基于离散对数问题的盲数字签名*

冯登国

（中科院研究生院信息安全国家重点实验室　北京 100039）

【摘要】 该文首先说明了 Harn 的分析方法对现有的基于离散对数问题的盲数字签名并没有带来真正的威胁。其次，基于一个登记协议和 Carmenisch 等的盲数字签名方案，提出一个新型的公平盲数字签名方案，该方案提供了部分不可联系性。

【关键词】 盲数字签名；密码协议

Blind Digital Signatures Based on the Discrete Logarithm Problem

Feng Dengguo

(State Key Laboratory of Information Security Graduate School of Academia Sinica　Beijing 100039)

【Abstract】 Firstly, It is shown that Harn's cryptanalysis method does not truly bring a threat to blind digital signaturs present based on the discrete logarithm problem. Secondly, based on a registration protocol and blind digital signature scheme of Carmenisch *et al.*, a new type of fair blind digital signature scheme is proposed, and the scheme provides partial unlinkable.

【Key words】 blind digital signature; cryptographic protocol.

1　引言

Chaum 在 1982 年提出了第一个盲数字签名方案[1]，这个方案的安全性是基于分解大整数的困难性。盲数字签名是一个普通的数字签名，但它需要满足两个附加的要求：(1)消息的内容对签名者是盲的；(2)在签名被发送者泄露后，签名者不能追踪签名。

盲数字签名方案已被用来实现需要提供匿名性的各种密码协议，诸如选举协议、安全电子支付系统等。不幸的是，这种匿名性能被犯罪分子滥用。因此，Stadle 等人为了阻止这种滥用提出了一类新型的数字签名方案——公平盲数字签名方案[2]，该方案具有一个附加的特性：借助于可信中心，可将消息—签名对和签名者在协议中的观察联系起来。

在本文中，我们首先说明了 Harn 的分析方法[3]对现有的基于离散对数问题的盲数字签名并

* 中国博士后科学基金资助项目。
文稿收到日期：1996—12—17.
作者简介：冯登国，男，1965 年生，博士后，副教授，目前的主要研究兴趣为密码协议和 E—Cash 等。

没有带来真正的威胁，这表明Carmenisch等人的方案仍然是安全的。Harn注意到的这种现象在现有的所有的基于离散对数问题的盲数字签名方案[2-9]中都存在，但这种现象对这些方案的安全性并没有带来真正的威胁，这里我们以Carmenisch等人的方案为例来说明这个问题，对其他方案可用类似的方法加以讨论。其次，基于一个登记协议和Carmenisch等人的盲数字签名方案，提出了一个新型的公平盲数字签名方案，该方案提供了部分不可联系性。这表明任何盲数字签名方案都能通过一个登记协议转化为公平盲数字签名方案。现有的基于离散对数问题的公平盲数字签名方案都没有提供不可联系性，而该方案能提供部分不可联系性，部分不可联系性正是这种方案的优点。在实用中，部分不可联系性是足够的。

2 基于离散对数问题的盲数字签名方案的盲性

Harn注意到的这种现象在所有的基于离散对数问题的盲数字签名方案[2-9]中都存在。下面我们将来说明这种现象对方案的盲性并没有带来真正的威胁[4]。

2.1 Carmenisch等人的方案

系统参数如下：

——选择两个大家知道的公平大素数 p 和 q，这里 $q|(p-1)$，选择一个知道的公平阶为 q 的整数 $\alpha\in Z_p^*$，在 Z_p 上计算离散对数是困难的。

——签名者选择一个秘密密钥 x 并公开他的公钥 $y=\alpha^x \bmod p$。

产生签名的协议如下：

发送者		签名者
	$\xleftarrow{\tilde{r}}$	$\tilde{k}\in_R Z_q^*$ $\tilde{r}=\alpha^{\tilde{k}} \bmod p$
$a,b\in_R Z_q$		
$r=\tilde{r}^a\alpha^b \bmod p$		
$\tilde{m}=am\tilde{r}r^{-1} \bmod q$	$\xrightarrow{\tilde{m}}$	$\tilde{s}=(x\tilde{r}+\tilde{k}\tilde{m}) \bmod q$
$s=(\tilde{s}r\tilde{r}^{-1}+bm) \bmod q$	$\xleftarrow{\tilde{s}}$	

