基于双线性对的部分盲签名中的“约分攻击”

侯整风 王 鑫 韩江洪 朱晓玲
(合肥工业大学计算机与信息学院 合肥 230009)

摘 要 研究了3个基于双线性对的部分盲签名方案,发现其签名公式存在相似性。随后对3种相应的“约分攻击”方法进行了对比分析,指出上述3个方案存在篡改协商信息攻击的根本原因。由上述分析结果得出一类基于双线性对的部分盲签名方案存在“约分攻击”的推论,并进一步对上述推论进行了验证。

关键词 双线性对,部分盲签名,篡改协商信息攻击
中图法分类号 TP309 **文献标识码** A

“Reduction Attacks” in Partially Blind Signature Based on Bilinear Pairings

HOU Zheng-feng WANG Xin HAN Jiang-hong ZHU Xiao-ling
(School of Computer and Science, Hefei University of Technology, Hefei 230009, China)

Abstract We studied three partially blind signature schemes, and found out the similarity in signature formulas of the three schemes. Then we compared and analized the three corresponding methods of “reduction attacks”, and the basic reason why these schemes are vulnerable to tampering common information attacks was pointed out. From the above analysis results, we deduced the conclusion that a class of partially blind signature schemes based on bilinear pairings are vulnerable to “reduction attacks”. Moreover, the deduction was verified.

Keywords Bilinear pairings, Partially blind signature, Tampering common information attacks

随着电子消费的不断普及与发展,传统的数字签名已难以满足人们不断提高的隐私保护的要求。1982年,Chaum[1]首次提出盲签名的概念。盲签名最基本的特性是盲性,即签名者无法得知待签名信息的具体内容,且当某一签名信息被公布时,签名者无法将其与先前具体的某次签名过程联系起来。盲签名类似于将待签名文件放入一个具有复写功能的信封中,签名者直接在信封上签名,通过信封的复写功能实现对信件的签名。

盲签名主要被应用于电子现金、电子投票等领域。然而,盲签名的完全盲性使得签名者无法确认待签名的信息,这在实际应用中会产生不便。例如,在电子现金系统中,银行为用户签发电子现金时,由于待签信息中的面值等信息无法公开,银行只能使用不同私钥代表不同的面值进行签名,导致密钥的管理复杂。

针对上述问题,Abe和Fujisaki[2]首次提出了部分盲签名的概念,即待签名消息部分公开、部分保密,并给出一个基于RSA的部分盲签名方案。此后,人们对部分盲签名展开了广泛而深入的研究。

2000年,Abe和Okamoto对部分盲签名的概念进行了形式化描述,并提出一种基于离散对数的可证安全的部分盲签名方案。Chien等[3]于2001年提出了一种基于RSA的部分盲签名方案,然而Hwang等[4]指出其不满足不可追踪性,并给出了一种攻击方法。2010年,Fang等人[5]分析了文献[4]中的攻击方法,并对文献[3]中的方案进行了改进,提出一种增强的基于RSA的部分盲签名方案。

近年来,基于双线性对的部分盲签名成为了研究的热点。2005年,Chow等人[6]利用双线性对设计了一种基于身份的部分盲签名方案,并定义了基于身份的部分盲签名方案的安全模型。2007年,Hu等人[7]提出一种基于身份的双线性对部分盲签名方案,并分析了安全性和效率,该方案比文献[6]的方案安全性更好,效率更高。之后,张学军等[8]和荣维坚[9]利用双线性对分别提出高效的基于身份的部分盲签名方案和无证书部分盲签名方案。2008年,崔巍等[10]提出了一个基于身份的部分盲签名方案和一个基于身份的受限部分盲签名方案,该方案与以往方案相比,具有更高的效率。

Kang等人[11]指出文献[7]的方案存在篡改协商信息攻击,即恶意请求者在签名过程中篡改事先协商好的公共信息,而签名依然有效。闫东升[12]分析了文献[8]的方案,指出该方案也存在篡改协商信息攻击,同时提出了一个新的基于身份的部分盲签名方案[12]。李明祥等[13]对文献[9,12]所提方案进行了分析,指出这两个方案都存在篡改协商信息攻击。

尽管人们提出了许多基于双线性对的部分盲签名方案,

到稿日期:2012-07-31 返修日期:2012-11-09 本文受安徽省自然科学基金(090412051),广东省教育部产学研结合项目(2008B0905002400)资助。

