4c) KPA-Unsicherheit von Π_{nope}

WSK aus der Vorlesung:

$$\frac{1}{2}\left(W[0 \leftarrow A(Enc_k(m_0))] + W[1 \leftarrow A(Enc_k(m_1))]\right)$$

Wenn diese WSK signifikant größer als $\frac{1}{2}$ ist, dann ist das Verfahren KPA unsicher

Angreifer Modell

geg: Π_{nope}

$Enc: F_k(m_i \oplus (IV+i))$ für $i=0\ldots,l-1$

$\rightarrow (IV, c_0, c_1, \ldots, c_{l-1})$

Idee: Deterministik von F_k ausnutzen.

Also beim XORn versuchen das gleiche Ergebnis trotz Inkrementation auszunutzen. Dann ist c auch gleich.

$\rightarrow$ letzte Bit flippt bei Inkrementation von IV

Bei Blocklänge $n=1$

$m^0 = m^0_0, \ldots, m^0_{l-1} = 0, 1, 0, 1, \ldots$

$m^1 = m^1_0, \ldots m^1_{l-1} = 1, 1, 1, 1, \ldots$

$\rightarrow$

1) $m^0 = 1, 0, 1, 0, \dots$

2) $m^1 = 1, 1, 1, 1, \dots$

3) Schick (m^0, m^1) an KPA-Spiel

4) erhalte (IV, c^b)

5) if $(c_0^b == c_1^b)$
   return 0
   else
   return 1

[redacted]

Erklärung: Wenn IV inkrementiert wird, dann flippt das letzte Bit. Dadurch dass m^0 stetig zw 1 und 0 wechselt kommt beim XORn bei Blocklänge 1 immer das gleiche raus. Weil F_k deterministisch ist kommt auch das gleiche c_i^0 raus.

$$\rightarrow \frac{1}{2}\left(W[0 \leftarrow A(Enc_k(m_0))] + W[1 \leftarrow A(Enc_k(m_1))]\right) = 1$$