对消息 m 的签名是一对整数 (r,s)。

验证方程是 $\alpha^s=y^r r^m \bmod p$。

2.2 Harn对Carmenisch等人的方案的分析

签名者对所有的盲签名消息存贮 $(\tilde{m},\tilde{r},\tilde{k},\tilde{s})$。在发送者公开泄露消息 m 的签名 (r,s) 后，签名者对每一个存贮值 $(\tilde{m},\tilde{r},\tilde{k},\tilde{s})$，计算一对整数 (a',b')，这里 $a'=\tilde{m}m^{-1}\tilde{r}^{-1}r \bmod q$，$b'=m^{-1}(s-\tilde{s}r\tilde{r}^{-1}) \bmod q$。Harn认为通过检测 $r=\tilde{r}^{a'}\alpha^{b'} \bmod p$ 签名者能追踪盲签名，说明Carmenisch等人的方案没有提供盲性。

2.3 Harn的分析的漏洞

我们首先看一个引理。

引理：在Carmenisch等人的方案中，对任何固定的 $r,\tilde{r}\in Z_p^*$，方程 $r=\tilde{r}^a\alpha^b \bmod p$ 在 Z_q 上恰有 q 对解 (a,b)。

证明：由方案的签名的产生过程知，存在 s_1 和 s_2 使得 $r=\alpha^{s_1}$，$\tilde{r}=\alpha^{s_2}$。这样方程 $r=\tilde{r}^a\alpha^b \bmod p$ 等价于方程 $\alpha^{s_1}=\alpha^{as_2+b} \bmod p$，也就是 $s_1=as_2+b \bmod q$。而方程 $s_1=as_2+b \bmod q$ 在 Z_q 上恰有 q 对解(a,b)。因此，方程 $r=\tilde{r}^a\alpha^b \bmod p$ 在 Z_q 上恰有 q 对解(a,b)。

假定签名者已经签了至少 N 个消息。如果发送者公开泄露 t 个消息的签名，那么由 Harn 的分析方法知，签名者将计算出 Nt 对整数(a',b')。而在 Z_q 上共有 q^2 对整数，所以在这计算出的 Nt 对整数中每个对出现的频率为 Nt/q^2。由引理知，在 Carmenisch 等人的方案中总共有 q 对整数满足方程 $r=\tilde{r}^a\alpha^b \bmod p$。平均来说，在计算出的 Nt 对整数中有 $q\times\frac{Nt}{q^2}=\frac{Nt}{q}$ 对整数满足方程 $r=\tilde{r}^a\alpha^b$。当 $Nt\geqslant 2q$ 时，即 $\frac{Nt}{q}\geqslant 2$，签名者不能区分开两个整数对的真正发送者。因此，签名者不能追踪发送者。这正是 Harn 的分析的漏洞。在一个系统中，$Nt\geqslant 2q$ 是很容易达到的。换句话说，Harn 的分析不能对方案的盲性带来真正的威胁。

3 一种新型的公平盲数字签名方案

任何盲数字签名方案都能通过一个登记协议转化为公平盲数字签名方案。这一节我们以 Carmenisch 等人的方案为例来说明具体的转化过程。

3.1 一种新型的公平盲数字签名方案

除了 Carmenisch 等人的方案中的参数外，系统还有如下参数：

——可信中心选择一个签名方案 $\mathrm{Sig}_{TC}(\cdot)$使得每个人能验证由可信中心签名的消息。

——选择一个安全参数 k。

方案由两个协议组成，一个是在可信中心的登记协议，另一个是盲数字签名产生协议。

登记协议：

发送者		可信中心
	请求 →	选择 $A_0\in Z_q^*$，$\alpha_i\in Z_q^*$，$1\leqslant i\leqslant k$，
	← $(A_0,\mathrm{Sig}_{TC}(A_0\parallel 0))$	$\alpha_i\neq\alpha_j$，$i\neq j$
$A_i=A_0^{\alpha_i}$	← $(\alpha_1,\mathrm{Sig}_{TC}(A_1\parallel 1))$	$A_i=A_0^{\alpha_i}$
$1\leqslant i\leqslant k$	⋮	存贮$(A_0,A_1,\cdots,A_k)$
	← $(\alpha_k,\mathrm{Sig}_{TC}(A_k\parallel k))$	

