文章编号: 1001-0920 (2010) 07-1031-04

一种安全有效的基于身份的门限签密方案

孙 华, 郑雪峰, 于义科, 周 芳

(北京科技大学 信息工程学院，北京 100083)

摘 要: 签密是一种将加密和数字签名技术结合在一起的思想, 它比采用先签名后加密的方法具有更高的效率. 基于双线性对技术, 提出了一种新的基于身份的门限签密方案. 它利用决策双线性Diffie-Hellman(DBDH) 问题的困难性在随机预言模型下给出了方案的语义安全性证明, 并利用计算Diffie-Hellman(CDH) 问题的困难性证明了方案的不可伪造性, 同时指出方案具有较高的效率.

关键词: 门限签密；双线性对；决策双线性Diffie-Hellman问题；随机预言模型

中图分类号: TP309 **文献标识码:** A

Secure and efficient identity-based threshold signcryption scheme

SUN Hua, *ZHENG Xue-feng*, *YU Yi-ke*, *ZHOU Fang*

(School of Information Engineering，University of Science and Technology Beijing，Beijing 100083，China. Correspondent：SUN Hua，E-mail：sh1227@163.com)

Abstract: The idea of signcryption is to provide a method to encrypt and sign data together in a way that is more efficient than using a signature scheme combined with an encryption scheme. A new identity-based threshold signcryption scheme is presented based on the bilinear pairings, which proves its semantic security on the hardness of decisional bilinear diffie-hellman(DBDH)problem and its unforgeability on the hardness of computational diffie-hellman(CDH) problem in the random oracle model. In addition, the scheme is proved to be efficient.

Key words: Threshold signcryption; Bilinear pairings; Decisional bilinear diffie-hellman problem; Random oracle model

1 引 言

1984 年, Shamir[1] 首先提出了基于身份的签名思想, 用以简化基于证书的PKI中的密钥管理, 然而早期的方案因为计算过于复杂而难以推广. Boneh 等[2]利用双线性对技术提出了一个实用的基于身份的加密方案, 随后人们又提出了一些基于身份的加密方案[3, 4], 同时也提出了一些基于身份的签名方案[5, 6].

消息的保密和认证是密码学中最重要的两个研究内容, 如何在消息通信过程中同时实现保密和认证是信息安全研究的主要目标之一. 1997 年, Zheng[7]首次提出了签密的概念, 即能够在一个合理的步骤内同时完成加密和数字签名两项功能, 而其通信成本和计算量都低于传统的先签名后加密方法. Dodis 等[8]第 1 次对签密方案的机密性和不可伪造性进行了形式化的描述, 随后一些可证安全的签密方案被相继提出[9].

Malone-Lee[10]提出了第 1 个基于身份的签密方案, 该方案具有消息的保密性和签名的不可伪造性. 然而 Libert 等[11]指出Malone-Lee的方案不是语义安全的, 并提出了满足语义安全的基于身份的签密方案. Duan 等[12]结合门限和基于身份的签密技术, 提出一个基于身份的门限签密方案, 但是该方案不满足不可否认性和语义安全性. Peng 等[13]基于Libert的方案提出一个基于身份的门限签密方案, 然而该方案不满足前向安全性. Li 等[14]利用双线性对技术提出了一个可证安全的基于身份的门限签密方案, 但当生成最终门限签密的指定结合者是其中的门限成员之一时, 它可以假冒这些成员生成一个对接受者来说是有效的伪造签密, 因而该方案不满足不可伪造性.

本文提出了一个安全的基于身份的门限签密方案, 并通过对方案的计算量进行分析, 得出该方案具有较高的效率.

收稿日期: 2009-06-16；**修回日期:** 2009-08-13.

基金项目: 国家自然科学基金项目(60674054)；国家杰出青年科学基金项目(51685168)；教育部重点科研基金项目(02152).

作者简介: 孙华(1980–), 男, 河南安阳人, 博士生, 从事密码学、信息安全技术的研究；郑雪峰(1951–), 男, 福州人, 教授, 博士生导师, 从事信息安全技术等研究.

