无双线性对的无证书两方认证密钥协商协议

潘 进, 刘小琼, 李国朋
(西安通信学院, 西安 710106)

摘 要: 鉴于双线性对运算复杂度较高,不适用于移动通信环境,提出新的无双线性对的基于无证书的两方认证密钥协商协议。新协议解决了基于身份的公钥密码方案中固有的密钥托管问题,实现了对通信双方的身份认证,采用非双线性对运算,极大地降低了计算开销。通过分析协议的正确性,采用 Applied Pi 演算对协议进行形式化分析,借助 ProVerif 工具验证了协议的安全性和认证性。与其他两方密钥协商协议相比,新方案具有更好的安全性和效率。

关键词: 密钥协商; 无证书密码体制; 无双线性对; Applied Pi 演算; 形式化分析
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2012)06-2240-03
doi:10.3969/j.issn.1001-3695.2012.06.063

Certificateless-based two-party authenticated key agreement protocol

PAN Jin, LIU Xiao-qiong, LI Guo-peng
(*Xi'an Communications Institute*, *Xi'an* 710106, *China*)

Abstract: Because of the high computational cost, bilinear pairing isn't equal to mobile communication environment . This paper proposed new certificateless-based two-party authenticated key agreement protocol without bilinear pairing. The agreement protocol solved the key escrow issues inherited in the identity-based schemes effectively and achieved identity authentication . And the computational cost decreased effectively without bilinear pairing. After confirming the correctness, the formal analysis based on Applied Pi calculus and ProVerif has shown fulfilled authentication and secure. Compared with other two-party authenticated key agreement protocols, the new proposed key agreement protocol has better security and efficiency.
Key words: key agreement; certificateless-based; without bilinear pairing; Applied Pi calculus; formal analysis

0 引言

基于无证书的公钥密码体制(certificateless-based)[1]消除了基于证书的公钥密码体制中复杂的证书管理,还解决了基于身份的公钥密码体制中固有的密钥托管问题,成为了当前研究的热点[2~7]。但是,目前大多数基于无证书的方案都采用了双线性对运算,计算复杂度较高,不适用于节点能量和带宽受限的移动通信环境。基于以上问题,本文在文献[8,9]的基础上,构建了一个适用于移动通信环境的无双线性对的无证书两方认证密钥协商协议,采用文献[10~12]中应用 Pi 演算方法对协议安全性进行了证明。与其他同类方案的分析比较表明,新方案满足目前已知的安全属性,同时保持了良好的性能。

1 密钥协商协议的安全属性[13]

a)已知会话密钥安全。已知旧的会话密钥不会影响到其他会话密钥的安全性。

b)前向安全性。如果一个或多个实体的长期私钥被攻破,以前建立的会话密钥的安全性不受影响。

c)密钥泄露伪装安全。如果 I 的长期私钥被攻破了,攻击者可以伪装成 I,但是不能对 I 伪装成其他实体。

d)未知密钥共享安全。实体 I 不能被迫与实体 C 共享一个会话密钥,而实际上 I 以为他正与实体 R 共享一个会话密钥。

e)已知临时会话信息安全性。临时私钥的泄露不能导致攻击者计算出会话密钥。

2 新的无双线性对的无证书两方认证密钥协商方案

2.1 系统建立

给定安全参数 $k \in N$,KGC 产生如下系统参数:

a)P 为椭圆曲线上循环群 G 中任意一个阶为 q 的生成元,KGC 随机选择主密钥 $x \in Z_q^*$,计算系统公钥 $y = xP$。

b)定义两个哈希函数 $H_1: \{0,1\}^* \times G \longrightarrow Z_q^*$, $H_2: \{0,1\}^* \longrightarrow Z_q^*$。

c)KGC 妥善保管主密钥 x,并公开系统参数 $\{q, P, G, y, H_1, H_2\}$,对任意的合法用户 i,IDi 是其唯一身份标志,KGC 随机选择 $r_i \notin Z_q^*$,计算 $R_i = r_i P$, $D_i = r_i + xH_1(ID_i, R_i)$,并通过安全渠道将 D_i 返回给用户 i 作为其部分私钥,R_i 作为部分公钥公开。

