Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Schau Bild Handy richtig

1. 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

=(x2, x3, x6, x1, x5, x9, x4, x7, x8) + 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

1. 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