AES 加密算法及实现

版本记录	版本修改说明
V0.1	1. 初始版本 @20150828

1 GCM 加密实现

1.1 GCM 加密

1.1.1 输入参数

密钥 K：128，192，256 bits 三种模式

初始化向量 IV：1~2^{64} bits

明文 P： 0~（2^{39}-256） bits ,按 128bits 分组，总长度（n-1）* 128 + u，1 ≤ u ≤ 128。即明文由一系列的 n 数据组成，最后一组数据长度为 u，其他长度均为 128 位，记这些明文块为 $P_1,P_2,P_3...P_{n-1},P_n$；

附加认证数据(AAD)，用 A 表示：0~2^{64} bits，按 128bits 分组，总长度为（m-1）* 128 + v，1 ≤ v ≤ 128；记为 $A_1,A_2,A_3...A_{n-1},A_n$

1.1.2 输出参数

密文 C：长度与明文一致，数据分组同明文，记为 $C_1,C_2,C_3...C_{n-1},C_n$

认证标签 T：0~128 bits

1.1.3 加密算法描述

$$
\begin{aligned}
&H = E(K, 0^{128})\\
&Y_0 = \begin{cases} IV\,||0^{31}1\,, & \text{if len}\,(IV) = 96\\ GHASH(H, \{\}, IV), & \text{otherwise}\end{cases}\\
&Y_i = \text{incr}_{32}(Y_i - 1), \qquad i = 1, \dots, n\\
&C_i = P_i \oplus E(K, Y_i), \qquad i = 1, \dots, n-1\\
&C_n = P_n \oplus \text{MSB}_u\big(E(K, Y_n)\big)\\
&T = \text{MSB}_t\,(GHASH(H, A, C) \oplus E(K, Y_0))
\end{aligned}
$$

注：

其中||表示串连接，0^U 表示 U bits 长度的 0

Len(S)返回数据 S（bit）长度，返回值为 64 bits 整型变量

E(K,Y)表示用密钥 K 对 Y 做 AES 加密

$Incr_{32}()$是将数据的最低 32 位看成一个无符号数，将其加 1 后取模 2^{32}，即 $incr(F||I)=F||(I+1)mod2^{32}$

$MSB_t(S)$返回数据 S 的最左边 t bits 数据

{}表示数据长度为 0

⊕表示异或运算

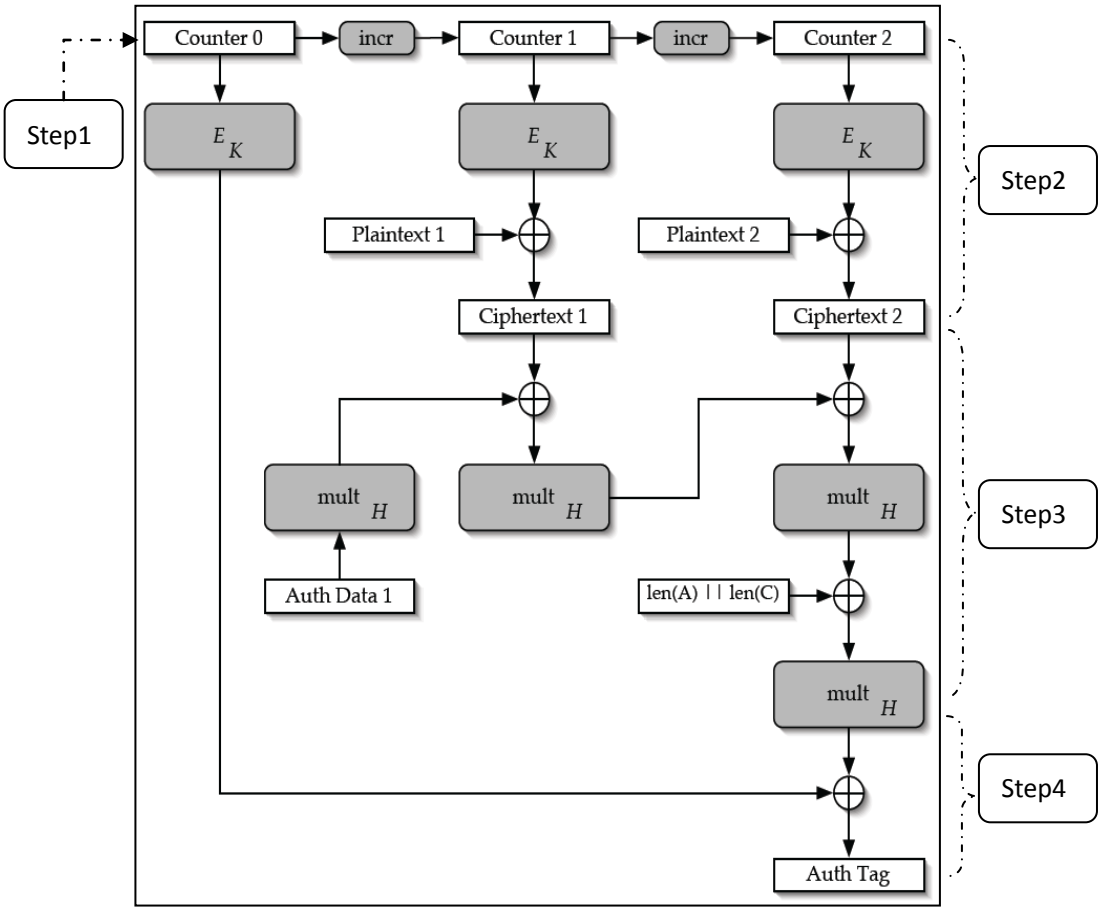
1.1.4 GHASH 算法描述

GHASH(*H, A, C*) = X_{m+n+1}, X=0,1...m+n+1,算法如下，

$$X_i = \begin{cases} 0, & i = 0 \\ (X_{i-1} \oplus A_i) \cdot H, & i = 1, \dots, m-1 \\ \left(X_{m-1} \oplus (A_m || 0^{128-v})\right) \cdot H, & i = m \\ (X_{i-1} \oplus C_{i-m}) \cdot H, & i = m+1, \dots, m+n-1 \\ \left(X_{m+n-1} \oplus (C_n || 0^{128-u})\right) \cdot H, & i = m+n \\ \left(X_{m+n} \oplus (Len(A) || Len(C))\right) \cdot H, & i = m+n+1 \end{cases}$$

1.1.5 流程框图

Step1：计算 H 初值及 Y0(Counter0)初值；
Step2：对明文 plaintext 进行 CTR_K 加密，K 为密钥，得到密文 Ciphertext
Step3：运算 GHASH(H,A,C)认证函数
Step4：step3 结果与 $E(K,Y_0)$异或，得到认证标签 T



注：
Counter i 为公式中的 Y_i ；
E_K 为公式中 E(K,Y)，mult $_H$ 为有限域乘法，为公式中的(S).H

1.2 GCM 解密

1.2.1 解密算法描述

解密过程与加密过程类似，仅需将明文和密文输入输出对调即可，不同的地方是，解密过程必须先进行标签认证，认证通过才可对密文解密。

$$
\begin{aligned}
&H = E(K, 0^{128}) \\
&Y_0 = \begin{cases} IV \,||0^{31}1\,, & \text{if len (IV)} = 96 \\ GHASH(H, \{\}, IV), & \text{otherwise} \end{cases} \\
&T' = MSB_t\,(GHASH(H, A, C) \oplus E(K, Y_0)) \\
&Y_i = incr_{32}(Y_i - 1), \qquad i = 1, \ldots, n \\
&P_i = C_i \oplus E(K, Y_i), \qquad i = 1, \ldots, n-1 \\
&P_n = C_n \oplus MSB_u\big(E(K, Y_n)\big)
\end{aligned}
$$

