文章编号:1001 - 9081(2005)02 - 0381 - 02

基于 RSA 签名的安全数字时间戳方案

张亚玲,禹 勇,王晓峰,王铁英
(西安理工大学 计算机科学与工程学院,陕西 西安 710048)
(genuine66@21cn.com)

摘 要:已存在的时间戳机制没有解决服务付费问题,即客户在请求时间戳服务机构给他的文档 Hash 值加盖时间戳时,应该如何向时间戳服务机构支付费用。介绍了已经存在的时间戳机制,基于盲数字签名,提出了一个解决问题的新方案,该方案引入了一个售票实体,解决了服务付费问题,并且基于 RSA 数字签名,构造了一个完整的时间戳系统。

关键词:时间戳;盲签名
中图分类号: TP309 **文献标识码**:A

New scheme for digital time-stamping based on signature

ZHANG Ya-ling, YU Yong, WANG Xiao-feng, WANG Tie-ying
(Institute of Computer Science and Engineering, Xi'an University of Technology, Xi'an Shannxi 710048, China)

Abstract: Billing service question is not solved in the existing time-stamp schemes. In other words, how the time-stamping Service will bill the service to its customers when they ask it for a Digital time-stamping. This article described the existing time-stamping schemes, based on blind signature, a new scheme solving the problem was presented. In the new scheme an issuing entity of tickets is introduced to solve billing service question. Based on RSA signature, an integrated time-stamping system was constructed in this article.

Key words: digital time-stamping; blind signature

0 引言

随着网络的发展,电子文档的使用越来越频繁。为了保证电子文档的合法性和完整性,电子文档也应该像普通文档一样,可以认证和签名。使用一个数字签名方案时,一个签名者的密钥可能被他人偷走,此时,对签名者在他人偷走密钥之前所做的签名的真实性会受到影响。出现这种情况的主要原因是没有办法确定一个消息签名的时间,解决问题的一个办法是使用安全数字时间戳。时间戳可以证明在某一给定的时间之前某一数字文档是否被创建或签名[1-2]。时间戳协议[3]和时间戳机制[4]都没有考虑服务付费问题。服务付费就是客户在请求时间戳服务机构加盖时间戳时,应该如何向时间戳服务机构支付一定的费用,这是时间戳执行过程中一个很重要的问题。本文基于 RSA 盲数字签名,构造了一个完整的安全数字时间戳系统。

1 时间戳机制

1.1 简单时间戳机制

签名者 B 自己可以产生一个可信的时间戳。B 首先获得目前公开可获得的某一信息,该信息在产生之前不可预测。例如,这种信息可由前一天的某种股票交易额构成,将这个信息记为 pub。现在假定 B 想时戳对消息 x 的签名,h 是一个公开的 Hash 函数。B 产生时间戳的方法如下:

1) B 计算 $z = h(x)$;

2) B 计算 $\tilde{z} = h(z \| pub)$;

3) B 计算 $y = Sig_B(\tilde{z})$;

4) B 在第二天的新闻报纸上公布(z, pub, y)。

信息 pub 的存在意味着 B 在所谈到的日期之前不能产生 y。将 y 公布在第二天的新闻报纸上这一事实证明了 B 在所谈到的日期之后不能计算 y。所以 B 的签名 y 被限制在周期为一天范围内。在这种方法中,B 没有泄漏 x,只公开 z。必要时,B 能证明 x 是他所签的消息。这种机制有很大的局限性,并不实用。目前,存在两种类型的时间戳机制,一种是存在一个可信任第三方(TSA)的时间戳机制,另一种是分布式信任机制。基于分布式信任的机制把信任分发给一组人。在基于 TSA 信任的机制中,B 产生时间戳的过程更改为:B 先计算 $z = h(x)$ 和 $y = Sig_B(\tilde{z})$,然后将(z, y) 发给 TSA。TSA 级联日期 D 并对 (z, y, D) 签名。但是仍然存在一个重要问题 —— 信任问题:TSA 有可能受贿而加盖不真实的时间。

