# 基于完全式公钥的叛徒追踪方案的密码分析*)

杨 军 周贤伟
(北京科技大学信息工程学院 北京 100083)

**摘 要** 由于广播加密容易受到串谋攻击,叛徒追踪方案已成为版权保护的一个重要工具。利用中国剩余定理让用户自己生成私钥,Lyuu 和 Wu 提出了面向无状态接收者的 ElGamal 类广播加密算法及黑盒可追踪方案。本文首先从群编码和参数配置的角度考察对该方案的几种安全威胁。接着,利用解密预言机发起一种适应性选择密文攻击。最后,针对其密钥管理与追踪算法的特点提出一种串谋攻击方法,使其不能追踪出所有的叛徒和真正的盗版者,表明在实际应用中完全式公钥方法存在冤枉无辜用户的安全风险。

**关键词** 广播加密,密钥管理,叛徒追踪,公钥密码学,群编码

## Cryptanalysis of Traitor-tracing Schemes Based on Fully Public Keys

YANG Jun ZHOU Xian-Wei
(School of Information Engineering, University of Science and Technology Beijing, Beijing 100083)

**Abstract** As broadcast encryption is prone to collusion attacks, traitor-tracing schemes have become an important tool for copyright protection. Using the Chinese remainder theorem Lyuu and Wu proposed an ElGamal-type broadcast encryption algorithm and a black-box traceable scheme for stateless receivers, each of which generates its own private key. We first investigate several security threats to the scheme from the perspectives of group encoding and parameter configuration. Then an adaptive chosen-ciphertext attack is launched via a decryption oracle. Finally, in accordance with the characteristics of the key management and tracing algorithm a method of collusion attack is presented so that the scheme can trace down neither all traitors nor the factual pirate, indicating that there exists the security risk of wrongly accusing innocent users when applying the approach of fully public keys in the real world.

**Keywords** Broadcast encryption, Key management, Traitor tracing, Public-key cryptography, Group encoding

## 1 引言

广播加密是在不安全信道上为大量用户安全分发数字内容的一条高效途径,它使发送者向动态变化的用户集传送秘密信息而仅有合法用户才能恢复数据成为可能。广播加密拥有大量的应用[1,2],尤其是受版权保护的媒体(DVD 电影、CD 音乐、CD-ROM 图书等)和实时 Web 商业信息通过 Internet 或有线电视的多信道广播、卫星电视订阅服务、组播通信以及对加密文件系统的访问控制等。

由于接收者子集可能随每次传输而改变(如 PPV, Pay-Per-View),动态管理密码密钥、为新用户子集高效地建立一条安全通道(即使所有的"非特权"用户一起串谋,而且即使该用户集可由一中央敌手自适应地加以选择,也不能解密给定的传输)就成为广播加密的一个重要研究课题。自从 Fiat 和 Naor 引入广播加密以来,该问题及其变体已受到极大关注和研究[1~4]。例如,接收者集合可以是固定、缓慢变化或快速变化的;方案可能支持一次、有限或无限次的广播;也可能周期地更新用户的私钥;也可能支持驱除有限或无限个的用户;还可能追踪出卖非法解密设备的"盗版者"(所谓"追踪叛徒");方案既可以基于对称密码学,也可以基于公钥密码学。

追踪叛徒的基本想法是采用一个算法,利用没收的盗版解码器追查出至少一个串谋者而以高概率不冤枉清白者。这些方案大多数是所谓黑盒可追踪的,即可用不同的输入对作为预言机的盗版解码器进行询问,但不能为了提取私钥而打开它。追踪叛徒所面临的最大困难是处理无状态的接收者,即分发给每个用户的密钥集在系统的整个生命周期内是不(能)更新的。如接收者不经常在线浏览过去的历史,或未更新其私钥,或密钥可能已被一劳永逸地置入一台防篡改的设备内。大多数叛徒追踪方案是基于对称密码机制,目前最好的这类方案[2,4]是由 Naor 等人提出的子集差分法及由 Halevi 和 Shamir 改进的分层子集差分法。

