

# **Sichere Kommunikation: Realität? Illusion? Teufelswerk?**

**Ueli Maurer**

**ETH Zürich**

11. Berner Tagung für Informationssicherheit, 25. Nov. 2008

**Sicherheit ???**

**Sicherheit ??? – Provokative Fragen:**

# **Sicherheit ??? – Provokative Fragen:**

- **Warum sind Informationssysteme so unsicher?**

# **Sicherheit ??? – Provokative Fragen:**

- **Warum sind Informationssysteme so unsicher?**
- **Warum ist Software so fehlerhaft?**

# **Sicherheit ??? – Provokative Fragen:**

- **Warum sind Informationssysteme so unsicher?**
- **Warum ist Software so fehlerhaft?**
- **Warum wird Verschlüsselung selten verwendet?**

# **Sicherheit ??? – Provokative Fragen:**

- **Warum sind Informationssysteme so unsicher?**
- **Warum ist Software so fehlerhaft?**
- **Warum wird Verschlüsselung selten verwendet?**
- **Warum gibt es keine brauchbare PKI?**

## **Sicherheit ??? – Provokative Fragen:**

- **Warum sind Informationssysteme so unsicher?**
- **Warum ist Software so fehlerhaft?**
- **Warum wird Verschlüsselung selten verwendet?**
- **Warum gibt es keine brauchbare PKI?**

**Gegenfragen:**

## **Sicherheit ??? – Provokative Fragen:**

- **Warum sind Informationssysteme so unsicher?**
- **Warum ist Software so fehlerhaft?**
- **Warum wird Verschlüsselung selten verwendet?**
- **Warum gibt es keine brauchbare PKI?**

## **Gegenfragen:**

- **Wer zahlt für Sicherheit?**

## **Sicherheit ??? – Provokative Fragen:**

- **Warum sind Informationssysteme so unsicher?**
- **Warum ist Software so fehlerhaft?**
- **Warum wird Verschlüsselung selten verwendet?**
- **Warum gibt es keine brauchbare PKI?**

## **Gegenfragen:**

- **Wer zahlt für Sicherheit?**
- **Was ist Sicherheit?**

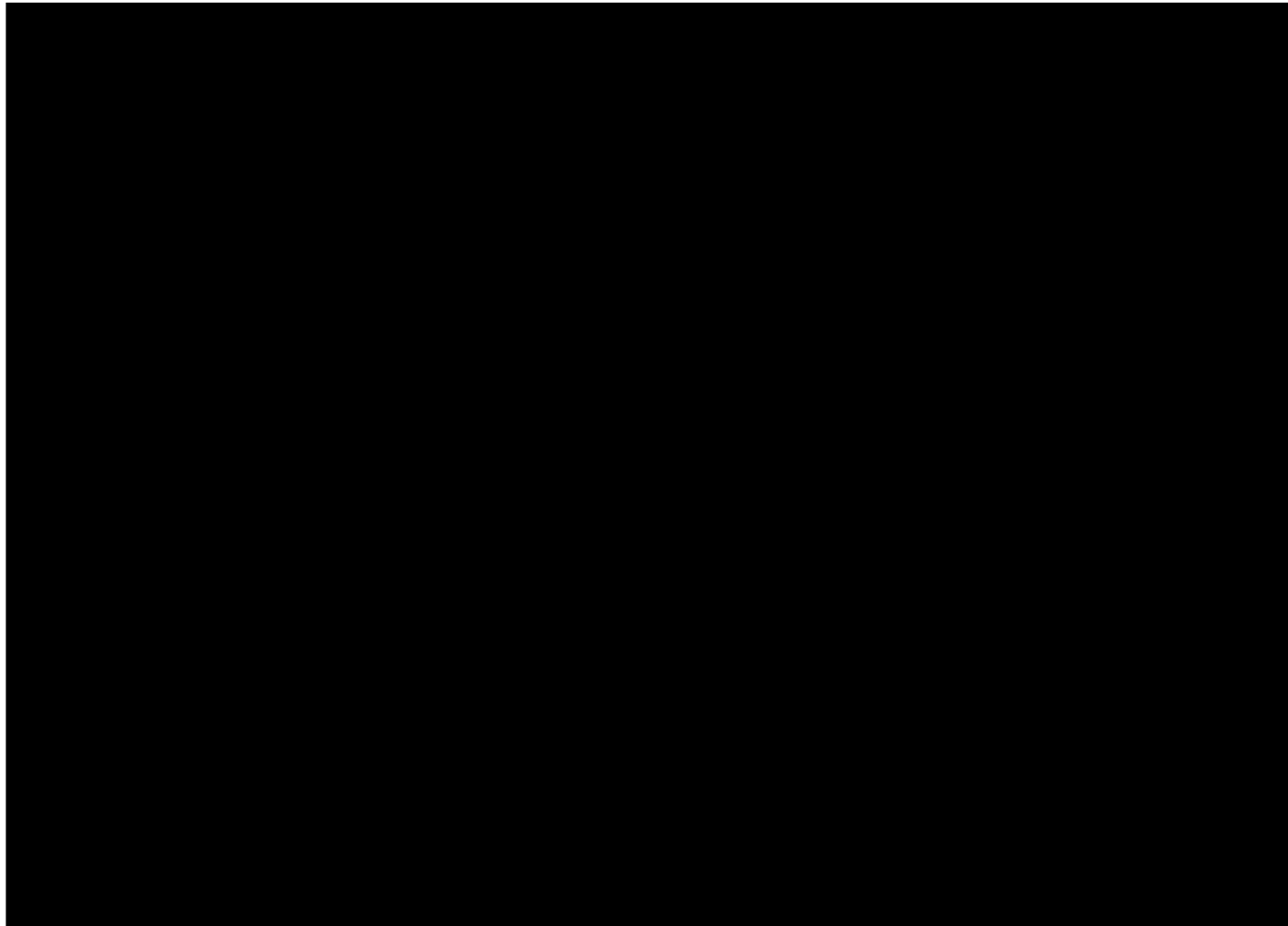
# **Sicherheit ??? – Provokative Fragen:**

- **Warum sind Informationssysteme so unsicher?**
- **Warum ist Software so fehlerhaft?**
- **Warum wird Verschlüsselung selten verwendet?**
- **Warum gibt es keine brauchbare PKI?**

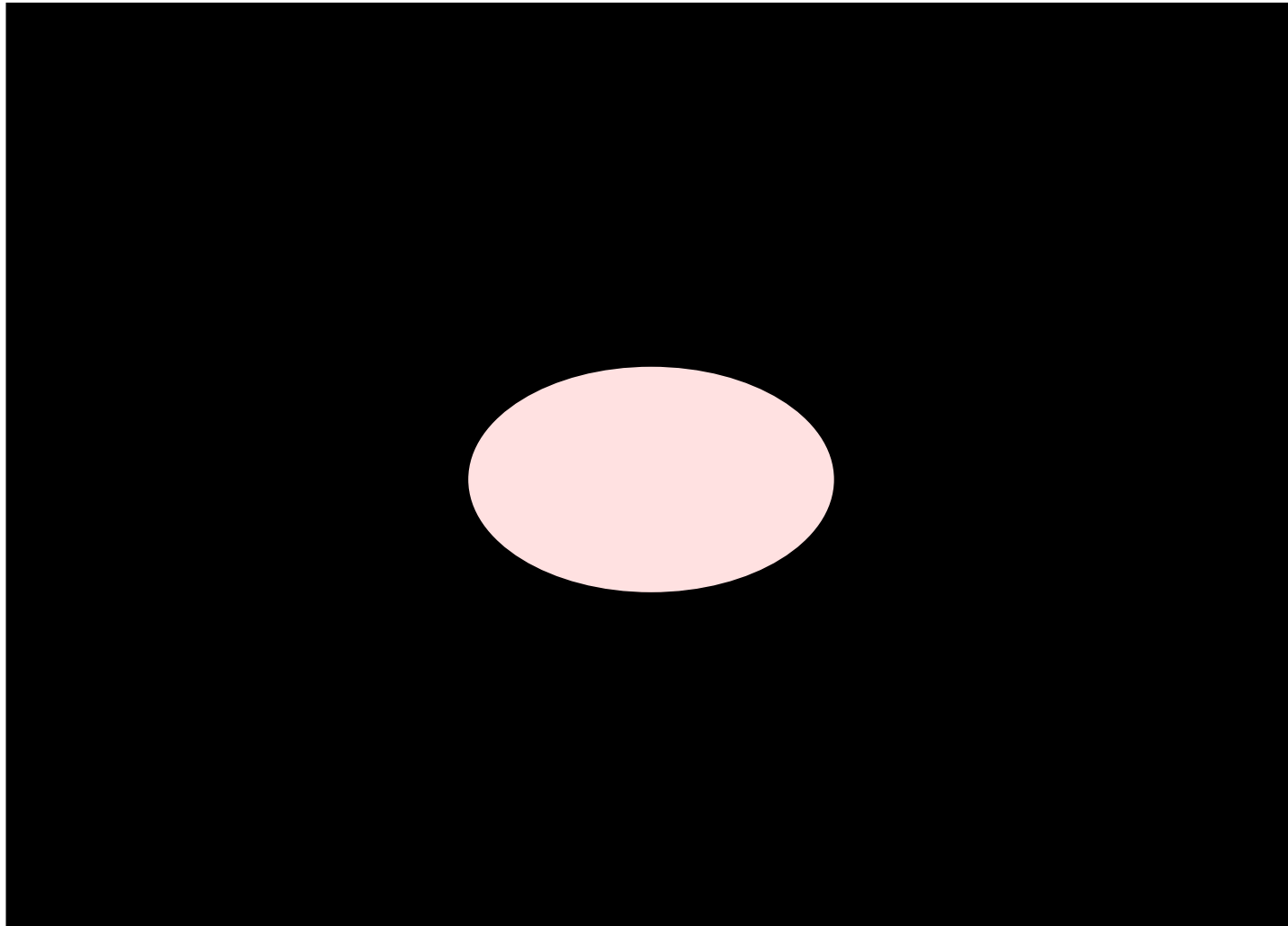
## **Gegenfragen:**

- **Wer zahlt für Sicherheit?**
- **Was ist Sicherheit?**
- **Wer will Sicherheit?**

