
*k* *(geheime) Zufallszahl* *(1 ≤ k ≤ n-1)*
*p, n, g* *Systemparameter*



Uni Siegen

Institut für digitale Kommunikationssysteme
Prof. Dr. Christoph Ruland

# Elliptische Kurven



- Gegeben: endlicher Primkörper GF(p). Dann kann man die elliptische Kurve E beschreiben als:

$$E: y^2 = x^3 + ax + b \quad \textit{mit } 4a^2 + 27b^2 \neq 0 \pmod p$$

- Die Koordinaten x,y aller Punkte P=(x,y) von E liegen in GF(p)
- Addition (+) und (darauf basierend) skalare Multiplikation (*) auf E definiert

Institut für digitale Kommunikationssysteme
Prof. Dr. Christoph Ruland

# Diskretes Logarithmusproblem auf elliptischen Kurven

- Sei E elliptische Kurve auf GF(p), der Punkt G $\epsilon$ E(GF(p)) mit Ordnung n, $n^2$ kein Teiler der Ordnung der Kurve #E(GF(p)), dann erfüllt ein Punkt Q die Gleichung

  $Q = d * G$ für ein d $\Leftrightarrow$ $n * Q = \sigma$

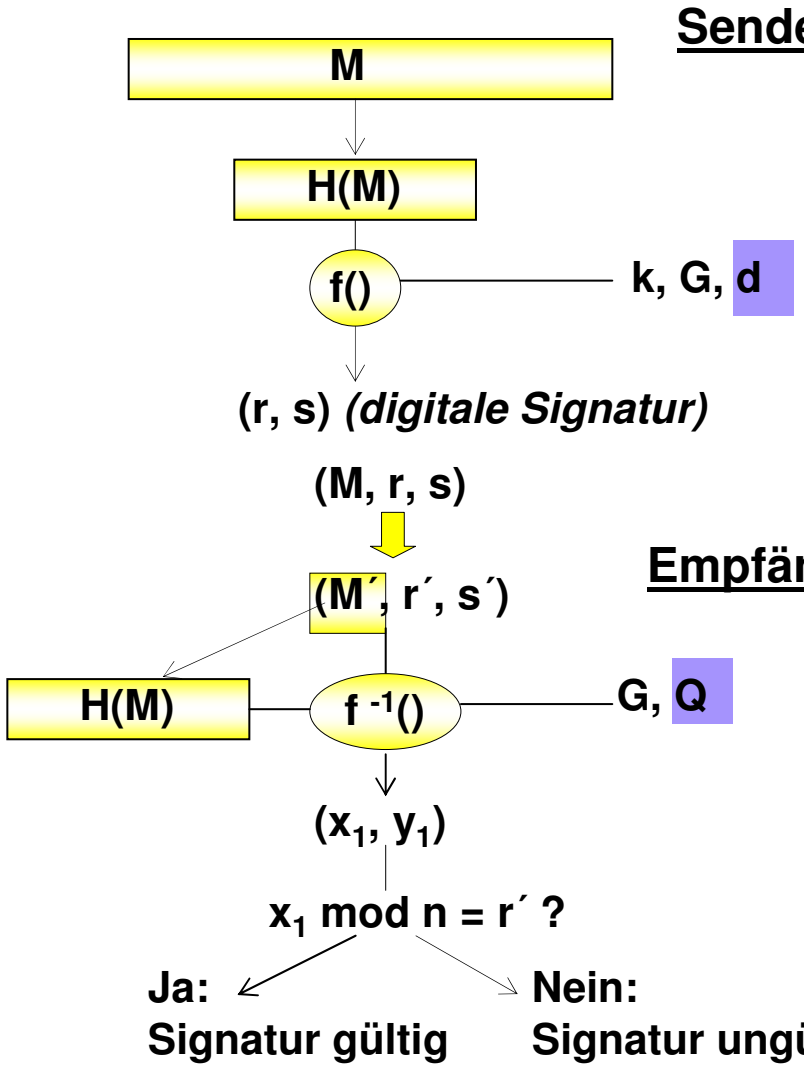
  *($\sigma$ ist der Punkt im Unendlichen)*

