



7 Hashing

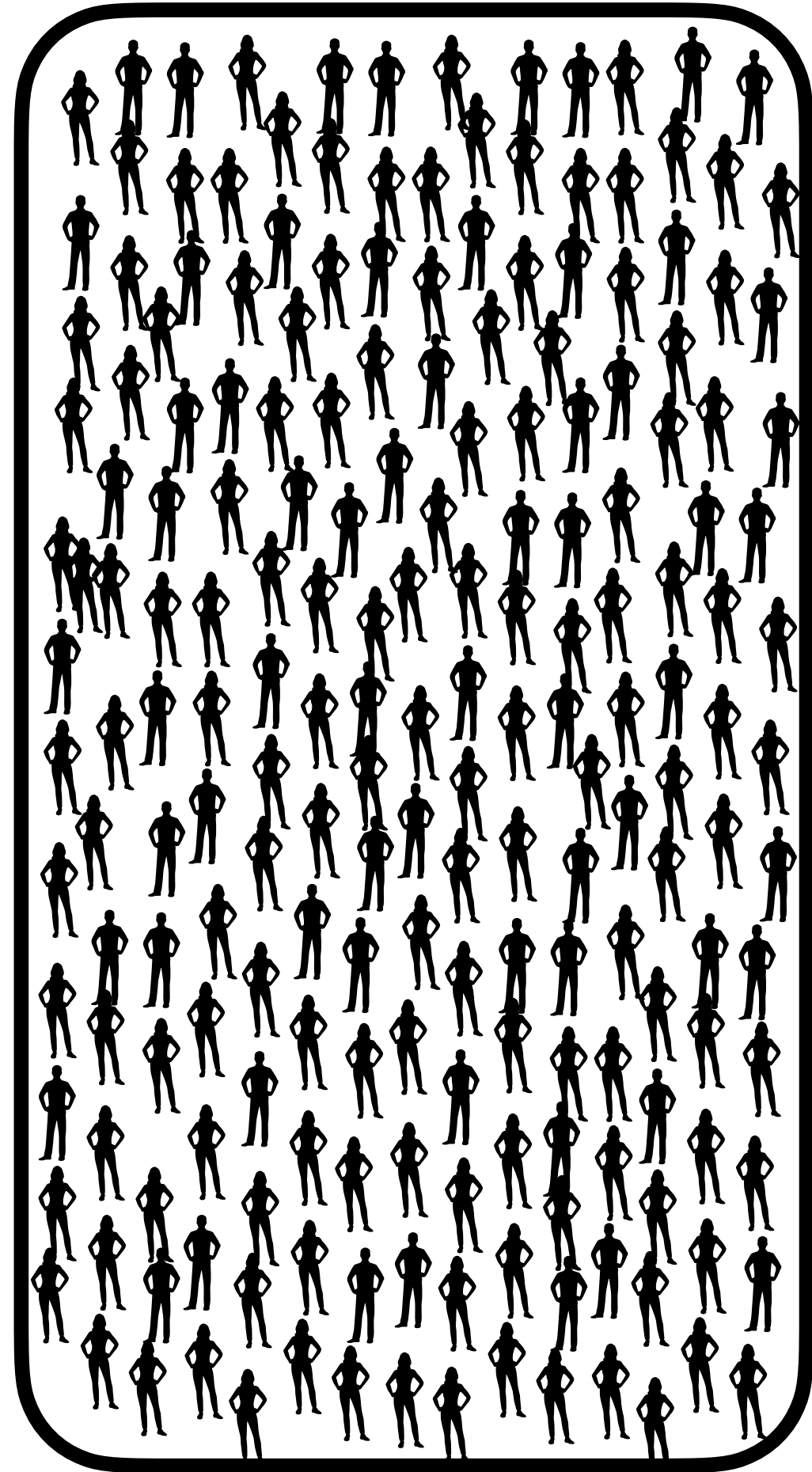
*Algorithmen und Datenstrukturen 2
Sommer 2021*

Prof. Dr. Sándor Fekete

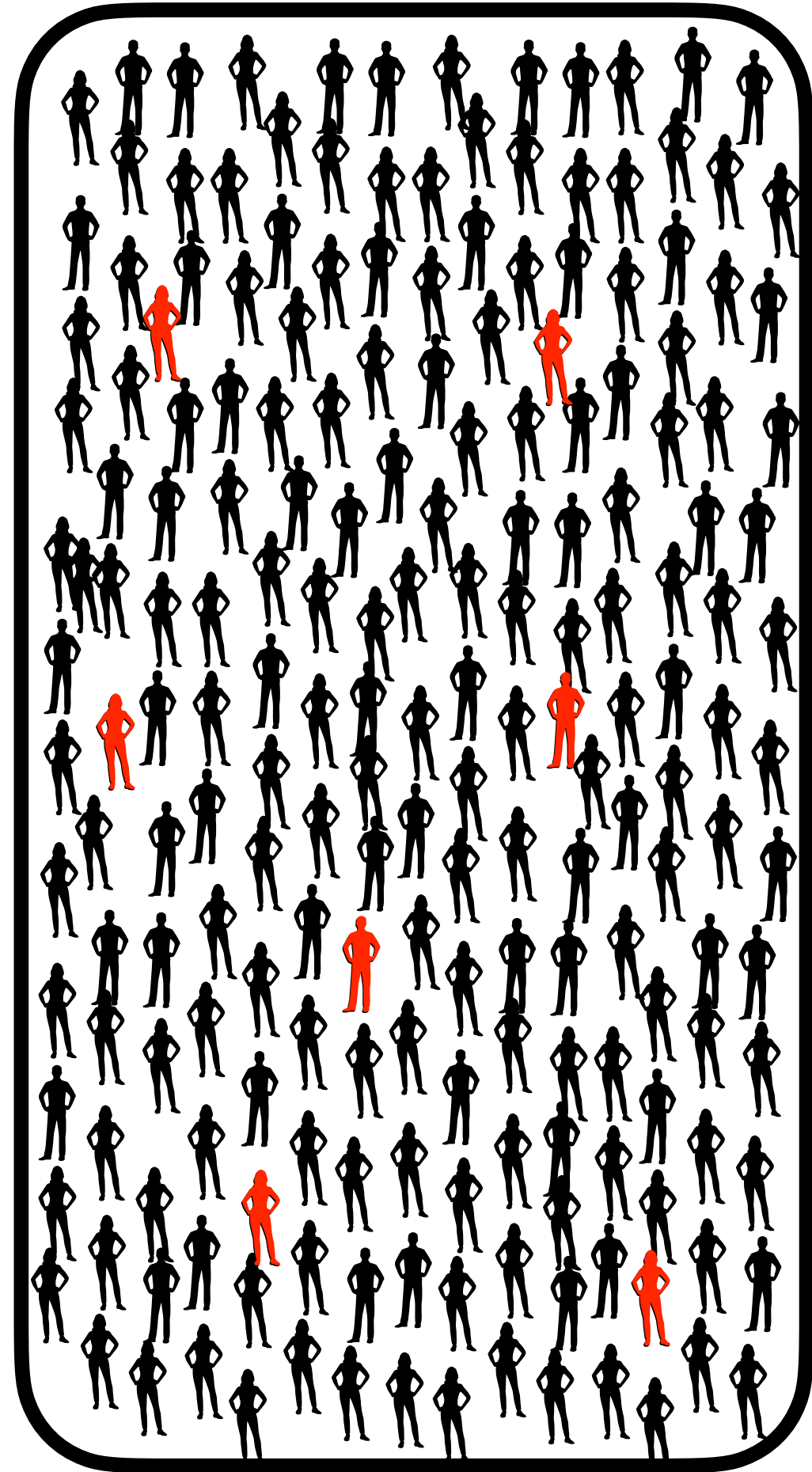
7.1 Motivation

Aufgabenstellung

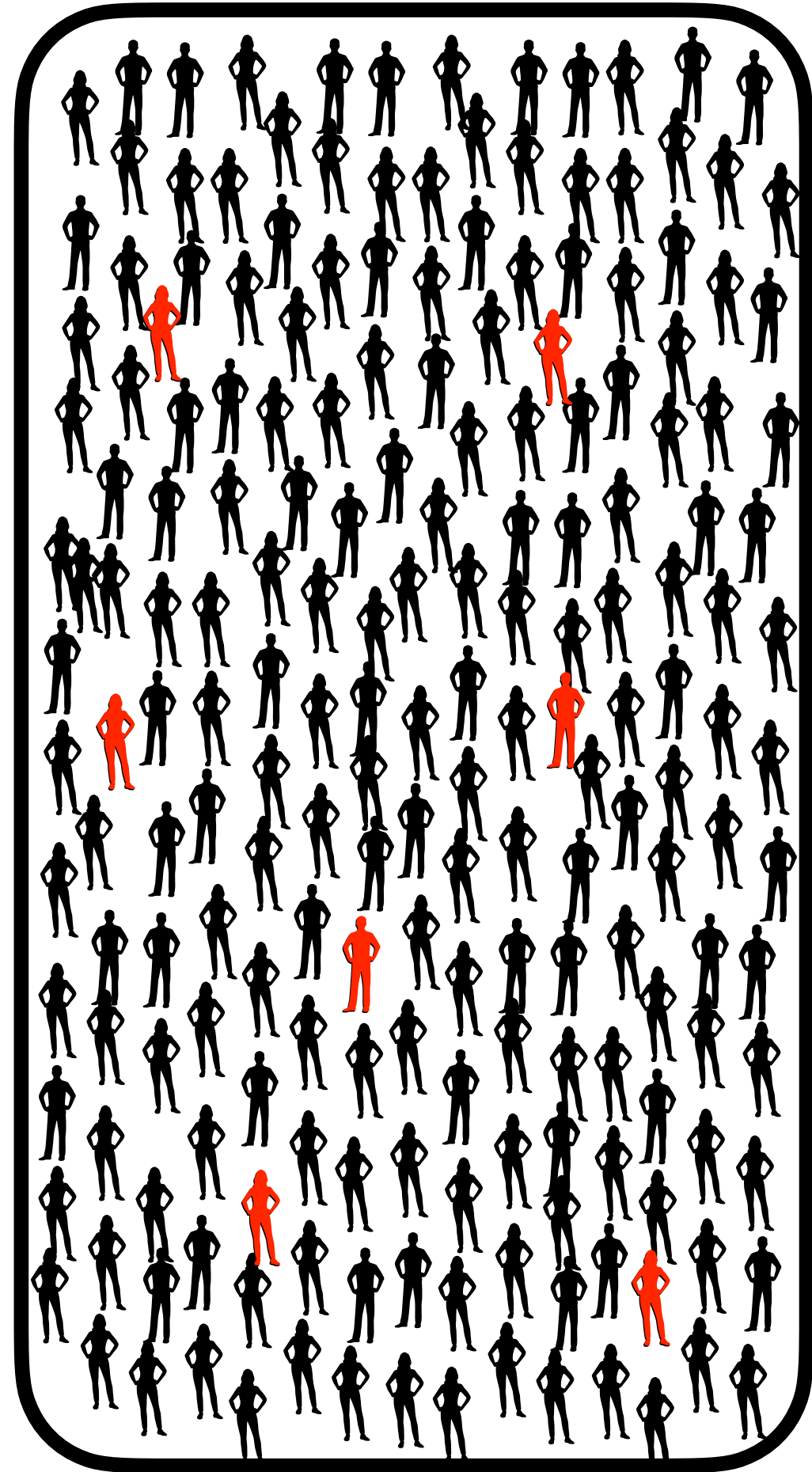
Aufgabenstellung



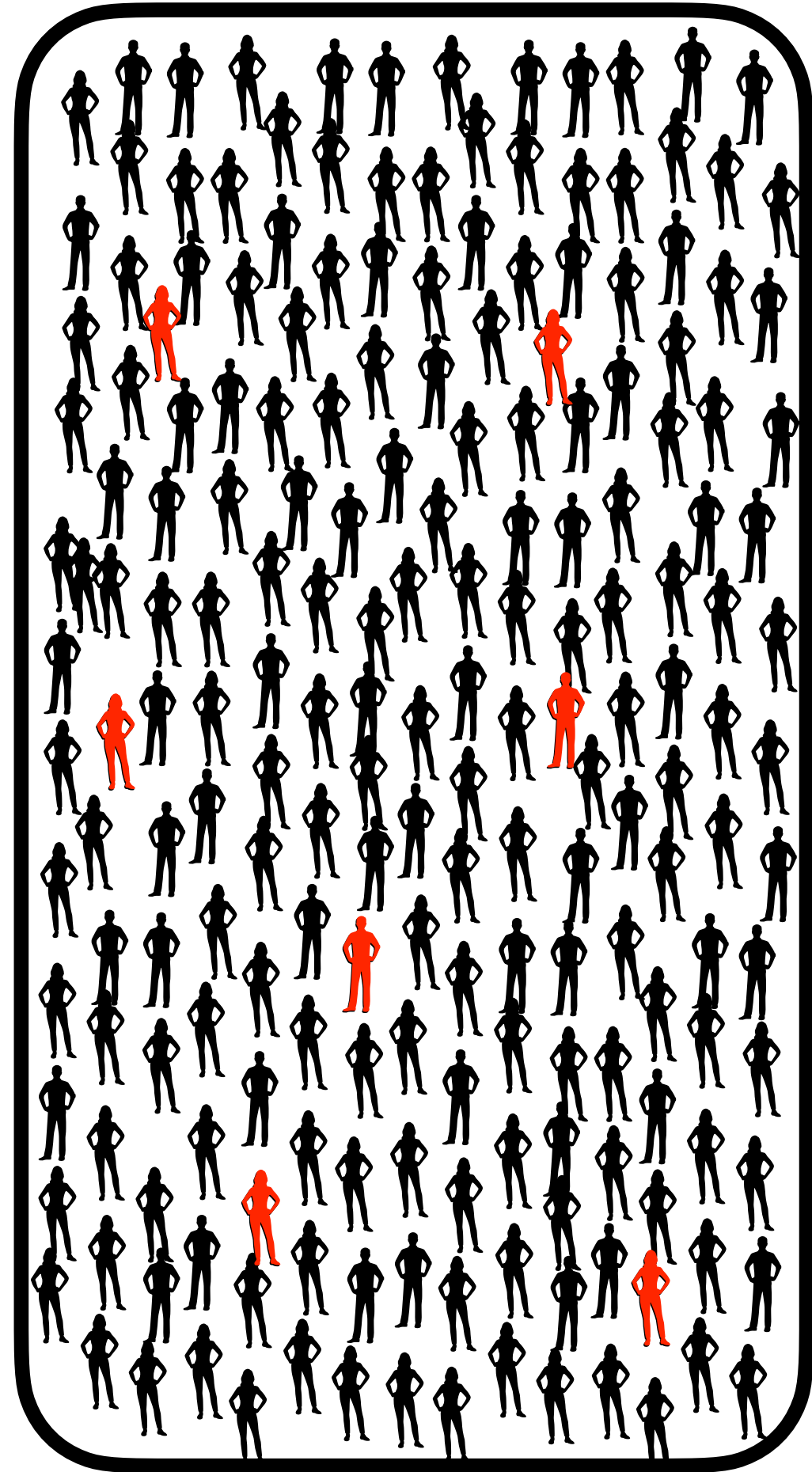
Aufgabenstellung



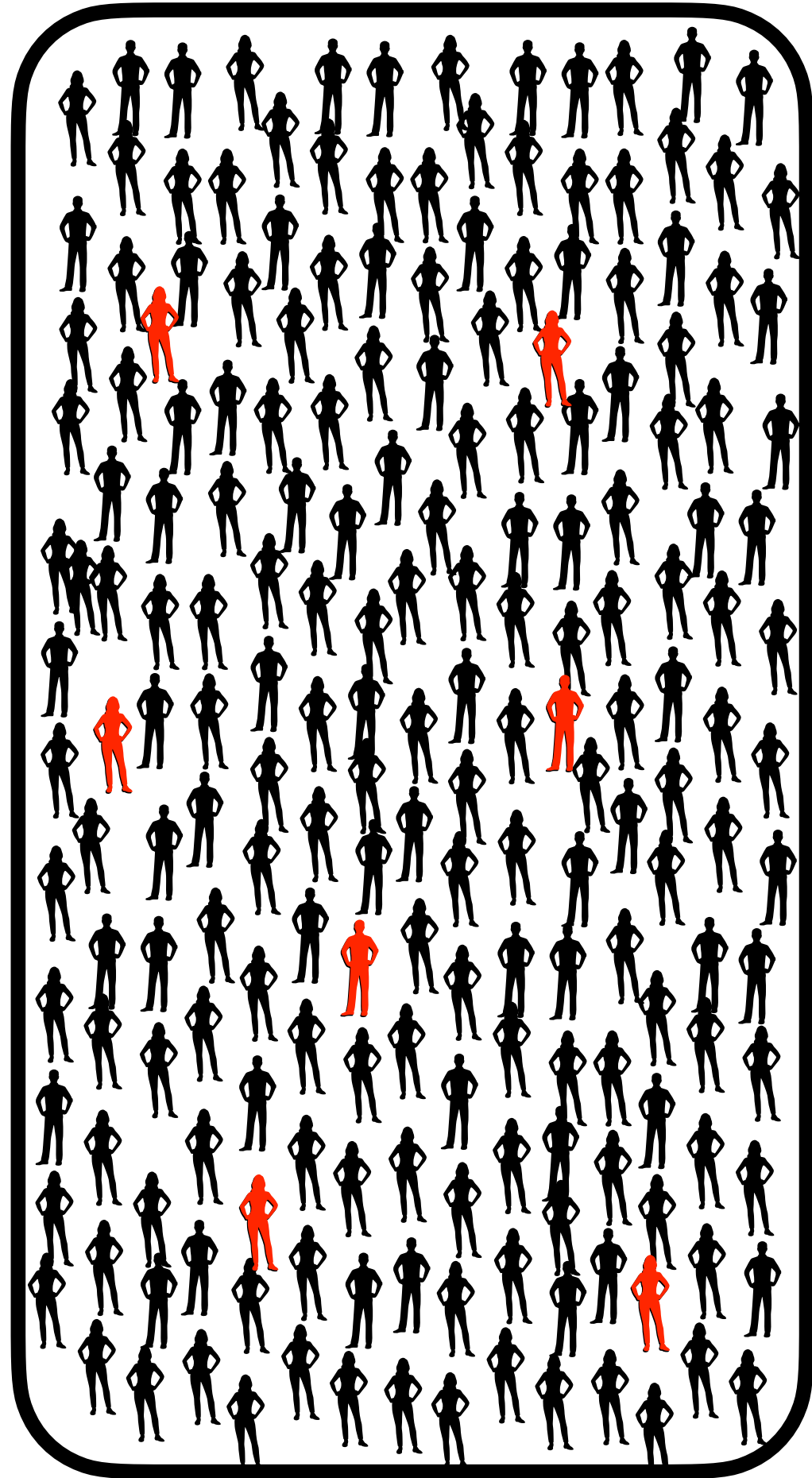
Aufgabenstellung



Aufgabenstellung



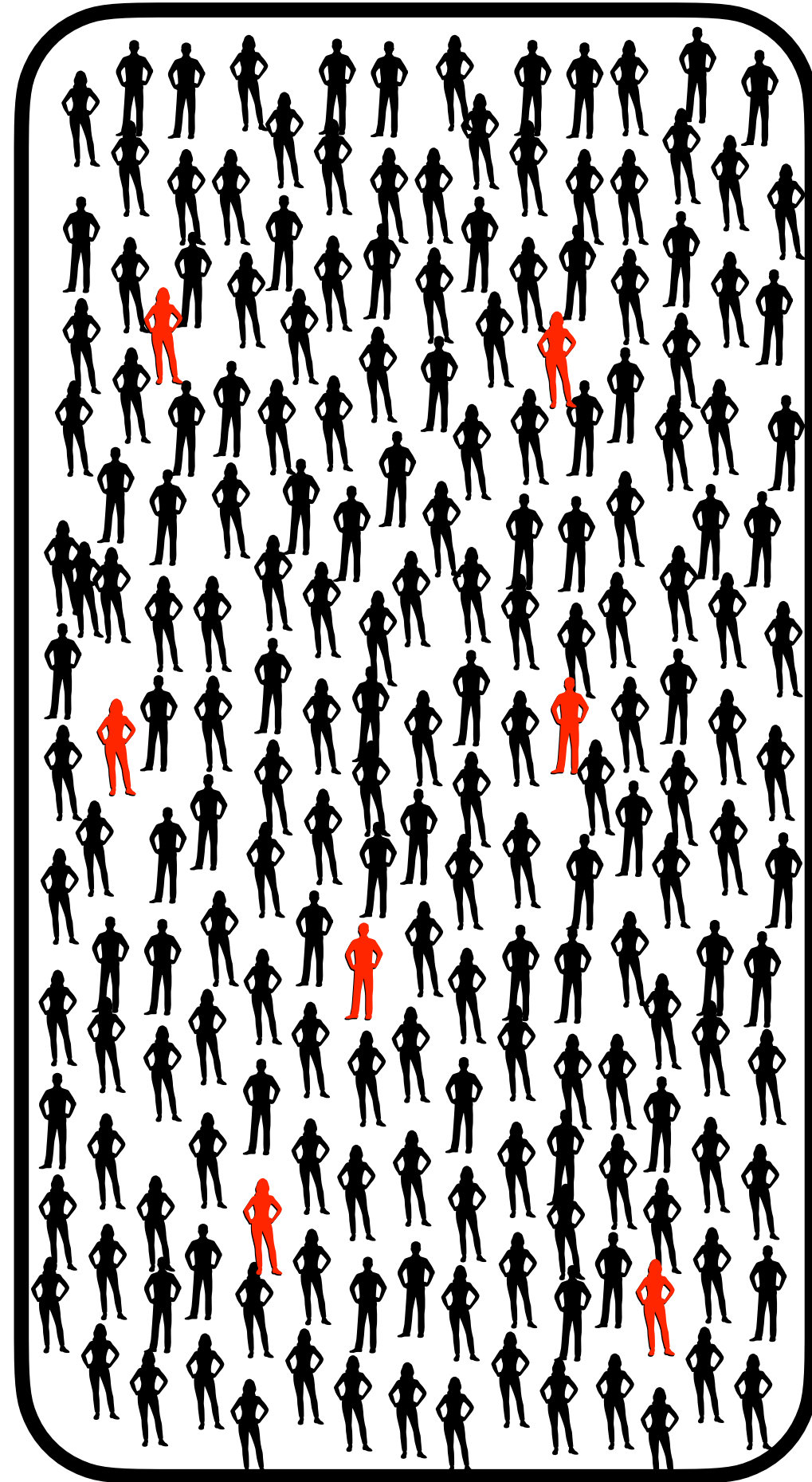
Aufgabenstellung



Hashing

A large, empty rectangular area with a light blue background, intended for writing or drawing. It is framed by a dark blue header containing the word "Hashing".

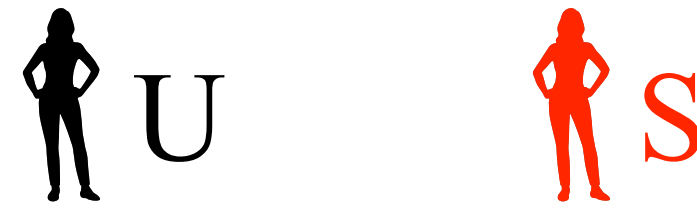
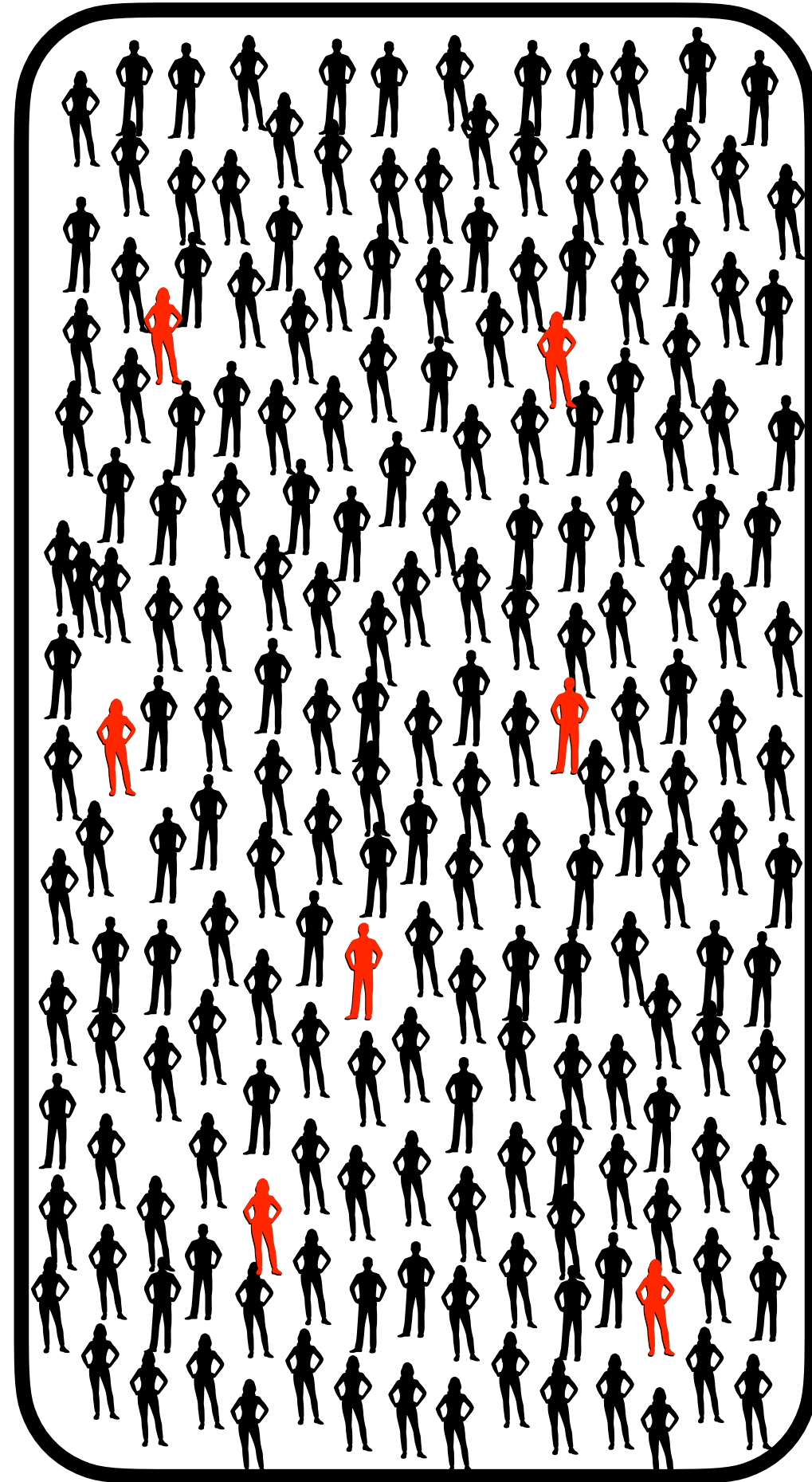
Aufgabenstellung



Hashing

- Menge U potentieller Schlüssel sehr groß,

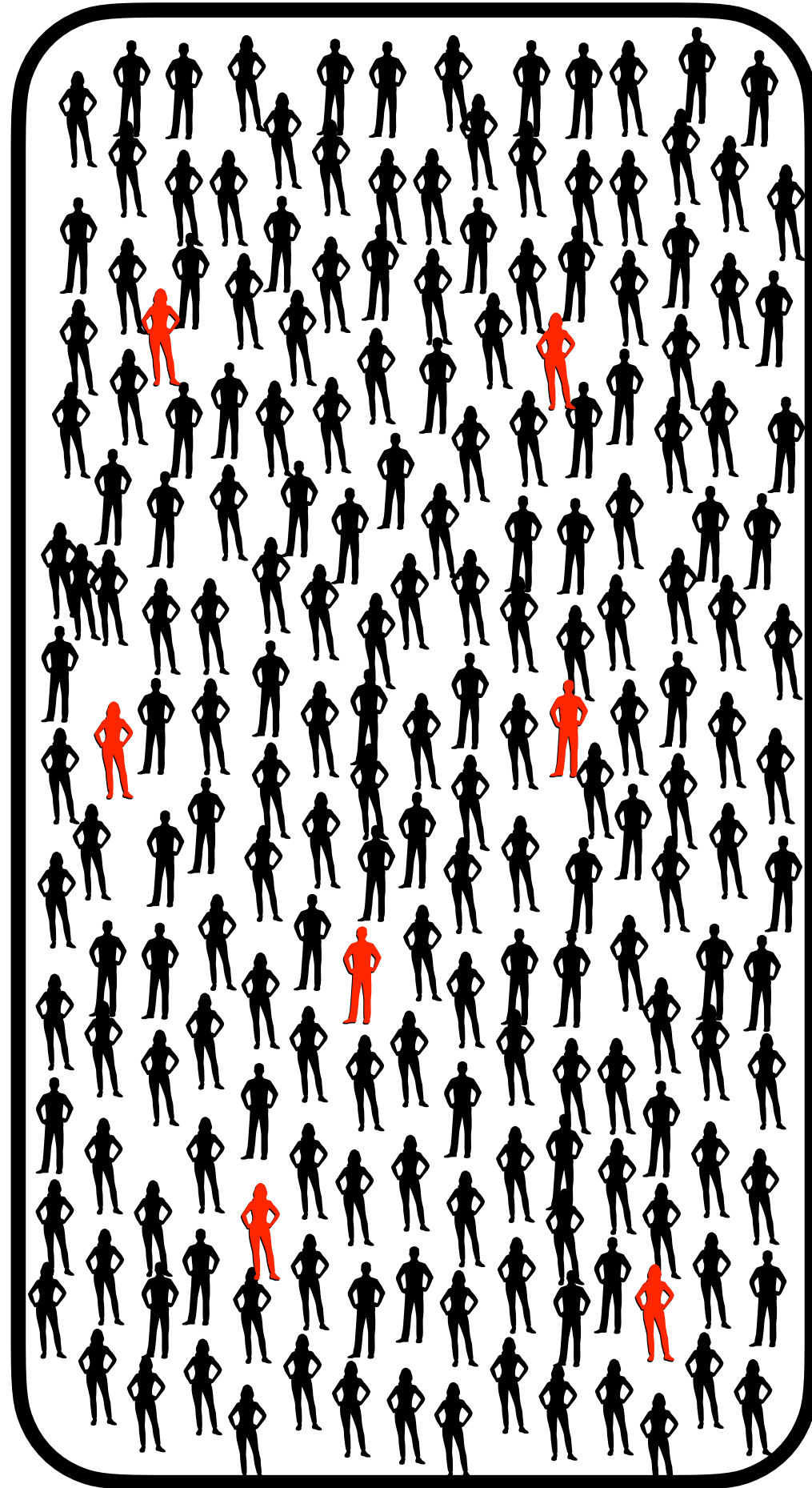
Aufgabenstellung



Hashing

- Menge U potentieller Schlüssel sehr groß, aktuelle Schlüsselmenge S jeweils nur kleine Teilmenge des Universums (im allgemeinen S nicht bekannt)

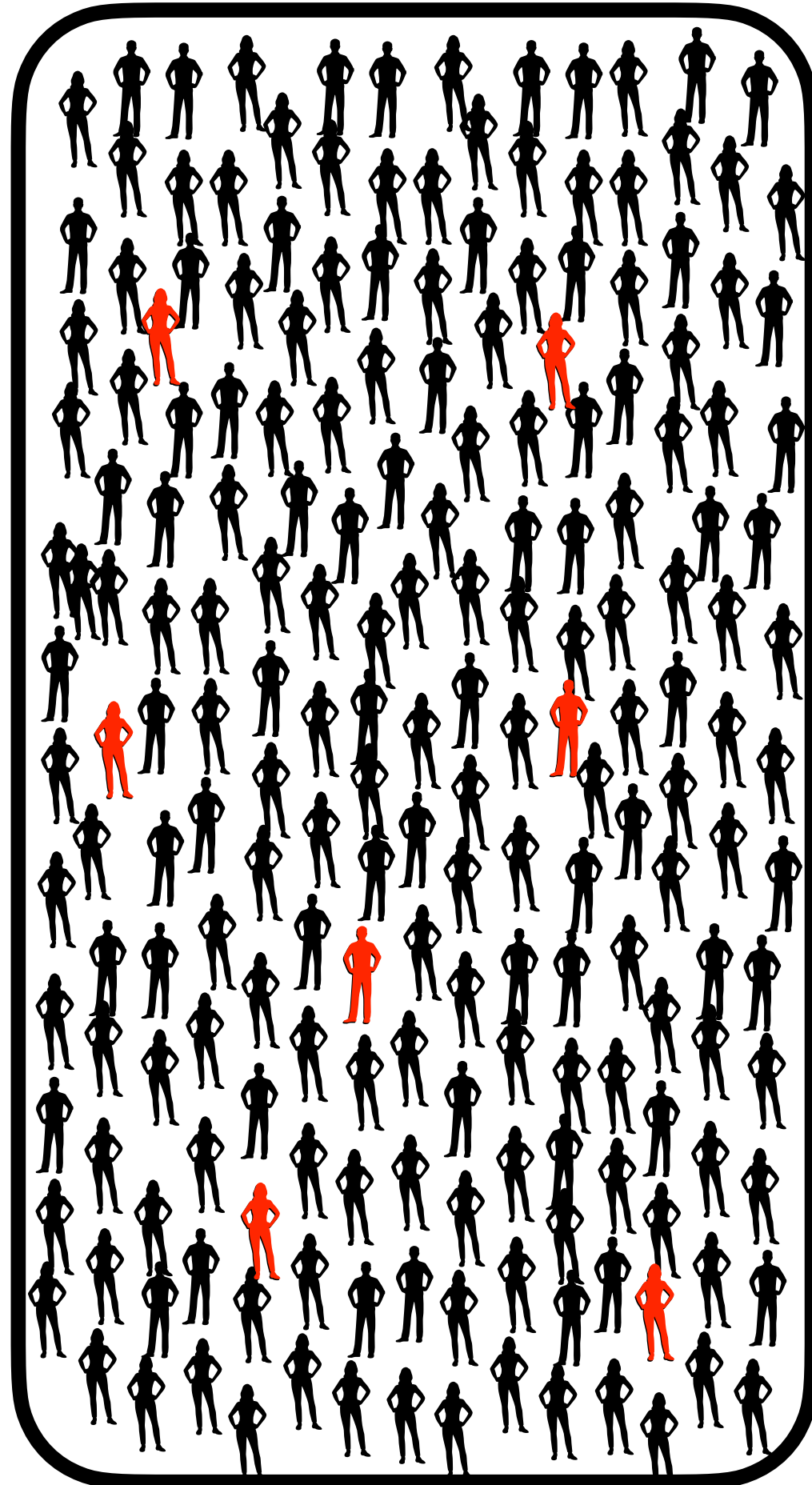
Aufgabenstellung



Hashing

- Menge U potentieller Schlüssel sehr groß, aktuelle Schlüsselmenge S jeweils nur kleine Teilmenge des Universums (im allgemeinen S nicht bekannt)
- **Idee:** durch Berechnung feststellen, wo Datensatz mit Schlüssel x gespeichert

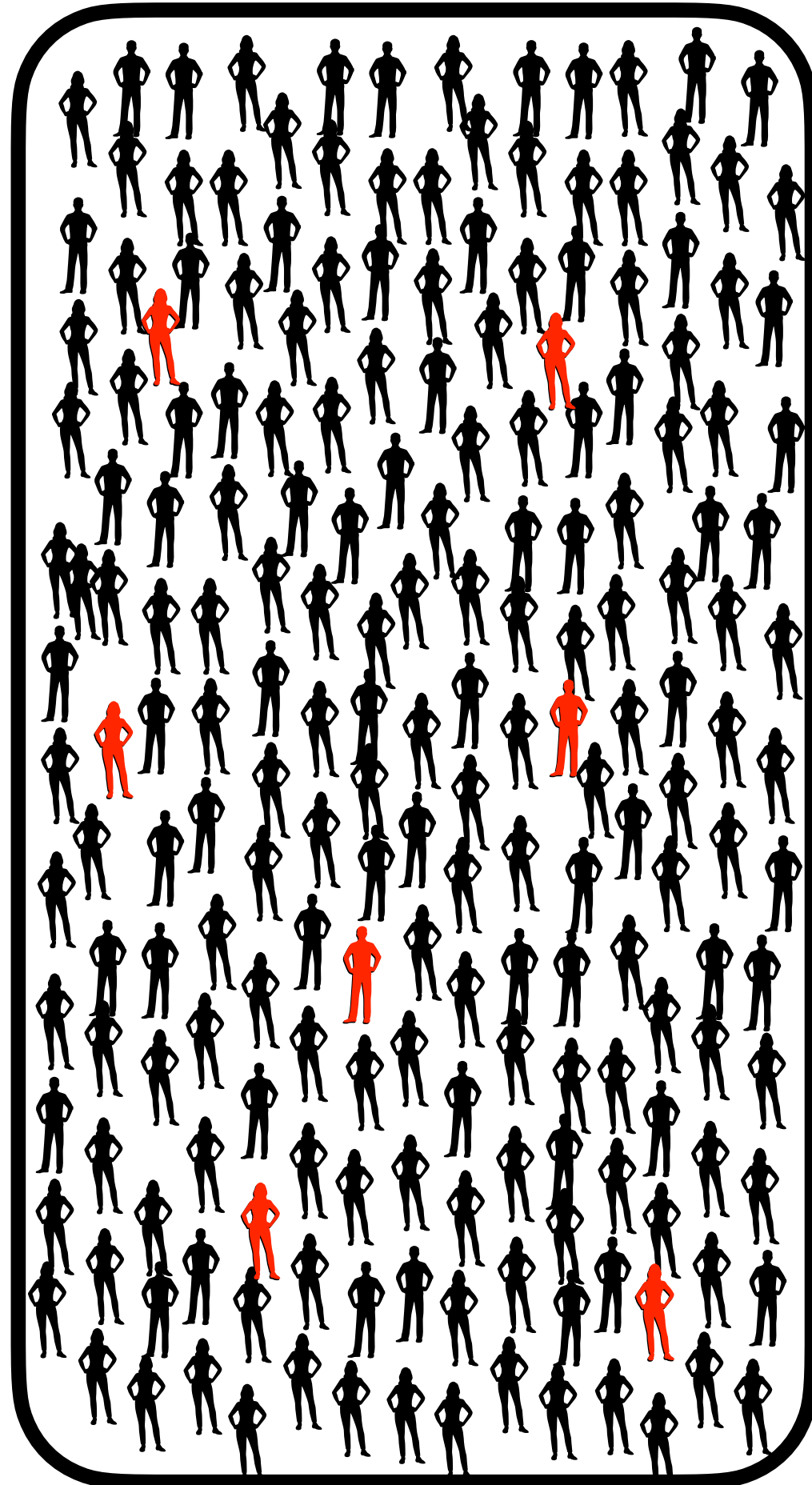
Aufgabenstellung



Hashing

- Menge U potentieller Schlüssel sehr groß, aktuelle Schlüsselmenge S jeweils nur kleine Teilmenge des Universums (im allgemeinen S nicht bekannt)
- **Idee:** durch Berechnung feststellen, wo Datensatz mit Schlüssel x gespeichert
- Abspeicherung der Datensätze in einem Array T mit Indizes $\{0, 1, \dots, m - 1\}$: **Hashtabelle**

Aufgabenstellung

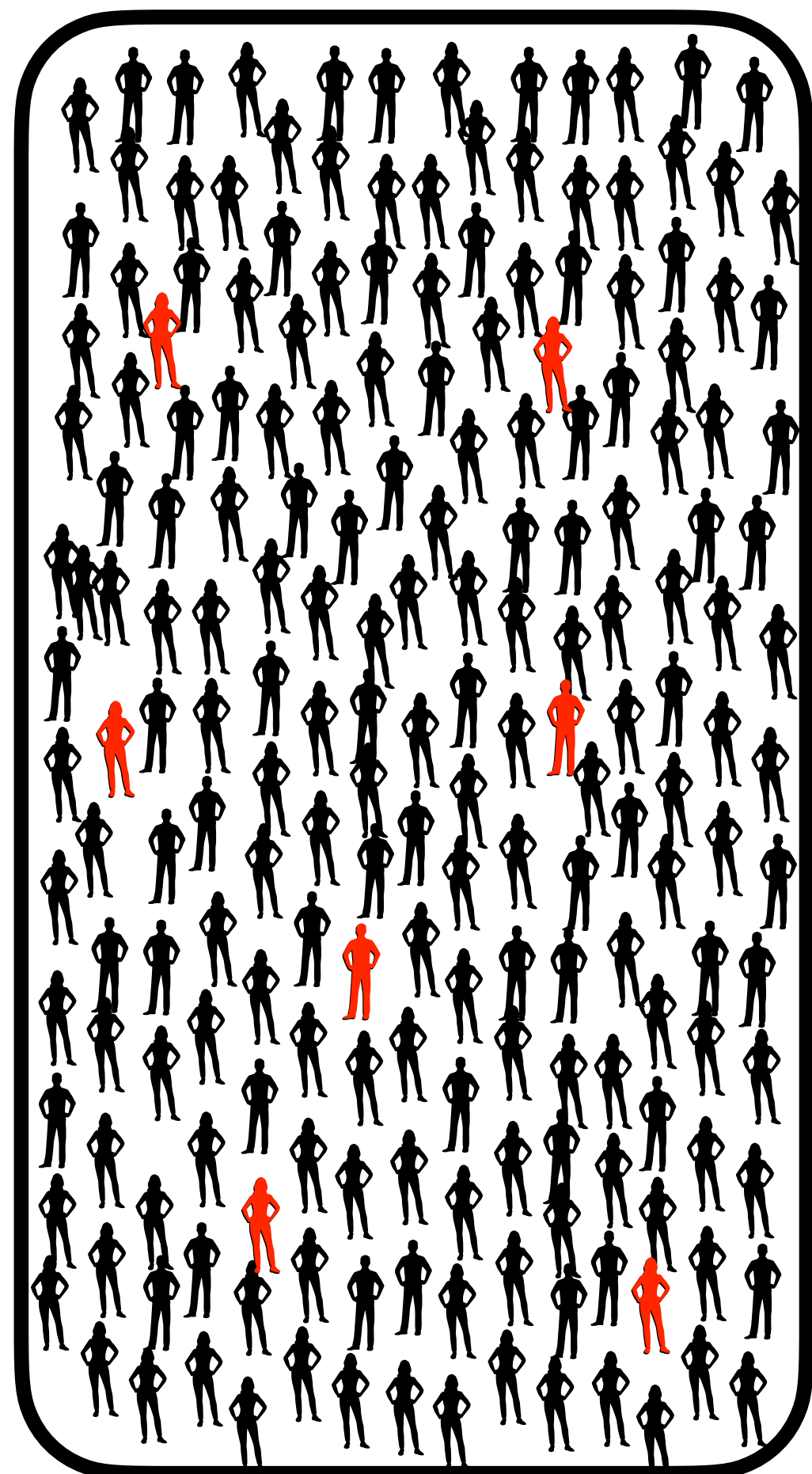


 U  S

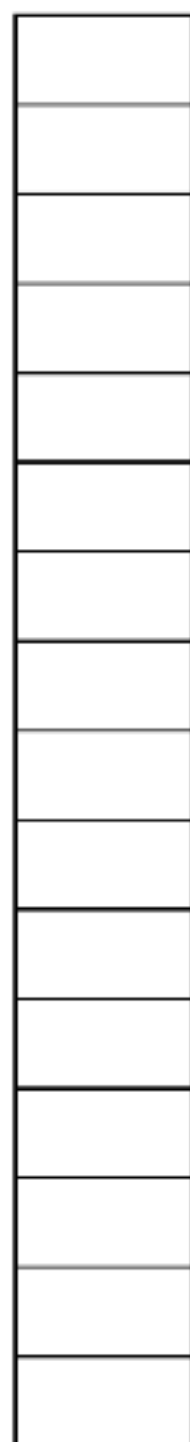
Hashing

- Menge U potentieller Schlüssel sehr groß, aktuelle Schlüsselmenge S jeweils nur kleine Teilmenge des Universums (im allgemeinen S nicht bekannt)
- **Idee:** durch Berechnung feststellen, wo Datensatz mit Schlüssel x gespeichert
- Abspeicherung der Datensätze in einem Array T mit Indizes $\{0, 1, \dots, m - 1\}$: **Hashtabelle**

