13.29 Aufgabe: Hashen mittels Sponge-Funktion

Gegeben seien die Parameter r=3, c=6, d=6 für eine fiktive Hash-Funktion, die nach der Sponge-Konstruktion arbeitet. In jeder Squeeze-Runde werden an Z die ersten r-Bits des States S konkateniert, d.h. $Z=Z \,||\, \text{Trunc}_r(S)$.

Die Runden-Funktion f ist wie folgt definiert:

$$f: \{0,1\}^9 \rightarrow \{0,1\}^9 \text{ mit}$$

$$f(x_1, \ldots, x_9) = \text{rot}_{AC}(x_1, \ldots, x_9) \oplus K$$

$$= (x_2, x_3, x_6, x_1, x_5, x_9, x_4, x_7, x_8) \oplus K$$

Dabei ist K=010101010 eine Konstante und rot_{AC} eine Funktion, die die Bits quadratisch dargestellt gegen den Uhrzeigersinn (AC = Anti Clockwise) um eine Position rotiert. D.h.,

x_1	x_2	x_3
x_4	x_5	x_6
x_7	x_8	x_9

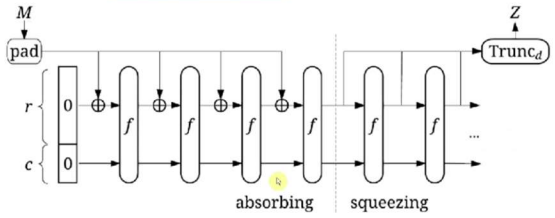
wird zu

x_2	x_3	x_6
x_1	x_5	x_9
x_4	x_7	x_8

Gepadded wird mit 0.

a) Berechnen Sie den Hashwert zur Nachricht M=111|11.
b) Wie oft müssen Sie durchschnittlich zufällige Nachrichten hashen, um eine Kollision zu finden?
c) Geben Sie eine Kollision an.

Funktionen (und Pseudozufallszahlenströme) und wird z.B. von SHA-3 verwendet.



a) M=111 11 gepadded M=111 110
   R=3 rate
   C=6 capacity
   D=6 länge hash

   F:{0,1}^9 -> {0,1}^9, f{x1,….,x9}=rotA{x1…..x9} + K
   =(x_2, x_3, x_6, x_1, x_5, x_9, x_4, x_7, x_8) + K

1. Runde
   M1=111+000=111
   F(1,1,1,0,0,0,0,0,0)=f(1,1,0,1,0,0,0,0,0)+010101010=100001010

2.

M2=110+100=010

F(0,1,0,0,0,0,0,0,0)=(1,0,0,0,0,0,0,0,0)+ 010101010=110101010

Squeeze:

1.Runde

Z1-3=(1,1,0)

F(1,1,0,1,0,1,0,1,0)=(1,0,1,1,0,0,1,1,0)+ 010101010=111001100

2.Runde

Z4-6=(1,1,1)

Z=Z1-3 vereinigt mit Z4-6=110111

b) Geburtstagsparadoxon:
Z = 1.17*2^3=9,35 => Durchschnittlich müssen wir 10 Hashwerte generieren bis es zu einer Kollision kommt

c)

Absorb:

2.Runde

M2=010+100=110

F(1,1,0,0,0,0,0,0,0)=(1,0,0,1,0,0,0,0,0)+010101010

=110001010

Squeeze

1 Runde

Z1-3=(1,1,0)

F(1,1,0,0,0,1,0,1,0)=(1,0,1,1,0,0,0,1,0)+010101010=111001000

2 Runde

Z4-6=(1,1,1)

Mkol=111 01 -> Kollision bei Mkol