无双线性对的无证书两方密钥协商方案 *

刘文浩, 许春香
(电子科技大学 计算机科学与工程学院, 成都 611731)

摘 要: 近几年来,有许多无证书密钥协商方案相继被提出,它们都需要双线性对运算,而且它们中大部分不能抵抗密钥泄露伪装攻击和临时私钥泄露产生的攻击。2009 年,Lippold 等人提出一个可证安全无证书密钥协商协议,但该协议需要较大计算量。为了解决上述问题,给出了一个新的无双线性对运算无证书两方密钥协商方案,并分析了它的安全属性,只要每方至少有一个未泄露的秘密,那么新方案就是安全的。因此,即使密钥生成中心知道双方的临时私钥,新方案也是安全的。与 Lippold 等人的协议相比,新方案降低了计算复杂度。

关键词: 密钥协商; 两方; 无证书密码学; 无双线性对
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2010)11-4287-03
doi:10.3969/j.issn.1001-3695.2010.11.078

Certificateless two-party key agreement scheme without bilinear pairing

LIU Wen-hao, XU Chun-xiang
(*School of Computer Science & Engineering, University of Electronic Science & Technology of China, Chengdu* 611731, *China*)

Abstract: A few of certificateless key agreement schemes have been proposed in recent years, all of them need pairing operations, what's more, most of them are vulnerable to the key compromise impersonation attack and resistance to leakage of ephemeral keys. The provably secure certificateless key agreement protocol was proposed by Lippold in 2009, but their protocol suffered from computation burden. In order to solve the above-mentioned problem, this paper proposed a new pairing-free certificateless two party key agreement scheme (CL-KA) and presened its security properties. The new scheme was secure as long as each party had at least one uncompromised secret. Thus, the new scheme was secure even if the key generation centre learned the ephemeral secrets of both parties. The new scheme achieves efficiency in computational cost when compared with Lippold's protocol.

Key words: key agreement; two party; certificateless cryptography; pairing-free

在传统的基于公钥证书的密码体制下,用户的公钥由证书权威机构颁发证书来认证,公钥证书的管理过程复杂且代价极高。1984 年,Shamir[1] 首次提出了基于身份的密码体制。在基于身份的密码体制中,使用能唯一代表用户身份的公开信息(电话号码或邮箱等)来代表用户的公钥,用户的公钥不再需要证书权威机构颁发证书认证。基于身份的密码体制克服了公钥证书复杂性管理,但由于用户的私钥由可信密钥生成中心(key generation center,KGC)产生,KGC 知道任何用户的私钥,基于身份的密码体制带来了密钥托管新问题。2003 年,Al-Riyami 等人[2] 首次提出了无证书密码学体制,它解决了基于身份密码体制中固有的密钥托管问题,并保持了基于身份密码体制无须使用公钥证书的优点。他们首先提出一种无证书两方认证密钥协商协议,但并没有给出安全模型和安全证明。随后,不同的无证书两方认证密钥协商协议[3~6] 被研究者相继提出,但是,这些协议都不能抵抗密钥泄露伪装攻击和中间人攻击。Gao 等人[7]、Swanson 等人[8,9] 详细分析了对上述方案产生的攻击。基于 LaMacchia 等人[10] 提出的扩展 CK(extended Canetti-Krawczyk,eCK)安全模型(eCK 安全模型介绍详见文献[10]),Swanson 定义了无证书两方认证密钥协商协议的安全模型。基于 Swanson[8] 提出的安全模型,Lippold 等人[11] 提出了无证书两方认证密钥协商协议的一个更强安全模型,并给出了一个可证安全无证书认证协议,但由于该协议使用了 10 次双线性对运算和 5 次指数运算,计算复杂度较高。到目前为止,所有已知的无证书密钥协商方案都采用了双线性对操作,比较指数运算和点乘运算,在有限域中,双线性对运算仍然是比它们更为耗时的运算。按照文献[7],执行一个 512 位 Tate pairing 需要花费 20 ms,而一个 1 024 位素数指数操作却只需要 8.80 ms,运行一次双线性双线性对操作的时间至少是椭圆曲线上点乘运算的 21 倍[12],因此,无双线性对运算的计算复杂度会越低。基于以上情况,在最强的安全模型下,其安全性基于计算 Diffie-Hellman 困难问题,提出了一个新的无须双线性对运算无证书两方密钥协商方案。新方案只需 3 次点乘运算,与 Lippold 等人的协议相比,新方案明显降低了计算复杂度。

