第41卷 第8期 西 安 交 通 大 学 学 报 Vol.41 №8
2007年8月 JOURNAL OF XI′AN JIAOTONG UNIVERSITY Aug. 2007

新的有效叛逆者追踪方案

杨晨，马文平，王新梅
（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，710049，西安）

摘要：为了解决数字版权保护中的用户密钥泄漏问题，提出了一种基于双线性映射的叛逆者追踪方案.该方案采用双主密钥的群密钥分发策略来计算各用户的解密密钥，并基于超椭圆曲线上的双线性对构造加密、解密方案.这样，广播中心仅需传输3个群元素的控制报头信息，而在接收端的合法授权用户可以解密、恢复加密会话密钥.安全性分析结果表明，在逆Weil对假设和k-BDHI假设下，所提方案的抗合谋攻击性比较好，能够有效地对抗单用户匿名盗版攻击，也可以用来构造有效的公钥叛逆者追踪方案.

关键词：叛逆者追踪；数字版权保护；双线性映射
中图分类号：TP309 **文献标识码**：A **文章编号**：0253-987X(2007)08-0931-03

New Efficient Traitor Tracing Scheme

Yang Chen, Ma Wenping, Wang Xinmei
(Ministry of Education Key Laboratory of Computer Networks and Information Security,
Xidian University, Xi′an 710071, China)

Abstract: A new efficient traitor tracing scheme using bilinear mapping is presented in order to solve the user-key leaking problem in digital right management. The group-key distribution strategy with double master keys is employed in the proposed scheme to compute the decryption key of each user, and the encryption and decryption algorithms are constructed based on bilinear pairings on super-singular elliptic curve. The broadcasting center only needs to broadcast a controlling header with three group elements, and the authorized users can correctly decrypt the broadcasting information and recover the session key. The security analysis shows that the proposed scheme can efficiently resist the k-collusion attack and the anonymous single-user pirate attack under inverse Weil-pairing assumption and k-BDHI assumption, and in addition, it can be used to construct efficient public key traitor tracing scheme.

Keywords: traitor tracing; digital right management; bilinear map

在广播加密业务中，识别泄漏秘密信息的授权用户是一个比较棘手的问题.叛逆者追踪正是加密广播业务中的一种防止密钥泄漏、有效对抗共谋密钥攻击的数字版权保护技术.随着网络技术和计算机技术的发展，利用数字、网络技术保护知识产权已受到人们的高度重视.1994年，Fiat等人首次提出了如何在加密广播中保护解密盒中的密钥问题[1]，之后许多研究者对叛逆者追踪方案[2-7]也做了相关的研究.基于椭圆曲线上双线性映射的叛逆者追踪方案是其中的一种，其传输的密文量与叛逆者的数目是相互独立的，安全性比较高，目前逐渐成为研究的重点[8-10].

本文基于双主密钥的群密钥分发策略，提出了一种基于双线性映射的叛逆者追踪方案，该方案能有效对抗单用户的匿名攻击[10]，可提高系统的广播通信效率.

收稿日期：2006-10-19. 作者简介：杨晨(1979～)，男，博士生；王新梅(联系人)，男，教授，博士生导师. 基金项目：国家自然科学基金资助项目(60373104，90604009).

1 对抗匿名攻击的叛逆者追踪方案

1.1 基于身份的公钥基础设施

为了减小密钥认证系统的复杂度，可借用基于身份的公钥密码体制的思想，根据用户不同的身份信息分配相应的个人解密密钥.

基于身份的公钥基础设施包括可信的密钥产生中心(KGC)和参与用户，基本过程主要是建立密钥和提取私钥.首先，KGC运行参数发生器产生2个阶为大素数 q 的循环群 G_1、G_2 和一个双线性映射 $e:G_1\times G_1\rightarrow G_2$，并选择一个抗碰撞的密码哈希函数 $H:\{0,1\}^*\rightarrow Z_q^*$，然后建立密钥，即KGC随机选择保密的 $x,y\in Z_q^*$ 和 G_1 的一个秘密生成元 g_2 作为广播中心的主密钥，提取私钥，即用户 i 将个人身份信息 ID_i 提交给KGC，KGC随机选择 $v_i\in Z_q^*$ 并计算 $K_i=g^{1/(H(\mathrm{ID}_i)+x+v_iy)}\in G_1$，在 $x+v_iy+H(\mathrm{ID}_i)=0$ 的情况下，重新选择新的随机数 v_i，此时用户 i 的个人解密密钥为 (v_i,K_i).

