**Computer Science and Application** 计算机科学与应用, 2023, 13(3), 568-578
Published Online March 2023 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2023.133056

Hans汉斯

# 椭圆曲线上代理盲签名方案的改进

**杨倩倩，范自强**

安徽理工大学数学与大数据学院，安徽 淮南

收稿日期：2023年2月20日；录用日期：2023年3月22日；发布日期：2023年3月31日

## 摘　要

**通过对Tan等人提出的基于椭圆曲线上的离散对数问题(ECDLP)的代理盲签名方案分析，指出该方案具有不安全性，不能抵抗四种常见的伪造攻击：原始签名者和签名接收者的伪造、一般性攻击及签名接收者的一般伪造攻击，且不满足不可链接性。为了克服上述不足之处，提出了一种改进的方案，在代理授权阶段引入委托证书改进代理签名私钥，同时去掉签名生成阶段的参数，使得可以抵抗原始签名者和接收者的伪造攻击，其安全性等价于解离散对数难题，同时方案也具有不可链接性。同时在签名阶段引入签名请求者的私钥，代理签名人无法将盲消息的签名和消息签名联系起来，即签名是不可追踪的。**

## 关键词

**ECDLP，伪造攻击，委托证书，不可链接性，椭圆曲线模拟**

# Improvement of Proxy Blind Signature Scheme on Elliptic Curve

**Qianqian Yang, Ziqiang Fan**

School of Mathematics and Big Data, Anhui University of Science and Technology, Huainan Anhui

Received: Feb. 20th, 2023; accepted: Mar. 22nd, 2023; published: Mar. 31st, 2023

## Abstract

**Through the analysis of the proxy blind signature scheme based on the discrete logarithm problem on elliptic curve (ECDLP) proposed by Tan *et al.*, it is pointed out that the scheme is insecure and cannot resist four common forgery attacks: forgery of the original signer and signature receiver, general attack and general forgery attack of the signature receiver, and does not meet the requirements of unlinkability. In order to overcome the above shortcomings, an improved scheme is proposed. In the proxy authorization phase, a delegation certificate is introduced to improve the proxy signature private key, and the parameters in the signature generation phase are removed,**

文章引用: 杨倩倩, 范自强. 椭圆曲线上代理盲签名方案的改进[J]. 计算机科学与应用, 2023, 13(3): 568-578.
DOI: 10.12677/csa.2023.133056

**so that it can resist the forgery attacks of the original signer and receiver. Its security is equivalent to solving the discrete logarithm problem, and the scheme is also non linkable. At the same time, the private key of the signature requester is introduced in the signature phase, so the proxy signer cannot associate the blind message signature with the message signature, that is, the signature is untraceable.**

## Keywords

**ECDLP, Forgery Attack, Trust Certificate, Unlinkability, Elliptic Eurve Simulation**



## 1. 引言

数字签名技术在现代社会中占有非常重要的地位，为了解决用户不想在签名者签名时泄露自己的消息内容的问题，许多隐藏消息的签名方案被提出。为解决此类问题 Chaum 于 1982 年首次提出盲签名，Chaum 在文献[1]中并没有详细介绍具体的算法和步骤来实现盲签名，而是举了一个投票的例子来解释盲签名。盲签名不仅满足一般签名所具有的性质，还具有不可伪造性、不可追踪性、盲性。因为其性质好，盲签名一被公开就有各种类型的盲签名方案被提出，1985 年 Chaum 给出基于 RSA 的盲签名体制，2007 年韩春霞[2]等人提出一种 ELGamal 体制的盲签名方案，基于有限域上离散对数难解的特点设计了一种盲签名方案。为了解决签名者由于某种原因不能及时对用户进行签名的问题，Mambo 于 1996 年首次提出的代理签名方案， Mambo，Usudu 和 Okamoto 在文献[3]中提出了完整的代理签名，部分代理签名和带有权利证书的签名。代理签名也像盲签名一样要满足代理签名被广泛用于网络计算、移动代理等诸多领域，同时有许多学者提出各种各样的代理签名方案[4] [5] [6]。