Aufgabenstellung



T



U

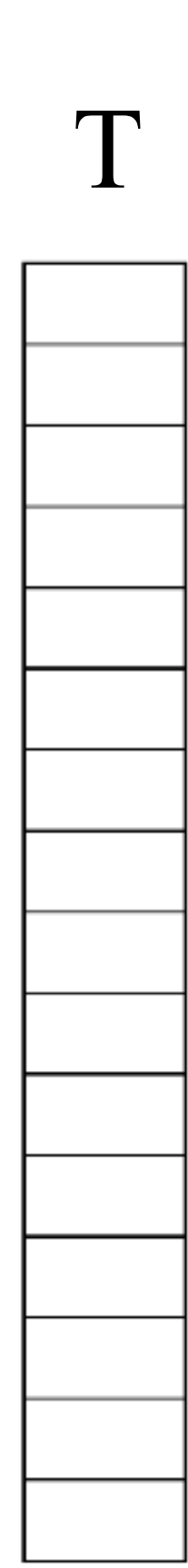
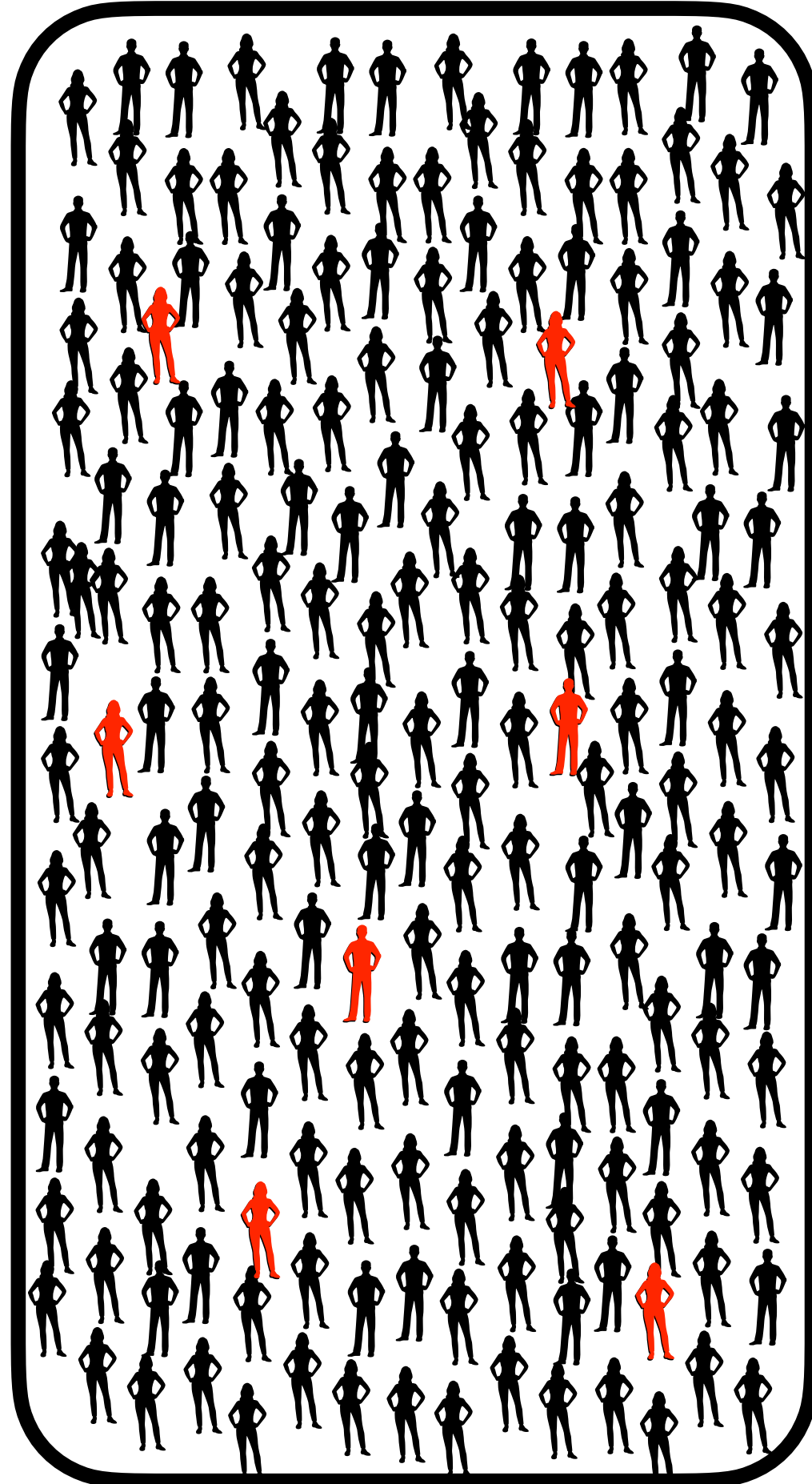


S

Hashing

- Menge U potentieller Schlüssel sehr groß, aktuelle Schlüsselmenge S jeweils nur kleine Teilmenge des Universums (im allgemeinen S nicht bekannt)
- **Idee:** durch Berechnung feststellen, wo Datensatz mit Schlüssel x gespeichert
- Abspeicherung der Datensätze in einem Array T mit Indizes $\{0, 1, \dots, m - 1\}$: **Hashtabelle**

Aufgabenstellung



U

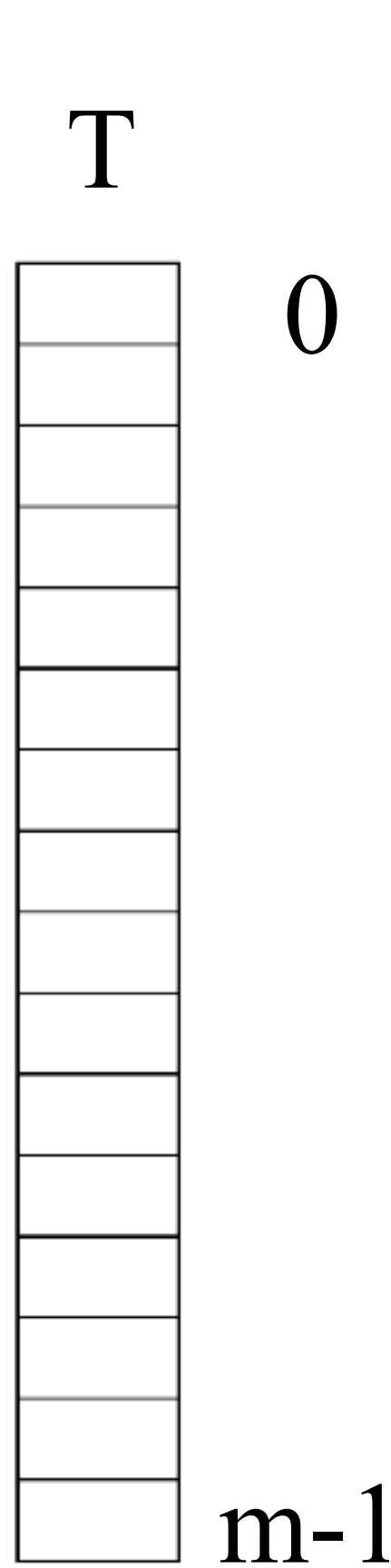
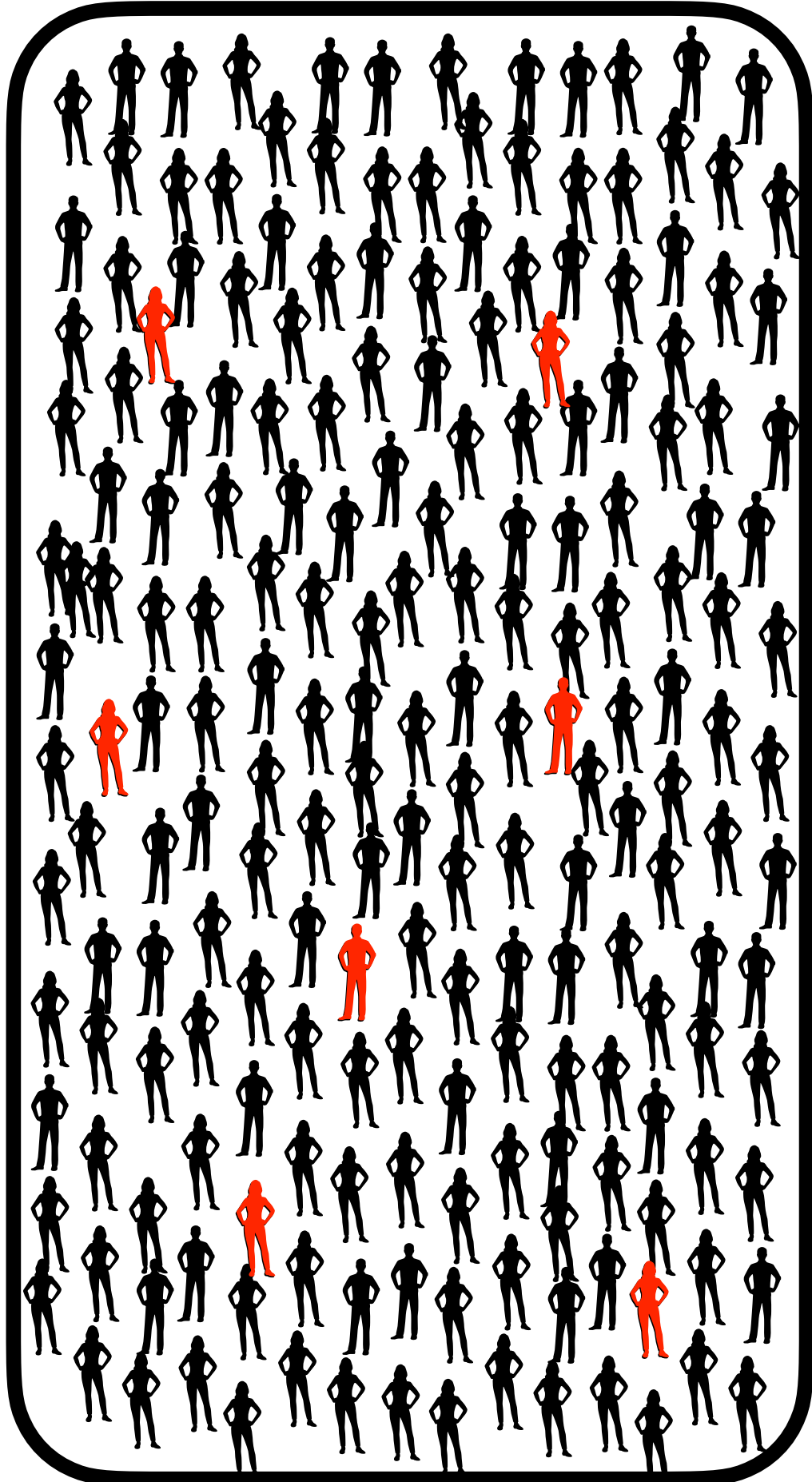
S

0

Hashing

- Menge U potentieller Schlüssel sehr groß, aktuelle Schlüsselmenge S jeweils nur kleine Teilmenge des Universums (im allgemeinen S nicht bekannt)
- **Idee:** durch Berechnung feststellen, wo Datensatz mit Schlüssel x gespeichert
- Abspeicherung der Datensätze in einem Array T mit Indizes $\{0, 1, \dots, m - 1\}$: **Hashtabelle**

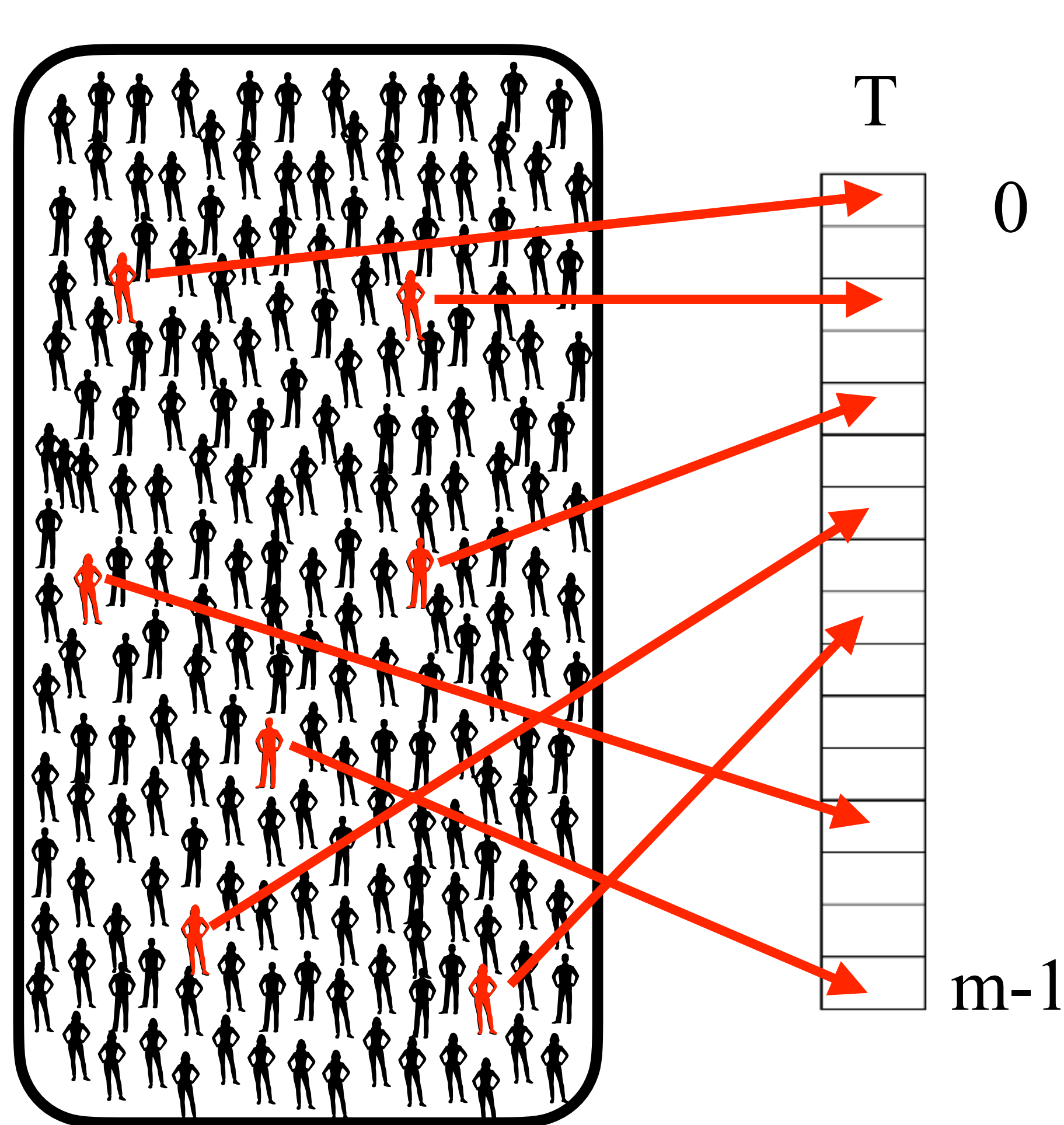
Aufgabenstellung



Hashing

- Menge U potentieller Schlüssel sehr groß, aktuelle Schlüsselmenge S jeweils nur kleine Teilmenge des Universums (im allgemeinen S nicht bekannt)
- **Idee:** durch Berechnung feststellen, wo Datensatz mit Schlüssel x gespeichert
- Abspeicherung der Datensätze in einem Array T mit Indizes $\{0, 1, \dots, m - 1\}$: **Hashtabelle**
- **Hashfunktion** h liefert für jeden Schlüssel $x \in U$ eine Adresse in Hashtabelle, d.h. $h : U \rightarrow \{0, 1, \dots, m - 1\}$.

Aufgabenstellung



 U  S

0

Hashing

- Menge U potentieller Schlüssel sehr groß, aktuelle Schlüsselmenge S jeweils nur kleine Teilmenge des Universums (im allgemeinen S nicht bekannt)
- **Idee:** durch Berechnung feststellen, wo Datensatz mit Schlüssel x gespeichert
- Abspeicherung der Datensätze in einem Array T mit Indizes $\{0, 1, \dots, m - 1\}$: **Hashtabelle**
- **Hashfunktion** h liefert für jeden Schlüssel $x \in U$ eine Adresse in Hashtabelle, d.h. $h : U \rightarrow \{0, 1, \dots, m - 1\}$.

m-1

Aufgabenstellung

Aufgabenstellung

Aufgabe

Dynamische Verwaltung von Daten, wobei jeder Datensatz eindeutig durch einen Schlüssel charakterisiert ist

Aufgabenstellung

Aufgabe

Dynamische Verwaltung von Daten, wobei jeder Datensatz eindeutig durch einen Schlüssel charakterisiert ist

Viele Anwendungen benötigen nur einfache Daten-Zugriffsmechanismen (**dictionary operations**):

Aufgabenstellung

Aufgabe

Dynamische Verwaltung von Daten, wobei jeder Datensatz eindeutig durch einen Schlüssel charakterisiert ist

Viele Anwendungen benötigen nur einfache Daten-Zugriffsmechanismen (**dictionary operations**):

- Suche nach Datensatz bei gegebenem Schlüssel x
search(x)

Aufgabenstellung

Aufgabe

Dynamische Verwaltung von Daten, wobei jeder Datensatz eindeutig durch einen Schlüssel charakterisiert ist

Viele Anwendungen benötigen nur einfache Daten-Zugriffsmechanismen (**dictionary operations**):

- Suche nach Datensatz bei gegebenem Schlüssel x
search(x)
- Einfügen eines neuen Datensatzes d mit Schlüssel x
insert(x, d) (abgekürzt **insert(x)**)

Aufgabenstellung

Aufgabe

Dynamische Verwaltung von Daten, wobei jeder Datensatz eindeutig durch einen Schlüssel charakterisiert ist

Viele Anwendungen benötigen nur einfache Daten-Zugriffsmechanismen (**dictionary operations**):

- Suche nach Datensatz bei gegebenem Schlüssel x
search(x)
- Einfügen eines neuen Datensatzes d mit Schlüssel x
insert(x, d) (abgekürzt **insert(x)**)
- Entfernen eines Datensatzes bei gegebenem Schlüssel x
delete(x)

Aufgabenstellung

Aufgabe

Dynamische Verwaltung von Daten, wobei jeder Datensatz eindeutig durch einen Schlüssel charakterisiert ist

Viele Anwendungen benötigen nur einfache Daten-Zugriffsmechanismen (**dictionary operations**):

- Suche nach Datensatz bei gegebenem Schlüssel x
search(x)
- Einfügen eines neuen Datensatzes d mit Schlüssel x
insert(x, d) (abgekürzt **insert(x)**)
- Entfernen eines Datensatzes bei gegebenem Schlüssel x
delete(x)

Menge potentieller Schlüssel (**Universum**) kann **sehr** groß sein!



Herausforderungen



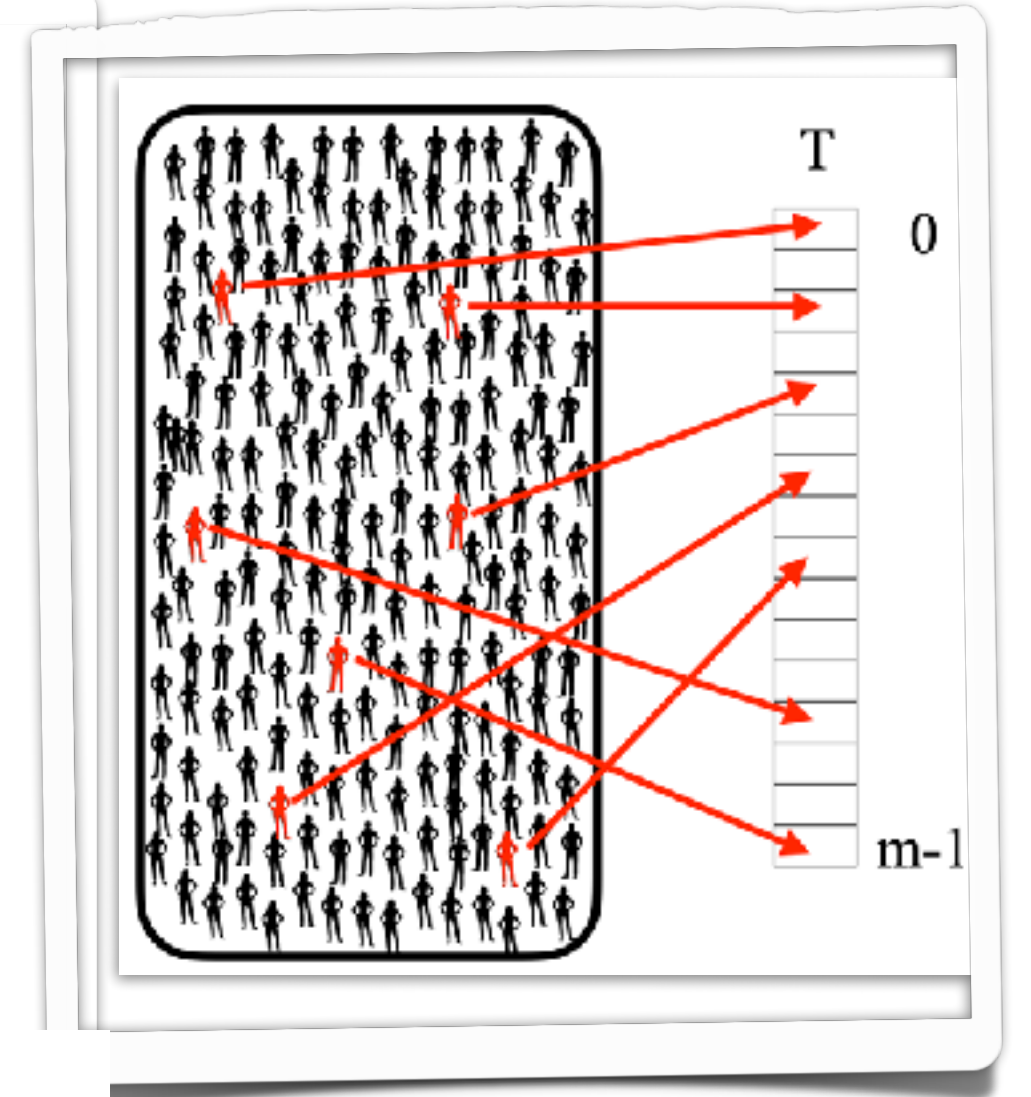
Herausforderungen

Anzahl möglicher Schlüssel viel größer als Hashtabelle, also

$$|U| \gg m$$

Herausforderungen

Anzahl möglicher Schlüssel viel größer als Hashtabelle, also
 $|U| \gg m$

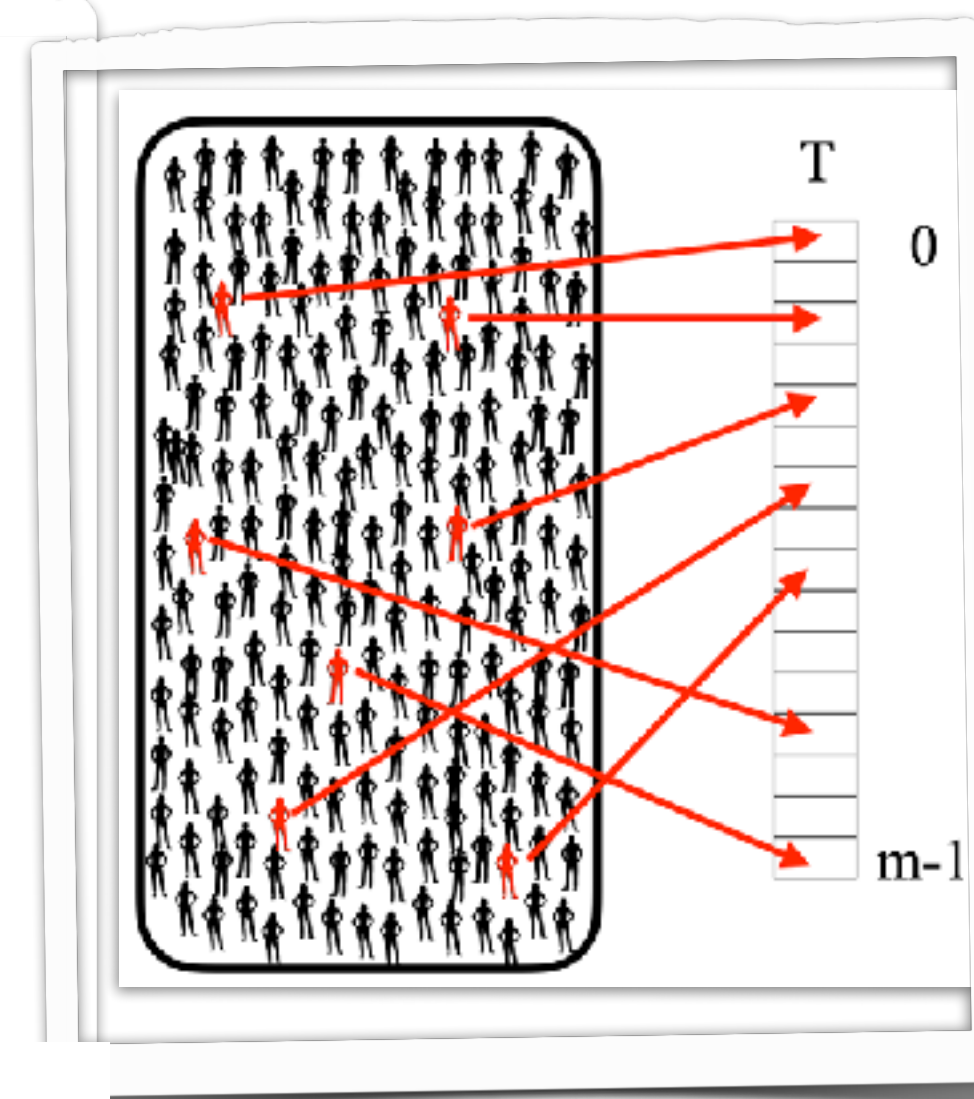


Herausforderungen

Anzahl möglicher Schlüssel viel größer als Hashtabelle, also

$$|U| \gg m$$

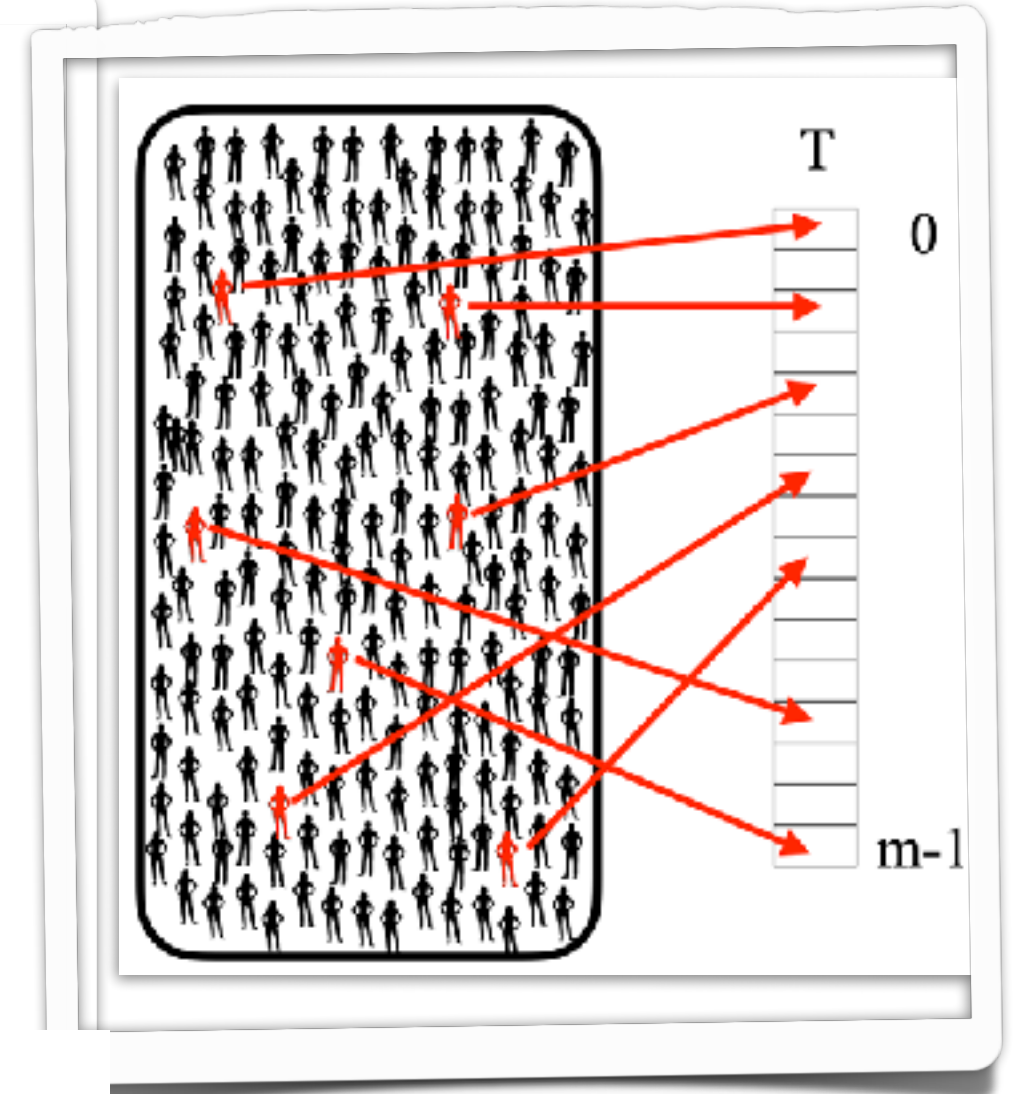
- Hashfunktion muss verschiedene Schlüssel x_1 und x_2 auf gleiche Adresse abbilden.



Herausforderungen

Anzahl möglicher Schlüssel viel größer als Hashtabelle, also
 $|U| \gg m$

- Hashfunktion muss verschiedene Schlüssel x_1 und x_2 auf gleiche Adresse abbilden.
- x_1 und x_2 beide in aktueller Schlüsselmenge
→ Adresskollision

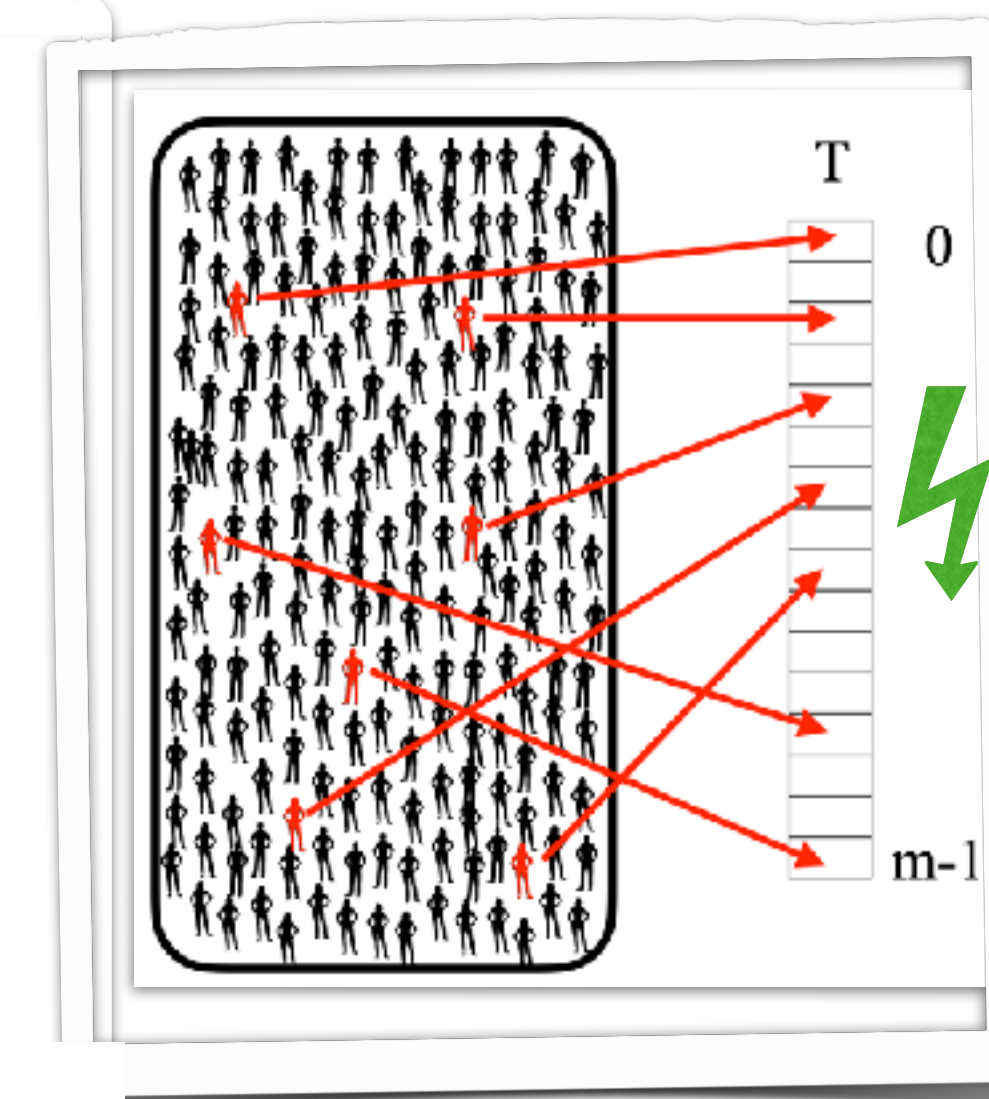


Herausforderungen

Anzahl möglicher Schlüssel viel größer als Hashtabelle, also

$$|U| \gg m$$

- Hashfunktion muss verschiedene Schlüssel x_1 und x_2 auf gleiche Adresse abbilden.
- x_1 und x_2 beide in aktueller Schlüsselmenge
→ Adresskollision

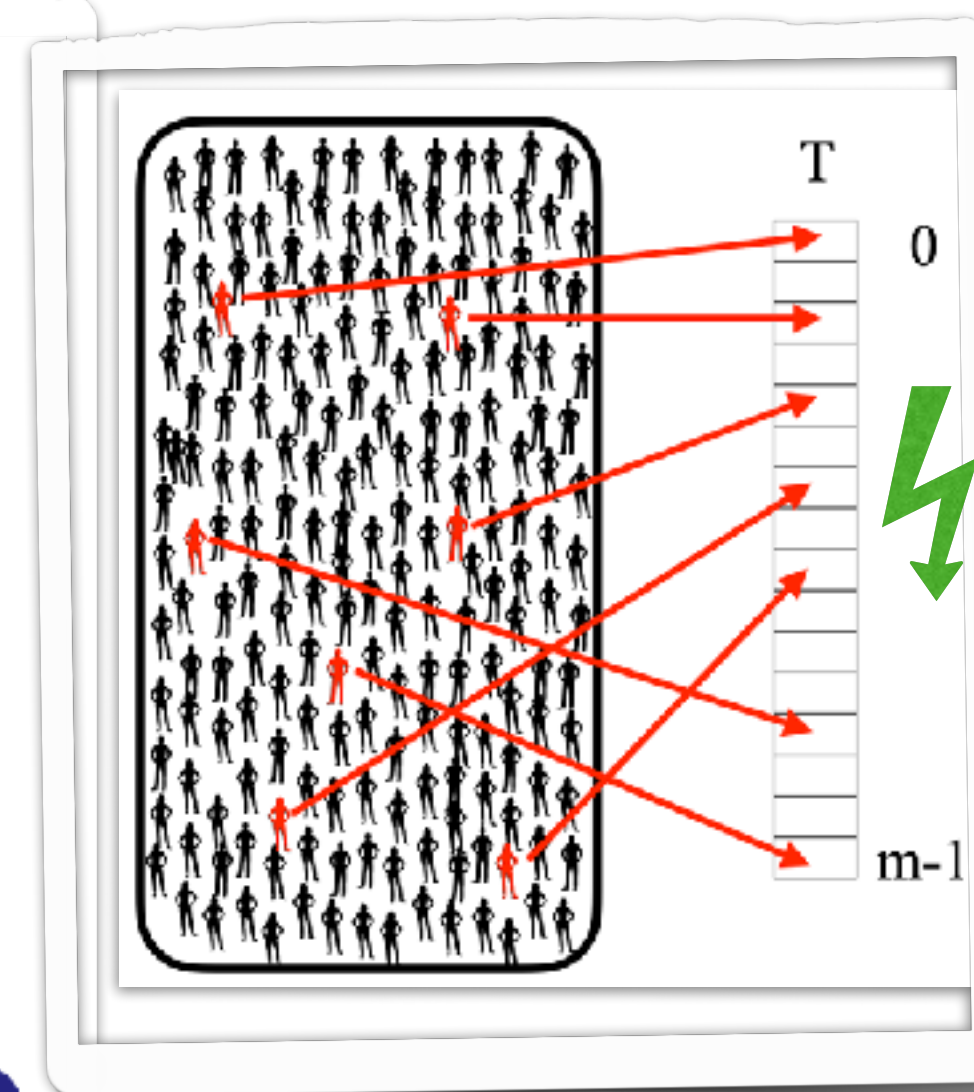


Herausforderungen

Anzahl möglicher Schlüssel viel größer als Hashtabelle, also

$$|U| \gg m$$

- Hashfunktion muss verschiedene Schlüssel x_1 und x_2 auf gleiche Adresse abbilden.
- x_1 und x_2 beide in aktueller Schlüsselmenge
→ Adresskollision



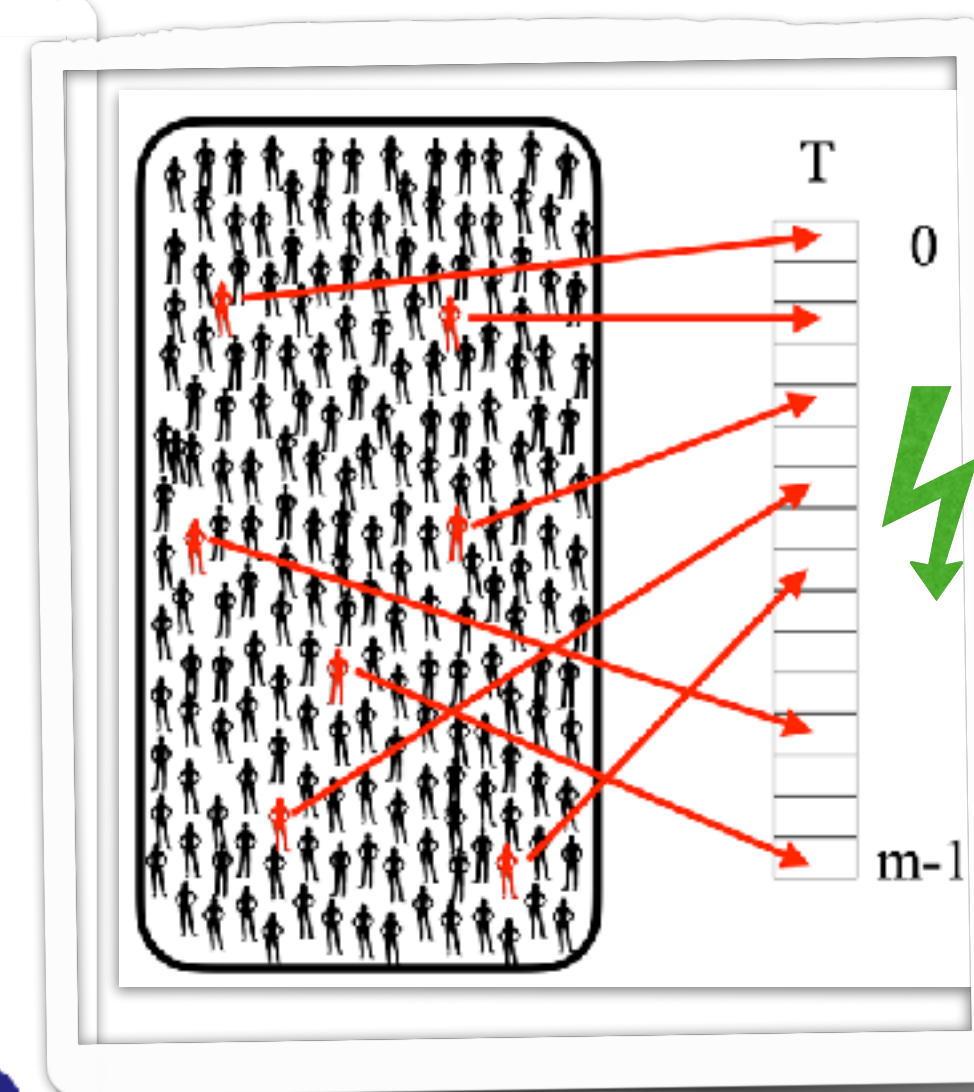
Hashverfahren gegeben durch:

Herausforderungen

Anzahl möglicher Schlüssel viel größer als Hashtabelle, also

$$|U| \gg m$$

- Hashfunktion muss verschiedene Schlüssel x_1 und x_2 auf gleiche Adresse abbilden.
- x_1 und x_2 beide in aktueller Schlüsselmenge
→ Adresskollision



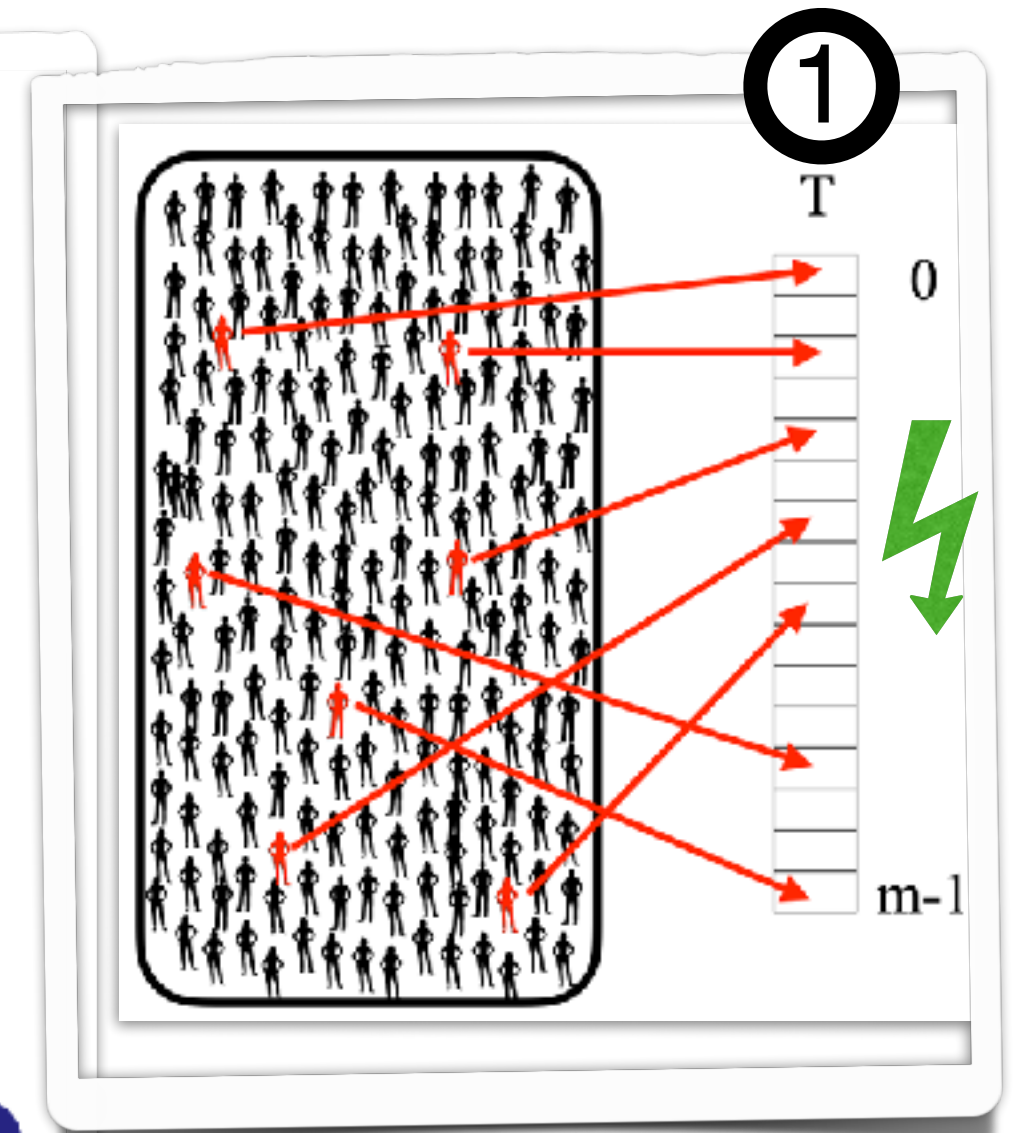
Hashverfahren gegeben durch:

① eine Hashtabelle,

Herausforderungen

Anzahl möglicher Schlüssel viel größer als Hashtabelle, also
 $|U| \gg m$

- Hashfunktion muss verschiedene Schlüssel x_1 und x_2 auf gleiche Adresse abbilden.
- x_1 und x_2 beide in aktueller Schlüsselmenge
→ Adresskollision