侯整风(1958—),男,教授,硕士生导师,主要研究方向为计算机网络、信息安全,E-mail:houzf@hfut.edu.cn;王 鑫(1986—),男,硕士生,主要研究方向为密码学、网络安全;韩江洪(1954—),男,教授,博士生导师,主要研究方向为智能控制、网络与信息系统;朱晓玲(1974—),女,博士生,主要研究方向为信息安全、无线自组织网络。

但许多存在篡改协商信息攻击问题。本文将研究对比 Hu 等人[7]、张学军等人[8]以及闫东升[12]分别提出的 3 种部分盲签名方案，分析这类方案不能抵抗篡改协商信息攻击的根本原因。随后对 3 种相应的攻击方法[11-13]进行对比分析，提出“约分攻击”的概念。最后推出基于双线性对的部分盲签名方案存在“约分攻击”的结论，并在崔巍等提出的两个部分盲签名方案上进行验证。

1 预备知识

1.1 双线性对

设 G_1 是一个 q 阶(q 为质数)循环加群，生成元为 P，G_2 是与 G_1 同阶的循环乘群，$a,b\in Z_q^*$。假设在 G_1 和 G_2 中离散对数问题(DLP)是困难的。双线性对是指满足以下性质的映射 $e:G_1\times G_1\to G_2$：

(1)双线性性：$e(aP,bQ)=e(P,Q)^{ab}$；　　(1)

(2)非退化性：存在 $P,Q\in G_1$，使得 $e(P,Q)\neq 1$；

(3)可计算性：对于所有的 $P,Q\in G_1$，存在有效的算法计算 $e(P,Q)$。

由上述 3 个双线性对的基本性质，可得如下 2 个推论：

(1)$e(aP,Q)=e(P,aQ)$；　　(2)

(2)$e(P+R,Q)=e(P,Q)e(R,Q)$。　　(3)

上述推论常被用于基于双线对的部分盲签名方案的验证过程。

1.2 部分盲签名的一般步骤

(1)初始化：选取参数、哈希函数，生成系统公钥等；

(2)部分盲化：请求者通过选取随机数对待签名消息进行盲化，然后通过线性运算或函数等方式将上述盲化信息与协商信息合并到一起，形成部分盲化信息；

(3)签名：签名者使用自己的私钥和协商信息对请求者发来的部分盲化信息进行签名；

(4)去盲：请求者对签名后的部分盲化信息进行去盲处理，得到最终的签名；

(5)验证：签名验证者验证签名的有效性。

1.3 篡改协商信息攻击

在部分盲签名中，签名信息一部分保密，一部分公开，公开的这部分信息称为协商信息。协商信息在部分盲签名过程中不得被修改，否则部分盲签名就失去了意义。

篡改协商信息攻击，是指签名者基于原协商信息进行部分盲签名，而攻击者在签名者无察觉的情况下，通过某种手段，用假的协商信息替换原协商信息，从而导致在验证过程中，假的协商信息有效，而原协商信息无效。

2 方案描述

Kang 等人[11]、闫东升[12]、李明祥等人[13]分别对文献[7,8,12]中的方案进行了详细分析，认为其均存在篡改协商信息攻击，并给出了相应的攻击方法。

2.1 Kang 的攻击方法

(1)篡改协商信息

文献[7]中用 c 表示协商信息，盲化阶段，请求者计算 $c'=H_3(m,Y')+bH_1(c)$，并将 c' 发送给签名者；签名者计算 $S=c'S_{ID}+rH_1(c)P_{pub}$，并将其发给请求者。请求者收到上述签名后，在去盲阶段计算 $S'=S+aH_1(c)P_{pub}$，产生部分盲签名 $\{m,c,S',Y'\}$。若验证等式

$$e(S',P)=e(H_3(m,Y')Q_{ID}+H_1(c)Y',P_{pub})$$

成立，则签名有效。

Kang 的攻击方法中，恶意请求者用假的协商信息 c^* 替换原来的协商信息 c，在盲化阶段计算 $c'^*=H_1(c)H_1(c^*)^{-1}H_3(m,Y')+bH_1(c)$，然后用 c'^* 代替 c' 发送给签名者。收到签名者返回的 $S=c'^*S_{ID}+rH_1(c)P_{pub}$ 后，恶意请求者在去盲阶段计算 $S'^*=H_1(c)^{-1}H_1(c^*)S+aH_1(c^*)P_{pub}$，产生部分盲签名 $\{m,c^*,S'^*,Y'\}$。

