维普资讯 http://www.cqvip.com

一种基于群签名的匿名数字指纹方案*)

谭示崇　王育民

(西安电子科技大学 综合业务网国家重点实验室　西安 710071)

摘　要　匿名数字指纹使用户可以在不向发行商泄露身份的情况下购买数字产品，而且，一旦发行商发现非法分发的拷贝，他仍然可以获得该非法用户的身份并起诉该用户。群签名允许任意一个群成员代表群进行匿名签名，如果发生争执，群管理员能够打开签名来揭示签名者的真实身份。本文基于一个安全的能抵抗联合攻击的群签名方案构造了一个匿名数字指纹方案。

关键词　匿名指纹，群签名，可撤销匿名性，数字产品

An Anonymous Fingerprinting Scheme Based on Group Signature

TAN Shi-Chong　WANG Yu-Min

(State Key Lab. of Integrated Services Networks, Xidian Univ., Xi'an 710071)

Abstract　An anonymous fingerprinting scheme allows a buyer to purchase digital goods without revealing her identity to the merchant. However, as soon as the merchant finds a sold version that has been illegally distributed, he is able to retrieve a buyer's identity and take her to court. A group signature scheme allows a group member to sign messages anonymously on behalf of the group. However, in case of a dispute, the identity of a signature's originator can be revealed only by a designated entity. In this paper, a new anonymous fingerprinting scheme based on group signature is proposed.

Keywords　Anonymous fingerprinting, Group signature schemes, Revocable anonymity, Digital goods

1　引言

随着多媒体技术和计算机网络的快速发展和广泛应用，对文本、图像、音频、视频、软件等数字产品的版权保护已经成为急需解决的问题。数字指纹技术是一种保护版权的技术，其核心思想是发行商向每个用户出售相互间存在细微差别的拷贝，以此来区别不同的用户。一般来说，数字指纹代表用户(购买者)或与该购买过程相关的信息。当发行商发现被非法分发的拷贝时，他可以根据其中所嵌的指纹来追踪出非法用户。在对称数字指纹方案[1,2]中，发行商知道用户获得的是哪个拷贝，他可以分发某个用户购买的拷贝并诬陷该用户，但他无法证明是该用户而不是他自己分发该拷贝。为了解决这个问题，Pfitzmann 和 Schunter[3] 提出了非对称指纹，在非对称指纹方案下，嵌入指纹的拷贝对发行商是不可见的，因此发行商一旦获得了某个非法拷贝，他就可以追踪出非法用户，并且能够向仲裁者提供证据证明正是该用户非法分发了该拷贝。

为了保护用户的隐私，为用户提供匿名性，Pfitzmann 和 Waidner 提出了匿名非对称数字指纹[4]。在该方案下，用户购买数字产品时不必向发行商泄露自己的身份，而且，只要用户不非法分发他所购买的拷贝，则他一直都是匿名的。更准确地说，发行商只有获得非法分发的拷贝之后，才能揭示对应用户的身份。近年来，人们对匿名指纹方案进行大量的研究[6~11]。Pfitzmann 和 Sadeghi[10] 提出了一个高效的匿名指纹方案，但该方案有两个缺点：1. 用户进行每次交易前都必须在注册中心注册一次；2. 发行商必须与注册中心合作才能恢复出非法用户的身份。为了克服这两个缺点，Camenisch[7] 提出了利用群签名来构造匿名指纹的框架。

本文将一个高效的安全的群签名方案[5]中的群管理员拆分为成员管理员和撤销管理员，并利用它来构造一个匿名非对称指纹方案。在本文的方案中，用户对一个描述交易的消息产生一个群签名，与普通的群签名方案不同的是，这里没有固定的撤销管理员。用户选择一个公钥和私钥对，该公钥用于产生群签名，而私钥被嵌入到用户所购买的数字产品中。这样，发行商一旦找到某个非法分发的拷贝，他就提取出私钥，充当该群签名的撤销管理员，从而可以恢复出该非法用户的身份。根据群签名方案的性质可知：每个用户只需注册一次(注册相当于加入群中)，而且发行商能够直接恢复出非法用户的身份而不必求助于注册中心。因此，本文的方案克服了文献[10]中的方案的两个缺点。