然而,基于对称密钥的广播加密存在一些局限性[2,5~8]。一是在某些情形下,人们希望让不可信的实体去广播消息(如代理加密),以改善可扩展性。二是它要求发送者存储系统所有的秘密密钥,这使得它成为一个单点故障。三是由于内容分发者知道用户的解密密钥,这样虽可追踪叛徒,但无法提供有力的证据加以起诉(可抵赖性)。Boneh 和 Franklin[5] 提出了一个公钥叛徒追踪方案:只要串谋者数量低于某个门限,则其追踪算法可抓到所有叛徒而无冤案。但该方案也有两个缺点:它只是部分地黑盒可追踪的;用户的私钥需由一可信赖的中心来生成。Lyuu 和 Wu[6] 提出了基于完全公钥的叛徒追踪方案(简称 LW 方案),声称克服了上述缺点:追踪算法是黑盒可追踪的(无论串谋者多少,可抓到所有叛徒而无冤案);用户自己生成其私钥(这种方案称为是完全式公钥的);私钥无

*)本课题得到国家自然科学基金(60573050)资助。杨 军 博士生,副教授,主要研究方向为应用密码学、网络安全和组播密钥管理;周贤伟 博士,教授,博士生导师,主要研究方向为通信网安全、宽带移动通信和组播安全等。

需随用户的添加或驱除而更新(这种方案称为是完全长寿的(perfectly long-lived))。本文在几种安全模型(明文-安全性[6](整个明文不能从它的加密形式中导出)、理想的语义特性及语义安全性)下分析LW方案面临的被动攻击;利用解密预言机对其发起一种适应性选择密文攻击;提出一种串谋攻击方法,使得完全式公钥叛徒追踪方案不能追踪出所有的串谋者和真正的盗版者,并使其在实际应用中存在冤枉无辜用户的可能性;讨论完全长寿性与"1影响$n$问题"[9](单个的组成员资格变化影响所有其他的组成员)的关系。分析表明,这类方案有若干安全隐患及局限性。

## 2 Lyuu-Wu方案:简要回顾

基于下述引理,Lyuu-Wu[6]提出了公钥加密-叛徒追踪-密钥更新方案(简称LW方案)。

**引理** 设$p$为安全素数,即$p=2q+1$,其中$q$也是素数,则$\forall a\in\{2,3,\cdots,p-2\}$,$-a^2$均为模$p$的二次非剩余及原根。

设$s$为一安全参数,$n$为订阅者总数。选择$n$个$s$-比特素数$p_i=2q_i+1$,其中诸$q_i$均为奇素数,$\sqrt{q_1}$足够大。记$M=\prod_{i=1}^{n}p_i$,不妨设$p_1<p_2<\cdots<p_n$。令$g$为诸模数$p_i$的一个公共原根(任选引理中的$-a^2$均可),则由Euler定理和中国剩余定理可得$g$模$M$的阶$\mathrm{ord}_M(g)=2q_1q_2\cdots q_n$。LW方案由以下六个算法组成:

密钥生成:任一用户$i$随机选择其私钥$d_i\in Z_{p_i}^*$,计算$\beta_i=g^{d_i} \bmod p_i$,并把$(\beta_i,p_i)$发送至分发器;分发器计算$M_i=M/p_i$,$y_i=M_i^{-1} \bmod p_i$及$\beta=\prod_{i=1}^{n}\beta_iM_iy_i \bmod M$。三元组$(g,\beta,M)$为加密密钥。所有的系统参数除$d_i$外均可公开。

加密:令明文$x\in Z_{p_1}$。分发器选择随机数$r\in Z_{p_1}$,然后计算密文$C=(z_1,z_2)$如下:

$$z_1=g^r \bmod M,\ z_2=x\beta^r \bmod M \tag{1}$$

解密:对任意给定的密文$C=(z_1,z_2)$,任一用户$i$用其解密密钥$(d_i,p_i)$恢复明文如下:

$$x=z_2(z_1^{d_i})^{-1} \bmod p_i$$

叛徒追踪:1)计算$\alpha_i=\beta \bmod M_i$;2)用公钥$(g,\alpha_i,M_i)$加密一条选择的明文$x$得到密文$C$;3)馈送$C$到黑盒解码器。若输出不是$x$,则用户$i$就是一个叛徒。判别准则的实质是:设$(d_1,p_1),(d_2,p_2),\cdots,(d_k,p_k)$是参与盗版的所有解密密钥,$M_k'=p_1p_2\cdots p_k$,则用户$i$为叛徒当且仅当$M_k'\equiv 0 \pmod{p_i}$。