代理盲签名是 Lin 和 Jan [7]于 2000 年首次提出的，该方案主要是结合代理签名与盲签名的优点。随着代理盲签名被用于不同的情景，不同的方案也被提出[8] [9] [10] [11] [12]。Tan 等(2002) [13]提出了两种分别基于 DLP 和 ECDLP 的代理盲签名方案。Lal 和 Awasthi (2003) [14]指出 Tan 等人的代理盲签名方案由于签名接收者的不诚实而遭受一种伪造攻击。与 Tan 等人的方案相比，Lal 和 Awasthi 进一步提出了一种更加有效和安全的代理盲签名方案，以克服 Tan 等人的方案中指出的缺点。Sun Hung-Min Sun 和 Bin-Tsan Hsieh [15]表明 Tan 等人的方案不满足不可伪造性和不可链接性，也指出 Lal 和 Awasthi 的方案也不具有不可链接性。但是他们没有给出克服不安全感的改进方案。针对 Tan 等人的方案不满足四种伪造攻击和不可链接性，本文结合文献[16]提出了一种的代理盲签名方案，以克服其不安全性，且证明了该方案比以前的方案更安全，更有效。

## 2. 系统参数及相关符号

设 $E$ 为有限域 $F_p$ 上的一组点集 $(x,y)$，$E$ 的整个加法群是由 $n$ 的，坐标 $x$ 和 $y$ 位于有限域 $F_p$ 且满足三次方程 $y^2 = x^3 + ax + b(modp)$，且 $4a^3 + 27b^2 \neq 0$。

$O$：原始签名者；

$P$：代理签名者；

$A$：签名验证者；

$C$：签名请求者；

$p,q$：两个大素数且 $q \mid p-1$；

$g$：$g \in Z_p^*$ 且 $g$ 的阶为 $q$；

$h(\ )$：一个安全的单向哈希函数；

$x_u$：用户 $u$ 的私钥；

$y_u$：用户 $u$ 的公钥，且 $y_u = g^{x_u}$；

$B$：$B \in E$，$B$ 是阶为 $q$ 的基点；

$Y_u$：用户 $u$ 的公钥，$Y_u = x_u B$；

$x(Q)$：点 $Q$ 的 $x$ 坐标；

$\omega$：$O,P$ 协商生成的代理签名委托证书，其中包含 $O,P$ 的身份标识、代理签名者 $P$ 的代理期限以及签名消息范围；

$A \to C$：$A$ 发消息给 $C$。

## 3. 回顾 Tan 等人提出的代理盲签名方案

Tan 等人在 Schnorr 盲签名的基础上，提出基于 DLP 和 ECDLP 的两种数字代理盲签名方案，两种方案都满足代理签名和盲签名的安全性。基于 ECDLP 的代理盲签名方案是在基于 DLP 签名方案的基础上提出的椭圆曲线模拟，在这一节我们简单回顾基于 ECDLP 的代理盲签名方案，同时给出关于该方案的密码分析。

现在我们从代理委托阶段、签名阶段、验证阶段三个方面简单描述 Tan 等人基于 ECDLP 的代理盲签名方案。

### 3.1. 代理委托阶段

步骤 1：原始签名者 $O$ 随机选择 $k_0 \in Z_q^*$，计算 $R_0$，$r_0$ 和 $s_0$

$$R_0 = k_0 B \tag{1}$$

$$r_0 = x(R_0) \tag{2}$$

$$s_0 = x_0 r_0 + k_0 \tag{3}$$

$O$ 把 $(R_0, r_0, s_0)$ 安全地发给代理签名者 $P$。

步骤 2：代理签名者 $P$ 检查等式 $R_0 = s_0 B - r_0 Y_0$，如果等式成立，$P$ 接受 $(R_0, r_0, s_0)$，承认原始签名者 $O$ 的委托签名。同时代理签名者 $P$ 代理私钥 $s_{pr} = s_0 + x_p$，上述过程可以用图清晰的描述，具体如图 1 所示。

