新的基于身份的广义指定多验证者签名

张学军
ZHANG Xue-jun

西北师范大学 教育技术与传播学院, 兰州 730070
College of Education Technology and Communication, Northwest Normal University, Lanzhou 730070, China
E-mail: xjzhang99@163.com

ZHANG Xue-jun.New ID-based universal designated multi-verifiers signature scheme.Computer Engineering and Applications, 2008, 44(13): 33-35.

Abstract: In a designated verifier signature scheme, only the designated verifier can verify the validity of the signature.In this paper, based on bilinear pairings, a new efficient identity-based universal designated multi-verifiers signature.The proposed scheme introduces two independent PKG to solve the secure trouble that the single PKG can impersonate the signers to forge their signatures.It is proved that the proposed scheme is secure under the BDH assumption and the random oracle model.
Key words: bilinear parings; identity-based; universal designated multi-verifiers signature

摘 要: 在一个指定验证者签名方案中, 只有指定的验证者才能验证签名的有效性。论文基于双线性对提出一种新的基于身份的广义指定多个验证者签名方案。新方案采用引进两个独立 PKG 的方法, 在一定程度上消除了单个 PKG 可以伪造用户签名的安全缺陷。证明了在 BDH 问题假设和随机预言机下新方案是安全的。
关键词: 双线性对; 基于身份; 广义指定多验证者签名
DOI: 10.3778/j.issn.1002-8331.2008.13.010 **文章编号**: 1002-8331(2008)13-0033-03 **文献标识码**: A **中图分类号**: TP309

对于一般的数字签名, 任何人都可以验证其有效性, 这种性质有时是签名者所不希望的。为了在数字签名传播中保护其秘密性, Steinfield 等提出了广义指定验证者签名[1]。在这种体制中, 签名持有者(不一定是签名者)可以将签名指定给任何他所期望的验证者。被指定的验证者可以通过验证相信签名者确实生成了签名, 但不能传递这个证据去说服任何第三方。广义指定验证者签名一般应满足如下的安全性质:(1)不可伪造性: 没有签名者或者指定验证者的私钥, 要伪造一个有效的指定验证者签名在计算上是不可行的。(2)不可转移性: 指定验证者能够生成一个有效的签名, 并且与签名持有者生成的签名是不可区分的。1984 年 Shamir 提出了基于身份的密码学[2]。其主要观点是, 系统中不需要证书, 可以使用用户的标识如姓名、IP 地址、电子邮件地址等作为公钥。用户的私钥通过一个被称作私钥生成器 PKG(Private Key Generator)的可信任第三方进行计算得到。后来, 人们发现利用双线性对可以实现密码学上基于身份的加密、签名等应用[3,4]。最近, Seo 等将单个验证者扩展为多个验证者提出了一种基于身份的广义指定多验证者签名方案[5], 但是该方案中只有一个 PKG, 要求 PKG 完全可信才行。王晓峰等提出了一种基于身份的广义指定验证者签名方案[6], 该方案采用引进两个独立 PKG 的方法, 在一定程度上消除了单个 PKG 可以伪造用户签名的安全缺陷。但是, 它不是一个多个验证者的方案。本文结合文献[5]和文献[6], 基于双线性对提出一种新的基于身份的广义指定多验证者签名方案。新方案类似文献[6]采用引进两个独立 PKG 的方法, 在一定程度上消除了单个 PKG 可以伪造用户签名的安全缺陷, 同时又是一个多验证者的方案。新方案证明了在 BDH 问题假设和随机预言机下是安全的。

1 预备知识

1.1 双线性映射

设 G_1 为循环加法群, G_2 为循环乘法群, G_1, G_2 的阶均为素数 q。假定在 G_1, G_2 中计算离散对数问题是困难的。设 $e: G_1 \times G_1 \to G_2$ 为一个双线性映射, 它满足以下三个性质:

(1)双线性: 对于所有的 $P, Q \in G_1$ 和所有的 $a, b \in Z_q$, 有 $e(aP, bQ)=e(P, Q)^{ab}$。

(2)非退化性: 存在 $P \in G_1$, 满足 $e(P, P) \neq 1$。

(3)可计算性: 如果 $P, Q \in G_1$, 则 $e(P, Q)$ 可以在多项式时间内有效计算出来。

群 G_1, G_2 能在有限域上的超奇异椭圆曲线或超椭圆曲线上找到, 双线性映射能通过 Weil 对或 Tate 对构造。

下面描述几个常用的与双线性映射有关的数学困难问题。

基金项目: 国家自然科学基金 the National Natural Science Foundation of China under Grant No.60573043); 中国博士后科学基金 No.20060400035)。
作者简介: 张学军(1968-), 男, 博士, 副教授, 主要研究方向: 密码学及应用。
收稿日期: 2007-12-25 **修回日期**: 2008-01-28

CDH 问题(Computational Diffie-Hellman Problem):对于 $a,b\in_R Z_q^*$, $P\in G_1$,已知 P,aP,bP,计算 abP。

BDH 问题(Bilinear Diffie-Hellman Problem):对于 $a,b\in_R Z_q^*$, $P\in G_1$,已知 P,aP,bP,cP,计算 $e(P,P)^{abc}$。

1.2 基本的基于身份的签名

设 q,G_1,G_2,e 含义与第 1.1 节中相同,$P\in G_1$ 作为 G_1 的生成元,定义两个密码学上的单向哈希函数 $H_1:\{0,1\}^*\rightarrow G_1$, $H_2:\{0,1\}^*\rightarrow Z_q^*$。本文基本的基于身份的签名实际上是文献[7]中基于身份签名的变形,由系统设置、密钥提取、签名、验证四部分组成。

(1)系统设置:为避免单个 PKG 权力过大的问题,引进两个独立的 PKG1 和 PKG2。PKG1 和 PKG2 分别独立选取 $s_1\in_R Z_q^*$ 和 $s_2\in_R Z_q^*$ 作为系统私钥,计算 $P_{pub1}=s_1P$ 和 $P_{pub2}=s_2P$ 作为系统公钥,公开系统参数:

$$params=\{G_1,G_2,e,q,P,P_{pub1},P_{pub2},H_1,H_2\}$$

(2)密钥提取:用户提交他的身份信息 ID 给 PKG1 和 PKG2,PKG1 和 PKG2 分别计算他相应的部分私钥为 $S_{ID_1}=s_1H_1(ID)$ 和 $S_{ID_2}=s_2H_1(ID)$,然后分别安全地发送给该用户。记该用户的公钥为 $Q_{ID}=H_1(ID)$,私钥为 $S_{ID}=S_{ID_1}+S_{ID_2}$。

(3)签名:对于消息 m,签名者 ID 选择 $r\in_R Z_q^*$,计算 $U=rP$, $h=H_2(m,U)$, $P_{pub}=P_{pub1}+P_{pub2}$, $V=rP_{pub}+hS_{ID}$,则在 m 上的签名为 $\sigma=(U,V)$。

(4)验证:对于消息 m 上的签名 $\sigma=(U,V)$,验证者验证等式 $e(V,P)=e(U+hQ_{ID},P_{pub})$ 否成立。如果成立接受签名,否则拒绝。

1.3 批量验证

基于身份的多个签名可采用批量验证[8]的方法进行处理:对于 n 消息 $m_1,m_2,\cdots,m_n$ 上的签名 (U_1,V_1),(U_2,V_2),$\cdots$,(U_n,V_n),一个验证者可以同时验证它们是否有效。也就是对于消息 $m_i(1\le i\le n)$ 上的签名 $\sigma_i=(U_i,V_i)$ 验证等式 $e(\sum_{i=1}^{n}V_i,P)=e(\sum_{i=1}^{n}(U_i+h_iQ_i),P_{pub})(h_i=H_2(m_i,U_i))$ 是否成立。如果成立接受签名,否则拒绝。