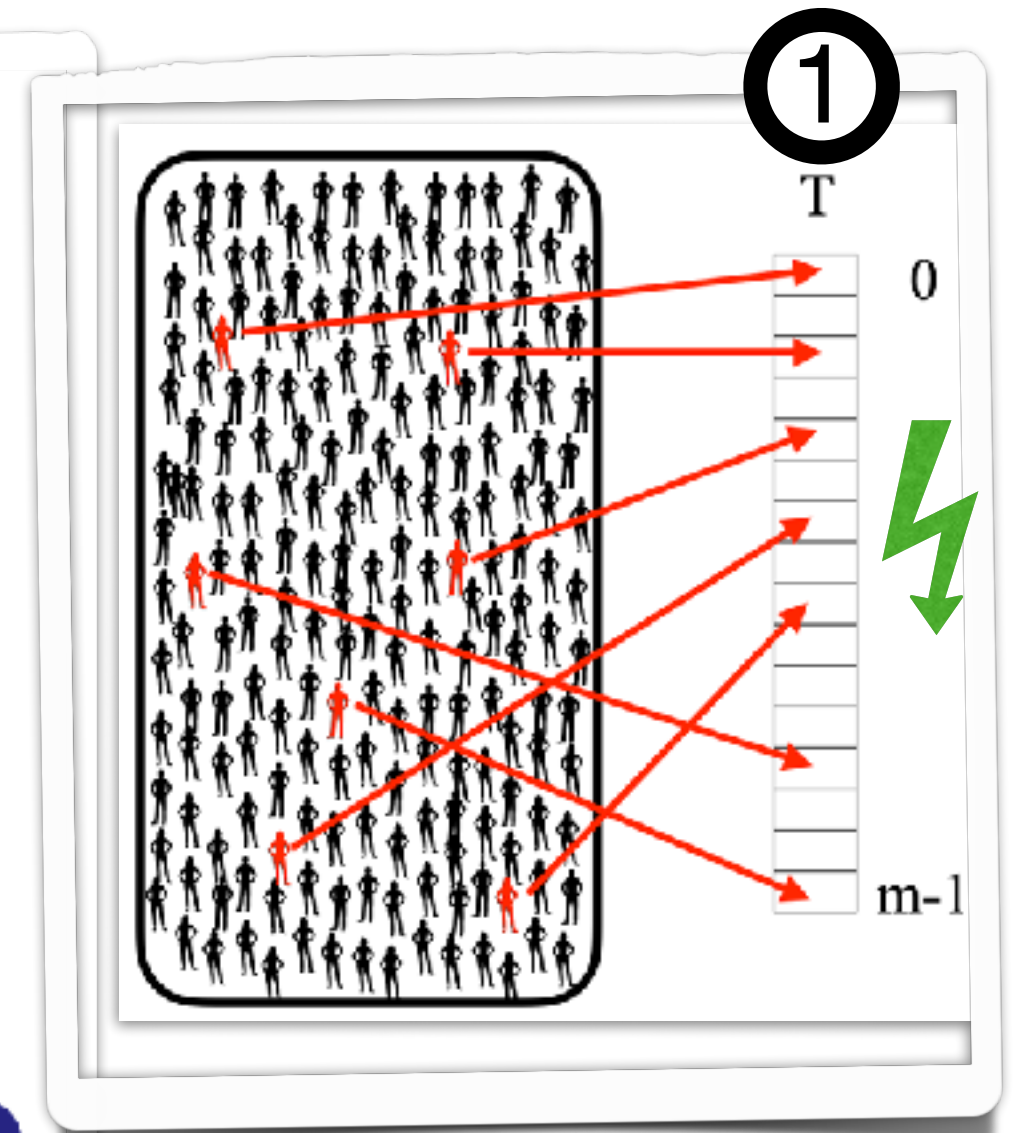
Hashverfahren gegeben durch:

① eine Hashtabelle,

Herausforderungen

Anzahl möglicher Schlüssel viel größer als Hashtabelle, also
 $|U| \gg m$

- Hashfunktion muss verschiedene Schlüssel x_1 und x_2 auf gleiche Adresse abbilden.
- x_1 und x_2 beide in aktueller Schlüsselmenge
→ Adresskollision



Hashverfahren gegeben durch:

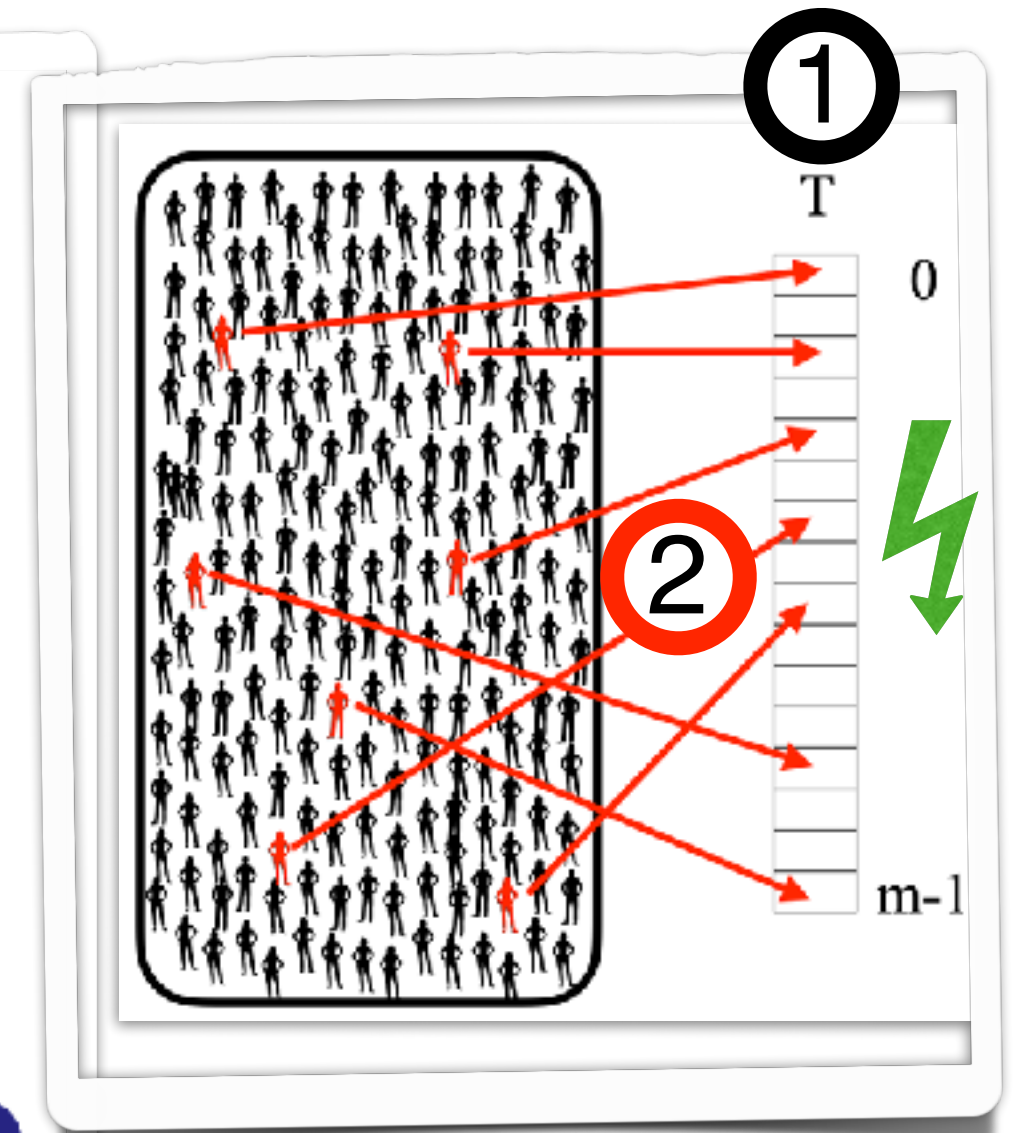
- ① eine Hashtabelle,
- ② eine Hashfunktion, die Universum der möglichen Schlüssel auf Adressen einer Hashtabelle abbildet,

Herausforderungen

Anzahl möglicher Schlüssel viel größer als Hashtabelle, also

$$|U| \gg m$$

- Hashfunktion muss verschiedene Schlüssel x_1 und x_2 auf gleiche Adresse abbilden.
- x_1 und x_2 beide in aktueller Schlüsselmenge
→ Adresskollision



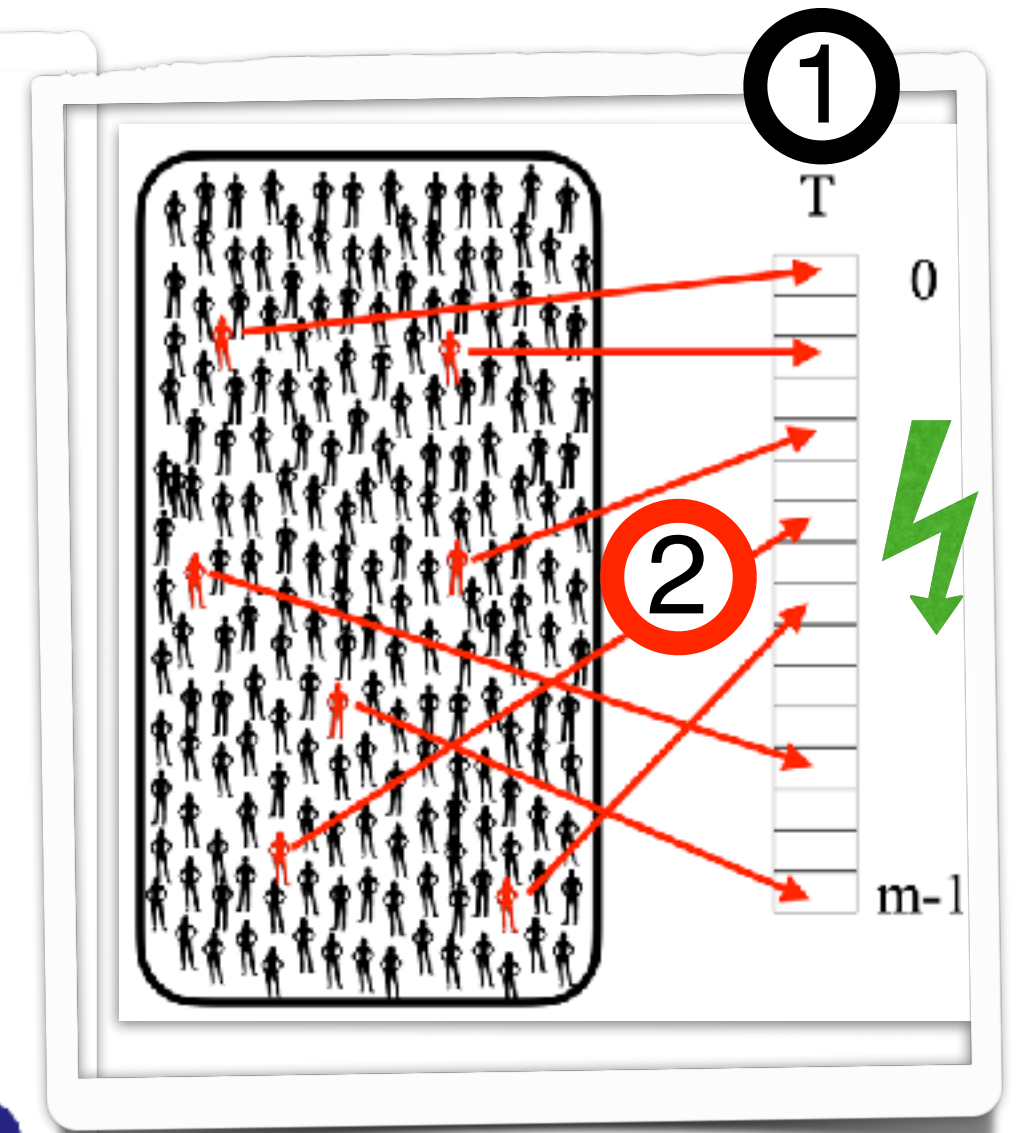
Hashverfahren gegeben durch:

- ① eine Hashtabelle,
- ② eine Hashfunktion, die Universum der möglichen Schlüssel auf Adressen einer Hashtabelle abbildet,

Herausforderungen

Anzahl möglicher Schlüssel viel größer als Hashtabelle, also
 $|U| \gg m$

- Hashfunktion muss verschiedene Schlüssel x_1 und x_2 auf gleiche Adresse abbilden.
- x_1 und x_2 beide in aktueller Schlüsselmenge
→ Adresskollision



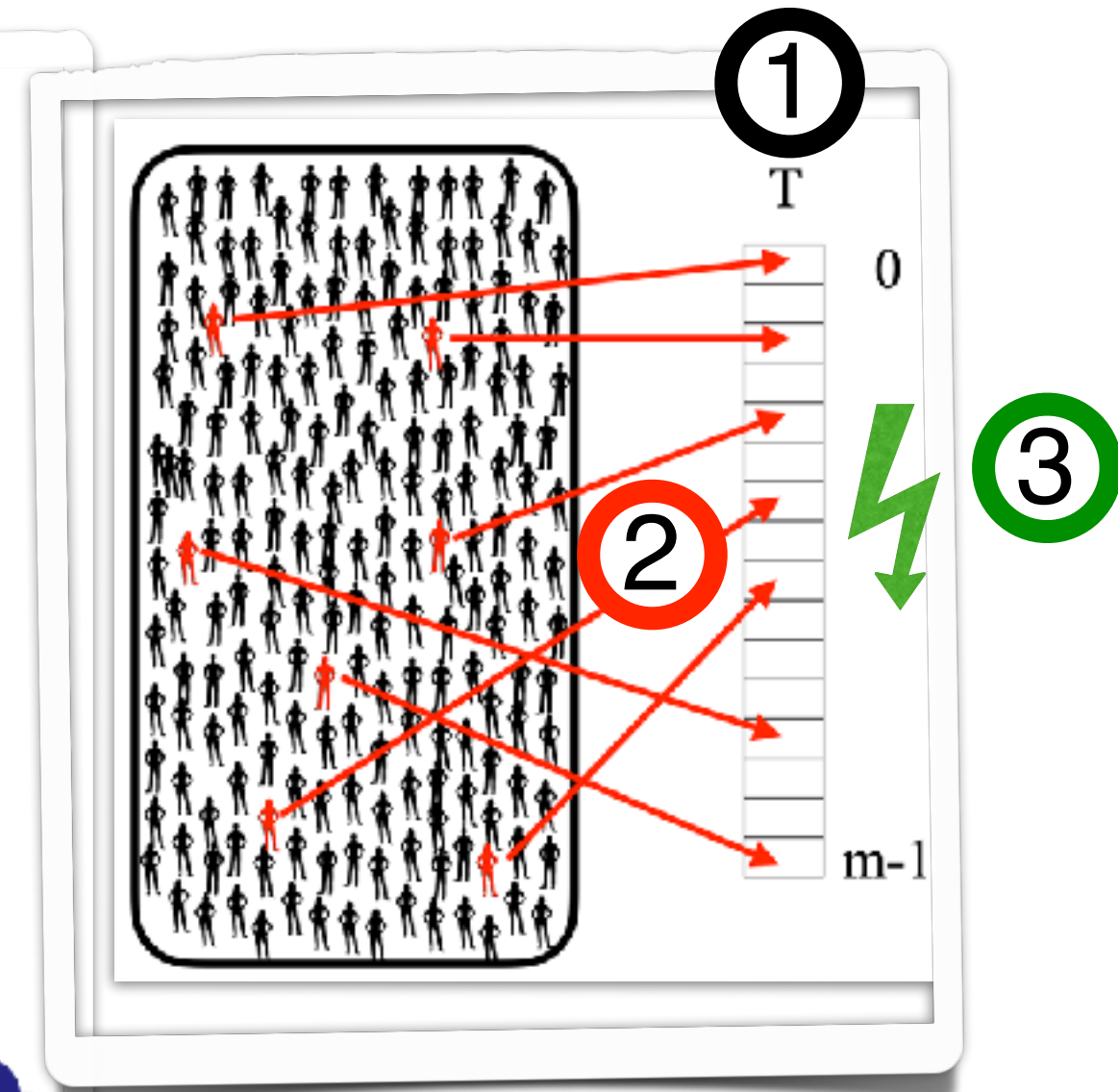
Hashverfahren gegeben durch:

- ① eine Hashtabelle,
- ② eine Hashfunktion, die Universum der möglichen Schlüssel auf Adressen einer Hashtabelle abbildet,
- ③ eine Strategie zur Auflösung möglicher Adresskollisionen.

Herausforderungen

Anzahl möglicher Schlüssel viel größer als Hashtabelle, also
 $|U| \gg m$

- Hashfunktion muss verschiedene Schlüssel x_1 und x_2 auf gleiche Adresse abbilden.
- x_1 und x_2 beide in aktueller Schlüsselmenge
→ Adresskollision



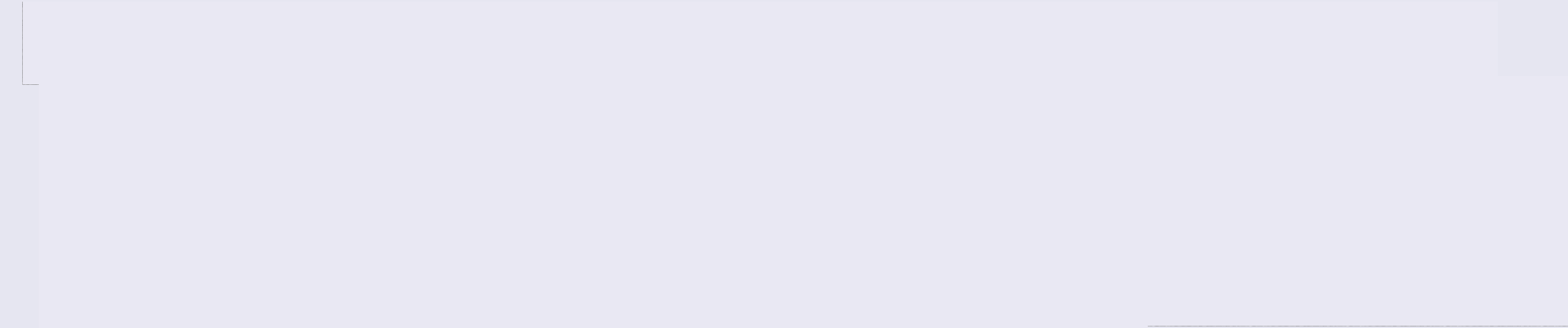
Hashverfahren gegeben durch:

- ① eine Hashtabelle,
- ② eine Hashfunktion, die Universum der möglichen Schlüssel auf Adressen einer Hashtabelle abbildet,
- ③ eine Strategie zur Auflösung möglicher Adresskollisionen.

Anforderungen

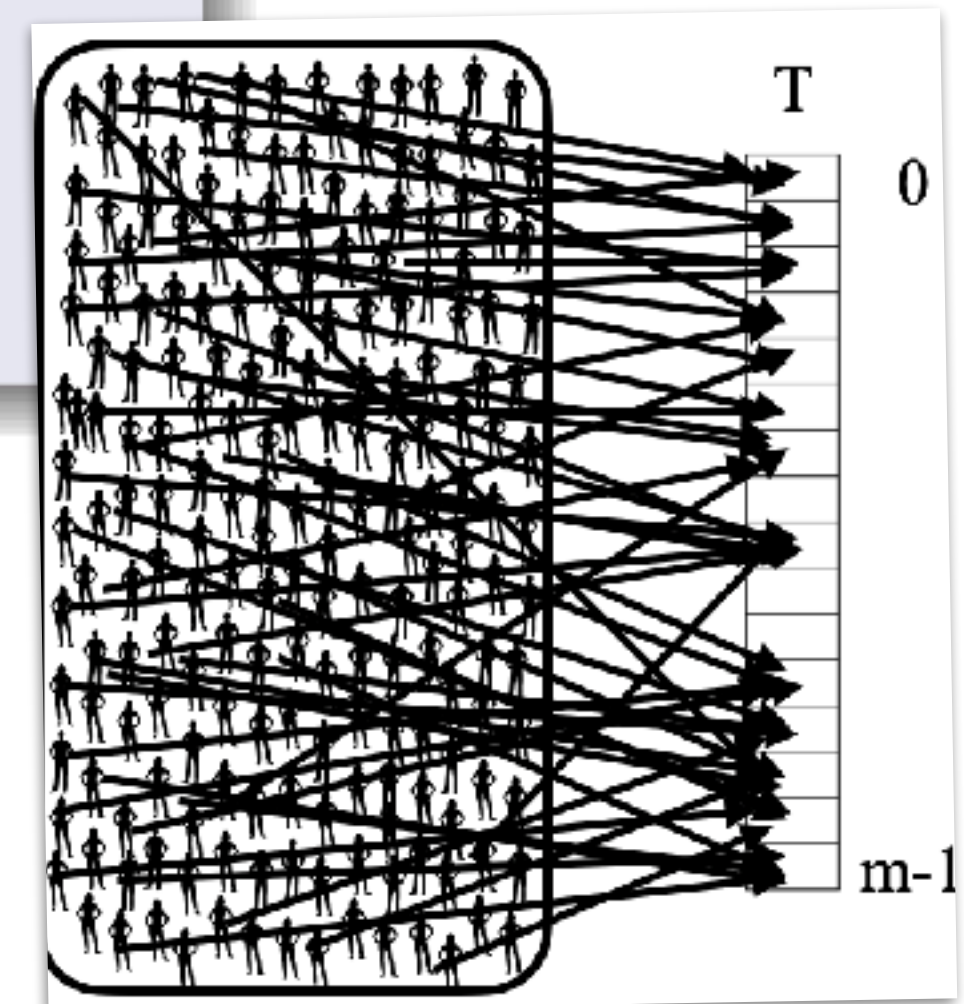
Anforderungen

Gute Hashfunktionen sollten:



Anforderungen

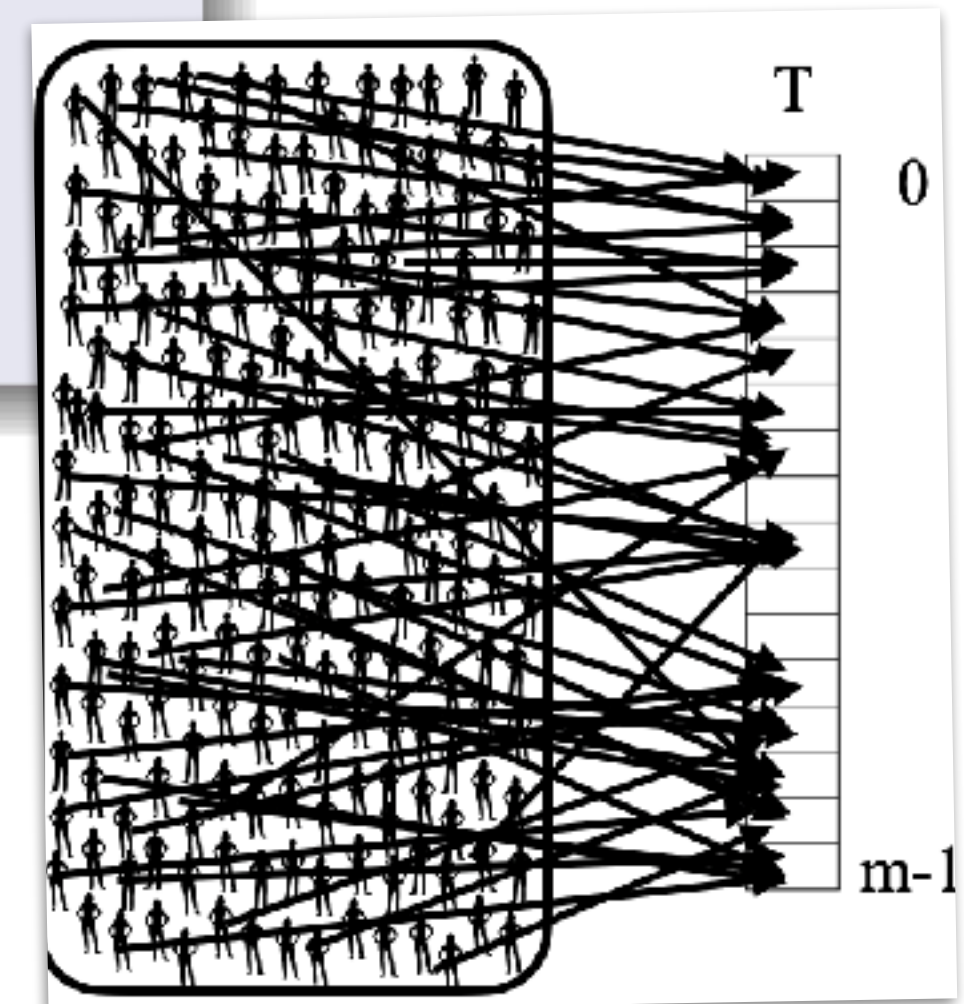
Gute Hashfunktionen sollten:



Anforderungen

Gute Hashfunktionen sollten:

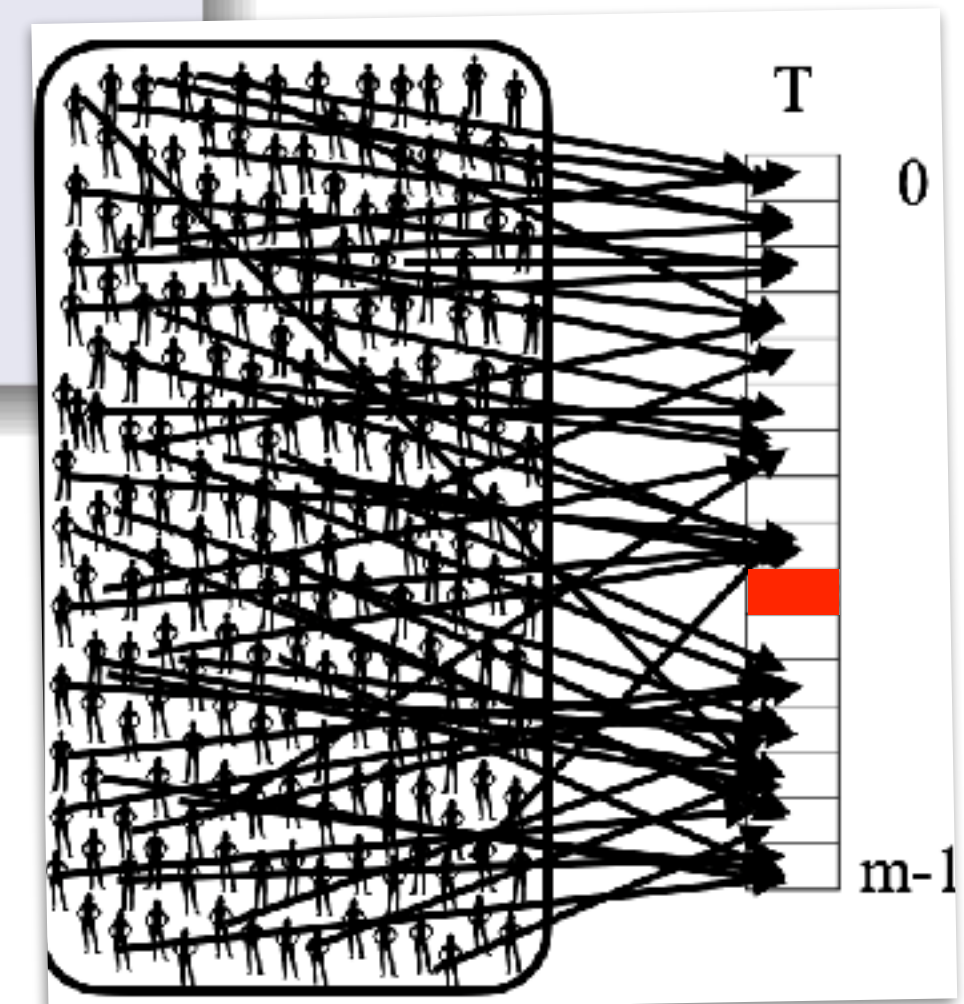
- surjektiv sein, d.h. den ganzen Wertebereich umfassen,



Anforderungen

Gute Hashfunktionen sollten:

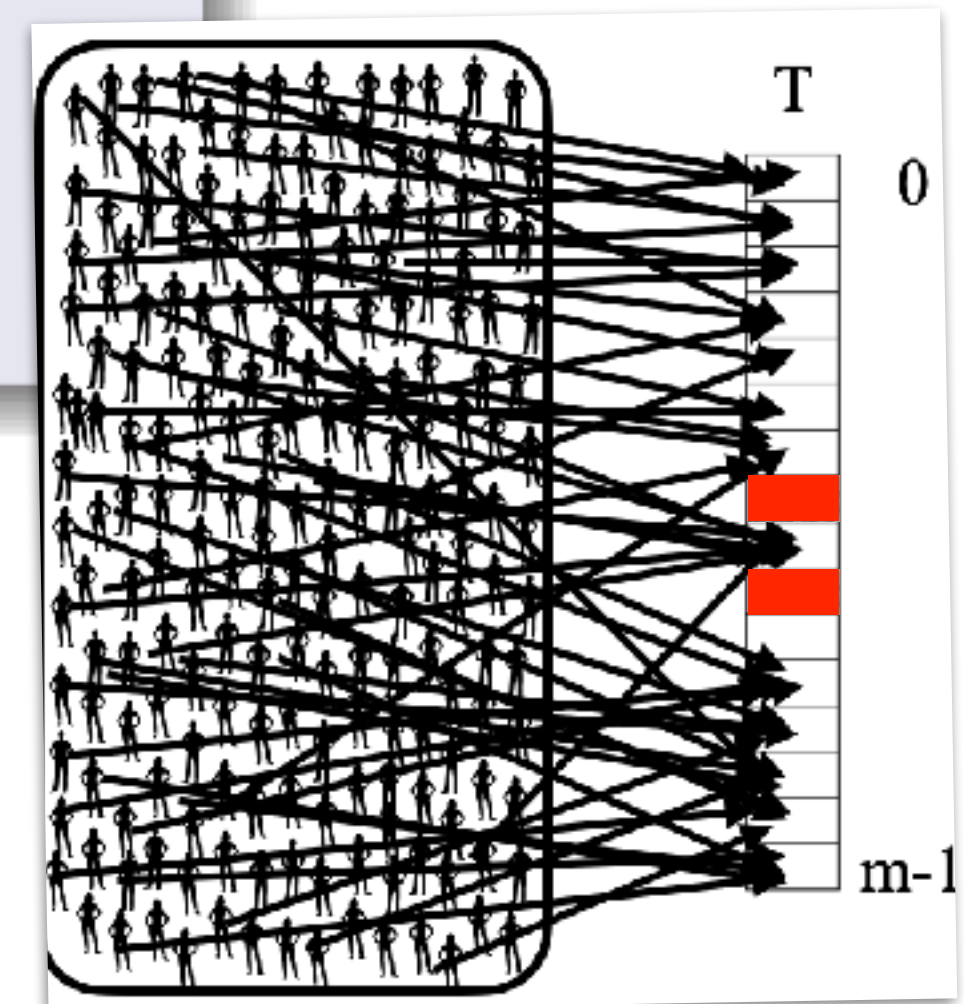
- surjektiv sein, d.h. den ganzen Wertebereich umfassen,



Anforderungen

Gute Hashfunktionen sollten:

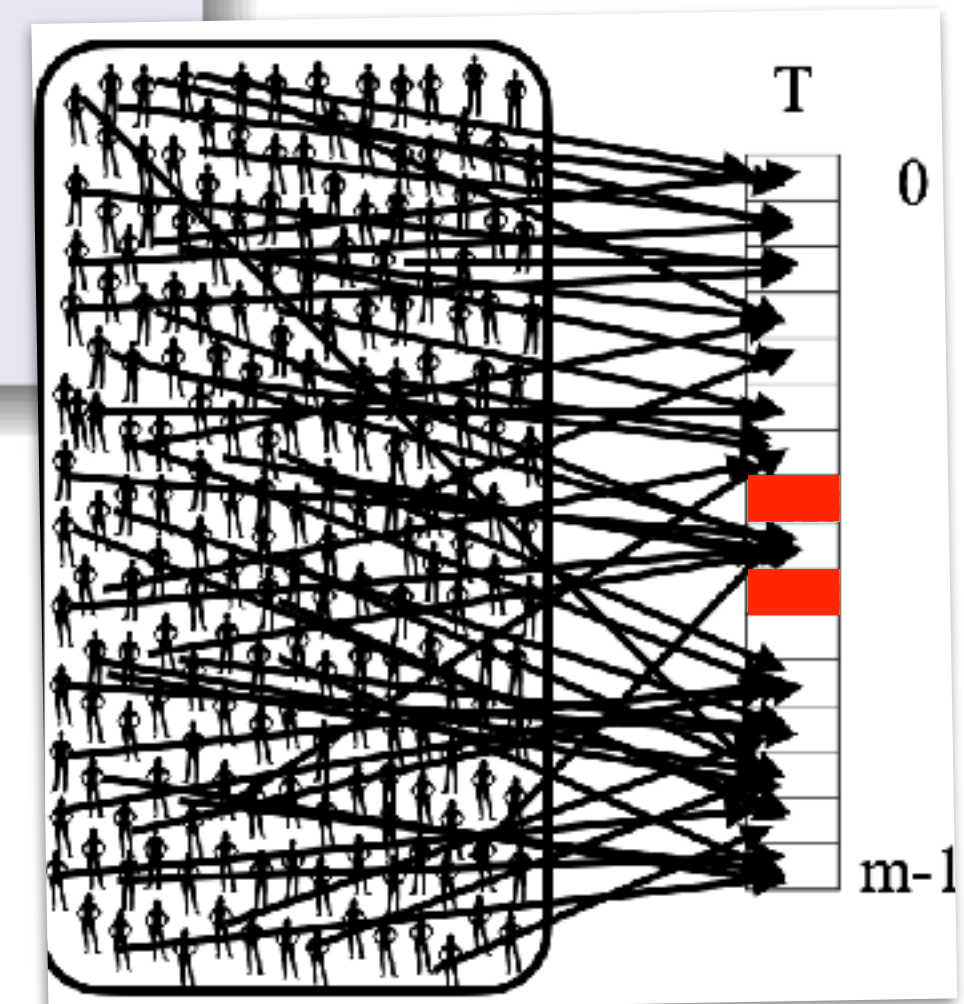
- surjektiv sein, d.h. den ganzen Wertebereich umfassen,



Anforderungen

Gute Hashfunktionen sollten:

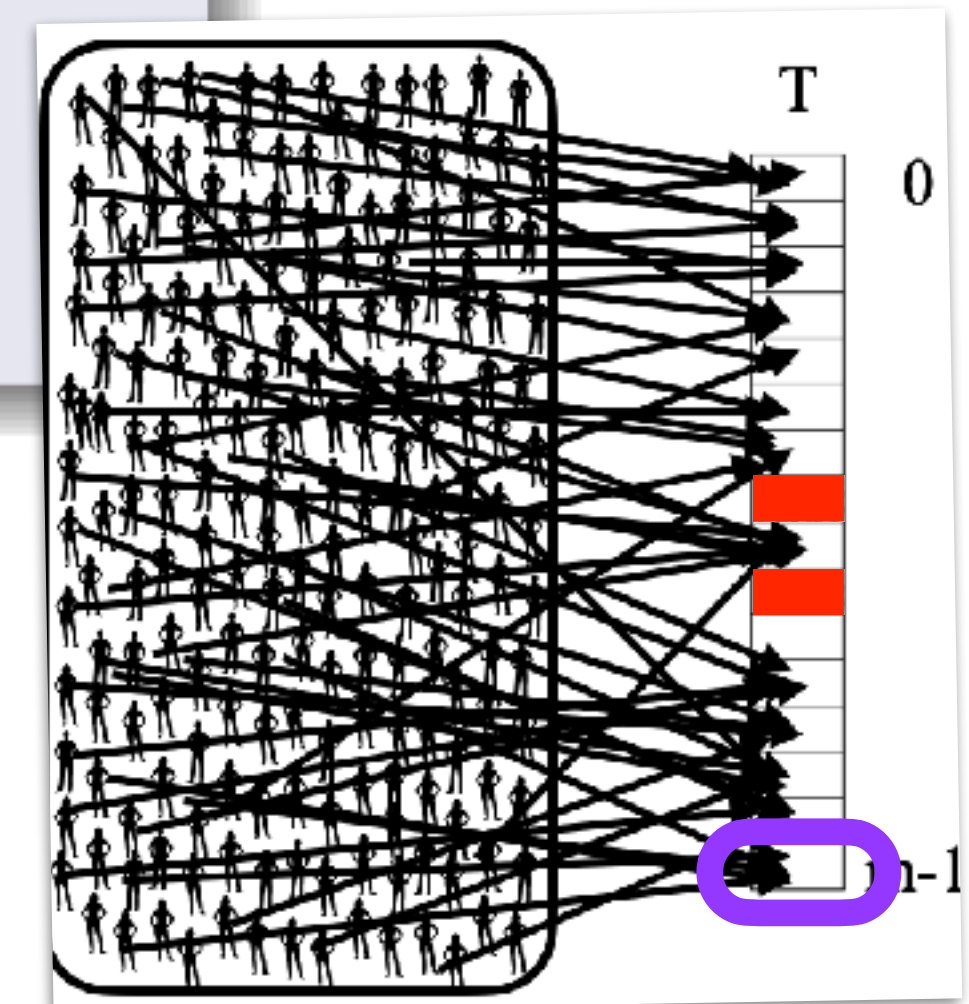
- surjektiv sein, d.h. den ganzen Wertebereich umfassen,
- die zu speichernden Schlüssel (möglichst) gleichmäßig verteilen, d.h. für alle Speicherplätze i und j sollte gelten $|h^{-1}(i)| \approx |h^{-1}(j)|$,



Anforderungen

Gute Hashfunktionen sollten:

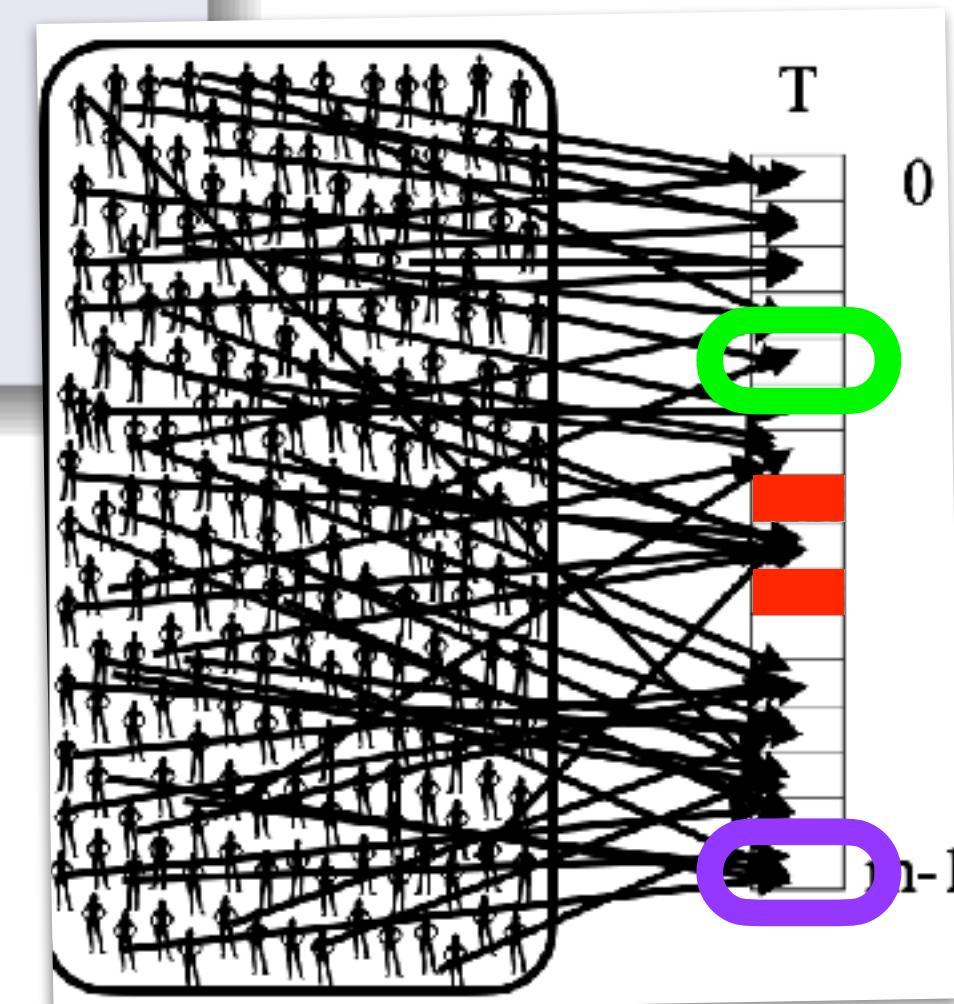
- surjektiv sein, d.h. den ganzen Wertebereich umfassen,
- die zu speichernden Schlüssel (möglichst) gleichmäßig verteilen, d.h. für alle Speicherplätze i und j sollte gelten $|h^{-1}(i)| \approx |h^{-1}(j)|$,



Anforderungen

Gute Hashfunktionen sollten:

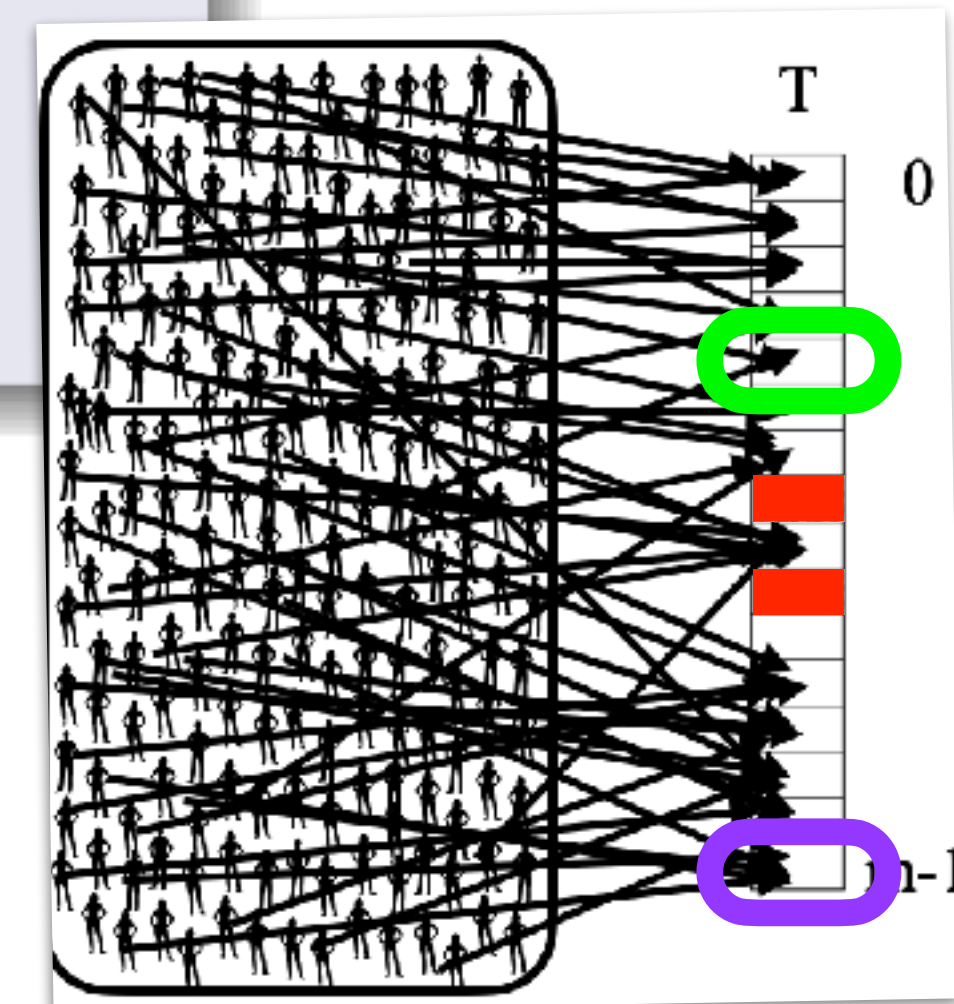
- surjektiv sein, d.h. den ganzen Wertebereich umfassen,
- die zu speichernden Schlüssel (möglichst) gleichmäßig verteilen, d.h. für alle Speicherplätze i und j sollte gelten $|h^{-1}(i)| \approx |h^{-1}(j)|$,



Anforderungen

Gute Hashfunktionen sollten:

- surjektiv sein, d.h. den ganzen Wertebereich umfassen,
- die zu speichernden Schlüssel (möglichst) gleichmäßig verteilen, d.h. für alle Speicherplätze i und j sollte gelten $|h^{-1}(i)| \approx |h^{-1}(j)|$,
- effizient berechenbar sein.



