# Schlüsselaustausch über unsichere Kanäle am Beispiel von Diffie-Hellman

Dr. Thorsten Weber
Juni 02, 2025

# Erfahrung & Expertise: Ein Blick auf meinen Werdegang

**Dr. Thorsten Weber**

## Beruflicher Werdegang:

- **Team Lead** Offensive Security & Awareness, SAP SE, Walldorf
- **Team Lead** IT-Security, oculavis GmbH, Aachen
- **IT-Security** Administrator, NATO, Brüssel

## Akademischer Werdegang:

- **Promotion** an der Universidad Católica San Antonio de Murcia (UCAM) in Kooperation mit der FOM
- **B.Sc. / M.Sc.**, RWTH Aachen Informatik

## Nebenberufliche Tätigkeit

- **Dozent**, FOM Hochschule, Aachen
- **ISO/IEC 27001 Lead Auditor**

# Was sollten Sie nach dieser Vorlesung wissen und können?

## Sicherheitsproblem verstehen

Warum ist der **Schlüsselaustausch** über **unsichere Kanäle** (etwa dem Internet) eine **Sicherheitsherausforderung**?

## Den Diffie-Hellman-Schlüsselaustausch erklären

Wie kann ein **geheimer Schlüssel** zwischen **zwei Kommunikationsteilnehmenden** über einen **unsicheren Kanal** erstellt werden?

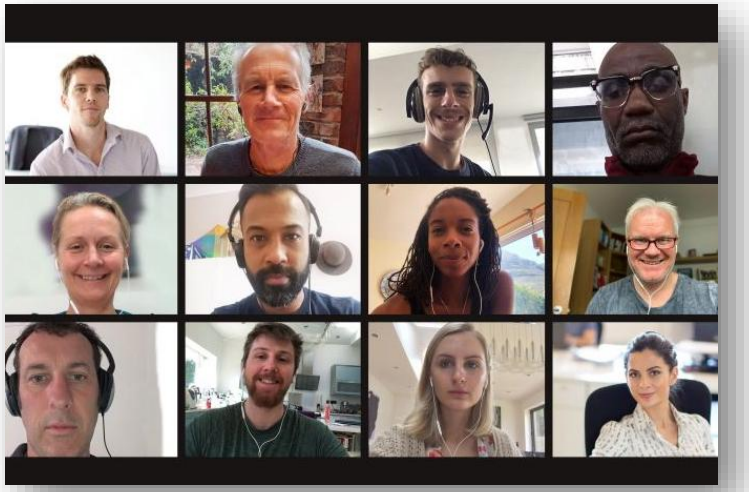
# Agenda

1. Einleitung
2. Diffie-Hellman-Schlüsselaustausch mit Farben
3. Diffie-Hellman-Schlüsselaustausch mit Zahlen
4. Sicherheit & Anwendung
5. Live Demo

# 1 Einleitung

# Wer von Ihnen hat schon einmal…

**… online-Banking verwendet?**



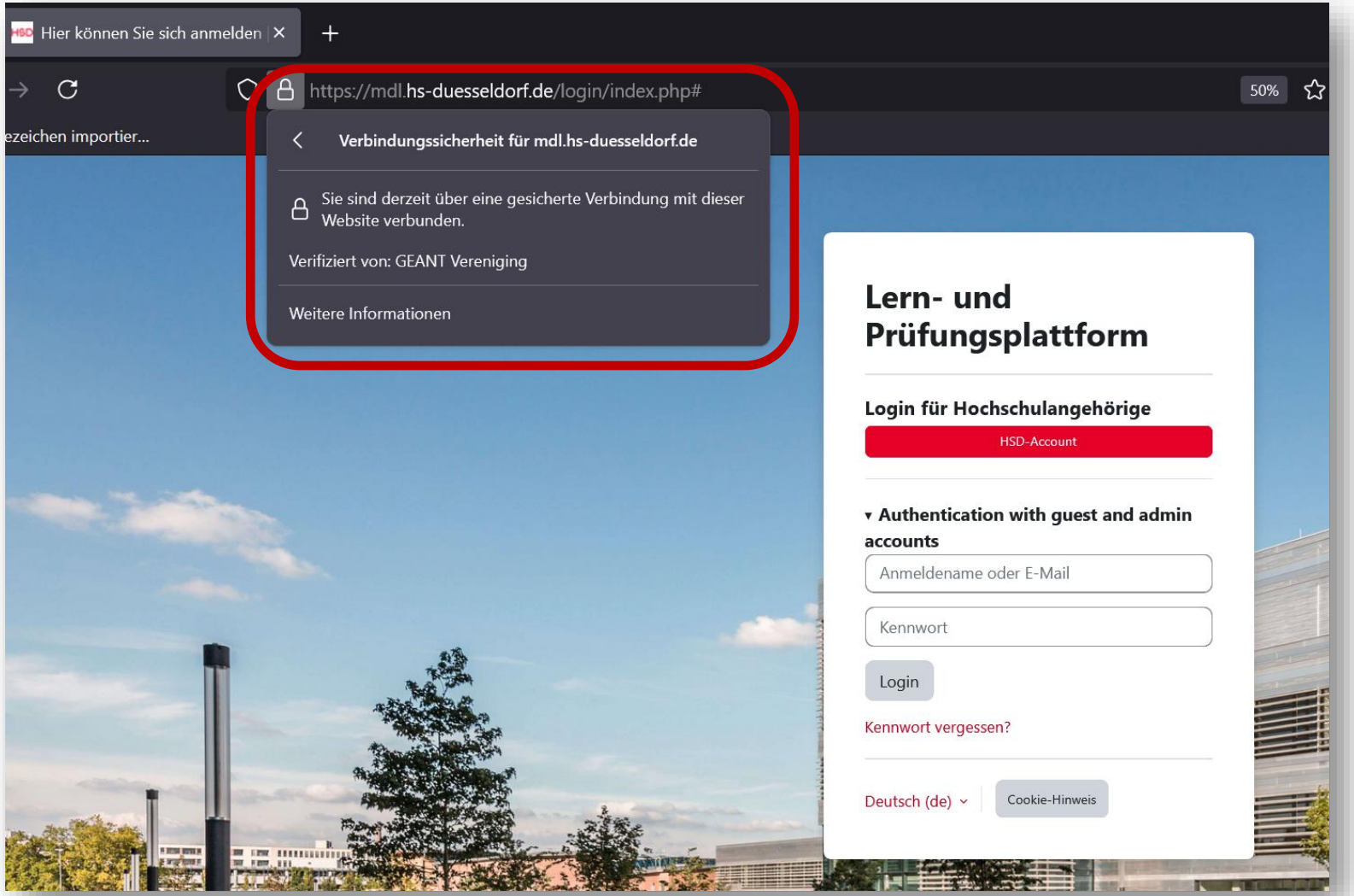
**… an einem Online-Meeting teilgenommen?**