2 预备知识

2.1 双线性对

设G, G_T是2个阶为素数q的循环加法群和循环乘法群, g是群G的生成元, 双线性对$e: G\times G\to G_T$是具有如下性质的映射:

1) 双线性: 对于所有的$P,Q\in G$与$a,b\in Z$, 都有$e(aP,bQ)=e(P,Q)^{ab}$;

2) 非退化性: $e(g,g)\neq 1$;

3) 可计算性: 存在一个有效的算法计算$e(P,Q)$, 其中$P,Q\in G$.

2.2 相关困难问题

定义 1 假设G和G_T是2个阶为素数q的群, P是群G的生成元, $e: G\times G\to G_T$为双线性映射, 则DBDH问题为: 给定$P,aP,bP,cP\in G$, $h\in G_T$, $a,b,c\in Z_q^*$, 判定是否$h=e(P,P)^{abc}$.

定义敌手解决DBDH问题的优势为

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{DBDH}}=$$
$$|P_r\big[\mathcal{A}\big(aP,bP,cP,e(P,P)^{abc}\big)=1\big]-$$
$$P_r[\mathcal{A}(aP,bP,cP,h)=1]|.$$

定义 2 假设G和G_T是2个阶为素数q的群, P是群G的生成元, $e: G\times G\to G_T$为双线性映射, 则CDH问题为: 给定$P,aP,bP\in G$, $a,b\in Z_q^*$, 计算abP.

定义敌手解决CDH问题的优势为

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{CDH}}=P_r[\mathcal{A}(P,aP,bP)=abP]. \tag{1}$$

3 一个新的基于身份的门限签密方案

3.1 方案描述

在本方案中包含4种角色的用户PKG, 一个可信的秘密分发者dealer, 一个身份为ID_A的发送成员组$U_A=\{M_1,M_2,\cdots,M_n\}$, 以及身份为$\mathrm{ID}_B$的签密接收者. 方案描述如下:

(1) Setup. 给定安全参数k, PKG选择阶为素数q的加法群G和乘法群G_T, 群G的生成元P, 一个双线性映射$e: G\times G\to G_T$, 安全的对称加密函数(E,D)以及3个哈希函数$H_1: \{0,1\}^*\to G$, $H_2: G_T\to\{0,1\}^{n_1}$, $H_3: \{0,1\}^*\to Z_q^*$. PKG随机选取主密钥s并计算公钥$P_{\mathrm{pub}}=sP$, 然后公布系统参数为$\mathrm{params}=(G,G_T,n_1,e,P,P_{\mathrm{pub}},E,D,H_1,H_2,H_3)$,将主密钥$s$保密.

(2) Extract. 给定身份ID, PKG计算$Q_{\mathrm{ID}}=H_1(\mathrm{ID})$和$S_{\mathrm{ID}}=sQ_{\mathrm{ID}}$, 然后把$S_{\mathrm{ID}}$秘密地发送给用户.

(3) Keydis. 给定门限值t和n满足$1\leqslant t\leqslant n\leqslant q$. 秘密分发者dealer按照如下方式把$S_{\mathrm{ID}_A}$在发送组成员$U_A$间进行共享.

1) 在G^*中随机选取元素$F_1,F_2,\cdots,F_{t-1}$, 构造多项式$F(x)=S_{\mathrm{ID}_A}+xF_1+\cdots+x^{t-1}F_{t-1}$.

2) 计算$S_i=F(i)$, $i=0,1,\cdots,n$, 其中$S_0=S_{\mathrm{ID}_A}$. 然后把S_i秘密地发送给M_i, $i=1,2,\cdots,n$.

3) 广播$y_0=e(P,S_{\mathrm{ID}_A})$和$y_j=e(P,F_j)$, $j=1,2,\cdots,t-1$.

4) 每个成员M_i通过计算$e(P,S_i)=\prod_{j=0}^{t-1}y_j^{ij}$来判定其秘密分享$S_i$是否正确. 如果$S_i$不是有效的秘密分享, 则$M_i$发出一个错误广播并要求一个正确的秘密分享.

(4) Signcrypt. 假定$M_1,\cdots,M_t$是代表群U_A对消息m进行签密的t个成员.

1) 每个成员M_i随机选取$x_i\in Z_q^*$, 计算$R_{1i}=x_iP$, $R_{2i}=et(P_{\mathrm{pub}},Q_{\mathrm{ID}_B})^{x_i}$, 并把$(R_{1i},R_{2i})$发送给门限签密的生成者$C$.

