

---

# Fortgeschrittene Techniken der Kryptographie

Jürgen Fuß

Episode 4: Diffie-Hellman Revisited

HAGENBERG | LINZ | STEYR | WELS



UNIVERSITY  
OF APPLIED SCIENCES  
UPPER AUSTRIA

# Diffie-Hellman

# Diffie-Hellman-Schlüsselaustausch

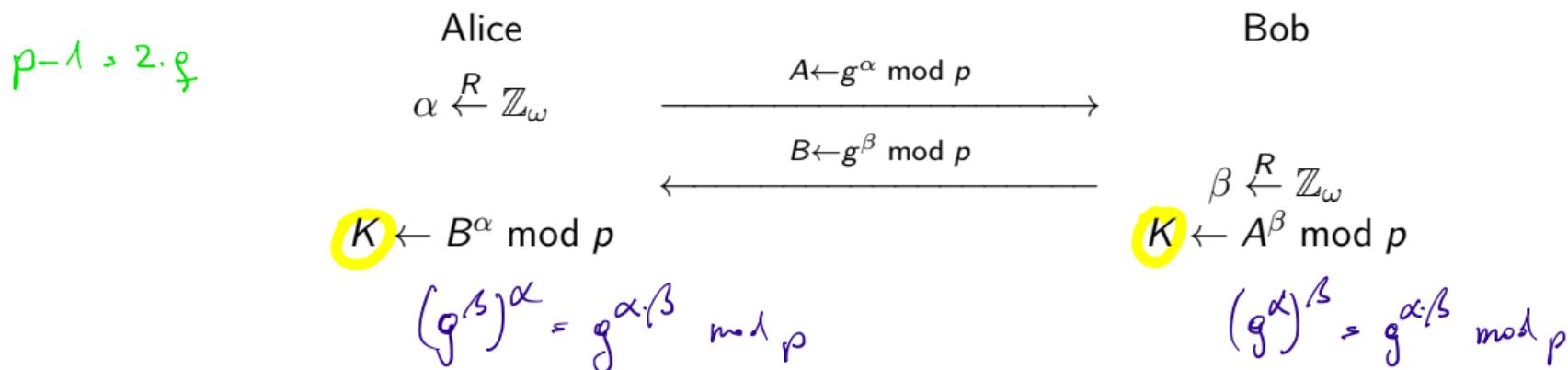
$$g^\alpha, g^\beta \xrightarrow{?} g^{\alpha\beta}, g^{\alpha+\beta}$$

$$g^\omega = 1 \pmod{p}$$

## Ephemeral Diffie-Hellman Key Agreement

Setup: Domain Parameter (öffentlich):  $p \in \mathbb{P}$ ,  $g \in \mathbb{Z}_p^*$  mit der Ordnung  $\omega$ .

Key Agreement:



Diffie-Hellman ist nur sicher, wenn das Berechnen diskreter Logarithmen schwierig ist.

- ▶ Ließe sich mit anderen „Zahlen“ anstatt mit Restklassen modulo  $p$  DH Key Agreement auch durchführen?
- ▶ Gibt es auch „Zahlen“, wo es noch schwieriger ist, diskrete Logarithmen zu berechnen?
- ▶ Wie muss das Rechnen mit diesen „Zahlen“ funktionieren, damit DH Key Agreement durchgeführt werden kann?

## Definition

Eine **Gruppe** ist ein Quadrupel  $(G, \circ, \perp, \wedge)$ , wobei  $G$  irgendeine Menge ist,  $\circ$  eine Funktion von  $G \times G$  nach  $G$ ,  $\wedge$  eine Funktion von  $G$  nach  $G$  und  $\perp \in G$ , und die folgenden Gesetze erfüllt sind:

- 1.
- 2.
- 3.

Die Funktion  $\circ$  wird auch als **Verknüpfung** oder **Gruppenoperation** bezeichnet.