### 3.2. 签名阶段

步骤 1：代理签名者 $P$ 随机选择数 $k \in Z_q^*$，计算 $T = kB$，再把 $k$ 发给签名验证者 $A$。

步骤 2：签名验证者 $A$ 随机挑选盲因子 $a,b \in Z_q^*$，计算：

$$L = T + bB + (-a-b)Y_P - aR_0 - (ar_0)Y_0 \tag{4}$$

$$r = x(L) \tag{5}$$

$$e = h(r \| m) \bmod q \tag{6}$$

$$U = (-e+b)R_0 + (-e+b)r_0 Y_0 - eY_0 \tag{7}$$

$$e' = (e - a - b) \bmod q \tag{8}$$

$A$ 把 $e'$ 发给 $P$。

步骤 3：$P$ 计算

$$s' = (e' s_{pr} + k) \bmod q \tag{9}$$

$P$ 把 $s'$ 再发给 $A$。

步骤 4：$A$ 计算

$$s = (s' + b) \bmod q \tag{10}$$

从而关于消息 $m$ 签名是 $(m, U, s, e)$，具体的过程如图 2 所示。

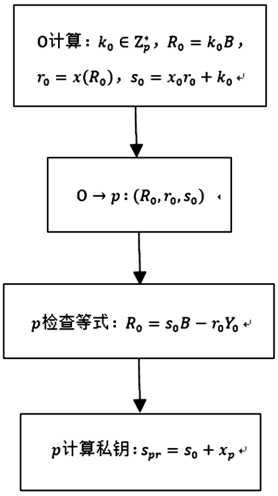


**Figure 1.** Tan *et al*.'s agent delegation stage in the ECDLP-based scheme
**图 1.** Tan 等人基于 ECDLP 的方案中的代理委托阶段

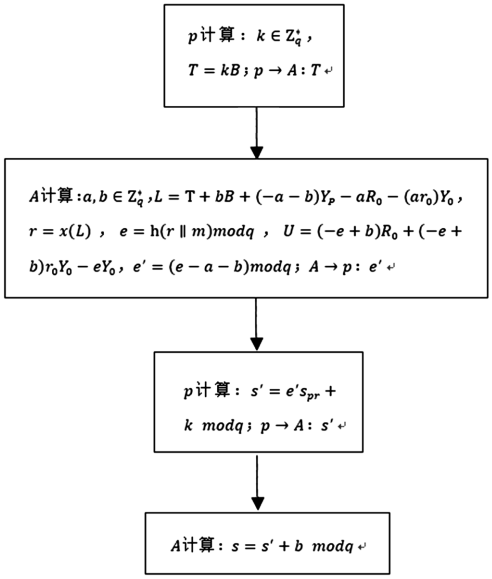


**Figure 2.** Tan *et al*. signature stage in ECDLP-based scheme
**图 2.** Tan 等人基于 ECDLP 的方案中的签名阶段

### 3.3. 验证阶段

签名验证者 $A$ 公开代理盲签名 $(m,U,s,e)$，签名接收者收到签名后，验证下面等式

$$e=h\left(x\left(sB-eY_P+eY_0+U\right)\|m\right) \tag{11}$$

若等式成立，则说明此签名是有效的；否则签名接收者拒绝接受签名。

### 3.4. 分析基于 ECDLP 的代理盲签名方案

在本节中，我们从常见的四个伪造攻击方面分析代理盲签名方案，同时也指出该方案不满足链接性。

1) 原始签名者的伪造

为了伪造一个有效的代理盲签名，原始签名者随机选择 $v\in Z_q^*$，计算点 $R_0'=\left(-Y_P+vB\right)modq$，$r_0'=x\left(R_0'\right)$，原始签名者利用参数 $v$ 伪造代理签名者的代理私钥 $s_{pr}'=\left(x_0r_0'+v\right)modq$，这是因为由 $Y_{pr}=Y_0r_0+R_0+Y_P$，从而对应 $s_{pr}'$ 的公钥为 $Y_{pr}'=Y_0r_0'+R_0'+Y_P=\left(x_0r_0'+v\right)B$，由 $Y_0r_0'+R_0'+Y_P=Y_0r_0'+vB$ 知，原始签名者利用伪造的 $s_{pr}'$ 可验证：

$$sB-eY_P+eY_0+Umodp=T+bB+\left(-a-b\right)Y_P-aR_0-\left(ar_0'\right)Y_0 \tag{12}$$

由(12)式左边可知：

$$\begin{aligned}
&sB-eY_P+eY_0+Umodp\\
&=\left[\left(e-a-b\right)\left(s_0+x_P\right)+k+b\right]B-eY_P+eY_0+Umodp\\
&=\left(e-a-b\right)s_0B+\left(e-a-b\right)x_PB+T+Bb-eY_P+eY_0+Umodp\\
&=T+Bb+\left(e-b\right)\left(Y_0r_0+R_0\right)-a\left(Y_0r_0+R_0\right)+Y_P\left(-a-b\right)+eY_0+Umodp\\
&=T+Bb+\left(-a-b\right)Y_P-aR_0-\left(ar_0\right)Y_0
\end{aligned}$$

