Atitit 防伪防篡改方法总结关键数据的防篡改检验方法

目录

[1. 篡改的两种方式： 1](#_Toc2680)

[1.1. 第三方篡改 1](#_Toc554)

[1.2. 2.用户自行修改 1](#_Toc5509)

[2. 常见证件钞票防伪技术 2](#_Toc3982)

[2.1. 紫外线敏感图案纸 2](#_Toc23255)

[2.2. 变色涂料 2](#_Toc3011)

[2.3. MRZ比对：OCRMRZ和RFIDMRZ的比对 2](#_Toc17370)

[2.4. 芯片 3](#_Toc29044)

[3. 常见防篡改方法 3](#_Toc952)

[3.1. rsa加密法 3](#_Toc26022)

[3.2. 校验码 签名法 3](#_Toc30685)

[3.3. 业务逻辑进行验证 3](#_Toc21160)

[3.4. 高级语言防止看到源码 ，算法保密 3](#_Toc8612)

[3.5. Key保密 key 3](#_Toc7050)

# 篡改的两种方式：

## ****第三方篡改****

意思是说在数据由用户发到服务器的途中，数据被第三方篡改，造成发送的数据和接收的数据不一致，防止此类情况的发生的常用做法如下：

1. 将要提交的参数先做加密 在做签名。。。
2. 如果第三方不知道加密方法，也可以不走签名，加密即可。。

## ****2.用户自行修改****

****其实这种方式不能算作被篡改，因为是用户自己修改的，并且是在发送数据前修改 的，这样发送和接收双的都是相同的数据，但是可能是不是期望的数据。****

****例如，一个充值页面，用户点击了充值10元的按钮，在提交前，F12把10改为10000，那么实际上发送的数据是10000，后台接收到的数据也是10000，那么这个值是没有被篡改的，但是不是期望的（对于服务端）。****

****对于这种修改方式，无法通过加密等手段进行验证，只能通过业务逻辑进行验证。比如要删除一篇文章，只能在业务层保证用户是删除的自己的，而不会通过修改id等方式删除了别人的。对于上边充值的例子也可以在业务逻辑上验证是给当前用户自己充值并是由当前用户支付的，这样付款的还是自己，就没有什么问题了。****

****————————————————****

# 常见证件钞票防伪技术

就目前而言，假护照要以假乱真几乎没有可能，尤其是当进入电子信息高度普及的时代。  
1、护照是世界上除了纸币之外最难伪假的。上面采用的技术特别多，基于不同原理的不同技术所呈现出来的效果和特征各不相同。此外，有些技术的使用成本极高。注意，是极高，除非你富可敌国，否则用不起。

作者：匿名用户  
链接：https://www.zhihu.com/question/21318382/answer/17878266  
来源：知乎  
著作权归作者所有。商业转载请联系作者获得授权，非商业转载请注明出处。

## 紫外线敏感图案纸

## 变色涂料

## MRZ比对：OCRMRZ和RFIDMRZ的比对

：通过复杂机读码的一致性，排除那些“粗心”的假护照。

护照真伪的鉴别方法虽然从可靠性可以参照人民币和身份证的防伪鉴别可靠性，紫外光防伪鉴别护照原理同人民币紫外防伪的原理一样，国家对变色涂料的控制可以保证这一方法的可靠性；而芯片读取鉴别护照原理同身份证读卡原理一样，护照芯片和机读码信息只掌握在制证机构且属国家机密，从这一点来看，此法可靠性非常强。

## 芯片

# 常见防篡改方法

## rsa加密法

## 校验码 签名法

：在数据库的记录中设置校验码，校验码根据记录中的关键数据生成；当检验时，生成关键数据的密文；将密文与校验码进行比较，根据比较结果确定关键数据是否被篡改。本发

## ****业务逻辑进行验证****

****。比如要删除一篇文章，只能在业务层保证用户是删除的自己的，而不会通过修改id等方式删除了别人的。****

## ****高级语言防止看到源码 ，算法保密****

## ****Key保密 key****

****可以用非编译语言加密****