**… online eingekauft?**

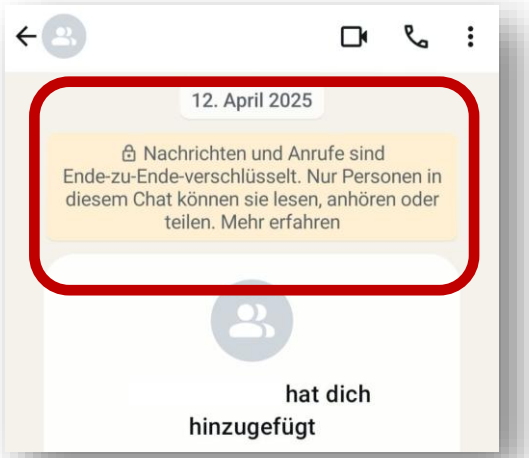
Warum hatten Sie **keine Angst**, dass Ihre **Daten gestohlen** oder **abgehört werden**?

# Weil unsere Daten (meist) verschlüsselt übertragen werden!

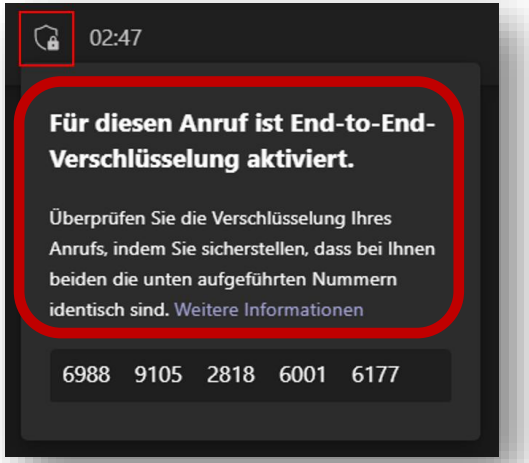
## Website



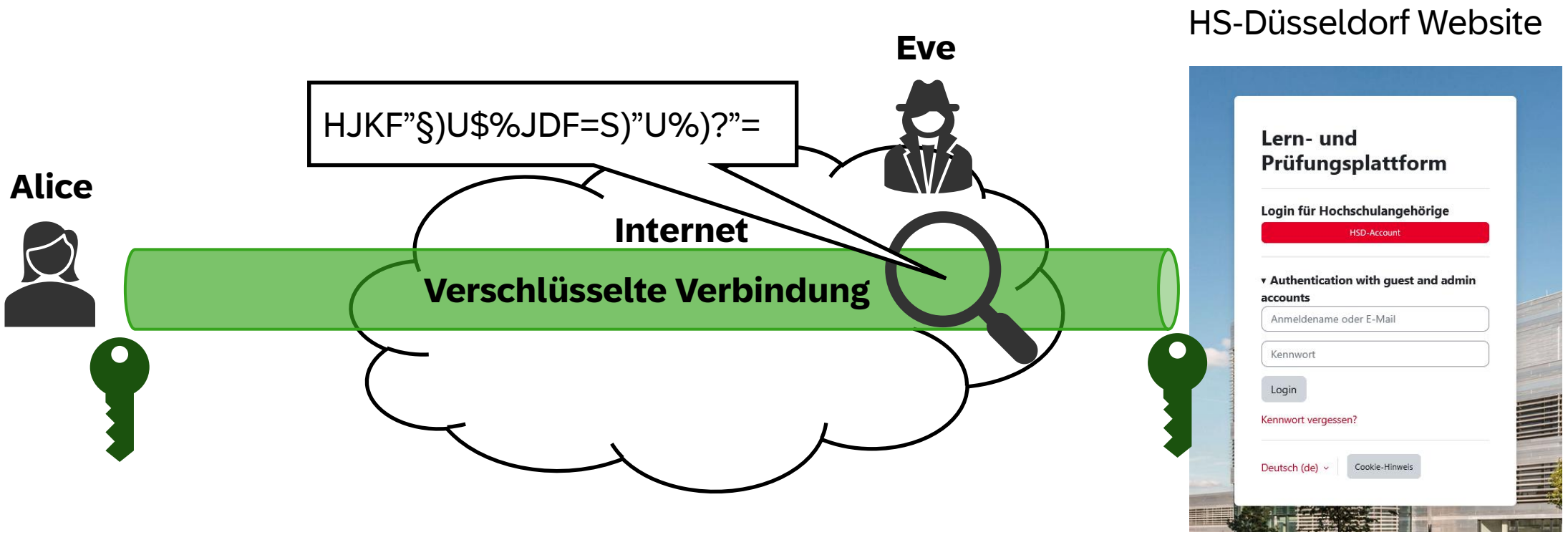

## Messenger




## Online-Meeting

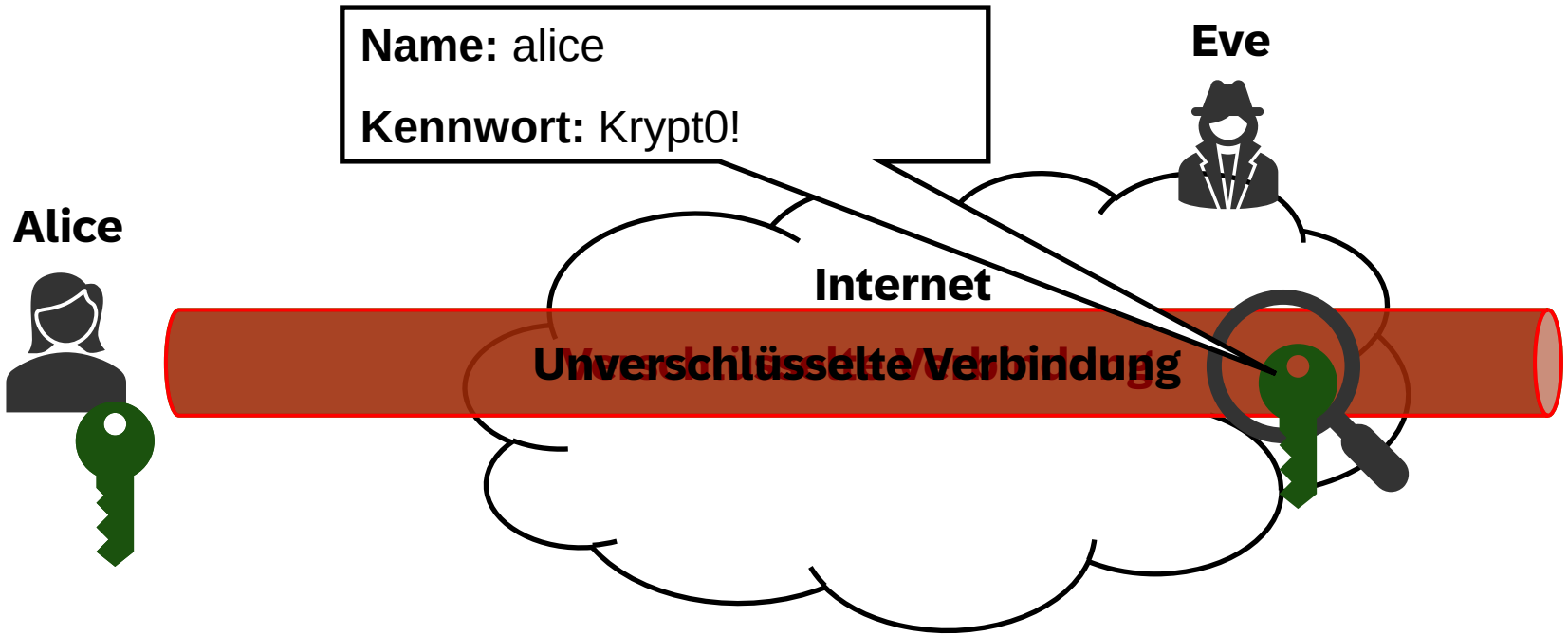


