基于双线性对的隐藏签名认证方案

王尚平 杨春霞 王晓峰 张亚玲
(西安理工大学密码理论与网络安全研究室 西安 710048)

摘 要：隐藏签名认证方案是指，当用户从 CA 得到签名(证书)后，在向服务提供商申请服务时，为防止攻击者截获签名或串通服务提供商来陷害自己，用户向服务提供商证明他(或她)有签名而不把该签名给服务提供商。现有的隐藏签名认证方案都不能阻止 CA 冒充用户身份。该文引入两个证书权威机构 CA，假设两个 CA 不勾结，提出了 3 个隐藏签名认证方案。这 3 个方案都能保护用户身份不被任何人(包括 CA)冒充；在用户端具备较强计算能力时，后两个方案实现了用户和服务提供商的双向认证；并且在 CA 具有一定可信度时，第 3 个方案还能部分抵抗拒绝服务攻击(DoS)。

关键词：隐藏签名的认证；数字签名；CA；DoS
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2008)02-0486-04

New Signature-Masked Authentication Schemes from the Bilinear Pairings

Wang Shang-ping Yang Chun-xia Wang Xiao-feng Zhang Ya-ling
(*Lab. of Cryptography and Network Security, Xi'an Univ. of Tech., Xi'an* 710048, *China*)

Abstract: Signature-masked authentication scheme means: when a user obtains a signature (certificate) from CA, in order to get service from a service provider and to prevent any adversary from intercepting the signature or colluding with the service provider to frame him (or her), the user is intent on proving that he (or she) really owns the signature but not transmits it to the service provider directly. Considering previous schemes can not prevent CA from impersonating legitimate users, two different CAs are introduced in this paper, and under the assumption that these two CAs do not collude, three signature-masked authentication schemes are given which guarantee that anyone including CA can not impersonate the legitimate user to get service from the provider. The first scheme is a simple scheme of unilateral authentication. Moreover, under the assumption that the user has enough computation power, mutual authentication between the user and the provider is realized in the last two schemes. Furthermore considering the first two schemes above are vulnerable to denial of service (DoS) attack, under the assumption that CA is of certain reliability, the third scheme which can also partially realize the resistance to DoS attack is proposed.

Key words: Signature-masked authentication; Digital signature; CA; DoS

1 引言

隐藏签名的认证方案是指：一个合法用户从 CA 得到一个签名(证书)后，为了从服务提供商那里得到服务，同时为了防止攻击者截获签名或者和服务提供商串通来陷害自己，该用户向服务提供商证明他有这个签名而不把原始签名给服务提供商。这种认证方案广泛应用于数字置顶盒(Digital Set-Top-Box) 之间以及数字视频广播(Digital Video Broadcasting)服务系统中的智能卡之间的身份认证。

最初，隐藏签名的认证方案是利用 RSA 签名和 Guillou-Quisquater 的身份认证协议实现的[1]，2002 年，Zhang 和 Kim 提出了一个基于身份的隐藏签名的认证[2]方案，但由于基于身份的密码学方案本身的缺陷，即 CA 知道用户的秘密钥，因此能冒充用户获得服务。本文借鉴 Zhang 和 Kim 的方法，在引入两个 CA 的情况下，给出了 3 个隐藏签名的认证方案，由于合法用户有自己的秘密值，当两个 CA 不勾结时，任何人包括 CA 也不能冒充合法用户获得服务。方案 1 是一个简单的单向隐藏签名认证方案。考虑到实际生活中往往也需要同时对服务提供商进行认证，提出了方案 2，方案 2 实现了保护隐私的隐藏签名的双向认证，同时并不增加交互的次数。由于这两个方案和 Zhang 和 Kim 的方案一样容易受到拒绝服务攻击，在假设 CA 有一定的可信度的基础上，本文提出方案 3 来实现部分抵抗拒绝服务攻击的双向认证。

2006-06-29 收到，2007-01-15 改回
国家自然科学基金项目(60273089)，陕西省教育厅专项科学研究计划项目(06JK213)，陕西省自然科学基础研究计划(2005F02)资助课题

2 双线性对的基本概念

设 G 是由 P 生成的加法循环群，阶为素数 q， V 是 q 阶

的乘法循环群，双线性对 $e: G\times G\to V$ 满足以下性质：

(1)双线性：$e(aP,bQ)=e(P,Q)^{ab}$ ；(2)非退化性：存在 $P\in G$ 和 $Q\in G$ ，满足 $e(P,Q)\neq 1$ ；(3)可计算性：对所有的 $P,Q\in G$ ，存在有效的算法来计算 $e(P,Q)$ 。

