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

Algorithmus

- Nachricht N
- $(P_0, ..., P_{n-1}) = \text{pad}(N)$
- $S = 0^b$
- Für $i = 0...n-1$:
  - $S = f(S \oplus P_i 0^c)$
- 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

Nachtrag

- Vor Aufruf der Funktion 01 an Nachricht anhängen!
- Inputbytes in little Endian interpretieren!

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:
- $a[i][j][k] \leftarrow$
  $a[i][j][k] \oplus \texttt{parity}(a[0...4][j-1][k]) \oplus \texttt{parity}(a[0...4][j+1][k-1])$

Funktion ρ

- Zyklisches Rotieren einzelner Blöcke
- Formal: Für alle $0 \leq t \leq 23$

$$\begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 0 \end{pmatrix}^t \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- Dann: $a[i][j] \leftarrow a[i][j] <<< (w_{ij} \mod 64)$
- Mit $w_{ij} = \frac{(t+1)(t+2)}{2}$
- $a[0][0]$ wird nicht rotiert
- Praktisch: Lookup Tabelle (Moodle)

Funktion π

- Rotation der einzelnen Wörter
- $a[i][j] = a[j][3i + j]$

Funktion χ

- Einzige nichtlineare Komponente
- $a[i][j] \leftarrow a[i][j] \oplus (\neg a[i][j+1] \& a[i][j+2])$
- Alle Operationen Bitweise
- $\oplus$ Bitweises XOr
- $\neg$ Bitweise negation
- Alle Operationen 'gleichzeitig'

Funktion ι

- $a[0][0] = a[0][0] \oplus C_r$
- C_r Rundenkonstante (Moodle)

Aufgabe

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