一种有效的分级的基于身份签名方案

孙 华[1] 王爱民[1] 郑雪峰[2]
(安阳师范学院计算机与信息工程学院 安阳 455000)[1]
(北京科技大学计算机与通信工程学院 北京 100083)[2]

摘 要 利用双线性对技术,依据Boneh等人提出的分级的基于身份加密方案,设计了一个在标准模型下分级的基于身份的签名方案。方案中签名的大小是一个常量,且与签名者所在的层数无关。最后,对方案的安全性进行了分析,证明方案在Diffie-Hellman Inversion(DHI)困难问题的假设下满足选择消息和选择身份攻击下的存在不可伪造性。

关键词 分级的基于身份的签名,双线性对,DHI问题
中图法分类号 TP309 **文献标识码** A

Efficient Hierarchical Identity-based Signature Scheme

SUN Hua[1] WANG Ai-min[1] ZHENG Xue-feng[2]
(School of Computer and Information Engineering, Anyang Normal University, Anyang 455000, China)[1]
(School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China)[2]

Abstract By using bilinear pairings technique, this paper presented a hierarchical identity based signature scheme in the standard model according to hierarchical identity based encryption scheme proposed by Boneh et al. The size of signature in the scheme is a constant and regardless of hierarchy depth of the signer. In the last, we proved the scheme is existential unforgeable against selective identity, selective chosen message attack in terms of the hardness of DHI problem.

Keywords Hierarchical identity based signature, Bilinear pairing, Diffie-hellman inversion problem

1984年,Shamir[1]首先提出了基于身份的公钥密码体制,用以解决传统公钥密码体制中的证书管理。在基于身份的密码体制中,用户的公钥为能够标识用户身份的信息,如E-mail地址或IP地址,而其私钥则由密钥生成器(PKG)产生。2001年,Boneh和Franklin[2]利用双线性对技术提出了第一个实用的基于身份的加密方案,此后对基于身份密码系统的研究迅速活跃起来,人们又提出了一些基于身份的加密方案[3,4]和签名方案[5,6]。

对于仅有一个PKG的基于身份密码系统而言,它不但要生成用户的私钥,还要验证用户身份并且通过建立安全通道来传送用户的私钥,从而导致系统效率不高。尤其是在用户规模庞大的网络环境下,PKG的工作负担是相当繁重的。2002年,Horwitz等人[7]提出了分级的基于身份密码系统的思想。在这种系统中,多个PKG按照树状结构分布,根PKG只为其下一层的PKG或用户产生私钥,下层的PKG又为它下一层的PKG或用户产生私钥,并且身份的验证和私钥的传输也可以在局部完成,这样不仅解决了单个PKG工作负担过重的问题,而且大大提高了系统的效率。Gentry等人[8]基于判定型双线性Diffie-Hellman(DBDH)问题提出了第一个分级的基于身份加密(HIBE)方案,并在随机预言模型下对方案的安全性进行了证明。2004年,Boneh等人[9]提出了一种在适应性选择密文攻击下安全的HIBE方案。随后人们又提出了几个HIBE方案[10,11],并在标准模型下证明了方案的安全性。

2002年,Gentry等人[8]提出了第一个分级的基于身份的签名(HIBS)方案,但是没有给出方案的安全性证明。Chow等人[12]提出第一个可证安全的HIBS方案,然而签名的长度随着用户身份级数的增加而增长。Au等人[13]以及Zhang等人[14]提出了在标准模型下可证安全的HIBS方案,然而方案的安全性基于较强的困难假设。李进等人[15]提出了两个HIBS方案,然而其均是基于随机预言模型的。2010年,Markus[16]首次基于格基归约算法提出了HIBS方案。2011年,吴青等人[17]提出了在标准模型下基于分级身份的短签名方案,然而方案的安全性也是基于较强的困难假设。

本文借鉴Boneh等人[10]方案的思想,设计了标准模型下签名长度固定的基于分级身份的签名方案,并且方案的安全性基于一般性困难假设。

1 预备知识

1.1 双线性对

设G、G_T是两个阶为素数p的循环加法群和循环乘法群,g是群G的生成元,双线性对$e:G\times G\rightarrow G_T$是具有如下性

到稿日期:2011-11-12 返修日期:2012-02-20 本文受国家自然科学基金项目(61170244),河南省科技攻关计划项目(112102210370),河南省教育厅自然科学基础研究计划项目(12A520002)资助。

