Hardcore-Prädikat

Ziel: Destilliere Komplexität des Invertierens auf ein Bit.

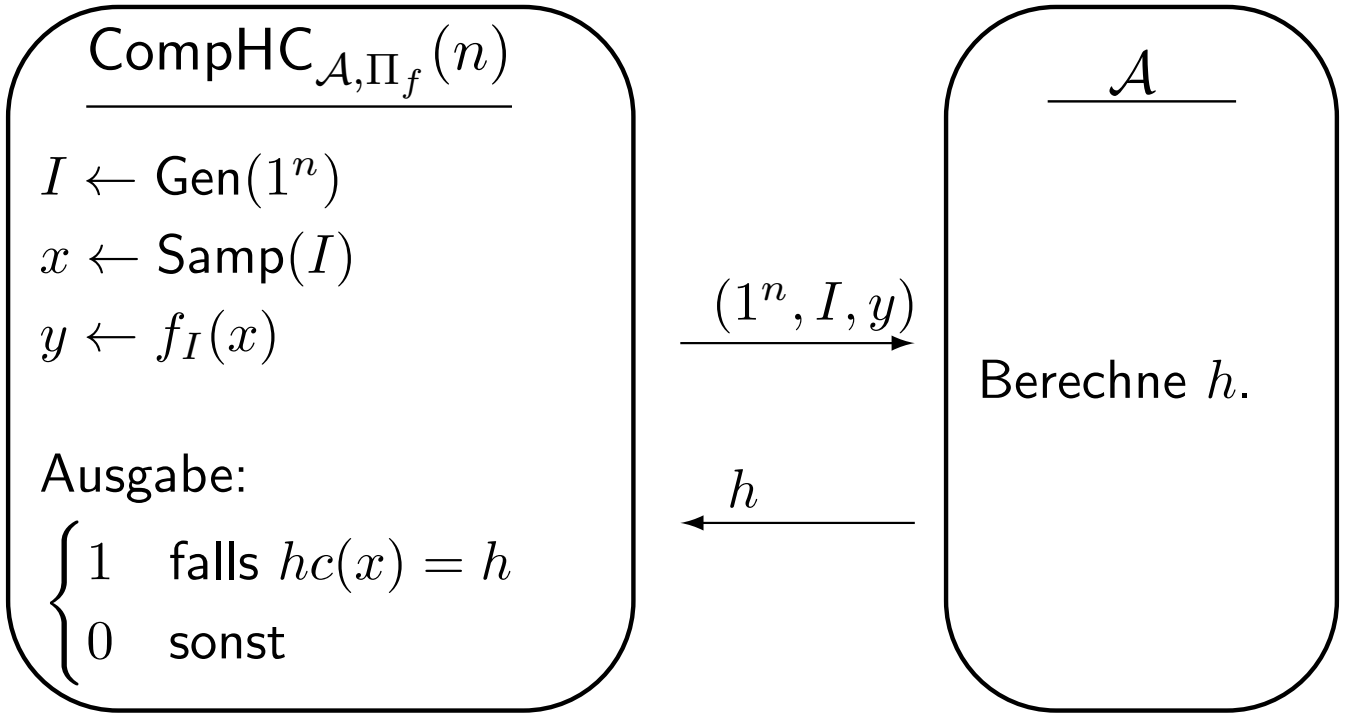
Definition Hardcore-Prädikat

Sei Π_f eine Einwegfunktion. Sei *hc* ein deterministischer pt Alg mit Ausgabe eines Bits $hc(x)$ bei Eingabe $x \in D$. *hc* heißt *Hardcore-Prädikat* für f falls für alle ppt Algorithmen $\mathcal{A}$ gilt:

$$\mathrm{Ws}[\mathcal{A}(1^n, I, f(x)) = hc(x)]] \leq \tfrac{1}{2} + \mathrm{negl}(n).$$

Intuition: Bild $f(x)$ hilft nicht beim Berechnen von $hc(x)$.

Spiel zum Berechnen des Hardcore-Prädikats



Falls *hc* ein Hardcoreprädikat ist, so gilt für alle ppt $\mathcal{A}$

$$\mathrm{Ws}[\mathit{CompHC}_{\mathcal{A},\Pi_f}(n) = 1] = \mathrm{Ws}[\mathcal{A}(1^n, I, f(x)) = hc(x)]] \leq \tfrac{1}{2} + \mathrm{negl}(n).$$

Hardcore-Prädikate

- $hc(x) := lsb(x)$ (least significant bit) ist ein Hardcoreprädikat für die RSA Einwegpermutation Π_{RSA} (unter der RSA Annahme).
- Es kann kein festes Hardcoreprädikat hc für alle Einwegfunktionen geben.
- Warum? Sei Π_f Einwegfunktion mit Hardcoreprädikat hc. Dann ist Π_g mit $g(x) := f(x)||hc(x)$ auch eine Einwegfunktion, aber hc kein Hardcoreprädikat von Π_g.
- Aber: Man kann jede Einwegfunktion Π_f zu einer Einwegfunktion Π_g mit einem festen Hardcoreprädikat verändern.