1.2.2 流程框图

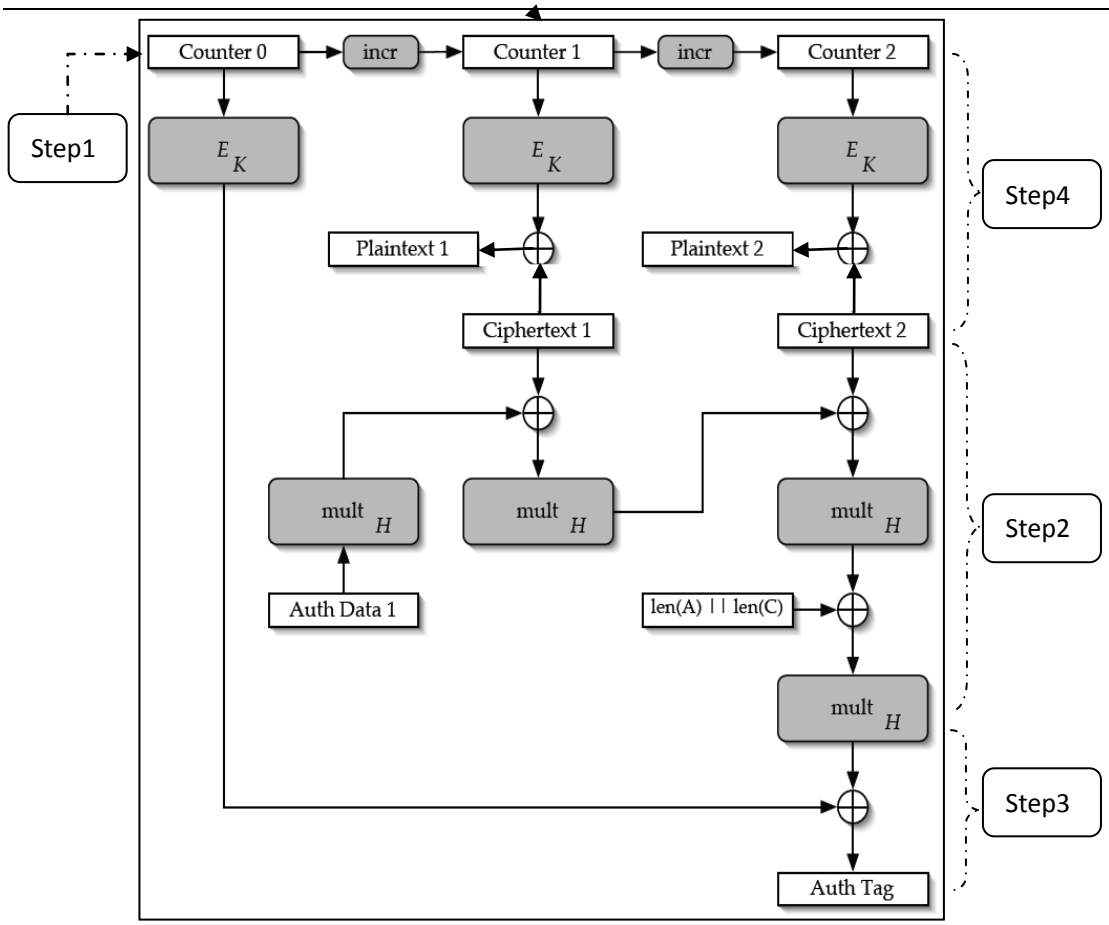
Step1：计算 H 初值及 Y0(Counter0)初值；

Step2：运算 GHASH(H,A,C)认证函数

Step3：step2 结果与 $E(K,Y_0)$异或，得到认证标签 T’，与实际 T 比对

Step2：若 T’=T，对密文 Ciphertext 进行 CTR_K 加密，K 为密钥，得到明文 plaintext

若 T’≠T，则认证失败


Counter 0
incr
Counter 1
incr
Counter 2
Step1
E K
E K
E K
Step4
Plaintext 1
Plaintext 2
Ciphertext 1
Ciphertext 2
mult H
mult H
mult H
Step2
Auth Data 1
len(A) || len(C)
mult H
Step3
Auth Tag

1.3 算法实现

1.3.1 集成模块

HT6X2X 和 HT501X 系列芯片，内部集成了 **AES 加密/解密模块**和 **GHASH 有限域乘法模块**；可以实现流程框图中 E_K 和 $muit_H$ 部分功能；

1.3.2 GCM 库函数

1. GCM 加密函数

函数声明：

void GCM_Encrypt(GCM_Encrypt_InputTypedef* GCM_InputStruct,
GCM_Encrypt_OutputTypedef* GCM_OutputStruct)；

入口参数:

GCM_InputStruct GCM 加密输入变量结构体指针，主要包含 8 个参数:
1) AESKeyMode ：加密解密模式选择
2) *pKeyAddr ：密钥地址指针
3) *pInitVectorAddr ：初始向量地址指针
4) LenIV ：初始向量数据长度（byte）
5) *pPtextAddr ：明文数据地址指针
6) LenPtext ：明文数据长度（byte）
7) *pAdataAddr ：附加认证数据地址指针
8) LenAdata ：附加认证数据长度（byte）

GCM_OutputStruct GCM 加密输出变量结构体指针，主要包含 3 个参数:
1) *pCtextAddr ：已加密数据密文地址指针
2) LenCtext ：已加密数据密文长度（byte）
3) AuthTag ：认证标签数据地址指针

返回参数: 无

2. GCM 解密函数

函数声明:

Bool GCM_Decrypt(GCM_Decrypt_InputTypedef* GCM_InputStruct,
GCM_Decrypt_OutputTypedef* GCM_OutputStruct)；

入口参数:

GCM_InputStruct GCM 解密输入变量结构体指针，主要包含 8 个参数:
1) AESKeyMode ：加密解密模式选择
2) *pKeyAddr ：密钥地址指针
3) *pInitVectorAddr ：初始向量地址指针
4) LenIV ：初始向量数据长度（byte）
5) *pCtextAddr ：数据密文地址指针

6) LenCtext ：数据密文长度（byte?
7) *pAdataAddr ：附加认证数据地址指针
8) LenAdata ：附加认证数据长度（byte）
9) AuthTag ：认证标签数据地址指针

GCM_OutputStruct GCM 解密输出变量结构体指针，主要包含 3 个参数:
1) *pPtextAddr ：明文数据地址指针
2) LenPtext ：明文数据长度（byte）

返回参数:

Bool = TRUE(1)： 认证成功
= FALSE(0)： 认证失败

1.4 TEST CASE

1.4.1 Testcase1

Variable	Value
K	00000000000000000000000000000000
P	
IV	000000000000000000000000
H	66e94bd4ef8a2c3b884cfa59ca342b2e
Y_0	00000000000000000000000000000001
$E(K, Y_0)$	58e2fccefa7e3061367f1d57a4e7455a
$\text{len}(A)\|\|\text{len}(C)$	00000000000000000000000000000000
$\text{GHASH}(H, A, C)$	00000000000000000000000000000000
C	
T	58e2fccefa7e3061367f1d57a4e7455a

1.4.2 Testcase2

Variable	Value
K	00000000000000000000000000000000
P	00000000000000000000000000000000
IV	000000000000000000000000
H	66e94bd4ef8a2c3b884cfa59ca342b2e
Y_0	00000000000000000000000000000001
$E(K, Y_0)$	58e2fccefa7e3061367f1d57a4e7455a
Y_1	00000000000000000000000000000002
$E(K, Y_1)$	0388dace60b6a392f328c2b971b2fe78
X_1	5e2ec746917062882c85b0685353deb7
$\text{len}(A)\|\|\text{len}(C)$	00000000000000000000000000000080
$\text{GHASH}(H, A, C)$	f38cbb1ad69223dcc3457ae5b6b0f885
C	0388dace60b6a392f328c2b971b2fe78
T	ab6e47d42cec13bdf53a67b21257bddf