1 安全定义

1.1 安全属性

1)已知密钥安全 协议参与者间的共同会话密钥被泄露后,获得该泄露密钥的攻击者无法根据已获得的会话密钥求出过去和未来的会话密钥。

2)抗未知密钥共享 实体 A 若不知道实体 B 的身份,A 不会与 B 共享会话密钥。

收稿日期: 2010-05-29; **修回日期**: 2010-07-12 **基金项目**: 国家"863"计划资助项目(2009AA01Z415)

作者简介: 刘文浩(1974-),男,湖北孝感人,博士,主要研究方向为信息安全、密码学(whl819_819@163.com);许春香(1965-),女,湖南宁乡人,教授,博导,博士,主要研究方向为信息安全、密码学.

3)抗密钥泄露伪装 假如实体 A 与实体 B 是协议的参与者,当 A 的长期私钥泄露后,获得该泄露密钥的攻击者能向 B 冒充 A,反之则不行。

4)前向安全 若协议参与者间的长期私钥被泄露,获得该泄露密钥的攻击者不能求出在这次被泄露之前协商得到的其他会话密钥。

5)密钥生成中心前向安全 在某一时刻,若密钥生成中心的主私钥泄露,获得该泄露密钥的攻击者不能求出在这次协商之前得到的其他会话密钥。

6)无密钥控制 无论谁都不能将实体间协商的会话密钥预先设置其控制的选定值。

7)已知会话临时信息安全 会话时用户的临时私钥被泄露也不会影响最终会话密钥的安全。即使 KGC 了解了某次会话时双方用户的临时私钥,它也不能计算出最终的会话密钥。

1.2 安全类型

在无证书密码学方案中,通信中的每方都有三个秘密值,分别为 KGC 生成用户的部分私钥、用户自己生成的长期私钥、会话时用户随机选择的临时私钥,按这三个秘密值定义了三种安全类型。

定义 1 类型Ⅰ密钥协商安全。如果两用户部分私钥泄露,他们只各自保留其他两个密钥中的一个,在概率多项式时间内攻击者没有不可忽略的优势在游戏中获胜,则称为类型Ⅰ密钥协商安全。

此类型的安全主要是防止 KGC 对用户密钥托管。如果某协议满足这种类型安全,则说明该协议具有无密钥托管,同时 KGC 具有前向安全性。

定义 2 类型Ⅱ密钥协商安全。如果两用户长期私钥泄露,他们只各自保留其他两个密钥中的一个,在概率多项式时间内攻击者没有不可忽略的优势在游戏中获胜,则称为类型Ⅱ密钥协商安全。

如果某协议满足这种类型安全,则说明该协议具有前向安全性。

定义 3 类型Ⅲ密钥协商安全。如果两用户临时私钥泄露,他们只各自保留其他两个密钥中的一个,在概率多项式时间内攻击者没有不可忽略的优势在游戏中获胜,则称为类型Ⅲ密钥协商安全。

此类型的安全主要是防止会话时用户临时私钥泄露产生的攻击。如果某协议满足这种类型安全,则说明该协议满足已知会话临时信息安全的特性。

2 有关困难问题及假设

计算性 Diffie-Hellman 问题(computational Diffie-Hellman problem,CDHP):设 $G=\langle P\rangle$,阶为 q 的一个加法循环群,$a,b\in Z_q^*$,$aP,bP\in G$,计算 abP。

