# 代码架构



代码调用示意图

代码目录中主要分为五部分：

1. **filter.pl**

是负责与git进行交互的perl代码，包括接收git传入的文件信息，将经过filter更改的加密文件再传回给git等功能。filter.pl会调用abe\_abs文件夹中的enc\_sig和verify\_dec代码。

1. **abe\_abs文件夹**

其中包括如下代码文件：

* enc\_sig.c：属于filter的clean部分，对git add的文件进行加密和签名。
* verify\_dec.c：属于filter的smudge部分，对git merge/checkout等文件进行验签和解密。
* setup.c：是初始化文件，在初始时运行该文件生成ABE/ABS公钥和用户私钥。
* commit.sh：在前两个代码中被调用，功能是获取git仓库最初的commit ID。

1. **abe文件夹**

此文件夹中的代码是通过cpabe和libbswabe[1]的API，加上调用模块使用[1]的加解密和处理函数。其中包括以下代码文件：

* abesetu.c：ABE的初始化代码。
* abekeygen.c ：ABE的用户密钥生成代码，需要输入用户的属性。
* abeenc.c：ABE加密代码，调用[1]的bswabe\_enc加密函数。
* abedec.c：ABE解密代码，调用[1]的bswabe\_dec解密函数。
* common.c（[1]原有代码）：包括AES加解密算法，文件的读写函数等通用函数。
* policy\_lang.c（[1]原有代码）：关于policy的解析和处理函数，其中使用到的有parse\_attribute（属性解析函数）。

1. **abs文件夹**

此文件夹中的代码是参考[1]的代码，对ABS算法进行了实现，所以代码内容比abe文件夹中多一些。包括以下文件：

* abssetup.c：ABS的初始化代码。
* abskeygen.c：ABS的用户密钥生成代码，需要输入用户的属性。
* abssign.c：ABS的签名代码，调用core.c中的mprabs\_sig签名函数。
* absverify.c：ABS的验签代码，调用core.c中的mprabs\_verify验签函数。
* common.c：ABS的文件读写函数。
* core.c：ABS的核心代码，包括ABS的初始化、密钥生成、签名验签等功能实现函数，以及policy转换函数等。
* misc.c：ABS代码中各种变量之间的转换函数，主要是为了serialize和unserialize。另外还有变量的free函数。
* private.h：ABS代码中的变量定义。

1. **blockchain文件夹**

此文件夹中的代码是为了从区块链的事件event中读取metadata。

* index1230-listen.js：监听事件是否有更新的代码，有更新会返回更新的metadata，一般不使用。
* index1230-pastevent.js：获取事件内容（policy）的代码，在enc\_sig.c和verify\_dec.c中被调用。
* index1230-write.js：向事件中写入新的metadata或修改旧的metadata的代码。

1. cpabe文件夹

存放了cpabe和libbswabe[1]的源代码供查看。

**参考：**

1. <http://acsc.cs.utexas.edu/cpabe/>