1.4.3 Testcase3

Variable	Value
K	feffe9928665731c6d6a8f9467308308
P	d9313225f88406e5a55909c5aff5269a
	86a7a9531534f7da2e4c303d8a318a72
	1c3c0c95956809532fcf0e2449a6b525
	b16aedf5aa0de657ba637b391aafd255
IV	cafebabefacedbaddecaf888
H	b83b533708bf535d0aa6e52980d53b78
Y_0	cafebabefacedbaddecaf88800000001
$E(K, Y_0)$	3247184b3c4f69a44dbcd22887bbb418
Y_1	cafebabefacedbaddecaf88800000002
$E(K, Y_1)$	9bb22ce7d9f372c1ee2b28722b25f206
Y_2	cafebabefacedbaddecaf88800000003
$E(K, Y_2)$	650d887c3936533a1b8d4e1ea39d2b5c
Y_3	cafebabefacedbaddecaf88800000004
$E(K, Y_3)$	3de91827c10e9a4f5240647ee5221f20
Y_4	cafebabefacedbaddecaf88800000005
$E(K, Y_4)$	aac9e6ccc0074ac0873b9ba85d908bd0
X_1	59ed3f2bb1a0aaa07c9f56c6a504647b
X_2	b714c9048389afd9f9bc5c1d4378e052
X_3	47400c6577b1ee8d8f40b2721e86ff10
X_4	4796cf49464704b5dd91f159bb1b7f95
$\text{len}(A)\|\|\text{len}(C)$	00000000000000000000000000000200
$\text{GHASH}(H, A, C)$	7f1b32b81b820d02614f8895ac1d4eac
C	42831ec2217774244b7221b784d0d49c
	e3aa212f2c02a4e035c17e2329aca12e
	21d514b25466931c7d8f6a5aac84aa05
	1ba30b396a0aac973d58e091473f5985
T	4d5c2af327cd64a62cf35abd2ba6fab4

1.4.4 Testcase4

Variable	Value
K	feffe9928665731c6d6a8f9467308308
P	d9313225f88406e5a55909c5aff5269a
	86a7a9531534f7da2e4c303d8a318a72
	1c3c0c95956809532fcf0e2449a6b525
	b16aedf5aa0de657ba637b39
A	feedfacedeadbeeffeedfacedeadbeef
	abaddad2
IV	cafebabefacedbaddecaf888
H	b83b533708bf535d0aa6e52980d53b78
Y_0	cafebabefacedbaddecaf88800000001
$E(K, Y_0)$	3247184b3c4f69a44dbcd22887bbb418
X_1	ed56aaf8a72d67049fdb9228edba1322
X_2	cd47221ccef0554ee4bb044c88150352
Y_1	cafebabefacedbaddecaf88800000002
$E(K, Y_1)$	9bb22ce7d9f372c1ee2b28722b25f206
Y_2	cafebabefacedbaddecaf88800000003
$E(K, Y_2)$	650d887c3936533a1b8d4e1ea39d2b5c
Y_3	cafebabefacedbaddecaf88800000004
$E(K, Y_3)$	3de91827c10e9a4f5240647ee5221f20
Y_4	cafebabefacedbaddecaf88800000005
$E(K, Y_4)$	aac9e6ccc0074ac0873b9ba85d908bd0
X_3	54f5e1b2b5a8f9525c23924751a3ca51
X_4	324f585c6ffc1359ab371565d6c45f93
X_5	ca7dd446af4aa70cc3c0cd5abba6aa1c
X_6	1590df9b2eb6768289e57d56274c8570
$\text{len}(A)\|\|\text{len}(C)$	00000000000000a000000000000001e0
$\text{GHASH}(H, A, C)$	698e57f70e6ecc7fd9463b7260a9ae5f
C	42831ec2217774244b7221b784d0d49c
	e3aa212f2c02a4e035c17e2329aca12e
	21d514b25466931c7d8f6a5aac84aa05
	1ba30b396a0aac973d58e091
T	5bc94fbc3221a5db94fae95ae7121a47

1.4.5 Testcase5

Variable	Value
K	feffe9928665731c6d6a8f9467308308
P	d9313225f88406e5a55909c5aff5269a
	86a7a9531534f7da2e4c303d8a318a72
	1c3c0c95956809532fcf0e2449a6b525
	b16aedf5aa0de657ba637b39
A	feedfacedeadbeeffeedfacedeadbeef
	abaddad2
IV	cafebabefacedbad
H	b83b533708bf535d0aa6e52980d53b78
N_1	6f288b846e5fed9a18376829c86a6a16
$\text{len}(\{\})\|\|\text{len}(IV)$	00000000000000000000000000000040
Y_0	c43a83c4c4badec4354ca984db252f7d
$E(K, Y_0)$	e94ab9535c72bea9e089c93d48e62fb0
X_1	ed56aaf8a72d67049fdb9228edba1322
X_2	cd47221ccef0554ee4bb044c88150352
Y_1	c43a83c4c4badec4354ca984db252f7e
$E(K, Y_1)$	b8040969d08295afd226fcda0ddf61cf
Y_2	c43a83c4c4badec4354ca984db252f7f
$E(K, Y_2)$	ef3c83225af93122192ad5c4f15dfe51
Y_3	c43a83c4c4badec4354ca984db252f80
$E(K, Y_3)$	6fbc659571f72de104c67b609d2fde67
Y_4	c43a83c4c4badec4354ca984db252f81
$E(K, Y_4)$	f8e3581441a1e950785c3ea1430c6fa6
X_3	9379e2feae14649c86cf2250e3a81916
X_4	65dde904c92a6b3db877c4817b50a5f4
X_5	48c53cf863b49a1b0bbfc48c3baaa89d
X_6	08c873f1c8cec3effc209a07468caab1
$\text{len}(A)\|\|\text{len}(C)$	00000000000000a000000000000001e0
$\text{GHASH}(H, A, C)$	df586bb4c249b92cb6922877e444d37b
C	61353b4c2806934a777ff51fa22a4755
	699b2a714fcdc6f83766e5f97b6c7423
	73806900e49f24b22b097544d4896b42
	4989b5e1ebac0f07c23f4598
T	3612d2e79e3b0785561be14aaca2fccb

1.4.6 Testcase6

Variable	Value
K	feffe9928665731c6d6a8f9467308308
P	d9313225f88406e5a55909c5aff5269a 86a7a9531534f7da2e4c303d8a318a72 1c3c0c95956809532fcf0e2449a6b525 b16aedf5aa0de657ba637b39
A	feedfacedeadbeeffeedfacedeadbeef abaddad2
IV	9313225df88406e555909c5aff5269aa 6a7a9538534f7da1e4c303d2a318a728 c3c0c95156809539fcf0e2429a6b5254 16aedbf5a0de6a57a637b39b
H	b83b533708bf535d0aa6e52980d53b78
N_1	004d6599d7fb1634756e1e299d81630f
N_2	88ffe8a3c8033df4b54d732f7f88408e
N_3	24e694cfab657beabba8055aad495e23
N_4	d8349a5eda24943c8fbb2ef5168b20cb
$\text{len}(\{\})\|\|\text{len}(IV)$	00000000000000000000000001e0
Y_0	3bab75780a31c059f83d2a44752f9864
$E(K, Y_0)$	7dc63b399f2d98d57ab073b6baa4138e
X_1	ed56aaf8a72d67049fdb9228edba1322
X_2	cd47221ccef0554ee4bb044c88150352
Y_1	3bab75780a31c059f83d2a44752f9865
$E(K, Y_1)$	55d37bbd9ad21353a6f93a690eca9e0e
Y_2	3bab75780a31c059f83d2a44752f9866
$E(K, Y_2)$	3836bbf6d696e672946a1a01404fa6d5
Y_3	3bab75780a31c059f83d2a44752f9867
$E(K, Y_3)$	1dd8a5316ecc35c3e313bca59d2ac94a
Y_4	3bab75780a31c059f83d2a44752f9868
$E(K, Y_4)$	6742982706a9f154f657d5dc94b746db
X_3	31727669c63c6f078b5d22adbbbca384
X_4	480c00db2679065a7ed2f771a53acacd
X_5	1c1ae3c355e2214466a9923d2ba6ab35
X_6	0694c6f16bb0275a48891d06590344b0
$\text{len}(A)\|\|\text{len}(C)$	00000000000000a000000000000001e0
$\text{GHASH}(H, A, C)$	1c5afe9760d3932f3c9a878aac3dc3de
C	8ce24998625615b603a033aca13fb894 be9112a5c3a211a8ba262a3cca7e2ca7 01e4a9a4fba43c90ccdcb281d48c7c6f d62875d2aca417034c34aee5
T	619cc5aefffe0bfa462af43c1699d050

1.4.7 Testcase7

Variable	Value
K	00000000000000000000000000000000
	0000000000000000
P	
IV	000000000000000000000000
H	aae06992acbf52a3e8f4a96ec9300bd7
Y_0	00000000000000000000000000000001
$E(K, Y_0)$	cd33b28ac773f74ba00ed1f312572435
$\text{len}(A)\|\|\text{len}(C)$	00000000000000000000000000000000
$\text{GHASH}(H, A, C)$	00000000000000000000000000000000
C	
T	cd33b28ac773f74ba00ed1f312572435

