BoxPics

Florian Giesen
CITS

April 9, 2010

Abstract

The `boxpics.tex` file contents diagrams and pictures in LaTeX-code for lecture notes of classes of the department of Cryptology and IT-Securety of the Ruhr-University Bochum (CITS).

1 Introduction

It is very simple to include the pictures in any documentclass. The pictures are scaled to fit in frames of the `beamerclass`. You only need to copy the `boxpics.tex` file to the directory in which you compile your `*.tex` file and add the line

```
\input{boxpics.tex}
```

to your preamble.

The pictures are written and saved in so called saveboxes in the `boxpics.tex` file. Every picture has an individual name (a complete list of all pictures and corresponding name is below in this manual) which allows you to call the picture in your lecture notes with the function `\boxpic{\name}`. If you need a frame around the picture like in this manual please use the function `\fboxpic{\name}`.

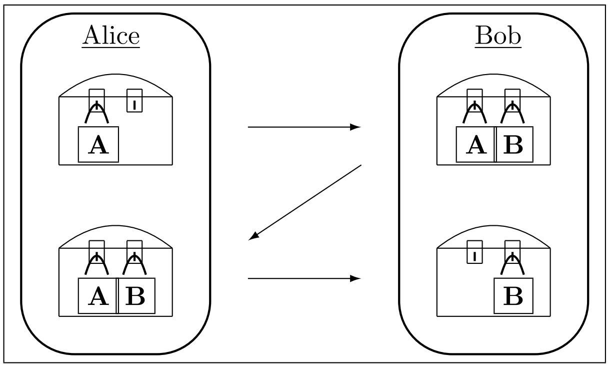
2 Cryptographie I

Comming soon.

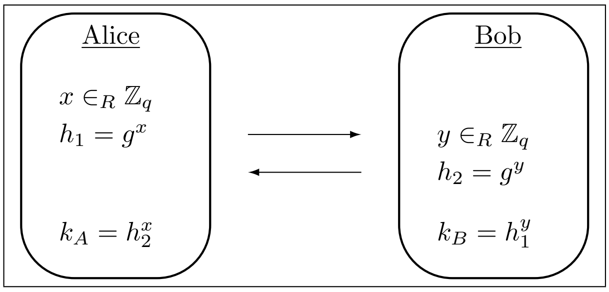
3 Cryptographie II

The referenced slidenumber is from the lecture notes of the class “Kryptographie 2” by Mr. May on Summer 2009.

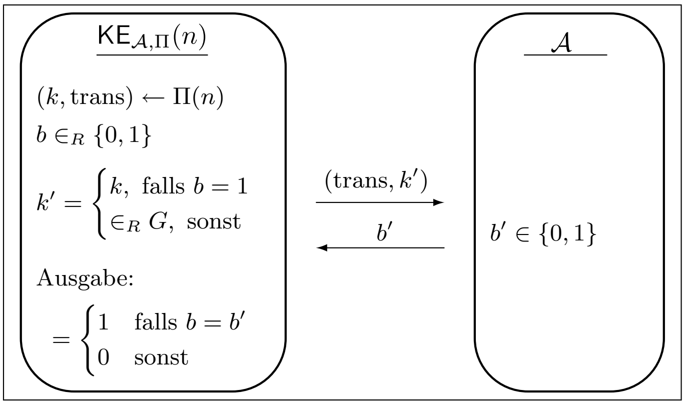
`\dRundenDH`: **3-Runden Diffie-Hellman Austausch** *(Folie 7)*



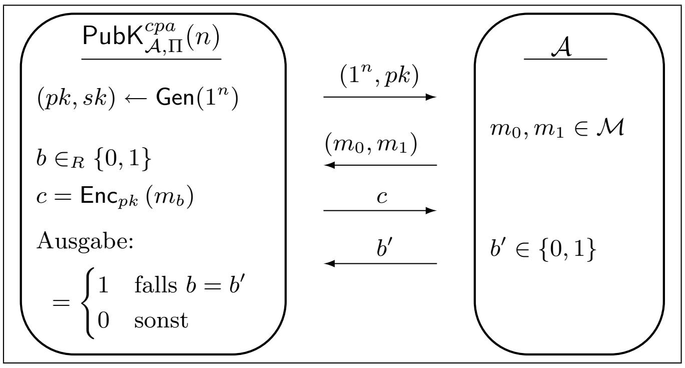
`\zRundenDH`: **2-Runden Diffie-Hellman Austausch** *(Folie 8)*



