一种支持多频道服务的抗共谋的非对称公钥叛逆者追踪方案

张学军① 余国林② 周利华①
①(西安电子科技大学 计算机网络与信息安全教育部重点实验室 西安 710071)
②(西北第二民族学院信计系 银川 750021)

摘 要 该文提出一种新的叛逆者追踪方案，将会话密钥S分解成S_1与S_2之和。基于离散对数困难问题，引入多频道服务参数和特殊多项式函数来解密S_1，利用中国剩余定理来解密S_2。新方案具有支持多频道服务、抗共谋、非对称性、用户密钥的耐用性、黑盒子追踪等优点，并且在DDH(Diffie-Hellman Problem)困难问题的假设下证明了新方案是语义上安全的，通过分析表明新方案的整体性能明显好于已有方案。

关键词 多频道服务，抗共谋，非对称，用户密钥的耐用性，黑盒子追踪
中图分类号：TN918，TP309 **文献标识码**：A **文章编号**：1009-5896(2006)11-2127-03

A Collusion-Resistant Asymmetric Public-Key Traitor Tracing Scheme for Multi-channel Services

Zhang Xue-jun① Yu Guo-lin② Zhou Li-hua①
①(*Ministry of Edu. Key Lab. of Computer Network and Info. Security, Xidian Univ., Xi'an* 710071, *China*)
②(*The Second Northwest Institute Ethnic Minority, Yinchuan* 750021, *China*)

Abstract A new traitor tracing scheme is proposed , whose essential idea is the session key S is divided into a sum of S_1 and S_2. Based on DL(discrete logarithm)problem, S_1 is decrypted by introducing a multi-channel service parameter and a special polynomial function, S_2 is decrypted by Chinese Remainder Theorem. The new scheme has many advantages such as multi-service, collusion-resistance, asymmetry, long-lived subscriber's key and black-box tracing. It is proved to be semantically secure under the DDH (Diffie-Hellman Problem) assumption and its whole capabilities are much better than that of the existing ones.

Key words Multi-channel service, Collusion-resistance, Asymmetry, Long-lived subscriber's key, Black-box tracing

1 引言

叛逆者追踪[1–4]是保护数据提供商(Data Supplier，DS)和合法用户的一个热点问题。文献[5]提出了一种抗共谋的付费电视方案，但其方案是对称方案(不具有不可否认性)，并且还属于私钥方案(只有特定的人才能发送加密数据)，同时仅支持单个电视频道的服务。文献[1]提出了一种完全的非对称公钥叛逆者追踪方案，但其方案不能抵抗共谋攻击。因此，本文提出了一种支持多频道服务(如多个电视频道服务等)的非对称公钥叛逆者追踪方案，核心思想是将会话密钥S分解成S_1与S_2之和，由方案1[5] 经过修改后来解密S_1，由方案2[1]来解密S_2。与现有方案相比较，新方案具有支持多频道服务、抗共谋、非对称、用户密钥的耐用性、黑盒子追踪等众多优点，并且在DDH(Diffie-Hellman Problem)困难问题的假设下证明了新方案是语义上安全的，通过分析表明新方案的整体性能明显好于已有方案[1,3–5]。

2 方案 1

该方案是方案 1[5]修改后的方案，原方案和本文修改后方案的比较如表 1 所示。

表 1 方案 1[5]和本文修改后的方案的比较

Tab.1 A comparison between scheme1[5] and our nodified scheme

	算法类型	频道类型	抗共谋	增加/撤消用户	用户密钥耐用性
方案 1[5]	私钥算法	单频道	支持	支持	部分支持
修改方案	公钥算法	多频道	支持	支持	部分支持

2.1 系统设置

系统管理员(System Manager，SM)任选大素数 p，Z_p^*是阶为 q 的乘法群，$q \mid p-1$，$g \in Z_p^*$为生成元。设 $x_i \in_R Z_q$，$i=0,1,\cdots,n$，则次数为 n 的多项式函数 $f(x)$ 构造如下：$f(x)=\prod_{i=1}^{n}(x-x_i)=\sum_{i=0}^{n}a_i x^i (\mathrm{mod}\, q)$，其中系数 $\{a_i\}$ 为 $a_0=\prod_{j=1}^{n}(-x_j)$，$a_1=\sum_{i=1}^{n}\prod_{i\neq j}^{n}(-x_j),\cdots,a_{n-2}=\sum_{i\neq j}^{n}(-x_i)(-x_j)$，$a_{n-1}=\sum_{i=1}^{n}(-x_j)$，$a_n=1$，$\sum_{i=0}^{n}a_i x_j^i=0$。令$\{g^{a_0},g^{a_1},\cdots,g^{a_n}\}=\{g_0,g_1,\cdots,g_n\}$，其中$\prod_{i=0}^{n}g_i^{x_j^i}=1$。