从而有 $s_{pr}'B=Y_0r_0'+R_0'+Y_P$，因为原始签名者已构造出合适的 $R_0'$ 和 $s_{pr}'$ 满足上面的等式，从而 $s_{pr}'$ 就是一个有效的代理签名私钥，攻击者可以伪造一个有效的代理签名。

2) 签名接受者的伪造

由原方案知 $(m,U,s,e)$ 是接受者 $A$ 接收到的关于消息 $m$ 的代理盲签名，假设接受者对消息 $m'$ 伪造出一个有效的签名 $\left(m,U',s,e_f\right)$，其中 $U'=\left(-e+b\right)R_0+\left(-e+b\right)r_0Y_0-e_fY_0-ZY_P$，$e_f=h\left(r\|m\right)modq$，$Z=e-e_f$，并声称此签名为代理签名者 $P$ 所签名的。若 $sB-eY_P+eY_0+U'mo$ $dp=T+Bb+\left(-a-b\right)Y_P-aR_0-\left(ar_0\right)Y_0$ 成立，则说明该签名有效。

由等式的左边知：

$$\begin{aligned}
&sB-eY_P+eY_0+U'modp\\
&=T+Bb+\left(e-a-b\right)\left(Y_0r_0+R_0\right)+Y_P\left(e-a-b\right)-e_fY_P+e_fY_0+U'modp\\
&=T+Bb+\left(e-a-b\right)\left(Y_0r_0+R_0\right)+Y_P\left(e-a-b\right)-e_fY_P+e_fY_0+\left(-e+b\right)\left(R_0+r_0Y_0\right)-e_fY_0-ZY_Pmodp\\
&=T+Bb+\left(e-a-b\right)\left(Y_0r_0+R_0\right)+Y_P\left(e-a-b\right)-e_fY_P+\left(-e+b\right)\left(R_0+r_0Y_0\right)-\left(e-e_f\right)Y_Pmodp\\
&=T+Bb-a\left(Y_0r_0+R_0\right)+\left(-a-b\right)Y_Pmodp
\end{aligned}$$

则说明该方案容易受到接受者的一般攻击。

3) 一般伪造攻击

为了伪造一个有效的代理盲签名，攻击者首先为消息 $m$ 选择一点 $R$，并计算 $e=h\left(x\left(R\right)\|m\right)$，其次再挑选随机数 $s$，计算 $R=sB-eY_P+eY_0+U$，从而签名 $(m,U,s,e)$ 是该消息 $m$ 的有效签名，因为 $(m,U,s,e)$

可以通过等式 $e=h\left(x\left(sB-eY_P+eY_0+U\right)\|m\right)$。

4) 签名接收者的一般伪造攻击

a) 恶意的接受者 $A$ 可以证明签名 $(m,U,s,e)$ 为代理人 $F$ 而不是 $P$ 的签名，$A$ 协助没有被授权的 $F$ 进行代理签名，具体过程如下：在签名阶段时 $A$ 与 $P$ 交互信息时，$A$ 计算 $U'=(-e+b)R_0+(-e+b)r_0Y_0-eY_F modq$ 代替 $U=(-e+b)R_0+(-e+b)r_0Y_0-eY_0 modq$，这样伪造并不会干扰其他方程，且 $A$ 可以验证等式 $e=h\left(x\left(sB-eY_P+eY_0+U\right)\|m\right)$，表明签名 $(m,U,s,e)$ 是代理签名者 $F$ 的有效代理签名，从而证明了 $F$ 参与该代理盲签名过程。

b) 若攻击者 $D$ 想要取代原始签名者 $O$ 的位置，只需与接受者 $A$ 联合。因为 $A$ 可以证明 $D$ 在验证阶段代替 $O$ 产生有效的代理盲签名，具体步骤如下：$A$ 首先计算 $U''=(-e+b)R_0+(-e+b)r_0Y_0-eY_0-eY_P+eY_D modq$，修改验证方程为 $e=h\left(x\left(sB-eY_D+eY_D+U\right)\|m\right)$，这样就可以保证签名组 $(m,U'',s,e)$ 为攻击者 $D$ 代替 $O$ 进行盲签名，但实际上 $O$ 从未将自己的私钥 $x_O$ 交给 $D$。

