一种无第三方参与的匿名指纹方案

王青龙, 杨 波
(北京交通大学计算机与信息技术学院, 北京 100044)

摘 要: 基于类 ElGamal 加密体制, 本文提出了一种无第三方参与的匿名数字指纹方案. 在无第三方参与的情况下, 该方案巧妙实现了销售商对匿名用户的身份认证, 确保了只有合法注册用户才能得到数字产品; 同时, 销售商在收缴到盗版拷贝时, 无须用户的参与就能够追踪出真正的盗版者. 此外, 方案还具备不可联系性, 防诬陷性. 方案的安全是基于解离散对数为困难问题.

关键词: 匿名指纹; 版权保护; 认证; 追踪
中图分类号: TP911.22 文献标识码: A 文章编号: 0372-2112 (2005) 11-2063-03

Anonymous Fingerprinting Scheme Without Third Party

WANG Qing-long, YANG Bo
(*Computer and information technology institute, Beijing Jiaotong University, Beijing* 100044, *China*)

Abstract: Based on the cryptosystem of ElGamal-like, this paper presents a new anonymous fingerprinting scheme without third party. Without involving any third party, this scheme helps merchants to verify the identity of anonymous buyers in order that only buyers registered can get the digital product. At the same time, merchants can trace back to the real pirate from a confiscated illegal copy without the buyer's participation. Moreover, this scheme has the properties of unlinkable and frame-proofing. The safety of this scheme is based on the intractable problem of solving Discrete Logarithm.

Key words: anonymous fingerprinting; copyright protection; certification; tracing

1 引言

近年来, 随着 Internet 的快速普及, 电子商务的发展也日新月异, 包括数字音频, 视频, 文件等在内的各种数字信息产品越来越多的通过网络销售与传播. 一方面, 网络为数字信息产品的发布提供了高效, 快捷的新途径, 为创作者和销售商提供了新的机遇; 另一方面, 数字化信息产品也很容易被非法复制与重传, 从而对信息所有者和销售商的权益造成侵害. 如何对数字化信息进行版权保护已经成为信息时代产权保护的核心问题, 也是当前得到广泛研究的一个热门问题.

数字水印技术是版权保护中的一个重要分支, 通过在所销售的拷贝中嵌入与创作者有关的特定信息来到达保护版权的目的, 数字水印技术可以用来证明一个数字产品的原始版权所有者是谁, 但是不能够追踪出非法拷贝与传播者; 数字指纹是数字版权保护中的另一个重要分支, 通过在所销售的拷贝中嵌入与购买者有关的特定信息(称为数字指纹), 销售商可以在收缴到盗版拷贝时对非法拷贝者进行追踪. 数字指纹可以分为三类: 对称数字指纹方案[1,2] (symmetric fingerprinting schemes); 非对称数字指纹方案[3] (asymmetric fingerprinting schemes); 匿名数字指纹方案[4~12] (anonymous fingerprinting schemes). 其中对称指纹方案不能提供不可否认性, 非对称方案虽能实现不可否认性, 但是不能隐藏购买者的身份信息, 即购买者的身份信息能够被销售商获得. 为解决此问题, 文献[4]首次提出了匿名指纹方案. 匿名指纹方案[4~12]虽然在实现方法上有所不同, 有的是基于群签字[7,9], 有的是基于双线性 Diffie-Hellman 假设[8], 有的是基于不经意传输[10], 但是它们的共同点是在实现上都需要第三方的参与, 第三方的作用是为用户颁发公钥证书及在销售商提取出盗版拷贝中的指纹后恢复出盗版者的真实身份. 文献[11]是基于数字水印的匿名指纹方案, 该方案中的第三方虽是不需要可信的, 但仍然需要第三方参与. 文献[12]是基于 Okamoto-Uchiyama 加密体制的方案, 其中没有提到第三方, 但是它假定用户事先已经获得了第三方颁发的证书, 因此一定程度上该方案也没有完全排除第三方的参与.

本文提出一种基于类 ElGamal 加密算法的匿名数字指纹方案, 与已有方案相比, 本方案的执行不需要任何第三方的参与, 减少了执行过程. 此外, 本方案满足不可联系性, 即销售商不能从已发生的诸多交易中识别出哪些是属于同一个购买者所为.