- Der Koeffizient d heißt der diskrete Logarithmus von Q, bezogen auf den Basispunkt G auf der elliptischen Kurve E
- Das diskrete Logarithmusproblem auf elliptischen Kurven ist das Finden von d zu einem Q (d. h. die Berechnung des diskreten Logarithmus auf E)
- Kryptographische Verfahren basierend auf dem diskreten Logarithmusproblem nutzen die Schwierigkeit, den diskreten Logarithmus auf elliptischen Kurven zu berechnen
  → **Elliptic Curve Cryptography (ECC)**

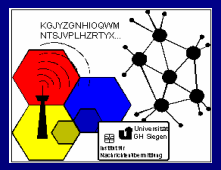
Uni Siegen

Institut für digitale Kommunikationssysteme
Prof. Dr. Christoph Ruland

# Elliptic Curve Cryptography (ECC) - EC-DSA Digitale Signatur




*M* *Klartext*
*d* *geheimer Schlüssel des Signators* *(1 ≤ d ≤ n-1)*
*Q* *öffentlicher Schlüssel des Signators* *(Q = d * G)*
*G,n* *Systemparameter*
*k* *Zufallszahl (1 ≤ k ≤ n-1)*



Uni Siegen

Institut für digitale Kommunikationssysteme
Prof. Dr. Christoph Ruland

# Einige andere Algorithmen der asymmetrischen Kryptographie

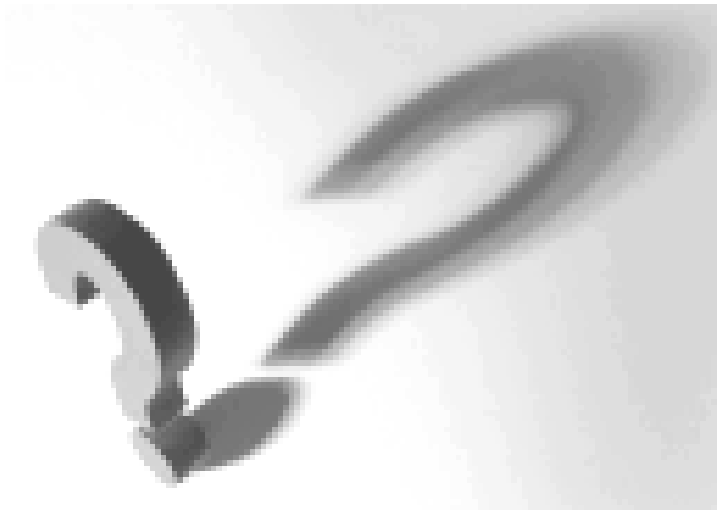
- El Gamal
  - Basiert auf dem Problem des diskreten Logarithmus
  - Variante: DSA
- EC-KCDSA und EC-GDSA
  - Koreanische und deutsche Version von ECC
  - Mit EC-DSA im ISO Standard IS 15946 enthalten
- Fiat-Shamir-Verfahren
  - Basiert auf dem Faktorisierungsproblem
  - Zero Knowledge Protokoll, verwendet Stichproben

# Komplexitätsvergleich und Schlüssellängen

- Basierend auf der Komplexität des zugrunde liegenden Problems und des Algorithmus werden die Schlüssellängen empfohlen. Dies wirkt sich auch auf die Signaturlänge aus.
- Beispiel:
  Vergleich von RSA und EC-DSA:
  - Da EC-DSA “komplexer” ist, können die Schlüssel kürzer gewählt werden bei gleicher Sicherheit, z. B. 160 Bit ECC ≈ 1024 Bit RSA
  - → Kürzere Berechnungszeiten bei EC-DSA
  - → Signaturlänge bei EC-DSA: 321 Bit, bei RSA 1024 Bit

Institut für digitale Kommunikationssysteme
**Prof. Dr. Christoph Ruland**

# Fragen?



**Vielen Dank für Ihre Aufmerksamkeit.**

Uni Siegen