在概率多项式时间内(PPT),算法 A 在解决 CDH 问题的优势定义如下:

$$\mathrm{adv}^{\mathrm{CDH}}(A)=Pr[A(aP,bP)=abP\mid a,b,\in Z_q^*]$$

CDH 假设:对任意 PPT 算法 A, $\mathrm{adv}^{\mathrm{CDH}}(A)$是可以忽略的。

3 新的无证书密钥协商方案

1)系统参数建立

输入安全参数 k,产生两个大素数 p、q,且 $q\mid p-1$。P 为椭圆曲线上循环群 G 中任意一阶为 q 的生成元,选择安全 hash 函数:$H_1:\{0,1\}^*\times G\to Z_q^*$,$H_2:\{0,1\}^*\to Z_q^*$,$H_3:G\to Z_q^*$,$H:\{0,1\}^*\times\{0,1\}^*\times Z_q^*\times G^7\to\{0,1\}^k$。KGC 随机选择主密钥 $x\in Z_q^*$,计算 $y=xP$,系统公开参数(p,q,P,y,H_1,H_2,H_3,H),保密 x。

2)用户密钥生成

给定用户身份 ID_i,KGC 随机选择 $r_i\in Z_q^*$,计算 $R_i=r_iP$,$D_i=r_i+xH_1(\mathrm{ID}_i,R_i)$,通过安全渠道返回 D_i 给用户 i,并作为其部分私钥。$R_i=r_iP$ 作为用户 i 的部分公钥。

用户 ID_i 随机选择 $x_i\in Z_q^*$ 作为其长期私钥,生成对应的私钥(x_i,D_i),计算 $X_i=x_iP$,生成公钥(X_i,R_i)。用户 ID_i 可以通过计算等式 $R_i+H_1(\mathrm{ID}_i,R_i)y=D_iP$ 是否成立来判断 KGC 分配给自己的部分私钥是否有效。

3)身份认证和密钥协商

用户 A 随机选取 $a,N_A\in Z_q^*$ 计算 $T_A=aP$,$h_1=H_1(\mathrm{ID}_B,R_B)$,$h=H_2(T_A\|N_A\|\mathrm{ID}_A)$,$s=a/(x_A+D_A+h)$,生成签名$(h,s)$,计算:$V_A=a(R_B+X_B+h_1y)$,$C=H_3(V_A)\oplus N_A$(完成加密),并发送消息$(\mathrm{ID}_A,h,s,C)$给用户 B。

用户 B 收到消息(ID_A,h,s,C)后,计算 $P_A=R_A+H_1(\mathrm{ID}_A,R_A)y$,$h_2=H_1(\mathrm{ID}_A,R_A)$,$V_B=s(x_B+D_B)(X_A+R_A+h_2y+hP)=(x_b+D_B)aP=a(R_B+X_B+h_1y)=V_A$,恢复消息 $N'_A=C\oplus H_3(V_B)$,$T'_A=s(X_A+R_A+h_2y+hP)=aP=T_A$,若 $H_2(T'_A\|N_A\|\mathrm{ID}_A)=h$ 成立,则用户 B 通过了对用户 A 的身份验证。

用户 B 随机选取 $b\in Z_q^*$,计算 $T_B=bP$,并使用 V_B 作为对称加密密钥计算 $e=E_{V_B}(T_B\|\mathrm{ID}_B)$,发送消息$(e,\mathrm{ID}_B)$给用户 A,并计算:

$$K_{B1}=x_B(X_A+P_A+T_A)=x_B(x_AP+P_A+aP)$$
$$K_{B2}=D_B(X_A+P_A+T_A)=D_B(x_AP+P_A+aP)$$
$$K_{B3}=b(X_A+P_A+T_A)=b(x_AP+P_A+aP)$$