## Definition

Eine **Gruppe** ist ein Quadrupel  $(\mathbb{G}, \circ, \perp, \wedge)$ , wobei  $\mathbb{G}$  irgendeine Menge ist,  $\circ$  eine Funktion von  $\mathbb{G} \times \mathbb{G}$  nach  $\mathbb{G}$ ,  $\wedge$  eine Funktion von  $\mathbb{G}$  nach  $\mathbb{G}$  und  $\perp \in \mathbb{G}$ , und die folgenden Gesetze erfüllt sind:

- 1.
- 2.
3. Für jedes  $a \in \mathbb{G}$  gilt:  $\perp \circ a = a$  und  $a \circ \perp = a$ .

Die Funktion  $\circ$  wird auch als **Verknüpfung** oder **Gruppenoperation** bezeichnet. Das Element  $\perp$  der Gruppe wird ihr **neutrales Element** genannt.

## Definition

Eine **Gruppe** ist ein Quadrupel  $(\mathbb{G}, \circ, \perp, \hat{\circ})$ , wobei  $\mathbb{G}$  irgendeine Menge ist,  $\circ$  eine Funktion von  $\mathbb{G} \times \mathbb{G}$  nach  $\mathbb{G}$ ,  $\hat{\circ}$  eine Funktion von  $\mathbb{G}$  nach  $\mathbb{G}$  und  $\perp \in \mathbb{G}$ , und die folgenden Gesetze erfüllt sind:

- 1.
2. Für jedes  $a \in \mathbb{G}$  gilt:  $a \circ \hat{a} = \perp$  und  $\hat{a} \circ a = \perp$ .
3. Für jedes  $a \in \mathbb{G}$  gilt:  $\perp \circ a = a$  und  $a \circ \perp = a$ .

Die Funktion  $\circ$  wird auch als **Verknüpfung** oder **Gruppenoperation** bezeichnet. Das Element  $\perp$  der Gruppe wird ihr **neutrales Element** genannt. Das Element  $\hat{a}$  heißt **inverses Element** von  $a$ .

## Definition

Eine **Gruppe** ist ein Quadrupel  $(\mathbb{G}, \circ, \perp, \hat{\phantom{a}})$ , wobei  $\mathbb{G}$  irgendeine Menge ist,  $\circ$  eine Funktion von  $\mathbb{G} \times \mathbb{G}$  nach  $\mathbb{G}$ ,  $\hat{\phantom{a}}$  eine Funktion von  $\mathbb{G}$  nach  $\mathbb{G}$  und  $\perp \in \mathbb{G}$ , und die folgenden Gesetze erfüllt sind:

1. Für alle  $a, b, c \in \mathbb{G}$  gilt:  $(a \circ b) \circ c = a \circ (b \circ c)$ .
2. Für jedes  $a \in \mathbb{G}$  gilt:  $a \circ \hat{a} = \perp$  und  $\hat{a} \circ a = \perp$ .
3. Für jedes  $a \in \mathbb{G}$  gilt:  $\perp \circ a = a$  und  $a \circ \perp = a$ .

Die Funktion  $\circ$  wird auch als **Verknüpfung** oder **Gruppenoperation** bezeichnet. Das Element  $\perp$  der Gruppe wird ihr **neutrales Element** genannt. Das Element  $\hat{a}$  heißt **inverses Element** von  $a$ .

## Definition

Eine **Gruppe** ist ein Quadrupel  $(\mathbb{G}, \circ, \perp, \hat{\phantom{a}})$ , wobei  $\mathbb{G}$  irgendeine Menge ist,  $\circ$  eine Funktion von  $\mathbb{G} \times \mathbb{G}$  nach  $\mathbb{G}$ ,  $\hat{\phantom{a}}$  eine Funktion von  $\mathbb{G}$  nach  $\mathbb{G}$  und  $\perp \in \mathbb{G}$ , und die folgenden Gesetze erfüllt sind:

1. Für alle  $a, b, c \in \mathbb{G}$  gilt:  $(a \circ b) \circ c = a \circ (b \circ c)$ .
2. Für jedes  $a \in \mathbb{G}$  gilt:  $a \circ \hat{a} = \perp$  und  $\hat{a} \circ a = \perp$ .
3. Für jedes  $a \in \mathbb{G}$  gilt:  $\perp \circ a = a$  und  $a \circ \perp = a$ .

