```
--------------------------------------------------------------------------------
-- sha256_compression_tb.vhd: Banc d'essai fonctions de compression SHA256
-- Jeferson S. Silva
--------------------------------------------------------------------------------

library ieee;
        use ieee.std_logic_1164.all;
        use ieee.numeric_std.all;

entity sha256_compression_tb is
end sha256_compression_tb;

architecture sha256_compression_tb of sha256_compression_tb is

        type vector32_t is array (integer range <>) of std_logic_vector(31 downto 0);

    constant X  : vector32_t(0 to 63) := (
        x"428a2f98", x"71374491", x"b5c0fbcf", x"e9b5dba5", x"3956c25b", x"59f111f1", x"923f82a4",
x"ab1c5ed5",
            x"d807aa98", x"12835b01", x"243185be", x"550c7dc3", x"72be5d74", x"80deb1fe",
x"9bdc06a7", x"c19bf174",
            x"e49b69c1", x"efbe4786", x"0fc19dc6", x"240ca1cc", x"2de92c6f", x"4a7484aa",
x"5cb0a9dc", x"76f988da",
            x"983e5152", x"a831c66d", x"b00327c8", x"bf597fc7", x"c6e00bf3", x"d5a79147",
x"06ca6351", x"14292967",
            x"27b70a85", x"2e1b2138", x"4d2c6dfc", x"53380d13", x"650a7354", x"766a0abb",
x"81c2c92e", x"92722c85",
            x"a2bfe8a1", x"a81a664b", x"c24b8b70", x"c76c51a3", x"d192e819", x"d6990624",
x"f40e3585", x"106aa070",
            x"19a4c116", x"1e376c08", x"2748774c", x"34b0bcb5", x"391c0cb3", x"4ed8aa4a",
x"5b9cca4f", x"682e6ff3",
            x"748f82ee", x"78a5636f", x"84c87814", x"8cc70208", x"90befffa", x"a4506ceb",
x"bef9a3f7", x"c67178f2");
    constant Y  : vector32_t(0 to 63) := (
        x"428a2f98", x"d728ae22", x"71374491", x"23ef65cd", x"b5c0fbcf", x"ec4d3b2f", x"e9b5dba5",
x"8189dbbc",
        x"3956c25b", x"f348b538", x"59f111f1", x"b605d019", x"923f82a4", x"af194f9b", x"ab1c5ed5",
x"da6d8118",
        x"d807aa98", x"a3030242", x"12835b01", x"45706fbe", x"243185be", x"4ee4b28c", x"550c7dc3",
x"d5ffb4e2",
        x"72be5d74", x"f27b896f", x"80deb1fe", x"3b1696b1", x"9bdc06a7", x"25c71235", x"c19bf174",
x"cf692694",
        x"e49b69c1", x"9ef14ad2", x"efbe4786", x"384f25e3", x"0fc19dc6", x"8b8cd5b5", x"240ca1cc",
x"77ac9c65",
        x"2de92c6f", x"592b0275", x"4a7484aa", x"6ea6e483", x"5cb0a9dc", x"bd41fbd4", x"76f988da",
x"831153b5",
        x"983e5152", x"ee66dfab", x"a831c66d", x"2db43210", x"b00327c8", x"98fb213f", x"bf597fc7",
x"beef0ee4",
        x"c6e00bf3", x"3da88fc2", x"d5a79147", x"930aa725", x"06ca6351", x"e003826f", x"14292967",
x"0a0e6e70");
    constant Z  : vector32_t(0 to 63) := (
        x"27b70a85", x"46d22ffc", x"2e1b2138", x"5c26c926", x"4d2c6dfc", x"5ac42aed", x"53380d13",
x"9d95b3df",
        x"650a7354", x"8baf63de", x"766a0abb", x"3c77b2a8", x"81c2c92e", x"47edaee6", x"92722c85",
x"1482353b",
        x"a2bfe8a1", x"4cf10364", x"a81a664b", x"bc423001", x"c24b8b70", x"d0f89791", x"c76c51a3",
x"0654be30",
        x"d192e819", x"d6ef5218", x"d6990624", x"5565a910", x"f40e3585", x"5771202a", x"106aa070",
x"32bbd1b8",
        x"19a4c116", x"b8d2d0c8", x"1e376c08", x"5141ab53", x"2748774c", x"df8eeb99", x"34b0bcb5",
x"e19b48a8",
        x"391c0cb3", x"c5c95a63", x"4ed8aa4a", x"e3418acb", x"5b9cca4f", x"7763e373", x"682e6ff3",
x"d6b2b8a3",
        x"748f82ee", x"5defb2fc", x"78a5636f", x"43172f60", x"84c87814", x"a1f0ab72", x"8cc70208",
```

```
x"1a6439ec",