7.3 Hashfunktionen

Divisions-Rest-Methode

Divisions-Rest-Methode

Divisions-Rest-Methode

$$h(x) = x \bmod m := x - \left\lfloor \frac{x}{m} \right\rfloor \cdot m$$

Divisions-Rest-Methode

Divisions-Rest-Methode

$$h(x) = x \bmod m := x - \left\lfloor \frac{x}{m} \right\rfloor \cdot m$$

Beispiel: $m=11$, $S=\{49, 22, 6, 52, 76, 34, 13, 29\}$

Divisions-Rest-Methode

Divisions-Rest-Methode

$$h(x) = x \bmod m := x - \left\lfloor \frac{x}{m} \right\rfloor \cdot m$$

Beispiel: $m=11$, $S=\{49, 22, 6, 52, 76, 34, 13, 29\}$

Hashwerte: $h(49) = 5$

Divisions-Rest-Methode

Divisions-Rest-Methode

$$h(x) = x \bmod m := x - \left\lfloor \frac{x}{m} \right\rfloor \cdot m$$

Beispiel: $m=11$, $S=\{49, 22, 6, 52, 76, 34, 13, 29\}$

Hashwerte: $h(49) = 5$
 $h(22) = 0$

Divisions-Rest-Methode

Divisions-Rest-Methode

$$h(x) = x \bmod m := x - \left\lfloor \frac{x}{m} \right\rfloor \cdot m$$

Beispiel: $m=11$, $S=\{49, 22, 6, 52, 76, 34, 13, 29\}$

Hashwerte: $h(49) = 5$
 $h(22) = 0$
 $h(6) = 6$

Divisions-Rest-Methode

Divisions-Rest-Methode

$$h(x) = x \bmod m := x - \left\lfloor \frac{x}{m} \right\rfloor \cdot m$$

Beispiel: $m=11$, $S=\{49, 22, 6, 52, 76, 34, 13, 29\}$

Hashwerte: $h(49) = 5$
 $h(22) = 0$
 $h(6) = 6$
 $h(52) = 8$

Divisions-Rest-Methode

Divisions-Rest-Methode

$$h(x) = x \bmod m := x - \left\lfloor \frac{x}{m} \right\rfloor \cdot m$$

Beispiel: $m=11$, $S=\{49, 22, 6, 52, 76, 34, 13, 29\}$

Hashwerte: $h(49) = 5$

$h(22) = 0$

$h(6) = 6$

$h(52) = 8$

$h(76) = 10$

Divisions-Rest-Methode

Divisions-Rest-Methode

$$h(x) = x \bmod m := x - \left\lfloor \frac{x}{m} \right\rfloor \cdot m$$

Beispiel: $m=11$, $S=\{49, 22, 6, 52, 76, 34, 13, 29\}$

Hashwerte: $h(49) = 5$

$h(22) = 0$

$h(6) = 6$

$h(52) = 8$

$h(76) = 10$

$h(34) = 1$

Divisions-Rest-Methode

Divisions-Rest-Methode

$$h(x) = x \bmod m := x - \left\lfloor \frac{x}{m} \right\rfloor \cdot m$$

Beispiel: $m=11$, $S=\{49, 22, 6, 52, 76, 34, 13, 29\}$

Hashwerte: $h(49) = 5$

$h(22) = 0$

$h(6) = 6$

$h(52) = 8$

$h(76) = 10$

$h(34) = 1$

$h(13) = 2$

Divisions-Rest-Methode

Divisions-Rest-Methode

$$h(x) = x \bmod m := x - \left\lfloor \frac{x}{m} \right\rfloor \cdot m$$

Beispiel: $m=11$, $S=\{49, 22, 6, 52, 76, 34, 13, 29\}$

Hashwerte: $h(49) = 5$

$h(22) = 0$

$h(6) = 6$

$h(52) = 8$

$h(76) = 10$

$h(34) = 1$

$h(13) = 2$

$h(29) = 7$

7.4 Kollisionen

Geburtstagsparadoxon

Geburtstagsparadoxon

Annahme:

- Daten unabhängig
- $\text{Prob}(h(x) = j) = 1/m$

Prob(i -tes Datum kollidiert nicht mit den ersten $i - 1$ Daten, wenn diese kollisionsfrei sind) = $\frac{m - (i - 1)}{m}$

Intuition:

Egal welche Speicherplätze die ersten $i - 1$ Daten belegen, $m - i + 1$ der m Möglichkeiten sind *gut*.

Prob(n Daten kollisionsfrei) = $\frac{m-1}{m} \cdot \frac{m-2}{m} \dots \frac{m-n+1}{m}$

Beispiel: $m = 365$

Prob(23 Daten kollisionsfrei) ≈ 0.49

Prob(50 Daten kollisionsfrei) ≈ 0.03

Geburtstagsparadoxon

Annahme:

- Daten unabhängig
- $\text{Prob}(h(x) = j) = 1/m$

Prob(i -tes Datum kollidiert nicht mit den ersten $i - 1$ Daten, wenn diese kollisionsfrei sind) = $\frac{m - (i - 1)}{m}$

Intuition:

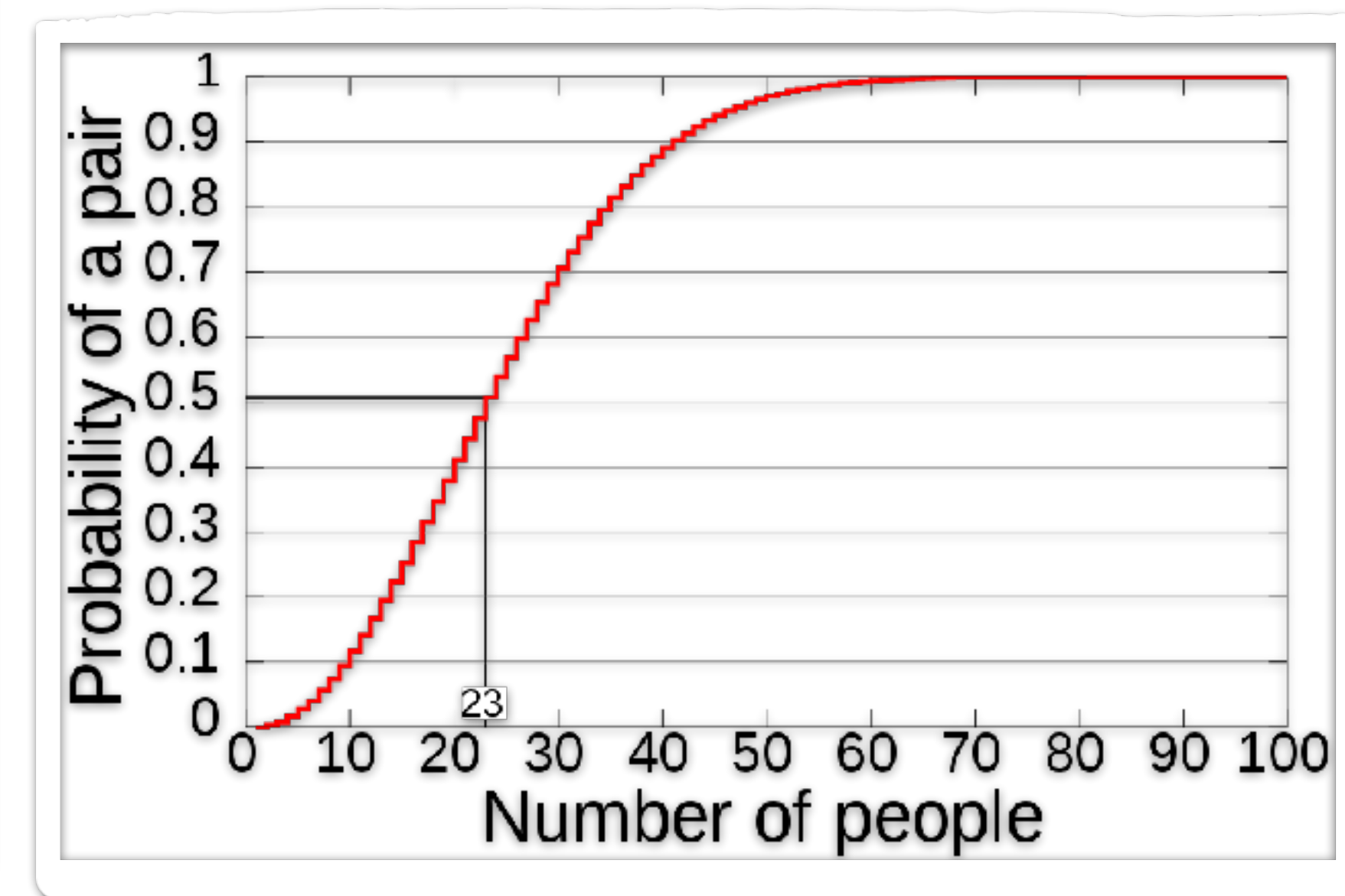
Egal welche Speicherplätze die ersten $i - 1$ Daten belegen, $m - i + 1$ der m Möglichkeiten sind *gut*.

Prob(n Daten kollisionsfrei) = $\frac{m-1}{m} \cdot \frac{m-2}{m} \dots \frac{m-n+1}{m}$

Beispiel: $m = 365$

Prob(23 Daten kollisionsfrei) ≈ 0.49

Prob(50 Daten kollisionsfrei) ≈ 0.03



Geburtstagsparadoxon (verallgemeinert)

Prob($2m^{1/2}$ Daten kollisionsfrei) =

$$\frac{m-1}{m} \cdots \frac{m-m^{1/2}}{m} \cdots \frac{m-2m^{1/2}+1}{m}$$
$$\leq 1 \cdot \left(\frac{m-m^{1/2}}{m} \right)^{m^{1/2}}$$

Geburtstagsparadoxon (verallgemeinert)

Prob($2m^{1/2}$ Daten kollisionsfrei) =

$$\frac{m-1}{m} \cdots \frac{m-m^{1/2}}{m} \cdots \frac{m-2m^{1/2}+1}{m}$$
$$\leq 1 \cdot \left(\frac{m-m^{1/2}}{m} \right)^{m^{1/2}} = \left(1 - \frac{1}{m^{1/2}} \right)^{m^{1/2}}$$

Geburtstagsparadoxon (verallgemeinert)

Prob($2m^{1/2}$ Daten kollisionsfrei) =

$$\frac{m-1}{m} \cdots \frac{m-m^{1/2}}{m} \cdots \frac{m-2m^{1/2}+1}{m}$$
$$\leq 1 \cdot \left(\frac{m-m^{1/2}}{m} \right)^{m^{1/2}} = \left(1 - \frac{1}{m^{1/2}} \right)^{m^{1/2}} \approx \frac{1}{e}$$

Geburtstagsparadoxon (verallgemeinert)

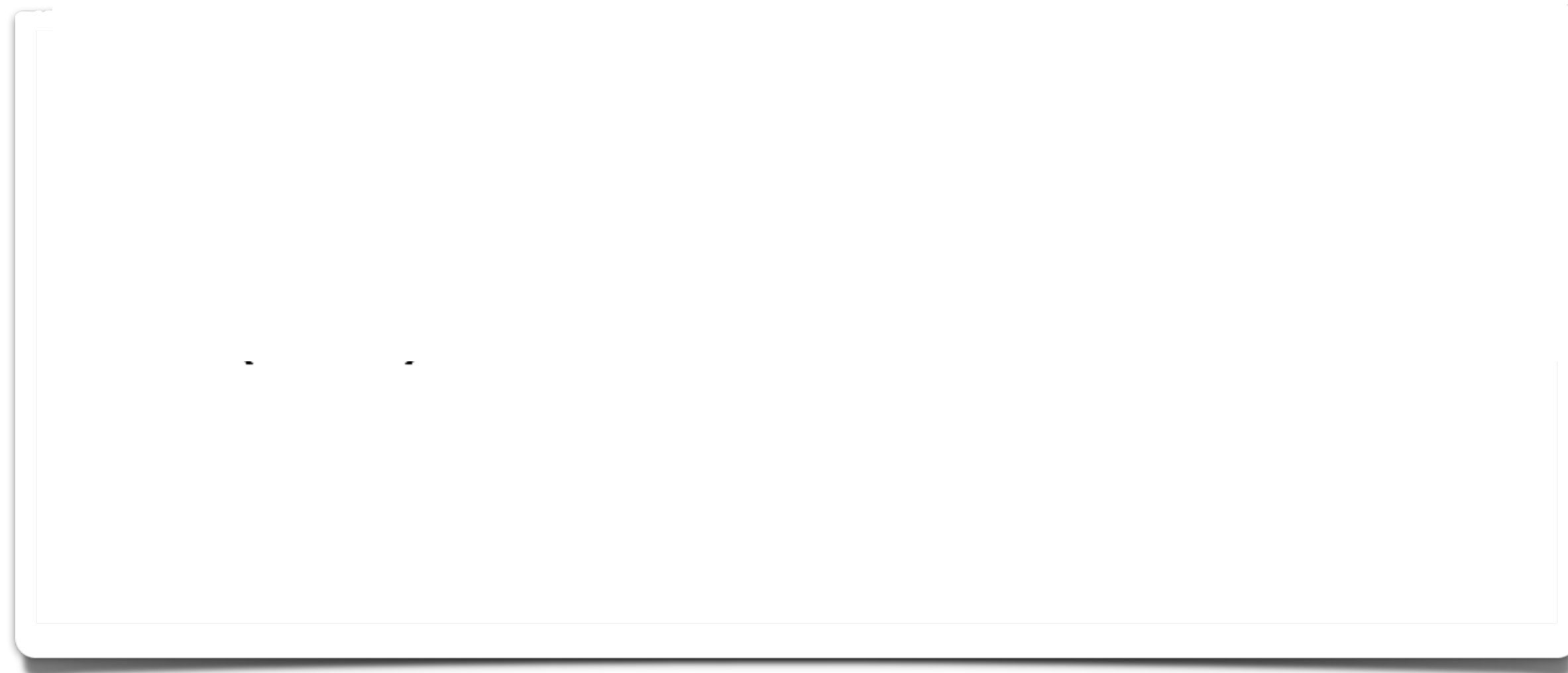
Prob($2m^{1/2}$ Daten kollisionsfrei) =

$$\frac{m-1}{m} \cdots \frac{m-m^{1/2}}{m} \cdots \frac{m-2m^{1/2}+1}{m}$$
$$\leq 1 \cdot \left(\frac{m-m^{1/2}}{m} \right)^{m^{1/2}} = \left(1 - \frac{1}{m^{1/2}} \right)^{m^{1/2}} \approx \frac{1}{e}$$

Hashing muss mit Kollisionen leben und benötigt Strategien zur Kollisionsbehandlung!

Kollisionbehandlung

Kollisionbehandlung



Kollisionbehandlung

Verschiedene Arten der Kollisionsbehandlung:

Kollisionbehandlung

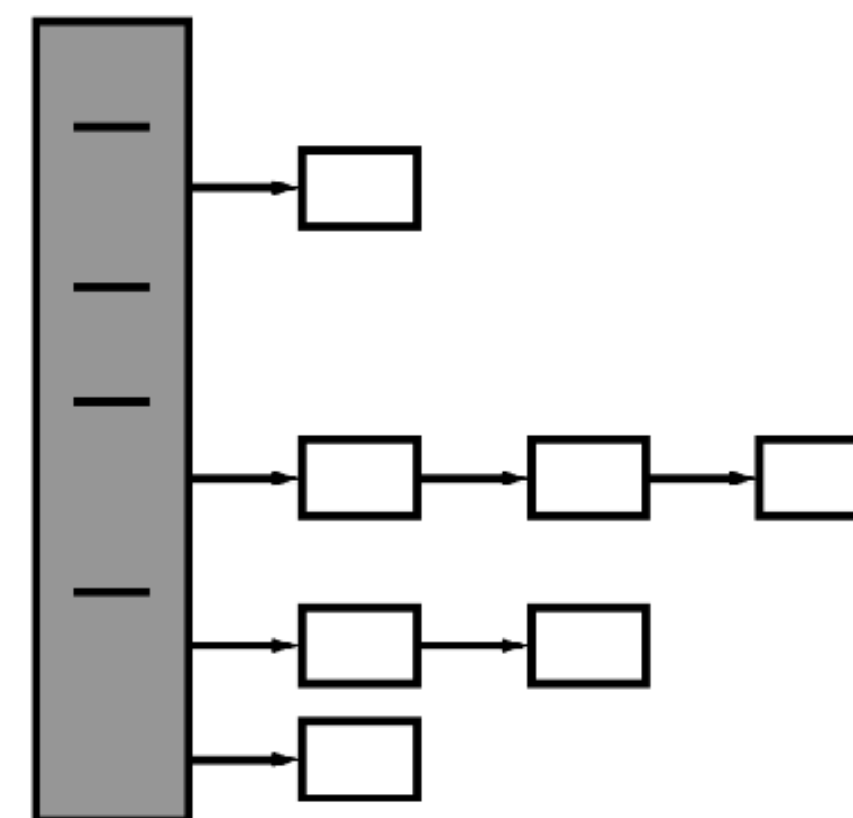
Verschiedene Arten der Kollisionsbehandlung:

- mittels verketteter Listen
(links)

Kollisionbehandlung

Verschiedene Arten der Kollisionsbehandlung:

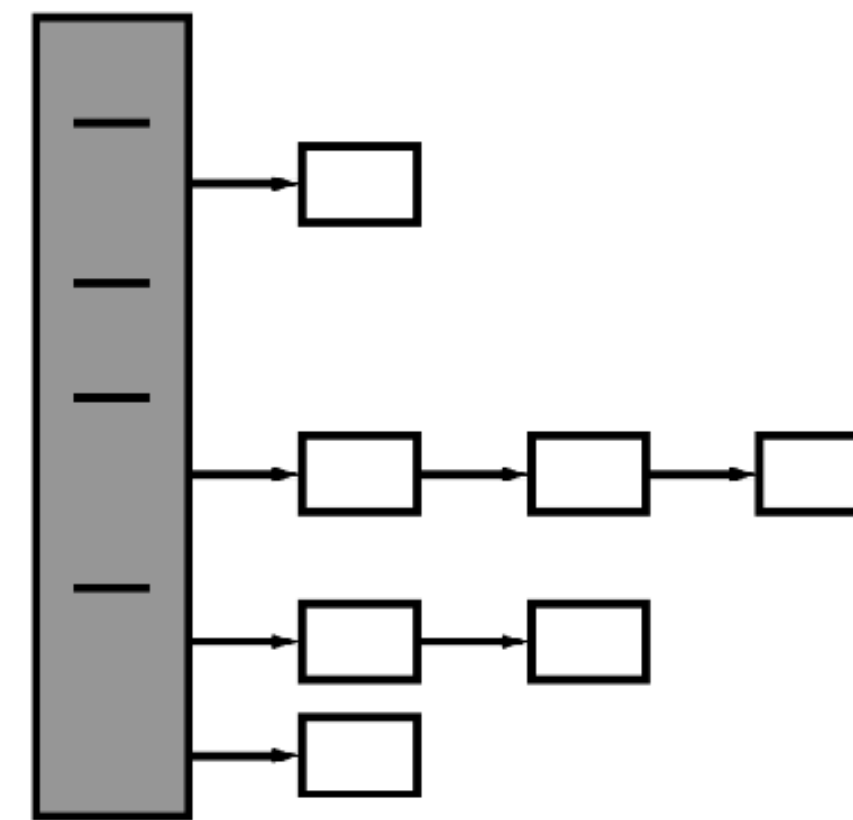
- mittels verketteter Listen
(links)



Kollisionbehandlung

Verschiedene Arten der Kollisionsbehandlung:

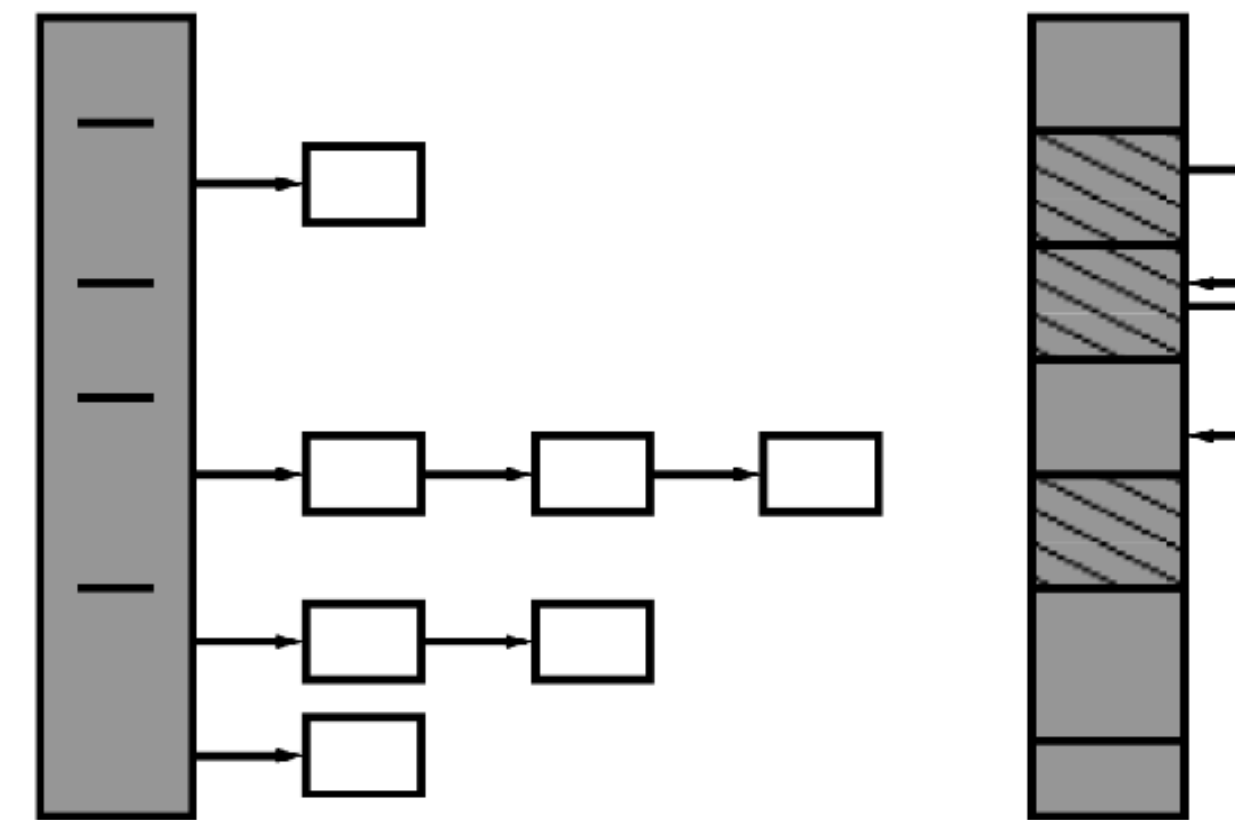
- mittels verketteter Listen
(links)
- mittels offener Adressierung
(rechts)



Kollisionbehandlung

Verschiedene Arten der Kollisionsbehandlung:

- mittels verketteter Listen
(links)
- mittels offener Adressierung
(rechts)



7.5 Verkettung von Überläufern

Analyse

Bei zufälligen Daten und ideal streuenden Hashfunktion gilt für

$$X_{ij} := \begin{cases} 1 & i\text{-tes Datum kommt in Liste } L(j) \\ 0 & \text{sonst} \end{cases}$$

$$\text{Prob}(X_{ij} = 1) = \frac{1}{m}$$

$$\rightarrow \text{E}(X_{ij}) = 1 \cdot \frac{1}{m} + 0 \cdot \frac{m-1}{m} = \frac{1}{m}$$

$X_j = X_{1j} + \dots + X_{nj}$ zählt Anzahl Daten in Liste $L(j)$.

$$\text{E}(X_j) = \text{E}(X_{1j} + \dots + X_{nj}) = \text{E}(X_{1j}) + \dots + \text{E}(X_{nj}) = \frac{n}{m}$$

Analyse

Bei zufälligen Daten und ideal streuenden Hashfunktion gilt für

$$X_{ij} := \begin{cases} 1 & i\text{-tes Datum kommt in Liste } L(j) \\ 0 & \text{sonst} \end{cases}$$

$$\text{Prob}(X_{ij} = 1) = \frac{1}{m}$$

$$\rightarrow \text{E}(X_{ij}) = 1 \cdot \frac{1}{m} + 0 \cdot \frac{m-1}{m} = \frac{1}{m}$$

$X_j = X_{1j} + \dots + X_{nj}$ zählt Anzahl Daten in Liste $L(j)$.

$$\text{E}(X_j) = \text{E}(X_{1j} + \dots + X_{nj}) = \text{E}(X_{1j}) + \dots + \text{E}(X_{nj}) = \frac{n}{m}$$

Analyse (2)

Analyse (2)

- Erfolgreiche Suche in Liste $L(j)$:

Inklusive nil-Zeiger durchschnittlich $1 + \frac{n}{m} = 1 + \beta$ Objekte betrachten

Beispiel: Für $n \approx 0.95 \cdot m$ ist dies ≈ 1.95 .

- Erfolgreiche Suche in Liste $L(j)$ der Länge ℓ :

Jede Position in der Liste hat Wahrscheinlichkeit $1/\ell$, also $\frac{1}{\ell}(1 + 2 + \dots + \ell) = \frac{\ell+1}{2}$.

Durchschnittliche Listenlänge hier: $1 + \frac{n-1}{m}$

(Liste enthält sicher das gesuchte Datum, und die anderen $n - 1$ Daten sind zufällig verteilt.)

Also erwartete Suchdauer $\frac{1}{2}(1 + \frac{n-1}{m} + 1) = 1 + \frac{n-1}{2m} \approx 1 + \frac{\beta}{2}$

Beispiel: Für $n \approx 0.95 \cdot m$ ist dies ≈ 1.475 .

Analyse (2)

- Erfolgreiche Suche in Liste $L(j)$:

Inklusive nil-Zeiger durchschnittlich $1 + \frac{n}{m} = 1 + \beta$ Objekte betrachten

Beispiel: Für $n \approx 0.95 \cdot m$ ist dies ≈ 1.95 .

- Erfolgreiche Suche in Liste $L(j)$ der Länge ℓ :

Jede Position in der Liste hat Wahrscheinlichkeit $1/\ell$, also $\frac{1}{\ell}(1 + 2 + \dots + \ell) = \frac{\ell+1}{2}$.

Durchschnittliche Listenlänge hier: $1 + \frac{n-1}{m}$

(Liste enthält sicher das gesuchte Datum, und die anderen $n - 1$ Daten sind zufällig verteilt.)

Also erwartete Suchdauer $\frac{1}{2}(1 + \frac{n-1}{m} + 1) = 1 + \frac{n-1}{2m} \approx 1 + \frac{\beta}{2}$

Beispiel: Für $n \approx 0.95 \cdot m$ ist dies ≈ 1.475 .

Analyse (2)

- Erfolgreiche Suche in Liste $L(j)$:

Inklusive nil-Zeiger durchschnittlich $1 + \frac{n}{m} = 1 + \beta$ Objekte betrachten

Beispiel: Für $n \approx 0.95 \cdot m$ ist dies ≈ 1.95 .

- Erfolgreiche Suche in Liste $L(j)$ der Länge ℓ :

Jede Position in der Liste hat Wahrscheinlichkeit $1/\ell$, also $\frac{1}{\ell}(1 + 2 + \dots + \ell) = \frac{\ell+1}{2}$.

Durchschnittliche Listenlänge hier: $1 + \frac{n-1}{m}$

(Liste enthält sicher das gesuchte Datum, und die anderen $n - 1$ Daten sind zufällig verteilt.)

Also erwartete Suchdauer $\frac{1}{2}(1 + \frac{n-1}{m} + 1) = 1 + \frac{n-1}{2m} \approx 1 + \frac{\beta}{2}$

Beispiel: Für $n \approx 0.95 \cdot m$ ist dies ≈ 1.475 .

7.6 Offene Adressierung

Anforderungen

Anforderungen

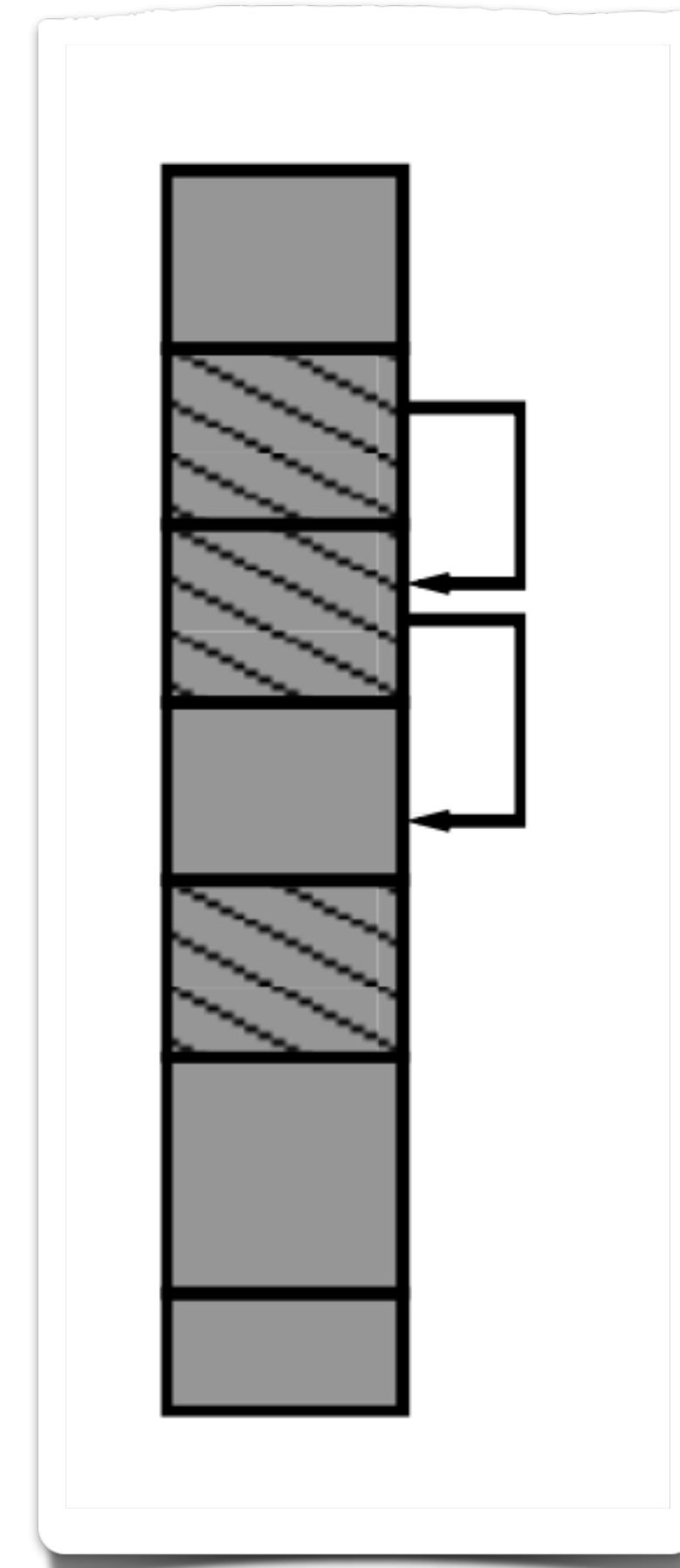
Zur Erinnerung:

Im Kollisionsfall nach fester Regel alternativen freien Platz in Hashtabelle suchen (**Sondierungsfolge**).

Anforderungen

Zur Erinnerung:

Im Kollisionsfall nach fester Regel alternativen freien Platz in Hashtabelle suchen (**Sondierungsfolge**).

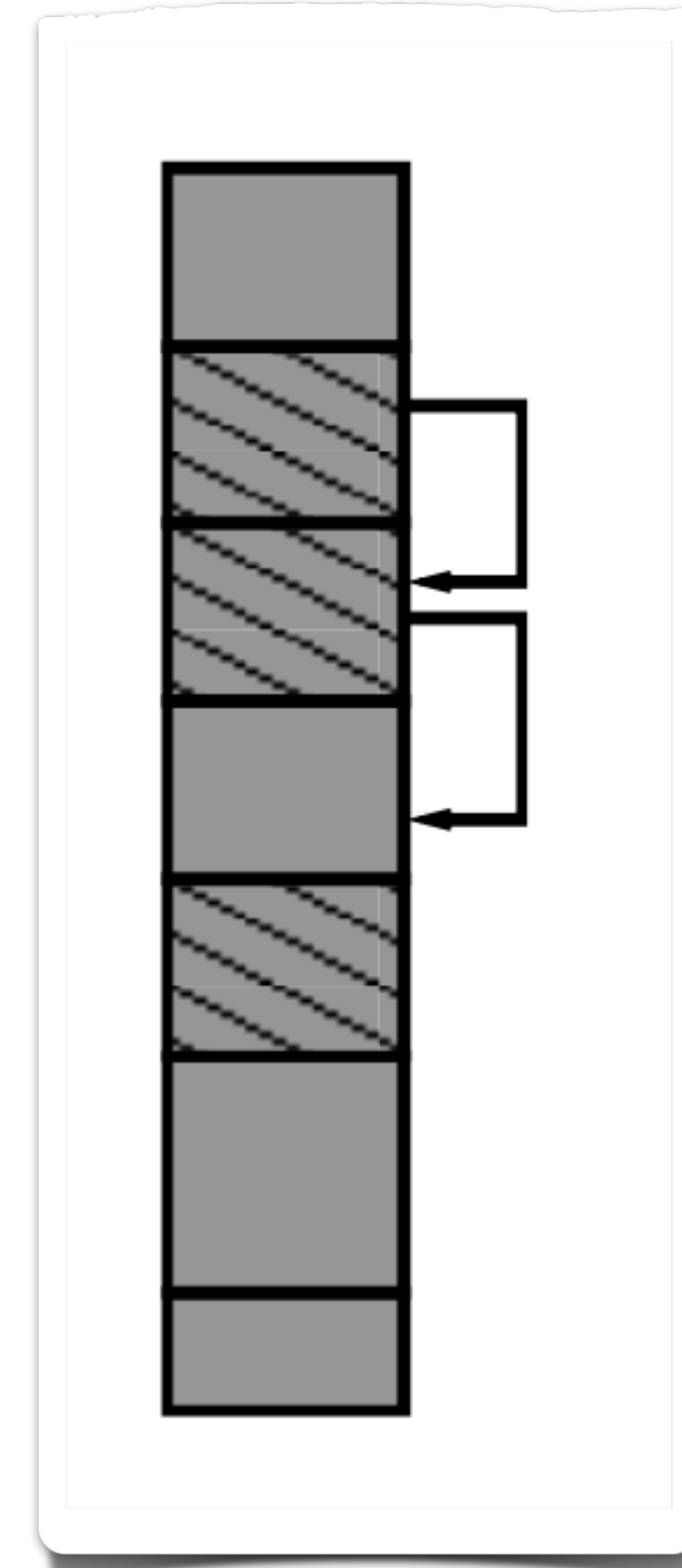


Anforderungen

Zur Erinnerung:

Im Kollisionsfall nach fester Regel alternativen freien Platz in Hashtabelle suchen (**Sondierungsfolge**).

Voraussetzung: Auswertung von h gilt als eine Operation.



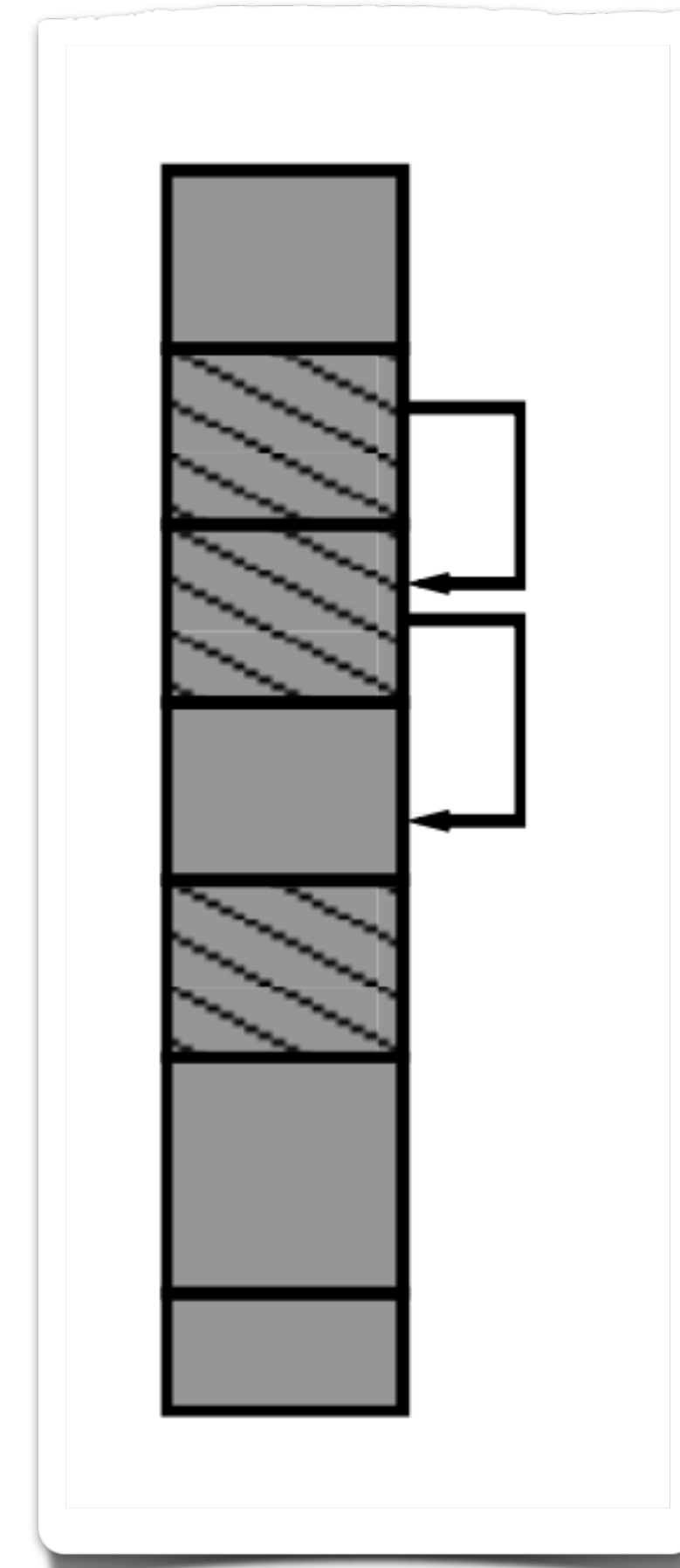
Anforderungen

Zur Erinnerung:

Im Kollisionsfall nach fester Regel alternativen freien Platz in Hashtabelle suchen (**Sondierungsfolge**).

Voraussetzung: Auswertung von h gilt als eine Operation.

$t(i, j) :=$ Position des i -ten Versuchs zum Einfügen von Daten x
mit $h(x) = j$



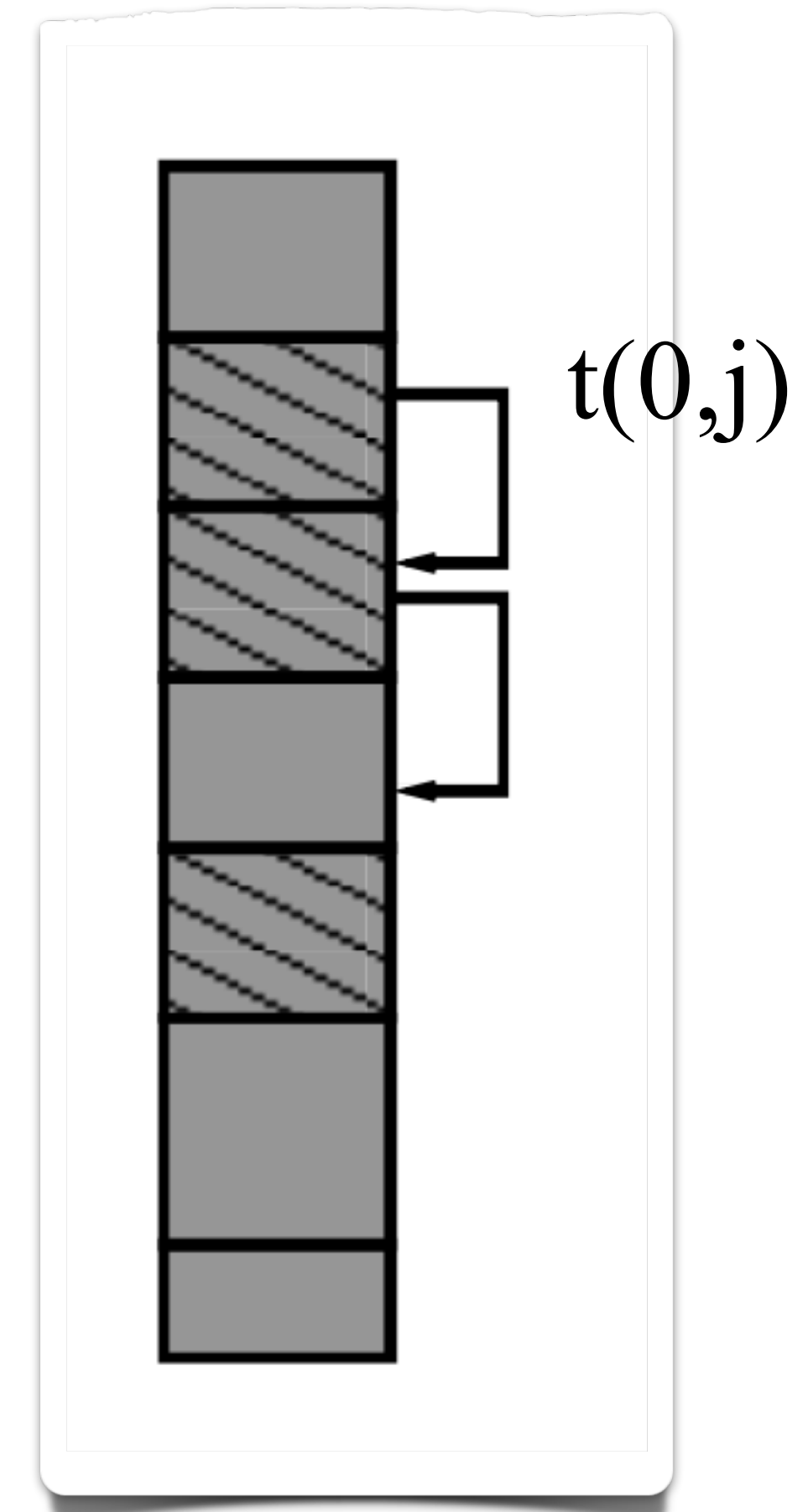
Anforderungen

Zur Erinnerung:

Im Kollisionsfall nach fester Regel alternativen freien Platz in Hashtabelle suchen (**Sondierungsfolge**).

Voraussetzung: Auswertung von h gilt als eine Operation.

$t(i, j) :=$ Position des i -ten Versuchs zum Einfügen von Daten x mit $h(x) = j$



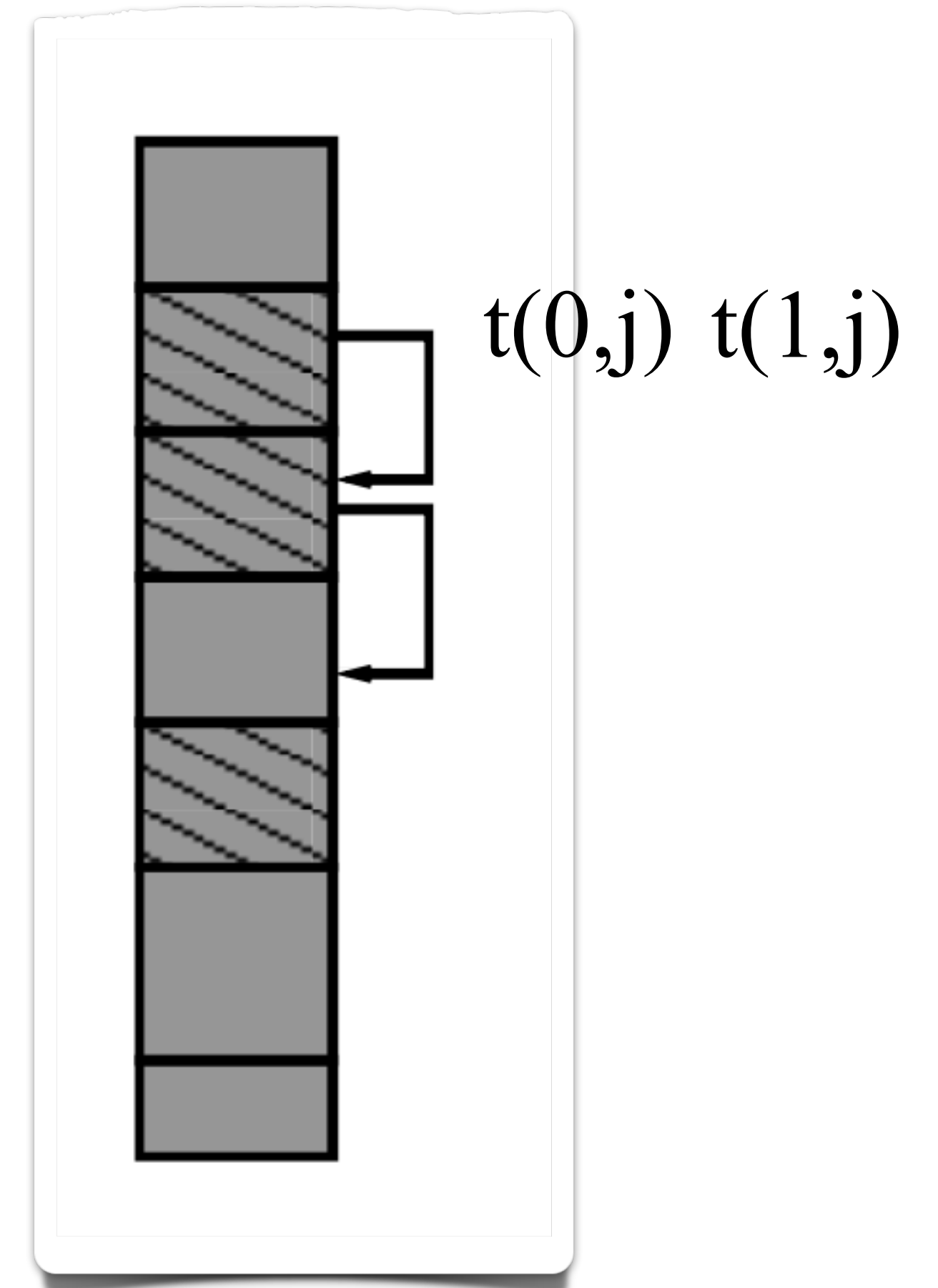
Anforderungen

Zur Erinnerung:

Im Kollisionsfall nach fester Regel alternativen freien Platz in Hashtabelle suchen (**Sondierungsfolge**).

Voraussetzung: Auswertung von h gilt als eine Operation.