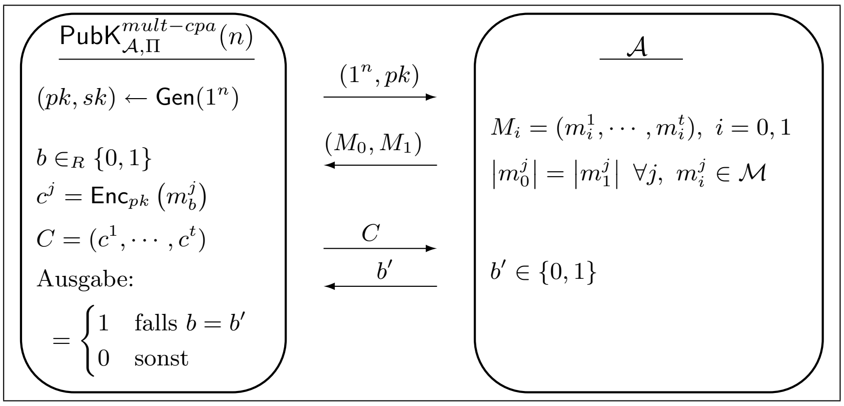
`\KESpiel`: **Spiel zur Unterscheidung des Schlüssels** *(Folie 10)*


$\mathsf{KE}_{\mathcal{A},\Pi}(n)$
$(k, \text{trans}) \leftarrow \Pi(n)$
$b \in_R \{0,1\}$
$k' = \begin{cases} k, & \text{falls } b = 1 \\ \in_R G, & \text{sonst} \end{cases}$
Ausgabe:
$= \begin{cases} 1 & \text{falls } b = b' \\ 0 & \text{sonst} \end{cases}$
(trans, k')
b'
$\mathcal{A}$
$b' \in \{0,1\}$

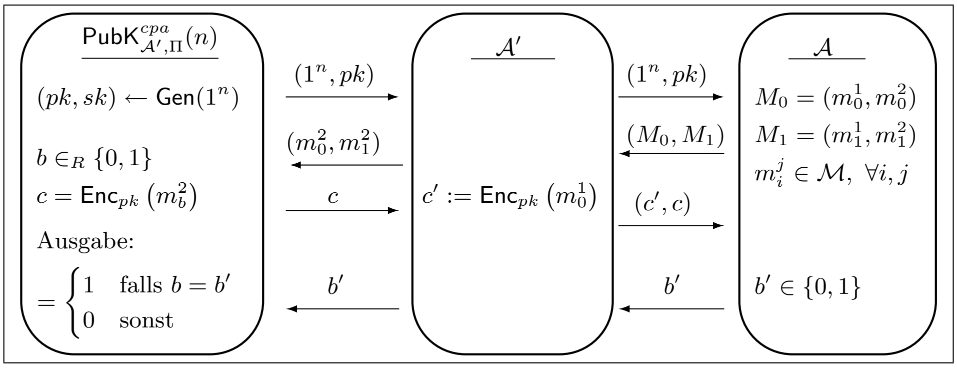
`\CPASpiel`: **CPA-Spiel** *(Folie 18)*


$\mathsf{PubK}^{cpa}_{\mathcal{A},\Pi}(n)$
$(pk, sk) \leftarrow \mathsf{Gen}(1^n)$
$b \in_R \{0,1\}$
$c = \mathsf{Enc}_{pk}(m_b)$
Ausgabe:
$= \begin{cases} 1 & \text{falls } b = b' \\ 0 & \text{sonst} \end{cases}$
$(1^n, pk)$
(m_0, m_1)
c
b'
$\mathcal{A}$
$m_0, m_1 \in \mathcal{M}$
$b' \in \{0,1\}$