2 基于身份的广义指定多验证者签名

设 q,G_1,G_2,e 含义与第 1.1 节中相同,$P\in G_1$ 作为 G_1 的生成元,定义两个密码学上的单向哈希函数 $H_1:\{0,1\}^*\rightarrow G_1$, $H_2:\{0,1\}^*\rightarrow Z_q^*$。基于身份的广义指定多验证者签名由系统设置、密钥提取、签名、公共验证、广义指定多验证者签名、广义指定多验证者验证六个部分组成,下面进行详细介绍。

2.1 系统设置

为避免单个 PKG 权力过大的问题,引进两个独立的 PKG1 和 PKG2。PKG1 和 PKG2 分别独立选取 $s_1\in_R Z_q^*$ 和 $s_2\in_R Z_q^*$ 作为系统私钥,计算 $P_{pub1}=s_1P$ 和 $P_{pub2}=s_2P$ 作为系统公钥,公开系统参数:

$$params=\{G_1,G_2,e,q,P,P_{pub1},P_{pub2},H_1,H_2\}$$

2.2 密钥提取

用户提交他的身份信息 ID 给 PKG1 和 PKG2,PKG1 和 PKG2 分别计算他相应的部分私钥为 $S_{ID_1}=s_1H_1(ID)$ 和 $S_{ID_2}=s_2H_1(ID)$,然后分别安全地发送给该用户。记该用户的公钥为 $Q_{ID}=H_1(ID)$,私钥为 $S_{ID}=S_{ID_1}+S_{ID_2}$。

2.3 签名

对于消息 m,签名者 ID_S 选择 $r\in_R Z_q^*$,计算 $U=rP$, $h=H_2(m,U)$, $P_{pub}=P_{pub1}+P_{pub2}$, $V=rP_{pub}+hS_{ID_S}$,则在 m 上的签名为 $\sigma=(U,V)$。

2.4 公共验证

对于消息 m 上的签名 $\sigma=(U,V)$,验证者验证等式 $e(V,P)=e(U+hQ_{ID_S},P_{pub})$ 是否成立。如果成立接受签名,否则拒绝。

2.5 广义指定多验证者签名

任何拥有消息-签名对 (m,σ)(其中 $\sigma=(U,V)$)的实体都可以作为指定者(这正是广义指定的广义性所在)。指定者根据需要选定多个验证者 $DV=\{ID_{V1},\cdots,ID_{Vn}\}$,计算 $\hat{V}_{DV}=e(V,\sum_{i=1}^{n}Q_{ID_i})$ $(Q_{ID_i}=H_1(ID_i)\in G_1)$。则对应于消息-签名对 (m,σ) 的广义指定多验证者签名为 $\hat{\sigma}_{DV}=(U,\hat{V}_{DV})$。

2.6 广义指定多验证者验证

设签名者的身份为 ID_S,含有身份和私钥对信息的验证者集合为 $\{(ID_{V1},S_{ID_{V1}}),\cdots,(ID_{Vn},S_{ID_{Vn}})\}$,广义指定多验证者签名为 $\hat{\sigma}_{DV}=(U,\hat{V}_{DV})$,每一个验证者按照以下步骤验证签名是否有效:

(1)计算 $e_i=e(U+H_2(m,U)Q_{ID_S},S_{ID_{Vi}})$。

(2)对于 $(e_i,S_{ID_{Vi}})$,通过 2.3 节生成签名的方法建立签名,消息-签名对为 (e_i,σ_i),在所有的 n 个验证者 $DV=\{ID_{V1},\cdots,ID_{Vn}\}$ 中公开 (e_i,σ_i)。

(3)通过 2.4 公共验证的方法检测 n 个签名 $(e_j,\sigma_j)(j=1,\cdots,n)$(为了加快验证速度,可运用 1.3 节的批量验证技术)。如果 n 个签名中有 1 个签名无效,则输出拒绝,退出。