2) C计算$R_1=\sum_{i=1}^{t}R_{1i}$, $R_2=\prod_{i=1}^{t}R_{2i}$, $k=H_2(R_2)$, $c=E_k(m)$, $h=H_3(R_1,k,m)$, 然后把h发送给成员$M_i(i=1,\cdots,t)$.

3) 每个成员M_i计算其部分签名$W_i=x_iQ_A+h\eta_iS_i$, 并把它发送给C, 其中$\eta_i=\prod_{j=1,j\neq i}^{t}\frac{-j}{i-j}\bmod q$为拉格朗日系数.

4) C通过检查等式

$$e(P,W_i)=e(R_{1i},Q_A)\cdot\Big(\prod_{j=0}^{t-1}y_j^{i^j}\Big)^{h\eta_i}$$

是否成立来验证部分签名的有效性. 如果该部分签名不正确, 那么C拒绝它并要求发送正确的签名, 然后C计算$W=\sum_{i=1}^{t}W_i$, 则最终的门限签密为$\sigma=(c,R_1,W)$.

(5) Unsigncrypt. 当收到签密σ, 接收者ID_B进行如下计算:

1) 计算$\gamma=e(R_1,S_{\mathrm{ID}_B})$和$k=H_2(\gamma)$;

2) 恢复出明文$m=D_k(c)$;

3) 计算$h=H_3(R_1,k,m)$, 当且仅当等式$e(P,W)=e(R_1+hP_{\mathrm{pub}},Q_A)$成立时, σ为一个有效的门限签密.

3.2 方案正确性

1) 由R_2和γ的值, 方案的一致性很容易得到验证, 即

$$\gamma=e(R_1,S_{\mathrm{ID}_B})=e\Big(\sum_{i=1}^{t}R_{1i},S_{\mathrm{ID}_B}\Big)=$$
$$e\Big(\sum_{i=1}^{t}x_iP,S_{\mathrm{ID}_B}\Big)=e\Big(\sum_{i=1}^{t}x_iP_{\mathrm{pub}},Q_{\mathrm{ID}_B}\Big)=$$

$$\prod_{i=1}^{t} R_{2i} = R_2.$$

2) 当接收者恢复出明文m和计算h后, 它可以验证σ确实是一个有效的签密.

$$e(P,W) =$$
$$e\Big(P,\sum_{i=1}^{t} W_i\Big) = e\Big(P,\sum_{i=1}^{t} x_i Q_A + h\eta_i S_i\Big) =$$
$$e\Big(P,\sum_{i=1}^{t} x_i Q_A + \sum_{i=1}^{t} h\eta_i S_i\Big) =$$
$$e\Big(\sum_{i=1}^{t} x_i P, Q_A\Big)\cdot e(P, hS_{\mathrm{ID}_A}) =$$
$$e(R_1, Q_A)\cdot e(P_{\mathrm{pub}}, hQ_A) = e(R_1 + hP_{\mathrm{pub}}, Q_A).$$

3.3 方案安全性

3.3.1 EUF-IDTSC-CMIA证明

定理 1　假设A是一个在适应性选择消息和身份下攻击本方案的伪造者, 它的运行时间至多为t, 获得的优势为ε. A可以提出至多$q_{H_i}(i=1,2,3)$次hash函数询问, q_E次私钥询问, q_S次签密询问, q_U次解签密询问. 假定$\varepsilon \geqslant (10(q_S+1)(q_S+q_{H_3})q_{H_1})/(l-1)$, 则CDH问题能够以至少$1/9$的概率在时间$23q_{H_1}q_{H_3}t/(\varepsilon(1-1/l))$内解决, 其中$l$为安全参数.

证明　构造算法C, 它利用A解决CDH问题. 将CDH问题的一个实例(P, aP, bP)给予C, 它的目标是计算abP. 为了响应对随机预言机$O_{H_1}, O_{H_2}, O_{H_3}$的询问, 算法C维护3个列表$L_1$,$L_2$,$L_3$. 假定在对身份ID进行extract, signcryption, unsigncryption询问前需要先进行H_1(ID)询问. 首先, C给出敌手A将要伪造签密的发送者身份ID_A; 然后C给定A系统参数params, $P_{\mathrm{pub}} = aP$. 可通过挑战者C与敌手A之间的游戏进行描述:

$H_1(\mathrm{ID}_i)$-Hash Query: C检查列表L_1中是否存在二元组(ID_i, x_i), 如果存在, 则C响应x_iP; 否则, 算法C作如下响应:

1) 如果$\mathrm{ID}_i = \mathrm{ID}_A$, 则C响应$bP$.