1.4.8 Testcase8

Variable	Value
K	00000000000000000000000000000000
	0000000000000000
P	00000000000000000000000000000000
IV	000000000000000000000000
H	aae06992acbf52a3e8f4a96ec9300bd7
Y_0	00000000000000000000000000000001
$E(K, Y_0)$	cd33b28ac773f74ba00ed1f312572435
Y_1	00000000000000000000000000000002
$E(K, Y_1)$	98e7247c07f0fe411c267e4384b0f600
X_1	90e87315fb7d4e1b4092ec0cbfda5d7d
$\text{len}(A)\|\|\text{len}(C)$	00000000000000000000000000000080
$\text{GHASH}(H, A, C)$	e2c63f0ac44ad0e02efa05ab6743d4ce
C	98e7247c07f0fe411c267e4384b0f600
T	2ff58d80033927ab8ef4d4587514f0fb

1.4.9 Testcase9

Variable	Value
K	feffe9928665731c6d6a8f9467308308
	feffe9928665731c
P	d9313225f88406e5a55909c5aff5269a
	86a7a9531534f7da2e4c303d8a318a72
	1c3c0c95956809532fcf0e2449a6b525
	b16aedf5aa0de657ba637b391aafd255
IV	cafebabefacedbaddecaf888
H	466923ec9ae682214f2c082badb39249
Y_0	cafebabefacedbaddecaf88800000001
$E(K, Y_0)$	c835aa88aebbc94f5a02e179fdcfc3e4
Y_1	cafebabefacedbaddecaf88800000002
$E(K, Y_1)$	e0b1f82ec484eea44e5ff30128df01cd
Y_2	cafebabefacedbaddecaf88800000003
$E(K, Y_2)$	0339b5b9b3db2e5e4cc9a38986906bee
Y_3	cafebabefacedbaddecaf88800000004
$E(K, Y_3)$	614b3195542ccc7683ae933c81ec8a62
Y_4	cafebabefacedbaddecaf88800000005
$E(K, Y_4)$	a988a97e85eec28e76b95c29b6023003
X_1	dddca3f91c17821ffac4a6d0fed176f7
X_2	a4e84ac60e2730f4a7e0e1eef708b198
X_3	e67592048dd7153973a0dbbb8804bee2
X_4	503e86628536625fb746ce3cecea433f
$\text{len}(A)\|\|\text{len}(C)$	00000000000000000000000000000200
$\text{GHASH}(H, A, C)$	51110d40f6c8fff0eb1ae33445a889f0
C	3980ca0b3c00e841eb06fac4872a2757
	859e1ceaa6efd984628593b40ca1e19c
	7d773d00c144c525ac619d18c84a3f47
	18e2448b2fe324d9ccda2710acade256
T	9924a7c8587336bfb118024db8674a14

1.4.10 Testcase10

Variable	Value
K	feffe9928665731c6d6a8f9467308308
	feffe9928665731c
P	d9313225f88406e5a55909c5aff5269a
	86a7a9531534f7da2e4c303d8a318a72
	1c3c0c95956809532fcf0e2449a6b525
	b16aedf5aa0de657ba637b39
A	feedfacedeadbeeffeedfacedeadbeef
	abaddad2
IV	cafebabefacedbaddecaf888
H	466923ec9ae682214f2c082badb39249
Y_0	cafebabefacedbaddecaf88800000001
$E(K, Y_0)$	c835aa88aebbc94f5a02e179fdcfc3e4
X_1	f3bf7ba3e305aeb05ed0d2e4fe076666
X_2	20a51fa2302e9c01b87c48f2c3d91a56
Y_1	cafebabefacedbaddecaf88800000002
$E(K, Y_1)$	e0b1f82ec484eea44e5ff30128df01cd
Y_2	cafebabefacedbaddecaf88800000003
$E(K, Y_2)$	0339b5b9b3db2e5e4cc9a38986906bee
Y_3	cafebabefacedbaddecaf88800000004
$E(K, Y_3)$	614b3195542ccc7683ae933c81ec8a62
Y_4	cafebabefacedbaddecaf88800000005
$E(K, Y_4)$	a988a97e85eec28e76b95c29b6023003
X_3	714f9700ddf520f20695f6180c6e669d
X_4	e858680b7b240d2ecf7e06bbad4524e2
X_5	3f4865abd6bb3fb9f5c4a816f0a9b778
X_6	4256f67fe87b4f49422ba11af857c973
$\text{len}(A)\|\|\text{len}(C)$	00000000000000a000000000000001e0
$\text{GHASH}(H, A, C)$	ed2ce3062e4a8ec06db8b4c490e8a268
C	3980ca0b3c00e841eb06fac4872a2757
	859e1ceaa6efd984628593b40ca1e19c
	7d773d00c144c525ac619d18c84a3f47
	18e2448b2fe324d9ccda2710
T	2519498e80f1478f37ba55bd6d27618c

1.4.11 Testcase11

Variable	Value
K	feffe9928665731c6d6a8f9467308308
	feffe9928665731c
P	d9313225f88406e5a55909c5aff5269a
	86a7a9531534f7da2e4c303d8a318a72
	1c3c0c95956809532fcf0e2449a6b525
	b16aedf5aa0de657ba637b39
A	feedfacedeadbeeffeedfacedeadbeef
	abaddad2
IV	cafebabefacedbad
H	466923ec9ae682214f2c082badb39249
N_1	9473c07b02544299cf007c42c5778218
$\text{len}(\{\})\|\|\text{len}(IV)$	00000000000000000000000000000040
Y_0	a14378078d27258a6292737e1802ada5
$E(K, Y_0)$	7bb6d647c902427ce7cf26563a337371
X_1	f3bf7ba3e305aeb05ed0d2e4fe076666
X_2	20a51fa2302e9c01b87c48f2c3d91a56
Y_1	a14378078d27258a6292737e1802ada6
$E(K, Y_1)$	d621c7bc5690a7b1487dbaab8ac76b22
Y_2	a14378078d27258a6292737e1802ada7
$E(K, Y_2)$	43c1ca7de78f4495ad0b18324e61fa25
Y_3	a14378078d27258a6292737e1802ada8
$E(K, Y_3)$	e1e0254a0f2f1626e9aa4ff09d7c64ec
Y_4	a14378078d27258a6292737e1802ada9
$E(K, Y_4)$	5850f4502486a1681a9319ce7d0afa59
X_3	8bdedafd6ee8e529689de3a269b8240d
X_4	6607feb377b49c9ecdbc696344fe22d8
X_5	8a19570a06500ba9405fcece4a73fb48
X_6	8532826e63ce4a5b89b70fa28f8070fe
$\text{len}(A)\|\|\text{len}(C)$	00000000000000a000000000000001e0
$\text{GHASH}(H, A, C)$	1e6a133806607858ee80eaf237064089
C	0f10f599ae14a154ed24b36e25324db8
	c566632ef2bbb34f8347280fc4507057
	fddc29df9a471f75c66541d4d4dad1c9
	e93a19a58e8b473fa0f062f7
T	65dcc57fcf623a24094fcca40d3533f8