(4)如果上述第(3)步通过,则验证等式 $\hat{V}_{DV}=\prod_{i=1}^{n}e_i=\prod_{i=1}^{n}e(U+H_2(m,U)Q_{ID_S},S_{ID_{Vi}})$ 是否成立。如果成立接受签名,否则拒绝。详细推导过程如下:

$$\prod_{i=1}^{n}e(U+H_2(m,U)Q_{ID_S},S_{ID_{Vi}})=e(U+H_2(m,U)Q_{ID_S},\sum_{i=1}^{n}S_{ID_{Vi}})=$$

$$e((s_1+s_2)rP+(s_1+s_2)hQ_{ID_S},\sum_{i=1}^{n}Q_{ID_{Vi}})=$$

$$e(rP_{pub}+hQ_{ID_S},\sum_{i=1}^{n}Q_{ID_{Vi}})=e(V,\sum_{i=1}^{n}Q_{ID_{Vi}})=\hat{V}_{DV}$$

2.7 安全性分析

(1)不可伪造性。基于身份广义指定多验证者签名具有不可伪造性,证明见定理 1。

定理 1(不可伪造性) 在没有签名者或者指定验证者私钥的前提下,如果一个敌手 F 在时间 t 内,能够以不可忽略的概率 ε 攻破提出的基于身份的广义指定多验证者签名方案,那么存在一个算法 B 能以不可忽略的概率解决 BDH 问题。

证明 本文证明方法与文献[5]类似。H_1, H_2 在证明中被看作是由 B 控制的随机预言机,算法 B 的目标是能以不可忽略的概率解决 BDH 问题,即对于 $a, b, c \in_R Z_q^*$, $P \in G_1$,已知 P, aP, bP, cP,计算 $\hat{e}(P, P)^{abc}$。B 作为一个任务运行 F,并模拟 F 的攻击环境。B 设置 $P_{pub}=P_{pub1}+P_{pub2}=aP$,这里 a 是系统主密钥,它对 B 来说是未知的,$ID_V \in DV=\{ID_{V1}, \cdots, ID_{Vn}\}$。B 将系统参数$\{G_1, G_2, e, q, P, P_{pub1}, P_{pub2}, H_1, H_2\}$发送给 F,并维护两个针对 H_1, H_2 询问的表 L_{H_1}, L_{H_2}(初始时为空)。B 模拟 F 的随机预言机询问如下:

H_1 询问:设 F 最多 q_{H_1} 次对 H_1 预言机进行询问。首先,B 选择随机 $j, k \in [1, q_{H_1}]$。当 F 对 ID_i($1 \le i \le q_{H_1}$)做了一次 H_1 询问后,B 就在表 L_{H_1} 中查找,B 给 F 如下回答:如果 $i=j$(设此时 $ID_i=ID_S^*$),则将返回 bP 作为回答并将(ID_S^*, bP)添加到表 L_{H_1} 中;如果 $i=k$(设此时 $ID_i=ID_V^*$, $ID_V^* \in DV$),则将返回 cP 作为回答并将(ID_V^*, cP)添加到表 L_{H_1} 中;否则,返回 t_iP($t_i \in_R Z_q^*$)作为回答并将(ID_i, t_i)添加到表 L_{H_1} 中。

H_2 询问:当 F 用(m_i, U_i)做了 H_2 预言机询问后,B 就在表 L_{H_2} 中查找。如果$(m_i, U_i, h_i) \in L_{H_2}$就输出 h_i 给 F 作为回答;否则,B 就选取 $h_i \in_R G_1$ 将它作为对于(m_i, U_i)的回答,并将(m_i, U_i, h_i)添加到表 L_{H_2} 中。

密钥提取询问:当 F 进行了 ID_i 的密钥提取询问后,如果 $ID_i \neq ID_S^*$ 并且 $ID_i \neq ID_V^*$,则 B 就在表 L_{H_1} 中查找(ID_i, t_i)并返回 t_iaP;否则 B 就输出失败信息并停止模拟。