设 n 为最大用户数的上限，实际用户数为 m，$0<m\le n$，$n-m$ 提供新用户加入系统时用。以下步骤 SM 将构造加密公钥和用户解密密钥：

步骤 1 选择 n 个不同的随机数 $x_i \in_R Z_q$，其中 $i=1,$

2005-04-14 收到，2006-01-06 改回
国家自然科学基金（60372046）和华为基金（YSCB2005037NP）资助课题

$2,\cdots,n$。

步骤 2 计算 $A=\prod_{j=1}^{n}(\prod_{i=0}^{n-1}g_i^{x_j^i})\bmod p$，$A$ 只需要计算一次。

步骤 3 计算 $\overline{x}_i=\sum_{k\neq i}^{n}x_k^n \bmod q$。

步骤 4 计算 $\hat{x}_i=s_i x_i^n \bmod q$。选取每对 $s_i,s_i'\in Z_q$，对于 $i=1,\cdots,n$，使得 $s_i s_i'=s_i' \bmod q$。

步骤 5 DS 选定频道 l 对应的随机数 e_l ($e_l\in Z_q$)，秘密安全地传送给 SM 作为对频道 l 的注册，e_l 是保密的。SM 然后选择随机数 b，令 $s=\prod_{i=1}^{n}s_i' \bmod q$。SM 的主密钥 SK 为 $f(x)$ 和 q，公钥 $\mathrm{PK}=(p,g,g^s,g^{bs},g^{-e_l s},A^{bs})$。

2.2 用户注册

用户 i 注册时，SM 将 $(\overline{x}_i,\hat{x}_i)$ 发送给 i 作为其密钥。

2.3 用户订阅频道

用户 i 订阅频道 l 后，SM 将频道密钥 $K_i^l=b\hat{x}_i+e_l\overline{x}_i\hat{x}_i$ 发送给用户 i，记录订购单 $\mathrm{text}=i\,\|\,g^{s\overline{x}_i}\,\|\,g^{bsK_i^l}\,\|\,g^{-e_l s\overline{x}_i\hat{x}_i}$。$(\overline{x}_i,\hat{x}_i,K_i^l)$ 为用户 i 对频道 l 的解密钥。

2.4 加密算法

数据提供商选 $\overline{s}\in_R Z_p^*$ 作为加密消息时使用的对称密钥，$r\in_R Z_q$，计算 $\overline{g}=g^{sr}$，$\hat{g}=g^{bsr}$，$\tilde{g}=g^{-e_l sr}$，$c=\overline{s}A^{bsr}$，广播密文 $(\overline{g},\hat{g},\tilde{g},c)$。

2.5 解密算法

$$c\hat{g}^{\overline{x}_i}\overline{g}^{K_i^l}\tilde{g}^{\overline{x}_i\hat{x}_i}=\overline{s}$$

定理 1 经过注册的合法用户能够按照上述的解密算法正确解密。

证明 根据 2.1 节步骤 4 和步骤 5 的构造，有 $s_i s_i'=s_i' \bmod q$，$s=\prod_{i=1}^{n}s_i' \bmod q$，据此可以看出，对于合法的订阅用户 i，$ss_i=s \bmod q$ 成立。

$$\begin{aligned}c\hat{g}^{\overline{x}_i}\overline{g}^{K_i^l}\tilde{g}^{\overline{x}_i\hat{x}_i}&=\overline{s}A^{bsr}g^{bsr\sum_{k\neq i}^{n}x_k^n}g^{sr(bs_i x_i^n+e_l\overline{x}_i\hat{x}_i)}g^{-e_l sr\overline{x}_i\hat{x}_i}\\&=\overline{s}A^{bsr}g^{bsr\sum_{k=1}^{n}x_k^n}=\overline{s}\left(\prod_{j=1}^{n}\prod_{i=0}^{n}g_i^{x_j^i}\right)^{bsr}=\overline{s}\end{aligned}$$