5) 关于不可链接性

代理签名者 $P$ 为了识别已公开的消息 $m$ 与盲签名之间的关系，记录每次代理签名的中间量，比如 $T(s)$，$e'(s)$ 和 $s'(s)$。当签名 $(m,U,s,e)$ 公开时，$P$ 计算 $b'=s-s'$，$a'=e-e'-b'$ 和 $L'=T+bB+(-a'-b')Y_P-a'R_0-(a'r_0)Y_0 modp$，$r'=x(L')$，其中 $s'\in s'(s)$，$T\in T(s)$，以及 $e'\in e'(s)$，最后 $P$ 检查等式 $L'=sB-eY_P+eY_0+U$。若等式成立，$P$ 知道 $(T,e',s')$ 是与消息 $m$ 相关的盲消息，从而该方案不满足不可链接性。

## 4. 改进的方案

针对 Tan 等人提出的代理盲签名方案存在的缺陷，本文基于 Lal 和 Awasthi [14]的代理盲签名方案和柳菊霞[16]的基于离散对数的代理签名方案，通过在代理授权阶段引入委托证书改进代理签名私钥，同时去掉签名生成阶段的参数 $U$，使得新方案可以抵抗恶意的原始签名者和接收者的四个伪造攻击，同时方案也具有不可链接性。

### 4.1. 代理委托阶段

步骤 1：原始签名者 $O$ 随机选择 $k_0\in Z_q^*$，$k_0\neq 1$，计算 $R_0$，$r_0$ 和 $s_0$：

$$R_0=k_0B \tag{12}$$

$$r_0=x(R_0) \tag{13}$$

$$s_0=x_0+k_0r_0\ (modq) \tag{14}$$

$O$ 把 $(R_0,r_0,s_0)$ 安全地发给代理签名者 $P$。

步骤 2：代理签名者 $P$ 在收到代理信息 $(R_0,r_0,s_0)$ 后，验证等式 $s_0B=Y_0+R_0r_0$ 是否成立。若成立 $P$ 计算 $s_{pr}=s_0+x_p h(\omega)(modp)$ 作为代理私钥，从而代理公钥 $Y_{pr}=\left(x_0+k_0r_0+x_p h(\omega)\right)B(modp)$。上述过程可以用图清晰的描述，具体如图 3 所示。

