BLAKE šifrirna zgoščevalna funkcija

Ivan Verdonik, FG UM

Bojan Novak, FERI UM

Šifrirna zgoščevalna funkcija

- Poljubno dolgo sporočilo pretvori v unikatno oznako fiksne velikosti
- Uporaba: MAC, MDC, PRNG, Error detection,…
- Merkle-Damgard konstrukcija
- Enosmerne šifrirne zgoščevalne funkcije (One-way function)
- Šifrirne zgoščevalne funkcije odporne na trke (Collision Resistant Cryptographic Hash Function)

Generični napadi

- Napad s “trkom” (collision)
- Napad na pred-podobo (pre-image attack)
- Napad na sekundarno predpodobo (second pre-image attack)

Kompresijske funkcije

- Sporočilo razdelimo na bloke fiksne dolžine
- Zadnji blok dopolnimo
- Blok sporočila je eden vhod v funkcijo
- Drugi vhod je trenutna verižna vrednost oz. inicializacijski vektor(ji)
- Izhod je nova verižna vrednost

Opis BLAKE

- Preprost, hiter in varen algoritem
- Kompresijska funkcija na osnovi ChaCha pretočne šifrirne funkcije (Stream Cipher)
- Wide pipe notranje stanje
- HAIFA ogrodje (Izboljšava konstrukcije Merkle-Damgard)
- Različice BLAKE so: BLAKE-32, BLAKE-28, BLAKE-64 in BLAKE-48 (256, 224, 512 in 384 bitov)

ChaCha pretočna šifrirna funkcija

- Stanje je sestavljeno iz 16 32-bitnih besed
- Psevdonaključna funkcija

$$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix}$$

$$QR(a,b,c,d)$$

$$a = a + b \bmod 32, d = d \oplus a, d = d <<< 16$$

$$c = c + d \bmod 32, b = b \oplus c, b = b <<< 12$$

$$a = a + b \bmod 32, d = d \oplus a, d = d <<< 8$$

$$c = c + d \bmod 32, b = b \oplus c, b = b <<< 7$$

ChaCha transformacija

- Stolpični korak in diagonalni korak

$QR_0(x_0, x_4, x_8, x_{12})$

$QR_1(x_1, x_5, x_9, x_{13})$

$QR_2(x_2, x_6, x_{10}, x_{14})$

$QR_3(x_3, x_7, x_{11}, x_{15})$

$QR_4(x_0, x_5, x_{10}, x_{15})$

$QR_5(x_1, x_6, x_{11}, x_{12})$

$QR_6(x_2, x_7, x_8, x_{13})$

$QR_7(x_3, x_4, x_9, x_{14})$

Sestava BLAKE

- ChaCha funkcija in HAIFA ogrodje
- K ChaCha dodajamo bloke sporočila, spremenjena koraka sta tako:

$$a = a + b + (M_{p_r(2i)} \oplus c_{p_r(2i+1)}) \bmod 32$$

$$a = a + b + (M_{p_r(2i+1)} \oplus c_{p_r(2i)}) \bmod 32$$

Inicializacija

- Vhod so trenutne verižne vrednosti (ali IV), “sol”, konstante in števca

$$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix} \leftarrow \begin{bmatrix} h_0 & h_1 & h_2 & h_3 \\ h_4 & h_5 & h_6 & h_7 \\ s_0 \oplus c_0 & s_1 \oplus c_1 & s_2 \oplus c_2 & s_3 \oplus c_3 \\ t_0 \oplus c_4 & t_0 \oplus c_5 & t_1 \oplus c_6 & t_1 \oplus c_7 \end{bmatrix}$$

Izvajanje in izhodna transformacija

- Deset (dvojnih) ponovitev stolpično-diagonalnih korakov. Potem, ko so s kompresijsko funkcijo obdelani vsi bloki sporočila, izvedemo izhodno transformacijo

$$h_0' = h_0 \oplus s_0 \oplus x_0 \oplus x_8$$

$$h_1' = h_1 \oplus s_1 \oplus x_1 \oplus x_9$$

$$h_2' = h_2 \oplus s_2 \oplus x_2 \oplus x_{10}$$

$$h_3' = h_3 \oplus s_3 \oplus x_3 \oplus x_{11}$$

$$h_4' = h_4 \oplus s_0 \oplus x_4 \oplus x_{12}$$

$$h_5' = h_5 \oplus s_1 \oplus x_5 \oplus x_{13}$$

$$h_6' = h_6 \oplus s_2 \oplus x_6 \oplus x_{14}$$

$$h_7' = h_7 \oplus s_3 \oplus x_7 \oplus x_{15}$$

Zaključek

- Učinkovita in enostavna šifrirna zgoščevalna funkcija
- Gradniki: ChaCha, HAIFA
- Kandidat za SHA-3 izbor, poleg funkcij Groestl, JH, Keccak in Skein
- Favorit za SHA-3 zmago je vseeno verjetno Skein