```
/*****************************************************************************
File name:    zuc.h
Version:      V1.1
Date:         Oct 28,2016
Description:  This headfile provide macro defination,parameter definition and function
declaration needed in ZUC stream cipher algorithm implementation.
Function List:
1.AddMod               // calculate a+b mod 2^31-1
2.PowMod               // calculate x*2^k mod 2^31-1
3.L1                   // linear transformation L1:X^(X<<< 2)^(X<<<10)^(X<<<18)^(X<<<24)
4.L2                   // linear transformation L2:X^(X<<< 8)^(X<<<14)^(X<<<22)^(X<<<30)
5.BitValue             // test if the value of M at the position i equals 0
6.GetWord              // get a 32bit word ki from bit strings k[i],k[i+1]...,
// namely ki=k[i]||k[i+1]||...||k[i+31]
7.LFSRWithInitMode     // Initialisation mode,refresh the current state of LFSR
8.LFSRWithWorkMode     // working mode,refresh the current state of LFSR
9.BR                   // Bit Reconstruction
10.F                   // nonlinear function
11.ZUC_Init            // Initialisation process of ZUC
12.ZUC_Work            // working stage of ZUC
13.ZUC_GenKeyStream    // generate key stream
14.ZUC_Confidentiality // the ZUC-based condifentiality algorithm
15.ZUC_Integrity       // the ZUC-based integrity algorithm
*****************************************************************************/

#include <stdio.h>
#include <stdlib.h>
#include <string.h>

unsigned char ZUC_S0[256] =
{0x3e,0x72,0x5b,0x47,0xca,0xe0,0x00,0x33,0x04,0xd1,0x54,0x98,0x09,0xb9,0x6d,0xcb,
0x7b,0x1b,0xf9,0x32,0xaf,0x9d,0x6a,0xa5,0xb8,0x2d,0xfc,0x1d,0x08,0x53,0x03,0x90,
0x4d,0x4e,0x84,0x99,0xe4,0xce,0xd9,0x91,0xdd,0xb6,0x85,0x48,0x8b,0x29,0x6e,0xac,
0xcd,0xc1,0xf8,0x1e,0x73,0x43,0x69,0xc6,0xb5,0xbd,0xfd,0x39,0x63,0x20,0xd4,0x38,
0x76,0x7d,0xb2,0xa7,0xcf,0xed,0x57,0xc5,0xf3,0x2c,0xbb,0x14,0x21,0x06,0x55,0x9b,
0xe3,0xef,0x5e,0x31,0x4f,0x7f,0x5a,0xa4,0x0d,0x82,0x51,0x49,0x5f,0xba,0x58,0x1c,
0x4a,0x16,0xd5,0x17,0xa8,0x92,0x24,0x1f,0x8c,0xff,0xd8,0xae,0x2e,0x01,0xd3,0xad,
0x3b,0x4b,0xda,0x46,0xeb,0xc9,0xde,0x9a,0x8f,0x87,0xd7,0x3a,0x80,0x6f,0x2f,0xc8,
0xb1,0xb4,0x37,0xf7,0x0a,0x22,0x13,0x28,0x7c,0xcc,0x3c,0x89,0xc7,0xc3,0x96,0x56,
0x07,0xbf,0x7e,0xf0,0x0b,0x2b,0x97,0x52,0x35,0x41,0x79,0x61,0xa6,0x4c,0x10,0xfe,
0xbc,0x26,0x95,0x88,0x8a,0xb0,0xa3,0xfb,0xc0,0x18,0x94,0xf2,0xe1,0xe5,0xe9,0x5d,
0xd0,0xdc,0x11,0x66,0x64,0x5c,0xec,0x59,0x42,0x75,0x12,0xf5,0x74,0x9c,0xaa,0x23,
0x0e,0x86,0xab,0xbe,0x2a,0x02,0xe7,0x67,0xe6,0x44,0xa2,0x6c,0xc2,0x93,0x9f,0xf1,
0xf6,0xfa,0x36,0xd2,0x50,0x68,0x9e,0x62,0x71,0x15,0x3d,0xd6,0x40,0xc4,0xe2,0x0f,
```

```
0x8e,0x83,0x77,0x6b,0x25,0x05,0x3f,0x0c,0x30,0xea,0x70,0xb7,0xa1,0xe8,0xa9,0x65,
0x8d,0x27,0x1a,0xdb,0x81,0xb3,0xa0,0xf4,0x45,0x7a,0x19,0xdf,0xee,0x78,0x34,0x60};

unsigned char ZUC_S1[256] =