文中涉及到的困难问题有：

(1)离散对数问题(DLP)：给定 P 和 Q ，假如有 $Q=nP(n\in Z_q^*)$ 存在，求 n 。

(2)计算 Diffie-Hellman 问题(CDHP)：给定 P ， aP ， bP ，其中 $a,b\in Z_q^*$ ，计算 abP 。

(3)判定 Diffie-Hellman 问题(DDHP)：给定 P ， aP ， bP ， cP ，其中 $a,b,c\in Z_q^*$ ，判断 $c\stackrel{?}{=}ab \bmod q$ 。

假设离散对数问题(DLP)在 G ， V 上是困难的，进一步假设 G 是一个 Gap-Diffie-Hellman(GDH)群，即在 G 上 DDHP 是容易的，CDHP 是困难的。

3　Zhang 和 Kim 的方案[2]

2002 年，Zhang 和 Kim 用基于身份的 BLS 签名方案[3,4]构造了一个隐藏签名的认证方案[2]。系统参数为 $(G,V,q,P,P_{\text{pub}},H)$ ，其中 G,V,P,q 定义同上， $P_{\text{pub}}=sP$ 是证书权威 CA 的公钥， s 是其私钥， $H_1:\{0,1\}^*\to G$ ， $H_2:\{0,1\}^*\to Z_q^*$ 是两个抗碰撞的哈希函数。具体方案分为两个阶段：

阶段 1　CA 对用户的身份 ID 进行 BLS 签名，用户验证通过后得到证书 $\sigma=sH_1(\text{ID})$ 。

阶段 2　(用户和服务提供商之间)：

用户		服务提供商
ID,σ	$\xrightarrow{\text{ID}}$	$Q_{\text{ID}}=H_1(\text{ID})$ $r\in_R Z_q^*, R=rP$
$a\in_R Z_q^*, A=aP$	$\xleftarrow{R}$	$e(C,P)\stackrel{?}{=}e(Q_{\text{ID}},P_{\text{pub}})^{H_2(A)}e(A,A)^r$
$C=H_2(A)\sigma+a^2R$	$\xrightarrow{A,C}$	若成立，则接受，否则拒绝。

在本阶段，用户不需要进行双线性对计算，这在用户端计算和存储能力有限的时候是很有优势的。但由于该方案是基于 ID 的，它也不能避免基于 ID 方案的一般缺陷，即用户加密时用到的私钥(阶段 1 中的证书)是由 CA 提供的，CA 可以很容易的冒充用户来获取服务提供商提供的服务。所以说该方案中，用户的隐私没有得到很好的保护。而且，可以看出该方案很容易受到拒绝服务攻击，比如，攻击者用假的 ID 发给提供商，当它收到提供商发送的质询 R 后，在群 G 中随机选择元素 C 来回答，那么提供商就需要验证 $e(C,P)\stackrel{?}{=}e(Q_{\text{ID}},P_{\text{pub}})^{H_2(A)}e(A,A)^r$ 是否成立，这需要 3 个对运算，对运算是花费很大的。如果攻击者很多，则提供商就要忙于进行对运算而无法正常运行，也就是受到了拒绝服务攻击。

4　新方案(方案 1，方案 2，方案 3)

为防止 CA 冒充合法用户，用户必须拥有秘密值，这就是方案 1 的思路[5,6]，并且考虑到在这样基于身份的方案中，如果只有一个 CA，那么这个 CA 则很容易利用用户提交的身份伪造另外一套证书[7]，所以在新方案中使用了两个独立的权威证书机构 CA_1 ， CA_2 ，他们的公钥分别为 $P_{\text{pub1}}=s_1P, P_{\text{pub2}}=s_2P$ ，其中 s_1,s_2 是其对应的私钥。新方案仍以 BLS 签名方案为基础，也分为两个阶段，其中， $H:G\times\{0,1\}^*\to G$ 是一个安全哈希函数，其它的系统参数同上。另外，本文以下出现的 CA 均指的是 CA_1 或 CA_2。

4.1 保护用户隐私的隐藏签名的认证方案(方案 1)