2　新的匿名数字指纹方案

将文献[5]中的群签名方案中的群管理员拆分为成员管理员和撤销管理员，并利用该群签名来构造一个新的匿名非对称指纹方案。在我们的方案中，匿名数字指纹方案中的注册中心充当群签名中的成员管理员。在注册中心注册的用户就成为群签名方案的群的成员，即群由所有的已注册的用户组成。当某个用户要购买数字产品 P_0 时，他首先执行群签名方案的撤销管理员的密钥产生协议，获得一个密钥对(x_R，y_R)。然后，该用户利用群签名方案对描述交易的订购单进

*)基金项目：国家自然科学基金资助项目(60473072)。谭示崇　博士生，主要研究方向为密码学理论，电子商务。王育民　教授，博士生导师，主要研究方向为信息论，密码，编码。

维普资讯 http://www.cqvip.com

行签名，其中 y_R 作为撤销管理员的公钥。最后，发行商和用户执行非对称的指纹嵌入协议，使得 x_R 嵌入用户购买的拷贝中。此后，一旦发行商发现一个非法分发的拷贝，他就提取出 x_R，这使得他成为利用 y_R 产生的群签名的撤销管理员，因此他能够撤销该用户的匿名性并确定他的身份。

本方案有四个参与者：用户(B)，发行商(M)，注册中心(RC)和仲裁者(J)，方案由五个子协议组成：注册中心的密钥分发，用户注册协议，指纹嵌入协议，鉴别协议和审判协议。

令(Emb,Re c)表示一个嵌入协议和一个提取算法，Com代表一个承诺方案。

方案的系统参数：设 $H:\{0,1\}^* \to \{0,1\}^k$ 是一个无碰撞的 hash 函数。设 $\varepsilon>1$，k 和 ℓ_p 为安全参数，定义两个整数区间 $\Delta=[2^{\lambda_1}-2^{\lambda_2},2^{\lambda_1}+2^{\lambda_2}]$，$\Gamma=[2^{\gamma_1}-2^{\gamma_2},2^{\gamma_1}+2^{\gamma_2}]$，这里 $\lambda_1>\varepsilon(\lambda_2+k)+2$，$\lambda_2>4\ell_p$，$\gamma_1>\varepsilon(\gamma_2+k)+2$，$\gamma_2>\lambda_1+2$。

2.1 注册中心的密钥分发

(1)RC 随机地秘密选择 ℓ_p 比特的素数 p'，q' 使得 $p=2p'+1$，$q=2q'+1$ 为素数。令 $n=pq$；

(2)RC 随机选择 $a,a_0,g,h\in_R QR(n)$；

(3)RC 的公钥为：$Y=(n,a,a_0,g,h)$，RC 的私钥为：$S(p',q')$。

2.2 用户注册协议

假定用户与注册中心之间的信道是安全的，注册过程如下：

(1)用户 B 产生一个秘密值 $\tilde{x_i}\in[0,2^{\lambda_2}]$，一个随机整数 $\tilde{r}\in[0,n^2]$，计算 $C_1=g^{\tilde{x_i}}h^{\tilde{r}} \bmod n$，B 把 C_1 发送给 RC 并向 RC 证明他知道 C_1 以 g 和 h 为底；

(2)RC 检查 $C_1\in QR(n)$。如果是，则 RC 随机选择 α_i 和 $\beta_i\in[0,2^{\lambda_2}]$并发送给 B；

(3)B 计算 $x_i=2^{\lambda_1}+(\alpha_i\tilde{x_i}+\beta_i \bmod 2^{\lambda_2})$，把 $C_2=a^{x_i} \bmod n$ 发送给 RC。B 向 RC 证明：

Ⅰ. C_2 对 a 的离散对数在 Δ 内；

Ⅱ. 知道 u,v,w 使得①u 在$[-2^{\lambda_2},2^{\lambda_2}]$内，②$u$ 等于 $C_2/a^{2^{\lambda_1}}$ 对 a 的离散对数；

Ⅲ. $C_1^{\alpha_i}g^{\beta_i}$ 等于 $g^u(g^{2^{\lambda_2}})^v h^w$；

(4)RC 检查 $C_2\in QR(n)$。如果是，而且上述证明正确，则 RC 随机选择一个素数 $e_i\in\Gamma$，计算 $A_i:=(C_2a_0)^{1/e_i} \bmod n$。RC 将新的成员证书$[A_i,e_i]$发送 给 B；

