两个可证明安全盲签名方案的密码学分析

胡小明　黄上腾

（上海交通大学计算机科学与工程系　上海 200240）

摘　要　最近，Liao 等人提出了一个基于双线性对的在标准模型下可证明安全的盲签名方案；Chen 等人提出了一个在随机预言机模型下可证明安全的限制性盲签名方案。在本文中，给出了这两个方案的密码学分析，指出它们都是不安全的。Liao 等人的方案和 Chen 等人的方案都不满足不可伪造的特性。同时，Liao 等人的方案也不满足盲性，Chen 等人的方案不满足限制性。

关键词　盲签名，伪造攻击，限制性，安全分析

Cryptanalysis of Two Provably Secure Blind Signature Schemes

HU Xiao-ming　HUANG Shang-teng

(Department of Computer Science and Engineering, Shanghai Jiaotong Univ., Shanghai 200240, China)

Abstract　Recently, Liao et al. proposed one pairing-based blind signature scheme that is provably secure in the standard model, and Chen et al. proposed one restrictive blind signature scheme that is provably secure in the random oracle. In this paper, security analysis of the two schemes is given, and their insecurity is pointed out. Both Liao et al.'s scheme and Chen et al.'s scheme don't satisfy the unforgeability property. At the same time, Liao et al.'s scheme also doesn't satisfythe blindness property and Chen et al.'s scheme doesn't satisfy the restrictiveness property.

Keywords　Blind signature, Forgery attack, Restrictiveness, Security analysis

1　引言

1982 年，Chaum 提出了盲签名的概念[1]。盲签名允许用户对任意给定的信息进行签名，但是签名者不能从签名的信息中得到任何关于所签消息的具体内容。盲签名有两个重要的特性：不可伪造性和盲性。不可伪造性保证用户即使从签名者那里得到了多个有效的盲签名也不能伪造一个有效的签名；而盲性保证在盲签名发布以后，签名者不能将发布的签名和他以前的签名联系起来。盲签名的这些特性使得它在现实生活中有着广泛的应用，如在电子现金系统、匿名电子投票系统等均有使用。从 Chaum 提出第一个盲签名以来，已经有许多的盲签名方案被提出和研究[2-6]。

在电子现金系统中，为了防止同一电子硬币的多次使用，Brands 提出了限制性盲签名的概念[7]。限制性盲签名是一种特殊的盲签名，它除了拥有盲签名的所有特性外，还具有限制性。所谓限制性就是要求用户提交给签名者的消息必须满足一定的规则（如必须包含用户的身份信息等）。在电子现金系统中，我们必须保证用户从银行提取的一个电子硬币只能支付一次，即防止同一电子硬币的多次使用。如果同一电子硬币能多次使用，那么银行将遭受巨大的损失。通过使用限制性，用户无论何时从银行提取电子硬币，银行都确信用户的身份信息已经嵌入到电子硬币中。这样，当用户重复使用同一电子硬币时，银行就能通过嵌入的身份信息将该用户揭露出来进行惩治。因此，一个安全的限制性盲签名必须满足限制性的特性。

最近，Liao 等人提出了一个基于双线性对的盲签名方案[2]，方案声称在标准模型下可证明是安全的，并给出了严格的不可伪造的安全证明。同时，方案也声称满足盲性。在 2006 年，Chen 等人提出了一个限制性盲签名方案[3]，方案声称满足正确性、盲性、限制性和不可伪造性，并构建了一个电子现金系统[3]。本文中，我们指出 Liao 等人的盲签名方案不满足不可伪造的特性，即一个攻击者能在他任意选择的消息上伪造有效的签名。我们也指出该方案不满足盲性，即当盲签名发布后，签名者能将他以前的签名与发布的签名联系起来。同时，我们给出 Chen 等人方案的安全性分析，指出该方案不满足限制特性，即签名者会对一个攻击者选择的不满足规则的消息进行签名，最终得到一个该消息的有效签名。如果用该方案构建一个电子现金系统，那么该系统不能防止同一电子硬币的多次使用，所以不能应用在实际中。另外，我们也指出该方案不能抵抗 Cheon 的攻击[8]。在 Cheon 的攻击下，攻击者最终能求得签名者的私钥，从而可以任意地伪造有效签名，所以该方案也不满足不可伪造的特性。

