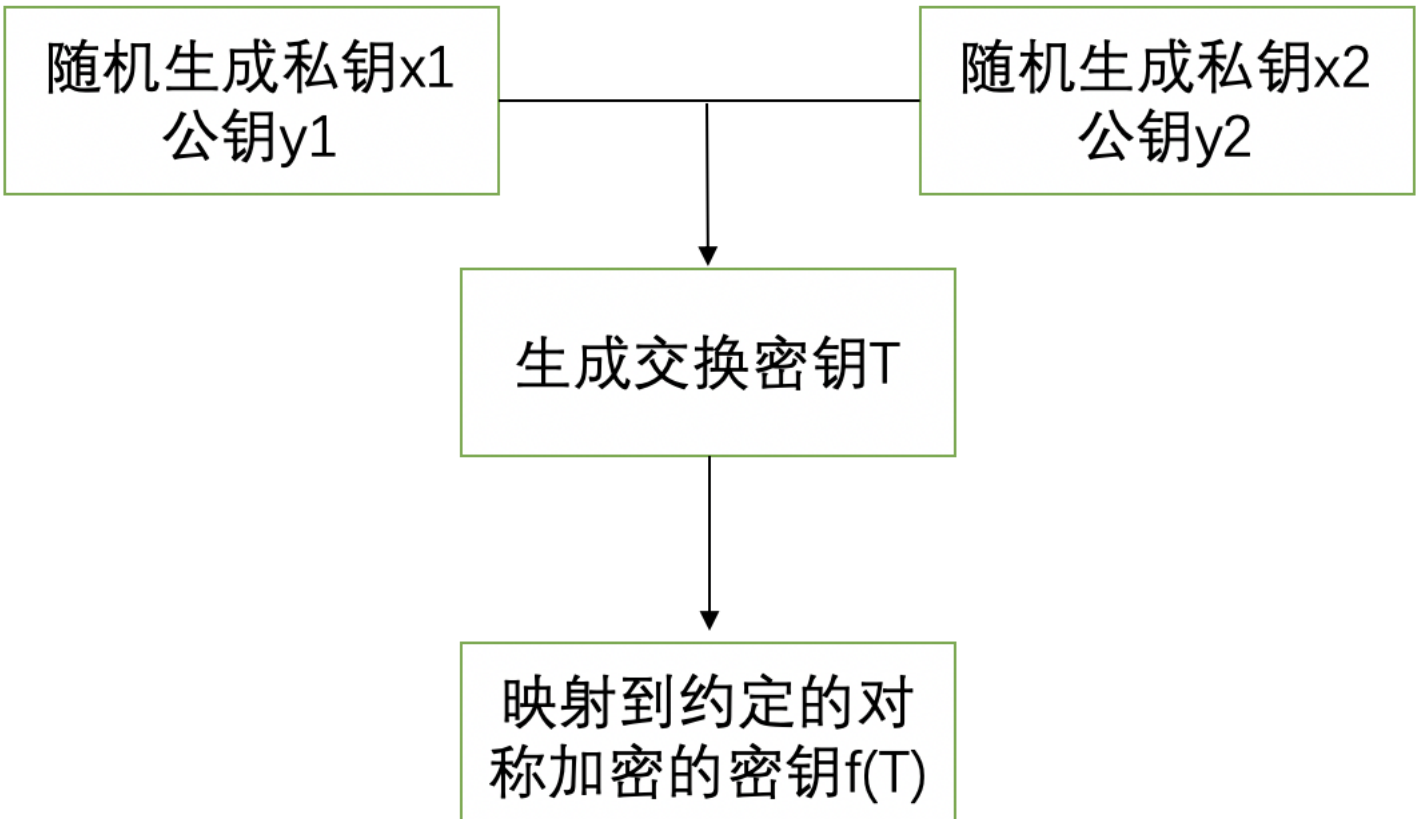
随机生成私钥x1
公钥y1
随机生成私钥x2
公钥y2
生成交换密钥T
映射到约定的对称加密的密钥f(T)