一种完整的非对称公钥叛逆者追踪方案

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 利用不经意多项式估值协议，该文提出了一种新的非对称公钥叛逆者追踪方案。当参与共谋的叛逆者数量不超过预先设置的范围时，与现有的非对称公钥追踪方案相比，该方案能够以完全的黑盒子追踪方式准确地确定出全部叛逆者；借助于密钥更新，该方案具有完善的撤销性，能够撤销任意数量的叛逆者。此外，与已有方案相比该方案显著降低了追踪时的计算量并且有着更高的传输效率。

关键词 保密通信，黑盒子追踪性，可撤销的，不经意多项式估值，追踪叛逆者
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2006)03-0407-03

A Complete Asymmetric Public-Key Traitor Tracing Scheme

Wang Qing-long Yang Bo
(*Computer and Information Technology Institute, Beijing Jiaotong University, Beijing* 100044, *China*)

Abstract Based on oblivious polynomial evaluation, this paper presents a new asymmetric public-key traitor tracing scheme. Compared with the previous schemes, this proposed scheme can accurately determine a or all traitor(s) from an illegal decoder by full black-box tracing when the number of traitors participating conspiracy is not larger than the defined number; and revoke unlimited traitors by means of the way of updating secret key. Moreover, this proposed scheme greatly decreases the computational cost of tracing a traitor and has a higher transmission efficiency compared with those of available.

Key words Secret communication, Black-box tracing, Revocable, Oblivious Polynomial Evaluation (OPE), Tracing traitors

1 引言

目前利用网络提供服务的行业越来越多。当这种服务是以广播发送的方式提供时，为了保护数据提供者(Data Supplier, DS)的合法权益，数据需要以加密方式传送，以保证只有授权用户才能使用解密钥获得所需的信息。这里 DS 面临的主要问题是某些授权用户(叛逆者)非法复制自己的或共谋的解密钥给非授权用户(非法者)，使得这些非授权用户能够非法获得 DS 提供的信息。为了指控叛逆者，DS 须确定出叛逆者并且能够提出令人信服的证据。由此导致叛逆者追踪方案的出现(当共谋者数量不超过某个预定值时要能确定出至少一个叛逆者)。应用场合包括付费电视系统、网上娱乐服务、网上金融信息的发布、CDROM 的在线发布、软件保护等。

自Chor的文章[1]发表后，各种叛逆者方案相继被提出来。文献[2]提出的公钥叛逆者追踪方案解决了文献[1,3]的分组长度随着用户数量的增长而增加的缺点。文献[4,5]进一步提出了具有非对称性的公钥叛逆者追踪方案，即只有用户自己知道解密钥，从而使DS可以提供不可否认证据。但是文献[4,5]两个方案共同的不足之处是都不具备完全的黑盒子追踪能力(不需要打开盗版解码器，而是通过输入输出之间的关系来确定其中包含的解密钥)，也没有提到如何撤销叛逆者(使叛逆者拥有的解密钥失去作用，不能再用来解密DS发送的加密数据，但合法用户不受影响)。

本文的贡献在于在文献[4,5]的基础上提出了一种具备完全黑盒子追踪并且能够撤销任意个叛逆者的非对称公钥叛逆者追踪方案。方案的执行不需要第 3 方的参与，也不需要使用陷门离散对数。完备的撤销性使得 DS 不仅可撤销叛逆者，也可撤销服务到期的用户，从而可更好地保护数据提供者的利益。

2 不经意多项式估值协议(Oblivious Polynomial Evaluation，OPE)[6]简介

Bob知道一个多项式 $p(x)$, Alice知道一个值 a 。协议执行结束后Alice 获得 $p(a)$ 但是不能得到 p 的任何信息，同时Bob也不能得到有关 a 的信息。协议过程如下：Bob随机选一个二元多项式 $Q(x,y)$ 满足 $Q(0,y)=p(y)$ 用来隐藏 $p(y)$; Alice随机选一元多项式 $s(x)$ 满足 $s(0)=a$ 用来隐藏 a 。最后Alice可以通过插值恢复出多项式 $R(x)=Q(x,s(x))$ ，显然有 $R(0)=Q(0,s(0))=p(s(0))=p(a)$ 。设 $R(x)$ 的次数为 z ，当Alice获得 $R(x)$ 上 $z+1$ 个点上的值 $\{(x_i,R(x_i)),i=1,2,\cdots,z+1\}$ 后就能利用Lagrange插值求出 $R(x)$ 。而每对 $(x_i,R(x_i))$ 可通过不经意传输协议[6](Oblivious transfer, OT_n^1)的方式来获取。OPE协议的安全性在文献[6]

