# 标准模型下可证安全的一种新的CL-PKE加密方案

杨 勇，徐秋亮

(山东大学计算机科学与技术学院 济南 250101)

【摘要】该文在标准模型下构建了一个实用的无证书公钥加密体制(CL-PKE)，相比于其他的CL-PKE加密体制，该体制在加密时没有椭圆曲线上的对运算，而且所基于的难解性问题假设是自然的双线性Diffie-Hellman(BDHP)问题。为提高安全性，该文的安全模型选用了标准模型下的选择性身份(Selective-ID)模型，在提高效率的同时也增强了安全性。

**关 键 词** 算法； 双线性Diffie-Hellman问题； 无证书公钥加密； 公钥密码学； 标准模型

**中图分类号** TP309.7 **文献标识码** A doi:10.3969/j.issn.1001-0548.2010.06.021

# New Provable Security CL-PKE Encryption Scheme in the Standard Model

YANG Yong and XU Qiu-liang

(Department of Computer Science and Technology, Shandong University Jinan 250010)

**Abstract** A certificateless public key encryption (CL-PKE) algorithm is presented. The proposed CL-PKE algorithm is based on the nature BDHP difficulty assumption and therefore avoids paring computation on elliptic curves, which is the most expensive operation in the encryption algorithm. In CL-PKE algorithm, the selective-ID model is applied instead of the random oracle model. The security and efficiency of the algorithm can be improved compared with some other CL-PKE schemes.

**Key words** algorithm; BDHP; CL-PKE; public key cryptography; standard model

文献[1]提出了CL-PKE(certificateless encryption scheme)无证书加密体制，该体制的目的在于增强基于身份的加密体制，使基于身份的加密体制可以阻止密钥生成中心KGC的伪造攻击。CL-PKE加密体制就集成了传统PKE加密体制和基于身份加密体制的优势，具有阻止KGC伪造攻击和无公钥证书的特点。

最初的CL-PKE加密体制都是基于Random Oracle模型的[1-2]，之后有学者提出了基于标准模型的加密算法，但基于标准模型的加密算法大都有着复杂的运算和经过变形的困难性问题假设[1-3]。在具体算法发展到一定程度后，有的学者又提出了基于各种模型的通用算法[2,4-5]，但有些通用算法在某些模型下被证明是错误的[6]，因此，需要进一步研究构建基于一定模型的好的通用算法。

相对于本文来讲，在[JCH07]方案中，虽然加密时没有对运算，但在检验用户公钥时有两个对运算[7]，[BSN05]的方案虽然没有椭圆曲线上的对运算，效率较高，但要求在产生用户公钥前必须先产生一个部分用户公钥[6]，使得这个方案更像自生成证书方案，而不是基于身份的方案。另外有一些方案[AP03]和[BSN05]提出的CL-PKE用的是安全性较低的Random Oracle模型[1,6]。

最近有学者提出了一种更严格的模型，该模型下的KGC能够在创建体制时在公共参数中留下只有其知道的后门[8]。而且已经有很大一部分CL-PKE加密体制被证明在该模型下是不安全的[1]。所以构造一个在这种模型下安全的加密体制是当前研究的一个热点[9]。本文在标准模型下构建的体制在加密时没有对运算，而且保持了基于身份的特点[10]。

## 1 基础知识

### 1.1 对运算

本文中，$G_1$表示一个加群，$G_2$表示一个有着同样阶的乘群，$p$表示$G_1$的生成元，对运算表示为$e:G_1\times G_1\to G_2$。对运算有以下一些性质。

(1) 双线型性：

收稿日期：2009－05－05； 修回日期：2010－09－14
基金项目：山东省自然科学基金(Y2007G37、2007G10001012)；
作者简介：杨 勇(1980－)，男，博士生，主要从事密码学、信息安全方面的研究.