2 方案叙述

2.1 系统参数设置

设 p 是一个大素数, 并且 $p-1$ 有一个大素数因子 q, g 为 Z_p 上的生成元. 这样在 p 中计算以 g 为底的离散对数被认

收稿日期: 2004-10-08; 修回日期: 2005-06-10
基金项目: 国家自然科学基金(No. 60372046); 现代通信国家重点实验室基金(No. 51436040204DZ0102)

为是困难问题. p 予以公开. 销售商(M)在 Z_p 上秘密选一个 k 次多项式 $f(x)=\sum_{i=0}^{k}a_ix^i$. 称 $f(x)$ 上对应的一个点$(i,f(i))$, $i\in Z_p\setminus\{0\}$ 为一个份额. 设 $\Phi=\{(i\|f(i))\mid i\in Z_p\setminus\{0\}\}$ 为已注册用户集合, 且 Φ 满足对任意 $i\neq j$ 有 $f(i)\neq f(j)$. 除非特别说明, 本方案的所有算术运算都在 Z_p 上.

2.2 注册过程

当一个新用户 B 申请注册时, M 随机选一个没有被使用的份额$(i,f(i))$传送过去作为 B 拥有的份额. 销售商记录 $text=i\|f(i)\|B$. 并进行更新 $\Phi=\Phi\cup\{(i\|f(i)\}$. 用户保存自己获得的份额$(i,f(i))$.

2.3 订购与指纹协议

设销售商已对所有要销售的数字产品进行了编号以及对应的内容说明, 用户可通过查阅内容说明来购买自己需要的产品.

当用户 B_i(拥有的份额为$(i,f(i))$)欲从销售商处购买编号为 N 的数字产品 $item$ 时, 任选 $A\in_R Z_p\setminus\{0\}$, 执行以下协议过程

Step1 计算 $g^A, g^{Af(i)}$, 发送订购单 $g^A\|g^{Af(i)}\|N$ 给 M.

Step2 销售商任选 $r_1, r_2, \cdots, r_n, r'_1, r'_2, \cdots, r'_n$, 计算 $T_j=(g^A)^{r_j}$, $T'_j=(g^{Af(i)})^{r'_j}$, $j=1,2,\cdots,n$. M 将全部的 T_j, T'_j, $j=1,\cdots,n$, 按随机顺序排列(如排列顺序为 $T_{j_1}T_{j_2}\cdots T_{j_n}T'_{i_1}T'_{i_2}\cdots T'_{i_n}$, $j_l,i_l\in\{1,2,\cdots,n\}$, $l=1,2,\cdots,n$ 这种形式则不用, 只需重新排列即可), 不妨设排列的顺序为 $I=T_1T'_1T_2T'_2\cdots T_nT'_n$, 则 M 发送 $\Psi=T_1\|T'_1\|T_2\|T'_2\|\cdots\|T_n\|T'_n$ 给 B_i.

Step3 B_i 按顺序分别计算 $(T_1)^{f(i)}, (T'_1)^{f^2(i)}, (T_2)^{f^3(i)}, \cdots, (T'_n)^{f^{2n}(i)}$, 发送 $\Delta=(T_1)^{f(i)}\|(T'_1)^{f^2(i)}\|(T'_1)^{f^2(i)}\|(T_2)^{f^3(i)}\|\cdots\|(T'_n)^{f^{2n}(i)}$ 给销售商 M.

Step4 M 把 I 中所有相邻顺序为 $T'_j\|T_l, j,l\in\{1,2,\cdots,n\}$ 形式的部分提取出来, 如本例 I 中可以提取的部分有 T'_1T_2, $T'_2T_3, \cdots, T'_{n-1}T_n$. 按照提取出的部分, M 分别对相应 Δ 中的项计算(以 T'_1T_2 部分为例): $((T'_1)^{f^2(i)})^{r'^{-1}_1}, ((T_2)^{f^3(i)})^{r_2^{-1}}$ 其中 r'^{-1}_j, r_j^{-1}, $j=1,\cdots n$ 满足 $r'_j\cdot r'^{-1}_j=1 \bmod (p-1)$, $r_j^{-1}\cdot r_j=1 \bmod (p-1)$, 验证两项计算结果是否相等, 因为有 $((T'_1)^{f^2(i)})^{r'^{-1}_1}=g^{Ar'^{-1}_1r'_1f^3(i)}=g^{Af^3(i)(K(p-1)+1)}=g^{Af^3(i)K(p-1)}\cdot g^{Af^3(i)}=(g^{p-1})^{KAf^3(i)}\cdot g^{Af^3(i)}=g^{Af^3(i)}$, $((T_2)^{f^3(i)})^{r_2^{-1}}=g^{Ar_2\cdot f^3(i)r_2^{-1}}=g^{Af^3(i)}$. 如果所有提取部分都通过相等的验证, M 进行下一步; 如果有提取部分没有通过验证, M 就中止协议执行.

