

EXTENDS *Integers, Sequences, TLC, Reals*

VARIABLES *A, B, C, D, E, AA, BB, CC, DD, EE, digest, Message*

$$\textit{Divide}(x, y) \triangleq x \div y$$

$$\textit{ModAdd}(x, y) \triangleq ((x + y) \% (2^8))$$

$$\textit{ModSub}(x, y) \triangleq ((x - y) \% (2^8))$$

$$\textit{ModMul}(x, y) \triangleq ((x * y) \% (2^8))$$

$$\textit{Xor}(x, y) \triangleq \textit{ModSub}(\textit{ModAdd}(x, y), \textit{ModMul}(2, \textit{ModMul}(x, y)))$$

$$\textit{LeftRotate}(x, c) \triangleq \textit{ModAdd}(((x * (2^c)) \% (2^{16})), ((x \div (2^{16-c})) \% (2^{16})))$$

$$\textit{F1A}(N, P, Q) \triangleq \textit{ModSub}(\textit{ModAdd}(N, \textit{ModSub}(\textit{ModAdd}(P, Q), \textit{ModMul}(P, Q))), \textit{ModMul}(N, \textit{ModSub}(1, Q)))$$

$$\textit{F2A}(N, P, Q) \triangleq \textit{ModAdd}(\textit{ModMul}(N, P), \textit{ModMul}(\textit{ModSub}(1, N), Q))$$

$$\textit{F3A}(N, P, Q) \triangleq \textit{ModSub}(\textit{ModAdd}(N, \textit{ModSub}(\textit{ModAdd}(P, \textit{ModSub}(1, Q))), \textit{ModMul}(P, \textit{ModSub}(1, Q))), \textit{ModMul}(P, \textit{ModSub}(1, Q)))$$

$$\textit{F4A}(N, P, Q) \triangleq \textit{ModAdd}(\textit{ModMul}(N, Q), \textit{ModMul}(P, \textit{ModSub}(1, Q)))$$

$$\textit{F5A}(N, P, Q) \triangleq \textit{ModSub}(\textit{ModAdd}(N, \textit{ModSub}(\textit{ModAdd}(P, \textit{ModSub}(1, Q))), \textit{ModMul}(P, \textit{ModSub}(1, Q))), \textit{ModMul}(P, \textit{ModSub}(1, Q)))$$

$$\textit{F1B}(N, P, Q) \triangleq \textit{ModSub}(\textit{ModAdd}(N, \textit{ModSub}(\textit{ModAdd}(P, Q), \textit{ModMul}(P, Q))), \textit{ModMul}(N, \textit{ModSub}(1, Q)))$$

$$\textit{F2B}(N, P, Q) \triangleq \textit{ModAdd}(\textit{ModMul}(N, Q), \textit{ModMul}(P, \textit{ModSub}(1, Q)))$$

$$\textit{F3B}(N, P, Q) \triangleq \textit{ModSub}(\textit{ModAdd}(\textit{ModAdd}(N, \textit{ModSub}(1, P)), Q), \textit{ModMul}(\textit{ModAdd}(N, \textit{ModSub}(1, P)), \textit{ModSub}(1, Q)))$$

$$\textit{F4B}(N, P, Q) \triangleq \textit{ModAdd}(\textit{ModMul}(N, P), \textit{ModMul}(\textit{ModSub}(1, N), Q))$$

$$\textit{F5B}(N, P, Q) \triangleq \textit{ModSub}(\textit{ModAdd}(N, \textit{ModSub}(\textit{ModAdd}(P, \textit{ModSub}(1, Q))), \textit{ModMul}(P, \textit{ModSub}(1, Q))), \textit{ModMul}(P, \textit{ModSub}(1, Q)))$$

$$\textit{K1A} \triangleq 0$$

$$\textit{K2A} \triangleq 11$$

$$\textit{K3A} \triangleq 13$$

$$\textit{K4A} \triangleq 17$$

$$\textit{K5A} \triangleq 19$$

$$\textit{K1B} \triangleq 23$$

$$\textit{K2B} \triangleq 27$$

$$\textit{K3B} \triangleq 31$$

$$\textit{K4B} \triangleq 37$$

$$\textit{K5B} \triangleq 0$$

$$\textit{S1A} \triangleq \langle 11, 14, 15, 12, 5, 8, 7, 9, 11, 13, 14, 15, 6, 7, 9, 8 \rangle$$

$$\textit{S2A} \triangleq \langle 7, 4, 13, 1, 10, 6, 15, 3, 12, 0, 9, 5, 2, 14, 11, 8 \rangle$$

$$\textit{S3A} \triangleq \langle 11, 13, 6, 7, 14, 9, 15, 8, 2, 0, 13, 11, 5, 14, 7, 13 \rangle$$

$$\textit{S4A} \triangleq \langle 7, 5, 6, 8, 11, 14, 14, 6, 8, 13, 5, 14, 13, 6, 5, 12 \rangle$$

$$\textit{S5A} \triangleq \langle 9, 15, 5, 11, 6, 8, 13, 12, 5, 7, 11, 12, 8, 15, 6, 5 \rangle$$

$$\textit{S1B} \triangleq \langle 8, 9, 11, 13, 15, 7, 12, 8, 6, 4, 14, 15, 8, 11, 10, 7 \rangle$$

$$\textit{S2B} \triangleq \langle 9, 13, 7, 15, 8, 14, 11, 2, 7, 1, 10, 13, 12, 5, 8, 9 \rangle$$

$$\textit{S3B} \triangleq \langle 8, 12, 4, 9, 10, 0, 15, 5, 3, 14, 7, 14, 5, 6, 11, 13 \rangle$$