阶段 1　(用户和 CA 之间)：

用户		$\text{CA}_1(\text{CA}_2)$
$\text{ID},x\in_R Z_q^*, X=xP$	$\xrightarrow{\text{ID},X}$	$U=H(X,\text{ID}),\sigma_1=s_1U$ $(U=H(X,\text{ID}),\sigma_2=s_2U)$
$e(\sigma_1,P)\stackrel{?}{=}e(H(X,\text{ID}),P_{\text{pub1}})$ $\left(e(\sigma_2,P)\stackrel{?}{=}e(H(X,\text{ID}),P_{\text{pub2}})\right)$	$\xleftarrow{\sigma_1(\ \sigma_2)}$	

在此阶段，用户先把自己的身份 ID 和公钥 $X\in G$ 分别发送给 CA_1 和 CA_2，在这两个机构用物理方法对用户的身份信息进行认证后，分别对用户提交的信息进行 BLS 签名，并通过秘密通道给他颁发证书 σ_1， σ_2 ，用户计算自己的最终证书：$\sigma=\sigma_1+\sigma_2$ 。注意到 x 只有用户才知道，CA_1 ，CA_2 也不知道。

阶段 2　(用户和服务提供商之间)：

用		服务提供
$\text{ID},X=xP$	$\xrightarrow{\text{ID},X}$	$r\in_R Z_q^*, R=rP$
$C=\sigma+x^2R$	$\xleftarrow{R}$	$e(C,P)\stackrel{?}{=}e(H(X,\text{ID}),P_{\text{pub1}})$ $e(H(X,\text{ID}),P_{\text{pub2}})e(X,X)^r$
	$\xrightarrow{C}$	若成立，则接受，否则拒绝。

在此阶段，用户要在隐藏签名 σ (即证书)的同时，向服务提供商说明它有这个证书。用户把身份 ID 和公钥 X 发送给提供商，提出服务请求，服务提供商发送质询 R 给用户，用户把证书的承诺 C 发给服务提供商，若验证式 $e(C,P)\stackrel{?}{=}e(H(X,\text{ID}),P_{\text{pub1}})e(H(X,\text{ID}),P_{\text{pub2}})e(X,X)^r$ 通过，则用户在不把证书 σ 给服务提供商的情况下，证明了自己有这个证书，并且知道该证书中公钥 X 对应的秘密钥 x 。

4.2 保护隐私的隐藏签名的双向认证方案(方案 2)

考虑到现实生活中用户往往也需要对服务提供商如网上银行，网上证券等进行认证，下面给出一个能保护隐私的隐藏签名的双向认证方案。在本方案中，假设除了用户有 CA_1，CA_2 颁发的证书外，服务提供商也有 CA_1，CA_2 颁发的证书。

阶段 1　用户证书的颁发过程同上。服务提供商证书的颁发：

服务提供商 $\mathrm{CA}_1(\mathrm{CA}_2)$

$\mathrm{ID}', y \in_R Z_q^*, Y = yP \xrightarrow{\mathrm{ID}', Y} U' = H(Y, \mathrm{ID}'),\ \sigma_1' = s_1 U'$

$\left(U' = H(Y, \mathrm{ID}'),\ \sigma_2' = s_2 U'\right)$

$e(\sigma_1', P) \stackrel{?}{=} e(H(Y, \mathrm{ID}'), P_{\mathrm{pub1}})$

$\left(e(\sigma_2', P) \stackrel{?}{=} e(H(Y, \mathrm{ID}'), P_{\mathrm{pub2}})\right)$ $\xleftarrow{\sigma_1'\left(\sigma_2'\right)}$

提供商把 $\sigma' = \sigma_1' + \sigma_2'$ 作为公钥 Y 的最终证书，同时，用户有公钥 X 的证书 σ 。

阶段 2

用户 服务提供商

$\mathrm{ID}, X, a \in_R Z_q^*, A = aP \xrightarrow{\mathrm{ID}, X, A}$ $C' = \sigma' + y^2 A$

$r \in_R Z_q^*, R = rP$

$e(C', P) \stackrel{?}{=} e(H(Y, \mathrm{ID}'), P_{\mathrm{pub1}}) \cdot e(H(Y, \mathrm{ID}'), P_{\mathrm{pub2}}) e(Y, Y)^a$ $\xleftarrow{\mathrm{ID}', Y, R, C'}$ $e(C, P) \stackrel{?}{=} e(H(X, \mathrm{ID}), P_{\mathrm{pub1}}) \cdot e(H(X, \mathrm{ID}), P_{\mathrm{pub2}}) e(X, X)^r$

