研究简报·

新的基于中国剩余定理的公钥叛逆者追踪方案

杨　晨　马文平　王新梅
(西安电子科技大学 综合业务网理论国家重点实验室, 陕西 西安　710071)

摘　要: 分析了 Lyuu 等所提出的叛逆者追踪方案的效率和安全性,并基于中国剩余定理提出了两个改进的公钥叛逆者追踪方案。与原方案相比较,改进后的方案可以节省近一半的系统广播通信带宽,并进一步强化了方案的安全性,同时还具有良好的可撤销性和保持性等优点及黑盒子追踪功能。

关键词: 叛逆者追踪; 数字版权保护; 广播加密; 中国剩余定理; 黑盒追踪
中图分类号: TP309

引　言

随着网络技术和计算机技术的发展,如何既充分利用数字技术和网络技术的便利,又能有效地保护知识产权,已受到人们的高度重视。现今世界各大知名公司如 IBM、NEC、Sony、Philips 等,都在加速数字版权保护技术的研制和完善,以便于保护自己的合法权益。叛逆者追踪技术是在数字水印技术和密码学技术的基础上衍生出来的一种新的数字版权保护策略,是对抗加密广播业务中共谋密钥攻击和非法重放攻击的主要技术。随着付费电视,在线数据库访问以及在线影视 CD 发布系统等广播加密业务的普及应用,叛逆者追踪技术在这些广播加密业务中有着广阔的商用前景:如就付费数字电视而言,该技术可以抑止盗版数字电视机顶盒的泛滥;就在线数据库访问系统而言,可以禁止非授权用户利用合谋密钥的非法访问;就在线影视发布系统而言,可以对抗非法访问和非法重放的威胁。随着加密广播业务越来越多的商业化需求,叛逆者追踪技术已经成为信息安全领域研究的热点之一。

1994 年,根据 Fiat 等[1]提出的加密广播中如何保护解密盒中密钥的问题, Chor 等[2]首次提出了叛逆者追踪的概念,并在单向函数的存在性及大整数的素分解困难的密码学假设基础上,构造了几种 k-弹性的对称叛逆者追踪方案; Pfitzmann[3]介绍了非对称叛逆者追踪的概念,与以前的对称方案相比,不诚实的数据供应商不能诬陷合法诚实用户,并使得数据供应商可以明确地向第三方证明叛逆者参与盗版的事实。随后,几种 k-弹性的叛逆者追踪方案[4-7]被提了出来。Lyuu 等[8]利用中国剩余定理理论构造了完全公钥叛逆者追踪方案 ——LW02 方案,并实现了保持性和动态增删用户的灵活性。

本文在分析 LW02 方案基础上给出了两个改进的公钥叛逆者追踪方案,在节省系统传输带宽和强化方案安全性的同时,保留了原方案的可撤销性和保持性等优点。

1　背景知识

定理 1　中国剩余定理

令 $a \geq 2$, 如果 $r_1, r_2, \cdots, r_a$ 是正整数, $n_1, n_2, \cdots, n_a$ 为素数,则存在 H 满足:

$$H \equiv r_i \pmod{n_i},\ i = 1, 2, \cdots, a$$

反过来说,如果存在另外的 H 满足上式,则必有

$$H \equiv H' \pmod{n_1 n_2 \cdots n_a}$$

同时 H 必具有下述形式:

$$H = \sum_{i=1}^{a} r_i X_i \pmod{N}$$

其中, $N = \prod_{i=1}^{a} n_i$, $X_i = y_i(N/n_i)$ 且满足

$$y_i(N/n_i) \equiv 1 \pmod{n_i}.$$

定理 2　同余式组

$$x = b_i \pmod{n_i},\ 1 \leq i \leq a$$

有解,当且仅当 $\gcd(n_i, n_j)$ 能整除 $b_i - b_j$,对任意 (i, j) $(1 \leq i < j \leq a)$;且该解在模 $N = \mathrm{lcm}(n_1, n_2, \cdots, n_a)$ 下唯一,并可由中国剩余定理给出。其中 gcd

收稿日期: 2006-09-23
基金项目: 教育部"新世纪优秀人才支持计划资助";国家自然科学基金(60373104/90604009)
第一作者: 男,1979 年生,博士生
E-mail: yfych@eyou.com

$(\cdots)$表示最大公约数,$\mathrm{lcm}(\cdots)$表示最小公倍数。

定理 3　设 $N = n_1 n_2 \cdots n_a$ 是奇素数的乘积,令 $\lambda(N) = \mathrm{lcm}(\phi(n_1), \phi(n_2), \cdots, \phi(n_a))$,设 $r_i (i = 1,2,\cdots,a)$ 是模 n_i 的一个本原根,则同余式组 $x = r_i \pmod{n_i}$, $1 \leq i \leq a$ 的解就产生一个阶为 $\lambda(N)$ 的整数 g。

