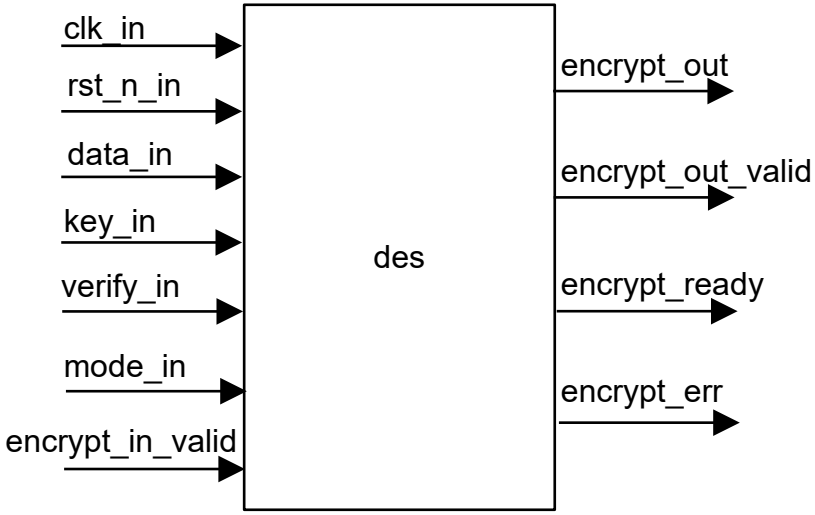
des: data encryption standard



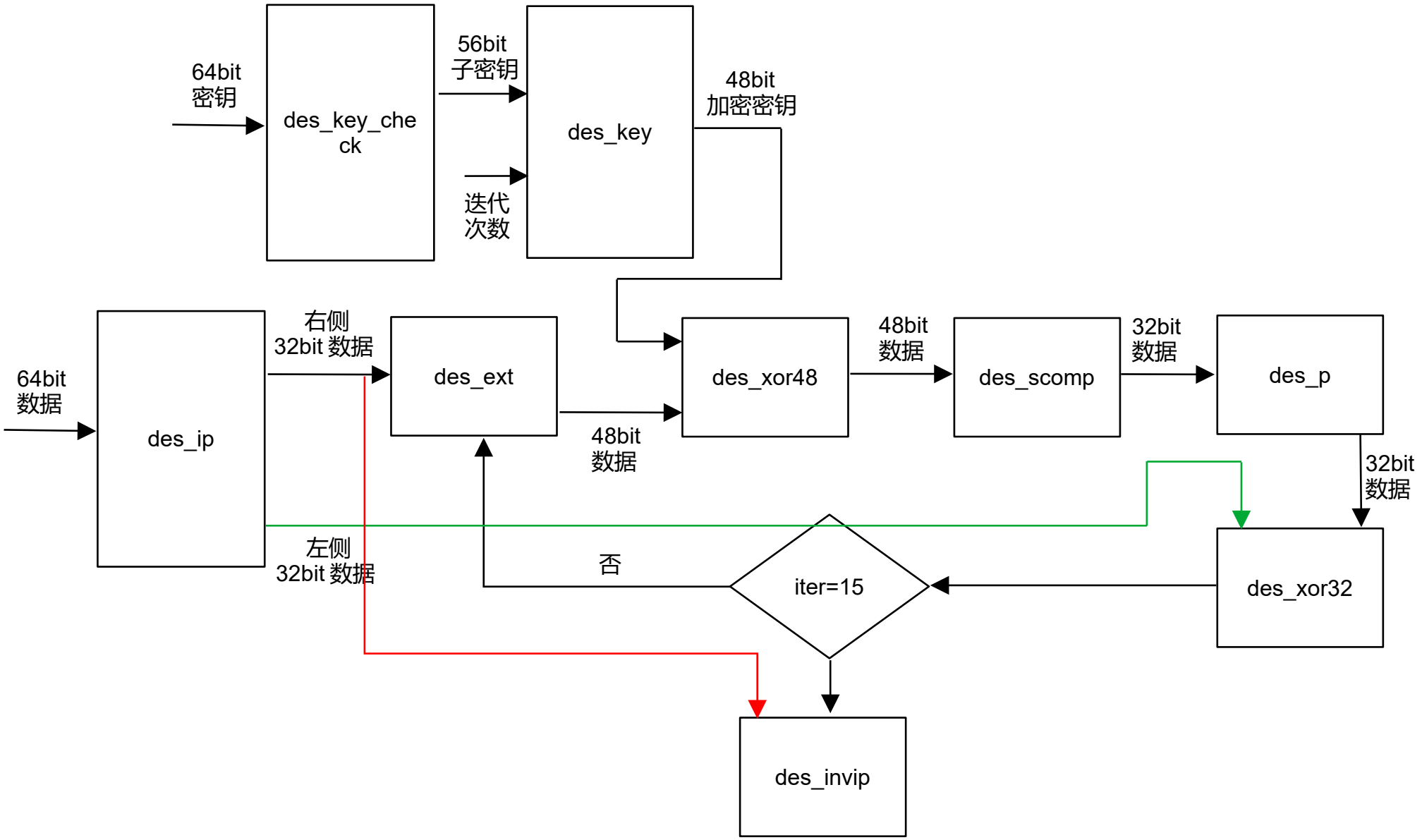
输入信号列表

信号	位宽	说明
clk_in	1 bit	时钟信号
rst_n_in	1 bit	复位信号，低有效
data_in	64 bit	输入数据
key_in	64 bit	输入密钥
mode_in	1 bit	模式选择 0: 加密 1: 解密
verify_in	1 bit	是否对 key 校验 0: 不校验 1： 校验
encrypt_in_valid	1 bit	输入有效信号