密钥更新:当用户$i$是叛徒或欲离开系统时,加密密钥更新为

$$(g,\hat{\beta},\hat{M})=(g,\beta \bmod (M/p_i),M/p_i)$$

当有新用户$n+1$加入系统时,加密密钥更新为

$$(g,\hat{\beta},\hat{M})=(g,(\beta p_{n+1}v+\beta_{n+1}Mw) \bmod (Mp_{n+1}),Mp_{n+1})$$

其中新选择的素数$p_{n+1}\notin\{p_1,p_2,\cdots,p_n\}$,$v=p_{n+1}^{-1} \bmod M$,$w=M^{-1} \bmod p_{n+1}$。在上述两种情形,所有旧用户的私钥均保持不变。

增强加密算法:在上述加密算法中把$g$换成$g^2$;在明文$x\in Z_{p_1}$中最不重要的位填充一位使其总是奇(或偶)数;对$x^2$加密,得密文$C=(z_1,z_2)$:

$$z_1=g^{2r} \bmod M,\ z_2=x^2\beta^r \bmod M \tag{2}$$

## 3 对LW方案的密码分析

LW方案中的两个加密算法可视为$Z_p^*$($p$为安全素数)上ElGamal加密体制[10,11]的某种多元($Z_M^*$上)推广。但因系统参数配置不同,以及循环群$Z_p^*$与Abel群$Z_M^*$之间具有不同态的结构(前者有个原根,为*Euler*函数,而后者没有原根[12]),故其实现效率与安全性质将有较大差异。

首先考虑加密算法的群编码问题。由$\beta\equiv\beta_i \pmod{p_i}$,知$\beta\in Z_M^*$。为将加密算法的安全性归约到$Z_M^*$的循环子群$\langle g\rangle=\{g^i \bmod M: 0\leqslant i<2q_1q_2\cdots q_n\}$上Diffie-Hellman问题的困难性,在加密之前必须[12~14]构造一个从消息空间$Z_{p_1}$到$\langle g\rangle$的1-1编码映射$\Omega$,然后才计算密文$z_2=\Omega(x)\beta^r \bmod M$。然而由于$M$为合数时,到$Z_M^*$的真子群内的编码是目前公认的困难工作[12~14],这样的加密算法不具有实用性。出于上述原因,加密算法回避了子群编码问题,直接在$Z_M^*$中进行密码运算。这就造成一定的安全隐患。

其次考虑增强加密算法的群编码问题。注意到$0\notin\langle g^2\rangle=\{g^{2i} \bmod M: 0\leqslant i<q_1q_2\cdots q_n\}$($Z_M^*$的所有二次剩余的循环子群),但有$\{x^2: x\in Z_{p_1}^*\}\subseteq\langle g^2\rangle$。可见,若将明文空间限制为$Z_{p_1}^*$,则编码映射可取为恒等映射,此时无需群编码。

注意到在ElGamal加密体制中没有私钥$\in Z_p^*$的取法。而在LW方案中,若允许私钥$d_i=p_i-1$,则根据Fermat定理,必有$\beta_i=g^{d_i} \bmod p_i=1$。于是,被动敌手观察到这样的传输消息$(\beta_i,p_i)$及(1)式中的密文$z_2$后,即可高效地计算出明文$x$:

$$\begin{aligned}z_2 \bmod p_i&=(x\beta^r \bmod M) \bmod p_i=(x\beta^r) \bmod p_i\\&=(x\beta_i^r) \bmod p_i=x\end{aligned}$$