(2)验证

签名验证者利用假的协商信息 c^* 进行如下验证：

$$\begin{aligned}
e(S'^*,P)&=e(H_1(c)^{-1}H_1(c^*)S+aH_1(c^*)P_{pub},P)\\
&=e(H_1(c)^{-1}H_1(c^*)(c'^*S_{ID}+rH_1(c)P_{pub})+aH_1(c^*)P_{pub},P)\\
&=e(H_1(c)^{-1}H_1(c^*)((H_1(c)H_1(c^*)^{-1}H_3(m,Y')+bH_1(c))S_{ID}+rH_1(c)P_{pub}))+aH_1(c^*)P_{pub},P)\\
&=e(H_3(m,Y')S_{ID}+bH_1(c^*)S_{ID}+rH_1(c^*)P_{pub}+aH_1(c^*)P_{pub},P)\\
&=e(H_3(m,Y')S_{ID},P)e(bH_1(c^*)S_{ID}+rH_1(c^*)P_{pub}+aH_1(c^*)P_{pub},P)\quad\text{由式(3)得}\\
&=e(H_3(m,Y')Q_{ID},P_{pub})e(H_1(c^*)(bQ_{ID}+R+aP),P_{pub})\quad\text{由式(2)得}\\
&=e(H_3(m,Y')Q_{ID},P_{pub})e(H_1(c^*)Y',P_{pub})\\
&=e(H_3(m,Y')Q_{ID}+H_1(c^*)Y',P_{pub})\quad\text{由式(3)得}
\end{aligned}$$

验证等式成立。因此，该攻击方法有效。

2.2 闫东升的攻击方法

(1)篡改协商信息

文献[8]中用 $share$ 表示协商信息，盲化阶段，请求者计算 $Y=rH_1(share)Q_{ID}$，$Y'=\alpha Y+\alpha\beta Q_{ID}$，$h=\alpha^{-1}H_0(m\parallel share,Y')+\beta$，将 h 发送给签名者；签名者计算 $S=(rH_1(share)+h)S_{ID}$，并将其发给请求者。请求者收到上述签名后，在去盲阶段计算 $S'=\alpha S$，即产生最终部分盲签名 $(Y',S',m,share,ID)$。若验证等式

$$e(S',P)=e(Y'+H_0(m\parallel share,Y')Q_{ID},P_{pub})$$

成立，则签名有效。

闫东升的攻击方法中，恶意请求者用假的协商信息 $share_1$ 替换原来的协商信息 $share$，在盲化阶段计算 $Y'=\alpha(H_1(share_1)/H_1(share))Y+\alpha\beta Q_{ID}$，$h=\alpha^{-1}H_0(m\parallel share_1,Y')+\beta$，$h'=hH_1(share)/H_1(share_1)$，然后将 h' 发送给签名者。收到签名者返回的 $S=(rH_1(share)+h')S_{ID}$ 后，在去盲阶段计算 $S'=\alpha(H_1(share_1)/H_1(share))S$，产生部分盲签名 $(Y',S',m,share_1,ID)$。

(2)验证

签名验证者利用假的协商信息 $share_1$ 进行如下验证：

$$\begin{aligned}
e(S',P)&=e(\alpha(H_1(share_1)/H_1(share))S,P)\\
&=e(\alpha(H_1(share_1)/H_1(share))(rH_1(share)+h')S_{ID},P)\\
&=e(\alpha(H_1(share_1)/H_1(share))(rH_1(share)+hH_1(share)/H_1(share_1))S_{ID},P)\\
&=e(\alpha(rH_1(share_1)+h)S_{ID},P)\\
&=e((\alpha rH_1(share_1)+H_0(m\parallel share_1,Y')+\alpha\beta)S_{ID},P)
\end{aligned}$$

$=e(\alpha r H_1(share_1)Q_{ID}+\alpha\beta Q_{ID}+H_0(m\|share_1,Y')Q_{ID},P_{pub})$ 由式(2)得