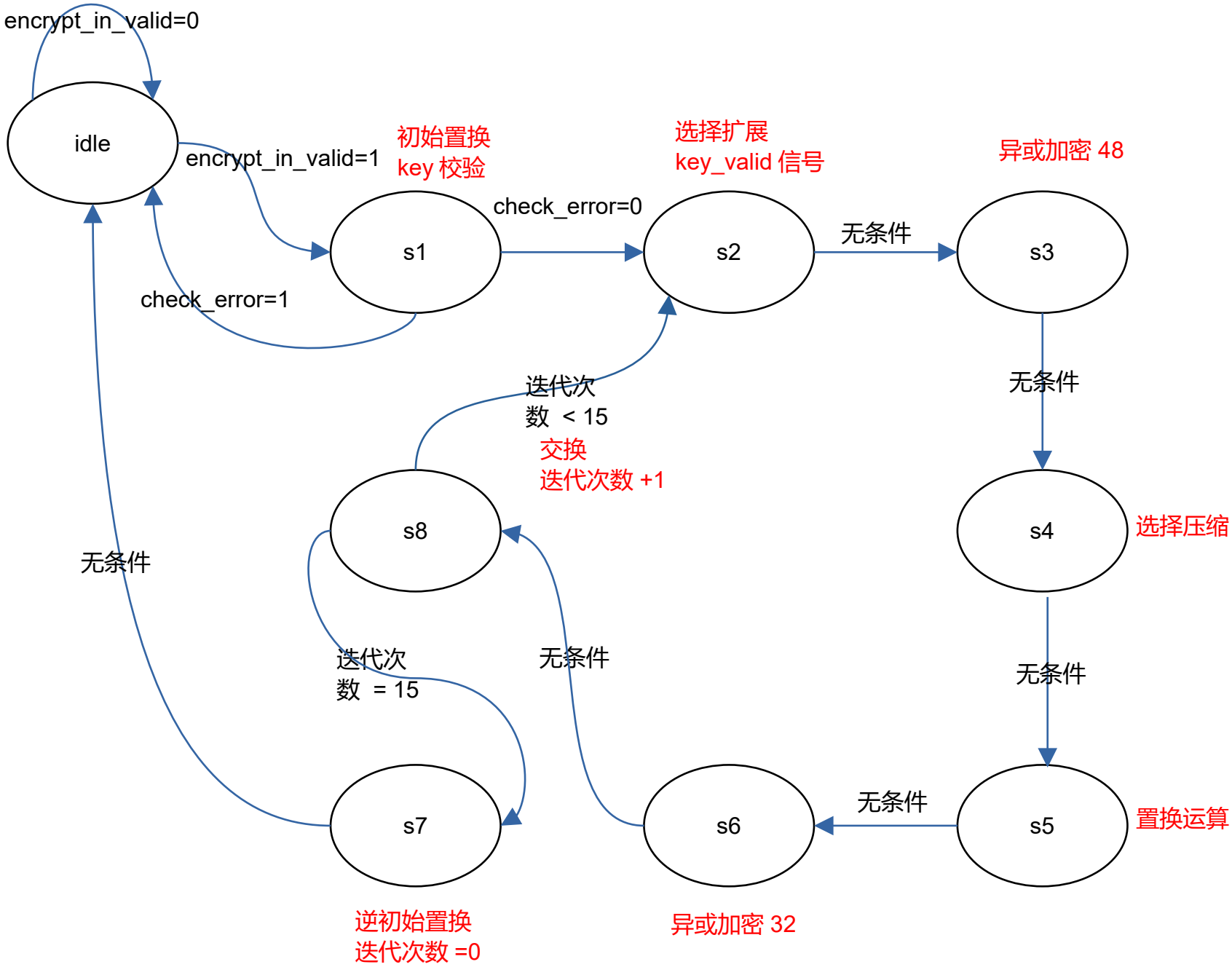
输出信号列表

信号	位宽	说明
encrypt_out	64 bit	mode=0 加密输出 mode=1 解密输出
encrypt_out_valid	1 bit	输出有效信号
encrypt_ready	1 bit	ready 信号
encrypt_err	1 bit	错误信号，密钥校验错误

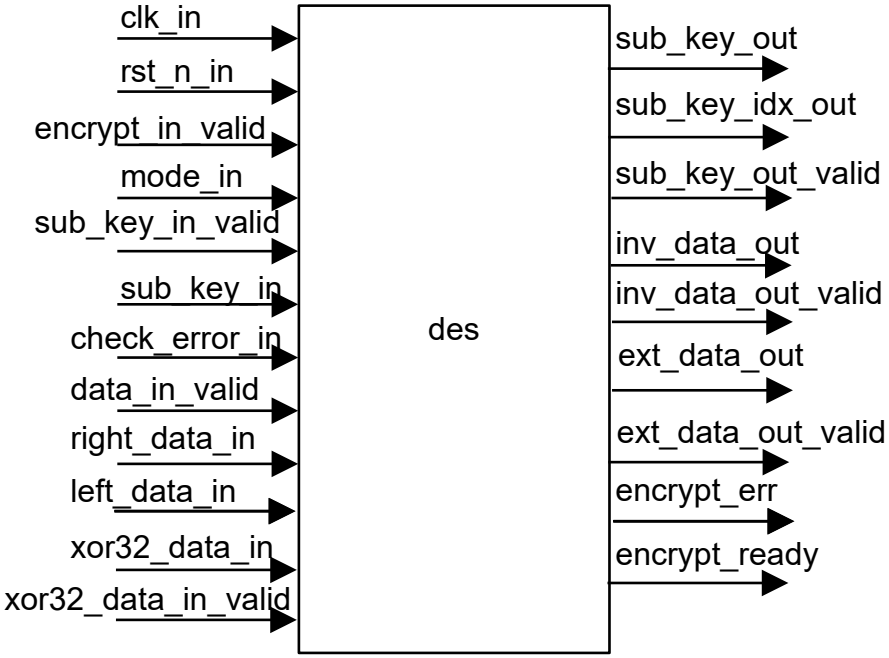
des 加密算法框图


64bit
密钥
des_key_che
ck
56bit
子密钥
迭代
次数
des_key
48bit
加密密钥
64bit
数据
des_ip
右侧
32bit 数据
左侧
32bit 数据
des_ext
48bit
数据
des_xor48
48bit
数据
des_scomp
32bit
数据
des_p
32bit
数据
否
iter=15
des_xor32
des_invip