用户 i 随机选择 $x_i \in Z_q^*$ 作为其长期私钥,生成对应的私钥 $\langle x_i, D_i \rangle$,计算 $P_i = x_i P$,生成公钥 (P_i, R_i)。用户 i 可以通过计算等式 $R_i + H_1(ID_i, R_i)y = D_i P$ 是否成立来判断 KGC 分配给自己的私钥是否有效。

2.2 会话密钥协商

约定通信双方分别为 A、B,按图 1 所示过程进行协商。

收稿日期: 2011-10-19; **修回日期**: 2011-11-24

作者简介:潘进(1959-),男,教授,博士,主要研究方向为网络安全与对抗;刘小琼(1985-),女(羌族),四川绵阳人,硕士研究生,主要研究方向为网络安全(xtyliuxiaoqiong@163.com);李国朋(1982-),男,讲师,博士,主要研究方向为网络安全与对抗.

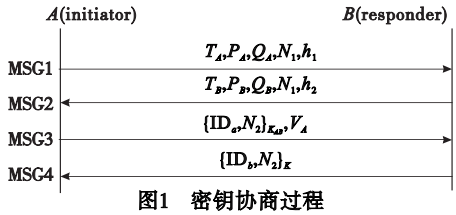

图1　密钥协商过程

a)用户 A 随机选择 $a, N_1 \in Z_q^*$,计算 $Q_A = R_A + H_1(ID_a, R_A)y = D_A P, T_A = aP, P_A = x_a P, h_1 = H_2(T_A, P_A, Q_A, N_1)$ 并向 B 发送消息 $eA_1: \{T_A, P_A, Q_A, N_1, h_1\}$。

b)用户 B 收到消息 eA_1 后,计算 $h_1' = H_2(T_A, P_A, Q_A, N_1)$,并判断 h_1' 与 h_1 是否相等,如果相等则随机选择 $b \in Z_q^*$,计算 $Q_B = R_B + H_1(ID_b, R_B)y = D_B P, T_B = bP, P_B = x_b P, V_B = x_b Q_A, h_2 = H_2(T_B, P_B, V_B, Q_B, N_1)$,并向 A 发送消息 $eB_1: \{T_B, P_B, V_B, Q_B, N_1, h_2\}$。

c)用户 A 收到消息 eB_1 后,计算 $h_2' = H_2(T_B, P_B, V_B, Q_B, N_1)$,并判断其与收到的 h_2 是否相等,如果相等则计算 $K_A = aT_B = abP, KK_A = P_A + P_B = (x_a + x_b)P, V_A = x_a Q_B, K_{AB} = x_a D_A^{-} V_B$,再随机选择 $N_2 \in Z_q^*$,用密钥 K_{AB} 对称加密并向 B 发送消息 $eA_2: (\{N_2, ID_a\}_{K_{AB}}, V_A)$。

d)用户 B 收到消息 eA_2 后,计算 $K_B = bT_A = baP, KK_B = P_B + P_A = (x_b + x_a)P, K_{BA} = x_b D_B^{-} V_A$,再用密钥 K_{BA} 解密 $\{N_2, ID_a\}_{K_{BA}}$ 得到 N_2' 和 IDa'。判断并计算会话密钥 $k = H_2((K_B, KK_B, K_{BA}))$,用会话密钥 k 对称加密 N_2',并向 A 方发送 $eB_2: \{N_2', ID_b\}_k$。

e)用户 A 接收到 B 方发送的消息后,计算会话密钥 $k' = H_2(K_A, KK_A, K_{AB})$,并解密 $\{N_2', ID_b\}_k$ 得到 N_2'' 与 ID_b'。如果 $N_2'' = N_2$,则认为 A 和 B 协商会话密钥 k' 成功,协商过程结束。