若成立，则计算 $C = \sigma + x^2 R$ $\xrightarrow{C}$ 若成立，则接受，否则拒绝。

用户先把自己的身份 ID，公钥 X 和质询 A 发送给提供商，提供商根据用户发送的质询 A 计算自己证书 σ' 的承诺 C'，并把该承诺和自己的身份 ID'，公钥 Y 和自己的质询 R 发送给用户，若用户验证 C' 确实是提供商的证书承诺，即用户认证了提供商，用户就计算自己证书 σ 的承诺 C ，并把它发送给提供商以便其认证自己。

本方案在交互次数没有增加的情况下，实现了用户和服务提供商之间的相互认证，这在用户也具有相当的计算和存储能力时是很有效的，而且用户的隐私 x 和服务提供商的隐私 y 受到相同的保护。

4.3 部分抵抗拒绝服务攻击的保护隐私的隐藏签名的双向认证方案(方案 3)

注意到方案 1 和方案 2 与原方案一样容易受到拒绝服务攻击(见第 3 节分析)，下面给出一个能部分避免此攻击的双向认证方案。之所以称为部分抵抗拒绝服务攻击，是因为该方案只能抵抗计算花费最大的对运算攻击而不能阻止其中的加法和乘法攻击。该方案仍然分为两个阶段，阶段 1，CA_1，CA_2 为用户和服务提供商颁发证书；阶段 2，用户和服务提供商在隐藏签名的同时进行相互认证，该认证过程能部分抵抗拒绝服务攻击。

阶段 1 证书机构向用户和服务提供商颁发证书的过程同方案 2，但注意到此时用户和 CA_1 之间有个共享的秘密 $\overline{\tau} = xs_1 P$，用户通过计算 xP_{pub1} 得到它，而 CA_1 可以通过计算 $s_1 X$ 得到它，并且因为 $\overline{\tau}$ 并不在用户和 CA_1 交互时发送，所以这个秘密只有用户和 CA_1 共享；同理，用户和 CA_2 有个共享的秘密 $\hat{\tau} = xs_2 P$，这样，用户可以计算得到一个只有自己才知道的秘密值 $\tau = \overline{\tau} + \hat{\tau} = x(s_1 + s_2)P$ 。假设这样的用户有很多个，我们用下标 i 来标识他们，CA_1 与 CA_2 分别维护更新一个注册用户列表 $\left\{(\mathrm{ID}_i, X_i, \overline{\tau}_i)\right\}, \left\{(\mathrm{ID}_i, X_i, \hat{\tau}_i)\right\}$，并通过安全信道发送给服务提供商(至于这个安全信道，CA 和服务提供商可以用他们之间共享的量 $\varpi_j = ys_j P (j = 1,2)$ 或其哈希来建立，也可以用其他方法来建立，这里不再讨论)。在提供商那里有个检测机制，若检测到从 CA_1 与 CA_2 传过来的两个列表中有相同的 (ID_i, X_i)，就把其对应的 $\overline{\tau}_i$，$\hat{\tau}_i$ 加起来计算 $\tau_i = \overline{\tau}_i + \hat{\tau}_i$ ，并把 $(\mathrm{ID}_i, X_i, \tau_i)$ 保存进自己的列表中。

阶段 2

用户 服务提供商

检查列表中是否有 (ID_i, X_i)，

$\mathrm{ID}_i, X_i, a \in_R Z_q^*, A = aP \xrightarrow{\mathrm{ID}_i, X_i, A}$ 若有，计算 $C' = \sigma' + y^2 A,$

$r \in_R Z_q^*, R = rP$

$e(C', P) \stackrel{?}{=} e(H(Y, \mathrm{ID}'), P_{\mathrm{pub1}}) \cdot e(H(Y, \mathrm{ID}'), P_{\mathrm{pub2}}) e(Y, Y)^a$ $\xleftarrow{\mathrm{ID}', Y, R, C'}$ 若没有，则停止协议。

根据列表中 (ID_i, X_i) 对应的 τ_i'，计算

若成立，则计算 $C = \sigma_i + x_i$

$T = H_1(\tau_i + R) \longrightarrow H_1(\tau_i' + R) \stackrel{?}{=} T$

若不等，停止协议，否则

验证 $e(C, P) \stackrel{?}{=} e(H(X_i, \mathrm{ID}_i), P_{\mathrm{pub1}}) \cdot e(H(X_i, \mathrm{ID}_i), P_{\mathrm{pub2}}) e(X_i, X_i)^r$