Step5 M 任选 $r\in_R Z_p\setminus\{0\}$, 再在 $f(x)$ 上任选 k 个没有分配给用户的份额 $(x_1,f(x_1)), (x_2,f(x_2)), \cdots, (x_k,f(x_k))$, 即 $(x_j,f(x_j))\notin\Phi, j=1,2,\cdots,k$. M 利用接收到的 $g^A\|g^{Af(i)}$ 计算 $(g^A)^{f(x_j)}, j=1,2,\cdots,k$ 和 $(g^{Af(i)})^r$, 发送 $x_1\|g^{Arf(x_1)}\|x_2\|g^{Arf(x_2)}\|\cdots\|x_k\|g^{Arf(x_k)}\|g^{Arf(i)}$ 给 B_i.

Step6 利用收到的 k 组数据 $(x_j,g^{Arf(x_j)}), j=1,2\cdots,k$, 再加上 B_i 可以得到的第 $k+1$ 个数据 $(i,g^{Arf(i)})$, B_i 利用 Lagrange 插值法可以求得 $g^{Arf(0)}$ 并发送给 M, 具体公式为 $g^{Arf(0)}=\prod_{j=1}^{k+1}g^{Ar\lambda_jf(x_j)}$, $\lambda_j=\prod_{0\leqslant l\neq j\leqslant k+1}\frac{x_l}{x_l-x_j}$, 其中 $x_{k+1}=i, f(x_{k+1})=f(i)$.

Step7 M 利用接收的 g^A 计算 $g^{Arf(0)}=g^{Ara_0}$, 并与 B_i 发送来的 $g^{Arf(0)}$ 相比较, 若不相等, 则 M 中止协议的执行; 若相等则 M 采用经典指纹嵌入算法 $Fing(\cdot)$ 将 emb 嵌入 N 与对应的数字产品 $item$ 中, 得 $item^*=Fing(item, emb)$, 其中 $emb=g^A\|g^{Af(i)}$. 把嵌有指纹的 $item^*$ 发送给 B_i. 完成整个协议过程.

2.4 追踪算法

销售商 M 一旦收缴到非法拷贝的产品 $item^*$, 只需从中提取出所嵌入的指纹 $emb=g^A\|g^{Af(i)}$, 对所有记录 $j\|f(j)\in\Phi$, 计算 $g^{Af(i)}$ 并与 emb 中的 $g^{Af(i)}$ 比较, 若相等则对应 $text=i\|f(i)\|B$ 中的 B 就是真正的盗版者.

3 安全分析

3.1 用户匿名安全

销售商要想从订购单 $g^A\|g^{Af(i)}\|N$ 中获取代表用户身份的信息 $f(i)$, 其困难性相当于破解离散对数困难问题, 因此用户的匿名是有安全保证的. 同时销售商因为不知道 $f(i)$ 也就无法陷害诚实用户, 即方案具有防诬陷性和不可否认性.

3.2 不可联系性

由于用户在每次订购产品时选取的 $A\in_R Z_p\setminus\{0\}$ 是随机的, 因此销售商要从已保存的订购单中辨别出属于同一个用户的不同订购单同样面临求解离散对数困难问题.