1.2 方案描述

方案中包括 $n+1$ 个参与者，即一个广播中心和 n 个用户，用户 i 的身份信息 $u_i=\mathrm{ID}_i$，$i=1,2,\cdots,n$.每个授权用户从基于身份的公钥基础设施中获得其个人解密密钥 (v_i,K_i).如果广播中心想把数字信息(会话密钥) $s\in Z_q^*$ 安全地发送给授权用户，应作如下操作.

(1)加密.随机选择 G_1 的一个生成元 g_1，计算 $X=g_1^x$ 和 $Y=g_1^y$.选择随机数 $r\in Z_q^*$，计算控制报头信息的报头

$$H=(X^r,Y^r,g_1^r,se^r(g_1,g_2))$$

(2)解密.收到 H 之后，用户 i 应用其个人解密密钥 (v_i,K_i) 解密会话密钥 s，即

$$s=se^r(g_1,g_2)/e(K_i,X^r(Y^r)^{v_i}(g_1^r)^{H(\mathrm{ID}_i)})$$

在实际应用中，可以采用定期更新加密密钥的策略，即周期地更新会话密钥 s，以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，同时又不影响系统的安全性.

1.3 效率分析

根据方案的构造可知，控制报头信息单元仅需3个群元素，对应于每个授权用户端的密钥存储量是2个群元素.此外，加密时的计算代价主要包括3次 G_1 中的指数运算和1次双线性映射运算.如果广播中心选择相同的 g_1，并预先计算 $e(g_1,g_2)$，则在以后的加密过程中不再进行双线性映射运算，相应地需增加1次 G_2 中的指数运算.解密时，用户端的主要计算代价包括1次 G_1 中的指数运算和1次双线性映射运算，因为 G_1 中的1次乘法运算的时间与1次指数运算或1次双线性映射运算相比是可以忽略的.

1.4 叛逆者追踪检测

当一个盗版的解码器被查抄以后，数据供应商可提取出解码器中使用过的解密密钥 (v_i,K_i)，然后再与用户的注册预订信息进行比较.若赋予某用户 u_i 的解密密钥与检测出的解密密钥 (v_i,K_i) 是一致的，则断定用户 u_i 为叛逆者.在应对法律诉讼时，数据供应商从解码器中提取的 (v_i,K_i) 可作为法庭证据.

2 方案安全性分析

假设1 逆Weil假设[8]，即给定 $P\in G_1$ 和 $e(P,Q)\in G_2$，在求解椭圆曲线上离散对数困难性假设下，不存在概率多项式时间算法能够在多项式时间内以不可忽略的概率计算出 $Q\in G_1$.

假设2 扩展的逆 k 元的双线性Diffie-Hellman (k-BDHI)假设[8]，即给定 k 元 $(P,P^x,P^{x^2},\cdots,P^{x^{k-1}})\in(G_1^*)^k$，在求解椭圆曲线上离散对数困难性假设下，不存在概率多项式时间算法能够在多项式时间内以不可忽略的概率计算出 $e^{1/x}(P,P)\in G_2^*$.

假设3 k 叛逆者的合谋攻击(k-CAA)为[8]：给定不同的 $P^{\frac{1}{H(\mathrm{ID}_1)+x+v_1y}},P^{\frac{1}{H(\mathrm{ID}_2)+x+v_2y}},\cdots,P^{\frac{1}{H(\mathrm{ID}_k)+x+v_ky}}$，计算 $P^{\frac{1}{H(\mathrm{ID}_0)+x+v_0y}}$.

基于上述假设，可证明本文方案能安全地对抗合谋攻击，值得强调的是，本文方案对于任意多的非授权用户的合谋是安全的.

定理1 在逆Weil假设下，非授权用户合谋从广播信息和公开参数中得不到会话密钥 s.