# In der Praxis sind unsere Verbindungen online (meist) verschlüsselt und sicher

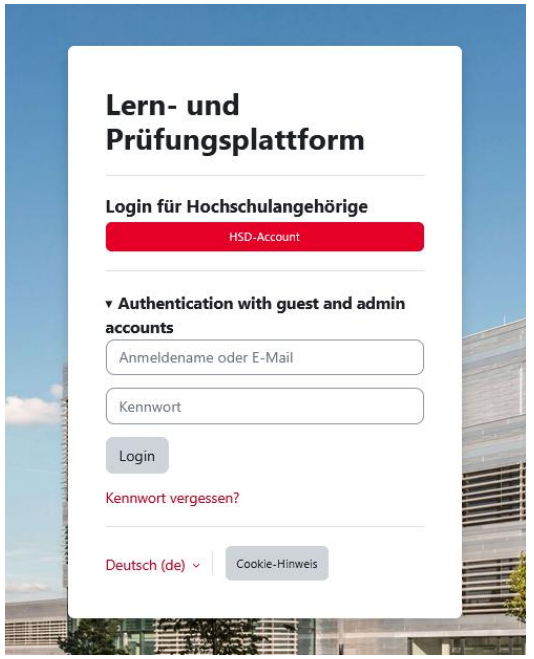



Wie können wir eine **verschlüsselte Verbindung** über das Internet aufbauen?

# Problem: Übertragung eines Schlüssels über einen unsicheren Kanal (Internet)



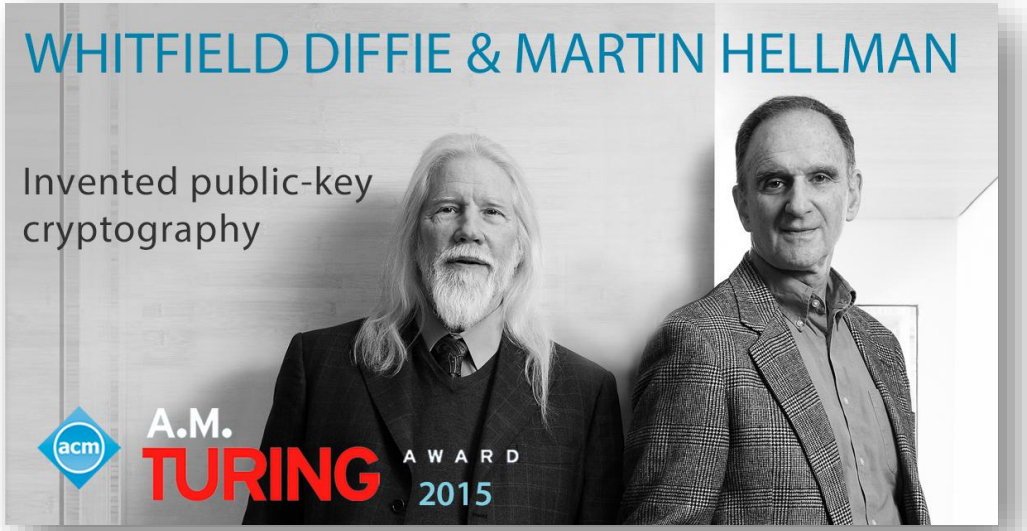

HS-Düsseldorf Website




Wie können wir eine **verschlüsselte** Verbindung über einen **unsicheren** Kanal (Internet) aufbauen?

