一个强安全的无证书密钥协商协议的安全性分析与改进

刘 唐[1,2] 汪小芬[3] 肖国镇[4]

(四川师范大学基础教学学院 成都 610068)[1] (四川大学计算机学院 成都 610065)[2]

(电子科技大学计算机科学与工程学院 成都 610054)[3]

(西安电子科技大学ISN国家重点实验室 西安 710071)[4]

摘 要 Yang和Tan提出一个不需要双线性对的无证书密钥协商协议,并声称该协议满足前向安全性,即双方参与者的私钥和临时秘密信息不全部泄露,敌手就无法获得双方参与者协商的会话密钥。给出一种攻击方法:敌手只要得到一个参与者的私钥和另一个参与者的临时秘密信息,就可以获得双方已经协商的会话密钥。针对此缺陷,对协议做了改进,在改进协议中,双方参与者的私钥和临时秘密信息互相交织在一起,因而能抵抗上述攻击。

关键词 无证书的公钥密码系统,前向安全性,会话密钥

中图法分类号 TP918.1 **文献标识码** A

Security Analysis and Improvement of a Strongly Secure Certificateless Key Agreement Protocol

LIU Tang[1,2] WANG Xiao-fen[3] XIAO Guo-zhen[4]

(College of Fundamental Education, Sichuan Normal University, Chengdu 610068, China)[1]

(College of Computer Science, Sichuan University, Chengdu 610065, China)[2]

(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China)[3]

(National Key Lab of Integrated Service Networks, Xidian University, Xi'an 710071, China)[4]

Abstract Yang and Tan proposed a certificateless key agreement protocol without pairing, and claimed their scheme satisfies forward secrecy, which means no adversary could derive an established session key unless the full user secret information(including a private key and an ephemeral secret key) of both communication parties are compromised. However, we pointed out their protocol is actually not secure as claimed by presenting an attack launched by an adversary who has learned the private key of one party and the ephemeral secret key of the other, but not the full user secret keys of both parties. Furthermore, to make up this flaw, we also provided an revised protocol in which the private key and the ephemeral secret key are closely intertwined with each other for generating the session key, thus above attack can be efficiently resisted.

Keywords Certificateless public key cryptosystem, Forward secrecy, Session key

1 引言

在传统的公钥密码体制PKC中,证书的产生、发布、撤消、存储和验证等带来很大的系统开销,给很多密码系统的性能带来瓶颈。为了解决这个问题,在1984年Shamir提出基于身份的密码体制(ID-PKC)[1]。在ID-PKC中,选取与用户身份相关的信息作为公钥,可信的私钥生成中心(PKG)利用其主密钥和用户的公钥产生对应的私钥。因此ID-PKC会带来密钥分发的问题。为消除传统公钥密码体制和基于身份的公钥密码体制的缺陷,在2003年Al-Riyami和Paterson提出了无证书公钥密码体制(CL-PKC)[2]。在CL-PKC中,用户的私钥是由密钥生成中心产生的部分私钥和用户自己的秘密值合并而成的,因此CL-PKC具有传统公钥密码体制和基于身份的公钥密码体制两者的优势。

密钥协商是两方或多方在不安全的信道中通过协商建立一个安全的会话密钥的过程。对于无证书的公钥加密和签名已经做了比较深入的研究[3-11],而无证书的密钥协商研究还较少。Al-Riyam和Paterson[2]提出了第一个无证书的密钥协商协议,然而该协议没有在安全模型中得到形式化证明。此后提出的无证书密钥协商协议[12-14]只是做了启发式的安全性分析。2008年,Swanson对他提出的无证书密钥协商协议[15]做了形式化的安全性证明。然而这些无证书密钥协商协议都是基于双线性对的,与指数运算相比较,其对的运算开销大,因此影响了无证书密钥协商的效率。于是Geng和Hou分别提出了不基于双线性对的无证书密钥协商协议[16,17],可惜这些协议都不安全[18]。最近Yang和Tan提出