### 4.2. 签名阶段

步骤 1：代理签名者 $P$ 随机选择 $k\in Z_q^*$，$k\neq 1$，计算 $T=kBmodp$，把 $T$ 签名请求者 $C$。

步骤 2：签名请求者 $C$ 随机挑选盲因子 $a,b\in Z_q^*$，计算：

$$L = T^2 + aB + bY_{pr} + Y_C \tag{15}$$

$$r = x(L) \tag{16}$$

$$e = h(r \| m) modq \tag{17}$$

$$e' = (b - e) modq \tag{18}$$

$C$ 把 $e'$ 发给 $P$。

步骤 3：$P$ 收到 $e'$ 后计算

$$s' = e's_{pr} + Tk(modq) \tag{19}$$

$P$ 把 $s'$ 再发给 $C$。

步骤 4：$C$ 收到 $s'$ 后计算

$$s = s' + a + x_C(modq) \tag{20}$$

从而关于消息 $m$ 的代理盲签名为 $(m, s, e)$，具体的过程如图 4 所示。

### 4.3. 验证阶段

签名接收者收到签名 $(m, s, e)$，通过验证等式：

$$e = h(x(sB + eY_{pr}) \| m)(modq) \tag{21}$$

若等式成立，则说明此代理盲签名是有效的；否则签名接收者拒绝接受签名。

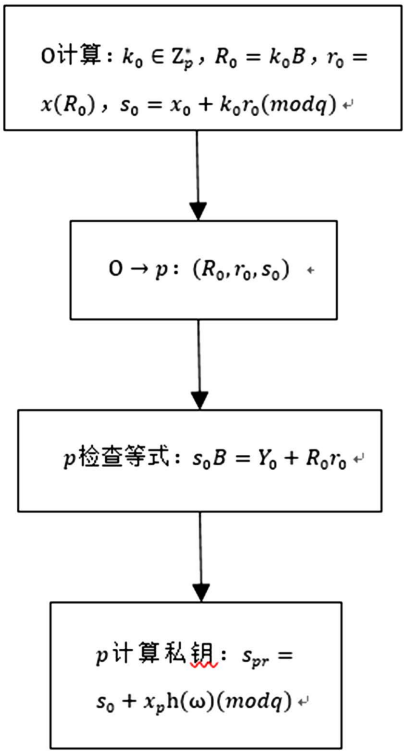


**Figure 3.** The agent delegation stage in the new scheme based on ECDLP
**图 3.** 基于 ECDLP 的新方案中的代理委托阶段

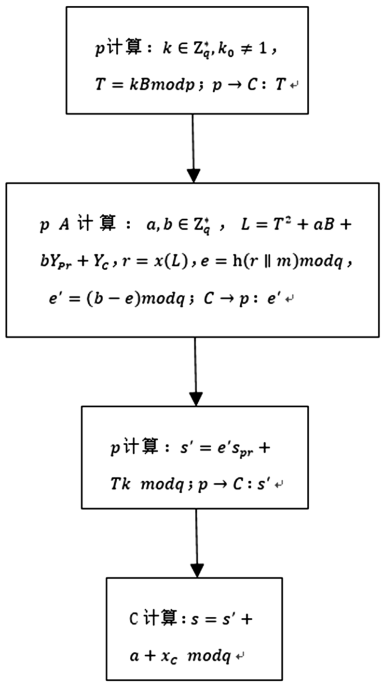


**Figure 4.** Signature phase in the new scheme based on ECDLP
**图 4.** 基于 ECDLP 的新方案中的签名阶段

## 5. 新方案的分析

### 5.1. 正确性分析

1) 在代理验证时只有当代理信息 $(R_0, r_0, s_0)$ 满足等式 $s_0 B = Y_0 + R_0 r_0 (modp)$，代理签名者 $P$ 才承认原始签名者 $O$ 的身份，从而计算代理签名私钥。

证明：等式的左边知：

$$\begin{aligned} s_0 B &= (x_0 + k_0 r_0) B \\ &= x_0 B + k_0 r_0 B \\ &= Y_0 + R_0 r_0 (modp) \end{aligned}$$

等于等式的右边，则等式 $s_0 B = Y_0 + R_0 r_0 (modp)$ 成立，代理签名者 $P$ 承认原始签名者 $O$ 的身份，从而计算代理签名私钥 $s_{pr}$。

2) 签名接收者收到签名 $(m, s, e)$ 后，验证等式(21)，若等式成立，则该代理盲签名是有效的。

证明：要验证 $e = h\left(x\left(sB + eY_{pr}\right) \| m\right)(modq)$ 等价于验证 $L = sB + eY_{pr}(modp)$，从而有

$$\begin{aligned} sB + eY_{pr} &= (s' + a + x_C) B + eY_{pr} \\ &= \left(e's_{pr} + Tk + a + x_C\right) B + eY_{pr} \\ &= \left[(b - e) s_{pr} + Tk + a + x_C\right] B + eY_{pr} \\ &= TkB + aB + (b - e) s_{pr} B + x_C B + eY_{pr} \\ &= T^2 + aB + bY_{pr} + Y_C \\ &= L(modp) \end{aligned}$$

从而有 $e=h\left(x\left(sB+eY_{pr}\right)\|m\right)(modq)=h\left(x(L)\|m\right)(modq)$。

## 5.2. 安全性分析

1) 抵抗原始签名者伪造的攻击

针对 Tan 等人的原始签名者伪造攻击，新方案的代理私钥加入签名授权证书 $h(\omega)$，即 $s_{pr}=s_0+x_P h(\omega)(modq)$。当 $h(\omega)$ 与 $Y_{pr}$ 被公开进行签名时，攻击者无法再次重新计算 $Y_{pr}$，因为伪造的签名公钥 $Y'_{pr}=Y_0+R_0 r_0+Y_P h(\omega)(modp)$，不能用于验证代理签名。同时也有原始签名者 $O$ 想伪造消息 $m'$ 的有效签名 $\left(m',s',e_f\right)$ 就必须有一个代理私钥 $s'_{pr}$ 且有 $Y'_{pr}=s'_{pr}B(modp)$，攻击者 $O$ 从等式 $sB+eY_{pr}(modp)=T^2+aB+bY_{pr}+Y_C$ 入手，即从下列等式分析：