# Wie zwei Menschen das Internet sicher machten – lange bevor es existierte [1]

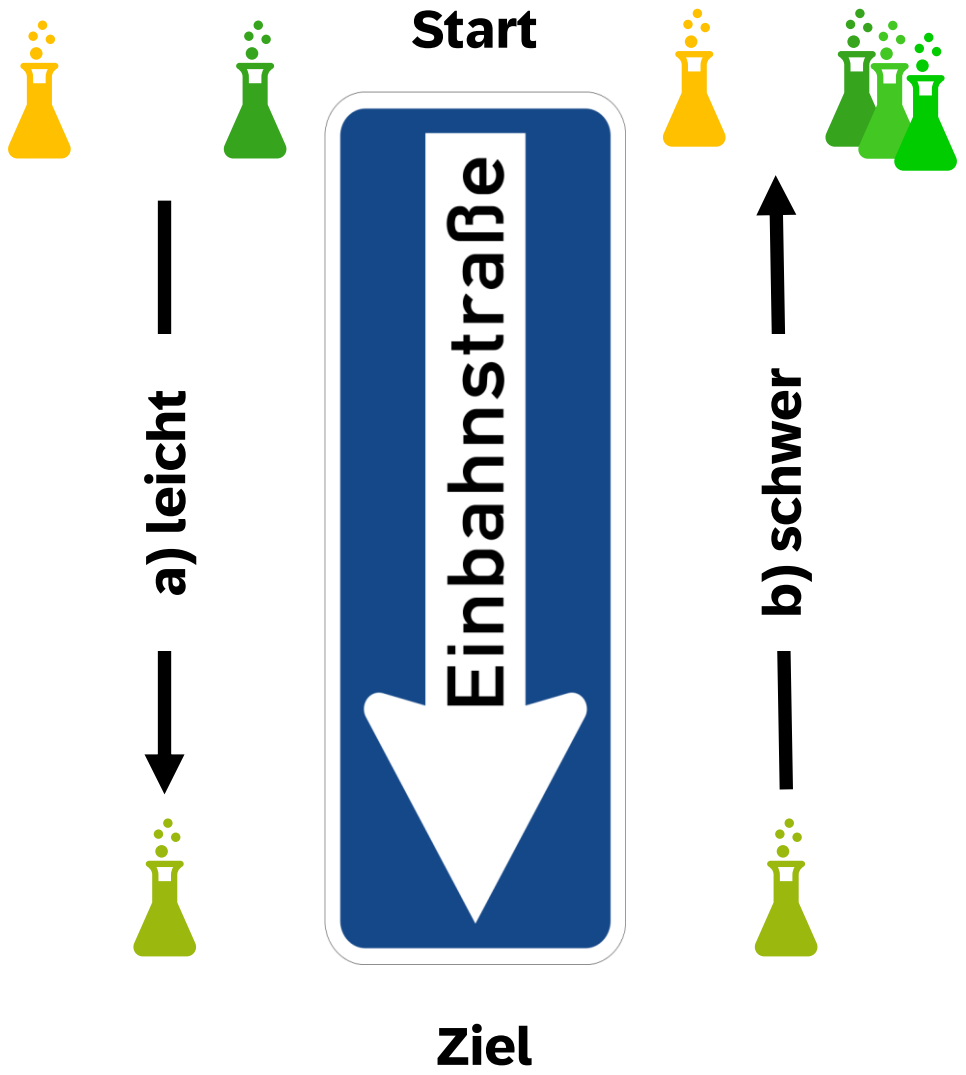
- Entwickelten 1976 das **Diffie-Hellman-Protokoll**
- Das erste **Verfahren** zum **sicheren Schlüsselaustausch** über **unsichere** Kanäle
- Legten den **Grundstein** für die **Public-Key-Kryptografie** (asymmetrische Kryptografie)