证明 为了计算会话密钥 s，必须计算非授权用户集合 $e^r(g_1,g_2)$，但是从广播信息和公开参数中仅知道 g_1^r，所以依据逆Weil假设是得不到有关 g_2 的任何信息的，因此利用非授权用户集合不可能计算出 $e^r(g_1,g_2)$，也不可能计算出会话密钥 s.

在逆Weil假设下，合法的授权用户从 $(g_1^r,e^r(g_1,g_2))$ 得不到有关 g_1 与 g_2 的任何信息，因此授权用户不能有效实施文献[10]中所描述的单用户匿名盗版攻击.

定理2 在 k-BDHI假设下，不存在概率多项式时间的 k-CAA算法，使得最多 k 个授权用户集合能够

在多项式时间内以不可忽略的概率成功地合谋出有效的解密密钥.

证明　为了简化证明，在用户的秘密参数 v_i 相等的情况下先考虑方案的安全性，此时 TSZ 方案[9]是本文方案的特例.

假设 k-CAA 是存在的，并给定了 $(g, g^t, g^{t^2}, \cdots, g^{t^{k-1}}) \in (G_1^*)^{k+1}$，在特例下记 $u=u_i=x+v_iy$，$i=1,2,\cdots,k$. 令 $u=t-H(\mathrm{ID}_0)$，$g_2=g^{\prod_{i=1}^{k}(u+H(\mathrm{ID}_i))}$，通过代换，可以得到 $g_2^{\frac{1}{u+H(\mathrm{ID}_j)}}=g^{\prod_{\substack{i=1\\ i\neq j}}^{k}(u+H(\mathrm{ID}_i))}=g^{\prod_{\substack{i=1\\ i\neq j}}^{k}(t-H(\mathrm{ID}_0)+H(\mathrm{ID}_i))}$，$j=1,2,\cdots,k$. 在其中的每个方程中，$g$ 的幂是关于变量 t 的次数最高为 $k-1$ 的多项式. 由假设 k-CAA 存在可得 $g_2^{\frac{1}{u+H(\mathrm{ID}_0)}}$，进而可计算

$$g_2^{\frac{1}{u+H(\mathrm{ID}_0)}}=g_2^{\frac{1}{t}}=g^{\frac{1}{t}\prod_{i=1}^{k}(u+H(\mathrm{ID}_i))}=g^{\sum_{i=-1}^{k}a_it^i}$$

又因为给定了 $(g, g^t, g^{t^2}, \cdots, g^{t^{k-1}}) \in (G_1^*)^k$，而且 $H(\mathrm{ID}_i)$，$i=0,1,2,\cdots,k$ 互不相同，所以能够在最多 $O(k^2)$ 时间内计算 $a_i, a_{-1}\neq 0$. 因此，有 $g^{\frac{1}{t}}=(g_2^{\frac{1}{u+H(\mathrm{ID}_0)}}/g^{\sum_{i=0}^{k}a_it^i})^{a_{-1}^{-1}}$，进而可以计算 $e^{\frac{1}{t}}(g,g)=e(g,g^{\frac{1}{t}})$. 因此，在 k-CAA 存在的假设下，k-BDHI 问题是可解的.

在上述方案中，由于主密钥 $x, y \in Z_q^*$ 和用户密钥 v_i 的存在，加上方案中用户所选用的 G_1 的生成元 g_1 和 g_2 都是保密的，所以当系统公开保密参数 g_1、y、v_i 时，上述方案与修正的 TSZ[9] 方案是等价的. 因此，上述方案的安全性至少不低于修正的 TSZ 方案，且修正的 TSZ 方案可以看作该方案的一个特例. 如果系统固定 g_1、$X=g_1^x$ 和 $Y=g_1^y$，则上述方案可以转化为公钥叛逆者追踪方案，任何实体都可应用公开参数向系统用户进行加密广播，同时又不影响系统的安全性.