在可信中心签名时，在假名 $A_i(0\leqslant i\leqslant k)$后级联数字是为了阻止不诚实的发送者置换假名。

产生签名的协议：

发送者		签名者
	$A_0,\mathrm{Sig}_{TC}(A_0\parallel 0)$ →	验证 $\mathrm{Sig}_{TC}(A_0\parallel 0)$
$\alpha_i\in_R\{\alpha_1,\alpha_2,\cdots,\alpha_k\}$	← $\tilde{Z}$	$\tilde{Z}=A_0^x$
$Z=\tilde{Z}^{\alpha_i}$		$\tilde{k}\in_R Z_q^*$
$a,b\in_R Z_q^*$	← $(\tilde{r}_1,\tilde{r}_2)$	$\tilde{r}_1=\alpha^{\tilde{k}}$，$\tilde{r}_2=A_0^{\tilde{k}}$
$\tilde{r}=\tilde{r}_1\tilde{r}_2 \bmod p$		$\tilde{r}=\tilde{r}_1\tilde{r}_2 \bmod p$
$r_1=\tilde{r}_1^a\alpha^b \bmod p$		

$r_2=\tilde{r}_1^{a}A_i^{b}\bmod p$

$r=r_1r_2\bmod p$

$\tilde{m}=amr^{-1}\tilde{r}\bmod q$ $\xrightarrow{\tilde{m}}$ $\tilde{s}=(x\tilde{r}+\tilde{k}\tilde{m})\bmod q$

$s=(\tilde{s}r\tilde{r}+bm)\bmod q$ $\xleftarrow{\tilde{s}}$

对消息 m 的签名是$(A_i,\mathrm{Sig}_{TC}(A_i\|i),z,r,s)$。

验证方程是$(A_i\alpha)^r=(yz)^r\cdot r^m$。

验证过程如下：

第一步：验证 $\mathrm{Sig}_{TC}(A_i\|i)$；

第二步：检查是否$(A_i\alpha)^r=(yz)^r\cdot r^m$。

3.2 方案的特性分析

方案的安全性、有效性和盲性等价于Carmenisch 等人的方案的安全性、有效性和盲性。显然该方案具有一个附加的特性：公平性。这里我们主要来分析一下方案的不可联系性。

同一个发送者的不同的消息—签名对之间的关系由不可联系性来表征。Carmenisch 等人的方案提供了完全的不可联系性，也就是同一个发送者的不同的消息—签名对是不可联系的。而现有的基于离散对数问题的公平盲数字签名方案都不能提供不可联系性，但我们这里提出的方案具有部分不可联系性。由签名的产生过程知，发送者为了获得消息 m 的一个盲签名，他不得不从他的 k 个假名中随机选择一个。发送者的同一个假名的不同的消息—签名对是可联系的，而发送者的不同的假名的不同的消息—签名对是不可联系的。显然，不可联系性依赖于参数 k。在实际应用中，这种部分不可联系性是足够的。

参考文献

1 Chaum D. Blind Signature for Untraceable Payments. In:Advances in cryptology:proc. crypto'82, New York:1983:199－203

2 Stadler M *et al.*,Fair Blind Signatures. In:Advances in cryptology:proc. Eurocrypt'95,New York:1995:209－219

3 Harn L. Crptanalysis of the Blind Signatures Based on the Discrete Logarithm Problem. Electronics letters,1995;31(14):1136

4 Carmenisch J L *et al.* Blind Signatures Based on the Discrete Logarithrm Problem. Rump session of Eurocrypt'94,Perugid:Italy,1994

5 Horster P *et al.* Meta Message Recovery and Meta Blind Signature based on the Discrete Logarithm Problem and their Applications pre－proceedings Asiacrypt'94,185－196

6 Chaum D *et al.* Wallet Databases with Observers. In:Advances in cryptology:proc. crypto'92, New York:1993;89－105

7 Okamoto T. Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes. In:Advances in cryptology:proc. crypto'92,New York:1993;31－53

8 Brands S. Untraceable off－line Cash in Wallet with Observers. In:Advances in cryptology:proc. crypto'93,New York:1994;302－317

9 Chen L R *et al.* Parallel Divertibility of Proofs of Knowledge Pre－proceedings Eurocrypt'94,137－149

10 Chanum D *et al.* A Secure and Privacy Protecting Protocol for Transmitting Personal Information Between Organizations. In:Advances in cryptology:proc. crypto'86, New York,1986;118－168