签名询问:当 F 提出对应于(ID_i, m_i)的签名询问后,B 选择 $r_i, h_i \in_R Z_q^*$,如果 $ID_i \neq ID_S^*$ 并且 $ID_i \neq ID_V^*$,B 就在表 L_{H_1} 中查找(ID_i, t_i),计算 $U_i=r_iP$, $V_i=r_iP_{pub}+h_it_iaP$ 并返回(U_i, V_i)给 F,然后 B 将(m_i, U_i, h_i)添加到表 L_{H_2} 中;如果 $ID_i=ID_S^*$,B 计算 $U_i=r_iP-h_ibP$, $V_i=r_iP_{pub}$ 并返回(U_i, V_i)给 F,然后 B 将(m_i, U_i, h_i)添加到表 L_{H_2} 中;如果 $ID_i=ID_V^*$,B 计算 $U_i=r_iP-h_icP$, $V_i=r_iP_{pub}$ 并返回(U_i, V_i)给 F,然后 B 将(m_i, U_i, h_i)添加到表 L_{H_2} 中。

最终,F 能够以不可忽略的概率 ε 输出一个有效的基于身份的广义指定多验证者签名$(ID_t, DV_t=\{ID_{V1}, \cdots, ID_{Vn}\}, m_t, \hat{\sigma}_{DV_t})$,其中 ID_t 是由 F 选择的目标用户的身份。如果 $ID_t \neq ID_S^*$ 并且 $ID_t \neq ID_V^* \in DV_t$,那么 B“失败”并停止模拟。否则,B 重复执行上述模拟过程,但要象分叉引理[9]那样对于 H_2 进行随机数据集的不同数据选择。B 得到两个有效的基于身份的广义指定多验证者签名$(ID_t, DV_t, m_t, \hat{\sigma}_{DV_t})$(其中$\hat{\sigma}_{DV_t}=(U_t, \hat{V}_{DV_t})$, $\hat{V}_{DV_t}=\hat{e}(V_t, \sum_{i=1}^{n} Q_{ID_{Vi}})$)和$(ID_t, DV_t, m_t', \hat{\sigma}_{DV_t'})$(其中$\hat{\sigma}_{DV_t'}=(U_t', \hat{V}_{DV_t'})$, $\hat{V}_{DV_t'}=\hat{e}(V_t', \sum_{i=1}^{n} Q_{ID_{Vi}})$)使得 $h \neq h'$。B 进行如下计算:

$$\frac{\hat{V}_{DV_t}}{\hat{e}(U_t+hQ_{ID_S}, \sum_{i=1, i\neq k}^{n} S_{V_i})}=\hat{e}(V_t, Q_{ID_{Vk}})$$

$$\frac{\hat{V}_{DV_t'}}{\hat{e}(U_t'+h'Q_{ID_S}, \sum_{i=1, i\neq k}^{n} S_{V_i})}=\hat{e}(V_t', Q_{ID_{Vk}})$$

$$\left[\frac{\hat{e}(V_t, Q_{ID_{Vk}})}{\hat{e}(V_t', Q_{ID_{Vk}})}\right]^{(h-h')^{-1} \bmod q}=\hat{e}(V_t-V_t', Q_{ID_{Vk}})^{(h-h')^{-1}}=$$

$$\hat{e}((h-h')S_{ID_S}, Q_{ID_{Vk}})^{(h-h')^{-1}}=\hat{e}((h-h')abP, cP)^{(h-h')^{-1}}=\hat{e}(P, P)^{abc}$$

B 在模拟中不失败的概率是 $2\varepsilon/q_{H_2}(q_{H_2}-1)$。换句话说,已知 P, aP, bP, cP, B 能以不可忽略的概率 $2\varepsilon/q_{H_2}(q_{H_2}-1)$ 解决 BDH 问题,这与 BDH 问题是一个困难的数学问题相矛盾。

(2)不可转移性。基于身份广义指定多验证者签名具有不可伪造性,证明见定理 2。

定理 2(不可转移性) 每一个指定验证者能够生成一个有效的签名,并且与签名持有者的签名是不可区分的。

证明 每一个指定验证者都能伪造一个有效的签名$(U', \hat{V}_{DV}')$,方法如下:

指定验证者 ID_{Vi} 选择 $r \in_R Z_q^*$,计算 $U'=rP$。然后,对于 U' 和消息 m',每一个的指定的验证者计算 $e_i=\hat{e}(U'+H_2(m', U')Q_{ID_S}, S_{ID_{Vi}})$。指定验证者 ID_{Vi} 计算$\hat{V}_{DV}'=\prod_{i=1}^{n}\hat{e}(U'+H_2(m', U')Q_{ID_S}, S_{ID_{Vi}})$。生成的签名$(U', \hat{V}_{DV}')$能够通过基于身份广义指定多验证者的验证,因为:

$$\prod_{i=1}^{n}\hat{e}(U'+H_2(m', U')Q_{ID_S}, S_{ID_{Vi}})=\hat{e}(rP_{pub}+hS_{ID_S}, \sum_{i=1}^{n} Q_{ID_{Vi}})=$$

$$\hat{e}(V', \sum_{i=1}^{n} Q_{ID_{Vi}})=\hat{V}_{DV}'$$

上述推导中 $h=H_2(m', U')$, $V=rP_{pub}+hS_{ID_S}$。很明显,签名 $\hat{\sigma}_{DV}=(U, \hat{V}_{DV})$ 和上述伪造的签名 $\hat{\sigma}_{DV}=(U', \hat{V}_{DV}')$ 是不可区分的。即任何第三方都不能确定签名是由签名者持有者生成还是指定验证者伪造的。

3 结束语

本文结合文献[5]和文献[6],基于双线性对提出一种新的基于身份的广义指定多验证者签名方案。新方案类似文献[6]采用引进两个独立 PKG 的方法,在一定程度上消除了单个 PKG 可以伪造用户签名的安全缺陷,同时又类似文献[5]是一个多验证者的方案。新方案证明了在 BDH 问题假设和随机预言机下是安全的,更适合在实际中使用。

参考文献:

[1] Steinfeld R, Bull L, Wang H, et al. Universal designated verifier signatures[C]//Advanced in Asiacrypt03. Berlin: Springer-Verlag, 2003: 523-542.

[2] Shamir A. Identity-based cryptosystems and signature schemes[C]// LNCS 196: Advances in Cryptology, Crypto '84, Berlin, 1984: 47-53.

[3] Boneh D, Franklin M. Identity-based encryption from the weil pairing[C]//LNCS 2139: Advances in Cryptology, Crypto 2001, 2001: 213-229.

(下转 43 页)

(x, y, z, w, requestForQuote, quoteAcceptance, orderConfirmation, delivery Details, requestNewPrice, responseQuote, acceptquote, creditOk, requestDeliveryDetails, deliveryDetails, creditRejection, requestNewPrice, , reqDelivery, returnsDelivery, sendChannel, checkCredit, checkFails, creditCheckPasse) =Buyer<>|Seller<>|Shipper< >|CreditCheck<>.

5.3 验证

Pi-演算的主要验证工具有 HAL(History-dependent Analysis Laboratory)，JACK(Just Another Concurrency Kit)，ABC(Another Bissimulation Checker)，MWB(the Mobility Workbench)等，本文采用基于 New Jersey SML 语言编译器的 MWB(Mobility Workbench)工具}。MWB 工具是用于操作和分析移动并发系统的自动化 Pi-演算工具。它使用函数式编程语言 SML(即标准元语言)构建。具体使用的是朗讯贝尔实验室实现的 SML/NJ110 版。本文采用 MWB 对用 Pi-演算描述的 WS-CDL 建模的 Web 服务组合进行了验证，由图 4 所示的实验结果可知交易处理服务无结构死锁存在。

图 4 实验结果

6 总结和下一步工作

本文将 Web 服务及其组合的关键属性抽象出来用 WS-CDL 对其建模，然后按照 WS-CDL 元素与 Pi-演算的对应关系将 WS-CDL 建模的组合 Web 服务用 Pi-演算描述出来，并用具体的实例来说明如何用 Pi-演算来描述 WS-CDL 编舞的组合 Web 服务，而且通过 Pi-演算的验证工具 MWB 对其进行正确性检测，由实验结果可知实例中的组合 Web 服务不存在死锁，这样就可以在组合 Web 服务建模后发现其流程的不合理之处，避免了服务执行之后发现存在死锁而造成的损失，特别是设计到商业应用时，这种损失可能无可估量。