定理 2 假设 DDH 问题在 Z_p^* 上是困难的，则方案 1 对于被动攻击者是语义上安全的。

证明 假设方案 1 对被动攻击者不是语义上安全的，那么就存在一个攻击者，在 Z_p^* 上可以利用此攻击者的输出结果，能够以不可忽略的优势来区分 Z_p^* 上一个四元组 (g_1,g_2,u_1,u_2) 是属于 Diffie-Hellman 四元组 $D=(g_1,g_2,g_1^a,g_2^a)$，还是属于随机四元组 $R=(g_1,g_2,g_1^a,g_2^b)$，具体过程如下：

步骤 1 设 $g_1=A^{bs}$，$g_2=g^s$。

步骤 2 将公钥 $\mathrm{PK}=(p,g,g^s,g^{bs},g^{-e_l s},A^{bs})$ 给攻击者，攻击者输出 $M_0,M_1\in Z_p^*$。

步骤 3 随机选择 $B\in\{0,1\}$，构造密文头 $C=(u_2,u_2^b,u_2^{-e_l},M_B u_1)$。

步骤 4 将密文头 C 给攻击者，攻击者输出 $B'\in\{0,1\}$。

步骤 5 如果 $B=B'$ 输出 D，否则输出 R。

可以看出，如果四元组 (g_1,g_2,u_1,u_2) 来自 D，则密文头 C 是 M_b 的加密。如果四元组 (g_1,g_2,u_1,u_2) 来自 R，那么密文头 C 是 $M_b u_1 u_2^{\lambda}$ 的加密，其中 $u_1=g_1^{\overline{a}_1}$，$u_2=g_2^{\overline{a}_2}$，$\lambda=b\sum_{i=1}^{n}x_i^n$，也就是说此时密文是随机消息的加密。因为攻击者对来自 D 或 R 的四元组 (g_1,g_2,u_1,u_2) 有不同的响应，故与 DDH 问题成立假设矛盾。 证毕

定理 3 如果用户共谋数量的上限为 k ($k<n$)，则方案 1 能以很高的概率抵抗共谋。

证明 不失一般性，先假设有两个合法用户 i 和 j，其解密钥分别为 $(\overline{x}_i,\hat{x}_i,K_i^l)$ 和 $(\overline{x}_j,\hat{x}_j,K_j^l)$。如果这两个用户共谋，其可能的解密钥为 $(\theta\overline{x}_i+(1-\theta)\overline{x}_j,\theta\hat{x}_i+(1-\theta)\hat{x}_j,\theta K_i^l+(1-\theta)K_j^l)$，其中 $\theta,(1-\theta)\in Z_q$，且 $-\theta$ 为 θ 关于 q 的加法逆元。因为 q 是 SM 的主密钥之一，用户 i 和 j 均不知道 q，而要得到 q 相当于解决 Z_p^* 上的离散对数问题，概率为 $1/p$。在不知道 q 的情况下要找到 θ 关于 q 的加法逆元 $-\theta$ 是很困难的。对于用户共谋数量为 $c(2<c\leq k)$ 的情况也有类似的结论。

3 方案 2[1]

设 m 是实际用户数，选择素数 $p_i=2q_i+1$，其中 q_i 是奇素数，为方便假设 $p_1<p_2<\cdots<p_m$。令 $M=\prod_{i=1}^{m}p_i$，$\tilde{g}$ 是模每一个 p_i 的公共素根。

3.1 密钥和公钥的建立

用户 i 选密钥 $d_i\in Z_{p_i}^*$，发送 (β_i,p_i) 给 SM，$\beta_i=\hat{g}^{d_i} \bmod p_i$。SM 计算 $\beta=\sum_{i=1}^{m}\beta_i M_i y_i \bmod M, M_i=M/p_i$，$M_i y_i\equiv 1(\bmod p_i)$，$(\beta,\tilde{g},M)$ 为公钥。

3.2 加密和解密

加密：令明文 $x\in Z_{p_1}$。DS 选择随机数 $0<r<p_1$，密文 $C=(z_1,z_2)=(\tilde{g}^r,x\beta^r)$。解密：$x=z_2(z_1^{d_i})^{-1} \bmod p_i$。

定理 4[1] 方案 2[1]对于被动的攻击者是语义上安全的。

4 新方案

除非另作说明，以下介绍中的符号含义同第 2、3 小节中的说明。SM 的主密钥 SK 为 $f(x)$ 和 q，SM 公布的公钥为 $\mathrm{PK}=(p,g,g^s,g^{bs},g^{-e_l s},A^{bs})\,\|\,(\beta,\tilde{g},M)$。

