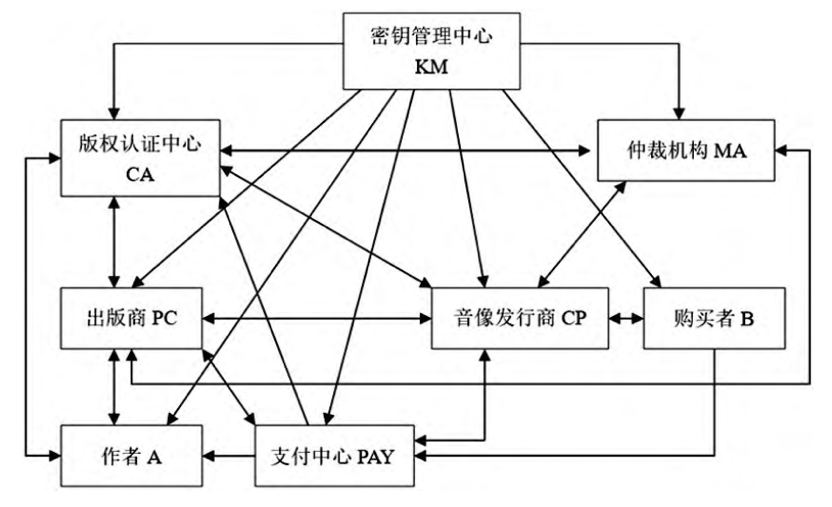
**网络空间安全导论大作业（三）**

学号： 姓名：

**数字水印版权保护原理**

随着网络和多媒体技术的发展，数字音像制品的使用和传播变得越来越便利。然而数字产品因极易复制、产品副本可以保持很好的质量以及传播成本极低的特性，很容易被盗版者滥用，有恶意的个人或团体可能在没有得到作品所有者许可的情况下复制和传播有版权的数字媒体内容。

为保护数字产品版权，实现的版权注册、网络发行、销售和版权纠纷等过程，数字水印应运而出。以下介绍一个数字水印的数字版权保护协议。

* 该基于数字水印的数字版权保护协议模型包含8个实体，如图：

各个实体的功能为：

1. 密钥管理中心KM：密钥生产、密钥存储、密钥备份、密钥恢复、密钥托管、密钥运算、选用对称密码算法、签名协议和一些hash函数。
2. 版权认证中心CA：版权认证中心颁发身份数字证书，对各种关于证书的请求进行应答。版权中心作为可信的第三方承担着注册版权、生成水印、提供水印算法、检测水印等任务。
3. 仲裁机构MA：当发生版权纠纷、侵权、盗版等行为时有仲裁机构来判决。
4. 出版商PC：出版商是版权所有者，可以向发行商转让部分使用权来分发其数字产品。
5. 音像发行商CP：音像发行商经出版商授权后，可以网络发行并销售数字产品。负责为购买者提供各种服务。
6. 支付中心PAY：支付中心作为可信第三方，负责买卖双方之间的金钱交易，并向支付实体提交支付信息。
7. 购买者B：购买者购买并使用数字产品实体。购买者不拥有版权，并且被要求只可自己使用，不能公开或非法传播购买的数字产品。
8. 作者A：数字音像制品创作完成后，作者既可以使自己成为该数字音像制品的版权所有者，也可以在得到一定版权转让费后，将版权全部转让给出版商。

* 以下介绍协议中的各种操作的符号定义：

：用X的公钥加密Y

：用X的私钥给Y签名

：数字产品

：公钥/私钥

：连接运算符

：X的信息

：X身份识别，其计算公式为

：作品W的水印

：为产品嵌入水印

：嵌入水印M以后的作品W

* 以下介绍协议下的各个子协议的具体流程

1. 版权注册子协议

该协议帮助作者A向版权认证中心CA注册自己创作的产品W，以获得W的版权。具体协议如下：

Step1:

Step2: CA用私钥解密后，通过的公钥信息两次解密来验证用户身份。通过以后进入Step3；若W已经注册且身份标识信息为，则定义为误操作；若W已经被注册且身份标识信息不是，则判断为侵权。上述两个操作均转到Step5

Step3: CA给作品W一个标识号，记为，之后根据注册信息计算，生成水印，在W中嵌入水印，，并将和存入版权数据库。

Step4: 通知注册成功，转到Step6。

Step5: 通知注册失败。

Step6: 结束。

1. 版权转让子协议

作者在获得一定的版权转让费以后，可以把版权卖给出版商，让出版商成为数字产品的版权拥有者。协议如下：

Step1:

Step2: CA用私钥解密后，通过的公钥信息两次解密来验证用户身份。若不通过转入Step6，若通过则完成注册。

Step3: CA根据作者报价通知PC向作者A支付版权费。若PC向A支付成功，则继续，否则转入Step6。

Step4: CA在数据库中检索，找到后，计算，生成水印并重新在W中加载水印。之后，用和来替换原数据库中的和。

Step5: 通知PC转让成功，转到Step7。

Step6: 通知PC转让失败。

Step7: 结束

1. 使用权转让子协议

出版商在拥有作品的版权以后，为了销售作品，会将部分版权转让给音像发行商。发行商购买一定数量的数字作品的使用权后将数字产品出售给购买者。其协议如下：

Step1:

Step2: CA用私钥解密后，通过的公钥信息两次解密来验证CP身份。若不通过则转到Step7，否则继续。

Step3: CA根据PC的报价来通知CP支付版权使用费，CP进行支付，若失败则转到Step5。

Step4: CA在数据库中检索，找到后，根据CP要购买的数字产品的使用权数量，此处假设为N，计算,其中,ID为CA随机产生的不重复序列号。计算,其中。计算，其中。将M集合和WM集合放入使用权数据库。

Step5:数字作品使用权转让成功，将传输给CP。转到Step7.

Step6: 数字作品使用权转让失败。

Step7: 结束。

1. 交易子协议

音像发行商获得的使用权后，在互联网上发布有关和的信息。购买者B可以进行购买，其协议如下：

Step1:, 传递给CP

Step2: CP 用私钥解密后,通过的公钥信息解密来验证B的身份，若身份检测不通过则转到Step7。

Step3: B根据网上的价格，通过支付中心向CP支付购买费用，若支付失败，则转入Step7。

Step4: CP将此时编号为i的作品使用权售卖给B，计算，生成水印,重新在上加载水印生成

Step5: 传递给B。

Step6: 交易成功，转到Step8。

Step7: 交易失败。

Step8: 结束。

Step9: 多次成功交易后，CP批量提交交易信息， 给CA，CA将交易信息保存到交易数据库。

1. 盗版跟踪仲裁协议

音像发行商CP可能会超出他所购买产品使用权的数量，额外销售出版商的产品以谋暴利，购买者B也可能非法拷贝出版商的产品。当PC发现自己的产品被盗版时，出版商必须追踪到是谁在盗版自己的产品。具体协议如下：

Step1: PC将正版和盗版产品提交给仲裁机构，申请仲裁。

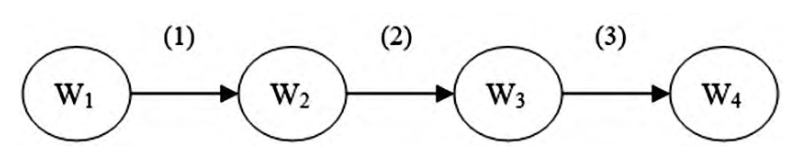
Step2: MA将提交给版权认证中心CA，请求验证。

Step3: CA提取中的水印信息,并在交易数据库中检索。若没有检索出与之对应，则盗版源于音像发行商CP；若检索出了与对应，则可以检索到相对应的，用购买者的公钥解密后得到和，若解密两者分别得到的与不相同，则说明音像发行商CP有盗版行为；若相同，则说明身份标识为的购买者B有盗版行为。

Step4: CA把盗版追踪结果发送给MA，MA依法对盗版行为进行制裁。

根据以上5个协议，便可以实现的版权注册、网络发行、销售和版权纠纷。

* 协议使用与可靠性

基于以上的5个协议，我们期望的流程为：

W1是具有A版权标识的数字水印图像。W2是具有PC版权标识的数字水印图像。W3是具有CP使用权和PC版权标识的数字水印图像。W4是具有B身份标识、CP使用权标识、PC版权标识的数字水印图像。

以上流程严格按照协议1-4的步骤进行，易知期望的步骤可以保护版权。

而根据协议5，不论是音像发行商CP额外销售出版商的产品，还是购买者B非法拷贝产品，都将被仲裁机构MA制裁，这也保护了版权。

以上即所介绍的数字水印的数字版权保护协议。随着数字水印技术和密码学的发展，对基于数字水印的版权保护协议的研究必将会得到越来越多的关注，数字水印的应用也必将越来越成熟。

参考文献：

[1]武卫翔,王杰华,张金宝.基于数字水印的数字版权保护协议研究[J].计算机时代,2022(09):87-91.DOI:10.16644/j.cnki.cn33-1094/tp.2022.09.019.

[2]朱长青,徐鼎捷,任娜,崔瀚川,赵亚宙.区块链与数字水印相结合的地理数据交易存证及版权保护模型[J].测绘学报,2021,50(12):1694-1704.