AUFGABE 3 (5 Punkte):

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

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

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

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

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

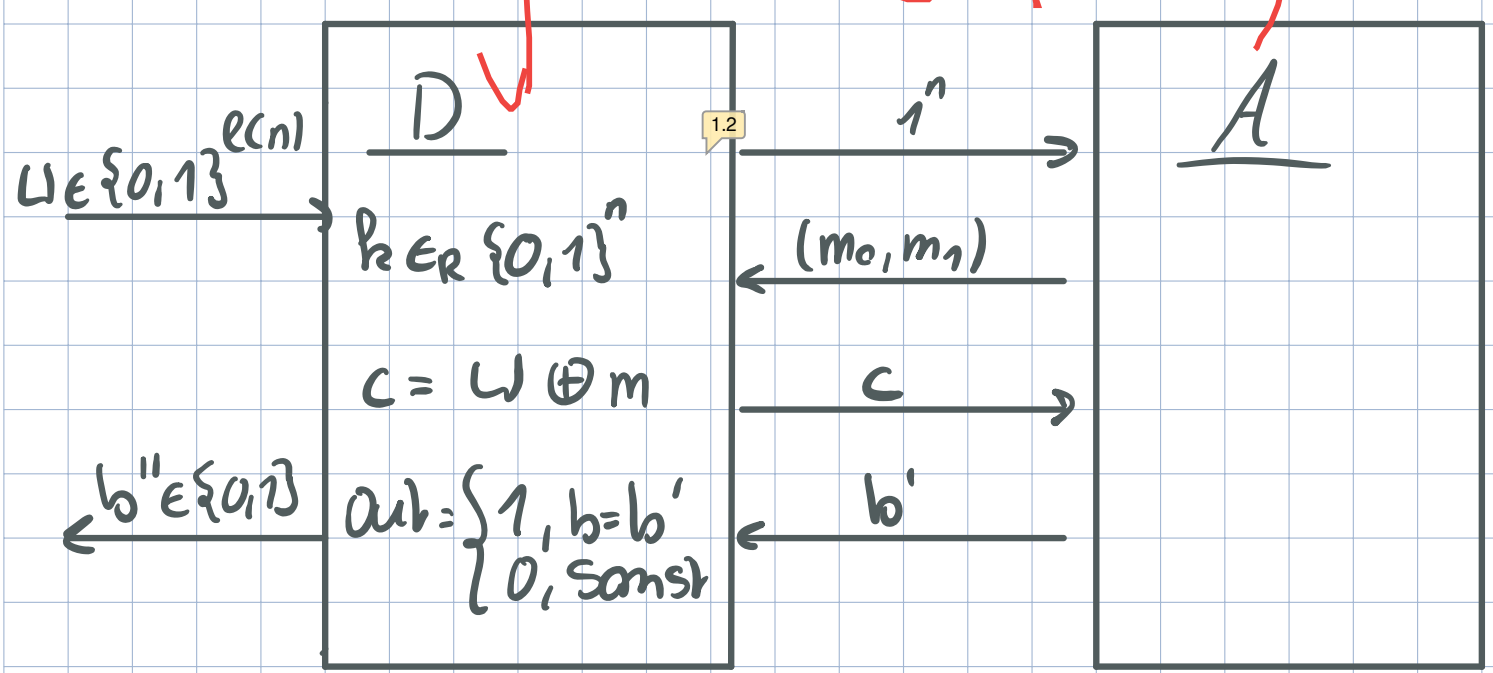
Π_s KPA $\Rightarrow$ G PRNG

Beh. G kein PRG $\Rightarrow$ Π_s nicht KPA

$\exists$ Unterscheider D mit Angreifer ppt A. $\forall$ A gilt:

$\varepsilon(n) > \frac{1}{2} + \text{negl}(n)$

Lückenfüller



1) $w = G(k)$

$$WS[D(G(k))=1] = WS[PrivK^{KPA}_{A,\Pi_s}(n)=1]$$
$$= \frac{1}{2} + \varepsilon(n)$$

2) $U_n \ni r \in_R \{0,1\}^n$

$U_S[D(r)=1] = \frac{1}{2}$ ✓ weil OTP

$\Rightarrow negl(n) < |\underbrace{U_S[D(r)=1]}_{\frac{1}{2}} - \underbrace{U_S[D(G(k))=1]}_{\frac{1}{2}+\varepsilon(n)}|$

$< \frac{1}{2} - \frac{1}{2} + \varepsilon(n)$

$< \varepsilon(n)$

Gezeigt: wenn G kein PRG, $\exists$ ppt A mit $\varepsilon(n) > \frac{1}{2} + negl(n)$ den D benutzen kann um Pseudozufall von 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	Mamberger	108	019	231	345
Max	Randhuhn	108	019	211	207

ÜG AF

Index der Kommentare