孙 华(1980-),男,博士,讲师,CCF会员,主要研究方向为密码学与信息安全,E-mail:sh1227@163.com;王爱民(1957-),男,教授,主要研究方向为可信计算、数据挖掘;郑雪峰(1951-),男,教授,主要研究方向为网络与信息安全。

质的映射：

1. 双线性：对于所有的 $U,V\in G$ 与 $a,b\in Z^*$，都有 $e(aU,bV)=e(U,V)^{ab}$；

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 $e(U,V)$，其中 $U,V\in G$。

1.2 困难问题假设

l 阶 Diffie-Hellman 逆*（l-DHI*）问题：已知 G 是阶为素数 p 的循环群，g 是群 G 的生成元，给定 $g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^l}\in G$，其中 $\alpha\in Z_p^*$ 且未知，计算 $g^{\alpha^{l+1}}$。

我们说(t,ε,l)-DHI* 假设成立，如果没有算法至多运行多项式时间 t，至少能以不可忽略的概率解决 l-DHI* 问题。

2 基于分级身份的签名

2.1 形式化定义

定义 1 在分级的基于身份的签名方案中，用户的身份是用向量来表示的，向量的维度代表了相应深度的用户身份。基于分级身份的签名方案可由以下 4 个算法组成，即系统建立、私钥提取、签名和验证。

1. 系统建立：给定安全参数 k，该算法生成系统参数 *params* 以及相应的主密钥 *msk*。系统参数 *params* 是公开的，而主密钥 *msk* 是保密的。

2. 私钥提取：输入系统参数 *params*、用户身份向量信息 $ID_{|k}$ 以及上一层 PKG 的密钥 $d_{ID|k-1}$，该算法输出身份 $ID_{|k}$ 的私钥 $d_{ID|k}$。

3. 签名：输入系统参数 *params*、消息 m 以及用户身份 ID 的私钥 d_{ID}，该算法输出在消息 m 下的签名 σ。

4. 验证：输入系统参数 *params*、签名 σ、消息 m 以及用户身份 ID，如果 σ 是用户身份 ID 在消息 m 上的签名，则输出 True；否则，输出 False。

这些算法必须满足基于身份签名方案的一致性要求，即如果 $\sigma=Sign(params,m,d_{ID})$，则 $\text{True}=Verify(params,\sigma,m,ID)$。

2.2 HIBS 的安全模型

下面介绍基于分级身份的签名方案的安全模型。

定义 2 一个基于分级身份的签名方案在适应性选择消息和选择身份攻击下是存在不可伪造性的（EU-sID-CMIA），即如果没有概率多项式时间的敌手 $\mathcal{A}$ 在下面的游戏中获得不可忽略的优势：

初始化：敌手 $\mathcal{A}$ 向挑战者 $\mathcal{C}$ 公开挑战身份 ID^*。

系统建立：挑战者 $\mathcal{C}$ 运行签名方案的系统建立算法，生成系统参数 *params* 并发送给敌手 $\mathcal{A}$，保存主密钥 *msk*。

询问：敌手 $\mathcal{A}$ 可以适应性地向挑战者 $\mathcal{C}$ 发出如下询问。

私钥询问：敌手 $\mathcal{A}$ 可以询问身份 ID 的私钥，这里要求 $ID\neq ID^*$ 并且 ID 不是 ID^* 的前缀。挑战者 $\mathcal{C}$ 运行私钥提取算法，计算其私钥 d_{ID} 并发送给 $\mathcal{A}$。

签名询问：敌手 $\mathcal{A}$ 可以询问任意身份 ID 在任意消息 m 上的签名 σ。挑战者 $\mathcal{C}$ 首先运行私钥提取算法，产生签名者的私钥 d_{ID}，然后运行签名算法，生成签名 σ 并将其发送给 $\mathcal{A}$。