TSA 的信任问题可以采用下面介绍的时间戳机制来解决。还需要考虑的一个问题是文档如何接受日期和时间的认证。认证分为绝对认证和相对认证:绝对认证包含的是真实的日期和时间的信息,相对认证包含的信息仅仅说明了一个

收稿日期:2004 - 07 - 19;**修订日期**:2004 - 10 - 18
基金项目:国家自然科学基金资助项目(60273089);陕西省自然科学研究计划资助项目(03JK165)
作者简介:张亚玲(1966 -),女,陕西风翔人,副教授,博士,主要研究方向:网络安全、办公自动化系统; 禹勇(1980 -),男,山东泰安人,硕士研究生,研究方向:数字签名理论及 XML 安全; 王晓峰(1966 -),女,河南新乡人,副教授,主要研究方向:密码学与网络安全; 王铁英(1980 -),男,江苏徐州人,硕士研究生,主要研究方向:VPN 技术与网络安全.

文档是否在另一个文档加盖时间戳之前加盖了时间戳。这两种认证机制都可以用于时间戳文档,但是绝对认证机制的前提是时间戳服务机构是完全可信任的实体。对于相对认证机制来说,可信任的实体不是必需的。因此,即使有时候时间戳服务机构怀有恶意,有些机制也可以保证文档能够用正确的日期和时间加盖时间戳。下面介绍几个相对时间戳认证机制[4,5]。

1.2 链接机制

链接机制的目的是能够尽量降低"完全信任 TSA"这一条件。时间戳服务机构应用 Hash 函数 H 把已提交的所有文档的 Hash 值链接成一个串。链接机制包含三个阶段:

1) 聚合。在这一阶段,把 TSA 在一个小的时间段(聚合周期)内收到的所有文档认为是同时的,聚合算法的输出是一个二进制串,它依赖于在该聚合周期内所提交的所有文档的 Hash 值。聚合是为了减轻服务器的负担。当然,如果服务器的处理能力足够强大,可以不聚合。

2) 链接。把第 n 个聚合周期的输出结果链接到第 $n-1$ 个聚合周期的输出结果。如果没有前一聚合周期的结果,那么这一聚合周期的结果就无法计算。如此以来,在聚合周期的输出结果之间就建立了一个单向关系,这样就得到了所谓的相对临时认证:不同聚合周期的结果值之间可以相互区分开。因此,在链接机制中,具体的时间值有时候不是必需的。

3) 公布。TSA 不时地通过媒体(比如新闻报纸)来公布最近发布过的时间戳。人们可以用已经公布的值来验证时间戳,其他人也可以用已经公布的值来检验 TSA 是否有欺骗行为。

为了获得机密性要求,时间戳服务机构可以用一个 Hash 函数 H 把所有提交的文档的 Hash 值链接成一个串。在这种情况下,第 n 个文档 H_n 的时戳 s 是:

$s = Sig_{TSA}(n, t_n, ID_n, H_n, L_n)$,其中 Sig_{TSA} 是时间戳服务的数字签名,t_n 是当前文档的日期,ID_n 是第 n 个文档的标识,H_n 是第 n 个文档的 Hash 值,I_n 是链接信息:$L_n = (t_{n-1}, ID_{n-1}, H_{n-1}, H(L_{n-1}))$,其中,$t_{n-1}$ 和 ID_{n-1} 分别表示前一个文档的时间和文档标识,H_{n-1} 是前一个文档的 Hash 值,L_{n-1} 是前一个文档的链接信息。图 1 给出了 8 个元素链接时的结构。

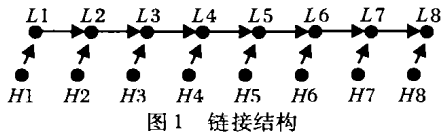

图 1 链接结构

用这种方法,时间戳服务机构把当前时间戳和前一个时间戳链接在一起,从而得到了一个无限的时间戳序列,解决了纠纷问题:因为时间戳服务可以识别是否一个文档在另一个文档加盖时间戳之前加盖了时间戳。

1.3 树机制

树机制是链接机制的普遍化机制,这个机制把时间戳链分解成很多小单元,每个单元称为轮。在每一轮,客户可以向时戳服务提出时戳请求。这个过程通过创建一棵树来实现,其中叶子是时戳请求,节点值通过一个安全的 Hash 函数 F 来计算。