        x"90befffa", x"23631e28", x"a4506ceb", x"de82bde9", x"bef9a3f7", x"b2c67915", x"c67178f2",
x"e372532b");
        constant CH_R   : vector32_t(0 to 63) := (
            x"67bf2f9d", x"57e02f6c", x"3b1b40b1", x"35a74187", x"7568efef", x"4a453b2d",
x"c1358fb7", x"9589fb9e",
        x"3d0ed35c", x"9b2c31de", x"527b0bb1", x"3c77d229", x"937e802e", x"c7390f9a", x"8b3e2e85",
x"d409851b",
        x"c227a8a0", x"a3430262", x"a29b7b09", x"9c42318d", x"e623873e", x"daec9399", x"d74c79e3",
x"54fdb6e2",
        x"51bef959", x"f6ff907d", x"c69a21ec", x"7b349691", x"b2ce36a7", x"07d7302d", x"10aae170",
x"26bbf09c",
        x"3c93c993", x"9ed1d0d0", x"5f3f4584", x"1049a743", x"0740154c", x"8b8ce1b1", x"3430b59d",
x"73a94c2d",
        x"39a92c33", x"4dcb1a61", x"4ed0a02a", x"6625cacb", x"5a9caa5e", x"b563e357", x"7c284af2",
x"c69018b3",
        x"7c2f43fa", x"4feedefc", x"78a5466f", x"67b73350", x"b4c07484", x"a9f8213a", x"9f5b4a47",
x"3a6e1eec",
        x"c4b07ff2", x"3be21f42", x"a49014ef", x"d202bfe1", x"2ecb6355", x"b286117f", x"54297967",
x"23026b79");
        constant MAJ_R  : vector32_t(0 to 63) := (
        x"428a2f98", x"57322eb0", x"35136199", x"69a7c9a5", x"3d44ebdf", x"58c53bed", x"d33d8ba5",
x"899ddbdd",
        x"7906e258", x"938b7318", x"747101bb", x"3405f089", x"92bec924", x"87ddaffe", x"9b5c0e85",
x"d08bb138",
        x"e09fe881", x"efb30346", x"0a835f43", x"2440218c", x"24698d7e", x"4af49688", x"552c79c3",
x"56fdbcf2",
        x"d0be5950", x"f27bc26d", x"909b27ec", x"3f55bf91", x"d6cc07a7", x"55e71027", x"00cae170",
x"162921b4",
        x"25b74985", x"bed340d8", x"4f3e6d8c", x"51492d53", x"27487744", x"df8ecbb9", x"2480a9ac",
x"f3ba0ca5",
        x"29bd2ca3", x"c90b4263", x"4a588a6a", x"e764c083", x"5990e85d", x"f741e374", x"742e2dd3",
x"9232b0b1",
        x"18aec156", x"5e67fea8", x"2821676d", x"25b43e30", x"b0082c90", x"88f8ab7a", x"9fdd4a4f",
x"3a6e2fe4",
        x"d4ae8bfa", x"39a10f6a", x"84c07847", x"9e82a729", x"96fae3f3", x"a042686f", x"967929f7",
x"c2727a72");
    constant SIGMA_UPPER_0_R    : vector32_t(0 to 63) := (
        x"44defebd", x"a5d41d5a", x"30e2ae23", x"702cace1", x"878516c5", x"1db14e93", x"cfa1e31d",
x"ed1119fb",
        x"7c6d49fb", x"91c44690", x"62ebb873", x"0aaeba47", x"0e79d365", x"55045089", x"a3d14126",
x"d4052384",
        x"5a8ef939", x"7ec6f7ad", x"6bb70142", x"35e53886", x"0cb298e5", x"65dddba7", x"9b69be80",
x"3d4ebc21",
        x"d5de1fc6", x"9e7886b5", x"1eda6b2b", x"7414bbc7", x"2e09fae7", x"e112563b", x"72b7ea9c",
x"2a977740",
        x"c1eeeb87", x"6ec3582f", x"cd1e8328", x"5c60d7c8", x"aa2ce512", x"206bdc27", x"e220065a",
x"c8020ef9",
        x"d200695d", x"b1c2f7e1", x"45393389", x"cd83a017", x"7f0a51d7", x"6098661b", x"e9fa3ac0",
x"ad1beb08",
        x"1ddda505", x"ba7d0ac1", x"926e170d", x"6a775e7a", x"dbec0728", x"a34d756c", x"f7b4d31b",
x"1c2f172f",
        x"b45bfd15", x"50df2012", x"c0766a55", x"2f7d8489", x"a004d04b", x"cffa9728", x"168c41cb",
x"b3e9a6ae");
    constant SIGMA_UPPER_1_R    : vector32_t(0 to 63) := (
        x"d715b5da", x"4c48b342", x"a75c5c2a", x"39f63321", x"8ce35c4d", x"03c402c9", x"d91bebb3",
x"02367825",
        x"33ae5233", x"25c5dd8e", x"57969f34", x"330071d2", x"206a1487", x"aa8b9e51", x"a49f5857",
x"3066e6db",
        x"721a1e38", x"3440cda1", x"40301d43", x"0f445501", x"c5c42e02", x"0622c9a7", x"12adba9c",