des 状态机


encrypt_in_valid=0
idle
encrypt_in_valid=1
初始置换
key 校验
s1
check_error=1
check_error=0
选择扩展
key_valid 信号
s2
无条件
异或加密 48
s3
无条件
选择压缩
s4
无条件
置换运算
s5
无条件
异或加密 32
s6
无条件
逆初始置换
迭代次数 =0
s7
迭代次
数 = 15
无条件
s8
迭代次
数 < 15
交换
迭代次数 +1
无条件

控制模块 des_ctrl



输入信号列表

信号	位宽	说明
clk_in	1 bit	时钟信号
rst_n_in	1 bit	复位信号，低有效
encrypt_in_valid	1 bit	输入有效信号
mode_in	1 bit	模式选择 0: 加密 1: 解密
sub_key_in_valid	1 bit	子密钥有效信号
sub_key_in	56 bit	子密钥
check_error_in	1 bit	密钥校验错误
data_in_valid	1 bit	数据有效信号
right_data_in	32 bit	右侧数据
left_data_in	32 bit	左侧数据
xor32_data_in	32 bit	xor32 后的数据
xor32_data_in_valid	1 bit	xor32 后的数据有效信号

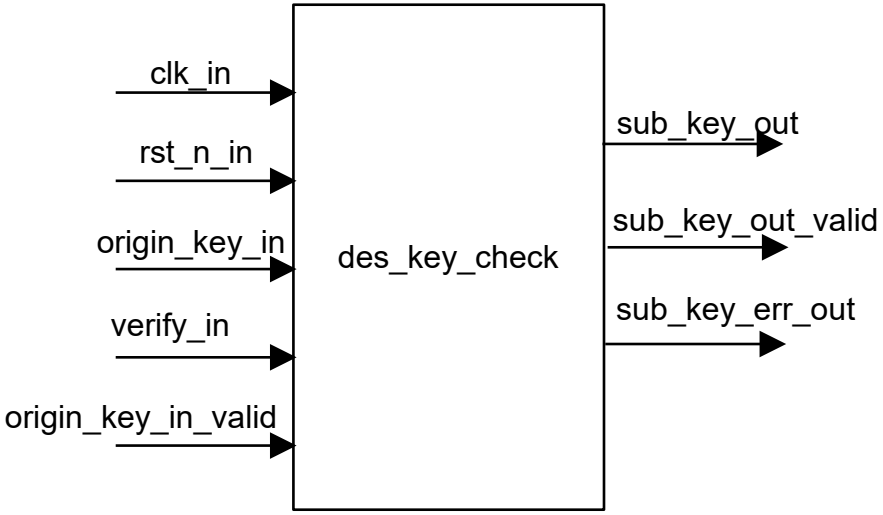
输出信号列表 -1

信号	位宽	说明
sub_key_out	56 bit	用于产生加密密钥的子密钥
sub_key_idx_out	4 bit	子密钥索引
sub_key_out_valid	1 bit	子密钥有效信号
inv_data_out	64 bit	逆置换的输入数据
inv_data_out_valid	1 bit	逆置换的输入数据有效信号
encrypt_err	1 bit	错误信号，密钥校验错误
encrypt_ready	1 bit	ready 信号
ext_data_out	32 bit	选择扩展的输入数据
ext_data_out_valid	1 bit	选择扩展的输入数据有效信号

输出信号列表 -2

信号	位宽	说明
xor32_left_data_out	32 bit	用于异或加密的左侧数据
xor32_left_data_out_valid	1 bit	数据有效信号