**Bildquelle:** © ACM Turing Award 2015, www.acm.org

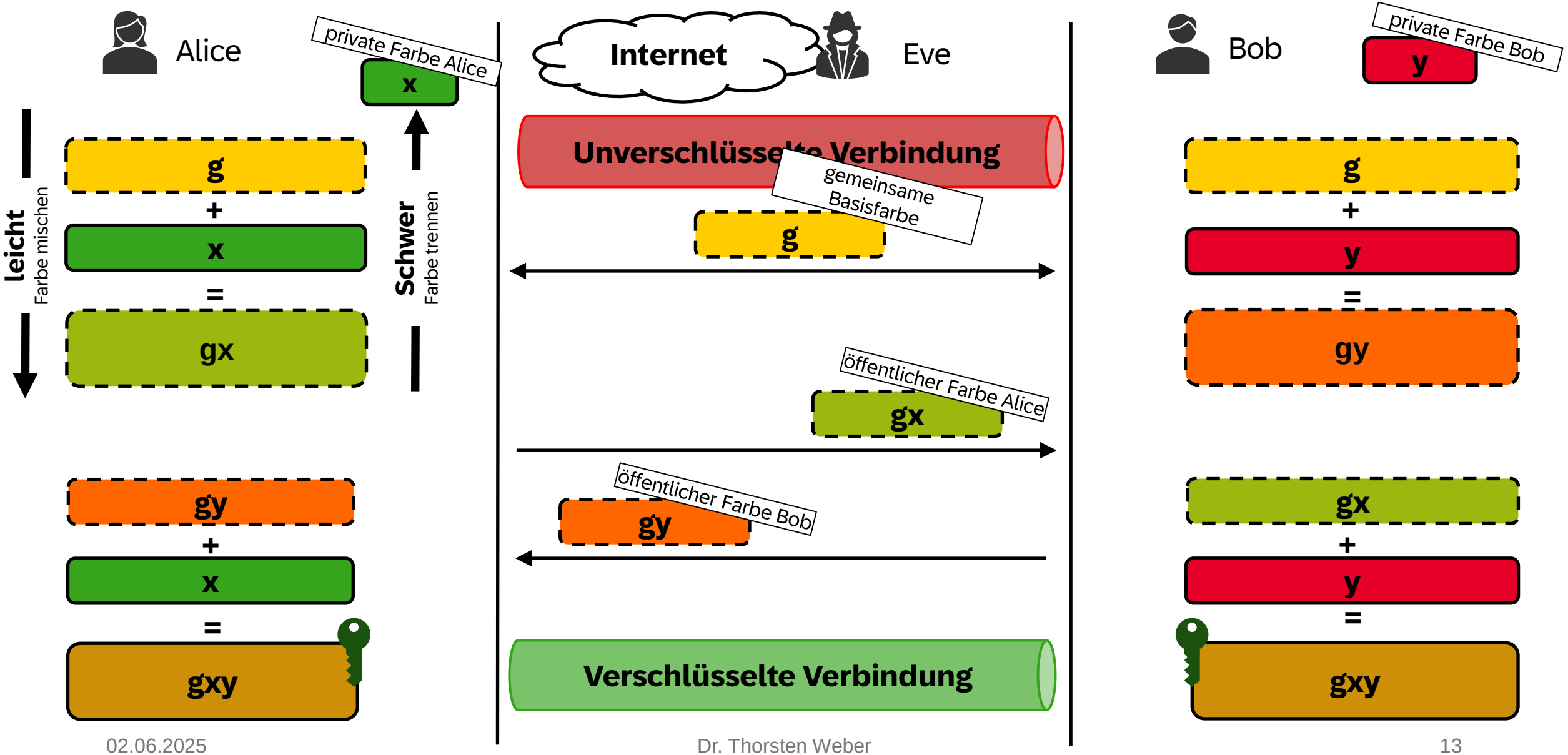
# Grundidee des Diffie-Hellman-Schlüsselaustausch – Die Einwegfunktion [2]