因此,该加密算法不是明文-安全的。对增强加密算法有同样的结论:$d_i=(p_i-1)/2\Rightarrow\beta_i=g^{2d_i} \bmod p_i=1\Rightarrow x^2=z_2 \bmod p_i=x_i$,即

$$x^2\equiv x_i \pmod{p_i} \tag{3}$$

当$x=0\in Z_{p_1}$时,$x_i=0\in Z_{p_i}$,此时被动敌手从(3)式能惟一确定明文$x=0$。当$x\in Z_{p_1}^*$时,有$x_i\in Z_{p_i}^*$。又因$p_i\equiv 3 \pmod 4$,故方程(3)恰有一奇一偶的两个解$x=\pm x_i^{(p_i+1)/4} \bmod p_i$,故此时被动敌手也能惟一确定出明文$x$。

选择消息空间为$Z_p^*$是实现*ElGamal*加密体制的理想语义特性的必要条件[11]。与之不同,LW方案不能取得理想的语义特性。事实上,对给定的明文$x_0=0\in Z_{p_1}$,无论(1)和(2)式中的随机数$r$如何选取,恒有$z_2=0$。这意味着LW方案不能通过概率加密算法把明文消息实现均匀分布,即不能保持理想的语义特性,同时也不符合分组密码的密文尽量不确定的要求[15]。

尽管增强加密算法隐藏了明文的二次剩余特性[10,11],但它仍然不是语义安全的。事实上,敌手可选择如下两条明文$x_0=0\in Z_{p_1}$及$x_1\in Z_{p_1}-\{0\}$,因为$x_1,\beta\in Z_M^*$,敌手以概率1(必然)区分$x_0$与$x_1$被加密的结果:$0^2\beta^r=0\neq x_1^2\beta^r \pmod M$。这样,随便指出,在基于LW方案的一个混合方案[8]中,被动攻击者成功解密的概率是不可忽略的。

下面考虑对LW方案的主动攻击。假定明文$x\in Z_{p_1}^*$,且Malice(攻击者)已窃听到(1)式中的密文$C=(z_1,z_2)$。鉴于"对随机询问的随机应答"[11]是一个许多密码协议中相当标准的运行模式,且广播用户众多,我们可合理地假定Malice有条件地控制着某个用户$i$的解密盒。为盲化密文$z_2$,他均匀地选择随机数$r_i^*\in Z_{p_i}^*$,计算$z_{i2}'=r_i^*z_2 \bmod p_i$,并把他选择的密文$(z_1,z_{i2}')$发给订阅者$i$。解密后的结果为$r_i^*x \bmod p_i$。因有$x\in Z_{p_i}^*$且模的$p_i$乘法运算是群$Z_{p_i}^*$上的一个置换,故解密后的结果在订阅者$i$看来是完全随机的。于是依照上述假设,订阅者$i$把该结果返回给Malice。最后,Malice把该

结果与$(r_i^*)^{-1} \bmod p_i$相乘即获明文$x$。不难看到，上述攻击对增强加密算法仍然奏效。因此，LW方案对适应性选择密文攻击(CCA2)非常脆弱。为此，文[7]基于消息空间$\{4,9,16,\cdots,\lceil\sqrt{p}\rceil^2\}$($p$为大的安全素数)在循环子群$\langle g^2\rangle$中仿照Cramer-Shoup体制的思想构造了一个完全式公钥叛徒追踪方案，并证明了它在判定式Diffie-Hellman假设下是CCA2-安全的，但尚未研究组密钥管理的抗串谋性及叛徒审判的抗抵赖性。