密钥校验和初始置换模块 des_key_check



输入信号列表

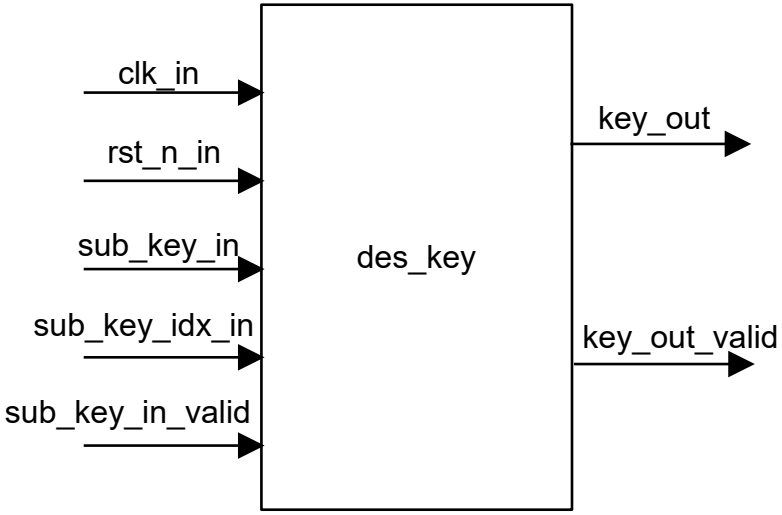
信号	位宽	说明
clk_in	1 bit	时钟信号
rst_n_in	1 bit	复位信号，低有效
origin_key_in	64 bit	输入密钥
verify_in	1 bit	是否进行密钥校验，奇校验
origin_key_in_valid	1 bit	输入密钥有效信号

输出信号列表

信号	位宽	说明
sub_key_out	56 bit	输出子密钥
sub_key_out_valid	1 bit	输出子密钥有效信号
sub_key_err_out	1 bit	密钥校验错误信号

des_key_check 模块产生的 sub_key 会送入 des_key 模块，产生用于加密的密钥序列

密钥产生模块 des_key



输入信号列表

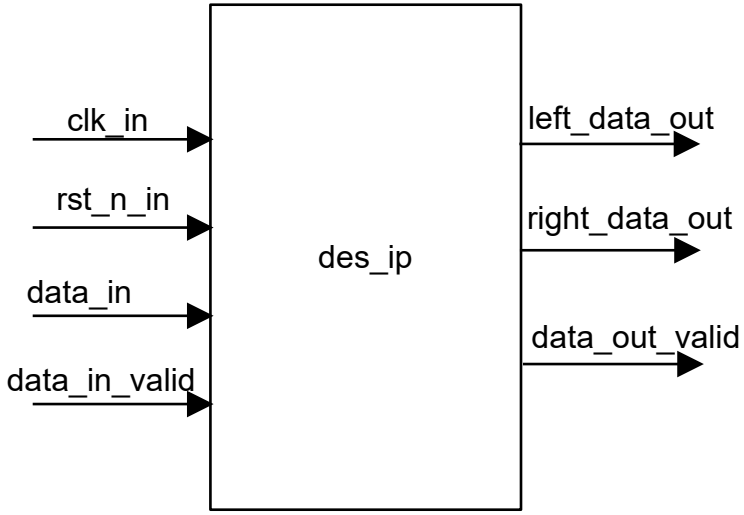
信号	位宽	说明
clk_in	1 bit	时钟信号
rst_n_in	1 bit	复位信号，低有效
sub_key_in	56 bit	输入密钥
sub_key_idx_in	4 bit	0-15 共 16 种密钥的索引
sub_key_in_valid	1 bit	输入密钥有效信号

输出信号列表

信号	位宽	说明
key_out	48 bit	输出密钥
key_out_valid	1 bit	输出密钥有效信号

1. 可以推导得出 key_out 与原始密钥的关系 (目前使用：推导得到的 key_out 与原始密钥进行置换后的 56bit 子密钥的关系)
2. 因此，理论上是可以将 des_key_check 和 des_key 模块进行合并的，但是考虑到对原始密钥进行奇校验因此将两部分拆开了