2.3　会话密钥的一致性验证

a)分析发起方 A 和响应方 B 分别计算的 K_{AB} 和 K_{BA} 值。

$$K_{AB} = x_a D_A^{-} V_B = x_a D_A^{-} (x_b (D_A P)) = = x_a x_b P$$

$$K_{BA} = x_b D_B^{-} V_A = x_b D_B^{-} (x_a (D_B P)) = x_b x_a P$$

b)分析发起方 A 和响应方 B 分别计算的 K_A 和 K_B 值。

$$K_A = aT_B = abP, K_B = bT_A = baP$$

c)分析发起方 A 和响应方 B 分别计算的 KK_A 和 KK_B 值。

$$KK_A = P_A + P_B = (x_a + x_b)P$$

$$KK_B = P_B + P_A = (x_b + x_a)P$$

又因 G 是阿贝尔群,易知 $K_{AB} = K_{BA} = x_a x_b P, K_A = K_B = abP, KK_A = KK_B = (x_a + x_b)P$。

会话密钥 $k = H_2(abP, (x_a + x_b)P, x_a x_b P)$。

2.4　安全属性分析

a)已知会话密钥安全。由于在产生会话密钥时使用了临时值 (a, b),因此,即使一个会话密钥被敌手获得也不影响以前的或者将来的会话。

b)前向安全性。如果实体 A 和 B 的长期私钥被泄露了,攻击者仍然不知道之前建立的会话密钥,因为计算 K_A 需要知道 a,而计算 K_B 需要知道 b。即使是 PKG 也不能恢复出会话密钥。

c)密钥泄露伪装安全。假设攻击者 E 知道 A 的私钥,并且拦截了 B 传递来的信息,但是 E 仍然无法得到会话密钥,因为计算 K_A 需要知道 a。

d)未知密钥共享安全。如果 A 和 B 协商会话密钥,B 需使用 D_B 来计算会话密钥。因此,C 如果想算出同样的会话密钥,必须得到 D_B,而只有 PKG 和实体 B 知道 D_B,因此 C 无法计算出会话密钥。

e)已知临时会话信息安全性。假设攻击者得到会话的临时秘密值 a 和 b,它仍然无法计算 K_{BA} 和 K_{AB}。但是如果攻击者是 PKG,那么它就能计算出来。此时,会话密钥的安全性则由 KK_A 和 KK_B 来保证,因为 PKG 不知道 x_A 和 x_B 的值。

f)无密钥控制。因为会话密钥的最终计算与 a、b、x_A、x_B、D_A、D_B 都有关,所以无论 A 还是 B 都不能提前预测最终的会话密钥。

3　安全性证明

3.1　协议的应用 Pi 演算模型

采用应用 Pi 演算[14]来形式化建模两方密钥协商过程用到的函数和代数相等关系主要包括:

```
fun  E/2  (对称密钥加密)
reduc  D(x,E(x,y)) = y    (对称密钥解密)
fun  H1/2  (序列与椭圆曲线上元素相乘映射到有限域上一点的函数)
fun  H2/1  (单向散列函数)
fun  f/1  (求倒运算)
fun  f1/2  (群点乘运算)
fun  f2/3  (群点加运算)
fun  f3/2  (数乘运算)
fun  f4/2  (数加运算)
equation  f1(x,f1(y,p)) = f1(y,f1(x,p))
equation  f1(f(x),f1(y,f1(x,p))) = f1(y,p)
```