伪造：敌手 $\mathcal{A}$ 输出在挑战身份 ID^* 和消息 m^* 下的伪造签名 σ^*，这里要求 (ID,m^*)（其中 $ID=ID^*$ 或 ID 是 ID^* 的前缀）没有出现在前面的签名询问中。如果对 σ^* 的验证结果不为 False，那么 $\mathcal{A}$ 赢得游戏，敌手 $\mathcal{A}$ 的优势定义为其赢得游戏的概率。在该游戏中，如果不存在运行时间至多为 t、优势至少为 ε 的敌手 $\mathcal{A}$，并且 $\mathcal{A}$ 私钥询问的次数最多为 q_e、签名询问的次数最多为 q_s，那么该 HIBS 方案是 (t,ε,q_e,q_s)-EU-sID-CMIA 安全的。

3 标准模型下分级的基于身份签名方案

3.1 方案描述

设 G、G_T 是阶为素数 p 的循环群，生成元 $g\in G$，$e:G\times G\to G_T$ 是一个双线性映射。设 HIBS 的最大深度为 l，第 j 级身份 $ID_{|j}=(ID_1,ID_2,\cdots,ID_j)$ 是由 j 个元素组成的向量，其中 $ID_1,\cdots,ID_j\in Z_p^*$。两个无碰撞哈希函数 $H_1:\{0,1\}^*\to Z_p^*$ 和 $H_2:\{0,1\}^*\to Z_p^*$ 将任意长度的分级身份中的元素和消息 m 映射为非零整数，则该 HIBS 方案可由如下算法构成：

(1)系统建立

PKG 随机选取 $\alpha\in Z_p$，生成元 $g\in G$，计算 $g_1=g^{\alpha}$。选取 $g_2,g_3\in G$，向量 $\hat{H}=(h_1,h_2,\cdots,h_l)\in G$，则系统公开参数为 $param=(G,G_T,e,g,g_1,g_2,g_3,\hat{H})$，主密钥为 $msk=g_2^{\alpha}$。

(2)私钥提取

为产生身份 $ID_{|j}=(ID_1,ID_2,\cdots,ID_j)$ 的私钥，其中 $1\leqslant j\leqslant l$，PKG 任选 $r\in Z_p^*$，计算其私钥为：

$$d_{ID|j}=(g_2^{\alpha}(h_1^{ID_1}\cdots h_j^{ID_j}g_3)^r,g^r,h_{j+1}^r,\cdots,h_l^r)$$
$$=(a_0,a_1,b_{j+1},\cdots,b_l)$$

另外，身份 $ID_{|j}$ 的私钥也可以由身份 $ID_{|j-1}$ 的私钥 $d_{ID|j-1}$ 直接产生。设 $d_{ID|j-1}=(a_0,a_1,b_j,\cdots,b_l)$，任选 $t\in Z_p$，计算：

$$d_{ID|j}=(a_0b_j^{ID_j}(h_1^{ID_1}\cdots h_j^{ID_j}g_3)^t,a_1g^t,b_{j+1}h_{j+1}^t,\cdots,b_lh_l^t),$$

显然，$d_{ID|j}$ 是身份 $ID_{|j}$ 的私钥。

(3)签名

为了生成身份 $ID_{|j}=(ID_1,ID_2,\cdots,ID_j)$ 在消息 m 上的签名，签名者首先计算 $m=H_2(ID_{|j},m)$，任选 $t\in Z_p$，然后利用其私钥 $d_{ID|j}$ 计算：

$C_1=g^t,C_2=a_1=g^r$

$C_3=a_0\cdot(g^m)^t$

最后输出该签名 $\sigma=(C_1,C_2,C_3)$。

(4)验证

当签名验证者收到在身份 $ID_{|j}=(ID_1,ID_2,\cdots,ID_j)$ 下对消息 m 的签名 $\sigma=(C_1,C_2,C_3)$ 时，可通过下列等式来验证签名的有效性：

当 $e(C_3,g)=e(g_1,g_2)e(C_2,(h_1^{ID_1}\cdots h_j^{ID_j}g_3))e(C_1,g)^m$ 成立时，σ 是一个有效的签名。