Goldreich-Levin Hardcore-Prädikat

Satz von Goldreich-Levin

Sei Π_f eine Einwegpermutation. Dann existiert eine Einwegpermutation Π_g mit Hardcoreprädikat *hc*.

Konstruktion: (ohne Beweis)

- Sei f eine Einwegpermutation mit Definitionsbereich $\{0,1\}^n$.
- Sei $x = x_1 \dots x_n \in \{0,1\}^n$. Konstruiere
$$g(x,r) := (f(x), r) \text{ mit } r \in_R \{0,1\}^n.$$
- Offenbar ist g ebenfalls eine Einwegpermutation.
- Wir konstruieren ein Hardcore-Prädikat hc für g mittels
$$hc(x,r) = \langle x, r \rangle = \sum_{i=1}^{n} x_i r_i \bmod 2.$$
- Beweis der Hardcore-Eigenschaft ist nicht-trivial.

Verschlüsselung aus Trapdoor-Einwegpermutation

Algorithmus Π_{cpa}

Sei Π_f eine Td-Einwegpermutation mit Hardcore-Prädikat hc.

1. **Gen:** $(I, td) \leftarrow Gen(1^n)$. Ausgabe $pk = I$ und $sk = td$.
2. **Enc:** Für $m \in \{0,1\}$ setze $x \leftarrow Sample(I)$ und berechne
$$c \leftarrow (f(x), hc(x) \oplus m).$$
3. **Dec:** Für Chiffretext $c = (c_1, c_2)$ berechne $x := Inv_{td}(c_1)$ und
$$m := c_2 \oplus hc(x).$$

Intuition:

- $hc(x)$ ist "pseudozufällig" gegeben $f(x)$.
- D.h. $hc(x) \oplus m$ ist ununterscheidbar von 1-Bit One-Time Pad.

Bsp: Verschlüsselung mit RSA-Td-Einwegpermutation

Algorithmus Π^{rsa}_{cpa}

Sei Π_{rsa} die RSA Td-Einwegpermutation mit Hardcore-Prädikat hc.

1. **Gen:** $(N, e, d) \leftarrow GenRSA(1^n)$. Ausgabe $pk = (N, e)$ und $sk = (N, d)$.
2. **Enc:** Für $m \in \{0,1\}$ wähle $r \in_R \mathbb{Z}_N^*$ und berechne
$$c \leftarrow (r^e \bmod N, hc(r) \oplus m).$$
3. **Dec:** Für Chiffretext $c = (c_1, c_2)$ berechne $r := c_1^d \bmod N$ und
$$m \leftarrow c_2 \oplus hc(r).$$

CPA-Sicherheit unserer Konstruktion

Satz CPA-Sicherheit von Π_{cpa}

Sei Π_f eine Trapdoor-Einwegpermutation mit Hardcore-Prädikat hc. Dann ist Π_{cpa} CPA-sicher.

Beweis:

- Sei $\mathcal{A}$ ein Angreifer mit Erfolgsws $\epsilon(n) = \mathrm{Ws}[PubK^{cpa}_{\mathcal{A},\Pi_f}(n) = 1]$.
- OBdA $(m_0, m_1) \leftarrow \mathcal{A}(pk)$ mit $\{m_0, m_1\} = \{0,1\}$. (Warum?)
- Verwenden $\mathcal{A}$, um $\mathcal{A}'$ im Spiel $CompHC_{\mathcal{A}',\Pi_f}(n)$ zu konstruieren.