定理 4　已知 $d_1, d_2, \cdots, d_v$, $\gcd(p_i - 1, p_j - 1)$ 能整除 $d_i - d_j$,则存在 d_H,并满足 $d_H = \sum_{i=1}^{v} d_i N_i y_i \bmod N$,

其中 $i = 1,2,\cdots,v$, $N = \mathrm{lcm}(n_1 - 1, n_2 - 1, \cdots, n_v - 1)$, $N_i = N/(n_i - 1)$, $N_i y_i \equiv 1 \pmod{n_i - 1}$。

定义 1　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内以不可忽略的概率计算 g^{xy}。

2　LW02 方案描述

(1) 系统参数产生

假定系统参数由一个密钥产生中心 KGC 产生,l 是一个安全参数, k 是系统用户的总数,每个用户 i 秘密选择一个 l 比特的素数 $n_i = 2q_i + 1$, q_i 是一个奇素数。

为方便起见,假设 $n_1 < n_2 < \cdots < n_k$,记 $N = \prod_{i=1}^{k} n_i$。所要传输的数据是 Z_{n_1} 中的元素,选取 g 为满足定理 3 的同余式组的解。

(2) 解密密钥的产生

每个用户 i 随机选择一个个人解密密钥 $d_i \in Z_{n_i}^*$,向 KGC 发送 (β_i, n_i),这里 $\beta_i \equiv g^{d_i} \bmod n_i$。KGC 计算 $\beta \equiv \sum_{i=1}^{k} \beta_i N_i y_i \bmod N$,这里 $N_i = N/n_i$, $N_i y_i \equiv 1 \bmod n_i (1 \leq i \leq k)$。则 (g, β, N) 是公开的加密密钥,$\beta \equiv \beta_i \pmod{n_i}$。

(3) 加密过程

设明文 $x \in Z_{n_1}$,数据供应商 DS 在 $\{0,1,\cdots,n_1 - 1\}$ 中随机选取一个 r,计算

$$z_1 \equiv g^r \bmod N,\ z_2 \equiv x\beta^r \bmod N$$

则密文为 $C = (z_1, z_2)$。

(4) 解密过程

给定密文 $C = (z_1, z_2)$,解密为

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

(5) 叛逆者追踪

若盗版解码器中的 d_H 和 N_H 可以被检测提取出来,则可由通过检验 $N_H \equiv 0 \pmod{n_i}$ 是否成立,若成立则判定第 i 个用户参与了盗版;反之,对于不能打开的盗版解码器,则可利用黑盒追踪算法找出所有的盗版者。

对 $i = 1,2,\cdots,k$,执行:

步骤 1　计算 $\alpha_i \equiv \beta \bmod N_i$,这里 $N_i = N/n_i$,且 $N = n_1 n_2 \cdots n_k$;

步骤 2　选择一个明文 x,利用加密密钥计算密文 C;

步骤 3　将 C 输入盗版解码器中,若输出不等于 x,那么用户 i 是一个盗版者。

(6) 安全性分析　因为 g 是模 $n_i (i = 1,2,\cdots,k)$ 的一个公共本原根, g 的阶为 $\lambda(N) = 2q_1 q_2 \cdots q_k$,于是由 g 生成 Z_N^* 的子群 H 阶为 $\lambda(N)$,并且 H 的阶必然包括一个不小于 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,该方案在被动攻击下是安全的,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 $g^{d_H} \equiv g^{d_i} \pmod{n_i}$, $i = 1,2,\cdots,t$,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。

3　公钥叛逆者追踪方案

本文提出两个改进的非对称公钥叛逆者追踪方案,分别简称方案 1 和方案 2。

3.1　方案 1

在该方案中,系统参数如上述 LW02,差别在于同时选取安全的密码哈希函数 $H_0: \{0,1\}^* \rightarrow Z_{n_1}^*$。

(1) 密钥生成

用户 i 随机选择一个随机数 $d_i \in Z_{n_i}^*$ 作为自己的解密密钥,计算 $\beta_i \equiv g^{d_i} \bmod n_i$,向 KGC 发送 (β_i, n_i)。当 KGC 收到系统中所有用户的 (β_i, n_i) 后,选取一个长 l 比特的素数 $n_0 = 2q_0 + 1$, q_0 是一个奇素数,并满足 $n_0 < n_1$。而后 KGC 计算 $\beta \equiv \sum_{i=0}^{k} \beta_i N_i y_i \bmod N$,这里 $N_i = N/n_i$, $N_i y_i = 1 \bmod n_i (1 \leq i \leq k)$。$(g, \beta, N)$ 是公开的加密密钥。