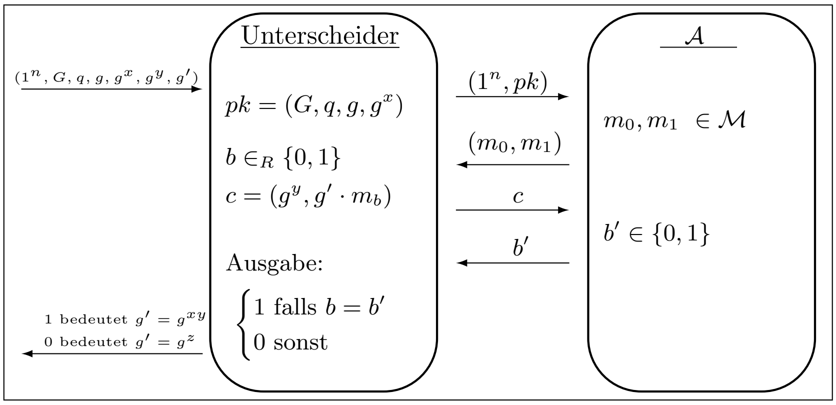
`\multCPASpiel`: **Mult-CPA-Spiel** *(Folie 21)*


$\mathsf{PubK}^{mult-cpa}_{\mathcal{A},\Pi}(n)$
$(pk, sk) \leftarrow \mathsf{Gen}(1^n)$
$b \in_R \{0,1\}$
$c^j = \mathsf{Enc}_{pk}\left(m_b^j\right)$
$C = (c^1, \cdots, c^t)$
Ausgabe:
$= \begin{cases} 1 & \text{falls } b = b' \\ 0 & \text{sonst} \end{cases}$
$(1^n, pk)$
(M_0, M_1)
C
b'
$\mathcal{A}$
$M_i = (m_i^1, \cdots, m_i^t),\ i = 0,1$
$\left|m_0^j\right| = \left|m_1^j\right|\ \forall j,\ m_i^j \in \mathcal{M}$
$b' \in \{0,1\}$

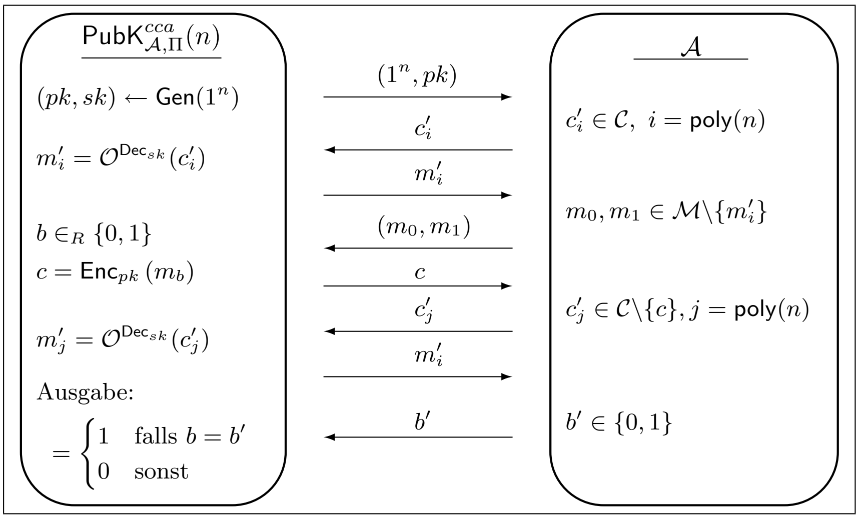
`\hybrid`: **Strategie im Hybridbeweis** *(Folie 23)*


$\mathsf{PubK}^{cpa}_{\mathcal{A}',\Pi}(n)$
$(pk, sk) \leftarrow \mathsf{Gen}(1^n)$
$b \in_R \{0,1\}$
$c = \mathsf{Enc}_{pk}\left(m_b^2\right)$
Ausgabe:
$= \begin{cases} 1 & \text{falls } b = b' \\ 0 & \text{sonst} \end{cases}$
$(1^n, pk)$
(m_0^2, m_1^2)
c
b'
$\mathcal{A}'$
$c' := \mathsf{Enc}_{pk}\left(m_0^1\right)$
$(1^n, pk)$
(M_0, M_1)
(c', c)
b'
$\mathcal{A}$
$M_0 = (m_0^1, m_0^2)$
$M_1 = (m_1^1, m_1^2)$
$m_i^j \in \mathcal{M},\ \forall i, j$
$b' \in \{0,1\}$