Die Funktion  $\circ$  wird auch als **Verknüpfung** oder **Gruppenoperation** bezeichnet. Das Element  $\perp$  der Gruppe wird ihr **neutrales Element** genannt. Das Element  $\hat{a}$  heißt **inverses Element** von  $a$ .

Gilt außerdem  $a \circ b = b \circ a$  für alle  $a, b \in \mathbb{G}$ , so heißt  $(\mathbb{G}, \circ, \perp, \hat{\phantom{a}})$  **abelsche Gruppe**.

Bsp.  $G = \mathbb{Z}$

$$\underline{a \circ b = a + b}$$

$(\mathbb{Z}, +, 0, -)$  Gruppe

1.  $(a+b)+c \stackrel{?}{=} a+(b+c) \quad \checkmark$

$$1 = 0$$

3.  $0+a = a+0 = a \quad \checkmark$

$$\hat{a} = -a$$

$$\hat{3} = -3$$

$$\hat{-5} = 5$$

2.  $a + (-a) = (-a) + a = 0 \quad \checkmark$

Bsp.  $G = \mathbb{R}$

$$a \circ b = \frac{a+b}{2}$$

Reine Gruppe

1.  $\underline{(a \circ b) \circ c} = a \circ (b \circ c)$

$$\frac{a+b}{2} \circ c = a \circ \frac{b+c}{2}$$

$$\frac{\frac{a+b}{2} + c}{2} = a + \frac{b+c}{2}$$

$$\frac{a+b}{4} + \frac{c}{2} = \frac{a}{2} + \frac{b+c}{4}$$

$$\frac{a}{4} + \frac{b}{4} + \frac{c}{2} \neq \frac{a}{2} + \frac{b}{4} + \frac{c}{4}$$

Bsp.  $G = \mathbb{Z}$

$$a \circ b = a - b$$

Reine Gruppe

1.  $(a - b) - c = a - (b - c)$

$$a - b - c \neq a - b + c$$

Bsp.  $G = \mathbb{R} \setminus \{0\}$

$$a \circ b = a \cdot b$$

$$1. (a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \checkmark$$

$$\underline{1} = 1$$

$$2. 1 \cdot a = a \cdot 1 = a \quad \checkmark$$

$$\hat{a}^{-1} = \left[ \begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix} \right]$$

$$\lambda: G \rightarrow G$$

keine Gruppe

$$\hat{1} = \frac{1}{2} \notin \mathbb{Z}$$

Gruppe

$$3. 1 = \underbrace{\hat{2} \cdot 2}_{1 \cdot 2}$$

Bsp.  $G = \{ A \in \mathbb{R}^{2 \times 2} \mid A \text{ ist invertierbar} \}$

$$a \circ b = a \cdot b$$

$$(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$$

nicht abelsche  
Gruppe

$$1. (A \cdot B) \cdot C = A \cdot (B \cdot C) \quad \checkmark$$

$$\perp = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E_2$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 2 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & -2 \end{pmatrix}$$

$$2. E_2 \cdot A = A \cdot E_2 = A$$

$$\overset{\wedge}{A} = A^{-1}$$

$$3. A \cdot A^{-1} = A^{-1} \cdot A = E_2$$

Bsp.

$$G = \mathbb{Z}_5^* \times \mathbb{Z}_7^* \leftarrow \perp = (1, 1)$$
$$(a_1, b_1) \circ (a_2, b_2) = (a_1 \cdot b_1, a_2 \cdot b_2)$$

$a_1, b_1 \in \mathbb{Z}_5^*$     $a_2, b_2 \in \mathbb{Z}_7^*$     $\mod 5$     $\mod 7$