$t(i, j) :=$ Position des i -ten Versuchs zum Einfügen von Daten x
mit $h(x) = j$



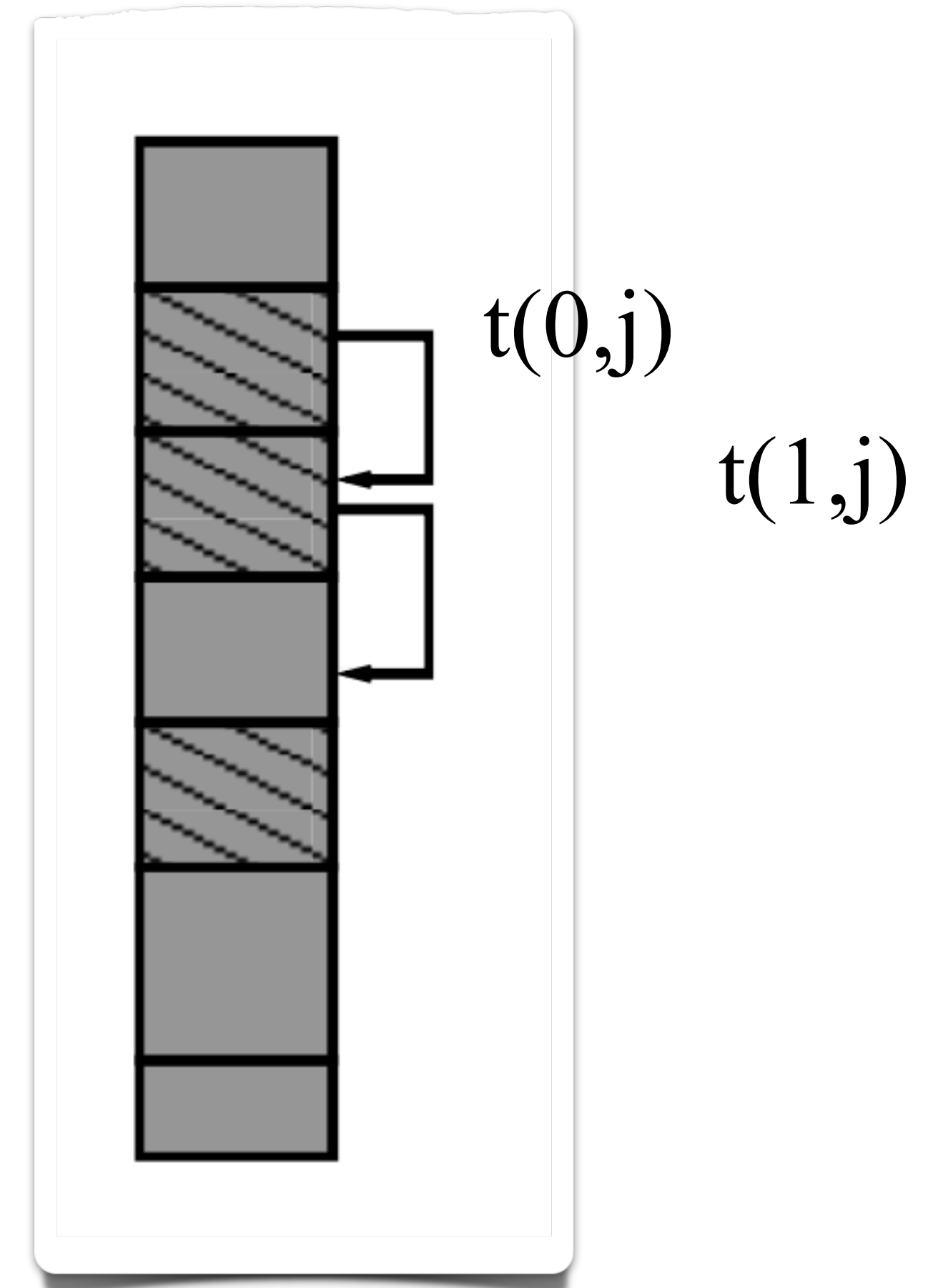
Anforderungen

Zur Erinnerung:

Im Kollisionsfall nach fester Regel alternativen freien Platz in Hashtabelle suchen (**Sondierungsfolge**).

Voraussetzung: Auswertung von h gilt als eine Operation.

$t(i, j) :=$ Position des i -ten Versuchs zum Einfügen von Daten x
mit $h(x) = j$



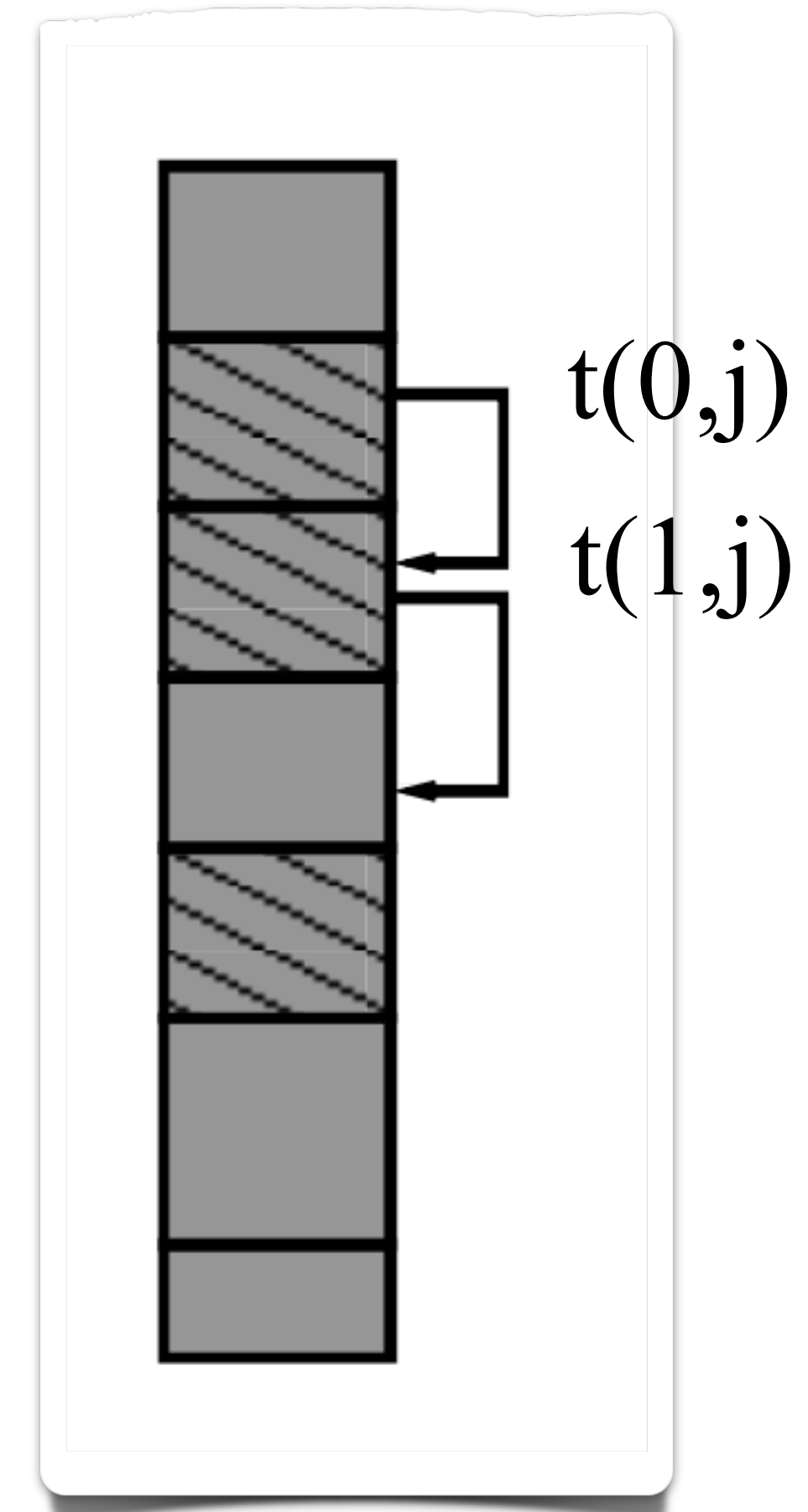
Anforderungen

Zur Erinnerung:

Im Kollisionsfall nach fester Regel alternativen freien Platz in Hashtabelle suchen (**Sondierungsfolge**).

Voraussetzung: Auswertung von h gilt als eine Operation.

$t(i, j) :=$ Position des i -ten Versuchs zum Einfügen von Daten x
mit $h(x) = j$



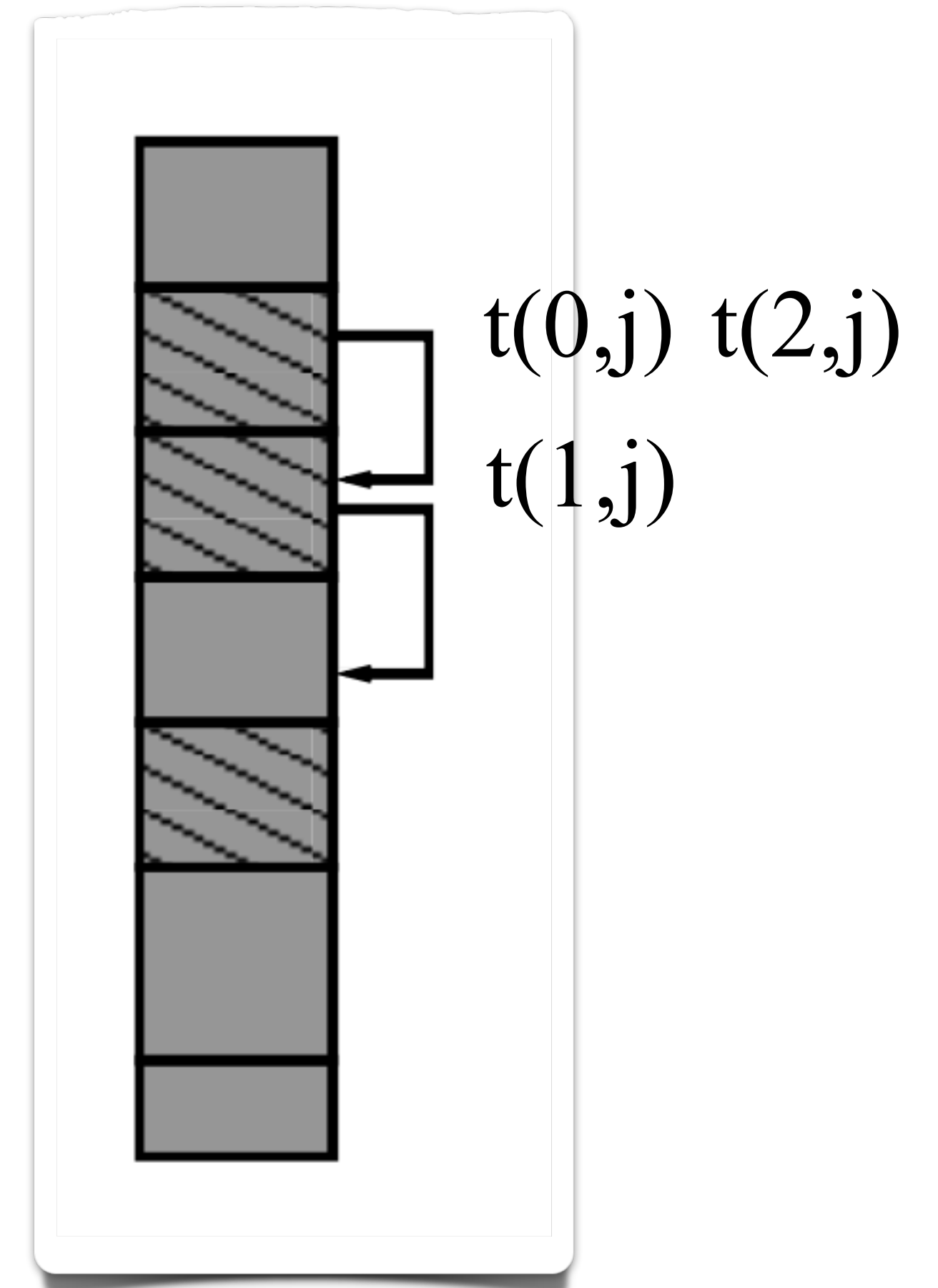
Anforderungen

Zur Erinnerung:

Im Kollisionsfall nach fester Regel alternativen freien Platz in Hashtabelle suchen (**Sondierungsfolge**).

Voraussetzung: Auswertung von h gilt als eine Operation.

$t(i, j) :=$ Position des i -ten Versuchs zum Einfügen von Daten x
mit $h(x) = j$



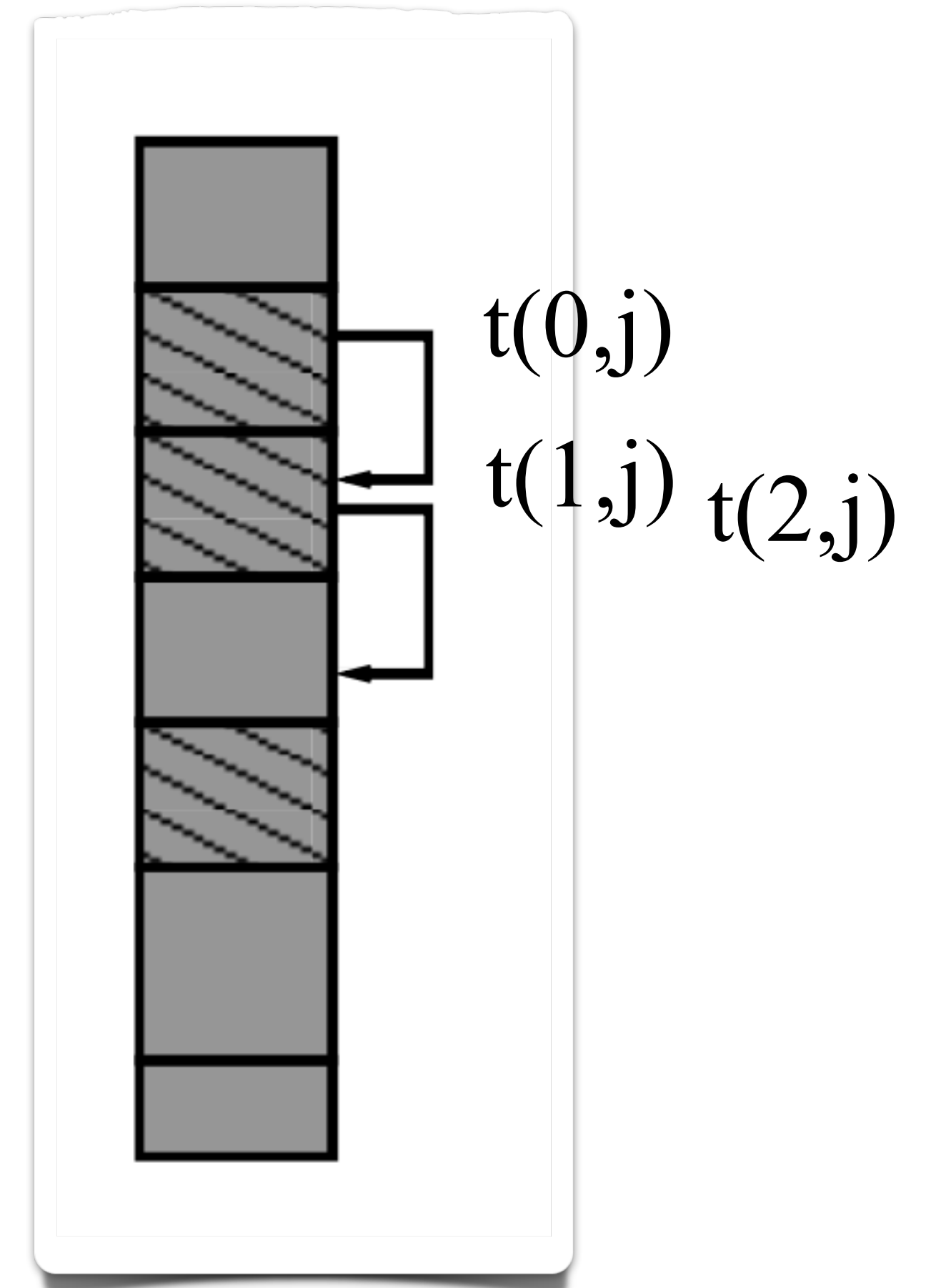
Anforderungen

Zur Erinnerung:

Im Kollisionsfall nach fester Regel alternativen freien Platz in Hashtabelle suchen (**Sondierungsfolge**).

Voraussetzung: Auswertung von h gilt als eine Operation.

$t(i, j) :=$ Position des i -ten Versuchs zum Einfügen von Daten x
mit $h(x) = j$



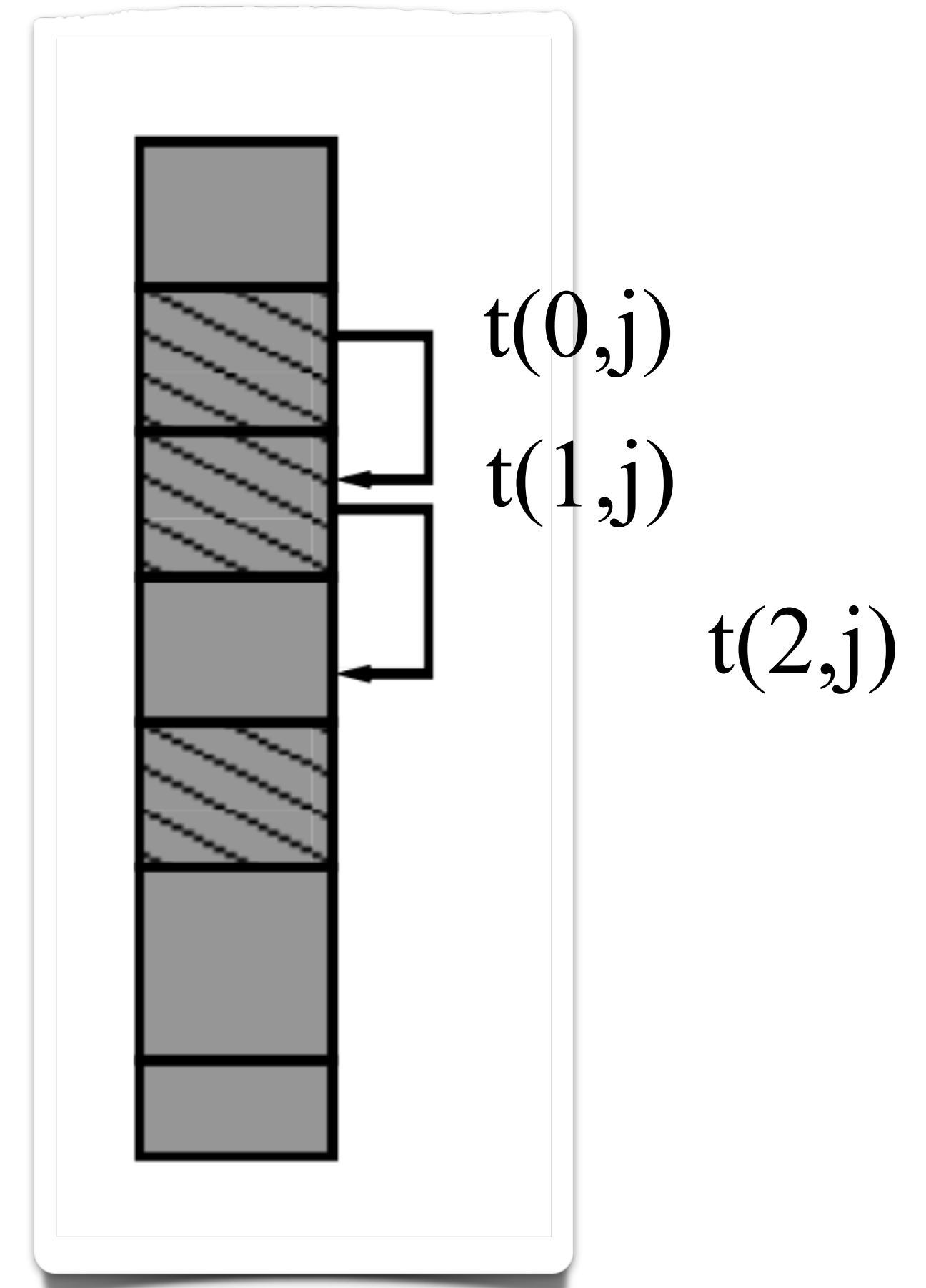
Anforderungen

Zur Erinnerung:

Im Kollisionsfall nach fester Regel alternativen freien Platz in Hashtabelle suchen (**Sondierungsfolge**).

Voraussetzung: Auswertung von h gilt als eine Operation.

$t(i, j) :=$ Position des i -ten Versuchs zum Einfügen von Daten x
mit $h(x) = j$



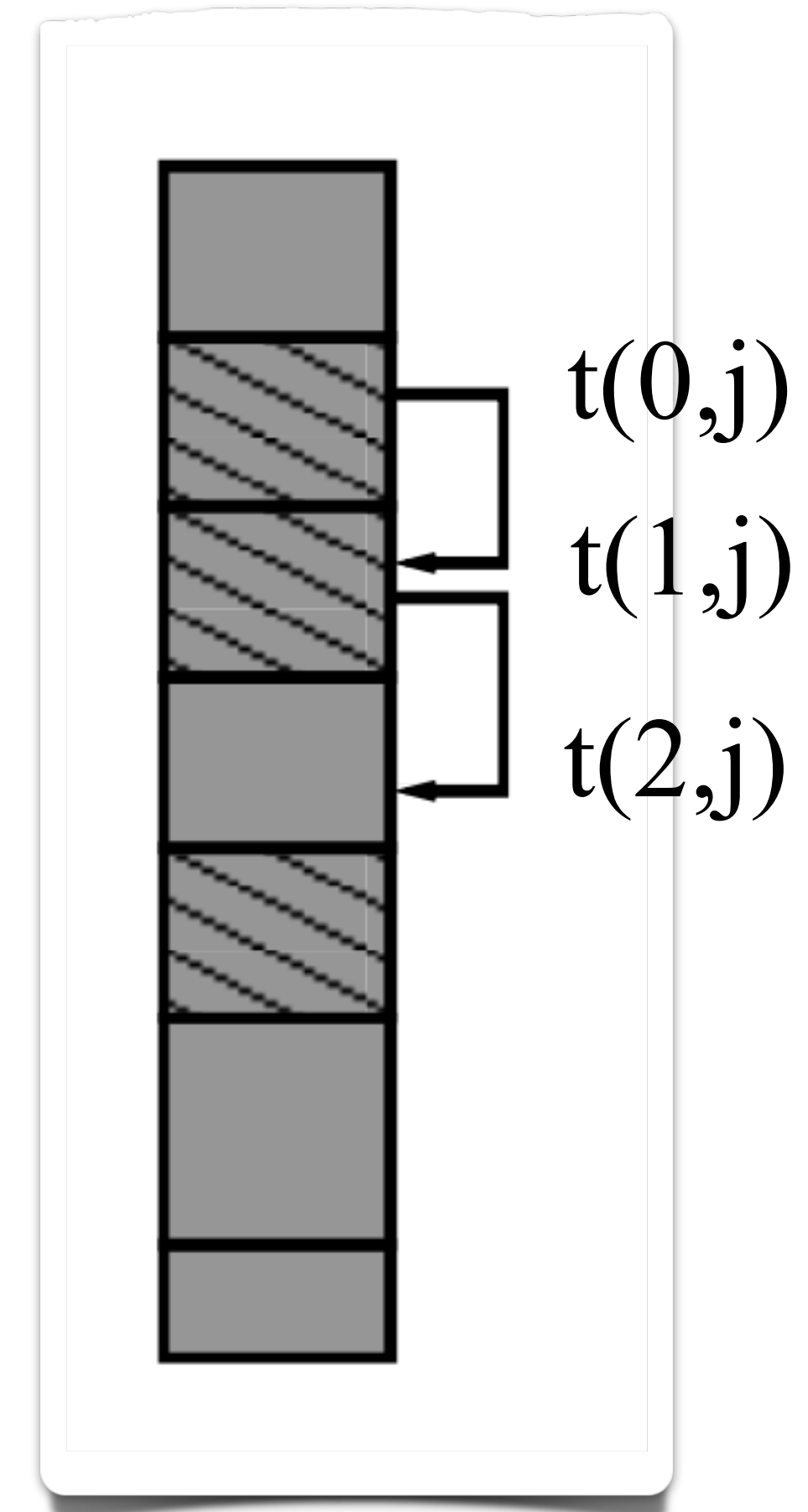
Anforderungen

Zur Erinnerung:

Im Kollisionsfall nach fester Regel alternativen freien Platz in Hashtabelle suchen (**Sondierungsfolge**).

Voraussetzung: Auswertung von h gilt als eine Operation.

$t(i, j) :=$ Position des i -ten Versuchs zum Einfügen von Daten x
mit $h(x) = j$



Anforderungen

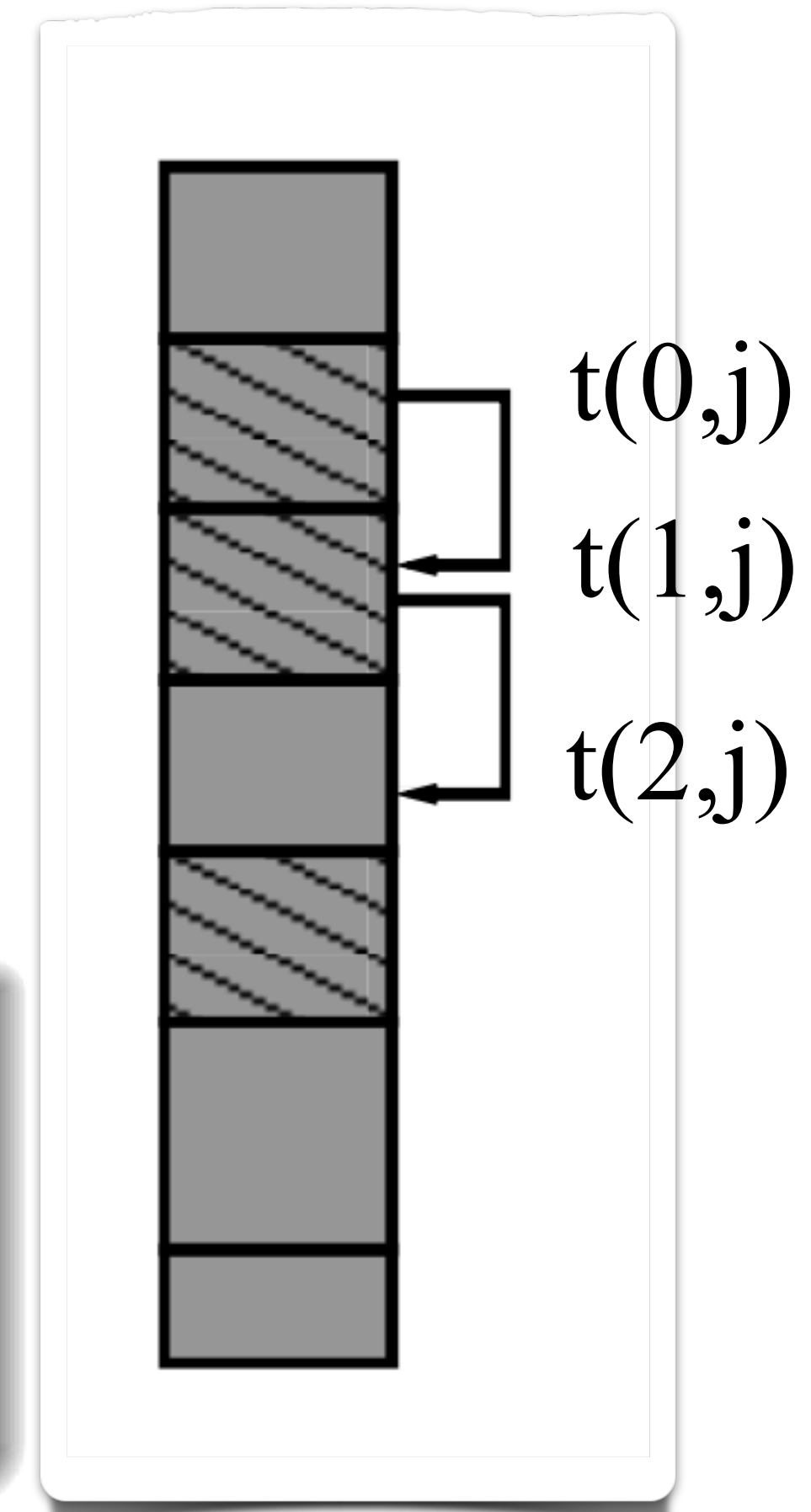
Zur Erinnerung:

Im Kollisionsfall nach fester Regel alternativen freien Platz in Hashtabelle suchen (**Sondierungsfolge**).

Voraussetzung: Auswertung von h gilt als eine Operation.

$t(i, j) :=$ Position des i -ten Versuchs zum Einfügen von Daten x
mit $h(x) = j$

Anforderung an Funktion t :



Anforderungen

Zur Erinnerung:

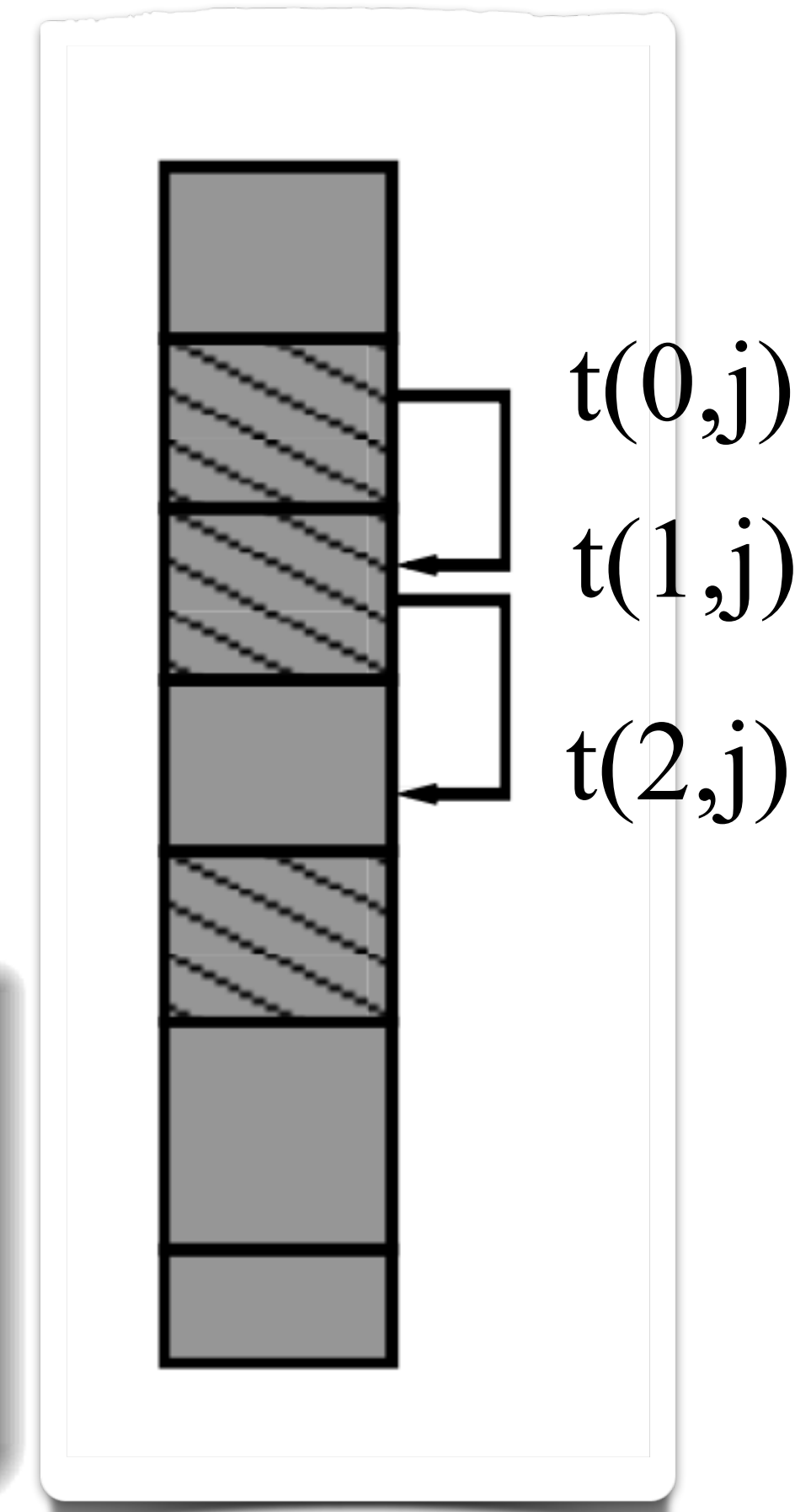
Im Kollisionsfall nach fester Regel alternativen freien Platz in Hashtabelle suchen (**Sondierungsfolge**).

Voraussetzung: Auswertung von h gilt als eine Operation.

$t(i, j) :=$ Position des i -ten Versuchs zum Einfügen von Daten x
mit $h(x) = j$

Anforderung an Funktion t :

- auch t in Zeit $O(1)$ berechenbar



Anforderungen

Zur Erinnerung:

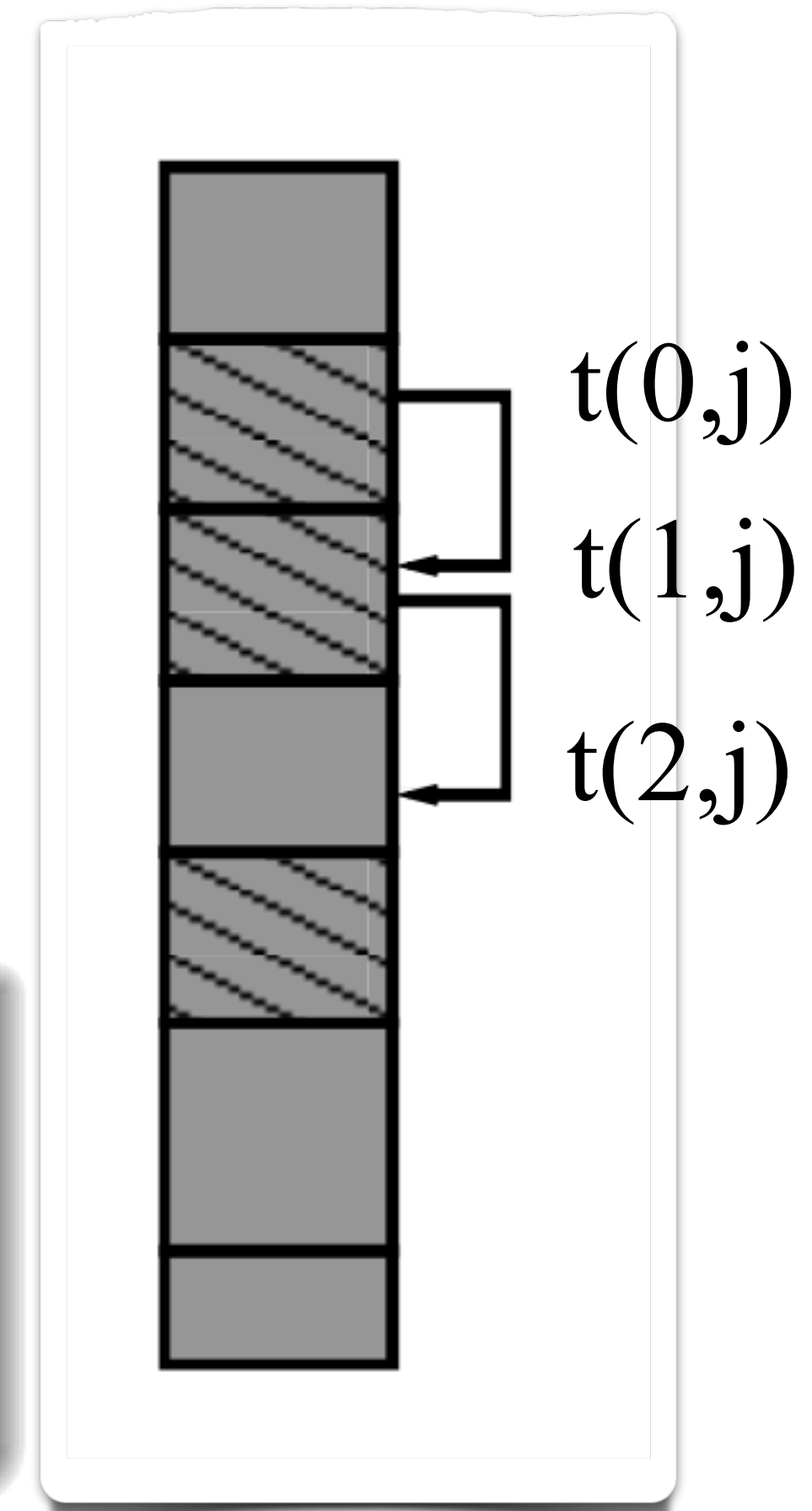
Im Kollisionsfall nach fester Regel alternativen freien Platz in Hashtabelle suchen (**Sondierungsfolge**).

Voraussetzung: Auswertung von h gilt als eine Operation.

$t(i, j) :=$ Position des i -ten Versuchs zum Einfügen von Daten x
mit $h(x) = j$

Anforderung an Funktion t :

- auch t in Zeit $O(1)$ berechenbar
- $t(0, j) = j$



Anforderungen

Zur Erinnerung:

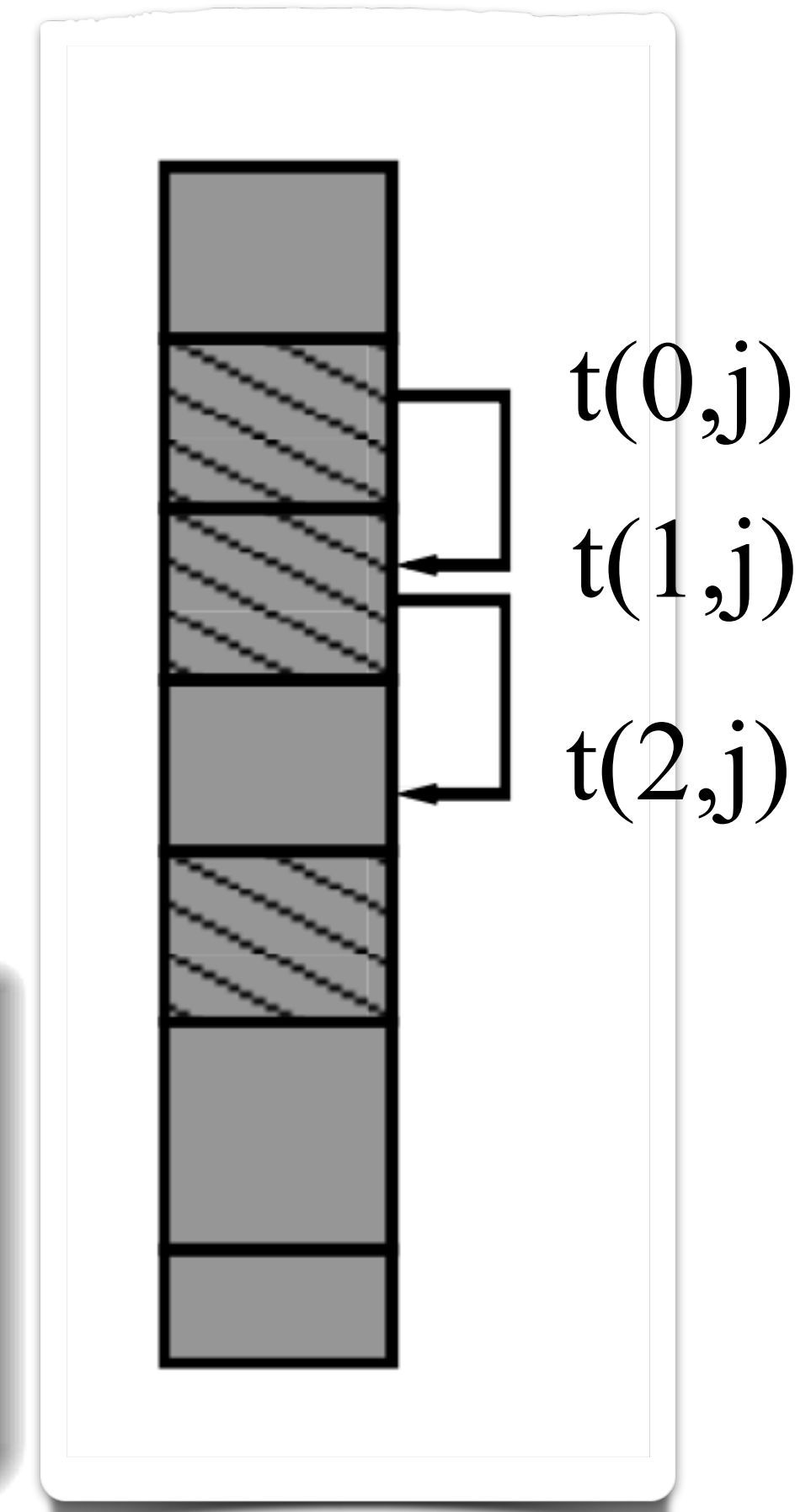
Im Kollisionsfall nach fester Regel alternativen freien Platz in Hashtabelle suchen (**Sondierungsfolge**).

Voraussetzung: Auswertung von h gilt als eine Operation.

$t(i, j) :=$ Position des i -ten Versuchs zum Einfügen von Daten x
mit $h(x) = j$

Anforderung an Funktion t :

- auch t in Zeit $O(1)$ berechenbar
- $t(0, j) = j$
- $t(\cdot, j) : \{0, \dots, m - 1\} \rightarrow \{0, \dots, m - 1\}$ bijektiv



Operationen

Operationen

- $\text{search}(x)$:
 - Berechne $j := h(x)$.
 - Suche x an den Positionen $t(0, j), \dots, t(m-1, j)$.
 - Abbruch, wenn x gefunden oder freie Stelle entdeckt (kein Datum mit Schlüssel x).
- $\text{insert}(x)$ nach erfolgloser Suche:
 - Freien Platz finden (sonst Overflow) und x dort einfügen.
- $\text{delete}(x)$ nach erfolgreicher Suche:
 - Das Datum kann nicht einfach entfernt werden, da search frühzeitig Lücken finden würde und eine Suche fälschlicherweise als erfolglos abbrechen könnte.

Löschen?!

Löschen?!

Problem: Datum kann bei Operation `delete(x)` nicht ohne weiteres gelöscht werden.

Löschen?!

Problem: Datum kann bei Operation `delete(x)` nicht ohne weiteres gelöscht werden.

Ausweg: Speicherplatz/Position als `besetzt`, `noch nie besetzt` oder `wieder frei` markieren.

Löschen?!

Problem: Datum kann bei Operation `delete(x)` nicht ohne weiteres gelöscht werden.

Ausweg: Speicherplatz/Position als `besetzt`, `noch nie besetzt` oder `wieder frei` markieren.

→ Suche wird nur an Positionen mit Markierung `noch nie besetzt` vorzeitig abgebrochen.

Löschen?!

Problem: Datum kann bei Operation `delete(x)` nicht ohne weiteres gelöscht werden.

Ausweg: Speicherplatz/Position als `besetzt`, `noch nie besetzt` oder `wieder frei` markieren.

→ Suche wird nur an Positionen mit Markierung `noch nie besetzt` vorzeitig abgebrochen.

Problem: Im Laufe der Zeit keine Position mehr, die mit `noch nie besetzt` markiert ist.

Löschen?!

Problem: Datum kann bei Operation `delete(x)` nicht ohne weiteres gelöscht werden.

Ausweg: Speicherplatz/Position als `besetzt`, `noch nie besetzt` oder `wieder frei` markieren.

→ Suche wird nur an Positionen mit Markierung `noch nie besetzt` vorzeitig abgebrochen.

Problem: Im Laufe der Zeit keine Position mehr, die mit `noch nie besetzt` markiert ist.

→ Hashing wird ineffizient.

Löschen?!

Problem: Datum kann bei Operation `delete(x)` nicht ohne weiteres gelöscht werden.

Ausweg: Speicherplatz/Position als `besetzt`, `noch nie besetzt` oder `wieder frei` markieren.

→ Suche wird nur an Positionen mit Markierung `noch nie besetzt` vorzeitig abgebrochen.

Problem: Im Laufe der Zeit keine Position mehr, die mit `noch nie besetzt` markiert ist.

→ Hashing wird ineffizient.

Offenes Hashing nur bei Anwendungen mit `search` und `insert`.