{0x55,0xc2,0x63,0x71,0x3b,0xc8,0x47,0x86,0x9f,0x3c,0xda,0x5b,0x29,0xaa,0xfd,0x77,
0x8c,0xc5,0x94,0x0c,0xa6,0x1a,0x13,0x00,0xe3,0xa8,0x16,0x72,0x40,0xf9,0xf8,0x42,
0x44,0x26,0x68,0x96,0x81,0xd9,0x45,0x3e,0x10,0x76,0xc6,0xa7,0x8b,0x39,0x43,0xe1,
0x3a,0xb5,0x56,0x2a,0xc0,0x6d,0xb3,0x05,0x22,0x66,0xbf,0xdc,0x0b,0xfa,0x62,0x48,
0xdd,0x20,0x11,0x06,0x36,0xc9,0xc1,0xcf,0xf6,0x27,0x52,0xbb,0x69,0xf5,0xd4,0x87,
0x7f,0x84,0x4c,0xd2,0x9c,0x57,0xa4,0xbc,0x4f,0x9a,0xdf,0xfe,0xd6,0x8d,0x7a,0xeb,
0x2b,0x53,0xd8,0x5c,0xa1,0x14,0x17,0xfb,0x23,0xd5,0x7d,0x30,0x67,0x73,0x08,0x09,
0xee,0xb7,0x70,0x3f,0x61,0xb2,0x19,0x8e,0x4e,0xe5,0x4b,0x93,0x8f,0x5d,0xdb,0xa9,
0xad,0xf1,0xae,0x2e,0xcb,0x0d,0xfc,0xf4,0x2d,0x46,0x6e,0x1d,0x97,0xe8,0xd1,0xe9,
0x4d,0x37,0xa5,0x75,0x5e,0x83,0x9e,0xab,0x82,0x9d,0xb9,0x1c,0xe0,0xcd,0x49,0x89,
0x01,0xb6,0xbd,0x58,0x24,0xa2,0x5f,0x38,0x78,0x99,0x15,0x90,0x50,0xb8,0x95,0xe4,
0xd0,0x91,0xc7,0xce,0xed,0x0f,0xb4,0x6f,0xa0,0xcc,0xf0,0x02,0x4a,0x79,0xc3,0xde,
0xa3,0xef,0xea,0x51,0xe6,0x6b,0x18,0xec,0x1b,0x2c,0x80,0xf7,0x74,0xe7,0xff,0x21,
0x5a,0x6a,0x54,0x1e,0x41,0x31,0x92,0x35,0xc4,0x33,0x07,0x0a,0xba,0x7e,0x0e,0x34,
0x88,0xb1,0x98,0x7c,0xf3,0x3d,0x60,0x6c,0x7b,0xca,0xd3,0x1f,0x32,0x65,0x04,0x28,
0x64,0xbe,0x85,0x9b,0x2f,0x59,0x8a,0xd7,0xb0,0x25,0xac,0xaf,0x12,0x03,0xe2,0xf2};

//D value in key loading
unsigned int ZUC_d[16] = {0x44D7, 0x26BC, 0x626B, 0x135E, 0x5789, 0x35E2, 0x7135, 0x09AF,
0x4D78, 0x2F13, 0x6BC4, 0x1AF1, 0x5E26, 0x3C4D, 0x789A, 0x47AC };

//rotate n bits to the left in a 32bit buffer
#define ZUC_rotl32(x, k)   (((x) << k) | ((x) >> (32 - k)))
//si = ki ¡¬di ¡¬ivi,in key loading
#define ZUC_LinkToS(a, b, c)   (((unsigned int)(a) << 23)|((unsigned int)(b) << 8)|(unsigned
int)(c))



unsigned int AddMod(unsigned int a, unsigned int b);
unsigned int PowMod(unsigned int x, unsigned int k);
unsigned int L1(unsigned int X);
unsigned int L2(unsigned int X);
unsigned char BitValue(unsigned int M[], unsigned int i);
unsigned int GetWord(unsigned int k[], unsigned int i);
void LFSRWithInitMode(unsigned int LFSR_S[],unsigned int u) ;
void LFSRWithWorkMode(unsigned int LFSR_S[]) ;
void BR(unsigned int LFSR_S[],unsigned int BR_X[]);
unsigned int F(unsigned int BR_X[],unsigned int F_R[]);
void ZUC_Init(unsigned char k[], unsigned char iv[],unsigned int LFSR_S[],unsigned int
BR_X[],unsigned int F_R[]);
```

```
void ZUC_Work(unsigned int LFSR_S[],unsigned int BR_X[],unsigned int F_R[], unsigned int pKeyStream[],int KeyStreamLen);
void ZUC_GenKeyStream(unsigned char k[], unsigned char iv[],unsigned int KeyStream[], int KeyStreamLen);
void ZUC_Confidentiality(unsigned char CK[], unsigned int COUNT, unsigned char BEARER,unsigned char DIRECTION,unsigned int IBS[],int LENGTH,unsigned int OBS[]);
unsigned int ZUC_Integrity(unsigned char IK[],unsigned int COUNT,unsigned char BEARER,unsigned char DIRECTION,unsigned int M[],int LENGTH);
```