3.2 方案正确性

方案的正确性很容易由下面的等式得到验证：

对 σ 进行验证可得：

$$e(C_3,g)=e(g,g_2^{\alpha}(h_1^{ID_1}\cdots h_j^{ID_j}g_3)^r\cdot g^{tm})$$
$$=e(g_1,g_2)e(C_2,(h_1^{ID_1}\cdots h_j^{ID_j}g_3))e(C_1,g)^m$$

3.3 方案安全性

下面证明方案在选择身份和选择消息攻击下的存在不可伪造性。

定理 1 在 l-DHI* 困难问题的假设下，我们的方案在选择身份和选择消息攻击下是存在不可伪造的。

证明：假设伪造者 $\mathcal{A}$ 能以不可忽略的优势攻击上面的方案，则能够构造算法 B，B 可以利用 $\mathcal{A}$ 解决 l-DHI* 问题。

给定 B 一个 l-DHI* 问题的实例 $(g, g^{\alpha}, \cdots, g^{\alpha^l})$，为了利用 $\mathcal{A}$ 解决该 l-DHI* 问题，从而计算出 $g^{\alpha^{l+1}}$，B 模仿 $\mathcal{A}$ 的挑战者，具体过程如下：

初始化：敌手 $\mathcal{A}$ 将挑战身份 $ID^* = (ID_1^*, ID_2^*, \cdots, ID_l^*)$ 发送给 B。

系统建立：为了构造上面方案中的公开参数，算法 B 首先选择 $\gamma \in_R Z_p$，设 $g_1 = g^{\alpha}$，$g_2 = g^{\alpha^l} \cdot g^{\gamma} = g^{\gamma + \alpha^l}$。其次，算法 B 选择 $\gamma_1, \cdots, \gamma_l \in_R Z_p$，并令 $h_i = g^{\gamma_i} / g^{\alpha^{l-i+1}}$，$1 \leqslant i \leqslant l$。最后，算法 B 选择 $\delta \in_R Z_p$，并令 $g_3 = g^{\delta} \cdot \prod_{i=1}^{l} g^{\alpha^{l-i+1} ID_i^*}$。可以看出，这些参数的分布与一个真正的挑战者产生公开参数的分布是一样的。算法 B 将公开参数 $params = (g, g_1, g_2, g_3, h_1, \cdots, h_l)$ 发送给敌手 $\mathcal{A}$，相应的主密钥为 $g_2^{\alpha} = g^{\alpha(\gamma + \alpha^l)}$。

询问：当敌手 $\mathcal{A}$ 发起如下询问时，算法 B 进行如下响应：

①私钥询问：当敌手 $\mathcal{A}$ 询问身份 $ID_{|u} = (ID_1, ID_2, \cdots, ID_u)$ 的私钥时，如果 $ID_{|u} = ID^*$ 或者 $ID_{|u}$ 是 ID^* 的前缀，那么算法 B 将失败退出。否则，存在 $k \leqslant u$，满足 $ID_k \neq ID_k^*$，这里假定 k 是满足条件的最小序号。为了响应敌手 $\mathcal{A}$ 的询问，算法 B 可以首先产生身份 $ID_{|k} = (ID_1, ID_2, \cdots, ID_k)$ 的私钥 $d_{ID|k}$，然后利用 $d_{ID|k}$ 构造私钥 $d_{ID|u}$。为了产生私钥 $d_{ID|k}$，B 任选 $\tilde{r} \in Z_p$，并令 $r = \frac{\alpha^k}{(ID_k - ID_k^*)} + \tilde{r}$，构造其私钥：

$$d_{ID|k} = (g_2^{\alpha} (h_1^{ID_1} \cdots h_k^{ID_k} g_3)^r, g^r, h_{k+1}^r, \cdots, h_{l-1}^r)$$，其中

$$a_0 = g^{\alpha(\gamma + \alpha^l)} (g^{\delta + \sum_{i=1}^{k} \gamma_i ID_i} \cdot \prod_{i=1}^{k-1} g^{\alpha^{l-i+1}(ID_i^* - ID_i)} \cdot g^{\alpha^{l-k+1}(ID_k^* - ID_k)} \cdot \prod_{i=k+1}^{l} g^{\alpha^{l-i+1} ID_i^*})^r$$