1.4.12 Testcase12

Variable	Value
K	feffe9928665731c6d6a8f9467308308 feffe9928665731c
P	d9313225f88406e5a55909c5aff5269a 86a7a9531534f7da2e4c303d8a318a72 1c3c0c95956809532fcf0e2449a6b525 b16aedf5aa0de657ba637b39
A	feedfacedeadbeeffeedfacedeadbeef abaddad2
IV	9313225df88406e555909c5aff5269aa 6a7a9538534f7da1e4c303d2a318a728 c3c0c95156809539fcf0e2429a6b5254 16aedbf5a0de6a57a637b39b
H	466923ec9ae682214f2c082badb39249
N_1	19aef0f04763b0c87903c5a217d5314f
N_2	62120253f79efc978625d1feb03b5b5b
N_3	b6ce2a84e366de900fa78a1653df77fb
N_4	374ecad90487f0bb261ba817447e022c
$\text{len}(\{\})\|\|\text{len}(IV)$	00000000000000000000000000001e0
Y_0	4505cdc367a054c5002820e96aebef27
$E(K, Y_0)$	5ea3194f9dd012a3b9bc5103d6e0284d
X_1	f3bf7ba3e305aeb05ed0d2e4fe076666
X_2	20a51fa2302e9c01b87c48f2c3d91a56
Y_1	4505cdc367a054c5002820e96aebef28
$E(K, Y_1)$	0b4fba4de46722d9ed691f9f2029df65
Y_2	4505cdc367a054c5002820e96aebef29
$E(K, Y_2)$	9b4e088bf380b03540bb87a5a257e437
Y_3	4505cdc367a054c5002820e96aebef2a
$E(K, Y_3)$	9ddb9c873a5cd48acd3f397cd28f9896
Y_4	4505cdc367a054c5002820e96aebef2b
$E(K, Y_4)$	5716ee92eff7c4b053d44c0294ea88cd
X_3	f70d61693ea7f53f08c866d6eedb1e4b
X_4	dc40bc9a181b35aed66488071ef282ae
X_5	85ffa424b87b35cac7be9c450f0d7aee
X_6	65233cbe5251f7d246bfc967a8678647
$\text{len}(A)\|\|\text{len}(C)$	00000000000000a000000000000001e0
$\text{GHASH}(H, A, C)$	82567fb0b4cc371801eadec005968e94
C	d27e88681ce3243c4830165a8fdcf9ff 1de9a1d8e6b447ef6ef7b79828666e45 81e79012af34ddd9e2f037589b292db3 e67c036745fa22e7e9b7373b
T	dcf566ff291c25bbb8568fc3d376a6d9

1.4.13 Testcase13

Variable	Value
K	00000000000000000000000000000000
	00000000000000000000000000000000
P	
IV	000000000000000000000000
H	dc95c078a2408989ad48a21492842087
Y_0	00000000000000000000000000000001
$E(K, Y_0)$	530f8afbc74536b9a963b4f1c4cb738b
$\text{len}(A)\|\|\text{len}(C)$	00000000000000000000000000000000
$\text{GHASH}(H, A, C)$	00000000000000000000000000000000
C	
T	530f8afbc74536b9a963b4f1c4cb738b

1.4.14 Testcase14

Variable	Value
K	00000000000000000000000000000000
	00000000000000000000000000000000
P	00000000000000000000000000000000
IV	000000000000000000000000
H	dc95c078a2408989ad48a21492842087
Y_0	00000000000000000000000000000001
$E(K, Y_0)$	530f8afbc74536b9a963b4f1c4cb738b
Y_1	00000000000000000000000000000002
$E(K, Y_1)$	cea7403d4d606b6e074ec5d3baf39d18
X_1	fd6ab7586e556dba06d69cfe6223b262
$\text{len}(A)\|\|\text{len}(C)$	00000000000000000000000000000080
$\text{GHASH}(H, A, C)$	83de425c5edc5d498f382c441041ca92
C	cea7403d4d606b6e074ec5d3baf39d18
T	d0d1c8a799996bf0265b98b5d48ab919

1.4.15 Testcase15

Variable	Value
K	feffe9928665731c6d6a8f9467308308
	feffe9928665731c6d6a8f9467308308
P	d9313225f88406e5a55909c5aff5269a
	86a7a9531534f7da2e4c303d8a318a72
	1c3c0c95956809532fcf0e2449a6b525
	b16aedf5aa0de657ba637b391aafd255
IV	cafebabefacedbaddecaf888
H	acbef20579b4b8ebce889bac8732dad7
Y_0	cafebabefacedbaddecaf88800000001
$E(K, Y_0)$	fd2caa16a5832e76aa132c1453eeda7e
Y_1	cafebabefacedbaddecaf88800000002
$E(K, Y_1)$	8b1cf3d561d27be251263e66857164e7
Y_2	cafebabefacedbaddecaf88800000003
$E(K, Y_2)$	e29d258faad137135bd49280af645bd8
Y_3	cafebabefacedbaddecaf88800000004
$E(K, Y_3)$	908c82ddcc65b26e887f85341f243d1d
Y_4	cafebabefacedbaddecaf88800000005
$E(K, Y_4)$	749cf39639b79c5d06aa8d5b932fc7f8
X_1	fcbefb78635d598eddaf982310670f35
X_2	29de812309d3116a6eff7ec844484f3e
X_3	45fad9deeda9ea561b8f199c3613845b
X_4	ed95f8e164bf3213febc740f0bd9c6af
$\text{len}(A)\|\|\text{len}(C)$	00000000000000000000000000000200
$\text{GHASH}(H, A, C)$	4db870d37cb75fcb46097c36230d1612
C	522dc1f099567d07f47f37a32a84427d
	643a8cdcbfe5c0c97598a2bd2555d1aa
	8cb08e48590dbb3da7b08b1056828838
	c5f61e6393ba7a0abcc9f662898015ad
T	b094dac5d93471bdec1a502270e3cc6c

1.4.16 Testcase16

Variable	Value
K	feffe9928665731c6d6a8f9467308308
	feffe9928665731c6d6a8f9467308308
P	d9313225f88406e5a55909c5aff5269a
	86a7a9531534f7da2e4c303d8a318a72
	1c3c0c95956809532fcf0e2449a6b525
	b16aedf5aa0de657ba637b39
A	feedfacedeadbeeffeedfacedeadbeef
	abaddad2
IV	cafebabefacedbaddecaf888
H	acbef20579b4b8ebce889bac8732dad7
Y_0	cafebabefacedbaddecaf88800000001
$E(K, Y_0)$	fd2caa16a5832e76aa132c1453eeda7e
X_1	5165d242c2592c0a6375e2622cf925d2
X_2	8efa30ce83298b85fe71abefc0cdd01d
Y_1	cafebabefacedbaddecaf88800000002
$E(K, Y_1)$	8b1cf3d561d27be251263e66857164e7
Y_2	cafebabefacedbaddecaf88800000003
$E(K, Y_2)$	e29d258faad137135bd49280af645bd8
Y_3	cafebabefacedbaddecaf88800000004
$E(K, Y_3)$	908c82ddcc65b26e887f85341f243d1d
Y_4	cafebabefacedbaddecaf88800000005
$E(K, Y_4)$	749cf39639b79c5d06aa8d5b932fc7f8
X_3	abe07e0bb62354177480b550f9f6cdcc
X_4	3978e4f141b95f3b4699756b1c3c2082
X_5	8abf3c48901debe76837d8a05c7d6e87
X_6	9249beaf520c48b912fa120bbf391dc8
$\text{len}(A)\|\|\text{len}(C)$	00000000000000a000000000000001e0
$\text{GHASH}(H, A, C)$	8bd0c4d8aacd391e67cca447e8c38f65
C	522dc1f099567d07f47f37a32a84427d
	643a8cdcbfe5c0c97598a2bd2555d1aa
	8cb08e48590dbb3da7b08b1056828838
	c5f61e6393ba7a0abcc9f662
T	76fc6ece0f4e1768cddf8853bb2d551b

1.4.17 Testcase17

Variable	Value
K	feffe9928665731c6d6a8f9467308308
	feffe9928665731c6d6a8f9467308308
P	d9313225f88406e5a55909c5aff5269a
	86a7a9531534f7da2e4c303d8a318a72
	1c3c0c95956809532fcf0e2449a6b525
	b16aedf5aa0de657ba637b39
A	feedfacedeadbeeffeedfacedeadbeef
	abaddad2
IV	cafebabefacedbad
H	acbef20579b4b8ebce889bac8732dad7
N_1	90c22e3d2aca34b971e8bd09708fae5c
$\text{len}(\{\})\|\|\text{len}(IV)$	00000000000000000000000000000040
Y_0	0095df49dd90abe3e4d252475748f5d4
$E(K, Y_0)$	4f903f37fe611d454217fbfa5cd7d791
X_1	5165d242c2592c0a6375e2622cf925d2
X_2	8efa30ce83298b85fe71abefc0cdd01d
Y_1	0095df49dd90abe3e4d252475748f5d5
$E(K, Y_1)$	1a471fd432fc7bd70b1ec8fe5e6d6251
Y_2	0095df49dd90abe3e4d252475748f5d6
$E(K, Y_2)$	29bd481e1ea39d20eb63c7ea118b1792
Y_3	0095df49dd90abe3e4d252475748f5d7
$E(K, Y_3)$	e2898e46ac5cada3ba83cc1272618a5d
Y_4	0095df49dd90abe3e4d252475748f5d8
$E(K, Y_4)$	d3c6aefbcea602ce4e1fe026065447bf
X_3	55e1ff68f9249e64b95223858e5cb936
X_4	cef1c034383dc96f733aaa4c99bd3e61
X_5	68588d004fd468f5854515039b08165d
X_6	2378943c034697f72a80fce5059bf3f3
$\text{len}(A)\|\|\text{len}(C)$	00000000000000a000000000000001e0
$\text{GHASH}(H, A, C)$	75a34288b8c68f811c52b2e9a2f97f63
C	c3762df1ca787d32ae47c13bf19844cb
	af1ae14d0b976afac52ff7d79bba9de0
	feb582d33934a4f0954cc2363bc73f78
	62ac430e64abe499f47c9b1f
T	3a337dbf46a792c45e454913fe2ea8f2