2004-06-18 收到，2005-10-17 改回
国家自然科学基金(60372046)和现代通信国家重点实验室基金(51436040204DZ0102)资助课题

中已给出了详细说明。

3 方案叙述

3.1 系统参数

q 和 p 为两个大素数，且 $q \mid p-1$。g 是 Z_p 上阶为 q 的本原元。

DS 在 Z_q 上秘密选一个 k 次多项式 $f_1(x)=\sum_{i=0}^{k} a_i x^i$。DS 再任选 $x_0, x_n \in Z_q^*$，$\{h_1,h_2,\cdots,h_k\} \subset Z_q \setminus \{0\}$，$\Omega=\{m_1,m_2,\cdots,m_k\} \subset Z_q \setminus (\{x_0,x_n\} \cup \{0\})$。设 $f(x,y)=f_1(x)+by$，$b \in Z_q^*$ 由 DS 秘密选取。又设 Φ 为已注册用户的集合，$\Phi \subseteq Z_q \setminus (\{x_0,x_n\} \cup \{0\} \cup \Omega)$。令 $\Delta=\{(m_1,g^{h_1}),(m_2,g^{h_2}),\cdots,(m_k,g^{h_k})\}$，DS 公开 g,p,q,Δ 和公开钥 $e=\left(g, g^{f_1(x_0)}, g^b, x_0, \left(x_1, g^{f_1(x_1)}\right), \cdots, \left(x_k, g^{f_1(x_k)}\right)\right)$，其中 $\{x_1,x_2,\cdots x_k\} \subset Z_q \setminus (\{0\} \cup \{x_0\} \cup \Phi)$。除非特别说明，本方案的所有算术运算都在 Z_p 上。$r_0 \in_R Z_n^*$

3.2 注册过程

步骤 1 当用户 $i \in Z_q \setminus (\{0\} \cup \{x_0\} \cup \Omega \cup \Phi)$ 注册时，i 秘密选一个数 $\alpha_i \in Z_q^*$，DS 秘密选一个数 $v \in Z_q^*$。使用 OPE 协议用户得到 $d=v(f_1(i)+b\cdot\alpha_i)$。

步骤 2 用户发送 $pk_i \| \mathrm{sgn}_{sk_i}(g^d \| g^{\alpha_i})$ 给 DS。(pk_i, sk_i 为用户的公开钥和秘密钥，sgn 为可恢复消息的签字)。

步骤 3 DS 恢复出 $g^d \| g^{\alpha_i}$ 并验证 $g^d=(g^{\alpha_i})^{vb} g^{vf_1(i)}$，若相等将 v 发给用户。并且将 Φ 更新为 $\Phi \cup \{i\}$。

步骤 4 令 $m_0=i, h_0=f_1(i)$，DS 计算 $B_i=\prod_{j=0}^{k}\left((g^{r_0})^{h_j}\right)^{\lambda_j}$，$\lambda_j=\prod_{0\le l\ne j\le k}\frac{m_l-x_n}{m_l-m_j}$，并记录定购单 $\mathrm{text}=i \| B_i \| pk_i \| \mathrm{sgn}_{sk_i}(g^d \| g^{\alpha_i})$。(注解：由于 Δ 中的 k 组点是随即选取的，所以其一般不在曲线 $f_1(x)$ 上，这样这 k 组点加上 $(i, f_1(i))$ 一共有 $k+1$ 组点，可以唯一确定一条 k 次曲线 $g_i(x)$，这步的目的实际上是计算 $(g_i(x_n))^{r_0}$。因为不同用户的解密钥不同，所以对应的 $g_i(x)$ 一般也不同，相应的 $(g_i(x_n))^{r_0}$ 也就不同。)

步骤 5 用户 i 的解密钥为 $d_i=(i,\alpha_i,d/v)=(i,\alpha_i,f_1(i)(+\alpha_i b))=(i,\alpha_i,f(i,\alpha_i))$。