Sondieren

Sondieren

- Lineares Sondieren

Sondieren

- Lineares Sondieren
- Quadratisches Sondieren

Sondieren

- Lineares Sondieren
- Quadratisches Sondieren
- Multiplikatives Sondieren

Sondieren

- Lineares Sondieren
- Quadratisches Sondieren
- Multiplikatives Sondieren
- Doppeltes Hashing

Sondieren

- Lineares Sondieren
- Quadratisches Sondieren
- Multiplikatives Sondieren
- Doppeltes Hashing

Hilfsmittel bei der Analyse: **ideales Hashing**

Lineares Sondieren

Lineares Sondieren

$$t(i, j) := (i + j) \bmod m$$

Lineares Sondieren

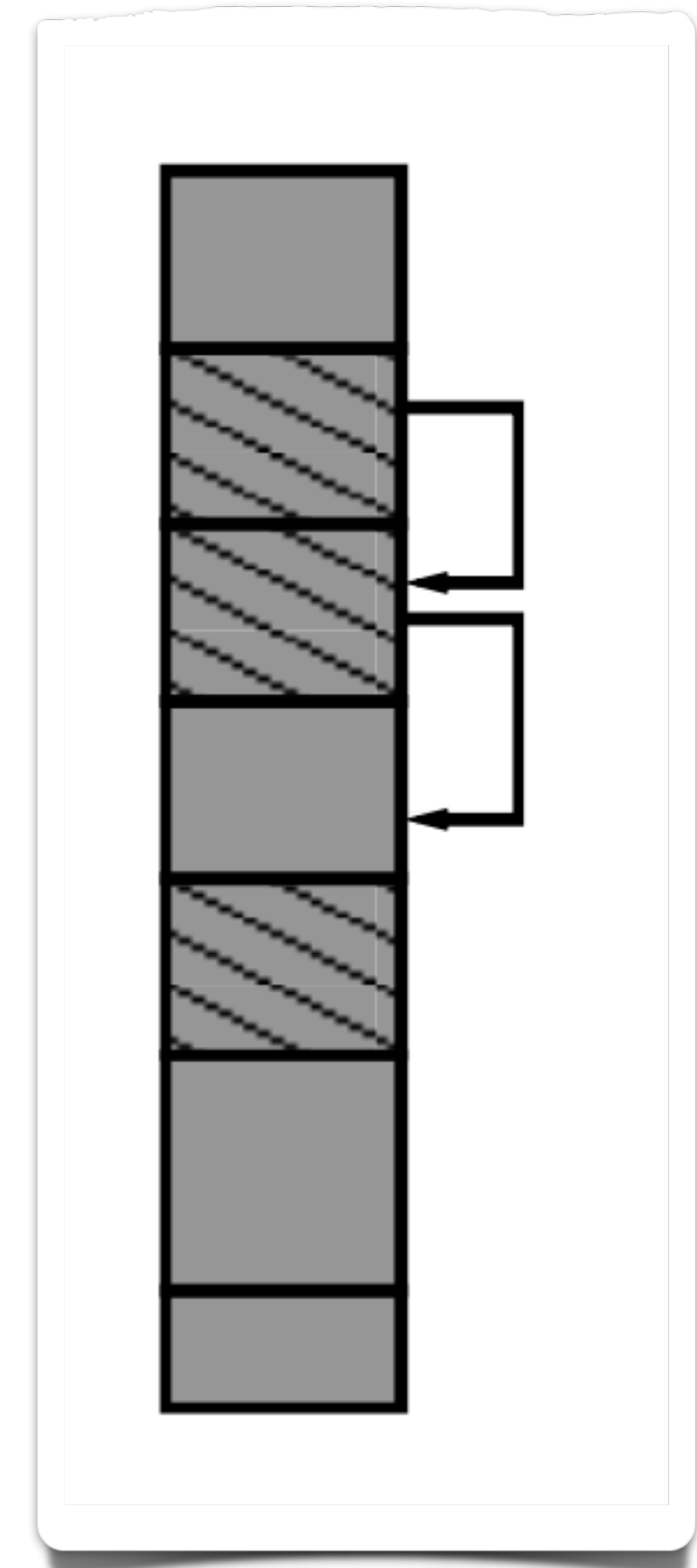
$$t(i, j) := (i + j) \bmod m$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Lineares Sondieren

$$t(i, j) := (i + j) \bmod m$$

Beispiel: $m = 19$ und $j = h(x) = 7$

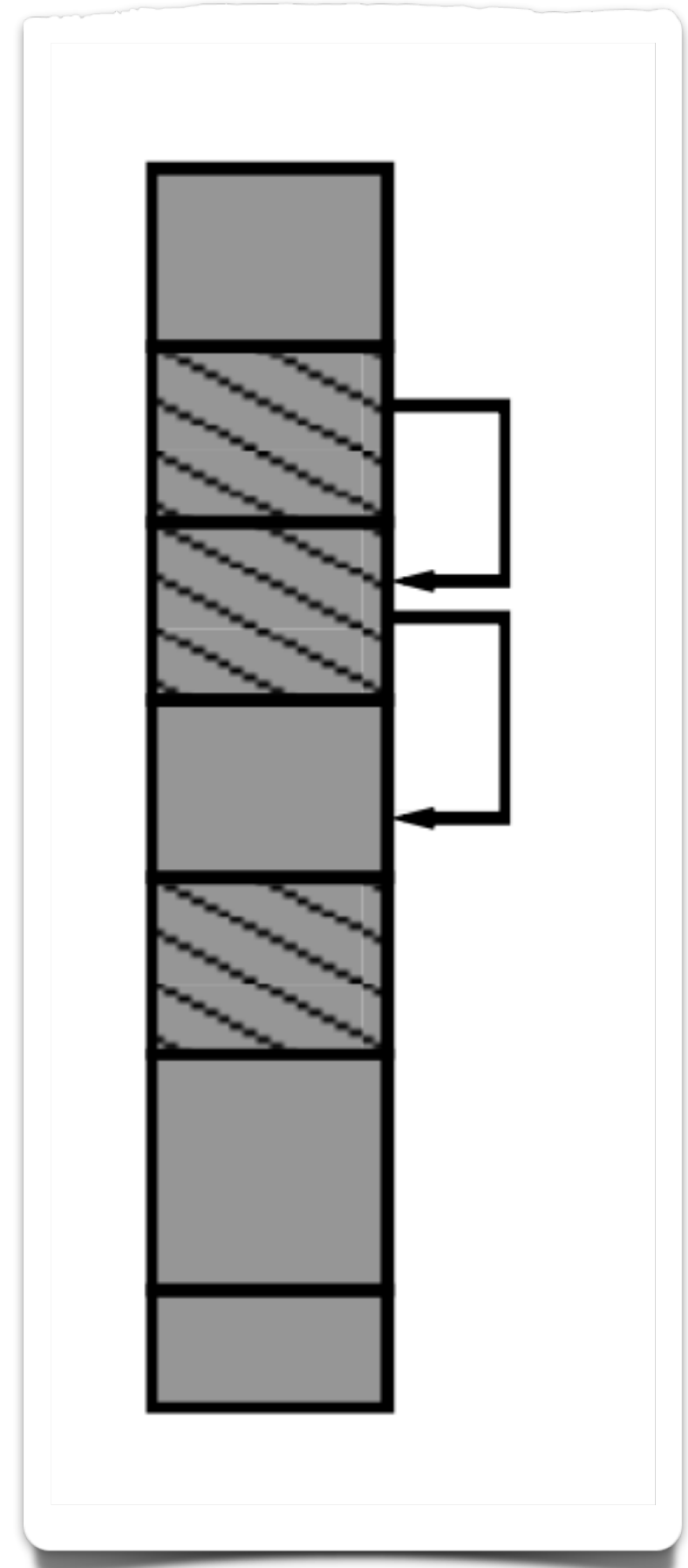


Lineares Sondieren

$$t(i, j) := (i + j) \bmod m$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:



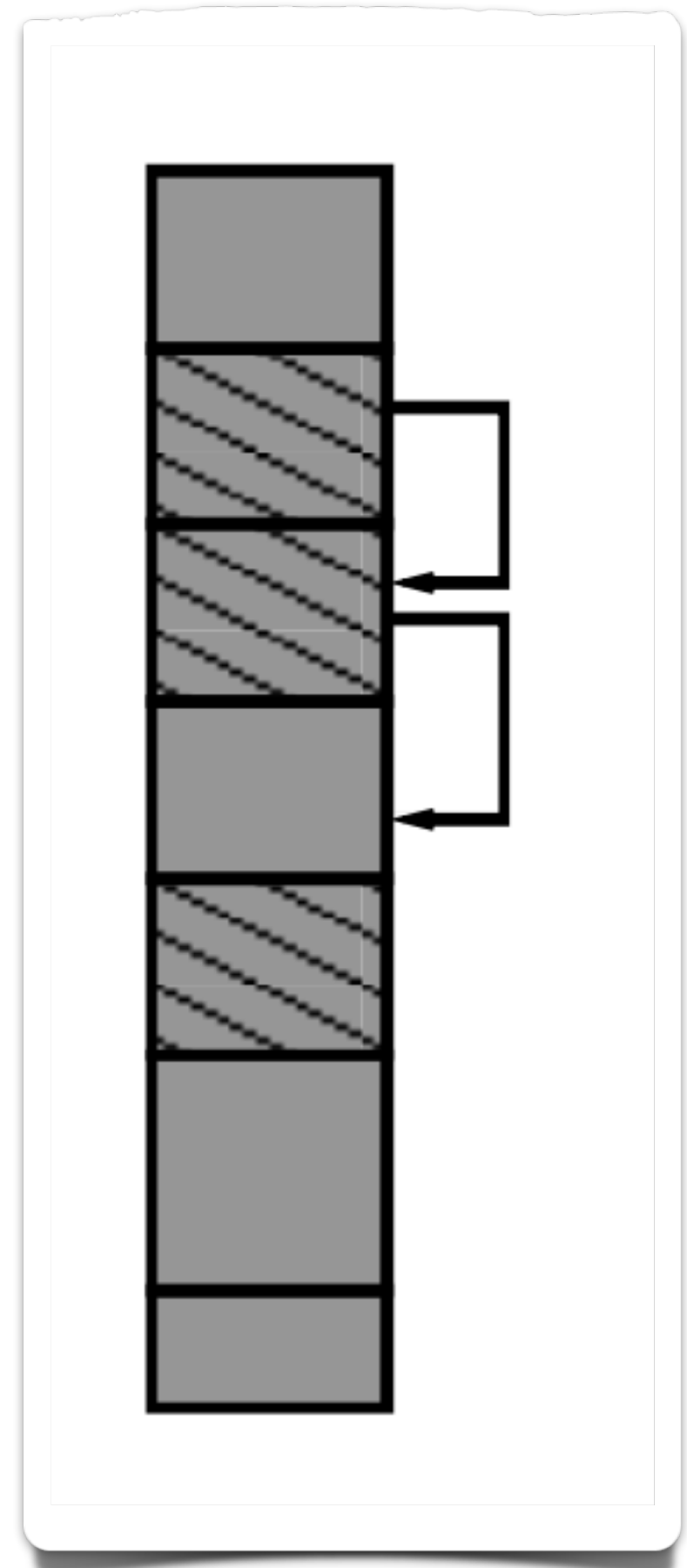
Lineares Sondieren

$$t(i, j) := (i + j) \bmod m$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 0, 1, 2, 3, 4, 5, 6



Lineares Sondieren

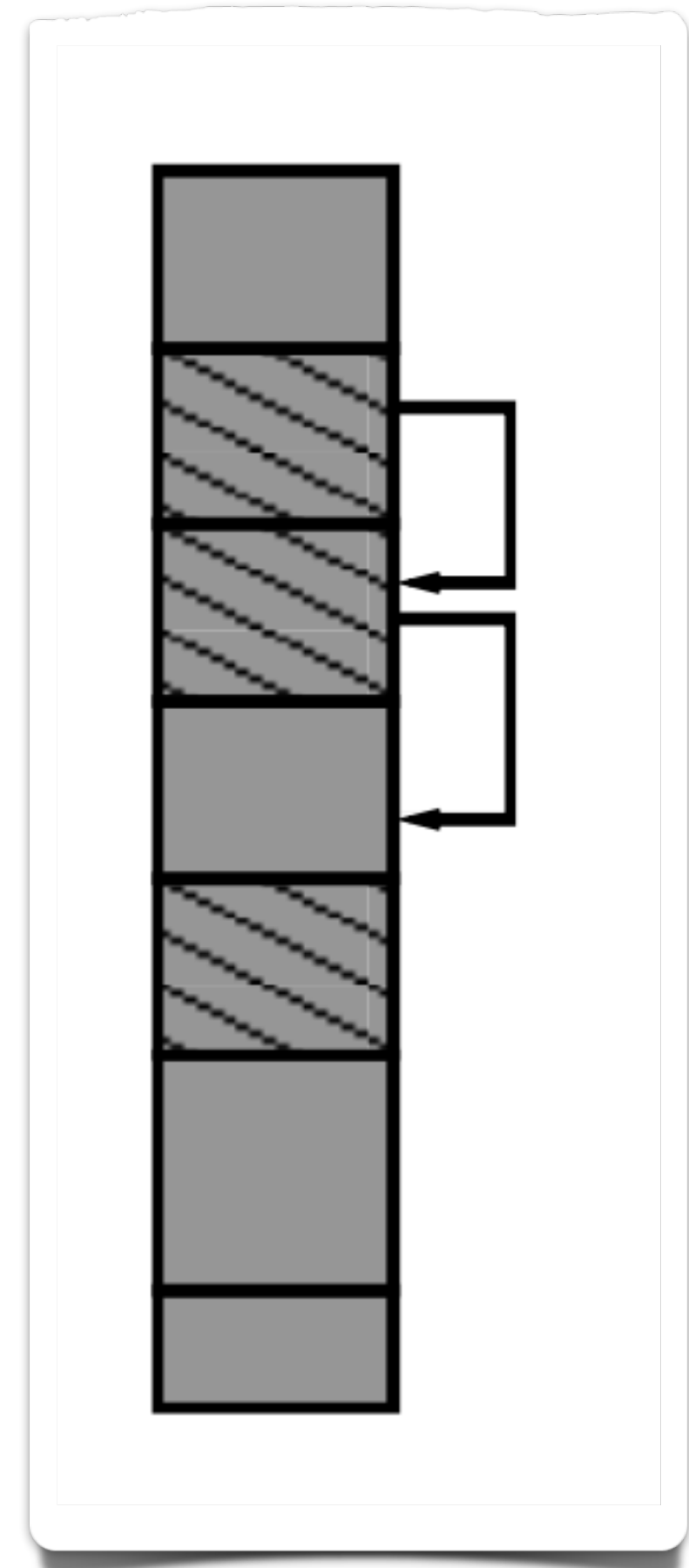
$$t(i, j) := (i + j) \bmod m$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 0, 1, 2, 3, 4, 5, 6

Problem: *Clusterbildung*



Lineares Sondieren

$$t(i, j) := (i + j) \bmod m$$

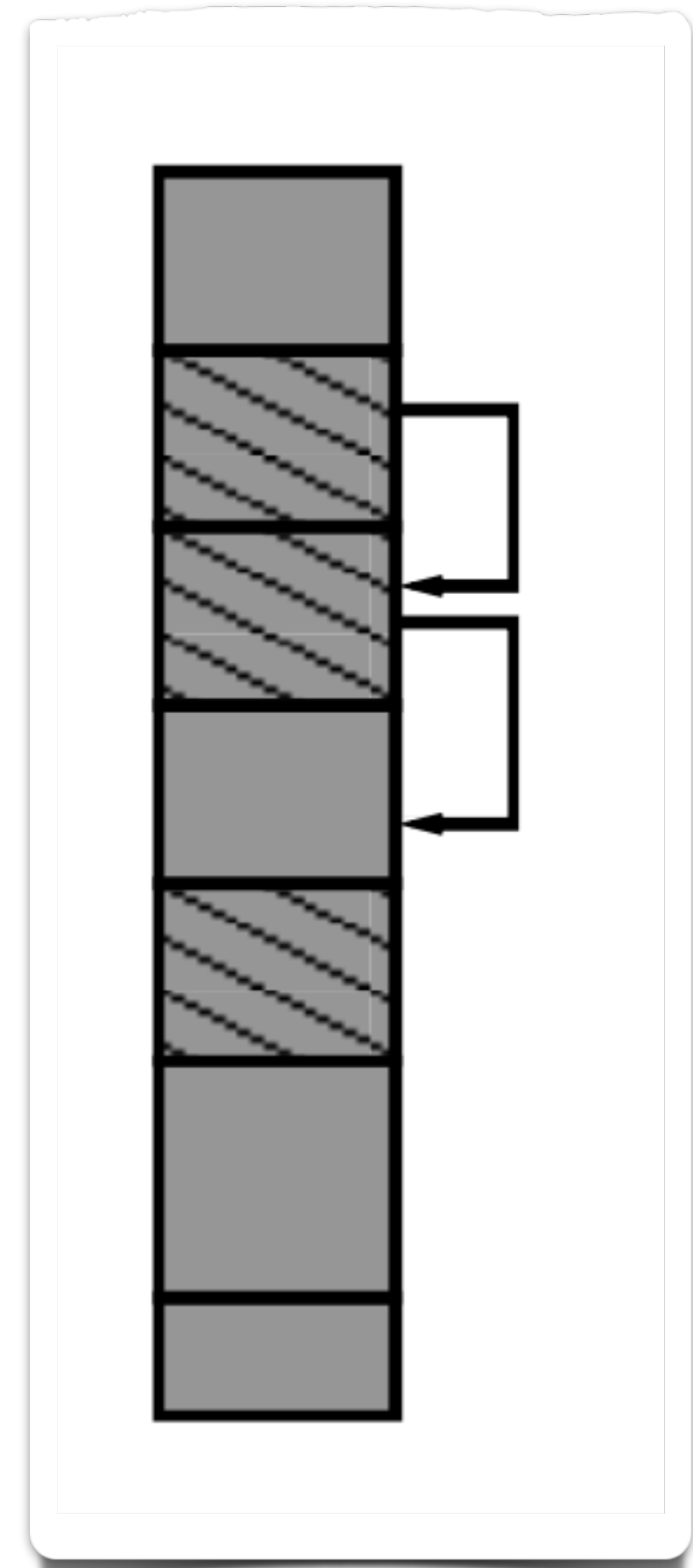
Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 0, 1, 2, 3, 4, 5, 6

Problem: *Clusterbildung*

Tendenz, dass immer längere zusammenhängende, belegte Abschnitte in der Hashtabelle entstehen. sogenannte *Cluster*



Lineares Sondieren

$$t(i, j) := (i + j) \bmod m$$

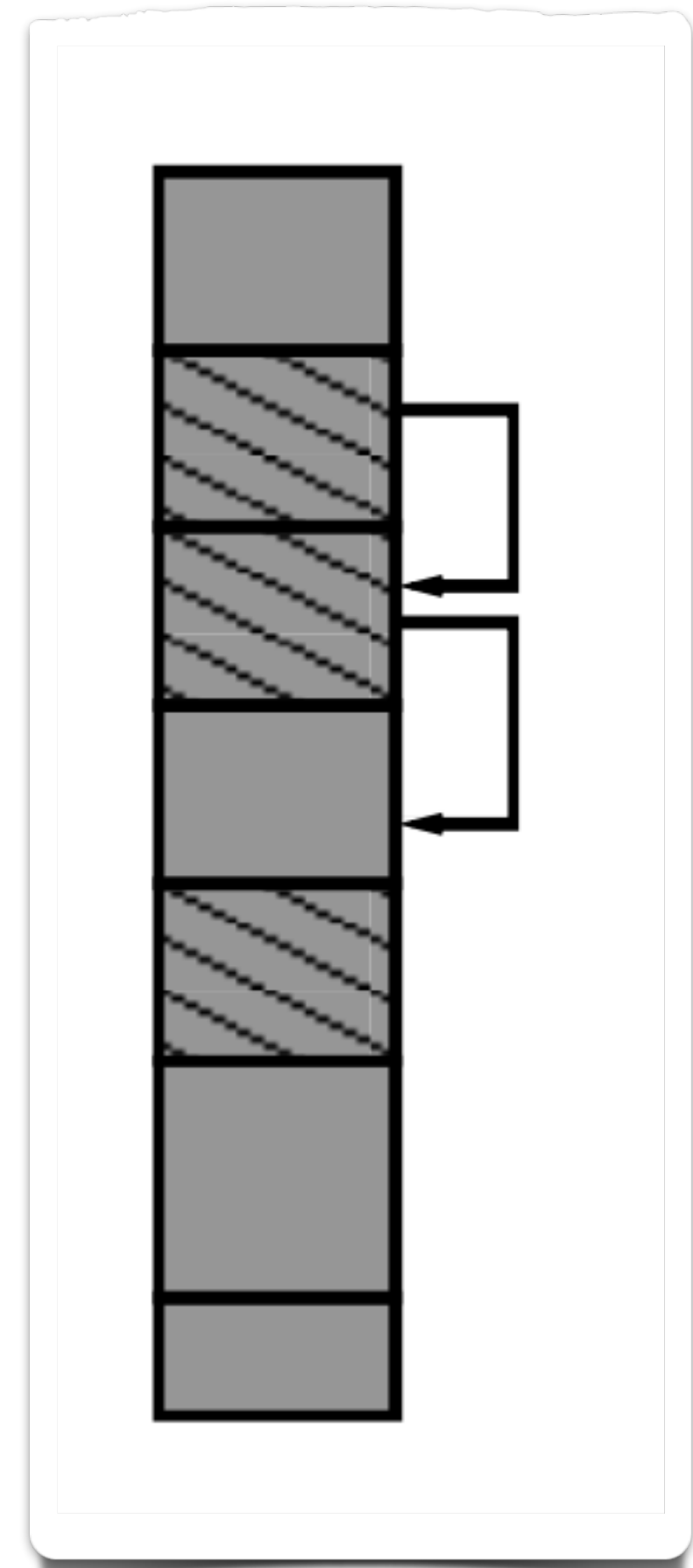
Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 0, 1, 2, 3, 4, 5, 6

Problem: *Clusterbildung*

Tendenz, dass immer längere zusammenhängende, belegte Abschnitte in der Hashtabelle entstehen, sogenannte *Cluster*
→ erhöhte Suchzeiten



Problem des Linearen Sondieren



Problem des Linearen Sondieren

Beispiel: $m = 19$, Positionen 2, 5, 6, 9, 10, 11, 12, 17 belegt



Problem des Linearen Sondieren

Beispiel: $m = 19$, Positionen 2, 5, 6, 9, 10, 11, 12, 17 belegt

$h(x):$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
---------	---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----

Problem des Linearen Sondieren

Beispiel: $m = 19$, Positionen 2, 5, 6, 9, 10, 11, 12, 17 belegt

$h(x)$:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
landet an																			
Position:	0	1	3	3	4	7	7	7	8	13	13	13	13	13	14	15	16	18	18

Problem des Linearen Sondieren

Beispiel: $m = 19$, Positionen 2, 5, 6, 9, 10, 11, 12, 17 belegt

$h(x)$:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
landet an																			
Position:	0	1	3	3	4	7	7	7	8	13	13	13	13	13	14	15	16	18	18

Problem des Linearen Sondieren

Beispiel: $m = 19$, Positionen 2, 5, 6, 9, 10, 11, 12, 17 belegt

$h(x)$:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
landet an																			
Position:	0	1	3	3	4	7	7	7	8	13	13	13	13	13	14	15	16	18	18

Problem des Linearen Sondieren

Beispiel: $m = 19$, Positionen 2, 5, 6, 9, 10, 11, 12, 17 belegt

$h(x)$:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
landet an																			
Position:	0	1	3	3	4	7	7	7	8	13	13	13	13	13	14	15	16	18	18

Problem des Linearen Sondieren

Beispiel: $m = 19$, Positionen 2, 5, 6, 9, 10, 11, 12, 17 belegt

$h(x)$:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
landet an																			
Position:	0	1	3	3	4	7	7	7	8	13	13	13	13	13	14	15	16	18	18

Problem des Linearen Sondieren

Beispiel: $m = 19$, Positionen 2, 5, 6, 9, 10, 11, 12, 17 belegt

$h(x)$:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
landet an																			
Position:	0	1	3	3	4	7	7	7	8	13	13	13	13	13	14	15	16	18	18



Problem des Linearen Sondieren

Beispiel: $m = 19$, Positionen 2, 5, 6, 9, 10, 11, 12, 17 belegt

$h(x)$:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
landet an																			
Position:	0	1	3	3	4	7	7	7	8	13	13	13	13	13	14	15	16	18	18



Problem des Linearen Sondieren

Beispiel: $m = 19$, Positionen 2, 5, 6, 9, 10, 11, 12, 17 belegt

$h(x)$:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
landet an																			
Position:	0	1	3	3	4	7	7	7	8	13	13	13	13	13	14	15	16	18	18



Problem des Linearen Sondieren

Beispiel: $m = 19$, Positionen 2, 5, 6, 9, 10, 11, 12, 17 belegt

$h(x)$:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
landet an																			
Position:	0	1	3	3	4	7	7	7	8	13	13	13	13	13	14	15	16	18	18



Problem des Linearen Sondieren

Beispiel: $m = 19$, Positionen 2, 5, 6, 9, 10, 11, 12, 17 belegt

$h(x)$:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
landet an																			
Position:	0	1	3	3	4	7	7	7	8	13	13	13	13	13	14	15	16	18	18
W.keit:	$\frac{1}{19}$	$\frac{1}{19}$	0	$\frac{2}{19}$	$\frac{1}{19}$	0	0	$\frac{3}{19}$	$\frac{1}{19}$	0	0	0	0	$\frac{5}{19}$	$\frac{1}{19}$	$\frac{1}{19}$	$\frac{1}{19}$	0	$\frac{2}{19}$



Ideales Hashing

Ideales Hashing

Wunsch:

Zu jedem Zeitpunkt haben alle Positionen die gleiche Wahrscheinlichkeit, besetzt zu werden.

Ideales Hashing

Wunsch:

Zu jedem Zeitpunkt haben alle Positionen die gleiche Wahrscheinlichkeit, besetzt zu werden.

Beobachtung:

Das geht numerisch nicht genau, im Beispiel 11 freie Plätze, 19 mögliche Hashwerte, also alle Wahrscheinlichkeiten $k/19$, nicht $k/11$.

Ideales Hashing

Wunsch:

Zu jedem Zeitpunkt haben alle Positionen die gleiche Wahrscheinlichkeit, besetzt zu werden.

Beobachtung:

Das geht numerisch nicht genau, im Beispiel 11 freie Plätze, 19 mögliche Hashwerte, also alle Wahrscheinlichkeiten $k/19$, nicht $k/11$.

Modell des idealen Hashings:

Alle $\binom{m}{n}$ Möglichkeiten, die n besetzten Plätze für m Schlüssel auszuwählen, haben die gleiche Wahrscheinlichkeit.

Ideales Hashing

Wunsch:

Zu jedem Zeitpunkt haben alle Positionen die gleiche Wahrscheinlichkeit, besetzt zu werden.

Beobachtung:

Das geht numerisch nicht genau, im Beispiel 11 freie Plätze, 19 mögliche Hashwerte, also alle Wahrscheinlichkeiten $k/19$, nicht $k/11$.

Modell des idealen Hashings:

Alle $\binom{m}{n}$ Möglichkeiten, die n besetzten Plätze für m Schlüssel auszuwählen, haben die gleiche Wahrscheinlichkeit.

Lineares Sondieren ist weit vom idealen Hashing entfernt.

Quadratisches Sondieren

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$j,$

:

:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2,$$

:

:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2,$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2,$$

:

:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots,$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2,$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

7,

:

:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

7, 8,

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + \left(\frac{m-1}{2}\right)^2, j - \left(\frac{m-1}{2}\right)^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

7, 8, 6,

:

:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

7, 8, 6, 11,

:

:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

7, 8, 6, 11, 3,

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

7, 8, 6, 11, 3, 16,

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$7, 8, 6, 11, 3, 16, -2$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2, & \\ & & & & & & = 17, & \vdots \end{array}$$

:

:

:

:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 \\ & & & & & & = 17, & : \end{array}$$

:

:

:

:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 \\ & & & & & & = 17, & = 4, \end{array}$$

:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 \\ & & & & & & = 17, & = 4, & \end{array}$$

:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 \\ & & & & & & = 17, & = 4, & = 10, \end{array}$$

:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 \\ & & & & & & = 17, & = 4, & = 10, & \end{array}$$

:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 \\ & & & & & & = 17, & = 4, & = 10, & = 13, \end{array}$$

:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & \end{array}$$

:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{ccccccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

43

:

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

$$\begin{array}{c} 43 \\ = 5, \end{array}$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{ccccccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

$$\begin{array}{ccc} 43 & -29 & \\ = 5, & & : \end{array}$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

$$\begin{array}{cc} 43 & -29 \\ = 5, & = 9, \end{array} \quad \dots$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

$$\begin{array}{ccc} 43 & -29 & 56 \\ = 5, & = 9, & : \end{array}$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

$$\begin{array}{ccc} 43 & -29 & 56 \\ = 5, & = 9, & = 18, \end{array}$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

$$\begin{array}{cccc} 43 & -29 & 56 & -42 \\ = 5, & = 9, & = 18, & \end{array}$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

$$\begin{array}{cccc} 43 & -29 & 56 & -42 \\ = 5, & = 9, & = 18, & = 15, \end{array}$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

$$\begin{array}{ccccc} 43 & -29 & 56 & -42 & 71 \\ = 5, & = 9, & = 18, & = 15, & \end{array}$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

$$\begin{array}{ccccc} 43 & -29 & 56 & -42 & 71 \\ = 5, & = 9, & = 18, & = 15, & = 14, \end{array}$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

$$\begin{array}{cccccc} 43 & -29 & 56 & -42 & 71 & -57 \\ = 5, & = 9, & = 18, & = 15, & = 14, & \end{array}$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

$$\begin{array}{cccccc} 43 & -29 & 56 & -42 & 71 & -57 \\ = 5, & = 9, & = 18, & = 15, & = 14, & = 0, \end{array}$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

$$\begin{array}{cccccc} 43 & -29 & 56 & -42 & 71 & -57 & 88 \\ = 5, & = 9, & = 18, & = 15, & = 14, & = 0, & \end{array}$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

$$\begin{array}{cccccc} 43 & -29 & 56 & -42 & 71 & -57 & 88 \\ = 5, & = 9, & = 18, & = 15, & = 14, & = 0, & = 12, \end{array}$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

$$\begin{array}{cccccc} 43 & -29 & 56 & -42 & 71 & -57 & 88 & -74 \\ = 5, & = 9, & = 18, & = 15, & = 14, & = 0, & = 12, & \end{array}$$

Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

$$\begin{array}{cccccc} 43 & -29 & 56 & -42 & 71 & -57 & 88 & -74 \\ = 5, & = 9, & = 18, & = 15, & = 14, & = 0, & = 12, & = 2 \end{array}$$

Quadratisches Sondieren (2)

Quadratisches Sondieren (2)

Frage: Ist $t(\cdot, j)$ für alle j und m bijektiv?

Quadratisches Sondieren (2)

Frage: Ist $t(\cdot, j)$ für alle j und m bijektiv?

Nein, aber immer wenn $m \equiv 3 \pmod{4}$ und m eine Primzahl ist
(Beweis: Zahlentheorie)

Quadratisches Sondieren (2)

Frage: Ist $t(\cdot, j)$ für alle j und m bijektiv?

Nein, aber immer wenn $m \equiv 3 \pmod{4}$ und m eine Primzahl ist
(Beweis: Zahlentheorie)

Besser als **lineares Sondieren**, aber für großes m sind die ersten Werte noch *nah* an j

Multiplikatives Sondieren

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$$

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$i \cdot j \quad 7$$

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$ 7 14

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21
-------------	---	----	----

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$ 7 14 21 28

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$ 7 14 21 28 35

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42
-------------	---	----	----	----	----	----

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49
-------------	---	----	----	----	----	----	----

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56
-------------	---	----	----	----	----	----	----	----

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
-------------	---	----	----	----	----	----	----	----	----

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$i \cdot j \quad 7 \quad 14 \quad 21 \quad 28 \quad 35 \quad 42 \quad 49 \quad 56 \quad 63$$

$$i \cdot j$$

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$i \cdot j \quad 7 \quad 14 \quad 21 \quad 28 \quad 35 \quad 42 \quad 49 \quad 56 \quad 63$$

$$i \cdot j \quad 70$$

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
-------------	---	----	----	----	----	----	----	----	----

$i \cdot j$	70	77
-------------	----	----

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$i \cdot j \quad 7 \quad 14 \quad 21 \quad 28 \quad 35 \quad 42 \quad 49 \quad 56 \quad 63$$

$$i \cdot j \quad 70 \quad 77 \quad 84$$

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$i \cdot j \quad 7 \quad 14 \quad 21 \quad 28 \quad 35 \quad 42 \quad 49 \quad 56 \quad 63$$

$$i \cdot j \quad 70 \quad 77 \quad 84 \quad 91$$

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$i \cdot j \quad 7 \quad 14 \quad 21 \quad 28 \quad 35 \quad 42 \quad 49 \quad 56 \quad 63$$

$$i \cdot j \quad 70 \quad 77 \quad 84 \quad 91 \quad 98$$

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$i \cdot j \quad 7 \quad 14 \quad 21 \quad 28 \quad 35 \quad 42 \quad 49 \quad 56 \quad 63$$

$$i \cdot j \quad 70 \quad 77 \quad 84 \quad 91 \quad 98 \quad 105$$

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
-------------	---	----	----	----	----	----	----	----	----

$i \cdot j$	70	77	84	91	98	105	112
-------------	----	----	----	----	----	-----	-----

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
-------------	---	----	----	----	----	----	----	----	----

$i \cdot j$	70	77	84	91	98	105	112	119
-------------	----	----	----	----	----	-----	-----	-----

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
-------------	---	----	----	----	----	----	----	----	----

$i \cdot j$	70	77	84	91	98	105	112	119	126
-------------	----	----	----	----	----	-----	-----	-----	-----

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$i \cdot j \quad 7 \quad 14 \quad 21 \quad 28 \quad 35 \quad 42 \quad 49 \quad 56 \quad 63$$

$$i \cdot j \bmod 19$$

$$i \cdot j \quad 70 \quad 77 \quad 84 \quad 91 \quad 98 \quad 105 \quad 112 \quad 119 \quad 126$$

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$ 7 14 21 28 35 42 49 56 63

$i \cdot j \bmod 19$ 7

$i \cdot j$ 70 77 84 91 98 105 112 119 126

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$i \cdot j \quad 7 \quad 14 \quad 21 \quad 28 \quad 35 \quad 42 \quad 49 \quad 56 \quad 63$$

$$i \cdot j \bmod 19 \quad 7 \quad 14$$

$$i \cdot j \quad 70 \quad 77 \quad 84 \quad 91 \quad 98 \quad 105 \quad 112 \quad 119 \quad 126$$

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
-------------	---	----	----	----	----	----	----	----	----

$i \cdot j \bmod 19$	7	14	2
----------------------	---	----	---

$i \cdot j$	70	77	84	91	98	105	112	119	126
-------------	----	----	----	----	----	-----	-----	-----	-----

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
-------------	---	----	----	----	----	----	----	----	----

$i \cdot j \bmod 19$	7	14	2	9					
----------------------	---	----	---	---	--	--	--	--	--

$i \cdot j$	70	77	84	91	98	105	112	119	126
-------------	----	----	----	----	----	-----	-----	-----	-----

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
$i \cdot j \bmod 19$	7	14	2	9	16				
$i \cdot j$	70	77	84	91	98	105	112	119	126

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
$i \cdot j \bmod 19$	7	14	2	9	16	4			
$i \cdot j$	70	77	84	91	98	105	112	119	126

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
$i \cdot j \bmod 19$	7	14	2	9	16	4	11		
$i \cdot j$	70	77	84	91	98	105	112	119	126

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
$i \cdot j \bmod 19$	7	14	2	9	16	4	11	18	
$i \cdot j$	70	77	84	91	98	105	112	119	126

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
$i \cdot j \bmod 19$	7	14	2	9	16	4	11	18	6
$i \cdot j$	70	77	84	91	98	105	112	119	126

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
$i \cdot j \bmod 19$	7	14	2	9	16	4	11	18	6
$i \cdot j$	70	77	84	91	98	105	112	119	126
$i \cdot j \bmod 19$									

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$$i \cdot j \quad 7 \quad 14 \quad 21 \quad 28 \quad 35 \quad 42 \quad 49 \quad 56 \quad 63$$

$$i \cdot j \bmod 19 \quad 7 \quad 14 \quad 2 \quad 9 \quad 16 \quad 4 \quad 11 \quad 18 \quad 6$$

$$i \cdot j \quad 70 \quad 77 \quad 84 \quad 91 \quad 98 \quad 105 \quad 112 \quad 119 \quad 126$$

$$i \cdot j \bmod 19 \quad 13$$

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
$i \cdot j \bmod 19$	7	14	2	9	16	4	11	18	6
$i \cdot j$	70	77	84	91	98	105	112	119	126
$i \cdot j \bmod 19$	13	1							

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
$i \cdot j \bmod 19$	7	14	2	9	16	4	11	18	6

$i \cdot j$	70	77	84	91	98	105	112	119	126
$i \cdot j \bmod 19$	13	1	8						

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
$i \cdot j \bmod 19$	7	14	2	9	16	4	11	18	6

$i \cdot j$	70	77	84	91	98	105	112	119	126
$i \cdot j \bmod 19$	13	1	8	15					

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
$i \cdot j \bmod 19$	7	14	2	9	16	4	11	18	6

$i \cdot j$	70	77	84	91	98	105	112	119	126
$i \cdot j \bmod 19$	13	1	8	15	3				

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
$i \cdot j \bmod 19$	7	14	2	9	16	4	11	18	6

$i \cdot j$	70	77	84	91	98	105	112	119	126
$i \cdot j \bmod 19$	13	1	8	15	3	10			

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
$i \cdot j \bmod 19$	7	14	2	9	16	4	11	18	6
$i \cdot j$	70	77	84	91	98	105	112	119	126
$i \cdot j \bmod 19$	13	1	8	15	3	10	17		

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
$i \cdot j \bmod 19$	7	14	2	9	16	4	11	18	6

$i \cdot j$	70	77	84	91	98	105	112	119	126
$i \cdot j \bmod 19$	13	1	8	15	3	10	17	5	

Multiplikatives Sondieren

Hier: $h(x) = x \bmod (m - 1) + 1$ und damit in $\{1, \dots, m - 1\}$

$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$

Hashwerte $1, \dots, m - 1$

Beispiel: $m = 19$ und $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
$i \cdot j \bmod 19$	7	14	2	9	16	4	11	18	6

$i \cdot j$	70	77	84	91	98	105	112	119	126
$i \cdot j \bmod 19$	13	1	8	15	3	10	17	5	12

Multiplikatives Sondieren (2)

Multiplikatives Sondieren (2)

Frage: Ist $t(\cdot, j)$ für alle j und m bijektiv?

Multiplikatives Sondieren (2)

Frage: Ist $t(\cdot, j)$ für alle j und m bijektiv?

Nein, aber immer wenn m Primzahl und $j \neq 0$

Multiplikatives Sondieren (2)

Frage: Ist $t(\cdot, j)$ für alle j und m bijektiv?

Nein, aber immer wenn m Primzahl und $j \neq 0$

Beweis: Durch Widerspruch!

Multiplikatives Sondieren (2)

Frage: Ist $t(\cdot, j)$ für alle j und m bijektiv?

Nein, aber immer wenn m Primzahl und $j \neq 0$

Beweis: Durch Widerspruch!

Falls nicht, gibt es $1 \leq i_1 < i_2 \leq m - 1$ mit

Multiplikatives Sondieren (2)

Frage: Ist $t(\cdot, j)$ für alle j und m bijektiv?

Nein, aber immer wenn m Primzahl und $j \neq 0$

Beweis: Durch Widerspruch!

Falls nicht, gibt es $1 \leq i_1 < i_2 \leq m - 1$ mit

$$i_1 \cdot j \equiv i_2 \cdot j \pmod{m}$$

Multiplikatives Sondieren (2)

Frage: Ist $t(\cdot, j)$ für alle j und m bijektiv?

Nein, aber immer wenn m Primzahl und $j \neq 0$

Beweis: Durch Widerspruch!

Falls nicht, gibt es $1 \leq i_1 < i_2 \leq m - 1$ mit

$$\begin{aligned} i_1 \cdot j &\equiv i_2 \cdot j \pmod{m} \\ \Rightarrow j \cdot (i_2 - i_1) &\equiv 0 \pmod{m} \end{aligned}$$

Multiplikatives Sondieren (2)

Frage: Ist $t(\cdot, j)$ für alle j und m bijektiv?

Nein, aber immer wenn m Primzahl und $j \neq 0$

Beweis: Durch Widerspruch!

Falls nicht, gibt es $1 \leq i_1 < i_2 \leq m - 1$ mit

$$i_1 \cdot j \equiv i_2 \cdot j \pmod{m}$$

$$\Rightarrow j \cdot (i_2 - i_1) \equiv 0 \pmod{m}$$

$$\Rightarrow j \cdot (i_2 - i_1) \text{ ist Vielfaches von } m$$

Multiplikatives Sondieren (2)

Frage: Ist $t(\cdot, j)$ für alle j und m bijektiv?

Nein, aber immer wenn m Primzahl und $j \neq 0$

Beweis: Durch Widerspruch!

Falls nicht, gibt es $1 \leq i_1 < i_2 \leq m - 1$ mit

$$i_1 \cdot j \equiv i_2 \cdot j \pmod{m}$$

$$\Rightarrow j \cdot (i_2 - i_1) \equiv 0 \pmod{m}$$

$$\Rightarrow j \cdot (i_2 - i_1) \text{ ist Vielfaches von } m$$

$$\Rightarrow \text{Primfaktorzerlegung von } j \cdot (i_2 - i_1) \text{ muss } m \text{ enthalten}$$

Multiplikatives Sondieren (2)

Frage: Ist $t(\cdot, j)$ für alle j und m bijektiv?

Nein, aber immer wenn m Primzahl und $j \neq 0$

Beweis: Durch Widerspruch!

Falls nicht, gibt es $1 \leq i_1 < i_2 \leq m - 1$ mit

$$i_1 \cdot j \equiv i_2 \cdot j \pmod{m}$$

$$\Rightarrow j \cdot (i_2 - i_1) \equiv 0 \pmod{m}$$

$$\Rightarrow j \cdot (i_2 - i_1) \text{ ist Vielfaches von } m$$

$$\Rightarrow \text{Primfaktorzerlegung von } j \cdot (i_2 - i_1) \text{ muss } m \text{ enthalten}$$

Widerspruch zu $1 \leq j \leq m - 1, 1 \leq i_2 - i_1 \leq m - 1$

Doppeltes Hashing

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$$h_1(47) \equiv 47 \pmod{19} = 9$$

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Sondierungsfolge:

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Sondierungsfolge:

9,

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Sondierungsfolge:

9, 4,

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Sondierungsfolge:

9, 4, 18,

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Sondierungsfolge:

9, 4, 18, 13,

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Sondierungsfolge:

9, 4, 18, 13, 8,

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Sondierungsfolge:

9, 4, 18, 13, 8, 3,

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Sondierungsfolge:

9, 4, 18, 13, 8, 3, 17,

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Sondierungsfolge:

9, 4, 18, 13, 8, 3, 17, 12,

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Sondierungsfolge:

9, 4, 18, 13, 8, 3, 17, 12, 7,

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Sondierungsfolge:

9, 4, 18, 13, 8, 3, 17, 12, 7, 2,

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Sondierungsfolge:

9, 4, 18, 13, 8, 3, 17, 12, 7, 2, 16,

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Sondierungsfolge:

9, 4, 18, 13, 8, 3, 17, 12, 7, 2, 16, 11,

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Sondierungsfolge:

9, 4, 18, 13, 8, 3, 17, 12, 7, 2, 16, 11, 6,

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Sondierungsfolge:

9, 4, 18, 13, 8, 3, 17, 12, 7, 2, 16, 11, 6, 1,

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Sondierungsfolge:

9, 4, 18, 13, 8, 3, 17, 12, 7, 2, 16, 11, 6, 1, 15, ...

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17} + 1 = 14$

Sondierungsfolge:

9, 4, 18, 13, 8, 3, 17, 12, 7, 2, 16, 11, 6, 1, 15, 10,

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17+1} = 14$

Sondierungsfolge:

9, 4, 18, 13, 8, 3, 17, 12, 7, 2, 16, 11, 6, 1, 15, 10, 5,

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17+1} = 14$

Sondierungsfolge:

9, 4, 18, 13, 8, 3, 17, 12, 7, 2, 16, 11, 6, 1, 15, 10, 5, 0,

Doppeltes Hashing

Sei $h_1(x) \equiv x \pmod{m}$ und $h_2(x) \equiv x \pmod{(m-2)+1}$.

i -te Position für x : $h_1(x) + i \cdot h_2(x) \pmod{m}$, $1 \leq i \leq m-1$

Beispiel: $m = 19$ und $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$ und $h_2(47) \equiv 47 \pmod{17+1} = 14$

Sondierungsfolge:

9, 4, 18, 13, 8, 3, 17, 12, 7, 2, 16, 11, 6, 1, 15, 10, 5, 0, 14

Doppeltes Hashing (2)

Doppeltes Hashing (2)

Beobachtung:

$i \cdot h_2(x)$ durchläuft für $1 \leq i \leq m - 1$ die Werte $1, \dots, m - 1$ in irgendeiner Reihenfolge, ergänzt wird $0 = 0 \cdot h_2(x)$

Doppeltes Hashing (2)

Beobachtung:

$i \cdot h_2(x)$ durchläuft für $1 \leq i \leq m - 1$ die Werte $1, \dots, m - 1$ in irgendeiner Reihenfolge, ergänzt wird $0 = 0 \cdot h_2(x)$

Durch den Summanden $h_1(x)$ wird der Anfang zufällig verschoben.

