1. 敌方向 MAC Oracle 提交一个查询$m$，其中$m=m_1,m_2,\cdots,m_l$，则可以得到相应的标签$(t_0,t_l)$，显然有$Vrfy_k(m,t_0,t_l)=1$。则初始化种子$t_0$，令$m^*=0^n,m_2,\cdots,m_l$且种子初始化为$t_0\oplus m_1$，即有$Vrfy_k(m^*,t_0\oplus m_1,t_l)=1$。根据 strong MAC 的定义可知，修改不安全。

2. 由 Feistel network 的计算方法可得，令初始串为$(L_0,R_0)$，则进行第一轮之后输出为$(R_0,L_0)$，第二轮的输出为$(L_0,R_0)$，依此类推可知，每一轮都是将左右半串进行位置交换，从而可知，当$r$为奇数的时候，第$r$轮的输出为$(R_0,L_0)$，当$r$为偶数的时候，则第$r$轮输出为$(L_0,R_0)$。

3. 由 Feistel network 的计算方法可得，令初始串为$(L_0,R_0)$，则进行第一轮之后输出为$(R_0,L_0\oplus R_0)$，第二轮的输出为$(L_0\oplus R_0,L_0)$，而第三轮之后的输出为$(L_0,R_0)$。依此类推可知，每 3 轮进行一次循环，从而可知，当$r$为 3 的倍数的时候，第$r$轮的输出为$(L_0,R_0)$。

4. 见源码

5. 假设向 MAC Oracle 提供一个查询$m$，其中$m=m_1,0^n,\cdots,0^n$，则可以得到相应的标签$(t_1,t_2,\cdots,t_l)$，显然$Vrfy_k(m,t_1,t_2,\cdots,t_l)=1$，其中$t_1^{'}=F_k(m_1)$，若令$m^*=0^n,0^n,\cdots,0^n$，则得到对应的标签$(t_1^{'},t_2^{'},\cdots,t_l^{'})$，显然$Vrfy_k(m^*,t_1^{'},t_2^{'},\cdots,t_l^{'})=1$，其中$t_1^{'}=F_k(0^n)$，若令$m^{**}=m_1,t_1,\cdots,t_l$，则显然$Vrfy_k(m^{**},t_1,t_1^{'},t_2^{'},\cdots,t_l^{'})=1$，根据 strong MAC 的定义可知，该修改方案不安全。