$$e(Q+W,Z)=e(Q,Z)\cdot(W,Z)$$
$$e(Z,Q+W)=e(Z,Q)\cdot(Z,W)$$

(2) 非退化性：

$$e(G,G)\neq 1_{G_2}$$

(3) 可计算性：对运算是可计算的。

### 1.2 困难性问题假设

本文使用椭圆曲线上的点构成的对运算的困难性问题假设BDHP(binlineary diffie-hellman problem)，定义如下。

设$G_1$、$G_2$、$p$、$e$的定义同上，并且$p$、$ap$、$bp$、$cp\in G_1$，其中$a$、$b$、$c$是从$Z_p^*$中均匀选择的，则BDHP困难性问题假设就是已知$p$、$ap$、$bp$、$cp$，求解$e(p,p)^{abc}\in G_2$的值，表达为：

$$A(\langle p,ap,bp,cp\rangle\rightarrow e(p,p)^{abc}$$

式中　$A$是任意多项式时间的概率算法。

**定义** 1　如果对于任何多项式时间的概率算法$A$，都至多有$\varepsilon$的优势概率在群$G_1$中解决BDHP困难性问题假设，则BDHP困难性问题假设在群$G_1$中是安全的，表达为：

$$\Pr(A(\langle p,ap,bp,cp\rangle\rightarrow e(p,p)^{abc})-1/2\leqslant\varepsilon$$

## 2 算法组成

CL-PKE加密体制有密钥生成中心KGC、系统内用户以及使用系统的外部参与者共3类参与者。最初，文献[1]定义的CP-PKE加密体制由7个算法组成[1]，后来被简化成为5个算法[7]，分别描述如下。

(1) Setup$(K)=$(Params, Master-Key)：该算法由KGC执行，目的是由KGC生成密码体制的系统参数和主密钥。算法输入安全参数$K\in 1^n$；输出CL-PKE加密体制的系统参数Params和Master-key。

(2) Partial-Private-Key-Extract (Params,Private-key, ID)= $D_A$：该算法由KGC执行，目的是为每一个系统内的用户生成一个系统范围内的部分私钥。算法输入Params和Master-key以及系统内任意用户的身份ID；输出相应用户的部分私钥$D_A$。通常情况下，该用户的部分私钥$D_A$通过安全的秘密信道交给用户。

(3) Set-User-Key ($D_A$,$S$,Params)=($U_{\mathrm{pk}}$,$U_{\mathrm{sk}}$)：该算法由系统内用户执行，目的是系统内用户生成一个只有自己知道的用户私钥。算法输入KGC交给用户的部分密钥$D_A$和用户均匀选择的一个随机数$S\in Z_p^*$；输出用户的公钥$U_{\mathrm{pk}}$和私钥$U_{\mathrm{sk}}$，其中$U_{\mathrm{pk}}$在系统内公开，$U_{\mathrm{sk}}$由用户秘密保存。

(4) Encrypt$(m,\mathrm{Params},\mathrm{ID},s)=C$：该算法由系统外任意参与者执行，目的是用相应的系统内用户公钥加密要保密的明文信息$m$。算法输入要加密的信息$m$、公共参数Params、用户ID、均匀选择的随机数$S\in Z_p^*$和用户公钥$U_{\mathrm{pk}}$；输出密文$C$。

(5) Decrypt$(C,U_{\mathrm{sk}},\mathrm{Params},\mathrm{ID})=m$：该算法由相应的系统内用户执行，目的是用相应的私钥解密密文$C$。算法输入密文$C$、用户私钥$U_{\mathrm{sk}}$、公共参数Params和用户ID；输出相应的明文$m$。

## 3 安全模型

安全模型可以用一种由两方参与的游戏模拟，一方为攻击者，用$A$表示，另一方为挑战者，用$C$表示。在游戏中，攻击者可以向挑战者发出各种不同的Oracle询问，挑战者模拟回答相应的询问。如果挑战者能够正确回答攻击者的各种询问，挑战者就成功模拟了安全模型；而且，如果攻击者赢得了游戏，攻击者就攻破了相应的加密体制[11]。

以下首先对选择性身份模型下CL-PKE的安全模型进行定义，如在引言中所述，CL-PKE加密体制可能遭受到如传统PKE的外部攻击，以及如IBE的内部密钥生成中心KGC的攻击，因此下面针对这两种攻击定义了两种安全模型。