到稿日期:2012-02-23 返修日期:2012-07-16 本文受国家自然科学基金项目(61003310,60970120),四川省教育厅科研项目(10ZB005),四川省科技创新苗子工程项目(2011-025,2011-005)资助。

刘 唐(1980—),男,博士生,讲师,CCF会员,主要研究方向为无线传感器网络、网络安全,E-mail:crikey@163.com;汪小芬(1982—),女,博士,讲师,主要研究方向为信息与网络安全;肖国镇(1939—),男,教授,博士生导师,主要研究方向为密码学。

了一个不基于对的无证书密钥协商协议[19]，并声称该协议在安全模型下是强安全的。

本文将对 Yang 和 Tan 的协议给出一种攻击：只要得到一个参与者的私钥和另一个参与者的临时秘密，就能得到两方协商的会话密钥。因此 Yang 和 Tan 的协议并不满足前向安全性。针对此缺陷，本文对协议做了改进，在改进的协议中，双方参与者的私钥和临时秘密信息互相交织在一起，因而能抵抗上述攻击。

2 无证书密钥协商协议及安全模型

2.1 无证书密钥协商

一个无证书的公钥系统的密钥由下列 5 个概率多项式算法生成：

$Setup(1^k)$：算法输入安全参数 k，返回系统主密钥 msk 和系统公钥 mpk。

$ExtractIDBasedKey(msk; ID)$：算法输入系统主密钥 msk 和用户的身份信息 ID，返回用户的部分私钥 D_{ID}。

$SetSecretValue(mpk; ID)$：算法输入系统公钥 mpk 和用户的身份信息 ID，返回用户的秘密值 S_{ID}。

$SetPublicKey(mpk; D_{ID}; S_{ID})$：算法输入系统公钥 mpk、用户的部分私钥 D_{ID} 和秘密值 S_{ID}，返回用户的公钥 pk_{ID}。

$SetPrivateKey(mpk; D_{ID}; S_{ID})$：算法输入系统公钥 mpk、用户的部分私钥 D_{ID} 和秘密值 S_{ID}，返回用户的私钥 sk_{ID}。

2.2 敌手模型

通过定义无证书密钥协商协议的敌手 $\mathcal{A}$ 与游戏模拟者 $\mathcal{S}$ 之间的游戏来定义敌手模型。首先 $\mathcal{S}$ 运行 $setup$ 算法产生 $(mpk; msk)$，并将 mpk 返回给 $\mathcal{A}$，然后敌手 $\mathcal{A}$ 可以在游戏中传递、插入、删除、修改信息。$\mathcal{A}$ 还可以做如下的预言机询问：

$CreateUser(ID)$：在这个询问中，$\mathcal{A}$ 建立身份信息为 ID 的用户，收到此询问后，$\mathcal{S}$ 产生 D_{ID}、S_{ID}、pk_{ID} 和 sk_{ID}，并返回 pk_{ID} 给 $\mathcal{A}$。

$Send(U; i; m)$：在这个询问中，$\mathcal{A}$ 输入消息 m 到会话实例 Π_U^i 中，Π_U^i 执行协议并返回 $Mout$ 给 $\mathcal{A}$。

$RevealMasterKey(U)$：此询问允许 $\mathcal{A}$ 得到 msk。

$RevealIDBasedKey(U)$：此询问允许 $\mathcal{A}$ 得到 D_U。

$RevealSecretValue(U)$：此询问允许 $\mathcal{A}$ 得到 S_U。

$RevealSecretKey(U)$：此询问允许 $\mathcal{A}$ 得到 sk_U。

$RevealEphemeralKey(U; i)$：此询问允许 $\mathcal{A}$ 得到 Π_U^i 产生的临时秘密值。

$RevealSessionKey(U; i)$：此询问允许 $\mathcal{A}$ 在 Π_U^i 接受(accept)时得到会话密钥 $sskey_U^i$；否则返回 $\perp$。