$=e(Y'+H_0(m\|share_1,Y')Q_{ID},P_{pub})$

验证等式成立。因此,该攻击方法有效。

2.3 李明祥的攻击方法

(1)篡改协商信息

文献[12]中用 c 表示协商信息,盲化阶段,请求者计算 $U'=U^{\alpha}e(P,P_{pub})^{\beta}$,$h=H_2(m,c_1,U')$,$h'=\alpha h$,并将 h' 发送给签名者;签名者计算 $S=(rh'+H_3(c)+1)S_{ID}$,并将其发给请求者。请求者收到上述签名后,在去盲阶段计算 $S'=S+\beta hP_{pub}$,产生部分盲签名(m,c,U',S')。若验证等式

$$e(S',P)=U'^{H_2(m,c,U')}e(Q_{ID},P_{pub})^{H_3(c)+1}$$

成立,则签名有效。

李明祥的方案中,恶意请求者使用假的协商信息 c_1 替换原协商信息 c,盲化阶段计算 $U'=U^{\alpha}e(P,P_{pub})^{\beta}$,$h=H_2(m,c_1,U')$,$h'=\beta h$,$h''=\frac{H_3(c)+1}{H_3(c_1)+1}h'$,将 h'' 发送给签名者。收到签名者返回的 $S=(rh''+H_3(c)+1)S_{ID}$ 后,在去盲阶段计算 $S'=\frac{H_3(c_1)+1}{H_3(c)+1}S$,$S''=S'+\beta hP_{pub}$,产生部分盲签名$(m,c_1,U',S')$。

(2)验证

签名验证者利用假的协商信息 c_1 进行如下验证:

$$\begin{aligned}
e(S'',P)&=e(S'+\beta hP_{pub},P)\\
&=e(\frac{H_3(c_1)+1}{H_3(c_1)+1}S+\beta hP_{pub},P)\\
&=e(\frac{H_3(c_1)+1}{H_3(c)+1}(rh''+H_3(c)+1)S_{ID}+\beta hP_{pub},P)\\
&=e((\frac{H_3(c_1)+1}{H_3(c)+1}rh''+H_3(c_1)+1)S_{ID}+\beta hP_{pub},P)\\
&=e((\frac{H_3(c_1)+1}{H_3(c)+1}r\frac{H_3(c)+1}{H_3(c_1)+1}h'+H_3(c_1)+1)S_{ID}+\beta hP_{pub},P)\\
&=e((rh'+H_3(c_1)+1)S_{ID}+\beta hP_{pub},P)\\
&=e((r\alpha h+H_3(c_1)+1)S_{ID}+\beta hP_{pub},P)\\
&=e((r\alpha H_2(m,c_1,U')+H_3(c_1)+1)S_{ID}+\beta H_2(m,c_1,U')P_{pub},P)\\
&=U'^{H_2(m,c_1,U')}e(Q_{ID},P_{pub})^{H_3(c_1)+1}
\end{aligned}$$ 由式(1)得

验证等式成立。因此,该攻击方法有效。

3 分析与推论

3.1 对比分析

(1)文献[7,8,12]中方案的签名公式具有相似性

为方便比较,对文献[7]中方案的签名公式做一个简单的变形。3 种方案的签名公式如表 1 所列。

表 1 文献[7,8,12]中方案的签名公式

方案	签名公式
文献[7]中的方案	$S=c'S_{ID}+rH_1(c)P_{pub}=(c'Q_{ID}+rH_1(c)P)s$
文献[8]中的方案	$S=(rH_1(share)+h)S_{ID}$
文献[12]中的方案	$S=(rh'+H_3(c)+1)S_{ID}$

3 种签名公式都采用了如下相似的签名公式:

$$S=(aX+bH(Y)+c)Z \tag{4}$$

式中,$a,b,c,H(\ )$为系统参数,X 表示部分盲化信息,Y 表示协商信息,Z 表示签名密钥。

(2)约分攻击

文献[11-13]中的 3 种攻击方法对比如表 2 所列。

表 2 文献[11-13]中的攻击方法

方案	盲化阶段		去盲阶段	
	攻击前	攻击后	攻击前	攻击后
文献[11]的攻击方法	$c'=H_3(m,Y')+bH_1(c)$	$c'^*=H_1(c)H_1(c^*)^{-1}H_3(m,Y')+bH_1(c)$	$S'=S+aH_1(c)P_{pub}$	$S'^*=H_1(c)^{-1}H_1(c^*)S+aH_1(c^*)P_{pub}$
文献[12]的攻击方法	h	$h'=hH_1(share)/H_1(share_1)$	$S'=\alpha S$	$S'=\alpha(H_1(share_1)/H_1(share))S$
文献[13]的攻击方法	$h'=\alpha h$	$h'=\alpha h$ $h''=\frac{H_3(c)+1}{H_3(c_1)+1}h'$	$S'=S+\beta hP_{pub}$	$S''=\frac{H_3(c_1)+1}{H_3(c)+1}S$ $S''=S'+\beta hP_{pub}$