在以上定义的基础上,可以建立如下协议模型。

I 代表发起方 A 的进程:

```
I = key_A(D_A). va. vN_1. vx_a.
let T_A = f1(a,P) in
let P_A = f1(x_a,P) in
let Q_A = f1(D_A,P) in
    let h_1 = H_2((T_A,P_A,Q_A,N1)) in
c⟨cons1(T_A,P_A,Q_A,N_1,h_1)⟩.
c(cons2(T_B,P_B,V_B,Q_B,N_1,h_2)).
let h_2' = H_2((T_B,P_B,V_B,ID_b,N_1))
if h_2' = h_2 then
    vN2.
let V_A = f1(x_a,Q_B) in
let K_A = f1(a,T_B) in
let KK_A = f2(P_A,P_B) in
let K_AB = f1(x_a,f1(f(D_A),V_B)) in
let e_A = E{K_AB}(N_2,IDa) in
c⟨cons3(e_A,V_A)⟩
c(cons4(e_B))
letk' = H_2((K_A,KK_A,K_AB)) in
let(N_2',ID_b) = D{k'}(e_B) in
ifN_2'' = N_2 then
connect(ID_a,ID_b,k').
```

R 代表响应方 B 的进程:

```
R = key_B(D_B).
c(cons1(T_A,P_A,Q_A,N_1,h_1)).
let h_1' = H_2((T_A,P_A,Q_A,N_1))
if h_1' = h_1 then
vb. vx_B.
let Q_B = f1(D_B,P) in
let T_B = f1(b,P) in
let P_B = f1(x_b,P) in
let K_B = f1(b,T_A) in
let KK_B = f2(P_B,P_A) in
```

let $V_B = f1(x_b, Q_A)$ in
let $h_2 = H_2((T_B, P_B, V_B, Q_B, N_1))$
$\overline{c}\langle cons2(T_B, P_B, V_B, Q_B, N_1, h_2)\rangle$.
$c(cons3(e_A, V_A))$.
let $K_{BA} = f1(x_b, f1(f(D_B), V_A))$ in
let $(N_2', ID_a) = D\{K_{BA}\}(e_A)$ then
letk = $H_2((K_B, KK_B, K_{BA}))$
let $e_B = E\{k\}(N_2')$ in
$\overline{c}\langle cons4(e_B)\rangle$.
$\overline{accept}(ID_a, ID_b, k)$.

系统进程 S 由 I 和 R 进程并发组成,同时包括了 PKG 进程,PKG 进程负责生成用户名及部分公/私钥,并通过私密通道 key_A、key_B 分别来为用户 *A* 和 *B* 分发部分私钥。

S = vIDa. vIDb. vx. vr_A. vr_B.
let $R_A = f1(r_A, P)$ in
let $l_1 = H_1(ID_a, R_A)$
let $D_A = f4(r_A, f3(x, l_1))$ in
$\overline{key_A}\langle D_A\rangle$.
let $R_B = f1(r_B, P)$ in
let $l_2 = H_1(ID_b, R_B)$ in
let $D_B = f4(r_B, f3(x, l_2))$ in
$\overline{key_B}\langle D_B\rangle$.
(! I) | (! R)

3.2 协议的保密性[15]

密钥协商过程中,当敌手无法区分通信双方传递的内容时,即协议满足保密性。对保密性的验证可以被建模为安全属性查询:攻击者能否获得消息中的内容 N_2、ID_a 和 ID_b。通过在自动化工具 ProVerif 中查询(query)以下事实是否成立以实现验证:

query attacker:N_2
query attacker:ID_a
query attacker:ID_b

输出结果如图 2 所示。

图2 协议的保密性与身份保护验证结果

由图 2 可知,ProVerif 的输出结果为 true,表明即使存在主动攻击,该协议也能够满足保密性;同时,由于身份也是加密传输,因此也实现了协商双方的身份保护。

3.3 协议的认证性[15]

密钥协商过程中,通信双方能够确认彼此的身份,即双方在确认了对方身份后再完成会话密钥的生成。协议认证性的证明也通过自动化工具 ProVerif 完成,查询语句如下:

query ev:BfinishedA(k) ==> ev:BverifA(ID_a)
query ev:AfinishedB(k) ==> ev:AverifB(N_2)&
(ev:BfinishedA(k) ==> ev:BverifA(ID_a))

