
# Perspektiven der Sicherheit kryptographischer Verfahren gegen starke Angreifer

Prof. Dr. Hannes Federrath

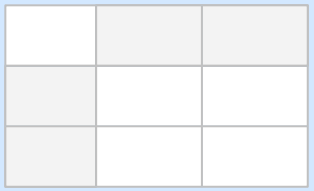
http://svs.informatik.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

„Technologische Aspekte der Internetüberwachung und der Kryptographie“ der Europäischen Akademie für Informationsfreiheit und Datenschutz, Berlin, 27.01.2014

# Einteilung von Kryptosystemen

- Kryptographische Basisbausteine
  - Konzelationssysteme
  - Authentikationssysteme
  - Hashfunktionen
  - Pseudozufallszahlengeneratoren
- Schlüsselbeziehung Sender–Empfänger
  - Symmetrische Systeme
  - Asymmetrische Systeme
- Erreichbare Sicherheit



# Anwendungsfall x Schlüsselbeziehung

| | Konzelation (Verschlüsselung) | Authentikation |
|---|---|---|
| symmetrische | *One-time-pad, DES, Triple-DES, AES, IDEA, A5/1 (GSM), A5/2 (GSM) …*<br>GnuPG/PGP, WPA2, IPSec, SSL/TLS | *Symmetrische Authentikationscodes, CCM, A3 (GSM), …*<br>SecurID, WPA2, IPSec, SSL/TLS |
| asymmetrische | *RSA, ElGamal, McEliece, …*<br>GnuPG/PGP, HBCI, SSL/TLS | *RSA, ElGamal, DSA, GMR, …*<br>GnuPG/PGP, HBCI, SSL/TLS |

*Algorithmus*

Anwendung

## Erreichbare Sicherheit

- Sicherheit
  - (informations) theoretisch sicher
  - kryptographisch stark (beweisbar)
    - gegen aktive Angriffe
    - gegen passive Angriffe
  - wohluntersucht (praktisch sicher)
    - Chaos
    - Zahlentheorie

  komplexitäts-theoretisch sicher
  - geheim gehaltene

- Kerckhoffs-Prinzip
  - Die Sicherheit eines kryptographischen Verfahrens soll von der Geheimhaltung des kryptographischen Schlüssels abhängen.
    - Geht zurück auf
      Auguste Kerckhoffs: La Cryptographie militaire, 1883

# Brechen kryptographischer Systeme

- Vollständiges Durchsuchen (brute-force, exaustive search)
  - Supercomputer
  - Quantencomputer

Stichwort: Schlüssellänge

betrifft alle komplexitätsth. sicheren Systeme

- Ausnutzen von verborgenen Designschwächen (cryptananlysis)
  - unabsichtlich: schlechtes Design
  - absichtlich: backdoors

Kryptologie als Geheimwissenschaft?

DES, A5/1 (GSM), ECC (NIST-Kurven)

- Ausnutzen von Implementierungsfehlern
  - Angriffe auf die physische Sicherheit
  - Seitenkanalangriffe (timing attacks, power analysis)
  - Protokollfehler

Diskrepanz zwischen Theorie und Praxis

Fault Injection, Cold Boot, GSM-Verschlüsselung

# Vollständiges Durchsuchen (brute-force, exaustive search)

- Angriff über Supercomputer und künftig Quantencomputer
  - betrifft nur komplexitätstheoretisch sichere Systeme
- Schutz gegen Supercomputer
  - Schlüssel ausreichend lang wählen
- Schutz gegen Quantencomputer
  - symmetrisch: Schlüssellänge verdoppeln auf mind. 256 Bit
  - asymmetrisch: [post-quantum cryptography]

| | Key lengths | Complexity | | nach: Bernstein, Buchmann, Dahmen: Post Quantum Cryptography. Springer, 2009 |
|---|---|---|---|---|
| | | Super Computer | Quantum Computer | |
| Symm. | 128 Bit | $2^{127}$ | $2^{64}$ | Grover, 1996 |
| | 256 Bit | $2^{255}$ | $2^{128}$ | |
| Asymm. | 1024 Bit | $\approx 2^{90}$ | $\approx 2^{25}$ | Shor, 1994 |
| | 2048 Bit | $\approx 2^{117}$ | $\approx 2^{28}$ | |

# Ausnutzen von verborgenen Designschwächen (cryptananlysis)

- Kryptographische Verfahren erweisen sich manchmal als schwächer als vermutet.
  - daher wenigstens: Offenlegung Algorithmus (Kerckhoffs, 1883)
- Risiken bei Geheimhaltung?
  - Verborgene Designschwächen?

