基于离散对数难解性的数字指纹体制

何少芳

(湖南农业大学 理学院信息科学系,湖南 长沙 410128)

摘 要:利用线性方程组解的结构,基于离散对数问题的难解性构造了一种数字指纹体制。将要发行的拷贝使用对称密码体制加密,而用户解密含有加密后拷贝的加密数据组使用的密钥是线性方程组的解向量,因此方案具有较好的实现效率。通过引入完全可信的第三方,不仅增加了用户的安全性,还能帮助发行商确定性地跟踪叛逆者。

关键词:解密密钥;离散对数;数字签名;数字指纹

中图分类号:TP309 **文献标识码**:A **文章编号**:1674-7720(2011)05-0075-02

Digital fingerprinting scheme based on discrete logarithm

He Shaofang

(Information Science Department of Science College, Hunan Agricultural University, Changsha 410128, China)

Abstract: This paper uses the structure of linear equations' solutions present a digital fingerprinting scheme based on discrete logarithm. It uses symmetric encryption to encrypt the copy that will be published, and custom uses solution vector of linear equations to decrypt coded data which has encrypted copy, so the scheme has rather efficient in implementing. By introducing authentic third party, it increases the safety of customs, and helps data distributor to trace traitor determinately.

Key words: decryption keys; discrete logarithm; digital sign; digital fingerprinting

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。数字水印是将相同的标识嵌入到同一个电子数据中,而数字指纹是将不同的标识嵌入到同一个电子数据中,数字指纹代表与用户(购买者)或与该次购买过程有关的信息。当发行商发现有被非法分发的授权信息时,可根据其中所嵌入的指纹信息追踪找出非法用户。但是,传统的对称数字指纹体制[1-2]不能对非法分发者的行为进行确定,因为发行商也可以分发带有某用户指纹的拷贝以对该用户进行陷害。针对此问题,Pfitzmann 和 SchunterDI[3]引入了非对称指纹的概念,当获得了非法拷贝时,发行商可以跟踪找出非法分发者并能向审判者提供证据。本文基于离散对数问题的难解性[4]构造了一种数字指纹体制,由于该体制对将发行的拷贝采用的是对称密码体制中的加解密算法,而用户用于解密数据组的密钥,是由系统给出的线性方程组的解向量,因此具有较好的实现效率。另外,本方案引入了完全可信的第三方指纹分发中心,用户的解密密钥以及嵌入拷贝中的数字指纹均由可信第三方提供,发行商和任一其他用户都无法陷害无辜用户,增加了用户的安全性。

1 基本方案描述

协议的参与实体有:发行商(M)、用户(B)、指纹分发中心(FIC)、法官(J)。基本协议有:初始化协议、带指纹拷贝生成(即指纹嵌入)协议、跟踪协议、审判协议。使用的密码学原语有:对称密码体制、数字签名体制。

1.1 初始化协议

所有实体产生经过认证的公钥和私钥对以及相应的数字签名机制,如用户 B 的密钥对为 pk_B, sk_B,相应的签名和验证函数为 $sign_{sk^*}, ver_{pk^*}$,并且公开他们相应的公钥和签名验证函数,各个实体之间的少量秘密信息传递可以通过该公钥密码体制进行。

系统随机选择两个大素数 p 和 q,$q|p-1$,g 为 Z_p 上阶为 q 的单位原根,即 $g^q \equiv 1 \bmod p$,再随机选择一个非素数 N,N 满足 $g^q \equiv 1 \bmod N$,随机生成一个线性方程组,设方程组为:

$$\begin{cases} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n\equiv b_1 \bmod q \\ a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n\equiv b_2 \bmod q \\ \vdots \\ a_{m1}x_1+a_{m2}x_2+\cdots+a_{mn}x_n\equiv b_m \times \bmod q \end{cases} \tag{1}$$

其中 $m<n$，$\boldsymbol{A}=(a_{ij})_{m\times n}$ 为方程组的系数矩阵，$\boldsymbol{A}$ 的秩为 m，又设方程组的基础解系为 $\alpha_1,\alpha_2,\cdots,\alpha_{n-m}$，特解为 β，则方程组的全部解可表示为：

$$\gamma_i=(\lambda_{i1}\alpha_1+\lambda_{i2}\alpha_2+\cdots+\lambda_{i,n-m}\alpha_{n-m}+\beta)\bmod q,\{\lambda_{i1},\cdots,\lambda_{i,n-m}\}\subset Z_q \tag{2}$$