(2) 加密过程

设明文 $x \in Z_{n_i}$,数据供应商 DS 在 $\{0,1,\cdots,n_1 - 1\}$ 中随机选取一个 r,计算:

$z_1 \equiv x \oplus H_0(g^r \bmod n_0) \bmod n_1$, $z_2 \equiv \beta^r \bmod N$

则密文为 $C = (z_1, z_2)$。

(3) 解密

给定密文 $C = (z_1, z_2)$,解密为

$x \equiv z_1 \oplus H_0(((z_2^{d_i^{-1}}) \bmod n_i) \bmod n_0)$。

(4) 效率与安全性分析

方案的安全性和追踪算法同 LW02 方案,易证明在计算的 Diffie-Hellman 假设下,该方案在被动攻击下仍是安全的,同时也具有较好的增删用户的灵活性。在计算密文分量的时候,由于我们得到的是 $Z_1 \in Z_{n_1}^*$,而非 Z_N^* 中的元素,所以在通信广播传输效率上,方案 1 可以比 LW02 方案节省近一半的广播通信传输带宽。

3.2 方案 2

系统参数产生如 LW02 方案,密钥产生算法如方案 1,数据供应商得到 (N_i, y_i), $i = 1, 2, \cdots k$,并选择对称密钥加密函数 $E(\cdot, \cdot)$ 对数据内容加密(比如 128bit-AES 等), $D(\cdot, \cdot)$ 为相应的解密函数。选择密码哈希函数 $H: \{0,1\}^* \rightarrow \{0,1\}^{128}$。

(1) 加密

采用加密广播并定期更新加密密钥的策略,即周期地(如 5 min)更新会话密钥 s 的方法达到连续安全广播的目的。数据供应商 DS 在中随机选取一个 $x, r_1, r_2, \cdots, r_k \in Z_{n_1}$,计算

$$z_1 \equiv \sum_{i=1}^{k} g^{r_i} N_i y_i \bmod N$$

$$z_2 \equiv s \sum_{i=1}^{k} \beta^{r_i} N_i y_i \bmod N$$

$$k_s = H(s)$$

则控制报头信息 $C = (z_1, z_2)$。

(2) 解密

给定控制报头信息 $C = (z_1, z_2)$,解密得会话密钥 $k_s = H(s) = H((z_2 (z_1)^{-d_i}) \bmod n_i)$。

在一个密钥更新周期内,其实上述过程只需一次的控制报头信息 (z_1, z_2) 的计算和广播以及用户端会话密钥的恢复计算。此后,数据供应商只需直接加密广播数字内容就可达到连续安全广播的目的,这样既大大减少了用户端和广播中心的计算负担,提高了系统的效率,同时又不影响系统安全性。

(3) 效率与安全性分析

易证明,方案 2 的安全性不低于 LW02 方案,且在计算的 Diffie-Hellman 假设下,该方案在被动攻击下仍是安全的,同时也具有较好的增删用户的灵活性,大大增加了盗版的困难性。广播数据所需的传输带宽与原 LW02 方案相当,但是强化了方案的安全性,更贴近于实际应用。

4 黑盒追踪算法

针对方案 2,本文提出一个能够识别所有参与盗版的叛逆者的黑盒追踪算法,并且在执行追踪算法时不需要任何的密钥更新计算。假定盗版解码器不能区分合法密文 $C = (z_1, z_2)$ 与特殊设计的密文 $C' = (z_1', z_2')$,所以该追踪算法与 LW02 方案相比更加实用有效。追踪算法描述如下:

对每一个 $j = 1, 2, \cdots, k$, 追踪者(可以是 DS)执行

(1) 计算

$$z_1' = g^{r_j} N_j y_j + \sum_{\substack{i=1 \\ i \neq j}}^{k} g^{r_i} N_i y_i \bmod N$$

$$z_2' = \left(x g^{r_j d_j} N_j y_j + \sum_{\substack{i=1 \\ i \neq j}}^{k} x g^{r_i d_i} N_i y_i \right) \bmod N$$

其中 $x, r_i, r_j, r_j', (i = 1, 2, \cdots, k; i \neq j)$ 是随机数,且满足 $r_j \neq r_j'$;

(2) 输入 $C' = (z_1', z_2')$ 给盗版解码器,若输出不等于 x, 则用户 j 将被识别为叛逆者。

5 结论

叛逆者追踪技术是目前数字版权保护领域中的一个热点研究问题。本文对 LW02 方案加以改进,提出了两个新的公钥叛逆者追踪方案。与原方案相比较,改进后的方案不仅减少了系统的广播通信带宽(第一个改进方案节省了近一半的通信传输带宽),而且更加强化了方案的安全性。此外,改进后的方案在保留了原方案良好的可撤销性和保持性的同时,还具有黑盒子追踪功能。基于中国剩余定理理论设计构造实用的多频道付费电视方案和在线数据库系统仍是一个值得深入研究的课题。

参考文献:

[1] FIAT A, NAOR M. Broadcast encryption[C] // Proceeding of CRYPTO '93. LNCS 1109. Berlin: Springer-Verlag, 1994: 480 - 491.