显然,3 种攻击方法也具有如下的相似性:

盲化阶段,恶意请求者在发给签名者的部分盲化信息前乘以一个系数 w,

$$w=\frac{H(Y)+c}{H(Y^*)+c} \tag{5}$$

式中,其中 Y^* 表示替换后的协商信息,其它符号表示与式(4)定义相同。

去盲阶段,恶意请求者在签名者返回的签名前乘以系数 w^{-1},实施篡改协商信息的攻击。

上述攻击实质上是通过盲化和去盲阶段乘以互为倒数的系数,在验证阶段可以约去签名公式中的原协商信息,从而达到篡改协商信息的目的。本文将这种篡改协商信息攻击的方法称为"约分攻击"。

3.2 推论

根据 3.1 节中的分析,文献[7,8,12] 3 个方案的签名公式本质上具有相似性,即请求者发来的部分盲化信息在实际签名前已经与签名者提供的原协商信息进行了加法运算,导致了这 3 个方案都存在"约分攻击"。由上述分析结论,本文得出如下推论:

推论:如果一个基于双线对的部分盲签名方案采用形如式(6)的签名公式,则该方案存在"约分攻击"。

$$S=(aX\#bH(Y)+c)Z \tag{6}$$

式中,$\#$ 表示某种四则运算,$a,b,c,H(\ )$为系统参数,X 表示部分盲化信息,Y 表示协商信息,Z 表示签名密钥。

3.3 验证

本小节将通过对文献[10]所提的两个部分盲签名方案的分析,验证上述推论。为叙述方便,本文将文献[10]中提出的第一个方案称为方案 1,第二个方案称为方案 2。

3.3.1 方案 1 的分析与验证

(1)方案 1 描述

1)建立

给定安全参数 k,私钥产生机构(PKG)选出 $p(p>2^k)$阶线性映射群(G_1,G_2,G_T),Q 为 G_2 中的生成元,$P=\psi(Q)\in G_1$,$g=e(P,Q)$。PKG 选择主密钥 $s\in_R Z_p^*$,$Q_{pub}=sQ\in G_2$,哈希函数 $H_1:\{0,1\}^*\rightarrow Z_p^*$,$H_2:\{0,1\}^*\times G_T^*\rightarrow Z_p^*$,$H_3:\{0,1\}^*\rightarrow Z_p^*$,系统公钥为 $params=\{G_1,G_2,G_T,P,Q,g,Q_{pub},e,\psi,H_1,H_2,H_3\}$。

2)提取

PKG对身份ID生成私钥 $S_{ID}=\frac{1}{s+H_1(ID)}P$，如果 $s+H_1(ID)\equiv 0 \bmod p$，则返回，重新选择 s。

3)发行协议

假设要对消息 M 进行盲签名，info 表示用户和签名者已经协商好的共同信息，步骤如下。

①承诺：签名者随机选择 $x\in_R Z_p^*$，计算 $r=g^x\in G_T$，并将 r 发送给用户。

②盲化：用户选择 $a,b\in Z_p^*$，计算 $r'=r^a g^{ab}$ 和 $h=a^{-1}H_2(M,r')+bH_3(info)$，并把 h 发送给签名者。

③签名：签名者计算 $V=(xH_3(info)+h)S_{ID}$，并将 V 发送给用户。

④解盲：用户计算 $V'=aV$，并输出签名 $sig=(M,info,r',V')$。

4)验证

若 $r'^{H_3(info)}g^{h'}=e(V',Q_{ID})$，其中 $Q_{ID}=H_1(ID)Q+Q_{pub}$，$h'=H_2(M,r')$，则接受签名。

(2)分析与验证

方案1采用的签名公式为 $V=(xH_3(info)+h)S_{ID}$，满足第3.2节中推论的条件，式(6)中的符号“#”在该方案中表示“+”运算，因此该方案存在“约分攻击”。