2　Liao 等人的盲签名方案和安全性分析

2.1　Liao 等人的盲签名方案回顾

Liao 等人基于双线性对提出了一个盲签名方案。下面给出这个方案的描述，具体的细节可以看参考文献[2]。Liao 等人的方案由四个阶段组成：系统参数生成阶段、密钥生成阶段、盲签名发布阶段和验证阶段。

系统参数生成阶段：设 G_1 是一个加法循环群，G_2 是一个乘法循环群，且阶数都为素数 q，P 是 G_1 的生成元，e 是一个双线性映射：$G_1\times G_1\rightarrow G_2$，系统参数为 $\{G_1, G_2, e, q, P\}$。

密钥生成阶段：签名者随机选取 $s\in_R Z_q^*$ 并计算 $P_{spub}=sP$，则公钥为 P_{spub}，私钥为 s。

盲签名发布阶段：假设 $m\in_R Z_q^*$ 是要签发的消息，签名者随机选取 $b\in_R Z_q^*$，$b\neq s$，并计算 $w=bP$，然后发送 w 给接收者。

胡小明　博士生，主要研究方向为数据库安全、信息安全；**黄上腾**　教授，博士生导师，主要研究方向为数据库、数据库安全、分布信息管理系统、计算机集成制造。

1) 接收者计算 $u=mP_{spub}+U+V$，其中 $U=aw$，$a\in_R Z_q^*$，$V=aP_{spub}$，然后把 u 发送给签名者。

2) 签名者接收 u 后，计算 $v=(b+s)^{-1}(u+bP_{spub})$，并把它发送给接收者。

3) 接收者计算 $\delta=v-aP$，则消息 m 的签名为 $\{m,U,V,\delta\}$。

验证阶段：验证者收到签名 $\{m,U,V,\delta\}$ 后，验证 $e(\delta,U+V)\stackrel{?}{=}e(mP,V)e(U,P_{spub})$ 是否成立，如果成立，则认为该签名是一个有效的签名并接受，否则拒绝。

2.2 Liao 等人的盲签名方案的安全性分析

我们给出 Liao 等人的盲签名方案的安全性分析，得出该方案不满足不可伪造性和盲性。

2.2.1 伪造性

假设 $m\in_R Z_q^*$ 是攻击者选取的消息，攻击者的目标是伪造一个消息 m 的有效签名。为了伪造一个消息 m 的有效签名，攻击者首先随机选取 $a,b,c\in_R Z_q^*$。然后攻击者计算 $U=acP$，$V=abP$，$\delta=(b+c)^{-1}(mbP+cP_{spub})$，则 $\{m,U,V,\delta\}$ 是一个有效的盲签名，因为

$$\begin{aligned}e(\delta,U+V)&=e((b+c)^{-1}(mbP+cP_{spub}),a(b+c)P)\\&=e(mbP+cP_{spub},aP)\\&=e(mbP,aP)e(cP_{spub},aP)\\&=e(mP,abP)e(P_{spub},acP)\\&=e(mP,V)e(p_{spub},U)\end{aligned}$$

由上面的等式可知，攻击者伪造的盲签名 $\{m,U,V,\delta\}$ 通过了盲签名方案的验证，所以对这个方案的伪造攻击成功。

2.2.2 盲性

为了将以前的签名与用户发布的签名联系起来，签名者首先记录他所签过的所有签名的这三项信息 (w,u,v)，我们用 $(w(i),u(i),v(i))(i=1,2,\cdots)$ 表示签名者第 i 次签名所对应的 (w,u,v)。当用户发布一个签名 $\{m,U,V,\delta\}$ 后，签名者计算 $u'=mP_{spub}+U+V$，然后签名者在记录中搜索是否存在某个 i 使得 $u(i)=u'(i=1,2,\cdots)$，如果签名者找到一个匹配的 $u(i)$，那么他就知道 $(w(i),u(i),v(i))$ 是消息 m 对应的盲信息，所以该方案不满足盲性。