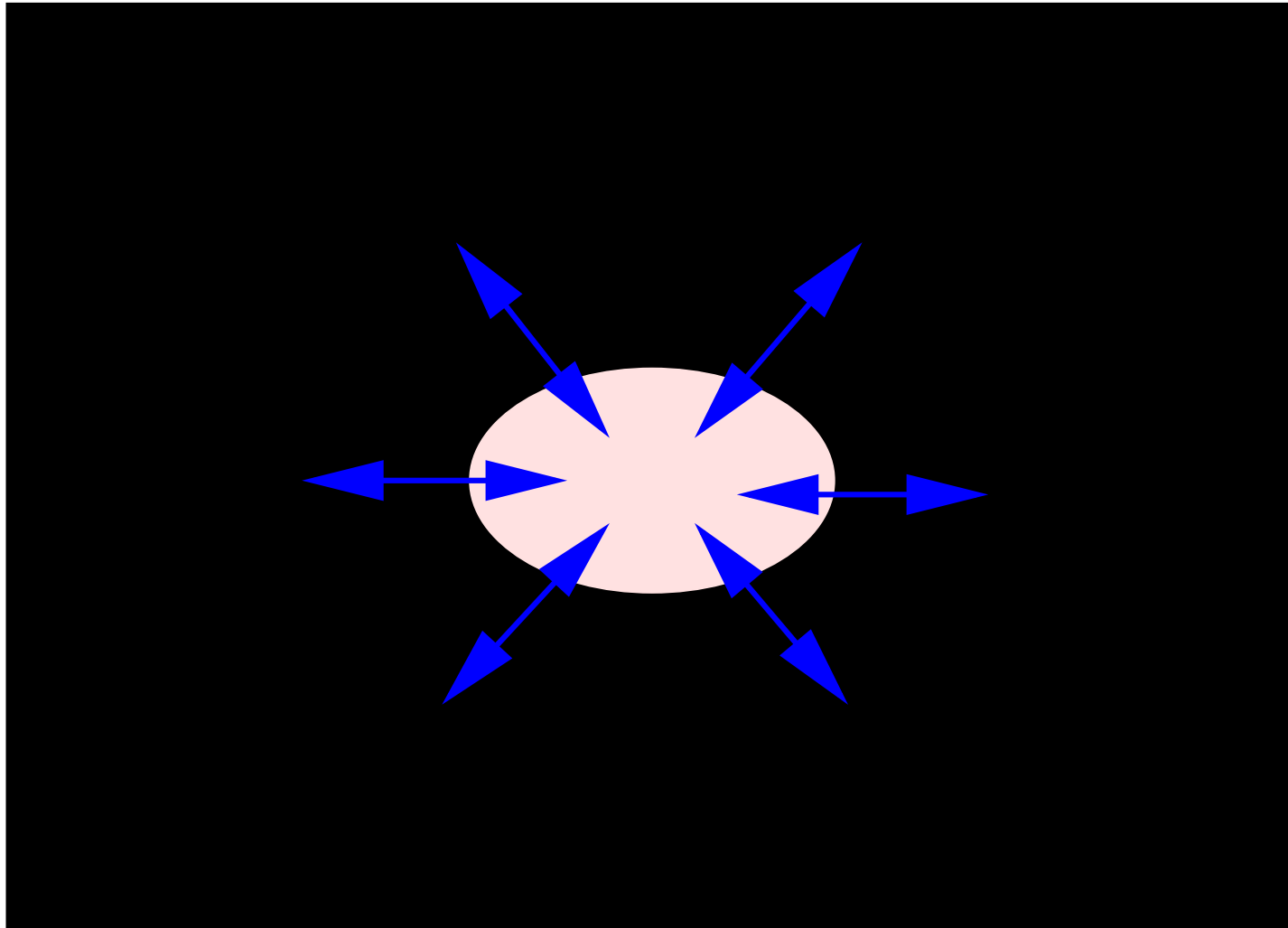
# Informationssicherheit: Klassifikation