当用户 A 收到消息后,计算 $P_B=R_B+H_1(\mathrm{ID}_B,R_B)y$,利用 V_A 解密 e 得到 T_B,计算:

$$K_{A1}=(x_A+D_A+a)X_B=(x_A+D_A+a)x_BP=K_{B1}=K_1$$
$$K_{A2}=(X_A+D_A+a)P_B=K_{B2}=K_2$$
$$K_{A3}=(x_A+D_A+a)T_B=(x_A+D_A+a)bP=K_{B3}=K_3$$

最终会话密钥为

$$K=H(\mathrm{ID}_A,\mathrm{ID}_B,N_A,X_A,X_B,T_A,T_B,K_1,K_2,K_3)$$

4 安全性分析

按照前面定义的安全类型,可分为三大类,共九小类来讨论其安全性。由于新方案中使用了签密技术,它对伪造攻击增加了一道安全屏障。

1)类型Ⅰ安全中

a)若攻击者知道 D_A、D_B、x_A、x_B,但 a、b 安全,攻击者求不出 abP,也就求不出 K_3。因为在不知道 a、b 的情况下,无法计算出 abP,要计算 abP 就需要解决 CDH 问题在(G,P)上一个的具体实例,在这种情况下,新方案满足前向安全和 KGC 前向安全特性。

b)若攻击者知道 D_A、D_B、a、b,但 x_A、x_B 安全,攻击者求不出 x_Ax_BP,也就求不出 K_1。因为在不知道 x_A、x_B 的情况下,无法计算出 x_Ax_BP 来,要计算 x_Ax_BP 就需要解决 CDH 问题在(G,P)上的一个具体实例,在这种情况下,新方案满足 KGC 前向安全和已知会话临时信息安全特性。

c)若攻击者知道 D_A、D_B、a、x_B,但 b、x_A 安全,攻击者求不出 bx_AP,也就求不出 K_3。因为在不知道 b、x_A 的情况下,无法计算出 bx_AP 来,要计算 bx_AP 就需要解决 CDH 问题在(G,P)上的一个具体实例,在这种情况下,新方案满足 KGC 前向安全特性,抗 KCI 攻击。若攻击者知道 D_A、D_B、x_A、b,但 a、x_B 安全,它求不出 ax_BP,也就求不出 K_1。新方案满足 KGC 前向安全特性,抗 KCI 攻击。

2)类型Ⅱ安全中

a)若攻击者知道 x_A、x_B、D_A、D_B,但 a、b 安全,攻击者求不出 abP。因为在不知道 a,b 的情况下,无法计算出 abP 来,也就求不出 K_3。要计算 abP 就需要解决 CDH 问题在(G,P)上的一个具体实例,在这种情况下,新方案满足前向安全和 KGC 前向安全特性。

b)若攻击者知道 x_A、x_B、a、b,但 D_A、D_B 安全,攻击者求不出 D_AD_BP,也就求不出 K_2。因为在不知道 D_A、D_B 的情况下,无法计算出 D_AD_BP,要计算 D_AD_BP 就需要解决 CDH 问题在(G,P)上的一个具体实例,在这种情况下,新方案满足已知会话临时信息安全和前向安全特性。

c)若攻击者知道 x_A、x_B、a、D_B,但 b、D_A 安全,攻击者求不出 bD_AP,也就求不出 K_3。在不知道 b、D_A 的情况下,无法计算出 bD_AP,要计算 bD_AP 就需要解决 CDH 问题在(G,P)上的一个具体实例,在这种情况下,新方案满足前向安全性。若攻击者知道 x_A、x_B、D_A、b,但 a、D_B 安全,攻击者求不出 aD_BP,也就求不出 K_2。在不知道 a、D_B 的情况下,无法计算出 aD_BP,要计算 aD_BP 就需要解决 CDH 问题在(G,P)上的一个具体实例,在这种情况下,新方案满足前向安全性。