3 Chen 等人的限制性盲签名方案和安全性分析

Chen 等人基于双线性对提出了一个限制性盲签名方案，下面给出这个方案的描述，具体的细节可以看参考文献[3]。

3.1 Chen 等人的限制性盲签名方案回顾

系统参数生成：设 G_1 是一个加法循环群，G_2 是一个乘法循环群，且阶数都为素数 q，g 是 G_1 的生成元，e 是一个双线性映射：$G_1\times G_1\to G_2$，$H:G_1\times G_1\to G_1$ 是一个密码学哈希函数，系统参数为 $\{G_1,G_2,e,q,g,H\}$。

密钥生成：(x,y) 是签名者的私钥和公钥对，其中 $y=g^x$。

签名发布：签名者随机选取 $r\in_R Z_q$，计算 $z=m^{rx}$，$b=m^r$，$a=y^r$。然后发送 (z,b,a) 给接收者。接收者验证是否 $e(z,g)=e(b,y)=e(m,a)$，如果不满足，那么接收者终止协议，否则，接收者随机选取 $\alpha,\lambda,u\in_R Z_q$ 并计算 $m'=m^\alpha$，$z'=z^{\alpha\lambda}$，$b'=b^{\alpha\lambda}$，$a'=a^\lambda$，$\overline{m}=H(m',z',b',a')y^u$，然后发送 $\overline{m}$ 给签名者。签名者计算 $\bar{\sigma}=\overline{m}^{x^{-1}}$ 并发送 $\bar{\sigma}$ 给接收者。最后，接收者计算 $\sigma=\bar{\sigma}g^{-u}$，则消息 $m'=m^\alpha$ 的签名为 (z',b',a',σ)。

签名验证：给定消息 m' 的一个签名 (z',b',a',σ)，验证者验证下面的等式是否成立：$e(\sigma,y)=e(H(m',z',b',a'),g)$；$e(z',g)=e(b',y)=e(m',a')$。如果成立，那么该签名被认为是一个有效的签名并接受，否则拒绝。

3.2 Chen 等人的限制性盲签名方案的安全性分析

我们给出 Chen 等人的限制性盲签名方案的安全性分析，得出该方案不满足限制性，即接收者能从签名者那里得到一个消息格式不满足 $m'=m^\alpha$（即签发的消息中不包含信息 m）的签名。同时，该方案也不满足不可伪造的特性。

3.2.1 限制性

假设 m 是要嵌入到消息中的信息，接收者为了得到一个消息中不包含信息 m 的签名（即 $m'\neq m^\alpha$），他跟签名者用如下方式执行签名协议。首先，签名者随机选取 $r\in_R Z_q$，并计算 $z=m^{rx}$，$b=m^r$，$a=y^r$，发送 (z,b,a) 给接收者。然后，接收者随机选取 $\alpha,\lambda,u\in_R Z_q$，并计算 $m'=g^\alpha(\text{or }=y^\alpha)$，$z'=y^{\alpha\lambda}$，$b'=g^{\alpha\lambda}$，$a'=y^\lambda(\text{or }=g^\lambda)$，$\overline{m}=H(m',z',b',a')y^u$，发送 $\overline{m}$ 给签名者。签名者计算 $\bar{\sigma}=\overline{m}^{x^{-1}}$ 并发送 $\bar{\sigma}$ 给接收者。最后，接收者计算 $\sigma=\bar{\sigma}g^{-u}$，则 (z',b',a',σ) 是消息 $m'=g^\alpha$ 的签名。显然 $m'=g^\alpha$ 与 m 完全无关，可以验证消息 $m'=g^\alpha$ 的签名 (z',b',a',σ) 是一个有效的签名，因为