# Informationssicherheit: Klassifikation

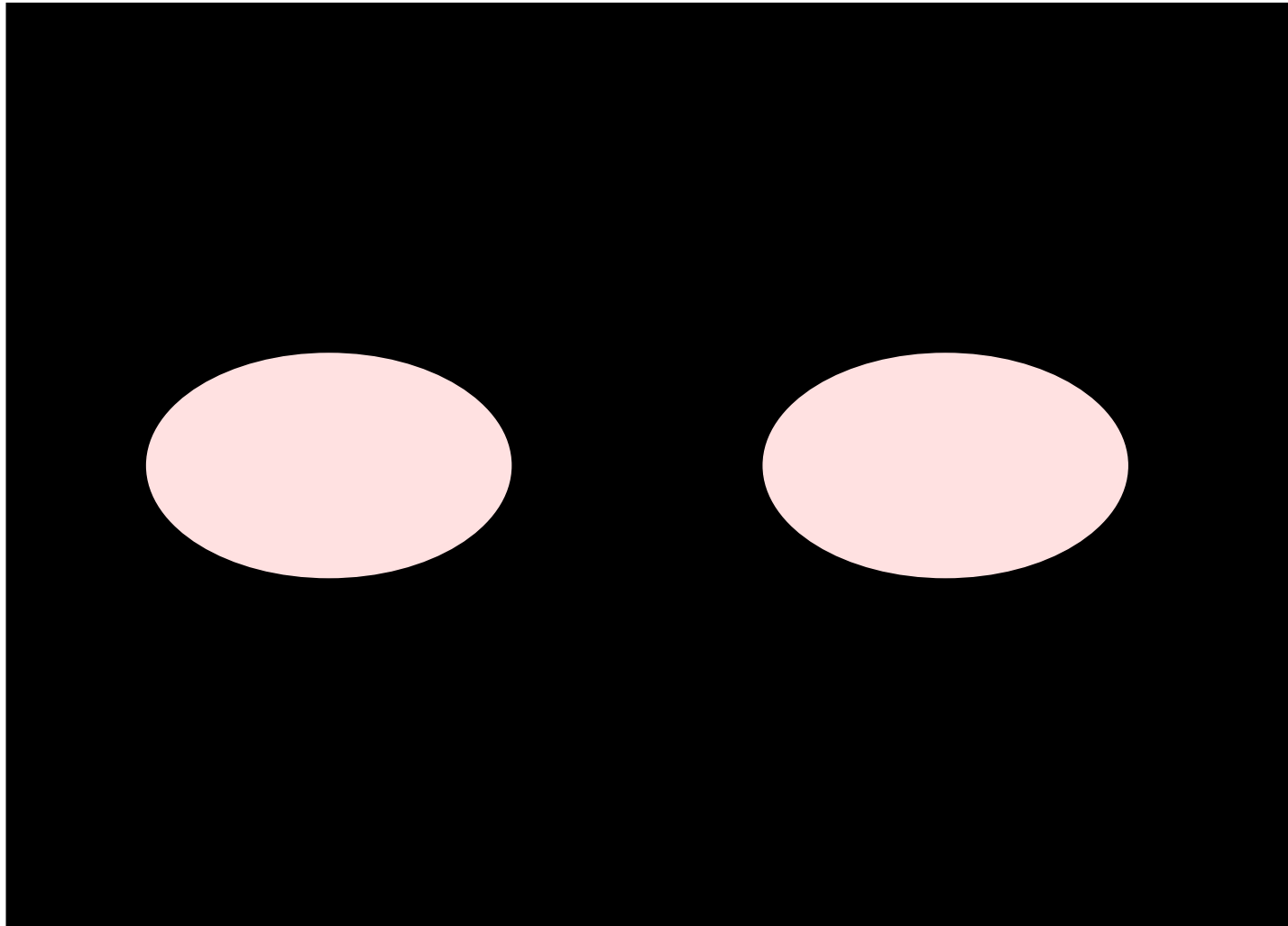


# Informationssicherheit: Klassifikation

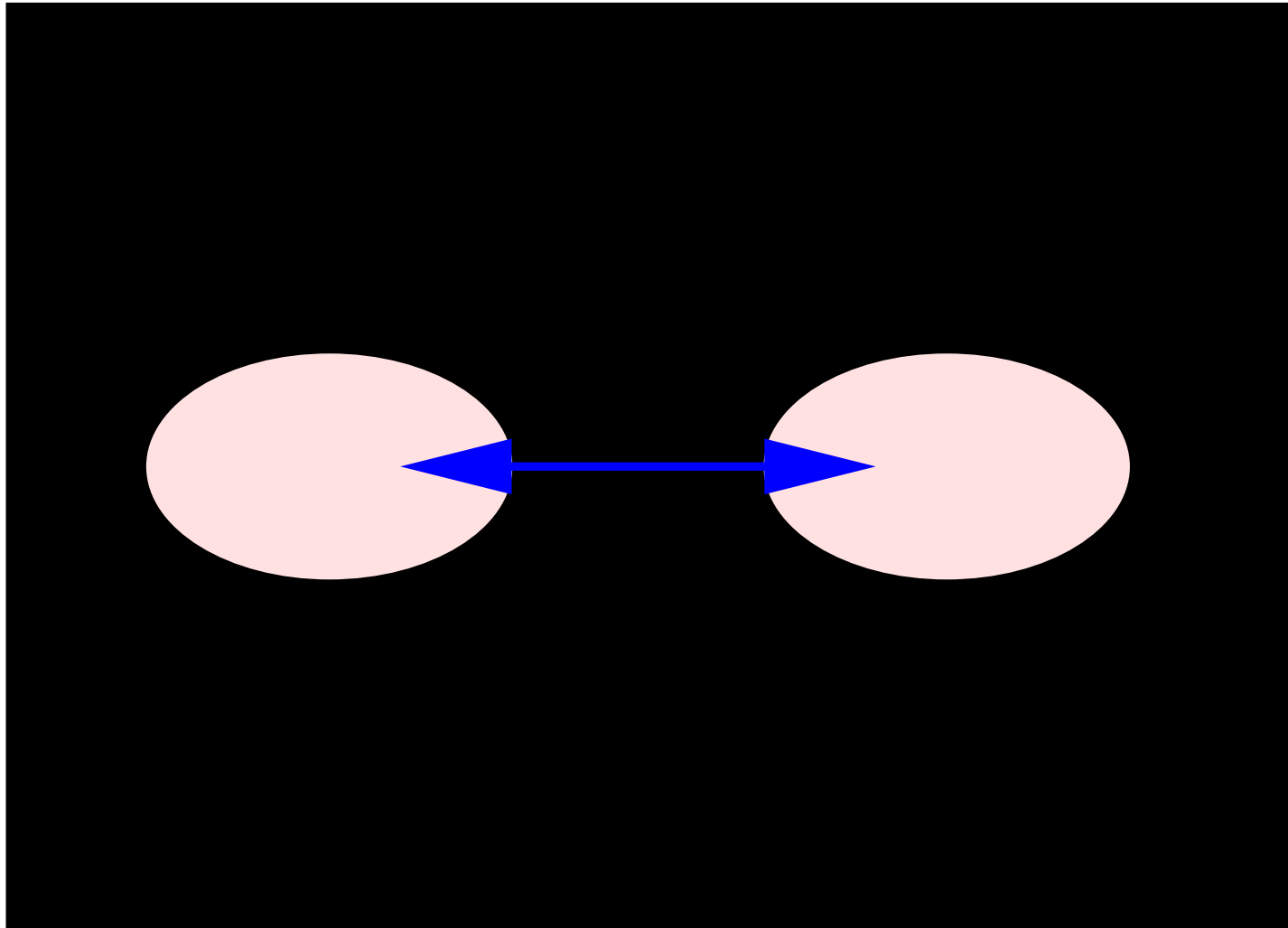


## 1. Unilaterale Sicherheit

# Informationssicherheit: Klassifikation

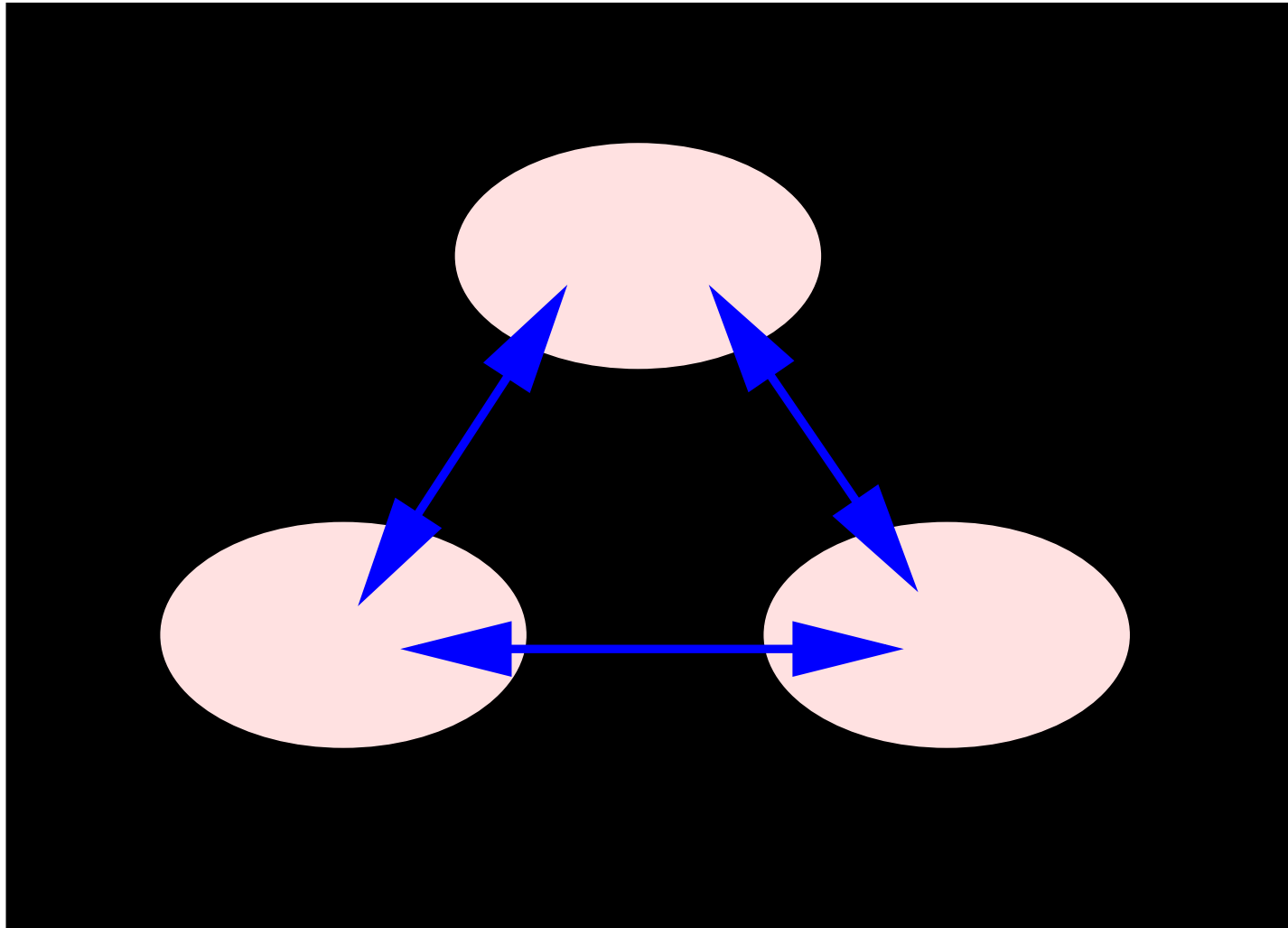