3.3 加密算法

设 M 为待加密消息，DS 任选 $r \in Z_q^*, s \in Z_q^*$，则 DS 发送的数据分组为 $\left(g^r, sg^{rf_1(x_0)}, g^{rb}, x_0, \left(x_1, g^{rf_1(x_1)}\right), \cdots, \left(x_k, g^{rf_1(x_k)}\right), s\oplus M\right)=(H, s\oplus M)$。($H$ 称为分组头，$\oplus$ 为比特间的“异或”运算，用来对消息进行加密)。

3.4 解密算法

用户 i 收到分组数据后，利用自己的解密钥 d_i 执行以下几步：

步骤 1 $\frac{(g^r)^{f(i,\alpha_i)}}{(g^{rb})^{\alpha_i}}=\frac{g^{rf_1(i)}g^{rb\alpha_i}}{g^{\alpha_i rb}}=g^{rf_1(i)}$。

步骤 2 令 $x_{k+1}=i$，利用 Lagrange 插值法计算：$g^{rf_1(x_0)}=\prod_{t=1}^{k+1}\left(g^{rf_1(x_t)}\right)^{\lambda_t}$，$t \in \{x_1,x_2,\cdots,x_{k+1}\}$。其中 $\lambda_t=\prod_{1\le j\ne t\le k+1}\frac{x_j-x_0}{x_j-x_t}$ 为 Lagrange 插值系数。

步骤 3 计算 $s=\frac{sg^{rf_1(x_0)}}{g^{rf_1(x_0)}}$。

步骤 4 计算 $s\oplus(s\oplus M)=M$，得到明文。

3.5 追踪算法

设盗版解码器中包含 $l(\le k)$ 个解密钥 $\{d_{i_1}, d_{i_2}, \cdots, d_{i_l}\}=\Lambda$。叛逆者的策略是每次解密时随机选用 Λ 中的一个解密钥 $d_i, i \in \{i_1,i_2,\cdots,i_l\}$ (由于本方案的公开钥中用 $g^{f_1(x_0)}$ 而不是用 $g^{a_0}=g^{f_1(0)}$ 隐藏 s，所以文献[4]中 Claim 1 提到的共谋方式在这里不适用——参见附录)。为了确定解密钥，DS 执行以下步骤：

步骤 1 往盗版解码器中输入数据 $\left(\left(g^{r_0}, A, g^{r_0 b}, x_n, \left(m_1, g^{r_0 h_1}\right), \left(m_2, g^{r_0 h_2}\right), \cdots, \left(m_k, g^{r_0 h_k}\right)\right), M_i\right)$。$M_i$ 是一随机选取的没加密的比特串。

步骤 2 设解码器使用的解密钥为 $d_i=(i,\alpha_i,f(i,\alpha_i)), i \in \{i_1,i_2,\cdots,i_l\}$，则 DS 可以利用解码器的输出结果计算出该解密钥对应的 B_i。解码器的详细计算过程为

(1) $\frac{(g^{r_0})^{f(i,\alpha_i)}}{(g^{r_0 b})^{\alpha_i}}=\frac{g^{r_0 f_1(i)}g^{r_0 b\alpha_i}}{g^{r_0\alpha_i b}}=g^{r_0 f_1(i)}$，令 $m_0=i, h_0=f_1(i)$，解码器计算 $\prod_{j=0}^{k}\left(g^{r_0 h_j}\right)^{\lambda_j}=B_i$，$\lambda_j=\prod_{0\le l\ne j\le k}\frac{m_l-x_n}{m_l-m_j}$。

(2) 解码器计算 $A/B_i=C_i$。

(3) 解码器输出 $D_i=C_i\oplus M_i$。

DS 获得 D_i 后计算 $D_i\oplus M_i=C_i\oplus M_i\oplus M_i=C_i$。由此可得 $B_i=A/C_i$。通过与保存的 text 相比较，找到与 B_i 相对应的 text，即可确定叛逆者。由于一次输入就能确定出一个叛逆者，所以经过有限次输入输出后即可确定出全部的叛逆者。