$$\begin{aligned}e(\sigma,y)&=e(\overline{m}^{x^{-1}}g^{-u},y)=e((H(m',z',b',a')y^u)^{x^{-1}}\\&\quad g^{-u},y)=e(H(m',z',b',a')^{x^{-1}}g^ug^{-u},y)=\\&\quad e(H(m',z',b',a'),g)\end{aligned}$$

$$\begin{aligned}e(z',g)&=e(y^{\alpha\lambda},g)=e(b',y)=e(g^{\alpha\lambda},y)=e(m',a')=\\&\quad e(g^\alpha,y^\lambda)(\text{or }=e(y^\alpha,g^\lambda))=e(g,g)^{xr\alpha\lambda}\end{aligned}$$

下面，我们用更通用的方式（即 Brands 的用基表示消息的方法[7]）显示 Chen 等人的方案不满足限制性。具体如下：假设存在一组使得 m 由两个基 g_1 和 g_2 组成的指数对 (μ_1,μ_2)，即 $m=g_1^{\mu_1}g_2^{\mu_2}$（多于两个基的情况类似）。下面，我们显示接收者能从签名者那里得到消息 $m'=g_1^{\beta_1}g_2^{\beta_2}$ 的一个有效签名，其中 β_1 和 β_2 是由接收者选取的，所以 m' 与 m 没有关联。为了得到消息 $m'=g_1^{\beta_1}g_2^{\beta_2}$ 一个签名，接收者作如下操作。

首先接收者发送 $m'=g_1^{\beta_1}g_2^{\beta_2}$ 给签名者让其在消息 $m'=g_1^{\beta_1}g_2^{\beta_2}$ 上签名，签名者返回 $m'^{x^{-1}}=(g_1^{\beta_1}g_2^{\beta_2})^{x^{-1}}$ 给接收者。注意，因为是盲签名，所以签名者对要签的消息没有任何信息，签名者会对接收者发送给他的任何消息进行签名，因此我们能将签名者看作是一个签名预言机 $(\cdot)^{x^{-1}}$[8]。这样，当接收者向签名者要求消息 $m'=g_1^{\beta_1}g_2^{\beta_2}$ 上的一个签名时，签名者会毫不犹豫地对该消息进行签名，并将签名后的信息 $m'^{x^{-1}}=(g_1^{\beta_1}g_2^{\beta_2})^{x^{-1}}$ 发送给接收者。接着，接收者向签名者提出执行一轮限制性盲签名协议的要求，执行过程如下：1）签名者随机选取 $r\in_R Z_q$，计算 $z=m^{rx}$，$b=m^r$，$a=y^r$，并发送 (z,b,a) 给接收者；2）接收者随机选取 $\alpha,\lambda,u\in_R Z_q$，计算 $m'=(g_1^{\beta_1}g_2^{\beta_2})^\alpha$，$z'=(g_1^{\beta_1}g_2^{\beta_2})^{\alpha\lambda}$，$b'=(g_1^{\beta_1}g_2^{\beta_2})^{\frac{\alpha\lambda}{x}}$，$a'=g^\lambda$，$\overline{m}=H(m',z',b',a')y^u$，然后发送 $\overline{m}$ 给签名者；3）签名者计算 $\bar{\sigma}=\overline{m}^{x^{-1}}$ 并发送 $\bar{\sigma}$ 给接收者；3）接收者计算 $\sigma=\bar{\sigma}g^{-u}$；4）消息 $m'=g_1^{\beta_1}g_2^{\beta_2}$ 的签名为 (z',b',a',σ)。它是一个有效的签名，因为

$$\begin{aligned}e(\sigma,y)&=e(\overline{m}^{x^{-1}}g^{-u},y)=e((H(m',z',b',a')y^u)^{x^{-1}}\\&\quad g^{-u},y)=e(H(m',z',b',a')^{x^{-1}}g^ug^{-u},y)=\\&\quad e(H(m',z',b',a'),g)\end{aligned}$$

$$\begin{aligned}e(z',g)&=e((g_1^{\beta_1}g_2^{\beta_2})^{\alpha\lambda},g)=e(b',y)=e((g_1^{\beta_1}g_2^{\beta_2})^{\frac{\alpha\lambda}{x}},y)\\&=e(m',a')=e((g_1^{\beta_1}g_2^{\beta_2})^\alpha,g^\lambda)=e(g_1^{\beta_1}g_2^{\beta_2},g)^{\alpha\lambda}\end{aligned}$$