抓住私钥由用户自己生成的特点，我们设计一种针对密钥更新的串谋攻击方法，表明完全式公钥方法中旧私钥的安全销毁问题(实践中此非易事：在磁性介质上完全清除数据是不可能的[16])可给叛徒的追踪与审判带来隐患(文[7]也面临类似问题)。设$u_j$是续订用户(串谋者1)，其当前解密密钥为$(d_j, p_j)$，旧的解密密钥为$(d_j', p_j')$；$u_{n+1}$是串谋者2(新加入的订阅者)，其解密密钥为$(d_{n+1}, p_{n+1})$，其中$p_j, p_j', p_{n+1}$互异，而$d_{n+1} \leftarrow d_j'$(通过串谋)。然后$u_j$把旧解码器卖给回收店。注意到由于一般有$\beta_{n+1} \neq \beta_j'$及离散对数问题的困难性，分发器事先不能从他们提交的信息$(\beta_{n+1}, p_{n+1})$及$(\beta_j', p_j')$中发现此类串谋。又因$p_{n+1}$可被窃听，$u_j$利用有效的解密密钥$(d_j', p_{n+1})$构造和出售盗版解码器。因$M_k' = p_{n+1}$，故运行$LW$叛徒追踪算法只能查出$u_{n+1}$为叛徒；按黑盒追踪方式对$u_j$却始终不能查出他为叛徒(因$(d_j, p_j)$没参与盗版，且$(d_j', p_j')$中的$p_j' \neq p_{n+1}$)。即使法官按打开盒子方式从盗版解码器中提取出物证$d_j'$，此时$u_{n+1}$把责任推到$u_j$，则$u_j$还可抵赖如下："在我第一次退出广播系统之后，由于系统进行了密钥更新，我的旧解码器已经不能正常解密，因此我在删除私钥后把它卖给了回收店。一定是某人(如回收店的工作人员)从中恢复和提取了$d_j'$，然后从事了不法活动。没想到它那么'长寿'，但我也没有物理地销毁我的过期的私钥的义务，否则哪个客户敢冒这样的风险购买这样的安全产品?"。$u_j$另一更有力的陈述是"我最近才发现旧的解码器失窃了"。另一条攻击途径是：假定$u_j^*$回收或盗窃了无辜的退订用户$u_j$的旧解码器。若$u_j$已记忆不起其中的旧私钥$d_j'$，则与第一条攻击途径类似，在$u_j^*$与$u_{n+1}$串谋盗版后$u_{n+1}$可在法官面前诬陷$u_j$！若$u_j$能记住旧私钥，则为防止受到诬陷他不得不赶在$u_{n+1}$注册之前通过安全通道向分发器挂失，但这又涉及对分发器的信任问题了。上述分析表明，鉴于离散对数问题的困难性，完全式公钥方法难于阻止私钥的非法重用。从而在实践中可导致抵赖性和诬陷问题。尽管基于密钥分发中心的方法(如Boneh-Franklin方案)在抗抵赖性方面也具有局限性，但它对上述串谋攻击是免疫的。

最后考察密钥的完全长寿性与"1影响$n$问题"[9](它被公认为是影响安全组通信方案可扩展性的一个根本原因)的关系。在逻辑密钥层次(Logical Key Hierarchy，LKH)模型中合法组成员的个体密钥也是完全长寿的，但因成员子集需共享若干密钥加密密钥(Key Encryption Keys)，故LKH遭遇"1影响$n$问题"。由于各用户之间无秘密共享，LW方案试图通过构造"多个解密密钥映射到一个加密密钥"的广播加密算法来实现合法私钥的完全长寿性，似乎解决了"1影响$n$问题"。然而，用公钥密码体制直接加密广播或组播业务数据违背了密码学应用惯例。实际上，为保障前向/后向机密性和抗串谋性，除采用周期(如每隔5秒[1])或批处理等安全策略外，广播发送方与所有用户必须始终共享一个随用户资格变化(加入/离开)而动态变化的会话密钥(如AES密钥)[4]，以发挥对称密码体制的高效性；在付费电视系统的条件接收系统[1,3]中，会话密钥还只是用于对传输加扰控制字(Control Word，CW)的加密，而CW才用于加密电视节目。换言之，若将会话密钥/ CW引入LW方案，则在每个用户完成密钥更新过程之前，这样的混合方案不能恢复新的加密广播。可见，这样的LW方案仍会遭遇"1影响$n$问题"。另外，接收方(各个用户)始终未利用加密密钥的公开性，因而在一定程度上失去了公钥密码体制用昂贵的计算代价换来的密钥管理优势。