3)类型Ⅲ安全中

a)若攻击者知道 a、b、D_A、D_B,但 x_A、x_B 安全,攻击者求不出 x_Ax_BP,也就求不出 K_1。因为在不知道 x_A、x_B 的情况下,无法计算出 x_Ax_BP 来,也就求不出 K_1。要计算 x_Ax_BP 就需要解决 CDH 问题在(G,P)上的一个具体实例,在这种情况下,新方案满足已知会话临时信息安全和 KGC 前向安全特性。

b)若攻击者知道 a、b、x_A、x_B,但 D_A、D_B 安全,攻击者求不出 D_AD_BP,也就求不出 K_2。因为在不知道 D_A、D_B 的情况下,无法计算出 D_AD_BP 来,要计算 D_AD_BP 就需要解决 CDH 问题在(G,P)上的一个具体实例,在这种情况下,新方案满足已知会话临时信息安全和前向安全特性。

c)若攻击者知道 a、b、x_A、D_B/a、b、D_A、x_B,但 x_B、D_A/x_A、D_B 安全,攻击者求不出 x_BD_AP/x_AD_BP。因为在不知道 x_B、D_A/x_A、D_B 的情况下,无法计算出 x_BD_AP/x_AD_BP 来,也就求不出 K_1/K_2,要计算 x_BD_AP/x_AD_BP 就需要解决 CDH 问题在(G,P)上的一个具体实例,在这种情况下,新方案抗 KCI 攻击,也满足已知会话临时信息安全特性。

由上述安全分析,可以得出如下重要结论:

a)如果两用户的部分私钥泄露而不影响方案的安全,则该方案无用户密钥托管,同时具有 KGC 前向安全特性。

b)如果两用户的长期私钥泄露而不影响方案的安全,则该方案具有前向安全性。

c)如果两用户的临时私钥泄露而不影响方案的安全,则该方案满足已知会话临时信息安全特性。

d)如果两用户中任意一个的长期私钥泄露而不影响方案安全,则该方案可抗 KCI 攻击。

1)已知密钥安全

因为攻击者(包括 KGC)不知道 A 和 B 每次变化着的暂时私钥(a,b)和长期私钥(x_A,x_B),即使他知道某次的会话密钥,在知道 A、B 各自一个秘密值的情况下,无法同时求出 K_1、K_2、K_3,所以新方案满足已知密钥安全。

2)前向安全

即使两用户的长期私钥 x_A、x_B 泄露给攻击者,攻击者仍然求不出最终的会话密钥,其原因见类型Ⅱ安全中的详细情况分析。

3)无密钥控制

因为计算最终的会话密钥与 a、b、x_A、x_B、D_A、D_B 都相关联,所以无论是 A 还是 B 都无法预先计算出最终的会话密钥,新方案满足无密钥控制特性。

4)抗未知密钥共享

由于新方案使用了签密技术(认证和加密同步进行),新方案满足抗未知密钥共享安全特性。

5)抗密钥泄露伪装攻击

详细分析见类型Ⅰ和类型Ⅲ安全分析中的 c)。因此,新方案抗 KCI 攻击。

6)已知会话临时信息安全

详细分析见类型Ⅲ安全分析。因此,新方案满足已知会话临时信息安全特性。

5　协议比较

新方案无须双线性对操作,在通信过程中,每个合法用户只需要进行三次椭圆曲线上的点乘运算,到目前为止,它是已知无证书安全认证协议中计算复杂性最低的。文献[3~5]都存在 KCI 攻击,尽管文献[11]与新方案一样不存在攻击,但它要比新方案多了 10 次双线性对运算。因此,新方案比本文提到的其他无证书密钥协商方案有明显的性能上的优势,如表 1 所示。