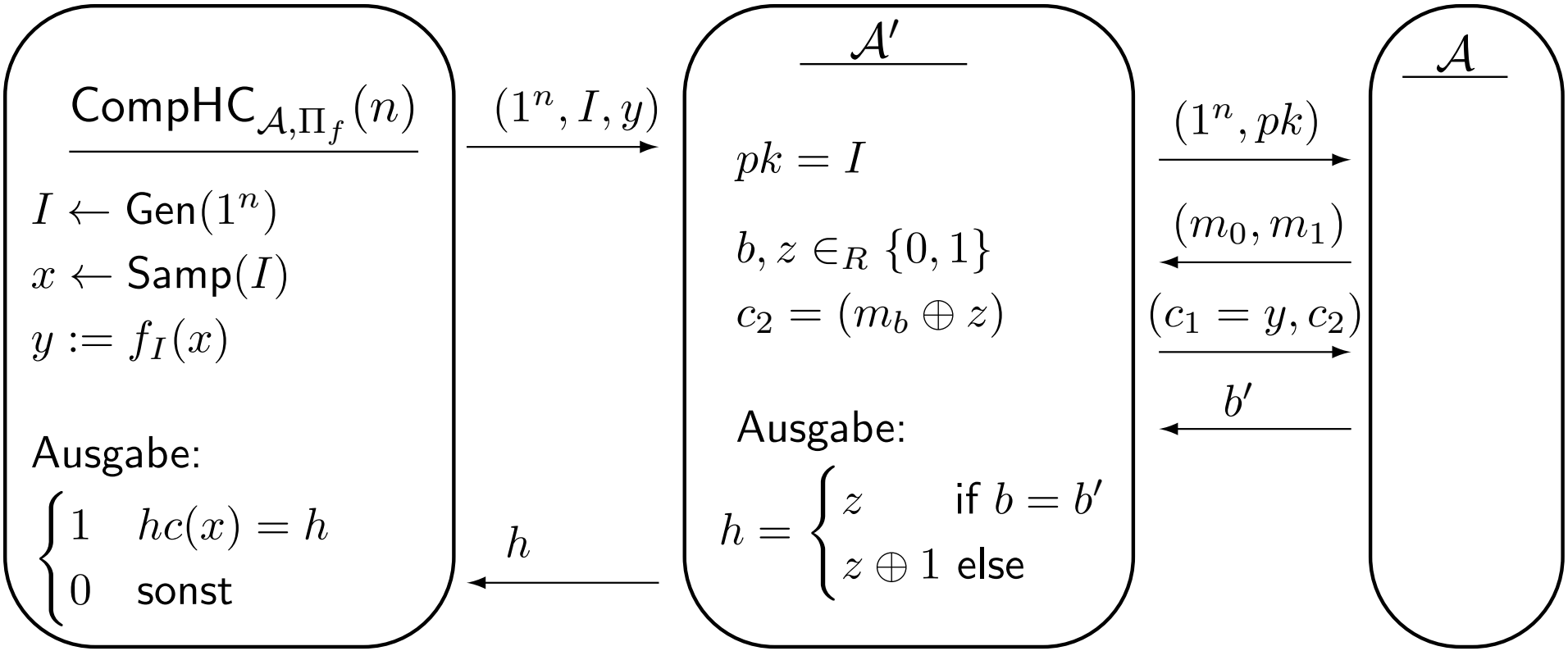
Algorithmus Angreifer $\mathcal{A}'$

Eingabe: $1^n, I, y = f(x) \in D$

1. Setze $pk \leftarrow I$ und berechne $(m_0, m_1) \leftarrow \mathcal{A}(pk)$.
2. Wähle $b, z \in_R \{0,1\}$. Setze $c_2 \leftarrow m_b \oplus z$.
3. $b' \leftarrow \mathcal{A}(y, c_2)$

Ausgabe: $h = \begin{cases} z & \text{falls } b = b' \\ \bar{z} & \text{sonst} \end{cases}$.

Angreifer $\mathcal{A}'$ für das Hardcore-Prädikat



CPA-Sicherheit von Π_{cpa}

Beweis: Fortsetzung

- Sei $x = f^{-1}(y)$. Idee: $\mathcal{A}'$ rät $z = hc(x)$.
- Es gilt $\mathrm{Ws}[\mathcal{A}'(f(x)) = hc(x)] =$
$$\frac{1}{2} \cdot \mathrm{Ws}[b = b' \mid z = hc(x)] + \frac{1}{2} \cdot \mathrm{Ws}[b \neq b' \mid z \neq hc(x)].$$
- **1. Fall** $z = hc(x)$: (y, c_2) ist korrekte Verschlüsselung von m_b, d.h.
$$\mathrm{Ws}[b = b' \mid z = hc(x)] = \epsilon(n).$$
- **2. Fall** $z \neq hc(x)$: Es gilt
$$\begin{aligned}(y, c_2) &= (f(x), z \oplus m_b) \\ &= (f(x), z \oplus 1 \oplus m_b \oplus 1) = (f(x), hc(x) \oplus m_b \oplus 1).\end{aligned}$$
D.h. (y, c_2) ist korrekte Verschlüsselung von $m_b \oplus 1 = m_{1-b}$.
$$\mathrm{Ws}[b \neq b' \mid z \neq hc(x)] = \mathrm{Ws}[1 - b = b' \mid z \oplus 1 = hc(x)] = \epsilon(n).$$

Da hc ein Hardcore-Prädikat ist, folgt

$$\frac{1}{2} + \mathrm{negl}(n) \geq \mathrm{Ws}[A'(f(x)) = hc(x)] = \epsilon(n).$$