$ReplacePublicKey(U; (pk_U)')$：此询问允许 $\mathcal{A}$ 将 U 的公钥替换成 $pk_U=(pk_U)'$。此询问之后，$\mathcal{S}$ 将使用 U 的新公私钥对。

$Test(U^*; i^*)$：此询问允许 $\mathcal{A}$ 选择挑战已经接受(accept)的会话实例 Π_U^i。收到此询问后，$\mathcal{S}$ 通过投掷硬币得到 b 的值，如果 $b=1$，则 $\mathcal{S}$ 返回 $sskey_{U^*}^{i^*}$ 给 $\mathcal{A}$，否则在密钥空间选取一个随机会话密钥返回给 $\mathcal{A}$。在游戏中 $\mathcal{A}$ 只能做一次该询问，$\Pi_{U^*}^{i^*}$ 必须接受会话，并且接受的会话是新鲜的(定义如下)。

游戏结束后，$\mathcal{A}$ 输出 b' 作为猜测的 b 的结果。敌手 $\mathcal{A}$ 赢得游戏的概率定义为 $Adv_{\mathcal{A}}^{ake}=2\Pr[b'=b]-1$。

会话实例 Π_U^i 使用长期密钥对 $((ID_U; pk_U); sk_U)$ 和短期密钥对 $(epk_U; esk_U)$，一旦 sk_U 和 esk_U 全部暴露，敌手就可以很容易计算出会话密钥 $sskey_i$。会话实例 Π_U^i 是安全的，如果下列任一条件都不成立：

(1)敌手做过 $RevealSessionKey(U; i)$ 询问。

(2)敌手同时做了 $RevealSecretKey(U)$ 和 $RevealEphemeralKey(U; i)$ 询问。

(3)敌手做了 $RevealMasterKey$ 或 $RevealIDBasedKey(U)$ 询问，并且同时做了 $RevealSecretValue(U)$ 询问和 $RevealEphemeralKey(U; i)$ 询问。

(4)Π_U^i 利用与原先的密钥对不同的公私钥对，敌手做了 $RevealMasterKey$ 或 $RevealIDBasedKey(U)$ 查询，并且做了 $RevealEphemeralKey(U; i)$ 查询。

定义 1(会话的新鲜性) 会话实例 Π_U^i 满足 $acc_U^i=\text{true}$ 和 $pid_U^i=V$。如果下列任一条件成立，则 Π_U^i 不是新鲜的：

(1)Π_U^i 被暴露。

(2)Π_U^i 的一个搭档会话实例是 Π_V^j，Π_V^j 被暴露。

(3) 如果 Π_U^i 没有搭档会话，下列情况至少有任一个发生：

(a) 敌手做了 $RevealMasterKey$ 或 $RevealIDBasedKey(V)$ 询问，并做了 $RevealSecretValue(V)$ 询问；

(b) 敌手做了 $RevealSecretKey(V)$ 询问；

(c) 敌手做了 $RevealMasterKey$ 或 $RevealIDBasedKey(V)$ 询问，并且做了 $ReplacePublicKey(U; (pk_U)')$ 询问。

定义 2 一个 CL-KE 是安全的如果：

(1) 只有存在良性的敌手(敌手只传达消息)时，两个搭档的会话实例才输出相同的会话密钥；

(2) 对任一多项式时间的敌手，赢得游戏的优势 $Adv_{\mathcal{A}}^{ake}(k)$ 是可忽略的。

3 Yang 和 Tan 的无证书密钥协商协议

令 $DS=\{KG; Sig; Ver\}$ 为一个能抵抗适应性选择消息攻击的数字签名方案[20]。Yang 和 Tan 的不基于双线性对的无证书密钥协商协议[19]由 6 个子算法构成：

1. $Setup(1^k)$：PKG 选择一个阶为 q 的循环群 G，选择一个随机数 $x\in Z_q$，选择 $g\in G\backslash\{1\}$，并计算 $y=g^x$。然后，PKG 运行密钥生成算法产生签名方案 DS 的签名/验证密钥对 $(sk; vk)$。最后，PKG 设置 $msk=(x; sk)$；$mpk=(y; vk)$。