Doppeltes Hashing (2)

Beobachtung:

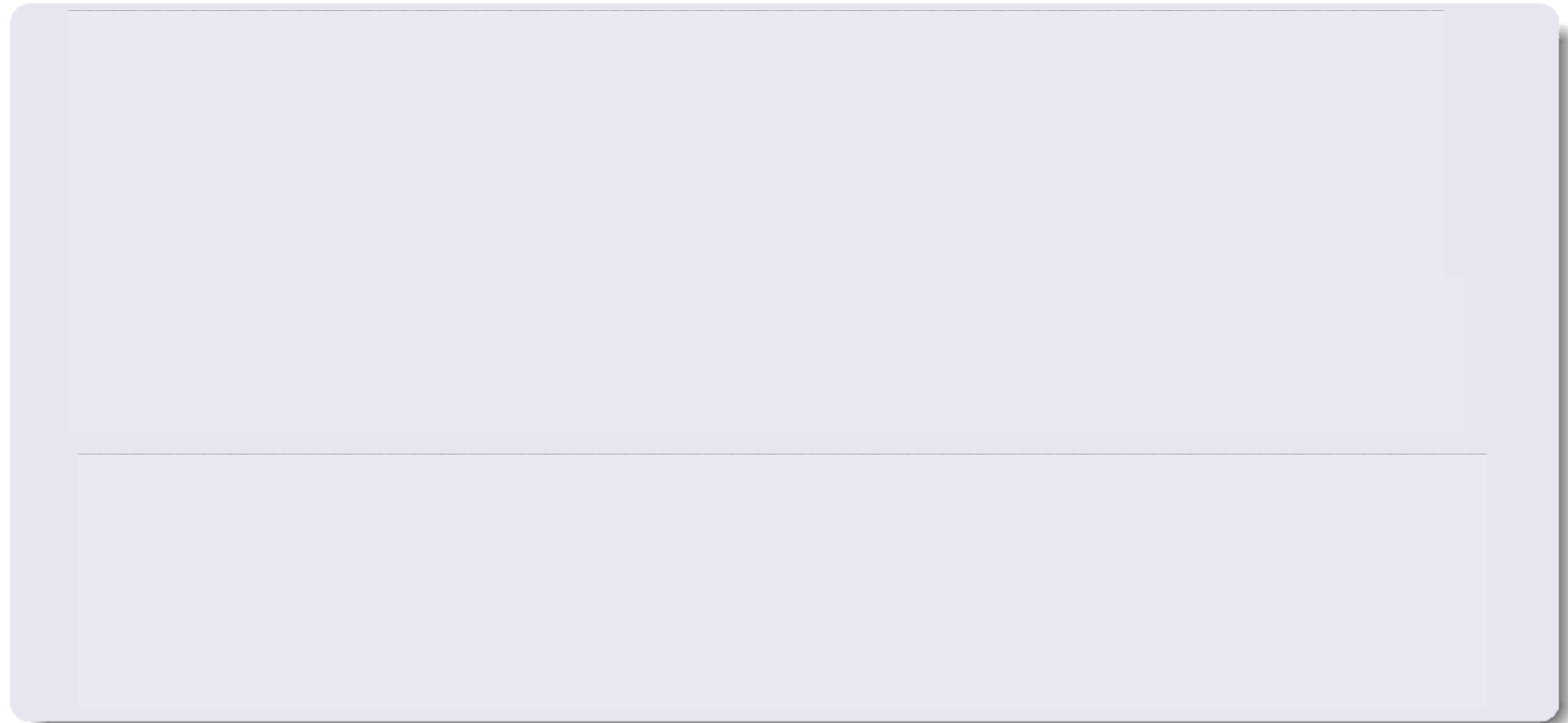
$i \cdot h_2(x)$ durchläuft für $1 \leq i \leq m - 1$ die Werte $1, \dots, m - 1$ in irgendeiner Reihenfolge, ergänzt wird $0 = 0 \cdot h_2(x)$

Durch den Summanden $h_1(x)$ wird der Anfang zufällig verschoben.

Doppeltes Hashing kommt dem **idealen Hashing** am nächsten.

Zusammenfassung

Zusammenfassung



Zusammenfassung

- Auch die beste Hashfunktion kann Kollisionen nicht ganz vermeiden, deshalb sind Hashverfahren im *Worst Case* ineffiziente Realisierungen der Operationen **search**, **insert**, **delete**.

Zusammenfassung

- Auch die beste Hashfunktion kann Kollisionen nicht ganz vermeiden, deshalb sind Hashverfahren im *Worst Case* ineffiziente Realisierungen der Operationen **search**, **insert**, **delete**.
- Im **Durchschnitt** sind sie jedoch weitaus effizienter als Verfahren, die auf Schlüsselvergleichen basieren.

Zusammenfassung

- Auch die beste Hashfunktion kann Kollisionen nicht ganz vermeiden, deshalb sind Hashverfahren im *Worst Case* ineffiziente Realisierungen der Operationen **search**, **insert**, **delete**.
- Im **Durchschnitt** sind sie jedoch weitaus effizienter als Verfahren, die auf Schlüsselvergleichen basieren.
- Die Anzahl benötigter Schritte zum Suchen, Einfügen und Entfernen hängt (im Durchschnitt) im wesentlichen vom Belegungsfaktor, d.h. dem Verhältnis von Anzahl aktueller Schlüssel zur Größe der Hashtabelle, ab.

7.7 Kryptographie

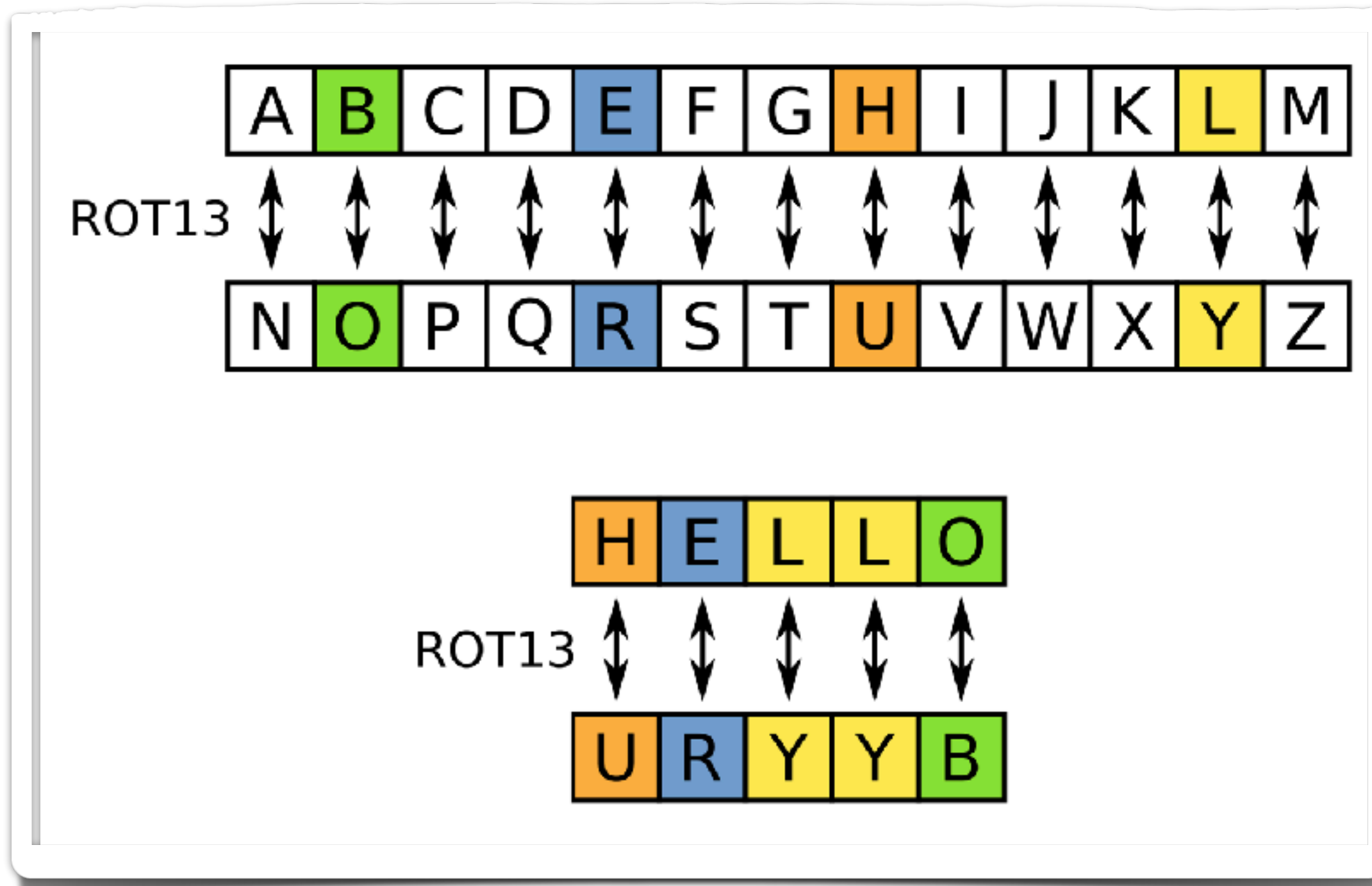
Veränderte Ziele

Veränderte Ziele

- Text codieren:

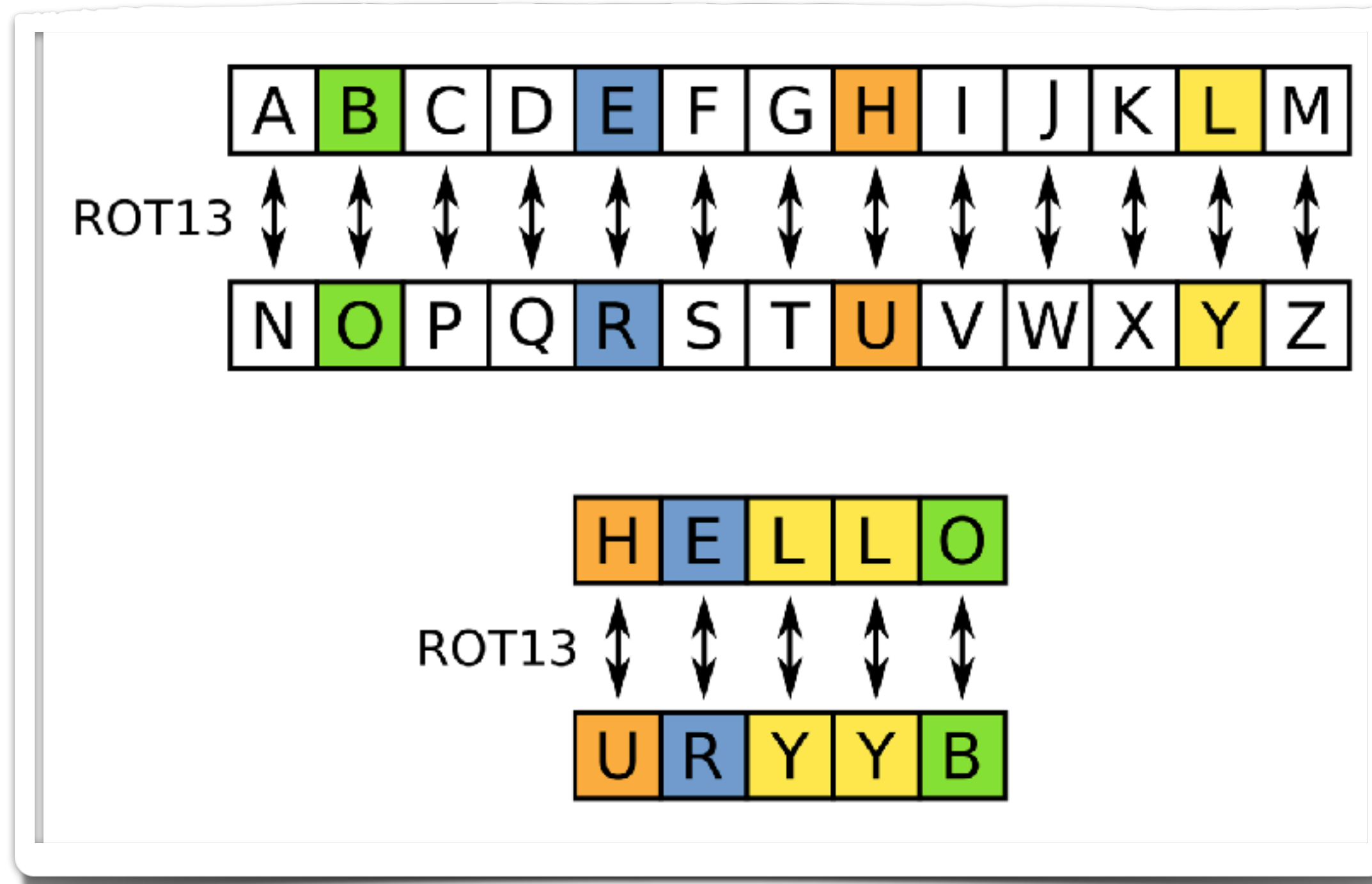
Veränderte Ziele

- Text codieren:



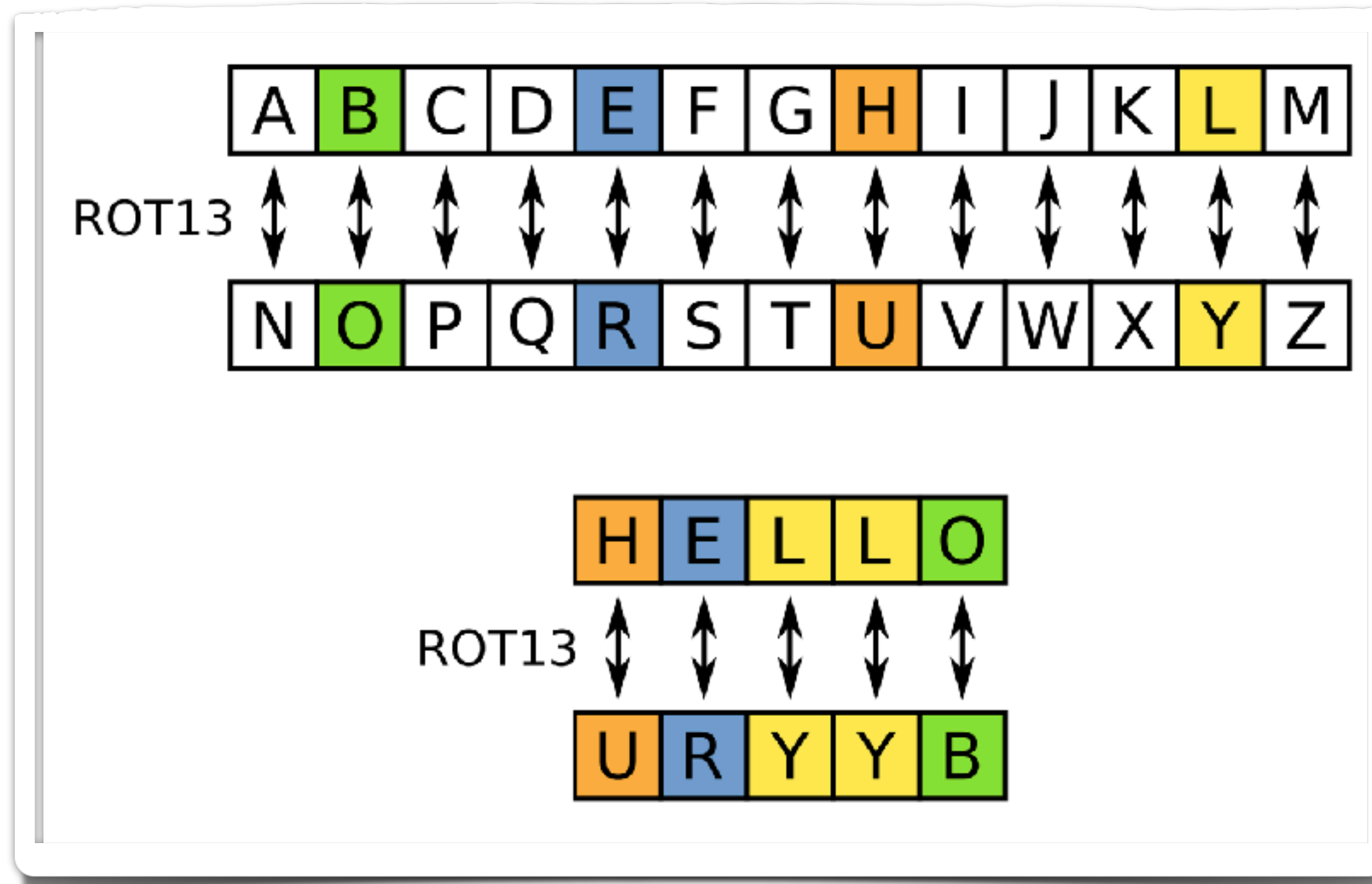
Veränderte Ziele

- Text codieren:
 1. Berechtigter Empfänger soll Nachricht entschlüsseln können.



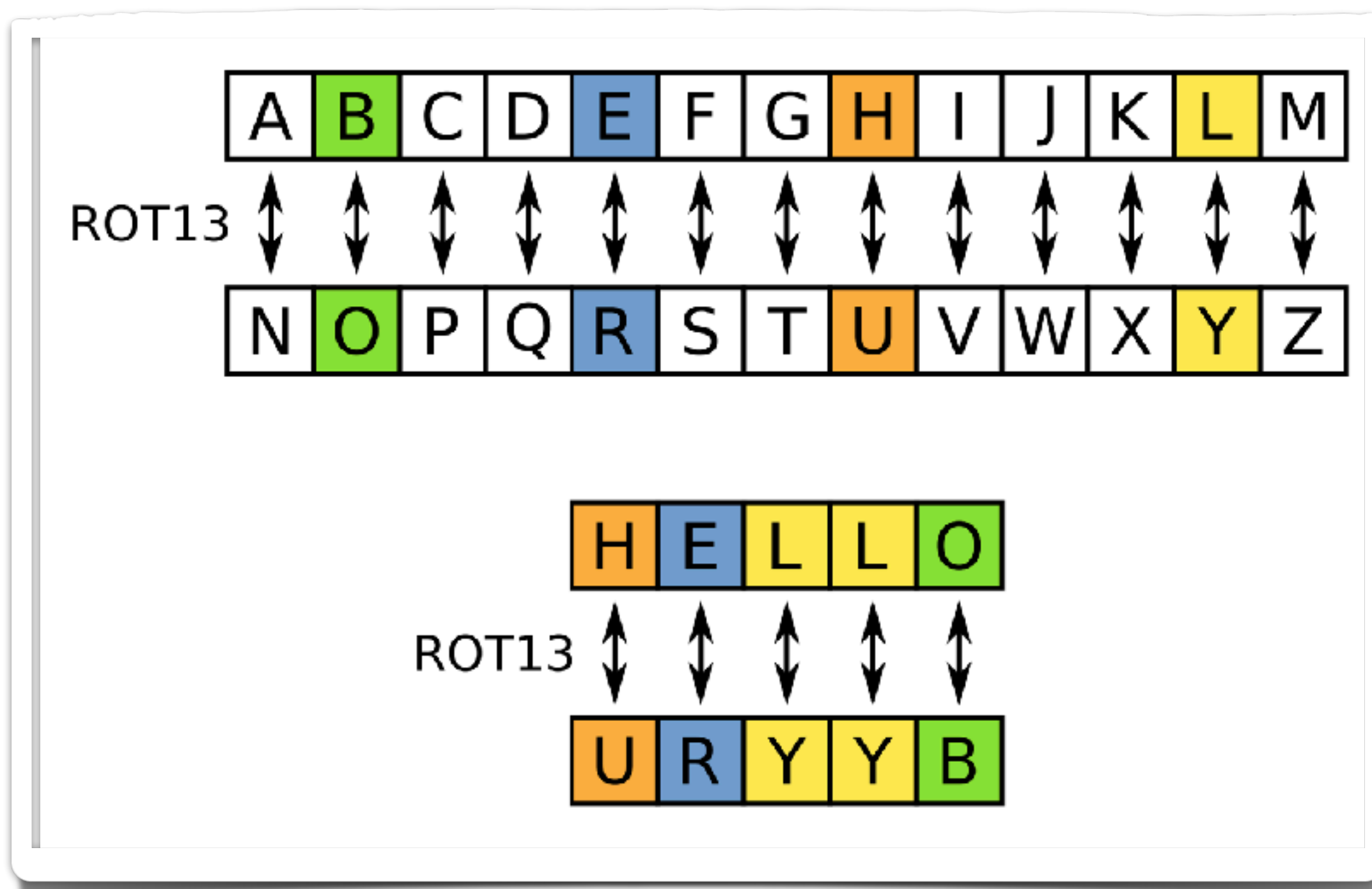
Veränderte Ziele

- Text codieren:
 1. Berechtigter Empfänger soll Nachricht entschlüsseln können.
 2. Unberechtigter Empfänger soll Nachricht nicht entschlüsseln können.



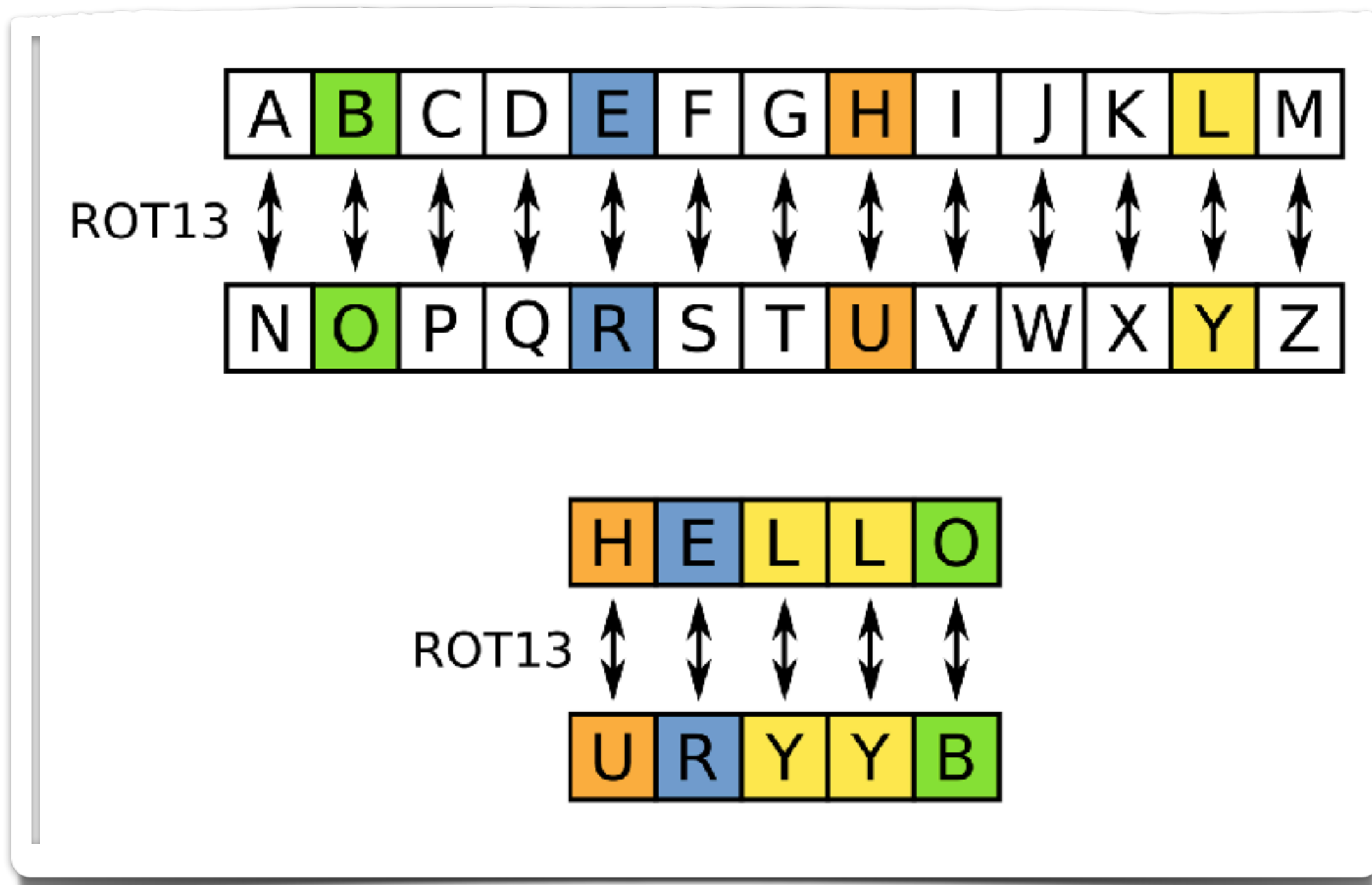
Veränderte Ziele

- Text codieren:
 1. Berechtigter Empfänger soll Nachricht entschlüsseln können.
 2. Unberechtigter Empfänger soll Nachricht nicht entschlüsseln können.



Veränderte Ziele

- Text codieren:
 1. Berechtigter Empfänger soll Nachricht entschlüsseln können.
 2. Unberechtigter Empfänger soll Nachricht nicht entschlüsseln können.



Veränderte Ziele

Veränderte Ziele

- Deterministisch, d.h. dieselbe Nachricht ergibt immer den selben Wert.

Veränderte Ziele

- Deterministisch, d.h. dieselbe Nachricht ergibt immer den selben Wert.
- Hashwert lässt sich schnell berechnen.

Veränderte Ziele

- Deterministisch, d.h. dieselbe Nachricht ergibt immer den selben Wert.
- Hashwert lässt sich schnell berechnen.
- SEHR schwer eine Nachricht mit demselben Hashwert zu generieren.

Veränderte Ziele

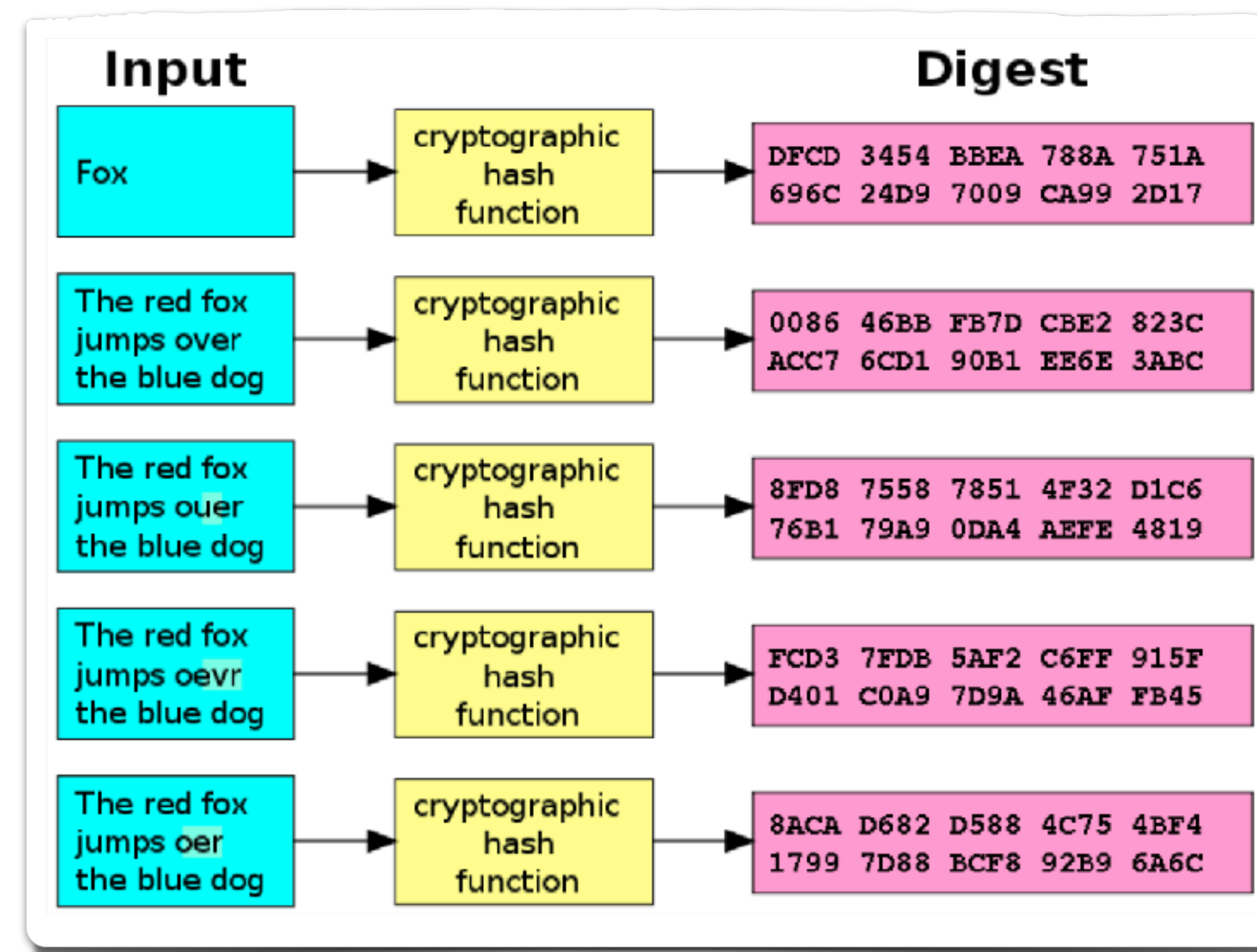
- Deterministisch, d.h. dieselbe Nachricht ergibt immer den selben Wert.
- Hashwert lässt sich schnell berechnen.
- SEHR schwer eine Nachricht mit demselben Hashwert zu generieren.
- SEHR schwer zwei Nachrichten mit demselben Hashwert zu finden.

Veränderte Ziele

- Deterministisch, d.h. dieselbe Nachricht ergibt immer den selben Wert.
- Hashwert lässt sich schnell berechnen.
- SEHR schwer eine Nachricht mit demselben Hashwert zu generieren.
- SEHR schwer zwei Nachrichten mit demselben Hashwert zu finden.
- Ein kleine Änderung in der Nachricht ändert das Ergebnis so stark, dass man aus den Hashwerten nicht auf ähnliche Nachrichten schließen kann.

Veränderte Ziele

- Deterministisch, d.h. dieselbe Nachricht ergibt immer den selben Wert.
- Hashwert lässt sich schnell berechnen.
- SEHR schwer eine Nachricht mit demselben Hashwert zu generieren.
- SEHR schwer zwei Nachrichten mit demselben Hashwert zu finden.
- Ein kleine Änderung in der Nachricht ändert das Ergebnis so stark, dass man aus den Hashwerten nicht auf ähnliche Nachrichten schließen kann.



PUBLIK KEY KRYPTO

PUBLIK KEY KRYPTO

idea-instructions.com/public-key/
v1.2, CC by-nc-sa 4.0



PUBLIK KEY KRYPTO

idea-instructions.com/public-key/
v1.2, CC by-nc-sa 4.0

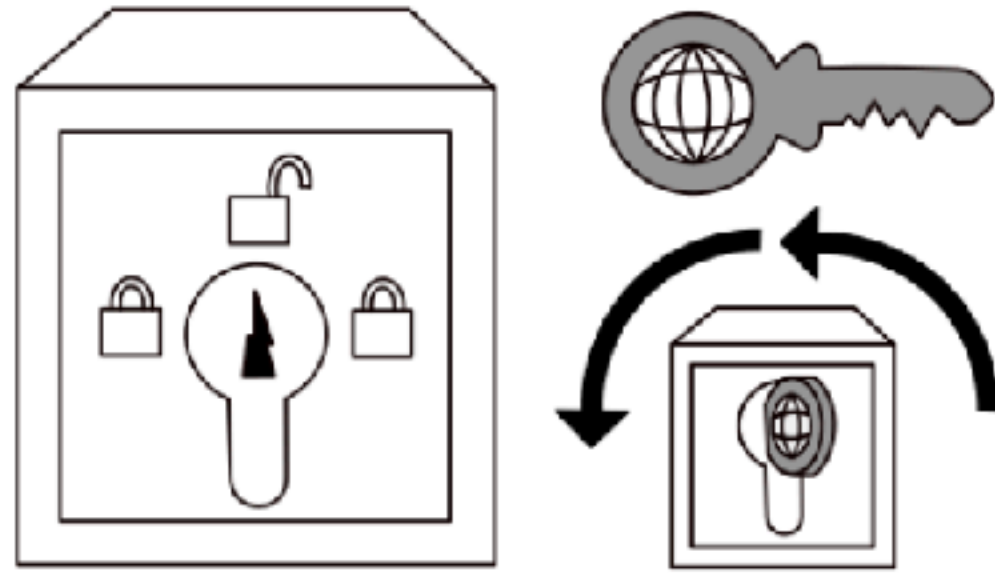
IDEA



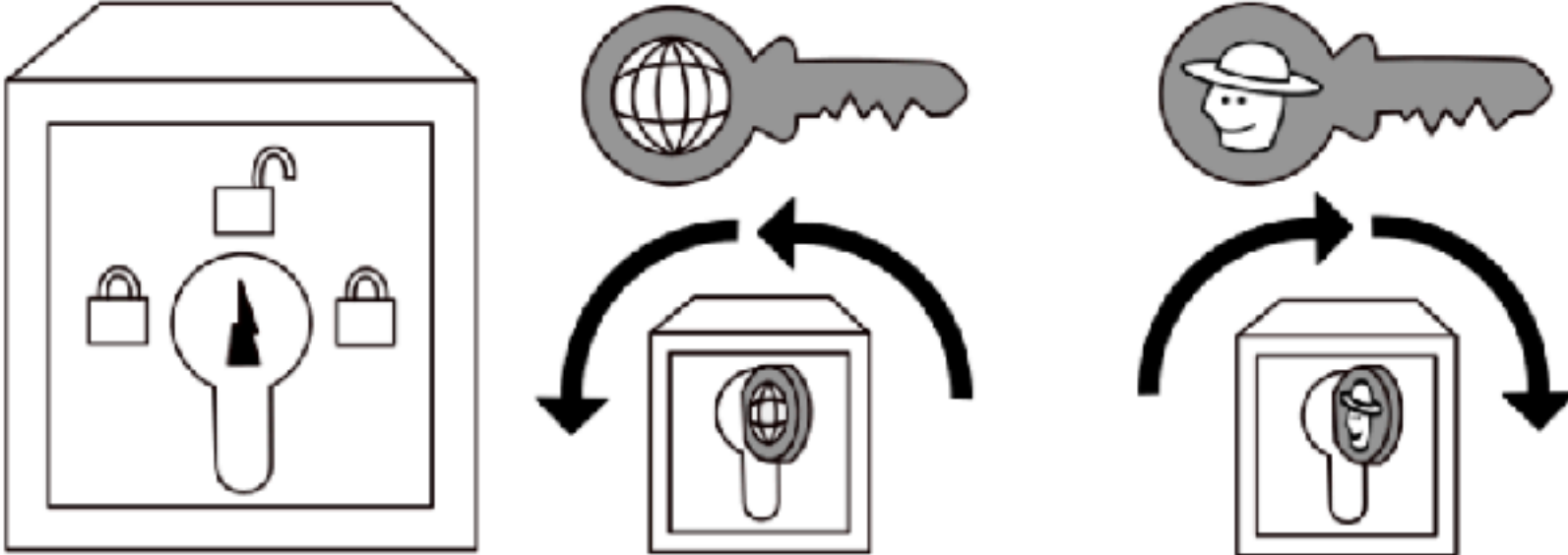
PUBLIK KEY KRYPTO

idea-instructions.com/public-key/
v1.2, CC by-nc-sa 4.0

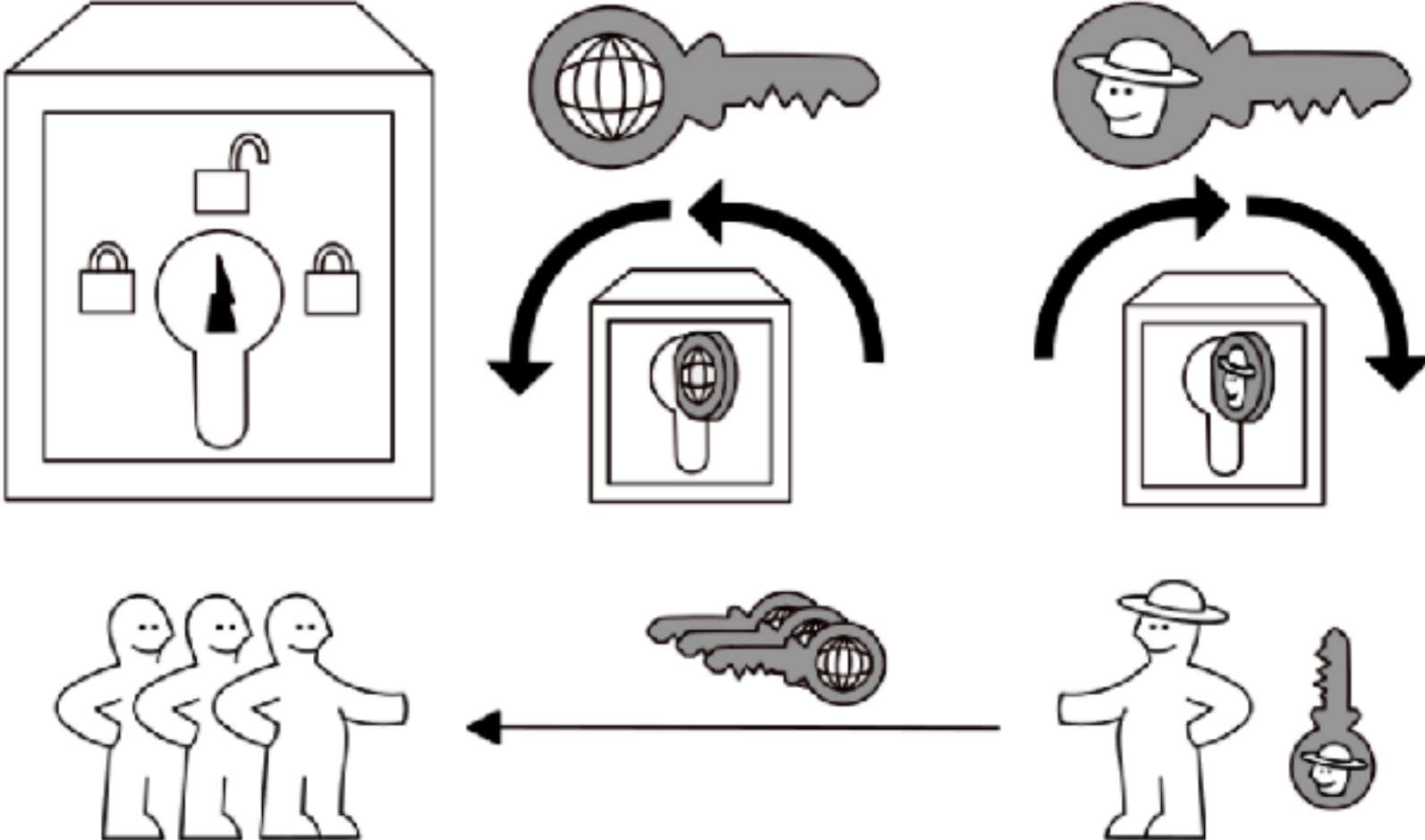
IDEA



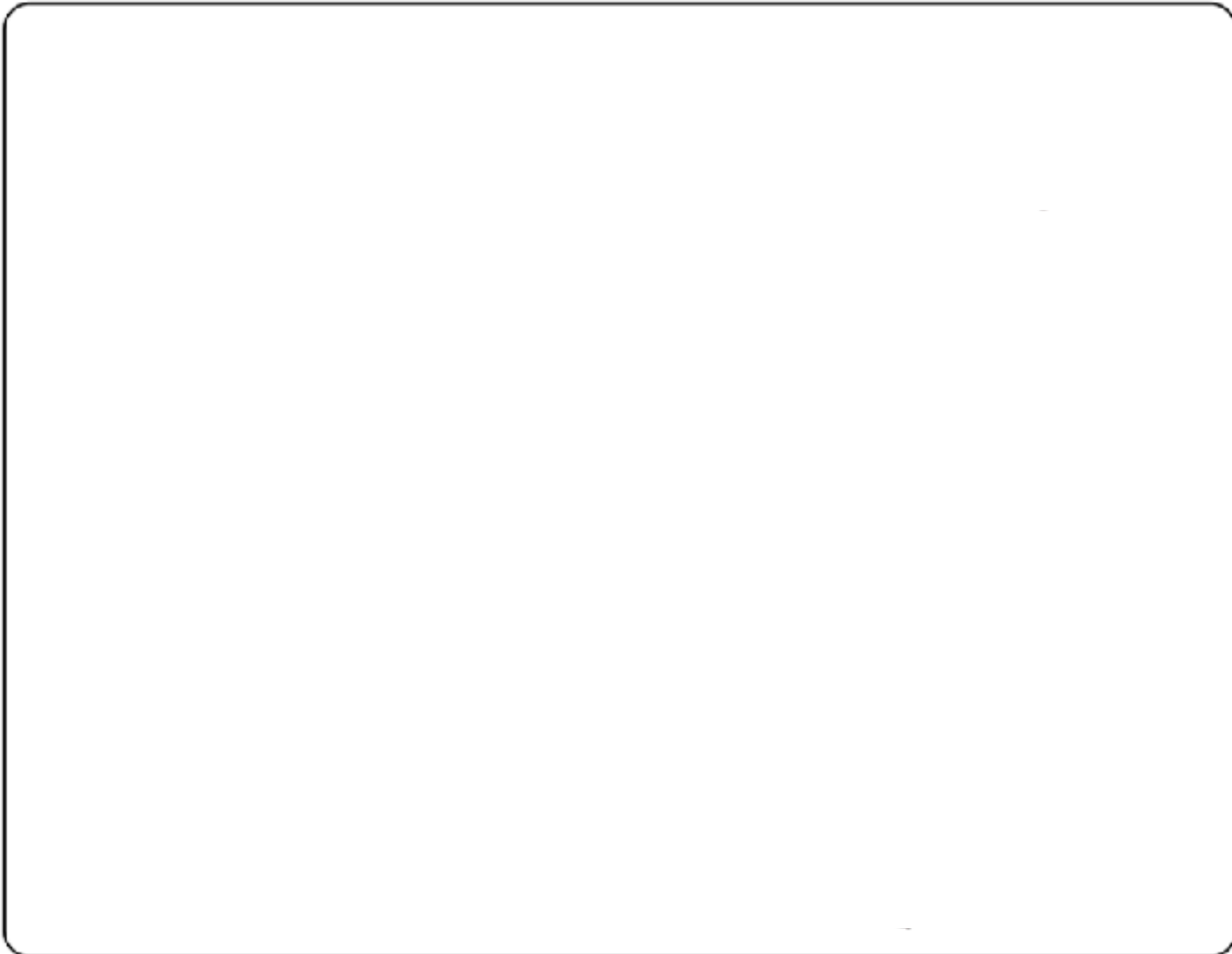
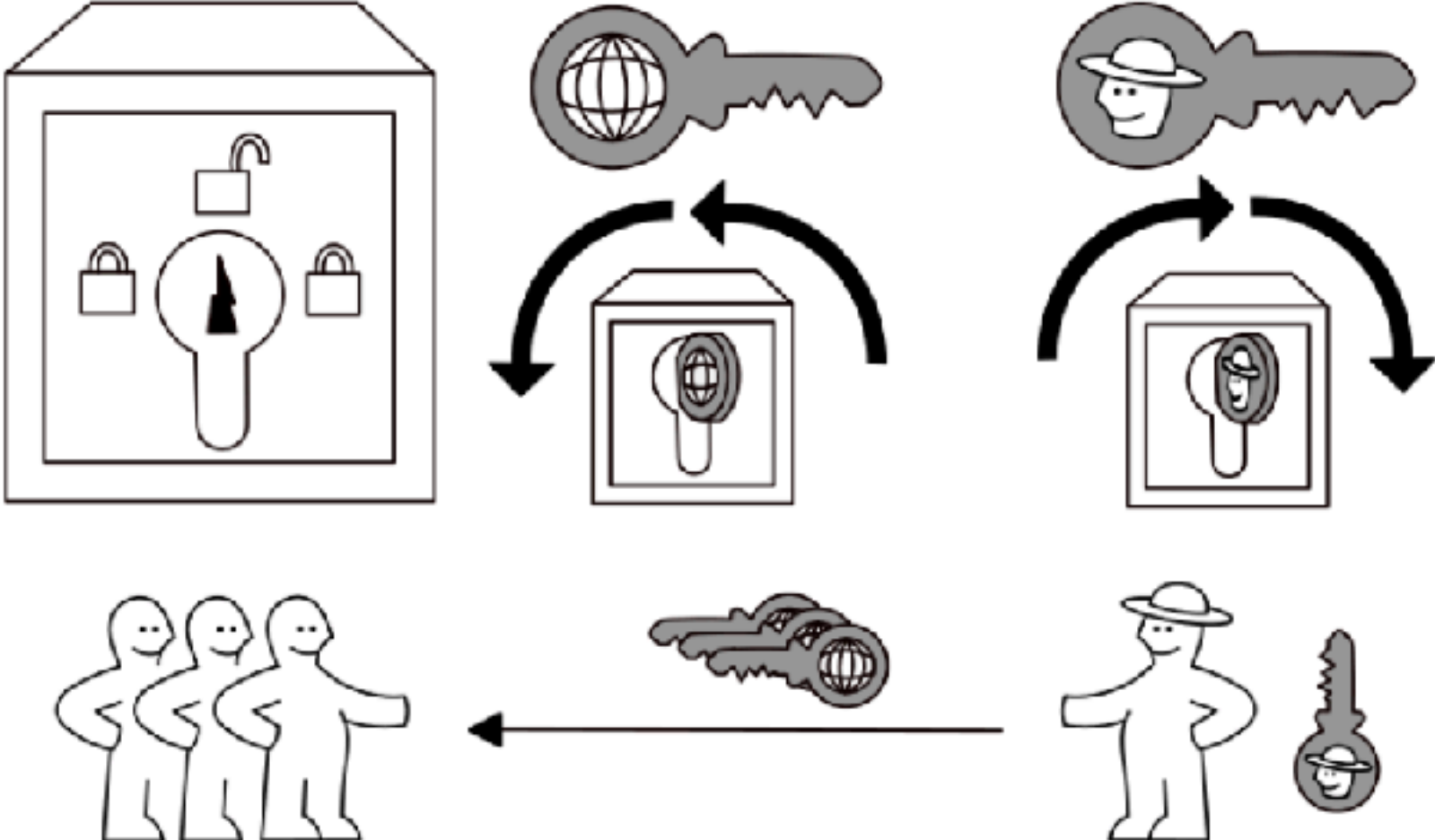
PUBLIK KEY KRYPTO