客户在第 r 轮发送 Hash 值 y_n 给时间戳服务机构,树的叶子就是由这些 y_n 构成的,树的每个节点 k 被命名为 $F_k = (F_{kL}, F_{kR})$,其中 kL 和 kR 分别是节点 k 的左右孩子。创建树的起点是在该轮中提交给时间戳服务的文档 Hash 值,利用这些 Hash 值和 Hash 函数 F 两两计算每个节点的值,如图 2 所示。其中 p 是树层次索引,$y_n^{(p)}$ 是通过函数 F 计算得到的每个节点的值:$y_n^p = F(y_{r(2i)}^{p-1}, y_{r(2i+1)}^{p-1})$,$l$ 是每一层的最大索引:$l = [(n+1)div2p] - 1$。

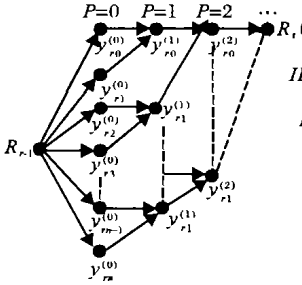

图 2 树机制

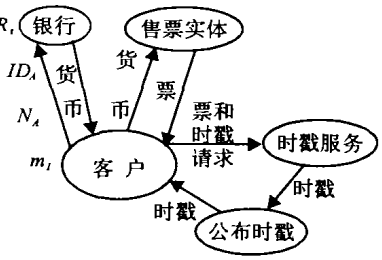

图 3 新方案加盖时间戳的全过程

2 基于 RSA 签名的时间戳方案

在新方案中,添加了一个售票实体解决了服务付费问题。加盖时间戳的整个过程如图 3 所示。

2.1 售票过程

客户在要求时间戳服务加盖时间戳之前,必须先从售票实体处购票。购票过程由 2 个协议构成:提取协议(客户从银行提取货币的协议)和支付售票协议(客户向售票实体付款、售票实体给客户发票的协议)。下面我们构造一种在线方案:

银行 B 选择两个大素数 p_B 和 q_B,以及一个 Hash 函数 f,令 $n_B = p_B q_B$,并选择 e_B 使得 e_B 和 $\varphi(n_B) = (p_B - 1)(q_B - 1)$ 互素,由 $e_B d_B = 1 \bmod \varphi(n_B)$ 求出 d_B。银行公开 n_B, e_B, f_B,秘密保存 p_B, q_B 和 d_B。银行 B 首先制定货币的单位,对任何消息 m 约定 $f(m)$ 的 e_B 次根价值 s 个货币单位。

提取协议: 客户 A 随机选择 $m, r \in Z_n^*$,计算 $m_1 = f_B(m) r^e$,客户 A 获得银行 B 的公钥 (e_B, n_B),并用 e_B 对 $m_c = (ID_A, N_A, m_1)$ 加密,计算 $c = m_c^{e_B} \bmod \varphi(n_B)$,其中 ID_A 和 N_A 分别是客户的身份和账号,然后客户把 c 发给银行 B。银行 B 用自己的私钥 d_B 对 c 解密,计算 $c^{d_B} \bmod \varphi(n_B) = (m_c^{e_B} \bmod \varphi(n_B))^{d_B} \bmod \varphi(n_B) = m_c^{e_B d_B} \bmod \varphi(n_B) = m_c \bmod \varphi(n_B)$。银行验证 A 的身份 ID_A,若合法,银行 B 就对 m 进行签名,即计算 $m_{1B}^{\frac{1}{}} = m_1^{d_B}$,并从 A 的账号 N_A 中去掉 s 个货币单位,这里假定客户 A 事先已在银行 B 存了一笔钱。B 将 $m_{1B}^{\frac{1}{}} = m_1^{d_B}$ 发送给 A,A 计算 $m_{1B}^{\frac{1}{}} / r = (f_B(m) r^{e_B}) / r = f^{d_B}(m)$。客户 A 得到了银行 B 对 m 的真实签名 $f^{d_B}(m)$。$f^{d_B}(m)$ 价值 s 个货币单位,就是客户 A 从银行取出的货币。