Game 1：外部攻击者和挑战者之间的游戏，攻击者定义为Type$_1$型。

Init：攻击者给挑战者一个要攻击的目标ID$^*$。

Setup：挑战者根据自己的参数模拟公共参数Params，并把Params交给攻击者。

Phase 1：攻击者可以向挑战者进行Extract Partial Private Key(提取用户的部分密钥)、Extract Private Key(提取用户私钥)、Request Public Key(询问用户公钥)、Replace Public Key(置换公钥)、Decryption Query(解密询问)多项式次询问。挑战者分别进行回答，当攻击者同意时，第一阶段结束。该阶段的目的是让挑战者用模拟得到的公共参数回答攻击者的询问，证明用一定的问题假设模拟的加密体制可以满足攻击者相应的询问。而询问本身就隐含着相应的攻击，为下一步的安全性归约做好了准备。

Challenge：攻击者提供两条明文$m_1$、$m_2$，挑战者均匀选择其中一条加密为$C_b$，其中$b$在(1,2)中均匀选择，并交给攻击者，让其辨别是那条明文的加密密文。该阶段的目的是把相应的困难性假设问题归约为辨别密文的困难性。

Phase 2：攻击者继续询问多项式次挑战者在Phase 1中同样的Oracle，并由攻击者决定何时结束。该阶段的目的和第一阶段相似，只是为了使安全模型拥有更高的安全性。

Guess：攻击者输出猜测$b'$，如果$b'=b$，那么攻击成功。这一阶段攻击者如果成功那么就辨别了密文，也就解决了相应的难解性问题。然而，实际上难解性问题在当前理论范围内不可解，所以攻击者不可能辨别密文，因而攻击者不可能成功，这就反证了加密体制的安全性。

$\text{Type}_1$型攻击者在Phase 1和Phase 2阶段进行询问时，有以下一些限制：

(1) 不能询问目标$\text{ID}^*$的用户私钥$U_{\text{sk}}$；

(2) 不能询问由目标$\text{ID}^*$加密、要求辨别的加密密文$(\text{ID}^*, m_b)$；

(3) 提交询问密文前，不能置换目标$\text{ID}^*$的用户公钥；

(4) 如果询问的加密密文的相应公钥已经被替换过，必须向挑战者提供相应用户私钥中的秘密值。

Game 2：内部攻击者KGC和挑战者之间的游戏，攻击者定义为$\text{Type}_2$型。该安全模型与Game 1相似。

**定义** 2 如果任何一个多项式时间攻击者都不能在不可忽略的时间内赢得Game 1(或Game 2)，则无证书加密体制(CL-PKE)是$\text{Type}_1$(或$\text{Type}_2$)型安全的，CL-PKE加密体制就是IND-CCA安全的。

# 4 新的CL-PKE加密体制和证明

## 4.1 新的CL-PKE加密体制

本文介绍的加密体制由5个算法组成，分别定义如下。

Setup：KGC输入参数$K$，分别输出mpk和msk，mpk由KGC公开，msk由KGC自己秘密保存。其中：

$$\text{mpk}=(g,g_1,h,V',V_1,V_2,\cdots,V_n)$$

式中 $g_1=g^{\alpha}$；$V'=g^{v'}$；$V_1=g^{v_1}$；$V_2=g^{v_2}$；$V_n=g^{v_n}$；$\text{msk}=(\alpha,v',v_1,v_2,\cdots,v_n)$。

Extract Partial Private Key：用户应向KGC提供自己的ID，KGC通过安全的秘密通道向用户输出用户的部分密钥$D_A=(r_{\text{ID}},h_{\text{ID}})$，其中$r_{\text{ID}}$是在$Z_p^*$中均匀选择的，$h_{\text{ID}}=(hg^{-r_{\text{ID}}})^{1/\alpha-\text{ID}}$。

Set-User-Key：用户输入用户的部分密钥$D_A$和一个均匀选择的随机数$x_{\text{ID}}\in Z_p^*$，输出用户密钥$U_{\text{sk}}$和用户公钥$U_{\text{pk}}$，$U_{\text{pk}}=(U_{\text{pk}_1}=e(g,h)^{x_{\text{ID}}}, U_{\text{pk}_2}=e(g,g)^{x_{\text{ID}}})$，$U_{\text{sk}}=(r_{\text{ID}},h_{\text{ID}},x_{\text{ID}})$，其中$x_{\text{ID}}$是用户选择的秘密。

