otp提供的总bit数，512bit, otp\_key[511:0]

otp valid信号，使用和troot相同的id\_vld信号。

1.支持的加密算法：

AES: O\_sk\_calg[2:0] = 3’b010;

2.支持的加密模式：

ECB: O\_sk\_cmode[3:0] = 4’b0000;

CBC: O\_sk\_cmode[3:0] = 4’b0001;

CTR: O\_sk\_cmode[3:0] = 4’b0010;

CCM: O\_sk\_cmode[3:0] = 4’b0011;

GCM: O\_sk\_cmode[3:0] = 4’b0101;

OFB: O\_sk\_cmode[3:0] = 4’b0111;

CFB: O\_sk\_cmode[3:0] = 4’b1000;

F8: O\_sk\_cmode[3:0] = 4’b1001;

3.支持的key size：

128bit (16byte): O\_sk\_ckey\_sz[1:0] = 2’b00;

196bit (24byte): O\_sk\_ckey\_sz[1:0] = 2’b01;

256bit (32byte): O\_sk\_ckey\_sz[1:0] = 2’b10;

4. 是否支持redundancy：

使用secure 寄存器控制。

5. 字大小端模式word\_endian

使用secure寄存器控制，

byte\_endian默认为1，每个字内部各byte为小端；byte\_endian为0，每个字内部各byte为大端

word\_endian默认为0，各字为大端；word\_endian为1，各字为小端。

如果otp输出Key为128’h12345678\_9abcdef0\_13579bdf\_2468ace0(MSB~LSB)

1. Default，word\_endian==0，byte\_endian==1

addr data

0 12345678

1 9abcdef0

2 13579bdf

3 2468ace0

实际使用的key为128’h12345678\_9abcdef0\_13579bdf\_2468ace0

1. word\_endian==1，byte\_endian==1

addr data

0 2468ace0

1 13579bdf

2 9abcdef0

3 12345678

实际使用的key为128’h2468ace0\_13579bdf\_9abcdef0\_12345678

1. word\_endian==0，byte\_endian==0

addr data

0 78563412

1 f0debc9a

2 df9b5713

3 e0ac6824

实际使用的key为128’h78563412\_f0debc9a\_df9b5713\_e0ac6824

1. word\_endian==1，byte\_endian==0

addr data

0 e0ac6824

1 df9b5713

2 f0debc9a

3 78563412

实际使用的key为128’he0ac6824\_df9b5713\_f0debc9a\_78563412

6. 只支持secure模式：

O\_sk\_secure必须为1。

7.不同key size和redundancy情况下，支持的key的映射，O\_sk\_ctx\_idx为key的索引号。即no redundancy时最大支持四个128bit的root key。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | O\_sk\_ctx\_idx | | | |
| Redundancy | Key Size | 0 | 1 | 2 | 3 |
| 0 | 128 | otp\_key[127:0] | otp\_key[255:128] | otp\_key[383:256] | otp\_key[511:384] |
| 192 | otp\_key[191:0] | otp\_key[447:256] | N/A | N/A |
| 256 | otp\_key[255:0] | otp\_key[511:256] | N/A | N/A |
| 1 | 128 | otp\_key[127:0] | otp\_key[255:128] | otp\_key[383:256] | otp\_key[511:384] | N/A | N/A |
| 192 | otp\_key[191:0] | otp\_key[447:256] | N/A | N/A | N/A |
| 256 | otp\_key[255:0] | otp\_key[511:256] | N/A | N/A | N/A |