2) 如果$\mathrm{ID}_i \neq \mathrm{ID}_A$, 则C任选$x \in Z_q^*$, 把$(\mathrm{ID}_i, x)$添加到列表$L_1$中, 并把$H_1(\mathrm{ID}_i) = xP$发送给A.

$H_2(R_2)$-Hash Query: C检查列表L_2中是否存在二元组(R_2, k_i), 如果存在, 则C响应k_i; 否则, 算法C任选$k \in Z_q^*$, 把(R_2, k)添加到列表L_2中, 并把k发送给A, 其中$(\cdot, k)$没有存在列表L_2中.

$H_3(m_i, R_1, k_i)-$Hash Query: C检查列表L_3中是否存在四元组(m_i, R_1, k_i, h_i). 如果存在, 则C响应h_i; 否则, 算法C任选$h \in Z_q^*$, 把(m_i, R_1, k_i, h)添加到列表L_3中, 并把h发送给A, 其中$(\cdot,\cdot,\cdot,h)$没有存在列表L_3中.

Extract(ID_i) Query: 如果$\mathrm{ID}_i = \mathrm{ID}_A$, 则C返回$\perp$; 如果$\mathrm{ID}_i \neq \mathrm{ID}_A$, 则C从列表$L_1$中找到$(\mathrm{ID}_i, x_i)$, 计算$x_iP_{\mathrm{pub}} = x_i(aP)$作为其私钥, 并发送给A.

Signcrypt(m,ID_S,ID_B) Query: 算法C作如下响应:

1) 如果$\mathrm{ID}_S \neq \mathrm{ID}_A$, 则C运行Extract算法, 计算$\mathrm{ID}_S$的私钥$S_{\mathrm{ID}_S}$; 然后运行Keydis算法计算$S_{\mathrm{ID}_S}$的$n$个私钥分享$\{S_i\}_{i=1,2,\cdots,n}$; 最后C返回Signcrypt($m_b$, $\{S_i\}_{i=1,2,\cdots,t}, \mathrm{ID}_B$), 作为对询问的响应.

2) 否则, C任选$x, h \in Z_q^*$, 计算$R_1 = xP - hP_{\mathrm{pub}}$, $W = x(bP)$, $\gamma = e(R_1, S_{\mathrm{ID}_B})$. 然后C计算$k = H_2(\gamma)$和$c = E_k(m)$, 并检查列表$L_3$中是否存在四元组$(m, R_1, k, h^*), h^* \neq h$. 如果存在, 则算法C重复这一过程直到找到一个新的四元组(m, R_1, k, h), 其前3个元素没有在列表L_3的某一四元组中出现. 最后C把该四元组(m, R_1, k, h)添加到L_3中, 并将(c, R_1, W)作为响应返回给A, 可知它是一个有效的签密.

Unsigncrypt Query: 对一个签密$\sigma^* = (c^*, R_1^*, W^*)$的unsigncryption query, 作如下考虑:

1) 如果$\mathrm{ID}_A = \mathrm{ID}_B$, 则C回答$\sigma^*$是无效的签密.

2) 如果$\mathrm{ID}_A \neq \mathrm{ID}_B$, 则C计算$\gamma^* = e(R_1^*, S_{\mathrm{ID}_B})$, $k^* = H_2(\gamma^*)$和$m^* = D_{k^*}(c^*)$; 然后C计算$h^* = H_3(R_1^*, k^*, m^*)$并检查等式$e(P, W^*) = e(R_1^* + h^*P_{\mathrm{pub},Q_A})$是否成立. 如果等式成立, 则C返回$m^*$; 否则拒绝$\sigma^*$.