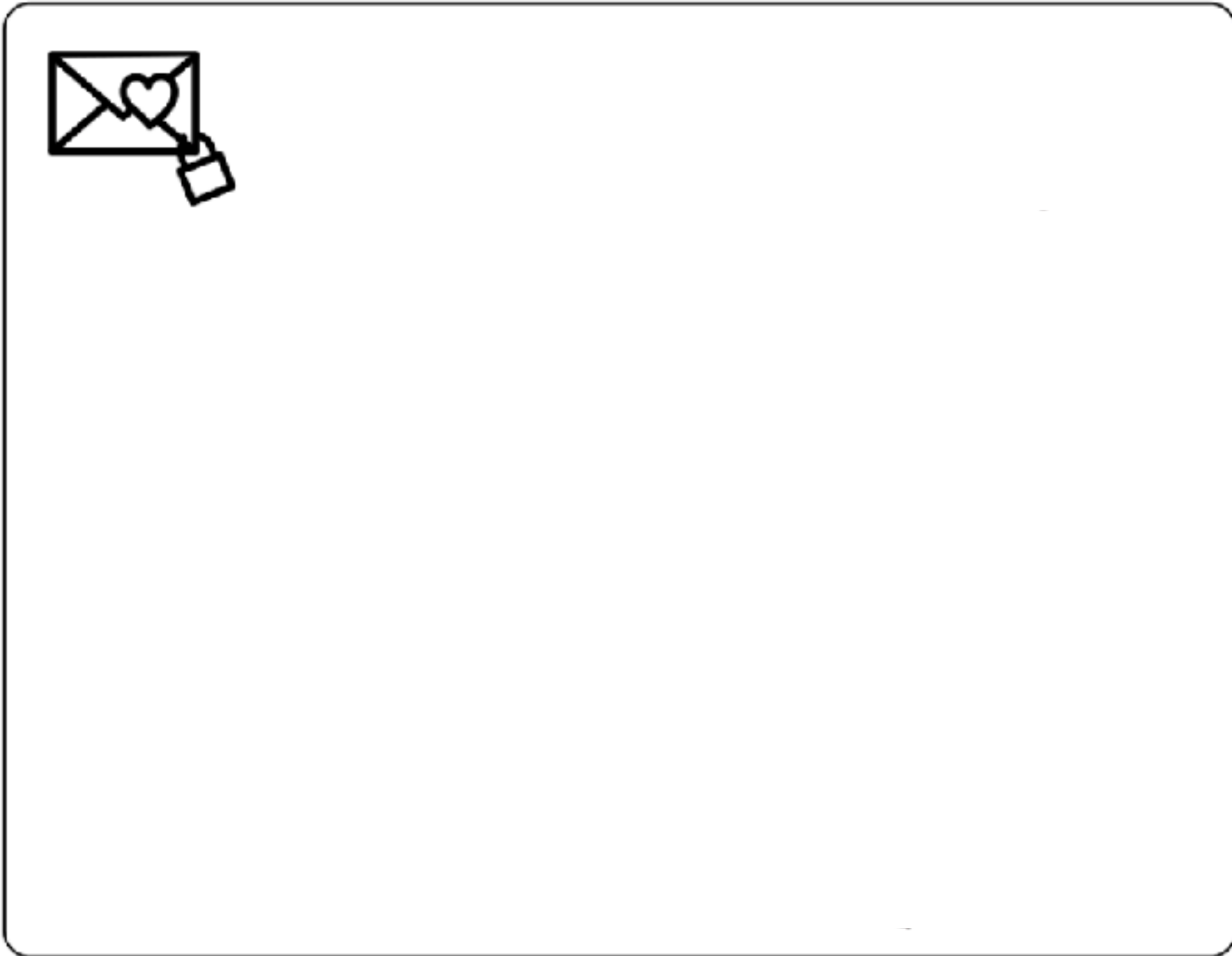
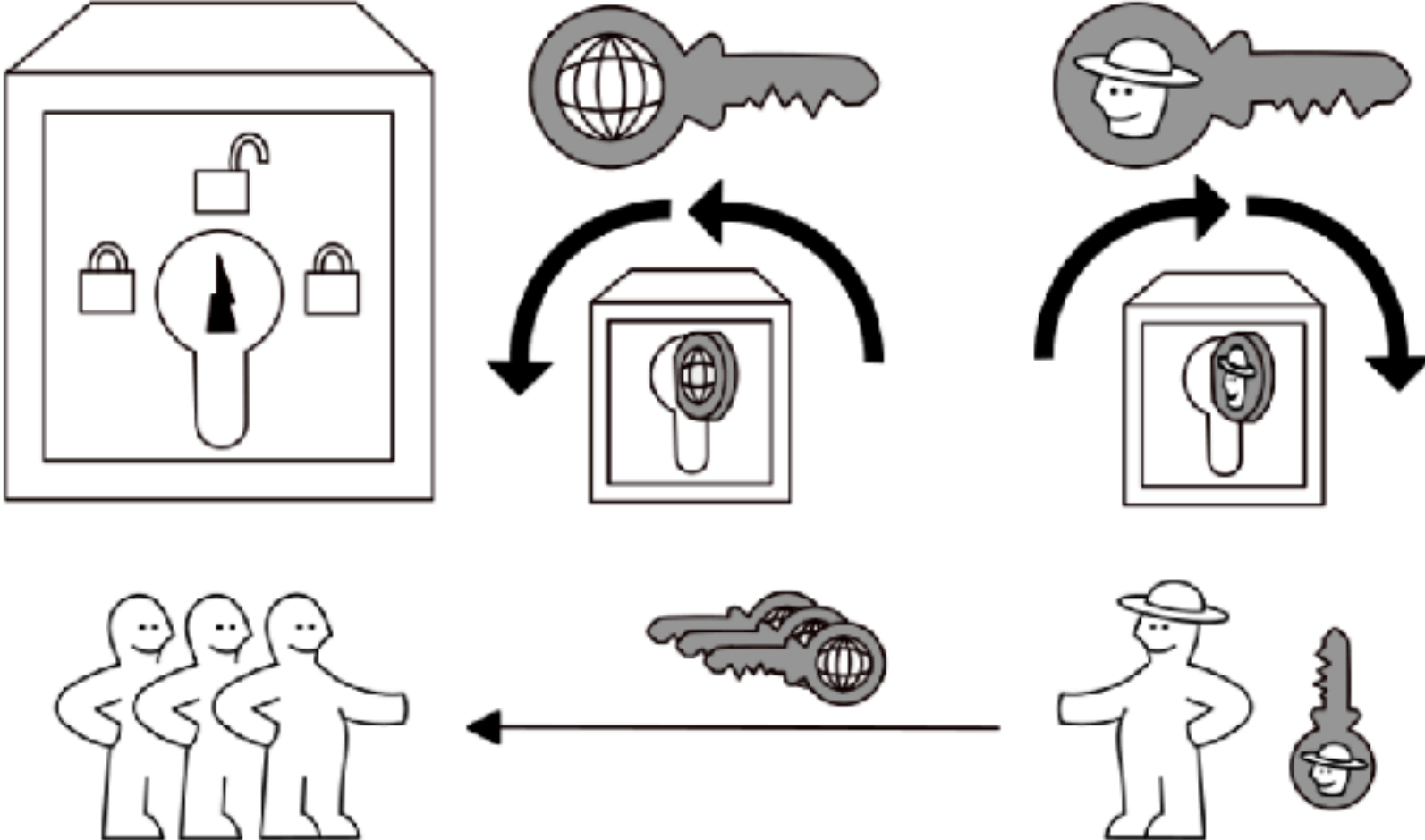
PUBLIK KEY KRYPTO



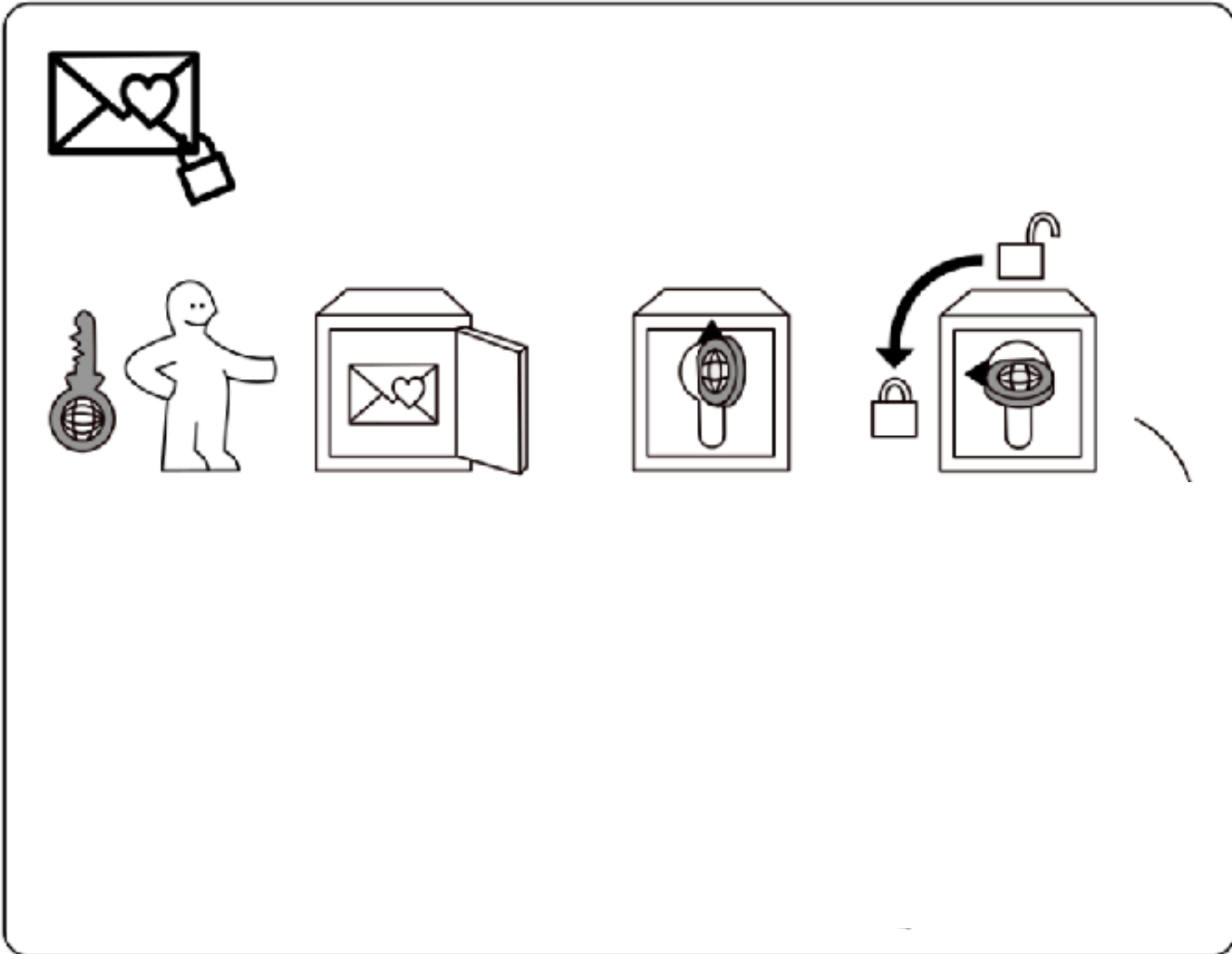
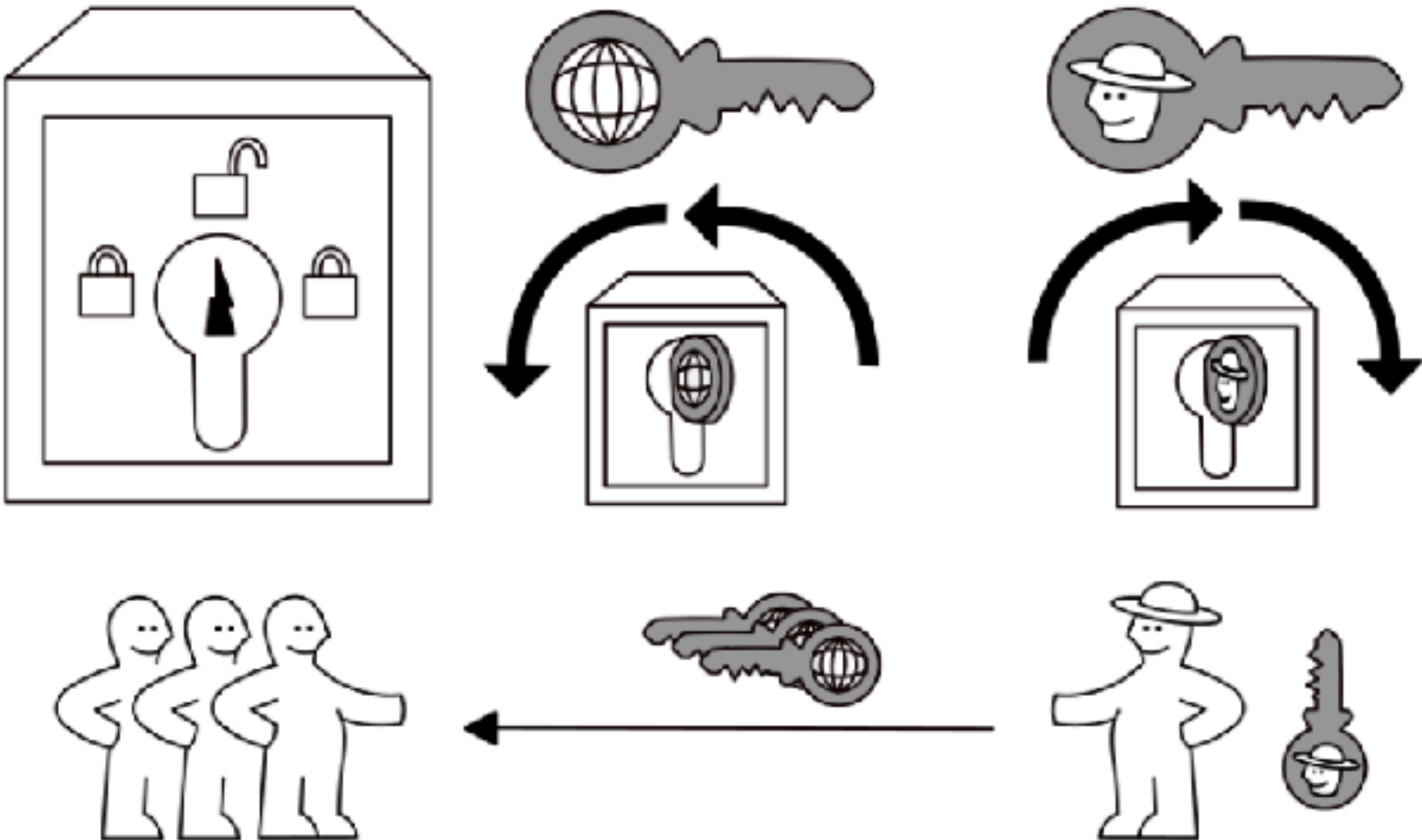
PUBLIK KEY KRYPTO



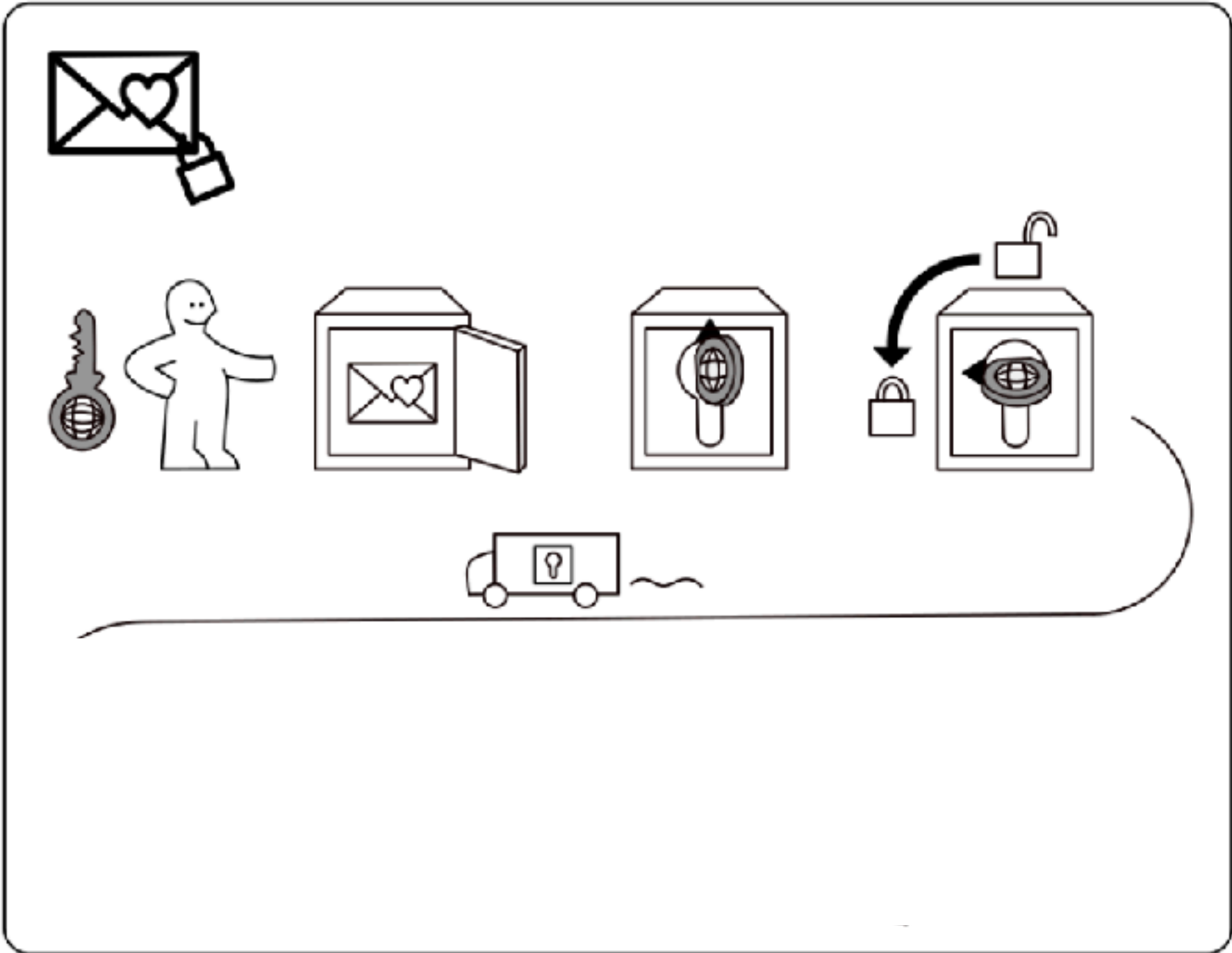
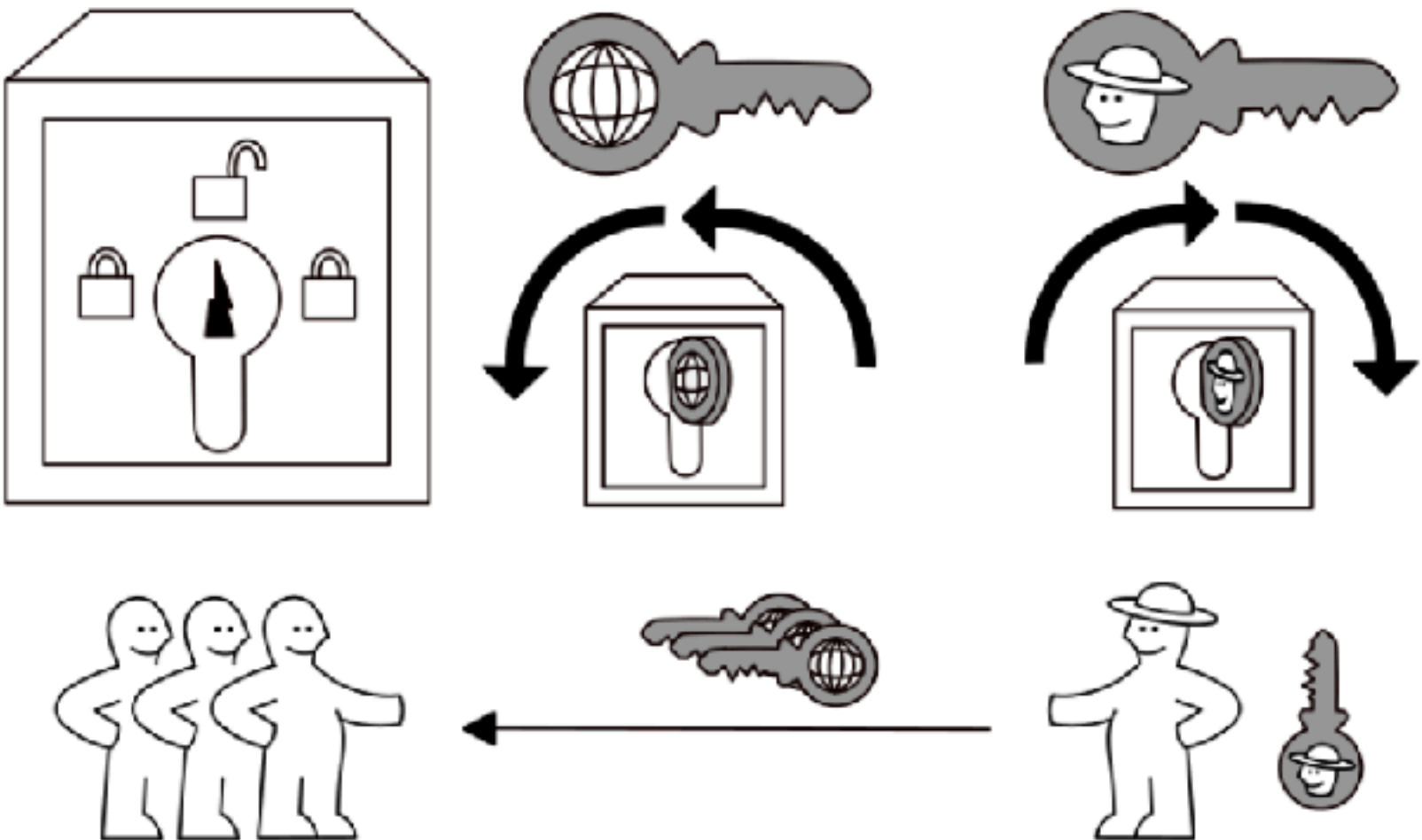
PUBLIK KEY KRYPTO



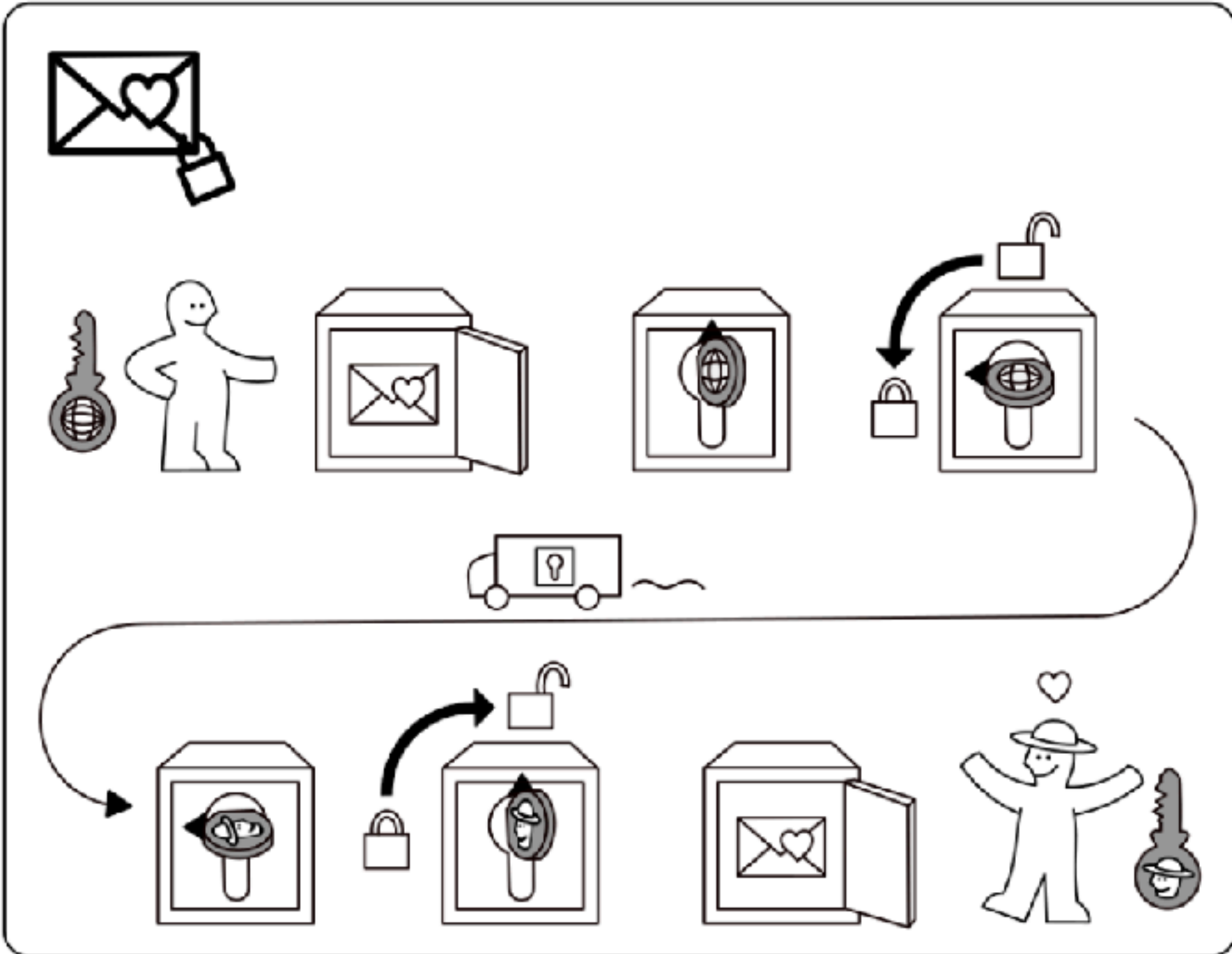
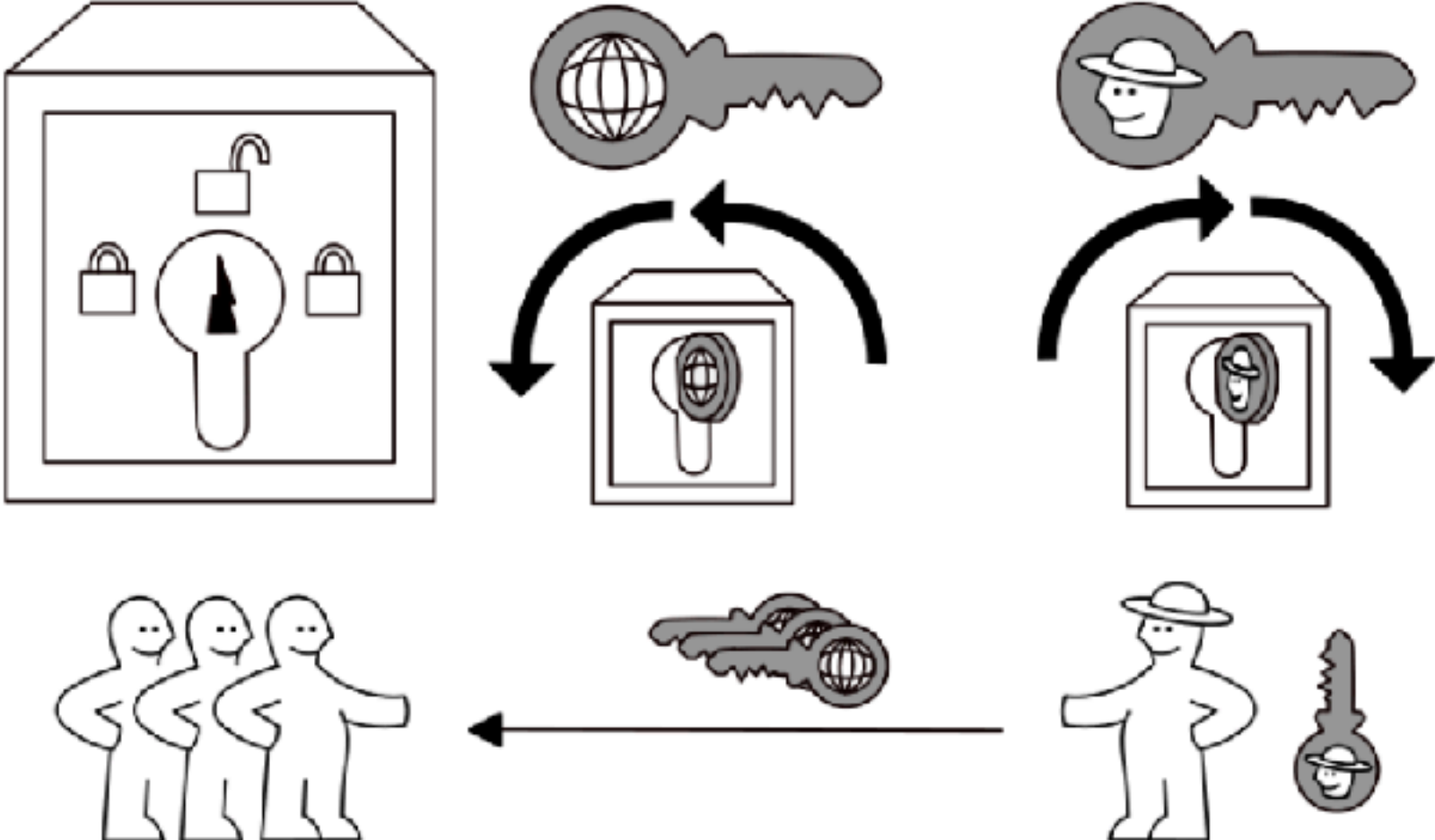
PUBLIK KEY KRYPTO



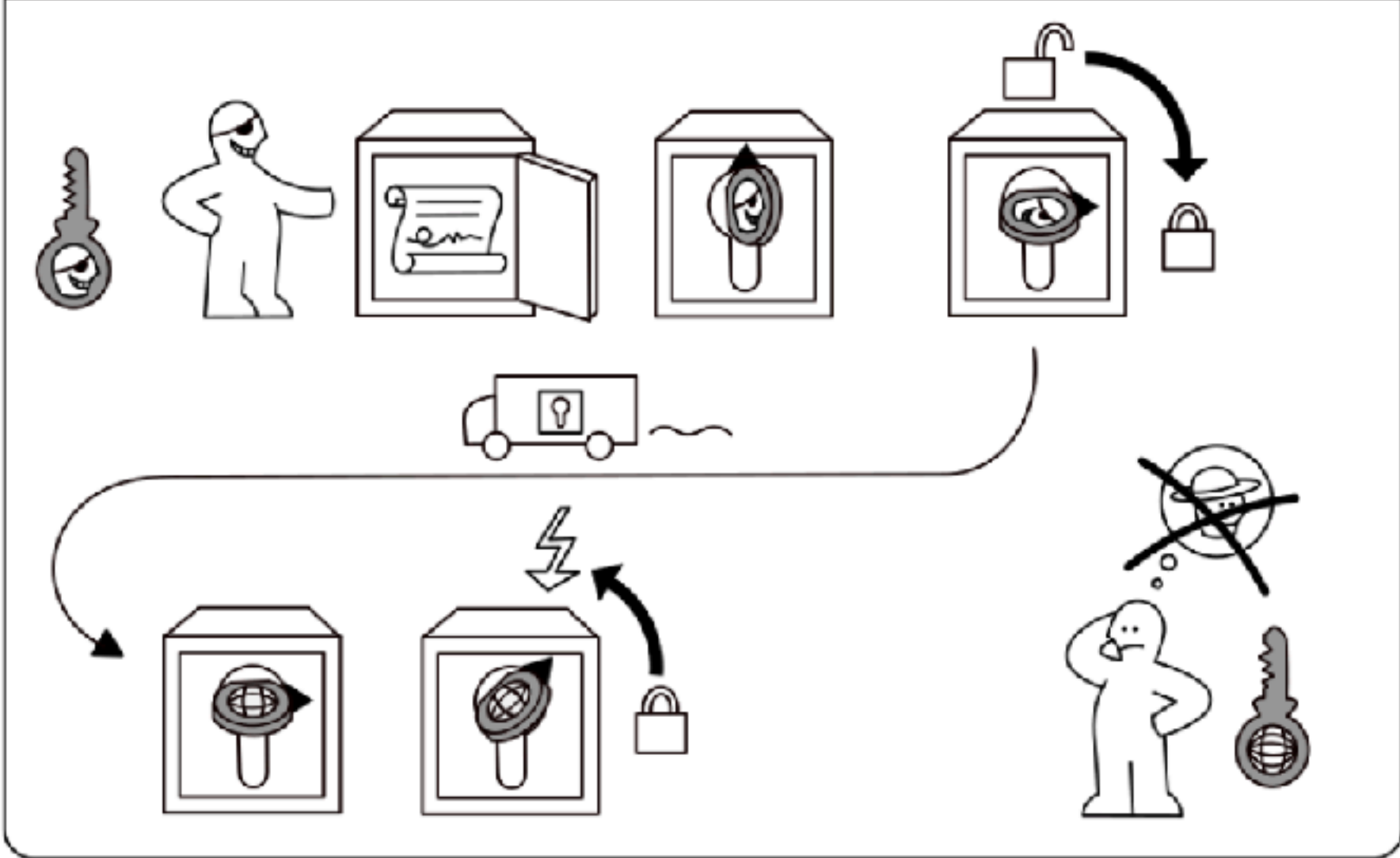
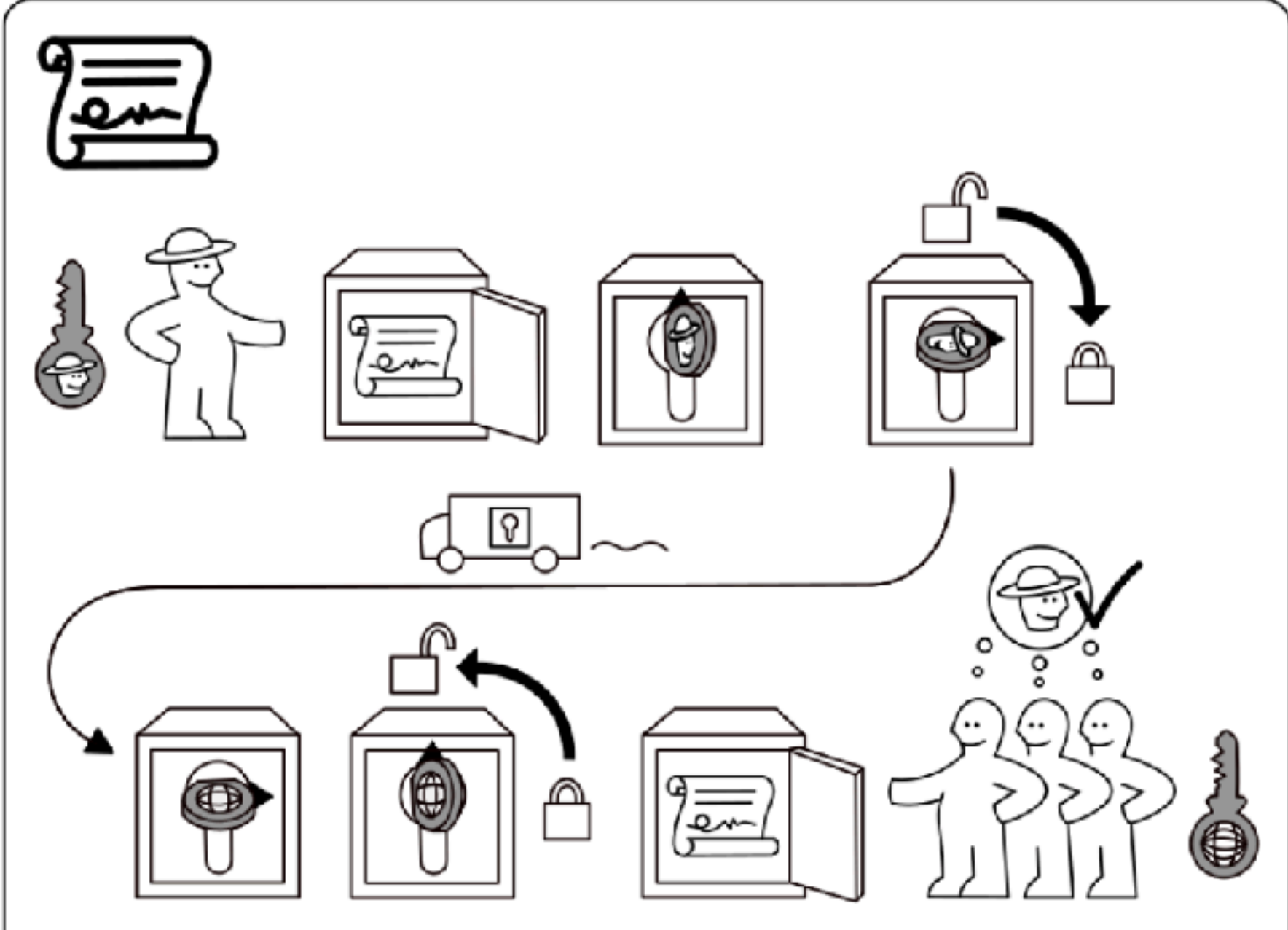
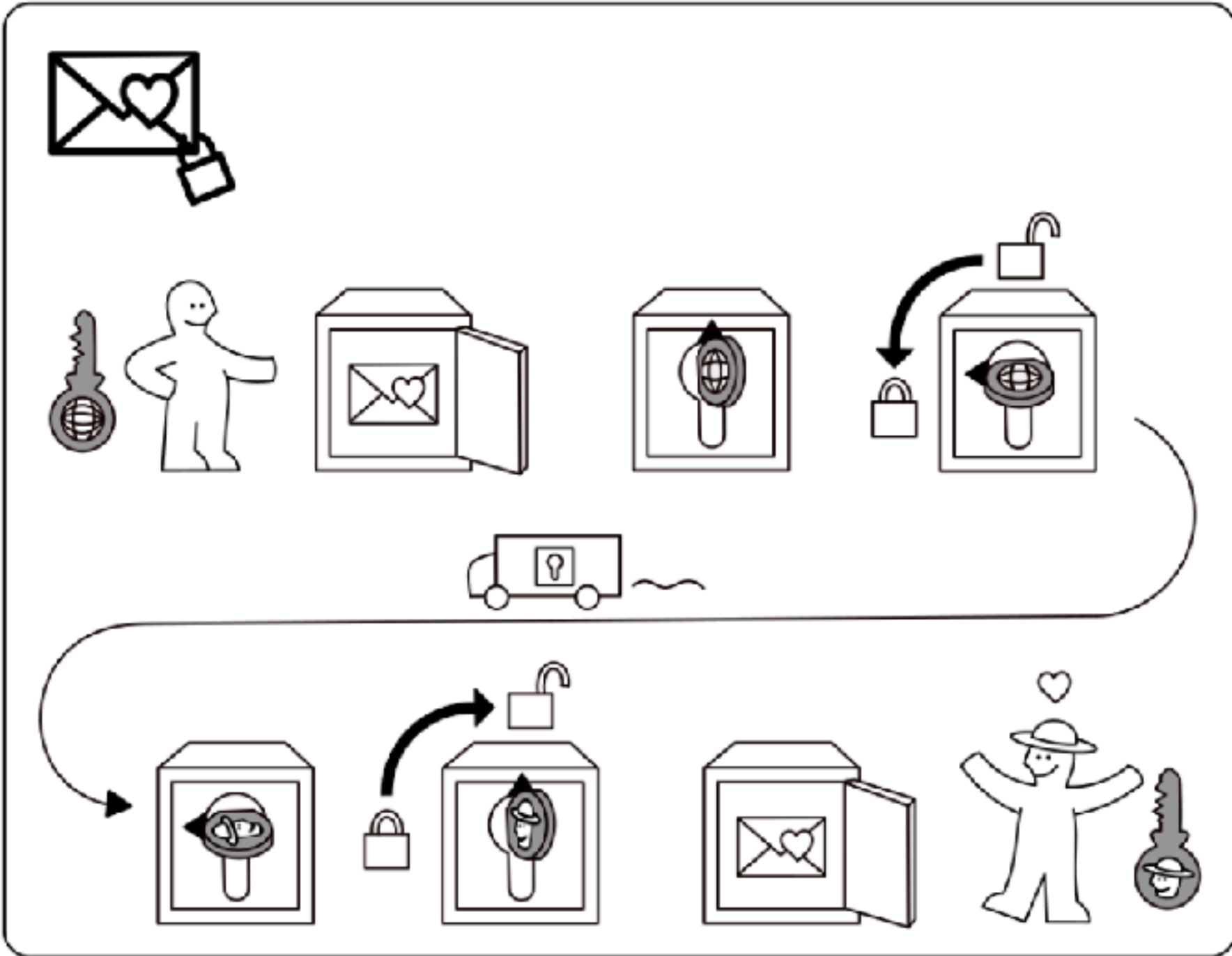
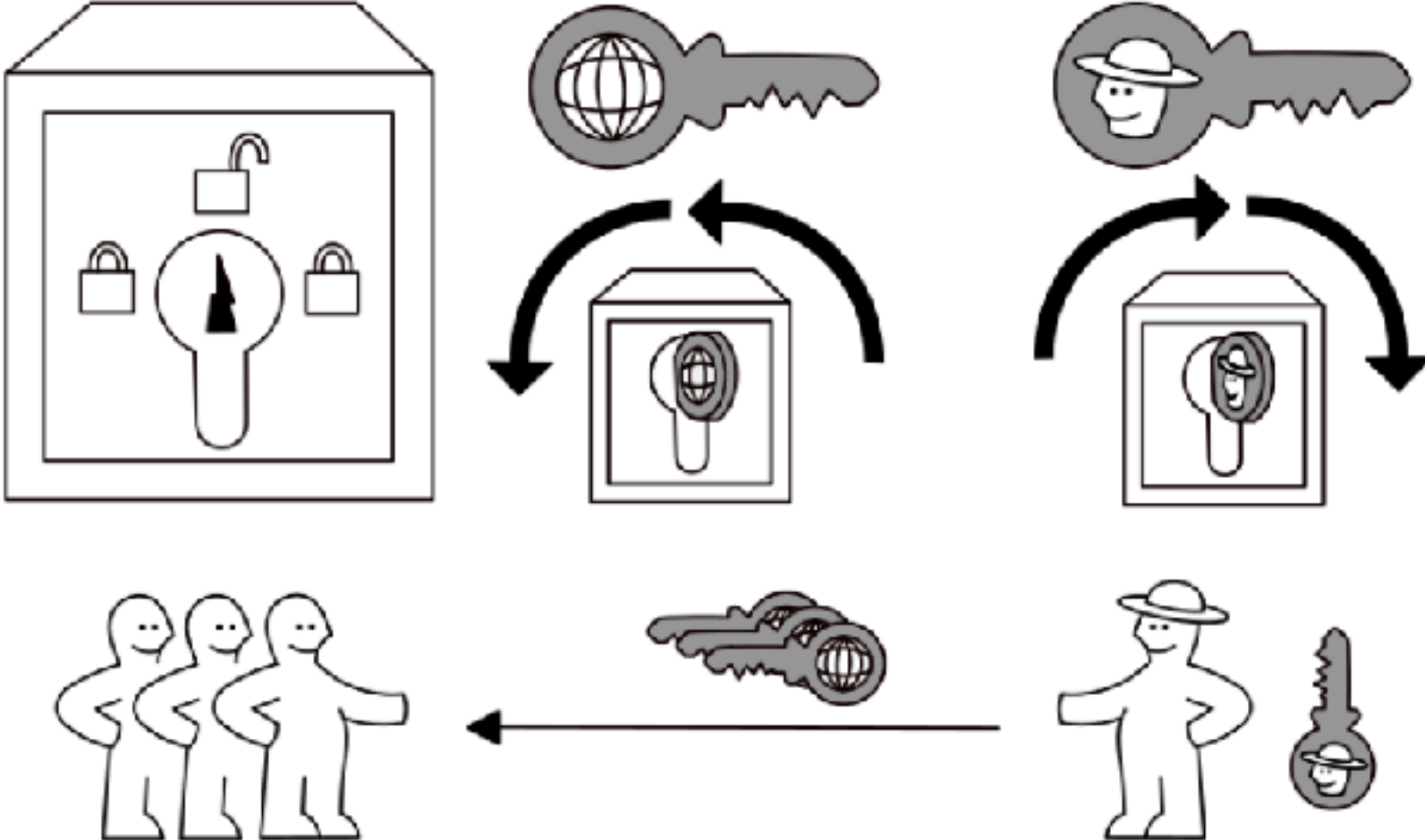
PUBLIK KEY KRYPTO



PUBLIK KEY KRYPTO



PUBLIK KEY KRYPTO



Vielen Dank!

s.fekete@tu-bs.de