- Der Diffie-Hellman-Schlüsselaustausch basiert auf einer sogenannten **Einwegfunktion**
- Einer **Rechenregel:**
  a) die sich **leicht anwenden** lässt,
  b) aber nur **extrem schwer rückgängig** gemacht werden kann.



# 2 Diffie-Hellman-Schlüsselaustausch mit Farben

# Diffie-Hellman-Schlüsselaustausch mit Farben: Gemeinsame geheime Farbe



# 3 Diffie-Hellman-Schlüsselaustausch mit Zahlen

# Wiederholung: Modulo [3]

*„Was bleibt übrig, wenn ich eine Zahl durch eine andere teile?“*

$a \ mod \ n = r$ *bedeutet: Rest* $r$ *bei* $a \div n$

**Beispiel: 15 mod 12**

Welcher **ganzzahlige Rest** bleibt bei der Division von **12** durch **15**?

**Antwort:**

1 Rest 3

15 mod 12 = 3

- BMI 14: Formale Modelle und Algorithmen
- BMI 18: Mathematik 3

# Diskrete Exponentialfunktion (modulares Potenzieren)

*„Ich nehme eine Basis g, potenziere sie x mal, und schaue: Was kommt dabei modulo einer festen Zahl p heraus?“*

*Formal:* $\mathbf{g^x \bmod p = y}$

**Beispiel:** $\mathbf{3^4 \bmod 11 = y}$

**Antwort:**

$$3^4 \; mod \; 11 = 81 \; mod \; 11$$

$$81 \; mod \; 11 = 4$$

**Fazit:**

Diskrete Exponentialfunktion kann **einfach berechnet** werden

# Diskreter Logarithmus (modulo Logarithmus)

*„Wie oft muss ich eine Zahl g modulo einer Zahl p mit sich selbst multiplizieren x, um auf eine andere Zahl y zu kommen?“*

*Formal:* $\log_g(y) \bmod p = x$

**Beispiel:** $log_3(5) \bmod 7$

**Antwort:**

Hierfür ist **kein effizienter Algorithmus** bekannt [2]

$3^1 = 3 \bmod 7 = 3$ ✗
$3^2 = 9 \bmod 7 = 2$ ✗
$3^3 = 27 \bmod 7 = 6$ ✗
$3^4 = 81 \bmod 7 = 4$ ✗
$3^5 = 243 \bmod 7 = \mathbf{5}$ ✓