3.6 撤销算法

设 $\Lambda_\gamma=\{i_1,i_2,\cdots,i_\gamma\}$，$\gamma \le k$，是由叛逆者组成的集合。则 DS 用 $\left\{\left(i_1, g^{f_1(i_1)}\right), \cdots, \left(i_\gamma, g^{f_1(i_\gamma)}\right)\right\}$ 替换公开钥 e 中的任意 γ 个 $\left\{\left(x_{j_1}, g^{f_1(x_{j_1})}\right), \cdots, \left(x_{j_\gamma}, g^{f_1(x_{j_\gamma})}\right)\right\}$，$\{j_1,j_2,\cdots,j_\gamma\} \subseteq \{1,2,\cdots,k\}$，这时对合法用户而言不会受到任何影响，但对叛逆者而言因其持有的份额被包含在发送的分组中，所以不能获得解密所需的 $k+1$ 个份额，即达到撤销叛逆者的目的。

3.7 更新过程

当撤销的叛逆者数量达到 k 时，执行密钥更新过程。DS 任选一 $u \in Z_q \setminus \{0\}$，发送 $\left(g^r, ug^{rf_1(x_0)}, g^{rb}, (i_1, g^{rf_1(i_1)}), \cdots, \left(i_\gamma, g^{rf_1(i_\gamma)}\right)\right)$，属于 $\Phi \setminus \Lambda_\gamma$ 中的合法用户按照解密算法得到 u，把自己的解密钥 $(i,\alpha_i,f(i,\alpha_i))$ 更新为 $(i,u\alpha_i,uf(i,\alpha_i))$，而叛逆者因不能得到 u，所以不能更新其解密钥。相应地，DS 将发送的分组数据更新为

$e'=\left(g^{r},s\left(g^{rf_1(x_0)}\right)^{u},g^{rb},\left(x_1,\left(g^{rf_1(x_1)}\right)^{u}\right),\cdots,\left(x_k,\left(g^{rf_1(x_k)}\right)^{u}\right),S\oplus M\right)$ $=(H,s\oplus M)$，就可以保证用户在密钥更新后按照解密算法仍能正确解密。经过这样更新后，DS 可继续撤销另外 k 个叛逆者。根据需要 DS 可无限次重复更新过程。

3.7.1 *更新后的追踪*　如果盗版解码器中包含的是更新后的解密钥，DS 在追踪时只须将输入盗版解码器的数据更新为 $(g^{r_0},A,g^{r_0b},x_n,(m_1,(g^{r_0h_1})^u),(m_2,(g^{r_0h_2})^u),\cdots,(m_k,(g^{r_0h_k})^u))$，假定盗版解码器中的解密钥为 $(i,u\alpha_i,uf(i,\alpha_i))$，则按照上述追踪算法 DS 同样可以获得 C_i，只是计算 B_i 的方式稍有不同，此时 DS 计算 B_i 的公式为 $B_i=(A/C_i)^{u^{-1}}$，经过与 text 比较确定出叛逆者。

3.7.2 *更新后的撤销*　设 $\Lambda_\gamma'=\{i_1,i_2,\cdots,i_\gamma\},\gamma\le k$ 为更新密钥后的叛逆者集合，DS 用 $\left\{\left(i_1,g^{uf_1(i_1)}\right),\cdots,\left(i_\gamma,g^{uf_1(i_\gamma)}\right)\right\}$ 取代 e' 中的任意 γ 个 $\left\{\left(x_{j_1},g^{uf_1(x_{j_1})}\right),\cdots,\left(x_{j_\gamma},g^{uf_1(x_{j_\gamma})}\right)\right\}$，$\{j_1,j_2,\cdots,j_\gamma\}\subseteq\{1,2,\cdots,k\}$，即可撤销叛逆者。

4　安全分析

设用户拥有的信息为：公开钥 e，足够多的已发送的分组头 $H_i=\left(g^{r_i},\ s_ig^{r_if_1(x_0)},\ g^{r_ib},\ x_0,\ \left(x_1,g^{r_if_1(x_1)}\right),\cdots,\left(x_k,g^{r_if_1(x_k)}\right)\right)$ 及对应的 s_i。则用户从一个新的分组头 $H=\left(g^{r},sg^{rf_1(x_0)},g^{rb},x_0,\left(x_1,g^{rf_1(x_1)}\right),\cdots,\left(x_k,g^{rf_1(x_k)}\right)\right)$ 中求 s 的计算复杂度相当于破译 ElGamal 加密体制下的密文。(证明参见文献[7]中的定理 14。)

k 个用户 $I=\{i_1,i_2,\cdots,i_k\}$ 利用他们的解密钥 $(l,\alpha_l,f(l,\alpha_l)),\ l\in I$ 和公开钥 e 构造出另外一个满足 $j\notin I,\ \alpha_j\in Z_q^*$ 的解密钥 $(j,\alpha_j,f(j,\alpha_j))$ 的计算复杂性相等于求解离散对数困难问题。(证明参见文献[3]中的引理 4)。