$$= g_1^{\gamma} \cdot Z \cdot g^{\tilde{r} \alpha^{l-k+1}(ID_k^* - ID_k)}$$

这里

$$Z = (g^{\delta + \sum_{i=1}^{k} \gamma_i ID_i} \cdot \prod_{i=1}^{k-1} g^{\alpha^{l-i+1}(ID_i^* - ID_i)} \cdot \prod_{i=k+1}^{l} g^{\alpha^{l-i+1} ID_i^*})^r$$

$$a_1 = g^r = (g^{\alpha^k})^{1/(ID_k - ID_k^*)} \cdot g^{\tilde{r}}$$

$$h_j^r = g^{(\gamma_j - \alpha^{l-j+1})(\frac{\alpha^k}{(ID_k - ID_k^*)} + \tilde{r})}, \quad k+1 \leqslant j \leqslant l$$

对于敌手 $\mathcal{A}$ 而言，算法 B 生成的私钥与真实挑战者生成的私钥是一致的。因此，算法 B 可以利用私钥 $d_{ID|u}$ 进一步产生身份 $ID_{|u} = (ID_1, ID_2, \cdots, ID_u)$ 的私钥 $d_{ID|u}$。

②签名询问：当敌手 $\mathcal{A}$ 对身份 $ID_{|u}$ 发起签名询问时，如果 $ID_{|u} = ID^*$ 或者 $ID_{|u}$ 是 ID^* 的前缀，那么算法 B 将失败退出；否则，算法 B 可以如同在私钥询问中那样，首先产生其私钥 $d_{ID|u}$，然后按照方案中的签名算法产生相应的签名。

伪造：敌手 $\mathcal{A}$ 输出在身份 $ID_{|u} = (ID_1, ID_2, \cdots, ID_u)$ $(u = l)$ 和消息 m^* 下的伪造分级签名 $\sigma^* = (C_1^*, C_2^*, C_3^*)$，这里要求身份 $ID_{|u}$ 以及身份的前缀没有出现在前面的私钥询问和签名询问中。如果在整个过程中算法 B 没有失败退出，则有：

$$C_1^* = g^t, C_2^* = g^r, C_3^* = a_0 \cdot (g^m)^t$$

其中，$m = H_2(ID_{|u}, m^*)$。

因此可得，$a_0 = C_3^* / (C_1^*)^m$。令 $\hat{r} \in Z_p$，并假设 $a_1 = g^{\hat{r}}$，由

$$a_0 = g_2^{\alpha} (g_3 \prod_{i=1}^{u} h_i^{ID_i^*})^{\hat{r}}$$

$$= g_2^{\alpha} (g^{\delta} \prod_{i=1}^{l} g^{\alpha^{l-i+1} ID_i^*} \prod_{i=1}^{u} (g^{\gamma_i} / g^{\alpha^{l-i+1}})^{ID_i^*})^{\hat{r}}$$

$$= g_2^{\alpha} (g^{\delta} \prod_{i=1}^{u} g^{\gamma_i ID_i^*})^{\hat{r}} = g_2^{\alpha} (g^{\delta + \sum_{i=1}^{u} \gamma_i ID_i^*})^{\hat{r}}$$

可得：

$$g^{\alpha^{l+1}} = g_2^{\alpha} / g^{\alpha\gamma} = a_0 / (a_1^{\delta + \sum_{i=1}^{u} \gamma_i ID_i^*} g_1^{\gamma}) = g^{\alpha^{l+1}}$$

这就是 l-DHI* 问题的解。

因此，一个敌手 $\mathcal{A}$ 如果可以不可忽略的概率伪造一个上述方案中的签名，那么就能够构造一个算法 B 以不可忽略的概率解决 l-DHI* 问题，而这与 l-DHI* 问题是一个困难问题相矛盾，故方案满足选择消息和选择身份攻击下的存在不可伪造性。

结束语 分级签名是一种重要的签名形式，本文在标准模型下设计了一个签名长度为常量的分级的基于身份签名方案。对方案的安全性进行了分析和证明，结果表明，方案在 l-DHI* 困难问题的假设下满足选择消息和选择身份攻击下的存在不可伪造性，因此，本文所提出的方案是安全的。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proceedings of CRYPTO 1984, volume 196 of LNCS. 1984:47-53