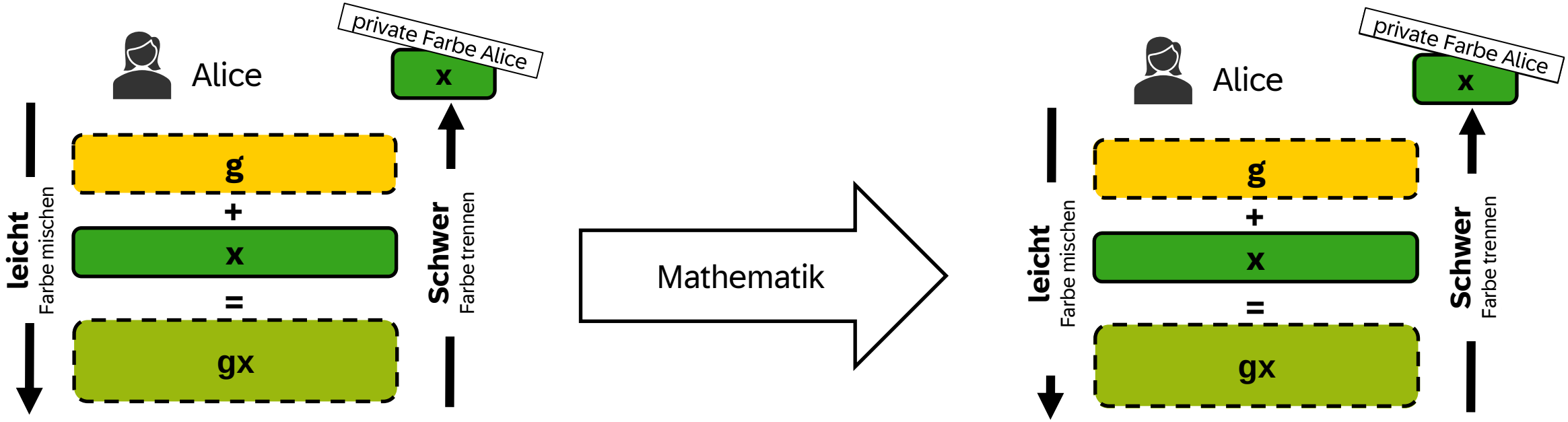
$\log_3(5) \bmod 7 = 5$

**Fazit:**

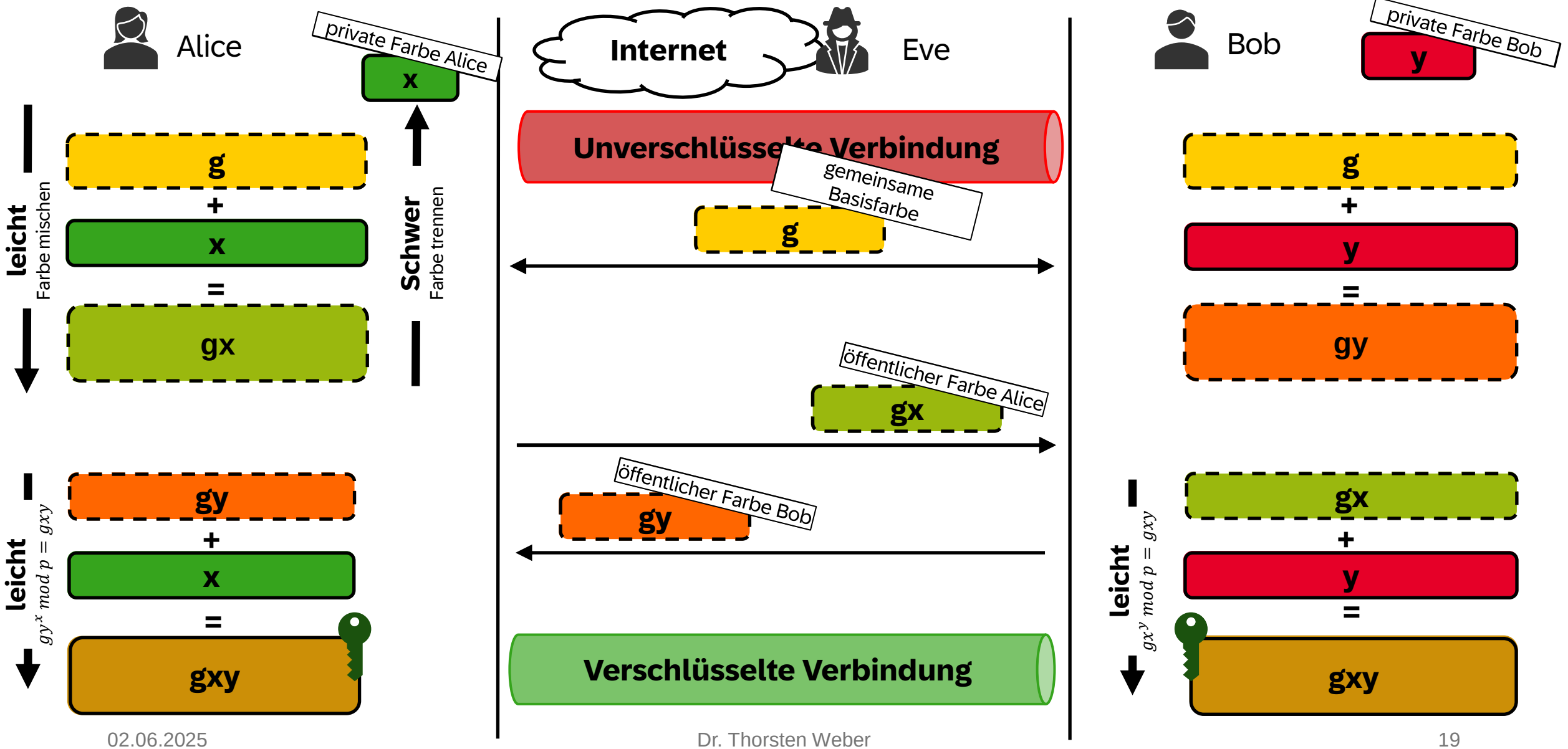
Diskreter Logarithmus kann nur **schwer berechnet** werden

# Der Weg von Farben zu Zahlen ist nicht weit

1. Der Diffie-Hellman-Schlüsselaustausch basiert auf einer sogenannten **Einwegfunktion**
2. Wir können modulo **einfach Exponentialrechnung** ausführen $g^x \; mod \; p = y$ ,
3. Wir können modulo **schwer den Logarithmus** ausführen $\log_g(y) \; mod \; p = x$.
4. Für die **Grundfarbe g** wählen wir eine **Basis g** und einen **Modulo p**
5. Die **private Farbe x** ersetzen wir durch einen **privaten Wert x**.



# Diffie-Hellman-Schlüsselaustausch mit Zahlen: Gemeinsame geheime Zahl



# 4 Sicherheit & Anwendung

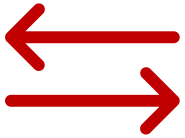
# Sicherheitsanforderungen für Diffie-Hellman-Schlüsselaustausch [2]

Die geheimen Werte **x** und **y** müssen **streng vertraulich** bleiben.

x und y sollten **mehr als 250 Bit** groß sein, p eine **große Primzahl mit über 2000 Bit**. (im Beispiel heute 5 Bit)

Das **diskrete Logarithmus-Problem** gilt als **nicht effizient – schwer – lösbar**.

