

# Trapdoor-Permutationsfamilie

## Definition Permutationsfamilie

Eine *Permutationsfamilie*  $\Pi_f = (Gen, Samp, f)$  besteht aus 3 ppt Alg:

- 1  $I \leftarrow Gen(1^n)$ , wobei  $I$  eine Urbildmenge  $D$  für  $f$  definiert.
- 2  $x \leftarrow Samp(I)$ , wobei  $x \in_R D$ .
- 3  $y \leftarrow f(I, x)$  mit  $y := f(x) \in D$  und  $f : D \leftarrow D$  ist bijektiv.

## Definition Trapdoor-Permutationsfamilie

*Trapdoor-Permutationsfamilie*  $\Pi_f = (Gen, Samp, f, Inv)$  besteht aus

- 1  $(I, td) \leftarrow Gen(1^n)$  mit  $td$  als Trapdoor-Information
- 2  $x \leftarrow Samp(I)$  wie zuvor
- 3  $y \leftarrow f(I, x)$  wie zuvor
- 4  $x \leftarrow Inv(td, y)$  mit  $Inv_{td}(f(x)) = x$  für alle  $x \in D$ .

# Invertieren einer Permutation

## Spiel Invertieren einer Permutation $\text{Invert}_{\mathcal{A}, \Pi_f}(n)$

Sei  $\mathcal{A}$  ein Invertierer für die Familie  $\Pi_f$ .

- 1  $I \leftarrow \text{Gen}(1^n)$ ,  $x \leftarrow \text{Samp}(I)$  und  $y \leftarrow f(I, x)$ .
- 2  $x' \leftarrow \mathcal{A}(I, y)$ .
- 3  $\text{Invert}_{\mathcal{A}, \Pi}(n) = \begin{cases} 1 & \text{falls } f(x') = y \\ 0 & \text{sonst} \end{cases}$ .

# Konstruktion einer Trapdoor-Einwegpermutation

## Definition Einweg-Permutation

Eine (Trapdoor-)Permutationsfamilie heißt *(Td-)Einwegpermutation* falls für alle ppt Algorithmen  $\mathcal{A}$  gilt  $\text{Ws}[\text{Invert}_{\mathcal{A}, \Pi_f}(n) = 1] \leq \text{negl}(n)$ .

**Bsp:** Trapdoor-Einwegpermutation unter RSA-Annahme

- **Gen( $1^n$ ):**  
 $(N, e, d) \leftarrow \text{GenRSA}(1^n)$ , Ausgabe  $I = (N, e)$  und  $td = (N, d)$ .
- **Samp( $I$ ):**  
Wähle  $x \in_R \mathbb{Z}_N$ .
- **f( $I, x$ ):**  
Berechne  $y \leftarrow x^e \bmod N$ .
- **Inv( $td, y$ ):**  
Berechne  $x \leftarrow y^d \bmod N$ .

# Hardcore-Prädikat

**Ziel:** Destilliere Komplexität des Invertierens auf ein Bit.

## Definition Hardcore-Prädikat

Sei  $\Pi_f$  eine Einwegpermutation. 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:

$$\text{Ws}[\mathcal{A}(f(x)) = hc(x)] \leq \frac{1}{2} + \text{negl}(n).$$

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

**Bsp:** Goldreich-Levin Hardcore-Prädikat (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  $g$  vermöge

$$hc(x, r) = \langle x, r \rangle = \sum_{i=1}^n x_i r_i \bmod 2.$$

- Beweis der Hardcore-Eigenschaft ist nicht-trivial.

# Verschlüsselung aus Trapdoor-Einwegpermutation

## Algorithmus $\text{VERSCHLÜSSELUNG}_{\Pi_f}$

Sei  $\Pi_f$  eine Td-Einwegpermutation mit Hardcore-Prädikat  $hc$ .

- ➊ **Gen:**  $(I, td) \leftarrow \text{Gen}(1^n)$ . Ausgabe  $pk = I$  und  $sk = td$ .
- ➋ **Enc:** Für  $m \in \{0, 1\}$  wähle  $x \in_R D$  und berechne
$$c \leftarrow (f(x), hc(x) \oplus m).$$
- ➌ **Dec:** Für Chiffretext  $c = (c_1, c_2)$  berechne  $x \leftarrow \text{Inv}_{td}(c_1)$  und
$$m \leftarrow c_2 \oplus hc(x).$$

## Intuition:

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

# CPA-Sicherheit unserer Konstruktion

## Satz CPA-Sicherheit von $\text{VERSCHLÜSSELUNG}_\Pi$

Sei  $\Pi_f$  eine Trapdoor-Einwegpermutation mit Hardcore-Prädikat  $hc$ .  
Dann ist  $\text{VERSCHLÜSSELUNG}_\Pi$  CPA-sicher.

