

SHA-3

Luc Spachmann

FSU Jena

25.01.2024

SHA-3 Parameter

- Implementieren SHA3-224
- Hashgröße d in Bit: 224
- Blockgröße (rate) r : 1152
- Kapazität c : 448
- Blockbreite $b = c + r$: 1600

- Nachricht N
- $(P_0, \dots, P_{n-1}) = \text{pad}(N)$
- $S = 0^b$
- Für $i = 0 \dots n - 1$:
 - $S = f(S \oplus P_i 0^c)$
- Hashwert Z sind erste $d = 224$ Bits aus S

Padding Funktion

- Nachricht N wird verlängert bis Bitlänge durch r teilbar ist
- 10^*1 wird angehängt (0 bis $r - 1$ Nullen)
- Wichtig: Einsen sind immer nötig!
- Danach aufteilen in r Bit Blöcke

Permutationsfunktion f

- Operiert auf $5 \times 5 \times 64$ Array auf Bits
- $a[i][j][k]$ ist i -te Zeile, j -te Spalte und $64 - k$ tes Bit
- Indizes Zyklisch
- 24 Runden der folgenden Operationen:
- θ : Parität einer Spalte berechnen:
 - $a[i][j][k] \leftarrow a[i][j][k] \oplus \text{parity}(a[0\dots 4][j-1][k]) \oplus \text{parity}(a[0\dots 4][j+1][k-1])$
- Nächste Woche zusätzlich:
 - ρ
 - π
 - χ
 - ι

- Implementiert (partiell) SHA3
- Eingabedatei: Hexadezimalziffern beliebiger Länge
- Ausgabe Hashwert (Hexadezimal)
- Dateiname [Input.txt] [Output.txt]