2. $ExtractIDBasedKey(msk; ID)$：给定身份信息 ID，PKG 选择随机数 $a\in Z_q$，计算 $R_{ID}=g^a$，$z_{ID}=a+H_1(ID\|R_{ID})x \bmod q$，产生签名 $\delta_{ID}=Sig(sk; ID\|R_{ID})$，然后设置 $D_{ID}=(R_{ID}; \delta_{ID}; z_{ID})$。

3. $SetSecretValue(mpk; ID)$：身份信息为 ID 的用户随机选择 $t\in Z_q$，设置 $S_{ID}=t$。

4. $SetPublicKey(mpk; D_{ID}; S_{ID})$：给定用户的私钥 S_{ID} 和基于身份的密钥 D_{ID}，用户计算 $U_{ID}=g^{S_{ID}}$，设置公钥为 $pk_{ID}=(U_{ID}; R_{ID}; \delta_{ID})$。

5. $SetPrivateKey(mpk; D_{ID}; S_{ID})$：给定用户的公钥 mpk、秘密值 S_{ID} 和基于身份的密钥 D_{ID}，设置私钥 $sk_{ID}=(D_{ID}; S_{ID})$。

6. 密钥协商：参与者 A 随机选取 $e_A\in Z_q$，B 随机选取 $e_B\in Z_q$，然后交换以下信息：

$A \rightarrow B: ID_A; pk_A; E_A = g^{e_A}$；

$B \rightarrow A: ID_B; pk_B; E_B = g^{e_B}$。

A 按照下列方法计算：

$Z_1 = E_B^{e_A}, Z_2 = U_B^{S_A}, Z_3 = (R_B mpk^{H_1(ID_B \| R_B)})^{z_A}$；

$Z_4 = U_B^{e_A}, Z_5 = E_B^{S_A}, Z_6 = (E_B R_B mpk^{H_1(ID_B \| R_B)})^{e_A + z_A}$；

$Z_7 = (U_B R_B mpk^{H_1(ID_B \| R_B)})^{S_A + z_A}$；

然后得到会话密钥为：

$ssk = H_2(sid \| Z_1 \| Z_2 \| Z_3 \| Z_4 \| Z_5 \| Z_6 \| Z_7)$

式中，$sid = ID_A \| ID_B \| pk_A \| E_A \| pk_B \| E_B$。

B 按照下列方法计算：

$Z_1 = E_A^{e_B}, Z_2 = U_A^{S_B}, Z_3 = (R_A mpk^{H_1(ID_A \| R_A)})^{z_B}$；

$Z_4 = U_A^{e_B}, Z_5 = E_A^{S_B}, Z_6 = (E_A R_A mpk^{H_1(ID_A \| R_A)})^{e_B + z_B}$；

$Z_7 = (U_A R_A mpk^{H_1(ID_A \| R_A)})^{S_B + z_B}$；

然后得到会话密钥为：

$ssk = H_2(sid \| Z_1 \| Z_2 \| Z_3 \| Z_4 \| Z_5 \| Z_6 \| Z_7)$

式中，$sid = ID_A \| ID_B \| pk_A \| E_A \| pk_B \| E_B$。

4 Yang 和 Tan 协议的攻击与改进

Yang 和 Tan[19] 声称他们的协议在随机预言机模型下是可证明安全的，并且满足前向安全性。也就是敌手在不完全掌握 $(D_A; S_A; esk_A)$ 和 $(D_B; S_B; esk_B)$ 的情况下，不能得到会话密钥。然而，将给出一个有效的攻击，即敌手不完全掌握协议参与两方的长期私钥和短期秘密值，也能得到会话密钥。