根据“约分攻击”的思想，设计攻击方法如下：

恶意请求者使用 $info^*$ 替换原协商信息 $info$，在盲化阶段，计算 $h''=H_3(info)H_3(info^*)^{-1}a^{-1}H_2(M,r')+bH_3(info)$，并将 h'' 发送给签名者。收到签名者返回的 $V=(xH_3(info)+h'')S_{ID}$，解盲阶段计算 $V''=H_3(info^*)H_3(info)^{-1}aV$，产生部分盲签名 $sig=(M,info^*,r',V')$。

签名验证者利用替换后的协商信息 $info^*$ 对产生的部分盲签名进行如下验证：

$$\begin{aligned}e(V'',Q_{ID})&=e(H_3(info^*)H_3(info)^{-1}aV,Q_{ID})\\&=e(H_3(info^*)H_3(info)^{-1}a(xH_3(info)+h'')S_{ID},Q_{ID})\\&=e(a(xH_3(info^*)+H_3(info^*)H_3(info)^{-1}h'')S_{ID},Q_{ID})\\&=e((axH_3(info^*)+H_2(M,r')+abH_3(info^*))S_{ID},Q_{ID})\\&=e(H_3(info^*)(ax+ab)S_{ID},Q_{ID})e(H_2(M,r')S_{ID},Q_{ID})\quad\text{由式(3)得}\\&=e(P,Q)^{H_3(info^*)(ax+ab)}e(P,Q)^{H_2(M,r')}\quad\text{由式(1)得}\\&=r'^{H_3(info^*)}g^{h'}\end{aligned}$$

验证等式成立。因此，攻击方法有效。

3.3.2 方案2的分析与验证

(1)方案2描述

方案2系统参数的建立、提取算法与方案1相同。发布协议和验证协议描述如下。

1)发布协议

假设要对消息 M 进行盲签名，$info$ 表示用户和签名者已经协商好的共同信息，步骤如下。

①承诺：签名者随机选择 $x\in_R Z_p^*$，计算 $R=g^x\in G_T$、$R_2=e(S_{ID},M)$、$R_2'=R_2^x$、$R_3=e(S_{ID},Q)$、$R'_3=R_3^x$，并将 R、R_2、R_2'、R_3、R_3'发送给用户。

②盲化：用户随机选择 $a,b,\alpha,\beta\in Z_p^*$，计算 $M_1=aM+bQ$、$U=R_2^{\alpha}R_3^{\beta}(=e(S_{ID},M_1))$、$t_1=R^{\alpha}g^{\alpha\beta H_3(info)}$、$t_2=R_2'^{a\alpha}R_3'^{b\alpha}U^{\alpha\beta H_3(info)}=(e(\alpha xS_{ID},M_1)U^{\alpha\beta H_3(info)})$、$c'=H_2(H_3(info)\|M_1\|U\|t_2\|t_1)$、$c=\alpha^{-1}c'+\beta$，并将 c 发送给签名者。

③签名：签名者计算 $V=(x+cH_3(info))S_{ID}$，并将 V 发送给用户。

④解盲：用户计算 $V'=\alpha V$，其中 $sig=(ID,M_1,info,U,c',V')$ 是对 M_1 的签名。

2)验证协议

如果 $c'=H_2(H_3(info)\|M_1\|U\|e(V',M_1)U^{-c'H_3(info)}\|e(V',Q_{pub}+H_1(ID)Q)g^{-c'H_3(info)})$ 成立，则接受签名。

(2)分析与验证

方案2采用的签名公式为 $V=(x+cH_3(info))S_{ID}$，满足第3.2节中推论的条件，式(6)中的符号“#”在该方案中表示“*”运算，因此该方案可能存在“约分攻击”。

根据“约分攻击”的思想，设计攻击方法如下：

恶意请求者使用 $info^*$ 替换原协商信息 $info$，在盲化阶段，计算 $c'^*=H_2(H_3(info^*)\|M_1\|U\|t_2\|t_1)$，$c=\alpha^{-1}c'^*+\beta$，$c''=H_3(info^*)H_3(info)^{-1}c$，将 c'' 发送给签名者。收到签名者返回的 $V=(x+c''H_3(info))S_{ID}$ 后，在解盲阶段计算 $V''=aV$，产生部分盲签名 $sig=(ID,M_1,info^*,U,c'^*,V'')$。