这个攻击对 Chen 等人提出的限制性部分盲签名方案也是成立的，攻击方法类似。

下面，将上面的攻击应用到 Chen 等人构建的电子现金系统中，我们指出银行账户拥有者能多次使用从银行提取的

同一电子硬币而不被银行抓住，这与作者声称的矛盾，所以该电子现金系统是不安全的。

用 U 表示一个用户，β 表示一个银行，用户 U 向银行 β 开了一个帐户 $I=g_1^{x_1}$，U 秘密地保存 u_1（u_1 是一个独一无二的信息，用来唯一地标识一个用户）并发送 I 给 β。β 保存 I，如果将来 U 多次使用同一电子硬币，那么 β 能使用 I 抓住 U。U 多次使用同一电子硬币而不被抓住的方法如下：

电子硬币提取协议阶段：U 向银行 β 提出提取一个电子硬币的要求。然后，银行 β 随机选取 $r\in_R Z_q$，计算 $z=(Ig_2)^{\alpha}$，$b=(Ig_2)^{r}$，$a=y^{r}$，发送 (z,b,a) 给用户 U。U 验证是否 $e(z,g)=e(b,y)=e(Ig_2,a)$，如果不满足，那么 U 停止该协议。否则，U 随机选取 $\alpha,\lambda,u,x_1,x_2\in_R Z_q$，计算 $A=(g_1^{\beta_1}g_2^{\beta_2})^{\alpha}$，$z'=(g_1^{\beta_1}g_2^{\beta_2})^{\alpha\lambda}$，$b'=(g_1^{\beta_1}g_2^{\beta_2})^{\frac{\alpha\lambda}{x}}$，$a'=g^{\lambda}$，$B=g_1^{x_1}g_2^{x_2}$，$\overline{m}=H(A,B,z',b',a')y^{u}$，发送 $\overline{m}$ 给 β。接着，β 计算 $\overline{\sigma}=\overline{m}^{x^{-1}}$ 并发送 $\overline{\sigma}$ 给 U。最后，U 计算 $\sigma=\overline{\sigma}g^{-u}$。这样，$U$ 从银行提取了一个电子硬币 $\{A,B,(z',b',a',\sigma)\}$，可以验证它是一个有效的电子硬币，验证过程同上。