4.1 攻击

在 PKG 不可信的情况下，敌手通过 *RevealExtractIDBasedKey* 询问得到 z_A 和 z_B，通过 *RevealSecretValue*(B) 询问得到 S_B，通过 *RevealEphemeralKey*$(A; i)$ 询问得到 e_A，而且保证敌手不能得到 S_A 和 e_B，这满足 Yang 和 Tan 的安全模型。敌手可以按照下列步骤得到会话密钥。

首先，因为敌手得到 e_A，可计算：

$Z_1 = E_B^{e_A}, Z_3 = (R_B mpk^{H_1(ID_B \| R_B)})^{z_A}, Z_4 = U_B^{e_A}$

$Z_6 = (E_B R_B mpk^{H_1(ID_B \| R_B)})^{e_A + z_A}$

其次，因为敌手得到 S_B，可计算：

$Z_2 = U_A^{S_B}, Z_5 = E_A^{S_B}, Z_7 = (U_A R_A mpk^{H_1(ID_A \| R_A)})^{S_B + z_B}$

于是，敌手很容易计算出会话密钥

$ssk = H_2(sid \| Z_1 \| Z_2 \| Z_3 \| Z_4 \| Z_5 \| Z_6 \| Z_7)$

式中，$sid = ID_A \| ID_B \| pk_A \| E_A \| pk_B \| E_B$。

由此可见，敌手可以成功得计算出 A 和 B 协商的会话密钥。

4.2 改进方案

从上述的安全性分析来看，Yang-Tan 的协议不安全是因为在计算会话密钥时，短期密钥 e_A, e_B 与长期的密钥 S_A, S_B 互相独立，而没有充分交织引起的。下面对 Yang-Tan 的协议做了改进，使得协议能抵抗上述攻击。改进的协议中 *Setup*，*ExtractIDBasedKey*，*SetSecretValue*，*SetPublicKey* 和 *SetPrivateKey* 与第 3 节相同，只对密钥协商部分做了修改，具体如下：

参与者 A 随机选取 $e_A \in Z_q$，B 随机选取 $e_B \in Z_q$，然后交换以下信息：

$A \rightarrow B: ID_A; pk_A; E_A = g^{e_A}$；

$B \rightarrow A: ID_B; pk_B; E_B = g^{e_B}$。

A 按照下列方法计算：

$Z_1 = (R_B mpk^{H_1(ID_B \| R_B)})^{z_A}$；

$Z_2 = (E_B U_B R_B mpk^{H_1(ID_B \| R_B)})^{e_A + S_A + Z_A}$；

$Z_3 = (U_B E_B)^{S_A + e_A}$；

然后得到会话密钥为 $ssk = H_2(sid \| Z_1 \| Z_2 \| Z_3)$；

式中，$sid = ID_A \| ID_B \| pk_A \| E_A \| pk_B \| E_B$。

B 按照下列方法计算：

$Z_1 = (R_A mpk^{H_1(ID_A \| R_A)})^{z_B}$；

$Z_2 = (E_A U_A R_A mpk^{H_1(ID_A \| R_A)})^{S_B + Z_B + e_B}$；

$Z_3 = (U_A E_A)^{S_B + e_B}$；

然后得到会话密钥为 $ssk = H_2(sid \| Z_1 \| Z_2 \| Z_3)$；

式中，$sid = ID_A \| ID_B \| pk_A \| E_A \| pk_B \| E_B$。

5 安全性与效率分析

这部分分析改进协议的安全性。我们的协议是基于 Yang-Tan 协议的改进，因此改进协议满足 Yang-Tan 协议已有的安全性。通过分析得到改进协议能抵抗一些攻击，包括公钥替换攻击、密钥泄露伪装攻击等。