(5)B 验证 $a^{x_i}a_0=A_i^{e_i} \bmod n$。

RC 将 B 的成员证书$[A_i,e_i]$和 B 的真实身份 ID_B 保存起来。B 保存他的成员证书$[A_i,e_i]$。

2.3 指纹嵌入协议

令 $m\{0,1\}^*$ 为描述该次交易的订购单。用户 B 随机地秘密选择 $x\in Z_{p'q'}$，并计算 $y=g^x \bmod n$。B 对 $m\in\{0,1\}^*$ 的签名过程如下：

(1)产生一个随机数 $w\in_R\{0,1\}^{2\ell_p}$，计算 $T_1=A_iy^w \bmod n$，$T_2=g^w \bmod n$，$T_3=g^{e_i}h^w \bmod n$。

(2)随机选择 $r_1\in\pm\{0,1\}^{\varepsilon(\gamma_2+k)}$，$r_2\in\pm\{0,1\}^{\varepsilon(\lambda_2+k)}$，$r_3\in\pm\{0,1\}^{\varepsilon(\gamma_1+2\ell_p+k+1)}$ 和 $r_4\in\pm\{0,1\}^{\varepsilon(2\ell_p+k)}$，计算

$d_1=T_1^{r_1}/(a^{r_2}y^{r_3})$，$d_2=T_2^{r_1}/g^{r_3}$，$d_3=g^{r_4}$，$d_4=g^{r_1}h^{r_4}$，

$c=H(g\|h\|y\|a_0\|a\|T_1\|T_2\|T_3\|d_1\|d_2\|d_3\|d_4\|m)$，

$s_1=r_1-c(e_i-2^{\gamma_1})$，$s_2=r_2-c(x_i-2^{\lambda_1})$，$s_3=r_3-ce_iw$，$s_4=r_4-cw$

(3)输出$(c,s_1,s_2,s_3,s_4,T_1,T_2,T_3)$。

B 将签名 $\sigma=(c,s_1,s_2,s_3,s_4,T_1,T_2,T_3)$，$y$ 和 $Com(x)$发送给发行商 M。而且，B 向 M 证明 $Com(x)$确实是对与 y 对应的秘密钥的承诺。

M 对签名 σ 的验证过程如下：

(1)计算：

$c'=H(g\|h\|y\|a_0\|a\|T_1\|T_2\|T_3\|a_0^{s_1}T_1^{1-c2^{\gamma_1}}/(a^{s_2-c2^{\lambda_1}}y^{s_3}) \bmod n\|T_1^{s_1-c2^{\gamma_1}}/g^{s_3} \bmod n\|T_2^{s_1}g^{s_4} \bmod n\|T_3^{s_1}g^{s_1-c2^{\gamma_1}}h^{s_4} \bmod n\|m)$

(2)当且仅当 $c=c'$，$s_1\in\pm\{0,1\}^{\varepsilon(\gamma_2+k)+1}$，$s_2\in\pm\{0,1\}^{\varepsilon(\lambda_2+k)+1}$，$s_3\in\pm\{0,1\}^{\varepsilon(\lambda_1+2\ell_p+k+1)+1}$，$s_4\in\pm\{0,1\}^{\varepsilon(2\ell_p+k)+1}$ 时，接受签名。

如果签名 σ 有效，那么 B 和 M 执行协议 Emb，M 输入 P_0 和 y，B 输入 x 和 y，协议 Emb 结束后，B 就获得 P_0 的一个拷贝 P_B。

2.4 鉴别协议

当 M 发现数字产品 P_0 的一个非法拷贝 $\overline{P}$ 时，他利用指纹提取方案 Rec 从 $\overline{P}$ 中提取 x，这使得 M 充当了群签名方案中的撤销管理员。M 计算出 y，并在他的数据库中搜索出相应的群签名 σ。接着，M 利用验证算法验证 σ 的有效性，计算出 $A_i=T_1/T_2^x$ 从而恢复出 B 的身份 ID_B。最后，M 证明 $\log_g^y=\log_{T_2}(T_1/A_i) \bmod n$。

2.5 审判协议

M 将证据 $proof=(x,y,A_i,ID_B)$发送给仲裁者 J，这时，J 可以充当群签名方案的撤销管理员，并尝试重复 M 在鉴别协议中的鉴别过程，如果能重复，则 J 确信 B 就是非法拷贝 $\overline{P}$ 的分发者从而可以起诉 B。