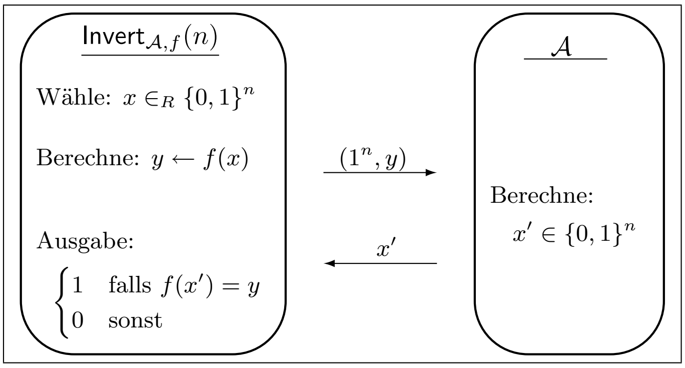
\`DDHUnterscheider`: **DDH-Unterscheider mit Angreifer $\mathcal{A}$** *(Folie 38)*



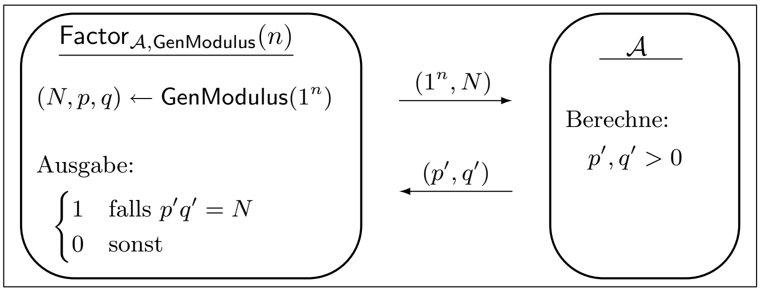
\`CCASpiel`: **CCA-Spiel** *(Folie 42)*


$\mathsf{PubK}^{cca}_{\mathcal{A},\Pi}(n)$
$(pk, sk) \leftarrow \mathsf{Gen}(1^n)$
$m_i' = \mathcal{O}^{\mathsf{Dec}_{sk}}(c_i')$
$b \in_R \{0,1\}$
$c = \mathsf{Enc}_{pk}(m_b)$
$m_j' = \mathcal{O}^{\mathsf{Dec}_{sk}}(c_j')$
Ausgabe:
$= \begin{cases} 1 & \text{falls } b = b' \\ 0 & \text{sonst} \end{cases}$
$(1^n, pk)$
c_i'
m_i'
(m_0, m_1)
c
c_j'
m_i'
b'
$\mathcal{A}$
$c_i' \in \mathcal{C},\ i = \mathsf{poly}(n)$
$m_0, m_1 \in \mathcal{M} \backslash \{m_i'\}$
$c_j' \in \mathcal{C} \backslash \{c\}, j = \mathsf{poly}(n)$
$b' \in \{0,1\}$

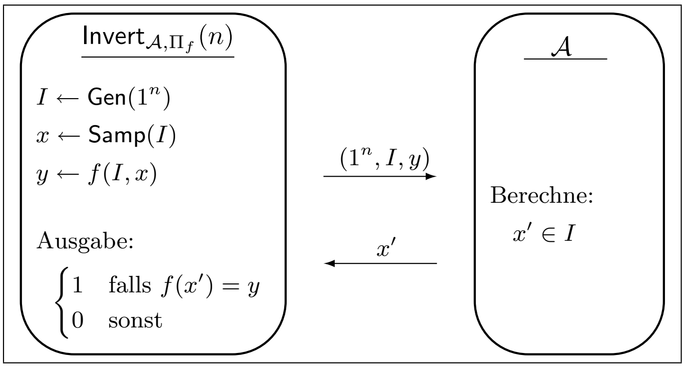
\`Invert`: **Spiel Invertieren** *(Folie 46)*


$\mathsf{Invert}_{\mathcal{A},f}(n)$
Wähle: $x \in_R \{0,1\}^n$
Berechne: $y \leftarrow f(x)$
Ausgabe:
$\begin{cases} 1 & \text{falls } f(x') = y \\ 0 & \text{sonst} \end{cases}$
$(1^n, y)$
x'
$\mathcal{A}$
Berechne:
$x' \in \{0,1\}^n$