# Informationssicherheit: Klassifikation



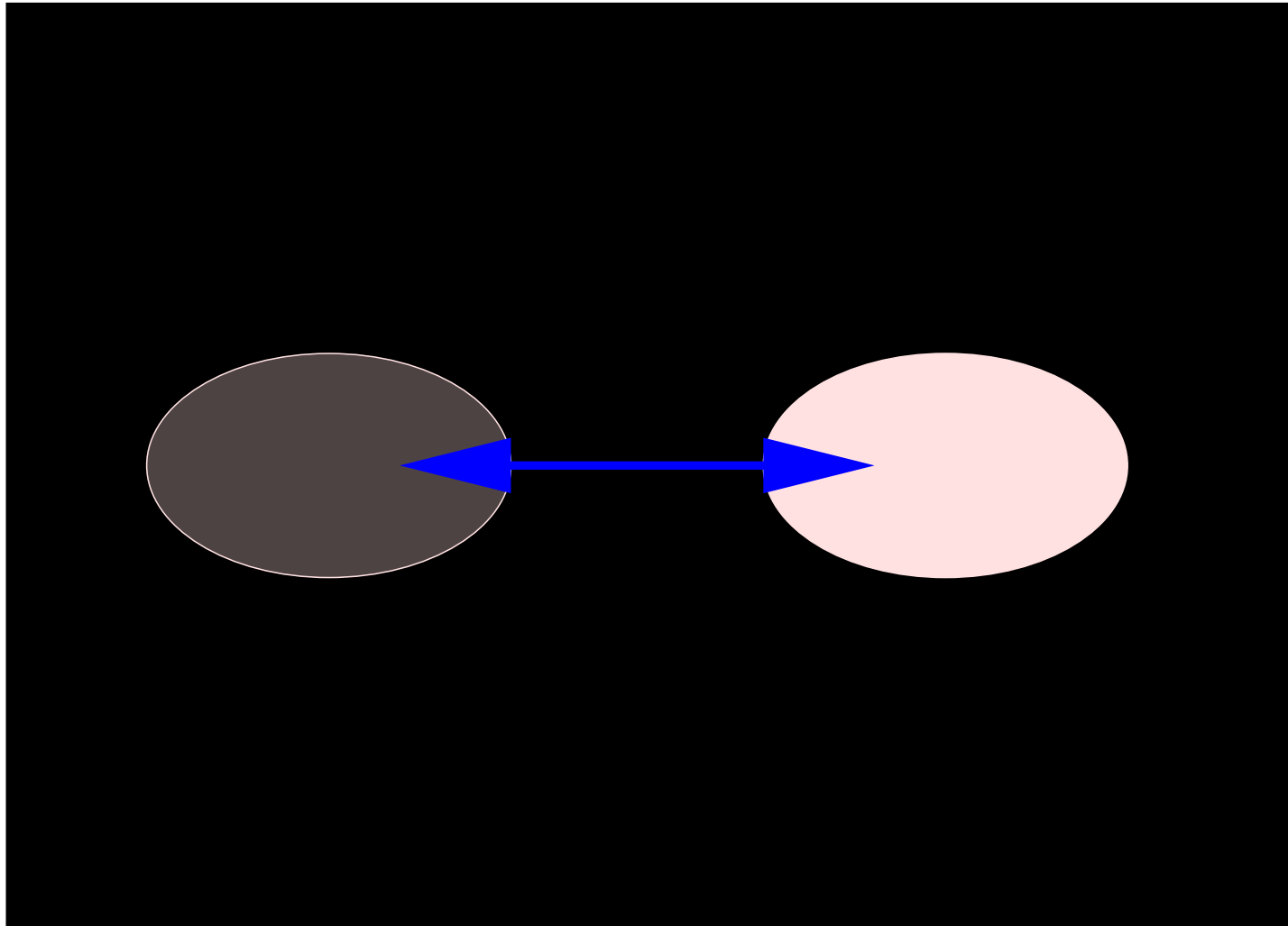
## 2. Sichere Kommunikation

# Informationssicherheit: Klassifikation

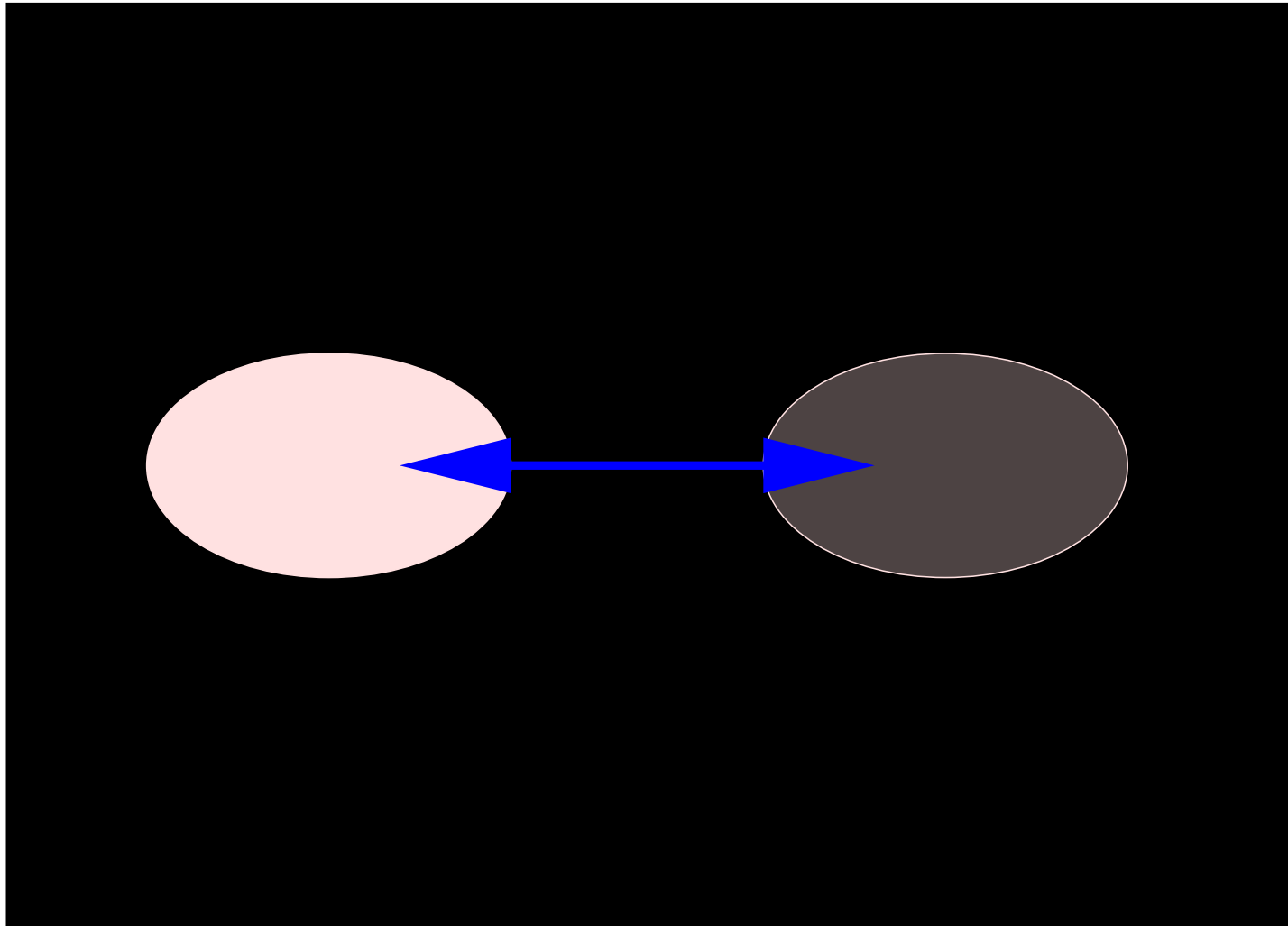


## 2. Sichere Kommunikation

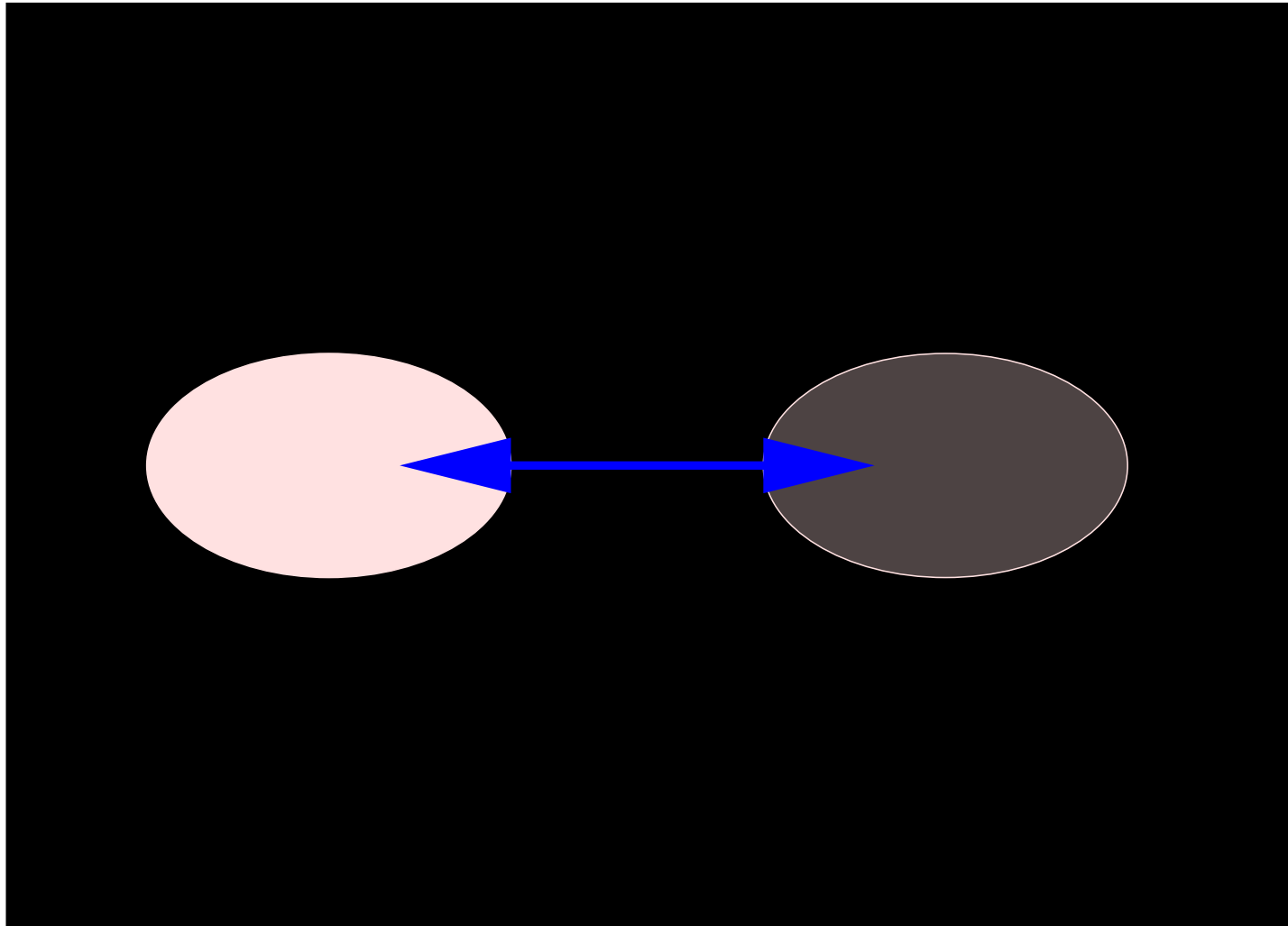
# Informationssicherheit: Klassifikation