$S4B \triangleq \langle 5, 6, 11, 14, 10, 2, 4, 9, 7, 8, 15, 11, 13, 9, 3, 1 \rangle$   
 $S5B \triangleq \langle 12, 5, 15, 13, 6, 8, 2, 10, 7, 0, 9, 14, 3, 5, 1, 6 \rangle$

$F(N, P, Q, isA, num) \triangleq$   
 IF  $isA$  THEN  
     IF  $num = 1$  THEN  $F1A(N, P, Q)$   
     ELSE IF  $num = 2$  THEN  $F2A(N, P, Q)$   
     ELSE IF  $num = 3$  THEN  $F3A(N, P, Q)$   
     ELSE IF  $num = 4$  THEN  $F4A(N, P, Q)$   
     ELSE  $F5A(N, P, Q)$   
 ELSE  
     IF  $num = 1$  THEN  $F1B(N, P, Q)$   
     ELSE IF  $num = 2$  THEN  $F2B(N, P, Q)$   
     ELSE IF  $num = 3$  THEN  $F3B(N, P, Q)$   
     ELSE IF  $num = 4$  THEN  $F4B(N, P, Q)$   
     ELSE  $F5B(N, P, Q)$

$ProcessChunk(chunk) \triangleq$   
 LET  
      $P \triangleq [j \in 0 \dots 15 \mapsto SubSeq(Message, (chunk - 1) * 512 + j * 32 + 1, (chunk - 1) * 512 + (j + 1) * 32)]$   
 IN  
      $\wedge AA' = A$   
      $\wedge BB' = B$   
      $\wedge CC' = C$   
      $\wedge DD' = D$   
      $\wedge EE' = E$   
      $\wedge \forall round \in 1 \dots 5 :$   
         LET  
              $K1 \triangleq$  IF  $round = 1$  THEN  $K1A$  ELSE IF  $round = 2$  THEN  $K2A$  ELSE IF  $round = 3$  THEN  $K3A$   
              $S1 \triangleq$  IF  $round = 1$  THEN  $S1A$  ELSE IF  $round = 2$  THEN  $S2A$  ELSE IF  $round = 3$  THEN  $S3A$   
              $K2 \triangleq$  IF  $round = 1$  THEN  $K1B$  ELSE IF  $round = 2$  THEN  $K2B$  ELSE IF  $round = 3$  THEN  $K3B$   
              $S2 \triangleq$  IF  $round = 1$  THEN  $S1B$  ELSE IF  $round = 2$  THEN  $S2B$  ELSE IF  $round = 3$  THEN  $S3B$   
         IN  
              $\wedge \forall i \in 1 \dots 16 :$   
                 LET  
                      $resultA \triangleq F(B, C, D, TRUE, round) \% (2^8)$   
                      $resultB \triangleq F(BB, CC, DD, FALSE, round) \% (2^8)$   
                 IN  
                      $\wedge A' = LeftRotate(Xor((E + resultA), K1), S1[i]) \% (2^8)$   
                      $\wedge E' = D \% (2^8)$   
                      $\wedge D' = LeftRotate(C, 10) \% (2^8)$   
                      $\wedge C' = B \% (2^8)$   
                      $\wedge B' = A \% (2^8)$   
                      $\wedge AA' = LeftRotate(Xor((EE + resultB), K2), S2[i]) \% (2^8)$   
                      $\wedge EE' = DD \% (2^8)$

$$\begin{aligned}
& \wedge DD' = \text{LeftRotate}(CC, 10)\%(2^8) \\
& \wedge CC' = BB\%(2^8) \\
& \wedge BB' = AA\%(2^8) \\
& \wedge \text{UNCHANGED } \langle \text{digest}, \text{Message} \rangle
\end{aligned}$$

$$\begin{aligned}
\text{Preprocess} & \triangleq \\
& \text{LET } msg \triangleq \text{Append}(\text{Message}, 0) \\
& \text{IN } \wedge \text{Len}(msg)\%512 = 448 \\
& \wedge \text{Message}' = \text{Append}(msg, \text{Len}(\text{Message})\%(2^{64}))
\end{aligned}$$

$$\begin{aligned}
\text{Init} & \triangleq \\
& \wedge A = 13 \\
& \wedge B = 17 \\
& \wedge C = 19 \\
& \wedge D = 23 \\
& \wedge E = 29 \\
& \wedge AA = 13 \\
& \wedge BB = 17 \\
& \wedge CC = 19 \\
& \wedge DD = 23 \\
& \wedge EE = 29 \\
& \wedge \text{digest} = \langle \rangle \\
& \wedge \text{Message} = \langle \rangle
\end{aligned}$$

$$\begin{aligned}
\text{FinalCombine} & \triangleq \\
& \wedge A' = \text{ModAdd}(A, AA) \\
& \wedge B' = \text{ModAdd}(B, BB) \\
& \wedge C' = \text{ModAdd}(C, CC) \\
& \wedge D' = \text{ModAdd}(D, DD) \\
& \wedge E' = \text{ModAdd}(E, EE) \\
& \wedge \text{digest}' = \langle A', B', C', D', E' \rangle \\
& \wedge \text{UNCHANGED } \langle AA, BB, CC, DD, EE, \text{Message} \rangle
\end{aligned}$$

$$\begin{aligned}
\text{Next} & \triangleq \\
& \vee \text{Preprocess} \\
& \vee \exists \text{chunk} \in 1 \dots \text{Divide}(\text{Len}(\text{Message}), 512) : \text{ProcessChunk}(\text{chunk}) \\
& \vee \text{FinalCombine}
\end{aligned}$$

$$\text{Spec} \triangleq \text{Init} \wedge \Box[\text{Next}]_{\langle A, B, C, D, E, AA, BB, CC, DD, EE, \text{digest}, \text{Message} \rangle}$$


---