$i=1,2,\cdots$，令 $\gamma_i=(\gamma_{i1},\gamma_{i2},\cdots,\gamma_{in})$，显然有 $\{\gamma_{i1},\gamma_{i2},\cdots,\gamma_{in}\}\subset Z_q$。

$e=(N,g,y,h_1,h_2,\cdots,h_n)=(N,g,(g^{b_1},g^{a_{11}},\cdots,g^{a_{1n}})\bmod N)$，其中线性方程组系统保密，$q$ 只对发行商公开，p 和全部解向量只对第三方指纹分发中心公开，g、N 和 e 对所有实体都公开。

1.2 指纹嵌入协议

(1)用户 B 向发行商 M 和指纹分发中心 FIC 提出购买申请，并提交自己经过认证的公钥，同时 B 随机选择一个小于 q 的正整数 i，自己保存 i，并将 i 签名得到 $sig_B(i)$，将签名用 FIC 的公钥加密成 $pk_{FIC}(i,sig_B(i))$，将其发送给 FIC。

(2)FIC 收到 $pk_{FIC}(i,sig_B(i))$ 后先将其用私钥解密，得到 i 及 $sig_B(i)$，检验 B 的签名，若通过，则为 B 随机选择一个解向量 $\boldsymbol{\gamma}=(\gamma_1,\gamma_2,\cdots,\gamma_n)$ 作为 B 的解密密钥。FIC 对所选择的解向量先用 B 的公钥加密，然后签名，将其秘密发送给 B，并记录 $\text{text}=(i\parallel sig_B(i)\parallel(g^i\parallel g^{\gamma_1}\parallel g^{\gamma_2}\parallel\cdots\parallel g^{\gamma_n})\bmod p)$。最后，FIC 将 $((g^i\parallel g^{\gamma_1}\parallel g^{\gamma_2}\parallel\cdots\parallel g^{\gamma_n})\bmod p)$ 经过签名后发送给 M。

(3)M 收到 FIC 经过签名的 $((g^i\parallel g^{\gamma_1}\parallel g^{\gamma_2}\parallel\cdots\parallel g^{\gamma_n})\bmod p)$，先检验签名，若通过，则 $((g^i\parallel g^{\gamma_1}\parallel g^{\gamma_2}\parallel\cdots\parallel g^{\gamma_n})\bmod p)$ 将作为指纹嵌入到将要发售给 B 的拷贝 P 中。M 随机为 B 选择 $s\in_R Z_q^*$ 作为加密带指纹的拷贝所使用的对称密钥，$r\in_R Z_q^*$，$-r$ 为 r 关于 q 的加法逆元，将加密数据组 $(N,(sy^{-r},h_1^r,h_2^r,\cdots,h_n^r)\bmod N,E_s(P))$ 用 B 的公钥加密，然后对其签名，发送给 B。

(4)B 收到发行商发来的消息，先检验 M 的签名，若通过，则将消息用私钥解密得到加密数据组 $(N,(sy^{-r},h_1^r,h_2^r,\cdots,h_n^r)\bmod N,E_s(P))$，结合使用 FIC 发来的解密密钥 $\boldsymbol{\gamma}=(\gamma_1,\gamma_2,\cdots,\gamma_n)$，通过计算 $sy^{-1}\bmod N\prod_{i=1}^{n}h_i^{r\cdot\gamma_i}\bmod N$ 得到对称密钥 s，再由 $D_s(E_s(P))=P$ 得到带指纹的拷贝 P。

1.3 跟踪协议

M 若发现非法拷贝 P_{found}，执行相应的跟踪算法，从该拷贝中提取指纹，若提不出，则协议终止；否则提取出某一指纹 $((g^i\parallel g^{\gamma_1}\parallel g^{\gamma_2}\parallel\cdots\parallel g^{\gamma_n})\bmod p)$，M 将该数字指纹提交给 FIC，申请协助跟踪。FIC 收到申请后，查询记录，找到与数字指纹相对应的记录 $\text{text}=(i\parallel sig_B(i)\parallel(g^i\parallel g^{\gamma_1}\parallel g^{\gamma_2}\parallel\cdots\parallel g^{\gamma_n})\bmod p)$，由此确定非法者为 B。

1.4 审判协议

M 和 FIC 将指纹 $((g^i\parallel g^{\gamma_1}\parallel g^{\gamma_2}\parallel\cdots\parallel g^{\gamma_n})\bmod p)$ 以及相对应的记录 $\text{text}=(i\parallel sig_B(i)\parallel(g^i\parallel g^{\gamma_1}\parallel g^{\gamma_2}\parallel\cdots\parallel g^{\gamma_n})\bmod p)$ 作为证据提交法官 J 用以 pk_B 相应的函数 ver_{pk_B} 验证 $sig_B(i)$ 是否为 B 对 i 的签名。若是，则认为 B 是非法分发者；否则认为 B 是无辜的。