由 OPE 协议的性质可知 (1) 若用户在执行 OPE 时使用一个与其所选 α 不同 α'，则用户不能通过 DS 的验证；(2) DS 不能陷害一个诚实的用户。(证明略)。

如果 DDH 问题是困难的，则盗版解码器不能识别输入数据是正常数据还是用来进行追踪的数据。(证明参见文献[5]引理 5)。

5　性能比较

为了更好地说明本方案的性能，表 1 列出了文中方案与现有非对称公钥叛逆者追踪方案的对比结果。

6　结束语

本文提出的非对称公钥叛逆者追踪方案有效地解决了现有方案中存在的追踪性和撤销性不足的问题。能以完全黑盒子追踪的方式快速、准确地确定出全部的叛逆者。完备的撤销性为数据提供者提供了更好的保护。同时传输效率得到显著改善。

附录

当解密过程中要用到 Largrange 插值法时，对于叛逆者能否通过共谋构造出与其所持有的解密钥不同的新的解密钥，Yuji Watanabe 等人在其文献[5]的 3.3 节中写到：On the other hand, it seems not to be applicable to the threshold-decryption- based scheme such as … …, since a session key can be computed by combining k + 1 shares using the Lagrange interpolation, and simple convex combination of the personal keys of k traitors does not lead to the pirate key。但是文献[4]中的 Claim1 提到一种破解方式(详细过程参见文献[4])。分析其破解成功的原因，主要因为文献[5]中使用了所选多项式在零点的函数值来隐藏会话密钥，由于函数在零点的值等于函数的常数项值，在使用共谋构造的解密钥时，可通过常数项求得解密时所需的 Largrang 插值系数。所以只要不用常数项来隐藏会话密钥，这种破解方式就失去了作用。

表 1　文中方案与文献[4,5]方案的比较

Tab.1　Compare of this scheme with Ref.[4,5] schemes

	OPE 使用次数	分组长度	撤销性	追踪方式	确定一个叛逆者所需的计算量	解密密钥长度
文献[5]	2	2k+2	不具备	直接打开*		3
文献[4]	1	2k +2	不具备	部分黑盒子	2k 次输入输出	3
本方案	1	k+4	能撤销任意叛逆者	完全黑盒子	一次输入输出	3

*文献[5]中提出的黑盒子追踪实际上是黑盒子确认方式。K 为共谋门限值。

参 考 文 献

[1] Chor B, Fiat A, Naor M. Tracing traitors[A]. Advances in Cryptology-CRYPTO'94 [C], Berlin：Springer-Verlag, 1994: 257−270.

[2] Boneh D, Franklin M. An efficient public key traitor tracing scheme[A]. Proc of CRYPTO'99[C]. Berlin: Sprinber-Verlag, 1999: 338−353.

[3] Pfitzmann B. Trails of traced traitors[A]. Proc of Information Hiding'96[C]. Berlin : Springer−Verlag, 1996: 49−64.

[4] Aggelos Kiayias, Moti Yung. Breaking and repairing asymmetric public-key traitor tracing[A].Digital Rights Management: revised papers. Washington, DC, USA, November 18, 2002. Berlin Springer-Verlag, 2003: 32−50.

[5] Yuji Watanabe, Goichiro Hanaoka, Hideki Imal. Efficient asymmetric public-key traitor tracing without trusted agents [A], Topics in Cryptology-CT-RSA 2001 [C]. San Francisco, CA, USA, April 8-12, 200Berlin: Springer-Verlag, 2001: 392−407.

[6] Naor M. Pinkas B. Oblivious transfer and polynomial evaluation [A]. In Proc of STOC'99[C], 1999: 245−254.

[7] Kurosawa K, Desmedt Y. Optimum traitor tracing and asymmetric scheme [A]. Proc of EUROCRYPTO'98[C] . Berlin : Springer-Verlag, 1998: 145−157.

王青龙：　男，1970年生，博士生，研究方向为信息安全.

杨　波：　男，1963年生，教授，博士生导师，研究方向为网络安全与电子商务.