签名验证者利用替换后的协商信息 $info^*$ 对产生的部分盲签名进行如下验证：

$$\begin{aligned}&(1)e(V'',M_1)U^{-c'^*H_3(info^*)}\\&=e(\alpha(x+c''H_3(info))S_{ID},M_1)U^{-c'^*H_3(info^*)}\\&=e(\alpha(x+cH_3(info^*))S_{ID},M_1)U^{-c'^*H_3(info^*)}\\&=e(S_{ID},M_1)^{\alpha x}e(S_{ID},M_1)^{c'^*H_3(info^*)+\alpha\beta H_3(info^*)}\\&\quad U^{-c'^*H_3(info^*)}\quad\text{由式(1)、式(3)得}\\&=R_2'^{a\alpha}R_3^{b\alpha}U^{\alpha\beta H_3(info^*)}=t_2\\&(2)e(V'',Q_{pub}+H_1(ID)Q)g^{-c'^*H_3(info^*)}\\&=e(\alpha(x+c''H_3(info))S_{ID},Q_{pub}+H_1(ID)Q)\\&\quad g^{-c'^*H_3(info^*)}\\&=e(\alpha(x+cH_3(info^*))S_{ID},Q_{pub}+H_1(ID)Q)\\&\quad g^{-c'^*H_3(info^*)}\\&=e(P,Q)^{\alpha x}e(P,Q)^{c'^*H_3(info^*)+\alpha\beta H_3(info^*)}g^{-c'^*H_3(info^*)}\\&\quad\text{由式(1)、式(3)得}\\&=R^{\alpha}g^{\alpha\beta H_3(info^*)}=t_1\end{aligned}$$

验证等式成立。因此，攻击方法有效。

3.3.3 结论

根据第3.3.1节和第3.3.2节中的分析，方案1和方案2满足本文第3.2节中所得推论的条件，且都存在“约分攻击”，验证了第3.2节的推论。

结束语 本文对3个部分盲签名方案及其相应的篡改协商信息攻击方法分别进行了对比研究，指出由于在签名公式中，盲化信息在实际签名前已经与签名者提供的原协商信息进行了某种四则运算，导致了这类方案都存在“约分攻击”。在此基础上，推出基于双线性对的部分盲签名方案存在“约分攻击”的结论，并通过分析崔巍等[10]提出的两个部分盲签名方案，对上述推论进行了验证。

参 考 文 献

[1] Chaum D. Blind signatures for untraceable payments[C]// Proc. Advances in Cryptology-Crypto'82. Santa Barbara, California, USA, Aug. 1982:199-203

[2] Abe M, Fujisaki E. How to Date Blind Signature [C]// Asiacrypt'96, LNCS 1136. Berlin: Springer-Verlag, 1996:244-251

[3] Chien H Y, Jan J K, Tseng Y M. RSA-Based Partially Blind Signature with Low Computation [C] // IEEE 8th International Conference on Parallel and Distributed Systems. 2001:385-389

[4] Wen H A, Lee K C, Hwang S Y, et al. On the traceability on RSA-based partially signature with low computation[J]. Applied Mathematics and Computation, 2005, 162:421-425

[5] Fang De-jian, Wang Na, Liu Cheng-lian. An Enhanced RSA-based Partially Blind Signature[C]// 2010 International Conference on Computer and Communication Technologies in Agriculture Engineering. 2010:565-567

[6] Chow S S M, Hui L C K, Yiu S M, et al. Two improved partially blind signature schemes from bilinear pairings[C]// Proc. Australasian Conference on Information Security and Pricacy-ACISP 2005, LNCS 3574. Brisbane, Australia: Springer-Verlag, 2005: 316-328

[7] Hu Xiao-ming, Huang Shang-teng. An Effcient ID-based Partially Blind Signature Scheme[C]// Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallell Distributed Computing. IEEE, 2007:291-296

[8] 张学军,王育民. 高效的基于身份的部分盲签名方案[J]. 计算机工程与应用,2007,43(11):211-213

[9] 荣维坚. 无证书部分盲签名方案[J]. 漳洲师范学院学报:自然科学版,2008,62(4):44-47

[10] 崔巍,辛阳,胡程瑜,等. 高效的基于身份的(受限)部分盲签名[J]. 北京邮电大学学报,2008,31(4):53-57

[11] Kang Bao-yuan, Han Jin-guang. On thesecurity of blind signature and partially blindsignature, Education Technology and Computer(ICETC)[C]// 2010 2nd International Conference. V5, 2010:206-208