超椭圆曲线密码可以提供更少的带宽需求，在同等安全水平下，所用的基域比一般椭圆曲线密码(ECC)所用的基域要小，同时可以模拟基于一般乘法群上的几乎所有的协议(如 DSA，ElGamal 等)，并在同样的定义域上，亏格越大($g\leqslant 4$)，曲线越多，可以选取用于密码中的安全曲线的余地也越大. 在实际操作中，操作数的长度在 50～80 之间(依赖于亏格的取值)，所建立的密码体制就能够抗击目前的已知攻击. 例如，取亏格为 3，则所基于的有限域的大小可以是 60 b，由此建立的密码体制的安全性与 180 b 的 ECC 等同，远远大于 1 024 b 的 DSA. 如果使用 64 b 处理器的计算机，则超椭圆曲线的运算就可以用单个计算机的字去处理，从而避免了多精度整数运算，存储和运算也更为简单. 为了优化系统的广播传输带宽，增强方案的安全性，可以根据实际需要适当地选用定义在 $GF(q^n)$ 上的形如 $y^2+xy=f(x)$ 的超椭圆曲线来构造所应用的双线性映射 $e: G_1\times G_1\rightarrow G_2$，该类曲线上的离散对数问题在对抗 Weil Descent 代数攻击上是安全的，详见文献[11-13].

3　结　论

本文利用超椭圆曲线上的双线性对构造了一种基于逆 Weil 对问题和 k-BDHI 问题的叛逆者追踪方案，它能安全、有效地对抗单用户匿名盗版攻击. 该方案减少了系统所需的广播通信带宽，降低了计算复杂度，提高了广播通信效率，同时也可以用来构造公钥叛逆者追踪方案. 所提方案具有构造简单、数据单元小、传输的密文量与用户的数目相互独立等优点. 在那些带宽和内存受限的情形下，设计这类安全、有效的叛逆者追踪方案将是一个很有意义的、挑战性很强的研究课题. 如何在此基础上构造出高效的黑盒追踪算法，将是一个急需解决的研究难题.

参考文献：

[1] Fiat A, Naor M. Broadcast encryption [C]// Proceedings of the 13th Annual International Cryptology Conference. Berlin: Springer-Verlag, 1994:480-491.

[2] Chor B, Fiat A, Naor M. Tracing traitors [C]// Proceedings of the 13th Annual International Cryptology Conference. Berlin: Springer-Verlag, 1994:257-270.

[3] Pftzmann B. Trials of traced traitors [C]// Proceedings of the 1996 1st International Workshop on Information Hiding. Berlin: Springer-Verlag, 1996:49-63.

[4] Boneh D, Franklin M. An efficient public key traitor tracing scheme [C]// Proceedings of 19th Annual International Cryptology Conference. Berlin: Springer-Verlag, 1999:338-353.

[5] Kiayias A, Yung Moti. Traitor tracing with constant transmission rate [C]// Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2002: 450-465.

[6] Kiyaias A, Yung M. Breaking and repairing asymmetric public-key traitor tracing [C]// ACM Workshop on Digital Right Management. Berlin: Springer-Verlag, 2002:32-50.

[7] McGregor J P, Yin Y L, Lee R B. A traitor tracing scheme based on RSA for fast decryption [C]// Proceedings of Applied Cryptography and Network Security. Berlin: Springer-Verlag, 2005: 56-74.

[8] Mitsunari S, Sakai R, Kasahara M. A new traitor tracing scheme [J]. IEICE Trans Fundamentals, 2002, E85-A(2):481-484.

[9] To V D, Safavi-Naini R, Zhang F. New traitor tracing schemes using bilinear map [C]// Proceedings of the ACM Workshop on Digital Rights Management. Berlin: Springer-Verlag, 2003:67-76.

[10] Chabanne H, Phan D H, Pointcheval D. Public traceability in traitor tracing schemes [C]// Proceedings of 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2005: 542-558.

[11] Menezes A J. Elliptic curve public key cryptosystems [M]. Dordrecht, Netherlands: Kluwer Academic Publishers, 1993.

[12] 张方国. 超椭圆曲线密码体制的研究 [D]. 西安:西安电子科技大学通信工程学院,2001.

[13] 程相国. 基于双线性对的签名体制的研究 [D]. 西安:西安电子科技大学通信工程学院,2006.

(编辑 苗凌)