若成立，则接受，否则拒绝。

用户首先把身份 ID_i, X_i 和所选的质询 $A \in_R G$ 发送给提供商，服务提供商根据自己保存的用户列表 $\left\{(\mathrm{ID}_i, X_i, \tau_i)\right\}$ (这个列表是不断更新的)查找是否有该 (ID_i, X_i)，若存在，就把自己证书的承诺 C' 发送给用户，让用户验证自己的身份，用户验证通过后，把秘密值 τ_i 的承诺 T 和自己证书的承诺 C 发送给提供商，提供商根据列表中与 (ID_i, X_i) 对应的 τ_i' 来验证用户所给的承诺是否正确，若正确，再对用户的证书承诺进行验证。

5 新方案的安全性和有效性分析

在 3 个新方案中，方案 2 和方案 3 的安全性分析是建立在方案 1 的安全性基础上的，所以我们重点讨论方案 1 的安全性。

方案 1 中，若 CA_1 与 CA_2 不互相勾结，则他们不能冒充合法用户从提供商那里获得服务。虽然 CA_1 与 CA_2 从阶段 1 可以各自获得用户的身份 ID、公钥 X 及对应的证书 σ_1 或 σ_2，但并不知道用户所选择的 x，所以单独一个证书机构要冒充合法用户从提供商那里请求服务时，就会因为不能计算正确的 C 而失败。以 CA_1 为例，如果他要想冒充成功，就必须计算正确的 $C = \sigma + x^2 R = \sigma_1 + \sigma_2 + x^2 R$，已知用户的部分证书 σ_1，因此只需要解出 σ_2 和 $x^2 R$ 即可。对于 $\sigma_2 = xs_2 P$，在知道 CA_2 的公钥 $P_{\mathrm{pub2}} = s_2 P$ 以及 $X = xP$ 的情况下，求解时需要解决 CDHP。对于 $x^2 R$，在知道 $X = xP$，

$R=rP$ 的情况下，如果他选择从 X 解出 x，再求 x^2R，则需要解决 DLP；如果要从 $X=xP$，$R=rP$，首先计算 $B=rxP$，再利用 $X=xP$，$B=rxP$ 计算得到 $x^2R=x^2rP$，则需要两次解决 CDHP；如果要从 $X=xP$，$R=rP$，首先计算 $\overline{B}=x^2P$，再利用 $R=rP$，$\overline{B}=x^2P$ 计算得到 $x^2R=x^2rP$，也需要两次解决 CDHP；而我们假设在群 G 上 DLP 和 CDHP 是困难的。因此方案 1，在群 G 上 DLP 和 CDHP 是困难的安全假设下，即使证书机构也不能冒充合法用户从提供商那里获得服务。另一方面，即使 CA_1 通过非正常手段从 CA_2 那里得到了另一部分证书 σ_2，亦即他可以得到用户的最终证书 σ，他也不能冒充成功，因为证书 σ 的承诺 $C=\sigma+x^2R$ 中嵌有用户的秘密值 x，这是他不知道的，那么在计算 C 的过程中将遇到困难问题，分析同上。

对手得不到证书 σ 也不能冒充合法用户从提供商那里获得服务。这里的对手包括其它攻击者和服务提供商。这时候，攻击者的难度要大于前面分析过的 CA 攻击者。因为证书机构已经知道部分证书 $\sigma_1(\sigma_2)$ 或最终证书 σ，尚且不能假冒成功，一般的攻击者面临得到证书 $\sigma=\sigma_1+\sigma_2$ 并且计算 x^2R 这两个问题。从计算上分析，要获得证书 $\sigma_j=s_jH(X,\mathrm{ID})$，$j=1,2$，需要从系统公钥 $P_{\mathrm{pub}j}=s_jP$ 中获取私钥 s_j 的信息，这是一个 DLP，猜测证书 σ 成功的概率可以忽略不计；计算 x^2R 这问题，如前分析是一个 CDHP。因此方案 1 中，在群 G 上 DLP 和 CDHP 是困难的安全假设下，对手得不到证书也不能冒充合法用户从提供商那里获得服务。