x"0e515429",
        x"7f1b57c3", x"63f6f7f5", x"da45e8a3", x"4ab56d0f", x"c166a5cd", x"e464895d", x"4b0a5842",
x"a426920a",
        x"9fbf6858", x"ca2d33f7", x"d88bea1c", x"73200e9c", x"be2122b1", x"8fb238d0", x"7eb3a43d",
x"bfedc43e",
```

```
        x"cd4af88e", x"eae64f01", x"88d4df3d", x"0d4d8d2f", x"ad087515", x"1b43a553", x"a0747bea",
x"fb139fdd",
        x"a8c52c90", x"bacd1f52", x"7d226ec0", x"1a2a0e7f", x"d4850a2f", x"0c279c9b", x"bae0271d",
x"24fa45c6",
        x"a3ddd8c1", x"82bc369d", x"34bfb2ad", x"00a380ae", x"4a6f1168", x"1bd3be6c", x"dcddc264",
x"edfd72af");
    constant SIGMA_LOWER_0_R    : vector32_t(0 to 63) := (
        x"b332410e", x"fde0da56", x"b72073fe", x"200caaae", x"01cebb9a", x"adf19661", x"bbcaabde",
x"a980d9a0",
        x"c016cc07", x"d6b52976", x"19a1dab0", x"937b4200", x"71efabbb", x"4165cb6b", x"5de5de2e",
x"0ded79aa",
        x"452a22cd", x"81c90f90", x"ea963373", x"b4ba8479", x"90fd3caf", x"7cf0eb01", x"99586344",
x"d8045fb4",
        x"22631087", x"bfcd314d", x"4e924eb6", x"c76472d1", x"fdad30d1", x"714e4863", x"3a00991e",
x"86f4b274",
        x"cc18c6a8", x"bdd159e3", x"ea40c62f", x"2f85a576", x"38be43ce", x"fa8f48d8", x"ff707cc7",
x"924bc555",
        x"ad3aea6a", x"1bc19203", x"1b11d6ea", x"4b0ba34c", x"93970cb7", x"12f7276e", x"9808a7d8",
x"4a318554",
        x"1f4257c9", x"c8f884d4", x"817497d5", x"43d23bc3", x"627d77c8", x"b7d437ab", x"a757763a",
x"70294b2a",
        x"32c3727b", x"893e3882", x"2795bec0", x"c0034d74", x"58c8062f", x"d8f84450", x"905f2887",
x"a37e7c73");
    constant SIGMA_LOWER_1_R    : vector32_t(0 to 63) := (
        x"24e98264", x"ad4abee5", x"21838569", x"2ce8072e", x"b4a06993", x"e74f933d", x"6238e3ad",
x"dd5c030f",
        x"96050440", x"6f2e8fea", x"c82e0ef1", x"82f91849", x"1a78d8b5", x"2c1c9d70", x"1e9d7460",
x"ad18910a",
        x"6a9377ee", x"d375cb78", x"2b8437e8", x"a4a0b52e", x"99313b47", x"39ae067d", x"645e651b",
x"58dd169e",
        x"806ca5d6", x"8e477e6e", x"46151a56", x"312a444b", x"ce5440f1", x"ed4b0d15", x"0870bbcc",
x"b9794c6a",
        x"f5c7951e", x"8494ef8f", x"7c987309", x"4cfa4450", x"1fe7e7f0", x"ac935c65", x"e302abae",
x"53fde677",
        x"7bb6640f", x"62431a03", x"b257a486", x"051812bf", x"3a711528", x"b3ab588a", x"d15d85da",
x"944bb224",
        x"c0423900", x"cdfe53ad", x"3e7d7729", x"c349484b", x"4d7c5012", x"3c619d58", x"a4317f68",
x"0044df21",
        x"4992d37a", x"119153c1", x"5d308367", x"c2513c50", x"35998657", x"a3252122", x"eaaaaf38",
x"e4360173");

    signal x_in            : std_logic_vector(31 downto 0);
    signal y_in            : std_logic_vector(31 downto 0);
    signal z_in            : std_logic_vector(31 downto 0);
    signal ch              : std_logic_vector(31 downto 0);
    signal maj             : std_logic_vector(31 downto 0);
    signal sigma_upper_0   : std_logic_vector(31 downto 0);
    signal sigma_upper_1   : std_logic_vector(31 downto 0);
    signal sigma_lower_0   : std_logic_vector(31 downto 0);
    signal sigma_lower_1   : std_logic_vector(31 downto 0);

begin

    -- Completer: Instantier votre module ici



    process
        begin
                -- Completer

                assert (false)
                        report "La simulation est terminee." severity failure;
        end process;
```

```
end sha256_compression_tb;
```