1.4.18 Testcase18

Variable	Value
K	feffe9928665731c6d6a8f9467308308
	feffe9928665731c6d6a8f9467308308
P	d9313225f88406e5a55909c5aff5269a
	86a7a9531534f7da2e4c303d8a318a72
	1c3c0c95956809532fcf0e2449a6b525
	b16aedf5aa0de657ba637b39
A	feedfacedeadbeeffeedfacedeadbeef
	abaddad2
IV	9313225df88406e555909c5aff5269aa
	6a7a9538534f7da1e4c303d2a318a728
	c3c0c95156809539fcf0e2429a6b5254
	16aedbf5a0de6a57a637b39b
H	acbef20579b4b8ebce889bac8732dad7
N_1	0bfe66e2032f195516379f5fb710f987
N_2	f0631554d11409915feec8f9f5102aba
N_3	749b90dda19a1557fd9e9fd31fed1d14
N_4	7a6a833f260d848793b327cb07d1b190
$\text{len}(\{\})\|\|\text{len}(IV)$	00000000000000000000000001e0
Y_0	0cd953e2140a5976079f8e2406bc8eb4
$E(K, Y_0)$	71b54d092bb0c3d9ba94538d4096e691
X_1	5165d242c2592c0a6375e2622cf925d2
X_2	8efa30ce83298b85fe71abefc0cdd01d
Y_1	0cd953e2140a5976079f8e2406bc8eb5
$E(K, Y_1)$	83bcdd0af41a551452047196ca6b0cba
Y_2	0cd953e2140a5976079f8e2406bc8eb6
$E(K, Y_2)$	68151b79baea93c38e149b72e545e186
Y_3	0cd953e2140a5976079f8e2406bc8eb7
$E(K, Y_3)$	13fccf22159a4d16026ce5d58c7e99fb
Y_4	0cd953e2140a5976079f8e2406bc8eb8
$E(K, Y_4)$	132b64628a031e79fecd050675a64f07
X_3	e963941cfa8c417bdaa3b3d94ab4e905
X_4	2178d7f836e5fa105ce0fdf0fc8f0654
X_5	bac14eeba3216f966b3e7e011475b832
X_6	cc9ae9175729a649936e890bd971a8bf
$\text{len}(A)\|\|\text{len}(C)$	00000000000000a000000000000001e0
$\text{GHASH}(H, A, C)$	d5ffcf6fc5ac4d69722187421a7f170b
C	5a8def2f0c9e53f1f75d7853659e2a20
	eeb2b22aafde6419a058ab4f6f746bf4
	0fc0c3b780f244452da3ebf1c5d82cde
	a2418997200ef82e44ae7e3f
T	a44a8266ee1c8eb0c8b5d4cf5ae9f19a

2 CTR 加密实现

2.1 CTR 加密

2.1.1 输入参数

密钥 K：128，192，256 bits 三种模式

初始化 Counter0（Y0）： 1~128 bits

明文 P： 按 128bits 分组，总长度（n-1）* 128 + u，1 ≤ u ≤ 128。即明文由一系列的 n 数据组成，最后一组数据长度为 u，其他长度均为 128 位，记这些明文块为 $P_1,P_2,P_3...P_{n-1},P_n$；

2.1.2 输出参数

密文 C：长度与明文一致，数据分组同明文，记为 $C_1,C_2,C_3...C_{n-1},C_n$

2.1.3 加密算法描述

$$
\begin{aligned}
Y_i &= \mathrm{incr}_{32}(Y_i - 1), && i = 1, \dots, n \\
C_i &= P_i \oplus E(K, Y_i), && i = 1, \dots, n-1 \\
C_n &= P_n \oplus \mathrm{MSB}_u\big(E(K, Y_n)\big)
\end{aligned}
$$

注：

其中 E(K,Y)表示用密钥 K 对 Y 做 AES 加密

$Incr_{32}()$是将数据的最低 32 位看成一个无符号数，将其加 1 后取模 2^{32}，即 $incr(F||I)=F||(I+1)mod2^{32}$

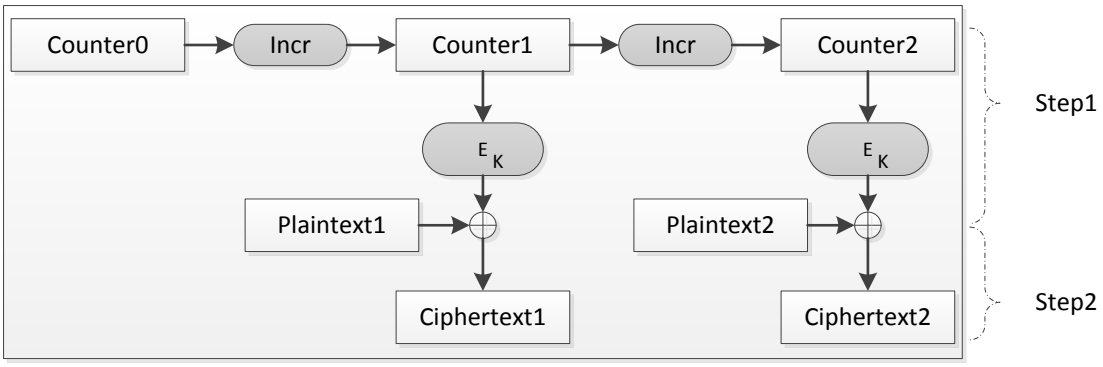
$MSB_t(S)$返回数据 S 的最左边 t bits 数据

⊕表示异或运算

2.1.4 流程框图

Step1：对 Counter 进行 AES 加密，K 为密钥

Step2：step1 结果与明文 plaintext 进行异或，得到密文 Ciphertext



注：

Counter i 为公式中的 Y_i ， E_K 为公式中 E(K,Y) ；

2.2 CTR 解密

2.2.1 加密算法描述

CTR 解密与加密相同，仅对明文密文对换即可。

$$Y_i = \mathrm{incr}_{32}(Y_i - 1), \qquad i = 1, \ldots, n$$
$$P_i = C_i \oplus E(K, Y_i), \qquad i = 1, \ldots, n-1$$
$$P_n = C_n \oplus \mathrm{MSB}_u\big(E(K, Y_n)\big)$$

注：

其中 E(K,Y)表示用密钥 K 对 Y 做 AES 加密

$\mathrm{Incr}_{32}()$是将数据的最低 32 位看成一个无符号数，将其加 1 后取模 2^{32}，即 $\mathrm{incr}(F||I)=F||(I+1)\mathrm{mod}2^{32}$

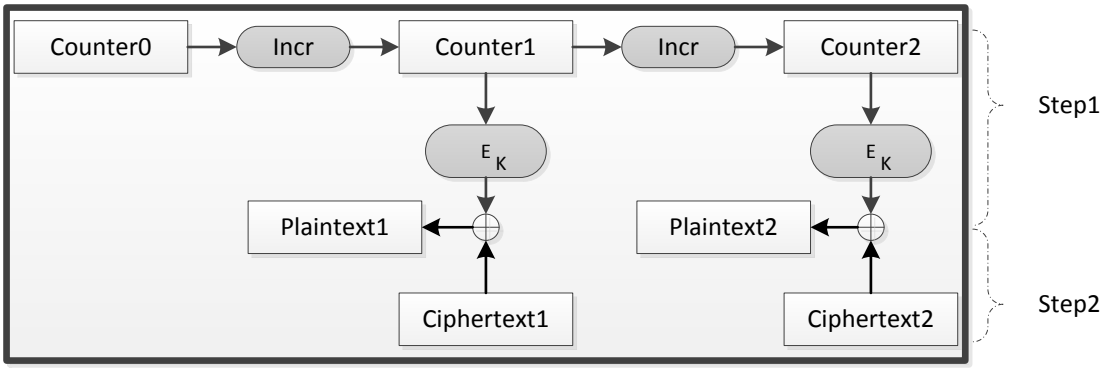
$\mathrm{MSB}_t(S)$返回数据 S 的最左边 t bits 数据