Encrypt：加密者输入要加密的密文$m$、相应的ID和公钥，加密如下：

首先检验公钥形式的合法性$U_{\text{pk}_1}\cdot e(g,g)=U_{\text{pk}_2}\cdot e(g,h)$，如果不相等，输出⊥终止算法，否则如下继续加密

$$C=(U=(g_1g^{-\text{ID}})^s, V=e(g,g)^s,$$
$$W=U_{\text{pk}_1}{}^{-s}\cdot m, F=F_v(\omega)^s)$$

密文$C$中$F_v(\omega)=V'\cdot V_{i_1}^{\omega_1}\cdot V_{i_2}^{\omega_2}\cdot\cdots\cdot V_{i_n}^{\omega_n}$，其中$\omega=H(U,V,W,ID,u_{\text{pk}})$，$\omega$的bit表示为$\omega=\omega_1\omega_2\cdots\omega_n$。

在加密算法中，因为$e(g,g)$、$e(g,h)$两个对运算可以提前预计算，所以只需要计算一次就可以被所有用户共享，因而在加密时实际上不需要对运算。

Decrypt：用户输入密文$C$和自己的私钥，解密如下：

$$W\cdot(e(U,h_{\text{ID}})\cdot V^{r_{\text{ID}}})^{x_{\text{ID}}}=m$$
$$\omega'=H(U,V,W,ID,u_{\text{pk}})$$

如果$e(g_1g^{-\text{ID}},F)=e(U,F_v(\omega'))$，则解密正确，否则完整性检验失败，解密不正确。

## 4.2 新的CL-PKE的形式化证明

如果能够用BDHP难解问题的参数模拟新的CL-PKE加密体制的系统参数，并且挑战者可以回答攻击者的相应询问，把难解性问题BDHP归约为辨别密文的困难性，则挑战者模拟成功，新的CL-PKE加密体制符合安全模型的安全性要求。对方案的形式化证明是在攻击者$A$和挑战者$C$之间进行的。

初始化：攻击者首先挑选一个攻击目标$\text{ID}^*\in Z_p^*$。

参数设置：挑战者用自己拥有的参数，即困难性假设BDHP的参数模拟CL-PKE的系统参数。(1) 挑战者设置$g^a$、$g^b=h$、$g^c$，其中$g^b=h$；$c$等于目标$\text{ID}^*$的用户在设置用户密钥时的秘密值$x_{\text{ID}^*}$。$a$、$b$、$c$在$Z_p^*$中均匀分布，$g^b$、$g^c$与原体制中的分布率相同。(2) 随机挑选$k\in(0,1,\cdots,n)$，并挑选$\tau$使得$(n+1)\tau<P$。然后在$Z_\tau$中随机挑选$(x',x_1,x_2,\cdots,x_n)$，在$Z_p$中随机挑选$(y',y_1,y_2,\cdots,y_n)$使得$V'=(g^b)^{x'-k\tau}g^{y'}$、$V_i=(g^b)^{x_i}g^{y_i}$，且$1\leqslant i\leqslant n$。根据以上所设参数，有$F_v(\omega)=V'\prod_{i=1}^{n}V_i=(g^b)^{J(\omega)}g^{k(\omega)}$，$k(\omega)=y'+\prod_{i=1}^{n}\omega_i y_i$，$J(\omega)=x'+\prod_{i=1}^{n}\omega_i x_i-k\tau$。(3) 如上设置，$\text{mpk}=(g,g_1,h,V',V_1,V_2,\cdots,V_n)$，$\text{msk}=(\alpha,k,\tau,x',x_1\ldots x_n,y',y_1\ldots y_n)$，mpk和msk就是挑战者模拟的系统参数。因为是$\text{Type}_1$攻