[2] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]// Proceedings of CRYPTO 2001, volume 2139 of LNCS. 2001:213-229

[3] Waters B. Efficient identity-based encryption without random oracles[C]// Advances in Cryptology-EUROCRYPT 2005, volume 3494 of LNCS. Springer-Verlag, 2005, 114-127

[4] Gentry C. Practical identity-based encryption without random oracles[C]// Advances in Cryptology-EUROCRYPT 2006, volume 4404 of LNCS. Springer-Verlag, 2006:445-464

[5] Hess F. Efficient identity based signature schemes based on pairings[C]// Proceedings of SAC 2002, volume 2595 of LNCS. Springer-Verlag, 2002:310-324

[6] Paterson K G, Schuldt J C N. Efficient identity-based signatures secure in the standard model[C]// Proceedings of ACISP 2006, volume 4058 of LNCS. Springer-Verlag, 2006:207-222

[7] Horwitz J, Lynn B. Toward hierarchical identity-based encryption[C]// Proceedings of EUROCRYPT 2002, volume 2332 of LNCS. Springer-Verlag, 2002:466-481

[8] Gentry C, Silverberg A. Hierarchical id-based cryptography[C]// Proceedings of ASIACRYPT 2002, volume 2501 of LNCS. Springer-Verlag, 2002:548-566

[9] Boneh D, Canetti R, Halevi S, et al. Chosen-ciphertext security from identity-based encryption[J]. SIAM Journal on Computing, 2006, 36(5):915-942

[10] Boneh D, Boyen X, Goh E. Hierarchical identity based encryption with constant size ciphertext[C]// Proceedings of EUROCRYPT 2005, volume 3494 of LNCS. Springer-Verlag, 2005:440-456

[11] Waters B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions[C]// Advances in Cryptology-CRYPTO 2009, volume 5677 of LNCS. Springer-Verlag, 2009:619-636

(下转第 110 页)

valued Decision Diagram-based Approach for Multistage System Sencitivity Analysis[J]. IEEE Transactions on Reliability, 2010, 59(3): 581-592

[9] 孙艳蕊，张祥德. 利用极小割计算随机流网络可靠度的一种算法[J]. 系统工程学报，2010，25(2)：284-288

[10] 李振，孙新利，姬国勋. 计算多状态网络可靠度的不交化改进算法[J]. 通信学报，2011，21(9A)：166-172

[11] 王芳，侯朝祯. 用蒙特卡罗和 Petri 网方法估计随机流网络的可靠性[J]. 北京理工大学学报，2004，24(7)：604-608

[12] Liu W, Liu Y, Gu X Q, et al. Monte-carlo Simulation for the Reliability Analysis of Multi-status Network System based on Breadth First Search[C]// 2009 Second International Conference on Information and Computing Science. 2009: 280-283

[13] 刘玲艳，吴晓平，田树新. 基于粗糙集和 Petri 网的随机流网络可靠性评价方法[J]. 控制与决策，2010，25(8)：1273-1276

[14] Hudson J C, Kapur K C. Reliability Bounds for Multistate System with Multistate Components[J]. Operation Research, 1985, 33(1): 153-160

[15] Satitsatain S, Kapur K C. An Algorithm for Multistate Network Reliability Bounds and Its Application[C]// ICQR2005. 2005: 409-417

[16] Satitsation S, Kapur K C. An Algorithm for Lower Reliability Bounds of Multistate Two-terminal Networks[J]. IEEE Transactions on Reliability, 2006, 55(2): 199-206

[17] Prekopa A, Vizvari B, Regos G, et al. Bounding the Probability of the Union of Events by the Use of Aggregation and Disaggregation in Linear Programs[R]. Rutcor Research Report, RRR-4-2001, 2001

[18] Meng F C. A Note on Two Reliability Lower Bounds for Multistate Systems[J]. Probability in the Engineering and Informational Sciences, 2002, 16(4): 485-498