初始置换模块 des_ip



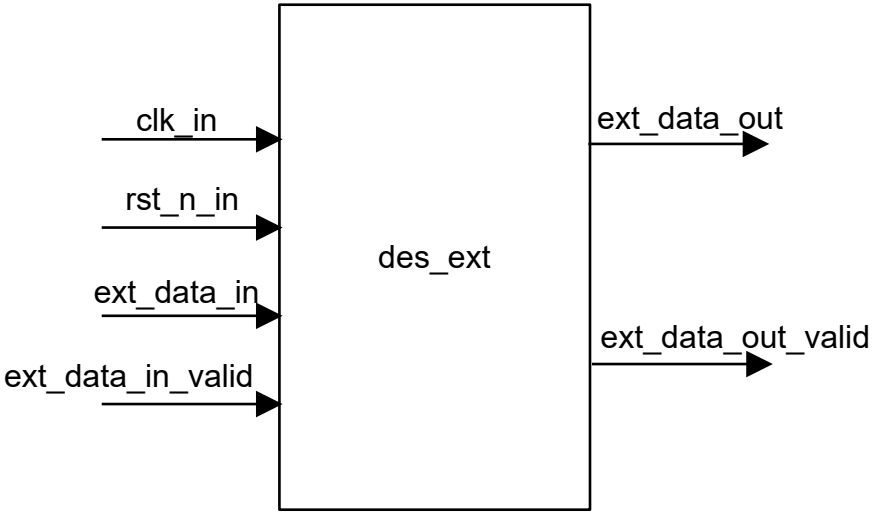
输入信号列表

信号	位宽	说明
clk_in	1 bit	时钟信号
rst_n_in	1 bit	复位信号，低有效
data_in	64 bit	输入数据
data_in_valid	1 bit	输入数据有效信号

输出信号列表

信号	位宽	说明
left_data_out	32 bit	des 初始置换后左边 32bit 数据
right_data_out	32 bit	des 初始置换后右边 32bit 数据
data_out_valid	1 bit	输出数据有效信号

选择扩展模块 des_ext



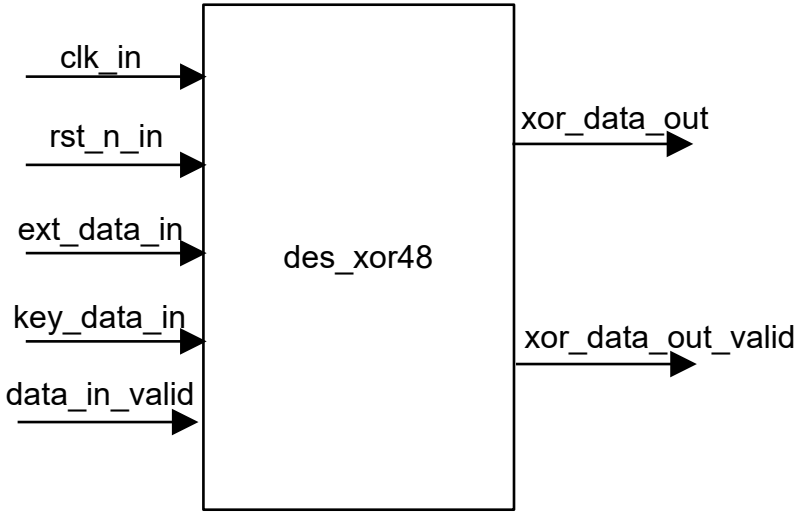
输入信号列表

信号	位宽	说明
clk_in	1 bit	时钟信号
rst_n_in	1 bit	复位信号，低有效
ext_data_in	32 bit	选择扩展的输入数据
ext_data_in_valid	1 bit	输入数据有效信号

