Journal of Computer Applications
计算机应用,2013,33(9):2529-2531,2556
ISSN 1001-9081
CODEN JYIIDU
2013-09-01
http://www.joca.cn

文章编号:1001-9081(2013)09-2529-03
doi:10.11772/j.issn.1001-9081.2013.09.2529

基于 El Gamal 算法的数字水印协议

闫丽霞*,肖明波
(杭州电子科技大学 通信工程学院,杭州 310018)
(*通信作者电子邮箱 hduyan@163.com)

摘　要:针对数字水印协议中需要买方的频繁参与,要求买方了解签名或水印生成嵌入等技术以及没有很好地考虑数字产品的使用控制等问题,提出一种安全实用、可扩展的数字水印协议。该协议利用具有同态性和可交换性的 El Gamal 加密算法及基于机器指纹的版权控制方案,在实现数字水印基本功能的同时,相当程度上兼顾了买卖双方的权益,以更接近传统交易的模式,改进用户的体验。

关键词:数字版权管理;数字水印协议;El Gamal 加密算法;使用控制;机器指纹
中图分类号:TP309.2;TP309.7　　**文献标志码**:A

Digital watermarking protocol based on El Gamal algorithm

YAN Lixia*, XIAO Mingbo
(*College of Communication Engineering, Hangzhou Dianzi University, Hangzhou Zhejiang 310018, China*)

Abstract: In light of the drawbacks of current digital watermarking protocols, such as requiring frequent involvement of buyers, assuming that buyers' knowledge of signature or watermark, and not considering appropriate usage control of digital products, a secure, practical and extensible watermarking protocol was proposed, by utilizing the homomorphic, commutative El Gamal encryption algorithm and the machine fingerprint-based copyright control scheme. Besides the basic functions of the digital watermarking protocol, this protocol also considered the interests of both buyer and seller to some extent, and improved user's experience with a transaction model similar to the traditional one.

Key words: Digital Rights Management (DRM); watermarking protocol; El Gamal encryption algorithm; usage control; machine fingerprint

0　引言

数字化和网络化技术的迅速发展,一方面为实现信息高速无失真的传播和灵活的编辑、修改提供了便利的手段,同时也对数字化产品的版权保护提出了严峻的挑战,信息安全问题日益成为人们关注的焦点。密码学技术不能对数字产品进行全程保护,数字水印技术应运而生。近年来,数字水印技术和密码学技术两者相结合,成为保护数字版权的主要手段。在保护数字版权的过程中,对于一个完整的数字水印体系来说,可靠的数字水印算法固然重要,但还需要技术的实现协议。

如今,许多的数字水印协议研究都是基于 Memon 等[1]提出的一种交互式的买方-卖方水印协议,并实现很好的性能,只是在考虑第三方的负担或是可信度即共谋攻击发生的可能有着不同的解决方案。文献[2]提出一种无第三方参与、水印的加载与检测全由买卖双方完成的协议,该协议完全避免了共谋攻击。为了减少可信任第三方的在线参与,文献[3]引入一个无记忆的水印认证授权中心 WCA,它为买方一次产生多个水印,从而不需要参与买卖双方的每次交易。文献[4]中的协议运用代理签名技术,文献[5]通过内容服务器产生数字水印池和移动代理动态分发许可证这两种机制。文献[6]提出了一种基于水印密钥共享的方案以解决缺席验证问题。这些协议在一定程度上解决了安全问题,但却忽视了买方的体验。它们大多需要买方的频繁参与,增加了网络开销和买方的负担,影响用户对协议的体验。而且,作为消费者的用户不一定知道签名加密等技术,再者,当发现非法拷贝并对其进行认证仲裁时,买方也是不愿多参加的。文献[7]针对这些问题,提出了一种解决方案,但是协议中出现的裸文件传输造成了很大的安全隐患。除了这些问题,文献中所提出的某些协议没有很好地考虑产品的使用控制,一般都是将加密的嵌入水印的数字产品传给用户,用户可直接使用其密钥对产品进行解密后读取。

基于上述分析,本文提出一种基于 El Gamal 加密算法的新型协议和交易模型。该协议运用具有乘同态性及加密可交换性的 El Gamal 加密算法,通过该加密算法,水印的生成与嵌入、文件的加解密以及对违法拷贝进行认证仲裁可由卖方和可信第三方两者完成,买方不用参与其中,买方只需发起购买申请及确认即可。同时,通过运用此算法,可信第三方的任务量也不再过重。此外,与许可证紧密结合并借助基于机器指纹加密的电子书交易平台模型,对协议进行设计,增强了系统的安全性与实用性,同时简化了买方操作步骤,进一步保护买方的利益。