3 安全性分析

(1)正确性。当验证者检验一个签名时，一个合法的群成员按照签名算法产生的群签名一定能够通过验证算法。

(2)匿名性和不相关性。在交易中，发行商所获得的所有信息就是用户对描述该次交易的订购单的群签名。根据协议 Emb 的特性，发行商无法获得与 y 对应的秘密钥 x 的任何信息。除了知道 x 的一方，该群签名对其他任何人都具有匿名性和不相关性，因此交易是匿名的和不相关的。

(3)对无辜用户的保护。为了诬陷一个无辜的用户，多个用户的勾结或与注册中心的勾结必须产生一个与他们选择的某个公开钥 y' 对应的群签名，或者生成一个嵌有该用户的秘密钥 x 的拷贝。由于该群签名具有不可伪造性和抗联合攻击性，而且协议 Emb 具有零知识特性，因此本文的匿名指纹方案能抵抗这两种攻击。

(4)可追踪性和抗合谋。假设协议 Emb 能抵抗合谋，则发行商能够获得某个合谋者的秘密钥，知道了某个用户的秘密钥使得发行商可以充当群签名方案中的撤销管理员，因此他可以获得该成员即用户的身份。

结束语 数字指纹协议为解决数字产品的盗版问题提供了可行的技术。本文基于一个安全的抗联合攻击的群签名方案，构造了一个匿名数字指纹方案，该方案的主要优点是用户只需注册一次，而且发行商不必求助于注册中心就可以确定非法用户的身份。

(下转第 82 页)

维普资讯 http://www.cqvip.com

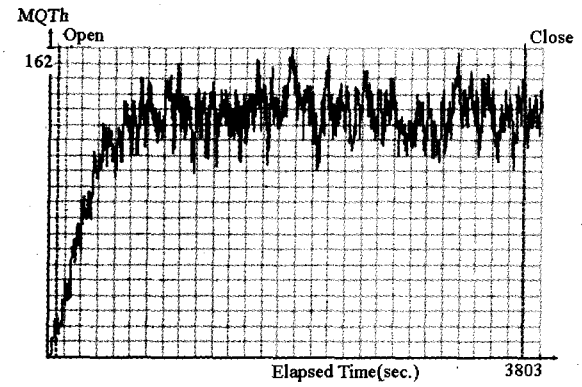

图 13　不加载复制服务器运行 3600s

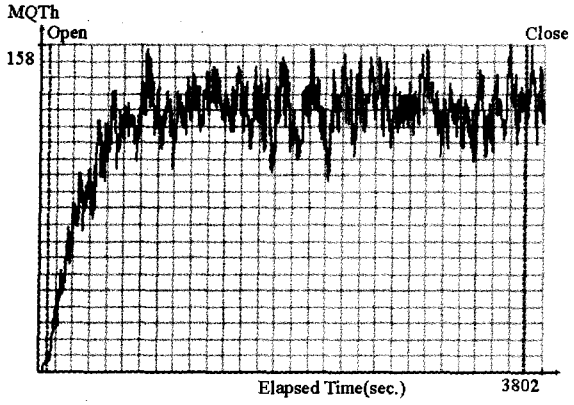

图 14　加载复制服务器运行 3600s

	不加载复制服务器	加载复制服务器
MQTH	122.1 tpmC	121.2 tpmC
Total Completed	7325	7277

从上面的测试数据可以看出，10 个 Warehouse 远没有达到压力的上限，两个测试都顺利地通过(在第二个测试中，从库的数据也得到了正确准时的同步)。虽然使用复制服务器要在主库上定义、执行 Trigger、存储过程等一些操作，对主库的性能带来了一定的影响，使得测试中总的提交事务相对少了一些，反应时间也较不加载时稍长，但是总体来说，主库在使用复制服务器的情况下性能稳定，可用性强。

结论　本文从实际应用的角度出发，为大型数据库系统设计并实现了一种基于虚拟日志的(由触发器触发生成)的高性能/高可用性的复制解决方案。该复制方案采用一主多从模式(Single Master，Multi Slaves)，使用异步分发技术，实行延迟远程存取和延迟传播技术对数据进行更新，提供跨平台支持。