输出结果如图 3 所示。

由图 3 可知,ProVerif 的输出结果为 true,表明通信双方互相确认了对方的身份,该协议满足认证性。

4 性能分析

协议的性能主要从信息交换的次数、需要传输信息的大小和执行运算的复杂度等方面来考虑。该密钥协商方案通过采用无双线性对的方法来实现两个节点用户之间带密钥确认的认证密钥协商,其开销如表 1 所示。

图3 协议的认证性验证结果

表 1 各方案的性能比较

方案性能	文献[5]	文献[6]	文献[8]	文献[9]	本文方案
双线性对运算	1	1	0	0	0
椭圆曲线上点乘运算	3	5	5	3	2

考虑到性能,双线性对、指数运算分别为点乘的 20 倍、3 倍[11],由表 1 可以看出,本文方案在保证协议安全性的同时,极大地降低了计算开销。

5 结束语

本文提出一个基于无双线性对的无证书两方认证密钥协商方案,解决了传统基于身份的密钥协商方案中固有的密钥托管问题,通过基于应用 Pi 演算的形式化分析方法,证明了协议具有私密性和认证性。性能分析表明,该方案在安全性和效率方面具有较大优势,更加适合于能量和带宽受限的移动通信环境。下一步将研究其性能优化和实际应用。

参考文献:

[1] Al-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Advances in Cryptology-ASIACRYPT'03. Berlin: Springer-Verlag, 2003: 452-473.

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

[3] MANDT T K, TAN C H. Certificateless authenticated two-party key agreement protocols[C]//Proc of the 11th Asima Computing Science Conference on Advances in Computer Science: Secure Software and Related Issues. Berlin: Springer-Verlag, 2008: 37-44.

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

[5] WANG Sheng-bao, CAO Zhen-fu, BAO Hai-yong. Efficient certificateless authentication and key agreement (CL-AK) for grid computing[J]. International Journal of Network Security, 2008, 7(3): 342-347.

[6] 朱志馨,董晓蕾. 高效安全的无证书密钥协商方案[J]. 计算机应用研究, 2009, 26(12): 4787-4789.

[7] 侯孟波,徐秋亮,蒋瀚. 构建无证书的两方认证密钥协商协议[J]. 计算机工程与应用, 2010, 46(8): 1-4.

[8] 曹雪菲,寇卫东,樊凯,张军. 无双线性对的基于身份的认证密钥协商协议[J]. 电子与信息学报, 2009, 31(5): 1241-1244.

[9] 刘文浩,许春香. 无双线性对的无证书两方密钥协商方案[J]. 计算机应用研究, 2010, 27(11): 4287-4290. (下转第 2267 页)

(上接第 2242 页)

[10] 韩明奎,潘进,李波. 一种改进的 IKEv2 协议及其形式化验证[J]. 计算机应用研究,2010,27(2):707-711.

[11] 陈安林,潘进,徐邢启,等. MANET 中可认证组密钥协商协议及验证[J]. 电脑知识与技术,2010,6(32):8966-8969.

[12] 陈安林,潘进,郭超,等. 移动自组网中跨域两方认证密钥协商协议研究[J]. 计算机应用研究,2011,28(7):2734-2737.

[13] ABADI M, FOURNET C. Mobile values, new names and secure communication [C]//Proc of the 28th ACM Symposium on Principles of Programming Languages. New York: ACM Press, 2001: 104-115.

[14] ABADI M, BLANCHET B. Analyzing security protocols with secrecy types and logic programs[J]. Journal of the ACM, 2005, 52(1): 102-146.

[15] 赵华伟,李大兴. 密钥交换协议的安全性分析[J]. 山东大学学报:理学版, 2006,41(4):101-106.

[16] BLAKE-WILSON S, JOLMSON D, MENEZES A. Key agreement protocols and their security analysis[C]//Proc of the 6th IMA International Conference on Cryptography and Coding. Berlin: Springer-Verlag, 1997:30-45.