⊕表示异或运算

2.2.2 流程框图

Step1：对 Counter 进行 AES 加密，K 为密钥

Step2：step1 结果与密文 Ciphertext 进行异或，得到明文 plaintext



注：

Counter i 为公式中的 Y_i ， E_K 为公式中 E(K,Y) ；

2.3 算法实现

2.3.1 集成模块

HT6X2X 和 HT501X 系列芯片，内部集成了 **AES 加密/解密模块**；可以实现流程框图中 E_K 部分功能；

2.3.2 CTR 库函数

1. CTR 加密/解密函数

CTR 加密解密共用一个函数，输入变量为明文为加密，输入变量为密文则为解密；

函数声明：

void CTR_Encrypt(CTR_Encrypt_InputTypedef* CTR_InputStruct,
CTR_Encrypt_OutputTypedef* CTR_OutputStruct)；

入口参数:

CTR _InputStruct CTR 加解密输入变量结构体指针，主要包含 8 个参数:

1) AESKeyMode ：加密解密模式选择
2) *pKeyAddr ：密钥地址指针
3) * pInttextAddr ：待加解密数据地址指针
4) LenInttext ：待加解密数据长度（byte）
5) *Counter0 : Counter0 地址指针

CTR _OutputStruct CTR 加解密输出变量结构体指针，主要包含 3 个参数:

1) *pOuttextAddr ：已加解密数据地址指针
2) LenOuttext ：已加解密数据长度（byte）

返回参数: 无

特殊说明: 加密操作时，pInttextAddr 和 LenInttext 为明文输入，pOuttextAddr 为密文输出
解密操作时，pInttextAddr 和 LenInttext 为密文输入，pOuttextAddr 为明文输出

2.4 TEST CASE

Variable	Value
K	feffe9928665731c6d6a8f9467308308
	feffe9928665731c6d6a8f9467308308
P	d9313225f88406e5a55909c5aff5269a
	86a7a9531534f7da2e4c303d8a318a72
	1c3c0c95956809532fcf0e2449a6b525
	b16aedf5aa0de657ba637b39
Y_0	0cd953e2140a5976079f8e2406bc8eb4
Y_1	0cd953e2140a5976079f8e2406bc8eb5
$E(K, Y_1)$	83bcdd0af41a551452047196ca6b0cba
Y_2	0cd953e2140a5976079f8e2406bc8eb6
$E(K, Y_2)$	68151b79baea93c38e149b72e545e186
Y_3	0cd953e2140a5976079f8e2406bc8eb7
$E(K, Y_3)$	13fccf22159a4d16026ce5d58c7e99fb
Y_4	0cd953e2140a5976079f8e2406bc8eb8
$E(K, Y_4)$	132b64628a031e79fecd050675a64f07
C	5a8def2f0c9e53f1f75d7853659e2a20
	eeb2b22aafde6419a058ab4f6f746bf4
	0fc0c3b780f244452da3ebf1c5d82cde
	a2418997200ef82e44ae7e3f

3 CBC 加密实现

3.1 CBC 加密

3.1.1 输入参数

密钥 K：128，192，256 bits 三种模式

初始向量 IV： 1~128 bits

明文 P： 按 128bits 分组，总长度（n-1）* 128 + u，1 ≤ u ≤ 128。即明文由一系列的 n 数据组成，最后一组数据长度为 u，其他长度均为 128 位，记这些明文块为 $P_1,P_2,P_3...P_{n-1},P_n$;

3.1.2 输出参数

密文 C：长度与明文一致，数据分组同明文，记为 $C_1,C_2,C_3...C_{n-1},C_n$

3.1.3 加密算法描述

$$
\begin{aligned}
C_i &= E(K,(P_1 \oplus IV)), && i = 1\\
C_i &= E(K,(P_i \oplus C_{i-1})), && i = 2,\dots,n-1\\
C_n &= E(K,(P_n||0^{128-u} \oplus Y_n)), && i = n
\end{aligned}
$$

注：

其中 E(K,Y)表示用密钥 K 对 Y 做 AES 加密

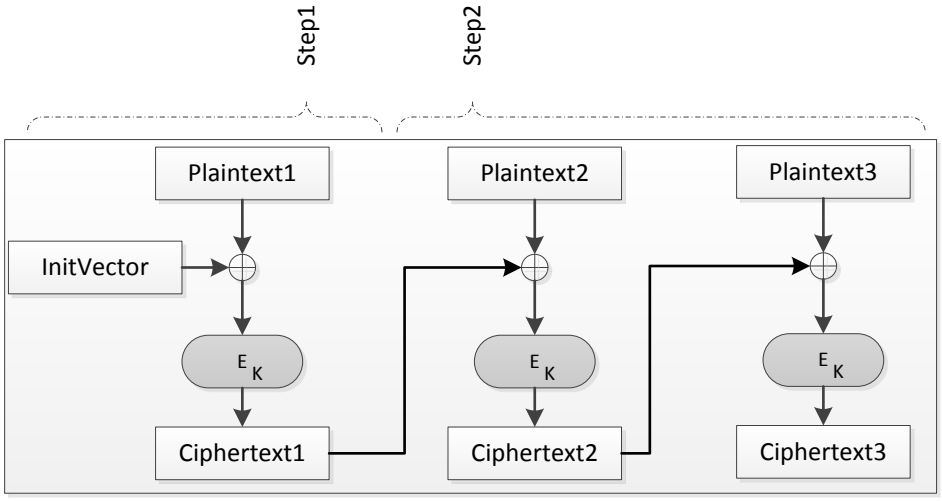
||表示串连接，0^U 表示 U bits 长度的 0;

⊕表示异或运算

3.1.4 流程框图

Step1：IV 与 P1 进行异或，对结果进行 AES 加密，加密结果存于 C1, K 为密钥

Step2：Ci-1 与 Pi 进行异或，对结果进行 AES 加密，加密结果存于 Ci, K 为密钥



注：

E_K 为公式中 E(K,Y) ；

3.2 CBC 解密

3.2.1 加密算法描述

$$P_i = E'(K, C_1) \oplus IV, \qquad i = 1$$
$$P_i = E'(K, C_i) \oplus C_{i-1}, \qquad i = 2, \ldots, n$$

注：

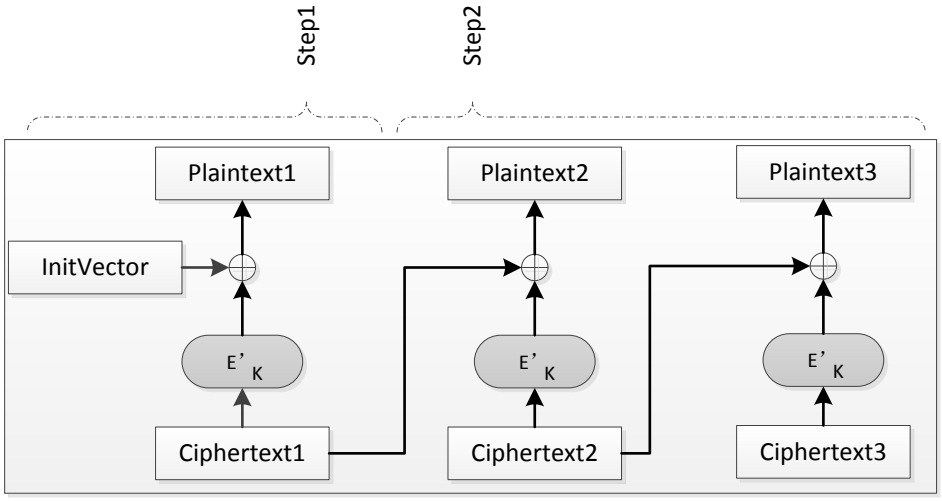
其中 E'(K,Y)表示用密钥 K 对 Y 做 AES 解密

⊕表示异或运算

3.2.2 流程框图

Step1：对 C1 进行 AES 解密，结果与 IV 进行异或，异或结果存于 P1, K 为密钥

Step2：对 Ci 进行 AES 解密，结果与 Ci-1 进行异或，异或结果存于 Pi, K 为密钥



注：

E'_K 为公式中 E'(K,Y) ；

3.3 算法实现

3.3.1 集成模块

HT6X2X 和 HT501X 系列芯片，内部集成了 **AES 加密/解密模块**；可以实现流程框图中 E_K 和 E'_K 部分功能；

3.3.2 CBC 库函数

1. CBC 加密函数

函数声明：

void CBC_Encrypt(CBC_Encrypt_InputTypedef* CBC_InputStruct,
CBC_Encrypt_OutputTypedef* CBC_OutputStruct)；