- Data Encryption Standard DES und differenzielle Kryptanalyse
  - 1993 vorgestellt von Biham und Shamir

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S1: | 0: | 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| | 1: | 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| | 2: | 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| | 3: | 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S2: | 0: | 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 |
| | 1: | 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
| | 2: | 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 |
| | 3: | 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S3: | 0: | 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 |
| | 1: | 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 |
| | 2: | 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 |
| | 3: | 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S4: | 0: | 7 | 13 | 14 | 3 | 0 | 6 | 9 | 10 | 1 | 2 | 8 | 5 | 11 | 12 | 4 | 15 |
| | 1: | 13 | 8 | 11 | 5 | 6 | 15 | 0 | 3 | 4 | 7 | 2 | 12 | 1 | 10 | 14 | 9 |
| | 2: | 10 | 6 | 9 | 0 | 12 | 11 | 7 | 13 | 15 | 1 | 3 | 14 | 5 | 2 | 8 | 4 |
| | 3: | 3 | 15 | 0 | 6 | 10 | 1 | 13 | 8 | 9 | 4 | 5 | 11 | 12 | 7 | 2 | 14 |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S5: | 0: | 2 | 12 | 4 | 1 | 7 | 10 | 11 | 6 | 8 | 5 | 3 | 15 | 13 | 0 | 14 | 9 |
| | 1: | 14 | 11 | 2 | 12 | 4 | 7 | 13 | 1 | 5 | 0 | 15 | 10 | 3 | 9 | 8 | 6 |
| | 2: | 4 | 2 | 1 | 11 | 10 | 13 | 7 | 8 | 15 | 9 | 12 | 5 | 6 | 3 | 0 | 14 |
| | 3: | 11 | 8 | 12 | 7 | 1 | 14 | 2 | 13 | 6 | 15 | 0 | 9 | 10 | 4 | 5 | 3 |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S6: | 0: | 12 | 1 | 10 | 15 | 9 | 2 | 6 | 8 | 0 | 13 | 3 | 4 | 14 | 7 | 5 | 11 |
| | 1: | 10 | 15 | 4 | 2 | 7 | 12 | 9 | 5 | 6 | 1 | 13 | 14 | 0 | 11 | 3 | 8 |
| | 2: | 9 | 14 | 15 | 5 | 2 | 8 | 12 | 3 | 7 | 0 | 4 | 10 | 1 | 13 | 11 | 6 |
| | 3: | 4 | 3 | 2 | 12 | 9 | 5 | 15 | 10 | 11 | 14 | 1 | 7 | 6 | 0 | 8 | 13 |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S7: | 0: | 4 | 11 | 2 | 14 | 15 | 0 | 8 | 13 | 3 | 12 | 9 | 7 | 5 | 10 | 6 | 1 |
| | 1: | 13 | 0 | 11 | 7 | 4 | 9 | 1 | 10 | 14 | 3 | 5 | 12 | 2 | 15 | 8 | 6 |
| | 2: | 1 | 4 | 11 | 13 | 12 | 3 | 7 | 14 | 10 | 15 | 6 | 8 | 0 | 5 | 9 | 2 |
| | 3: | 6 | 11 | 13 | 8 | 1 | 4 | 10 | 7 | 9 | 5 | 0 | 15 | 14 | 2 | 3 | 12 |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S8: | 0: | 13 | 2 | 8 | 4 | 6 | 15 | 11 | 1 | 10 | 9 | 3 | 14 | 5 | 0 | 12 | 7 |
| | 1: | 1 | 15 | 13 | 8 | 10 | 3 | 7 | 4 | 12 | 5 | 6 | 11 | 0 | 14 | 9 | 2 |
| | 2: | 7 | 11 | 4 | 1 | 9 | 12 | 14 | 2 | 0 | 6 | 10 | 13 | 15 | 3 | 5 | 8 |
| | 3: | 2 | 1 | 14 | 7 | 4 | 10 | 8 | 13 | 15 | 12 | 9 | 0 | 3 | 5 | 6 | 11 |

# Ausnutzen von verborgenen Designschwächen (cryptananlysis)

- Kryptographische Verfahren erweisen sich manchmal als schwächer als vermutet.
  - daher wenigstens: Offenlegung Algorithmus (Kerckhoffs, 1883)
- Risiken bei Geheimhaltung?
  - Verborgene Designschwächen?