1）已知密钥安全性

即使某会话密钥已经泄露，也不会影响此前和此后协商的会话密钥的安全性，因为参与会话密钥计算的短期密钥在每次协商时都是随机选取的新的秘密值。

2）完善前向安全性

即使长期私钥泄露，敌手没有同时获得 A 和 B 的短期密钥，他仍然无法计算 Z_2 和 Z_3，因此改进协议满足完善前向安全性。

3）PKG 前向安全性

无证书公钥的优势是即使 PKG 的主密钥泄露了，因为敌手无法获得计算会话密钥的短期私钥和完整的私钥，敌手（包括 PKG）仍无法获得会话双方之前协商的会话密钥。

4）抗未知密钥共享攻击的安全性

因为在计算会话密钥时必须加入参与双方的身份标识，所以该协议能抵抗未知密钥共享攻击。

5）抗密钥泄露伪装攻击的安全性

假设 A 的密钥泄露，敌手可以伪装成 A，但敌手不知道 B 的私钥，仍不能计算 Z_2 的值，因此改进协议能抵抗密钥泄露伪装攻击。

下面再分析改进协议能抵抗第 4.1 节的攻击。

假设敌手通过 *RevealExtractIDBasedKey* 询问得到 z_A 和 z_B，通过 *RevealSecretValue*(B) 询问得到 S_B，通过 *RevealEphemeralKey*$(A; i)$ 询问得到 e_A，而且保证敌手不能得到 S_A 和 e_B。在这种情况下，敌手可以计算 Z_1，但无法计算 Z_2 和 Z_3。因此改进协议能抵抗 4.1 节给出的攻击。

改进协议在效率方面也有很大的提高。假设 $mpk^{H_1(ID_B \| R_B)}$ 和 $mpk^{H_1(ID_A \| R_A)}$ 可以预先计算。在 Yang-Tan 的协议中，每个参与者需要做 7 次指数运算，而改进协议只需要做 3 次指数运算，效率提高了一半以上。

结束语 本文通过具体的攻击发现 Yang-Tan 协议在他们给出的安全模型下是不安全的，敌手只要得到一个参与者的私钥和另一个参与者的临时秘密信息，就可以获得双方已经协商的会话密钥。本文对协议做了改进以抵抗这种攻击，并且改进协议效率提高了一半以上，因此更为安全实用。

（下转第 106 页）

参 考 文 献

[1] Feng Zai-wen, He Ke-qing, Ma Yu-tao, et al. Towards individualized requirements specification evolution for networked software based on aspect[C]// Making Globally Distributed Software Development a Success Story. Leipzig, Germany, 2008

[2] Laprie J. Dependable computing and fault tolerance: concepts and terminology[C]// IEEE the 15th International symposium on fault-tolerant computing. Michigan, USA, 1985

[3] Avizienis A, Laprie J C, Randell B, et al. Basic Concept and Taxonomy of Depenable and Secure Computing [J]. Dependable and Secure Computing, 2004, 1(1): 11-33.

[4] Caban D. Dependability of Large Reconfigurable Information Systems [C]// IEEE DepCos-RELCOMEX. Brunow, Poland, 2009

[5] Boon Y O, Huah Y C, Cheah Y N. Dynamic service placement and redundancy to ensure service availability during resource failures [C]// 2010 International Symposium in Information Technology (ITSim). Kuala Lumpur, Malaysia, 2010

[6] Droguett E L, Moura M D C, Jacinto C M, et al. A semi-Markov model with Bayesian belief network based human error probability for availability assessment of downhole optical monitoring systems [J]. Simulation Modelling Practice and Theory, 2008, 16(10): 1713-1727

[7] Kang C W, Golay M W. A Bayesian belief network-based advisory system for operational availability focused diagnosis of complex nuclear power systems [J]. Expert Systems with Applications, 1999, 17(1): 21-32

[8] Marko P, Antti E, Eila O. The Reliability Estimation, Prediction and Measuring of Component-Based Software [J]. The Journal of Systems and Software, 2011, 84(6): 1054-1070

[9] Chao J H, Chin Y H. An Adaptive Reliability Analysis Using Path Testing for Complex Component-Based Software Systems [J]. IEEE Transactions on Reliability, 2011, 60(1): 158-170

[10] Haiyang H. Reliability Analysis for Component-based Software System in Open Distributed Environments [J]. International Journal of Computer Science and Network Security, 2007, 7(5): 193-202