# Informationssicherheit: Klassifikation

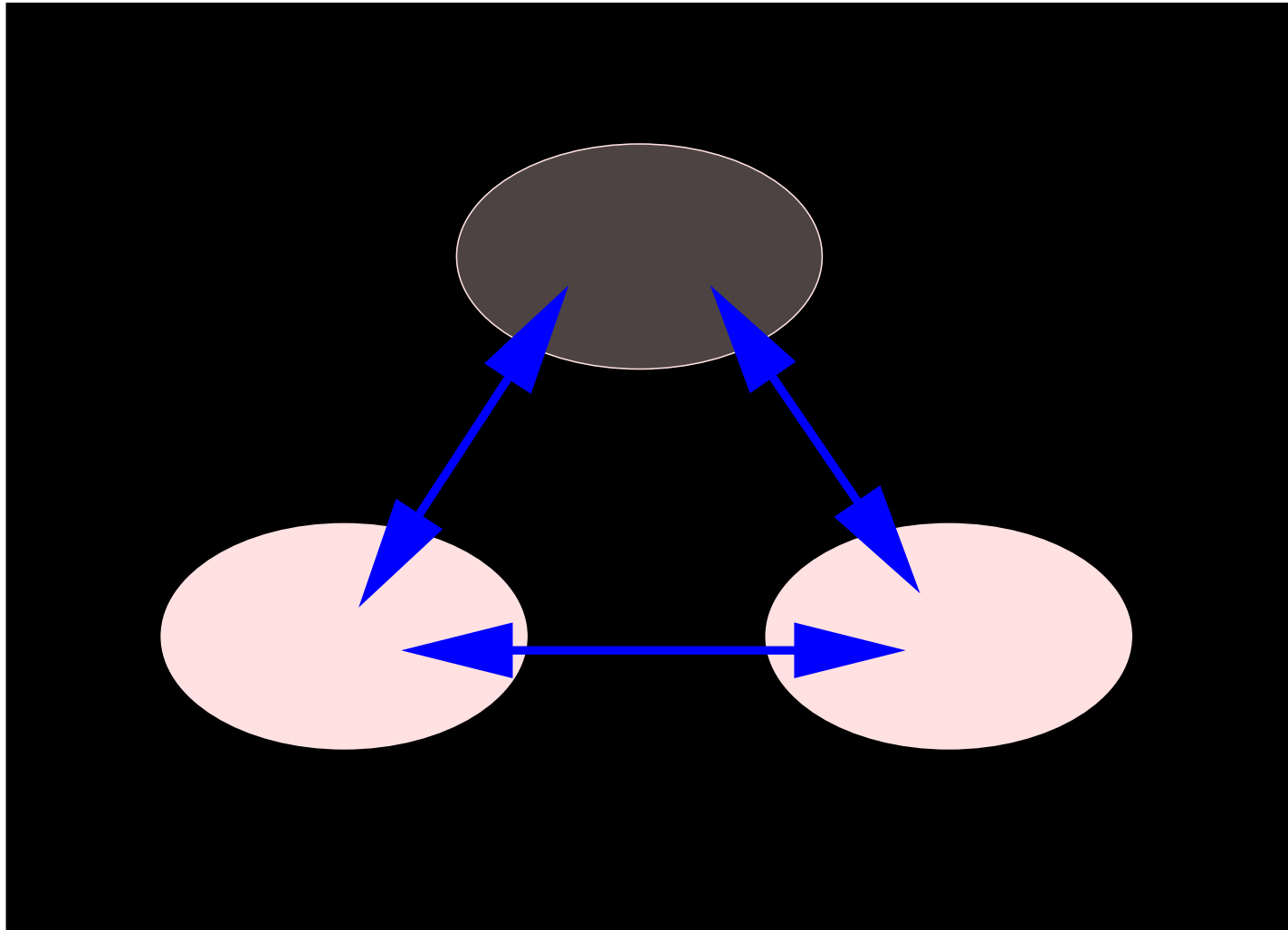


# Informationssicherheit: Klassifikation



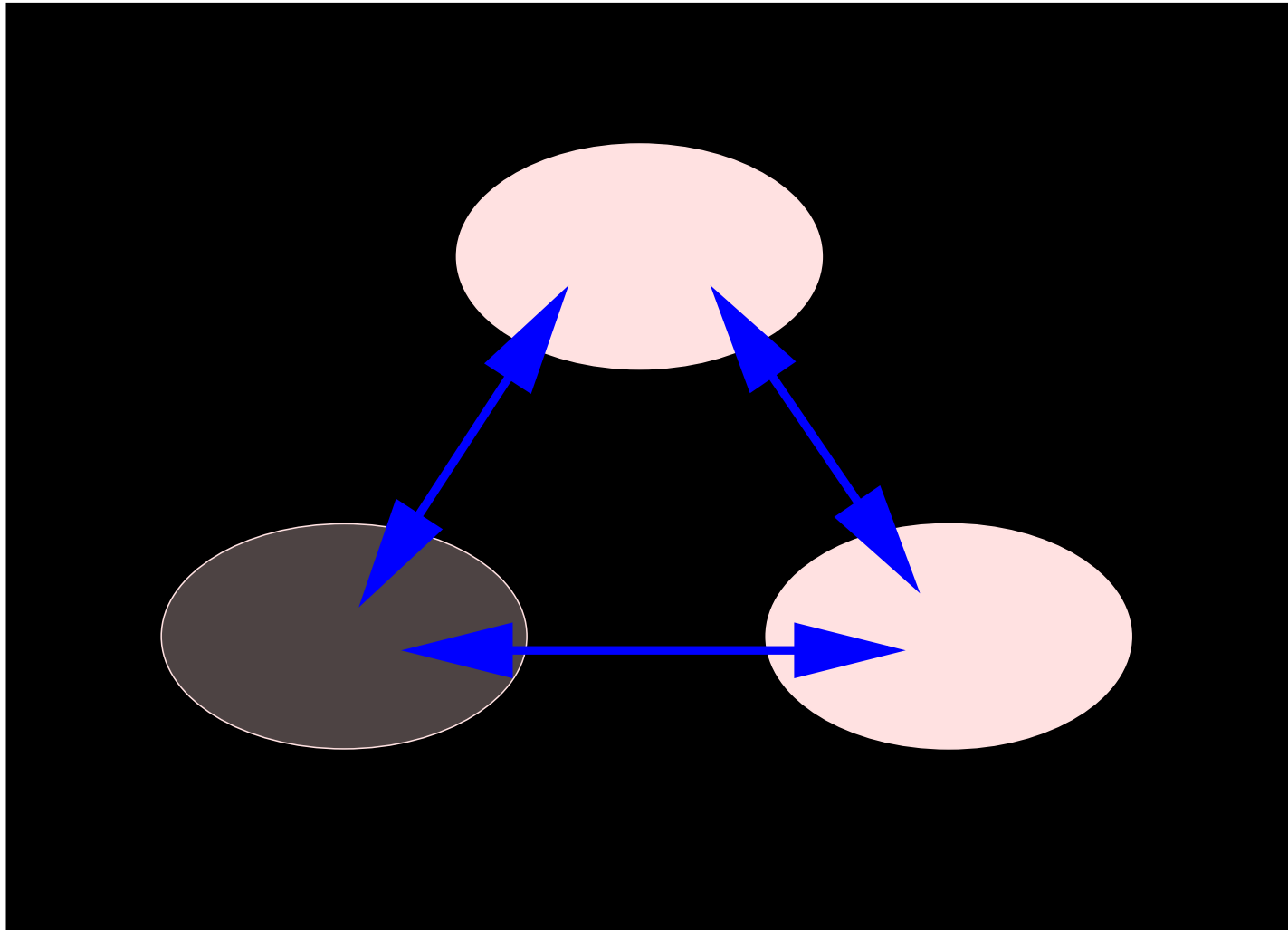
## 3. Bilaterale Sicherheit

# Informationssicherheit: Klassifikation



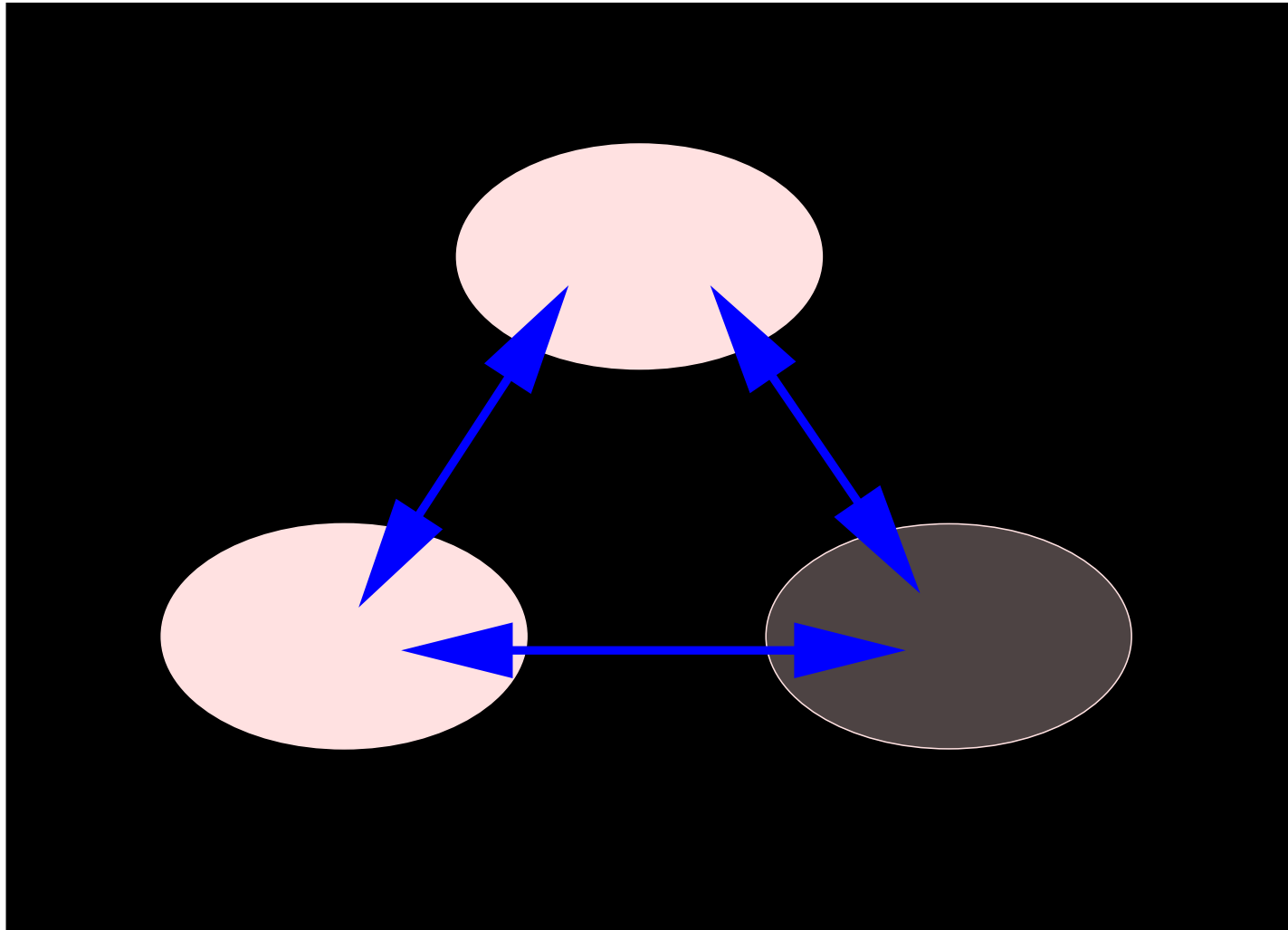
## 3. Multilaterale Sicherheit

# Informationssicherheit: Klassifikation



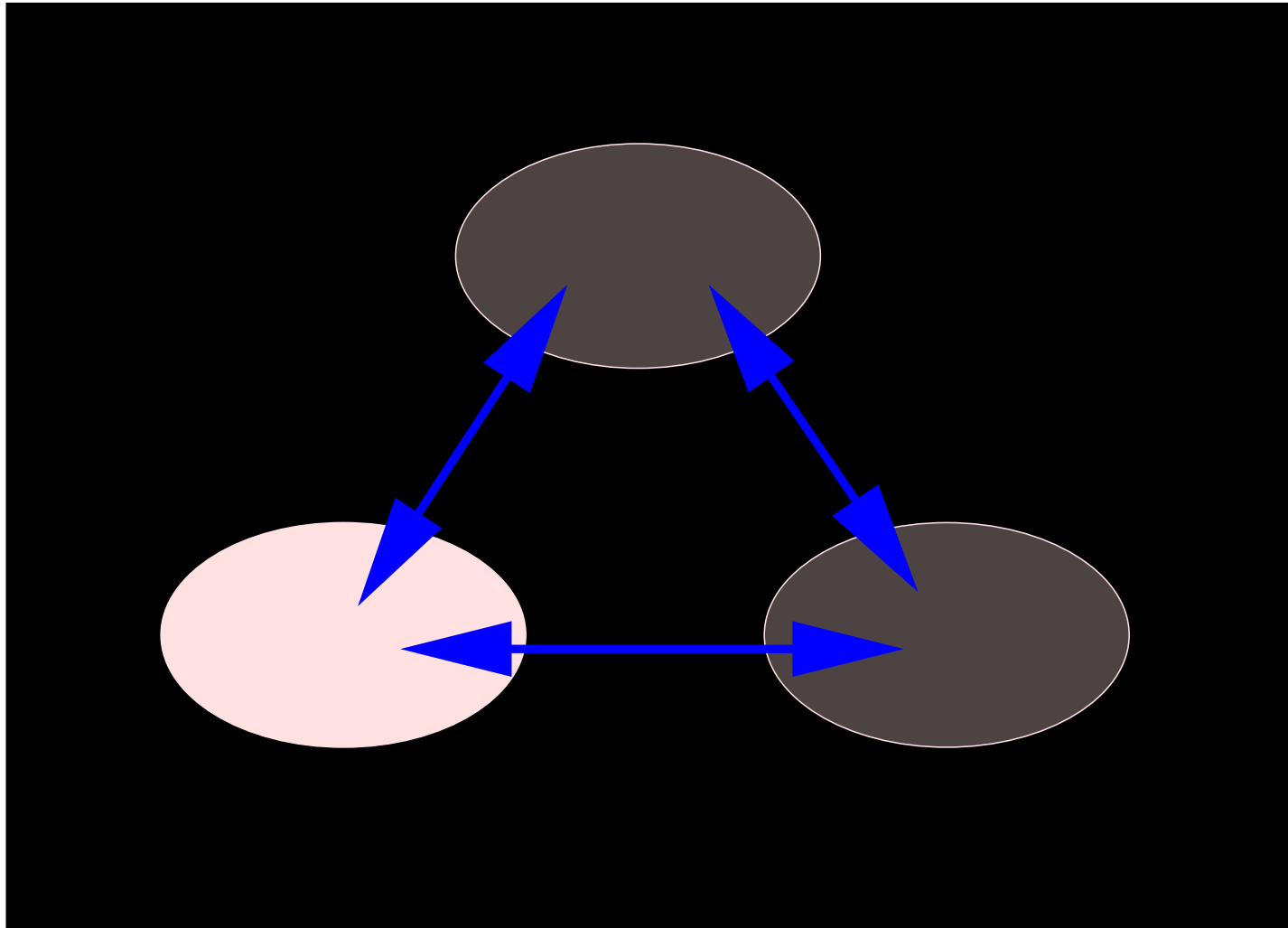
## 3. Multilaterale Sicherheit

# Informationssicherheit: Klassifikation



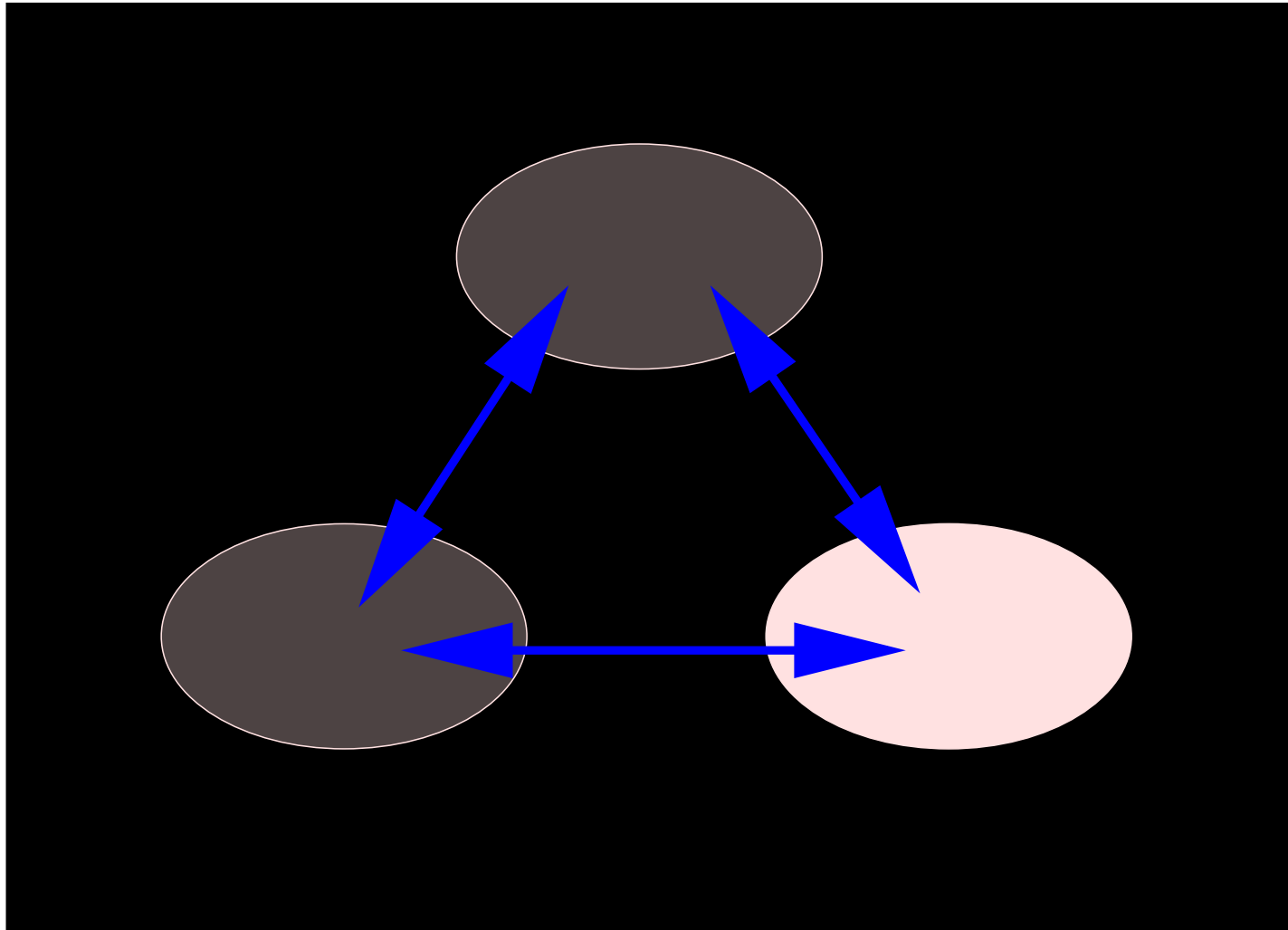