[12] 闫东升. 一个新的高效的基于身份的部分盲签名方案[J]. 计算机工程与应用,2008,44(2):137-140

[13] 李明祥,王涛,罗新方. 对两种基于双线性对的部分盲签名方案的密码学分析[J]. 计算机应用研究,2011,28(2):435-438

(上接第 106 页)

参 考 文 献

[1] Leavitt N. Is Cloud Computing Really Ready for Prime Time? [J]. IEEE Computer Society Press, 2009, 42(1):15-20

[2] 周红伟,李琦. 基于云计算的空间信息服务系统研究[J]. 计算机应用研究,2011,28(7):2586-2588

[3] Vaquero L, Rodero-Marino L, Caceres J, et al. A break in the clouds : towards a cloud definition[J]. SIGCOMM Computer Communication Review, 2009, 39(1):50-55

[4] 孙香花. 云计算研究现状与发展趋势[J]. 计算机测量与控制,2011,19(5):998-1001

[5] 李乔,郑啸. 云计算研究现状综述[J]. 计算机科学,2011,38(4):32-37

[6] 孙坦,黄国彬. 基于云服务的图书馆建设与服务策略[J]. 图书馆建设,2009,9:1-6

[7] Ferrer A J, Hernandez F, Tordsson J, et al. OPTIMIS: Aholistic appraoch to cloud service provisioning[J]. Future Generation Computer Systems, 2012, 28:66-77

[8] Gutierrez-Garcia J O, Sim K-M. Self-Organiziing Agents for Service Composition in Cloud Computiiong[C]// The Procee-dings of the International Conference on Cloud Computing Technology and Sciences. 2010:59-66

[9] Canfora G, Penta D, Esposito M, et al. A lightweight approach for QoS-aware service composition[C]// Proc. 2nd International Conference on Service oriented Computing (ICSOC, 04). New-York, USA, 2004:36-47

[10] Zeng L, Benatallah B, Ngu A H H, et al. QoS-Aware Middleware for Web Services Composition[J]. IEEE Transactions on Software Engineering, 2004, 30(5):311-327

[11] 刘书雷,刘云翔,张帆. 一种服务聚合中 QoS 全局最优服务动态选择算法[J]. 软件学报,2007,18(3):646-656

[12] Fang Qi-qing, Peng Xiao-ming, Liu Qing-hua, et al. A Global QoS Optimizing Web Services Selection Algorithm based on MOACO for Dynamic Web Service Composition[J]. International Forum on Information Technology and Application, 2009, 1: 37-42

[13] 孙学胜,曹玖新,刘波,等. 基于多目标粒子群优化的服务选择算法[J]. 东南大学学报:自然科学版,2009,39(4):684-689

[14] Xie X F, Zhang W J. Solving engineerin g design problems by social cognitive optimization[C]// Proceedings of the Genetic and Evolutionary Computat ion Conference. 2004:26

[15] Xie X F, Zhang W J, Yang Z L. Social cognitive optimization for nonlinear programming problems[C]// Proceedings of the International Conference on Machine Learning and Cybernetics. Beijing, China, 2002:779-783

[16] Reynolds R G. An introduction to cultural algorithms[C]// Proceedings of the Third Annual Conference on Evolutionary Programming. 1994:131-139

[17] Wang Xiao-ying, Xue Yuan-yuan, Fan Li-hua, et al. Research on Adaptive QoS-Aware Resource Reservation Management in Cloud Service Environments[C]// The Proceedings of the International Conference on Services Computing Conference (APSCC). IEEE Asia-Pacific, 2011:147-152

[18] Wang Zhi-jian, Liu Zhi-zhong, Zhou Xiao-feng, et al. An approach for composite web service selection based on DGQoS[J]. The International Journal of Advanced Manufacturing Technology, 2011, 56:1-13

[19] 陈彦萍,张建科,孙家泽,等. 一种基于混合智能优化的服务选择模型[J]. 计算机学报,2010,33(11):2116-2125

[20] Dillenbourg P. Collaborative Learning: Cognitive and Computational Approaches. Advances in Learning and Instruction Series [M]. New York, NY: Elsevier Science, Inc, 1999

[21] Peng B. Knowledge and population swarms in cultural algorithms for dynamic environments [D]. USA Wayne State University, 2005

[22] 张佩云. 基于语义的 Web 服务组合研究[D]. 南京:南京理工大学,2008