击者，因而挑战者把mpk传给攻击者，自己保留msk。

Phase 1：(1)攻击者向挑战者询问用户的部分密钥 $D_A$、用户私钥 $U_{\mathrm{sk}}$、用户公钥 $U_{\mathrm{pk}}$ 时，挑战者根据新的CL-PKE体制中的Partial-Private-Key-Extract、Set-User-Key算法，用以上模拟的参数进行计算，并把结果传给攻击者，攻击者可在任何时刻对任意用户的公钥进行置换。(2) 当挑战者询问不包括目标 $ID^*$ 在内的解密Oracle时，挑战者运行新的CL-PKE加密体制中的Decrypt，并把结果传给攻击者。此外在询问解密Oracle时，如果攻击者置换了公钥，攻击者应把置换后的秘密值 $x_{\mathrm{ID}}$ 和要解密的信息 $C$ 一起传给挑战者，并且在Challenge阶段前不置换 $\mathrm{ID}^*$ 的公钥。(3) 当攻击者询问由 $\mathrm{ID}^*$ 加密的密文C时，挑战者检查事件 $B$，如果 $J(\omega)\bmod\tau=0$，挑战者退出，攻击者随机输出猜测比特 $b'$。(4) 如果所询问密文是由 $\mathrm{ID}^*$ 加密，并且 $J(\omega)\bmod\tau\neq 0$，可知 $J(\omega)\bmod P\neq 0$。设攻击者要求解密的密文是 $C=(U,V,W,F)$，则挑战者解密 $\omega=H(U,V,W,\mathrm{ID},u_{\mathrm{pk}})$、$g^s=U^{(\alpha-\mathrm{ID})^{-1}}$、$(g^b)^s=(F/(g^s)^{k(\omega)})^{1/J(\omega)}$、$m=W\cdot e((g^b)^s,g^{x_{\mathrm{ID}^*}})=W\cdot e((g^b)^s,g^c)$，并把 $m$ 传给攻击者。(5) 挑战者在加密计算 $\omega=H(U,V,W,\mathrm{ID},u_{\mathrm{pk}})$ 时，把每次计算得到的 $\omega$ 都存到一个表中，以后每当计算 $\omega$ 时把所得结果与表中所有的值进行比较，如果有相同的，说明发生碰撞，挑战者退出，攻击者随机输出猜测比特 $b'$。

当攻击者决定结束询问时，Phase 1结束。

Challenge：攻击者输出两个长度相等的明文 $m_1$ 和 $m_2$，挑战者随机挑选其中一个 $C_b$，然后检查事件 $A$，如果 $J(\omega^*)\bmod P\neq 0$，挑战者退出，攻击者随机输出猜测比特 $b'$，如果等于0，加密 $\omega=H(U,V,W,\mathrm{ID},u_{\mathrm{pk}})$、$U=(g^a)^{\alpha-\mathrm{ID}}=(g^{\alpha-\mathrm{ID}})^a=(g_1g^{-\mathrm{ID}})^s$、$V=e(g^a,g)=e(g,g)^a=e(g,g)^s$、$W=X^{-1}\cdot m$、$F=(g^a)^{k(\omega^*)}=(g^{k(\omega^*)})^s$，其中 $s=a$。

难解性问题BDHP归约为辨别密文的困难性。

Phase 2：攻击者继续询问多项式次挑战者在Phase 1中同样的Oracle，并由攻击者决定何时结束。

Guess：如果攻击者在不可忽略的概率下使得猜测比特 $b'=b$，则 $X=e(g,h)^{s\cdot x_{\mathrm{ID}^*}}=e((g^b)^a,g^c)=e(g,g)^{abc}$，否则 $X$ 是 $Z_p^*$ 中任一元素，说明如果可以辨别密文，就可以解决BDHP问题，反之如果BDHP问题不可解，密文就不可辨别，也就反证了新的CL-PKE密码体制的安全性。

$\mathrm{Type}_2$ 攻击者的形式化证明类似，在此省略。

**引理 1**　事件 $A$ 的概率 $\Pr[J(\omega^*)=0 \bmod P]>1/\tau(n+1)$。

证明　因为 $J(\omega^*)=0 \bmod P$ 当且仅当 $k\tau=(x'+\prod_{j=1}^{n}w_jx_j)$，又因为 $k\tau<\tau(n+1)$，所以 $k\tau<\tau(n+1)<P$，则 $\Pr[J(\omega^*)=0 \bmod P]<1/\tau(n+1)$。得证。

**引理 2**　事件 $B$ 的概率 $\Pr[J(\omega)\neq 0 \bmod \tau]\geqslant 1/2$。

证明　显而易见 $\Pr[J(\omega)=0 \bmod \tau]=1/\tau$，再者，如果攻击者询问解密Oracle的次数为 $q_d$，则 $\Pr[J(\omega)\neq 0 \bmod \tau]=(1-1/\tau)^{q_d}\geqslant(1-q_d/\tau)$。

