一种基于中国剩余定理的数字指纹体制

何少芳

(湖南农业大学 理学院信息科学系,湖南 长沙 410128)

摘 要：数字指纹技术可以追踪盗版拷贝的来源,在版权保护方面具有很重要的作用,受到越来越广泛的关注。本文提出了一种基于中国剩余定理的数字指纹体制,避免使用一般的安全多方计算协议,该方案不仅具有较好的实现效率,而且还能确定性地跟踪叛逆者。

关键词：数字指纹;中国剩余定理;叛逆者追踪

中图分类号：TP309 **文献标识码**：A

A digital fingerprinting scheme based on Chinese remainder theorem

HE Shao-Fang

(Information Science department of Science College, Hunan Agriculture University, Changsha 410128, China)

Abstract: Digital fingerprinting is a technology used to trace illegal redistributors and protect copyright, and has been get more and more attention. This paper presents a fingerprinting scheme based on Chinese remainder theorem. That avoids using the general multiparty computations protocol. Furthermore, the scheme not only has efficiency in implementing, but also allows deterministic traitor tracing.

Key words: digital fingerprinting; Chinese remainder theorem; traitor tracing

随着整个社会数字化程度的提高以及网络的发展,越来越多的图像和视频信息以数字化的形式影响着人们的生活。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,可以根据其中所嵌的指纹信息追踪出非法用户。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 Schunter[3]引入了非对称指纹的概念。当获得了非法拷贝时,发行商可以跟踪出非法分发者并能向审判者提供证据,此概念一经提出便引起了研究者的广泛关注。为避免使用一般的安全多方计算协议,本文提出了一种基于中国剩余定理的数字指纹体制,该方案不仅具有较好的实现效率,而且还能确定性地跟踪叛逆者。

* 基金项目:湖南农业大学校青年科学基金项目(编号:08QN11)

1 背景知识

定理 1:中国剩余定理[4]

设自然数 $n_1, n_2, \cdots, n_k$ 两两互素,记 $N=n_1\times n_2\times\cdots n_k$, $r_1, r_2, \cdots, r_k$ 是正整数,则同余方程组

$$\{x\equiv r_i \bmod n_i\} \quad i=1,2,\cdots,k$$

在模 M 同余的意义下有惟一解

$$x\equiv\sum_{i=1}^{k} r_i N_i y_i \bmod M$$

其中,$N_i=N/n_i$;$N_i y_i\equiv 1 \bmod n_i$, $i=1,2,\cdots,k$

定理 2:同余式组 $\{x\equiv r_i \bmod n_i\}$ $i=1,2,\cdots,k$ 有解,当且仅当 $\gcd(n_i,n_j)$ 能整除 r_i-r_j,对任意 (i,j) $(1\leqslant i<j\leqslant k)$;且该解在模 $N=\mathrm{lcm}(n_1,n_2,\cdots,n_k)$ 下惟一,并可由中国剩余定理给出。其中 $\gcd(\cdots)$ 表示最大公约数,$\mathrm{lcm}(\cdots)$ 表示最小公倍数。

定理 3:设 $N=n_1\times n_2\times\cdots n_k$ 是奇素数的乘积,令 $\lambda(N)=\mathrm{lcm}(\phi(n_1),\phi(n_2),\cdots,\phi(n_k))$ 设 $r_i(i=1,2,\cdots k)$ 是模 n_i 的一个本原根,则同余式组 $\{x\equiv r_i \bmod n_i\}$, $i=1,2,\cdots,k$ 的解

就产生 1 个阶为 $\lambda(N)$的整数 g。

定理 4：已知 $d_1, d_2, \cdots, d_v, \gcd(n_i-1, n_j-1)$能整除 d_i-d_j，则存在 $d_H \equiv \sum d_i N_i y_i \bmod N$，其中 $i=1,2,\cdots,v$，$N=\mathrm{lcm}(n_1-1, n_2-1, \cdots, n_v-1)$，$N_i=N/n_i-1$，$N_i y_i \equiv 1 \bmod n_i-1$。

定义 计算性 Diffie-Hellman 假设：给定 g, g^x, g^y，不存在概率多项式时间算法能够在多项式时间内以不可忽略的概率计算 g^{xy}。

2 基本方案描述

协议的参与实体有：发行商(M)、用户(B)(在指纹嵌入协议中，第 i 个用户称为用户 i)、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。

2.1 初始化协议

系统参数产生，假定系统参数由指纹分发中心产生，l 是安全参数，k 是系统用户的总数，每个用户 i 秘密选择 1 个 l 比特的素数 $n_i=2q_i+1$，q_i 是 1 个奇素数。不妨假设 $n_1<n_2<\cdots n_k$，记 $N=n_1\times n_2\times \cdots n_k$。所要嵌入的指纹是 Z_{n_1} 中的元素，选取 g 是满足定理 3 中同余式组中的解。