支付售票协议: 售票实体选择两个大素数 p_1 和 q_1,以及一个安全 Hash 函数 f_1,并随机选择 e_1,使得 $\gcd(e_1, \varphi(n_1)) = 1$,其中 $n_1 = p_1 q_1$,由 $e_1 d_1 = 1 \bmod \varphi(n_1)$ 知 $d_1 = e_1^{-1} \bmod \varphi(n_1)$。售票实体公布 n_1, e_1, f_1,保密 p_1, q_1 和 d_1。客户 A 把取得的货币发给售票实体 S,这里可能涉及到找零钱协议,该方案不考虑这个问题。由于是在线支付,在客户 A 付款的过程中,银行 B 把 A 发给 S 的货币存入 S 的账户上。客户 A 首先产生一个消息 x,并随机地选择一个 $k \in Z_p^*$(盲因子),计算 $x' = f_1(x) k^{e_1} \bmod n_1$,将 $(m, f_1^{d_1}(m), x')$ 发给售票实体 S,S 将

(下转第 389 页)

互之间的大小关系与初始序参量的相同。可见,用初始序参量定量评价图像水印的鲁棒性,与用相关系数的评价是一致的,但更易区分。

表 4　相关系数

	1	2	3	4	5
未处理	1	0.9585	0.9548	0.9645	0.9504
高斯噪声(方差 0.001)	0.8846	0.8531	0.8544	0.8641	0.8452
椒盐噪声(方差 0.005)	0.9062	0.8686	0.8677	0.8776	0.8668
JPEG 压缩(50%)	0.9593	0.9158	0.9191	0.9284	0.9110
中值滤波	0.9292	0.8868	0.8953	0.9030	0.8830
维纳滤波	0.9527	0.9114	0.9127	0.9218	0.9034
对比度增强	0.7174	0.7084	0.7353	0.7320	0.7149
对比度减弱	0.9419	0.9365	0.9303	0.9455	0.9546
灰度均衡	0.6357	0.6246	0.6523	0.6495	0.6301
旋转(0.05)	0.7943	0.7688	0.7746	0.7872	0.7782
放大(1.05)	0.9419	0.9271	0.9274	0.9403	0.9419

5　结语

协同序参量是一种宏观参量,用于描述系统的整体行为,主宰着系统演化过程。系统从无序转变为有序以及从有序转变为更为复杂的有序过程,也就是在一再形成新的自组织过程中,序参量支配其他稳定模而形成了一定的结构或序。系统状态将由一个最强的初始序参量决定,获胜的序参量代表了被识别的原型模式。

协同序参量方法和相关系数法应用于图像水印鲁棒性评价中,所获得的结果是一致。用初始序参量定量来定量评价图像水印的鲁棒性,理论依据充分,计算简单,识别结果明显。本方法还特别适用于对含水印载体图像声称具有版权的多个嵌入者的场合。在发生版权争议时,仲裁者可用各人的水印组成水印模式集,计算协同序参量的初始值,从而判断图像的归属。

对模式集中模式数量较大的情况,初始序参量的计算和比较还有待进一步研究。

参考文献:

[1] COX IJ, MILLER ML, BLOOM JA. 数字水印[M]. 北京: 电子工业出版社, 2003.

[2] HANKEN H. Synergetic computers and cognition - a top - down ap proach to neural nets[M]. Berlin: Springer – Verlag, 1991.

[3] COX IJ, KILIAN J, LEIGHTON T, *et al.* A Secure, Robust Watermark for Multimedia[A]. Proceedings of the First International Workshop on Information Hiding[C], 1996. 185 – 206.

