**Notations**

Les registres sont A,B,C,D. Le bloc de 512 bits est scindé en 16 mots de 32 bits, et stockés dans M[0],...,M[15].  
On définit une table T[i] de 64 éléments, à partir de la fonction sinus. T[i] vaut la partié entière de 4294967296 × abs(sin(i)).  
X <<< s est la rotation à gauche de X par s bits.

**Une étape de calcul**

Pour j = 0 à 15 faire  
Initialiser X[j] à M[j].  
Fin pour.  
  
/\* Sauvegarde des registres \*/  
AA = A  
BB = B  
CC = C  
DD = D  
  
/\* Premier tour. \*/  
/\* Soit [abcd k s i] notant l'opération  
a = b + ((a + F(b,c,d) + X[k] + T[i]) <<< s). \*/  
/\* On fait les 16 opérations. \*/  
[ABCD 0 7 1] [DABC 1 12 2] [CDAB 2 17 3] [BCDA 3 22 4]  
[ABCD 4 7 5] [DABC 5 12 6] [CDAB 6 17 7] [BCDA 7 22 8]  
[ABCD 8 7 9] [DABC 9 12 10] [CDAB 10 17 11] [BCDA 11 22 12]  
[ABCD 12 7 13] [DABC 13 12 14] [CDAB 14 17 15] [BCDA 15 22 16]  
  
/\* Deuxième tour. \*/  
/\* Soit [abcd k s i] l'opération  
a = b + ((a + G(b,c,d) + X[k] + T[i]) <<< s). \*/  
/\* On fait les 16 opérations. \*/  
[ABCD 1 5 17] [DABC 6 9 18] [CDAB 11 14 19] [BCDA 0 20 20]  
[ABCD 5 5 21] [DABC 10 9 22] [CDAB 15 14 23] [BCDA 4 20 24]  
[ABCD 9 5 25] [DABC 14 9 26] [CDAB 3 14 27] [BCDA 8 20 28]  
[ABCD 13 5 29] [DABC 2 9 30] [CDAB 7 14 31] [BCDA 12 20 32]  
  
/\* Etape 3. \*/  
/\* Soit [abcd k s t] l'opération  
a = b + ((a + H(b,c,d) + X[k] + T[i]) <<< s). \*/  
/\* On fait les 16 opérations. \*/  
[ABCD 5 4 33] [DABC 8 11 34] [CDAB 11 16 35] [BCDA 14 23 36]  
[ABCD 1 4 37] [DABC 4 11 38] [CDAB 7 16 39] [BCDA 10 23 40]  
[ABCD 13 4 41] [DABC 0 11 42] [CDAB 3 16 43] [BCDA 6 23 44]  
[ABCD 9 4 45] [DABC 12 11 46] [CDAB 15 16 47] [BCDA 2 23 48]  
  
/\* Etape 4. \*/  
/\* Soit [abcd k s t] l'opération  
a = b + ((a + I(b,c,d) + X[k] + T[i]) <<< s). \*/  
/\* On fait les 16 opérations. \*/  
[ABCD 0 6 49] [DABC 7 10 50] [CDAB 14 15 51] [BCDA 5 21 52]  
[ABCD 12 6 53] [DABC 3 10 54] [CDAB 10 15 55] [BCDA 1 21 56]  
[ABCD 8 6 57] [DABC 15 10 58] [CDAB 6 15 59] [BCDA 13 21 60]  
[ABCD 4 6 61] [DABC 11 10 62] [CDAB 2 15 63] [BCDA 9 21 64]  
  
/\* On réécrit dans les registres!\*/  
  
A = A + AA  
B = B + BB  
C = C + CC  
D = D + DD