3.3 销售商的安全

假如用户 B_i 发送给 M 的订购单形式为 $emb=g^{A_1}\|g^{A_2f(i)}$, $A_1\neq A_2$, 则 B_i 不能通过前述 step4 的验证. 设 B_i 随即找一对 $x, x^{-1}\in Z_p\setminus\{0\}$ 满足 $x\cdot x^{-1}=1 \bmod (p-1)$, 发送 $g^{A_1}\|g^{A_1\cdot x\cdot f(i)}$ 给 M. 但是由于 M 用随机数 r_j, r'_j 分别对 $g^{A_1}, g^{A_1xf(i)}$ 的加密, B_i 不能从得到的 Ψ 中识别出哪些数据是由 $g^{A_1xf(i)}$ 得来的, 哪些是由 g^{A_1} 得来的, 因此没办法利用 x^{-1} 正确对 Ψ 中形式为 $(g^{A_1xf(i)})^{r'_j}$ 的项进行 $((g^{A_1xf(i)})^{r'_j})^{x^{-1}}$ 运算, 当 n 的大小选取适当时, B_i 通过 2.3 中 step4 验证的概率可忽略不计(设 $n=20$, 如 I 中有三个提取部分, 则 B_i 正确找到全部对应项的概率为 $(1/40)^3$). 又 step5, step6, step7 确保了 B_i 拥有的份额是真实有效的. 因此销售商的安全也是有保证的.

4 结论

本文提出的匿名数字指纹方案在没有可信第三方的参与下, 保证了用户的认证与销售商的追踪. 与已有方案相比较, 有效降低了执行协议时的复杂过程, 既保护了用户的个人信息也保证了销售商的权益.

参考文献:

[1] D Boneh, J Shaw. Collusion secure fingerprinting for digital data[A]. Advances in Cryptology-crypto' 1995[C]. LNCS 963, Berlin: Springer verlag, 1995. 452-465.

[2] W Trappe, M Wu, K J R Liu. Collusion resistant fingerprinting

for multimedia[J]. IEEE International Conference on Acoustics, Speech, and Signal Processing. 2002, 14: 3309- 3312.

[3] B Pfitzmann, M Schunter. Asymmetric fingerprinting[A]. Eurocrypt 96[C]. LNCS 1070, Berlin: Springer verlag, 1996. 84 - 95.

[4] B Pfitzmann, M Waidner. Anonymous fingerprinting[A]. Advances in cryptoloty-Eurocrypt 1997[C]. LNCS 1233, Berlin: Springer verlag, 1997. 88- 102.

[5] C Chung, S Choi, Y Choi, D Won. Efficient anonymous fingerprinting of electronic information with improved automatic identification of redistributors[A]. ICISC 2000[C]. LNCS 2015, Berlin: Springer-verlag, 2001. 221- 234.

[6] J Domingo-Ferrer. Anonymous fingerprinting of electronic information with automatic identification redistributors[J]. IEE Electronics Letters, 1998, 43(13): 1303- 1304.

[7] J Camenisch. Efficient anonymous fingerprinting with group signatures[A]. Advances incryptology-Aisacrypt 2000[C]. LNCS 1976, Berlin: Springer verlag, 2000. 415- 428.

[8] Myungsum Kim, Jongseong Kim, Kwangjo Kim. Anonymous fingerprinting as secure as the Bilinear Diffie-Hellman Assumption[A]. Proceedings of ICICS 2002[C]. LNCS 2513, Berlin: Springer Verlag, 2002. 97- 108.

[9] Popescu C. Applications of group signatures to anonymous fingerprinting schemes[A]. Video/ Image processing and multimedia communications 4th Eurasip-IEEE Region 8 International Symposium on VIProm Com[C]. Zadar, Croatia; Croatian Society Electronics in Marine-ELMAR, 2002. 177- 182.

[10] J Domingo-Ferrer. Anonymous fingerprinting based on committec oblivious transfer[A]. PKC 1999[C]. LNCS 1560, Springer verlag, 1999. 43- 52.

[11] Jae-Gwi Choi, Kouichi Sakurai, Ji-Hwanpark. Does It Need Trusted Third Party? Design of Buyer-Seller Watermarking Protocol without Trusted Third Party[A]. Applied Cryptography and Networking Security[C]. LNCS 2846, Springer Verlag, Heidelberg, 2003. 265- 279.

[12] Minoru Kuribayashi, Hatsukazu Tanaka. A New Anonymous Fingerprinting Scheme with High Enciphering Rate[A]. Proceeding of the second international conference on cryptology in India[C]. 2001. 30- 39.

作者简介:

王青龙　男, 1970 年生, 山西新绛人, 北京交通大学博士研究生.
E-mail: wangqinglong2002@ hotmail. com.

杨　波　男, 1963 年出生, 北京交通大学教授、博士生导师, 主要从事信息安全、网络安全、电子商务领域的研究.