如果整个过程C没有失败退出, 则A以概率ε输出一个有效的伪造签密$\sigma^* = (c, R_1, W)$. 应用oracle重放技术和文献[15]中的分叉引理, 可得到算法C以至少$1/9$的概率在时间$23q_{H_1}q_{H_3}t/(\varepsilon(1-1/l))$内得到两个有效的签密$\sigma_1 = (c, R_1, W_1)$和$\sigma_2 = (c, R_1, W_2)$, 其中$h_1 \neq h_2$. 由

$$W_1 = \sum_{i=1}^{t} x_i Q_A + h_1 S_A,\ W_2 = \sum_{i=1}^{t} x_i Q_A + h_2 S_A,$$

算法C容易得到

$$t(W_1 - W_2)(h_1 - h_2)^{-1} = abP,$$

这就是CDH问题的解. 因此, 如果存在一个敌手以不可忽略的概率伪造一个有效的签密, 则存在一个算法以不可忽略的概率解决CDH问题, 而这与CDH问题是一个困难问题相矛盾, 故方案是EUF-IDTSC-CMIA安全的. □

3.3.2 IND-IDTSC-CCA2证明

定理 2　假设DBDH问题是困难的, 则本方案在随机预言模型下是IND-IDTSC-CCA2安全的.

证明　构造算法C, 它利用敌手A解决DBDH问

题. 将DBDH问题的一个实例(P, aP, bP, cP, h)给予C, 它的目标是判定是否$h = e(P,P)^{abc}$. 为了响应对随机预言机$O_{H_1}, O_{H_2}, O_{H_3}$的询问, 算法C维护3个列表$L_1, L_2, L_3$. 假定在对身份ID进行extract, signcryption, unsigncryption询问前, 需要进行$H_1(\mathrm{ID})$询问. 首先, C给出敌手A将要伪造的发送者身份ID_A; 然后C给定A系统参数params, $P_{\mathrm{pub}} = aP$. 可通过挑战者C与敌手A之间的游戏进行描述:

$H_1(\mathrm{ID}_i)$-Hash Query: C检查列表L_1中是否存在二元组(ID_i, x_i), 如果存在, 则C响应x_iP; 否则, 算法C作如下响应:

1) 如果$\mathrm{ID}_i = \mathrm{ID}_A$, 则C响应$bP$.

2) 如果$\mathrm{ID}_i \neq \mathrm{ID}_A$, 则C任选$x \in Z_q^*$, 把$(\mathrm{ID}_i, x)$添加到列表$L_1$中, 并把$H_1(\mathrm{ID}_i) = xP$发送给A.

$H_2(R_2)$-Hash Query: C检查列表L_2中是否存在二元组(R_2, k_i), 如果存在, 则C响应k_i; 否则, 算法C任选$k \in Z_q^*$, 把(R_2, k)添加到列表L_2中, 并把k发送给A, 其中$(\cdot, k)$没有存在列表L_2中.

$H_3(m_i, R_1, k_i)$-Hash Query: C检查列表L_3中是否存在四元组(m_i, R_1, k_i, h_i), 如果存在, 则C响应h_i; 否则, 算法C任选$h \in Z_q^*$, 把(m_i, R_1, k_i, h)添加到列表L_3中, 并把h发送给A, 其中$(\cdot, \cdot, \cdot, h)$没有存在列表L_3中.

Extract(ID_i) Query: 如果$\mathrm{ID}_i = \mathrm{ID}_A$, 则C返回$\perp$; 如果$\mathrm{ID}_i \neq \mathrm{ID}_A$, 则C从列表$L_1$中找到$(\mathrm{ID}_i, x_i)$, 计算$x_iP_{\mathrm{pub}} = x_i(aP)$作为其私钥, 并发送给A.

Signcrypt(m, ID_S, ID_B) Query: 算法C作如下响应:

1) 如果$\mathrm{ID}_S \neq \mathrm{ID}_A$, 则C运行Extract算法, 计算$\mathrm{ID}_S$的私钥$S_{\mathrm{ID}_S}$; 然后运行Keydis算法, 计算$S_{\mathrm{ID}_S}$的$n$个私钥分享$\{S_i\}_{i=1,2,\cdots,n}$; 最后C返回Signcrypt($m_b$, $\{S_i\}_{i=1,2,\cdots,t}$, ID_B), 作为对询问的响应.