付费协议阶段：现在假设 U 在商店 Q 购买了商品，并用上面提取的电子硬币 $\{A,B,(z',b',a',\sigma)\}$ 进行付费。首先，U 发送从银行提取的电子硬币 $\{A,B,(z',b',a',\sigma)\}$ 给 Q。然后，Q 发送 $d=H_1(A,B,IDs,date/time)$ 给 U。U 计算 $r_1=d\beta_1\alpha+x_1$ 和 $r_2=d\beta_2\alpha+x_2$ 并将 (r_1,r_2) 发送给 Q。最后，Q 验证是否 $e(\sigma,y)=e(H(A,B,z',b',a'),g),e(z',g)=e(b',y)=e(A,a')$ 和 $g_1^{r_1}g_2^{r_2}=A^dB$。在前面我们已经证明 $e(\sigma,y)=e(H(A,B,z',b',a'),g),e(z',g)=e(b',y)=e(A,a')$，所以我们只要证明 $g_1^{r_1}g_2^{r_2}=A^dB$。因为 $g_1^{r_1}g_2^{r_2}=g_1^{d\beta_1\alpha+x_1}g_2^{d\beta_2\alpha+x_2}=(g_1^{\beta_1}g_2^{\beta_2})^{\alpha d}(g_1^{x_1}g_2^{x_2})=A^dB$，所以 $\{A,B,(z',b',a',\sigma)\}$ 是一个有效的电子硬币，Q 接受该电子硬币，U 付费后取走商品。然后，用户 U 到另一家商店 S 购买商品，并想再次使用该电子硬币向 S 支付费用。U 为了向 S 支付电子硬币，他与 S 执行如下的付费协议。首先，U 发送从银行提取的电子硬币 $\{A,B,(z',b',a',\sigma)\}$ 给 S。然后，S 发送 $d'=H_1(A,B,IDs',date'/time')$ 给 U。U 计算 $r_1'=d'\beta_1\alpha+x_1$ 和 $r_2'=d'\beta_2\alpha+x_2$ 并将 (r_1',r_2') 发送给 S。最后，S 验证是否 $e(\sigma,y)=e(H(A,B,z',b',a'),g),e(z',g)=e(b',y)=e(A,a')$ 和 $g_1^{r_1'}g_2^{r_2'}=A^{d'}B$。在前面我们已经证明 $e(\sigma,y)=e(H(A,B,z',b',a'),g),e(z',g)=e(b',y)=e(A,a')$，所以我们只要证明 $g_1^{r_1'}g_2^{r_2'}=A^{d'}B$。因为 $g_1^{r_1'}g_2^{r_2'}=g_1^{d'\beta_1\alpha+x_1}g_2^{d'\beta_2\alpha+x_2}=(g_1^{\beta_1}g_2^{\beta_2})^{\alpha d'}(g_1^{x_1}g_2^{x_2})=A^{d'}B$，所以 $\{A,B,(z',b',a',\sigma)\}$ 是一个有效的电子硬币，S 接受该电子硬币，U 付费后取走商品。

存款协议阶段：一段时间后，商店 Q 将 U 的电子硬币存入银行：Q 首先将该电子硬币 $\{A,B,(z',b',a',\sigma),r_1,r_2\}$ 的交易数据发送给银行 β。然后 β 检查该电子硬币的有效性（前面我们已经证明该电子硬币是有效的）。接着 β 在它的存款数据库中查找是否 A 已经存在，因为 U 首次使用该电子硬币向 Q 支付，所以在 β 的数据库中还没有 A 的记录。β 接受该电子硬币，将数据 $\{A,date/time,r_1,r_2\}$ 存入数据库，并在 Q 的帐户上增加存款。又一段时间后，商店 S 准备将用户 U 的电子硬币存到银行去。同样地，S 首先将该电子硬币 $\{A,B,(z',b',a',\sigma),r_1',r_2'\}$ 的交易数据发送给银行 β。然后 β 检查该电子硬币的有效性（前面我们已经证明该电子硬币是有效的）。接着 β 在它的存款数据库中查找是否 A 已经存在，因为 Q 已经将该电子硬币存入银行，所以在银行数据库中已经有 A 的记录。这样 β 发现 A 已经存在，所以 β 计算 $r_1-r_1'=(d-d')\beta_1\alpha$，$r_2-r_2'=(d-d')\beta_2\alpha$。但是 $(r_1-r_1')/(r_2-r_2')=\beta_1/\beta_2$ 是一个与 u_1 毫无关系的数，所以 β 不能抓住这个多次使用同一电子硬币的用户 U。