如果设置 $\tau$ 的大小为 $2q_d$，则成功的概率为 $(1-1/\tau)^{q_d}\geqslant(1-q_d/\tau)\geqslant(1-q_d/2q_d)\geqslant 1/2$。得证。

**定理 1**　假如 $A$ 是任意一个 $\mathrm{Type}_1$(或 $\mathrm{Type}_2$)型多项式时间攻击者，由形式化证明可知，$A$ 在多项式时间内不可能赢得游戏，因而CL-PKE加密体制在任意 $\mathrm{Type}_1$(或 $\mathrm{Type}_2$)型多项式攻击者多项式时间攻击者的攻击下是安全的，并且安全性符合安全模型的要求。

证明　假设 $\mathrm{Type}_1$(或 $\mathrm{Type}_2$)型攻击者至多询问解密Oracle的次数为 $q_d$，询问用户公钥Oracle的次数为 $q_{\mathrm{upk}}$，询问用户私钥Oracle的次数为 $q_{\mathrm{usk}}$；另假设存在攻击者 $A'$ 和 $A''$。

(1) 攻击者 $A'$ 在多项式时间 $o(t)$ 内攻击困难性假设问题BDHP的优势概率为 $\mathrm{Adv}_{A'}^{\mathrm{BDHP}}(k)$。

(2) 攻击者 $A''$ 在多项式时间 $o(t)$ 内攻击碰撞稳固的hash函数 $\omega$ 的优势概率为 $\mathrm{Adv}_{A''}^{\mathrm{CR}}(k)$。

根据挑战者模拟成功的概率，$\mathrm{Type}_1$(或 $\mathrm{Type}_2$)型攻击者 $A$ 攻击本文加密体制的优势概率为：攻击者 $A'$ 在事件 $A$ 与事件 $B$ 发生的情况下攻击BDHP的优势概率与攻击hash函数的优势概率的和，由引理1和引理2可知，$\mathrm{Type}_1$(或 $\mathrm{Type}_2$)型攻击者的优势概率为：

$$\mathrm{Adv}_A^{\mathrm{CL-CCA-1}}(k)<1/\tau(n+1)\cdot 1/2\cdot\mathrm{Adv}_{A'}^{\mathrm{BDHP}}(k)+\mathrm{Adv}_{A''}^{\mathrm{CR}}(k)$$

**定理 2**　由定理1可知，加密体制在 $\mathrm{Type}_1$(或 $\mathrm{Type}_2$)型多项式时间攻击者下是安全的，所以本文新的CL-PKE加密体制在困难性问题假设BDHP下是IND- CCA安全的。

## 5　结 束 语

本文选用自然的困难性假设BDHP构建了加密

体制，同时为了获得更好的安全性选用了安全性较高的标准模型，所以本文的基础更加自然，安全性更可靠。如何在保证安全性的前提下提高效率是下一步的工作目标。

## 参 考 文 献


[1] Al-RIYAMI S S, PATERSON K. Certificateless public key cryptography[C]//Advances in Cryptology Asiacrypt 2003. Taibei: Springe Verlagr, 2003: 452-473.

[2] GENTRY C. Practical identity-based encryption without random oracle[C]//Advances in Cryptology Eurocrypt 2006. Saint Petersburg: Springe Verlag, 2006: 445-464.

[3] AU M H, CHEN J, LIU J K, et al. Malicious KGC attack in certificateless cryptography[C]//ACM Symposium on Information, Computer and Communications Security 2006. Taibei: ACM Press, 2007.

[4] HUANG Q, WONG D S. Generic certificateless encryption in the standard model[C]//Advances in Information and Computer Security, IWSEC 2007. Nara: Springe Verlag, 2007: 278-291.

[5] DENT A W, LIBERT B, PATERSON K G. Certificateless encryption schemes strongly secure in the standard model[C]//11th International Conference on Public Key Cryptography. Barcelona: Springe Verlag , 2007.

[6] ONG H, CHOI K Y, HWANG J Y, et al. Certificateless public key encryption in the selective-ID security model (Without Random Oracles) [C]//Pairing-Based Cryptography-Pairing 2007. Tokyo: Springe Verlag , 2007: 60-82.

