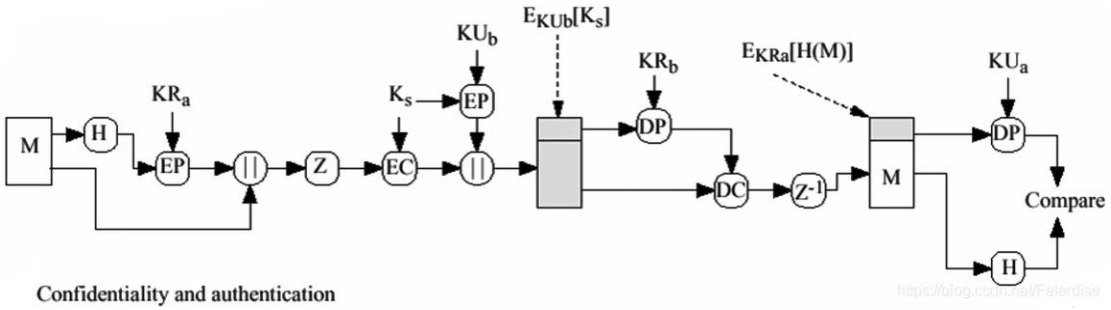
Project12

一、实验原理

1.PGP



Confidentiality and authentication

PGP（Pretty Good Privacy）加密，由一系列散列、数据压缩、对称密钥加密，以及公钥加密的算法组合而成，每个步骤支持几种算法。PGP 支持消息认证和完整性检测：完整性检测被用来检查消息在传输过程中是否变更过（即验证消息完整性）；消息认证则是被用来决定消息是否确由某特定的人或实体发出（即数字签名验证）。在 PGP 中，这些特性默认是和消息加密同时开启的，而且同样可以被应用到明文的验证。发送者只需使用 PGP 为消息创建一个数字签名，即以数据或信息创建一个散列，然后使用发送者的私钥利用散列生成数字签名。

二、实验结果

使用 SM2 来实现 PGP 方案，这里的对称密码使用的是 AES。实验结果为：

```
消息为： shandawangluokongjiananquan
加密值为： b'\x89\x1b\xab\x18I\x8e\xf6\xb8\x06Y>\xd3\x00\xcc\x81\x05\xf6=*A\x15\x9bEK\xdb\x9a\xfb\x99 M\x80\xe1'
原消息值为： shandawangluokongjiananquan
```