3.2.2 伪造性

我们指出，Chen 等人的方案不能抵抗 Cheon 提出的攻击[8]，具体攻击如下：

假设攻击者被允许与签名者执行 l 轮盲签名协议。这 l 轮盲签名协议的执行过程如下：第一轮：攻击者随机选取 $u_1\in_R Z_q$，然后向签名者要求消息 $\overline{m}_1=gy^{u_1}$ 的签名。注意，因为是盲签名，所以签名者对要签的消息没有任何信息，签名者会对攻击者发送给他的任何消息进行签名，因此我们能将签名者看作是一个签名预言机 $(\cdot)^{x^{-1}}$[8]。这样，当签名者收到攻击者发来的消息 $\overline{m}_1$ 后，返回 $\sigma_1=(gy^{u_1})^{x^{-1}}$ 给攻击者。最后，攻击者计算 $g_1=\sigma_1 g^{-u_1}=g^{x^{-1}}$。第二轮：攻击者随机选取另一个整数 $u_2\in_R Z_q$，然后向签名者要求消息 $\overline{m}_2=g_1y^{u_2}$ 的签名。签名者返回 $\sigma_2=(g_1y^{u_2})^{x^{-1}}$ 给攻击者。最后，攻击者计算 $g_2=\sigma_2 g^{-u_2}=g^{x^{-2}}$。类似地，攻击者与签名者执行剩下的 $l-2$ 轮盲签名协议。最后，攻击者在与签名者执行了 l 轮盲签名协议后，得到 $(g^{x^{-1}},g^{x^{-2}},\cdots,g^{x^{-l}})$。根据文献[8]，如果 $p-1$ 有一个除数 $d\leqslant\min\{l,p^{\frac{1}{2}}\}$ 或者 $p+1$ 有一个除数 $d\leqslant\min\{\frac{l}{2},p^{\frac{1}{3}}\}$，那么在时间复杂度 $O(\sqrt{\frac{p}{d}})$ 内就能求解 $\frac{1}{x}$（由 $\frac{1}{x}$ 求解私钥 x 是非常容易的）（Cheon 指出，迄今为止，几乎所有的参数 p 都有上面的性质，即 $p-1$ 有一个除数 $d\leqslant\min\{l,p^{\frac{1}{2}}\}$ 或者 $p+1$ 有一个除数 $d\leqslant\min\{\frac{l}{2},p^{\frac{1}{3}}\}$，而找到一个没有上面性质的 p 是至今为止的一个开放问题，具体细节可以参看文献[8]）。因此，在执行了上面的操作后，攻击者成功地求得了 Chen 等人方案的签名者的私钥。在求得了私钥以后，攻击者就能使用该私钥对他任意选取的消息进行签名。所以，Chen 等人的限制性盲签名方案不满足不可伪造的特性。

这个攻击对 Chen 等人提出的限制性部分盲签名方案也是成立的，攻击方法类似。

结束语 本文回顾了 Liao 等人的基于双线性对的盲签名方案和 Chen 等人的限制性盲签名方案，并对这两个方案的安全性进行了分析。分析显示这两个方案都是不安全的，Liao 等人的方案不满足不可伪造性和盲性，而 Chen 等人的方案不满足不可伪造性和限制性。

参 考 文 献

[1] Chaum D. Blind Signatures for Untraceable Payments // Proc. Crypto 1982. New York: Plenum press, 1983: 199-203

[2] Liao J, Qi Y H, Huang PW, et al. Pairing-Based Provable Blind Signature Scheme Without Random Oracles // Proc. CIS 2005. LNCS 3802, Berlin: Springer-Verlag, 2005: 161-166

[3] Chen X F, Zhang F G, Mu Y, et al. Efficient Provably Secure Restrictive Partially Blind Signatures from Bilinear Pairings // Proc. Financial Cryptography and Data Security (FC'06). LNCS 4107, Springer-Verlag, 2006: 251-265

[4] Okamoto T. Efficient blind and partially blind signatures without random oracles // Proc. TCC 2006. LNCS 3876, Berlin: Springer-Verlag, 2006: 80-99

[5] 明洋，王育民. 两个代理签名方案的密码学分析[J]. 计算机科学，2006，33(8)：128-129

[6] 明洋，王育民. 一些可证明安全签名方案的密码学分析[J]. 计算机科学，2007，34(5)：83-84

[7] Brands S. Untraceable off-line cash in wallets with observers // Proc. Crypto 1993. LNCS 773, Berlin: Springer-Verlag, 1993: 302-318

[8] Cheon J H. Security Analysis of the Strong Diffie-Hellman Problem // Proc. Eurocrypt 2006. LNCS 4004, Springer-Verlag, 2006: 1-11