本文虽将 WS-CDL 的元素进行 Pi-演算的描述，但这一过程主要是手动进行的，还不能适应 WS-CDL 编舞的 Web 服务验证的实时性的要求，因此，实现 WS-CDL 编舞到 Pi-演算的自动转换和验证将是下一步工作的努力方向。

参考文献：

[1] 邓水光，吴健，李莹，等.基于回溯树的 Web 服务自动组合[J].软件学报，2007(8)：1896-1910.
[2] 胡海涛，李刚，韩燕波.一种面向业务用户的大粒度服务组合方法[J].计算机学报，2005(4)：694-703.
[3] 喻坚，韩燕波.面向服务的计算：原理和应用[M].北京：清华大学出版社，2006：171-177.
[4] 李英杰，余雪丽，王睿.基于描述逻辑的语义 Web 服务动态复合推理和验证[C]//第一届中国 Web 智能学术：CRSSC-CWI-CGrC'2007.广西师范大学学报，2007.
[5] Wei Yinxing, Zhang Shensheng, Zhong Farong.On formalizing and verifying Web services[J].High Technology Letters, 2005, 11(1)：47-50.
[6] Milner R, Parrow Y, Walker D.A calculus of mobile processes Part I and II[J].Information and Computation, 1992, 100：1-77.
[7] 张佩云，孙亚民.动态 Web 服务组合研究[J].计算机科学，2007(5)：4-7.
[8] Chen Jinjun, Yang Yun.Key research issues in grid workflow verification and validation[C]//The 4th Australasian Symposium on Grid Computing and e-research：AusGrid 2006, Hobart, Australia, 2006：97-104.
[9] 岳昆，王晓玲，周傲英.Web 服务核心支撑技术：研究综述[J].软件学报，2004(3)：428-442.
[10] 郭小群，郝克刚.Web 服务的 Pi 演算描述[J].计算机科学，2006(3)：261-262.
[11] Salaun G, Bordeaux L, Schaerf M.Describing and reasoning on Web services using process algebra[C]//the 2nd IEEE International Conference on Web Services, San Diego, California, USA, 2004：43-50.
[12] Foster H, Uchitel S, Magee J, et al.Model-based Verification of Web Service Compositions[C]//ASE'03.Canada：IEEE Computer Society Press, 2003：152-163.
[13] Fu X, Bultan T, Su J.Analysis of Interacting BPEL Web Services[C]//WWW'04.USA：ACM Press, 2004：621-630.
[14] 廖军，谭浩，刘锦德.基于 Pi-演算的 Web 服务组合的描述和验证[J].计算机学报，2005，28(4)：635-643.
[15] Hamadi R, Benatallah B.A petri net-based model for Web service composition[C]//ADC'03, Australia.Australia：Australian Computer Society, 2003, 17.

(上接 35 页)

[4] Boneh D, Lynn B, Shacham H.Short signature from the weil pairing[C]//LNCS 2248：Advances in Cryptology, Asiacrypt 2001, 2001：514-532.
[5] Seo S-H, Huang J H, Choi K Y, et al.Identity-based universal designated multi-verifiers signature schemes[J].Computer Standards & Interfaces, 2007, 9：1-8.
[6] 王晓峰，张璟，王尚平，等.新的基于身份的广义指定验证者签名方案[J].电子学报，2007，35(8)：1432-1436.
[7] Yi X.An identity-based signature scheme from the weil pairing[J].IEEE Communications Letters, 2003, 7(2)：76-78.
[8] Bellare M, Garay J A, Rabin T.Fast batch verification for modular exponentiation and digital signatures[C]//LNCS 1403：Advances in Cryptology-Eurocrypt'98.[S.l.]：Springer-Verlag, 1998：236-250.
[9] Pointcheval D, Stern J, Security arguments for digital signatures and blind signatures[J].Journal of Cryptology, 2000, 13：361-396.