1　背景知识

1.1　El Gamal 加密算法

记加密参与方是 A 和 B,E_A 和 D_A 分别为 A 的加密算法

收稿日期:2013-03-25;**修回日期**:2013-04-28。
基金项目:国家自然科学基金资助项目(30900328);杭州电子科技大学启动基金资助项目(KYS085612006)。
作者简介:闫丽霞(1987-),女,河南新乡人,硕士研究生,主要研究方向:数字版权保护;　肖明波(1971-),男,湖南沅江人,教授,博士生导师,博士,主要研究方向:无线网络、数字版权保护、智慧城市。

和解密算法，相应的 E_B 和 D_B 为 B 的加密算法和解密算法。当对任何的信息 m，一个加密算法满足 $E_A(E_B(m)) = E_B(E_A(m))$；$E_A(D_B(m)) = D_B(E_A(m))$；$D_A(D_B(m)) = D_B(D_A(m))$ 时，本文认为此算法具有加密交换性。当加密算法满足 $E_A(m_1) * E_A(m_2) = E_A(m_1 * m_2)$ 时，就认为此算法具有乘同态性，其中 m_1 和 m_2 表示两个不同的文件。

同态加密技术是交互式水印协议的基础，本文运用具有乘同态性和交换性的 El Gamal 加密算法进行水印的嵌入与加密。El Gamal 算法的密钥对的产生过程：首先选择一个大的素数 P 和两个随机数 g 和 k，$(g,k<p)$。计算 $\alpha = g^k \bmod p$，则其公钥为 p、g 和 α，私钥为 k。用 El Gamal 算法对文件的加解密过程：设原文件为 x，其对应的密文 x' 为 (y_1,y_2)。加密方对文件 x 进行加密时，选择一个随机数 r，则有：$y_1 = g^r \bmod p, y_2 = x * g^{k*r} \bmod p$。对 x' 进行解密，有：$D_k(y_1,y_2) = y_2(y_1^k)^{-1} = x$，可知该算法具有可交换性[8]，也不难验证其乘同态性[9]：

$$E(m_1) * E(m_2) = (g^{r1}, m_1\alpha^{r1}) * (g^{r2}, m_2\alpha^{r2}) = (g^{r1+r2}, (m_1 * m_2)\alpha^{r1+r2}) = E(m_1 * m_2)$$

1.2 基于机器指纹加密的数字内容交易平台模型

在此模型中，出版商可用设备生产商提供的设备密钥对产品进行加密[10]。设备生产商采用密钥生成算法对机器指纹进行运算得设备密钥，当进行阅读时，阅读设备采用同样的算法，自动生成其自身设备密钥，对需要解密的产品或文件进行解密[11]。这样使得文件与设备绑定更进一步地保护文件的安全性。设备生产商的加入使得基于机器指纹的设备密钥的生成更加容易。

本文内容许可证的加密密钥选择设备密钥，当许可证被用户下载到阅读设备上后，阅读设备对许可证自动解密并存于安全区，许可证中的文件加密密钥自动被提取，以对加密文件进行解密。这样既保证了内容许可证对买方透明，增强系统安全性；又满足本文所提的新型协议所要达到的要求，简化买方操作步骤，进一步保护买方的利益。

2 协议设计

本协议有 5 个参与者：可信的交易平台 TTP、可信的仲裁机构 ARB、买方、卖方、设备生产商。本协议中，假设 TTP 与 ARB 是完全可信的，其中涉及的符号及其意义如表 1 所示。整个协议由 3 个部分组成：用户注册、水印的生成及嵌入、纠纷仲裁，其简单执行过程如图 1 所示。其中，TTP 与水印生成服务器、CA(可信的认证中心)、支付管理中心等进行通信。

表 1 协议中所用主要符号及其意义

符号	意义
TTP	可信的交易平台
ARB	可信的仲裁机构
ID_B	买方的身份信息
ID_B'	买方在交易过程中所使用的假名
X	买方要购买的数字作品
X'	嵌入水印后的作品
ARG	交易协议
W	数字水印
$SIGN_I(M)$	参与方 I 对信息 M 的数字签名
$\otimes$	水印嵌入算法
(PK^*, SK^*)	TTP 为本次交易选择的密钥对
(PK_S, SK_S)	卖方选择的密钥对
$\|$	连接符

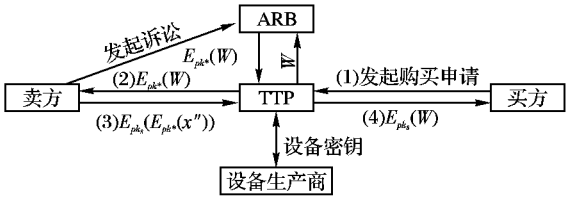

图 1 协议的简单执行过程

2.1 用户注册

此过程由买方和 TTP 完成。

买方将阅读设备与 TTP 相连，并将自己的身份信息 ID_B 发送给 TTP 进行用户及设备注册，TTP 对 ID_B 进行哈希运算得 ID_B'，根据 ID_B' 生成匿名证书 $Cert(ID_B')$，然后为买方建立账户，并将 ID_B' 和 $Cert(ID_B')$ 发给买方。此 ID_B' 即为买方在交易过程中所使用的假名。若买方不用在交易过程中匿名，则其可不用申请匿名证书，直接进行注册即可。TTP 上有卖方的产品简介，可供买方浏览。

2.2 水印的生成及嵌入

此过程由买方、卖方和 TTP 完成。

1)买方在 TTP 上浏览卖方的作品，选购自己想要的，就选中的作品 X 填写订单，即达成协议 ARG。ARG 对作品 X 进行一定的描述，并记载协议生成时间，同时规定了交易双方卖方和买方的权利与义务。达成的 ARG 一式两份，卖方与买方一方一份，ARG 将此次交易与作品进行了绑定。

TTP 就本次交易选择一个密钥对 (PK^*, SK^*)，同时根据 ARG 中的信息生成水印 W。TTP 将 $E_{PK*}(W)$、PK^*、$SIGN_{TTP}(ARG \| E_{PK*}(W) \| PK^*)$ 发送给卖方，并对买方发送一个付款信息，买方进行付款，TTP 暂管交易金。

2)卖方收到来自 TTP 的信息后，对签名进行验证。若签名为真，生成唯一的一个与本次交易相关的检索水印 V，并选择用于本次交易的密钥对 (PK_S, SK_S)。卖方将检索水印 V 嵌入作品 X 中，即 $X' = X \otimes V$。卖方用 PK^* 对 X' 进行加密，即 $E_{PK*}(X')$，并对作品 X 进行二次水印嵌入，即 $E_{PK*}(X'') = E_{PK*}(X') \otimes E_{PK*}(W) = E_{PK*}(X' \otimes W)$；然后用公钥 PK_S 对 $E_{PK*}(X'')$ 进行加密，即 $E_{PK_S}(E_{PK*}(X''))$。同时卖方替买方申请内容许可证，此内容许可证由设备密钥进行加密，具体过程在 2.4 节进行描述。卖方将 $E_{PK_S}(E_{PK*}(X''))$、$SIGN_S(E_{PK_S}(E_{PK*}(X''))$ 和内容许可证发送给 TTP，并存储信息 $E_{PK*}(W)$、ARG、PK^*、$SIGN_{TTP}(ARG \| E_{PK*}(W) \| PK^*)$、$V$、$\otimes$。

3)TTP 收到卖方发来的信息后，对签名进行验证，若验证通过，用 SK^* 对 $E_{PK_S}(E_{PK*}(X''))$ 进行解密得 $E_{PK_S}(X'')$。因为本文采用的加密算法是具有加密交换性的 El Gamal 算法，故满足 $D_{SK*}(E_{PK_S}(E_{PK*}(X''))) = D_{SK*}(E_{PK*}(E_{PK_S}(X''))) = E_{PK_S}(X'')$。

TTP 将 $E_{PK_S}(X'')$ 和内容许可证放到买方的账户中，供买方下载。

4)买方将 $E_{PK_S}(X'')$ 和内容许可证下载到阅读器后，阅读器自动对内容许可证进行解密，并提取内容许可证中的 SK_S 对 $E_{PK_S}(X'')$ 进行解密，即 $D_{SK_S}(E_{PK_S}(X'')) = X''$。买方对 X'' 进行验证，若 X'' 的内容、质量等达到了自己的要求，就向 TTP 发送交易完成信息，TTP 支配交易金打入卖方的账户中。

第 2)步中，卖方的私钥 SK_S 也可是设备生产商提供的基于机器指纹生成的设备密钥，这样，内容许可证中可不用包含 SK_S。对 $E_{PK_S}(X'')$ 进行解密时，阅读设备根据同样的密钥生成算法，生成设备密钥，即解密密钥 SK_S 对 $E_{PK_S}(X'')$ 解密，不

必再对解密密钥 SK_S 进行提取,只需由内容许可证开启解密程序即可。

2.3 纠纷仲裁

卖方若发现作品 X 的非法复制品 Y,则对 Y 中的检索水印 V 进行提取,并根据检索水印 V 搜寻自己的交易信息库,找到与之匹配的买方。具体过程如下:

1)若买方不承认作品是从自己这边泄露的,卖方就搜寻与 V 相关的信息 $E_{PK*}(W)$、ARG、PK^*、$SIGN_{TTP}(ARG \| E_{PK*}(W) \| PK^*)$、$V$、$\otimes$,并将这些信息发给仲裁机构 ARB,进行诉讼。

2) ARB 对签名进行验证,并将 $E_{PK*}(W)$ 和 PK^* 发给 TTP,TTP 检索出与 PK^* 相对应的 SK^*,并用其对 $E_{PK*}(W)$ 进行解密。

3) TTP 将解密得的 W 及 $SIGN_{TTP}(W)$ 发送给 ARB。ARB 将 W、V、Y 作为水印检测器的输入,检测 Y 中是否含有水印 W,若有,则可证明买方是非法盗卖者,并对其真实身份进行揭露;若没有,则撤销诉讼。

2.4 内容许可证的建立与使用

本协议由卖方替买方申请内容许可证,内容许可证的加密密钥的生成采用基于机器指纹的设备密钥生成方案[11],即许可证的加密密钥采用设备密钥。内容许可证包含数字产品的解密密钥、用户对产品的使用权限和授权使用期限等规则信息。方案中,采用对称加密体制对内容许可证进行加密[12]。记内容许可证密钥为 LK,则 $LK = S(Tag)$,其中 Tag 为用户机器的指纹,S 表示对 Tag 进行的哈希算法,这样内容许可证就与机器指纹绑定。当在阅读器上阅读产品时,阅读器根据同样的算法产生内容许可证解密密钥,即设备密钥,而后自动提取产品解密密钥对产品进行解密(可由操作系统和多媒体中间件负责解密并强制执行使用规则检测工作),并将解密后的内容许可证放在安全保护存储区内,使其对用户透明,这样用户不必知道产品的解密密钥,且只能用特定的阅读器读取产品。

3 协议分析

3.1 协议功能分析

1)数字作品的安全性。数字作品在交易传输的整个过程中都是以加密形式出现,使其得到良好的保护。数字水印的嵌入对作品使用过程中盗版行为的发生起到威慑作用,若出现盗版,可根据水印信息进行盗版追踪,准确追查出违法盗版者。

2)水印的安全性。水印的嵌入使用 El Gamal 加密算法的乘同态性,实现了水印及终极作品 X'' 对卖方不可见,同时,用签名将水印与作品 X 进行绑定,这样卖方不能将水印进行移植或提取来诬陷买方。买方也不知道水印信息,无法将水印从作品中移除,这样很好地保护了交易双方的权益。

3)协议的简单性及可扩展性。加密算法的加密可交换性使得多方对文件的无序加解密成为可能,大大降低了整个协议的复杂度。其中:(PK_S, SK_S) 是卖方为本次交易专门选择的密钥对,SK_S 也可是设备生产商提供的设备密钥,视具体情况而定。

4)协议的实用性。在整个过程中,买方只参与注册、付款和使用等过程,在最后仲裁阶段也不需要买方的参与,实现了缺席验证。协议加入基于机器指纹控制的版权控制模块,有效控制用户对产品的使用权限。同时,通过 TTP 对交易金的暂管,良好地保护了买方的公平权益,改善了用户的体验。另外,买方与卖方只与第三方联系,减少了买卖双方之间的认证,从而减小了网络开销。但是,该协议中所运用的加密算法单一,在实际应用时有一定的局限性。

5)匿名问题。买方可根据需要选择交易过程中是否需要匿名,如果买方选择了匿名交易,那么在整个交易过程中,此协议可以很好地保持买方的匿名,直至其非法进行产品拷贝,被依法追究。

3.2 协议性能分析

该协议假设第三方 TTP 与 ARB 是完全可信的,水印的生成由 TTP 执行,水印的加载由卖方完成,认证仲裁由 ARB 负责。该协议在保证实现所要求的功能,即保证数字产品安全的同时减少买方的参与,最大限度地减少信息传递次数,以减小网络开销。具体传递次数的比较如表 2 所示。

4 结语

数字化产业的和谐、快速、稳定的发展,数字版权管理(Digital Rights Management, DRM)技术已经是不可或缺的一部分。利用具有同态性和可交换性的 El Gamal 加密算法及基于机器指纹的版权控制方案,本文提出了一种安全、实用、可扩展的数字水印协议,在保持协议尽可能简单实用的同时,保护了交易双方的权益。进一步可研究的方向包括水印嵌入算法,以尽可能地达到协议与技术的有效结合,实现一个更完整的数字水印安全体系。

表 2　水印协议信息传递次数的比较

传递方式	文献[3]协议		文献[5]协议		本文协议	
	数字产品的传递次数	水印及其他信息的传递次数	数字产品的传递次数	水印及其他信息的传递次数	数字产品的传递次数	水印及其他信息的传递次数
卖方←→TTP	0	0	1	3	1	1
卖方←→买方	1	1	0	0	0	0
TTP←→买方	1	1	1	2	1	0

参考文献:

[1] MEMON N D, WONG P W. A buyer-seller watermarking protocol [J]. IEEE Transactions on Image Processing, 2001, 10(4): 643 - 649.

[2] ZHANG J, KOU W, FAN K. Secure buyer-seller water marking protocol[J]. IEE Proceedings on Information Security, 2006, 153(1): 15 - 18.

[3] 胡玉平,张军. 用于盗版追踪的数字水印协议研究[J]. 计算机科学,2010, 37(1): 91 - 94.

[4] HAJI M K N, ESLAMI Z. An efficient buyer-seller watermarking protocol based on proxy signatures [C]// Proceedings of IEEE the 8th International ISC Conference on Information Security and Cryptology. Piscataway, NJ: IEEE Press, 2011: 73 - 77.

[5] 王菲,陈虹,肖振久. 基于买方-卖方的安全数字水印协议[J]. 计算机应用,2011,31(5): 1288 - 1291.

[6] 徐蕾. 基于数字水印的 DRM 技术研究[D]. 郑州:信息工程大学,2007.

(下转第 2556 页)

表 4 Benchmarks 实验结果对照表 %

数据集	标准 C-SVM				IR 方法				AD 方法				本文方法			
	fp	*fn*	*acc*	*g-means*	*fp*	*fn*	*acc*	*g-means*	*fp*	*fn*	*acc*	*g-means*	*fp*	*fn*	*acc*	*g-means*
diabetis	47	94	88	66.58	47	94	88	66.58	50	95	88	68.84	60	88	84	72.67
flare-solar	46	92	74	65.26	37	96	93	59.61	45	94	74	65.00	48	86	71	64.49
german	65	96	92	78.85	63	94	90	76.80	69	97	94	81.62	73	93	90	82.48
heart	73	96	89	83.66	70	93	87	81.12	77	95	90	85.81	75	94	89	84.12
image	96	98	97	96.92	94	98	97	96.22	97	98	97	97.64	98	94	96	96.27
splice	87	94	92	90.32	87	94	92	90.33	87	94	92	90.33	90	92	92	91.34
thyroid	85	100	97	91.99	77	100	95	87.71	81	100	96	89.87	100	82	86	90.82
twonorm	94	99	97	96.11	94	98	97	96.26	94	99	97	96.11	95	98	97	96.42

表 5 总体效果对比表 %

评价标准	标准 C-SVM	IR 方法	AD 方法	本文方法
fp	74.125	71.125	75.000	79.875
fn	96.125	95.875	96.500	90.875
acc	90.750	92.375	91.000	88.125
g-means	83.711	81.828	84.402	84.826

4 结语

通过引入 Fisher 判别中的类内散度的概念分析了 SVM 训练中各类样本的分布情况，并根据类内散度决定的平均分布比对 SVM 的最优分类面进行修正以提高 SVM 分类模型的泛化性。这种方法不仅可以解决样本个数差异给训练带来的问题，而且可以解决样本分布不均造成的问题，具有较强的适应性。这为 SVM 方法在更看重少数类样本识别率（如故障诊断、健康评估、信用风险评估等）数据不均衡问题的实际运用中提供了算法支撑。在今后的研究中尝试将修正最优分类面的 SVM 运用于此类问题中。

参考文献：

[1] VAPNIK V. The nature of statistical learning theory[M]. Berlin: Springer-Verlag, 1995.

[2] ORRU G, PETTERSSON-YEO W, MARQUAND A F, *et al*. Using support vector machine to identify imaging biomarkers of neurological and psychiatric disease: a critical review[J]. Neuroscience and Biobehavioral Reviews, 2012, 36(4): 1140 – 1152.

[3] GUO L, GE P S, ZHANG M H, *et al*. Pedestrian detection for intelligent transportation systems combining AdaBoost algorithm and support vector machine[J]. Expert Systems with Application, 2012, 39(4): 4272 – 4286.

[4] MOUNTRAKIS G, IM J, OGOLE C. Support vector machines in remote sensing: a review[J]. ISPRS Journal of Photogrammetry and Remote Sensing, 2011, 66(3): 247 – 259.

[5] JIN W, ZHANG J Q, ZHANG X. Face recognition method based on support vector machine and particle swarm optimization[J]. Expert Systems with Applications, 2011, 38(4): 4390 – 4393.

[6] WU G, CHANG E. Class-boundary alignment for imbalanced dataset learning[C]// Proceedings of ICML 2003 Workshop on Learning from Imbalanced Data Sets. Washington, DC: AAAI Press, 2003: 786 – 795.

[7] 金鑫，李玉鑑，不平衡支持向量机的惩罚因子选择方法[J]. 计算机工程与应用，2011，47(33)：129 – 133.

[8] 郑恩辉，李平，宋执环. 不平衡数据挖掘：类分布对支持向量机的影响[J]. 信息与控制，2005，34(6)：703 – 708.

[9] CRISTIANINI N, SHAWE-TAYLOR J. 支持向量机导论[M]. 李国正，王猛，曾华军，译. 北京：电子工业出版社，2004.

[10] CHAWLA N V, JAPKOWICZ N, KOTCZ A. Special issue on learning from imbalanced data sets[J]. SIKDD Explorations Newsletters, 2004, 6(1): 1 – 6.

[11] FU Y, SUN R X, YANG Q, *et al*. A block-based support vector machine approach to the protein homology prediction task in KDD cup[J]. ACM SIGKDD Explorations Newsletter, 2004, 6(2): 120 – 124.

[12] AKBANI R, KWEK S, JAPKOWICZ N. Applying support vector machine to imbalanced datasets[C]// ECML 2004: Proceedings of the 15th European Conference on Machine Learning, LNCS 3201. Berlin: Springer-Verlag, 2004: 39 – 50.

[13] SUN X, LIM E-P, LIU Y, On strategies for imbalanced text classification using SVM: a comparative study[J]. Decision Support Systems, 2009, 48(1): 191 – 201.

[14] 周皓，李少洪. SVM 最优分类面相对位置的修正[J]. 北京航空航天大学学报，2009，35(11)：1302 – 1305.

[15] MIKA S, RATSCH G, JASON G. Fisher discriminant analysis with kernels[C]// Proceedings of the 1999 IEEE Signal Processing Society Workshop. Piscataway, NJ: IEEE Press, 1999: 41 – 48.

[16] VEROPOULOS K, CAMPBELL C, CRISTIANINI N. Controlling the sensitivity of support vector machines[C]// Proceedings of the International Joint Conference on Artificial Intelligence. Washington, DC: Morgan Kaufmann, 1999: 55 – 60.

（上接第 2531 页）

[7] HU D F, LI Q L. A secure and practical buyer-seller watermarking protocol [C]// Proceedings of 2009 IEEE International Conference on Multimedia Information Networking and Security. Piscataway, NJ: IEEE Press, 105 – 108.

[8] ZHAO W L, VARADHARAJAN V, MU Y. A secure mental poker protocol over the Internet [C]// ACSW Frontiers 2003: Proceedings of the Australasian Information Security Workshop Conference on ACSW Frontiers. New York: ACM Press, 2003, 21: 105 – 109.

[9] 闫世斗，刘念，李子臣. 公钥密码体制的同态性分析[J]. 北京电子科技学院学报，2012，20(2)：55 – 59.

[10] XIAO M B, ZHANG J. A general platform for e-book transactions with digital rights management [C]// Proceedings of the 3rd International Conference on e-Business and Information System Security. Wuhan: [s. n.], 2011: 218 – 221.

[11] 蔡伟鸿，彭思喜，李岱素. 基于机器指纹的版权控制系统的设计与实现[J]. 汕头大学学报：自然科学版，2005，20(2)：49 – 55.

[12] 肖芸，肖明波. 基于特征图像的数字版权保护系统[J/OL]. 计算机工程与应用. http://www.cnki.net/kcms/detail/11.2127.TP.20120925.1001.040.html.