同时，我们针对国产大型数据库系统 KingbaseES 具体实现了该复制方案，从而提供了一个现实的、可扩展的复制系统框架。

由于采用触发器机制捕捉主库的数据更新，而主流的数据库系统均支持触发器，因此该方案并不依赖于特定的数据库，可以方便地实现对异源数据的复制支持，具备良好的扩展性。针对不同的数据库系统，如果作为主库，需要根据该数据库的特点进行触发器的定义并实现相应的快照扫描接口；如果作为从库，需要定制相应的更新应用程序接口。目前，我们也已经成功地实现了主库对 Oracle、SQL Server 等异源数据库的复制。

在实际的测试中，复制服务器也表现出了优异的稳定性和可靠性，能够很好地与数据库系统配合，提供稳定高效的数据复制解决方案，具有准时复制、响应时间短等优点，在及时同步业务数据、灾难备份恢复，改善决策支持系统等许多关键服务中有很高的应用前景。

参 考 文 献

1　Oracle. Replication with Oracle Streams[M/OL]. June 2002. 3～10
2　Oracle. Oracle9i Database Online Documentation (Release 2 (9.2)) Advanced Replication[M/DK]. Part Number A96567-01, 2002
3　MicroSoft. SQL Server 2000 联机丛书[M/DK]. 2000 复制部分
4　Rodolphe M, Silvia C, Joji J, et al. IBM Replication Solutions for Pervasive Computing with DB2 Everyplace and DB2 Satellite Edition[M/OL]. ibm. com/redbooks, April 2001
5　Shirai T, Crompton G, Priest V. Migrating to the IBM Replication Solution[M/OL]. ibm. com/redbooks, February 2001
6　Gu Li-jun, Budd L I, Cayci A, et al. A Practical Guide to DB2 UDB Data Replication V8[M/OL]. ibm. com/redbooks, December 2002
7　Sybase. Replication Server 管理指南[M]. 2000. 1～44
8　Sybase. Replication Server 参考手册[M]. 2000. 415～426
9　BaseSoft. Kingbase ES V4.0 程序员参考手册[M]. 2004
10　石骁翀 . Oracle 8 高级数据复制技术[N/OL]. 2001-03-28. http://www0. ccidnet. com/tech/guide/2001/03/28/58_1900. html

(上接第 57 页)

参 考 文 献

1　Blakley G R, Meadows C, Purdy G B. Fingerprinting Long Forgiving Messages. Crypto'85, LNCS218, Springer-Verlag, Berlin, 1986. 180～189
2　Boneh D, Shaw J. Collusion-Secure Fingerprinting for Digital Data. Crypto'95, LNCS963, Springer-Verlag, Berlin, 1995. 452～465
3　Pfitzmann B, Schunter M. Asymmetric Fingerprinting. Eurocrypt'96, LNCS1070, Springer-Verlag, Berlin, 1996. 84～95
4　Pfitzmann B, Waidner M. Anonymous Fingerprinting. Eurocrypt'97, LNCS1233, Springer-Verlag, Berlin, 1997. 88～102
5　Ateniese G, Camenisch J, Joye M, Tsukik G. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. Crypto2000, LNCS 1880, Springer-Verlag, Berlin, 2000. 255～270
6　Wang Yan, Lü Shuwang, Liu Zhenhua. A Simple Anonymous Fingerprinting Scheme Based on Blind Signature. ICICS2003, LNCS2836, Springer-Verlag, Berlin, 2003. 260～268
7　Camenisch J. Efficient Anonymous Fingerprinting with Group Signatures. ASIACRYPT2000, LNCS1976, Springer-Verlag, Berlin, 2000. 425～428
8　Domingo-Ferrer J, Herrera-Joancomarti J. Efficient Smart-card Based Anonymous Fingerprinting. Smart Card Research and Advanced Application-CARDIS'98. Springer-Verlag, Berlin, 1998. 221～228
9　Domingo-Ferrer. J. Anonymous Fingerprinting Based on Committed Oblivious Transfer. Public Key Cryptography'99, LNCS1560, Springer-Verlag, Berlin, 1999. 43～52
10　Pfitzmann B, Sadeghi A R. Coin-Based Anonymous Fingerprinting. Eurocrypt'99, LNCS1592, Springer-Verlag, Berlin, 1999. 150～164
11　李勇，杨波，华翔. 一种高效匿名的数字指纹方案[J]. 西安电子科技大学学报，2003，30(3)：394～398