[19] Claudio C, Rocco S, Marco M. Approximate Multi-State Reliability Expressions Using A New Machine Learning Technique [J]. Reliability Engineering and System Safety, 2005, 89(3): 261-270

[20] Ramirez-Marquez J E, Coit D W, et al. Bounds for Multistate Network Two-terminal Reliability[R]. Rutgers University IE Working Paper, 03-121, 2003

[21] Ramirez-Marquez J E. Innovative Approaches in Multistate Network Reliability Modeling and Computation[D]. New Brunswick: The State University of New Jersey, 2004

[22] Jane C C, Laih Y W. A Dynamic Bounding Algorithm for Approximating Multi-State Two-terminal Reliability[J]. European Journal of Operational Research, 2010, 205(3): 625-637

[23] Chiou S N, Li O K. Reliability Analysis of A Communication Network with Multimode Components[J]. IEEE Journal on Selected Areas in Communications, 1986, 4(7): 1156-1161

[24] Yang C L, Kubat P. Efficient Computation of Most Probable States for Communication Networks with Multimode Components[J]. IEEE Transactions on Communications, 1989, 37(5): 535-538

[25] Gaebler R F, Chen R J. An Efficient Algorithm for Enumerating States of a System with Multimode Unreliable Components[R]. U. S. Sprint Communications, Overland Park, Kansas, Technical Report, 1987

[26] Shier D R, Bibelnieks E, Jarvis J P, et al. Algorithms for Approximating the Performance of Multimode Systems[C]// IEEE INFOCOM 90. 1990: 741-748

[27] Shier D R. Network Reliability and Algebraic Structures[M]. Oxford: Clarendon Press, 1991

[28] 宋月. 若干复杂系统的可靠性分析[D]. 西安：西安电子科技大学，2006

[29] 王冰山，宋月，王玉梅. 两端多状态网络可靠度的研究[J]. 计算机应用研究，2011，28(5)：1863-1865

(上接第 66 页)

[8] Joseph J F C, Lee B S, Das A. Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA [J]. IEEE Transactions on Dependable and Secure Computing, 2011, 8(2): 233-245

[9] Thamilarasu G, Sridhar R. Game Theoretic Modeling of Jamming Attacks in Ad hoc Networks[C]// Proceedings of 18th Internatonal Conference on Computer Communications and Networks. 2009: 1-6

[10] Yu S Z, Kobayashi H. An Efficient Forward-Backward Algorithm for an Explicit Duration Hidden Markov Model[J]. IEEE Signal Processing Letters, 2003, 10(1): 11-14

[11] Rabiner L R. A tutorial on hidden markov models and selected applications in speech recognition[J]. Proc. of the IEEE, 1989, 77(2): 257-286

[12] Smith L I. A Tutorial on Principal Components Analysis [EB/OL]. http://www.snl.salk.edu/~shlens/pub/notes/pca.pdf, 2003

[13] Yu S Z, Kobayashi H. A Hidden Semi-Markov Model with Missing Data and Multiple Observation Sequences for Mobility Tracking[J]. Signal Processing, 2003, 83(2): 235-250

(上接第 69 页)

[12] Chow S S M, Hui L C K, Siu Ming Yiu, et al. Secure hierarchical identity based signature and its application[C]// Proceedings of ICICS 2004, volume 3269 of LNCS. Springer-Verlag, 2004: 480-494

[13] Au M H, Liu J K, Yuen T H, et al. Efficient hierarchical identity based signature in the standard model[EB/OL]. http://eprint.iacr.org/2007/068

[14] Zhang Le-you, Hu Yu-pu, Wu Qing. New construction of short hierarchical id-based signature in the standard model[J]. Fundamenta Informaticae, 2009, 90(1): 191-201

[15] 李进，张方国，王燕鸣. 两个高效的基于分级身份的签名方案[J]. 电子学报，2007，35(1)：150-152

[16] Ruckert M. Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles [C]// Proceedings of the 3rd international workshop on PQCrypto 2010, volume 6061 of LNCS. Springer-Verlag, 2010: 182-200

[17] 吴青，张乐友，胡予濮. 标准模型下一种新的基于分级身份的短签名方案[J]. 计算机研究与发展，2011，48(8)：1357-1362