输出信号列表

信号	位宽	说明
ext_data_out	48 bit	选择扩展后的输出数据
ext_data_out_valid	1 bit	输出数据有效信号

异或加密模块 des_xor48



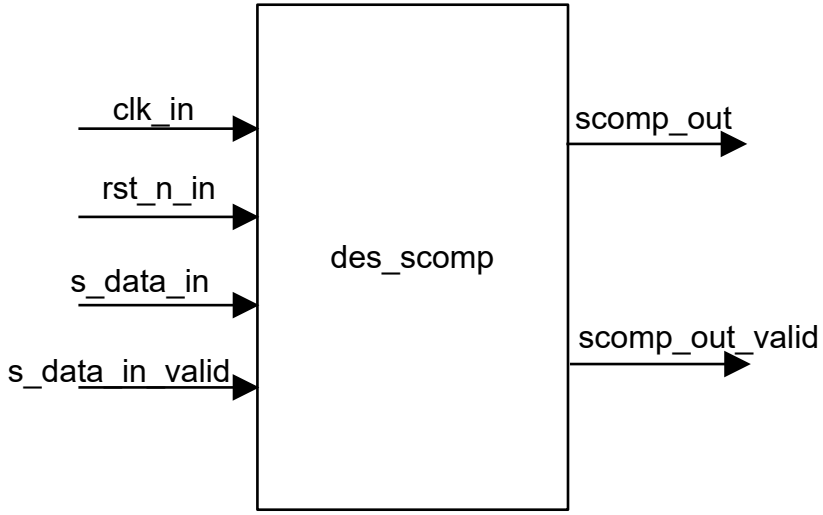
输入信号列表

信号	位宽	说明
clk_in	1 bit	时钟信号
rst_n_in	1 bit	复位信号，低有效
ext_data_in	48 bit	选择扩展后的输入数据
key_data_in	48 bit	子密钥输入数据
data_in_valid	1 bit	输入数据有效信号

输出信号列表

信号	位宽	说明
xor_data_out	48 bit	异或加密后的输出数据
xor_data_out_valid	1 bit	输出数据有效信号

选择压缩运算 S 模块 des_scomp



输入信号列表

信号	位宽	说明
clk_in	1 bit	时钟信号
rst_n_in	1 bit	复位信号，低有效
s_data_in	48 bit	S 压缩输入数据
s_data_in_valid	1 bit	输入数据有效信号