$$\begin{aligned}sB+eY_{pr}(modp)&=\left(e's'_{pr}+Tk+a+x_C\right)B+eY_{pr}\\&=\left[(b-e)s'_{pr}+Tk+a+x_C\right]B+eY_{pr}\\&=aB+T^2+(b-e)s'_{pr}B+Y_C+eY_{pr}(modp)\end{aligned}$$

则上式变为 $aB+T^2+(b-e)s'_{pr}B+Y_C+eY_{pr}=T^2+aB+bY_{pr}+Y_C(modp)$ 入手，从而可得 $(b-e)s'_{pr}B=(b-e)Y_{pr}(modp)$，因为 $O$ 不知道随机数 $b$ 且也不知道 $e=h(r\|m)$，则原始签名者不能伪造出有效的签名。

2) 抵抗接收者的伪造攻击

由前面分析知接收者想伪造消息 $m'$ 签名 $\left(m',s,e_f\right)$，其中 $e_f=h(r\|m')(modq)$，想要此攻击成立必须有 $sB+e_f Y_{pr}(modq)=T^2+aB+bY_{pr}+Y_C$。等式左边为：

$$\begin{aligned}sB+e_f Y_{pr}(modq)&=\left(e's'_{pr}+Tk+a+x_C\right)B+e_f Y_{pr}\\&=T^2+aB+(b-e)s'_{pr}B+Y_C+e_f Y_{pr}(modq)\end{aligned}$$

则可得 $T^2+aB+(b-e)s'_{pr}B+Y_C+e_f Y_{pr}(modq)=T^2+aB+bY_{pr}+Y_C$，有 $(b-e)s'_{pr}B=\left(b-e_f\right)Y_{pr}(modq)$。因为 $e=h(r\|m)\neq e_f$，所以上式不成立，该攻击也不成立。

3) 抵抗一般伪造攻击

这里为克服一般伪造攻击，对 $U$ 进行删除，从而攻击者无法任找一点 $R$ 就可以计算出 $R=sB+eY_P$，因为 $s$ 中含有代理私钥 $s_{pr}$，由于 $s_{pr}$ 中引入授权证书 $\omega$，从而这种攻击是不成立的。且针对签名接收者的一般攻击伪造也不能成功，因为可以伪造的 $U$ 被删除了，该方案对这种类型的伪造是安全的。

4) 具有不可链接性

针对 Tan 等人的方案中不满足不可链接性，我们通过在签名阶段引入签名请求者 $C$ 的私钥 $x_C$ 求代理签名 $s=s'+a+x_C(modq)$，即使代理签名者 $P$ 保留每次签名消息也无法从 $s=s'+a+x_C(modq)$ 中获取盲因子 $a$，假设 $P$ 在等式 $e'=(b-e)modq$ 中得到 $b$，但是由于不知道 $a$ 也无法从 $L=T^2+aB+bY_{pr}+Y_C(modq)$ 得到 $L$，从而该方案具有不可链接性。

## 5.3. 效率分析

在本部分中将计算新提出的方案与 Tan 等人的方案的计算效率，设 $M$，$A$ 和 $S$ 分别表示求模乘，模加和模减的计算量，用下列的表展示我们的方案与 Tan 等人的比较，如表 1 所示。

**Table 1.** Total calculated amount of the newly proposed scheme and the scheme of Tan *et al.*
**表 1.** 新提出的方案与 Tan 等人的方案的计算总量

| 方案 | 代理委托阶段 | 签名阶段 | 验证阶段 | 总计算量 |
|---|---|---|---|---|
| Tan 等人的方案 | $4M+2A+S$ | $15M+5A+9S$ | $3M+2A+S$ | $22M+9A+11S$ |
| 我们的方案 | $6M+3A$ | $5M+6A+S$ | $2M+A$ | $13M+10A+S$ |