表 1　协议比较

协议	P	E	M	攻击
AP[2]	4 次	1 次	1 次	MA
MT[3]	2 次	1 次	2 次	MA + KCI
SL[4]	1 次	1 次	1 次	MA + KCI
W[5]	1 次	0	3 次	MA + KCI
Lippold[11]	10 次	5 次	5 次	无攻击
新方案	0	0	3 次	无攻击

其中:MA 表示临时私钥泄露产生的攻击;KCI 表示密钥泄露伪装攻击;P 表示双线性对运算;E 表示指数运算;M 表示椭圆曲线上的点乘运算。

6　结束语

新方案无须双线性双线性对操作,与安全无证书密钥协商协议[11]相比,降低了计算复杂度。由于新方案中使用了签密技术,它对伪造攻击增加了一道安全屏障。只要每方保留一个秘密值,只要 CDH 假设成立,那么新方案就是安全的。如何设计标准模型下无双线性双线性对运算的无证书密钥协商方案将是下一步主要研究的新课题。

参考文献:

[1] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Proc of CRYPTO on Advances in Cryptology. Berlin:Springer-Verlag,1984:47-53.

(下转第 4292 页)

其中:$f(x,y)$为载体图像,$f'(x,y)$为隐秘图像。

图6　隐藏效果

当 PSNR > 40 dB 时,8 幅测试图像能够隐藏的信息量及 PSNR 值如表 1 所示。从中可以看出,当 PSNR > 40 dB 时,最低也可以隐藏 145 800 bit,信息隐藏量比较可观。

表 1　PSNR > 40 dB 时信息最低隐藏容量

载图	Lena 密图		Lena 密图		
	隐藏量/bit	PSNR/dB	隐藏量/bit	PSNR/dB	
Lena	156 800	41.069	Boat	168 200	40.119
Camera	145 800	40.656	GoldHills	177 608	40.056
Woman	180 000	40.864	Peppers	177 608	42.177
Wood	177 608	46.193	Zelda	180 000	41.268

以 GoldHills、Zelda 作载体图像,140 × 140 的 Lena、Camera、GoldHills、Boat 作密图为例,隐藏信息后的 PSNR 值如表 2 所示。从纵向看,当 GoldHills 为载图时,隐藏上述 4 幅秘密信息后,PSNR ∈ [44,45];而以 Zelda 为载图时, PSNR ∈ [41,42]。也就是说,同一幅载体图像隐藏相同大小的不同秘密信息后,PSNR 值几乎相等。从横向看,当不同的载体图像隐藏同一秘密信息后,PSNR 值差别很大。从而可以证明,信息的隐藏容量取决于载体图像,而与秘密信息没有关系。

表 2　隐藏相同大小的不同密图的 PSNR 值

密图	GoldHills 载图		Zelda 载图	
	隐藏量/bit	PSNR/dB	隐藏量/bit	PSNR/dB
Lena	156 800	44.625	156 800	41.489
Camera	156 800	44.66	156 800	41.867
GoldHills	156 800	44.579	156 800	41.849
Boat	156 800	44.614	156 800	41.993

3.2　算法对比分析

文献[4]是通过平移直方图峰值点来隐藏信息;而文献[5]虽然信息隐藏量很大,但是对图像的质量影响很大,因此在这里不作比较;文献[6]是利用相邻像素的差值来隐藏信息;而本文提出的算法并非是直接在载体图像的像素灰度值上简单加减 0 或 1。就信息隐藏量而言,从表 3 中可以看出 PSNR ≥ 48.2 dB 时,本文算法的隐藏量都在 60 000 bit 以上,而文献[6]的只有 33 000 bit,文献[4]的隐藏容量最多仅有 14 310 bit。本文算法比文献[6]的隐藏量提升了近一倍,比文献[4]的隐藏量提升了近 6 倍。

