证明 SM4 可逆

1901210530 吴宏凯

结论：SM4 的加密是可逆的。

证明：

1、假设输入的明文为$(X0, X1, X2, X3)$,第 i 轮使用的轮密钥为 rki，轮函数 F，合成置换 T，则加密表达式为：

$$X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) = X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i)$$

其中 $i = 0\sim31$，T 是非线性变换 τ 和线性变换 L 的一个组合过程。

2、轮密钥 rki 的生成由用户输入的主密钥$MK = (MK0, MK1, MK2, MK3)$、系统参数$FK = (FK0, FK1, FK2, FK3)$和固定参数$CK = (CK0, CK1, \dots, CK31)$决定，每一轮生成对应的轮密钥 rki，但 rki 在 T 中只参与异或计算，生成密钥的操作是独立进行的，与加解密无关，与轮数有关。所以解密过程使用的轮密钥与加密过程相同。

3、在完成 32 轮变换后，最终得到密文$(X32, X33, X34, X35)$。

现假设解密设备的输入数据为密文:$(X32, X33, X34, X35)$，先对其做逆序处理，得到$(X35, X34, X33, X32)$，第一轮解密的公式推导：

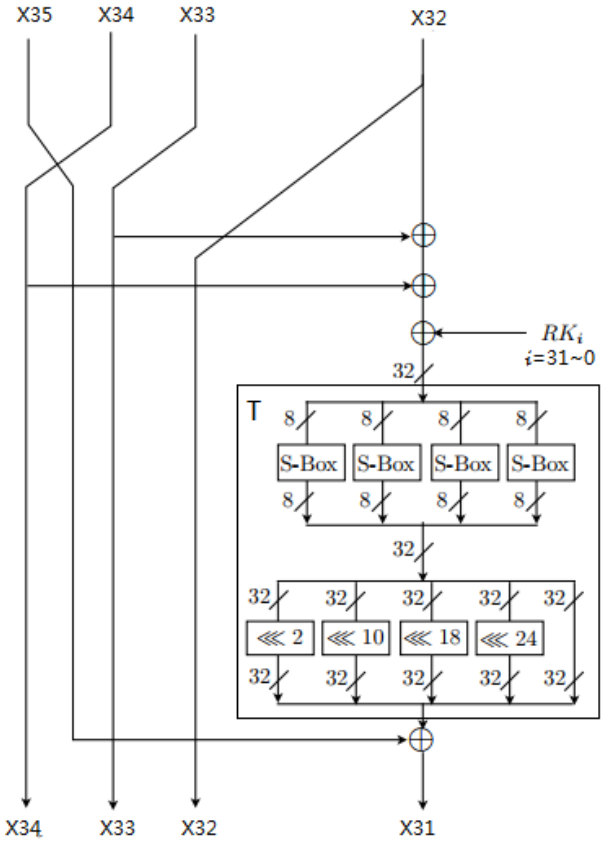
在加密过程中，$X_{35} = X_{31} \oplus T(X_{34} \oplus X_{33} \oplus X_{32} \oplus rk_{31})$，根据异或的自反性质：$A \oplus A = 0, B \oplus 0 = B$，等式两边同时再与$X_{35}$和$X_{31}$异或。得到：

$$X_{35} \oplus X_{35} \oplus X_{31} = X_{31} \oplus X_{31} \oplus X_{35} \oplus T(X_{34} \oplus X_{33} \oplus X_{32} \oplus rk_{31})$$

化简得：

$$X_{31} = X_{35} \oplus T(X_{34} \oplus X_{33} \oplus X_{32} \oplus rk_{31})。$$

根据公式得到第一轮解密的流程图：



其中 T 的处理与加密过程相同，即 SM4 的加密解密可以使用同一套加解密设备。
将第一轮解密操作继续推广，可得：
加密：$X_{34} = X_{30} \oplus T(X_{33} \oplus X_{32} \oplus X_{31} \oplus rk_{30})$，解密 $X_{30} = X_{34} \oplus T(X_{33} \oplus X_{32} \oplus X_{31} \oplus rk_{30})$。
以此类推，解密过程可以得到一般性结论：

$$X_i = X_{i+4} \oplus T(X_{i+3} \oplus X_{i+2} \oplus X_{i+1} \oplus rk_i)$$

其中$i = 31\sim0$，即轮密钥 rki 的使用顺序与加密过程相反。
经过 32 轮解密后，可得到明文：（X0,X1,X2,X3）.
综上，SM4 加密是可逆的。