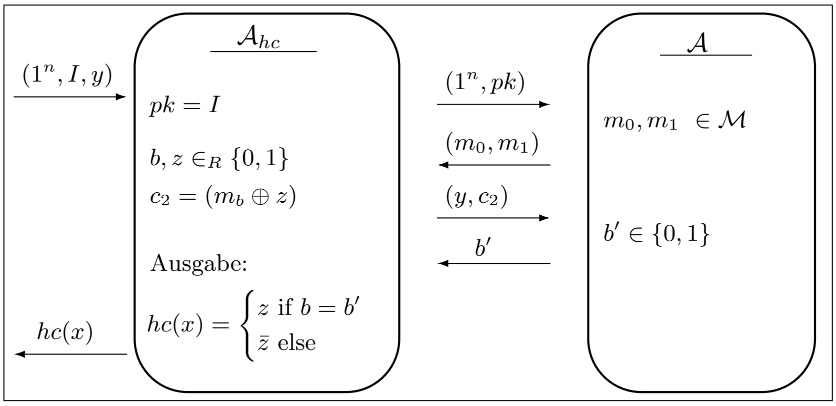
`\Factor`: **Spiel Faktorisieren** *(Folie 47)*


$\mathsf{Factor}_{\mathcal{A},\mathsf{GenModulus}}(n)$
$(N,p,q) \leftarrow \mathsf{GenModulus}(1^n)$
Ausgabe:
$\begin{cases} 1 & \text{falls } p'q' = N \\ 0 & \text{sonst} \end{cases}$
$(1^n, N)$
(p', q')
$\mathcal{A}$
Berechne:
$p', q' > 0$

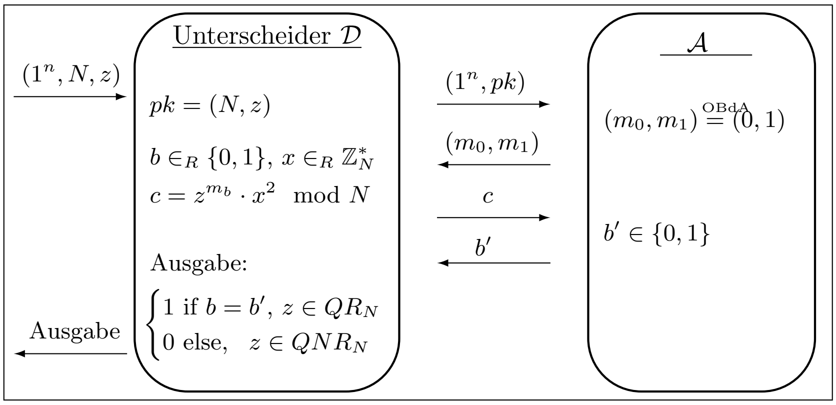
`\InvertTD`: **Spiel Invertieren eine Permutation** *(Folie 51)*


$\mathsf{Invert}_{\mathcal{A},\Pi_f}(n)$
$I \leftarrow \mathsf{Gen}(1^n)$
$x \leftarrow \mathsf{Samp}(I)$
$y \leftarrow f(I,x)$
Ausgabe:
$\begin{cases} 1 & \text{falls } f(x') = y \\ 0 & \text{sonst} \end{cases}$
$(1^n, I, y)$
x'
$\mathcal{A}$
Berechne:
$x' \in I$

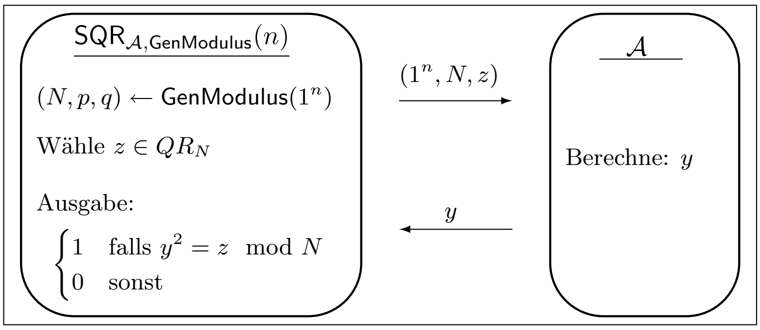
`\hcAngreifer`: **Algorithmus Angreifer $\mathcal{A}_{hc}$** *(Folie 55)*