[7] BAEK J, SAFAVI, NAINI R, SUSILO W. Certificateless public key encryption without pairing[C]//Information Security. Singapore : Springe Verlag , 2005:. 134-148.

[8] CHENG Zhao-hui, CHEN Li-qun, LING Li, et al. General and efficient certificateless public key encryption constructions[C]// Pairing-Based Cryptography-Pairing 2007. Tokyo: Springe Verlag , 2007: 83-107.

[9] WATERS B. Efficient identity-based encryption without random oracles[C]//Advances in Cryptology EUROCRYPT 2005. Aarhus: Springe Verlag, 2005: 114-127.

[10] DENT A W. A survey of certificateless encryption schemes and security models[J]. International Journal of Information Security, 2008,7(5): 349-377.

[11] CHENG Z, COMLEY R. Efficient certificateless public key encryption[R/OL]. [2009-03-14]. http://eprint.iacr.org/2005/012/


编 辑 黄 莘

---

(上接第899页)

## 参 考 文 献


[1] FEI Chun, TANG Xue-fei. Research on the E-learning application of web service[J]. Journal of Electronic Science and Technology of China, 2005, 3(3): 218-221.

[2] 郑向宏, 李院春, 李增智, 等. 面向语用Web服务的Qos评价模型研究[J]. 电子科技大学学报, 2007, 36(6): 1477-1480.
ZHENG Xiang-hong, LI Yuan-chun, LI Zeng-zhi, et al. Research on pragmatic web-oriented Qos evaluation model [J]. Journal of University of Electronic Science and Technology of China, 2007, 36 (6): 1477-1480.

[3] 赵文峰, 孟祥武, 陈俊亮. 信息提供类Web服务与RDF数据源的集成[J]. 北京邮电大学学报, 2008, 31 (6): 109-112.
ZHAO Wen-feng, MENG Xiang-wu, CHEN Jun-liang. Integration of information-providing web services and RDF data sources[J]. Journal of Beijing University of Posts and Telecommunications, 2008, 31(6). 109-112.

[4] PAPAZOGLOU M P, GEORGAK O D. Service oriented computing[J]. Communication of the ACM, 2003, 46 (10): 25-28.

[5] DAY J, DETERS R. Selecting the best web service[C]// Proceedings of the 2004 Conference of the Centre for Advanced Studies on Collaborative Research Tabel of Contents. Markham: [s.n.], 2004.

[6] 林清滢. 基于UDDI的语义Web服务发现研究[J]. 计算机工程与设计, 2006, 27(12): 2215-2217.
LIN Qing-ying. UDDI based semantic web service discovery research[J]. Computer Engineering and Design, 2006, 27(12): 2215-2217.

[7] KAMVAR S D, SCHLOSSER M T. In: Reputation management in P2P networks[C]//Proc of the 12th World Wide Web Conference. Hawaii: ACM Press, 2004: 123-134.

[8] RAMA A. RICHARD C. A method for semantically enhancing the service discovery capabilities of transaction on web service, 2003, 3(3): 310-323.

[9] 艾未华, 宋自林, 魏 磊, 等. 基于领域本体的Web服务发现[J]. 电子科技大学学报, 2007, 36(3): 506-509.
AI Wei-hua, SONG Zi-lin, WEI Lei, et al. Web service discovery based on domain ontology[J]. Journal of University of Electronic Science and Technology of China, 2007, 36(3): 506-509.

[10] 王 慧, 王金华, 赵煜辉, 等. 基于信誉的语义Web服务发现[J]. 计算机科学, 2007, 34(8): 130-134.
WANG Hui, WANG Jin-Hua, ZHAO Yu-Hui, et al. Reputation-based semantic web service discovery[J]. Computer Science, 2007, 34(8): 130-134.

[11] CURBERA F, KHALAF R, MUKHI N. The next step in web service[J]. ACM, 2003, 46(10): 29-34.

[12] 白东伟, 刘传昌, 陈俊亮. 一种增强语义精确度的Web服务匹配方法[J]. 北京邮电大学学报, 2006, 29(5): 40-44.
BAI Dong-wei, LIU Chuan-chang, CHEN Jun-liang. A web services matchmaking method with enhanced semantic precision[J]. Journal of Beijing University of Posts and Telecommunications, 2006, 29(5): 40-44.


编 辑 漆 蓉