我们的方案中的每个阶段都有比较少的计算量，除了代理委托阶段它比 Tan 等人的方案多了 2 个模乘和 1 个模加，可以在签名阶段把这部分多出的计算量折中减少了，在某些应用中，代理签名者被委托一次但签名和验证却是多次的，在这种情况下，提议的方案的效率会随着签名和验证次数增加而增加。此外，提议方案的总量为 $13M+10A+S$，而 Tan 等人的方案的计算总量为 $22M+9A+11S$，因此，新的方案的计算效率更高。

## 6. 结语

在本文中我们回顾了 Tan 等人的方案的基于 ECDLP 的代理盲签名方案，指出基于 ECDLP 的方案容易受到多种攻击，且不满足不可链接性。在基于已有的代理盲签名方案中，通过改进代理私钥，在签名阶段引入签名请求者的私钥，提出一种新的基于 ECDLP 的代理盲签名方案，通过分析发现新方案是正确的，可以抵抗原始签名者和接收者伪造的攻击及抵抗一般伪造攻击，具有不可链接性。比较新方案与 Tan 等人的方案的计算总量，发现新方案的计算总量低于 Tan 等人的方案，进一步说明该方案的计算效率高。

## 致　谢

感谢导师范老师对本文在创作过程中提供的帮助与指导。

## 基金项目

安徽理工大学 2022 年研究生创新基金立项建设项目(2022CX2134)。

## 参考文献

[1] Chaum, D. (1983) Blind Signatures for Untraceable Payments. In: Chaum, D., Rivest, R.L. and Sherman, A.T., Eds., *Advances in Cryptology Crypto*'82, *LNCS*, Springer, Berlin, 199-203. https://doi.org/10.1007/978-1-4757-0602-4_18

[2] 韩春霞, 王琳杰. 一种 ELGamal 体制的盲签名方案[J]. 网络安全技术与应用, 2007(12): 88-89.

[3] Mambo, M., Usuda, K. and Okamoto, E. (1996) Proxy Signatures: Delegation of the Power to Sign Messages. *IEICE Transactions on Fundamentals of Electronics*, *Communications and Computer Sciences*, **E79-A**, 1338-1354.

[4] 刘为民. 基于 RSA 的代理签名方案[J]. 网络与信息, 2007(5): 66.

[5] 张计光, 王静, 尹德玉. 基于 ElGamal 体制的代理签名[J]. 高等函授学报(自然科学版), 2009(3): 57-58.

[6] 刘翠翠, 辛小龙. 基于 RSA 和 ELGamal 的代理签名方案[J]. 西南民族大学学报: 自然科学版, 2011, 37(4): 551-555.

[7] Lin, W.D. and Jan, J.K.A. (2000) Security Personal Learning Tools Using a Proxy Blind Signature Scheme. *Proceedings of International Conference on Chinese Language Computing*, lllinois, 2000, 273-277.

[8] 伊丽江, 白国强, 肖国镇. 代理多重签名: 一类新的代理签名方案[J]. 电子学报, 2001, 29(4): 569-570.

[9] 贺军, 李丽娟, 李喜梅, 等. 前向安全的代理多重数字签名方案[J]. 计算机工程, 2010, 36(14): 122-123, 126.

[10] 祁传达, 陶建平, 金晨辉. 一个安全的多重代理签名方案[J]. 计算机应用研究, 2006, 23(4): 110-111.

[11] 杨长海. 基于身份的门限多代理多盲签名方案[J]. 计算机工程与应用, 2010, 46(18): 121-124.

[12] 秦艳琳, 吴晓平. 基于 ECC 的多重代理多重盲签名方案[J]. 计算机工程, 2010, 36(11): 134-136, 139.

[13] Tan, Z., Liu, Z. and Tang, C. (2002) Digital Proxy Blind Signature Schemes Based on DLP and EDDLP. *MM Research*

*Preprints*, **21**, 212-217.

[14] Lal, S. and Awasthi, A.K. (2003) Proxy Blind Signature Scheme. *Transaction on Cryptology*, **2**, 5-11. http://eprint.iacr.org

[15] Sun, H.M., Hsieh, B.T. and Tseng, S.M. (2005) On the Security of Some Proxy Blind Signature Schemes. *Journal of Systems and Software*, **74**, 297-302. https://doi.org/10.1016/j.jss.2004.02.015

[16] 柳菊霞, 苏靖枫. 基于离散对数的代理盲签名方案[J]. 计算机工程与应用, 2010, 46(25): 94-96.