[11] Meng Ling-zhong, Lu Min-yan, Lai Jing, et al. The Multi-Agent Based Reliability Simulation Approach for Networked Software System [J]. International Journal of Advancements in Computing Technology, 2011, 3(10): 197-207

[12] Wooldridge M, Jennings N R. Agent Theories, Architectures, and langeuages: A Survey [C]// Workshop on Agent Theories Architectures and Languages. Montreal, Canada, 1995

[13] Wooldridge M J, Jennings N R. Intelligent Agent: theory and practice [J]. Knowledge Engineering Review, 1995, 10(2): 115-152

(上接第 75 页)

参 考 文 献

[1] Shamir A. Identity based cryptosystems and signature scheme [C]// Crypto 1984, LNCS 196. Springer-Verlag, 1984: 47-53

[2] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[C]// Advance in Cryptology-ASIACRYPT 2003. 2003: 452-473

[3] Baek J, Safavi-Naini R, Susilo W. Certificateless public key encryption without paring[C]// Information Security Conference (ISC). 2005: 134-148

[4] Dent A W, Libert B, Paterson K G. Certificateless encryption schemes[Z]. Strongly cryptography, 2008: 344-359

[5] Huang Xin-yi, Mu Yi, Susilo W, et al. Certificateless signature revisited[C]// ACISP. 2007: 308-322

[6] Liu J K, Au M H, Susilo W. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model: extended abstract[C]// ACM Symposium on Information, Computer and Communications Security (ASIACCS). 2007: 273-283

[7] Huang Qiong, Wong D S. Generic certificateless encryption in the standard model[C]// IWSEC. 2007: 278-291

[8] Huang Qiong, Wong D S. Generic certificateless key encapsulation mechanism[C]// ACISP. 2007: 215-229

[9] Dent A W. A survey of certificateless encryption schemes and security models[J]. Int. J. Inf. Sec., 2008, 7(5): 349-377

[10] Bentahar K, Farshim P, Malone-LEE J, et al. Generic constructions of identity-based and certificateless KEMs[J]. J. Cryptology, 2008, 21(2): 178-199

[11] Fiore D, Gennaro R, Smart N P. Constructing certificateless encryption and id-based encryption from id-based key agreement [C]// Pairing-Based Cryptography. 2010: 167-186

[12] Mandt T K, Tan C H. Certificateless authenticated two-party key agreement protocols[C]// Proc. ASIAN 2006. 2006: 37-44

[13] Shao Zu-hua. Efficient authenticated key agreement protocol using self-certified public keys from pairings[J]. Wuhan University Journal of Natural Sciences, 2005, 10(1): 267-270

[14] Wang Sheng-bao, Cao Zhen-fu, Wang Li-cheng. Efficient certificateless authenticated key agreement protocol from pairings[J]. Wuhan University Journal of Natural Science, 2006, 11(5): 1278-1282

[15] Swanson C M. Security in key agreement: Two-party certificateless scheme[D]. University of Waterloo, 2008

[16] Geng Man-man, Zhang Fu-tai. Provably secure certificateless two-party authenticated key agreement protocol without pairing [C]// International Conference on Computational Intelligence and Security. 2009: 208-212

[17] Hou Meng-bo, Xu Qiu-liang. A two-party certificateless authenticated key agreement protocol without paring[C]// 2nd IEEE International Conference on Computer Science and Information Technology. 2009: 412-416

[18] He De-biao, Chen Yi-tao, Chen Jian-hua, et al. A new two-round certificateless authenticated key agreement protocol without bilinear prirings [J]. Mathematical and Computer Modelling, 2011, 54(11/12): 3143-3152

[19] Yang Guo-min, Tan C-H. Strongly secure certificateless key exchange without pairing[C]// ASIACCS'11. 2011: 22-24

[20] Goldwasser S, Micali S, Rivest R. A digital signature scheme secure against adaptive chosen-message attack[J]. Siam J. Computing, 1988, 17(2): 281-308