基于加同态公钥密码体制的匿名数字指纹方案*

孙中伟+, 冯登国, 武传坤

(信息安全国家重点实验室(中国科学院 软件研究所),北京 100080)

An Anonymous Fingerprinting Scheme Based on Additively Homomorphic Public Key Cryptosystem

SUN Zhong-Wei+, FENG Deng-Guo, WU Chuan-Kun

(State Key Laboratory of Information Security (Institute of Software, The Chinese Academy of Sciences), Beijing 100080, China)

+ Corresponding author: Phn: +86-10-62555958, E-mail: sunzwcn@yahoo.com.cn

Received 2004-09-24; Accepted 2005-07-28

Sun ZW, Feng DG, Wu CK. An anonymous fingerprinting scheme based on additively homomorphic public key cryptosystem. *Journal of Software*, 2005,16(10):1816–1821. DOI: 10.1360/jos161816

Abstract: This paper proposes an anonymous fingerprinting scheme based on the additively homomorphic public key cryptosystems. The proposed fingerprinting scheme enables the merchant to identify the illegal distributors without the help of a trusted third party when he/she finds an illegally redistributed fingerprinted copy. Furthermore, it allows two-party trials, i.e. there is no need for the accused (and possibly innocent) buyer to take part in the dispute resolution protocol and reveal his/her secrets. In addition, the problem of how to construct the anonymous public key and private key pairs is also addressed in the scheme. The security analysis shows that the proposed scheme is secure for both seller and buyer, and has the properties of anonymity and unlinkability for the buyer.

Key words: copyright protection; homomorphic public key cryptosystems; anonymous fingerprinting; two-party trials

摘 要: 提出了一种基于加同态公钥密码算法的匿名数字指纹方案,并给出了具有匿名功能的公钥和私钥对的具体构造方法,从而使该匿名指纹方案在发现盗版的情况下,销售商不需要第三方的帮助就能鉴别出数字多媒体作品的非法分发者,解决版权纠纷时也不需要购买者参与并提供相关的秘密信息,从而达到实现两方审判的目的.分析结果表明,该方案具有用户匿名及不可关联、销售商的可保证安全性和用户的可保证安全性等特点.

关键词: 版权保护;同态公钥密码体制;匿名指纹;两方审判

中图法分类号: TP309 文献标识码: A

* Supported by the National Natural Science Foundation of China under Grant Nos.60273027, 60373039, 90304007 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035802 (国家重点基础研究发展规划(973))

作者简介: 孙中伟(1969－),男,湖南益阳人,博士,主要研究领域为多媒体信号处理与安全;冯登国(1965－),男,博士,研究员,博士生导师,主要研究领域为网络与信息安全;武传坤(1964－),男,博士,研究员,博士生导师,主要研究领域为密码学,信息安全.

随着多媒体技术和计算机网络的飞速发展,人们获取数字信息已变得越来越便利,但是随之出现的对数字多媒体作品的版权保护问题也日显突出.早期,人们通过加密、访问受限等方法保护它们的版权,可一旦恶意的用户获得了这些数据,就无法阻止其进行非法复制.数字水印和数字指纹技术是近几年发展起来的新型数字版权保护技术.通常来讲,数字指纹代表用户以及与该次购买过程有关的信息.通过信号处理的方法,这些信息以不可感知的形式被嵌入到原始媒体数据中.一旦销售商发现有被非法分发的数字多媒体作品,就可以根据提取的指纹信息,找到非法分发该作品的用户.

数字指纹方案可以分为 3 种基本类型,它们分别是对称指纹模式、非对称指纹模式和匿名指纹模式[1].由于匿名指纹模式既能保护用户的隐私,又能使买卖双方的权益得到保障,因此,它成为目前数字多媒体版权保护问题的一个研究热点.自从 Pfitzmann 和 Waidner 在文献[1]中引入匿名指纹的概念以来,已有许多匿名指纹方案提出[2−4].但是,大多数匿名指纹方案由于基于过于复杂的密码协议而在实际应用中并不可行.因此,如何避免使用复杂协议构造匿名数字指纹方案是数字指纹研究需要解决的一个关键问题[5].在文献[6]中,Memon 和 Wong 利用公钥密码算法的同态性质提出了一种数字多媒体作品的买卖协议,但是,该方案不具备为购买者提供匿名购买的能力,而且在发现非法分发的数字作品时,销售商需要被指控的购买者参与并提供自己的秘密信息才能解决版权纠纷的问题.尽管利用公钥密码算法的同态性质构造匿名指纹方案因其简单实用受到研究者的广泛关注,也取得了一定的研究成果[7−9],但是,匿名指纹方案与密码协议以及密码算法密切相关,到底如何去构造具有匿名功能的公钥和私钥对,并且保证指纹嵌入的非对称性,仍然是基于同态公钥密码算法的匿名指纹技术没有解决的一个瓶颈问题.例如,Choi 等人在文献[8]中采用了 El Gamal 密码算法来构造基于同态公钥密码算法的匿名指纹方案.事实上,该方法是错误的,因为用户和销售商在加密时选取的随机数是不同的.本文将针对这些问题开展匿名数字指纹技术的研究.

在文献[10]中,Domingo 提出了一种不需要第三方帮助就能鉴别出盗版者的匿名指纹方案,然而,这个方案是基于零知识证明和多方安全计算的.本文在密码算法的最新研究成果的基础上,提出了一种基于同态公钥密码体制的加嵌入匿名数字指纹新方案.该匿名指纹方案在销售商发现盗版的情况下,不需要第三方的帮助就能鉴别出数字多媒体作品的非法分发者,解决版权纠纷时也不需要购买者参与并提供相关的秘密信息.

1 同态公钥密码体制

对于两个代数结构 A 和 B,其中 $\circ$ 是 A 中的运算,$*$ 是 B 中的运算,如果 $\forall x,y\in A$,有 $f(x\circ y)=f(x)*f(y)$,则映射 $f:A\mapsto B$ 称为 A 到 B 的同态[11].对于公钥加密算法 $E(\cdot)$,如果给定 $E(x)$ 和 $E(y)$,在没有私钥的情况下能够计算出 $E(x\circ y)$,则称该公钥加密算法具有同态性质.例如,RSA 公钥密码算法具有乘同态性质[12],而 Paillier 算法具有加同态性质[13].

为了构造一种不需要第三方的帮助就能鉴别出盗版者的匿名指纹方案,这里将采用 Bresson 等人提出的公钥密码算法[14],算法描述如下:

参数设置:设 $N=pq$,其中 p 和 q 为素数,且 $p=2p_0+1$, $q=2q_0+1$,而 p_0 和 q_0 也为素数, G 为模 N^2 的二次剩余循环群.

密钥生成:随机选择 $\alpha\in Z_{N^2}^*$ 和 $a\in[1,ord(G)]$,并使 $g=\alpha^2 \bmod N^2$, $h=g^a \bmod N^2$,那么公钥为 (N,g,h),而对应的私钥为 a.

加密:对于明文 $m\in Z_N$,在 Z_{N^2} 中选择随机数 r,按下列方式计算密文对 (A,B):

$$A=g^r \bmod N^2,\quad B=h^r(1+mN) \bmod N^2 \tag{1}$$

解密:有两种解密方式,其中一种解密方法是已知密钥 a,按下面的公式计算明文:

$$m=\frac{B/A^a-1 \bmod N^2}{N} \tag{2}$$

对于明文 m_1 和 m_2,如果使用 Bresson 密码算法对它们进行加密,那么其密文分别为 $E(m_1)=(A_1,B_1)$ 和 $E(m_2)=(A_2,B_2)$,其中:

$$A_1 = g^{r_1} \bmod N^2, \quad B_1 = h^{r_1}(1+m_1N) \bmod N^2 \tag{3}$$

$$A_2 = g^{r_2} \bmod N^2, \quad B_2 = h^{r_2}(1+m_2N) \bmod N^2 \tag{4}$$

若定义 $\otimes$ 为两个向量对应分量的乘积,即

$$E(m_1) \otimes E(m_2) = (A_1A_2, B_1B_2) \tag{5}$$

而

$$A_1A_2 = g^{r_1+r_2} \bmod N^2, B_1B_2 = h^{r_1+r_2}[1+(m_1+m_2)N] \bmod N^2 \tag{6}$$

因此

$$E(m_1) \otimes E(m_2) = E(m_1+m_2) \tag{7}$$

由此可见,Bresson 密码算法具有加同态属性.它与 El Gamal 密码算法同态性质的区别是:尽管加密 m_1 和 m_2 时选取的随机数完全不同,Bresson 算法仍具有同态性.

数字指纹既可以以加嵌入方式嵌入到原始媒体数据中,又可以以乘嵌入方式嵌入到原始媒体数据中,而乘嵌入可以看成是加嵌入的特殊形式[15,16].在原始媒体数据的时/空域或变换域,数字指纹采用加嵌入方式嵌入到原始的媒体数据中,若不考虑感知掩蔽模型,则嵌入规则为

$$y_i = x_i + w_i, i = 1,...,n \tag{8}$$

其中 $X = \{x_1, x_2,..., x_n\}$ 为选取的原始载体序列, $Y = \{y_1, y_2,..., y_n\}$ 是嵌入指纹后的载体序列, $W = \{w_1, w_2,..., w_n\}$ 为嵌入的指纹信号.由 Bresson 公钥密码算法的同态性质可知:

$$E(y_i) = E(x_i + w_i) = E(x_i) \otimes E(w_i) \tag{9}$$

2 匿名指纹方案

2.1 基本思想

提出的匿名指纹方案有 4 个参与实体:销售商(*S*)、用户(*B*)、证书机构(CA)、仲裁者(*A*).其中 CA 为可信的第三方.该方案包括初始化、指纹嵌入、跟踪与仲裁 3 个子协议.在初始化协议执行阶段,*B* 根据购买需求,以真实身份向 CA 提出申请,CA 为 *B* 生成假名,并为该次购买行为生成相应的数字指纹.然后,通过指纹嵌入协议,*S* 将指纹信息嵌入到 *B* 所购买的媒体数据中,并将带有指纹的媒体数据发送给用户.尽管由 *S* 实施指纹的嵌入操作,由于采用了同态公钥密码算法,*S* 并不知道嵌入到媒体数据中的指纹的具体内容.一旦发现了非法复制的媒体数据,即可启动跟踪与仲裁子协议,使得 *S* 在不需要第三方帮助的情况下能够找到非法分发者.如果被指控的购买用户 *B* 否认其非法分发行为,设计的匿名指纹方案使 *A* 在没有购买用户 *B* 参与的情况下,只需 *S* 提供的证据就可以作出 *B* 是否无辜的公正仲裁.

2.2 具体方案

假设参与各方具备执行协议所需的加密和解密以及签名和验证签名的能力.CA 规定了一个为参与各方认可的针对数字指纹的编码和解码规则.需要指出的是:这里可使用密码学中常规的数字签名机制,但是为了发送加密信息给用户 *B*,参与者需要使用 Bresson 密码算法对明文信息进行加密,对应于 *B* 真实身份的公钥为 (N, g, h_B).

2.2.1 初始化协议

初始化协议是用户 *B* 和证书机构 CA 之间执行的双方协议,即 *B* 向 CA 提出申请,CA 为 *B* 生成匿名身份并提供嵌入到媒体数据中的指纹.

(1) *B* 以真实身份向 CA 提交描述该次购买行为的电子订单 *text* ,以及对该电子订单的签名 $sign_B(text)$.

(2) CA 验证 *B* 对电子订单的签名,若检验失败,协议终止;否则,CA 根据 Bresson 公钥密码算法的设置选择秘密的随机数 sk_B^* ,并计算 $h_B^* = g^{sk_B^*} \bmod N^2$,同时选择 *FP* ,使得 $h_B^* \cdot FP = h_B$.

(3) CA 对 *FP* 作分组编码预处理得到 $FP' = \{fp_1, fp_2,..., fp_m\}$,其中 *m* 为分组数.选择 $R = \{r_1, r_2,..., r_m\}$ 作为加密用的随机数,以 (N, g, h_B^*) 作为 *B* 的匿名公钥 pk_B^* 对 *FP'* 的元素分别进行加密,即 $E_{pk_B^*}(FP') = \{E_{pk_B^*}(fp_1),$

$E_{pk_B^*}(fp_2),...,E_{pk_B^*}(fp_m)\}$.同时,对 R 中的元素 r_i 进行同样的编码得到 R',其中 $r_i'=\{r_{i1},r_{i2},...,r_{im}\}$.将 R' 的元素加密并与 $E_{pk_B^*}(FP')$ 级连,则

$$E_{pk_B^*}(FP'\|R')=\{E_{pk_B^*}(fp_1),E_{pk_B^*}(fp_2),...,E_{pk_B^*}(fp_m),E_{pk_B^*}(r_{11}),...,E_{pk_B^*}(r_{1m}),...,E_{pk_B^*}(r_{m1})...E_{pk_B^*}(r_{mm})\} \tag{10}$$

(4) CA 将 sk_B^*, $text$, pk_B^*, $E_{pk_B^*}(FP'\|R')$ 以及 CA 签名的 $sign_{CA}(sk_B^*)$ 和 $sign_{CA}(text, pk_B^*, E_{pk_B^*}(FP'\|R'))$ 发送给 B.

其中 pk_B^* 既是 B 的假名,同时又作为他的匿名公钥,对应的私钥为 sk_B^*;而 $FP'\|R'$ 则将被用作指纹(因为关于 FP 和 R 的编码与解码规则为指纹方案中的各方所知,因此,知道 FP 和 R 与知道 FP' 和 R' 本质上是等价的).对于每次购买行为,通过执行初始化协议,B 可获得不同的假名和相应的指纹.

2.2.2 指纹嵌入协议

(1) B 将 $text$, pk_B^*, $E_{pk_B^*}(FP'\|R')$ 和 $sign_{\mathrm{CA}}(text, pk_B^*, E_{pk_B^*}(FP'\|R'))$ 发送给 S.S 验证收到信息的真实性.如果验证通过,则继续下一步;否则,协议终止.

(2) S 产生一个用来标示该次交易的指纹 V,并由密钥控制将它嵌入到 B 将要购买的原始媒体数据 X 中,得到 $X'=X+V$.

(3) S 将置乱函数 σ 作用于 $E_{pk_B^*}(FP'\|R')$,因为对 FP' 的加密是对它的元素分别加密,所以

$$\sigma(E_{pk_B^*}(FP'\|R'))=E_{pk_B^*}(\sigma(FP'\|R')) \tag{11}$$

(4) S 用 pk_B^* 对 X' 进行加密得到 $E_{pk_B^*}(X')$,尽管 CA 已经用 B 的匿名公钥 pk_B^* 对 $FP'\|R'$ 进行了加密,S 得到的只是 $E_{pk_B^*}(FP'\|R')$,由式(9)可知,S 在加密的情况下仍可按下式完成 $\sigma(FP'\|R')$ 的嵌入:

$$E_{pk_B^*}(X'')=E_{pk_B^*}(X')\otimes\sigma(E_{pk_B^*}(FP'\|R'))=E_{pk_B^*}(X')\otimes E_{pk_B^*}(\sigma(FP'\|R'))=E_{pk_B^*}(X'+\sigma(FP'\|R')) \tag{12}$$

(5) S 将 $E_{pk_B^*}(X'')$ 发送给 B,同时以 V 为索引,将 $text$, pk_B^*, $E_{pk_B^*}(FP'\|R')$,σ和 $sign_{\mathrm{CA}}(text, pk_B^*, E_{pk_B^*}(FP'\|R'))$ 作为发行记录保存起来.

(6) B 用私钥 sk_B^* 解密 $E_{pk_B^*}(X'')$,得到加了数字指纹的媒体数据,即

$$D_{sk_B^*}(E_{pk_B^*}(X''))=X''=X'+\sigma(FP'\|R')=X+V+\sigma(FP'\|R') \tag{13}$$

2.2.3 跟踪与仲裁协议

仲裁协议是销售商 S、用户 B 和仲裁者 A 三方之间执行的协议.销售商 S 一旦发现有 X 的非法分发拷贝,便执行以下步骤:

(1) S 提取 V 和 $\sigma(FP'\|R')$.若提取失败,协议终止;否则,销售商 S 将置乱逆函数作用于 $\sigma(FP'\|R')$,获得指纹 $FP'\|R'$,对它们进行解码,得到 FP 和 R.

(2) S 以 V 作为索引,在自己的销售记录中找到对应 pk_B^*,计算 $h_B^*\cdot FP=h_B$,并由此确定公钥 (N,g,h_B) 的拥有者为非法分发用户.

当用户 B 否认他的非法分发行为时,销售商向仲裁者 A 提供 B 是非法分发者的相应证据,由 A 作出 B 是否无辜的权威性结论.为了达到这个目的,协议继续执行如下步骤:

(3) S 将盗版证据 $text$, pk_B^*, $E_{pk_B^*}(FP'\|R')$, $sign_{\mathrm{CA}}(text, pk_B^*, E_{pk_B^*}(FP'\|R'))$, FP', R', σ和 (N,g,h_B) 提交给 A.

(4) A 首先验证 $sign_{\mathrm{CA}}(text, pk_B^*, E_{pk_B^*}(FP'\|R'))$ 的有效性,然后验证由 S 提供的非法拷贝中确实存在 $\sigma(FP'\|R')$.如果条件成立,则继续下一步;否则,协议终止.

A 对 $FP'\|R'$ 进行解码得到 FP 和 R,并根据 Bresson 密码算法用 pk_B^* 和 R 对 FP' 进行加密.如果加密结果与由 CA 签名的加密结果一致,且 $y_B^*\cdot FP=h_B$ 成立,则 A 认为 B 是非法分发者;否则 A 认为 B 是无辜的.

3 安全性分析

一个匿名指纹系统对数字多媒体的购买者来讲,应该满足其购买行为的匿名和不可关联,并且销售商无法

诬陷购买者.而对销售商来讲,一旦发现有非法分发的数字作品,销售商根据该数字作品能够追踪到非法分发的用户,并且提供该用户是非法分发者的充分证据.

3.1 用户的匿名及不可关联

在给出的匿名指纹方案中,对于每次购买行为,用户 B 使用了匿名的公钥/私钥对,由于 CA 是可信的第三方,不会与销售商 S 进行合谋.根据匿名指纹协议,销售商 S 知道用户 B 的假名 pk_B^*, pk_B^* 中的 h_B^* 通过等式 $h_B^* \cdot FP = h_B$ 与 B 的非匿名公钥联系起来.尽管关于 FP 的编码和解码规则是公开的,但是已经对 FP 的编码结果 FP' 进行了加密,S 得到的只是 $E_{pk_B^*}(FP')$,由此可见,用户购买行为的匿名性能够得到保证.

另外,只要用户 B 需要购买某个数字多媒体作品,初始化协议都会被执行一次,从而为 B 产生一对用于该次交易的匿名公钥/私钥对,因此,无法通过两个数字多媒体作品来判断购买的是否属于同一个人,也就满足不可关联的要求.

3.2 销售商的安全性

如果所采用的签名体制是安全的,那么恶意的用户 B 无法修改或替换由证书机构 CA 产生的数字指纹.销售商 S 为了维护自己的利益,在数字作品中嵌入了 V 和 $\sigma(FP'\|R')$,尽管 B 能用 sk_B^* 解密 $E_{pk_B^*}(FP'\|R')$ 而获得数字指纹 $FP'\|R'$,但不能移去 $FP'\|R'$,因为他不知道由密钥控制的指纹嵌入位置,也不知道销售商对 W 进行的置乱 $\sigma(\cdot)$.电子订单 $text$ 规定了该次交易,而 $E_{pk_B^*}(FP'\|R')$ 和 pk_B^* 的绑定使用使得 B 无法利用以前申请的匿名身份或指纹对它们进行替代使之不匹配.如果 S 发现了非法分发的数字作品,那么只要提取数字指纹,他就可以追踪到非法分发的用户 B.而 B 也无法对自己的行为进行反驳,因为指纹嵌入是在加密的状态下进行的,只有用户 B 能够解密并获得带指纹的数字作品 X''.

3.3 用户的安全性

如果用户 B 并没有非法分发其所购买的媒体数据,销售商 S 为了伪造带有某一指纹 $FP'\|R'$ 的数字多媒体作品,销售商 S 要么知道 sk_B^*,以便解密 $E_{pk_B^*}(FP'\|R')$;要么 S 直接得到 B 的指纹 FP 和 R.由于证书机构 CA 是可信的第三方,而由 $E_{pk_B^*}(FP'\|R')$ 求 FP 和 R 是一个基于离散对数的难题.因而销售商 S 得不到用户 B 的指纹,也就无法伪造用户 B 所购买的多媒体作品.

另一种情况是,S 想诬陷用户 B,而 B 可能从未与 S 有过交易.S 的做法是她从公钥字典中找到用户 B 所对应的 h_B,然后她在自己保存的销售记录中任意选择匿名购买用户 B'所对应的匿名身份 $pk_{B'}^*$ 和 $E_{pk_{B'}^*}(FP'\|R')$,并由 $h_{B'}^* \cdot FP = h_B$ 计算出由她本人伪造的指纹 $FP_{B'}$.当这种情况出现时,用户 B 一定会否认这种指控,尽管他无法提供自己是无辜的证据.这必然需要仲裁者 A 作最后的裁决.Bresson 加密算法属于非确定性加密,因此 S 还需要伪造加密 FP' 所选择的随机数 R.仲裁者 A 在应用 B'的 $pk_{B'}^*$ 和伪造的 R 加密伪造的 FP' 之后,会发现结果与由 CA 签名的加密结果不一致,A 将会作出 B 是无辜的裁决.

4 结束语

本文在密码理论的最新研究成果的基础上,提出了一种基于同态公钥密码算法的匿名指纹方案.该方案既隐匿了用户的身份,又保证了嵌有指纹的数字媒体对销售商是不可见的.同时给出了具有匿名功能的公钥/私钥对的具体构造,从而使该方案在发现非法分发的拷贝的情况下,使销售商不需要第三方的帮助就能鉴别出数字多媒体的非法分发者,解决版权纠纷时也不需要购买者提供相关的秘密信息以证明自己.本文构造出的匿名指纹方案避免了常见的匿名指纹方案中,如安全多方计算或零知识证明等过于复杂的密码协议的使用,从而使协议的实现变得简单.本文提出的方案也容易与感知掩蔽模型结合,从而提高数字指纹的鲁棒性.

本文没有设立独立运行的注册机构 RA,因为在 PKI 体系结构中已经指出,可以把注册管理的职能由 CA 来完成.一个基本的事实是:协议中引入的参与实体越多,效率就越低,而且实体之间因为存在合谋的问题而使方案变得不安全.由于 CA 是可信的第三方,由此可见,本文给出的方案不存在参与实体之间的合谋问题.当然,该方案也很容易扩展到有 RA 的情况.不过,本文没有考虑多个用户之间的合谋问题,这涉及到数字指纹的纠错编码

等问题.它们本质上属于叛逆者追踪(traitor tracing)的研究范畴.我们在今后的工作中将对此作进一步的研究.

致谢 张振峰博士对本文工作提出了许多宝贵建议,在此表示感谢.同时感谢对本文工作给予支持和建议的其他同行.

References:

[1] Pfitzmann B, Waidner M. Anonymous fingerprinting. In: Walter F, ed. Eurocrypt'97. LNCS 1233, Berlin: Springer-Verlag, 1997. 88−102.

[2] Domingo-Ferrer J. Anonymous fingerprinting based on committed oblivious tranfer. In: Imai H, Zheng Y, eds. PKC'99. LNCS 1560, Berlin: Springer-Verlag, 1999. 43−52.

[3] Chung C, Choi S, Choi Y, Won D. Efficient anonymous fingerprinting of electronic information with improved automatic identification of redistributors. In: Won D, ed. Information Security and Cryptology—ICISC 2000. LNCS 2015, Berlin: Springer-Verlag, 2000. 221−234.

[4] Camenisch J. Efficient anonymous fingerprinting with group signatures. In: Okamoto T, ed. Advances in Cryptology—Asiacrypt 2000. LNCS 1976, Berlin: Springer-Verlag, 2000. 415−428.

[5] Lü SW, Wang Y, Liu ZH. Asymmetric fingerprinting. In: Proc. of the 4th China Information Hiding Workshop. Beijing: China Mechine Press, 2002. 105−111 (in Chinese).

[6] Memon N, Wong PW. A Buyer-Seller watermarking protocol. IEEE Trans. on Image Processing, 2001,10(4):643−649.

[7] Ju HS, Kim HJ, Lee DH, Lim JI. An anonymous Buyer-Seller watermarking protocol with anonymity control. In: Lee PJ, Lim CH, eds. ICISC 2002. LNCS 2587, Berlin: Springer-Verlag, 2002. 421−432.

[8] Choi JG, Sakurai K, Park JH. Does it need trusted third party? Design of Buyer-Seller watermarking protocol without trusted third party. In: Zhou J, Yung M, Han Y, eds. Applied Cryptography and Network Security 2003. LNCS 2846, Berlin: Springer-Verlag, 2003. 265−279.

[9] Goi B, Phan RC, Yang Y, Bao F, Deng RH, Siddiqi MU. Cryptanalysis of two anonymous Buyer-Seller watermarking protocols and an improvement for true anonymity. In: Jakobsson M, Yung M, Zhou J, eds. Applied Cryptography and Network Security 2004. LNCS 3089, Berlin: Springer-Verlag, 2004. 369−382.

[10] Domingo-Ferrer J. Anonymous fingerprinting of electronic information with automatic identification of redistributors. Electronics Letters, 1998,34(13):1303−1304.

[11] Mao W. Modern Cryptography: Theory and Practice. New Jersy: Pearson Education Inc., 2003.

[12] Schneinier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed., New York: John Wiley & Sons, 1996.

[13] Paillier P. Public-Key cryptosystems based on composite degree residuosity classes. In: Stern J, ed. Eurocrypt'99. LNCS 1592. Berlin: Springer-Verlag, 1999. 223−238.

[14] Bresson E, Catalano D, Pointcheval D. A simple public key cryptosystem with a double trapdoor decryption mechanism and its applications. In: Laih CS, ed. Aciacrypt 2003. LNCS 2894, Berlin: Springer-Verlag, 2003. 37−54.

[15] Langelaar G, Setyawan I, Lagendijk R. Watermarking digital image and video data. IEEE Signal Processing Magazine, 2000,17(9): 20−46.

[16] Cox I, Kilian J, Leighton T, Shammoon T. Secure spread spectrum watermarking for multimedia, IEEE Trans. on Image Processing, 1997,6(12):1673−1687.

附中文参考文献:

[5] 吕述望,王彦,刘振华.非对称数字指纹技术.见:全国第 4 届信息隐藏研讨会论文集.北京:机械工业出版社,2002.105−111.