- Data Encryption Standard DES und differenzielle Kryptanalyse
  - 1993 vorgestellt von Biham und Shamir

    - zufällige S-Boxen: «geringer» Schutz gegen diff. Kryptan.
      - Komplexität etwa $2^{37}$ bis $2^{47}$
    - standardisierte S-Boxen: «Hohe» Resistenz dagegen
      - Komplexität etwa $2^{52}$ bis $2^{58}$

## Ausnutzen von verborgenen Designschwächen (cryptananlysis)

- Kryptographische Verfahren erweisen sich manchmal als schwächer als vermutet.
  - daher wenigstens: Offenlegung Algorithmus (Kerckhoffs, 1883)
- Risiken bei Geheimhaltung?
  - Verborgene Designschwächen
  - Absichtliche Designschwächen?

- Data Encryption Standard DES und differenzielle Kryptanalyse
  - 1993 vorgestellt von Biham und Shamir

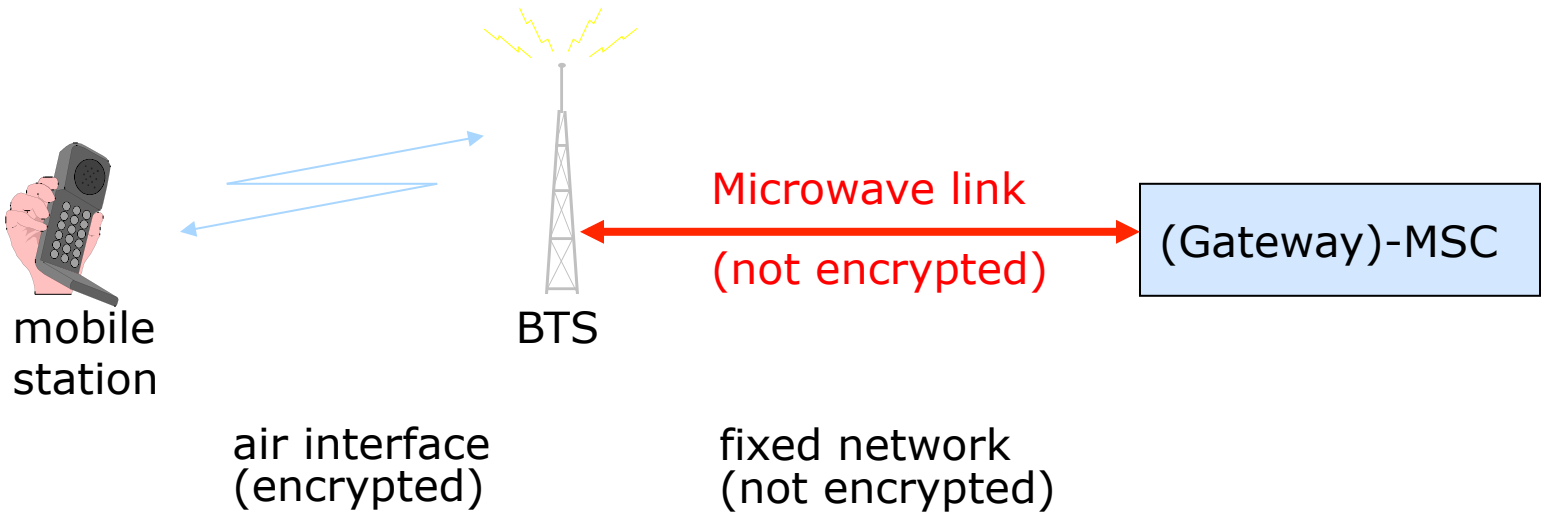
- Global System for Mobile Communication GSM A5/1
  - 2010 praktisch gebrochen von Nohl
    - benötigt ca. 2 TByte vorberechneter Rainbow tables