[2] CHOR B, FIAT A, NAOR M. Tracing traitors [C] // Proceeding of CRYPTO '94. LNCS 839. Berlin: Springer-Verlag, 1994: 257 - 270.

[3] PFITZMANN B. Trials of Traced Traitors [C] // Advance in CRYPTO '96. LNCS 1174. Berlin: Springer-Verlag, 1996: 49 - 63.

[4] BONEH F M. An efficient public key traitor tracing scheme [C] // Proceeding of CRYPT '99. LNCS 1992. Berlin: Springer-Verlag, 1999: 338 - 353.

[5] KIYAIAS A, YUNG M. Breaking and repairing asymmetric public-key traitor tracing [C] // ACM Workshop on DRM 2002. LNCS 2696. Berlin: Springer-Verlag, 2002: 32 - 50.

[6] CHABANNE H, PHAN D H, POINTCHEVAL D. Public traceability in traitor tracing schemes [C] // Advance in CRYPTO '05. LNCS 3494. Berlin: Springer-Verlag, 2005: 542 - 558.

[7] MCGREGOR J P, YIQUN L Y, RUBY B L. A traitor tracing scheme based on RSA for fast decryption [C] // Proceeding of ACNS 2005. LNCS 3531. Berlin: Springer-Verlag, 2005: 56 - 74.

[8] LYUU Y D, WU Minglun. A fully public-key traitor tracing scheme [J]. WSEA Transaction on Circuits 1, 2002(1):88 - 93.

New public-key traitor tracing schemes using chinese remainder theorem

YANG Chen　MA WenPing　WANG XinMei

(State Key Laboratory of Integrated Series Networks, Xidian University, Xi'an Shaanxi 710071, China)

Abstract: An analysis of the efficiency and security of the Lyuu-Wu traitor tracing (LW02) scheme is presented, and two improved public-key traitor tracing schemes based on Chinese remainder theorem are proposed. Compared with the original scheme, the proposed schemes can save almost half of the broadcasting communication bandwidth and also enhance the security of the system. In addition, both schemes have the advantages of fast revocation and good holding properties as well as black-box tracing capability.

Key words: traitor tracing; digital right management; broadcast encryption; Chinese remainder theorem; black-box tracing

下 期 预 告

热态气-液-固三相搅拌反应槽的气-液分散特性　黄小华等
应用改进的正规溶液模型关联氨基酸在水中的溶解度　龙秉文等
超声/ Fenton 试剂氧化耦合处理染料废水　彭晓云等
回转梁受强动载荷作用的刚-塑性动力响应　张　娅等
迷宫螺旋泵内部流动的 CFD 模拟　田国文等
基于无先导卡尔曼滤波的 RBFN 训练算法研究　张海涛等
正壬烷构象的振动光谱研究　王良玉等
氧化铝熟料溶出过程二次反应的热力学讨论　陈　滨等
离子液体中纤维素的溶解及再生特性研究　翟　蔚等
三孢酸机构类似物对番茄红素发酵产量的影响　徐军伟等
一类混杂构形的特征多项式　董　芸等
固定化假丝酵母 99-125 脂肪酶催化合成甘油二酯　胡　隼等
参数曲线的隐式化　孙永利等
基于 VaR 控制下的动态优化投资组合　王锦玉等
正壬烷构象的振动光谱研究　王良玉等
氧化铝熟料溶出过程二次反应的热力学讨论　陈　滨等
固定化假丝酵母 99-125 脂肪酶催化合成甘油二酯　胡　隼等
基于离差最大化的决策者权重的确定方法　马永红等
咪唑啉型缓蚀剂的合成及其缓蚀行为研究　赵　昀等
紫外光引发的玉米淀粉在软材料表面的改性　黄振华等
十二烷基硫酸钠柱撑水滑石的固体核磁共振研究　曹　永等
环氧树脂/氰酸酯共固化体系热性能的研究　黄　丽等
长链分子对热可逆透明成像材料性能的影响　季长亮等
三环类环氧合酶抑制剂的三维定量构效关系研究　李顺来等
壳聚糖/聚乙烯醇/氧氟沙星共混无纺布的制备及体外释放研究　甄洪鹏等
三羟甲基庚烷的合成　支晓华等
化学镀法制备电磁屏蔽聚酯织物的研究　杜　宁等