Joonyeoup Kim

ECE 40400

HW07

3/5/2024

For Homework 7, we were required to implement SHA-512 algorithm. First, I declared the Initialization Vector K and 8 register vectors a, b, c, d, e, f, g, and h that were given to me via lecture notes, which I turned into a BitVector module. Then, I would import the input file and turn it into a BitVector module also. I would then calculate the length of the input BitVector. I would also add a single 1-bit to the input BitVector, and pad the vector with zeros till the length of the vector is in multiples of 1024 – 128, which is used for the storage of the 128 bit vector displaying its length. I would add the 128 bit long BitVector representing the original length of the input BitVector. Then, I would make an empty vector with the size of 80 bits to store my words into it. Then, I would read in 1024 bits of the input file till there are no more to read from, and declare each 1024 bits as a block. The first 16 words would be from the inputted BitVector and they would just be 64 bits of the inputted BitVector. Then, I would calculate sigma0 and sigma1 by the equation: $\sigma0(x) = ROTR1\ (x) \oplus ROTR8\ (x) \oplus SHR7\ (x)$, $\sigma1(x) = ROTR19(x) \oplus ROTR61(x) \oplus SHR6\ (x)$, where ROTR(n) means circular right shift of the 64 bit arg by n bits and SHR(n) means the right shift of the 64 bit arg by n bits with padding by zeros on the left. I would also determine words for each round using the equation $Wi = Wi{-}16 +64\ \sigma0(Wi{-}15) +64\ Wi{-}7 +64\ \sigma1(Wi{-}2)$, where +64 means modular addition of 2^64. Then, I would store the register vectors into temporary 8 64 bit variables named h0 to h7. Then, for 80 rounds, I would calculate the hash values with the equation h7 = h6, h6 = h5, h5 = h4, h4 = h3 +64 T1, h3 = h2, h2 = h1, h1 = h0, h0 = T1 +64 T2. The values of T1, T2 are calculated through these functions:

T1 = h7 +64 Ch(h4, h5, h6) +64 sum(h4) +64 Wi +64 K[i], T2 = sum(h0) +64 Maj(h0, h1, h2) Ch(h4, h5, h6) = (h4 AND h6) ⊕ (NOT h4 AND h6), Maj(h0, h1, h2) = (h0 AND h1) ⊕ (h0 AND h2) ⊕ (h1 AND h2) sum(h0) = ROTR28(h0) ⊕ ROTR34(h0) ⊕ ROTR39(h0) sum(h4) = ROTR14(h4) ⊕ ROTR18(h4) ⊕ ROTR41(h4). Then, I would update the hash values calculated for the previous message block by adding it to the values in the temporary variables h0-h7. After 80 rounds, I would concatenate all the hexvalues and write it to the output file.