2.2 指纹嵌入协议

(1)首先 i 向 M 和 FIC 提出购买申请，i 秘密选择 1 个 l 比特的素数 $n_i=2q_i+1$，q_i 是 1 个奇素数，并随机选择个人解密密钥 $d_i \in Z^*_{n_i}$，然后向 FIC 发送 (β_i, n_i)，其中 $\beta_i \equiv g^{d_i} \bmod n_i$，FIC 计算 $\beta \equiv \sum_{i=1}^{k} \beta_i N_i y_i \bmod N$，其中 $N_i=N/n_i$，且 $N_i y_i \equiv 1 \bmod n_i (1 \leqslant i \leqslant k)$。则 (g, β, N)是公开的加密密钥，$\beta \equiv \beta_i \bmod n_i$

(2)M 收到 FIC 发来的(g, β, N)，假设 M 将要发送给 i 有用拷贝中含明文 $x \in Z_{n_1}$，M 在 $\{0, 1, 2, \cdots, n_1-1\}$中随机选取 r，计算 $z_1 \equiv g^r \bmod N$，$z_2 \equiv x\beta^r \bmod N$，得到密文 $C=(z_1, z_2)$，将 C 嵌入拷贝中作为 i 的指纹，M 将带用户指纹的拷贝发送给 i。

(3)i 得到密文 C 以后，利用个人解密密钥 $d_i \in Z^*_{n_i}$解密，$x \equiv z_2 (z_1^{d_i})^{-1} \bmod n_i$，得到明文 x，这样就得到含明文 x 的有用拷贝。

2.3 跟踪协议

若发现盗版拷贝，M 将其中的 d_H 和 N_H 提取出来，保存(d_H, N_H)作为证据。反之，对于不能打开的盗版拷贝，则可利用黑盒跟踪算法找出盗版者。

2.4 审判协议

M 将 (d_H, N_H) 提交给 J，J 检验 $N_H \equiv 0 \bmod n_i$ 是否成立，若成立则判定 i 参与了盗版，否则认为 i 是无辜的。

3 正确性及安全性分析

(1)正确性分析

命题：在指纹嵌入协议(3)中，i 得到密文 C，利用个人解密密钥匙 $d_i \in Z^*_{n_i}$ 计算 $x \equiv z_2 (z_1^{d_i})^{-1} \bmod n_i$，得到发行商嵌入的明文 x。

证明：已知 $\beta_i \equiv g^{d_i} \bmod n_i$，$\beta \equiv \beta_i \bmod n_i$，$z_1 \equiv g^r \bmod N$，

$$\begin{aligned} z_2 &\equiv x\beta^r \bmod N \\ &\equiv x\beta_i^r (\bmod n_i) \bmod N \\ &\equiv x(g^{d_i})^r (\bmod n_i) \bmod N \\ &\equiv x(g^r)^{d_i} (\bmod n_i) \bmod N \\ &\equiv x(g^r \bmod N)^{d_i} \bmod n_i \\ &\equiv x z_1^{d_i} \bmod n_i \end{aligned}$$

因此，有 $x \equiv z_2 (z_1^{d_i})^{-1} \bmod n_i$

(2)安全性分析

因为 g 是模 $n_i (i=1,2,\cdots,k)$的 1 个公共本原根，g 的阶为 $\lambda(N)=2q_1q_2\cdots q_k$，于是由 g 生成 Z_N^* 的子群 H，H 的阶为 $\lambda(N)$，并且 H 的阶必然包括 1 个不小于 q_1 的素因子，而 $q_1^{1/2}$ 又是充分大的。因而易证明在计算的 Diffie-Hellman 假设下，该方案在被动攻击时是安全的，同时也具有较好的增删用户的灵活性。但是由定理 4 可知，t 个合法授权用户的合谋可以利用同余式组 $g^{d_H} \equiv g^{d_i} \bmod n_i$，$i=1,2,\cdots,t$，由其解密密钥 $d_1, d_2, \cdots, d_t$ 来伪造新的解密密钥 d_H，该方案不能抵抗线性组合合谋攻击，但可以由追踪算法识别出参与盗版者。

本文基于中国剩余定理构造了一种数字指纹体制，由于该体制主要采用的是同余式定理进行加密解密运算，因此具有较好的实现效率，且该方案还具有可确实性地跟踪叛逆者的优点。

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, 1985:180-189.

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

[3] PFITZMANN B, SCHUNTER M. Asymmetric finger-printing [A]. Ueli M Maurer ed. Advances in Cryptology-EUROCRYPT' 96[C]. Berlin: Springer 1996:84-95.

[4] 胡向东，魏琴芳.应用密码学[M].北京：电子工业出版社，2006.

(收稿日期：2009-07-13)