(上接第 382 页)

$(ID_S, N_S, m, f^{d_1}(m))$ 发送给银行 B,B 验证收到的签名,并检查 m 在以前是否被花费过。如果签名合法并且 m 没被花费过,那么银行 B 就在 S 的账号 N_S 上存入 A 发给 S 的货币。售票实体收到货币之后,它对 x' 签名得 $y' = Sig_T(x') = (x')^{d_1} \bmod n_1$,然后售票实体把签名 y' 发送给客户,客户把盲因子去掉,计算:$y = y'/k \bmod n_1 = (f_1(x)k^{e_1})^{d_1}/k \bmod n_1 = f_1^{d_1}(x) \bmod n_1$,$y$ 是 x 的合法签名,也就是客户从售票实体那里得到的票。利用这张票,客户再向时间戳服务请求给文档 Hash 值加盖时间戳。

2.2　加盖时间戳过程

时间戳服务实体选择两个大素数 p_2 和 q_2,以及一个安全 Hash 函数 f_2,并随机选择 e_2,使得 $\gcd(e_2, \varphi(n_2)) = 1$,其中 $n_2 = p_2 q_2$,由 $e_2 d_2 = 1 \bmod \varphi(n_2)$ 知 $d_2 = e_2^{-1} \bmod \varphi(n_2)$。时间戳服务公布 n_2, e_2, f_2,保密 p_2, q_2 和 d_2。

客户如果要对自己的一个文档 m_2 加盖时间戳,客户首先计算 $z_2 = h_2(m_2)$,其中 h_2 是安全的 Hash 函数。客户发送 (y, x, z_2) 给时间戳服务。

时间戳服务收到 (y, x, z_2) 之后:

1) 首先验证票 y 是否有效:

时间戳服务得到售票实体的公钥 (e_1, n_1);计算 $y^{e_1} \bmod \varphi(n_1)$;时间戳服务计算 $f_1(x)$;如果 $y^{e_1} \bmod \varphi(n_1) = f_1(x)$,则票有效,可以给它加盖时间戳;否则,票无效。

2) 其次在客户的票被验证有效之后,给 z_2 加盖时间戳:

时间戳服务得到当前的日期和时间 t;时间戳服务计算:$\hat{z}_2 = f_2(z_2 \| t)$;时间戳服务对 $\hat{z}_2$ 签名,计算:$z' = (\hat{z}_2)^{d_2} \bmod \varphi(n_2)$;时间戳服务公布 $(z', \hat{z}_2, t)$。

2.3　客户验证过程

客户得到时间戳服务公布的 (z', z_2, t) 之后,可以验证时间戳的有效性,验证过程如下:

1) 客户得到时间戳服务的公钥 (e_2, n_2);

2) 客户计算 $(z')^{d_2} \bmod \varphi(n_2)$;

3) 客户计算 $f_2(z_2 \| t)$;

4) 比较,如果 $(z')^{d_2} \bmod \varphi(n_2) = f_2(z_2 \| t)$,则时间戳有效,客户把它保存起来;否则,时间戳无效,客户应请求时间戳服务重新加盖一次时间戳。

3　结语

随着我国数字签名法的即将出台,安全数字时间戳也将具备法律效力,其重要性不言而喻。本文基于 RSA 数字签名,提出了一种新的安全数字时间戳方案,新方案通过引入一个售票实体成功地解决了服务付费问题。并且基于 RSA 数字签名,构造了一个完整的安全数字时间戳系统。

参考文献:

[1] LIPMAA H. Secure and efficient time-stamping systems[J]. Ph. d, University of Tartu – Estonia, July 1999.

[2] MASSIAS H, AVILA XS, QUISQUATER J-J. Timestamps: Main issues on their use and implementation[A]. IEEE 8th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises[C], 1999.

[3] Protocols and data formats for time-stamping service[J]. 17th September 2002.

[4] HABER S, STORNETTA WS. How to Time-Stamp a Digital Document[J]. in Journal of Cryptology, 1991, 3(2): 99 – 111.

[5] BULDAS A, LAUD P, LIPMAA H, *et al.* Time – stamping with binary linking schemes[Z]. Advances in Cryptology-CRYPTO'98, LCNCS1462, 1998.

[6] 冯登国, 裴定一. 密码学导引[M]. 北京: 科学出版社, 2001.

[7] STADLER M, PIVETEAU JM, CAMENISCH J. Fair Blind Signature[J]. Advance in Cryptology-Eurocrypt'95, Springer-Verlga, 209 – 219.