## 3. Multilaterale Sicherheit

# Informationssicherheit: Klassifikation



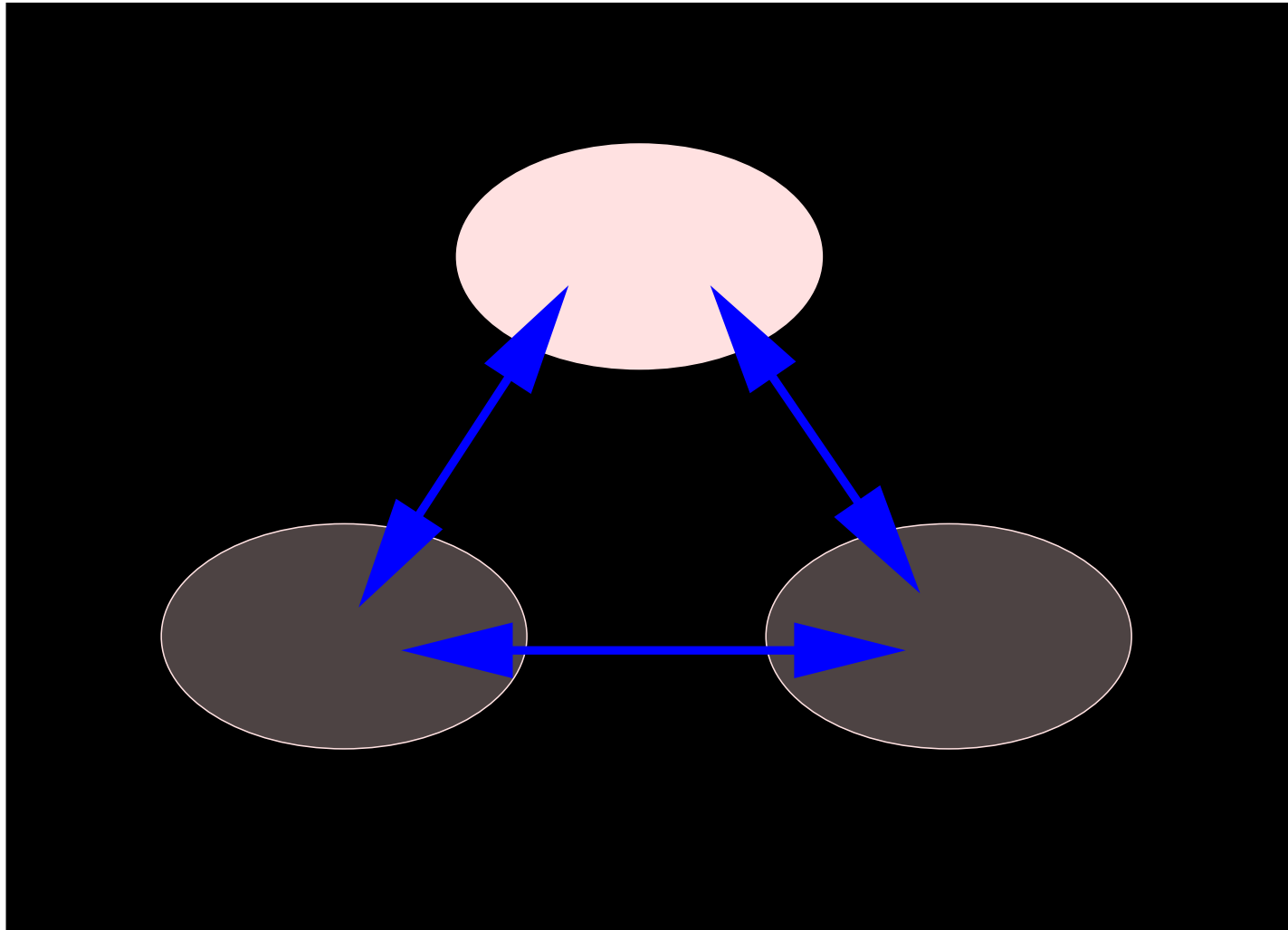
## 3. Multilaterale Sicherheit

# Informationssicherheit: Klassifikation



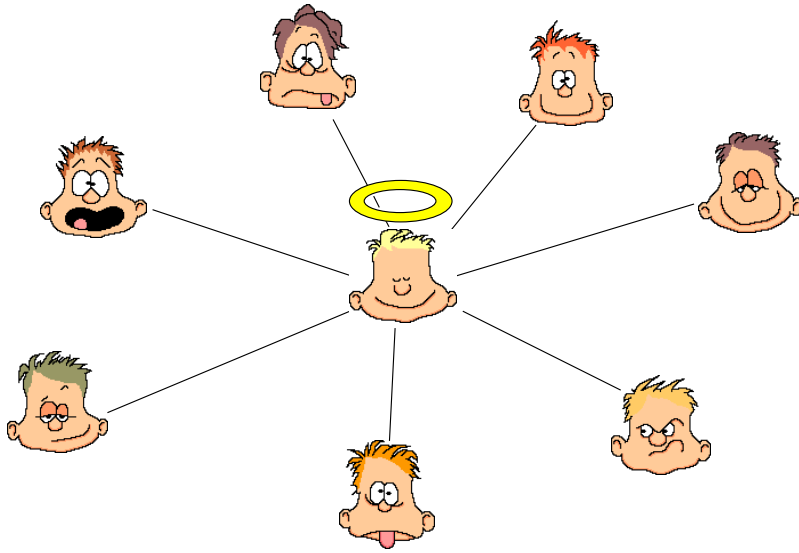
## 3. Multilaterale Sicherheit

# Informationssicherheit: Klassifikation



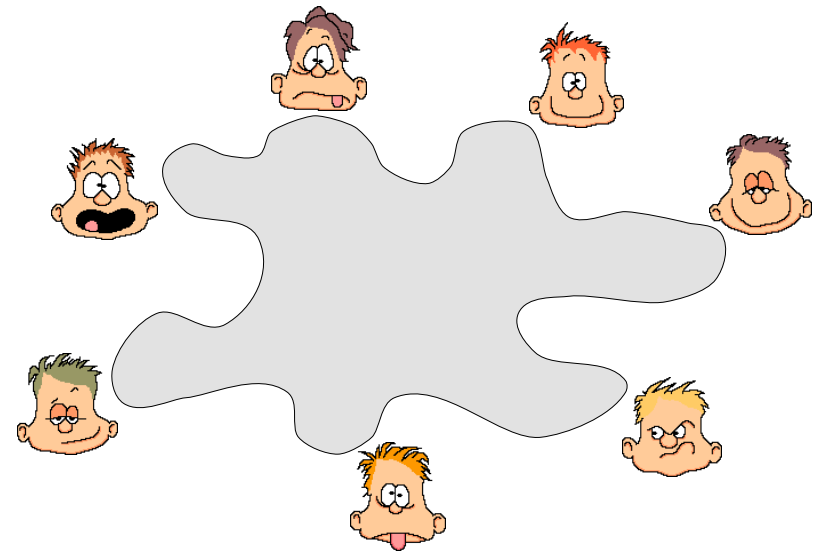
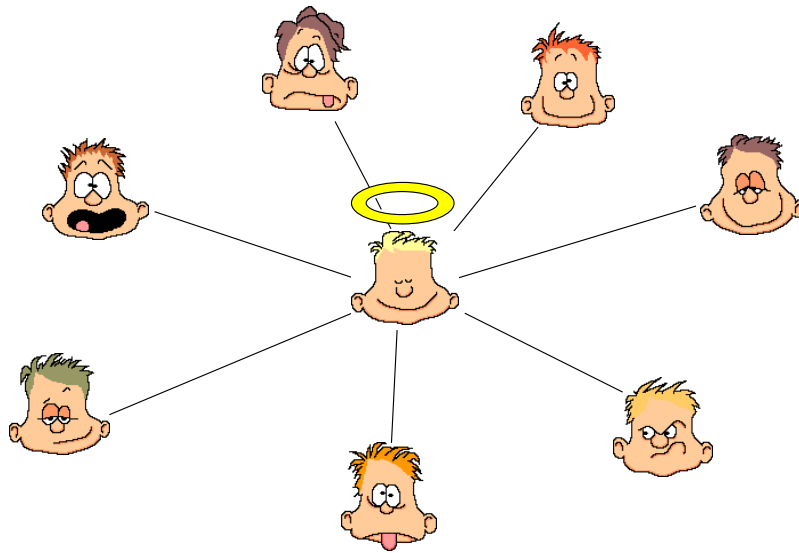
## 3. Multilaterale Sicherheit