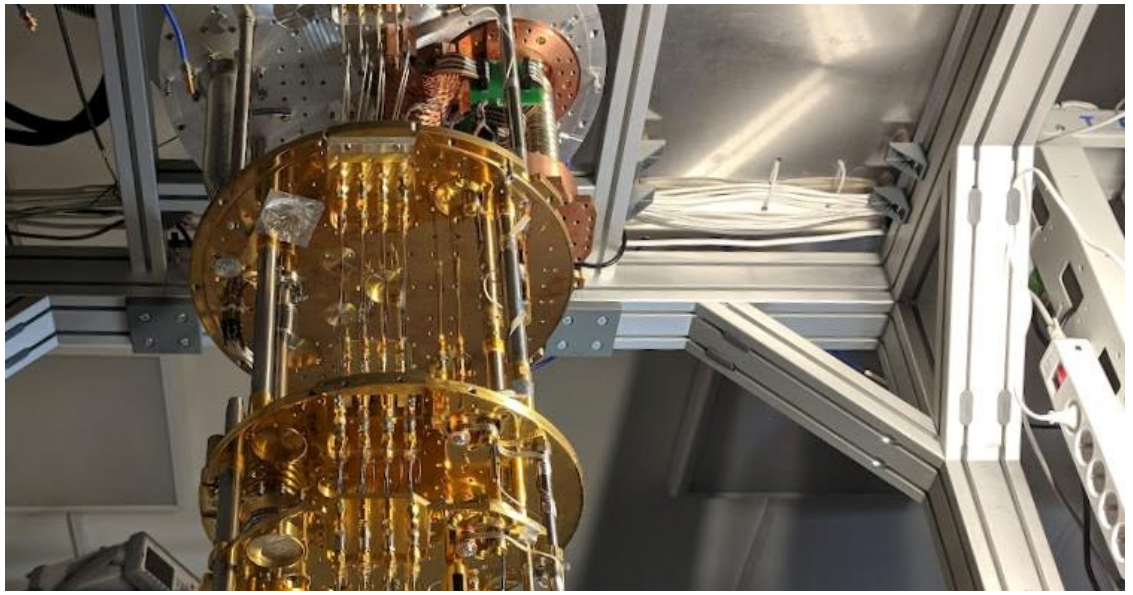
(offenes Problem der Informatik [2])



**Kommunikationspartner** (z. B. Alice & Bob) müssen vor Annahme öffentlicher Werte z. B. per **Zertifikat** verifiziert werden.

(Person-in-the-Middle Attack möglich)

# Ausblick: Was kommt nach dem Diffie-Hellman-Schlüsselaustausch [4]

**Protokolle** wie **TLS**, **IPsec** oder **Signal** nutzen Varianten von Diffie-Hellman, um **Vertraulichkeit** sicherzustellen.

Post-Quantum-Kryptographie (PQC): Auf leistungsstarken **Quantencomputern** ist das diskrete **Logarithmusproblem** effizient lösbar.

# Was Sie heute mitnehmen sollten

- **Das Problem:** Sicherer Schlüsselaustausch ist entscheidend – besonders über unsichere Kanäle wie das Internet.
- **Die Idee hinter Diffie-Hellman:** Ein gemeinsames Geheimnis wird erstellt, ohne es jemals direkt zu übertragen – mithilfe einer Einwegfunktion.
- **Die Technik:**
  - Exponentiation modulo p ist einfach zu berechnen.
  - Diskreter Logarithmus ist (klassisch) schwer umzukehren.
- **Die Praxis:** Diffie-Hellman ist Grundlage vieler Sicherheitsprotokolle (z. B. TLS, VPN, Signal).
- **Der Ausblick:** Quantencomputer bedrohen diese Verfahren – Post-Quantum-Kryptografie steht in den Startlöchern.

# 5 Live Demo

# Live Demo

Vielen Dank!

Gibt es Fragen?

https://tinyurl.com/DiffieDemo

**Dr. Thorsten Weber**
thorsten.weber88@web.de

# Quellen

[1] Interviewzitat sinngemäß wiedergegeben, Quelle: Yemen Science (https://yemenscience.net/?p=3106)

[2] Eckert, C. (2013). *IT-Sicherheit: Konzepte–Verfahren–Protokolle*. Oldenbourg Wissenschaftsverlag Verlag.

[3] Teschl, G., & Teschl, S. (2013). *Mathematik für Informatiker: Band 1: Diskrete Mathematik und Lineare Algebra*. Springer-Verlag.

[4] Föry, A. (2023). Praktische Quantenkryptographie. In Chancen und Risiken von Quantentechnologien: Praxis der zweiten Quantenrevolution für Entscheider in Wirtschaft und Politik (pp. 69-73). Wiesbaden: Springer Fachmedien Wiesbaden.