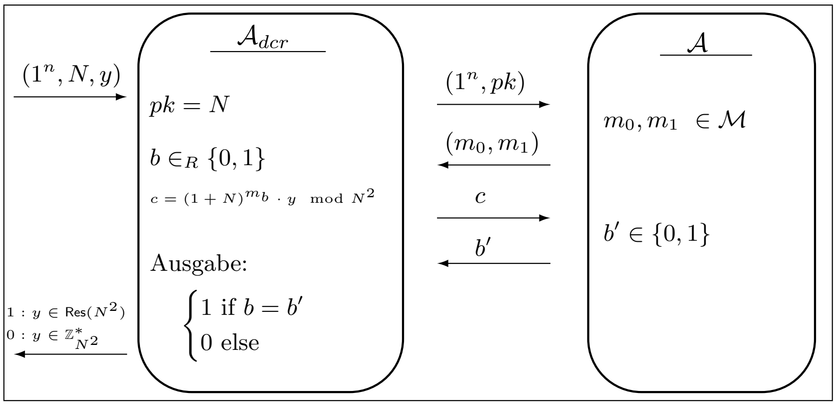
`\QRUnterscheider`: **Algorithmus QR-Unterscheider** *(Folie 64)*


Unterscheider $\mathcal{D}$
$(1^n, N, z)$
$pk = (N, z)$
$b \in_R \{0,1\}$, $x \in_R \mathbb{Z}_N^*$
$c = z^{m_b} \cdot x^2 \mod N$
Ausgabe:
$\begin{cases} 1 \text{ if } b = b',\ z \in QR_N \\ 0 \text{ else}, \quad z \in QNR_N \end{cases}$
Ausgabe
$(1^n, pk)$
(m_0, m_1)
c
b'
$\mathcal{A}$
$(m_0, m_1) \overset{\text{OBdA}}{=} (0, 1)$
$b' \in \{0,1\}$

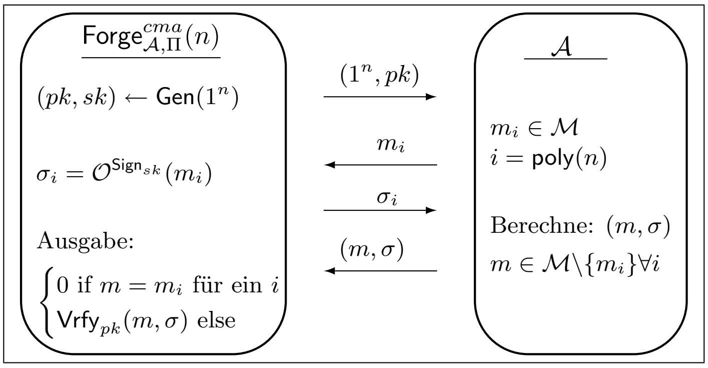
`\SQR`: **Spiel Wurzelziehen** *(Folie 68)*


$\mathsf{SQR}_{\mathcal{A},\mathsf{GenModulus}}(n)$
$(N, p, q) \leftarrow \mathsf{GenModulus}(1^n)$
Wähle $z \in QR_N$
Ausgabe:
$\begin{cases} 1 & \text{falls } y^2 = z \mod N \\ 0 & \text{sonst} \end{cases}$
$(1^n, N, z)$
y
$\mathcal{A}$
Berechne: y

`\dcrUnterscheider`: **Algorithmus DCR Unterscheider $\mathcal{A}_{dcr}$** *(Folie 86)*


$(1^n, N, y)$
$\mathcal{A}_{dcr}$
$pk = N$
$b \in_R \{0,1\}$
$c = (1+N)^{m_b} \cdot y \mod N^2$
Ausgabe:
$\begin{cases} 1 \text{ if } b = b' \\ 0 \text{ else} \end{cases}$
$1 : y \in \mathsf{Res}(N^2)$
$0 : y \in \mathbb{Z}^*_{N^2}$
$(1^n, pk)$
(m_0, m_1)
c
b'
$\mathcal{A}$
$m_0, m_1 \in \mathcal{M}$
$b' \in \{0,1\}$

\CMAForge: **CMA Spiel Forge** *(Folie 93)*


$\mathsf{Forge}^{cma}_{\mathcal{A},\Pi}(n)$
$(pk, sk) \leftarrow \mathsf{Gen}(1^n)$
$\sigma_i = \mathcal{O}^{\mathsf{Sign}_{sk}}(m_i)$
Ausgabe:
$\begin{cases} 0 \text{ if } m = m_i \text{ für ein } i \\ \mathsf{Vrfy}_{pk}(m, \sigma) \text{ else} \end{cases}$
$(1^n, pk)$
m_i
σ_i
(m, σ)
$\mathcal{A}$
$m_i \in \mathcal{M}$
$i = \mathsf{poly}(n)$
Berechne: (m, σ)
$m \in \mathcal{M} \backslash \{m_i\} \forall i$