输出信号列表

信号	位宽	说明
scomp_out	32 bit	压缩后的输出数据
scomp_out_valid	1 bit	输出数据有效信号

首尾 2bit 看成是 S 盒中的行信号，其余的 4bit 用来确定列号

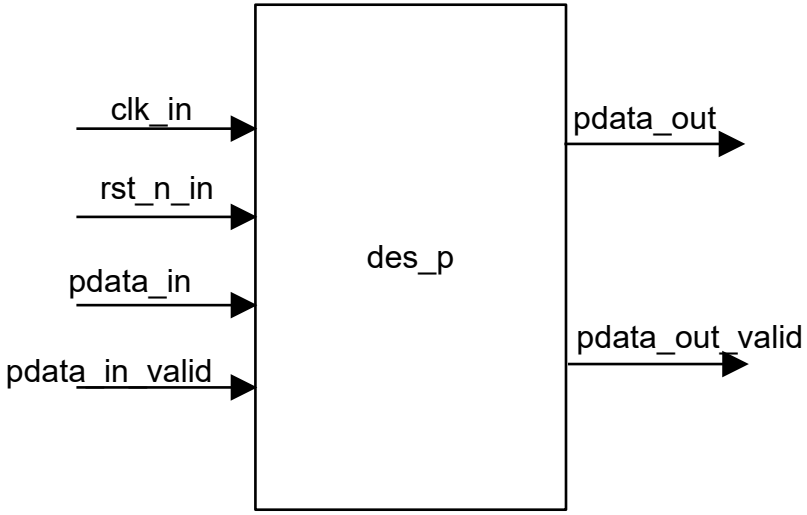
直接进行打表操作

X5 x4 x3 x2 x1 x0

x0 x5 x1 x2 x3 x4

结果赋给 o0 o1 o2 o3

置换运算 P 模块 des_p



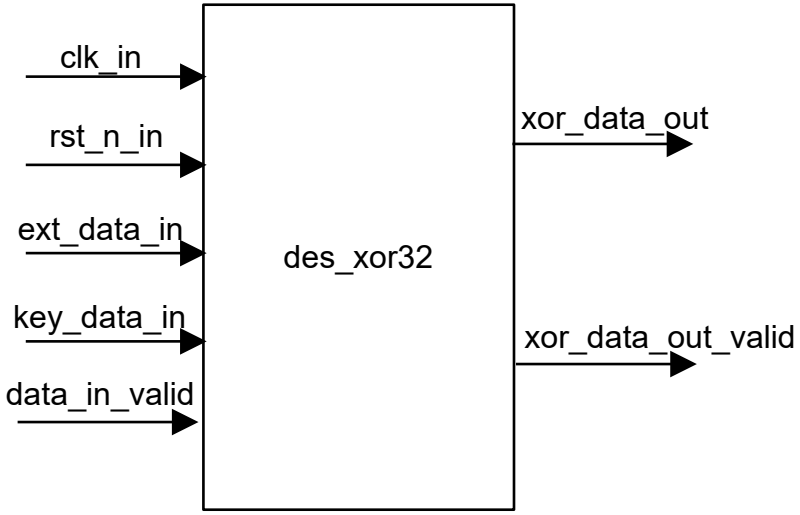
输入信号列表

信号	位宽	说明
clk_in	1 bit	时钟信号
rst_n_in	1 bit	复位信号，低有效
pdata_in	32 bit	置换运算输入数据
pdata_in_valid	1 bit	输入数据有效信号

输出信号列表

信号	位宽	说明
pdata_out	32 bit	置换运算输出数据
pdata_out_valid	1 bit	输出数据有效信号

异或加密模块 des_xor32



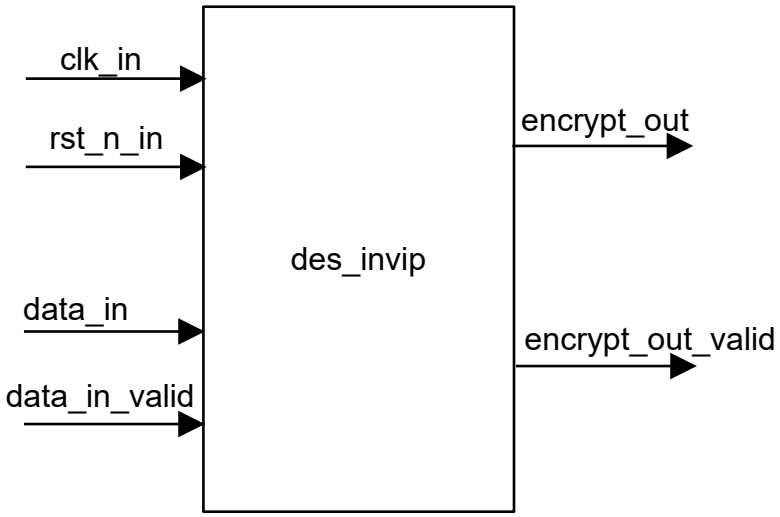
输入信号列表

信号	位宽	说明
clk_in	1 bit	时钟信号
rst_n_in	1 bit	复位信号，低有效
ext_data_in	32 bit	选择扩展后的输入数据
key_data_in	48 bit	子密钥输入数据
data_in_valid	1 bit	输入数据有效信号

输出信号列表

信号	位宽	说明
xor_data_out	32 bit	异或加密后的输出数据
xor_data_out_valid	1 bit	输出数据有效信号

逆初始置换模块 des_invip



输入信号列表

信号	位宽	说明
clk_in	1 bit	时钟信号
rst_n_in	1 bit	复位信号，低有效
data_in	64 bit	输入数据
data_in_valid	1 bit	输入数据有效信号

输出信号列表

信号	位宽	说明
encrypt_out	64 bit	加密输出数据
encrypt_out_valid	1 bit	输出数据有效信号