- Elliptic Curve Cryptography NIST FIPS 186-3
  - Skepsis ist wohl zunächst berechtigt

# Ausnutzen von Implementierungsfehlern

- Selbst wenn die kryptographischen Algorithmen in der Theorie als sicher eingeschätzt werden, so müssen sie auch praktisch implementiert werden.
- Typische Angriffsszenarien
  - Angriffe auf die physische Sicherheit
  - Seitenkanalangriffe (timing attacks, power analysis)
  - Protokollfehler

Fault Injection, Cold Boot, GSM-Verschlüsselung



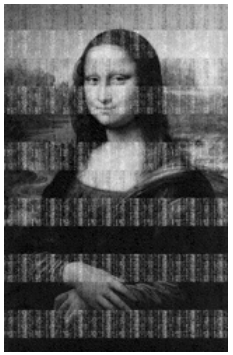
# Ausnutzen von Implementierungsfehlern

- Selbst wenn die kryptographischen Algorithmen in der Theorie als sicher eingeschätzt werden, so müssen sie auch praktisch implementiert werden.
- Typische Angriffsszenarien
  - Angriffe auf die physische Sicherheit
  - Seitenkanalangriffe (timing attacks, power analysis)
  - Protokollfehler

Speicherinhalt…

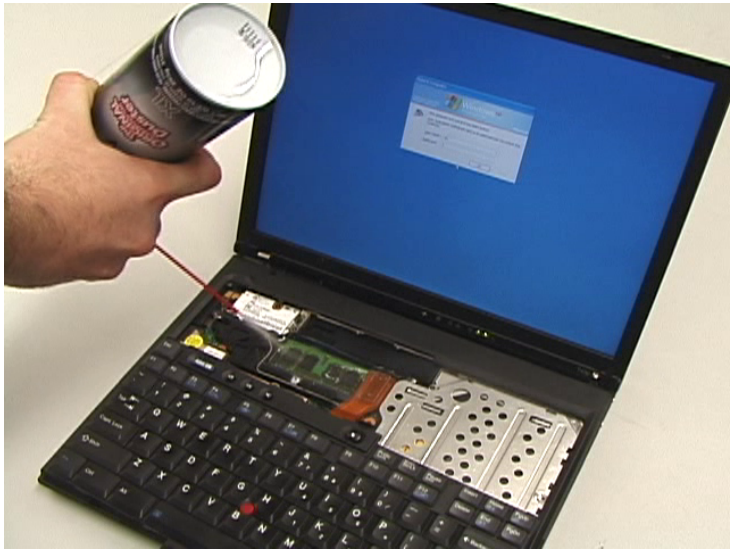
normales Ausschalten

gekühlter Speicher



… nach t Minuten

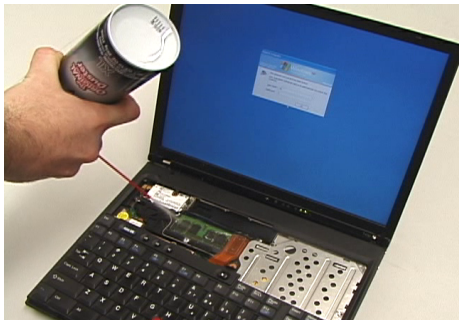
Cold Boot



citp.princeton.edu/research/memory/

# Brechen kryptographischer Systeme

- Vollständiges Durchsuchen (brute-force, exaustive search)
  - Supercomputer
  - Quantencomputer
- Ausnutzen von verborgenen Designschwächen (cryptananlysis)
  - unabsichtlich: schlechtes Design
  - absichtlich: backdoors
- Ausnutzen von Implementierungsfehlern
  - Angriffe auf die physische Sicherheit
  - Seitenkanalangriffe (timing attacks, power analysis)
  - Protokollfehler



Bilder: UHH, Wikipedia, priceton.edu


Universität Hamburg
Fachbereich Informatik
Arbeitsbereich SVS
Prof. Dr. Hannes Federrath
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de

Telefon +49 40 42883 2358

http://svs.informatik.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG