一种基于同态公钥加密体制的匿名数字指纹方案*

孙中伟, 冯登国
(中国科学院软件所信息安全国家重点实验室, 北京 100080)

摘 要: 随着电子商务的日益普及, 如何保护数字多媒体作品的版权已成为当前迫切需要解决的问题。基于同态公钥密码体制的匿名指纹模式因为实现简单而受到人们的重视。分析了现有的基于同态公钥加密体制的数字指纹方案所存在的问题, 提出了一种基于同态公钥加密体制的匿名数字指纹方案。分析表明, 该方案具有用户的匿名及不可关联、发行商的可保证安全和用户的可保证安全等特性。

关键词: 同态公钥加密体制; 数字水印; 匿名指纹
中图分类号: O436 文献标识码: A 文章编号: 0529-6579 (2004) S2-0109-04

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, 但是随之而出现的对数字媒体的版权保护问题也日显突出。数字水印技术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, 数字指纹代表购买者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。一旦发行商发现有被非法分发的数字媒体时, 就可以根据嵌入的数字指纹找出非法分发的用户。

数字指纹技术大致可以分为三类, 即对称指纹模式、非对称指纹模式和匿名指纹模式。由于匿名指纹模式既能保护了购买者的隐私, 又能使买卖双方的权益得到保障, 因此, 它成了目前数字指纹技术的一个研究热点。自从 Pfitzmann 和 Waidner[1] 首次引入匿名指纹的概念以来, 已有许多的匿名指纹方案被提了出来[2-5]。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。例如, 基于一般的安全多方计算协议实现的匿名指纹方案就是这样。因此, 人们一直尝试利用密码算法和密码协议来设计高效实用的是数字指纹方案[6]。Memon 和 Wong 在文献[7] 中利用具有同态性质的公钥加密算法提出了一种数字作品买卖的水印 (指纹) 协议, 但该协议没有考虑用户的匿名性和用户与所买数字产品的不可关联性。针对这个问题, Ju 等人提出了一种数字作品买卖的匿名指纹协议[8]。然而, 正如 Choi 等人在文献 [9] 中所指出的那样, 这个协议容易受到合谋攻击。因此, 他们利用可交换密码体制 (commutative cryptosystem) 提出了一种不需要可信的第三方的匿名指纹协议。但是, 这个方案并没有解决合谋的问题, 而且在使用可交换密码体制时还存在漏洞。而文献 [10] 给出的方案由用户来生成指纹, Memon 和 Wong 在他们的文献中已经指出了这样作的缺点: 用户很容易去掉嵌入到数字媒体中的指纹。

1 预备知识

数字指纹的嵌入可以通过数字水印嵌入算法来完成, 它既可以加嵌入方式嵌入到原始媒体数据中, 又可以乘嵌入方式嵌入到原始媒体数据中。在原始媒体数据的时/空域或变换域, 如果数字指纹以乘嵌入方式嵌入到原始媒体数据之中, 嵌入规则为:

$$y_i = (1 + \alpha w_i)\, x_i \qquad i = 1, \cdots, N \qquad (1)$$

而以加嵌入方式嵌入到原始媒体数据之中, 则嵌入规则为:

$$y_i = x_i + \alpha w_i \qquad i = 1, \cdots, N \qquad (2)$$

其中 $X = \{x_1, x_2, \cdots, X_N\}$ 为选取的原始载体序列, $Y = \{Y_1, Y_2, \cdots, Y_N\}$ 是嵌入指纹后的系数序列, $W' = \{W_1, W_2, \cdots, W_N\}$ 为嵌入的指纹信号, α 为指纹嵌入的强度因子。

对于定义在代数结构 $(G, *)$ 上的公钥加密函数 $E: G \to R$, 如果给定 $E(x)$ 和 $E(y)$, 其中 $x, y \in$

* 收稿日期: 2004-09-11
基金项目: 国家 973 资助项目 (G1999035802); 国家杰出青年科学基金资助项目 (60025205); 国家自然科学基金资助项目 (90304007)
作者简介: 孙中伟 (1969 年和), 男, 副研究员; E-mail: sunzwcn@yahoo.com.cn

G, 在没有私钥的情况下能够计算出计算 $E(x*y)$, 则称该公钥加密系统具有同态性质。例如, RSA 公钥密码算法满足乘同态性, 即 $E(x)\cdot E(y)=E(x\cdot y)$。而 Paillier 公钥密码体制[11] 满足加同态性, 即 $E(x)+E(y)=E(x+y)$。同态公钥密码体制目前在安全投票协议、多方计算和签名等方面得到了广泛的应用。

若数字指纹采用乘嵌入方式嵌入到原始的媒体数据中, 并采用 RSA 公钥密码体制对其进行加密, 由 (1) 式可知:

$$E(y_i)=E(1+\alpha w_i)\cdot E(x_i) \tag{3}$$

若数字指纹采用加嵌入方式嵌入到原始的媒体数据中, 且采用 Paillier 公钥密码体制对其进行加密, 由 (2) 式可知:

$$E(y_i)=E(\alpha w_i)\cdot E(x_i) \tag{4}$$

2 匿名指纹方案

协议的参与实体有：发行商 (S)、用户 (B)、注册中心 (RC)、仲裁者 (A)。其中注册中心为可信的第三方。基本协议有：指纹生成协议、指纹嵌入协议、跟踪协议、仲裁协议.

我们以数字指纹采用乘嵌入的方式为例来说明我们构造的匿名指纹方案。首先给出建立匿名指纹方案的系统条件：假设存在一个鲁棒的数字指纹检测与提取算法 Det。发行商 S、用户 B 和注册机构 RA 使用 RSA 公钥密码体制来完成数字媒体的加密及解密操作, 并设嵌入强度 α 为 1。其中加密算法为 $E(\cdot)$, 解密算法 $D(\cdot)$, 他们各自拥有经过认证的 RSA 公钥/私钥对, 分别为 (sk_S, pk_S)、(sk_B, pk_B) 和 (sk_C, pk_C)。另外, 他们还拥有经过认证的签名函数 sign 和验证函数 ver, 以及与之对应的密钥对。

2.1 指纹生成协议

指纹生成协议是在用户 B 向发行商 S 和注册中心 RC 提出购买请求之后, 在用户 B 和注册中心 RC 之间执行的双方协议。

(1) 用户 B 选择自己的匿名公钥/私钥对 (sk_B^*, pk_B^*), 并生成自己拥有匿名私钥 sk_B^* 证据 pf, B 对匿名公钥 pk_B^* 和 pf 签名, 将签名结果 $\mathrm{sign}_B(pk_B^*, pf)$ pk_B^*、pf 以及 pk_B 发送给注册中心 RC, 并请求生成一个数字指纹。

(2) 注册中心 RC 首先验证用户 B 的签名 $\mathrm{sign}_B(pk_B^*, pf)$, 如果验证通过, 则 R 为用户 B 随机地生成数字指纹 $W=\{w_1, w_2, \cdots, w_N\}$; 否则, 协议终止。

(3) 注册中心 RC 用 pk_B^* 加密嵌入的指纹 W, 即

$$E_{pk_B^*}(W)=\{E_{pk_B^*}(1+w_1), E_{pk_B^*}(1+w_2), \cdots, E_{pk_B^*}(1+w_N)\}$$

并将 pk_B^* 和 $E_{pk_B^*}(W)$ 以及对它们的签名

$$s=\mathrm{sign}_{RC}(E_{pk_B^*}(W), pk_B^*)$$

发送给 B。

(4) 用户 B 验证注册中心 RC 关于签名 s 的真实性。若通过验证, 则解密 $E_{pk_B^*}(W)$ 获得指纹 W; 否则, 协议终止。

2.2 指纹嵌入协议

(1) 用户 B 将 pk_B^*、$E_{pk_B^*}(W)$ 以及注册中心的对它们的签名

$$s=\mathrm{sign}_{RC}(E_{pk_B^*}(W), pk_B^*)$$

发送给发行商 S。

(2) 发行商 S 验证 $\mathrm{sign}_{RC}(E_{pk_B^*}(W), pk_B^*)$ 的真实性。如果验证通过, 则继续下一步; 否则, 协议终止。

(3) 发行商 S 产生一个用来唯一标示与该用户交易的指纹 V, 并将它嵌入到用户 B 将要购买的原始媒体数据中 X, 得到 $X'=X+V$。

(4) 发行商 S 产生一个随机的置乱 σ 作用于用户 B 发送过来的 $E_{pk_B^*}(W)$ 上, 计算结果为

$$\sigma(E_{pk_B^*}(W))=E_{pk_B^*}(\sigma(W)) \tag{5}$$

(5) 发行商 S 将 $\sigma(W)$ 作为第二个数字指纹嵌入到 X' 中。尽管 W 已经用用户 B 的公钥 pk_B^* 进行了加密, S 得到的只是 $E_{pk_B^*}(W)$, 利用 RSA 公钥密码体制的同态性, S 在不解密 W 的情况下可按下面的计算方法完成 $\sigma(W)$ 的嵌入：

$$E_{pk_B^*}(X'')=E_{pk_B^*}(X')\cdot\sigma E_{pk_B^*}(W))=E_{pk_B^*}(X'+\sigma(W)) \tag{6}$$

(6) 发行商 S 将 $E_{pk_B^*}(X'')$ 发送给用户 B, 同时将 V、$pk_B^*(W)$、$E_{pk_B^*}(X)$、s 和 σ 作为发行记录保存起来。

(7) 用户 B 用自己的私钥解密 $E_{pk_B^*}(X'')$, 得到加了数字指纹的媒体数据, 即:

$$D_{sk_B^*}(E_{pk_B^*}(X''))=X+V+\sigma(W) \tag{7}$$

2.3 跟踪协议

发行商 S 一旦发现盗版拷贝 Z, 便利用相应的指纹提取和解码算法提取标示与用户交易的指纹 U。若提取失败, 协议终止; 否则, S 在其发行记

录中与指纹 U 最相似的 V，并找到与 V 关联的用户信息 pk_B^*、$E_{pk_B^*}(W)$、s 和 σ，将它们作为起诉非法分发用户的证据。

2.4　仲裁协议

仲裁协议由发行商 S 提出，它是发行商 S、用户 B 以及仲裁者 A 三方执行的协议，目的是仲裁者 A 证明用户 B 是数字媒体的非法分发者。

(1) 发行商 S 将盗版证据 V、pk_B^*、$E_{pk_B^*}(W)$、s 和 σ 提交给仲裁者 A，A 首先验证注册中心 RC 对 s 的签名。如果验证通过，则继续下一步；否则，协议终止。

(2) 仲裁者 A 要求用户 B 出示其数字指纹 W，并用 pk_B^* 加密 W。若加密结果与 $E_{pk_B^*}(W)$ 不符合，那么 B 提交的是一个伪造的指纹，则认为 B 是非法分发者；如果符合，则继续下一步。

(3) 仲裁者 A 根据 σ 和 W 计算 $\sigma(W)$，并检测 $\sigma(W)$ 是否存在于盗版拷贝 Z 中，若存在，则认为用户 B 是非法分发者；否则，则认为 B 是无辜的。

3　安全性分析

一个匿名指纹系统对购买数字产品的用户来讲，应该满足其购买行为的匿名和不可关联，并且发行商无法诬陷用户。而对发行商来讲，当用户在非法分发了购买的数字产品之后，发行商能根据非法分发的数字产品追踪到该用户，并且用户无法否认。同时，由于匿名指纹系统涉及多个参与实体，它还须具备合谋容忍的特点。

3.1　匿名及不可关联

用户 B 除了具有由证书认证中心 (CA) 颁发的公钥/私钥对之外，对于每次购买行为，他还生成了匿名的公钥/私钥对，而注册中心是可信的第三方，不会与发行商进行合谋，因此，用户购买行为的匿名性能够得到保证。另外，只要用户购买某个数字多媒体作品，匿名指纹协议就会为该次购买行为产生一对匿名的公钥/私钥，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　发行商的安全性

如果所采用的公钥加密算法和签名体制是安全的，那么恶意的用户无法修改或替换由注册中心产生的数字指纹。发行商 B 为了维护自己的利益，在数字作品中嵌入了 V 和 $\sigma(W)$，尽管用户知道数字指纹 W，但他不能移去 $\sigma(W)$，因为不知道发行商对 W 进行的置乱的 $\sigma(\cdot)$。如果发行商 B 发现了非法分发的数字作品，那么只要存在一个鲁棒的指纹提取算法，他就可以追踪到非法分发用户 B。而用户 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，只有用户 B 能解密并获得带指纹的数字作品 X''。另外，使用时间戳能够阻止 B 用以前的指纹替代当前的指纹。

3.3　用户的安全性

为了伪造一个带特定指纹的数字多媒体作品，发行商 S 要么知道用户 B 的私钥 sk_B^*，用以解密 $E_{pk_B^*}(W)$，而私钥 sk_B^* 只有用户 B 知道；要么 S 直接得到 B 的指纹 W，这必须通过注册中心 RC 方可实现，但是，RC 是可信的第三方，因此发行商 S 不能与 RC 合谋得到 B 的指纹 W，因此，对用户 B 来说，发行商 S 没法诬陷用户 B。

微观层次的分子动力学、宏观层次的热力学和联系这两个层次的统计力学，但在信息

4　结束语

本文给出了一种基于同态公钥加密体制的匿名数字指纹方案，该方案不仅保证了嵌有指纹的数字媒体对销售商是不可见的，同时隐匿了用户的身份。由于利用了公钥加密算法的同态性质，数字指纹在保证非对称嵌入的同时，实现相对非常简单。需要指出的是，本文没有特别强调证书认证中心 CA 的作用，可以借鉴 PKI 的结构模型，对于规模较大的匿名指纹系统，CA 与注册中心 RC 是相互独立的实体，而对于小型匿名指纹系统，CA 与 RC 可合二为一。本文没有考虑多个用户的合谋问题，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。

参考文献：

[1] PFITZMANN B, WAIDNER M. Anonymous fingerprinting [C]. Eurocrypt '97, LNCS, New York: Springer-Verlag, 1997, 1233: 88－102.

[2] DOMINGO-FERRER O. Anonymous fingerprinting of electronic information with automatic identification of redistributor[J]. Electronics Letters, 1998, 34(13): 1303－1304.

[3] CHUNG C, CHOI S, CHOI Y, et al. Efficient anonymous fingerprinting of electronic information with improved automatic identification of redistributors[C]. ICISC 2000, 2015: 221－234.

[4] CAMENISCH J. Efficient anonymous fingerprinting with group signatures. Advances in Cryptology-Asiacrypt, 2000, 1976: 415－428.

[5] KURIBAYASHI M, TANAKA H. A new anonymous

fingerprinting scheme with high enciphering rate[C]. Indocrypt, 2001, 2247: 30—39.

[6] 吕述望, 王彦, 刘振华. 非对称数字指纹技术//北京电子技术应用研究所. 全国第四届信息隐藏研讨会论文集[C]. 北京: 机械工业出版社, 2002: 105—111.

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

[8] JU H S, KIM H J, LEE D H, et al. An anonymous buyer-seller watermarking protocol with anonymity control[C]. ICISC 2002, 2587: 421—432.

[9] CHOI J G, SAKURAI K, PARK J H. Does it need trusted third party? [C]. Design of Buyer-Seller Watermarking Protocol without Trusted Third Party, Proc Applied Cryptography and Network Security 2003, 2846: 265—279.

[10] GOI B, PHAN R C W, YANG Y J, et al. Cryptanalysis of two anonymous buyer-seller watermarking protocols and an improvement for true anonymity[C]. Applied Cryptography and Network Security'2004, 2004, 3089: 369—382.

[11] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]. Eurocrypt'99, 1999, 1592: 223—238.

An Anonymous Fingerprinting Scheme Based on Homomorphic Public Key Cryptosystems

SUN Zhong wei, FENG Deng guo

(State Key Laboratory of Information Security, Institute of Software, CAS, Beijing 100080, China)

Abstract: With the widespread applications of the e-commerce, copyright protection of multimedia content being sold is a key problem to be solved. Because of their superior efficiency for practical implementation, the anonymous fingerprinting schemes based on homomorphic public key cryptosystems have attracted a lot of attentions recently. This paper presents a new type of anonymous fingerprinting scheme, which is based on homomorphic public key cryptosystems. 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: homomorphic public key cryptosystems; digital watermarking; anonymous fingerprinting