**结束语** 鉴于在Abel群$Z_M^*$($M$为合数)的子群上编码工作的困难性，LW加密算法回避了群编码问题，但导致了若干安全隐患。私钥空间$Z_{p_i}^*$的选法使LW方案不是明文-安全的；消息空间$Z_{p_1}$的取法使其既无理想的语义特性亦非语义安全；仅用一次解密预言机即可对其形成适应性选择密文攻击。我们提出的串谋攻击方法使完全式公钥叛徒追踪方案不能用黑盒追踪方式查出所有的叛徒；即使法官用打开黑盒方式从盗版解码器中提取出了私钥而且叛徒交代了盗版的主谋，真正的盗版者还有一定的抵赖性理由，并存在冤枉无辜用户的安全风险。尽管基于完全长寿的私钥，但它在实际应用中仍然遭遇"1影响$n$问题"。面向无状态的接收者设计抗串谋、黑盒可追踪、抗抵赖和可扩展的广播加密和密钥管理方案是我们下一步的研究工作。

## 参考文献


1 Fiat A, Tassa T. Dynamic Traitor Tracing. In: Proc. Advances in Cryptology-Crypto'99 [C], LNCS. Springer-Verlag, 1999, 1666: 388～397

2 Dodis Y, Fazio N. Public-key broadcast encryption for stateless receivers. In: Feigenbaum J, ed. ACM Workshop in Digital Rights Management-DRM 2002 [C]. LNCS. Springer-Verlag, 2003, 2696: 61～80

3 屈劲，葛建华，蒋铭. 基于用户概率分组模型的密钥分法方法研究[J]. 电子学报，2003，31(8)：1266～1268

4 Adelsbach A, Greveler U. A Broadcast Encryption Scheme with Free-Riders but Unconditional Security. In: First International Conference on Digital Rights Management: Technology, Issues, Challenges and Systems [C]. Sydney, Australia, 31 October - 2 November 2005

5 Boneh D, Franklin M. An efficient public key traitor tracing scheme. In: Proc. of Crypto'99 [C], LNCS. Springer-Verlag, 1999, 1666: 338～353

6 Lyuu Y, Wu M. A fully public-key traitor-tracing scheme. WSEAS Transactions on Circuits [J], 2002, 1(1): 88～93

7 谭作文，刘卓军，肖红光. 一个安全公钥广播加密方案[J]. 软件学报，2005，16(7)：1333～1343

8 张学军，周利华，王育民. 一种抗共谋的非对称叛逆者追踪方案[J]. 计算机科学，2006，33(8)：118～120

9 Challal Y, Bouabdallah A, Seba H. A Taxonomy of Group Key Management Protocols: Issues and Solutions. Transactions on Engineering, Computing and Technology [J], 2005,6: 5～17

10 Stinson D R 著. 密码学原理与实践. 第二版. 冯登国译[M]. 北京：电子工业出版社，2003

11 Mao W 著. 现代密码学理论与实践. 王继林，等译[M]. 北京：电子工业出版社，2004

12 Menezes A J, van Oorschot P, Vanstone S 著. 应用密码学手册. 胡磊，等译[M]. 北京：电子工业出版社，2005

13 Chevallier-Mames B, Paillier P, Pointcheval D. Encoding-Free ElGamal Encryption without Random Oracles. In: Yung M, ed. The 9th International Conference on Theory and Practice in Public Key Cryptography-PKC 2006 [C], LNCS. Springer-Verlag, 2006, 3958: 91～104

14 Schnorr C P, Jakobsson M. Security of signed ElGamal encryption. In: Advances in Cryptology - ASIACRYPT 2000 [C], 6th International Conference on the Theory and Application of Cryptology and Information Security, LNCS. Springer-Verlag, 2000, 1976: 73～89

15 吴文玲，冯登国. 分组密码工作模式的研究现状[J]. 计算机学报，2006，29(1)：21～36

16 Schneier B 著. 应用密码学：协议、算法与C源程序. 第二版. 吴世忠，等译[M]. 北京：机械工业出版社，2000