### Beweis:

- Sei  $\mathcal{A}$  ein Angreifer mit Erfolgsws  $\epsilon(n) = \mathbb{W}_S[\text{PubK}_{\mathcal{A}, \Pi_f}^{\text{cpa}}(n) = 1]$ .
- OBdA  $(m_0, m_1) \leftarrow \mathcal{A}(pk)$  mit  $\{m_0, m_1\} = \{0, 1\}$ . (Warum?)
- Verwenden  $\mathcal{A}$  um einen Angreifer  $\mathcal{A}_{hc}$  für  $hc$  zu konstruieren.

## Algorithmus Angreifer $\mathcal{A}_{hc}$

**Eingabe:**  $I, y = f(x) \in D$

- 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:**  $hc(x) = \begin{cases} z & \text{falls } b = b' \\ \bar{z} & \text{sonst} \end{cases}$ .

## Beweis: Fortsetzung

- Sei  $x = f^{-1}(y)$ .  $A_{hc}$  rät  $z = hc(x)$ .
- Es gilt  $\text{Ws}[\mathcal{A}_{hc}(f(x)) = hc(x)] =$   
$$\frac{1}{2} \cdot \text{Ws}[b = b' \mid z = hc(x)] + \frac{1}{2} \cdot \text{Ws}[b \neq b' \mid z \neq hc(x)].$$
- **1. Fall**  $z = hc(x)$ :  $(y, c_2)$  ist korrekte Verschlüsselung von  $m_b$ , d.h.  
$$\text{Ws}[b = b' \mid z = hc(x)] = \epsilon(n).$$
- **2. Fall**  $z \neq hc(x)$ :  $(y, c_2)$  ist Verschlüsselung von  $\bar{m}_b = m_{\bar{b}}$ , d.h.  
$$\text{Ws}[b \neq b' \mid z \neq hc(x)] = \epsilon(n).$$
- Da  $hc$  ein Hardcore-Prädikat ist, folgt  
$$\frac{1}{2} + \text{negl}(n) \geq \text{Ws}[\mathcal{A}_{hc}(f(x)) = hc(x)] = \epsilon(n).$$

# Jacobi-Symbol

**Erinnerung Jacobi-Symbol:** Beweise siehe Diskrete Mathematik II

## Definition Quadratischer Rest

Sei  $N \in \mathbb{N}$ . Ein Element  $a \in \mathbb{Z}_N$  heißt *quadratischer Rest* in  $\mathbb{Z}_N$ , falls es ein  $b \in \mathbb{Z}_N$  gibt mit  $b^2 = a \bmod N$ . Wir definieren

$$QR_N = \{a \in \mathbb{Z}_N^* \mid a \text{ ist quadratischer Rest}\} \text{ und } QNR_N = \mathbb{Z}_N^* \setminus QR_N.$$

## Lemma Anzahl quadratischer Reste in primen Restklassen

Sei  $p > 2$  prim. Dann gilt  $|QR_p| = \frac{|\mathbb{Z}_p^*|}{2} = \frac{p-1}{2}$ .

### Beweisidee:

- Quadrieren auf  $\mathbb{Z}_p^*$ ,  $x \mapsto x^2$ , ist eine 2:1-Abbildung.
- Die verschiedenen Werte  $x, (-x)$  werden beide auf  $x^2$  abgebildet.



# Legendre-Symbol

## Definition Legendre Symbol

Sei  $p > 2$  prim und  $a \in \mathbb{N}$ . Das *Legendre Symbol* ist definiert als

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{falls } p|a \\ 1 & \text{falls } (a \bmod p) \in QR_p \\ -1 & \text{falls } (a \bmod p) \in QNR_p \end{cases}.$$

## Satz

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$$

## Eigenschaften Quadratischer Reste

- 1 Multiplikativität:  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$
- 2  $(QR_p, \cdot)$  ist eine multiplikative Gruppe.

# Das Jacobi Symbol

## Definition Jacobi Symbol

Sei  $N = p_1^{e_1} \cdot \dots \cdot p_k^{e_k} \in \mathbb{N}$  ungerade und  $a \in \mathbb{N}$ . Dann ist das *Jacobi Symbol* definiert als

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdot \dots \cdot \left(\frac{a}{p_k}\right)^{e_k}.$$

- **Warnung:**  $\left(\frac{a}{N}\right) = 1$  impliziert nicht, dass  $a \in QR_N$  ist.
- Bsp:  $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1)(-1) = 1$ .
- D.h.  $2 \in QNR_3$  und  $2 \in QNR_5$ . Damit besitzt  $x^2 = 2$  weder Lösungen modulo 3 noch modulo 5.
- Nach CRT besitzt  $x^2 = 2 \bmod 15$  ebenfalls keine Lösung.