

AUFGABE 3 (5 Punkte):

Sei G ein pt-Algorithmus, der eine Funktion $\{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$ mit $\ell(n) > n$ berechnet. Wir definieren $\Pi_s = (\text{Gen}, \text{Enc}, \text{Dec})$ mit Sicherheitsparameter n für Nachrichten der Länge $\ell(n)$ wie in der Vorlesung:

$\text{Gen}(1^n)$: Gib $k \in_R \{0,1\}^n$ zurück.

$\text{Enc}_k(m)$: Gib $c := G(k) \oplus m$ zurück.

$\text{Dec}_k(m)$: Gib $m := G(k) \oplus c$ zurück.

Zeigen Sie, dass G ein Pseudozufallsgenerator ist, wenn Π_s KPA-sicher ist.

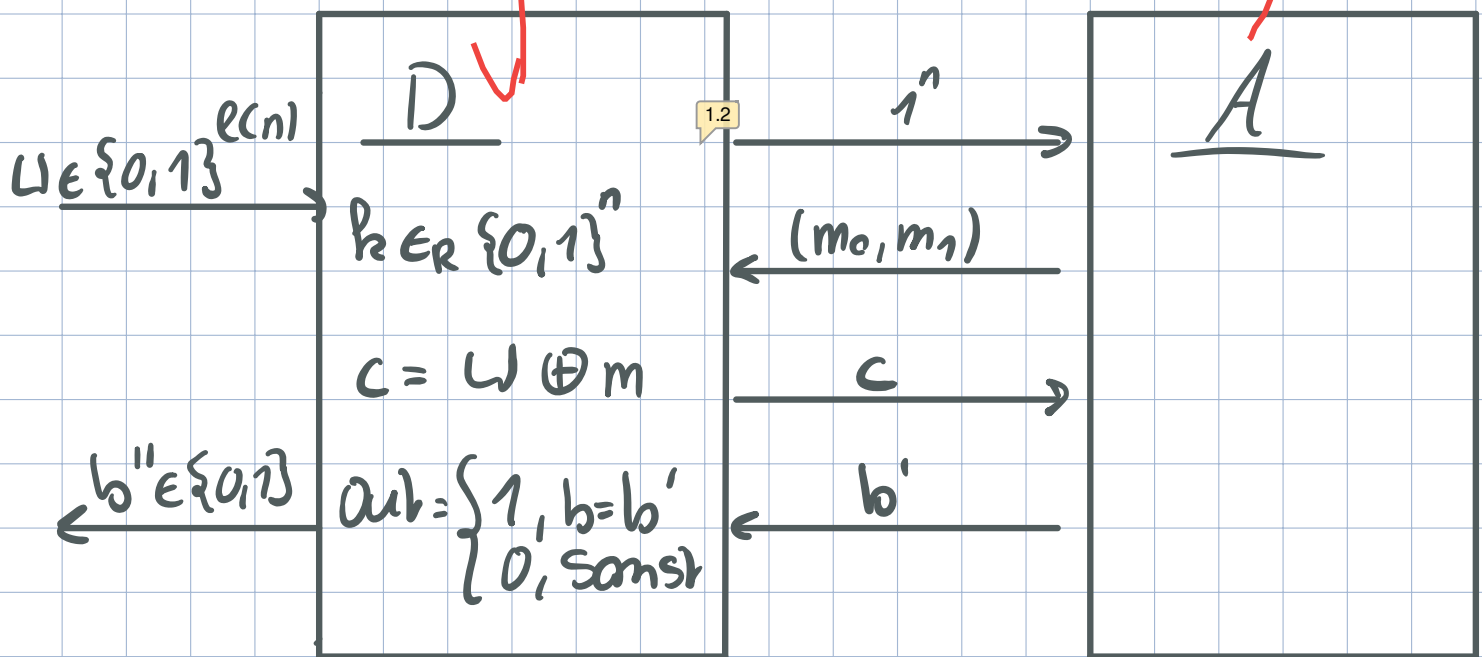
$\Pi_s \text{ KPA} \Rightarrow G \text{ PRNG}$

Beh. $G \text{ kein PRG} \Rightarrow \Pi_s \text{ nicht KPA}$

\exists Unterscheider D mit Angreifer ppt A . $\forall A$ gilt:
 $\epsilon(n) > \frac{1}{2} + \text{negl}(n)$

1.1

Laufzeitanalyse



$$1) w = G(k)$$

$$\begin{aligned} \text{US}[D(G(k)) = 1] &= \text{US}[\text{PrivK}_{A, \Pi_s}^{\text{KPA}}(n) = 1] \\ &= \frac{1}{2} + \epsilon(n) \end{aligned}$$

$$2) \omega = r \in_R \{0,1\}^n$$

$$\text{US}[D(\omega)=1] = \frac{1}{2} \quad \checkmark \quad \text{weil O.P.}$$

$$\begin{aligned} \Rightarrow \text{negl}(n) &< \underbrace{\text{US}[D(\omega)=1]}_{\frac{1}{2}} - \underbrace{\text{US}[D(G(R))=1]}_{\frac{1}{2} + \epsilon(n)} \\ &< \frac{1}{2} - \frac{1}{2} + \epsilon(n) \\ &< \epsilon(n) \end{aligned}$$

Gezeigt: Wenn G kein PRG, \exists ppt A mit $\epsilon(n) > \frac{1}{2} + \text{negl}(n)$ den D benutzen kann um Pseudozufall vom echtem zu unterscheiden $\Rightarrow \Pi_S$ nicht KPA.

Also folgt aus Kontraposition:

Wenn Π_S KPA $\Rightarrow G$ ist PRG

| | | | | | |
|--------|-----------|-----|-----|-----|-----|
| Daniel | Benford | 108 | 019 | 210 | 217 |
| Sergej | Mambeyser | 108 | 019 | 231 | 345 |
| Max | Randhuhn | 108 | 019 | 211 | 207 |

UG AF

Index der Kommentare

- 1.1 Aber wer sagt, dass dieser so aussehen muss???
- 1.2 Euch ist schon klar, dass ihr für jeden Unterscheider D zeigen müsst, dass dieser keinen Vorteil haben kann, nun habt ihr hier nur eine spezielle Familie von Unterscheidern angegeben.
- 2.1 Nein, ihr habt einen beliebigen Angreifer genommen, über den nur bekannt sein kann, dass er nicht vernachlässigbaren Vorteil hat (P_i sicher), womit euer spezieller Unterscheider D dann nicht besser als vernachlässigbar unterscheiden kann. Ihr müsst dies aber für alle Unterscheider zeigen!!