2 正确性及安全性分析

2.1 正确性分析

命题 用户 B 能用收到的解密密钥 $\boldsymbol{\gamma}=(\gamma_1,\gamma_2,\cdots,\gamma_n)$ 将加密数据组 $(N,(sy^{-r},h_1^r,h_2^r,\cdots,h_n^r)\bmod N,E_s(P))$ 解密，通过计算得到带指纹的拷贝 P。

证明：解密密钥 $\boldsymbol{\gamma}=(\gamma_1,\gamma_2,\cdots,\gamma_n)$ 是线性方程组的一个解向量，因此有 $a_{i1}\gamma_1+a_{i2}\gamma_2+\cdots+a_{in}\gamma_n\equiv b_i \bmod q$，即 $\sum_{i=1}^{n}a_{ii}\gamma_i=kq+b_1,k\in Z^+$，又 $e=(N,g,y,h_1,h_2,\cdots,h_n)=(N,g,(g^{b_1},g^{a_{11}},\cdots,g^{a_{1n}})\bmod N)$，则：

$$\prod_{i=1}^{n}h_i^{r\cdot\gamma_i}\bmod N=\prod_{i=1}^{n}g^{a_{ii}r\cdot\gamma_i}\bmod N=g^{r\cdot\sum_{i=1}^{n}a_{ii}\cdot\gamma_i}\bmod N=$$

$$g^{r\cdot(kq+b_1)}\bmod N=(g^q)^{kr}\cdot g^{rb_1}\bmod N=y^r\bmod N$$

$$sy^{-r}\bmod N\cdot y^r\bmod N=sy^{-r}y^r\bmod N=s,D_s(E_s(P))=P$$

2.2 安全性分析

(1)发行商 M 的安全性

带拷贝的加密数据组是 M 使用 B 的公钥加密，经过签名后发送给 B，第三方指纹分发中心得不到带指纹的拷贝，避免了第三方非法使用拷贝，降低了发行商的风险。

(2)用户 B 的安全性

B 的解密密钥对 M 和其他用户都是不可见的（即不知道用户的解密密钥），系统对线性方程组保密，M 和其他用户也无法从其他途径得到解向量；数字指纹中含有 $(g^i\bmod p)$，其中 i 是用户随机选择并保存的正整数，p 只对指纹分发中心公开，因此，M 和其他用户无法伪造数字指纹陷害无辜用户。

(3)第三方指纹分发中心的安全性

本方案建立在第三方指纹分发中心完全可信的基础上。指纹产生所需的 p 及解密密钥对指纹分发中心都公开，只有带指纹的拷贝对指纹分发中心保密，若第三方指纹分发中心得到了带指纹的拷贝并将其非法使用，则发行商和用户都会有很大的风险。因此，第三方指纹分发中心必须是完全可信的。

本文基于离散对数问题的难解性构造了一种数字指纹体制。由于该体制主要采用的是对称密码体制中的

加解密算法，而对称密钥由发行商随机选取；用户用于解密数据组的密钥，即系统随机生成的线性方程组的解向量，计算简便，具有较好的实现效率。拷贝中的数字指纹由用户和可信第三方指纹分发中心确定，使得发行商和其他用户无法陷害无辜用户，增加了用户的安全性。值得注意的是，本方案要求第三方指纹分发中心必须完全可信，否则发行商和用户都有风险。

参考文献

[1] BLAKLEY G R, MEADOWS C, PRUDY C B. Finger-printing long forgiving messages [A]. Williams Hugh C ed. Advances in Cryptogogy-CRYPTO'85 [C]. Berlin: Springer, 1985.

[2] BONEH D, SHAW J. Collusion-secure fingerprinting for digital data [J]. IEEE Trans. On Inform. Theory, 1997(44): 1897-1905.

[3] PFITZMANN B, SCHUNTER M. Asymmetric finger-printing [A]. Ueli M Maurer ed. Advances in Cryptology - EUROCRYPT' 96[C]. Berlin: Springer 1996.

[4] 胡向东，魏琴芳.应用密码学教程[M].北京：电子工业出版社，2007.

(收稿日期：2010-08-04)

作者简介：

何少芳，女，1980年生，讲师，硕士，主要研究方向：信息安全。