4.1 用户注册

用户 i 注册时，产生的密钥为 $(\overline{x}_i,\hat{x}_i)\,\|\,d_i$。

4.2 用户订阅频道

用户 i 订阅频道 l 后，$(\overline{x}_i,\hat{x}_i,K_i^l)\,\|\,d_i$ 成为用户 i 对频道 l 的解密钥，SM 记录订购单 $\mathrm{text}=i\,\|\,(g^{s\overline{x}_i}\,\|\,g^{bsK_i^l}\,\|\,g^{-e_l s\overline{x}_i\hat{x}_i})\cdot \bmod p\,\|\,\tilde{g}^{d_i} \bmod p_i$。

4.3 加密算法

DS 随机选 $\overline{s}<p$ 作为加密消息时使用的对称密钥，不妨设 $p_1<p_2<\cdots<p_m<p$。令 $\overline{s}=\overline{s}_1+\overline{s}_2$，其中 $\overline{s}_1<p,\overline{s}_2<p_1$，选择 $r\in_R Z_{p_1}$。DS 发送的六元组密文头为

$$((\overline{g},\hat{g},\tilde{g},c),\ (z_1,z_2))=((g^{sr},g^{bsr},g^{-e_l sr},\overline{s}_1A^{bsr}) \bmod p,\ (\tilde{g}^r,\overline{s}_2\beta^r) \bmod M)$$

4.4 解密算法

步骤 1　利用 2.5 节解密算法可得到 $\overline{s}_1 \bmod p$ 。

步骤 2　利用 3.2 节解密方法可得到 $\overline{s}_2 \bmod p_i$ 。

步骤 3　$\overline{s}_1 \bmod p + \overline{s}_2 \bmod p_i = (\overline{s}_1 + \overline{s}_2) \bmod p = \overline{s} \bmod p = \overline{s}$ 。

4.5 追踪算法

定理 5[3]　假设DDH问题是困难的，则盗版解码器不能识别合法密文头与非法密文头。

当 SM 得到一个解密钥为 $(\alpha_1,\alpha_2,\alpha_3)\|d_i$ 的盗版解码器后，任选 3 个线性无关的向量 $\boldsymbol{Z}_j=(z_{j1},z_{j2},z_{j3})\in Z_q^3$，$j=1,2,3$，构造 3 个非法密文头：$C_j=((g^{sz_{j1}},g^{bsz_{j2}},g^{-e_l sz_{j3}},W) \bmod p,(g^r,\overline{s}_2\beta^r) \bmod M)=((h_1^{z_{j1}},h_2^{z_{j2}},h_3^{z_{j3}},W) \bmod p,(g^r,\overline{s}_2\beta^r) \bmod M)$。

当输入一个非法头 C_j 给解码器时，解码器按照正常的解密算法输出一个值 $R_j=(Wh_1^{z_{j1}\alpha_1}h_2^{z_{j2}\alpha_3}\ h_3^{z_{j3}\alpha_1\alpha_2})+\overline{s}_2 (\bmod p)$。通过输入 3 个非法头 $C_j, j=1,2,3$，得到 3 个不同的输出 R_j。由 R_1,R_2,R_3 联立可解出 $h_1^{\alpha_1}$，$h_2^{\alpha_3}$ 和 $h_3^{\alpha_1\alpha_2}$，即 $g^{s\alpha_1},g^{bs\alpha_3},g^{-e_l s\alpha_1\alpha_2}$。通过比较确定出与之相对应的定购单 $\text{text}=i\|(g^{s\overline{x}_i}\|g^{bsK_i^l}\|g^{-e_l s\overline{x}_i\hat{x}_i}) \bmod p\|\hat{g}^{d_i} \bmod p_i$，即用户 i 为叛逆者。因为具有非对称性，所以 SM 可以提供不可否认证据，用户不能抵赖其叛逆行为。

4.6 用户密钥的耐用性

用户密钥的耐用性是指当增加用户或者撤消用户时无需改变现有用户的密钥，而只需改变公钥 $\text{PK}=(p,g,g^s,g^{bs},g^{-e_l s},A^{bs})\|(\beta,\hat{g},M)$ 即可。

情形 1　若用户 γ 已被撤消(用户 γ 是叛逆者或自愿离开系统)，则 SM 进行如下操作：先计算新的 s,M：$s'=\prod_{i=1,i\neq\gamma}^{n} s_i' \bmod q$，$M'=M(p_\gamma)^{-1}$。然后，公布新的公钥 PK：$\text{PK}=(p,g,g^{s'},g^{bs'},g^{-e_l s'},A^{bs'})\|(\beta \bmod M',\hat{g},M')$。这样一来，用户 γ 不能解密 $\overline{s}$，从而其密钥就失效了，但是现有用户的密钥此时无需改变。