入口参数:

CBC _InputStruct　CBC 加密输入变量结构体指针，主要包含 5 个参数:

1) AESKeyMode　：加密解密模式选择
2) *pKeyAddr　：密钥地址指针
3) *pInitVectorAddr　：初始向量地址指针
4) *pPtextAddr　：明文数据地址指针
5) LenPtext　：明文数据长度（byte）

CBC _OutputStruct　CBC 加密输出变量结构体指针，主要包含 2 个参数:

1) *pCtextAddr　：已加密数据密文地址指针
2) LenCtext　：已加密数据密文长度（byte）

返回参数: 无

2. CBC 解密函数

函数声明:

Bool CBC_Decrypt(CBC_Decrypt_InputTypedef* CBC_InputStruct,
CBC_Decrypt_OutputTypedef* CBC_OutputStruct);

入口参数:

CBC _InputStruct CBC 解密输入变量结构体指针，主要包含 2 个参数:
1) AESKeyMode : 加密解密模式选择
2) *pKeyAddr : 密钥地址指针
3) *pInitVectorAddr : 初始向量地址指针
4) *pCtextAddr : 数据密文地址指针
5) LenCtext : 数据密文长度（byte?

CBC _OutputStruct CBC 解密输出变量结构体指针，主要包含 2 个参数:
1) *pPtextAddr : 明文数据地址指针
2) LenPtext : 明文数据长度（byte）

返回参数:

Bool = TRUE(1)： 解密成功
= FALSE(0)： 解密失败，密文格式有误

3.4 TEST CASE

Variable	Value
K	feffe9928665731c6d6a8f9467308308
	feffe9928665731c6d6a8f9467308308
P	d9313225f88406e5a55909c5aff5269a
	86a7a9531534f7da2e4c303d8a318a72
	1c3c0c95956809532fcf0e2449a6b525
	b16aedf5aa0de657ba637b39
IV	83bcdd0af41a551452047196ca6b0cba
C	ad2719767021b1e8fa5a5a9a5a65a94a
	e993963e1c5b89e21e8cd941da11f2d6
	97de1dcc403687f1a4c36163f1c09259
	5e4dbbbb41b82d00eb48088187947171

4 ECB 加密实现

4.1 ECB 加密

4.1.1 输入参数

密钥 K：128，192，256 bits 三种模式

明文 P： 按 128bits 分组，总长度（n-1）* 128 + u，$1 \le u \le 128$。即明文由一系列的 n 数据组成，最后一组数据长度为 u，其他长度均为 128 位，记这些明文块为 $P_1,P_2,P_3...P_{n-1},P_n$;

4.1.2 输出参数

密文 C：长度与明文一致，数据分组同明文，记为 $C_1,C_2,C_3...C_{n-1},C_n$

4.1.3 加密算法描述

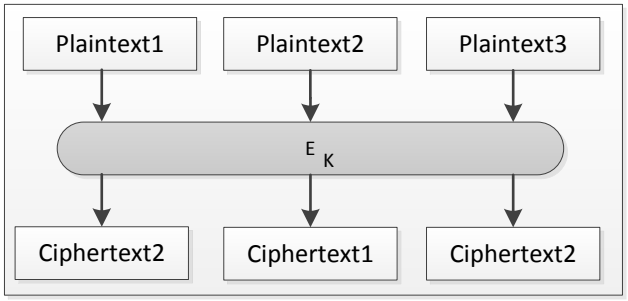
$$C_i = E(K, P_i), \qquad i = 1, \dots, n-1$$
$$C_n = \left(E(K, P_n || 0^{128-U})\right)$$

注：

其中||表示串连接，0^U 表示 U bits 长度的 0;

E(K,Y)表示用密钥 K 对 Y 做 AES 加密

4.1.4 流程框图



注：

E_K 为公式中 E(K,Y) ；

4.2 ECB 解密

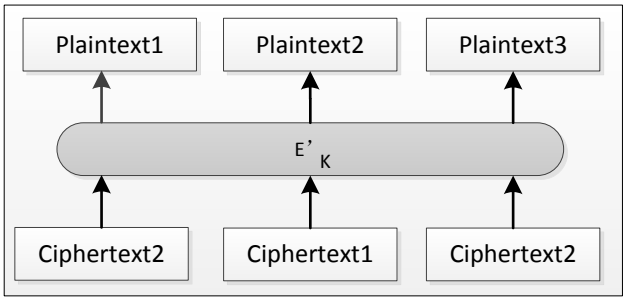
4.2.1 加密算法描述

$$P_i = E'(K, C_i), \qquad i = 1, \ldots, n$$

注：

E’(K,Y)表示用密钥 K 对 Y 做 AES 解密

4.2.2 流程框图



注：

E'_K 为公式中 E’(K,Y) ；

4.3 算法实现

4.3.1 集成模块

HT6X2X 和 HT501X 系列芯片，内部集成了 **AES 加密/解密模块**；可以实现流程框图中 E_K 和 E'_K 部分功能；

4.3.2 ECB 库函数

1. ECB 加密函数

函数声明：

```
void ECB_Encrypt(ECB_Encrypt_InputTypedef* ECB_InputStruct,
                 ECB_Encrypt_OutputTypedef* ECB_OutputStruct);
```

入口参数:

ECB _InputStruct　　ECB 加密输入变量结构体指针，主要包含 4 个参数:

1) AESKeyMode　　：加密解密模式选择

2) *pKeyAddr　　：密钥地址指针

3) *pPtextAddr　　：明文数据地址指针

4) LenPtext　　：明文数据长度（byte）

ECB _OutputStruct　　ECB 加密输出变量结构体指针，主要包含 2 个参数:

1) *pCtextAddr　　：已加密数据密文地址指针

2) LenCtext　　：已加密数据密文长度（byte）

返回参数: 无

2. ECB 解密函数

函数声明:

Bool ECB_Decrypt(ECB_Decrypt_InputTypedef* ECB_InputStruct,
ECB_Decrypt_OutputTypedef* ECB_OutputStruct)；

入口参数:

ECB _InputStruct　　ECB 解密输入变量结构体指针，主要包含 4 个参数:

1) AESKeyMode　　：加密解密模式选择

2) *pKeyAddr　　：密钥地址指针

3) *pCtextAddr　　：数据密文地址指针

4) LenCtext　　：数据密文长度（byte?

ECB _OutputStruct　　ECB 解密输出变量结构体指针，主要包含 2 个参数:

1) *pPtextAddr　　：明文数据地址指针

2) LenPtext　　：明文数据长度（byte）

返回参数:

Bool　　= TRUE(1)：　解密成功

= FALSE(0)：　解密失败，密文格式有误

4.4 TEST CASE

Variable	Value
Y_0	0cd953e2140a5976079f8e2406bc8eb4
Y_1	0cd953e2140a5976079f8e2406bc8eb5
Y_2	0cd953e2140a5976079f8e2406bc8eb6
Y_3	0cd953e2140a5976079f8e2406bc8eb7
$E(K, Y_0)$	71b54d092bb0c3d9ba94538d4096e691

$E(K, Y_1)$	83bcdd0af41a551452047196ca6b0cba
$E(K, Y_2)$	68151b79baea93c38e149b72e545e186
$E(K, Y_3)$	13fccf22159a4d16026ce5d58c7e99fb