# Multilaterale Sicherheit



**Spezifikation**

# Multilaterale Sicherheit

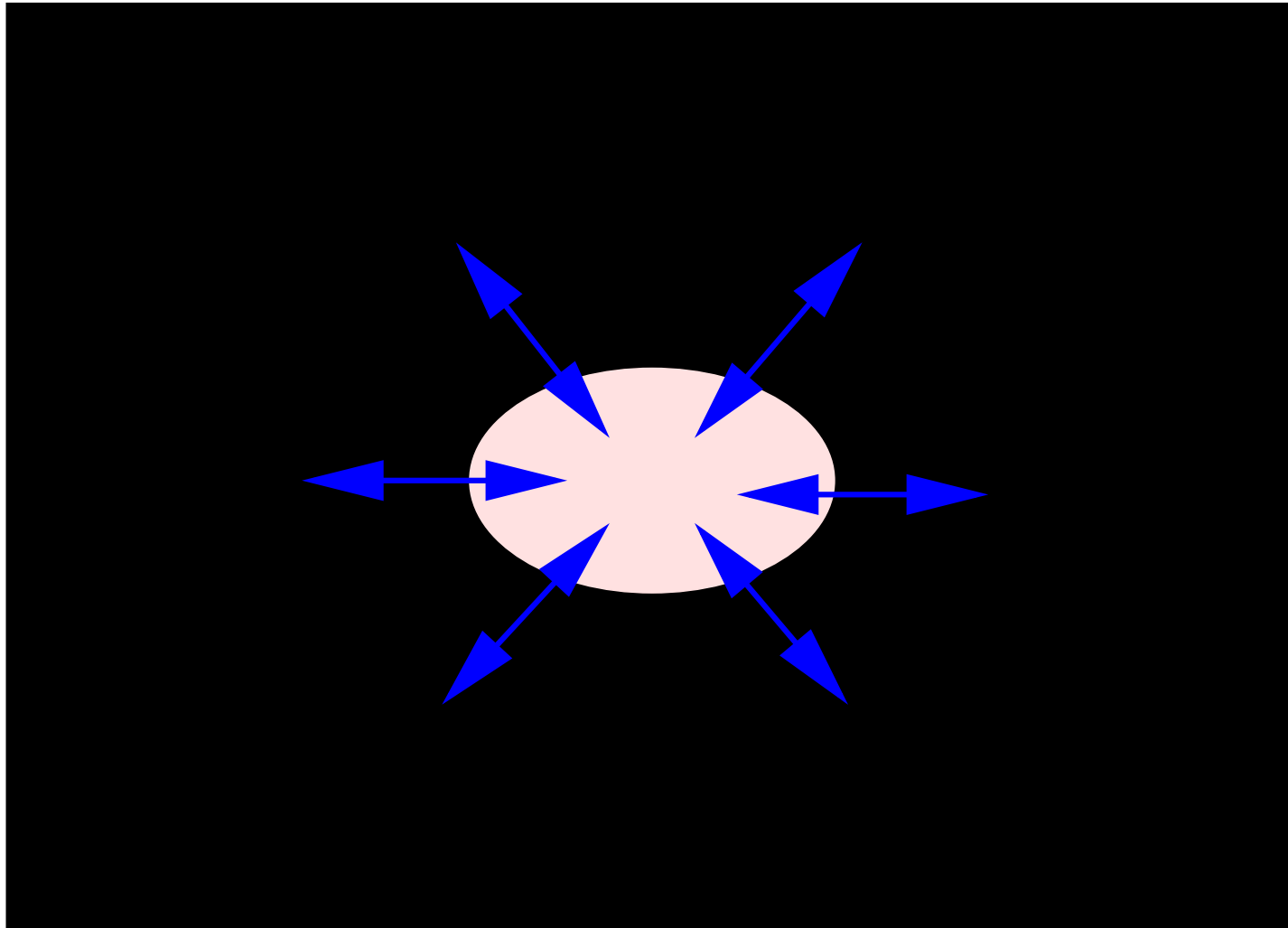


**Spezifikation**



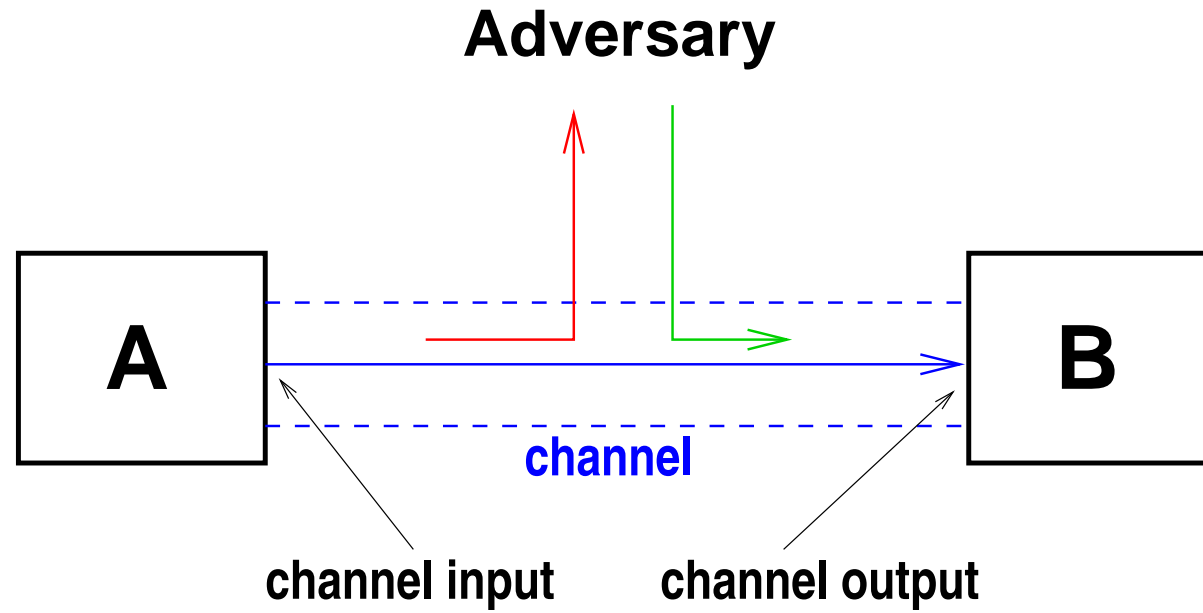
**Implementation**

# Informationssicherheit: Klassifikation

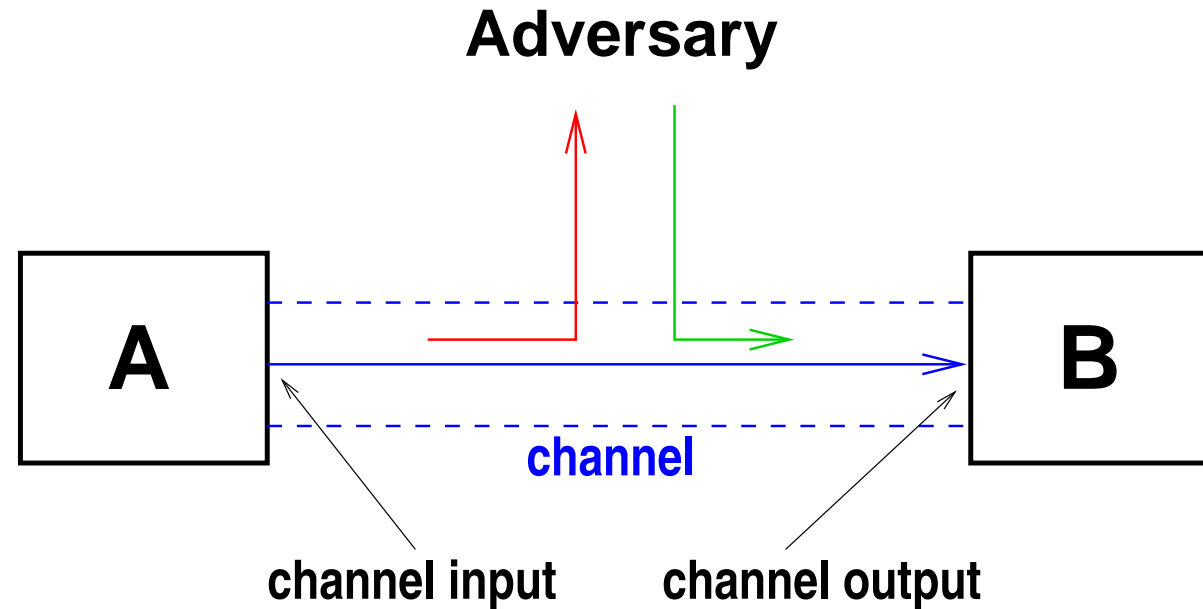


## 1. Unilaterale Sicherheit

# Sichere Kommunikation



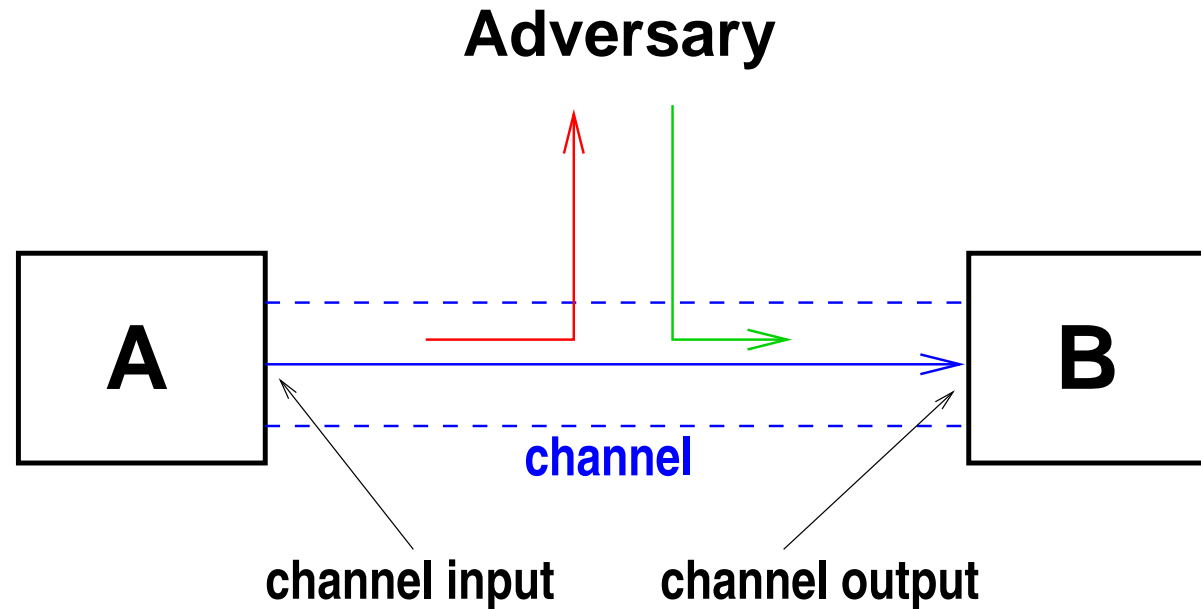
# Sichere Kommunikation



## Sicherheitsziele:

- Vertraulichkeit, Authentizität (inkl. Integrität)