情形 2　若一个新用户 $m+1$ 加入这个系统，则 SM 只需重新计算 PK 中的 $(\beta,\hat{g},M)$：$(\hat{\beta},\hat{g},\hat{M})=(\beta p_{m+1}v+\beta_{m+1}Mw \cdot \bmod Mp_{m+1},\hat{g},Mp_{m+1})$，其中 p_{m+1} 是新的素数且不同于 $p_1,p_2,\cdots,p_m$，$p_m v\equiv 1(\bmod M)$，$Mw\equiv 1(\bmod p_{m+1})$。SM 公布新的 PK 为：$\text{PK}=(p,g,g^s,g^{bs},g^{-e_l s},A^{bs})\|(\hat{\beta},\hat{g},\hat{M})$。这样一来，合法的新用户 $m+1$ 不能解密加入系统前的 $\overline{s}$，现有用户的密钥此时也无需改变。

4.7 安全性分析

(1)新方案对被动攻击者来说是语义上安全的。新方案由方案 1 和方案 2 以“叠加”方式组成，由定理 2 和定理 4 可以直接推出。

(2)如果用户共谋数量的上限为 k ($k<n$)，则新方案能以很高的概率抵抗共谋。虽然方案 2 不能抵抗共谋，但是由定理 3 可知，若用户共谋数量上限为 k ($k<n$)，则方案 1 能以很高的概率抵抗共谋，所以总体来说新方案仍能以很高的概率抵抗共谋。

(3)新方案具有前向安全性和后向安全性。由 4.6 节的分析可知，用户被撤消后，公钥已经改变，公钥中与被撤消用户相关的部分信息已经被去掉，因此被撤消用户不能解密未来的加密信息，所以新方案具有前向安全性。另一方面，增加新用户后，虽然新方案中对应于方案 1 中的公钥部分没有改变，但是新方案中对应于方案 2 中的公钥部分已经改变，因此新增加用户不能解密加入系统前的加密信息，所以总体来说新方案仍具有后向安全性。

4.8 与其它有关方案的性能比较

表 2　本文方案与其它有关方案的性能比较(n 表示实际用户总数)

Tab.2 Comparison of capabilities between our scheme and other schemes(n is the number of total users)

	文献[3]	文献[1]	文献[5]	文献[4]	本文方案
算法类型	公钥	公钥	私钥	公钥	公钥
非对称性	不支持	支持	不支持	不支持	支持
频道服务类型	单频道	单频道	单频道	单频道	多频道
抗共谋攻击	不支持	不支持	支持	不支持	支持
增加/撤消用户	不支持	支持	支持	不支持	支持
用户钥耐用性	不支持	支持	部分支持	不支持	支持
黑盒追踪	低效	n	不支持	1	3

5　结束语

本文提出了一种支持多频道服务抗共谋的非对称公钥叛逆者追踪方案，主要贡献是具有支持多频道服务、抗共谋、非对称性、用户密钥的耐用性和黑盒子追踪等优点。在DDH困难问题假设下证明了新方案是语义上安全的，分析表明其整体性能明显好于已有方案[1,3–5]。

参 考 文 献

[1] Lyuu Y, Wu M. A fully public-key traitor-tracing scheme[J]. *WSEAS Trans. on Circuits and Systems*, 2002, 1(1): 88−93.

[2] Kurosawa K, Desmedt Y. Optimum traitor tracing and asymmetric schemes.Eurocrypt’98, Espoo, Finland, 1998, LNCS, Vol.1403: 145−157.

[3] Boneh D, Franklin F. An efficient public key traitor tracing scheme. Crypto’99, Santa Barbara, California, USA,1999, LNCS Vol.1666: 338−353.

[4] Kiayias A, Yung M. Traitor tracing with constant transmission rate. Euocrypt2002, Amsterdam, the Netherlands, 2002, LNCS, Vol. 2332: 450−465.

[5] Mu Y, Varadharajan V. Robust and secure broadcasting. Indocrypt2001, Chennai, India, 2001, LNCS, Vol. 2247: 223−231.

张学军：　男，1968年生，副教授，博士生，研究方向为信息安全、叛逆者追踪.

余国林：　男，1974年生，博士生，研究方向为最优化理论与方法、信息安全.

周利华：　男，1942年生，教授，博士生导师，研究方向为网络多媒体、信息安全.