方案 2 中要求服务提供商也像普通用户那样到 CA 那里申请证书，其请求服务过程(阶段 2)与方案 1 中的相比较，只是多了用户认证提供商的合法性这一过程，其安全性分析可参考方案 1。这时用户的计算量会增加 4 个对运算(其中 3 个可以离线计算)和一个指数运算，但当用户有足够的计算能力和存储空间时，该方案能实现用户和提供商的隐藏签名的双向认证，而且交互次数并不增加，这在网上银行、网上证券等方面还是有相当的应用空间的。

方案 3 是在方案 2 的基础上要求 CA 向提供商不断传递他们的用户列表 $\left\{(\mathrm{ID}_i,X_i,\overline{\tau}_i)\right\},\left\{(\mathrm{ID}_i,X_i,\hat{\tau}_i)\right\}$ 以便提供商更新自己的用户列表 $\left\{(\mathrm{ID}_i,X_i,\tau_i)\right\}$，这样在阶段 2，提供商就可以实现部分抵抗拒绝服务攻击。具体来说，在阶段 2，对手若没有正确匹配的 (ID_i,X_i)，则其请求被直接抛弃，服务提供商只需查表而没有任何计算花费。若对手有正确的 (ID_i,X_i)，服务提供商就需要计算它的证书承诺 C'，但这也只是一个乘法和一个加法运算，相对于双线性对运算，花费并不大。但是如果用户在下一步不能提供有效的承诺值 T，则提供商根本不需要进行双线性对运算而放弃协议运行。因此，对手不能对服务提供商发动完全拒绝服务攻击。当然这里说的对手不应包括 CA，如果 CA_1 与 CA_2 互相勾结，那么他们就会拥有用户列表 $\left\{(\mathrm{ID}_i,X_i,\tau_i)\right\}$，很容易发动拒绝服务攻击。所以说，在两个 CA 不勾结的情况下，并且 CA 在某种程度可信(它们提供给服务提供商的列表是正确的并且不会恶意公开用户列表)时，方案 3 实现了部分抵抗拒绝服务攻击的隐藏签名的双向认证。

6　结束语

本文在两个证书机构 CA_1 与 CA_2 不互相勾结的情况下，提出了一个能保护用户隐私的隐藏签名的认证方案(方案 1)，该方案能避免 CA 知道用户太多的信息而能冒充用户，因而比 Zhang 和 Kim 的方案[2]安全；然后在方案 1 的基础上提出了一个能保护用户隐私的隐藏签名的双向认证方案(方案 2)，该方案实现了用户和服务提供商之间的双向认证；最后，针对前面方案容易受到拒绝服务攻击的缺陷，提出了一个部分抵抗拒绝服务攻击的保护隐私的隐藏签名的双向认证方案(方案 3)，在 CA 有一定可信度的基础上，它在实现双向认证的同时，实现拒绝服务攻击。设计能完全抵抗拒绝服务攻击的保护隐私的隐藏签名的双向认证方案还有待于进一步研究。

参 考 文 献

[1] Guillou L and Quisquater J. A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory. Advances in Cryptology-Eurocrypt'1988, Springer-Verlag, 1988, LNCS 330: 123–128.

[2] Zhang F G and Kim K. Signature-masked authentication using the bilinear pairings. Cryptology & Information Security Laboratory (CAIS), Information and Communications University, technical report, 2002.

[3] Boneh D, Lynn B, and Shacham H. Short signatures from the Weil pairing. Advance in Cryptology-Asciacrypt'2001, Springer-Verlag, 2001, LNCS 2248: 514–532.

[4] Freeman D. Pairing-based identification schemes. HP Laboratories Palo AltoHPL-2005-154, 2005, August 24.

[5] Chen X F, Zhang F G, and Kim K. A new ID-based group signature scheme from bilinear pairings. Cryptology ePrint Archive, Report 2003/116.

[6] Chen X F, Zhang F G, and Konidala D M, *et al*.. New ID-based threshold signature scheme from bilinear pairings. In INDOCRYPT 2004, Springer-Verlag, 2004, LNCS 3348: 371–383.

[7] Boneh D and Franklin M. Identity-based encryption from the Weil pairing. Advances in Cryptology-Crypto'2001, Springer-Verlag, 2001, LNCS 2139: 213-229.

王尚平：　男，1963 年生，教授，博士，研究方向为密码理论与网络安全.

杨春霞：　女，1979 年生，硕士生，研究方向为密码理论与网络安全.

王晓峰：　女，1966 年生，副教授，博士生，研究方向为密码理论与网络安全.

张亚玲：　女，1966 年生，副教授，博士生，研究方向为网络信息安全.