2) 否则, C任选$x, h \in Z_q^*$, 计算$R_1 = xP - hP_{\mathrm{pub}}$, $W = x(bP)$, $\gamma = e(R_1, S_{\mathrm{ID}_B})$. 然后C计算$k = H_2(\gamma)$和$c = E_k(m)$, 并检查列表$L_3$中是否存在四元组$(m, R_1, k, h^*)$,$h^* \neq h$. 如果存在, 则算法C重复这一过程直到找到一个新的四元组(m, R_1, k, h), 其前3个元素没有在列表L_3的某一四元组中出现. 最后C把该四元组(m, R_1, k, h)添加到L_3中, 并将(c, R_1, W)作为响应返回给A, 可知它是一个有效的签密.

Unsigncrypt Query: 对一个签密$\sigma^* = (c^*, R_1^*, W^*)$的unsigncryption query, 作如下考虑:

1) 如果$\mathrm{ID}_A = \mathrm{ID}_B$, 则C回答$\sigma^*$是无效的签密.

2) 如果$\mathrm{ID}_A \neq \mathrm{ID}_B$, 则C计算$\gamma^* = e(R_1^*, S_{\mathrm{ID}_B})$, $k^* = H_2(\gamma^*)$和$m^* = D_{k^*}(c^*)$; 然后C计算$h^* = H_3(R_1^*, k^*, m^*)$并检查等式$e(P, W^*) = e(R_1^* + h^*P_{\mathrm{pub}}, Q_A)$是否成立, 如果等式成立, 则C返回$m^*$; 否则, 拒绝$\sigma^*$.

在第1阶段结束后, A选择一对它将要发起挑战的身份$(\mathrm{ID}_i, \mathrm{ID}_j)$. 注意到如果敌手A询问了身份$\mathrm{ID}_A$, 则它在上面步骤中已经失败, 然后A输出两个明文m_0和m_1, C任意选取一位$b \in \{0,1\}$并对m_b签密. 在这个过程中, C令$R_1^{**} = cP$, 得到$k^{**} = H_2(h)$(其中h为DBDH实例中的h), 并计算$c_b = E_{k^{**}}(m_b)$. 然后C任意选择$W^{**} \in G^*$, 并把$\sigma^{**} = (c_b, R_1^{**}, W^{**})$发送给A. A像第1阶段那样发起一定数量的询问. 在游戏过程的最后, A输出对b的猜测b^*, 并认为等式$\sigma^{**} = \mathrm{Signcrypt}(m_{b^*}, \{S_i\}_{i=1,2,\cdots,t}, \mathrm{ID}_j)$成立. 此时, 如果$b = b^*$, 则C输出$h = e(R_1^{**}, S_{\mathrm{ID}_j}) = e(cP, abP) = e(P,P)^{abc}$作为DBDH问题的解; 否则, C停止游戏并输出失败.

如果存在一个敌手以不可忽略的概率成功地进行CCA2攻击, 则存在一个有效的算法以不可忽略的概率解决DBDH问题, 这与DBDH问题是一个困难问题相矛盾, 故方案是IND-IDTSC-CCA2安全的. □

3.4 方案效率

双线性对计算所花费的计算成本远高于诸如群中元素的点乘运算和指数运算, 因此这里只考虑双线性对的计算成本. 文献[13]和[14]中的签密和解密阶段所进行的双线性对计算分别为$3t$和4及$2t+1$和3, 而在本方案中, 签密和解密阶段分别需要$2t$和3个, 因此具有较高的效率.

4 结 论

本文利用双线性对知识提出了一个在随机预言模型下可证安全的基于身份的门限签密方案. 通过证明得出该方案不仅满足语义安全性, 同时具有不可伪造性. 最后, 通过对方案的计算量进行分析, 得出该方案相比已有的方案具有较高的效率.

参考文献(References)

[1] Shamir A. Identity-based cryptosystems and signature schemes[C]. Proc of Crypto 1984. Berlin: Springer-Verlag, 1984: 47-53.

[2] Boneh D, Franklin M. Identity-based encryption from the weil pairing[C]. Proc of Crypto 2001. Berlin: Springer-Verlag, 2001: 213-229.

[3] Waters B. Efficient identity-based encryption without random oracles[C]. Proc of Eurocrypt 2005. Berlin: Springer-Verlag, 2005: 114-127.

[4] Gentry C. Practical identity-based encryption without random oracles[C]. Proc of Eurocrypt 2006. Berlin: Springer-Verlag, 2006: 445-464.

(下转第1039页)