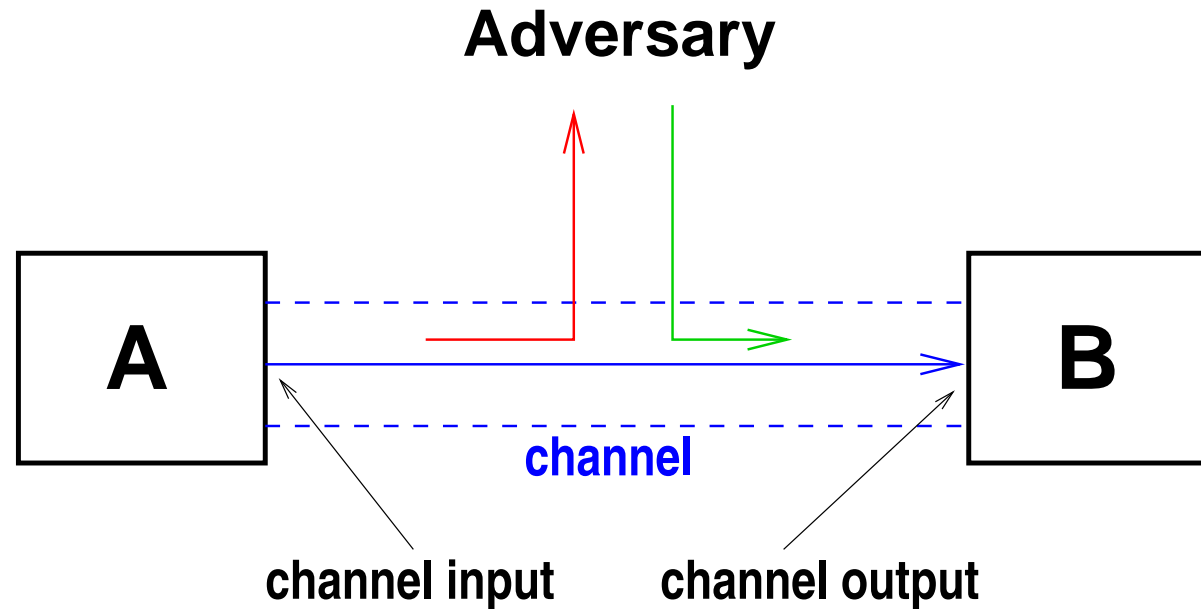
# Sichere Kommunikation



## Sicherheitsziele:

- Vertraulichkeit, Authentizität (inkl. Integrität)
- Verfügbarkeit

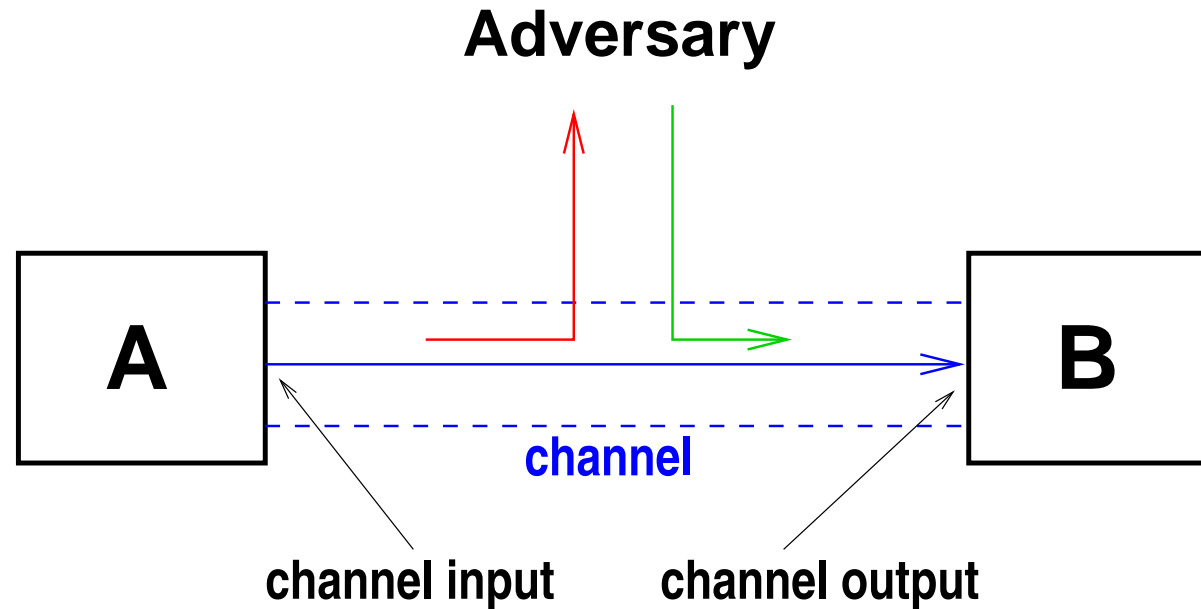
# Sichere Kommunikation



## Sicherheitsziele:

- Vertraulichkeit, Authentizität (inkl. Integrität)
- Verfügbarkeit
- Beweisbarkeit

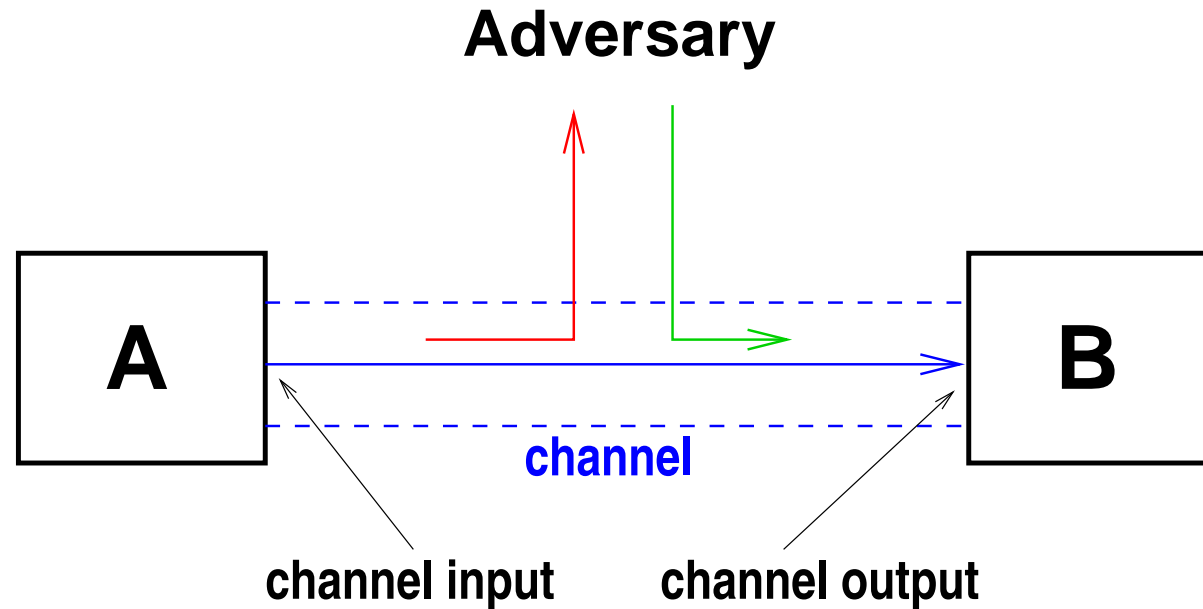
# Sichere Kommunikation



## Sicherheitsziele:

- Vertraulichkeit, Authentizität (inkl. Integrität)
- Verfügbarkeit
- Beweisbarkeit
- Anonymität

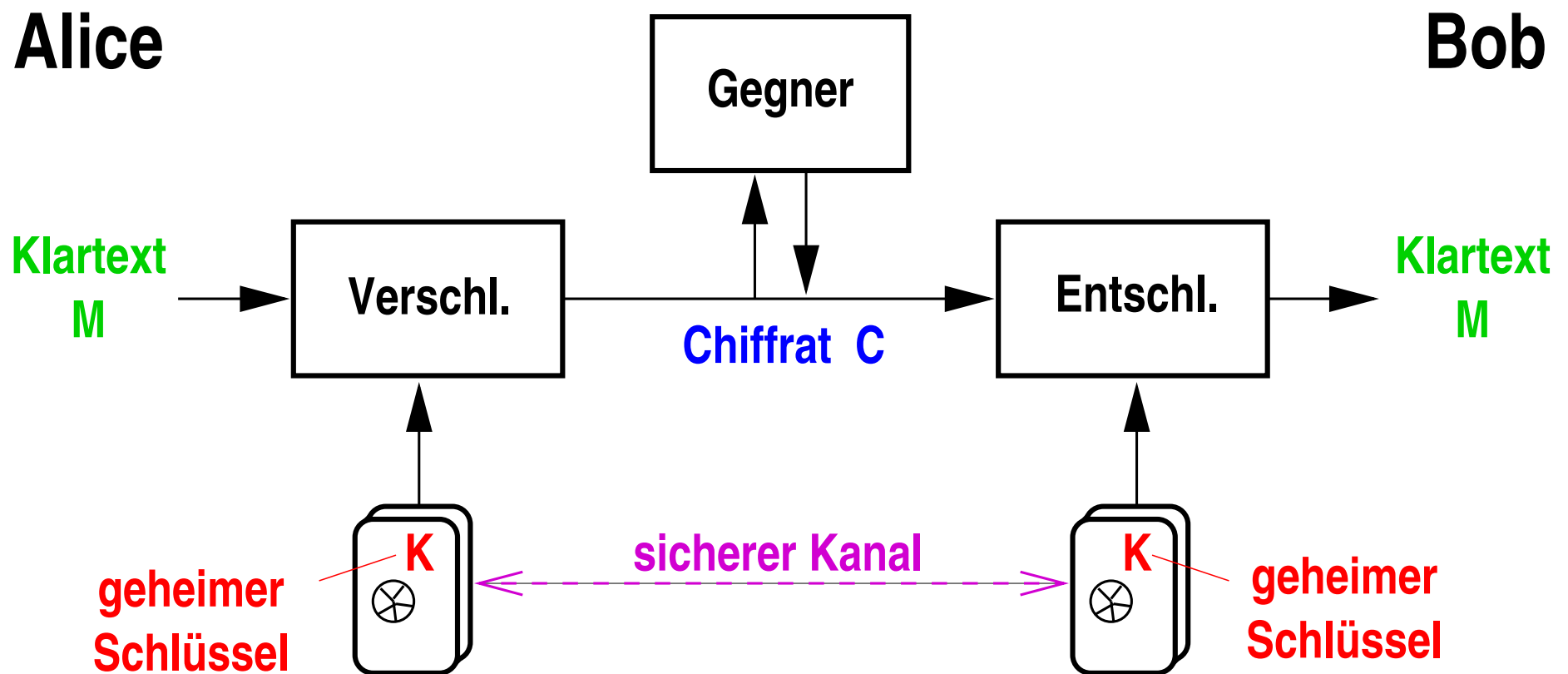
# Sichere Kommunikation



## Sicherheitsziele:

- Vertraulichkeit, Authentizität (inkl. Integrität)
- Verfügbarkeit
- Beweisbarkeit
- Anonymität
- Gleichzeitigkeit (Austausch), Nichterpressbarkeit, ...

# Verschlüsselung



# Fazit

# Fazit

- **“Sicherheit” ist oft das Problem mangelnder Spezifikation und fehlerhafter Implementation.**

# Fazit

- **“Sicherheit” ist oft das Problem mangelnder Spezifikation und fehlerhafter Implementation.**
- **Neue Businessmodelle, die Fehler reduzieren.**

# Fazit

- **“Sicherheit” ist oft das Problem mangelnder Spezifikation und fehlerhafter Implementation.**
- **Neue Businessmodelle, die Fehler reduzieren.**
- **Sicherheit als konstruktive Disziplin:**
  - defensive Sicht ablegen!
  - Sicherheit beweisen, nicht vage vermuten.
  - Sicherheit beruht immer auf Annahmen!  
→ explizit machen und minimieren.

# Fazit

- **“Sicherheit” ist oft das Problem mangelnder Spezifikation und fehlerhafter Implementation.**
- **Neue Businessmodelle, die Fehler reduzieren.**
- **Sicherheit als konstruktive Disziplin:**
  - defensive Sicht ablegen!
  - Sicherheit beweisen, nicht vage vermuten.
  - Sicherheit beruht immer auf Annahmen!  
→ explizit machen und minimieren.
- **Zentrales Thema in Forschung und Ausbildung.**

# Fazit

- **“Sicherheit” ist oft das Problem mangelnder Spezifikation und fehlerhafter Implementation.**
- **Neue Businessmodelle, die Fehler reduzieren.**
- **Sicherheit als konstruktive Disziplin:**
  - defensive Sicht ablegen!
  - Sicherheit beweisen, nicht vage vermuten.
  - Sicherheit beruht immer auf Annahmen!  
→ explizit machen und minimieren.
- **Zentrales Thema in Forschung und Ausbildung.**
- **Packen wir's an! Auf welcher Seite stehen Sie?**