表 3　隐藏容量对比

载图	提出算法		文献[6]算法		文献[4]算法	
	PSNR/dB	隐藏量/bit	PSNR/dB	隐藏量/bit	PSNR/dB	隐藏量/bit
Lena	48.624	60 552	48.216	38 088	48.2	5 460
Tiffany	49.293	69 192	48.459	33 800	48.2	8 782
GoldHills	51.349	60 552	48.479	48 672	48.3	14 310
Boat	51.24	75 272	48.395	39 200	48.2	7 301

4　结束语

本文根据双线性插值的思想,提出了一种新的像素灰度值插值方法,并与相邻两像素的相关性相结合,进而提出了一种新的信息隐藏算法。实验结果表明,当 PSNR > 40 dB 时,最低也可以隐藏 145 800 bit。证实了本文提出的算法在相同信噪比的情况下,有较大的信息隐藏能力及很好的不可感知性。

参考文献:

[1] FRIDRICH J, GOLJIAN M, DU Rui. Lossless data embedding: new paradigm in digital watermarking[J]. EURASIP Journal on Applied Signal Process, 2005, 14(2): 253-266.

[2] TIAN J. Reversible data embedding using a difference expansion[J]. IEEE Trans in Circuits and Systems for Video Technology, 2003, 13(8): 890-896.

[3] ADANA M A. Reversible watermarking using difference expansion of quads[C]//Proc of IEEE International Conference on Acoustics, Speech, and Signal Processing. 2004: 1147-1156.

[4] NI Z C, SHI Y, ANSARI N. Reversible data hiding[J]. IEEE Trans on Circuits and System for Video Technology, 2006, 16(3): 354-362.

[5] LIN C C, HSUEH N L. A lossless data hiding scheme based on three-pixel block difference[J]. Pattern Recognition, 2008, 41(4): 1415-1425.

[6] REN Hong-e, CHANG Chun-wu, ZHANG Jian. Image hiding algorithm based on displacement block on odd-even layer[C]//Proc of International Workshop on Chaos-Fractal Theories and Applications. 2009: 186-189.

(上接第 4289 页)

[2] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Proc of ASIACRYPT. 2003: 452-473.

[3] MANDT T K, TAN C H. Certificateless authenticated two-party key agreement protocols[D]. [S. l.]: University of Gjovik, 2006.

[4] SHI Y, LI J. Two-party authenticated key agreement in cerfiticateless public key cryptography[J]. Wuhan University Journal of Natural Sciences, 2007, 12(1): 71-74.

[5] WANG Sheng-bao, CAO Zhen-fu, WANG L. Efficient certificateless authenticated key agreement protocol form pairings[J]. Wuhan University Journal of Natural Sciences, 2006, 11(5): 1278-1282.

[6] 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): 262-270.

[7] GAO Meng, ZHANG Fu-tai. Key-compromise impersonation attacks on some certificateless key agreement protocols and two improved protocols[C]//Proc of the 1st International Workshop on Education Technology and Computer Science. 2009: 62-66.

[8] SWANSON C M. Security in key agreement: two-party certificateless schemes[D]. [S. l.]: University of Waterloo, 2008.

[9] SWANSON C, JAO D. A study of two-party certificateless authenticated key agreement protocols[C]//Proc of INDOCRYPT. Berlin: Springer-Verlag. 2009: 57-71.

[10] LAMACCHIA B A, LAUTER K, MITYAGIN A. Stronger security of authenticated key exchange, cryptology ePrint archive[R/OL]. (2006-07-03). http://eprint.iacr.org/2006/073.

[11] LIPPOLD G, BOYD C, NIETO J G. Stronger secure certificateless key agreement[C]//Proc of Pairing-based Cryptography. Berlin: Springer-Verlag. 2009: 206-230.

[12] MIRACL. Multiprecision integer and rational arithmetic C/C++ library[EB/OL]. http://indigo.ie/mscott/.

[13] XIA L, WANG S, SHEN J, *et al*. Breaking and repairing the certificateless key agreement protocol from ASIAN 2006[J]. Wuhan University Journal of Natural Science, 2008, 13(5): 562-566.