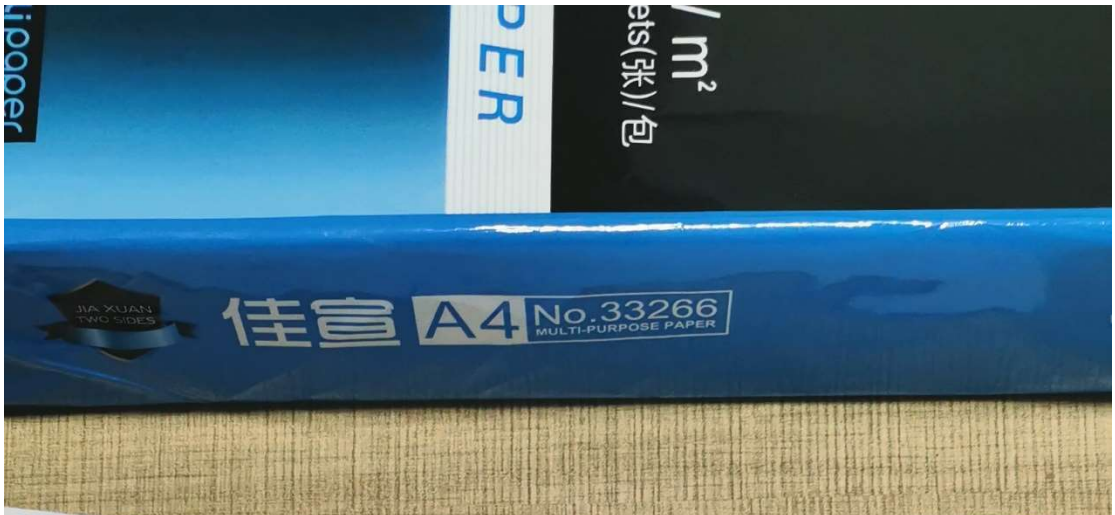

19012105 40 谢成沐.

SM4轮函数F:

$F(X_0, X_1, X_2, X_3, rk) = X_0 \oplus T(X_1 \oplus X_2 \oplus X_3 \oplus rk)$.

其中, (X_0, X_1, X_2, X_3) 为输入, rk 为轮密钥, T 为*S盒中T变换 及线性变换L

加密:

$X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i)$, $i = 0, 1, \cdots, 31$, X_i 为明文.

反序: $(Y_0, Y_1, Y_2, Y_3) = (X_{35}, X_{34}, X_{33}, X_{32})$, Y_i 为密文.

解密: $X_i = F(X_{i+4}, X_{i+3}, X_{i+2}, X_{i+1}, rk_i)$, Y_i 为密文.

反序: $(X_3, X_2, X_1, X_0) = (M_0, M_1, M_2, M_3)$, X_i 为明文.

密钥扩展:

密钥 $MK = (MK_0, MK_1, MK_2, MK_3)$.

中间数据: $(K_0, K_1, K_2, K_3) = (MK_0 \oplus FK_0, MK_1 \oplus FK_1, MK_2 \oplus FK_2, MK_3 \oplus FK_3)$

轮密钥 $rk_i = K_{i+4} = K_i \oplus T'(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i)$

其中"T'"与T变换基本一致, 只需将L变换改为 $L'(B) = B \oplus (B <<< 13) \oplus (B <<< 23)$

证明: 轮函数 $F_i = G_i E$

其中, $G_i(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) = (X_i \oplus T(X_{i+1}, X_{i+2}, X_{i+3}, rk_i), X_{i+1}, X_{i+2}, X_{i+3})$

$E(X_{i+4}, (X_{i+1}, X_{i+2}, X_{i+3})) = ((X_{i+1}, X_{i+2}, X_{i+3}), X_{i+4})$

$(G_i)^2 = G_i(X_i \oplus T(X_{i+1}, X_{i+2}, X_{i+3}, rk_i), X_{i+1}, X_{i+2}, X_{i+3}, rk_i)$

$= (X_i \oplus T(X_{i+1}, X_{i+2}, X_{i+3}, rk_i) \oplus T(X_{i+1}, X_{i+2}, X_{i+3}, rk_i), X_{i+1}, X_{i+2}, X_{i+3}, rk_i)$

$= (X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i)$

$= I$

$\Rightarrow G_i$ 为对合函数.

$E^2(X_{i+4}, (X_{i+1}, X_{i+2}, X_{i+3})) = I$

$\Rightarrow E$ 为对合函数

$\Rightarrow$ SM4对合

再由

SM4加密过程：

$$(X_i, X_{i+1}, X_{i+2}, X_{i+3}) \to (X_{i+1}, X_{i+2}, X_{i+3}, X_{i+4})$$

$$\vdots$$

若干轮后，反序

SM4解密过程：

$$(X_{i+3}, X_{i+2}, X_{i+1}, X_{i+0}) \to (X_{i+2}, X_{i+1}, X_i, X_{i-1})$$

$$\vdots$$

若干轮后反序

由于轮函数 F_i 对合，SM4过程对合。

$$F_i^{-1} = F_i \Rightarrow SM4^{-1}(SM4(X_0, X_1, X_2, X_3)) = (X_0, X_1, X_2, X_3)$$

$\Rightarrow$ SM4 可逆。