Gruppe

1. ✓

$$\perp = ([1], [1])$$

2. ✓

$$(a_1, a_2) = (\widehat{a_1}, \widehat{a_2})$$

$\uparrow$   
 $\text{Kw mod } 5$

Kw mod 7

$$(1, 1)^1 = (1, 1)$$

$$(3, 1)^1 = (3, 1)$$

$$(3, 1)^2 = (3, 1) \circ (3, 1)$$

$$= (3 \cdot 3, 1 \cdot 1)$$

$$= (4, 1)$$

$$(3, 1)^3 = (3, 1)^2 \circ (3, 1) =$$

$$(4, 1) \circ (3, 1)$$

$$(4 \cdot 3, 1 \cdot 1) = (2, 1)$$

Kw mod 7

$$(3, 1)^4 = (3, 1)^3 \circ (3, 1)$$

$$(2, 1) \circ (3, 1)$$

$$(2 \cdot 3, 1 \cdot 1)$$

$$(1, 1)$$

# Wozu $(a \circ b) \circ c = a \circ (b \circ c)$ ?

Für Square & Multiply erwartet man sich beispielsweise, dass sich  $x^4 = ((x \circ x) \circ x) \circ x$  auch als  $(x^2)^2 = (x \circ x) \circ (x \circ x)$  berechnen lässt (was sich mit einer Verknüpfung weniger erledigen lässt). Dies klappt, denn

$$x^4 = \underbrace{((x \circ x) \circ x) \circ x}_{(a \circ b) \circ c} = \underbrace{(x \circ x) \circ (x \circ x)}_{a \circ (b \circ c)} = (x^2)^2$$

Dieser Trick lässt sich jedoch nur anwenden, wenn die Klammern auch anders gesetzt werden dürfen, ohne das Ergebnis zu beeinflussen. Umgekehrt reicht diese Eigenschaft aber aus, dass alle möglichen Potenzen beliebig – also auch mit Square & Multiply – berechnet werden können.

## Definition

Besitzt eine Gruppe unendlich viele Elemente (wie z.B.  $(\mathbb{Z}, +, 0, -)$ ), so nennen wir sie eine unendliche Gruppe. Andernfalls heißt die Gruppe **endlich**. Bspw. ist  $(\mathbb{Z}_p^*, \cdot, 1, -1)$  endlich.

Ist  $(G, \circ, \perp, \wedge)$  eine endliche Gruppe, so bezeichnen wir mit  $|G|$  die Anzahl der Elemente der Gruppe und nennen  $|G|$  die **Ordnung von G**.

# Ordnung eines Elements einer Gruppe

## Definition

Ist  $g$  ein Element der Gruppe  $(\mathbb{G}, \circ, \perp, \wedge)$  und  $\alpha \in \mathbb{N}$ , so schreiben wir

$g^\alpha$  statt  $\underbrace{g \circ g \circ \cdots \circ g}_{\alpha \text{ mal}},$

$g^{-\alpha}$  statt  $\underbrace{\hat{g} \circ \hat{g} \circ \cdots \circ \hat{g}}_{\alpha \text{ mal}}$  (insbes.  $\hat{g} = g^{-1}$ ) und definieren

$$g^0 := \perp$$

Die kleinste natürliche Zahl  $\omega$ , so dass  $g^\omega = \perp$ , heißt (sofern es so eine Zahl gibt) die **Ordnung von  $g$**  und wird mit  $\text{ord}(g)$  bezeichnet. Gibt es keine solche Zahl, so sagen wir, die Ordnung von  $g$  ist unendlich.

```
> import si
> si.multiplicative_order(4,197)
98
> pow( 4, 98, 197 )
1
> [ pow(4,i,197) for i in range(99) ]
[1, 4, 16, 64, 59, 39, 156, 33, 132, 134, 142, 174, 105, 26, 104, 22,
88, 155, 29, 116, 70, 83, 135, 146, 190, 169, 85, 143, 178, 121,
90, 163, 61, 47, 188, 161, 53, 15, 60, 43, 172, 97, 191, 173, 101,
10, 40, 160, 49, 196, 193, 181, 133, 138, 158, 41, 164, 65, 63,
55, 23, 92, 171, 93, 175, 109, 42, 168, 81, 127, 114, 62, 51, 7,
28, 112, 54, 19, 76, 107, 34, 136, 150, 9, 36, 144, 182, 137,
154, 25, 100, 6, 24, 96, 187, 157, 37, 148, 1]
```